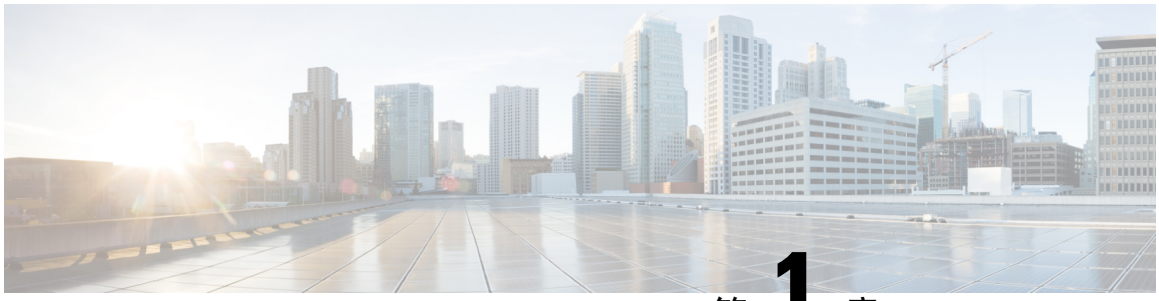
Cisco身份服务引擎管理员指南，版本 3.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

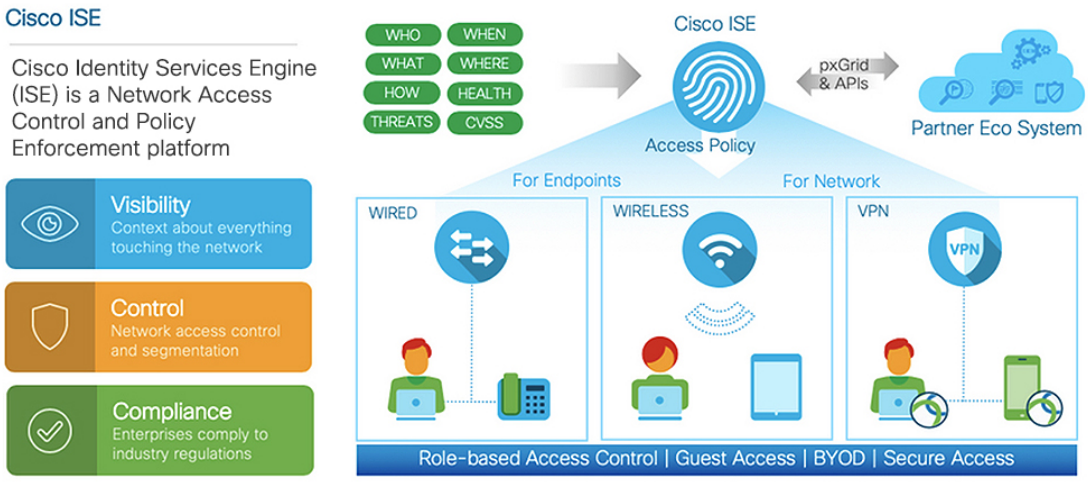
目录



第 1 章

概述

思科 ISE 概述



Cisco身份服务引擎 (ISE) 是一个基于身份的网络访问控制和策略实施系统。它作为一个通用策略引擎，让企业能够控制终端访问和管理网络设备。

您可以利用Cisco ISE 确保合规、增强基础设施安全性并简化服务操作。

Cisco ISE管理员可以收集网络的实时情景数据，包括用户和用户组（谁？）、设备类型（什么？）、访问时间（何时？）、访问位置（哪里？）、访问类型（有线、无线或 VPN）（如何？）以及网络威胁和漏洞。

作为Cisco ISE 管理员，您可以使用此信息制定网络监管决策。您还可以将身份数据与各种网络元素绑定，以创建监管网络访问和使用的策略。

思科 ISE 功能

Cisco ISE 软件必须按原样安装。不能在底层操作系统级别安装任何其他第三方应用。

Cisco ISE 为您提供以下功能：

- **设备管理 (Device Administration)**：Cisco ISE 使用 TACACS+ 安全协议来控制和审核网络设备的配置。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。网络设备可以配置为向Cisco ISE 查询对设备管理员操作所进行的身份验证和授权。这些设备还会向Cisco ISE 发送记账消息，以记录此类操作。
- **访客和安全无线 (Guest and Secure Wireless)**：Cisco ISE 使您能够为访客、承包商、顾问和客户提供安全的网络访问。您可以使用基于 Web 的门户和移动门户将访客加入公司的网络和内部资源。您可以为不同类型的访客定义访问权限，并分配发起人以创建和管理访客帐户。
- **自带设备 (BYOD) (Bring Your Own Device [BYOD])**：Cisco ISE 可以让您的员工和访客在企业网络上安全地使用他们的个人设备。BYOD功能的最终用户可以使用所配置的路径添加其设备，并调配预定义的身份验证和网络访问级别。
- **资产可视性 (Asset Visibility)**：Cisco ISE 在无线连接、有线连接和 VPN 连接中提供一致的可视性，并控制网络上的人员和内容。Cisco ISE 使用探测器和设备传感器来侦听设备连接到网络的方式。然后，庞大的Cisco ISE 配置文件数据库将对设备进行分类。这可以提供您所需要的可视性和情景，以便授予适当级别的网络访问权限。
- **安全有线访问 (Secure Wired Access)**：Cisco ISE 使用各种身份验证协议为网络设备和终端提供安全的有线网络访问。这些协议包括但不限于802.1X、RADIUS、MAB、基于Web、EasyConnect 和启用外部代理的身份验证方法。
- **分段 (Segmentation)**：Cisco ISE 使用有关网络设备和终端的情景数据来促进网络分段。安全组标记、访问控制列表、网络访问协议，以及用来定义授权、访问和身份验证的策略集是Cisco ISE 实现安全网络分段的一些方式。
- **终端安全评估或合规性 (Posture or Compliance)**：Cisco ISE 可以让您检查终端的合规性（也称为终端安全评估），然后再允许它们连接您的网络。您可以确保终端接收适当的终端安全评估代理以提供终端安全评估服务。
- **威胁遏制 (Threat Containment)**：如果Cisco ISE 检测到来自终端的威胁或漏洞属性，则发送自适应网络控制策略以动态更改其终端访问级别。在评估并解决威胁或漏洞后，终端将获得其原始访问策略。
- **安全生态系统集成 (Security Ecosystem Integrations)**：通过 pxGrid 功能，Cisco ISE 可以与相连的网络设备、第三方供应商或Cisco合作伙伴系统安全地共享情景相关信息、策略和配置数据等。

思科 ISE 管理员

管理员可使用管理员门户执行下列操作：

- 管理部署、服务中心操作、网络设备以及节点监控和故障排除。
- 管理Cisco ISE 服务、策略、管理员帐户以及系统配置和操作。
- 更改管理员和用户密码。

CLI 管理员可以启动和停止Cisco ISE 应用、应用软件补丁和升级、重新加载或关闭Cisco ISE 设备，以及查看所有系统和应用日志。由于授予 CLI 管理员的特殊权限，建议您保护 CLI 管理员凭证并创建基于 Web 的管理员来配置和管理Cisco ISE 部署。

在设置过程中配置的用户名和密码仅用于对 CLI 进行管理访问。此角色被视为 CLI 管理员用户，也称为CLI管理员。默认情况下，CLI管理员用户的用户名为admin，密码是设置过程中定义的密码。没有默认密码。此 CLI 管理员用户是默认管理员用户，无法删除此用户帐户。不过，其他管理员可以编辑此用户帐户，包括启用、禁用或更改此帐户密码的选项。

可以创建管理员，也可以将现有用户升级为管理员角色。通过禁用对应的管理权限，还可以将管理员降级为简单网络用户状态。

管理员是具有配置和操作Cisco ISE 系统的本地权限的用户。

管理员会分配到一个或多个管理员组。

相关主题

思科 ISE 管理员组，第 5 页

强制 CLI 管理员使用外部身份存储库

使用外部身份源进行身份验证比使用内部数据库更安全。适用于 CLI 管理员的 RBAC 支持外部身份库。

必备条件

您必须已定义管理员用户，并将其添加到管理员组。管理员必须是超级管理员。

在 AD 用户目录中定义用户的属性

在运行 Active Directory 的 Windows 服务器上，修改您计划配置为 CLI 管理员的每个用户的属性。

1. 打开服务器管理器窗口，然后导航至**服务器管理器 (Server Manager) > 角色 (Roles) > Active Directory 域服务 (Active Directory Domain Services) > Active Directory 用户和计算机 (Active Directory Users and Computers) > [ad.adserver]<ad_server> .local**。
2. 在**视图 (View)** 菜单下启用**高级功能 (Advanced Features)**，以便您编辑用户的属性。
3. 导航至包含管理员用户的 Active Directory 组，并找到该用户。

4. 双击用户以打开**属性 (Properties)** 窗口并选择**属性编辑器 (Attribute Editor)**。
5. 点击任意属性并开始键入“gid”以查找属性 `gidNumber`。如果找不到gidNumber属性，请点击**过滤器 (Filter)** 按钮并取消选中**仅显示具有值的属性 (Show only attributes that have values)**。
6. 双击属性名称以编辑每个属性。对于每个用户：
   - 分配大于 60000 的 `uidNumber`，并确保该数字是唯一的。
   - 将 `gidNumber` 分配为 110 或 111。
   - GidNumber 110 表示管理员用户，而 111 表示只读用户。
   - 请勿在分配后更改 uidNumber。
   - 如果修改 gidNumber，请至少等待五分钟，然后再建立 SSH 连接。

将管理员 CLI 用户加入 AD 域

连接到Cisco ISE CLI，运行 **identity-store** 命令，并将管理员用户分配到 ID 存储区。例如，要将 CLI 管理员用户作为 adpool1 映射到 ISE 中定义的 Active Directory，请运行 **identity-store active-directory domain-name adpool1 user admincliuser**。

完成加入后，连接到Cisco ISE CLI 并以管理员 CLI 用户身份登录，验证您的配置。

如果在此命令中使用的域之前已加入 ISE 节点，则必须在管理员控制台中重新加入该域。

1. **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources)**。
2. 在左侧窗格中，选择 **Active Directory** 并选择您的 Active Directory 名称。
3. 在右侧窗格中，您的 AD 连接的状态可能显示**运行 (Operational)**。但是，如果使用 MS-RPC 或 Kerberos，通过**测试用户 (Test User)** 测试连接，则会收到错误。
4. 验证您是否仍可以用管理员 CLI 用户身份登录Cisco ISE CLI。

创建新管理员

Cisco ISE 管理员需要分配有特定角色的帐户才能执行特定管理任务。可以创建管理员帐户，并根据管理员必须执行的管理任务向这些管理员分配一个或多个角色。

可以使用**管理员用户 (Admin Users)** 窗口查看、创建、修改、删除、复制或搜索Cisco ISE 管理员的属性或更改其状态。

注释 如果管理员用户的域在 CLI 和 GUI 中相同，建议您先在 CLI 中配置 Active Directory 访问权限，然后再将其加入 GUI。另外，必须从 GUI 重新加入域，以避免此域发生身份验证失败。

步骤 1 选择 管理 **(Administration)** > 系统 **(System)** > 管理员访问权限 **(Admin Access)** > 管理员 **(Administrators)** > 管理员用户 **(Admin Users)** > 添加 **(Add)**。

步骤 2 管理 **(Administration)** > 系统 **(System)** > 管理员访问权限 **(Admin Access)** > 管理员 **(Administrators)** > 管理员用户 **(Admin Users)** > 添加 **(Add)**

步骤 3 从下拉列表中，选择以下选项之一：

- **创建管理员用户 (Create an Admin User)**

  如果选择**创建管理员用户 (Create an Admin User)**，将显示**新建管理员 (New Administrator)** 窗口，从中可配置新管理员用户的帐户信息。

- **从网络访问用户选择 (Select from Network Access Users)**

  如果选择**从网络访问权限用户中选择 (Select from Network Access Users)**，将显示当前用户列表，从中可创建用户。将显示与此用户对应的**管理员用户 (Admin User)** 窗口。

步骤 4 在字段中输入值。**名称 (Name)** 字段支持的字符为 # $ ’ ( ) * + -。/ @ _。

管理员用户名必须唯一。如果输入了现有用户名，错误弹出窗口将显示以下消息：

无法创建用户。已存在具有相同名称的用户。(User can't be created. A User with that name already exists.)

步骤 5 点击**提交 (Submit)** 在Cisco ISE 内部数据库中创建新管理员。

相关主题

只读管理员策略，第 20 页
创建内部只读管理员，第 442 页
自定义只读管理员的菜单访问权限，第 20 页
将外部组映射至只读管理员组，第 442 页

思科 ISE 管理员组

管理员组是CiscoISE中基于角色的访问控制（RBAC）组。属于同一组的所有管理员共用同一身份并且具有相同的权限。管理员作为特定管理组成员的身份可用作授权策略中的条件。管理员可以属于不止一个管理员组。

具有任何访问权限级别的管理员帐户可以在其有权访问的任何窗口上，修改或删除其拥有权限的对象。

在Cisco ISE 安全模式下，管理员只能创建与其具有相同权限集的管理组。提供的权限基于Cisco ISE 数据库中定义的用户管理角色。这样，管理组就形成了定义访问Cisco ISE 系统的权限的依据。

下表列出了Cisco ISE 中预定义的管理组以及这些组成员可以执行的任务。

表 *1:* 思科 *ISE* 管理员组、访问级别、权限和限制

管理组角色	访问级别	权限	限制
自定义管理员	管理发起人、访客和个人设备门户。	• 配置访客和发起人访问权限。 • 管理访客访问设置。 • 自定义最终用户 Web 门户。	• 无法在Cisco ISE 中执行任何策略管理、身份管理或系统级别配置任务。 • 无法查看任何报告
帮助台管理员	查询监控和故障排除操作	• 运行所有报告。 • 运行所有故障排除流程。 • 查看Cisco ISE 控制板和实时日志。 • 查看警报。	无法创建、更新或删除报告、故障排除流程、实时身份验证或警报。
身份管理员	• 管理用户帐户和终端。 • 管理身份源。	• 添加、编辑和删除用户帐户和终端。 • 添加、编辑和删除身份源。 • 添加、编辑和删除身份源序列。 • 为用户帐户配置常规设置（属性和密码策略）。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。	无法在Cisco ISE 中执行任何策略管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
MnT 管理员	执行所有监控和故障排除操作。	• 管理所有报告（运行、创建和删除）。 • 运行所有故障排除流程。 • 查看Cisco ISE 控制板和实时日志。 • 管理警报（创建、更新、查看和删除）。	无法在Cisco ISE 中执行任何策略管理、身份管理或系统级别配置任务。
网络设备管理员	管理Cisco ISE 网络设备和网络设备存储库。	• 对网络设备拥有读写权限 • 对网络设备组和所有网络资源对象类型拥有读写权限。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。	无法在Cisco ISE 中执行任何策略管理、身份管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
策略管理员	为所有与身份验证、授权、终端安全评估、分析器和客户端调配和工作中心有关的跨网络 Cisco ISE 服务创建和管理策略。	• 对策略中使用的所有元素（例如授权配置文件、NDG 和条件）拥有读写权限。 • 对身份、终端和身份组（用户身份组和终端身份组）拥有读写权限。 • 对服务策略和设置拥有读写权限。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。 • 设备管理 - 对设备管理工作中心拥有访问权限。对 TACACS 策略条件和结果拥有权限。TACACS 代理和代理序列的网络设备权限。	无法在Cisco ISE 中执行任何身份管理或系统级别配置任务 设备管理 - 能够访问工作中心并不保证能够访问从链路。

管理组角色	访问级别	权限	限制
RBAC 管理员	**操作 (Operations)** 菜单下除终端保护服务 (Endpoint Protection Services) 自适应网络控制 (Adaptive Network Control) 之外的所有任务，以及对**管理 (Administration)** 下某些菜单项的部分访问权限。	• 查看身份验证详细信息。 • 启用或禁用终端保护服务 (Endpoint Protection Services) 自适应网络控制 (Adaptive Network Control) • 创建、编辑和删除警报；生成和查看报告；以及使用 Cisco ISE 对网络中的问题进行故障排除。 • 对管理员帐户设置和管理组设置拥有读取权限 • 对管理员访问和数据访问权限以及 RBAC 策略页面拥有查看权限。 • 查看Cisco ISE 控制板、实时日志、警报和报告。 • 运行所有故障排除流程。	无法在Cisco ISE 中执行任何身份管理或系统级别配置任务

管理组角色	访问级别	权限	限制
只读管理员	对 ISE GUI 拥有只读访问权限。	• 查看并使用控制板、报告以及实时日志或会话的功能，例如过滤数据、查询、保存选项、打印和输出数据。 • 更改其自有帐户的密码。 • 使用全局搜索、报告以及实时日志或会话查询 ISE。 • 基于属性过滤并保存数据。 • 导出与身份验证策略、配置文件策略、用户、终端、网络设备、网络设备组、身份（包括组）及其他配置相关的数据。 • 自定义报告查询，保存、打印和导出这些查询。 • 生成自定义报告查询，保存、打印或导出结果。 • 保存UI设置以供将来参考。 • 从以下位置下载 ise-psc-log 等日志：**操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** 窗口。	

管理组角色	访问级别	权限	限制
			• 对各种对象（例如授权策略、身份验证策略、终端安全评估策略、分析器策略、终端和用户）执行任何配置更改，例如创建、更新、删除、导入、隔离以及移动设备管理 (MDM) 操作。 • 执行系统操作，例如备份和恢复；节点注册或注销；节点同步；创建、编辑和删除节点组；或升级和安装补丁。 • 导入与策略、网络设备、网络设备组、身份（包括组）及其他配置相关的数据。 • 执行操作，例如 CoA、终端调试、修改收集过滤器、绕过实时会话数据的抑制、修改 PAN-HA 故障转移设置，以及编辑 Cisco ISE 节点的角色或服务。 • 运行可能会对性能造成严重影响的命令。例如，访问**操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断 (Diagnostic)** > **常规工具 (General Tools)** 窗口中的 TCP

管理组角色	访问级别	权限	限制
			转出会受限制。 • 生成支持捆绑包。
超级管理员	所有Cisco ISE 管理功能。默认管理员帐户属于此组。	对所有Cisco ISE 资源拥有创建、读取、更新、删除和执行 (CRUDX) 权限。 **注释** 超级管理员用户无法修改系统生成的默认 RBAC 策略和权限。要执行此操作，您必须根据您的需要利用必要的权限创建新的 RBAC 策略，并且将这些策略映射至管理员组。 设备管理 - 对设备管理工作中心的访问权限。 对 TACACS 策略条件和结果拥有权限。 TACACS 代理和代理序列的网络设备权限。此外，启用 TACACS 全局协议设置的权限。	• 设备管理 - 能够访问工作中心并不保证能够访问从属链接。 • 只有默认超级管理员组的管理员用户才能修改或删除其他管理员用户。即使是管理员组中克隆有超级管理员组的菜单和数据访问权限的外部映射用户也无法修改或删除管理员用户。

管理组角色	访问级别	权限	限制
系统管理员	所有Cisco ISE 配置和维护任务。	拥有执行**操作 (Operations)** 选项卡下所有活动的完全访问权限（读写权限），以及对**管理 (Administration)** 选项卡下某些菜单项的部分访问权限： • 对管理员帐户设置和管理员组设置拥有读取权限。 • 对管理员访问和数据访问权限以及 **RBAC 策略 (RBAC policy)** 窗口拥有读取权限。 • 对以下位置下方的所有选项拥有读取和访问权限： **管理 (Administration)** > **系统 (System)**。 • 查看身份验证详细信息。 • 启用或禁用终端保护服务 (Endpoint Protection Services) 自适应网络控制 (Adaptive Network Control) • 创建、编辑和删除警报；生成和查看报告；以及使用 Cisco ISE 对网络中的问题进行故障排除。 • 设备管理 - 启用 TACACS 全局协议设置的权限。	无法在Cisco ISE 中执行任何策略管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
升级的系统管理员（在 Cisco ISE 版本 2.6 补丁 2 及更高版本中提供）	所有Cisco ISE 配置和维护任务。	除了系统管理员的所有权限外，升级的系统管理员还可以创建管理员用户。	• 无法创建或删除超级管理员用户。 • 无法管理超级管理员组。
外部 RESTful 服务 (ERS) 管理员	对所有 ERS API 请求（GET、POST、DELETE、PUT）的完全访问权限	• 创建、读取、更新和删除 ERS API 请求。	此角色仅适用于支持 ERS 授权的内部用户、身份组、终端、终端组和 SGT
外部 RESTful 服务 (ERS) 运算符	对 ERS API、仅 GET 的只读访问权限	• 只能读取 ERS API 请求	此角色仅适用于支持 ERS 授权的内部用户、身份组、终端、终端组和 SGT。
TACACS+ Admin	完全访问权限	访问： • 设备管理工作中心。 • 部署 - 启用 TACACS+ services。 • 外部身份存储库。 • **操作 (Operations)** > **TACACS 实时日志 (TACACS Live Logs)** 窗口。	—

相关主题

思科 ISE 管理员，第 3 页

创建管理员组

管理员组 (Admin Groups) 窗口允许您查看、创建、修改、删除、复制或过滤Cisco ISE 网络管理员组。

开始之前

要配置外部管理员组类型，您必须已经指定了一个或多个外部身份库。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**。

步骤 2 点击**添加 (Add)**，并输入名称和说明。

名称 (Name) 字段支持的特殊字符包括：空格、# $ & ‘ ( ) * + -。/ @ _。

步骤 3 指定您所配置的管理员组类型：

- 内部 (Internal)：分配到此组类型的管理员将对存储在Cisco ISE 内部数据库中的凭证进行身份验证。
- 外部 (External)：分配给此组的管理员根据您在**管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 身份验证 (Authentication) > 身份验证方式 (Authentication Method)** 窗口中选择的外部身份库中存储的凭证进行身份验证。如果需要，您可以指定外部组。

如果内部用户配置了用于身份验证的外部身份库，则在登录到 ISE 管理员门户时，内部用户必须选择外部身份库作为**身份源**。如果选择了**内部身份源 (Internal Identity Source)**，身份验证将失败。

步骤 4 点击**成员用户 (Member Users)** 区域中的**添加 (Add)** 将用户添加到此管理员组。

步骤 5 点击 **提交 (Submit)**。

要删除管理员组中的用户，请选中您希望删除的用户所对应的复选框，并点击**删除 (Remove)**。

对思科 ISE 的管理访问

Cisco ISE 管理员可以根据其所属的管理组执行各种管理任务。这些管理任务至关重要。仅向有权在网络中管理 Cisco ISE 的用户授予管理访问权限。

利用Cisco ISE，您可以通过以下选项控制对其 Web 界面的管理访问。

注释 当将Cisco ISE服务器添加到网络时，一旦其Web界面出现，它就会被标记为处于运行状态。但是，由于一些高级服务（如终端安全评估服务）可能需要更长的时间才能完全可用，因此可能需要更多时间才能使所有服务完全运行。

管理访问方法

有多种方式可以连接到 Cisco ISE 服务器。PAN 运行管理员门户，需要管理员密码才能登录。其他 ISE 角色服务器可通过 SSH 或控制台（在其中运行 CLI）进行访问。本节介绍可用于每种连接类型的进程和密码选项。

- **管理员密码**：默认情况下，安装期间创建的 Cisco ISE 管理员用户在 45 天内超时。为防止此情况，可以在以下位置通过关闭密码有效期： **管理 (Administration)** > **系统 (System)** > **管理设置 (Admin Settings)**。点击**密码策略 (Password Policy)** 选项卡，并取消选中**密码有效期 (Password Lifetime)** 下的**管理密码到期 (Administrative passwords expire)**。

如果不执行此操作，当密码到期时，可以在 CLI 中运行 **application reset-passwd** 命令以重置管理员密码。要重置管理密码，可以连接至控制台以访问 CLI，或重新引导 ISE 映像文件以访问引导选项菜单。

- **CLI 密码 (CLI password)**：必须在安装期间输入 CLI 密码。如果在登录 CLI 时因密码无效而遇到问题，可以重置 CLI 密码。连接至控制台，并运行 **password** CLI 命令以重置密码。有关详细信息，请参阅《*ISE CLI* 参考》。
- **SSH 访问 CLI (SSH access to the CLI)**：可以在安装期间或安装后使用 **service sshd** 命令启用 SSH 访问。还可以强制 SSH 连接使用密钥。请注意，在执行此操作时，SSH 与所有网络设备的连接也会使用此密钥，请参阅SSH 密钥验证，第 922 页。可以强制 SSH 密钥使用 Diffie-Hellman 算法。请注意，SSH 密钥不支持 ECDSA 密钥。

思科 ISE 中基于角色的管理员访问控制

Cisco ISE 提供角色型访问控制 (RBAC) 策略，通过限制管理权限确保安全性。RBAC 策略与默认管理组关联，以定义角色和权限。每个预定义管理组都配有一套标准权限（适用于菜单和数据访问），因此，与关联的角色和工作职能保持一致。

用户界面中的某些功能要求具备特定权限才可使用。如果功能不可用，或者不允许您执行特定任务，您的管理组可能没有执行利用此功能的任务所需的权限。

无论访问权限级别如何，任何管理员帐户都可以在任何它能够访问的页面上，修改或删除其拥有权限的对象。

注释 只有具有超级管理员或只读管理员权限的系统定义管理员用户才能查看不属于用户组的基于身份的用户。如果创建的管理员没有这些权限，将无法看到这些用户。

基于角色的权限

Cisco ISE 允许您在菜单和数据级别配置权限：它们称为菜单访问权限和数据访问权限。

菜单访问权限允许您显示或隐藏Cisco ISE 管理界面的菜单项和子菜单项。您可以通过此功能创建权限，从而限制或允许菜单级别的访问。

通过数据访问权限，您可以允许读/写访问、只读访问或禁止访问Cisco ISE 界面中以下数据：管理员组 (Admin Groups)、用户身份组 (User Identity Groups)、终端身份组 (Endpoint Identity Groups)、位置 (Locations) 和设备类型 (Device Types)。

RBAC 策略

RBAC 策略确定是否可以授予管理员对菜单项或其他身份组数据元素的特定类型的访问权限。可以使用 RBAC 策略基于管理员组向管理员授予或拒绝对菜单项或身份组数据元素的访问权限。当管理员登录到管理门户时，他们可以访问基于为与其关联的管理员组定义的策略和权限的菜单和数据。

RBAC 策略将管理员组映射到菜单访问权限和数据访问权限。例如，您可以防止网络管理员查看 Admin Access 操作菜单和策略数据元素。通过为与网络管理员关联的管理员组创建自定义 RBAC 策略，可以实现此目的。

注释 如果使用自定义 RBAC 策略授予或拒绝管理员访问权限，请确保对给定的数据访问权限提供所有相关的菜单访问权限。例如，要添加或删除具有身份或策略管理员数据访问权限的终端，必须提供对**工作中心 (Work Center)** > **网络访问 (Network Access)** 以及**管理 (Administration)** > **身份管理 (Identity Management)** 的菜单访问权限。

默认菜单访问权限

Cisco ISE 提供一组与一系列预定义的管理员组相关联的现成权限。通过预定义管理员组权限，您可以设置权限，以便任意管理员组的成员可以完全或有限地访问管理界面中的菜单项（称为菜单访问权限）和委派管理员组使用其他管理员组的数据访问要素（称为数据访问权限）。这些权限可进一步用于制定多种管理员组的 RBAC 策略的可重用的实体。Cisco ISE 提供已用于默认 RBAC 策略的一组系统定义的菜单访问权限。除了预定义的菜单访问权限外，Cisco ISE 还允许您在 RBAC 策略中使用的自定义菜单访问权限。钥匙图标表示菜单和子菜单的菜单访问权限，带叉号的钥匙图标表示不同 RBAC 组不可访问的菜单项。

注释 对于超级管理员用户，所有菜单项均可用。对于其他管理员用户，**菜单访问权限 (Menu Access Privileges)** 列中的所有菜单项均可供独立部署及分布式部署中的主要节点使用。对于分布式部署中的辅助节点，**“管理”(Administration)** 选项卡下的菜单项不可用。

配置菜单访问权限

Cisco ISE 允许创建可映射到 RBAC 策略的自定义菜单访问权限。根据管理员的角色，您可以仅允许其访问特定菜单选项。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **权限 (Permissions)** > **菜单访问 (Menu Access)**。

步骤 2 点击**添加 (Add)**，输入**名称 (Name)** 和**说明 (Description)** 字段的值。

a) 将 **ISE 导航结构 (ISE Navigation Structure)** 菜单展开至所需级别，然后点击要为其创建权限的选项。

b) 在**菜单访问的权限 (Permissions for Menu Access)** 窗格中，点击**显示 (Show)**。

步骤 3 点击**提交 (Submit)**。

授予数据访问权限的先决条件

当RBAC管理员对某个对象（例如，用户身份组数据类型的Employee）具有完全访问权限时，管理员可以查看、添加、更新和删除属于该组的用户。确保管理员已为**用户 (Users)** 窗口（**管理**

[Administration] > 身份管理 [Identity Management] > 身份 [Identities] > 用户 [Users]）授予菜单访问权限。这适用于网络设备和终端对象（基于授予网络设备组和终端身份组数据类型的权限）。

不能对属于默认网络设备组对象（**所有设备类型 [All Device Types]** 和**所有位置 [All Locations]**）的网络设备启用或限制数据访问。如果向在这些默认网络设备组对象下创建的对象授予完全访问数据权限，则显示所有网络设备。因此，我们建议您为网络设备组数据类型创建一个独立于默认网络设备组对象的单独层次结构。您应将网络设备对象分配给新创建的网络设备组，以创建受限访问。

注释 只能为用户身份组、网络设备组和终端身份组启用或限制数据访问权限，而不能为管理员组启用或限制数据访问权限。

默认数据访问权限

Cisco ISE 具有一系列预定义的数据访问权限。这些权限允许多名管理员在同一个用户群中具有数据访问权限。您可以启用数据访问权限或将其限制在一个或更多管理员组范围。此过程允许向一个管理员组的管理员授予自主委派控制，通过选择性关联允许所选管理员组重复使用数据访问权限。对于查看所选管理员组或网络设备组，数据访问权限范围从完全访问权限直到无访问权限。通过基于策略的管理员（RBAC）组菜单访问和数据访问权限定义。您应首先创建菜单访问和数据访问权限，然后创建将管理员组与对应菜单访问和数据访问权限关联的 RBAC 策略。RBAC 策略采用以下形式：If admin_group=Super Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission。除了预定义的数据访问权限外，Cisco ISE 还允许您创建可与 RBAC 策略的自定义数据访问权限。

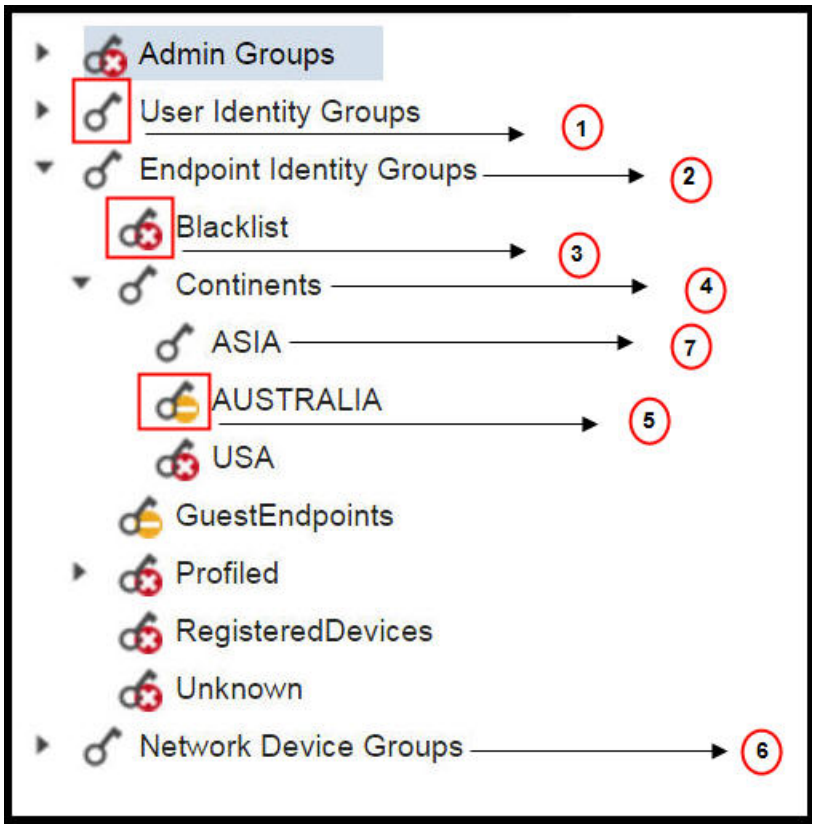
可向管理员组授予三种数据访问权限，即完全访问权限、无访问权限和只读访问权限。

只读访问权限可授予以下管理员组：

- 管理 (Administration) > 管理员访问权限 (Admin Access) > 管理员 (Administrators) > 管理员组 (Admin Groups)
- 管理 (Administration) > 组 (Groups) > 用户身份组 (User Identity Group)
- 管理 (Administration) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)
- 网络可视性 (Network Visibility) > 终端 (Endpoints)
- 管理 (Administration) > 网络资源 (Network Resources) > 网络设备组 (Network Device Groups)
- 管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)
- Administration（管理）> Identity Management（身份管理）> Identities（身份）
- 管理 (Administration) > 身份管理 (Identity Management) > 用户身份组 (User Identity Groups)
- 管理 (Administration) > 身份管理 (Identity Management) > 终端身份组 (Endpoint Identity Groups)

如果您对某一数据类型（例如，终端身份组）具有只读访问权限，则无法对该数据类型执行 CRUD 操作。如果您对某对象具有只读访问权限（例如，GuestEndpoints），则无法对该对象执行编辑/删除操作。

图 *1:* 下图描述了如何在包含不同 ***RBAC*** 组的其他子菜单或选项的第二或第三级菜单中应用数据访问权限。



编号	说明
1	表示用户身份组数据类型的完全访问权限。
2	表示终端身份组派生授予其子项（亚洲）的最大权限（完全访问权限）。
3	表示对该对象无访问权限（阻止列表）。
4	表示父项（大洲）获得授予其子项（亚洲）的最大访问权限。
5	表示对对象的（澳大利亚）的只读访问权限。
6	表示向父项（网络设备组）授予完全访问权限时，会导致子项自动继承权限。
7	表示向父项（亚洲）授予完全访问权限时，会导致对象继承完全访问权限，除非明确授予对象权限。

配置数据访问权限

通过Cisco ISE，可以创建自定义数据访问权限，并将其映射到 RBCA 策略。根据管理员的角色，可以选择仅为他们提供选择数据的访问权限。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **权限 (Permissions)**。

步骤 2 选择**权限 (Permissions)** > **数据访问 (Data Access)**。

步骤 3 点击**添加 (Add)**，输入名称 和 说明 字段的值。

a) 点击以展开管理员组，选择所需的管理员组。

b) 点击**完全访问 (Full Access)**、**只读权限 (Read Only Access)** 或 **不能访问 (No Access)**。

步骤 4 点击**保存 (Save)**。

只读管理员策略

默认只读管理员策略在**管理 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 授权 (Authorization) > RBAC 策略 (RBAC Policy)** 页面提供。此策略可用于新安装和升级部署。只读管理员策略可用于只读管理员组。默认情况下，将向只读管理员授予超级管理员菜单访问权限和只读数据访问权限。无法复制此策略，也无法编辑关联的**数据访问权限**。

注释

- 默认只读策略映射到只读管理员组。无法使用只读管理员组创建自定义 RBAC 策略。
- 思科 ISE 仅基于只读管理员组的静态检查支持只读功能。

自定义只读管理员的菜单访问权限

默认情况下，只读管理员具有超级管理员菜单访问权限和只读管理员数据访问权限。不过，如果超级管理员需要只读管理员仅查看“主页”(Home) 和“管理”(Administration) 选项卡，则超级管理员可以创建自定义菜单访问权限或自定义默认权限，例如MnT管理员菜单访问权限或策略管理员菜单访问权限。超级管理员无法修改映射到只读管理员策略的只读数据访问权限。

步骤 1 以超级管理员身份登录管理员门户。

步骤 2 导航至 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions) > 菜单访问 (Menu Access)** 页面。

步骤 3 点击**添加 (Add)**，然后输入**名称**（如 MyMenu）和**说明**。

步骤 4 在**菜单访问权限 (Menu Access Privileges)** 部分中，可以选择**显示/隐藏 (Show/Hide)** 选项来选择应向只读管理员显示的所需选项（如“主页”(Home) 和“管理”(Administration) 选项卡）。

步骤 5 点击**提交 (Submit)**。

自定义菜单访问权限显示在与只读管理员策略（显示在“管理”(Administration) > “系统”(System) > “管理员访问权限权限”(Admin Access) > “授权”(Authorization) > “策略”(Policy) 页面中）对应的**权限 (Permissions)** 下拉列表中。

步骤 6 导航至**管理员 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 授权 (Authorization) > RBAC 策略 (RBAC Policy)** 页面。

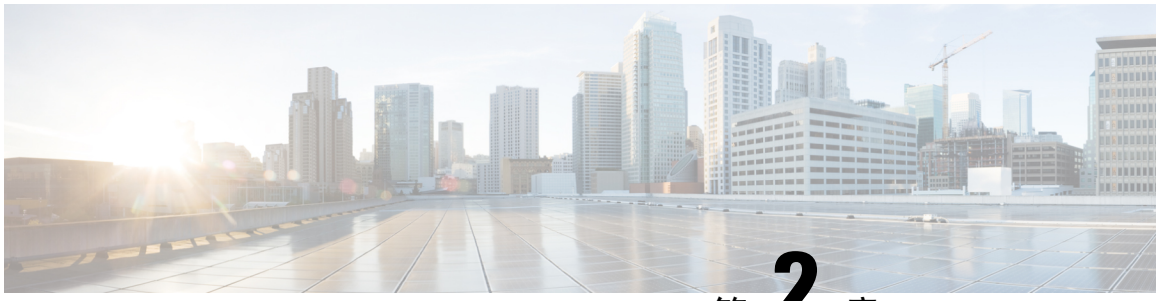
步骤 7 点击与**只读管理员策略 (Read-Only Admin Policy)** 对应的**权限 (Permissions)** 下拉列表。

步骤 8 选择默认菜单访问权限（MnT 管理员菜单访问）或自定义菜单访问权限 (MyMenu)。 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions) > 菜单访问 (Menu Access)** 页面。

步骤 9 点击**保存 (Save)**。

如果为只读管理员策略选择数据访问权限，将遇到错误。

注释 登录只读管理员门户时，屏幕顶部将显示一个只读图标，您只能查看指定的菜单选项，而没有数据访问权限。



第 2 章

许可

思科 ISE 许可证

Cisco ISE 版本 3.0 及更高版本不支持Cisco ISE 版本 2.x 中使用的传统许可证，例如 Base、Plus 和 Apex 许可证。Cisco ISE 版本 3.0 许可证完全通过叫做 Cisco Smart Software Manager (CSSM) 的集中式数据库进行管理。通过单令牌注册轻松、高效地注册、激活和管理所有许可证。

为最大限度地提高客户的经济性，Cisco ISE 的许可在以下软件包中提供：

- **层级许可证**

  从Cisco ISE 版本 3.0 开始，一组称为“层级许可证”的新许可证将取代之前版本中使用的 Base、Apex 和 Plus 许可证。层级许可证包含三种许可证：Essentials、Advantage 和 Premier。

  如果您当前拥有 Base、Apex 和 Plus 许可证，请使用 Cisco Smart Software Manager (CSSM) 将其转换为新的许可证类型。

- **设备管理许可证**

  上面启用了 TACACS+ 角色的策略服务节点 (PSN) 将使用设备管理许可证。

- **虚拟设备许可证**

  虚拟设备许可证有三种形式：VM 小型、VM 中型和 VM 大型。

- **评估许可证**

  当您首次安装Cisco ISE 版本 3.0 时，默认情况下会启用评估许可证。评估许可证是 90 天的许可证，允许您访问所有Cisco ISE 功能。在评估期间，许可证使用量不会报告给 CSSM。

如果用现有的智能许可证升级到Cisco ISE 版本 3.0，您的智能许可证将升级到Cisco ISE 中的新许可证类型。但是，您必须在 CSSM 中注册新的许可证类型，才能激活Cisco ISE 版本 3.0 中的许可证。

如果您拥有传统Cisco ISE 许可证，必须将其转换为智能许可证，才能在Cisco ISE 版本 3.0 中开始使用许可证。要将Cisco ISE 2.x 许可证转换为新的许可证类型，请通过支持案例管理器 (http://cs.co/scmswl) 或使用 http://cs.co/TAC-worldwide 中提供的联系信息在线提交支持案例。

对于所有活动的Cisco ISE 许可证，有关许可证到期的通知会在到期前的 90天、60 天和 30 天显示在 Cisco ISE 中。有关许可证使用不合规的通知也会显示在Cisco ISE 中。如果您的许可证使用在 45 天内不合规，您将无法访问所有Cisco ISE 功能，直到您购买并激活所需的许可证。

从一个许可包升级到另一个许可包时，Cisco ISE 会继续提供升级之前的早期包中提供的所有功能。您无需重新配置已配置的任何设置。

例如，您当前使用 Essentials 许可证并在以后添加 Advantage 许可证，则使用 Essentials 许可证已配置的功能不会更改。

在以下情况下，您应更新许可协议：

- 试用期结束，而您尚未注册您的许可证。
- 您的许可证已过期。
- 终端使用量超过您的许可协议。

ISE 社区资源

思科身份服务引擎订购指南

有关如何获取评估许可证的信息，请参阅如何获取 ISE 评估许可证。

层级许可证

下表指定新的层级许可证启用的功能。

表 *2:* 思科 ***ISE*** 层级许可证

许可证名称	此许可证可启用什么功能？
Essentials	• RADIUS 身份验证、授权和记账，包括 802.1X、MAC 身份验证绕过和轻松连接，以及 Web 身份验证。 • MACsec。 • 基于单点登录 (SSO)、安全断言标记语言 (SAML) 和开放式数据库连接 (ODBC) 标准的身份验证。 • 访客门户和发起人服务。 • 用于监控目的的具象状态传输 (REST) API，以及用于 CRUD 操作的外部 RESTful 服务 API。 • PassiveID 服务。 • 安全有线和无线接入。
Advantage	• Cisco ISE Essentials 许可证启用的所有功能。 • 自带设备 (BYOD) 设备注册和调配，内置证书颁发机构。设备注册通过已配置的“我的设备”门户进行。 • 安全组标记、TrustSec 和Cisco以应用为中心的基础设施 (ACI) 集成。 • 分析服务，包括基本资产可视性和实施功能。 • 终端分析，包括高级资产可视性和实施功能。 • 源服务。 • 基于位置的服务的可视性和实施。 • 情景共享（如 pxGrid）和安全生态系统集成。

许可证名称	此许可证可启用什么功能？
Premier	• Cisco ISE Essentials 和 Advantage 许可证启用的所有功能。 • 终端保护服务。 • 快速遏制威胁（使用自适应网络控制和情景共享服务）。 • 终端安全评估可视性和实施。 • 通过企业移动管理和移动设备管理实现的合规可视性和实施。 • 以威胁为中心的网络访问控制可视性和实施。

设备管理许可证

设备管理许可证允许您在策略服务节点上使用 TACACS 服务。在高可用性独立部署中，设备管理许可证允许您在高可用性对中的单个策略服务节点上使用 TACACS 服务。

虚拟设备许可证

Cisco ISE 还可作为虚拟设备出售。根据网络中虚拟机节点的数量以及每个虚拟机节点的资源规格（如 CPU 和内存），选择虚拟机 (VM) 许可证。提供三种 VM 许可证类别：VM 小型、VM 中型和 VM 大型。

下表显示了不同类别的最小 VM 资源：

表 *3:* 不同类别的最小 *VM* 资源

VM 许可证	**VM** 节点的 **RAM** 容量	**VM** 节点的 **CPU** 数量
VM 小型	16 GB	12 个 CPU
VM 中型	64GB	16 个 CPU
VM 大型	256GB	16 个 CPU

例如，如果使用具有 16 个 CPU 和 64 GB RAM 的 3595 等效 VM 节点，则需要 VM 中型许可证才能在此 VM 节点上启用Cisco ISE 服务。即使仅注册和激活了 VM 小型许可证，Cisco ISE 也会注册 VM 节点使用的是 VM 中型许可证。这是因为所使用的许可证是由 VM 节点的 RAM 和 CPU 规格决定的。

然后，您将收到有关许可证使用不合规的警告和通知，直到您购买并安装所需的 VM 许可证为止。但是，Cisco ISE 服务不会中断。

您可以根据部署中的 VM 数量及其资源安装多个 VM 许可证。

VM许可证是基础设施许可证。因此，安装VM许可证时无需考虑部署中可用的终端许可证。但是，要使用层级许可证所实现的功能，还必须安装相应的层级许可证。

安装或升级到Cisco ISE 2.4 或更高版本后，如果部署的 VM 节点数量和安装的 VM 许可证数量存在任何不一致，则系统会每 14 天在主页的**警报 (Alarms)** Dashlet 中显示警报。如果 VM 节点的资源发生任何更改，以及当注册或取消注册 VM 节点时，系统也会显示警报。

VM 许可证是永久性许可证。您每次登录Cisco ISE GUI 时，系统都会显示 VM 许可更改情况，直到您在显示的弹出通知中选中**不再显示此消息 (Do not show this message again)** 复选框为止。

评估许可证

当您安装或升级到Cisco ISE 版本 3.0 时，默认激活评估许可证。评估许可证有效期为 90 天，您可以在此期间访问所有Cisco ISE 功能。当使用评估许可证时，Cisco ISE 被视为处于评估模式。

Cisco ISE 管理门户的右上角显示一条消息，其中包含评估模式下剩余的天数。您必须注册在评估模式结束前购买的Cisco ISE 许可证，才能继续使用所需的Cisco ISE 功能。

思科 ISE 智能许可证

当激活智能许可证令牌并在Cisco ISE 管理门户中注册该令牌后，CSSM 会监控每个产品许可证各个终端会话的许可证使用情况。智能许可通过Cisco ISE 中的简单表格布局通知管理员终端会话的许可证使用情况。智能许可 (Smart Licensing) 每天向集中式数据库报告各个以启用许可证的高峰使用情况。当许可证可用且未使用时，管理员会收到可用许可证通知，并可继续监控使用情况。当使用量超过可用许可证数量时，系统会激活警报，并通过警报和通知来告知管理员。

借助智能许可，还可以通过Cisco智能账户管理所包含的不同许可证权益，如 Essential、Advantage、Premier 或 Device Admin。通过Cisco ISE，可以监控每个许可证权益的基本使用量统计信息。通过您的 CSSM 帐户，还可以查看更多信息、统计数据和通知，以及更改您的帐户和授权。

注释 思科智能软件管理器辅助设备

Cisco ISE 每 30 分钟获取一次内部许可证使用样本。系统会相应地更新许可证合规性和使用情况。要在Cisco ISE 的**许可证 (Licenses)** 表中查看此信息，请从主菜单中选择 **管理 (Administration)** > **系统 (System)** > **许可 (Licensing)**），然后点击**刷新 (Refresh)**。

从您向 CSSM 注册Cisco ISE 主管理节点 (PAN) 以来，Cisco ISE 会每六小时向 CSSM 服务器报告一次许可证使用峰值计数。峰值计数报告可帮助确保Cisco ISE 中的许可证使用符合所购买和注册的许可证。Cisco ISE 通过存储 CSSM 证书的本地副本与 CSSM 服务器通信。在每日同步期间以及刷新**许可证 (Licenses)** 表时，系统会自动重新授权 CSSM 证书。通常，CSSM 证书有效期为六个月。

如果与 CSSM 服务器同步时合规状态有变化，则**许可证 (Licenses)** 表的**最后授权 (Last Authorization)** 列会相应更新。此外，当权益不再合规时，**不合规天数 (Days Out of Compliancy)** 列中会显示它们处于不合规状态地天数。此外，还会在**许可 (Licensing)** 区域顶部的“通知”(Notifications) 中，以及

Cisco ISE 工具栏的**许可警告 (License Warning)** 链接位置指明不合规。除通知之外，还可以查看警报。

注释 Device Admin 许可证会在思科 ISE 与 CSSM 服务器通信时获得授权，但它们不基于会话，因此**许可证 (Licenses)** 表中没有与之关联的使用量计数。

许可证 (Licenses) 表的合规性列显示以下值之一：

- **合规 (In Compliance)**：此许可证的使用符合规定。
- **已发放权益 (Released Entitlement)**：已购买并发放许可证以供使用，但到目前为止，此Cisco ISE 部署中尚未使用其中任何许可证。在这种情况下，将会看到许可证的**使用计数 (Consumption Count)** 为 0。
- **评估 (Evaluation)**：可使用评估许可证。

注册并激活智能许可证

开始之前

- 如果您有传统的Cisco ISE 许可证，必须将其转换为智能许可证。
- 如果要使用现有智能许可证升级到Cisco ISE 版本 3.0，请在 CSSM 中将许可证转换为新的智能许可证类型。
- 在 CSSM 中注册新的智能许可证类型，以接收注册令牌。

步骤 1 在Cisco ISE GUI 中，点击**菜单** (Menu) 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **许可 (Licensing)**。

步骤 2 点击**注册详细信息 (Registration Details)**。

步骤 3 在显示的**注册详细信息 (Registration Details)** 区域中，在**注册令牌 (Registration Token)** 字段中输入从 CSSM 收到的注册令牌。

步骤 4 从**连接方法 (Connection Method)** 下拉列表中选择连接方法。

- **直接 HTTPS (Direct HTTPS)**，如果已配置与互联网的直接连接。
- **HTTPS 代理 (HTTPS Proxy)**，如果没有与互联网的直接连接且需要使用代理服务器。
- **传输网关 (Transport Gateway)** 是推荐选项。如果已配置传输网关，则默认选择此连接。您必须删除传输网关配置才能选择其他连接方法。

步骤 5 从**层 (Tier)** 和**虚拟设备 (Virtual Appliance)** 区域，选中您需要启用的所有许可证的复选框。系统将激活所选许可证，并由 CSSM 跟踪其使用情况。

步骤 6 点击**注册 (Register)**。

在 ISE 中管理智能许可

激活并注册智能许可令牌后，即可通过以下操作从Cisco ISE 管理许可证授权：

- 启用、禁用和刷新许可证授权证书。
- 更新智能许可注册。
- 识别合规和不合规的许可问题。

开始之前

确保已激活并注册您的智能许可令牌。

步骤 1 首次安装思科 ISE 版本 3.0 时，将自动启用所有许可证授权并将其作为评估模式的一部分。注册许可证令牌后，如果您的 CSSM 帐户不包括特定授权，并且您没有在注册期间禁用它们，则Cisco ISE 中将显示不合规通知。将这些授权添加到您的 CSSM 帐户（请联系您的 CSSM 客户代表寻求帮助），然后从**许可证 (Licenses)** 表中点击**刷新 (Refresh)** 以删除不合规通知并继续使用相关功能。刷新授权后，注销然后重新登录Cisco ISE 以删除相关的不合规消息。

步骤 2 如果每天自动授权由于任何原因失败，则显示不合规消息。点击**刷新 (Refresh)** 重新获得您的授权。刷新授权后，注销然后重新登录Cisco ISE 以删除相关的不合规消息。

步骤 3 首次安装思科 ISE 版本 3.0 时，将自动启用所有许可证授权并将其作为评估期的一部分。注册令牌后，如果您的 CSSM 帐户不包括特定授权，并且您没有在注册期间禁用它们，仍然可以在 ISE 中通过智能许可禁用这些授权，以避免不必要的不合规通知。从**许可证 (Licenses)** 表中，选中令牌中未包括的许可证授权的复选框，然后在工具栏上点击**禁用 (Disable)**。禁用许可证授权后，注销然后重新登录Cisco ISE 以从菜单中删除相关的功能，并且删除不合规消息。

步骤 4 为您的帐户添加授权后，请启用这些授权。从**许可证 (Licenses)** 表中，选中所需的已禁用许可证的复选框，并在工具栏上点击**启用 (Enable)**。

步骤 5 注册证书每六个月自动刷新一次。要手动刷新智能许可证书注册，请在**许可 (Licensing)** 窗口顶部点击**更新注册 (Renew Registration)**。

步骤 6 要从智能账户删除Cisco ISE 产品注册（由 UDI 指示），但是继续使用智能许可直到评估期结束，请在**思科智能许可 (Cisco Smart Licensing)** 区域的顶部点击**取消注册 (Deregister)**。例如，如果需要更改在注册过程中指定的 UDI，可以执行此操作。如果评估期仍有剩余时间，则Cisco ISE 仍处于智能许可中。如果评估期已结束，则在浏览器刷新时将显示通知。取消注册后，您可以遵循注册流程以相同或不同的 UDI 再次注册。

步骤 7 要从智能账户完全删除Cisco ISE 产品注册（由 UDI 指示）并恢复为传统许可，请在**思科智能许可 (Cisco Smart Licensing)** 区域的顶部点击**禁用 (Disable)**。例如，如果需要更改在注册过程中指定的 UDI，可以执行此操作。禁用后，您可以遵循注册流程以相同或不同的 UDI 再次激活并注册。。

未注册的许可证使用量

问题

许可证使用量依赖于与终端匹配的授权策略中使用的属性。

假设只在系统中注册了 Essentials 许可证（已删除 90 天的评估许可证）。您将能够查看和配置相应的 Essentials 菜单项和功能。

如果将授权策略配置（错误配置）为使用需要 Advantage 许可证的功能（例如：Session:PostureStatus），且如果终端与此授权策略相匹配，那么：

- 终端将使用 Advantage 许可证，即使尚未在系统中注册 Advantage 许可证。
- 每当您登录时，系统会显示对此影响的通知。
- Cisco ISE 将发出通知和警报：“许可证使用量超出可用量”(Exceeded license usage than allowed)（从技术上来说，这是意料之中的，因为系统中未注册 Advantage 许可证，但终端仍在使用此许可证）。

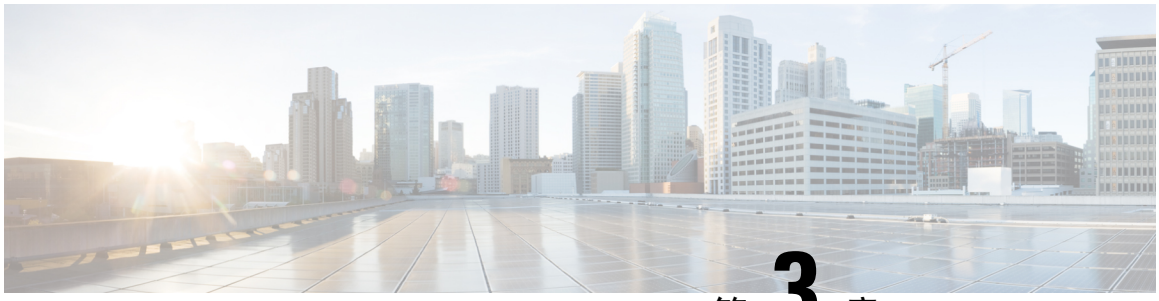
如果使用的 所有三层许可证在 45 天内不合规，则在上传正确的许可证文件之前，Cisco ISE 的所有管理控制都将丢失。在注册正确的许可证之前，您将只能访问Cisco ISE GUI 中的**许可 (Licensing)** 窗口。但是，Cisco ISE 将继续处理身份验证。

可能的原因

由于授权策略配置错误，**许可 (Licensing)** 表可显示Cisco ISE 正在使用您尚未购买和注册的许可证。在购买 一个许可证之前，Cisco ISE GUI 不会显示该许可证所涵盖的功能。但是，购买许可证之后，用户界面会继续显示许可证功能，即使在许可证已过期或超出其终端使用量之后亦如此。因此，即使没有系统的有效许可证，仍可以进行配置。

解决方案

在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰) 并选择**策略 (Policy)** > **策略集 (Policy Sets)**，确定正在使用尚无注册许可证的功能的授权规则，然后重新配置该规则。



第 3 章

部署

思科 ISE 部署术语

以下是讨论Cisco ISE 部署方案时常用的术语：

- 服务：服务是角色提供的特定功能，例如网络访问、分析器、终端安全评估、安全组访问、监控和故障排除等。
- 节点：节点是运行Cisco ISE 软件的单个实例。Cisco ISE 可用作设备，也可用作能在 VMware 上运行的软件。运行Cisco ISE 软件的每个实例（设备或 VMware）叫节点。
- 角色：节点的角色决定节点提供的服务。Cisco ISE 节点可以承担以下任意角色：管理、策略服务、监控和 pxGrid。通过管理员门户可用的菜单选项取决于Cisco ISE 节点承担的职责和角色。
- 部署模式：决定您的部署是分布式、独立式还是作为基本双节点部署的独立式高可用性部署。

分布式思科 ISE 部署中的角色

Cisco ISE 节点可以承担管理、策略服务或监控角色。

Cisco ISE 节点可以根据它承担的角色提供各种服务。部署中的每个节点均可承担管理、策略服务和监控角色。在分布式部署中，您可以在网络中使用以下节点组合：

- 支持高可用性的主策略管理节点（主 PAN）和辅助策略管理节点（辅助 PAN）
- 支持高可用性的主监控节点（主 MnT 节点）和辅助监控节点（辅助 MnT 节点）
- 用于主 PAN 自动故障转移的一对运行状况检查节点或单个运行状况检查节点
- 用于会话故障转移的一个或多个策略服务节点 (PSN)

环境下载成功，结果中仅显示正在运行的Cisco ISE 节点。

配置思科 ISE 节点

在安装Cisco ISE 节点后，系统会在其上运行管理、策略服务和监控角色提供的默认服务。此节点将处于独立状态。您必须登录Cisco ISE 节点的 Admin 门户进行配置。您无法编辑独立Cisco ISE 节点的角色或服务。但是，您可以编辑主要和辅助Cisco ISE 节点的角色和服务。您必须先配置主要 ISE 节点，然后向主要 ISE 节点注册辅助 ISE 节点。

如果首次登录节点，您必须更改默认管理员密码并安装有效许可证。

建议不要更改生产中在Cisco ISE 上配置的主机名和域名。如有必要，则在初始部署期间为设备重置映像，执行更改，并配置详细信息。

开始之前

您应该对如何在Cisco ISE 中设置分布式部署有基本了解。请参阅设置分布式部署的规定。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选中您要配置的Cisco ISE 节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 按照需要输入相应值，然后点击**保存 (Save)**。

配置主策略管理节点 (PAN)

要设置分布式部署，必须首先将Cisco ISE 节点配置为主 PAN。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

一开始 Register 按钮将会处于禁用状态。要启用此按钮，必须配置主 PAN。

步骤 2 选中当前节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**设为主 (Make Primary)** 以配置主 PAN。

步骤 4 点击**保存 (Save)**，保存节点配置。

下一步做什么

1. 向您的部署添加辅助节点。
2. 如有必要，请启用分析器服务并配置探测功能。

注册辅助思科 ISE 节点

您可以将Cisco ISE 节点注册到主 PAN 以形成多节点部署。部署中除主 PAN 以外的节点称为辅助节点。在注册节点时，可以选择必须在节点上启用的角色和服务。注册的节点可从主 PAN 管理（例如，管理节点角色、服务、证书、许可证、应用补丁等）。

注册辅助节点后，主PAN 会将配置数据推送到辅助节点，而辅助节点上的应用服务器会重启。完成数据后，在主PAN 上完成的进一步配置更改将复制到辅助节点。在辅助节点上复制更改所需的时间取决于各种因素，如网络延迟、系统负载等。

开始之前

确保主 PAN 和正在注册的节点可相互进行 DNS 解析。如果正在注册的节点使用不受信任的自签证书，则系统会提示包含证书详细信息的证书警告。如果接受该证书，则会将其添加到主PAN 的受信任证书存储区，以启用与节点的 TLS 通信。

如果节点使用非自签证书（例如，由外部 CA 签名），则必须将该节点的相关证书链手动导入到主 PAN 的受信任证书库。当将辅助节点的证书导入受信任证书库时，请选中**受信任证书 (Trusted**

Certificates) 窗口中的**信任 ISE 中的身份验证 (Trust for Authentication within ISE)** 复选框，以便主 PAN 验证辅助节点的证书。

在注册启用了会话服务（如网络访问、访客、终端安全评估等）的节点时，可以将其添加到节点组。有关详细信息，请参阅创建策略服务节点组，第 78 页一节。

步骤 1 登录到主 PAN。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击**注册 (Register)** 以开始注册辅助节点。

步骤 4 输入要注册的独立节点的可 DNS 解析完全限定域名 (FQDN)，采用的格式为 hostname.domain-name，例如，abc.xyz.com。主 PAN 的 FQDN 和正在注册的节点必须能够相互解析。

步骤 5 在**用户名 (Username)** 和 **密码 (Password)** 字段中，输入辅助节点的基于 UI 的管理员凭证。

步骤 6 点击**下一步 (Next)**。

主 PAN 会尝试与正在注册的节点（首次）建立 TLS 通信。

- 如果节点使用受信任的证书，则可以继续执行第 7 步。
- 如果节点使用不受信任的自签证书，则会显示证书警告消息。证书警告消息显示有关证书的详细信息（如颁发给、颁发者、序列号等），可对照节点上的实际证书进行验证。您可以选择**导入证书并继续 (Import Certificate and Proceed)** 选项以信任此证书并继续注册。Cisco ISE 会将该节点的默认自签证书导入到主 PAN 的受信任证书库。如果不想使用默认的自签证书，请点击**取消注册 (Cancel Registration)** 并将该节点的相关证书链手动导入到主 PAN 的受信任证书库。当将辅助节点的证书导入到受信任证书库时，请选中**信任 ISE 内部的身份认证 (Trust for Authentication within ISE)** 复选框，以便 PAN 验证辅助节点的证书。
- 如果节点使用 CA 签名的证书，则系统会显示一条错误消息，指出在设置证书信任之前无法继续注册。

步骤 7 选择要在节点上启用的角色和服务，然后点击**保存 (Save)**。

注册节点时，主 PAN 上会生成警报（确认已将节点添加到部署中）。在Cisco ISE GUI **控制板 (Dashboard)** 的**警报 (Alarms)** Dashlet 中查看此警报。注册节点同步并重新启动后，您可以使用主 PAN 上所用的相同凭证登录到辅助节点 GUI。

下一步做什么

- 对于时间敏感型任务（例如访客用户访问和授权、登录等），请确保节点上的系统时间已经同步。
- 如果您注册了辅助 PAN，并计划使用内部Cisco ISE CA 服务，则必须备份主 PAN 的Cisco ISE CA 证书和密钥，并在辅助 PAN 恢复这些证书和密钥。

  请参阅 思科 ISE CA 证书和密钥的备份与恢复，第 186 页

支持多种部署方案

可以在企业基础网络架构中部署Cisco ISE，支持 802.1X 有线、无线和虚拟专用网络 (VPN)。

Cisco ISE 架构同时支持独立和分布式（也称为高可用性 或冗余）部署，其中一台计算机承担主要角色，另一台“备份”计算机承担辅助角色。Cisco ISE 具有不同的可配置角色、服务和职责，允许创建和应用网络中所需的Cisco ISE 服务。这样得到的是一个用作功能齐全的集成式系统的全面Cisco ISE 部署。

可以使用一个或多个管理、监控和策略服务角色部署Cisco ISE 节点。每个角色在整体网络策略管理拓扑中发挥不同的重要作用。使用管理角色安装Cisco ISE，可以从集中式门户配置和管理网络以提高效率和易用性。

思科 ISE 分布式部署

具有不止一个Cisco ISE 节点的部署称作分布式部署。要支持故障切换和提高性能，您可以以分布式方式为您的部署设置多个Cisco ISE 节点。在Cisco ISE 分布式部署中，管理和监控活动会进行集中，而处理则分布在多个 PSN 上。根据您对性能的要求，您可以扩展您的部署。部署中的每个Cisco ISE 节点可以承担以下任意角色：管理、策略服务和监控。

思科 ISE 部署设置

在所有节点上安装Cisco ISE 后，如《思科身份服务引擎硬件安装指南》所述，节点显示为独立状态。然后必须定义一个节点作为主 PAN。定义主 PAN 时，必须在该节点上启用管理和监控角色。您可以在主 PAN 上选择启用策略服务角色。在主 PAN 上完成定义角色的任务后，可以向主 PAN 注册其他辅助节点，为辅助节点定义角色。

所有Cisco ISE 系统和功能相关配置应当只在主 PAN 上进行。在主 PAN 上执行的配置更改被复制到部署中的所有辅助节点上。

分布式部署中必须至少有一个 MnT。配置主 PAN 时，必须启用监控角色。在部署中注册 MnT 节点后，如果需要，可以编辑主 PAN 并禁用监控角色。

从主要 ISE 节点将数据复制至辅助 ISE 节点

当您将Cisco ISE 节点注册为辅助节点时，Cisco ISE 会立即创建一个从主节点到辅助节点的数据复制通道并开始执行复制进程。复制是从主要节点向辅助节点共享Cisco ISE 配置数据的过程。复制可确保部署中的所有Cisco ISE 节点的配置数据一致。

首次将Cisco ISE 节点注册为辅助节点时，通常会进行完全复制。完全复制之后进行增量复制，确保在辅助节点中反映所有新的更改，例如对 PAN 中配置数据的添加、修改或删除。复制过程可确保部署中的所有Cisco ISE 节点保持同步。在Cisco ISE 管理员门户的**部署 (Deployment)** 窗口中，可从**节点状态 (Node Status)** 列查看复制状态。当您将Cisco ISE 节点注册为辅助节点或执行与 PAN 的手动同步时，节点状态显示橙色图标，表示正在进行所请求的操作。同步完成后，节点状态会变为绿色，表示辅助节点已与 PAN 同步。

思科 ISE 节点取消注册

要从部署中删除节点，您必须对该节点取消注册。从主 PAN 取消注册辅助节点时，被取消注册的节点的状态更改为独立，主节点和辅助节点之间的连接将丢失。复制更新不再发送到被取消注册的独立节点。

取消注册 PSN 时，终端数据将丢失。如果您希望 PSN 在成为独立节点后保留终端数据，可以执行以下任一操作：

- 从主 PAN 获取备份，并在 PSN 成为独立节点时在其上恢复此数据备份。
- 将 PSN 的角色更改为“管理”(Administration)（辅助 PAN），从管理员门户的**部署 (Deployment)** 窗口同步数据，然后取消注册节点。此节点现在拥有所有数据。然后可以将辅助 PAN 添加至现有部署。

注释 无法取消注册主 PAN。

设置分布式部署的规定

在分布式环境中设置Cisco ISE 之前，请仔细阅读以下声明。

- 选择Cisco ISE 服务器节点类型。对于管理、策略服务和监控功能，必须选择Cisco ISE 节点。
- 为所有节点选择同一网络时间协议 (NTP) 服务器。要避免节点之间发生时区问题，您必须在每个节点的设置过程中提供同一 NTP 服务器名称。此设置可确保来自部署中的各种节点的报告和日志与时间戳始终同步。
- 安装Cisco ISE 时配置Cisco ISE 管理员密码。以前的Cisco ISE 管理员默认登录凭证 (admin/cisco) 不再有效。使用初始设置过程中创建的用户名和密码或当前密码（如果后来更改了密码）。
- 配置域名系统 (DNS) 服务器。在 DNS 服务器中输入分布式部署中包含的所有Cisco ISE 节点的 IP 地址和完全限定域名 (FQDN)。否则，节点注册将失败。
- 在 DNS 服务器中为分布式部署中的所有Cisco ISE 节点配置正向和反向 DNS 查找。否则，在注册并重新启动Cisco ISE 节点时可能会遇到部署相关问题。如果未为所有节点配置反向 DNS 查找，则性能可能会降低。
- （可选）从主 PAN 注销辅助Cisco ISE 节点以从中卸载Cisco ISE。
- 备份主 MnT，然后将数据恢复到新的辅助 MnT。由于会复制新的更改，因此这可确保主 MnT 的历史记录与新 MnT 同步。
- 确保即将注册为辅助节点的主 PAN 和独立节点运行的是同一版本的Cisco ISE。
- 在向部署中添加新节点时，请确保通配符证书的颁发者证书链是新节点的受信任证书的一部分。将新节点添加到部署中时，通配符证书随后会复制到新节点。

- 在将Cisco ISE 部署配置为支持Cisco TrustSec 时，或者在Cisco ISE 与Cisco DNA 中心集成时，请勿将 PSN 配置为仅 SXP。SXP 是Cisco TrustSec 和非Cisco TrustSec 设备之间的接口。SXP 不与支持Cisco TrustSec 的网络设备通信。

主要节点和辅助节点上可用的菜单选项

作为分布式部署组成部分的Cisco ISE 节点中可用的菜单选项取决于在节点上启用的角色。您必须通过主 PAN 执行所有管理和监控活动。对于其他任务，您必须使用辅助节点。因此，根据辅助节点上启用的角色，辅助节点的用户界面提供有限的菜单选项。

如果节点担任不止一个角色，例如某个主职责同时具备策略服务角色和监控角色，则针对 PSN 和主 MnT 列出的菜单选项在该节点上可用。

下表列出在担任不同角色的Cisco ISE 节点上可用的菜单选项。

表 *4:* 思科 *ISE* 节点和可用的菜单选项

Cisco ISE 节点	可用的菜单选项
所有节点	• 查看和配置系统时间以及 NTP 服务器设置 • 安装服务器证书并管理证书签名请求。您可以通过集中管理所有服务器证书的主 PAN 为该部署中的所有节点执行服务器证书操作 **注释** 私钥不存储于本地数据库中，也不从相关节点复制。私钥存储于本地文件系统中。
主策略管理节点（主 PAN）	所有菜单和子菜单
主监控节点（主 MnT 节点）	• 提供对监控数据的访问 **注释** 只能从主 PAN 查看**操作 (Operations)** 菜单。**操作 (Operations)** 菜单不显示在Cisco ISE 2.1 及更高版本的监控节点中。
PSN（策略服务节点）	加入、离开和测试 Active Directory 连接的选项可用。必须单独将每个 PSN 加入到 Active Directory 域中。必须先定义域信息并且将 PAN 联接到 Active Directory 域中。然后，逐一将其他 PSN 加入到 Active Directory 域中。

Cisco ISE 节点	可用的菜单选项
辅助策略管理节点（辅助 PAN）	将辅助 PAN 升级为主 PAN 的选项 注释 在向主 PAN 注册了辅助节点之后，在登录任意辅助节点的管理员门户时，您必须使用主 PAN 的登录凭证。

部署和节点设置

您可以通过**部署节点 (Deployment Nodes)** 窗口配置Cisco ISE（PAN、PSN 和 MnT）节点并设置部署。

部署节点列表 窗口

下表介绍了**部署节点列表** 窗口上的字段，您可以使用此窗口在部署中配置Cisco ISE 节点。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**.

字段名称	使用指南
主机名 (Hostname)	显示节点的主机名。
相关角色 (Personas)	（只有在节点类型为Cisco ISE 时才显示）列出 Cisco ISE 节点承担的角色。 例如，**管理 (Administration)**、**策略服务 (Policy Service)**、**监控 (Monitoring)** 或 **pxGrid**。
角色 (Rol)e	如果在此节点上启用了管理和监控角色，则指示管理和监控角色承担的职责（主要、辅助或独立职责）。职责可以是以下一项或多项： • **PRI(A)**：指主 PAN • **SEC(A)**：指辅助 PAN • **PRI(M)**：指主 MnT • **SEC(M)**：指辅助 MnT

字段名称	使用指南
服务 **(Services)**	（只有在启用策略服务角色时才显示）列出此Cisco ISE 节点上运行的服务。服务可包括以下任意一项： • 身份映射 • 会话 • 剖析 • 全部
节点状态	指示部署中每个Cisco ISE 节点的数据复制状态。 • 绿色（已连接）：表示部署中已注册的Cisco ISE 节点与主 PAN 处于同步状态。 • 红色（断开）：表示Cisco ISE 节点无法到达、已断开或未进行数据复制。 • 橙色（处理中）：表示向主PAN新注册了新Cisco ISE 节点、您已执行手动同步操作或Cisco ISE 节点与主 PAN 不同步。 有关详细信息，请点击**节点状态 (Node Status)** 列中每个Cisco ISE 节点的快速查看图标。

相关主题

思科 ISE 分布式部署，第 35 页
思科 ISE 部署术语，第 32 页
配置思科 ISE 节点，第 32 页
注册辅助思科 ISE 节点

常规节点设置

下表说明Cisco ISE 节点的**常规设置 (General Settings)** 窗口中的字段。在此窗口中，可以将角色分配给节点并配置要在其上运行的服务。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **部署节点 (Deployment Node)** > **编辑 (Edit)** > **常规设置 (General Settings)**。

表 *5:* 常规节点设置

字段名称	使用指南
主机名 **(Hostname)**	显示Cisco ISE 节点的主机名。

字段名称	使用指南
FQDN	显示Cisco ISE 节点的完全限定域名。例如 ise1.cisco.com。
IP 地址 (IP Address)	显示Cisco ISE 节点的 IP 地址。
节点类型 (Node Type)	显示节点类型。
相关角色 (Personas)	
管理 (Administration)	如果Cisco ISE 节点承担管理角色，请启用此切换按钮。只有在受许可提供管理服务的节点上才可以启用 Administration 角色。 **角色 (Role)** - 显示管理角色在部署中承担的职责。角色可以采用以下任一值：**独立 (Standalone)**、**主 (Primary)** 或**辅助 (Secondary)**。 **设为主要 (Make Primary)** - 选择此按钮可使该节点成为主Cisco ISE 节点。在部署中您只能有一个主要Cisco ISE 节点。当您将此节点设置为主要节点之后，此页面的其他选项将进入活动状态。在部署中您只能有两个 Administration 节点。如果节点具有**独立 (Standalone)** 角色，则旁边会显示**设为主要 (Make Primary)** 按钮。如果节点具有**辅助 (Secondary)** 角色，则旁边会显示**升级为主要 (Promote to Primary)** 按钮。如果节点具有**主要 (Primary)** 角色，并且没有其他节点注册到该节点，则旁边会显示**设为独立 (Make Standalone)** 按钮。您可以点击此按钮以使您的主要节点成为独立节点。

字段名称	使用指南
监控 (Monitoring)	如果要Cisco ISE 节点承担监控角色并充当日志收集器，请启用此切换按钮。分布式部署中必须至少有一个监控节点。配置主 PAN 时，必须启用监控角色。在部署中注册辅助监控节点之后，如有必要，可以编辑主 PAN 和禁用监控角色。 要在 VMware 平台上将Cisco ISE 节点配置为您的日志收集器，请使用以下规定确定您所需要的最低磁盘空间：您的网络中每天每个终端 180 KB，您的网络中每天每个Cisco ISE 节点 2.5 MB。 您可以根据您想要将多少个月的数据至于监控模式下，计算您所需的最大磁盘空间。如果您的部署中只有一个监控节点，则该节点会承担独立职责。如果在部署中有两个监控节点，Cisco ISE 会显示另一个监控节点的名称以供您配置主要/辅助角色。要配置这些职责，请选择以下选项之一： • **主 (Primary)**：使当前节点成为主监控节点。 • **辅助 (Secondary)**：使当前节点成为辅助监控节点。 • **无 (None)** - 如果要使监控节点不承担主要-辅助角色。 如果您将您的一个监控节点配置为主要或辅助节点，另一个监控节点相应地自动成为辅助或主要节点。主要监控节点和辅助监控节点都接收管理和策略服务日志。如果将一个监控节点的角色改为**无 (None)**，则另一个监控节点的角色也会成为**无 (None)**，从而会在您将某个节点指定为监控节点之后取消高可用性对。您会在**远程日志记录目标 (Remote Logging Targets)** 窗口中发现此节点被列为系统日志目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

字段名称	使用指南
策略服务 **(Policy Service)**	

字段名称	使用指南
	启用此切换按钮可启用以下任一或所有服务： • **启用会话服务 (Enable Session Services)**：选中此复选框可启用网络访问、终端安全评估、访客和客户端调配服务。从**在节点组中包含节点 (Include Node in Node Group)** 下拉列表中选择此策略服务节点所属的组。请注意，证书颁发机构 (CA) 和安全传输注册 (EST) 服务只能在已启用会话服务的策略服务节点上运行。 对于**在节点组中包含节点 (Include Node in Node Group)**，如果不希望此策略服务节点加入任何组，请选择**无 (None)**。 同一个节点组中的所有节点都应在网络接入设备上配置为 RADIUS 客户端，并获 CoA 授权，因为这些节点中的任何一个节点均可为通过节点组中的任何节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，则节点组中的节点应与在NAD上配置的RADIUS服务器和客户端相同，或作为RADIUS服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。 虽然可以使用多个Cisco ISE 节点将单个NAD配置为RADIUS服务器和动态授权客户端，但并不要求所有节点都属于同一个节点组。 一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。有关详细信息，请参阅《》中的“创建策略服务节点组”部分请参阅创建策略服务节点组，第 78 页。 • **启用分析服务 (Enable Profiling Service)**：选中此复选框可启用分析服务。如果启用分析服务，必须点击**分析配置 (Profiling Configuration)** 选项卡并根据要求输入详细信息。当您启用或禁用策略服务节点上运行的任意服务或对此节点做任何更改时，您将重新启动运行这些服务的应用服务器进程。这些服务重新启动时预计会有延迟。您可以从 CLI 使用 *show application status ise* 命令，确定何时在节点上重新启动了应用服务器。

字段名称	使用指南
	• **启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)**：选中此复选框可启用威胁中心网络访问控制 (TC-NAC) 功能。通过此功能，您可依据威胁和漏洞适配器发送的威胁和漏洞属性创建授权策略。威胁严重级别和漏洞评估结果可用于动态控制终端或用户的访问级别。 • **启用 SXP 服务 (Enable SXP Service)**：选中此复选框可在节点上启用 SXP 服务。您还必须指定 SXP 服务使用的接口。 如果已配置 NIC 绑定或组合，则还会在使用**接口 (Use Interface)** 下拉列表中列出绑定接口以及物理接口。 • **启用设备管理员服务 (Enable Device Admin Service)**：选中此复选框可创建 TACACS 策略集和策略结果等，以便控制和审计网络设备的配置。 • **启用被动身份服务 (Enable Passive Identity Service)**：选中此复选框可启用身份映射功能。通过此功能，您可以监控通过域控制器 (DC)（而不是Cisco ISE）进行身份验证的用户。在Cisco ISE 不主动对用户进行网络访问身份验证的网络中，您可以使用身份映射功能从 Active Directory (AD) 域控制器收集用户身份验证信息。
pxGrid	选中此复选框可启用 pxGrid 角色。Cisco pxGrid 用于将来自Cisco ISE 会话目录区分上下文的信息共享给Cisco自适应安全设备 (ASA)。此 pxGrid 框架还可用于在节点之间交换策略和配置数据，例如在Cisco ISE 和第三方供应商之间共享标签和策略对象，以及交换威胁信息等非Cisco ISE 相关信息。

相关主题

分布式思科 ISE 部署中的角色，第 32 页
管理节点，第 53 页
策略服务节点，第 60 页
监控节点，第 63 页
思科 pxGrid 节点，第 70 页
同步主要和辅助思科 ISE 节点，第 77 页

创建策略服务节点组，第 78 页
部署思科 pxGrid 节点，第 71 页
更改节点角色和服务，第 77 页
配置用于自动故障切换的监控节点，第 69 页

分析节点的设置

下表介绍“分析配置”(Profiling Configuration) 窗口上的字段，您可以使用此窗口为分析器服务配置探测功能。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **ISE 节点 (ISE Node)** > **编辑 (Edit)** > **分析配置 (Profiling Configuration)**。

表 *6:* 分析节点的设置

字段名称	使用指南
NetFlow	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 NetFlow，以便接收从路由器发送的 NetFlow 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入从路由器接收 NetFlow 导出数据的 NetFlow 侦听器端口号。默认端口为 9996。
DHCP	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入 DHCP 服务器 UDP 端口号。默认端口为 67。
DHCP SPAN	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 DHCP，以便收集 DHCP 数据包。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。

字段名称	使用指南
HTTP	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。
RADIUS	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 RADIUS，以便收集 RADIUS 会话属性，以及来自已启用 IOS 传感器的设备的Cisco设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
网络扫描 (NMAP) (Network Scan [NMAP])	启用此切换按钮可启用 NMAP 探测。
DNS	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 DNS，以便对 FQDN 执行 DNS 查找。以秒为单位输入**超时 (Timeout)** 期间。 注释 要使 DNS 探测功能在分布式部署中特定Cisco ISE 节点上运行，您必须启用以下任一探测功能：DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用上述另一个探测功能。
SNMP 查询 (SNMP Query)	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。为以下字段输入值：**重试次数 (Retries)**、**超时 (Timeout)**、**事件超时 (Event Timeout)**和可选的**说明 (Description)**。 注释 除配置 SNMP 查询探测功能之外，还必须在以下位置配置其他 SNMP 设置：**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。当在网络设备上配置 SNMP 设置时，请确保在网络设备上全局启用 CDP 和 LLDP。

字段名称	使用指南
SNMP 陷阱 (SNMP Trap)	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 SNMP 陷阱探测，以便从网络设备接收链路接通、链路断开和MAC通知陷阱。为以下选项输入所需的值： • **链路陷阱查询 (Link Trap Query)**：启用此切换按钮可接收和解释通过 SNMP 陷阱接收的链路接通和链路断开通知。 • **MAC 陷阱查询 (MAC Trap Query)**：启用此切换按钮可接收和解释通过 SNMP 陷阱接收的 MAC 通知。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入要使用的主机 UDP 端口。默认端口为 162。
Active Directory	启用此切换按钮可扫描所定义的 Active Directory 服务器，以获取有关 Windows 用户的信息。 • **重新扫描前的天数 (Days before rescan)**：选择您希望经过多少天后再次进行扫描。
pxGrid	启用此切换按钮可允许Cisco ISE 通过 pxGrid 收集（配置文件）终端属性。

相关主题

思科 ISE 分析服务，第 603 页
分析服务使用的网络探测功能，第 606 页
在思科 ISE 节点中配置分析服务，第 605 页

日志记录设置

下面的小节解释了如何配置调试日志的严重性、创建外部日志目标，并使Cisco ISE 能够将日志消息发送到这些外部日志目标。

远程日志记录目标设置

下表介绍“远程日志记录目标”(Remote Logging Targets) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

表 *7:* 远程日志记录目标设置

字段名称	使用指南
名称 (Name)	输入新目标的名称。
目标类型 (Target Type)	选择目标类型。默认情况下设置为 UDP Syslog。
说明	输入新目标的简短说明。
IP 地址 (IP Address)	输入要存储日志的目标计算机的 IP 地址或主机名。 思科 ISE 支持 IPv4 和 IPv6 格式的日志记录。
端口 (Port)	输入目标计算机的端口号。
设备代码 (Facility Code)	选择要用于日志记录的系统日志设备代码。有效选项为 Local0 至 Local7。
最大长度 (Maximum Length)	输入远程日志目标消息的最大长度。有效选项为 200 至 1024 字节。
服务器关闭时缓冲消息 (Buffer Message When Server is Down)	如果希望Cisco ISE 在 TCP 系统日志目标和安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。Cisco ISE 会在连接恢复时重新尝试将消息发送到目标。连接恢复后，消息按从最旧到最新的顺序进行发送，并且缓冲消息始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
缓冲区大小 (MB) (Buffer Size [MB])	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。
重新连接超时（秒）(Reconnect Timeout [Sec])	输入时间（以秒为单位），提及在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
选择 CA 证书 (Select CA Certificate)	选择客户端证书。
忽略服务器证书验证 (Ignore Server Certificate Validation)	如果希望 ISE 忽略服务器证书身份验证并接受任何系统日志服务器，请选中此复选框。

相关主题

思科 ISE 日志记录机制 ，第 249 页
思科 ISE 系统日志 ，第 250 页
远程系统日志消息格式
思科 ISE 消息目录 ，第 252 页

集合过滤器，第 253 页
事件抑制绕行过滤器，第 254 页
配置远程系统日志收集位置，第 250 页
配置集合过滤器，第 254 页

日志记录类别设置

下表介绍了**日志记录类别 (Logging Categories)** 窗口中的字段，可以使用此窗口配置日志严重性级别，并为要存储的所选类别的日志选择日志记录目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

表 *8:* 日志记录类别设置

字段名称	使用指南
名称 (Name)	显示日志记录类别的名称。
日志严重性级别 (Log Severity Level)	允许您从以下选项中选择诊断日志记录类别的严重性级别： • **严重 (FATAL)**：紧急情况。此选项意味着无法使用Cisco ISE，并且必须立即采取操作。 • **错误 (ERROR)**：此选项表示严重或错误情况。 • **警告 (WARN)**：此选项表示正常但值得注意的情况。这是默认情况。 • **信息 (INFO)**：此选项表示信息性消息。 • **调试 (DEBUG)**：此选项表示诊断错误消息。
本地日志记录 (Local Logging)	选中此复选框可为本地节点上的类别启用日志记录事件。
目标 (Targets)	允许使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 框之间转移目标来更改类别的目标。**可用 (Available)** 框包含本地（预定义）和外部（用户定义）的现有日志记录目标。初始为空的**所选 (Selected)** 框包含特定类别的选定目标。

相关主题

远程系统日志消息格式
思科 ISE 消息代码，第 252 页

配置远程系统日志收集位置，第 250 页
设置消息代码的严重性级别，第 252 页

管理员访问设置

您可以通过这些页面为管理员配置访问设置。

管理员密码策略设置

下表介绍了“管理员密码策略”(Administrator Password Policy) 窗口中的字段，可以使用此窗口定义管理员密码应满足的条件。。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。

表 *9:* 管理员密码策略设置

字段名称	使用指南
最小长度 (Minimum Length)	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。

字段名称	使用指南
密码不得包含 **(Password must not contain)**	**管理员名称或其反向顺序的字符 (Admin name or its characters in reverse order)**：选中此复选框可限制使用管理员用户名或其反向顺序的字符。
	“cisco”或其反向顺序的字符 ("cisco" or its characters in reverse order)：选中此复选框可限制使用单词“cisco”或其反向顺序的字符。
	此单词或其反向顺序的字符 (This word or its characters in reverse order)：选中此复选框可限制使用您定义的任何单词或其反向顺序的字符。
	连续重复四次或以上的字符 (Repeated characters four or more times consecutively)：选中此复选框可限制使用连续重复四次或以上的字符。
	字典单词、其反向顺序的字符或其替换为其他字符的字母 (Dictionary words, their characters in reverse order or their letters replaced with other characters)：选中此复选框可限制使用字典单词、其反向顺序的字符或其替换为其他字符的字母。 不允许使用“$”替代“s”、“@”替代“a”、“0”替代“o”、“1”替代“l”、“!”替代“i”、“3”替代“e”。例如 Pa$$w0rd • **默认字典 (Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。 默认情况下，此选项已选中。 • **自定义字典 (Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**浏览**选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。
密码必须包含每个所选类型的至少一个字符 (Password must contain at least one character of each of the selected types)	指定管理员密码必须包含从以下选项中选择的类型的至少一个字符： • 小写字母字符 • 大写字母字符 • 数字字符 • 非字母数字字符

字段名称	使用指南
密码历史记录 **(Password History)**	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
密码有效期 **(Password Lifetime)**	指定以下选项来强制用户在经过指定时间段后更改密码： • “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。”(Time (in days) before the administrator account is disabled if the password is not changed.)（允许的范围是 0 至 2147483647 天。） • “禁用管理员帐户之前的提醒时间（按天计）。”(Reminder (in days) before the administrator account is disabled.)
显示网络设备敏感数据 **(Display Network Device Sensitive Data)**	
要求管理员密码 **(Require Admin Password)**	如果您希望管理员用户输入登录密码来查看网络设备敏感数据，例如共享密钥和密码，请选中此复选框。
密码缓存用于 **(Password cached for)**	在此段时间内，会对管理员用户输入的密码进行缓存。在此期间，如果管理员用户要查看网络设备敏感数据，系统不会再次提示输入密码。有效范围为 1 至 60 分钟。

相关主题

思科 ISE 管理员，第 3 页
创建新管理员，第 4 页

会话超时和会话信息设置

下表介绍**会话 (Session)** 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *10:* 会话超时和会话信息设置

字段名称	使用指南
会话超时 **(Session Timeout)**	

字段名称	使用指南
会话空闲超时 (Session Idle Timeout)	输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。
会话信息 (Session Info)	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后点击 **失效 (Invalidate)**。

相关主题

管理员访问设置，第 212 页
配置管理员会话超时，第 216 页
终止活动管理会话，第 217 页

管理节点

通过具有管理角色的Cisco ISE 节点，您可以在Cisco ISE 上执行所有管理操作。此节点处理与诸如身份验证、授权和审核等功能有关的所有系统相关配置。在分布式环境中，最多可以具有两个运行管理角色的节点。管理角色可以承担以下任何一个角色：独立角色、主角色或辅助角色。

管理节点的高可用性

在高可用性配置中，主策略管理节点 (PAN) 处于活动状态。辅助 PAN 处于备用状态，这意味着它会从主 PAN 接收所有配置更新，但在Cisco ISE 网络中不处于活动状态。

Cisco ISE 支持手动和自动故障转移。对于自动故障转移，当主 PAN 关闭时，辅助 PAN 会自动升级。自动故障转移需要非管理辅助节点（称为运行状况检查节点）。运行状况检查节点检查主 PAN 的运行状况。如果运行状况检测到主 PAN 已关闭或无法访问，则运行状况检查节点会让辅助 PAN 升级以接管主节点角色。

要部署自动故障转移功能，您必须至少有三个节点，其中两个节点承担管理角色，一个节点充当运行状况检查节点。运行状况检查节点为非管理节点，可以是 PSN、MnT、pxGrid 节点或其组合。如果主 PAN 和辅助 PAN 位于不同的数据中心，则每个 PAN 都必须有运行状况检查节点。

下表列出主 PAN 关闭且辅助 PAN 尚未接管时受影响的功能。

功能	主 **PAN** 关闭时是否可用？（是/否）
现有的内部用户 RADIUS 身份验证	是
现有或新的 AD 用户 RADIUS 身份验证	是
无配置文件更改的现有终端	是
有配置文件更改的现有终端	否

功能	主 **PAN** 关闭时是否可用？（是/否）
通过分析了解的新终端。	否
现有访客：本地 Web 身份验证 (LWA)	是
现有访客：集中式 Web 身份验证 (CWA)	是（除了为设备注册启用的流程之外，例如热点、自带设备和带自动设备注册功能的 CWA）
访客更改密码	否
访客：AUP	否
访客：最大登录失败次数实施	否
新访客（发起或自注册）	否
终端安全评估	是
具有内部 CA 的 BYOD	否
现有的注册设备	是
MDM 自行激活服务	否
pxGrid 服务	否
登录辅助节点的 GUI	是（登录过程延迟，因为对 PAN 发起了阻塞调用以更新上次登录详细信息。在上述调用超时后继续登录）

为支持使用内部证书颁发机构调配的证书，必须在升级后将原始主 PAN 的根证书及其密钥导入新的主要节点。自动故障转移之后，对于在辅助节点升级为主 PAN 后添加的 PSN 节点，证书调配不起作用。

高可用性运行状况检查节点

主 PAN 的运行状况检查节点称为主动运行状况检查节点。辅助 PAN 的运行状况检查节点称为被动运行状况检查节点。主动运行状况检查节点负责检查主 PAN 的状态，并管理管理节点的自动故障切换。我们建议使用两个非管理 ISE 节点作为运行状况检查节点，一个用于主 PAN，一个用于辅助 PAN。如果仅使用一个运行状况检查节点，并且该节点发生故障，则不会发生自动故障切换。

当两个 PAN 都位于同一数据中心时，可以使用单个非管理 ISE 节点作为主 PAN 和辅助 PAN 的运行状况检查节点。当一个运行状况检查节点同时检查主 PAN 和辅助 PAN 的运行状况时，它将承担主动和被动两种角色。

运行状况检查节点为非管理节点，意味着它可以是策略服务、监控或 pxGrid 节点，或它们的组合。我们建议将与管理节点处于同一数据中心的 PSN 节点指定为运行状况检查节点。但是，在两个管理节点不在相同位置（局域网或数据中心）的小型部署或集中部署中，没有管理角色的任意节点 (PSN/pxGrid/MnT) 都可用作运行状况检查节点。

如果选择不启用自动故障切换，并且在主PAN发生故障时依赖手动升级辅助节点，则无需任何检查节点。

辅助 PAN 的运行状况检查节点

辅助 PAN 的运行状况检查节点是一个被动监控器。在辅助 PAN 升级为主 PAN 之前，它不执行任何操作。当辅助PAN接管主要节点职责时，其关联的运行状况检查节点会承担主动职责，为管理节点管理自动故障切换。之前主 PAN 的运行状况检查节点现在成为辅助 PAN 的运行状况检查节点，并对此节点执行被动监控。

禁用和重新启动运行状况检查

当从运行状况检查角色删除某个节点或禁用自动故障切换配置时，系统会在该节点上停止运行状况检查服务。在指定的高可用性运行状况检查节点上启用自动故障切换配置时，节点又开始检查管理节点的运行状况。在节点上指定或删除高可用性运行状况检查角色不涉及在该节点上重新启用应用；系统只会启动或停止运行状况检查活动。

如果高可用性运行状况检查节点重新启动，该节点会忽略主PAN的之前停机并重新开始检查运行状态。

运行状况检查节点

活动的运行状况检查节点按照已配置的轮询间隔检查主PAN的运行状况。它会向主PAN发送请求，如果接收到的响应符合配置，则运行状况检查节点认为主PAN的运行状况良好。否则，运行状况检查节点认为主 PAN 的运行状况不佳。如果主 PAN 的运行状况持续不佳，超过了所配置的故障切换期，则运行状况检查节点会开始故障切换至辅助 PAN 。

在运行状况检查期间，如果发现之前报告为不佳的运行状况在故障切换期内转为良好，则运行状况检查节点会将主 PAN 的状态标记为良好，并重置运行状况检查周期。

主PAN运行状况检查的响应会对照其运行状况检查节点上的配置值进行验证。如果响应不匹配则会发出警报。但是，会向辅助 PAN 发送升级请求。

更改运行状况节点

您可以更改用于运行状况检查的Cisco ISE 节点，但需要考虑一些事项。

例如，假定运行状况节点 (H1) 无法同步而另一个节点 (H2) 被指定为主 PAN 的运行状况检查节点。在这种情况下，一旦主 PAN 关闭，H1 就无法获知还存在另一个节点 (H2) 在检查相同的主 PAN。稍后，如果 H2 也关闭或断开网络连接，则需要真正的故障切换。但是，辅助 PAN 会保留拒绝升级请求的权利。因此，一旦辅助 PAN 升级为主要角色，则来自 H2 的升级请求就会被拒绝，并出现错误。即使主 PAN 的运行状况检查节点无法同步，它仍会继续检查主 PAN 的运行状况。

自动故障转移至辅助 PAN

您可以将Cisco ISE 配置为在主 PAN 不可用时自动升级辅助 PAN。此配置是在**部署 (Deployment)** 窗口中的主策略管理节点（主 PAN）上完成的。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。故障转移时间段定义为**故障转移**

前轮询失败次数 (Number of Failure Polls Before Failover) 中配置的次数乘以**轮询间隔 (Polling Interval)** 中配置的秒数。使用默认配置时，该时间为 10 分钟。将辅助 PAN 升级为主 PAN 需要额外 10 分钟。因此，默认情况下，从主 PAN 故障到辅助 PAN 工作的总时间为 20 分钟。

当辅助 PAN 收到故障转移调用时，会在真正执行故障转移前进行以下验证：

- 主 PAN 在网络中不可用。
- 故障转移请求来自有效的运行状况检查节点。
- 故障转移请求面向此 PAN。

如果这些验证全部通过，则辅助 PAN 会自行升级为主角色。

以下是（但不限于）会尝试辅助 PAN 自动故障转移的部分场景示例。

- 在轮询期间，就**故障转移前轮询失败次数 (Number of failure polls before failover)** 值而言，主 PAN 的运行状况持续不佳。
- 主 PAN 上的Cisco ISE 服务被手动停止，并在故障转移期间保持停止状态。
- 主 PAN 通过软停止或重新启动选项关闭，并在配置的故障转移期间保持关闭状态。
- 主 PAN 突然关闭（断电），并在故障转移期间保持关闭状态。
- 主 PAN 的网络接口关闭（网络端口关闭或网络服务停止），或由于任何其他原因导致运行状况检查节点无法与之接通，并在配置的故障转移期间保持关闭状态。

运行状况检查节点重新启动

重新启动后，高可用性运行状况检查节点会忽略主 PAN 之前的停机并重新检查运行状况。

在自动故障转移到辅助 PAN 情况下自带设备

当主 PAN 故障时，对于已具有由主 PAN 根 CA 链颁发的证书的终端，身份验证不会中断。这是因为部署中的所有节点都具有用于信任和验证目的的整个证书链。

但是，在辅助 PAN 升级为主 PAN 之前，不会激活新的自带设备。自带设备激活需要处于活动状态的主 PAN。

当原主 PAN 恢复或升级辅助 PAN 后，新的自带设备终端将激活，不会出现任何问题。

如果发生故障的主 PAN 无法重新作为主 PAN 加入，请在新升级的主 PAN（原辅助 PAN）上重新生成根 CA 证书。

对于现有证书链，触发新的根 CA 证书会自动生成从属 CA 证书。即使生成新的从属证书，由上一个链生成的终端证书也继续有效。

避免自动故障转移时的示例场景

以下是描绘将会避免运行状况检查节点进行自动故障转移或将会拒绝向辅助节点提出的升级请求的情况的一些示例场景。

- 收到升级请求的节点不是辅助节点。
- 辅助 PAN 收到的升级请求没有正确的主 PAN 信息。
- 从错误的运行状况检查节点收到升级请求。
- 收到升级请求，但是主 PAN 已启动并处于良好运行状况。
- 收到升级请求的节点不同步。

受 PAN 自动故障转移功能影响的功能

下表列出如果部署中启用 PAN 自动故障转移配置而被阻止或需要其他配置更改的功能。

功能	影响详细信息
被阻止的操作	
升级	通过 CLI 的升级被阻止。 将Cisco ISE 从旧版本升级到 1.4 版本之后，可配置 PAN 自动故障转移功能。默认情况下，此功能处于禁用状态。 要部署自动故障转移功能，必须至少有三个节点，其中两个节点承担管理角色，一个节点充当运行状况检查节点。运行状况检查节点为非管理节点，可以是 PSN、MnT、pxGrid 节点或其组合。如果PAN位于不同的数据中心，则每个PAN都必须有运行状况检查节点。
备份恢复	通过 CLI 和用户界面的恢复将被阻止。 如果PAN自动故障转移配置已在恢复之前启用，则必须在成功恢复后重新配置。
更改节点角色	通过用户界面更改以下节点角色的操作将被阻止： • 主 PAN 和辅助 PAN 中的管理角色 • PAN 的角色 • 在启用PAN自动故障转移功能后注销运行状况检查节点

功能	影响详细信息
其他 CLI 操作	以下通过 CLI 的管理员操作将被阻止： • 补丁安装和回滚 • DNS 服务器更改 • eth1、eth2 和 eth3 接口的 IP 地址更改 • eth1、eth2 和 eth3 接口的主机别名更改 • 时区更改
其他管理门户操作	通过用户界面执行的以下管理员操作将被阻止： • 补丁安装和回滚 • 更改 HTTPS 证书 • 将管理员身份验证类型从基于密码的身份验证更改为基于证书的身份验证，或者相反
连接设备最多的用户无法连接。	某些会话数据存储在故障 PAN 上，无法由 PSN 更新。
需要禁用 PAN 自动故障转移的操作	
CLI 操作	如果 PAN 自动故障转移配置已启用，则通过 CLI 执行的以下管理操作将显示警告消息。如果服务或系统未在故障转移窗口期内重新启动，则这些操作可能会触发自动故障转移。因此，在执行以下操作时，建议禁用 PAN 自动故障转移配置： • 手动停止Cisco ISE 服务 • 使用管理员 CLI 对Cisco ISE 进行软重新加载（重新引导）

配置自动故障转移的主 PAN

开始之前

要部署自动故障转移功能，您必须至少有三个节点，其中两个节点承担管理角色，一个节点充当运行状况检查节点。运行状况检查节点为非管理节点，可以是 PSN、MnT、pxGrid 节点或其组合。如果 PAN 位于不同的数据中心，则每个 PAN 都必须有运行状况检查节点。

步骤 1 登录主要 PAN 的用户界面。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **PAN 故障转移 (PAN Failover)**。

步骤 3 选中**启用 PAN 自动故障转移 (Enable PAN Auto Failover)** 复选框以启用主 PAN 的自动故障转移。

只能将辅助 PAN 升级为主 PAN。仅作为 PSN、MnT、pxGrid 节点或其组合的Cisco ISE 节点不能升级成为主 PAN。

步骤 4 从包含所有可用辅助节点的**主运行状况检查节点 (Primary Health Check Node)** 下拉列表中选择主 PAN 的运行状况检查节点。

建议将此节点保存在与主 PAN 相同的位置或数据中心。

步骤 5 从包含所有可用辅助节点的**辅助运行状况检查节点 (Secondary Health Check Node)** 下拉列表中选择辅助 PAN 的运行状况检查节点。

建议将此节点保存在与辅助 PAN 相同的位置或数据中心。

步骤 6 在**轮询间隔 (Polling Interval)** 中提供轮询间隔时间，在此时间之后，系统将检查 PAN 状态。有效范围为 30 - 300 秒。

步骤 7 为**故障转移前的故障轮询次数 (Number of Failure Polls before Failover)** 提供计数。

如果 PAN 的状态不适用于指定故障轮询次数，将发生故障转移。有效计数范围为 2 - 60。

步骤 8 点击**保存 (Save)**。

下一步做什么

将辅助 PAN 升级到主 PAN 之后，请执行以下操作：

- 手动同步旧的主 PAN 以将其带回至部署中。
- 手动同步任何其他不同步的辅助节点，以将其带回至部署中。

手动将辅助 PAN 升级为主 PAN

如果主 PAN 出现故障而且您没有配置 PAN 自动故障转移，则必须手动将辅助 PAN 升级为新的主 PAN。

开始之前

确保已配置具有管理角色的第二个Cisco ISE 节点，以将其升级为主 PAN。

步骤 1 登录辅助 PAN 的用户界面。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 在“编辑节点”(Edit Node) 页面，点击**升级为主节点 (Promote to Primary)**。

只能将辅助 PAN 升级为主 PAN。仅承担策略服务角色和/或监控角色的Cisco ISE 节点无法升级为主 PAN。

步骤 4 点击保存 **(Save)**。

下一步做什么

如果原来为主PAN的节点恢复运行，则会自动降级成为辅助PAN。必须对此节点（原来为主PAN）执行手动同步，才能将其恢复到部署中。

在辅助节点的**编辑节点 (Edit Node)** 页面，无法修改角色或服务，因为这些选项已禁用。您必须登录 Admin 门户才能进行更改。

将现有思科 ISE 部署的节点重新用作新思科 ISE 部署的主 PAN

如果要将现有Cisco ISE 部署的节点重新用作新Cisco ISE 部署的主 PAN，必须执行以下步骤：

步骤 1 首先按照适用于您的Cisco ISE 版本的《Cisco ISE 安装指南》所述，运行Cisco ISE 实用程序“执行系统擦除” https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

步骤 2 按照《Cisco ISE 安装指南》所述，执行Cisco ISE 的全新安装。

步骤 3 参阅配置主策略管理节点 (PAN)，第 33 页，将独立节点配置为主策略管理节点。

将服务恢复到主 PAN

Cisco ISE 不支持自动回退至原主 PAN。在启动到辅助 PAN 的自动故障切换后，如果将原主 PAN 重新接入网络，则应将其配置为辅助 PAN。

支持管理节点的自动故障转移

Cisco ISE 支持管理角色的自动故障转移。要启用自动故障转移功能，分布式设置中至少有两个节点应承担管理角色，一个节点应承担非管理角色。当主 PAN 关闭时，辅助 PAN 会自动升级。为此，系统将非管理辅助节点指定为每个PAN的运行状况检查节点。运行状况检查节点按配置的间隔检查主 PAN 的运行状况。如果收到的主 PAN 运行状况检查响应由于设备关闭或无法访问而不理想，运行状况检查节点会启动辅助PAN的升级，从而在等待已配置的阈值对应的时间后接管主角色。在辅助 PAN 自动故障转移后，有些功能不可用。Cisco ISE 不支持回退到原始主 PAN。有关详细信息，请参阅管理节点的高可用性部分。

策略服务节点

策略服务节点 (PSN) 是承担策略服务角色的Cisco ISE 节点，提供网络访问、终端安全评估、访客访问、客户端调配和分析服务。

分布式设置中至少有一个节点应当承担策略服务角色。此角色评估策略并制定所有决策。通常，分布式部署中会有多个 PSN。

驻留在同一高速局域网 (LAN) 中或负载均衡器后面的所有 PSN 可以组合在一起，形成一个节点组。如果节点组中的一个节点发生故障，其他节点会检测到故障，并重置任何 URL 重定向会话。

策略服务节点的高可用性

要检测节点故障并在故障节点上重置所有 URL 重定向的会话，可将两个或多个 PSN 放置在同一节点组中。当属于节点组的节点出现故障时，同一个节点组中的另一个节点会为故障节点上的所有 URL 重定向会话发出授权更改 (CoA) 请求。

同一个节点组中的所有节点都应在网络接入设备 (NAD) 上配置为 RADIUS 客户端并拥有 CoA 授权，因为这些节点中的任何一个节点均可为通过该节点组中的任一节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或是 RADIUS 服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。

虽然单个 NAD 可以配置多个Cisco ISE 节点以作为 RADIUS 服务器和动态授权客户端，但节点不必全部位于同一个节点组。

一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。请参阅 创建策略服务节点组，第 78 页 章节了解更多详细信息。

用于在 PSN 之间均匀分配请求的负载均衡器

如果您在部署中具有多个 PSN，则可以使用负载均衡器均匀分配请求。负载均衡器会将请求分配给其后面的功能节点。请参阅《思科和 F5 部署指南：使用 BIG-IP 的 ISE 负载均衡》中的信息并了解有关在负载均衡器后面部署 PSN 的最佳实践。

策略服务节点中的会话故障切换

节点组中的 PSN 共享会话信息。节点交换心跳消息以检测节点故障。如果某个节点出现故障，其节点组中的一个对等体会了解故障 PSN 上的会话并发出 CoA 以断开这些会话。大多数客户端会自动重新连接并建立新会话。

某些客户端不会自动重新连接。例如，如果客户端通过 VPN 连接，则此客户端可能看不到 CoA。作为 IP 电话、多主机 802.1X 端口或虚拟机的客户端也可能看不到或无法响应 CoA。URL 重定向客户端 (webauth) 也无法自动连接。这些客户端必须手动重新连接。

时间问题也会阻止重新连接。例如，如果发生 PSN 故障切换，终端安全评估处于待处理状态。

有关 PSN 会话共享的详细信息，请参阅轻量数据分配，第 62 页。

策略服务节点组中的节点数量

节点组中可以具有的节点数量取决于部署要求。节点组确保检测到节点故障，并且对等节点针对已获授权但尚未进行安全评估的会话发出 CoA。节点组的规模不必非常大。

如果节点组的规模增大，那么节点之间交换的消息和心跳数量也会显著增加。因此，流量也会随之增加。节点组中的节点较少时，有助于减少流量，同时提供足够的冗余来检测 PSN 故障。

节点组集群可以包含的 PSN 数量没有硬性限制。

轻量数据分配

轻量数据分布用于存储用户会话信息并在部署中的 PSN 之间复制这些信息，从而无需依赖 PAN 或 MnT 节点来获取用户会话详细信息。

轻量数据分布包括以下两个目录：

- Radius 会话目录
- 终端所有者目录

此外，还可以在**高级设置 (Advanced Settings)**下配置以下选项：

- **批量大小 (Batch Size)**：可以批量发送会话更新。此值可指定从一个轻量数据分布实例发送到部署中其他 PSN 的每一批记录的数量。如果此字段设置为 1，则不分批发送会话更新。默认值为 10 个记录。
- **TTL**：此值指定在更新轻量数据分布之前，会话等待批处理完成的最长时间。默认值为 1000 毫秒。

如果 PSN 之间存在连接问题（例如，当 PSN 关闭时），系统会从 MnT 会话目录检索会话详细信息并存储以供将来使用。

大型部署最多可以保留 2,000,000 个会话记录。小型部署可以存储 1,000,000 个会话记录。当收到会话的记账停止请求时，系统会从所有轻量数据分布实例中删除对应的会话数据。当存储的记录数量超过最大限制时，系统会根据时间戳删除最早的会话。

注释

- 如果会话的 IPv6 前缀长度小于 128 位并且未指定接口 ID，则 IPv6 前缀会被拒绝，从而防止多个会话具有相同的密钥。
- 轻量数据分布使用Cisco ISE 消息服务进行节点间通信。Cisco ISE 消息服务使用不同的证书（由内部 CA 链签名）。当遇到Cisco ISE 消息服务问题时，需要重新生成Cisco ISE 消息服务证书。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书签名请求 (Certificate Signing Request)**。在**证书将用于 (Certificate(s) will be used for)** 部分选择 **ISE 消息服务 (ISE Messaging service)**。点击**生成 ISE 消息服务证书 (generate ISE messaging service certificate)**。

Radius 会话目录

RADIUS 会话目录用于存储用户会话信息，并在部署中的 PSN 之间复制信息。**RADIUS 会话目录**仅存储授权更改 (CoA) 所需的会话属性。

自Cisco ISE 2.7 版起，默认启用此功能。您可以通过选中或取消选中**轻量数据分配 (Light Data Distribution)** 窗口中的 **RADIUS 会话目录 (RADIUS Session Directory)** 复选框启用或禁用此功能。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **轻量数据分配 (Light Data Distribution)**。

终端所有者目录

在Cisco ISE 版本 2.6 之前，当在策略服务节点 (PSN) 上收到的终端探测不同于最初为该特定终端处理请求的终端探测时，终端所有者将更改为新的 PSN。这会导致终端所有权摆动。

从Cisco ISE 版本 2.7 开始，**终端所有者目录**用于存储连接到Cisco ISE 的每个 MAC 地址的 PSN FQDN，并在部署中的 PSN 之间复制此数据。这可以避免终端所有权摆动，因为所有 PSN 现在都知道所有终端所有者。现在，仅当在另一个 PSN 上成功进行该终端的 RADIUS 身份验证后，终端所有权才会更改。

此外，静态终端分配优先于同一终端的传入探测器接收的属性，从而避免属性覆盖问题。

自Cisco ISE 2.7 版起，默认启用此功能。如果需要，您可以将其禁用以回退到不使用终端所有者目录的旧机制。**终端所有者目录**还用于分析，禁用此选项将使用传统分析器所有者的目录。您可以通过选中或取消选中**轻量数据分配 (Light Data Distribution)** 窗口中的**启用终端所有者目录 (Enable Endpoint Owner Directory)** 复选框启用或禁用此功能。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **轻量数据分配 (Light Data Distribution)**。

监控节点

承担监控角色的Cisco ISE 节点用作日志收集器，并将来自 PAN 和 PSN 的日志消息存储在网络中。此角色提供高级监控和故障排除工具，可用于有效地管理网络和资源。承担此角色的节点会整合并关联收集到的数据，以报告形式向您提供有意义的信息。

Cisco ISE 最多允许有两个节点承担此角色（由主或辅助节点承担此角色），以实现高可用性。主要和辅助 MnT 节点均收集日志消息。如果主 MnT 断开，则主 PAN 将指向辅助节点以收集监控数据。但辅助节点不会自动升级为主节点。可以通过手动修改 MnT 角色 来完成升级。

在分布式设置中，至少应有一个节点应承担监控角色。我们建议您不要对同一个Cisco ISE 节点启用监控和策略服务角色。我们建议您只将该节点用于监控，以实现最佳性能。

您可以从部署中的 PAN 访问监控 (Monitoring) 菜单。

注释 如果已启用 pxGrid，必须为 pxGrid 节点创建新证书。创建使用数字签名用法的证书模板，并生成新的 pxGrid 证书。

手动修改 MnT 角色

您可以从主要 PAN 手动修改 MnT 角色（从主要改为辅助，从辅助改为主要）。

步骤 1 登录主要 PAN 的用户界面。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 从节点列表中，选中要更改角色的 MnT 节点旁边的复选框。

步骤 4 点击**编辑 (Edit)**。

步骤 5 在**监控 (Monitoring)** 部分中，将角色更改为**主要 (Primary)** 或**辅助 (Secondary)**。

步骤 6 点击**保存 (Save)**。

注释 如果要禁用该节点上启用的所有其他角色和服务，可以启用**专用 MnT (Dedicated MnT)** 选项。启用此选项后，系统将停止该节点上的配置数据复制过程。这有助于提高MnT节点的性能。当禁用此选项时，将触发手动同步。

经思科 ISE 消息服务传递的系统日志

Cisco ISE 版本 2.6 为默认内置 UDP 系统日志收集目标 LogCollector 和 LogCollector2 提供 MnT WAN 生存性。要启用此生存性，请使用选项**使用“ISE 消息服务”将 UDP 系统日志发送到 MnT (Use "ISE Messaging Service" for UDP Syslogs delivery to MnT)**（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **系统 (System)** > **日志记录 (Logging)** > **日志设置 (Log Settings)**）。启用此选项时，UDP 系统日志受传输层安全 (TLS) 保护。

在Cisco ISE 版本 2.6 首次发货 (FCS) 中，**使用“ISE 消息服务”将 UDP 系统日志发送到 MnT (Use "ISE Messaging Service" for UDP Syslogs delivery to MnT)** 选项在默认情况下处于禁用状态。在Cisco ISE 版本 2.6 累积补丁 2 及更高版本中，此选项在默认情况下处于启用状态。

将Cisco ISE 消息服务用于 UDP 系统日志可在有限的持续时间内保留运行数据，即使无法访问 MnT 节点也是如此。MnT WAN 生存期约为 2 小时 30 分钟。

此服务使用 TCP 端口 8671。请相应地配置网络，并允许从部署中的所有其他Cisco ISE 节点连接到每个Cisco ISE 节点上的 TCP 端口 8671。以下功能也使用Cisco ISE 消息服务：轻型会话目录（请参阅《思科身份识别服务引擎管理员指南》中“在分布式环境中设置Cisco ISE”一章中的“轻型会话目录”部分分析转发器持久化队列。

注释 如果您的部署将 TCP 或安全系统日志用于思科 ISE 部署，则此功能与早期版本相同。

队列-链接警报

Cisco ISE 消息服务使用由内部 CA 链签名的不同证书。您可能会在Cisco ISE GUI 控制板的**警报 (Alarms)** Dashlet 中收到队列-链接警报。如果您正在执行任何部署操作（例如，将节点注册到部署、从主 PAN 手动同步节点、节点处于不同步状态或在节点中重新启动应用服务），则会触发此警报。确保符合以下条件以解决警报：

- 所有节点均已连接并同步。
- 所有节点和思科 ISE 消息服务均正常运行。
- 防火墙等外部实体不会阻止思科 ISE 消息服务端口。
- 每个节点上的思科 ISE 消息证书链未中断且证书状态良好。

如果满足上面列出的先决条件，则队列-链接警报将因以下操作而触发：

- 更改 PAN 或 PSN 的域名或主机名。
- 在新部署中恢复备份。
- 在升级后将旧的主 PAN 升级为新的主 PAN。

替换Cisco ISE 根 CA 链时，Cisco ISE 消息服务证书也将替换。此后将重新启动Cisco ISE 消息服务，停机时间约为 2 分钟。因此，系统日志将在此停机期间丢失。为避免在停机期间丢失系统日志，可在短时间内禁用Cisco ISE 消息服务。

启用或禁用Cisco ISE 消息服务以将 UDP 系统日志传送到 MnT：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **系统 (System)** > **日志记录 (Logging)** > **日志设置 (Log Settings)**。

步骤 2 选中或取消选中**使用“ISE 消息服务”将 UDP 系统日志传送到 MnT (Use “ISE Messaging Service” for UDP Syslogs delivery to MnT)** 复选框以启用或禁用 ISE 消息服务。

步骤 3 点击**保存 (Save)**。

MnT 节点中的自动故障转移

MnT 节点不提供高可用性，但支持主用备用。PSN 会将操作审核数据同时复制到主 MnT 节点和辅助 MnT 节点。

自动故障转移过程

当主 MnT 节点断开时，辅助 MnT 节点会接管所有监控和故障排除信息。

要将辅助节点转换为主节点，请参阅手动修改MnT角色。如果主节点在辅助节点升级后恢复运行，则将承担辅助节点的角色。如果未升级辅助节点，则主 MnT 节点将在恢复运行后继续承担主要角色。

⚠

注意 当主节点在故障转移后恢复正常时，请获取辅助节点的备份并恢复数据以更新主节点。

MnT 节点主用备用对设置指南

您可以在Cisco ISE 网络上指定两个 MnT 节点，然后将其配置为主用备用对。我们建议备份主 MnT 节点，然后将数据恢复到新的辅助 MnT 节点。由于会复制新数据，因此这可确保主 MnT 节点的历史记录与新的辅助节点同步。以下规则适用于主用备用对：

- 所有更改都会记录到主 MnT 节点。辅节点为只读。
- 对主节点所做的更改会在辅助节点上自动复制。
- 主节点和辅助节点列为日志收集器，其他所有节点会向其发送日志。
- Cisco ISE 控制面板是监控和故障排除的主要入口点。控制板上显示来自 PAN 的监控信息。如果主节点关闭，可以从辅助节点获得信息。
- 备份和清除 MnT 数据不在标准Cisco ISE 节点备份过程中。必须同时在主辅 MnT 节点上为备份和数据清除配置存储库，并且在每个节点上使用相同的存储库。

MnT 节点故障转移方案

以下方案适用于 MnT 节点对应的主用备用或单节点配置：

- 在 MnT 节点的主用备用配置中，主 PAN 始终指向主 MnT 节点以收集监控数据。在主 MnT 节点故障后，PAN 会指向备用 MnT 节点。从主节点到辅助节点的故障转移发生在其关闭超过五分钟后。

  但是，在主节点发生故障后，辅助节点不会成为主节点。如果主节点启动，PAN 会再次开始从恢复的主节点收集监控数据。

- 如果主 MnT 节点关闭，并且您希望将备用 MnT 节点升级为主用状态，则可以通过手动修改 MnT 角色或注销现有主 MnT 节点来实现。注销现有 MnT 节点时，备用节点成为主 MnT 节点，并且 PAN 自动指向新升级的主节点。
- 在主用-备用对中，如果注销辅助 MnT 节点或辅助 MnT 节点关闭，则现有主 MnT 节点仍然为当前主节点。
- 如果Cisco ISE 部署中只有一个 MnT 节点，则该节点用作主 MnT 节点，并向 PAN 提供监控节点。但是，当注册新 MnT 节点并使其成为部署中的主节点时，现有主 MnT 节点会自动成为备用节点。PAN 会指向新注册的主 MnT 节点以收集监控数据。

监控数据库

鉴于监控功能使用的数据的比例和数量，需要在专用节点上将一个单独的数据库用于这些用途。

像 PSN 一样，MnT 节点有一个专用数据库，要求您执行维护任务，例如本节所涵盖的主题所涉及的任务：

监控数据库的备份和恢复

监控数据库处理大量数据。随着时间推移，MnT 节点的性能和效率取决于您对这些数据的管理水平。要提高效率，我们建议您定期备份数据并将其传输到远程存储库。通过计划自动备份，您可以将此任务自动化。

注释 如果正在进行清除操作，则不应执行备份。如果在清除操作过程中启动备份，则清除操作会停止或失败。

如果注册辅助 MnT 节点，我们建议先备份主 MnT 节点，然后将数据恢复到新的辅助 MnT 节点。由于会复制新的更改，因此这可确保主 MnT 节点的历史记录与新的辅助节点同步。

监控数据库清除

清除过程允许您通过以月为单位指定在清除期间保留数据的时间，管理监控数据库的大小。默认值为三个月。当达到清除流程的磁盘空间使用率阈值（占磁盘空间的百分比）时，会用到此值。对于该选项，每月包括 30 天。三个月的默认值等于 90 天。

监控数据库清除指南

请遵循以下监控数据库磁盘使用量的相关指南：

- 如果监控数据库磁盘使用量超过 80% 的阈值设置，则会生成严重警报，表示数据库大小已超过所分配的磁盘容量。如果磁盘使用量超过百分之九十，则会生成另一个警报。

  系统将运行清除过程，并创建状态历史报告，可以在**数据清除审核 (Data Purging Audit)** 窗口中查看该报告。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **数据清除审核 (Data Purging Audit)**。清除完成后会生成信息 (INFO) 警报。

- 清除同样依据数据库已使用的磁盘空间。当监控数据库已使用的磁盘空间达到或超过阈值时（默认为 80%），则会启动清除过程。此过程仅删除最近七天的监控数据，不论在管理员门户中进行了怎样的配置。系统将循环继续此过程直至磁盘空间使用量低于百分之八十。系统总会在检查监控数据库磁盘空间限制之后，才继续执行清除。

运营数据清除

Cisco ISE 监控操作数据库包含作为Cisco ISE 报告生成的信息。在Cisco ISE 最新版本中，可以选择在运行Cisco ISE 管理 CLI 命令 **application configure ise** 后清除监控操作数据并重置监控数据库。

清除选项用于清除数据，会通过提示符询问保留天数。重置选项用于将数据库重置为出厂默认设置，这将永久删除所有备份的数据。如果文件占用了文件系统的过多空间，您可以重置数据库。

注释 重置选项会导致思科 ISE 服务在系统完成重启前暂时不可用。

操作数据清除 (Operational Data Purging) 窗口包含**数据库利用率 (Database Utilization)** 和**立即清除数据 (Purge Data Now)** 区域。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **操作数据清除 (Operational Data Purging)**。可以查看总可用数据库空间，以及存储在**数据库利用率 (Database Utilization)** 区域中的 RADIUS 和 TACACS 数据。您可以将鼠标悬停在状态栏上以显示可用磁盘空间，以及现有数据存储在数据库中的天数。可以指定在**数据保留期 (Data Retention Period)** 区域保留 RADIUS 和 TACACS 数据的时间段。系统在每天凌晨 4 点清除数据，此外，您还可以进行配置，以在清除数据前通过指定保留天数将其导出到存储库。可以选中**启用导出存储库 (Enable Export Repository)** 复选框以选择和创建存储库，并指定**加密密钥**。

在**立即清除数据 (Purge Data Now)** 区域中，可以清除所有 RADIUS 和 TACACS 数据，或指定天数以在超过该天数时将数据清除。

注释 可以在清除前将 RADIUS 身份验证和记账、TACACS 授权和记账、RADIUS 错误和错误配置的请求方表导出到存储库。

相关主题

清除较旧的运营数据，第 68 页

清除较旧的运营数据

运营数据在一段时间内收集到服务器上。可以立即或定期清除它。可以通过查看**数据清除审核 (Data Purging Audit)** 报告，验证数据清除是否成功。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **运行数据清除 (Operational Data Purging)**。

步骤 2 执行以下操作之一：

- 在**数据保留期 (Data Retention Period)** 区域：
  1. 以日为单位指定 RADIUS 和 TACACS 数据的应保留期限。指定期限之前的所有数据都会导出到存储库。
  2. 在**存储库 (Repository)** 区域中，选中**启用导出存储库 (Enable Export Repository)** 复选框以选择保存数据的存储库。
  3. 在**加密密钥 (Encryption Key)** 文本框中，输入所需的密码。
  4. 点击**保存 (Save)**。

注释　如果配置的保留期限短于与诊断数据对应的现有保留阈值，则配置值将覆盖现有阈值。例如，如果将保留期配置为三天，而且该值小于诊断表中的现有阈值（例如，默认值为五天），则将根据在此窗口中配置的值（三天）清除数据。

- 在**立即清除数据 (Purge Data Now)** 区域：
  1. 选择清除所有数据或清除超过指定天数的数据。数据不会保存在任何存储库中。
  2. 点击**清除 (Purge)**。

配置用于自动故障切换的监控节点

如果部署中有两个MnT节点，则可以配置用于自动故障切换的主节点-辅助节点对，以避免Cisco ISE监控服务出现停机。主节点-辅助节点对可确保辅助 MnT 节点在主节点出现故障时自动提供监控。

开始之前

- 要配置用于自动故障切换的 MnT 节点，必须将这些节点注册为Cisco ISE 节点。
- 您必须在两个节点上配置监控角色和服务，适当地根据其主要和辅助角色进行命名。
- 在主要和辅助MnT节点上同时配置用于备份和数据清除的存储库。要让备份和清除功能正常运行，请对这两个节点使用相同的存储库。清除同时在冗余对的主要和辅助节点中发生。例如，如果主要 MnT 节点将两个存储库用于备份和清除，则必须为辅助节点指定相同的存储库。

  使用系统 CLI 中的 **repository** 命令为 MnT 节点配置数据存储库。

> ⚠ **注意**　要让计划的备份和清除在监控冗余对的节点上正常工作，请使用 CLI 在主节点和辅助节点上同时配置相同的存储库。存储库不会自动在两个节点之间同步。

在Cisco ISE 控制板中，验证 MnT 节点是否准备就绪。**系统摘要 (System Summary)** Dashlet 会在 MnT 节点服务准备就绪时显示左侧带绿色复选标记的 MnT 节点。

步骤 1　在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2　在**部署节点 (Deployment Nodes)** 窗口中，选中要指定主节点的 MnT 节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3　点击**常规设置 (General Settings)** 选项卡，然后从**角色 (Role)** 下拉列表中选择**主要 (Primary)**。

选择 MnT 节点作为主节点时，另一个 MnT 节点将自动成为辅助节点。如果是独立部署，主要和辅助角色配置会处于禁用状态。

步骤 4 点击**保存 (Save)**。主节点和辅助节点都会重新启动。

思科 pxGrid 节点

可以使用Cisco pxGrid 与其他网络系统（例如Cisco ISE 生态系统合作伙伴系统）和其他Cisco平台共享Cisco ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在Cisco ISE 与第三方供应商之间、在节点（例如共享标记）与策略对象之间交换策略和配置数据，还能进行其他信息的交换。Cisco pxGrid 还允许第三方系统调通过自适应网络控制操作 (EPS) 来隔离用户和/或设备以应对网络或安全事件。可通过Cisco TrustSec 主题将标签定义、值和说明等Cisco TrustSec 信息从Cisco ISE 传输到其他网络。可通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从Cisco ISE 传输到其他网络。Cisco pxGrid 还支持标签和终端配置文件的批量下载。

可通过Cisco pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅 安全组标记交换协议 ，第 929 页。

在高可用性配置中，Cisco pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 关闭时，Cisco pxGrid 服务器会停止处理客户端注册和订用。需要手动升级 PAN，以激活Cisco pxGrid 服务器。可以查看“思科 pxGrid 服务”(Cisco pxGrid Services) 窗口（“管理”(Administration) > “pxGrid 服务”(pxGrid Services)）以验证思科 pxGrid 节点当前处于主用状态还是备用状态。

在活动 Cisco pxGrid 1.0 节点上，这些进程显示为**正在运行 (Running)**。在备用 Cisco pxGrid 1.0 节点上，它们显示为**已禁用 (Disabled)**。如果活动 pxGrid 1.0 节点关闭，备用 pxGrid 节点会检测到此情况，并启动四个 pxGrid 进程。在几分钟内，这些进程显示为**正在运行 (Running)**，备用节点成为活动节点。可以运行 CLI 命令 **show logging application pxgrid** 或 **show logging application pxgrid.state** 来验证Cisco pxGrid 服务在此节点上是否处于备用状态。

对于 XMPP（可扩展消息传送和在线状态协议）客户端，Cisco pxGrid 节点在主用-备用高可用性模式下工作，这意味着Cisco pxGrid 服务在主用节点上处于“正在运行”(Running) 状态，在备用节点上处于“已禁用”(Disabled) 状态。

注释 在Cisco pxGrid 1.0 中，节点在主用-备用高可用性模式下工作表示Cisco pxGrid 服务在主用节点上处于“正在运行”(Running) 状态，在备用节点上处于“已禁用”(Disabled) 状态。可以运行 CLI 命令 **show logging application pxgrid** 或 **show logging application pxgrid.state** 来验证Cisco pxGrid 在此节点上是否处于备用状态。pxGrid 2.0 不存在此问题，pxGrid 显示备用。

启动面向辅助Cisco pxGrid 节点的自动故障切换后，如果原始主Cisco pxGrid 节点重新接入网络，则除非当前主节点关闭，否则原始主Cisco pxGrid 节点将继续具有辅助角色，并且不会重新升级到主角色。

注释 有时，原始主思科 pxGrid 节点可能会自动重新升级回主角色。

在高可用性部署中，当主 pxGrid 节点关闭时，可能需要大约 3 到 5 分钟来切换到辅助 pxGrid 节点。建议客户端等待故障切换完成，然后再清除缓存数据，以防主Cisco pxGrid 节点发生故障。

以下日志可用于Cisco pxGrid 节点：

- pxgrid.log：状态变更通知。
- pxgrid-cm.log：有关客户端与服务器之间的发布者和/或用户以及数据交换活动的更新。
- pxgrid-controller.log：显示客户端功能、组和客户端授权的详细信息。
- pxgrid-jabberd.log：与系统状态和身份验证相关的所有日志。
- pxgrid-pubsub.log：与发布者和用户事件相关的信息。

注释 如果在节点上禁用思科 pxGrid 服务，则端口 5222 将关闭，但是端口 8910（由 Web 客户端使用）将正常工作，并将继续对请求作出响应。

注释 可以使用思科 ISE Advantage 许可证启用 Cisco pxGrid 和 Cisco pxGrid 角色。

注释 应定义Cisco pxGrid，以便使用被动 ID 工作中心。有关详细信息，请参阅 被动 ID 工作中心 ，第 514 页。

部署思科 pxGrid 节点

在独立节点和分布式部署节点上都可以启用Cisco pxGrid 角色。

开始之前

- 您必须具有Cisco ISE Advantage 许可证才能启用Cisco pxGrid 角色。
- 有关许可要求，请参阅 ISE 许可/订购。
- 所有节点都将 CA 证书用于Cisco pxGrid 服务用途。如果在升级之前对Cisco pxGrid 服务使用默认证书，则升级时会将该证书替换为内部 CA 证书。
- 必须为 Websocket (pxGrid 2.0) 打开端口 8910，并为 XMPP (pxGrid V1.0) 打开端口 5222。如果在节点上禁用Cisco pxGrid 服务，则端口 5222 将关闭，但是端口 8910 仍正常工作，并继续响应请求。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 在**部署节点 (Deployment Nodes)** 窗口中，选中要为其启用Cisco pxGrid 服务的节点旁的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**常规设置 (General Settings)** 选项卡， 启用 **pxGrid** 切换按钮。

步骤 4 点击**保存 (Save)**。

当从以前的版本升级时，系统可能会禁用**保存 (Save)** 选项。当浏览器缓存引用以前版本的Cisco ISE 中的旧文件时，就会发生这种情况。清除浏览器缓存以启用**保存 (Save)** 选项。

配置思科 pxGrid 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid服务 (pxGrid Services)** > **设置 (Settings)**。

步骤 2 根据您的需求选择以下选项：

- **自动审批新的基于证书的帐户 (Automatically approve new certificate-based accounts)**：选中此复选框可自动批准来自新Cisco pxGrid 客户端的连接请求。
- **允许创建基于密码的帐户 (Allow password based account creation)**：选中此复选框可为Cisco pxGrid 客户端启用基于用户名或密码的身份验证。如果启用此选项，则无法自动批准Cisco pxGrid 客户端。

  Cisco pxGrid 客户端可以通过 REST API 发送用户名，从而向Cisco pxGrid 控制器注册自身。在客户端注册时，Cisco pxGrid 控制器会为Cisco pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。

步骤 3 点击**保存 (Save)**。

您可以使用Cisco pxGrid **设置 (Settings)** 窗口上的**测试 (Test)** 选项对Cisco pxGrid 节点执行运行状况检查。在 pxgrid 或 pxgrid-test.log 文件中可以查看详细信息。

生成思科 pxGrid 证书

开始之前

某些版本的Cisco ISE 具有使用 NetscapeCertType 的Cisco pxGrid 证书。建议您生成新证书。

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 必须从主 PAN 生成Cisco pxGrid 证书。
- 如果Cisco pxGrid 证书使用了使用者替代名称 (SAN) 扩展名，请确保将使用者身份的 FQDN 包含为 DNS 名称条目。

- 创建使用数字签名用法的证书模板，并使用该模板生成新的Cisco pxGrid 证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **客户端管理 (Client Management)** > **证书 (Certificates)**。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **生成无证书签名请求的单个证书 (Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。
- **生成单个证书（带证书签名请求）Generate a single certificate (with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。
- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载根证书，并将其添加到受信任证书存储区。必须指定主机名和证书的下载格式。

步骤 3 **通用名称 (CN) (Common Name (CN))**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入 pxGrid 客户端的 FQDN。

步骤 4 **证书签名请求详细信息 (Certificate Signing Request Details)**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入完整的证书签名请求详细信息。

步骤 5 **说明**：（可选）可以输入此证书的说明。

步骤 6 **证书模板 (Certificate Template)**：点击 **pxGrig_Certificate_Template** 链接可下载证书模板，并根据您的要求进行编辑。

步骤 7 **使用者备用名称 (SAN) (Subject Alternative Name (SAN))**：可以添加多个 SAN。可提供以下选项：

- **IP 地址 (IP address)**：输入要与证书关联的Cisco pxGrid 客户端的 IP 地址。
- **FQDN**：输入 pxGrid 客户端的完全限定域名。

注释　如果选定**生成批量证书 (Generate Bulk Certificate)** 选项，则不会显示此字段。

步骤 8 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE) ----”标签。终端实体的私钥使用 PKCS* PEM 存储。其开头采用“-----加密私钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密私钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。
- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format (including certificate chain; one file for both the certificate chain and key))**：CA 根证书、CA 中间证书以及终端实体的证书和私钥存储在一个加密文件时，所采用的二进制格式。

步骤 9 **证书密码 (Certificate Password)**：输入证书的密码，并在下一字段中再次输入以确认密码。

步骤 10 点击**创建 (Create)**。

您创建的证书在Cisco ISE 的**已颁发证书 (Issued Certificates)** 窗口中可见。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发证书 (Issued Certificates)**。证书也会下载到浏览器的“下载”目录中。

注释 从Cisco ISE 2.4 补丁 13 开始，pxGrid 服务的证书要求变得更加严格。如果您使用Cisco ISE 默认自签名证书作为 pxGrid 证书，则Cisco ISE 可能会在应用Cisco ISE 2.4 补丁 13 或更高版本后拒绝此证书。这是因为此证书的旧版本具有指定为 **SSL 服务器 (SSL Server)** 的 **Netscape 证书类型 (Netscape Cert Type)** 扩展，此扩展现在会失败（现在还需要客户端证书）。

任何具有不合规证书的客户端都无法与Cisco ISE 集成。使用内部 CA 颁发的证书或生成具有正确使用扩展名的新证书：

- 证书中的**密钥使用 (Key Usage)** 扩展必须包含**数字签名 (Digital Signature)** 和**密钥加密 (Key Encipherment)** 字段。
- 证书中的**扩展密钥使用 (Extended Key Usage)** 扩展必须包含**客户端身份验证 (Client Authentication)** 和**服务器身份验证 (Server Authentication)** 字段。
- 不需要 **Netscape 证书类型 (Netscape Certificate Type)** 扩展。如果要包含此扩展，则必须在扩展中同时添加 **SSL 客户端 (SSL Client)** 和 **SSL 服务器 (SSL Server)**。
- 如果使用的是自签名证书，则**基本约束 CA (Basic Constraints CA)** 字段必须设置为 True，并且**密钥使用 (Key Usage)** 扩展必须包含**密钥证书签名 (Key Cert Sign)** 字段。

Cisco pxGrid 客户端的控制权限

您可以创建 Cisco pxGrid 授权规则来控制 Cisco pxGrid 客户端的权限。使用这些规则可控制提供给 Cisco pxGrid 客户端的服务。

您可以创建不同类型的组，并将提供给 Cisco pxGrid 客户端的服务映射到这些组。使用**客户端管理 (Client Management)** 窗口中的**组 (Groups)** 选项可添加新组。您可以在**客户端管理 (Client Management)** > **策略 (Policies)** 窗口中查看使用预定义组（如 EPS 和 ANC）的预定义授权规则。请注意，只能更新预定义规则的**自定义操作 (Custom Operations)** 字段。

要为 pxGrid 客户端创建授权规则，请执行以下操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **客户端管理 (Client Management)** > **策略 (Policy)**。

步骤 2 从**服务 (Service)** 下拉列表中，选择以下选项之一：

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

步骤 3 从**操作 (Operation)** 下拉列表中，选择以下选项之一：

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

  注释　　如果选择此选项，可以指定自定义操作。

步骤 4 从**组 (Groups)** 下拉列表中，选择要映射到此服务的组。

预定义组（如 EPS 和 ANC）和手动添加的组列在此下拉列表中。

查看部署中的节点

在**部署节点 (Deployment Nodes)** 窗口，可以查看部署中的所有思科 ISE 节点（主节点和辅助节点）。

步骤 1 登录主Cisco ISE 管理员门户。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击左侧导航窗格中的 **Deployment**。

列出部署中的所有Cisco ISE 节点。

从 MnT 节点下载终端统计数据

您可以从MnT节点下载联网终端的统计数据。关键性能指标(KPM)，其中包括负载、CPU使用率、身份验证流量数据，您使用这些指标监控并排除网络中的问题。在Cisco ISE 命令行界面 (CLI) 中使用 **application configure ise** 命令并选择选项 12 或 13 来分别下载每日 KPM 统计信息或过去八周的 KPM 统计信息。

此命令的输出提供以下终端数据：

- 网络中的终端总数
- 成功建立连接的终端数量
- 身份验证失败的终端数量
- 每日连接的新终端总数
- 每日连接的终端总数

输出还包括时间戳详情、通过部署中各策略服务节点 (PSN) 连接的终端总数、终端总数、活动的终端、负载以及身份验证流量详情。

请参阅思科身份服务引擎 *CLI* 参考指南查看有关此命令的更多信息。

数据库崩溃或文件损坏问题

如果 Oracle 数据库文件因断电或其他原因导致数据丢失而损坏，则Cisco ISE 可能会崩溃。根据具体的事件，按照以下步骤恢复丢失的数据。

- 如果部署中发生 PAN 损坏，则应将辅助 PAN 升级为主 PAN。
- 如果由于小型部署或任何其他原因导致无法升级辅助 PAN，请恢复最新的可用备份。
- 如果 PSN 损坏，请按照以下步骤取消注册、重置配置并重新注册节点。
- 如果是独立设备，请恢复最新的可用备份。

注释 定期从独立设备中获取备份，以避免丢失最新的配置更改。

设备的监控配置

MnT 节点会接收网络中设备的数据，并用于填充控制板显示内容。要启用 MnT 节点与网络设备之间的通信，必须正确配置交换机和 NAD。

同步主要和辅助思科 ISE 节点

只能通过主 PAN 对Cisco ISE 的配置进行更改。系统会将配置更改复制到所有辅助节点。如果出于某些原因未能正常执行复制，则可以手动同步辅助 PAN 与主 PAN。

步骤 1 登录到主 PAN。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 选中要与主 PAN 同步的节点旁边的复选框，然后点击**同步 (Syncup)** 强制执行数据库完全复制。

更改节点角色和服务

您可以编辑Cisco ISE 节点配置来更改在节点上运行的角色和服务。

开始之前

- 当启用或禁用在PSN上运行的任何服务或对PSN进行任何更改时，将会重新启动运行这些服务的应用服务器进程。这些服务重新启动时，预计会有延迟。
- 由于服务重新启动时的这一延迟，可能会启动自动故障转移（如果在部署中已启用）。要避免此问题，请确保关闭自动故障转移配置。

步骤 1 登录到主 PAN。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 选中要更改其角色或服务的节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 4 选择所需的角色和服务。

步骤 5 点击**保存 (Save)**。

步骤 6 验证在主 PAN 上是否收到警报，以确认角色或服务更改。如果未成功保存角色或服务更改，则不会生成警报。

在思科 ISE 中修改节点的影响

在Cisco ISE 中对节点进行以下任一更改后，节点将重新启动，这会导致延迟：

- 注册节点（独立节点至辅助节点）
- 注销节点（辅助节点至独立节点）
- 将主要节点更改为独立节点（如果未向其注册任何其他节点；主要节点至独立节点）
- 升级管理节点（辅助节点升级为主节点）
- 更改角色（当向某个节点分配策略服务或监控角色或从该节点删除角色时）
- 修改策略服务节点中的服务（启用或禁用会话和分析器服务）
- 恢复主要节点上的备份，然后系统会触发一项同步操作，将数据从主要节点复制到辅助节点

创建策略服务节点组

当两个或多个策略服务节点 (PSNs) 连接到同一高速局域网 (LAN) 时，建议您将他们放入同一个节点组中。通过保留较少的本地组重要属性以及减少复制到网络中远程节点的信息，此设计对终端分析数据复制进行了优化。节点组成员还检查对等组成员的可用性。如果该组检测到某成员发生故障，则尝试重置和恢复失败节点上所有 URL 重定向的会话。

注释 我们建议您将同一个本地网络中的所有 PSN 放入同一个节点组。要加入同一个节点组，PSN 不需要成为负载均衡集群的一部分。但是，负载均衡集群中的每个本地 PSN 通常应该属于同一个节点组。

注释 节点组用于对实施 URL 重定向（终端安全评估服务、访客服务和 MDM）的会话执行 PSN 故障转移。

在您将 PSN 作为成员添加进某个节点组之前，您必须首先创建该节点组。您可以从管理员门户的“部署”(Deployment) 页面创建、编辑和删除 PSN 组。

开始之前

节点组成员可以通过 TCP/7800 通信。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 点击左侧导航窗格顶部的**设置 (Settings)** 图标。

步骤 3 点击**创建节点组 (Create Node Group)**。

步骤 4 输入节点组的唯一名称。

步骤 5 （可选）输入节点组的说明。

步骤 6 （可选）选中**启用 MAR 缓存分布 (Enable MAR Cache Distribution)** 复选框并填写其他选项。在启用此选项之前，请确保在 **Active Directory** 窗口中启用 MAR。

步骤 7 点击**提交 (Submit)** 保存节点组。

保存节点组之后，节点组应显示在左侧的导航窗格中。如果节点组未显示在左侧窗格中，则可能已隐藏。点击导航窗格中的**展开 (Expand)** 按钮可查看隐藏的对象。

下一步做什么

将节点添加到节点组。从**策略服务 (Policy Service)** 区域的**在节点组中包含节点 (Include node in node group)** 下拉列表中选择节点组，对节点进行编辑。

从部署中删除节点

要从部署中删除节点，您必须注销该节点。已注销的节点会成为独立Cisco ISE 节点。

它保留其从主 PAN 接收的最新配置，并且承担独立节点的默认角色，包括“管理”(Administration)、“策略服务”(Policy Service) 和“监控”(Monitoring)。如果注销 MnT 节点，则此节点将不再是系统日志目标。

注销主 PSN 时，终端数据将丢失。如果您希望 PSN 在成为独立节点后保留终端数据，可以执行以下任一操作：

- 从主 PAN 获取备份，并在 PSN 成为独立节点时在其上恢复此数据备份。
- 将 PSN 的角色更改为“管理”(Administration)（辅助 PAN），从管理员门户的**部署 (Deployment)** 窗口同步数据，然后注销节点。此节点现在拥有所有数据。然后可以将辅助 PAN 添加至现有部署。

可以从主 PAN 的**部署 (Deployment)** 窗口查看这些更改。但是，预计更改会延迟 5 分钟生效并显示在**部署 (Deployment)** 窗口上。

开始之前

在从部署中删除任何辅助节点之前，请对Cisco ISE 配置执行备份，稍后可在需要时恢复该备份。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选择要删除的辅助节点旁边的复选框，然后点击**注销 (Deregister)**。

步骤 3 点击**确定 (OK)**。

步骤 4 验证在主PAN上是否收到警报，以确认辅助节点成功注销。如果从主PAN注销辅助节点失败，则不会生成警报。

关闭思科 ISE 节点

从Cisco ISE 命令行界面 (CLI) 发出 `halt` 命令之前，建议您停止Cisco ISE 应用服务，并确保它不执行任何备份、恢复、安装、升级或删除操作。如果在Cisco ISE 执行上述任一操作时发出 halt 命令，您将会收到以下其中一条警告消息：

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

在使用 halt 命令时，如果系统没有运行任何进程，或如果您输入`是 (Yes)`来回应显示的警告消息，则必须回答以下问题：

```
Do you want to save the current configuration?
```

如果输入`是 (Yes)`保存现有Cisco ISE 配置，系统将显示以下消息：

```
Saved the running configuration to startup successfully.
```

注释 建议您在重新引导设备之前停止应用进程。

也可以重新引导Cisco ISE。有关详细信息，请参阅《思科身份识别服务引擎 CLI 参考指南》

更改独立思科 ISE 节点的主机名或 IP 地址

可以更改独立Cisco ISE 节点的主机名、IP 地址或域名。不能使用 `localhost` 作为节点的主机名。

开始之前

如果Cisco ISE 节点是分布式部署的一部分，必须将其从部署中删除并确保该节点为独立节点。

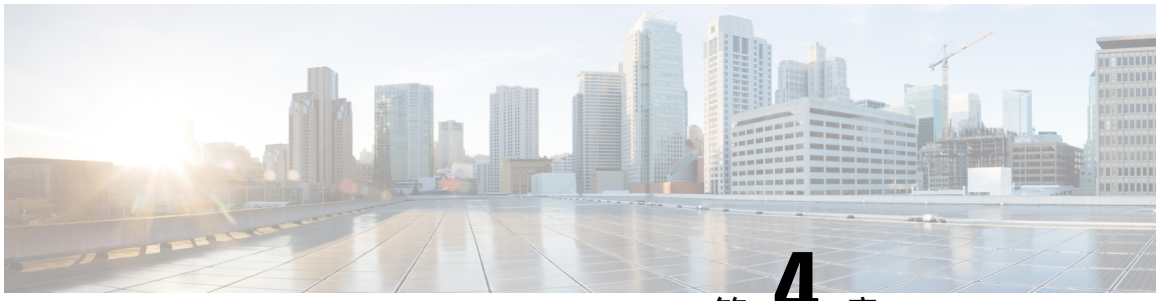
步骤 1 从Cisco ISE CLI 使用 **hostname**、**ip address** 或 **ip domain-name** 命令更改Cisco ISE 节点的主机名或 IP 地址。

步骤 2 从Cisco ISE CLI 使用 **application stop ise** 命令重置Cisco ISE 应用配置以重启所有服务。

步骤 3 如果Cisco ISE 节点为分布式部署的一部分，则将其注册到主 PAN。

注释 如果您在注册Cisco ISE 节点时使用主机名，注册的独立节点的完全限定域名 (FQDN) 必须可以从主 PAN 进行 DNS 解析，例如 FQDN 可以为 *abc.xyz.com*。否则，节点注册将失败。必须输入作为 DNS 服务器上分布式部署一部分的Cisco ISE 节点的 IP 地址和 FQDN。

将Cisco ISE注册为辅助节点后，主PAN会将IP地址、主机名或域名中的更改复制到您的分布式部署中另一个Cisco ISE 节点。



第 4 章

基本设置

管理门户

图 *2:* 思科 ***ISE*** 管理门户

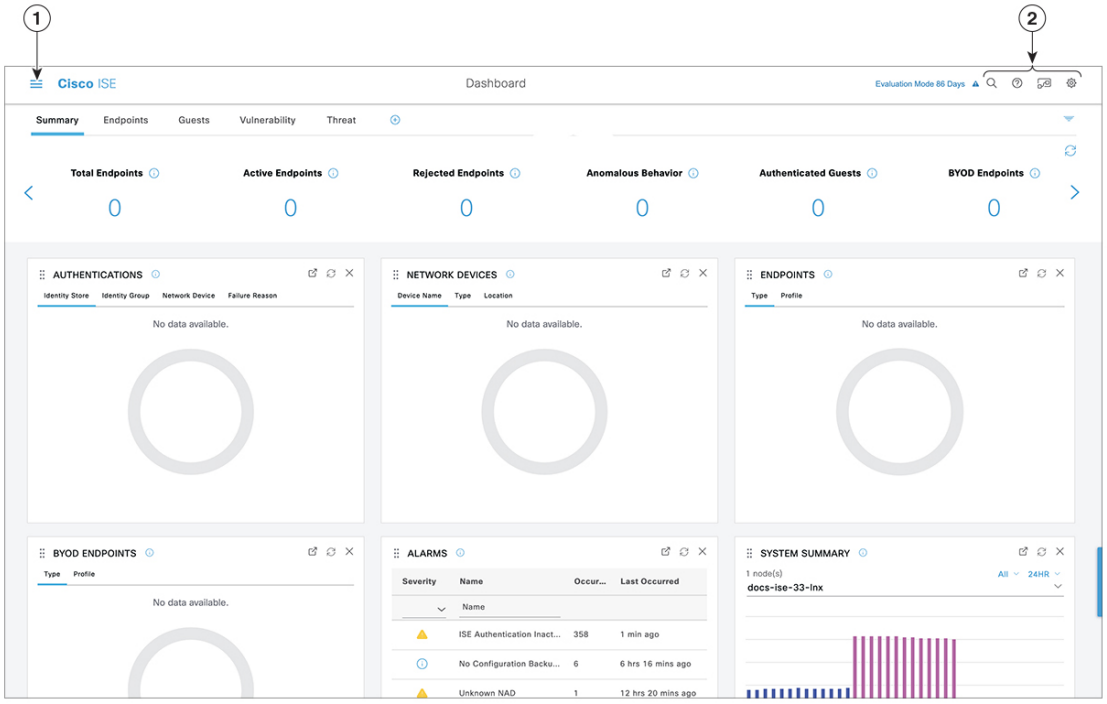
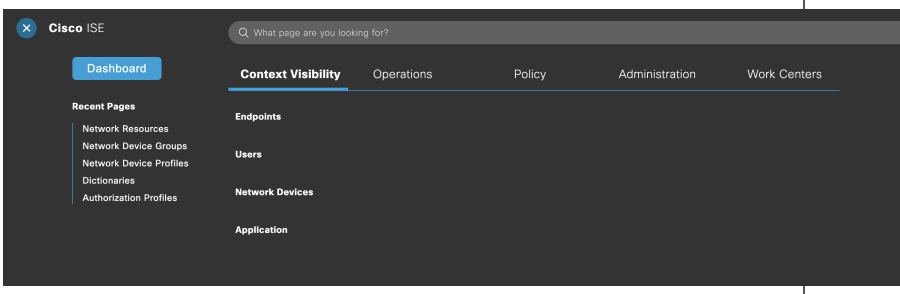


表 *11:* 思科 *ISE* 管理门户的组件

1	菜单图标	点击包含以下菜单的滑入式窗口的**菜单 (Menu)** 图标 (☰)。滑入式菜单窗口还包含一个搜索栏，您可以在其中找到所需的窗口。点击主页的**控制板 (Dashboard)**。 图 *3:* 思科 *ISE* 主菜单  • **情景可视性 (Context Visibility)**：情景可视性窗口显示有关终端、用户和网络访问设备 (NAD) 的信息。情景可视性信息按功能、应用、自带设备 (BYOD) 和其他类别进行细分，具体取决于您注册的许可证。情景可视性窗口使用中央数据库并从数据库表、缓存和缓冲区收集信息。因此，情景可视性 Dashlet 和列表中的内容会快速更新。情景可视性窗口由上方的 Dashlet 和底部的信息列表组成。通过修改列表中的列属性来过滤数据时，Dashlet 会刷新以显示修改的内容。 • **策略 (Policy)**：“策略”(Policy) 窗口包含用于管理身份验证、授权、分析、安全评估和客户端调配区域中的网络安全的工具。 • **管理 (Administration)**：“管理”(Administration) 窗口包含用于管理Cisco ISE 节点、许可证、证书、网络设备、用户、终端和访客服务的工具。

2	右上角菜单图标	

- 

  使用此图标搜索终端并按配置文件、故障、身份库、位置、设备类型等显示其分布。

- 

  点击此图标可查看交互式帮助 菜单，由此可访问多个资源。

- 

  点击此图标可访问以下选项：

  - **PassiveID 设置 (PassiveID Setup)**：**PassiveID 设置 (PassiveID Setup)** 选项将启动 **PassiveID 设置 (PassiveID Setup)** 向导以使用 Active Directory 设置被动身份。配置服务器以从外部身份验证服务器收集用户身份和 IP 地址，并将经过身份验证的 IP 地址传送给相应的用户。

  - **可视性设置 (Visibility Setup)**：**可视性设置 (Visibility Setup)** 是一种价值证明 (PoV) 服务，它收集终端数据，例如应用、硬件资产、USB 状态、防火墙状态和 Windows 终端的总体合规性状态。然后，收集的数据将发送到Cisco ISE。当您启动 **ISE 可视性设置 (ISE Visibility Setup)** 向导时，可指定 IP 地址范围，以便对首选网段或一组终端运行终端发现。

    该 PoV 服务使用 Cisco Stealth Temporal 代理收集终端安全评估数据。Cisco ISE 会将 Cisco Stealth Temporal 代理推送到具有管理员帐户类型的运行 Windows 的计算机，该帐户会自动运行临时可执行文件以收集情景信息。然后，代理会自行删除。要体验 Cisco Stealth Temporal 代理的可选调试功能，请选中**终端日志记录 (Endpoint Logging)** 复选框（点击**菜单 (Menu)** 图标 () 并选择**可视性设置 (Visibility Setup)** > **终端安全评估 (Posture)**），将调试日志保存在一个或多个终端中。您可以在以下任一位置查看日志：

    - C:\WINDOWS\syswow64\config\systemprofile\（64 位操作系统）
    - C:\WINDOWS\system32\config\systemprofile\（32 位操作系统）

  - **运行终端脚本 (Run Endpoint Scripts)**：选择此选项可在连接的终端上运行脚本，以执行符合组织要求的管理任务。这包括卸载过时软件、启动或终止进程或应用以及启用或禁用特定服务等任务。

- 

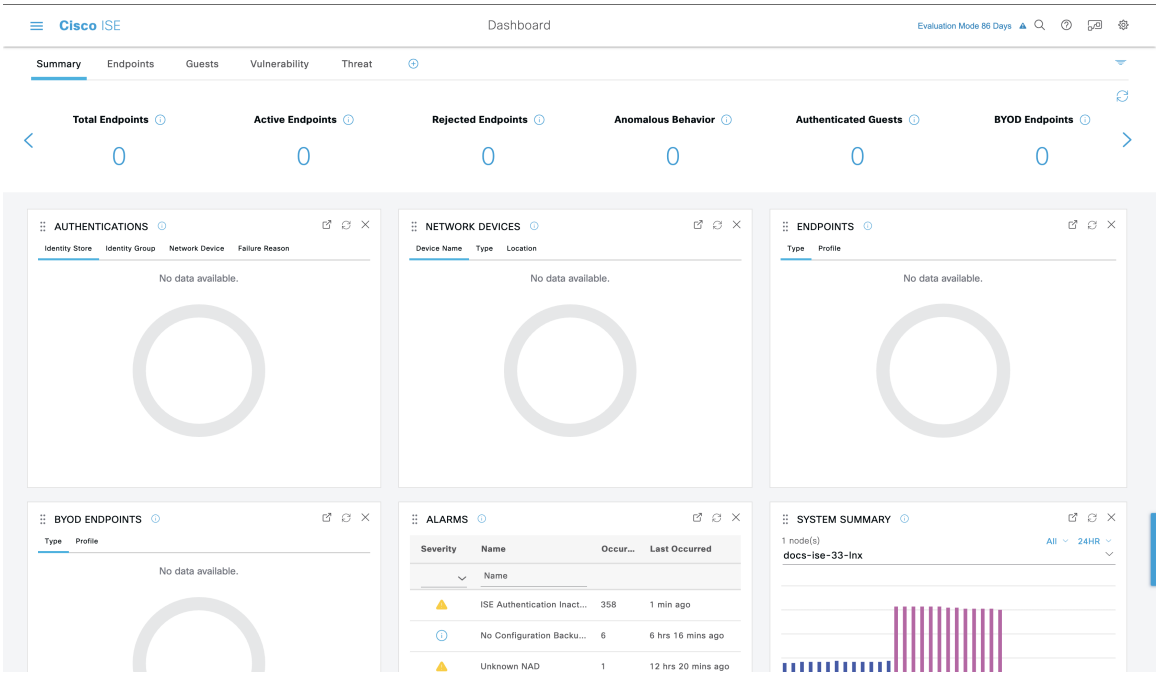
  点击此图标可查看系统活动的菜单，包括启动在线帮助和配置帐

		户设置。

思科 ISE 主页控制板

Cisco ISE 主页控制板显示对于有效地进行监控和故障排除很重要的综合性相关统计数据。控制板元素通常显示 24 小时内的活动。下图是Cisco ISE 控制板上提供的一些信息示例。仅可以在主策略管理节点 (PAN) 门户上查看Cisco ISE 控制板数据。

图 *4:* 思科 *ISE* 主页控制板



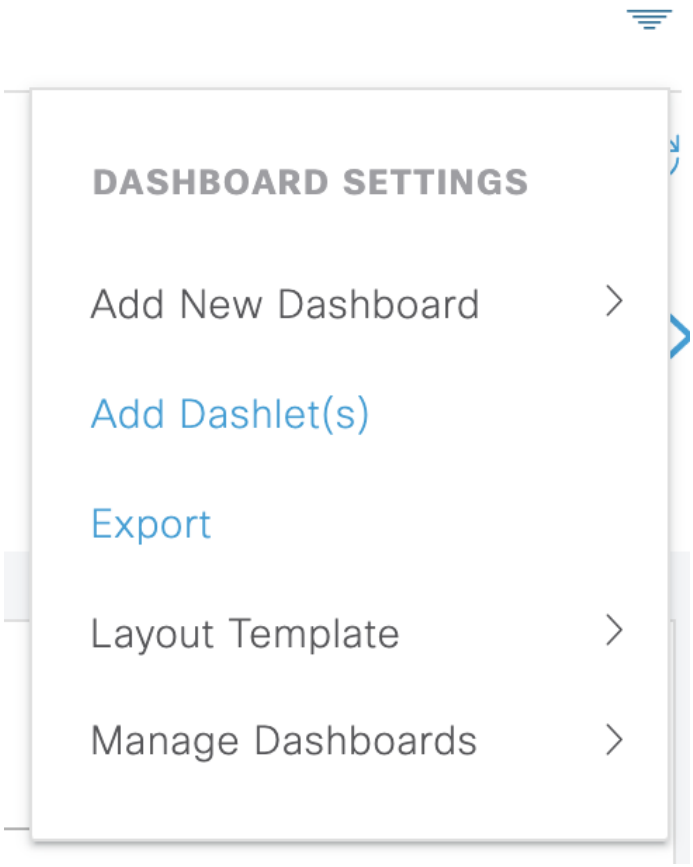
主页有五个显示Cisco ISE 数据的默认控制板。其中每个控制板都有多个预定义的 Dashlet。

- **摘要 (Summary)**：此控制板包含线性指标 Dashlet、饼形图 Dashlet 和列表 Dashlet。指标 Dashlet 不可配置。默认情况下，此控制板包含**状态 (Status)**、**终端 (Endpoints)**、**终端类别 (Endpoint Categories)** 和**网络设备 (Network Devices)** Dashlet。
- **终端 (Endpoints)**：默认情况下，此控制板包含**状态 (Status)**、**终端 (Endpoints)**、**终端类别 (Endpoint Categories)** 和**网络设备 (Network Devices)** Dashlet。
- **访客 (Guests)**：此控制板包含提供有关访客用户类型、登录失败和活动位置的信息的 Dashlet。
- **漏洞 (Vulnerability)**：此控制板显示漏洞服务器向Cisco ISE 报告的信息。
- **威胁 (Threat)**：此控制板显示威胁服务器向Cisco ISE 报告的信息。

配置主页控制面板

您可以点击页面右上角的**倒金字塔**图标来自定义主页控制板：

图 *5:* 自定义控制板



下拉列表中显示以下选项：

- **添加新控制板 (Add New Dashboard)** 可以让您添加新的控制板。在显示的字段中输入值，然后点击**应用 (Apply)**。
- **添加 Dashlet (Add Dashlet(s))** 会显示一个对话框，其中包含可用的 Dashlet 列表。点击 Dashlet 名称旁边的**添加 (Add)** 或**删除 (Remove)**，可从控制板添加或删除 Dashlet。
- **导出 (Export)** 会将选定的主页视图保存为 PDF。
- **布局模板 (Layout Template)** 会配置此视图中显示的列数。
- **管理控制板 (Manage Dashboards)** 包含两个选项：
  - **标记为默认控制板 (Mark As Default Dashboard)**：选择此选项可将当前控制板设为您选择主页时的默认视图。

- **重置所有控制板 (Reset All Dashboards)**：使用此选项可以重置所有控制板，并删除所有主页控制板上的配置。

情景可视性视图

“情景可视性”(Context Visibility) 页面的结构类似于主页，不同之处在于“情景可视性”(Context Visibility) 页面：

- 当您过滤显示数据时，保留当前环境（浏览器窗口）
- 可定制程度更高
- 侧重终端数据

您可以仅从主要管理节点 (PAN) 上查看情景可视性数据。

情景 (Context) 页面上的 Dashlet 显示有关终端和终端到 NAD 的连接信息。当前显示的信息取决于每个页面上的 Dashlet 下数据列表中的内容。每页根据选项卡名称显示终端数据视图。过滤数据时，列表和 Dashlet 都将更新。您可以点击圆形图的一个或多个部分，也可以过滤表中的行，或者任意组合这些操作来过滤数据。在您选择过滤器时，效果是可以叠加的，也称为级联过滤器，可让您深入查找想要的特定数据。您也可以点击列表中的终端，获得该终端的详细视图。

“情景可视性”(Context Visibility) 下有四个主视图：

- 终端 - 您可以根据设备类型、合规状态、身份验证类型、硬件清单等选择要显示哪些终端。有关其他信息，请参考硬件控制板 ，第 94 页部分。

注释 我们建议在 NAD 上启用记账设置，以确保将记账开始和更新信息发送到思科 ISE。

仅当启用记账后，Cisco ISE 才能收集记账信息，如最新的 IP 地址、会话状态（已连接、已断开或已拒绝）、终端的非活动天数。这些信息显示在“实时日志/实时会话”(Live Logs/Live Session) 和“情景可视性”(Context Visibility) 页面中。在 NAD 上禁用记账时，“实时日志/实时会话”(Live Logs/Live Session) 和“情景可视性”(Context Visibility) 页面之间的记账信息可能缺失、不正确或不匹配。

注释 通过“可视性设置”(Visibility Setup) 向导，可以为终端发现添加 IP 地址范围列表。配置此向导后，Cisco ISE 会对终端进行身份验证，但未包含在配置的IP地址范围内的终端不会显示在“情景可视性”(Context Visibility) >“终端”(Endpoints) 选项卡和终端列表页面（在“工作中心”(Work Centers)>“网络访问”(Network Access)>“身份”(Identities)>“终端”(Endpoints)）中。

- 基于用户 (User-Based) - 显示来自用户身份源的用户信息。

  使用此视图时请注意以下几点：

  1. 如果用户名或密码属性发生任何更改，当身份验证状态发生变化时，将立即反映在此页面上。
  2. 如果在 Active Directory 中更改了除用户名以外的任何其他属性，则更新后的属性仅在重新身份验证后 24 小时后显示。
  3. 如果在 Active Directory 中更改用户名和其他属性，则更新后的更改将在重新身份验证后立即显示。

- 网络设备 (Network Devices) - 已连接终端的 NAD 列表。您可以点击 NAD 上的终端数量（最右列），以显示一个“情景可视性”(Context Visibility) 屏幕，其中列出按照该 NAD 过滤的所有设备。

  注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的网络设备会话状态摘要报告（“操作”[Operations]>“报告”[Reports] >“目录”[Catalog] >“网络设备”[Network Device]>“会话状态摘要”[Session Status Summary]）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。

- 应用 (Application) -“应用”(Application) 视图用于确定已安装指定应用的终端数量。结果以图形和表格格式显示。图形表示形式可帮助进行比较分析。例如，可以在表和条形图中找到使用 Google Chrome 软件的终端数量及其版本、供应商和类别（反网络钓鱼、浏览器等）。有关详细信息，请参阅应用控制板部分。

您可以在情景可视性 (Context Visibility) 下创建新视图，以创建自定义列表来进行其他过滤。此版本的自定义视图不支持 Dashlet。

在 Dashlet 中点击圆形图的一部分，打开新页面，其中包含在情景可视性 (Context Visibility) 模式下通过该Dashlet过滤的数据。在该新页面中，可以继续过滤所显示的数据，如在视图中过滤显示的数据，第 97 页中所述。

有关使用情景可视性查找终端数据的详细信息，请参阅以下使用 ISE 2.1 的Cisco YouTube 视频 https://www.youtube.com/watch?v=HvonGhrydfg。

相关主题

硬件控制板 ，第 94 页

情景可视性中的属性

为情景可视性提供属性的系统和服务有时对相同属性名称有不同值。几个示例如下所示：

操作系统

- *OperatingSystem* - 终端安全评估操作系统
- *operating-system* - NMAP 操作系统
- *operating-system-result* - 分析器整合操作系统

注释 在思科 ISE 中为终端启用多个探测时，“情景可视性”(Context Visibility) 页面中显示的终端操作系统数据可能存在一些差异。

门户名称

- *Portal.Name* - 打开设备注册时的访客门户名称
- *PortalName* - 未打开设备注册时的访客门户名称

门户用户

- *User-Name* - 来自 RADIUS 身份验证的用户名
- *GuestUserName* - 访客用户
- *PortalUser* - 门户用户

应用控制板

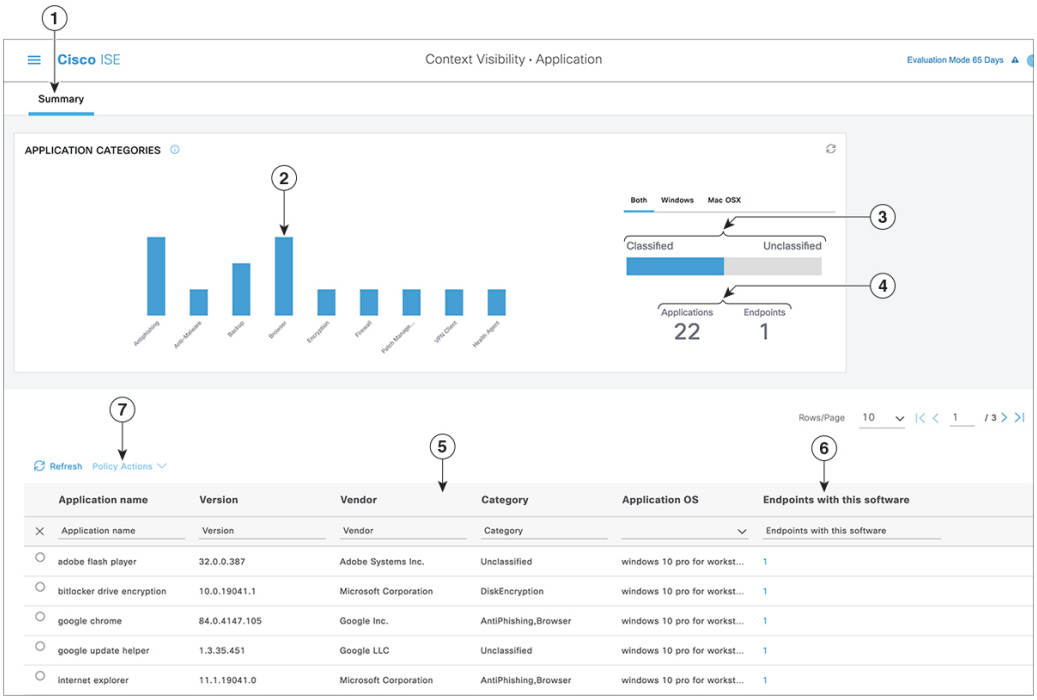


表 *12:* 应用控制板的说明

编号	说明
1	系统会默认选择**摘要 (Summary)** 选项卡。它显示**应用类别 (Application Categories)** Dashlet，其中包含条形图。应用分为 13 个类别：不属于这些类别的应用称为“未分类”应用。 可用类别包括防恶意软件、反钓鱼、备份、浏览器、防数据丢失、数据存储、加密、防火墙、即时消息程序、补丁管理、公共文件共享、虚拟机和 VPN 客户端。
2	每个条形对应一个类别。您可以将鼠标悬停在每个条形上，以查看与所选应用类别对应的应用和终端总数。
3	属于“分类”(Classified) 类别的应用和终端以蓝色显示。未分类的应用和终端显示为灰色。您可以将鼠标悬停在分类或未分类的类别条上，以查看属于该类别的应用和终端的总数。您可以点击**分类 (Classified)**，查看条形图和表 (5) 中的结果。当您点击**未分类 (Unclassified)** 时，条形图被禁用（灰显），结果显示在表 (5) 中。
4	系统根据所选过滤器显示应用和终端。您可以在点击不同的过滤器时查看浏览路径记录。您可以点击**清除所有过滤器 (Clear All Filters)**，删除所有过滤器。

<table>
<tr><th>编号</th><th>说明</th></tr>
<tr><td>5</td><td>当您点击多个条形时，表中会显示相应的分类应用和终端。例如，如果您选择“防恶意软件”(Antimalware) 和“补丁管理”(Patch Management) 类别，则显示以下结果。
<table>
<tr><th>应用名称</th><th>版本</th><th>供应商</th><th>类别</th><th>应用操作系统</th><th>有此软件的终端</th></tr>
<tr><td>网守</td><td>9.9.5</td><td>Apple Inc.</td><td>反恶意软件</td><td>windows 7 64 位、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
<tr><td>网守</td><td>10.9.5</td><td>Apple Inc.</td><td>反恶意软件</td><td>Windows 8 64 位、mac osx 10.10</td><td>3</td></tr>
<tr><td>软件更新</td><td>2.3</td><td>Apple Inc.</td><td>补丁管理</td><td>windows 7 64 位、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>点击表中有此软件的终端 (Endpoints With This Software) 列中的某个终端，查看终端详细信息，例如 Mac 地址、NAD IP 地址、NAD 端口 ID/SSID，IPv4 地址等。</td></tr>
<tr><td>7</td><td>您可以选择一个应用名称并从策略操作 (Policy Actions) 下拉列表中选择创建应用合规性 (Create App Compliance) 选项，以创建应用合规性条件和补救。</td></tr>
</table>

硬件控制板

“情景可视性”(Context Visibility) 下的“端点硬件”(Endpoint Hardware) 选项卡可以帮助您收集、分析和报告短时间内的终端硬件资产信息。可以收集信息，例如查找内存容量低的终端或查找终端的 BIOS 型号/版本。可以根据这些结果增加内存容量或升级 BIOS 版本。可以在计划购买资产之前评估要求。可以确保及时更换资源。可以收集此信息，而无需安装任何模块或与终端交互。总而言之，可以有效地管理资产生命周期。

在传出数据包通过以太网微处理器退出前，此 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **硬件 (Hardware)** 页面显示**制造商 (Manufacturers)** 和**终端利用率 (Endpoint Utilizations)** Dashlet。这些 Dashlet 反映基于所选过滤器的更改。**制造商 (Manufacturers)** Dashlet 显示装有 Windows 和 Mac OS 的终端的硬件资产详细信息。**终端利用率 (Endpoint Utilizations)** 面板显示终端的 CPU、内存和磁盘利用率。可以选择三个选项中的任何一个，以查看利用率百分比。

- CPU 使用率超过 n% 的设备。
- 内存使用率超过 n% 的设备。
- 磁盘使用率超过 n% 的设备。

注释 硬件资产数据需要 120 秒才能显示在 ISE GUI 中。将收集硬件资产数据以提供终端安全评估合规和不合规状态。

注释
- “硬件可视性”(Hardware Visibility) 页面中的快速过滤器至少需要 3 个字符才能生效。另一种使快速过滤器高效工作的方法是，在输入字符后点击其他列属性的过滤器。
- 一些列属性显示为灰色，这是因为此表仅用于根据与硬件相关的属性进行过滤。
- 操作系统过滤器仅适用于**制造商 (Manufacturers)** 图表。它与下面的表无关。

终端及其连接的外部设备的硬件属性以表格格式显示。系统将显示以下硬件属性：

- MAC 地址
- BIOS 制造商 (BIOS Manufacturer)
- BIOS 序列号 (BIOS Serial Number)
- BIOS 型号 (BIOS Model)
- 附加设备 (Attached Devices)
- CPU 名称
- CPU 速度 (GHz) (CPU Speed (GHz))
- CPU 利用率 (%) (CPU Usage (%))
- 核心数量
- 处理器数量 (Number of Processors)
- 内存 (GB) (Memory Size (GB))
- 内存使用率 (%) (Memory Usage (%))
- 内部磁盘总大小 (GB) (Total Internal Disk(s) Size (GB))
- 内部磁盘总可用大小 (GB) (Total Internal Disk(s) Free Size (GB))
- 内部磁盘总使用率 (%) (Total Internal Disk(s) Usage (%))
- 内部磁盘数 (Number of Internal Disks)
- NAD 端口 ID (NAD Port ID)
- 状态
- 网络设备名称
- 位置

- UDID
- IPv4 地址
- 用户名
- 主机名 (Hostname)
- 操作系统类型
- 异常行为
- 终端配置文件
- 说明
- 终端类型
- 身份组
- 注册日期
- 身份库
- 授权配置文件

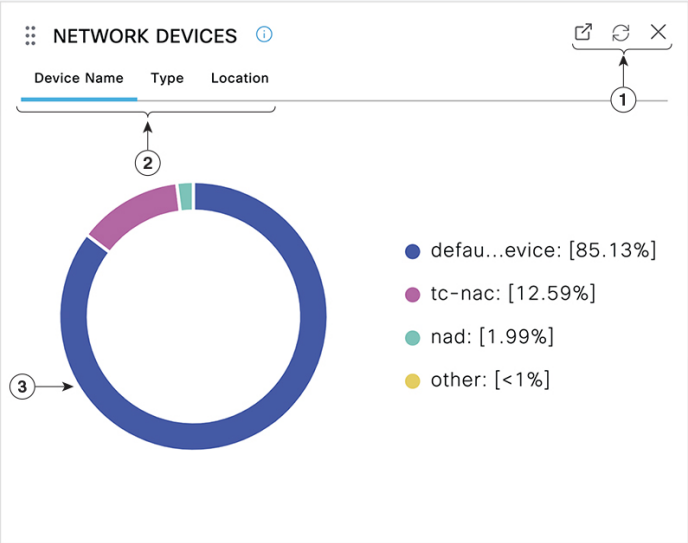
可以点击**已连接设备 (Attached Devices)** 列中与终端对应的编号，以查看当前连接到终端的 USB 设备的名称、类别、制造商、类型、产品 ID 和供应商 ID。

注释 Cisco ISE 会分析客户端系统的硬件属性，但对于某些硬件属性，Cisco ISE 不会进行分析。这些硬件属性可能不会显示在“硬件情景可视性”(Hardware Context Visibility) 页面中。

可以在以下位置控制硬件资产数据收集间隔 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)** 页面。默认间隔为 5 分钟。

Dashlet

下图是 Dashlet 的示例：



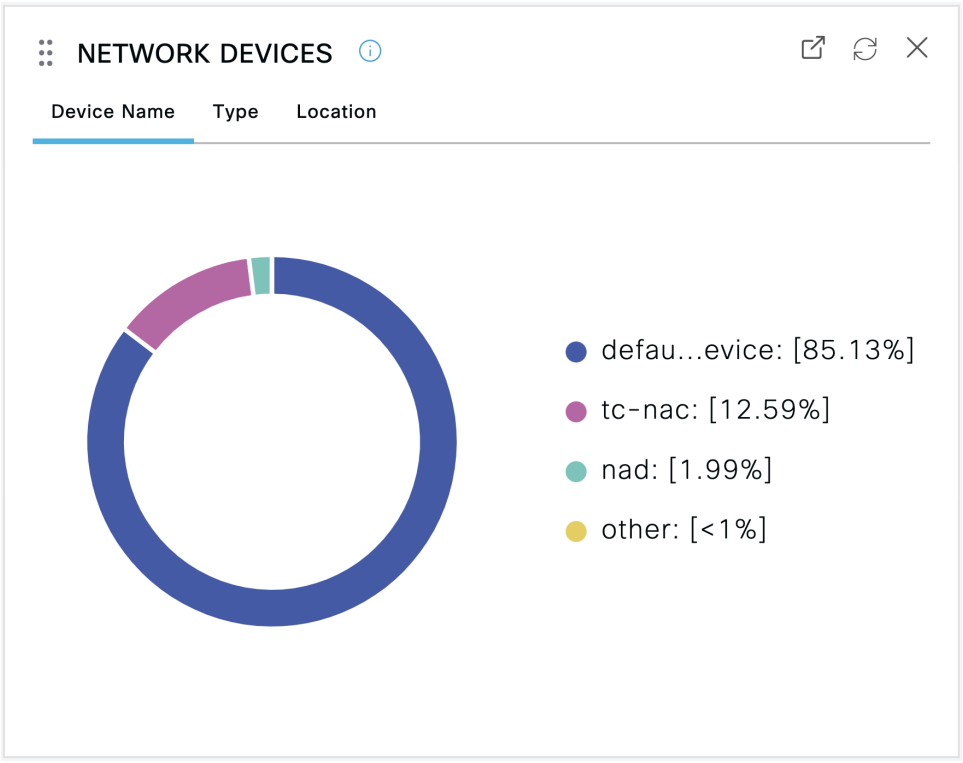
1. 打开新窗口图标表示可在新的浏览器窗口中打开此Dashlet。圆圈用于刷新。**X**用于删除此Dashlet，但仅在主页上可用。使用屏幕右上角的齿轮符号可删除情景可视性 (Context Visibility) 中的Dashlet。
2. 某些 Dashlet 具有不同类别的数据。点击类别以查看该数据集的饼形图。
3. 饼形图显示您已选择的数据。点击其中一个饼形区域将在情景可视性 (Context Visibility) 中打开新选项卡,其中包含基于该饼形区域过滤得到的数据。

在主页控制面板中点击该饼形图的一部分，将打开一个新的浏览器窗口，其中显示由您点击的饼形图部分过滤得到的数据。

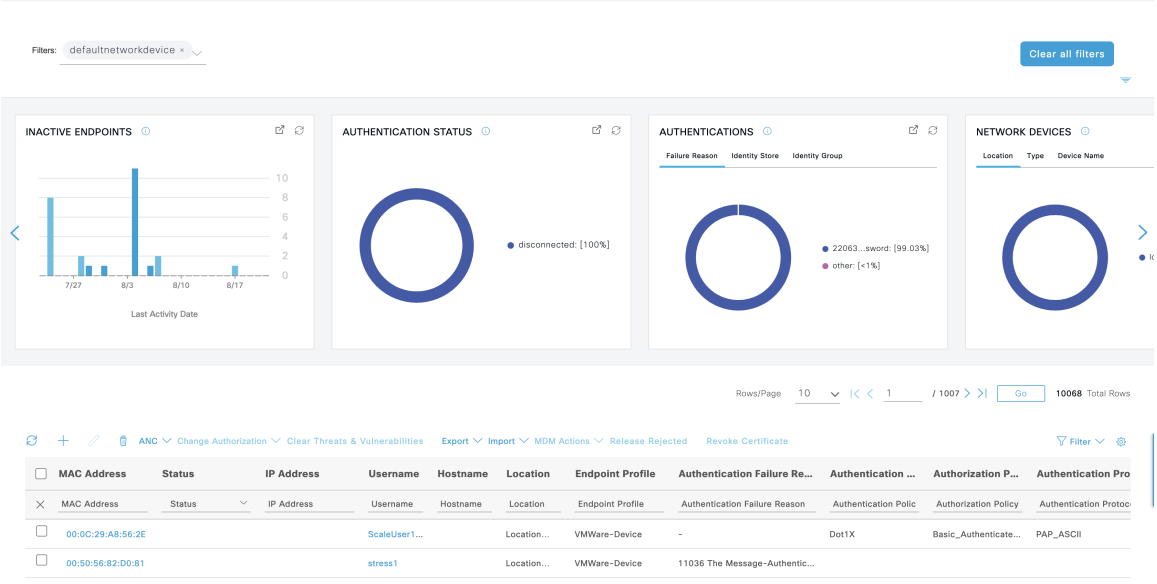
在情景视图 (Context Visibility) 中点击该饼形图的一部分将过滤显示数据，但不会更改情景；已过滤数据显示在同一浏览器窗口中。

在视图中过滤显示的数据

点击情景可视性 (Context Visibility) 页面上的任何 dashlet，可按您点击的项目过滤显示的数据，例如，饼图的一部分。



如果在**网络设备 (Network Devices)** Dashlet 中点击 **defau...evice**，系统会显示包含数据的新窗口，如下图所示：



通过点击饼图的更多部分进一步过滤数据。您还可以使用**过滤器 (Filter)** 下拉列表或数据列表右上角的齿轮图标来管理显示的数据。

您可以保存您的自定义过滤器。

创建自定义过滤器

可以创建和保存自定义过滤器，并修改预设过滤器中的筛选条件。自定义过滤器不保存在Cisco ISE数据库中。只能使用用于创建自定义过滤器的同一计算机和浏览器访问这些过滤器。

步骤 1 点击**显示 (Show)** 下拉列表，然后选择**高级过滤器 (Advanced Filter)**。

步骤 2 从 Filter 菜单中指定搜索属性，如字段、运算符和值。

步骤 3 点击 **+** 可添加更多条件。

步骤 4 点击**开始 (Go)** 可显示与指定属性匹配的条目。

步骤 5 点击**保存 (Save)** 图标可保存过滤器。

步骤 6 输入名称，然后点击**保存 (Save)**。过滤器现在显示在“显示”(Show) 下拉列表中。

使用高级过滤器按条件过滤数据

您可以使用高级过滤器根据指定的条件（例如 First Name = Mike and User Group = Employee）过滤信息。您可以指定不止一个条件。

步骤 1 点击**显示 (Show)** 下拉列表，然后选择**高级过滤器 (Advanced Filter)**。

步骤 2 从“过滤器”(Filter) 菜单指定搜索属性（例如字段、运算符和值）。

步骤 3 点击 **+** 可添加更多条件。

步骤 4 点击**开始 (Go)** 可显示与指定属性匹配的条目。

使用快速过滤器按字段属性过滤数据

通过快速过滤器，您可以输入列表页面中显示的任何字段属性的值，引用页面，并且仅列出与筛选条件相匹配的记录。

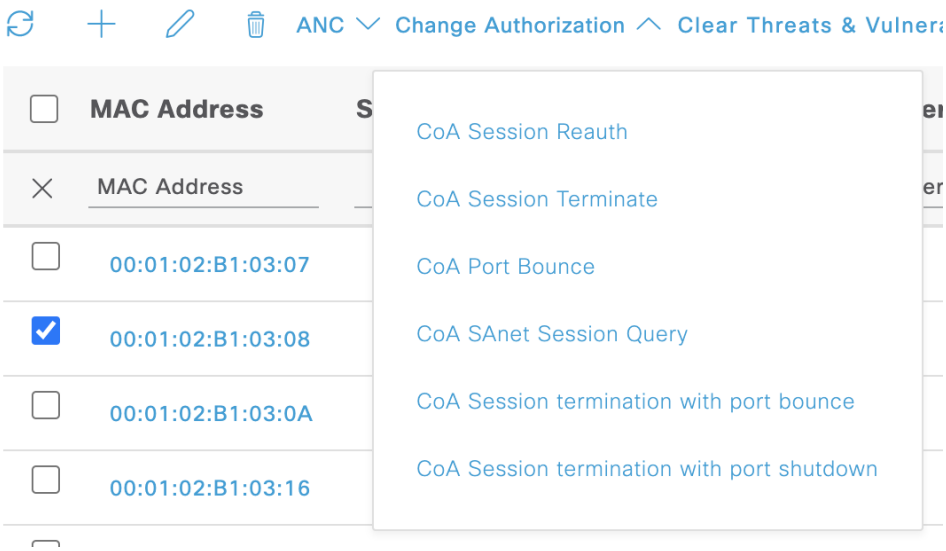
步骤 1 点击**显示 (Show)** 下拉列表并选择**快速过滤器 (Quick Filter)**。

步骤 2 在一个或多个属性字段中输入搜索条件，然后与指定属性相匹配的条目会自动显示。

视图列表中的终端操作

列表顶部的工具栏允许您对所选列表中的终端执行操作。并非每个列表的所有操作都已启用，某些操作取决于启用的功能。以下列表显示了必须在Cisco ISE 中启用后才能使用的两项终端操作。

- 已启用自适应网络控制 (ANC)，您可以选择列表中的终端，并分配或撤销网络访问。您也可以发出授权更改 (CoA)：



ANC（终端保护服务）需要在Cisco ISE 的**自适应网络服务 (Adaptive Network Service)** 窗口中启用。在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **端点保护服务 (Endpoint Protection Service)** > **自适应网络控制 (Adaptive Network Control)**\. 有关详细信息，请参阅在思科 ISE 中启用自适应网络控制，第 223 页。

- 如果已安装 MDM，您可以对选中的终端执行 MDM 操作。

思科 ISE 控制面板

Cisco ISE 控制板或主页（**主页 [Home]** > **摘要 [Summary]**）是您登录Cisco ISE 管理控制台之后显示的登录页面。此控制面板是一个集中管理控制台，由窗口顶部的仪表和下面的 Dashlet 组成。默认控制板为**摘要 (Summary)**、**终端 (Endpoints)**、**客户 (Guests)**、**漏洞 (Vulnerability)** 和**威胁 (Threat)**。有关其他信息，请查阅思科 ISE 主页控制板，第 88 页部分。

注释 您应该仅在主 PAN 上查看控制板数据。

控制板的实时数据概要显示访问您的网络的设备和用户的状态以及系统的运行状况。

点击二级菜单栏中的齿轮图标，查看控制板设置的下拉列表。下表显示**控制板设置 (Dashboard Settings)** 菜单下可用选项的相关信息：

选项	说明
添加新控制面板 (Add New Dashboard)	您最多可以有 20 个控制板，包括 5 个默认控制板。

选项	说明
重新命名控制面板 **(Rename Dashboard)**	要重新命名控制面板（仅适用于自定义控制面板），请执行以下操作： **1.** 点击**重命名控制板 (Rename Dashboard)**。 **2.** 指定新名称。 **3.** 点击**应用 (Apply)**。
添加 **Dashlet (Add Dashlet)**	要将 Dashlet 添加到主页控制板，请执行以下操作： **1.** 点击**添加 Dashlet (Add Dashlet[s])**。 **2.** 在**添加 Dashlet (Add Dashlet[s])** 窗口中，点击要添加的 Dashlet 旁的**添加 (Add)**。 **3.** 点击**保存 (Save)**。 **注释** 您最多可以为每个控制板添加 9 个 Dashlet。

选项	说明
导出 (Export)	您可以将 Dashlet 数据导出为 PDF 或 CSV 文件。 为此： 1. 从Cisco ISE 主页中选择相应的控制板，例如，“摘要”(Summary)。 2. 选择控制面板设置 (Dashboard Settings) > 导出 (Export)。 3. 在导出 (Export) 对话框中，选择以下文件格式之一： • PDF 格式用于查看选定 Dashlet 的快照。 • CSV 格式用于下载 ZIP 文件形式的选定控制板数据。 4. 在 Dashlet 部分，选择所需的 Dashlet。 5. 点击导出 (Export)。 压缩文件中包含所选控制面板的单个面板CSV文件。与 Dashlet 中的每个选项卡相关的数据在相应的 Dashlet CSV 文件中显示为单独的部分。 导出自定义控制板时，ZIP 文件将使用同一名称导出。例如，如果导出名为“MyDashboard”的自定义控制板，则导出的文件名为 MyDashboard.zip。
布局模板 (Layout Template)	您可以更改显示面板的模板布局。 要更改布局，请执行以下操作： 1. 选择控制面板设置 (Dashboard Settings) > 布局模板 (Layout Template)。 2. 从可用选项中选择所需的布局。

选项	说明
管理控制面板 (Manage Dashboards)	管理控制板 (Manage Dashboards) 菜单下提供以下选项： • “标记为默认控制板”(Mark as Default Dashboard)：使用该选项可将控制板设置为默认控制板（主页）。 • “重置所有控制板”(Reset all Dashboards)：使用该选项可将所有控制板还原为初始设置。

您可以点击相应自定义控制板旁的关闭 (**x**) 图标删除已创建的控制板。

注释 您不能重命名或删除默认控制面板。

所有 Dashlet 的右上角都有一个工具栏，包含以下选项：

- 分离 (Detach)：在单独的窗口中查看 Dashlet。
- 刷新 (Refresh)：刷新 Dashlet。
- 删除 (Remove)：从控制板中删除 Dashlet。

您可以使用 Dashlet 左上角的抓手图标拖放 Dashlet。

警报 Dashlet 中的快速过滤器 (Quick Filter in Alarms Dashlet)：可以根据严重性（如严重 (Critical)、警告 (Warning) 和信息 (Info)）过滤警报。“警报”（Alarms）Dashlet 位于主页上，包含具有“快速过滤器”(Quick Filter) 选项的过滤器下拉列表。

思科 ISE 国际化和本地化

Cisco ISE 国际化调整用户界面以适应受支持的语言。用户界面本地化采用区域特定组件和翻译文本。在 Windows、MAC OSX 和 Android 设备中，本地请求方调配向导可用于以下任何受支持的语言。

在Cisco ISE 中，国际化和本地化支持专注于支持（面向最终用户的门户中的）采用 UTF-8 编码的非英语文本以及管理门户中的选择性字段。

支持的语言

Cisco ISE 为以下语言和浏览器区域设置提供本地化和国际化支持。

表 *13:* 支持的语言和区域设置

语言	浏览器区域设置
中文（繁体）	zh-tw
中文（简体）	zh-cn
捷克语	cs-cz
荷兰语	nl-nl
英语	en
法语	fr-fr
德语	de-de
匈牙利语	hu-hu
意大利语	it-it
日语	ja-jp
韩语	ko-kr
波兰语	pl-pl
葡萄牙语（巴西）	pt-br
俄语	ru-ru
西班牙语	es-es

最终用户 Web 门户本地化

访客门户、发起人门户、我的设备门户和客户端调配门户会本地化为所有受支持的语言和区域设置。这包括文本、标签、消息、字段名称和按钮标签。如果客户端浏览器请求的区域设置未映射到Cisco ISE 中的模板，则门户会使用英语模板显示内容。

通过使用管理门户，您可以针对每种语言修改用于访客门户、发起人门户和我的设备门户的字段。您还可以添加其他语言。当前，您无法自定义客户端调配门户的这些字段。

您可以通过将 HTML 页面上传到Cisco ISE，进一步自定义访客门户。上传自定义页面时，您负责为部署提供相应的本地化支持。Cisco ISE 通过可以用作指南的样本 HTML 页面提供本地化支持示例。Cisco ISE 可以让您上传、存储和呈现自定义国际化 HTML 页面。

注释 NAC 和 MAC 代理安装程序及 WebAgent 页面未本地化。

支持 UTF-8 字符数据条目

向最终用户公开的Cisco ISE字段（通过Cisco客户端代理或请求方，或者发起人门户、访客门户、我的设备门户和客户端调配门户）支持所有语言的 UTF-8 字符集。UTF-8 是 Unicode 字符集的多字节字符编码，其中包括许多不同语言字符集，例如希伯来语、梵语和阿拉伯语。

字符集以 UTF-8 形式存储在管理配置数据库中，并且 UTF-8 字符集正确显示在报告和用户界面组件中。

UTF-8 凭证身份验证

网络访问身份验证支持 UTF-8 用户名和密码凭证。这包括来自访客和管理门户登录身份验证的 RADIUS、EAP、RADIUS 代理、RADIUS 令牌和 Web 身份验证。对用户名和密码的 UTF-8 支持适用于对照本地身份库及外部身份库进行的身份验证。

UTF-8 身份验证取决于用于网络登录的客户端请求方。某些 Windows 本地请求方不支持 UTF-8 凭证。

注释 RSA 不支持 UTF-8 用户，因此，使用 RSA 的 UTF-8 身份验证不受支持。兼容Cisco ISE 的 RSA 服务器也不支持 UTF-8。

UTF-8 策略和安全评估

Cisco ISE 中以属性值为条件的策略规则可以包含 UTF-8 文本。规则评估支持使用 UTF-8 属性值。此外，也可以通过管理门户使用 UTF-8 值配置条件。

终端安全评估要求根据 UTF-8 字符集修改为文件、应用和服务条件。

对发送至请求方的消息的 UTF-8 支持

RSA 提示符和消息使用 RADIUS 属性 REPLY-MESSAGE 转发到请求方，或者在 EAP 数据中。如果文本包含 UTF-8 数据，请求方将根据客户端的本地操作系统语言支持显示文本。某些 Windows 本地请求方不支持 UTF-8 凭证。

Cisco ISE 提示和消息可能与请求方运行所在的客户端操作系统的区域设置不同步。您必须调整最终用户请求方区域设置与Cisco ISE 支持的语言，使它们保持一致。

报告和警报 UTF-8 支持

对于Cisco ISE 中支持的语言，监控和故障排除报告和警报支持相关属性使用 UTF-8 值：支持以下活动：

- 查看实时身份验证。
- 查看详细的报告记录页面。
- 导出和保存报告。
- 查看Cisco ISE 控制板。

- 查看警报信息。
- 查看 tcpdump 数据。

门户中的 UTF-8 字符支持

Cisco ISE 字段中支持的字符集 (UTF-8) 比门户和最终用户消息中的本地化支持的字符集多得多。例如，尽管支持字符集本身，但是Cisco ISE不支持从右到左书写的语言（例如希伯来语或阿拉伯语）。

下表列出管理员和最终用户门户中支持 UTF-8 字符的字段，这些字符用于数据输入和查看，带有以下限制：

- Cisco ISE 不支持包含 UTF-8 字符的访客用户名和密码。
- Cisco ISE 不支持证书中的 UTF-8 字符。

表 *14:* 管理员门户 *UTF-8* 字符字段

管理员门户要素	UTF-8 字段
Network access user configuration	• User name 用户名可以由任意组合的大写和小写字母、数字、空格和特殊字符组成（`、%、^、;、:、[、{、|、}、]、\、‘、“、=、<、>、?、!和控制字符除外）。也不允许使用只包含空格的用户名。 • 名字 • Last name • e-mail
User list	• 所有过滤器字段 • User List 页面上显示的值 • 左侧导航快速视图上显示的值

管理员门户要素	UTF-8 字段
User password policy	密码可以由任意组合的大写和小写字母、数字和特殊字符组成（包括：“!”、“@”、“#”、“$”、“^”、“&”、“*”、“(”和“)”。密码字段接受任何字符，包括UTF-8字符，但不接受控制字符。 某些语言不支持大写或小写字母。如果用户密码策略要求用户输入含大写或小写字符的密码，并且如果用户的语言不支持这些字符，则用户无法设置密码。若要使用户密码字段支持 UTF-8 字符，在用户密码策略页面（**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **用户密码策略 (User Password Policy)**）中，必须取消选中以下选项： • 小写字母字符 • 大写字母字符 不能使用字典字词，其反序字符或用其他字符替换的字母。
Administrator list	• 所有过滤器字段 • Administrator List 页面上显示的值 • 左侧导航快速视图上显示的值
Admin login page	• User name
RSA	• 消息 • 提示符
RADIUS token	• Authentication tab > Prompt
Posture Requirement	• 名称 (Name) • Remediation action > Message shown to Agent User • 要求列表显示

管理员门户要素	UTF-8 字段
Posture conditions	• File condition > File path • Application condition > Process name • Service condition > Service name • 条件列表显示
Guest and My Devices settings	• Sponsor > Language Template：所有支持的语言，所有字段 • Guest > Language Template：所有支持的语言，所有字段 • My Devices >Language Template：所有支持的语言，所有字段
System settings	• SMTP Server > Default e-mail address
Operations > Alarms > Rule	• Criteria > User • Notification > e-mail Notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the av expression within policy conditions • Authorization / posture / client provisioning > other conditions > value for the av expression within policy conditions

管理员门户要素	UTF-8 字段
Attribute value in policy library conditions	• Authentication > simple condition / compound condition > value for the av expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition / compound condition > value for the av expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition / Dictionary compound condition > value for the av expression • Guest > simple condition / compound condition > value for the av expression

用户界面外的 UTF-8 支持

本节包含在Cisco ISE 用户界面之外提供 UTF-8 支持的区域。

调试日志和 CLI 相关的 UTF-8 支持

某些调试日志中会显示属性值和安全评估条件详细信息，因此所有调试日志都应接受 UTF-8 值。您可以下载包含原始 UTF-8 数据的调试日志，使用支持 UTF-8 的查看器便能够查看这些数据。

ACS 迁移 UTF-8 支持

Cisco ISE 允许迁移 ACS UTF-8 配置对象和值。Cisco ISE UTF-8 语言可能不支持某些 UTF-8 对象的迁移，它可能会使用管理门户或报告方法，使迁移过程中提供的某些 UTF-8 数据变得无法读取。您必须将无法读取的 UTF-8 值（从 ACS 迁移）转换为 ASCII 文本。有关从 ACS 迁移到 ISE 的详细信息，请参阅适用于您的 ISE 版本的思科安全 ACS 到思科 ISE 迁移工具。

支持导入和导出 UTF-8 值

Admin 门户和发起人门户都支持纯文本与 .csv 文件，并且支持在导入用户帐户详细信息时使用 UTF-8 值。所提供的导出文件为 csv 文件。

REST 上的 UTF-8 支持

外部 REST 通信支持 UTF-8 值。这适用于Cisco ISE 用户界面上支持 UTF-8 的可配置项，管理员身份验证除外。REST 上的管理员身份验证要求使用 ASCII 文本凭证进行登录。

身份库授权数据的 UTF-8 支持

Cisco ISE 允许 Active Directory 和 LDAP 在授权策略中使用 UTF-8 数据进行策略处理。

MAC 地址标准化

ISE 支持对以下列任意格式输入的 MAC 地址进行标准化：

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

对于以下 ISE 窗口，可以提供完整 MAC 地址或部分 MAC 地址：

- Policy > Policy Sets
- Policy > Policy Elements > Conditions > Authorization
- Authentications > Filters (Endpoint and Identity columns)
- Global Search
- Operations > Reports > Reports Filters
- Operations > Diagnostic Tools > General Tools > Endpoint Debug

对于以下 ISE 窗口，应提供完整的 MAC 地址（六个八位字节，用“:”或“-”或“.”分隔）：

- Operations) > Endpoint Protection Services Adaptive Network Control
- Operations > Troubleshooting > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting
- Operations > Troubleshooting > Diagnostic Tools > General Tools > Posture Troubleshooting
- Administration > Identities > Endpoints
- Administration) > System > Deployment
- Administration > Logging > Collection Filter

REST API 也支持完整 MAC 地址的标准化。

有效的八位字节仅包含 0-9、a-f 或 A-F。

思科 ISE 部署升级

通过Cisco ISE，可以从管理门户执行基于 GUI 的集中式升级。升级过程是相当简单的，升级进度和节点状态显示在屏幕上。有关升级前和升级后任务的列表，请参阅《思科身份服务引擎升级指南》。

“升级概述”(Upgrade Overview) 页面列出了部署中的所有节点、这些节点上启用的角色、所安装 ISE 的版本以及节点的状态（指示节点是处于活动状态还是非活动状态）。只有在节点处于活动状态时，才能开始升级。

管理员访问控制台

以下步骤说明了如何登录管理门户。

步骤 1 在浏览器地址栏中输入Cisco ISE URL（例如 https://<ise hostname or ip address>/admin/）。

步骤 2 输入在Cisco ISE 初始设置过程中指定和配置的用户名及区分大小写的密码。

步骤 3 点击**登录 (Login)** 或按 **Enter**。

如果您登录不成功，请在“登录”(Login) 页面点击**登录遇到问题？(Problem logging in?)** 链接并按照说明操作。

管理员登录浏览器支持

Cisco ISE 管理门户支持以下支持 HTTPS 的浏览器：

- Mozilla Firefox 79 及更低版本
- Mozilla Firefox ESR 60.9 及更低版本
- Google Chrome 84 及更低版本

ISE 社区资源

使用 Adblock Plus 时，ISE 页面无法完全加载

登录尝试失败后锁定管理员

如果在输入管理员用户 ID 的密码时错误次数足够多，则该帐户将在指定时间内暂停使用或被锁定（根据配置而定）。如果您选择锁定，则管理员门户会将您“封锁”在系统之外。Cisco ISE 在“服务器管理员登录”(Server Administrator Logins) 报告中添加一条日志，并吊销该管理员 ID 的凭证。您可以重置该管理员 ID 的密码，如《思科身份服务引擎安装指南》中的“重置因管理员锁定而禁用的密码”一节所述。禁用管理员帐户之前允许的失败尝试次数是可配置的，具体见《思科身份服务引擎管理员指南》中的 对思科 ISE 的管理访问，第 15 页一节。管理员用户帐户被锁定后，Cisco ISE 会向关联的管理员用户（如已配置）发送电子邮件。

任意超级管理员（包括 Active Directory 用户）均可启用被禁用的系统管理员状态。

在思科 ISE 中指定代理设置

如果现有网络拓扑要求您对Cisco ISE 使用代理来访问外部资源（例如可在其中查找客户端调配和安全评估相关资源的远程下载站点），则您可以使用管理门户指定代理属性。

代理设置会影响以下Cisco ISE 功能：

- 合作伙伴移动管理
- 终端分析器源服务更新
- 终端安全评估更新
- 终端安全评估代理资源下载
- CRL（证书吊销列表）下载
- 访客通知
- SMS 消息传输
- 社交媒体登录

Cisco ISE 代理配置支持代理服务器的基本身份验证。不支持 NT LAN Manager (NTLM) 身份验证。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **代理 (Proxy)**。

步骤 2 输入代理 IP 地址或 DNS 可解析主机名，并在**代理主机服务器：端口 (Proxy host server : port)** 中指定代理流量与 Cisco ISE 之间来回传播所通过的端口。

步骤 3 如果需要，请选中**必填密码 (Password required)** 复选框。

步骤 4 在**用户名 (User Name)** 和 **密码 (Password)** 字段中输入用于向代理服务器进行身份验证的用户名和密码。

步骤 5 在**用于这些主机和域的旁路代理 (Bypass proxy for these hosts and domain)** 中输入要绕行的主机或域的 IP 地址或地址范围。

步骤 6 点击**保存 (Save)**。

管理员门户使用的端口

管理员门户设置为使用 HTTP 80 端口和 HTTPS 443 端口，并且您无法更改这些设置。Cisco ISE 同时防止您分配任何最终用户门户使用相同的端口，这降低了管理员门户的风险。

启用外部 RESTful 服务 API

外部宁静的服务API根据HTTPS协议和其他方式和使用端口9060。

外部宁静的服务API支持基本身份验证。身份验证凭证加密并是请求报头的一部分。

您可以使用 REST 客户端（如 JAVA）、curl linux 命令、python 或任何其他客户端来调用外部 RESTful 服务 API 调用。

ESS管理员分配种类到用户执行操作使用外部宁静的服务API。在Cisco ISE 2.6 及更高版本中，ERS 用户可以是内部用户，也可以属于外部 AD。外部用户所属的 AD 组必须映射到 ERS 管理员组或 ERS 操作员组：

- 外部 RESTful 服务管理员 - 对所有 ERS API（GET、POST、DELETE、PUT）的完整访问权限。此用户可以创建、读取、更新和删除 ERS API 请求。
- 外部 RESTful 服务操作人员 - 只读权限（只能使用 GET 请求）。

注释 超级管理员用户可以访问所有 ERS API。

ERS 会话空闲超时为 60 秒。因此，如果在此期间发送了多个请求，则使用相同的会话，意味着相同的 CSRF。在空闲 60 秒后，它会重置并使用新的 CSRF。

默认情况下外部RESTful API服务未启用。如果您尝试调用API在启用之前呼叫的外部宁静的服务，您将收到错误响应。您必须启用Cisco ISE REST API对于Cisco ISE开发的应用REST API可以访问Cisco ISE。Cisco REST API使用HTTPS端口9060，默认情况下会关闭。Cisco ISE REST API在Cisco ISE管理员服务器上未启用，客户端应用程序从所有访客REST API请求的服务器将收到超时错误。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **ERS 设置 (ERS Settings)**。

步骤 2 对主管理节点选择**启用 ERS 进行读/写 (Enable ERS for Read/Write)**。

步骤 3 如果有任何辅助节点，请选择**为所有其他节点启用 ERS 进行读取 (Enable ERS for Read for All Other Nodes)**。

所有类型外部宁静的服务请求的主要ESS节点有效。辅助节点可以访问（GET请求）。

步骤 4 选择以下选项之一：

- 使用 CSRF 检查以增强安全性 (Use CSRF Check for Enhanced Security) - 如果启用此选项，ERS 客户端必须发送 GET 请求以从Cisco ISE 获取跨站请求伪造 (CSRF) 令牌，并将 CSRF 令牌包含在发送到Cisco ISE 的请求中。当收到来自 ERS 客户端的请求时，Cisco ISE 将验证 CSRF 令牌。Cisco ISE 仅在令牌有效时处理请求。此选项不适用于 ISE 2.3 之前的客户端。
- 对 ERS 请求禁用 CSRF (Disable CSRF for ERS Request) - 如果启用此选项，则不会执行 CSRF 验证。此选项可用于 ISE 2.3 之前的客户端。

步骤 5 点击保存 (Save)。

所有其它操作进行审核，并记录登录系统日志。外部宁静的服务API具有调试记录class，您可以从Cisco ISE GUI的调试日志记录的页面启用。

当您在Cisco ISE 中禁用外部 RESTful 服务时，端口 9060 保持开放，但不允许通过该端口进行通信。

相关主题

外部宁静的服务SDK，第 115 页

为 ERS API 启用外部 AD 访问

通过以下步骤，您可以为 ERS API 启用外部 AD 访问：

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

步骤 2 添加外部用户所属的 AD 组作为外部身份源。

请参阅将 Active Directory 用作外部身份源，第 471 页

步骤 3 从 AD 添加用户组。

请参阅添加用户，第 458 页

步骤 4 选择 管理 (Administration) > 管理员访问 (Admin Access) > 身份验证 (Authentication) > 身份验证方式 (Authentication Method)。

步骤 5 从身份源 (Identity Source) 下拉列表选择 AD：<加入点名称> (AD: <Join Point Name>)。

步骤 6 选择基于密码 (Password Based) 或基于客户端证书 (Client Certificate Based) 的身份验证。

步骤 7 选择管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 管理员 (Administrators) > 管理员组 (Admin Groups)。

步骤 8 将外部组作为成员用户添加到 ERS 管理员组或 ERS 操作员组。请转至 管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 管理员 (Administrators) > 管理员组 (Admin Groups) > ERS 管理员 (ERS Admin)ERS 操作员 (ERS Operators)。

步骤 9 点击添加 (Add)。

步骤 10 选择该用户。

步骤 11 点击保存 (Save)。

ESS管理员分配种类到用户执行操作使用外部宁静的服务API。在Cisco ISE 2.6 及更高版本中，ERS 用户可以是内部用户，也可以属于外部 AD。外部用户所属的 AD 组必须映射到 ERS 管理员组或 ERS 操作员组：

- 外部 RESTful 服务管理员 - 对所有 ERS API（GET、POST、DELETE、PUT）的完整访问权限。此用户可以创建、读取、更新和删除 ERS API 请求。
- 外部 RESTful 服务操作人员 - 只读权限（只能使用 GET 请求）。

注释 超级管理员用户可以访问所有 ERS API。

外部宁静的服务SDK

您可以使用外部宁静的服务SDK开始迁移工具支持工具。您可以从以下URL访问外部宁静的服务SDK：https:// <ISE - ADMIN - NODE> ：9060/ers/sdk、外部宁静的服务SDK可以只通过外部宁静的服务管理员用户访问。

SDK包括以下组件

- 快速参考API文档
- 所有可用 API 操作的完整列表
- 架构文件可下载
- 在Java的示例应用程序可以下载
- curl 脚本格式的使用案例
- Python 脚本格式的使用案例
- 使用 Chrome Postman 的说明

指定系统时间和 NTP 服务器设置

Cisco ISE 允许最多配置三个网络时间协议 (NTP) 服务器。您可以使用 NTP 服务器维护正确时间和同步不同时区的时间。您还可以指定Cisco ISE 是否应仅使用经过身份验证的NTP 服务器，您可以为此目的输入一个或更多身份验证密钥。

Cisco建议将所有Cisco ISE 节点均设置为协调世界时 (UTC) 时区，特别是在您的思科 ISE 节点都安装于分布式部署中的情况下。此程序可确保无论时间戳如何，来自您的部署中各个节点的报告和日志始终同步。

对于 NTP 服务器，Cisco ISE 也支持公钥身份验证。NTPv4 使用对称密钥加密，但是也可根据公钥加密提供新的自动密钥方案。公钥加密通常被认为比对称密钥加密更安全，因为其安全性基于各个服务器生成的不会泄露的专用值。如果使用自动密钥，所有密钥分发和管理功能都将仅涉及公共值，可在很大程度上简化密钥分发和存储。

您可以在配置模式下从Cisco ISE CLI 将 NTP 服务器配置为使用自动密钥。我们建议您使用 IFF（敌我识别）识别方案，因为这种方案的使用最为广泛。

开始之前

您必须分配到了超级管理员角色或系统管理员角色。

如果您有一个主要和辅助Cisco ISE 节点，您必须登录辅助节点的用户界面并在您的部署中每个Cisco ISE 节点上逐一配置系统时间和 NTP 服务器。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **系统时间 (System Time)**。

步骤 2 输入您的 NTP 服务器的唯一 IP 地址 (IPv4/IPv6/FQDN)。

步骤 3 如果您想要限制Cisco ISE 仅使用经过身份验证的NTP 服务器保留系统和网络时间，请选中 **Only allow authenticated NTP servers** 复选框。

步骤 4 （可选）如果要使用私钥对 NTP 服务器进行身份验证，并且您指定的服务器中有任意服务器要求通过身份验证密钥进行身份验证，请点击 **NTP Authentication Keys**（NTP 身份验证密钥）选项卡并指定一个或更多身份验证密钥，如下所示：

a) 点击**添加 (Add)**。

b) 输入必要的**密钥 ID** 和**密钥值**。从下拉列表中选择 **HMAC**。Key ID 字段支持 1 至 65535 之间的数值，Key Value 字段支持最多 15 个字母数字字符。

c) 输入 NTP 服务器身份验证密钥后，请返回 NTP Server Configuration 选项卡。

步骤 5 （可选）如果要使用公共密钥身份验证对 NTP 服务器进行身份验证，请从命令行界面 (CLI) 配置 Cisco ISE 上的自动密钥。有关详细信息，请参阅对应于您的 ISE 版本的《思科身份识别服务引擎 CLI 参考指南》中的 **ntp server** 和 **crypto** 命令。

步骤 6 点击**保存 (Save)**。

更改系统时区

设置后，您便无法从管理门户编辑时区。要更改时区设置，必须在Cisco ISE CLI 中输入以下命令：

clock timezone *timezone*

有关 **clock timezone** 命令的详细信息，请参阅《思科身份服务引擎 CLI 参考指南》。

注释 Cisco ISE 在时区名称和输出缩写中使用 POSIX 式符号。因此，格林威治西部时区中有一个正号，东部时区中有一个负号。例如 TZ='Etc/GMT+4' 对应于标准时间 (UT) 后 4 小时。

注意 安装后，在Cisco ISE 设备上更改时区需要在该特定节点上重新启动 ISE 服务。因此，我们建议您在维护窗口内执行此类更改。此外，务必将单个 ISE 部署中的所有节点都配置为同一时区。如果 ISE 节点位于不同地理位置或时区中，则应在所有 ISE 节点上使用全球时区，例如 UTC。

配置 SMTP 服务器以支持通知

要更新 SMTP 服务器详细信息，请转至**管理 (Administration) > 系统 (System) > 设置 (Settings) > 代理 (Proxy) > SMTP 服务器 (SMTP server)**。配置简单邮件传输协议 (SMTP) 服务器，以执行以下操作：发送警报的电子邮件通知，使发起人向访客发送包含登录凭证和密码重置说明的电子邮件通知，使访客在自行成功注册后自动接收登录凭证以及访客帐户到期前要采取的操作。

警报通知的收件人可以是已启用**在电子邮件中包括系统警报 (Include system alarms in emails)** 选项的任何内部管理员用户。发送警报通知的发件人的邮件地址硬编码为 ise@<hostname>。

下表显示了分布式 ISE 环境中哪些节点会发送电子邮件。

电子邮件用途	发送电子邮件的节点
访客过期	主 PAN
alarms	活动 MnT
来自访客和发起人门户的发起人和访客通知	PSN
密码过期	主 PAN

以下字段用于配置 SMTP 服务器。

- **SMTP 服务器设置**
  - **SMTP 服务器 (SMTP Server)**：输入出站 SMTP 服务器的主机名。
  - **SMTP 端口 (SMTP Port)**：输入 SMTP 端口号。此端口必须打开才能连接到 SMTP 服务器。
  - **连接超时 (Connection Timeout)**：输入Cisco ISE 在开始新连接之前等待连接到 SMTP 服务器的最长时间。
- **加密设置 (Encryption Settings)**：选中“使用 TLS/SSL 加密”(Use TLS/SSL encryption) 以与安全 SMTP 服务器通信。如果使用 SSL，请将 SMTP 服务器的根证书添加到Cisco ISE 受信任证书。
- **身份验证设置 (Authentication Settings)**：授权可以是用户名和密码，也可以是 SSL。SSL 是默认设置。选中“使用密码身份验证”(Use Password Authentication) 以改为使用用户名和密码。

交互式帮助

交互式帮助为用户提供提示和分步指导，帮助用户轻松完成任务，从而有效地使用Cisco ISE。

默认情况下启用此功能。要启用或禁用此功能，请选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **交互式帮助 (Interactive Help)**，然后选中或取消选中**启用交互式帮助 (Enable Interactive Help)** 复选框。

启用安全解锁客户端机制

安全解锁客户端机制可在特定时间段内在Cisco ISE 命令行界面 (CLI) 上提供根外壳访问。一旦会话关闭或退出，根访问也会被撤销。

已使用同意令牌工具实施安全解锁客户端功能。同意令牌是一种统一的多因素身份验证方案，用于以可信的方式安全地授予对Cisco产品的特权访问权限，并且仅在客户和Cisco双方同意之后授予。

要在Cisco ISE CLI 上启用根外壳，请执行以下步骤：

步骤 1 在Cisco ISE CLI 中，输入 **permit rootaccess**：

```
ise/admin# permit rootaccess 1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出    输入 CLI 选项：
```

步骤 2 通过选择选项1生成同意令牌挑战：

```
1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出输入 CLI 选项：1 正在生成质
询..................................... 质询字符串（请仅复制星号行之间的所有内容）：
********************************************************************************
GLOX/gAAAQEBAAQAAAABAgAEAAAAAAMACImJxgubOhitBAAQiUwv+XeD3pnJ4HLnJy30MQUAEAAADhAGAANUUUHAAZUUVfQlQIAANUUUUACcJIDU2NGQ5NjgwMTEmZmEtOWI0ZS0wZjYtMTdlZDllMGQlM2UzNQo=
 ********************************************************************************* 启动 15 分钟后
台计时器 1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出     输入 CLI 选项：
```

步骤 3 将同意令牌质询发送至Cisco技术支持中心 (TAC)：

Cisco TAC 将使用您提供的同意令牌质询生成同意令牌响应。

步骤 4 选择选项 **2**，然后输入Cisco TAC 提供的同意令牌响应：

```
输入 CLI 选项：2 请准备就绪后输入响应.....................
[redacted]
 响应签名验证成功！授予外壳访问权限    sh-4.2# 是
```

注释 如果响应签名验证成功，则启用特权访问。

下一步做什么

要退出外壳模式，请运行 **exit** 命令：

```
sh-4.2# exit exit Root shell exited
```

您可以通过选择选项 **3** 查看根访问会话的历史记录：

```
1. 生成质询令牌请求 2. 输入根访问的质询响应 3. 显示历史记录 4. 退出输入 CLI 选项：3
********************************** SN No : 1 ********************************** Challenge

3/WcyAAAQEBAAQAAABAgAEAAAAAAMCM89hCTWWBAQwc9lyianffO4C5il+v8OAQUAEAAADhAGAANUUUHAAZUUVfQlQIAANUUUUACcJIDU2NGQ5NjgwMTEmZmEtOWI0ZS0wZjYtMTdlZDllMGQlM2UzNQo=
```

```
 generated at 2019-06-12 15:40:01.000 ********************************** SN No : 2
**********************************
```

设置思科 ISE API 网关

Cisco ISE API 网关是一种 API 管理解决方案，它是通往多个Cisco ISE 服务 API 的单一入口点，改善了安全和流量管理。来自外部客户端的 API 请求将路由到Cisco ISE 上的 API 网关。这些请求会根据内部算法进一步转发到运行服务 API 的Cisco ISE 节点。

在Cisco ISE 版本 3.0 中，只有 MNT（监控）API 通过 API 网关路由。您可以选择要在其中启用 API 网关的Cisco ISE 节点。我们建议您在Cisco ISE 部署中的至少两个节点上运行 API 网关。

步骤 1 登录主策略管理节点。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **API 网关设置 (API Gateway Settings)**

步骤 3 在 **ISE API 网关节点列表 (ISE API Gateway Nodes List)** 区域中，选中要启用 API 网关的节点旁边的复选框。

步骤 4 点击**启用 (Enable)**。

故障排除

要排除与 API 网关相关的问题，请在**调试日志配置 (Debug Log Configuration)** 窗口中将以下组件的**日志级别 (Log Level)** 设置为**调试 (DEBUG)**。（要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)**.）

- ise-kong
- kong

可从**下载日志 (Dowload Logs)** 窗口下载日志。（要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)**.) 您可以选择从**支持捆绑包 (Support Bundle)** 选项卡下载支持捆绑包，也可以从**调试日志 (Debug Logs)** 选项卡下载 kong 调试日志。

验证

如果您每次都能成功登录Cisco ISE 主策略管理节点 (PPAN)，则 API 网关设置将按预期工作。

FIPS 模式支持

ISE FIPS 140 模式将Cisco FIPS 对象模块加密模块初始化为 FIPS 140-2 模式。Cisco身份识别服务引擎使用嵌入式 FIPS 140-2 验证加密模块。有关FIPS 合规要求的详细信息，请参阅 FIPS 合规证明书。

启用 FIPS 模式时，Cisco ISE 管理员界面会在该页面右上角的节点名称左侧显示一个 FIPS 模式图标。

如果Cisco ISE 检测到使用了 FIPS 140-2 标准不支持的协议或证书，它会显示一条警告，其中包含不合规的协议或证书的名称，并且不会启用 FIPS 模式。确保只选择符合 FIPS 的协议并替换不符合 FIPS 的证书，然后再启用 FIPS 模式。

如果 FIPS 不支持证书中使用的加密方法，则必须重新颁发安装在Cisco ISE 中的证书。

打开 FIPS 模式时，以下功能会受影响：

- 基于安全套接字层 (SSL) 的轻量级目录访问协议 (LDAP)
- Cisco ISE 通过 RADIUS 共享密钥和密钥管理措施实现 FIPS 140-2 合规性。当启用 FIPS 模式时，使用不符合 FIPS 的算法的任何功能都将失败。

启用 FIPS 模式时：

- 对于 EAP-TLS、PEAP 和 EAP-FAST，将禁用所有不符合 FIPS 的密码套件
- 将在 SSH 中禁用所有不符合 FIPS 的密码套件
- 证书和私钥只能使用符合 FIPS 的散列和加密算法
- RSA 私钥必须为 2048 位或更高
- ECDSA 私钥必须为 224 位或更高
- ECDSA 服务器证书仅适用于 TLS 1.2
- 对于所有 ISE TLS 客户端，DHE 密码适用于 2048 位或更高的 DH 参数
- 不允许将 3DES 密码用于 ISE 服务器
- 不允许使用 SHA1 生成证书
- 不允许在客户端证书中使用 SHA1
- EAP-FAST 中的匿名 PAC 调配选项已禁用
- 本地 SSH 服务器将在 FIPS 模式下运行
- RADIUS 不支持以下协议：
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

启用 FIPS 模式后，部署中的所有节点将自动重新启动。Cisco ISE 通过先重新启动主 PAN、然后重新启动每个辅助节点（一次一个）来执行滚动重启。因此，建议您在更改配置之前计划停机时间。

提示 建议您在完成任何数据库迁移过程之前不要启用 FIPS 模式。

在思科 ISE 中启用 FIPS 模式

要启用 FIPS 模式，请执行以下操作：

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **FIPS 模式 (FIPS Mode)**。

步骤 2 从 **FIPS 模式 (FIPS Mode)** 下拉列表中选择**已启用 (Enabled)** 选项。

步骤 3 点击**保存 (Save)**，然后重新启动计算器。

下一步做什么

启用 FIPS 模式之后，请启用并配置以下符合 FIPS 140-2 的功能：

- 生成自签证书，第 142 页
- 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 160 页
- 请参阅《》中的“网络设备定义设置”部分
- 在网络设备定义设置，第 721 页下配置 RADIUS 身份验证设置。

此外，可能要使用通用访问卡 (CAC) 功能启用管理员帐户授权。尽管严格而言，将 CAC 功能用于授权并不是一项 FIPS 140-2 要求，但它是一项众所周知的安全访问措施，用于在多种环境中提高 FIPS 140-2 合规性。

配置思科 ISE 以进行管理员 CAC 身份验证

开始之前

在开始配置前，请执行以下操作：

- 确保Cisco ISE 中的域名服务器 (DNS) 已针对 Active Directory 进行设置。
- 确保 Active Directory 用户和用户组成员已针对各管理员证书进行定义。

要确保Cisco ISE 可根据从浏览器提交的基于 CAC 的客户端证书对管理员进行身份验证和授权，请确保您已配置以下项目：

- 外部身份源（在下面的示例中为 Active Directory）
- 管理员所属的 Active Directory 中的用户组
- 如何在证书中查找用户身份
- Active Directory 用户组到Cisco ISE RBAC 权限映射

- 签发客户端证书的证书颁发机构（信任）证书
- 确定客户端证书是否已被 CA 吊销的方法

在登录Cisco ISE 时，您可以使用通用访问卡 (CAC) 对凭证进行身份验证。

步骤 1 在Cisco ISE 中配置 Active Directory 身份源并将所有Cisco ISE 节点加入 Active Directory。

步骤 2 根据指南配置证书身份验证配置文件。

请确保选择证书中包含 Principal Name X.509 Attribute 字段中的管理员用户名的属性。（对于 CAC 卡，卡上的签名证书通常用于查找 Active Directory 中的用户。Principal Name 可在此证书的“Subject Alternative Name”扩展中找到，确切的说是在名为“Other Name”的扩展的字段中。因此此处的属性选择应为“Subject Alternative Name - Other Name。”）

如果用户的 AD 记录包含用户的证书，并且您希望将从浏览器接收的证书与 AD 中的证书相比较，请选中 Binary Certificate Comparison 复选框，并选择之前指定的 Active Directory 实例名称。

步骤 3 启用 Active Directory 以进行基于密码的管理员身份验证。选择您之前连接并加入Cisco ISE 的 Active Directory 实例名称。

注释 在完成其他配置前，您必须使用基于密码的身份验证。接着，在此过程的最后一步，您可以将身份验证类型更改为基于客户端证书。

步骤 4 创建外部管理员组并将其映射到 Active Directory 组。选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**。创建外部系统管理员组。

步骤 5 配置管理员授权策略，将 RBAC 权限分配给外部管理员组。

注意 我们强烈建议您创建外部超级管理员组，将其映射到 Active Directory 组，并使用超级管理员权限（菜单访问和数据访问）配置管理员授权策略，并在该 Active Directory 组中至少创建一名用户。此映射确保基于客户端证书的身份验证启用后，至少一名外部管理员拥有超级管理员权限。此操作失败可能导致Cisco ISE 管理员被锁定，以致无法使用管理员门户中的关键功能。

步骤 6 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书存储区 (Certificate Store)**，将证书颁发机构证书导入Cisco ISE 证书信任存储区。

除非客户端证书信任链中的 CA 证书位于Cisco ISE 证书库中，否则Cisco ISE 不接受客户端证书。您必须将相应的 CA 证书导入到Cisco ISE 证书库中。

a) 点击**浏览 (Browse)** 以选择证书。
b) 选中“客户端身份验证的信任”(Trust for client authentication) 复选框。
c) 点击**提交 (Submit)**。

Cisco ISE 会提示您在导入证书后重启部署中的所有节点。您可以在导入所有证书后再重启。但是，在导入所有证书后，您必须重启Cisco ISE 才能继续。

步骤 7 配置证书颁发机构证书以验证吊销状态。

a) 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **OSCP 服务 (OSCP Services)**。
b) 输入 OSCP 服务器的名称、说明（可选）和服务器的 URL。

c) 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书存储区 (Certificate Store)**。
d) 对于对客户端证书签名的 CA 证书，指定如何执行该 CA 的吊销状态检查。从列表中选择一个 CA 证书并点击“编辑”(Edit)。在编辑页面中，选择 OCSP 和/或 CRL 验证。如果选择 OCSP，请选择用于该 CA 的 OCSP 服务。如果选择 CRL，请指定 CRL 分发 URL 和其他配置参数。

步骤 8 启用基于客户端证书的身份验证。选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)**。

a) 在 Authentication Method 选项卡中选择基于客户端证书的身份验证类型。
b) 选择您之前配置的证书身份验证配置文件。
c) 选择 Active Directory 实例名称。
d) 点击**保存 (Save)**。

此时，您可以从基于密码的身份验证切换到基于客户端证书的身份验证。您之前配置的客户端身份验证配置文件决定了管理员证书的身份验证方式。使用外部身份源对管理员进行授权，此示例中的外部身份源为 Active Directory。

证书身份验证配置文件的 Principal Name 属性用于查找 Active Directory 中的管理员。

您现在已经完成了用于进行管理员 CAC 身份验证的Cisco ISE 配置。

支持的通用访问卡标准

Cisco ISE 支持使用通用访问卡 (CAC) 身份验证设备对自身进行身份验证的美国政府用户。CAC 是一种带电子芯片的身份识别卡，电子芯片包含一组标识特定员工身份的 X.509 客户端证书。通过 CAC 访问需要一个读卡器，您可将卡插入其中并输入 PIN。之后，卡中的证书会传输到 Windows 证书库，它们可供运行Cisco ISE 的本地浏览器等应用使用。

思科 ISE 中的通用访问卡操作

可以配置管理员门户，以便仅允许使用客户端证书向Cisco ISE 进行身份验证。不允许执行基于凭证的身份验证，例如提供用户 ID 和密码。在客户端证书身份验证中，您要插入通用访问卡 (CAC)，输入 PIN，然后在浏览器地址栏输入Cisco ISE Admin 门户 URL。浏览器将证书转发至Cisco ISE，Cisco ISE 进行身份验证并根据证书的内容向您授予登录会话权限。如果此进程执行成功，系统会向您显示Cisco ISE 监控和故障排除主页并提供相应的 RBAC 权限。

使用 Diffie-Hellman 算法保护 SSH 密钥交换

可以将Cisco ISE 配置为仅允许 Diffie-Hellman-Group14-SHA1 SSH 密钥交换。为此，必须从Cisco ISE 命令行界面 (CLI) 配置模式输入以下命令：

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

示例如下：

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

将思科 ISE 配置为发送安全系统日志

开始之前

要将Cisco ISE 配置为仅在Cisco ISE 节点之间和向监控节点发送受 TLS 保护的安全系统日志，您必须执行以下任务：

- 确保部署中的所有Cisco ISE 节点都配置具有相应的服务器证书。
- 确保默认网络访问身份验证策略不允许任何版本的 SSL 协议。
- 确保您部署的所有节点都注册到主 PAN。此外，确保部署中至少有一个节点已启用监控角色，从而用作安全系统日志接收器（TLS 服务器）。
- 检查支持的系统日志 RFC 标准。请参阅Cisco ISE 版本对应的《思科身份服务引擎网络组件兼容性》指南。

步骤 1 配置安全系统日志远程日志记录目标。

步骤 2 启用日志记录类别，以将可审核事件发送到安全系统日志远程日志记录目标。

步骤 3 禁用 TCP 系统日志和 UDP 系统日志收集器。仅应启用受 TLS 保护的系统日志收集器。

配置安全系统日志远程记录目标

Cisco ISE 系统日志由日志收集器收集和存储，用于各种用途。必须选择Cisco ISE 监控节点作为日志收集器，配置安全系统日志目标。

步骤 1 登录到管理员门户。

步骤 2 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

步骤 3 点击**添加 (Add)**。

步骤 4 输入安全系统日志服务器的名称。

步骤 5 从**目标类型 (Target Type)** 下拉列表中选择**安全系统日志 (Secure Syslog)**。

步骤 6 从**状态 (Status)** 下拉列表中选择**已启用 (Enabled)**。

步骤 7 在**主机/IP 地址 (Host/IP Address)** 字段中输入部署中Cisco ISE 监控节点的主机名或 IP 地址。

步骤 8 在**端口 (Port)** 字段中，输入 *6514* 作为端口号。安全系统日志接收器在 TCP 端口 6514 上进行侦听。

步骤 9 从**设备代码 (Facility Code)** 下拉列表中选择系统日志设备代码。默认值为 **LOCAL6**。

步骤 10 选中以下复选框以启用相应配置：

a) **包括此目标的警报 (Include Alarms For This Target)**

b) **符合 RFC 3164 (Comply to RFC 3164)**

c) 启用服务器身份检查 **(Enable Server Identity Check)**

步骤 11 选中服务器关闭时缓冲消息 **(Buffer Messages When Server is Down)** 复选框。如果选中此选项，Cisco ISE 会存储日志，如果安全系统日志接收器不可达，Cisco ISE 则会定期查看安全系统日志接收器，并在安全系统接收器出现时转发日志。

a) 在缓冲区大小 **(MB) (Buffer Size (MB))** 字段中输入缓冲区大小。

b) 要让Cisco ISE 定期检查安全系统日志接收器，请在重新连接时间（秒）**(Reconnect Time (Sec))** 字段中以秒为单位输入重新连接超时值。

步骤 12 在选择 **CA** 证书 **(Select CA Certificate)** 下拉列表中选择想要Cisco ISE 呈现给安全系统日志服务器的 CA 证书。

步骤 13 在配置安全系统日志时，确保不要选中忽略服务器证书验证 **(Ignore Server Certificate validation)** 复选框。

步骤 14 点击提交 **(Submit)**。

远程日志记录目标设置

下表介绍“远程日志记录目标”(Remote Logging Targets) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。要查看此处窗口，请点击菜单 **(Menu)** 图标 (☰)，然后选择管理 **(Administration)** > 系统 **(System)** > 日志记录 **(Logging)** > 远程日志记录目标 **(Remote Logging Targets)**。

表 ***15:*** 远程日志记录目标设置

字段名称	使用指南
名称 **(Name)**	输入新目标的名称。
目标类型 **(Target Type)**	选择目标类型。默认情况下设置为 UDP Syslog。
说明	输入新目标的简短说明。
IP 地址 **(IP Address)**	输入要存储日志的目标计算机的 IP 地址或主机名。 思科 ISE 支持 IPv4 和 IPv6 格式的日志记录。
端口 **(Port)**	输入目标计算机的端口号。
设备代码 **(Facility Code)**	选择要用于日志记录的系统日志设备代码。有效选项为 Local0 至 Local7。
最大长度 **(Maximum Length)**	输入远程日志目标消息的最大长度。有效选项为 200 至 1024 字节。

字段名称	使用指南
服务器关闭时缓冲消息 **(Buffer Message When Server is Down)**	如果希望Cisco ISE 在 TCP 系统日志目标和安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。Cisco ISE 会在连接恢复时重新尝试将消息发送到目标。连接恢复后，消息按从最旧到最新的顺序进行发送，并且缓冲消息始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
缓冲区大小 **(MB) (Buffer Size [MB])**	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。
重新连接超时（秒）**(Reconnect Timeout [Sec])**	输入时间（以秒为单位），提及在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
选择 **CA** 证书 **(Select CA Certificate)**	选择客户端证书。
忽略服务器证书验证 **(Ignore Server Certificate Validation)**	如果希望 ISE 忽略服务器证书身份验证并接受任何系统日志服务器，请选中此复选框。

相关主题

思科 ISE 日志记录机制，第 249 页
思科 ISE 系统日志，第 250 页
远程系统日志消息格式
思科 ISE 消息目录，第 252 页
集合过滤器，第 253 页
事件抑制绕行过滤器，第 254 页
配置远程系统日志收集位置，第 250 页
配置集合过滤器，第 254 页

启用日志记录类别以将可审核事件发送至安全系统日志目标

您必须为Cisco ISE 启用日志记录类别，才能将可审核的事件发送到安全系统日志目标。

步骤 1 登录到管理员门户。

步骤 2 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

步骤 3 点击**管理和操作审核 (Administrative and Operational Audit)** 日志记录类别旁的单选按钮，然后点击**编辑 (Edit)**。

步骤 4 从**日志严重性级别 (Log Severity Level)** 下拉列表中选择 WARN。

步骤 5 在**目标 (Targets)** 字段中，将之前创建的安全系统日志远程记录目标移动到**选定 (Selected)** 框。

步骤 6 点击**保存 (Save)**。

步骤 7 重复此程序以启用下列日志记录类别：

- **AAA 审核 (AAA Audit)**。

  请注意，INFO 是此类别的默认日志严重性级别，无法编辑。

- **终端安全评估和客户端调配审核**。

日志记录类别设置

下表介绍了**日志记录类别 (Logging Categories)** 窗口中的字段，可以使用此窗口配置日志严重性级别，并为要存储的所选类别的日志选择日志记录目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

表 *16:* 日志记录类别设置

字段名称	使用指南
名称 (Name)	显示日志记录类别的名称。
日志严重性级别 (Log Severity Level)	允许您从以下选项中选择诊断日志记录类别的严重性级别： • **严重 (FATAL)**：紧急情况。此选项意味着无法使用Cisco ISE，并且必须立即采取操作。 • **错误 (ERROR)**：此选项表示严重或错误情况。 • **警告 (WARN)**：此选项表示正常但值得注意的情况。这是默认情况。 • **信息 (INFO)**：此选项表示信息性消息。 • **调试 (DEBUG)**：此选项表示诊断错误消息。
本地日志记录 (Local Logging)	选中此复选框可为本地节点上的类别启用日志记录事件。
目标 (Targets)	允许使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 框之间转移目标来更改类别的目标。**可用 (Available)** 框包含本地（预定义）和外部（用户定义）的现有日志记录目标。初始为空的**所选 (Selected)** 框包含特定类别的选定目标。

相关主题

远程系统日志消息格式
思科 ISE 消息代码，第 252 页
配置远程系统日志收集位置，第 250 页
设置消息代码的严重性级别，第 252 页

禁用 TCP 系统日志和 UDP 系统日志收集器

为确保Cisco ISE 只在 ISE 节点间发送安全系统日志，必须禁用 TCP 和 UDP 系统日志收集器，并且只启用安全系统日志收集器。

注释 如果启用Cisco ISE 消息服务来向 MnT 节点传送 UDP 系统日志，则Cisco ISE 版本 2.6 及更高版本包括 TLS 保护的 UDP 系统日志。请参阅 经思科 ISE 消息服务传递的系统日志，第 64 页

步骤 1 登录到管理员门户。
步骤 2 选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 远程日志记录目标 (Remote Logging Targets)。
步骤 3 点击 TCP 系统日志收集器旁的单选按钮。
步骤 4 点击编辑 (Edit)。
步骤 5 从状态 (Status) 下拉列表中选择禁用 (Disabled)。
步骤 6 点击保存 (Save)。
步骤 7 重复此过程，直到您禁用所有 TCP 或 UDP 系统日志收集器。

默认安全系统日志收集器

Cisco ISE 为 MnT 节点提供默认安全系统日志收集器。默认情况下，没有日志记录类别映射到这些默认的安全系统日志收集器。默认安全系统日志收集器的命名方式如下：

- 主 MnT 节点 - SecureSyslogCollector
- 辅助 MnT 节点 - SecureSyslogCollector2

可以在“远程日志记录目标”(Remote Logging Targets) 页面（“管理”(Administration) > “系统”(System) > “日志记录”(Logging)）上查看此信息。无法删除默认系统日志收集器，也无法更新默认系统日志收集器的以下字段：“名称”(Name)、“目标类型”(Target type)、“IP/主机地址”(IP/Host address) 和“端口”(Port)。

在Cisco ISE 全新安装过程中，系统中的“默认自签名服务器证书”将添加到信任存储区，并标记为“信任客户端身份验证和系统日志”(Trust for Client authentication and Syslog) 用法，从而可用于安全系统日志用法。在配置部署或更新证书时，必须将相关证书分配至安全系统日志目标。

在升级期间，如果有任何现有安全系统日志目标指向端口 6514 上的 MnT 节点，系统将保留相同的名称和配置，但升级后，无法删除这些系统日志目标，并且无法编辑以下字段：“名称”(Name)、“目标类型”(Target type)、“IP/主机地址”(IP/Host address) 和“端口”(Port)。如果在升级时不存在此类目标，则将创建类似于全新安装情景的默认安全系统日志目标，无需任何证书映射。可以将相关证书分配至这些系统日志目标。如果尝试将未映射至任何证书的安全系统日志目标映射至日志记录类别，则将显示以下消息：

```
请为 log_target_name 配置证书 (Please configure the certificate for log_target_name)
```

离线维护

如果维护时间段小于一小时，请使 ISE 节点离线并执行维护任务。当节点重新联机时，PAN 会自动同步维护期间发生的所有更改。如果更改未自动同步，可以手动将其与 PAN 同步。

如果维护时间段超过一小时，请在维护时注销节点，然后在将节点添加回部署时重新注册。

我们建议将维护安排在活动较少的时间段。

注释

1. 如果队列包含超过 1, 000,000 条消息或 ISE 节点离线超过 6 小时，则可能会出现数据复制问题。
2. 如果计划在主 MnT 节点上执行维护，我们建议在执行维护活动之前对 MnT 节点进行操作备份。

终端登录配置

此页面用于配置登录凭证，以便Cisco ISE 可以登录客户端。它用于：

- 终端脚本向导
- 无代理终端安全评估

为以下项配置登录凭证：

- **Windows 域用户 (Windows Domain User)**：用于通过 SSH 登录客户端的域凭证。您可以根据需要输入任意数量的 Windows 登录。如果配置了域用户，则会忽略本地用户配置。
- **Windows 本地用户 (Windows Local User)**：Cisco ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。
- **MAC 本地用户 (MAC Local User)**：Cisco ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。

思科 ISE 中的证书管理

证书是标识个人、服务器、公司或其他实体并将实体与公钥关联的电子文档。自签证书由证书创建者签名。证书可以自签或由外部证书颁发机构 (CA) 进行数字签名。CA 签名的数字证书被视为行业标准而且更安全。

证书用于在网络中提供安全访问。Cisco ISE 使用证书进行节点间通信和与外部服务器（例如系统日志服务器、源服务器）及所有最终用户门户（访客、发起人和个人设备门户）进行通信。证书会标识连接终端的Cisco ISE 节点并且保护该终端和Cisco ISE 节点之间的通信。

您可以使用 Admin 门户为您的部署中的所有节点管理证书。

思科 ISE 提供安全访问所用的证书

Cisco身份服务引擎 (ISE) 依赖公钥基础设施 (PKI) 提供与终端和管理员之间的安全通信，以及多节点部署内Cisco ISE 节点之间的安全通信。PKI 依赖 X.509 数字证书传输用于消息加密和解密的公钥，并验证代表用户和设备的其他证书的真实性。Cisco ISE 提供管理员门户管理以下两类 X.509 证书：

- 这些证书是识别Cisco ISE 节点到客户端应用的服务器证书。每个Cisco ISE 节点都有自己的系统证书，每个证书及相应的私钥均存储在该节点上。
- 受信任证书 - 这些证书由证书颁发机构 (CA) 颁发，用于为从用户和设备接收的公钥建立信任。受信任证书库还包含由简单证书注册协议 (SCEP) 分发的证书，可将移动设备注册到企业网络中。在主管理节点 (PAN) 上管理受信任证书库中的证书，并且系统会自动将这些证书复制到 Cisco ISE 部署中的所有其他节点。

在分布式部署中，您只能将证书导入到 PAN 的证书信任列表 (CTL) 中。证书会被复制到辅助节点。

一般来说，为了确保Cisco ISE 中的证书身份验证功能不会受到证书驱动的验证功能中细微差别的影响，请为网络中部署的所有Cisco ISE 节点使用小写主机名。

证书使用

当您将证书添加或导入到Cisco ISE 中时，应指定证书的用途：

- Admin：用于节点间通信，以及对管理门户进行身份验证
- EAP：用于基于 TLS 的 EAP 身份验证
- RADIUS DTLS：用于 RADIUS DTLS 服务器身份验证
- Portal：用于与所有Cisco ISE 最终用户门户进行通信
- xGrid：用于与 pxGrid 控制器进行通信

您可以关联每个节点中的不同证书，以便与管理员门户 (Admin)、pxGrid 控制器 (pxGrid) 进行通信，以及进行基于 TLS 的 EAP 身份验证 (EAP)。但针对其中的每种用途，您只能关联每个节点中的一个证书。

由于部署中有多个策略服务节点 (PSN) 可以支持 Web 门户请求，所以Cisco ISE 需要使用唯一标识符来标识必须用于门户通信的证书。当您添加或导出指定用于门户用途的证书时，您必须定义证书组标签并将其与您的部署中各个节点上的对应证书关联。您必须将此证书组标签与对应的最终用户门户关联（访客、发起人和个人设备门户）。此证书组标签是一种唯一标识符，帮助Cisco ISE 标识与这每一个门户通信时必须使用的证书。您可以从每个节点为每个门户指定一个证书。

注释 EAP-TLS 客户端证书应具有 KeyUsage=Key Agreement 和 ExtendedKeyUsage=Client Authentication 以用于以下密码：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS 客户端证书应具有 KeyUsage=Key Encipherment 和 ExtendedKeyUsage=Client Authentication 以用于以下密码：

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

思科 ISE 中的证书匹配

设置部署中的Cisco ISE 节点后，这两个节点将互相通信。系统将检查每个 ISE 节点的 FQDN，以确保其匹配（例如 ise1.cisco.com 和 ise2.cisco.com，如果使用通配符证书，则为 *.cisco.com）。此外，当外部机器向 ISE 服务器提供证书时，将根据 ISE 服务器中的证书对提供用于身份验证的外部证书进行检查（或匹配）。如果两个证书匹配，则身份验证成功。

对于 ，匹配操作将在 节点之间（如果有两个）或 与 pxGrid 之间执行。

Cisco ISE 按以下方式检查匹配的主题名称：

1. Cisco ISE 查看证书的主题别名 (SAN) 扩展。如果 SAN 包含一个或多个 DNS 名称，则其中必须有一个 DNS 名称与Cisco ISE 节点的 FQDN 相匹配。如果使用通配符证书，则通配符域名必须与 Cisco ISE 节点的 FQDN 中的域匹配。
2. 如果 SAN 中不包含 DNS 名称、或 SAN 完全缺失，则证书主题字段中的通用名称或通配符域必须与节点的 FQDN 匹配。
3. 如果未找到匹配项，则会拒绝该证书。

注释 导入到Cisco ISE 的 X.509 证书必须为隐私增强邮件 (PEM) 格式或可辩别编码规则 (DER) 格式。可导入包含证书链（即带有签署该系统证书的受信任证书序列的系统证书）的文件，但会受到某些限制。

X.509 证书的有效性

X.509 证书仅从特定日期开始有效。当系统证书到期时，取决于证书的Cisco ISE 功能会受到影响。当距离到期日还有 90 天时，Cisco ISE 会通知您系统证书即将到期。系统以多种方式显示此通知：

- 彩色到期状态图标显示在 System Certificates 页面。
- 到期消息显示在Cisco ISE 系统诊断报告中。
- 在距离到期日 90 天和 60 天时生成到期警报，在最后 30 天内，每天生成一次警报。

如果即将到期的证书为自签证书，您可以编辑证书，延长到期日。对于 CA 签名的证书，必须留出足够的时间，从 CA 获取替换证书。

在思科 ISE 中启用 PKI

公钥基础结构 (PKI) 是一种加密技术，用于实现安全通信和验证使用数字签名的用户的身份。

步骤 1 在每个部署节点上为启用 TLS 的身份验证协议（如 EAP-TLS）建立系统证书，以用于管理员门户身份验证、供浏览器和 REST 客户端访问Cisco ISE Web 门户，以及用于 pxGrid 控制器。

默认情况下，Cisco ISE 节点预先安装用于 EAP 身份验证、管理员门户、门户和 pxGrid 控制器的自签证书。在典型的企业环境中，此证书由受信任 CA 签名的服务器证书代替。

步骤 2 用与用户建立信任所需的 CA 证书以及向Cisco ISE 出示的设备证书填充受信任证书库。

要使用包含一个根CA证书以及一个或更多中间CA证书的证书链来验证用户或设备证书的真实性，请执行以下操作：

- 为根 CA 启用信任选项。

  从Cisco ISE GUI 中，选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **证书管理 (Certificate Management) 受信任证书 (Trusted certificates)** 在此窗口中，选择根 CA 证书，然后点击**编辑 (Edit)**。在**使用 (Usage)** 选项卡中，选择**信任范围 (Trusted For)** 部分中的复选框。

- 如果不想为根 CA 启用信任选项，请将整个 CA 证书链导入受信任证书存储区。

对于节点间通信，您必须使用验证属于Cisco ISE 部署中每个节点的管理员系统证书所需的信任证书填充受信任证书库。如果您想要使用默认自签证书进行节点间通信，则必须从每个Cisco ISE节点的“系统证书”(System Certificates)页面导出该证书并将其导入受信任证书库。如果您用 CA 签名的证书代替自签证书，只需用相应的根 CA 和中间 CA 证书填充受信任证书库。请注意，在完成此步骤之前，您无法在Cisco ISE 部署中注册节点。

当自带设备用户从一个位置移动到另一个位置时，如果您使用自签证书确保部署中客户端与PSN之间的安全通信，EAP-TLS 用户身份验证会失败。对于这种必须在某些 PSN 之间实现的身份验证请求，您必须通过外签 CA 证书或使用外部 CA 签名的通配符证书确保客户端与 PSN 之间的通信。

注释 在您从独立Cisco ISE 节点或PAN获取备份后，如果您更改您的部署中一个或更多节点上的证书配置，您必须再获得一个备份以恢复数据。否则，如果您尝试使用较旧的备份恢复数据，节点之间的通信可能会发生故障。

通配符证书

通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。例如，Certificate Subject中的CN值可以是一些通用主机名（例如aaa.ise.local），SAN字段会包含相同的通用主机名和通配符表示法（例如 DNS.1=aaa.ise.local 和 DNS.2=*.ise.local）。

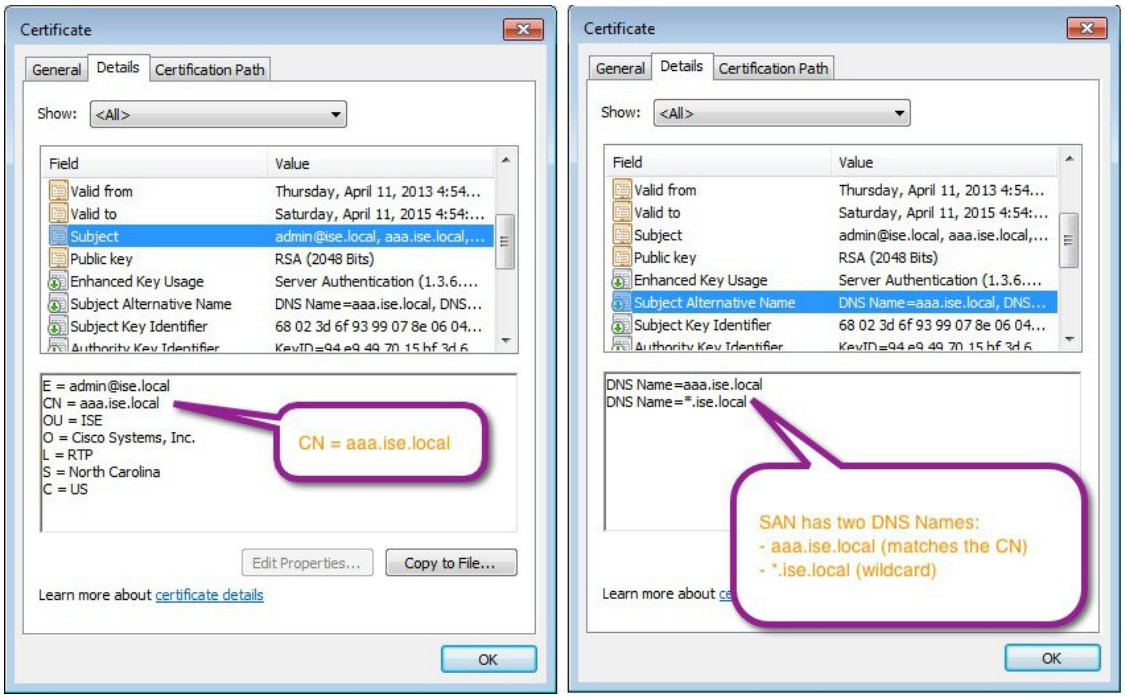
如果将某个通配符证书配置为使用 *.ise.local，可以使用同一证书来保护 DNS 名称以“.ise.local”结尾的任何其他主机，例如：。：

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

通配符证书用与普通证书一样的方式保护通信安全，并且使用相同的验证方法处理请求。

下图显示用于保护 Web 站点的一个通配符证书的示例。

图 *6:* 通配符证书示例



思科 ISE 中的通配符证书支持

Cisco ISE 支持通配符证书。在较低版本中，Cisco ISE 会验证为 HTTPS 启用的任何证书以确保 CN 字段与主机的完全限定域名 (FQDN) 完全一致。如果字段不一致，则证书无法用于 HTTPS 通信。

在较低版本中，Cisco ISE 使用该 CN 值来替换 url-redirect A-V 对字符串中的变量。此 CN 值还曾用于所有集中式 Web 身份验证 (CWA)、自行激活、安全评估重定向等。

Cisco ISE 使用 ISE 节点的主机名作为 CN。

适用于 HTTPS 和 EAP 通信的通配符证书

您可以在Cisco ISE 中将通配符服务器证书用于使用 SSL/TLS 隧道的 Admin（基于 Web 的服务）和 EAP 协议。通过使用通配符证书，不再需要为每个Cisco ISE 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的多个节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个Cisco ISE 节点分配唯一服务器证书的安全性低。

在向访客门户分配公共通配符证书并随根 CA 证书一起导入从属 CA 时，直到 ISE 服务重新启动后才会发送证书链。

注释 如果使用通配符证书，我们强烈建议您将域空间进行分区，以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，就可能导致严重的安全问题。

通配符证书在域名前使用星号 (*) 和一个句点。例如，证书的使用者名称的 CN 值是一般主机名称（例如 aaa.ise.local）,SAN 字段可以使用通配符，例如 *.ise.local。Cisco ISE 支持使用通配符证书，其中通配符 (*) 是所显示标识符最左侧的字符。例如，*.example.com 或 *.ind.example.com。Cisco ISE 不支持所显示的标识符中连通配符一起显示其他字符的证书。例如，abc*.example.com 或 a*b.example.com 或 *abc.example.com。

URL 重定向中的完全限定域名

当Cisco ISE 建立授权配置文件重定向时（用于集中 Web 身份验证、设备注册 Web 身份验证、本地请求方调配、移动设备管理和客户端调配与安全评估服务），所产生的 cisco-av-pair 包括一个类似于以下内容的字符串：

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

处理此请求时，Cisco ISE 会用实际值代替此字符串中的某些关键字。例如，Cisco ISE 会将 SessionIdValue 替换为该请求的实际会话 ID。对于 eth0 接口，Cisco ISE 将 URL 中的 IP 替换为Cisco ISE 节点的 FQDN。对于非 eth0 接口，Cisco ISE 使用 URL 中的 IP 地址。您可以为接口 eth1 至 eth3 分配主机别名（名称），然后在 URL 重定向期间，Cisco ISE 可以用其代替 IP 地址。

要实现此操作，您可以在配置模式下从 ISE CLI ISE /admin(config)# 提示符处使用 **ip host** 命令：

ip host *IP_address host-alias FQDN-string*

其中 IP_address 是网络接口的 IP 地址（eth1 或 eth2 或 eth3），host-alias 是您分配给网络接口的名称。FQDN-string 是网络接口的完全限定域名。使用此命令，您可以向网络接口分配主机别名或FQDN 字符串，或同时分配主机别名和 FQDN 字符串。

这是使用 **ip host** 命令的一个示例：ip host a.b.c.d sales sales.amerxyz.com

向非 eth0 接口分配主机别名之后，您必须在Cisco ISE 上使用 **application start ise** 命令重新启动应用服务。

使用此命令的 no 形式可删除主机别名与网络接口的关联。

no ip host *IP_address host-alias FQDN-string*

使用 **show running-config** 命令以查看主机别名定义。

如果您提供 FQDN 字符串，Cisco ISE 会使用 FQDN 替换 URL 中的 IP 地址。如果您仅提供主机别名，Cisco ISE 会将主机别名与所配置的 IP 域名组合以形成完整的 FQDN，并用 FQDN 替换 URL 中的 IP 地址。如果您不将网络接口映射至主机别名，则Cisco ISE 会使用 URL 中的网络接口的 IP 地址。

当您将非 eth0 接口用于客户端调配或本地请求方或访客流程时，您必须确保在策略服务节点证书的 SAN 字段中正确配置非 eth0 接口的 IP 地址或主机别名。

使用通配符证书的优势

- 节约成本。由第三方证书颁发机构签名的证书都很昂贵，尤其是当服务器数量增加的时候。在 Cisco ISE 部署中，可以在多个节点上使用通配符证书。

- 提高运营效率。通配符证书允许所有策略服务节点 (PSN) EAP 和 Web 服务共享同一证书。除了能显著节约成本之外，由于可以只创建证书一次，然后就可以将其应用于所有 PSN，所以还能简化证书管理。
- 降低身份验证错误。通配符证书可以解决 Apple iOS 设备常见的证书问题，即客户端将受信任证书存储于配置文件中，而不遵循信任签名 root 的 iOS Keychain。当 iOS 客户端首次与 PSN 通信时，它不会明确信任 PSN 证书，即使受信任证书颁发机构已为该证书签名。使用通配符证书，所有 PSN 上证书都将一样，所以用户只须接受一次该证书，接下来对不同 PSN 的身份验证就会继续进行，而不会报错或出现提示。
- 简化请求方配置。例如，启用 PEAP-MSCHAPv2 和服务器证书信任的 Microsoft Windows 请求方要求您指定要信任的各个服务器证书，否则当客户端使用不同的 PSN 进行连接时，系统会提示用户是否信任各个 PSN 证书。使用通配符证书，可以信任一个统一的服务器证书，而不需从每个 PSN 逐一信任各个证书。
- 通配符证书可以减少提示，增强无缝连接，从而提高用户体验。

使用通配符证书的缺点

以下是与通配符证书相关的一些安全问题：

- 失去可审核性和不可否认性
- 提高了私钥的泄露风险
- 不常见或管理员不了解

通常认为通配符证书没有每个 ISE 节点均拥有的唯一的服务器证书那么安全。但是，成本和运营因素比安全风险更重要。

ASA 等安全设备也支持通配符证书。

部署通配符证书时，一定要谨慎。例如，如果您使用 *.company.local 创建一个证书，而某个攻击者能够发现其私钥，则该攻击者就可以监听 company.local 域中的任意服务器。因此，最好给域空间分区以避免这类威胁。

要解决可能出现的这个问题和限制使用范围，也可以使用通配符证书保护您的组织的具体子域。在您想要指定通配符的通用名称子域部分添加一个星号 (*)。

例如，如果您为 *.ise.company.local 配置通配符证书，则可以将该证书用于保护 DNS 名称以“.ise.company.local”结尾的任意主机，例如：

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

通配符证书兼容性

通常在创建通配符证书时，会将通配符列为证书使用者的公用名 (CN)。Cisco ISE 支持这种类型的结构。但并不是所有的终端请求方都支持在证书使用者中使用通配符字符。

通过测试的所有 Microsoft 本机请求方（包括 Windows Mobile）不支持在证书使用者中使用通配符字符。

您可以使用另一个请求方，例如 Cisco AnyConnect 网络访问管理器 (NAM)，它可能允许在 Subject 字段中使用通配符字符。

您还可以使用特殊通配符证书（例如设计为与不兼容设备配合使用的 DigiCert 的 Wildcard Plus），方法是在证书的 Subject Alternative Name 中包含特定子域。

尽管 Microsoft 请求方限制似乎禁止使用通配符证书，但仍有其他方法创建通配符证书，允许它与通过测试的所有设备配合使用，从而实现安全访问，包括 Microsoft 本机请求方。

为此，您必须在 Subject Alterative Name (SAN) 字段中使用通配符字符，而不是在 Subject 中使用通配符字符。SAN 字段保留专为检查域名而设计的扩展名（DNS 名称）。有关详细信息，请参阅 RFC 6125 和 2128。

证书层次结构

在管理员门户中，您可以查看所有终端、系统和受信任证书的证书层次结构或证书信任链。证书层级包括证书、所有中间证书颁发机构 (CA) 证书和根证书。例如，当选择从管理员门户查看系统证书时，默认情况下会显示相应系统证书的详细消息。证书层级显示在该证书的顶部。点击层次结构中的任何证书可查看其详细信息。自签名证书没有任何层次结构或信任链。

在证书列表页面的“状态”(Status) 列中，您将会看到以下图标之一：

- 绿色图标 - 表示有效证书（有效信任链）
- 红色图标 - 表示存在错误（例如，信任证书缺失或过期）
- 黄色图标 - 警告证书即将到期并提示续订

系统证书

Cisco ISE 系统证书是向部署中的其他节点和客户端应用标识Cisco ISE 节点身份的服务器证书。系统证书的用途如下：

- 用于Cisco ISE 部署中的节点间通信。在 Usage 字段中为这些证书选择 Admin 选项。
- 由浏览器和连接到Cisco ISE Web 门户的 REST 客户端使用。在 Usage 字段中为这些证书选择 Portal 选项。
- 用于与 PEAP 和 EAP-FAST 组成外部 TLS 隧道。在 Usage 字段中选择 EAP 选项，以使用 EAP-TLS、PEAP 和 EAP-FAST 进行相互身份验证。
- 用于 RADIUS DTLS 服务器身份验证。
- 用于与 SAML 身份提供程序 (IdP) 进行通信。在“使用”(Usage) 字段中为这证书选择 SAML 选项。如果选择了 SAML 选项，则该证书不可用于其它服务。
- 用于与 pxGrid 控制器通信。在 Usage 字段中为这些证书选择 pxGrid 选项。

必须在Cisco ISE 部署中的每个节点上安装有效的系统证书。默认情况下，在安装期间，将在Cisco ISE 节点上创建两个自签证书和一个由内部Cisco ISE CA 签名的证书：

- 指定用于 EAP、管理员、门户和 RADIUS DTLS 的自签名服务器证书（密钥长度为 2048，有效期为一年）
- 可用于确保与 SAML IdP 之间安全通信的自签名 SAML 服务器证书（密钥长度为 2048，有效期为一年）
- 可用于确保与 pxGrid 客户端之间安全通信的内部Cisco ISE CA 签名的服务器证书（密钥长度为 4096，有效期为一年）。

设置部署并注册辅助节点时，指定用于 pxGrid 控制器的证书将自动替换为由主要节点的 CA 签名的证书。因此，所有 pxGrid 证书将属于同一 PKI 信任层次结构。

注释 当导出要导入其他节点的通配符系统证书（用于节点间通信）时，请确保导出证书和私钥，并指定加密密码。在导入过程中，将需要证书、私钥和加密密码。

注释 要确定对应于您的版本的支持密钥和密码信息，请查找适当版本的《思科身份识别服务引擎网络组件兼容性》指南。

为了提高安全性，建议您使用 CA 签名的证书替换自签证书。要获取 CA 签名的证书，您必须：

1. 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 160 页
2. 将根证书导入受信任证书库，第 154 页
3. 将 CA 签名的证书与 CSR 绑定，第 160 页

ISE 社区资源

步骤：实施 ISE 服务器端证书

思科身份识别服务引擎上的证书更新配置指南

查看系统证书

“系统证书”(System Certificate) 页面列出添加至Cisco ISE 的所有系统证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

系统显示“系统证书”(System Certificates) 页面，提供关于本地证书的以下信息：

- “友好名称”(Friendly Name) - 证书的名称。
- “使用者”(Used By) - 使用此证书的服务。
- “门户组标记”(Group Tag) - 仅适用于指定用于门户用途的证书。指定必须将哪个证书用于门户。
- “颁发给”(Issued To) - 证书使用者的通用名称。
- “颁发者”(Issued By) - 证书颁发者的通用名称。
- “生效日期”(Valid From) - 创建证书的日期，也称为开始时间证书属性。
- “到期日期”(Expiration Date) - 证书的到期日期，也称为截止时间证书属性。指示证书何时过期。到期日期有五个类别，每个类别有一个如下所述的关联图标：
  - 距到期还有 90 天以上（绿色图标）
  - 距到期还有 90 天或不足 90 天（蓝色图标）
  - 距到期还有 60 天或不足 60 天（黄色图标）
  - 距到期还有 30 天或不足 30 天（橙色图标）
  - 已到期（红色图标）

步骤 2 选择一个证书并选择 **查看 (View)** 以显示证书详细信息。

导入系统证书

可以从管理员门户为任意Cisco ISE 节点导入系统证书。

注释 在主 PAN 上更改管理员角色证书时会在所有其他节点上重新启动服务。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

开始之前

- 确保您在运行客户端浏览器的系统上拥有系统证书和私钥文件。
- 如果您导入的系统证书由外部 CA 签名，则将相关根 CA 或中间 CA 证书导入受信任证书存储区（**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任的证书 (Trusted Certificates)**）。
- 如果导入的系统证书中包含 CA 标志设置为 true 的基本约束扩展，请确保有密钥用法扩展并且设置了 keyEncipherment 位或 keyAgreement 位。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1

步骤 2 点击**导入 (Import)**。
此时将打开“导入服务器证书”(Import Server Certificate) 屏幕。

步骤 3 输入您要导入的证书的值。

步骤 4 点击**提交 (Submit)**。

系统证书导入设置

下表介绍可用于导入服务器证书的“导入系统证书”(Import System Certificate) 窗口上的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)** > **导入 (Import)**。

表 *17:* 系统证书导入设置

字段名称	说明
选择节点 (Select Node)	（必填）选择您要导入系统证书的Cisco ISE 节点。
证书文件 (Certificate File)	（必填）点击**浏览 (Browse)**，从本地系统中选择证书文件。
私钥文件 (Private Key File)	（必填）点击 **浏览 (Browse)** 选择私钥文件。
密码 (Password)	（必填）输入密码以解密私钥文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，Cisco ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
允许通配符证书 (Allow Wildcard Certificates)	如果要导入通配符证书，请选中此复选框。通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。 如果选中此复选框，Cisco ISE 会将此证书导入到部署中的所有其他节点。
验证证书扩展名 (Validate Certificate Extensions)	如果希望Cisco ISE 验证证书扩展，请选中此复选框。如果选中此复选框，并且要导入的证书包含 CA 标志设为 true 的基本限制扩展，请确保密钥用法扩展存在，并且设置了 keyEncipherment 位和/或 keyAgreement 位。

字段名称	说明
使用情况 (Usage)	选择应使用此系统证书的服务： • **管理员 (Admin)**：用于确保与部署中的管理员门户和 ISE 节点之间安全通信的服务器证书 注释 在主 PAN 上更改管理员角色证书时会在所有其他节点上重新启动服务。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL/TLS 隧道的身份验证的服务器证书 • **RADIUS DTLS**：用于 RADIUS DTLS 身份验证的服务器证书 • **pxGrid**：用于确保pxGrid客户端和服务器之间的安全通信的客户端和服务器证书。 • **ISE 消息服务 (ISE Messaging Service)**：用于**经思科 ISE 消息传递的系统日志 (Syslog Over Cisco ISE Messaging)** 功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **门户 (Portal)**：用于确保与所有Cisco ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书，第 138 页
查看系统证书，第 139 页
导入系统证书，第 140 页

生成自签证书

通过生成自签证书添加新的本地证书。Cisco建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署Cisco ISE，务必尽可能使用CA签名证书，确保生产网络中更统一地接受。

注释 如果正使用自签证书并且必须更改Cisco ISE 节点的主机名，则必须登录Cisco ISE 节点的管理员门户，删除采用旧主机名的自签证书，然后生成新的自签证书。否则，Cisco ISE 将继续使用采用旧主机名的自签证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

自签证书设置

下表介绍“生成自签证书”(Generate Self Signed Certificate) 页面上的字段。您可以通过此页面为节点间通信、EAP-TLS 身份验证、Cisco ISE Web 门户创建系统证书以及与 pxGrid 控制器通信。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)** > **生成自签名证书 (Generate Self Signed Certificate)**。

表 *18:* 自签证书设置

字段名称	使用指南
选择节点 (Select Node)	（必填）您要生成系统证书的节点。
公共名称 (CN) (Common Name [CN])	（如果您不指定 SAN，则此字段必填）默认情况下，Common Name 为您要生成自签证书的 ISE 节点的完全限定域名。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
主体可选名称 (SAN) (Subject Alternative Name [SAN])	与该证书关联的 IP 地址、DNS 名称或统一资源标识符 (URI)。
密钥类型 (Key Type)	指定要用于创建公共密钥的算法：RSA 或 ECDSA。

字段名称	使用指南
密钥长度 (Key Length)	指定公共密钥的位大小。以下选项可用于 RSA： • 512 • 1024 • 2048 • 4096 以下选项可用于 ECDSA： • 256 • 384 注释 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。 如果您计划获得公共 CA 签名的证书或将思科 ISE 部署为符合 FIPS 的策略管理系统，请选择 2048。
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。
过期 TTL (Expiration TTL)	指定证书到期之前的天数。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，Cisco ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
允许通配符证书 (Allow Wildcard Certificates)	如果要生成自签名通配符证书，请选中此复选框。通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。

字段名称	使用指南
使用情况 (Usage)	选择应使用此系统证书的服务： • **管理 (Admin)**：用于确保与部署中的管理员门户和 ISE 节点之间安全通信的服务器证书。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL/TLS 隧道的身份验证的服务器证书。 • **RADIUS DTLS**：用于 RADIUS DTLS 身份验证的服务器证书。 • **pxGrid**：用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务器证书。 • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **门户 (Portal)**：用于确保与所有Cisco ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书，第 138 页
查看系统证书，第 139 页
生成自签证书，第 142 页

编辑系统证书

可以使用此页面编辑系统证书，续订自签证书。当编辑通配符证书时，更改将被复制到部署中的所有节点上。当删除通配符证书时，此通配符证书将从部署中的所有节点删除。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要编辑的证书旁边的复选框，然后点击**Edit**。

步骤 3 要续订自签证书，请选中**续签期限 (Renewal Period)** 复选框，然后输入以天、周、月或年为单位的到期 TTL。

步骤 4 点击**保存 (Save)** 保存更改。

如果选中**管理 (Admin)** 复选框，系统将重新启动Cisco ISE 节点上的应用服务器。此外，如果Cisco ISE 节点是部署中的 PAN，系统还将重新启动部署中所有其他节点上的应用服务器。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

注释 使用 Chrome 65 及更高版本启动 ISE 可能会导致 BYOD 门户或访客门户无法在浏览器中启动，即使 URL 已成功重定向也是如此。这是因 Google 引入的新安全功能所致，此功能要求所有证书具有“主题备用名称”(Subject Alternative Name) 字段。对于版本 ISE 2.4 及更高版本，必须填充“主题备用名称”(Subject Alternative Name) 字段。

要使用 Chrome 65 及更高版本启动，请执行以下步骤：

1。通过填充“主题备用名称”(Subject Alternative Name) 字段，从 ISE GUI 生成新的自签证书。必须同时填写 DNS 和 IP 地址。

2. ISE 服务此时会重新启动。

3. 在 Chrome 浏览器中重定向门户。

4. 在浏览器中，“查看证书”(View Certificate) > “详细信息”(Details) > 通过选择 base-64 编码来“Copy the certificate”(复制证书)。

5. 将证书安装到受信任路径。

6. 关闭 Chrome 浏览器，然后尝试重定向门户。

注释 在为操作系统 Win RS4 或 RS5 中的浏览器 Firefox 64 及更高版本配置无线 BYOD 设置时，可能无法添加证书例外。如果是全新安装 Firefox 64 及更高版本，此行为是预计行为，如果是从先前版本升级到 Firefox 64 及更高版本，则不会出现此行为。在这种情况下，可以通过以下步骤添加证书例外：

1. 针对 BYOD 流程单/双 PEAP 或 TLS 进行配置。

2. 通过 Windows ALL 选项配置 CP 策略。

3. 在最终客户端 Windows RS4/RS5 中连接 Dot1.x/MAB SSID。

4. 在 FF64 浏览器中键入 1.1.1.1 以重定向至访客/BYOD 门户。

5. 点击**添加例外 (Add Exception)** > **无法添加证书 (Unable to add certificate)**，然后继续执行流程。

变通方案是，需要导航至**选项 (Options)** > **隐私和设置 (Privacy & Settings)** > **查看证书 (View Certificates)** > **服务器 (Servers)** > **添加例外 (Add Exception)**

，手动为 Firefox 64 添加证书。

删除系统证书

您可以删除不再使用的系统证书。

可以一次从系统证书存储区中删除多个证书，但必须至少具有一个可用于管理员和 EAP 身份验证的证书。此外，无法删除用于管理员、EAP 身份验证、门户或 pxGrid 控制器的任何证书。但是，在禁用服务时可以删除 pxGrid 证书。

如果您选择删除通配符证书，则系统会从部署中的所有节点删除该证书。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中想要删除的证书旁边的复选框，然后点击**删除 (Delete)**。

系统将显示一条警告消息。

步骤 3 点击**是 (Yes)**，删除证书。

导出系统证书

您可以导出所选择的系统证书或某个证书及其关联的私钥。如果您导出证书及其私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要导出的证书旁的复选框，然后点击**导出 (Export)**。

步骤 3 选择是仅导出证书，还是导出证书及其关联的私钥。

提示 由于可能会暴露私钥值，我们不建议导出与证书关联的私钥。如果您必须导出私钥（例如，导出要导入其他节点以用于节点间通信的通配符系统证书时），请指定私钥加密密码。在将此证书导入另一Cisco ISE节点时，需要指定此密码以解密私钥。

步骤 4 如果您已选择导出私钥，请输入此密码。此密码至少必须包含 8 个字符。

步骤 5 点击**导出 (Export)** 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以隐私强化邮件的格式进行存储。如果同时导出证书和私钥，则证书会导出为 .zip 文件，其中包含隐私强化邮件格式的证书和已加密的私钥文件。

受信任证书库

受信任证书库包括用于信任和简单证书注册协议 (SCEP) 的 X.509 证书。

受信任证书库中的证书在 PAN 上进行管理，并且复制至Cisco ISE 部署中的每个节点。Cisco ISE 支持通配符证书。

Cisco ISE 将受信任证书用于以下用途：

- 验证由终端和访问ISE-PIC管理员门户的Cisco ISE 管理员（使用基于证书的管理员身份验证）用于身份验证的客户端证书。
- 确保部署中Cisco ISE 节点之间的安全通信。受信任证书库必须包含与部署中每个节点上的系统证书建立信任所需的 CA 证书链。

- 如果将自签证书用于系统证书，则各个节点的自签证书必须放在 PAN 的受信任证书库中。
- 如果将自签证书用于系统证书，则 CA root 证书以及信任链中的任何中间证书都必须放在 PAN 的受信任证书库中。

- 实现安全的 LDAP 身份验证，在定义将通过 SSL 访问的 LDAP 身份源时，必须从证书存储区选择证书。
- 向准备使用个人设备门户在网络中进行注册的个人设备进行分配。Cisco ISE 在策略服务节点 (PSN) 上实施 SCEP 以支持个人设备注册。注册设备使用 SCEP 协议从 PSN 请求客户端证书。PSN 包含作为中介的注册机构 (RA)；RA 接收并验证来自注册设备的请求，然后将请求转发给颁发客户端证书的外部 CA 或内部Cisco ISE CA。CA 将证书发送回 RA，RA 再将其返回至设备。

  Cisco ISE 使用的每个SCEP CA 都通过 SCEP RA 配置文件定义。当创建 SCEP RA 配置文件时，系统将以下两个证书自动添加到受信任证书库：

  - CA 证书（自签证书）
  - RA 证书（证书请求代理证书），由 CA 签名。

  SCEP 协议要求 RA 将这两个证书提供给注册设备。通过将这两个证书放入受信任证书库，系统将其复制至所有 PSN 节点，以供这些节点上的 RA 使用。

注释 删除 SCEP RA 配置文件时，关联的 CA 链也会从受信任证书库中删除。但是，如果安全系统日志、LDAP 系统或信任证书引用相同的证书，则仅删除 SCEP 配置文件。

注释

- 导入到Cisco ISE 的 X.509 证书的格式必须为隐私增强邮件 (PEM) 或卓越编码规则 (DER)。可以根据特定限制，导入包含证书链的文件，也就是系统证书以及签名的受信任证书的序列。
- 在向访客门户分配公共通配符证书并随根 CA 证书一起导入子 CA 时，直到 ISE 服务重新启动后才会发送证书链

ISE 社区资源

在 ISE 2.0 中安装第三方 CA 证书

受信任证书库中的证书

受信任证书库中包含受信任的证书：生产证书、根证书、 和其他受信任的证书。根证书（Cisco根 CA）给生产（Cisco CA 生产）证书签名。默认情况下禁用这些证书。如果您在部署中将Cisco IP 电话作为终端，您应启用这两个证书，从而可以对用于电话的Cisco签名的客户端证书进行身份验证。

受信任证书库页面

下表介绍“受信任证书库页面”(Trusted Certificates Store) 窗口上的字段，您可以使用此页面查看添加到管理节点的证书。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

表 *19:* 证书库页面

字段名称	使用指南
友好名称 (Friendly Name)	显示证书的名称。
状态 (Status)	“启用”(Enabled) 或“禁用”(Disabled)。如果选择“禁用”(Disabled)，ISE 将不使用此证书建立信任。
信任范围 (Trusted for)	显示使用此证书的服务。
颁发给 (Issued To)	证书使用者的通用名称 (CN)。
颁发者 (Issued By)	证书颁发者的通用名称 (CN)。
生效日期 (Valid From)	“开始时间”证书属性。
到期日期 (Expiration Date)	“截止时间”证书属性。
到期状态 (Expiration Status)	提供有关证书到期状态的信息。此列显示五个图标和提示消息类别： • **绿色**：距到期还有 90 天以上 • **蓝色**：距到期还有 90 天或更短 • **黄色**：距到期还有 60 天或更短 • **橙色**：距到期还有 30 天或更短 • **红色**：已到期

相关主题

受信任证书库，第 147 页
查看受信任证书库证书，第 150 页
更改受信任证书库中的证书状态，第 151 页
在受信任的证书库中添加证书，第 151 页

受信任证书命名限制

CTL 中的受信任证书可以包含名称限制扩展。此扩展为证书链中后续证书的所有主题名称和主题替代名称的值定义命名空间。Cisco ISE 不检查根证书中指定的限制。

Cisco ISE 支持以下名称限制：

- 目录名称

  目录名称限制应该是主题/SAN 中目录名称的前缀。例如，

  - 正确的主题前缀：

    CA 证书名称限制：Permitted: O=Cisco

    客户端证书主题：O=Cisco,CN=Salomon

  - 不正确的主题前缀：

    CA 证书名称限制：Permitted: O=Cisco

    客户端证书主题：CN=Salomon,O=Cisco

- DNS
- 邮件
- URI（URI 限制必须以一个 URI 前缀开头，例如 http://、https://、ftp:// 或 ldap://）。

Cisco ISE 不支持以下名称限制：

- IP 地址
- 其他名称

当受信任证书包含不支持的限制并且验证的证书不包含相应字段时，系统会拒绝此证书，因为Cisco ISE 无法验证不支持的限制。

以下是受信任证书中名称限制的一个示例：

```
 X509v3 Name Constraints: critical Permitted: othername:<unsupported> email:.abcde.at
email:.abcde.be email:.abcde.bg email:.abcde.by DNS:.dir DirName: DC = dir, DC = emea
DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic DirName: C = BG, ST =
EMEA, L = BG, O = ABCDE Group, OU = Domestic DirName: C = BE, ST = EMEA, L = BN, O = ABCDE
 Group, OU = Domestic DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service
Z100 URI:.dir IP:172.23.0.171/255.255.255.255 Excluded: DNS:.dir URI:.dir
```

以下是与以上定义匹配的一个可接受客户端证书主题：

```
 Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1, CN=cwinwell
```

查看受信任证书库证书

“受信任证书”(Trusted Certificates) 页面列出所有已添加到Cisco ISE 的受信任证书。 要查看受信任的证书，您必须成为超级管理员或系统管理员。

要查看所有证书，请依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。系统将显示受信任证书页面，其中列出了所有受信任的证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

更改受信任证书库中的证书状态

必须启用证书状态，Cisco ISE 才能使用此证书建立信任。将证书导入受信任证书库时，将自动启用此证书。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 3 选中想要启用或禁用的证书旁边的复选框，然后点击 **编辑 (Edit)**。

步骤 4 更改状态。

步骤 5 点击**保存 (Save)**。

在受信任的证书库中添加证书

可以通过“证书存储区”(Certificate Store) 页面向Cisco ISE 添加 CA 证书。

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 确保证书库证书位于运行您的浏览器的计算机文件系统上。证书必须是 PEM 或 DER 格式。
- 如果您计划将证书用于管理员或 EAP 身份验证，请确保在证书中定义基本限制并且确保 CA 标志设置为 true。

编辑受信任证书

在将证书添加到受信任证书库之后，可以通过使用编辑设置进行进一步编辑。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2 选中要编辑的证书旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 根据需要修改可编辑字段。

步骤 4 点击**保存 (Save)** 以保存对证书库所做的更改。

编辑证书设置

下表介绍了“证书存储区编辑证书”(Certificate Store Edit Certificate) 窗口上的字段，可以使用此窗口编辑证书颁发机构 (CA) 证书属性。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管**

理 **(Administration)** > 系统 **(System)** > 证书 **(Certificates)** > 受信任证书 **(Trusted Certificates)** > 证书 **(Certificate)** > 编辑 **(Edit)**。

表 ***20:*** 证书库编辑设置

字段名称	使用指南
证书颁发者 (Certificate Issuer)	
友好名称 (Friendly Name)	输入证书的友好名称。
状态 (Status)	选择“启用”(Enabled) 或“禁用”(Disabled)。如果选择“禁用”(Disabled)，ISE 将不使用此证书建立信任。
说明	输入可选的说明。
使用情况 (Usage)	
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您想要使用此证书验证服务器证书（从其他 ISE 节点或 LADP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅适用于选中“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框的情况）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部Cisco服务，请选中此复选框。
证书状态验证 (Certificate Status Validation)	ISE 支持使用两种方法检查特定 CA 颁发的客户端或服务器证书的吊销状态。第一种方法是使用在线证书状态协议 (OCSP) 验证证书，其将向 CA 维护的 OCSP 服务发送请求。第二种方法是按照从 CA 下载至 ISE 的证书吊销列表 (CRL) 验证证书。可以同时启用这两种方法，在这种情况下首先使用 OCSP 方法，只有在无法确定证书状态时，才会使用 CRL 方法。
验证 OCSP 服务 (Validate Against OCSP Service)	选中此复选框以按照 OCSP 服务验证证书。您必须先创建 OCSP 服务才能选中此复选框。
如果 OCSP 返回未知状态则拒绝请求 (Reject the request if OCSP returns UNKNOWN status)	如果 OCSP 无法确定证书状态，则选中此复选框以拒绝请求。在选中此复选框的情况下，如果 OCSP 服务返回未知状态值，此服务将导致 ISE 拒绝当前评估的客户端或服务器证书。

字段名称	使用指南
OCSP 响应器无法访问时拒绝请求 (Reject the request if OCSP Responder is unreachable)	选中此复选框供 ISE 在 OCSP 响应器无法访问时拒绝请求。
下载 CRL (Download CRL)	选中此复选框以使Cisco ISE 下载 CRL。
CRL 分类的 URL (CRL Distribution URL)	输入用于从 CA 下载 CRL 的 URL。如果在证书颁发机构证书中指定了URL，则系统会自动填写此字段。URL 必须以“http”、“https”或“ldap”开头。
检索 (Retrieve CRL)	可以自动或定期下载 CRL。请配置下载时间间隔。
如果下载失败，请稍候 (If download failed, wait)	配置在Cisco ISE 再次尝试下载 CRL 之前等待的时间间隔。
如果 CRL 没有收到，绕过此 CRL 验证 (Bypass CRL Verification if CRL is not Received)	选中此复选框，以使系统在收到CRL之前接受客户端请求。如果取消选中此复选框，Cisco ISE会拒绝使用选定CA签名的证书的所有客户端请求，直到收到 CRL 文件为止。
忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)	如果您希望Cisco ISE忽略开始日期和到期日期并继续使用非活动或已过期 CRL 以及根据 CRL 内容允许或拒绝EAP-TLS身份验证，请选中此复选框。 如果您希望Cisco ISE 在 Effective Date 字段指定的开始日期和 Next Update 字段指定的到期日期检查CRL文件，请取消选中此复选框。如果CRL尚未激活或已到期，Cisco ISE 会拒绝使用此 CA 签名的证书的所有身份验证。

相关主题

受信任证书库，第 147 页
编辑受信任证书，第 151 页

删除受信任证书

可以删除不再需要的受信任证书。不过，请确保不会删除 ISE 内部 CA（证书颁发机构）证书。ISE 内部 CA 证书只能在替换整个部署的 ISE 根证书链时删除。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2 选中想要删除的证书旁边的复选框，然后点击**删除 (Delete)**。

系统将显示一条警告消息。如果已选择删除 ISE 内部 CA 证书，则点击：

- **删除 (Delete)** - 删除 ISE 内部 CA 证书。ISE 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。要允许终端再次接入网络，请将相同的 ISE 内部 CA 证书导入受信任证书存储区。
- **删除并撤销 (Delete & Revoke)** - 删除并撤销 ISE 内部 CA 证书。ISE 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。此操作无法撤销。必须替换整个部署的 ISE 根证书链。

步骤 3 点击**是 (Yes)**，删除证书。

从受信任证书库导出证书

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

注释 如果从内部CA导出证书，并计划使用该导出从备份恢复，则必须使用CLI命令 `application configure ise`。有关详细信息，请参阅导出思科 ISE CA 证书和密钥，第 187 页。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 。

步骤 2

步骤 3 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

步骤 4 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。

将根证书导入受信任证书库

导入根 CA 和中间 CA 证书时，您可以指定要为其使用受信任 CA 证书的服务。

开始之前

您必须具有来自已对 CSR 进行签名并返回数字签名 CA 证书的证书颁发机构的根证书和其他中间证书。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 2

步骤 3 点击**导入 (Import)**。

步骤 4 在显示的**将新证书导入证书存储区 (Import a new Certificate into the Certificate Store)** 窗口中，点击**选择文件 (Choose File)** 以选择您的 CA 签名和返回的根 CA 证书。

步骤 5 在**友好名称 (Friendly Name)** 中输入友好的名称。

如果没有输入**友好名称**，Cisco ISE 将使用 *common-name#issuer#nnnnn* 格式的名称填充此字段， 其中 *nnnnn* 是唯一编号。可以再次编辑证书来更改**友好名称**。

步骤 6 选中要为其使用此受信任证书的服务旁边的复选框。

步骤 7 （可选）在**说明** 字段中，输入此证书的说明。

步骤 8 点击**提交 (Submit)**。

下一步做什么

将中间 CA 证书导入到受信任证书库（如果适用）。

受信任证书导入设置

下表说明了“受信任证书导入”(Trusted Certificate Import) 窗口上的字段，可以使用此窗口将证书颁发机构 (CA) 证书添加到Cisco ISE。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)**。

表 ***21:*** 受信任证书导入设置

字段名称	说明
证书文件 (Certificate File)	点击**浏览 (Browse)** 从运行浏览器的计算机选择证书文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果不指定名称，Cisco ISE 会自动按照 <通用名称>#<颁发者>#<nnnnn> 的格式创建名称，其中 <nnnnn> 为唯一的五位数编号。
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您希望将此证书用于验证服务器证书（从其他 ISE 节点或 LDAP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅在选中了“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部Cisco服务，请选中此复选框。

字段名称	说明
验证证书扩展名 (Validate Certificate Extensions)	（仅适用于同时选中“信任客户端身份验证和系统日志”(Trust for client authentication and Syslog) 选项和“证书扩展上启用验证”(Enable Validation of Certificate Extensions) 选项的情况下）确保有“keyUsage”扩展并且设置了“keyCertSign”位，而且有将 CA 标志设置为 true 的基本限制扩展。
说明	输入可选的说明。

相关主题

受信任证书库，第 147 页
证书链导入，第 156 页
将根证书导入受信任证书库，第 154 页

证书链导入

您可以从单个文件导入多个证书，这个文件中包含从证书库接收的证书链。文件中的所有证书都必须为隐私增强邮件 (PEM) 格式，并且这些证书必须按照以下顺序排列：

- 文件中的最后一个证书必须是 CA 颁发的客户端证书或服务器证书。
- 前面的所有证书必须是根 CA 证书和所颁发证书的签名链中的所有中间 CA 证书。

导入证书链的过程分为两个步骤：

1. 在 Admin 门户中将证书链文件导入受信任证书库。此操作会将除最后一个证书之外的所有证书导入受信任证书库。
2. 使用绑定CA签名的证书操作导入证书链文件。此操作会将文件中的最后一个证书导入作为本地证书。

为思科 ISE 节点间通信安装受信任证书

当您设置部署时，在注册辅助节点之前，您必须使用适当CA证书填充PAN的证书信任列表(CTL)，这些证书用于验证辅助节点的管理员证书。对于不同的场景，填充 PAN 的 CTL 的程序也不同。

- 如果辅助节点使用 CA 签名的证书与管理门户通信，则您必须将辅助节点的 CA 签名证书、相关的中间证书（如果有）和根 CA 证书（属于签署辅助节点证书的 CA）导入到 PAN 的 CTL。
- 如果辅助节点使用自签证书与管理门户通信，则您可以将辅助节点的自签证书导入到 PAN 的 CTL。

注释

- 如果您更改了已注册辅助节点的管理员证书，则您必须获取适当 CA 证书（可用于验证辅助节点的管理员证书）并将其导入到 PAN 的 CTL。
- 当自带设备用户从一个位置移动到另一个位置时，如果您使用自签证书确保部署中客户端与PSN之间的安全通信，EAP-TLS用户身份验证会失败。对于这种必须在某些PSN之间实现的身份验证请求，您必须通过外签 CA 证书或使用外部 CA 签名的通配符证书确保客户端与 PSN 之间的通信。

确保由外部 CA 颁发的证书已经定义了基本约束且 CA 标记设置为 true。要为节点间通信安装 CA 签名证书：

步骤 1 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 160 页

步骤 2 将根证书导入受信任证书库，第 154 页

步骤 3 将 CA 签名的证书与 CSR 绑定，第 160 页

思科 ISE 中的默认受信任证书

Cisco ISE 中的受信任证书库（**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）包含默认可用的一些证书。这些证书会自动导入到库中，以满足安全要求。但是，并非必须使用所有这些证书。除非下表中另有说明，否则您可以使用您选择的证书，而不是已提供的证书。

表 22:

受信任证书名称	序列号	证书的用途	含证书的Cisco ISE 版本
Baltimore CyberTrust Root CA	02 00 00 B9	在某些地区，此证书可用作 cisco.com 使用的 CA 链中的根 CA 证书。https://s3.amazonaws.com 上托管的 ISE 2.4 终端安全评估/CP 更新 XML 文件中也使用该证书。	版本 2.4 及更高版本。
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	此证书可用作 cisco.com 使用的 CA 链的根 CA 证书。	版本 2.4 及更高版本。

受信任证书名称	序列号	证书的用途	含证书的Cisco ISE 版本
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	此证书可用作 cisco.com 和 perfigo.com 使用的 CA 链的根 CA 证书。	版本 2.4 及更高版本。
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	此证书用作 VeriSign Class 3 Secure Server CA-G3 的根 CA 证书。 在Cisco ISE 中配置 Profiler Feed Service 时，必须使用此证书。	版本 2.4 及更高版本。
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	这是一个中级 CA 证书，于 2020 年 2 月 7 日到期。您不需要更新此证书。 您可以按照以下任务删除证书。	版本 2.4 及更高版本。
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	连接到Cisco ISE 的某些Cisco设备可能使用此证书。默认情况下禁用此证书。	版本 2.4 和 2.6。
Cisco Manufacturing CA SHA2	02	此证书可在管理员身份验证、终端身份验证和部署基础设施流的 CA 链中使用。	版本 2.4 及更高版本。
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	连接到Cisco ISE 的某些Cisco设备可使用此证书。默认情况下禁用此证书。	版本 2.4 及更高版本。
Cisco Root CA M2	01	此证书可在管理员身份验证、终端身份验证和部署基础设施流的 CA 链中使用。	版本 2.4 及更高版本。
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	必须在使用 Facebook 的访客登录流中使用此证书。	版本 2.4 及更高版本。
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	必须在使用 Facebook 的访客登录流中使用此证书。	版本 2.4 及更高版本。

受信任证书名称	序列号	证书的用途	含证书的Cisco ISE 版本
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Cisco服务的受信任证书。	版本 2.4 和 2.6。
QuoVadis Root CA 2	05 09	您必须在分析器、终端安全评估和客户端调配流中使用此证书。	版本 2.4 及更高版本。
Cisco ECC Root CA	01	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6。
Cisco Licensing Root CA	01	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco RXC-R2	01	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
Cisco ECC Root CA 2099	03	此证书是Cisco ISE 中使用的Cisco信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。

从思科 ISE 删除默认受信任证书

- 请转至 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** 查看您的所有受信任证书。
- 导出要删除的证书并保存，以便在需要时再次导入。

  点击要导出的证书对应的复选框，然后点击上方菜单栏上的**导出 (Export)**。密钥链将下载到您的系统。

- 删除证书。点击要删除的证书对应的复选框，然后点击上方菜单栏上的**删除 (Delete)**。如果任何 CA 链、安全系统日志或安全 LDAP 在使用该证书，则不允许删除它。
- 进行必要的配置更改，从 CA 链、安全系统日志和证书所属的系统日志中移除证书，然后再删除它。
- 删除证书后，检查相关服务（请参阅证书用途）是否如期运行。

证书签名请求

对于证书颁发机构 (CA)，要签发签名证书，您必须创建证书签名请求 (CSR) 并将其提交给 CA。

Certificate Signing Requests 页面会提供您已创建的证书签名请求 (CSR) 的列表。要从证书颁发机构 (CA) 获得签名，您必须导出 CSR，然后将证书发送至 CA。CA 给证书签名，然后返回证书。

您可以从 Admin 门户集中管理证书。您可以为您的部署中的所有节点创建 CSR 并导出这些 CSR。然后，您应该将这些 CSR 提交给 CA，从 CA 获取 CA 签名的证书，将 CA 返回的 root 和中间 CA 证书导入受信任证书库，并且将 CA 签名的证书与 CSR 绑定。

创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构

可以生成证书签名请求 (CSR)，为部署中的节点获取 CA 签名的证书。可以为部署中的选定节点或所有节点生成 CSR。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

步骤 2 输入用于生成 CSR 的值。有关每个字段的信息，请参阅证书签名请求设置。

步骤 3 点击**生成 (Generate)** 以生成 CSR。

系统将生成 CSR。

步骤 4 点击**导出 (Export)** 以在 Notepad 中打开 CSR。

步骤 5 复制从“-----BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST-----”的所有文本。

步骤 6 将 CSR 的内容粘贴到选定 CA 的证书请求中。

步骤 7 下载签名证书。

某些 CA 可能会将签名的证书通过邮件发送给您。签名的证书采用 ZIP 文件形式，其中包含必须添加到Cisco ISE 受信任证书存储区的 CA 新颁发证书和公共签名证书。将数字签名的 CA 证书、根 CA 证书和其他中间 CA 证书（如果适用）下载到运行客户端浏览器的本地系统中。

将 CA 签名的证书与 CSR 绑定

在具有由 AC 返回的数字签名证书之后，您必须将其绑定到证书签名请求 (CSR)。您可以从管理门户为部署中的所有节点执行绑定操作。

开始之前

- 您必须具有数字签名的证书，以及由 CA 返回的相关根和中间 CA 证书。
- 将相关的根和中间 CA 证书导入受信任证书存储区（**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

选择您正为其绑定 CSR 与 CA 签名的证书的节点旁边的复选框。

步骤 2 点击**绑定 (Bind)**。

步骤 3 点击**浏览 (Browse)** 选择 CA 签名的证书。

步骤 4 为证书指定“友好名称”(Friendly Name)。

步骤 5 如果您希望Cisco ISE 验证证书扩展，请选中**验证证书扩展 (Validate Certificate Extensions)** 复选框。

如果您启用**验证证书扩展 (Validate Certificate Extensions)** 选项，且您正在导入的证书包含 CA 标志设置为 ture 的基本约束扩展，则请确保存在密钥用法扩展，且已设置 keyEncipherment 位或 akeyAgreement 位。

注释 ISE 要求 EAP-TLS 客户端证书具有数字签名密钥使用扩展。

步骤 6 选中要为其将此证书用于“使用情况”(Usage) 区域的服务。

如果您在生成 CSR 时已启用“使用情况”(Usage) 选项，则此信息会自动填充。 如果您不想在绑定证书时指定用法，请取消选中“使用情况”(Usage) 选项。您可以稍后编辑证书并指定用法。

注释 在主 PAN 上更改管理员角色证书的证书将在所有其他节点上重新启动服务

在主 PAN 上更改管理员角色证书的证书将在所有其他节点上重新启动服务。主管理节点 (PAN) 重启完成后，系统每次重新启动一个节点。

步骤 7 点击**提交 (Submit)** 以绑定 CA 签名的证书。

如果您已选择将此证书用于Cisco ISE 节点间通信，则Cisco ISE 节点上的应用服务器会重新启动。

要在其他节点上绑定 CSR 与 CA 签名的证书，请重复此流程。

下一步做什么

将根证书导入受信任证书库，第 154 页

导出证书签名请求

您可以使用此页面导出证书签名请求。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

步骤 2 选中想要导出的证书旁边的复选框，点击**导出 (Export)**。

步骤 3 点击**确定 (OK)**，将文件保存到正在运行客户端浏览器的文件系统中。

证书签名请求设置

通过Cisco ISE，只需一个请求即可从管理员门户为部署中的所有节点生成 CSR。此外，还可以选择为部署中的单个节点或多个两个节点生成 CSR。如果选择为单个节点生成 CSR，则 ISE 会自动在证书使用者的 CN= 字段中替换特定节点的完全限定域名 (FQDN)。如果选择在证书的“主体可选名称 (SAN)”(Subject Alternative Name (SAN)) 字段中包含某个条目，则除了其他 SAN 属性之外，还必须输入 ISE 节点的 FQDN。如果选择为部署中的所有节点生成 CSR，请选中“允许通配符证书”(Allow Wildcard Certificates) 复选框，然后在 SAN 字段（“DNS 名称”(DNS name)）中输入通配符 FQDN 符号，例如，*.amer.example.com。如果计划对 EAP 身份验证使用证书，请不要在 CN= 字段中输入通配符值。

通过使用通配符证书，不再需要为每个Cisco ISE 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的多个两个节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个Cisco ISE 节点分配唯一服务器证书的安全性低。

下表列出 Certificate Signing Request (CSR) 页面中的字段，可以使用此页面生成可由证书颁发机构 (CA) 签名的 CSR。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书签名请求 (Certificate Signing Request)**。

表 *23:* 证书签名请求设置

字段	使用指南
证书将用于 **(Certificate(s) will be used for)**	

字段	使用指南
	选择即将对其使用证书的服务： **思科 ISE 身份证书** • **多用途 (Multi-Use)**：用于多种服务（管理员、EAP-TLS 身份验证、pxGrid 和门户）。多用途证书同时使用客户端和服务器密钥用法。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) • **管理 (Admin)** - 用于服务器身份验证（以确保与管理员门户之间的安全通信，以及部署中 ISE 节点之间的安全通信）。签名 CA 的证书模板通常称为 Web 服务器证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **EAP 身份验证 (EAP Authentication)**：用于服务器身份验证。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) **注释** EAP-TLS 客户端证书需要使用数字签名密钥。 • **RADIUS DTLS**：用于 RADIUS DTLS 服务器身份验证。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **ISE 消息服务 (ISE Messaging Service)**：用于“经Cisco ISE 消息传递的系统日志”功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **门户 (Portal)**：用于服务器身份验证（以确保与所有 ISE Web 门户之间的

字段	使用指南
	安全通信）。签名CA的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **pxGrid** - 同时用于客户端和服务器身份验证（以确保 pxGrid 客户端与服务器之间的安全通信）。签名CA的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 注释 建议您不要将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符。如果将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符，系统会将此证书视为无效，并显示以下错误消息： `source=local type=fatal message="unsupported certificate"` **思科 ISE 证书颁发机构颁发的证书**

字段	使用指南

	• **ISE 根 CA (ISE Root CA) -**（仅适用于内部 CA 服务）用于重新生成整个内部 CA 证书链，包括主 PAN 上的根 CA 和 PSN 上的辅助 CA。
	• **ISE 中间 CA (ISE Intermediate CA)：**（仅适用于当 ISE 用作外部 PKI 的中间 CA 时的内部 CA 服务）用于在主 PAN 上生成中间 CA 证书，在 PSN 上生成从属 CA 证书。签名 CA 的证书模板通常称为辅助证书颁发机构。此模板具有以下属性：
	  • **基本约束 (Basic Constraints)：**关键、是证书颁发机构
	  • **密钥使用 (Key Usage)：**证书签名、数字签名
	  • **扩展密钥使用 (Extended Key Usage)：**OCSP 签名 (1.3.6.1.5.5.7.3.9)
	• **更新 ISE OCSP 响应方证书 (Renew ISE OCSP Responder Certificates)：**（仅适用于内部 CA 服务）用于更新整个部署的 ISE OCSP 响应方证书（不是证书签名请求）。出于安全原因，建议您每六个月更新一次 ISE OCSP 响应方证书。

允许通配符证书 (Allow Wildcard Certificates)	选中此复选框以在 CN 中和/或证书的 SAN 字段的 DNS 名称中使用通配符 (*)。如果选中此复选框，系统会自动选择部署中的所有节点。必须在最左侧的标签位置使用星号 (*) 通配符。如果使用通配符证书，我们建议您对域名空间进行分区以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，可能会导致安全问题。
为这些节点生成 CSR (Generate CSRs for these Nodes)	选中要为其生成证书的节点旁边的复选框。要为部署中的选定节点生成CSR，必须取消 Allow Wildcard Certificates 选项。
公共名称 (CN) (Common Name [CN])	默认情况下，公用名是您正为其生成 CSR 的 ISE 节点的 FQDN。$FQDN$ 表示 ISE 节点的 FQDN。当为部署中的多个节点生成 CSR 时，CSR 中的 Common Name 字段会替换为各个 ISE 节点的 FQDN。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。

字段	使用指南
主体可选名称 (SAN) (Subject Alternative Name [SAN])	“IP 地址”(IP address)、“DNS 名称”(DNS name)、“统一资源标识符”(Uniform Resource Identifier, URI) 或与证书关联的“目录名称”(Directory Name)。 • **DNS 名称 (DNS name)**：如果选择“DNS 名称”(DNS name)，请输入 ISE 节点的完全限定域名。如果已启用 Allow Wildcard Certificates 选项，请指定通配符符号（域名前的星号和句号）。例如：*.amer.example.com。 • **IP 地址 (IP address)**：将与证书关联的 ISE 节点的 IP 地址。 • **统一资源标识符 (Uniform Resource Identifier)**：您希望与证书关联的 URI。 • **目录名称 (Directory Name)**：根据 RFC 2253 定义的可区分名称 (DN) 的字符串表示。使用逗号 (,) 隔开多个 DN。对于“dnQualifier”RDN，避免使用逗号而是使用反斜杠“\”作为分隔符。例如，CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
密钥类型 (Key Type)	指定要用于创建公共密钥的算法：RSA 或 ECDSA。
密钥长度 (Key Length)	指定公共密钥的位大小。 以下选项可用于 RSA： • 512 • 1024 • 2048 • 4096 以下选项可用于 ECDSA： • 256 • 384 **注释** 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。 如果计划获取公共的 CA 签名证书，请选择 2048 或更大长度。
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。

相关主题

证书签名请求，第 160 页
创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 160 页
将 CA 签名的证书与 CSR 绑定，第 160 页

设置供门户使用的证书

由于部署中有多个策略服务节点 (PSN) 可以支持 Web 门户请求，所以Cisco ISE 需要使用唯一标识符来标识必须用于门户通信的证书。当您添加或导出指定用于门户用途的证书时，您必须定义证书组标签并将其与您的部署中各个节点上的对应证书关联。您必须将此证书组标签与对应的最终用户门户关联（访客、发起人和个人设备门户）。此证书组标签是一种唯一标识符，帮助Cisco ISE 标识与这每一个门户通信时必须使用的证书。您可以从每个节点为每个门户指定一个证书。

注释 思科 ISE 在 TCP 端口 8443（或者您为使用门户而配置的端口）上提供门户证书。

步骤 1 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 160 页。

您必须选择您已定义的证书组标签或为门户创建一个新证书组标签。例如 mydevicesportal。

步骤 2 将根证书导入受信任证书库，第 154 页。

步骤 3 将 CA 签名的证书与 CSR 绑定，第 160 页。

将默认门户证书组标签重新分配给 CA 签名的证书

默认情况下，所有Cisco ISE 门户使用自签证书。如果您要对门户使用 CA 签名的证书，您可以将默认门户证书组标签分配至 CA 签名的证书。您可以使用现有的 CA 签名证书或生成 CSR，并获取新的 CA 签名证书以供门户使用。您可以重新将任何门户组标签从一个证书分配到另一个证书。

注释 当您编辑现有的证书时，如果与证书关联的门户标签 (guest) 已被任意一个门户使用，则您无法将默认门户证书组标签或任何其他门户组标签重新分配到此证书。系统将列出使用“guest”门户标签的门户。

以下程序介绍了如何将默认门户证书组标签重新分配至 CA 签名的证书。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

将鼠标悬停在默认门户证书组标签旁边的i图标上，以查看使用此标签门户的列表。您还可以查看部署中具有已向其重新分配此标签的门户证书的 ISE 节点。

步骤 2 选中要用于门户的 CA 签名证书旁边的复选框，然后点击**编辑 (Edit)**。

请务必选择一个未被任何门户使用的 CA 签名证书。

步骤 3 在**使用情况 (Usage)** 区域，选中**门户 (Portal)** 复选框，然后选择“默认门户证书组标签”(Default Portal Certificate Group Tag)。

步骤 4 点击**保存 (Save)**。

系统将显示一条警告消息。

步骤 5 点击**是 (Yes)** 将默认门户证书组标签重新分配至 CA 签名的证书。

注册节点之前关联门户证书标签

如果您在注册新 ISE 节点之前对部署中的所有门户都使用“Default Portal Certificate Group”标签，请确保导入相关的 CA 签名证书，选择“Portal”作为服务，然后将“Default Portal Certificate Group”标签与此证书相关联。

向部署中添加新节点时，默认自签名证书与“Default Portal Certificate Group”标签相关联，并且门户配置为使用此标签。

注册新节点后，您无法更改 Certificate Group 标签关联。因此，在将节点注册到部署之前，您必须执行以下操作：

步骤 1 创建自签名证书，选择“Portal”作为服务，然后分配其他证书组标签（例如，tempportaltag）。

步骤 2 更改门户配置以使用新创建的证书组标签 (tempportaltag)。

步骤 3 编辑默认自签名证书并删除 Portal 角色。

此选项可删除与默认自签名证书的 Default Portal Certificate Group 标签关联。

步骤 4 执行以下操作之一：

选项	说明
生成 CSR	当生成 CSR 时： **1.** 选择“Portal”作为将为其使用此证书的服务并关联“Default Portal Certificate Group”标签。 **2.** 将 CSR 发送到 CA 并获取签名证书。 **3.** 导入已将您的证书签入到受信任证书库中的 CA 的根证书和任何其他中间证书。 **4.** 将 CA 签名证书与 CSR 绑定。
导入私钥和 CA 签名证书	当导入 CA 签名证书时： **1.** 选择“Portal”作为将为其使用此证书的服务并关联“Default Portal Certificate Group”标签。 **2.** 导入已将您的证书签入到受信任证书库中的 CA 的根证书和任何其他中间证书。

选项	说明
编辑现有 CA 签名证书。	当编辑现有 CA 签名证书时： 选择“Portal”作为将为其使用此证书的服务并关联“Default Portal Certificate Group”标签。

步骤 5 将 ISE 节点注册到部署
部署中的门户配置会配置到“Default Portal Certificate Group”标签，并且门户配置为在新节点上使用与“Default Portal Certificate Group”标签关联的 CA 签名证书。

用户和终端证书续订

默认情况下，Cisco ISE 拒绝来自证书已过期设备的请求。但是，您可以更改此默认行为并配置 ISE 以满足这些请求并提示用户更新证书。

如果选择允许用户更新证书，Cisco建议您配置一个授权策略规则，检查在进一步处理请求之前证书是否已续签。处理来自证书过期设备的请求可能导致潜在的安全威胁。因此，必须配置正确的授权配置文件和规则来确保贵公司的安全不受影响。

在证书到期前或到期后，有些设备支持证书续订。但是在 Windows 设备上，您只能在证书到期前续订证书。Apple iOS、Mac OSX 和 Android 设备支持在证书到期前或到期后，进行证书续订。

策略条件中用于证书续订的字典属性

Cisco ISE 证书字典包含在策略条件中用于允许用户续订证书的以下属性：

- Days to Expiry：此属性规定证书有效的天数。您可以使用此属性创建可用于授权策略的条件。此属性可采用 0 至 15 之间的值。值 0 表示证书已过期。值 1 表示证书不到 1 天就要到期。
- Is Expired：此布尔属性表示证书是否已到期。如果想要只允许在证书接近到期时而不是在证书已到期之后续订证书，请在授权策略条件中使用此属性。

证书续订的授权策略条件

您可以使用授权策略中的CertRenewalRequired简单条件（默认情况下可用）以确保在Cisco ISE进一步处理请求之前更新证书（已到期或即将到期）。

用于续订证书的 CWA 重定向

如果用户证书在证书到期前已被吊销，则Cisco ISE会检查CA发布的CRL并拒绝身份验证请求。如果被撤消的证书已过期，则CA不得在其CRL中发布此证书。在此场景中，Cisco ISE可更新被撤消的证书。要避免此问题，在更新证书之前，请确保请求重新定向到集中式 Web 身份验证 (CWA) 以进行完整的身份验证。必须创建授权配置文件才能重定向用户以进行 CWA。

将思科 ISE 配置为允许用户续订证书

您必须完成此程序中列出的任务，才能将Cisco ISE 配置为允许用户续订证书。

开始之前

在 WLC 上配置受限访问 ACL 以重定向 CWA 请求。

步骤 1 更新允许的协议配置， 第 171 页
步骤 2 为 CWA 重定向创建授权策略配置文件， 第 171 页
步骤 3 创建授权策略规则以更新证书， 第 172 页
步骤 4 在访客门户中启用 BYOD 设置， 第 173 页

更新允许的协议配置

步骤 1 选择 策略 **(Policy)** > 策略元素 **(Policy Elements)** > 结果 **(Results)** > 身份验证 **(Authentication)** > 允许的协议 **(Allowed Protocols)** > 默认网络访问 **(Default Network Access)**。

步骤 2 选中 EAP-TLS 协议以及 PEAP 和 EAP-FAST 协议的 EAP-TLS 内部方法下的 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy** 复选框。

使用 EAP-TLS 协议的请求将通过 NSP 流。

对于 PEAP 和 EAP-FAST 协议，必须手动配置Cisco AnyConnect，使Cisco ISE 处理请求。

步骤 3 点击提交 **(Submit)**。

下一步做什么

为 CWA 重定向创建授权策略配置文件， 第 171 页

为 CWA 重定向创建授权策略配置文件

开始之前

确保您已在 WLC 上配置受限访问 ACL。

步骤 1 选择 策略 **(Policy)** > 策略元素 **(Policy Elements)** > 结果 **(Results)** > 授权 **(Authorization)** > 授权配置文件 **(Authorization Profiles)**。

步骤 2 点击添加 **(Add)**。

步骤 3 为授权配置文件输入名称。例如 CertRenewal_CWA。

步骤 4 在“常见任务”(Common Tasks) 区域，选中 **Web 重定向（CWA、DRW、MDM、NSP、CPP）(Web Redirection (CWA, DRW, MDM, NSP, CPP))** 复选框。

步骤 5 从下拉列表和受限访问 ACL 选择**集中式 Web 身份验证 (Centralized Web Auth)**。

步骤 6 选中**显示证书续订消息 (Display Certificates Renewal Message)** 复选框。

URL-redirect 属性值改变并且包含证书有效的天数。

步骤 7 点击**提交 (Submit)**。

注释 如果您为思科 ISE 1.2 中的无线设备配置了以下设备注册 Web 身份验证 (DRW) 策略：

- DRW-Redirect policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-drw-redirect
- DRW-Allow policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-Permit

在升级到 ISE 1.3 或更高版本后，您必须如下更新 DRW-Allow 策略条件：

- Condition = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) and Profile = Wireless-Permit

---

下一步做什么

创建授权策略规则以更新证书，第 172 页

创建授权策略规则以更新证书

开始之前

确保您已创建集中式 Web 身份验证重定向的授权配置文件。

在以下位置启用策略集 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **策略设置 (Policy Settings)**。

步骤 1 选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略集 (Policy Sets)**。

步骤 2 点击**创建于…之上 (Create Above)**。

步骤 3 输入新规则的名称。

步骤 4 选择以下简单条件和结果：

如果 CertRenewalRequired 等于 True，则为权限选择先前创建的授权配置文件 (CertRenewal_CWA)。

步骤 5 点击**保存 (Save)**。

下一步做什么

当使用其证书已到期的设备访问公司网络时，请点击**续订 (Renew)** 重新配置设备。

在访客门户中启用 BYOD 设置

要使用户能够更新个人设备证书，必须在所选访客门户中启用 BYOD 设置。

步骤 1 依次选择**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)**。

a) 选择所选 CWA 门户并点击**编辑 (Edit)**。

步骤 2 从 BYOD 设置中，选中**允许员工在网络上使用个人设备 (Allow employees to use personal devices on the network)** 复选框。

步骤 3 点击**保存 (Save)**。

Apple iOS 设备的证书续订失败

当您使用 ISE 在 Apple iOS 设备上续订终端证书时，您可能会遇到“Profiled Failed to Install”错误消息。如果在相同策略服务节点 (PSN) 或另一个 PSN 上，与处理续订所使用的证书不同的管理员 HTTPS 证书已签名要过期或已过期的网络配置文件，则系统会显示此错误消息。

作为一个解决方案，请为部署中的所有 PSN 上的管理员 HTTPS 使用多域 SSL 证书（通常称为统一通信证书 [UCC]）或通配符证书。

证书定期检查设置

Cisco ISE 定期检查证书撤销列表 (CRL)。使用此页面，您可以对Cisco ISE 进行配置以对照自动下载的 CRL 检查正在进行的会话。您可以指定一天中的某个时间作为 CRL 或 OCSP 每天应当开始检查的时间和Cisco ISE 需要等待的时间间隔（按小时计），在此间隔之后再次对 OCSP 服务器或 CRL 进行检查。

下表列出“证书定期检查设置”(Certificate Periodic Check Settings) 窗口中的字段，可以使用该窗口来指定检查证书（OCSP 或 CRL）状态时的时间间隔。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书定期检查设置 (Certificate Periodic Check Settings)**。

表 *24:* 证书定期检查设置

字段名称	使用指南
证书检查设置	

字段名称	使用指南
“对照自动撤销的 CRL 检查正在进行的会话”(Check ongoing sessions against automatically retrieved CRL)	如果您希望Cisco ISE 对照自动下载的 CRL 检查正在进行的会话，选中此复选框。
CRL/OCSP 定期检查证书	
首先检查	指定一天中的某个时间作为 CRL 或 OCSP 每天应当开始检查的时间。输入 00:00 和 23:59 小时之间的数值
检查每	指定Cisco ISE 需要等待的时间间隔（按小时计），在此间隔之后再次对 CRL 或 OCSP 服务器进行检查。

相关主题

OCSP 服务，第 206 页
添加 OCSP 客户端配置文件，第 208 页

思科 ISE CA 服务

证书可以自签或由外部证书颁发机构 (CA) 进行数字签名。思科 ISE 内部证书颁发机构 (ISE CA) 从集中控制台为终端颁发和管理数字证书，以允许员工在公司网络上使用其个人设备。CA 签名的数字证书被视为行业标准而且更安全。主 PAN 为根 CA。策略服务节点 (PSN) 是主 PAN 的从属 CA (SCEP RA)。ISE CA 提供以下功能：

- 颁发证书：为连接您的网络的终端验证和签发证书签名请求 (CSR)。
- 密钥管理：在 PAN 和 PSN 节点上生成并安全地存储密钥和证书。
- 存储证书：存储向用户和设备颁发的证书。
- 支持在线证书状态协议 (OCSP)：提供 OCSP 响应器以检查证书的有效性。

当 CA 服务在主管理节点上禁用时，CA 服务仍被视为在辅助管理节点的 CLI 上运行。理想情况下，CA 服务应被视为禁用。此为已知的Cisco ISE 问题。

思科 ISE 证书指纹

证书指纹识别过程用于评估证书即时颁发者指纹 SHA256 以与受信任证书匹配。这将为多个 CA 实施安全机制，以支持不同的域，并允许锁定 802.1x 协议的受信任 CA。

确保在更新策略条件中的证书之前，将颁发者-指纹 SHA-256 证书添加到Cisco ISE 部署。

注释 为受信任证书配置策略后，无法删除该证书。以下消息显示在**受信任证书 (Trusted Certificates)** 窗口中的**此受信任证书由策略集引用 (This Trusted Certificate Refered by Policy Sets)** 部分中。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**：

无法删除证书，因为正在策略中使用它。要删除证书，请先修改策略条件。

要为Cisco ISE 配置证书指纹，请按照顺序执行以下步骤：

1. 创建内部用户。有关详细信息，请参阅《思科身份服务引擎管理员指南*3.0*版》“资产可视性”一章中的“添加用户”部分。
2. 添加网络设备。有关详细信息，请参阅《思科身份服务引擎管理员指南*3.0*版》“基本设置”一章中的“在Cisco ISE 中添加网络设备”部分。
3. 在外部证书中导入外部CA。有关详细信息，请参阅《思科身份服务引擎管理员指南*3.0*版》“基本设置”一章中的“导入系统证书”部分。

   您还可以使用SCEP协议导入颁发者-指纹SHA-256证书。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **外部 CA 设置 (External CA Settings)**。在显示的**添加 SCEP RA 配置文件 (Add SCEP RA Profile)** 窗口中，点击**添加 (Add)**。在**名称 (Name)** 字段中，输入证书名称。在 **URL** 字段中输入 CA 服务器 URL。点击**测试连接 (Test Connection)**。
4. 使用 SHA-256 指纹创建策略
5. 使用 SHA-256 指纹创建并映射身份验证策略
6. 创建授权策略。
7. 验证 PRRT 日志

使用 SHA-256 指纹创建策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Set)**。

步骤 2 在显示的**策略集 (Policy Set)** 窗口中，点击**设置 (Settings)**，然后从下拉列表中选择**插入新行 (insert a new row)**。

步骤 3 在**新策略名称 (New Policy Name)** 字段中输入名称。

步骤 4 输入策略的**说明**。

步骤 5 点击**条件 (Conditions)** 列下新**策略集名称 (Policy Set Name)** 旁边的**添加 (Add)** (+) 图标。

步骤 6 在显示的**条件 Studio (Condition Studio)** 窗口中，点击**点击以添加属性 (Click to Add Attribute)** 字段。

步骤 7 从**所有字典 (All dictionary)** 下拉列表中选择**网络访问-协议 (Network Access-Protocol)**（**字典-属性 (Dictionary-Attribute**）组合。

步骤 8 选择 **Equals** 运算符以构建逻辑条件。

步骤 9 从**从列表或类型中选择 (Choose from List or Type)** 下拉列表中选择 **RADIUS**。

步骤 10 点击使用 (Use)。

步骤 11 在显示的策略集 (Policy Set) 窗口中，从允许的协议/服务器序列 (Allowed Protocols/Server Sequence) 下拉列表中选择默认网络访问 (Default Network Access)。

步骤 12 点击保存 (Save)。

使用 SHA-256 指纹创建并映射身份验证策略

步骤 1 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 策略 (Policy) > 策略集 (Policy Set) > 默认值 (Default)。

步骤 2 点击身份验证策略 (Authentication Policy)。

步骤 3 点击设置图标并选择插入新行 (insert a new row)。

步骤 4 在身份验证规则名称 (Authentication Rule Name)窗口中，输入名称。

步骤 5 点击规则名称旁的添加 (Add) 图标 (+)。

步骤 6 在显示的 Condition Studio 窗口中，点击点击以添加属性 (Click to add Attributes) 字段。

步骤 7 从所有字典 (All Dictionary) 下拉列表中，选择 CERTIFICATE-Issuer- Fingerprint SHA-256 (Dictionary-Attribute) 组合。

步骤 8 选择等于 (Equals) 运算符以构建逻辑条件。

步骤 9 从从列表或类型中选择 (Choose from List or Type) 下拉列表中，选择思科制造 SHA2 指纹 sha256CA (Cisco Manufacturing CA SHA2 fingerprint sha256)。

步骤 10 点击使用 (Use)。

步骤 11 在显示的策略集 (Policy Set) 窗口中，从允许的协议/服务器序列 (Allowed Protocols/Server Sequence) 下拉列表中，选择 Preloaded_Certificate_Profile。

步骤 12 点击保存 (Save)。

创建授权策略

步骤 1 选择 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 策略 (Policy) > 策略集 (Policy Set) > 默认值 (Default)。

步骤 2 点击授权策略 (Authorization Policy)。

步骤 3 点击设置图标，然后从下拉列表中选择插入新行 (insert a new row)。

步骤 4 在授权规则名称 (Authorization Rule Name) 窗口中，输入名称。

步骤 5 点击规则名称旁的添加 (Add) 图标 (+) 图标。

步骤 6 在显示的 Condition Studio 窗口中，点击点击以添加属性 (Click to Add Attributes) 字段。

步骤 7 从所有字典 (All Dictionary) 下拉列表中，选择 CERTIFICATE-Issuer- Fingerprint SHA-256 (Dictionary-Attribute) 组合。

步骤 8 选择等于 (Equals) 运算符以构建逻辑条件。

步骤 9 从从列表或类型中选择 **(Choose from List or Type)** 下拉列表中，选择思科根 CA 2099 指纹 sha **(Cisco Root CA 2099 fingerprint sha)**。

步骤 10 点击使用 **(Use)**。

步骤 11 在显示的策略集 **(Policy Set)** 窗口中，从允许的协议/服务器序列 **(Allowed Protocols/Server Sequence)** 下拉列表中选择 **PermitAccess**。

步骤 12 点击保存 **(Save)**。

验证 PRRT 日志

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 操作 **(Operations)** > **RADIUS** > 实时日志 **(Live logs)**。

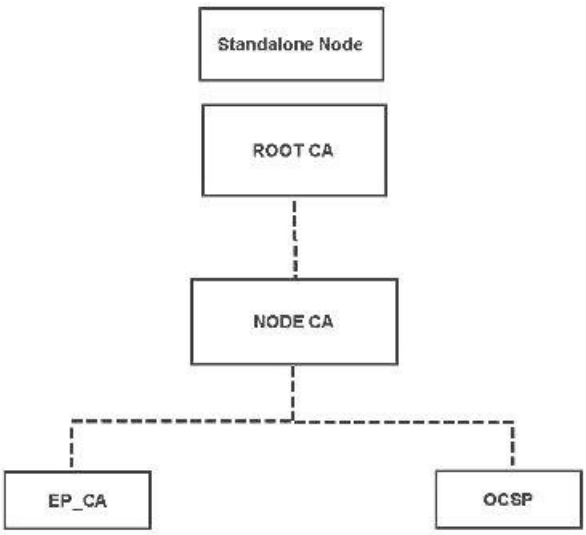
步骤 2 在显示的实时日志 **(Live Logs)** 窗口中，点击最新的日志详细信息。

步骤 3 在显示的身份验证详细信息 **(Authentication Details)** 窗口中，查看 **Issuer- Fingerprint SHA-256** 列中的 SHA-256 值，确认已成功添加并验证 **Issuer- Fingerprint SHA-256** 证书。

管理和策略服务节点上调配的 ISE CA 证书

安装Cisco ISE 节点后，系统会为它调配 CA 根证书和节点 CA 证书，以便为终端管理证书。

图 *7:* 在独立节点上调配 *ISE CA* 证书

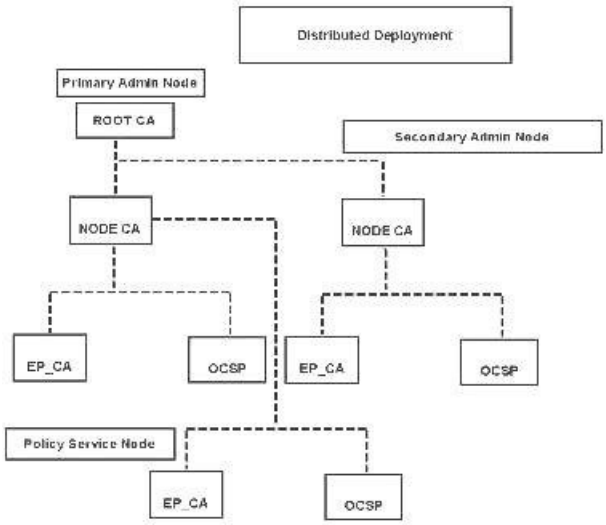


当您建立部署时，您指定为主管理节点 (PAN) 的节点将成为根 CA。PAN 具有一个根 CA 证书和一个由根 CA 签名的节点 CA 证书。

当您登记辅助管理节点至 PAN 时，会生成节点 CA 证书，并由主要管理节点的根 CA 签名。

系统将为您在 PAN 登记的所有策略服务节点 (PSN) 调配一个终端 CA 和一个由 PAN 的节点 CA 签名的 OCSP 证书。策略服务节点 (PSN) 是 PAN 的从属 CA。当您使用 ISE CA 时，PAN 上的终端 CA 颁发证书给访问您网络的终端。

图 *8:* 部署中管理和策略服务节点上调配的 ***ISE CA*** 证书



CA 与思科 ISE 实现互通性的要求

在 CA 服务器中使用Cisco ISE 时，请确保满足以下要求：

- 密钥大小应为 1024、2048 或更高。在 CA 服务器中，密钥大小使用证书模板定义。您可以使用请求方配置文件在Cisco ISE 上定义密钥大小。
- 密钥使用应允许在扩展中应用签名和加密。
- 通过 SCEP 协议使用 GetCACapabilities 时，应支持加密算法和请求散列。建议使用 RSA 和 SHA1。
- 支持在线证书状态协议 (OCSP)。虽然这在自带设备 (BYOD) 中并不会直接使用，但是可以使用能充当 OCSP 服务器的 CA 来撤销证书。

注释 Cisco ISE 支持使用企业 Java Beans 证书颁发机构 (EJBCA) 进行标准 EAP 身份验证（例如 PEAP、EAP-TLS 等）。您必须禁用 EJBCA 中的**启用终端实体配置文件限制 (Enable End Entity Profile Limitations)** 选项（在**系统 (System) > 基本配置 (Basic Configurations)** 下）才能启用对代理 SCEP 的 EJBCA 支持。

- 如果您使用企业 PKI 为 Apple iOS 设备颁发证书，请务必在 SCEP 模板中配置密钥用法并启用**密钥加密 (Key Encipherment)** 选项。

如果您使用 Microsoft CA，请在证书模板中编辑“密钥用法扩展”(Key Usage Extension)。在**加密 (Encryption)** 区域中，点击**只在密钥加密时允许密钥交换（密钥加密）(Allow Key Exchange only with Key Encryption (Key encipherment))** 单选按钮，并选中**允许对用户数据加密 (Allow encryption of user data)** 复选框。

- Cisco ISE 支持为信任证书和终端证书使用 RSASSA-PSS 算法，以进行 EAP-TLS 身份验证。查看证书时，签名算法以 1.2.840.113549.1.1.10 形式列出，而非算法名称。

注释 如果您对自带设备流量使用Cisco ISE 内部 CA，则不应使用 RSASSA-PSS 算法（由外部 CA 签名）对管理员证书签名。Cisco ISE 内部 CA 无法验证使用此算法签名的管理员证书，请求将会失败。

基于证书的身份验证对客户端证书的要求

要在Cisco ISE 上进行基于证书的身份验证，客户端证书应满足以下要求：

表 *25: RSA* 和 *ECC* 的客户端证书要求

RSA		
支持的密钥大小	1024、2048 和 4096 位	
支持的安全散列算法 (SHA)	SHA-1 和 SHA-2（包括 SHA-256）	
ECC [12]		
支持的曲线类型	P-192、P-256、P-384 和 P-521	
支持的安全散列算法 (SHA)	SHA-256	
客户端计算机操作系统和支持的曲线类型		
Windows	8 及更高版本	P-256、P-384 和 P-521
Android	4.4 及更高版本 **注释** Android 6.0 需要 2016 年 5 月的补丁以支持 ECC 证书。	所有曲线类型（Android v6.0 除外，它不支持 P-192 曲线类型）。

1 Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。
2 此思科 ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

重新生成 ISE CA 链

当您重新生成Cisco ISE CA 链时，会重新生成所有证书，包括根 CA、节点 CA 和终端 CA 证书。更改 PAN 或 PSN 的域名或主机名时，必须重新生成 ISE CA 链。从较早版本升级到版本 2.0 或更高版本时，我们建议您重新生成 ISE CA 链，以便从两个根层次结构转变为单个根层次结构。

重新生成系统证书时，无论是根 CA 证书还是中间 CA 证书，ISE 消息服务都会重新启动以加载新的证书链。在 ISE 消息服务再次可用之前，审核日志将丢失。

注释 无论何时在部署中更换思科 ISE 内部 CA，到时都必须刷新 ISE 消息服务以检索完整的证书链。

重新生成思科 ISE 内部 CA 链时，链中所有证书的**有效期自 (Valid From)** 字段将显示重新生成日期前一天的日期。

省略曲线加密证书支持

Cisco ISE CA 服务支持基于忽略曲线加密 (ECC) 算法的证书。与其他加密算法相比，ECC 提供的安全性和性能更高，即使使用更小的密钥大小也是如此。

下表比较了 ECC 和 RSA 的密钥大小以及安全强度。

ECC 密钥大小（位）	**RSA 密钥大小（位）**
160	1024
224	2048
256	3072
384	7680
521	15360

由于密钥大小较小，加密速度更快。

Cisco ISE 支持以下 ECC 曲线类型。曲线类型越高，密钥规模越大，安全性就越强。

- P-192
- P-256
- P-384
- P-521

ISE 不支持证书中 EC 部分的显式参数。如果尝试导入具有显式参数的证书，将显示以下错误：“证书验证失败: 仅支持命名的 EC 参数”(Validation of certificate failed: Only named ECParameters supported)。

对于通过自有设备流量连接的设备， Cisco ISE CA 服务支持 ECC 证书。您也可以从以证书调配门户生成 ECC 证书。

注释 下表列出了支持ECC的操作系统和版本以及支持的曲线类型。如果设备未在受支持的操作系统或受支持的版本上运行，可以使用基于 RSA 的证书代替。

操作系统 (Operating System)	支持的版本 (Supported Versions)	支持的曲线类型 (Supported Curve Types)
Windows	8 及更高版本	P-256、P-384 和 P-521
Android	4.4 及更高版本 注释 Android 6.0 需安装 2016 年 5 月补丁才能支持 ECC 证书。	所有曲线类型（Android 6.0 除外，它不支持 P-192 曲线类型）。

Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。此Cisco ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

如果使用了 Enrollment over Secure Transport (EST) 协议的自带设备流量未正常工作，请检查以下项：

- 证书服务终端子 CA 证书链完整。要检查证书链是否完整，请执行以下操作：
  1. 选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 证书颁发机构证书 (Certificate Authority Certificates)**。
  2. 选中要检查的证书旁边的复选框，然后点击**查看 (View)**。
- 确保 CA 和 EST 服务正常运行。如果服务未运行，请转至**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 内部 CA 设置 (Internal CA Settings)** 启用 CA 服务。
- 如果您已将低于 2.0 版本的 ISE 升级到Cisco ISE 2.1，请在升级后替换 ISE CA 根证书链。为此：
  1. 选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书管理 (Certificate Management) > 证书颁发签名请求 (Certificate Signing Requests)**。
  2. 点击**生成证书签名请求 (Generate Certificate Signing Requests)**。
  3. 从一个或多个**证书将用于 (Certificates will be used for)** 下拉列表中选择“ISE 根 CA”(ISE Root CA)。
  4. 点击**替换 ISE CA 根证书链 (Replace ISE Root CA Certificate chain)**。

注释 此版本的思科 ISE 不支持 EST 客户端直接根据思科 ISE 内部的 EST 服务器进行身份验证。

在 Android 或 Windows 终端上登录时，如果该请求用于基于 ECC 的证书，则 ISE 将触发 EST 流。

思科 ISE 证书颁发机构证书

“证书颁发机构 (CA) 证书”(Certificate Authority (CA) Certificates) 页面列出了与内部Cisco ISE CA 相关的所有证书。在以前的版本中，这些 CA 证书存在于受信任证书存储中，现在已移至“CA 证书”(CA Certificates) 页面。此页面按节点列出这些证书。可以展开某个节点以查看该特定节点的所有 ISE CA 证书。主要和辅助管理节点具有根 CA、节点 CA、从属 CA 和 OCSP 响应器证书。部署中的其他节点具有终端从属 CA 和 OCSP 证书。

启用Cisco ISE CA 服务时，将在所有节点上自动生成和安装这些证书。此外，在替换整个 ISE 根 CA 链时，将在所有节点上自动重新生成和安装这些证书。不需要手动干预。

Cisco ISE CA 证书遵循以下命名约定：**证书服务 <终端从属 *CA*/节点 *CA*/根 *CA/OCSP* 响应器>-**<节点主机名>**#**证书编号。

在“CA 证书”(CA Certificates) 页面中，可以编辑、导入、导出、删除和查看Cisco ISE CA 证书。

编辑思科 ISE CA 证书

在添加证书到Cisco ISE CA 证书存储区之后，可以采用编辑设置对其进行进一步编辑。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 。

步骤 3 选中要编辑的证书旁边的复选框，然后点击**编辑 (Edit)**。

步骤 4 根据需要修改可编辑字段。有关字段的说明，请参阅编辑证书设置。

步骤 5 点击**保存 (Save)** 以保存对证书库所做的更改。

导出思科 ISE CA 证书

要导出Cisco ISE 根 CA 和节点 CA 证书：

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 。

步骤 3 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

步骤 4 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。

导入思科 ISE CA 证书

如果终端尝试使用来自其他部署的Cisco ISE 颁发的证书对您的网络进行身份验证，您必须将来自该部署的Cisco ISE 根 CA 证书、节点 CA 证书和终端从属 CA 证书导入到Cisco ISE 受信任证书存储区。

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 将 ISE 根 CA 证书、节点 CA 证书和终端从属 CA 证书从终端证书签名的部署中导出，并将其存储在浏览器运行所在的计算机的文件系统。

步骤 1 登录到终端正从其获得身份认证的部署的管理门员户。

步骤 2 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 3

步骤 4 点击**导入 (Import)**。

步骤 5 如有必要，配置这些字段值。有关详细信息，请参阅受信任证书导入设置。

如果启用基于证书的客户端身份验证，则Cisco ISE 将重新启动您的部署中每个节点上的应用服务器，从 PAN 上的应用服务器开始，然后依次是其他各个节点。

证书模板

证书模板包含证书颁发机构 (CA) 基于该模板颁发的所有证书通用的属性。证书模板定义了主题、主题备选名称 (SAN)、密钥类型、密钥大小、必须使用的 SCEP RA 配置文件、证书的有效期以及扩展密钥用法 (EKU)（指定必须将证书用于客户端身份验证、服务器身份验证，还是用于两者）。内部 Cisco ISE CA (ISE CA) 使用证书模板颁发基于该模板的证书。

Cisco ISE 为 ISE CA 提供了以下默认证书模板。如果需要，您可以创建其他证书模板。默认证书模板如下：

- CA_SERVICE_Certificate_Template - 用于使用Cisco ISE 作为证书颁发机构的其他网络服务。例如，在配置给 ASA VPN 用户颁发证书的 ISE 时使用此证书模板。您仅可在此证书模板中修改有效期。
- EAP_Authentication_Certificate_Template - 用于 EAP 身份验证。
- pxGrid_Certificate_Template - 用于从证书调配门户生成证书时的 pxGrid 控制器。

证书模板扩展名

Cisco ISE 内部 CA 包含一个扩展名，表示用于创建终端证书的证书模板。由内部 CA 颁发的所有终端证书都包含证书模板扩展名。此扩展名表示用于创建该终端证书的证书模板。扩展 ID 为 1.3.6.1.4.1.9.21.2.5。您可以在授权策略条件中使用 CERTIFICATE: Template Name 属性，并根据评估结果分配相应的访问权限。

在授权策略条件中使用证书模板

您可以在授权策略规则中使用证书模板名称扩展名。

步骤 1 选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开“默认策略集”(Default policy set) 以查看授权策略规则。

步骤 2 添加新规则或编辑现有规则。此示例对编辑 Compliant_Device_Access 规则描述如下：

a) 编辑 Compliant_Device_Access 规则

b) 选择**添加属性/值 (Add Attribute/Value)**。

c) 从字典选择**证书：模板名称 (CERTIFICATE: Template Name)** 属性和**等于 (Equals)** 运算符。

d) 输入证书模板名称值。例如，EAP_Authentication_Certificate_Template。

步骤 3 点击**保存 (Save)**。

为 pxGrid 控制器部署思科 ISE CA 证书

Cisco ISE CA 为 pxGrid 控制器提供一个证书模板，用于从证书调配门户生成证书。

开始之前

为 pxGrid 客户端生成证书签名请求 (CSR) 并复制 CSR 的内容到剪贴板。

步骤 1 创建网络访问用户帐户（通过“管理”(Administration) >“身份管理” (Identity Management) >“身份”(Identities) >“用户” (Users) >“添加”(Add)）。

记录用户分配到的用户组。

步骤 2 修改证书调配门户设置（通过“管理”(Administration) >“设备门户管理” (Device Portal Management) >“证书调配”(Certificate Provisioning)）。

a) 选择证书调配门户，然后点击**编辑 (Edit)**。

b) 点击**门户设置 (Portal Settings)** 下拉列表。从“配置授权组可用列表”(Configure authorized groups Available list)，选择网络访问用户所属的用户组并将其移至选定的列表。

c) 点击**证书调配门户设置 (Certificate Provisioning Portal Settings)** 下拉列表。选择 pxGrid_Certificate_Template。有关详细信息，请参阅证书调配门户的门户设置。

d) 保存门户设置。

步骤 3 启动“证书调配门户”(Certificate Provisioning Portal)。点击“门户测试 URL”(Portal test URL) 链接。

a) 使用在步骤 1 中创建的用户帐户登录证书调配门户。

b) 接受 AUP，然后点击**继续 (Continue)**。
c) 从**我想 (I want to)**下拉列表中，选择**生成单个证书（通过证书签名请求）(Generate a single certificate (with certificate signing request))**。
d) 在“证书签名请求详细信息”(Certificate Signing Request Details) 字段，从剪贴板粘贴 CSR 的内容。
e) 从**证书下载格式 (Certificate Download Format)** 下拉列表中，选择 **PKCS8 格式 (PKCS8 format)**。

注释 如果您选择PKCS12格式，则必须将单个证书文件转换为单独的证书和密钥文件。证书和密钥文件必须为二进制 DER 编码的或 PEM 格式，才能将其导入Cisco ISE。

f) 从**选择证书模板 (Choose Certificate Template)** 下拉列表中，选择 **pxGrid_Certificate_Template**。
g) 输入证书密码。
h) 点击**生成 (Generate)**。

系统将生成证书。

i) 导出证书

系统会将证书连同证书链一起导出。

步骤 4 将Cisco ISE CA 链导入至 pxGrid 客户端中受信任的证书存储库中。

简单证书注册协议配置文件

为了帮助为用户可在网络上注册的各类移动设备启用证书调配功能，Cisco ISE 允许您配置一个或多个简单证书注册协议 (SCEP) 证书颁发机构 (CA) 配置文件（称为Cisco ISE 外部 CA 设置），从而使Cisco ISE指向多个CA位置。允许多个配置文件的优点在于，可帮助确保高可用性并在您指定的CA位置执行负载均衡。如果对特定的 SCEP CA 请求连续三次未获得应答，则Cisco ISE 会声明该特定服务器不可用，并会自动移至下一个具有已知最低负载和最少响应次数的CA，然后即会开始进行定期轮询直至服务器恢复联机。

关于如何设置 Microsoft SCEP 服务器与Cisco ISE 互操作的详细信息，请参阅

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf。

已颁发的证书

管理门户列出了内部 ISE CA 颁发给终端的所有证书（“管理”(Administration) > “系统”(System) > “证书”(Certificates) > “终端证书”(Endpoint Certificates)）。已颁发的证书 (Issued Certificates) 页面提供证书状态概览。如果证书已被吊销，可以将鼠标悬停在 Status 列上找出吊销原因。您可以将鼠标悬停在“证书模板”(Certificate Template) 列上查看更多详细信息，如证书的密钥类型、密钥大小或曲线类型、主题、主题备选名称 (SAN) 和有效期。可以点击终端证书来查看证书。

“终端证书”(Endpoint Certificates) 页面列有 ISE CA 颁发的所有证书（通过自带设备流程自动调配证书并从证书调配门户获得证书）。您可以在此页面管理这些证书。

例如，如果要查看颁发给 user7 的证书，请在出现在 Friendly Name 字段下方的文本框中输入 user7。系统会显示Cisco ISE 颁发给此用户的所有证书。从文本框中删除搜索条件可取消筛选。还可以根据各种搜索条件，使用 Advanced Filter 选项查看记录。

此 Endpoint Certificates 页面还为您提供用于在必要时撤销终端证书的选项。

Certificate Management Overview 页面显示部署中每个 PSN 节点颁发的终端证书的总数。还可以查看每个节点的被吊销证书的总数，以及已失败的证书的总数。可以根据任意属性筛选此页面上的数据。

颁发及撤销的证书

下表介绍颁发及撤销的证书概述 页面中的字段。您的部署中的PSN节点会向终端发出证书。此页面向您提供关于您的部署中每个PSN节点发出的终端证书的信息。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **概述 (Overview)**。

表 *26:* 颁发及撤销的证书

字段	使用指南
Node name	发出证书的策略服务节点 (PSN) 的名称。
颁发的证书 (Certificates Issued)	PSN 节点发出的终端证书的数量。
撤销的证书 (Certificates Revoked)	已吊销的证书的数量（已由 PSN 节点发出的证书）。
证书请求 (Certificates Requests)	PSN 节点处理的基于证书的身份验证请求数量。
失败的证书 (Certificates Failed)	PSN 节点处理的失败身份验证请求数量。

相关主题

已颁发的证书，第 185 页
用户和终端证书续订，第 170 页
配置思科 ISE 以使用证书对个人设备进行身份验证，第 189 页
将思科 ISE 配置为允许用户续订证书，第 171 页
吊销终端证书，第 206 页

思科 ISE CA 证书和密钥的备份与恢复

必须安全地备份Cisco ISE CA 证书和密钥，以在出现 PAN 故障以及您要将辅助管理节点升级作为外部 PKI 的根 CA 或中间 CA 的情况下在辅助管理节点上恢复这些证书和密钥。Cisco ISE 配置备份不包括 CA 证书和密钥。您应使用命令行界面 (CLI) 将 CA 证书和密钥导出至存储库，然后再导入。**application configure ise** 命令现在包含导出和导入选项，用于备份和恢复 CA 证书和密钥。

来自受信任证书库的以下证书存储于辅助管理节点上：

- Cisco ISE Root CA 证书
- Cisco ISE 子 CA 证书
- Cisco ISE 终端 RA 证书
- Cisco ISE OCSP 响应器证书

在以下情况下，您必须备份和恢复Cisco ISE CA 证书和密钥：

- 部署中有辅助管理节点
- 替换整个Cisco ISE CA 根链
- 配置Cisco ISE 根 CA 作为外部 PKI 的从属 CA
- 从 1.2 版本升级到更高版本
- 从配置备份恢复数据。在这种情况下，必须首先重新生成Cisco ISE CA 根链，然后备份和恢复 ISE CA 证书和密钥。

注释 无论何时在部署中更换思科 ISE 内部 CA，到时都必须刷新 ISE 消息服务以检索完整的证书链。

导出思科 ISE CA 证书和密钥

您必须从 PAN 导出 CA 证书和密钥，才能将其导入到辅助管理节点。通过此选项，辅助管理节点可以在 PAN 关闭和您将辅助管理节点升级到 PAN 时为终端颁发和管理证书。

开始之前

确保您已经创建了用于存储 CA 证书和密钥的存储库。

步骤 1 从Cisco ISE CLI 输入 **application configure ise** 命令。

步骤 2 输入 7 以导出证书和密钥。

步骤 3 输入存储库名称。

步骤 4 输入加密密钥。

系统将显示成功消息和已导出的证书列表，以及主题、颁发机构和序列号。

示例：

```
以下 4 个 CA 密钥对导出到了存储库“sftp”，后者位于“ise_ca_key_pairs_of_ise-vm1”：Subject:CN=Cisco ISE
Self-Signed CA of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x621867df-568341cd-944cc77f-c9820765 Subject:CN=Cisco ISE Endpoint CA of ise-vm1 Issuer:CN=Cisco
 ISE Self-Signed CA of ise-vm1 Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa Subject:CN=Cisco ISE Endpoint
 RA of ise-vm1 Issuer:CN=Cisco ISE Endpoint CA of ise-vm1 Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2
 Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
 Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1 ISE CA 密钥导出成功完成
```

导入思科 ISE CA 证书和密钥

在注册辅助管理节点之后，您必须从 PAN 导出 CA 证书和密钥并将它们导入到辅助管理节点。

步骤 1 从Cisco ISE CLI 中输入 **application configure ise** 命令。

步骤 2 输入 8 以导入 CA 证书和密钥。

步骤 3 输入存储库名称。

步骤 4 输入要导入的文件的名称。文件名应采用以下格式 **ise_ca_key_pairs_of_<vm hostname>**。

步骤 5 输入加密密钥以解密文件。

系统将显示一条成功消息。

示例：

```
导入了以下 4 个 CA 密钥对 (The following 4 CA key pairs were imported): Subject:CN=Cisco ISE Self-Signed CA
 of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1 Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4
 Subject:CN=Cisco ISE Endpoint CA of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56 Subject:CN=Cisco ISE Endpoint RA of ise-vm1 Issuer:CN=Cisco
 ISE Endpoint CA of ise-vm1 Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca Subject:CN=Cisco ISE OCSP
Responder Certificate of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5 正在停止 ISE 证书颁发机构服务...(Stopping ISE Certificate
Authority Service...) 正在启动 ISE 证书颁发机构服务...(Starting ISE Certificate Authority Service...) ISE
CA 密钥导入成功 (ISE CA keys import completed successfully)
```

在主 PAN 和 PSN 上生成根 CA 和从属 CA

设置部署时，Cisco ISE 会在主 PAN 上为思科 ISE CA 服务生成根 CA，在策略服务节点 (PSN) 上生成从属 CA 证书。但是，当更改 PAN 或 PSN 的域名或主机名时，必须分别在主 PAN 上重新生成根 CA，在 PSN 上重新生成从属 CA。

如果您要在 PSN 上更改主机名，而不是分别在 PAN 和 PSN 上重新生成根 CA 和从属 CA，则您可以在更改主机名之前对 PSN 取消注册，然后重新注册。新的辅助证书会在 PSN 上自动调配。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**

步骤 2 点击**生成证书签名请求 (Generate Certificate Signing Requests)**。

步骤 3 从 **Certificate(s) will be used for** 下拉列表中选择 ISE 根 CA。

步骤 4 点击 **Replace ISE Root CA Certificate chain**。

系统会为部署中的所有节点生成根 CA 和从属 CA 证书。

下一步做什么

如果部署中具有辅助 PAN，请从主 PAN 获取Cisco ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助PAN可以在主PAN故障时用作根CA，您可将辅助PAN升级为主PAN。

将思科 ISE 根 CA 配置为外部 PKI 的从属 CA

如果您希望主 PAN 上的根 CA 作为外部 PKI 的从属 CA，则生成 ISE 中间 CA 证书签名请求，将其发送到外部 CA，获取根 CA 证书和 CA 签名的证书，将根 CA 证书导入受信任证书存储区，将 CA 签名的证书绑定到 CSR。在这种情况下，外部 CA 为根 CA，主 PAN 为外部 CA 的从属 CA，PSN 为 主 PAN 的从属 CA。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

步骤 2 点击 **Generate Certificate Signing Requests (CSR)**。

步骤 3 从 **Certificate(s) will be used for** 下拉列表选择 ISE 中级 CA。

步骤 4 点击**生成 (Generate)**。

步骤 5 导出 CSR，将其发送到外部 CA，获取 CA 签名的证书。

步骤 6 将根 CA 证书从外部 CA 导入受信任证书库。

步骤 7 将 CA 签名证书与 CSR 绑定。

下一步做什么

如果部署中具有辅助 PAN，请从主 PAN 获取Cisco ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。然后，服务器和根证书会在辅助 PAN 中自动复制。这可确保在管理节点发生故障切换时，辅助 PAN 可用作外部 PKI 的从属 CA。

配置思科 ISE 以使用证书对个人设备进行身份验证

可以配置Cisco ISE，为连接到网络的终端（个人设备）发送和管理证书。可以使用内部Cisco ISE 证书授权 (CA) 服务签署来自终端的证书签名请求 (CSR)，或者将 CSR 转发到外部 CA。

开始之前

- 从主 PAN 获取Cisco ISE CA 证书和密钥备份，将其保存在安全位置，用于灾难恢复目的。
- 如果部署中具有辅助 PAN，请从主 PAN 备份Cisco ISE CA 证书和密钥，然后在辅助 PAN 上恢复备份。

步骤 1 将用户添加到 Employee 用户组 ， 第 190 页

可以将用户添加到内部身份库或外部身份库，例如 Active Directory。

步骤 2 为基于 TLS 的身份验证创建证书身份验证配置文件 ， 第 190 页

步骤 3 为基于 TLS 的身份验证创建身份源序列，第 191 页

步骤 4 创建客户端调配策略。

a) 配置证书颁发机构设置，第 191 页
b) 创建 CA 模板，第 193 页
c) 创建要用于客户端调配策略的本地请求方配置文件，第 195 页
d) 从思科站点下载适用于 Windows 和 Mac OS X 操作系统的代理资源，第 196 页
e) 为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则，第 196 页

步骤 5 为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则，第 197 页

步骤 6 为基于 TLS 的身份验证配置授权策略规则。

a) 为集中式 Web 身份验证和请求方调配流程创建授权配置文件，第 197 页
b) 创建授权策略规则，第 198 页

当您使用基于 ECDHE-RSA 的证书时，从您的个人设备连接无线 SSID 期间，系统将提示您再次输入密码。

将用户添加到 Employee 用户组

以下程序介绍如何在Cisco ISE 身份库中将用户添加到 Employee 用户组。如果使用外部身份库，请确保具有可向其添加用户的 Employee 用户组。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入用户详细信息。

步骤 4 在**密码 (Passwords)** 部分，选择**登录密码 (Login Password)** 和 TACACS+ **启用密码 (Enable Password)** 设置网络设备的访问级别。

步骤 5 从 User Group 下拉列表中选择 Employee。

属于 Employee 用户组的所有用户共享同一组权限。

步骤 6 点击**提交 (Submit)**。

下一步做什么

为基于 TLS 的身份验证创建证书身份验证配置文件，第 190 页

为基于 TLS 的身份验证创建证书身份验证配置文件

要使用证书对连接到您网络的终端进行身份验证，您必须在Cisco ISE 中定义证书身份验证配置文件或编辑默认的 Preloaded_Certificate_Profile。证书身份验证配置文件包括应用作主体用户名的证书字段。例如，如果用户名在通用名称字段中，则您可以使用主体用户名定义证书身份验证配置文件，即主题 - 通用名称，该名称可对身份库进行验证。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > 证书验证配置文件 (Certificate Authentication Profile)。

步骤 2 输入证书身份验证配置文件的名称。例如，CAP。

步骤 3 选择主题 - 通用名称作为 **Principal Username X509 Attribute**。

步骤 4 点击保存 (Save)。

下一步做什么

为基于 TLS 的身份验证创建身份源序列 ， 第 191 页

为基于 TLS 的身份验证创建身份源序列

在创建证书身份验证配置文件后，必须将其添加到身份源序列，以便Cisco ISE 可从证书获取属性并将其与您在身份源序列中定义的身份源进行匹配。

开始之前

确保您已完成以下任务：

- 向 Employee 用户组添加用户。
- 为基于证书的身份验证创建证书身份验证配置文件。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)。

步骤 2 点击添加 (Add)。

步骤 3 输入身份源序列的名称。例如 Dot1X。

步骤 4 选中选择证书身份验证配置文件 (Select Certificate Authentication Profile) 复选框，然后选择之前创建的证书身份验证配置文件，即 CAP。

步骤 5 将包含您的用户信息的身份源移至 Authentication Search List 区域的 **Selected** 列表框。

您可以添加更多身份源，Cisco ISE 会按照顺序搜索这些数据存储区，直到找到匹配项。

步骤 6 点击 **Treat as if the user was not found and proceed to the next store in the sequence** 单选按钮。

步骤 7 点击提交 (Submit)。

下一步做什么

配置证书颁发机构设置 ， 第 191 页

配置证书颁发机构设置

如果您计划将外部 CA 用于为证书签名请求 (CSR) 提供签名，则必须配置外部 CA 设置。在以前版本的Cisco ISE 中，外部 CA 设置称为 SCEP RA 配置文件。如果您使用的是Cisco ISE CA，则不必明

确配置 CA 设置。您可以在 Administration > System > Certificates > Internal CA Settings 下查看内部 CA 设置。

用户的设备收到已验证的证书后，会按照下表中的说明驻留于设备上。

表 *27*: 设备证书位置

设备	证书存储位置	访问方法
iPhone/iPad	标准证书库	Settings > General > Profile
Android	加密证书库	不对最终用户显示。 **注释** 可以使用“设置”(Settings) > “位置和安全”(Location & Security) > “清除存储”(Clear Storage) 来删除证书。
Windows	标准证书库	从 **/cmd** 提示符启动 mmc.exe 或在 snap-in 证书中进行查看。
Mac	标准证书库	Application > Utilities > Keychain Access

开始之前

如果您计划将外部证书颁发机构用于为证书签名请求 (CSR) 提供签名，您必须拥有外部 CA 的 URL。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **外部 CA 设置 (External CA Settings)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为外部 CA 设置输入名称。例如 EXTERNAL_SCEP。

步骤 4 在 URL 文本框中输入外部 CA 服务器 URL。

点击 **Test Connection**，检查是否可以访问外部 CA。点击 + 按钮以添加更多 CA 服务器 URL。

步骤 5 点击**提交 (Submit)**。

下一步做什么

创建 CA 模板，第 193 页

创建 CA 模板

证书模板定义必须（用于内部或外部CA）的SCEP RA配置文件、密钥类型、密钥大小或曲线类型、使用者、使用者备选名称(SAN)、证书有效期和扩展密钥用法。此示例假定您即将使用内部Cisco ISE CA。对于外部 CA 模板，有效期由外部 CA 确定，而您无法指定有效期。

您可以创建新的 CA 模板或编辑默认证书模板 EAP_Authentication_Certificate_Template。

默认情况下，Cisco ISE 中的以下 CA 模板可用：

- CA_SERVICE_Certificate_Template - 用于使用 ISE CA 的其他网络服务。例如，在配置给 ASA VPN 用户颁发证书的 ISE 时使用此证书模板。
- EAP_Authentication_Certificate_Template - 用于 EAP 身份验证。
- pxGrid_Certificate_Template - 用于从证书调配门户生成证书时的 pxGrid 控制器。

注释 使用 ECC 密钥类型的证书模板仅可用于内部思科 ISE CA。

开始之前

确保您已配置 CA 设置。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **CA 服务 (CA Service)** > **内部 CA 证书模版 (Internal CA Certificate Template)**。

步骤 2 输入内部 CA 模板的名称。例如 Internal_CA_Template。

步骤 3 （可选）输入“组织单位”(Organizational Unit)、“企业”(Organization)、“城市”(City)、“省”(State) 和“国家/地区”(Country) 字段的值。

在证书模板字段（“组织单位”[Organizational Unit]、“企业”[Organization]、“城市”[City]、“省”[State] 和“国家/地区”[Country]）中不支持 UTF-8 字符。如果在证书模板中使用 UTF-8 字符，则证书调配将会失败。

生成证书的内部用户的用户名用作证书的通用名称。Cisco ISE 内部 CA 的“通用名称”(Common Name) 字段不支持“+”或“*”字符。确保用户名不包含特殊字符“+”或“*”。

步骤 4 指定使用者备选名称 (SAN) 和证书的有效期。

步骤 5 指定密钥类型。选择 RSA 或 ECC。

下表列出了支持 ECC 和曲线类型的操作系统和版本。如果设备未在受支持的操作系统或受支持的版本上运行，可以使用基于 RSA 的证书代替。

操作系统	支持的版本	支持的曲线类型
Windows	8 及更高版本	P-256、P-384 和 P-521

操作系统	支持的版本	支持的曲线类型
Android	4.4 和更高版本 注释 Android 6.0 需要 2016 年 5 月的补丁才能支持 ECC 证书。	所有曲线类型（Android 6.0 除外，它不支持 P-192 曲线类型）。

Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。此Cisco ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

如果您网络中的设备运行的操作系统不支持（Windows 7、Mac OS X 或 Apple iOS），我们建议您选择 RSA 为密钥类型。

步骤 6 （选择 RSA 密钥类型时适用）指定密钥大小。您必须选择 1024 或更高的密钥大小。

步骤 7 （仅在选择 ECC 密钥类型时适用）指定曲线类型。默认值为 P-384。

步骤 8 选择 ISE 内部 CA 作为 SCEP RA 配置文件。

步骤 9 输入有效期（天）。默认值为 730 天。有效范围为 1 到 730。

步骤 10 指定扩展密钥用法。如果要将证书用于客户端身份验证，选中**客户端验证 (Client Authentication)** 复选框。如果要将证书用于服务器身份验证，选中**服务器身份验证 (Server Authentication)** 复选框。

步骤 11 点击**提交 (Submit)**。

系统将创建内部 CA 证书模板并供内部客户端调配策略使用。

下一步做什么

创建要用于客户端调配策略的本地请求方配置文件，第 195 页

内部 CA 设置

下表介绍“内部 CA 设置 (Internal CA Settings)”窗口中的字段。您可以查看内部 CA 设置和从该页面禁用内部 CA 服务。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **内部 CA 设置 (Internal CA Settings)**。

表 *28*: 内部 *CA* 设置

字段名称	使用指南
禁用证书权限 (Disable Certificate Authority)	点击此按钮以禁用内部 CA 服务。
主机名 (Host Name)	运行 CA 服务的Cisco ISE 节点的主机名。
相关角色 (Personas)	在运行 CA 服务的节点上启用的Cisco ISE 节点角色。例如管理角色、策略服务角色等。

字段名称	使用指南
角色 [Role(s)]	运行 CA 服务的Cisco ISE 节点承担的职责。例如，独立、主要或辅助职责。
CA、EST 和 OCSP 响应方状态 (CA, EST & OCSP Responder Status)	启用或禁用
OCSP 响应者 URL (OCSP Responder URL)	Cisco ISE 节点用于访问 OCSP 服务器的 URL。
SCEP URL	Cisco ISE 节点用来访问 OCSP 服务器的 URL。

相关主题

思科 ISE CA 服务 ， 第 174 页
配置思科 ISE 以使用证书对个人设备进行身份验证 ， 第 189 页

创建要用于客户端调配策略的本地请求方配置文件

可以创建本地请求方配置文件，使用户能够将个人设备带入公司网络。Cisco ISE 对不同的操作系统使用不同的策略规则。每个客户端调配策略规则都包含一个本地请求方配置文件，其指定针对哪个操作系统而使用哪个调配向导。

开始之前

- 在Cisco ISE 中配置 CA 证书模板。
- 打开 TCP 端口 8905 和 UDP 端口 8905 以启用客户端代理和请求方调配向导的安装。有关端口用法的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“Cisco ISE 设备端口参考”附录。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 选择 **添加 (Add)** > **本地请求方配置文件 (Native Supplicant Profile)**。

步骤 3 输入本地请求方配置文件的名称。例如 EAP_TLS_INTERNAL。

步骤 4 从**操作系统 (Operating System)** 下拉列表中选择“全部”(ALL)。

注释 MAC OS 版本 10.10 用户需手动连接到双 SSID PEAP 流的调配 SSID。

步骤 5 选中**有线 (Wired)** 或**无线 (Wireless)** 复选框。

步骤 6 从**允许协议 (Allowed Protocol)** 下拉列表中选择 TLS。

步骤 7 选择之前创建的 CA 证书模板。

步骤 8 点击**提交 (Submit)**。

下一步做什么

从思科站点下载适用于 Windows 和 Mac OS X 操作系统的代理资源， 第 196 页

从思科站点下载适用于 Windows 和 Mac OS X 操作系统的代理资源

对于 Windows 和 Mac OS X 操作系统，您必须从Cisco站点下载远程资源。

开始之前

验证是否已为您的网络正确配置代理设置，确保能够访问相应的远程位置以将客户端调配资源下载至Cisco ISE。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **资源 (Resources)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 选择 **添加 (Add)** > **思科站点的代理资源 (Agent resources from Cisco site)**。

步骤 3 选中 **Windows** 和 **MAC OS X** 包旁边的复选框。确保包含最新的版本。

步骤 4 点击**保存 (Save)**。

下一步做什么

为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则， 第 196 页

为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则

客户端调配资源策略可确定哪些用户会在登录和用户会话启动后从Cisco ISE 收到什么版本的资源（代理、代理合规性模块和代理自定义包/配置文件）。

当您下载代理合规性模块时，它始终会覆盖系统中可用的现有模块（如果有）。

要允许员工携带 iOS、Android、MACOSX 设备，必须在“客户端调配策略”(Client Provisioning Policy) 页面为上述每一种设备创建策略规则。

开始之前

您必须已经配置了所需的本地请求方配置文件并已从 Client Provisioning Policy 页面下载了所需的代理。

步骤 1 选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 为 Apple iOS、Android 和 MACOSX 设备创建客户端调配策略规则。

步骤 3 点击保存 (Save)。

下一步做什么

为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则，第 197 页

为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则

此任务显示如何为基于 TLS 的身份验证更新 Dot1X 身份验证策略规则。

开始之前

确保您已为基于 TLS 的身份验证创建证书身份验证配置文件。

步骤 1 选择 策略 (Policy) > 策略集 (Policy Sets)。

步骤 2 点击视图 (View) 列中的箭头图标 ›，打开集合视图屏幕，查看、管理和更新身份验证策略。

默认基于规则的身份验证策略包括一条适用于 Dot1X 身份验证的规则。

步骤 3 要编辑 Dot1X 身份验证策略规则的条件，请将鼠标悬停在条件 (Conditions) 列中的单元格上，然后点击 。Conditions Studio 将打开。

步骤 4 从 Dot1X 策略规则的操作 (Actions) 列中，点击齿轮图标，然后从下拉菜单中，根据需要通过选择任何插入或重复选项来插入新策略集。
“策略集”(Policy Sets) 表中会显示一个新行。

步骤 5 为规则输入名称。例如，eap-tls。

步骤 6 在条件 (Conditions) 列中，点击 (+) 符号。

步骤 7 在 Conditions Studio 页面中创建所需的条件。在编辑器 (Editor) 部分中，点击文本框点击以添加属性 (Click To Add an Attribute)，选择所需的词典和属性（例如，Network Access:UserName Equals User1）。

您可以将库条件拖放到点击以添加属性 (Click To Add an Attribute) 文本框。

步骤 8 点击使用 (Use)。

步骤 9 保留默认规则。

步骤 10 点击保存 (Save)。

下一步做什么

为集中式 Web 身份验证和请求方调配流程创建授权配置文件，第 197 页

为集中式 Web 身份验证和请求方调配流程创建授权配置文件

必须定义授权配置文件以确定在基于证书的身份验证成功后必须授予用户的访问权限。

开始之前

确保已在无线 LAN 控制器 (WLC) 上配置所需的访问控制列表 (ACL)。有关如何在 WLC 上创建 ACL 的信息，请参阅《*TrustSec* 操作指南：将证书用于差异化访问》。

本示例假定已在 WLC 上创建以下 ACL。

- NSP-ACL - 适用于本地请求方调配
- BLACKHOLE - 适用于限制对列入阻止列表的设备的访问
- NSP-ACL-Google - 适用于调配 Android 设备

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 点击**添加 (Add)** 以创建新的授权配置文件。

步骤 3 为授权配置文件输入名称。

步骤 4 从 **Access Type** 下拉列表中选择 ACCESS_ACCEPT。

步骤 5 点击**添加 (Add)**，为集中式 Web 身份验证、适用于 Google Play 的集中式 Web 身份验证、本地请求方调配和适用于 Google 的本地请求方调配添加授权配置文件。

步骤 6 点击**保存 (Save)**。

下一步做什么

创建授权策略规则，第 198 页

创建授权策略规则

Cisco ISE 评估授权策略规则并授予对基于策略规则中指定的授权配置文件的网络资源的用户访问权限。

开始之前

确保已创建所需的授权配置文件。

步骤 1 选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开策略集以查看授权策略规则。

步骤 2 请在默认规则之上插入其他策略规则。

步骤 3 点击**保存 (Save)**。

CA 服务策略参考

本节提供您在启用Cisco ISE CA 服务之前必须创建的授权和客户端调配策略规则的参考信息。

证书服务的客户端调配策略规则

本节将列出在使用Cisco ISE 证书服务时，您必须创建的客户端调配策略规则。下表将提供详细信息。

规则名称	身份组	操作系统	其他条件	结果
iOS	任意	Apple iOS 全部	条件	EAP_TLS_INTERNAL（较早创建的本地请求方配置文件）。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。
Android	任意	Android	条件	EAP_TLS_INTERNAL（较早创建的本地请求方配置文件）。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。
MACOSX	任意	MACOSX	条件	在本地请求方配置下，指定以下项目： 1. 配置向导：选择您从Cisco网站上下载的MACOSX 请求方向导。 2. 向导配置文件：选择您较早创建的EAP_TLS_INTERNAL本地请求方配置文件。如要使用外部CA，请选择您已经为外部 CA 创建的本地请求方配置文件。

证书服务的授权配置文件

本节列出您为在Cisco ISE 中启用基于证书的身份验证而必须创建的授权配置文件。您必须已在无线 LAN 控制器 (WLC) 上创建 ACL（NSP-ACL 和 NSP-ACL-Google）。

- CWA - 此配置文件用于完成集中式 Web 身份验证流程的设备。选中 **Web Authentication** 复选框，从下拉列表中选择 Centralized，然后在 ACL 文本字段中输入 NSP-ACL。
- CWA_GooglePlay - 此配置文件用于完成集中式 Web 身份验证流程的 Android 设备。此配置文件使 Android 设备能够访问 Google Play 商店并下载Cisco网络设置助理。选中 **Web Authentication** 复选框，从下拉列表中选择 Centralized，然后在 ACL 文本框中输入 NSP-ACL-Google。
- NSP - 此配置文件用于完成请求方调配流程的非 Android 设备。选中 **Web Authentication** 复选框，从下拉列表中选择 Supplicant Provisioning，然后在 ACL 文本框中输入 NSP-ACL。
- NSP Google - 此配置文件用于完成请求方调配流程的 Android 设备。选中 **Web Authentication** 复选框，从下拉列表中选择 Supplicant Provisioning，然后在 ACL 文本框中输入 NSP-ACL-Google。

查看默认 Blackhole_Wireless_Access 授权配置文件。Advanced Attributes Settings 应为如下所示：

- Cisco:cisco-av-pair = url-redirect=https://*ip*:*port*/blacklistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

证书服务的授权策略规则

本节列出您在启用Cisco ISE CA 服务时必须创建的授权策略规则。

- Corporate Assets - 此规则适用于使用 802.1X 和 MSCHAPV2 协议连接到公司无线 SSID 的公司设备。
- Android_SingleSSID - 此规则适用于访问 Google Play Store 以下载Cisco网络设置助理进行调配的 Android 设备。此规则专门针对单一 SSID 设置。
- Android_DualSSID - 此规则适用于访问 Google Play Store 以下载Cisco网络设置助理进行调配的 Android 设备。此规则专门针对双 SSID 设置。
- CWA - 此规则适用于需要完成集中式 Web 身份验证流程的设备。
- NSP - 此规则适用于需要通过使用证书进行 EAP-TLS 身份验证来完成本地请求方调配流程的设备。
- EAP-TLS - 此规则适用于已完成请求方调配流程并使用证书调配的设备。系统将向设备授予访问网络的权限。

下表列出您在配置适用于Cisco ISE CA 服务的授权策略规则时必须选择的属性和值。本示例假设您在Cisco ISE 中已配置相应的授权配置文件。

规则名称	条件	权限（要应用的授权配置文件）
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess

规则名称	条件	权限（要应用的授权配置文件）
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

ISE CA 颁发证书给 ASA VPN 用户

ISE CA 可以向通过 ASA VPN 连接的客户端计算机颁发证书。使用此功能，您可以自动将证书调配给通过 ASA VPN 连接的终端设备。

Cisco ISE 使用简单证书注册协议 (SCEP) 进行注册并将证书调配给客户端计算机。AnyConnect 客户端通过 HTTPS 连接向 ASA 发送 SCEP 请求。ASA 将评估请求并实施策略，然后通过Cisco ISE 与 ASA 之间建立的 HTTP 连接将请求中继到Cisco ISE。来自Cisco ISE CA 的响应将被中继回客户端。ASA 无法读取 SCEP 消息的内容，将充当Cisco ISE CA 的代理。Cisco ISE CA 从客户端解密 SCEP 消息，并采用加密形式发送响应。

ISE CA SCEP URL 为 http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe。如果您将使用 ISE 节点的 FQDN，则连接到 ASA 的 DNS 服务器必须能够解析该 FQDN。

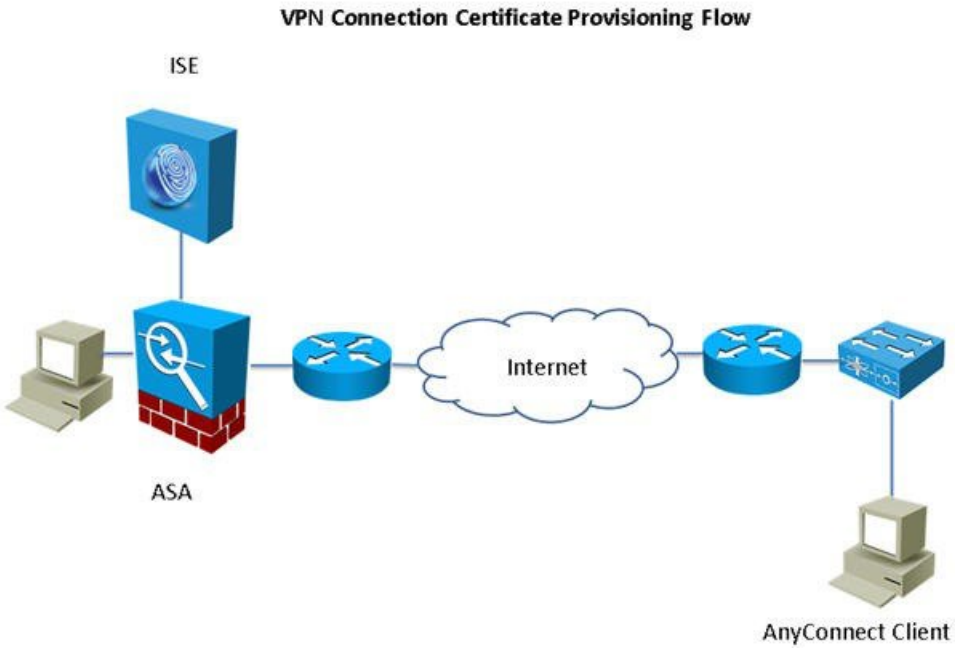
您可以在证书过期之前使用 AnyConnect 客户端配置文件配置续订。如果证书已过期，则续订流程类似于新的注册流程。

支持的版本包括：

- 运行软件版本 8.x 的 Cisco ASA 5500 系列自适应安全设备
- Cisco AnyConnect VPN 2.4 或更高版本

VPN 连接的证书调配流程

图 *9: ASA VPN* 用户的证书调配



1. 用户启动 VPN 连接。
2. AnyConnect 客户端扫描客户端机器，并将包括唯一设备标识符在内的属性（例如 IMEI）发送至 ASA。
3. ASA 从客户端请求基于证书的身份验证。身份验证因为没有证书失败。
4. ASA 使用用户名/密码执行主要用户身份验证 (AAA)，并将信息传递给身份验证服务器 (ISE)。
    1. 如果身份验证失败，连接将立即终止。
    2. 如果身份验证通过，将授予有限访问权限。您可以使用 aaa.cisco.sceprequired 属性为请求证书的客户端机器配置动态访问策略 (DAP)。您可以将此属性的值设置为“True”，并应用 ACL 和 Web ACL。
5. 在应用相关策略和 ACL 后，VPN 连接已建立。客户端仅在 AAA 身份验证成功和已建立 VPN 连接后开始 SCEP 密钥生成。
6. 客户端开始 SCEP 注册并将 SCEP 请求通过 HTTP 发送到 ASA。
7. 如果会话被允许注册，ASA 将查找请求的会话信息并将请求传递至 ISE CA。
8. ASA 将来自 ISE CA 的响应回传至客户端。
9. 如果注册成功，则客户端向用户显示一条可配置的消息，并断开 VPN 会话连接。
10. 用户可以使用证书重新验证，正常的 VPN 连接已建立。

配置思科 ISE CA 向 ASA VPN 用户颁发证书

您必须在Cisco ISE 和 ASA 上执行以下配置以向 ASA VPN 用户提供证书。

开始之前

- 确保Cisco ISE 内部或外部身份源中存在 VPN 用户帐户。
- 确保 ASA 和Cisco ISE 策略服务节点使用相同的 NTP 服务器进行同步。

步骤 1 将 ASA 定义为Cisco ISE 中的网络访问设备。参阅在思科 ISE 中添加网络设备，第 203 页查看有关如何将 ASA 添加为网络设备的信息。

步骤 2 在 ASA 上配置组策略，第 204 页。

步骤 3 为 SCEP 注册配置 AnyConnect 连接配置文件，第 204 页。

步骤 4 在 ASDM 中配置 VPN 客户端配置文件，第 205 页。

步骤 5 将思科 ISE CA 证书导入到 ASA。

在思科 ISE 中添加网络设备

您可以在Cisco ISE 中添加网络设备或使用默认网络设备。

您还可以在**网络设备 (Network Devices)** 窗口（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）中添加网络设备。

开始之前

必须在要添加的网络设备上启用 AAA 功能。请参阅启用 AAA 功能的命令，第 1197 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**名称 (Name)**、**说明** 和 **IP 地址 (IP Address)** 字段中输入相应的值。

步骤 4 从**设备配置文件 (Device Profile)**、**型号名称 (Model Name)**、**软件版本 (Software Version)** 和**网络设备组 (Network Device Group)** 字段的下拉列表中选择所需的值。

步骤 5 （可选）选中 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 复选框以配置用于身份验证的 RADIUS 协议。

步骤 6 （可选）选中 **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框以配置用于身份验证的 TACACS 协议。

步骤 7 （可选）选中 **SNMP 设置 (SNMP Settings)** 复选框以为Cisco ISE 分析服务配置 SNMP，以便从设备收集信息。

步骤 8 （可选）选中**高级 Trustsec 设置 (Advanced Trustsec Settings)** 复选框以配置启用Cisco Trustsec 的设备。

步骤 9 点击**提交 (Submit)**。

在 ASA 上配置组策略

配置 ASA 中的组策略以定义 ISE CA URL 供 AnyConnect 转发 SCEP 注册请求。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，点击**组策略 (Group Policies)**。

步骤 3 点击**添加 (Add)** 以创建组策略。

步骤 4 输入组策略的名称。例如 ISE_CA_SCEP。

步骤 5 在“转发 URL SCEP”(SCEP forwarding URL) 字段中，取消选中**沿用 (Inherit)** 复选框并输入带端口号的 ISE SCEP URL。

如果在使用 ISE 节点的 FQDN，连接至 ASA 的 DNS 服务器必须能够解析 ISE 节点的 FQDN。

示例：

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe。

步骤 6 点击**确定 (OK)** 保存组策略。

为 SCEP 注册配置 AnyConnect 连接配置文件

在 ASA 上配置 AnyConnect 连接配置文件可指定 ISE CA 服务器、身份验证方法和 ISE CA SCEP URL。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，点击 **AnyConnect 连接配置文件 (AnyConnect Connection Profile)**。

步骤 3 点击**添加 (Add)** 创建连接配置文件。

步骤 4 输入连接配置文件的名称。例如 Cert-Group。

步骤 5 （可选）在“别名”(Aliases) 字段中，输入连接配置文件的描述。例如 SCEP-Call-ASA。

步骤 6 在“身份验证”(Authentication) 区域，指定以下信息：

- “方法”(Method) - 点击**两者都 (Both)** 单选按钮
- “AAA 服务器组”(AAA Server Group) - 点击**管理 (Manage)** 并选择您的 ISE 服务器

步骤 7 在“客户端地址分配”(Client Address Assignment) 区域，选择要使用的 DHCP 服务器和客户端地址池。

步骤 8 在“默认组策略”(Default Group Policy) 区域中，点击**管理 (Manage)** 并选择已创建的带有 ISE SCEP URL和端口号的“组策略”(Group Policy)。

示例：

例如 ISE_CA_SCEP。

步骤 9 选择 **高级 (Advanced)** > **常规 (General)** 并为此连接配置文件选中**启用简单认证登记协议 (Enable Simple Certificate Enrollment Protocol)** 复选框。

步骤 10 点击**确定 (OK)**。

AnyConnect 连接配置文件已创建。

下一步做什么

在 ASDM 中配置 VPN 客户端配置文件

为 SCEP 注册在 AnyConnect 配置 VPN 客户端配置文件。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，点击 **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 3 选择要使用的客户端配置文件，然后点击**编辑 (Edit)**。

步骤 4 点击左侧“配置文件”(Profile) 导航窗格中的**认证登记 (Certificate Enrollment)**。

步骤 5 选中**认证登记 (Certificate Enrollment)** 复选框。

步骤 6 在以下字段中输入值：

- “证书过期阈值”(Certificate Expiration Threshold) - 在证书过期日前，AnyConnect 提醒用户其证书即将过期的天数（启用 SCEP 时不支持该功能）。默认值为零（不显示警告）。值范围为 0 到 180 天。
- “自动 SCEP 主机”(Automatic SCEP Host) - 输入已配置 SCEP 证书检索的 ASA 的主机名和连接配置文件（隧道组）。输入 ASA 的完全限定域名 (FQDN) 或连接配置文件名称。例如主机名 asa.cisco.com 和连接配置文件名称 scep_eng。
- CA URL - 识别 SCEP CA 服务器。输入 ISE 服务器的 FQDN 或 IP 地址。例如 http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe。

步骤 7 输入定义客户端如何请求证书内容的证书内容值。

步骤 8 点击**确定 (OK)**。

AnyConnect 客户端配置文件已创建。有关其他信息，请参阅适用于您的 AnyConnect 版本的《思科 AnyConnect 安全移动客户端》。

将思科 ISE CA 证书导入到 ASA

将Cisco ISE 内部 CA 证书导入到 ASA。

开始之前

导出Cisco ISE 内部 CA 证书。请转至 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书颁发机构证书 (Certificate Authority Certificates)**。选中**证书服务节点 CA (Certificate Services Node CA)** 和**证书服务根 CA (Certificate Services Root CA)** 证书旁边的复选框并将其导出，一次导出一个证书。

步骤 1 登录Cisco ASA ASDM。

步骤 2 从左侧的“远程访问 VPN 导航”(Remote Access VPN Navigation) 窗格中，选择 **证书管理 (Certificate Management)** > **CA 证书 (CA Certificates)**。

步骤 3 点击**添加 (Add)**并选择Cisco ISE 内部 CA 证书可将其导入 ASA。

吊销终端证书

如果您需要吊销向员工个人设备颁发的证书，您可以从终端证书 (Endpoint Certificates) 页面进行吊销。例如，如果员工的设备被盗或丢失，您可以登录Cisco ISE Admin 门户，然后从终端证书 (Endpoint Certificates) 页面吊销颁发给该设备的证书。在此页面上，您可以根据友好名称 (Friendly Name)、设备唯一 Id (Device Unique Id) 或序列号 (Serial Number) 过滤数据。

如果 PSN（子 CA）已被破坏，您可以通过从终端证书 (Endpoint Certificates) 页面过滤 Issued By 字段，吊销 PSN 颁发的所有证书。

当您吊销颁发给员工的证书时，如果有活动会话（已使用该证书进行身份验证），会话将立即终止。吊销证书可确保证书一撤销，未授权的用户就无法访问资源。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发的证书 (Issued Certificates)**。

步骤 2 选中您要吊销的终端证书旁边的复选框，然后点击**吊销 (Revoke)**。

您可以根据友好名称 (Friendly Name) 和 设备类型 (Device Type) 搜索证书。

步骤 3 输入吊销证书的原因。

步骤 4 点击**是 (Yes)**。

OCSP 服务

在线证书状态协议 (OCSP) 是一种用于检查 x.509 数字证书状态的协议。此协议替代证书吊销列表 (CRL) 并解决导致处理 CRL 的问题。

Cisco ISE 能够通过 HTTP 与 OCSP 服务器进行通信，以在身份验证中验证证书的状态。OCSP 配置在可从Cisco ISE 中配置的任何证书颁发机构 (CA) 证书引用的可重用配置对象中进行配置。

您可以根据 CA 配置 CRL 和/或 OCSP 验证。如果同时选择两者，则Cisco ISE 会先通过 OCSP 执行验证。如果检测到主 OCSP 服务器和辅助 OCSP 服务器均有通信问题，或者如果针对给定证书返回未知状态，则Cisco ISE 会切换至检查 CRL。

思科 ISE CA 服务在线证书状态协议响应器

Cisco ISE CA OCSP 响应器是与 OCSP 客户端进行通信的服务器。Cisco ISE CA 的 OCSP 客户端包括内部Cisco ISE OCSP 客户端和自适应安全设备 (ASA) 上的 OCSP 客户端。OCSP 客户端应使用 RFC 2560 和 5019 中定义的 OCSP 请求/响应结构与 OCSP 响应器进行通信。

ISE CA 向 OCSP 响应器颁发证书。OCSP 响应器在端口 2560 上侦听任何传入请求。此端口配置为仅允许 OCSP 流量。

OCSP 响应器接受遵循 RFC 2560 和 5019 中定义的结构的请求。OCSP 请求中支持随机数扩展。OCSP 响应器获取证书的状态，然后创建 OCSP 响应并对其进行签名。OCSP 响应不会缓存到 OCSP 响应器上，但您可以将 OCSP 响应缓存到客户端上，最长期限为 24 小时。OCSP 客户端应验证 OCSP 响应中的签名。

PAN 上的自签名 CA 证书（如果 ISE 用作外部 CA 的中间 CA，则是中间 CA 证书）颁发 OCSP 响应器证书。PAN 上的此 CA 证书颁发 PAN 和 PSN 上的 OCSP 证书。此自签名 CA 证书也是整个部署的根证书。整个部署中的所有 OCSP 证书都放在 ISE 的受信任证书库中，以验证任何使用这些证书签名的响应。

OCSP 证书状态值

OCSP 服务面向给定的证书请求返回以下值：

- Good - 表示对状态查询的肯定回答。它意味着仅在下次时间间隔（存活时间）值之前证书未被吊销并且状态良好。
- Revoked - 证书被吊销。
- Unknown - 证书状态未知。如果证书不是由此 OCSP 响应者的 CA 颁发，则 OCSP 服务会返回此值。
- Error - 没有收到 OCSP 请求的任何响应。

OCSP 高可用性

Cisco ISE 能够为每个 CA 配置最多两台 OCSP 服务器，我们将其称为主 OCSP 服务器和辅助 OCSP 服务器。每个 OCSP 服务器配置均包含以下参数：

- URL - OCSP 服务器 URL。
- Nonce - 请求中发送的随机数。此选项可确保重放攻击无法利用旧通信数据。
- Validate response - Cisco ISE 验证从 OCSP 服务器接收到的响应签名。

在超时（5 秒钟）情况下，当Cisco ISE 与主要 OCSP 服务器进行通信时，它会切换为辅助 OCSP 服务器。

Cisco ISE 在尝试再次使用主要服务器之前，会在可配置的时间内使用辅助 OCSP 服务器。

OCSP 故障

以下是三个一般 OCSP 故障情况：

- OCSP 缓存或 OCSP 客户端（Cisco ISE）故障。
- OCSP 响应器故障情况，例如：

第一个主要 OCSP 响应器无响应，辅助 OCSP 响应器响应Cisco ISE OCSP 请求。

无法从Cisco ISE OCSP 请求接收错误或响应。

OCSP 响应器可能不向Cisco ISE OCSP 请求提供响应或可能返回一个不成功的 OCSP Response Status 值。可能的 OCSP Response Status 值如下所示：

- tryLater
- signRequired
- unauthorized
- internalError
- malformedRequest

  OCSP 请求中有很多日期时间检查、签名验证检查等。有关详细信息，请参阅 *RFC 2560 X.509* 互联网公钥基础结构在线证书状态协议 - *OCSP*，其中描述了所有可能的状态，包括错误状态。

- OCSP 报告故障

添加 OCSP 客户端配置文件

您可以使用 OCSP Client Profile 页面，将新 OCSP 客户端配置文件添加到Cisco ISE。

开始之前

如果 Certificate Authority (CA) 正在非标准端口（不是 80 或 443）上运行 OCSP 服务，则必须在交换机上配置 ACL，允许在Cisco ISE 和 CA 之间通过此端口进行通信。例如：

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP* 端口号>

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **OCSP 客户端配置文件 (OCSP Client Profile)**。

步骤 2 输入值，添加 OCSP 客户端配置文件。

步骤 3 点击**提交 (Submit)**。

OCSP 客户端配置文件设置

下表介绍了“OCSP 客户端配置文件”(OCSP Client Profile) 窗口上的字段，可以使用此窗口配置 OCSP 客户端配置文件。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **OCSP 客户端配置文件 (OCSP Client Profile)**。

表 *29: OCSP* 客户端配置文件设置

字段名称	使用指南
名称 **(Name)**	OCSP 客户端配置文件的名称。
说明	输入可选的说明。
配置 **OCSP** 响应器 **(Configure OCSP Responder)**	
启用辅助服务器 **(Enable Secondary Server)**	选中此复选框来以启用高可用性辅助 OCSP 服务器。
始终先访问主服务器 **(Always Access Primary Server First)**	使用此选项以在尝试移至辅助服务器之前先检查主要服务器。即使之前已检查主要服务器并且发现主服务器无响应，Cisco ISE 在移至辅助服务器之前仍会尝试向主要服务器发送请求。
在 ***n*** 分钟后回退至主服务器 **(Fallback to Primary Server After Interval n Minutes)**	当您希望Cisco ISE 移至辅助服务器，然后再回退到主服务器时，请使用此选项。在这种情况下，系统将跳过所有其他请求，并按照该文本框中配置的时间使用辅助服务器。允许的时间范围是 1 至 999 分钟。
主服务器和辅助服务器 **(Primary and Secondary Servers)**	
URL	输入主要和/或辅助 OCSP 服务器的 URL。
启用 **Nonce** 扩展支持 **(Enable Nonce Extension Support)**	您可以配置一个作为 OCSP 请求的一部分发送的 Nonce。Nonce 会在 OCSP 请求中包含一个伪随机数。系统会验证在响应中接收的数值是否与请求中包含的此数相同。此选项可确保重放攻击无法利用旧通信数据。
验证响应签名 **(Validate Response Signature)**	OCSP 响应器用以下一个证书为响应签名： • CA 证书 • 与 CA 证书不同的证书 为了使Cisco ISE 验证响应签名，OCSP 响应器需要连同该证书一起发送响应，否则响应验证会失败，而且证书状态不可靠。根据 RFC，OCSP 可以使用不同的证书给响应签名。只要 OCSP 发送给响应签名的证书以供Cisco ISE 进行验证，就会如此。如果 OCSP 使用Cisco ISE 中未配置的其他证书给响应签名，响应验证将失败。
使用授权信息访问 **(AIA)** 中指定的 **OCSP URL**。**(Use OCSP URLs specified in Authority Information Access [AIA])**	点击单选按钮以使用授权信息访问扩展名中指定的 OCSP URL。
响应缓存 **(Response Cache)**	

字段名称	使用指南
缓存条目生存时间 *n* 分钟 (Cache Entry Time To Live n Minutes)	以分钟为单位输入缓存项目在多长时间之后过期。来自 OCSP 服务器的每个响应都有一个 nextUpdate 值。此值显示服务器上接下来将于何时更新证书的状态。缓存 OCSP 响应时，系统会比较两个值（一个是来自配置的值，另一个是来自响应的值），系统会按照这两个值中最低的值将响应缓存相应的时间。如果 nextUpdate 值为 0，则根本不缓存响应。Cisco ISE 将 OCSP 响应缓存所配置的时间。缓存不复制，也不是持久性的，所以当Cisco ISE 重新启动时，系统会清除缓存。使用 OCSP 缓存是为了保持 OCSP 响应以及出于以下原因： • 减少网络流量和降低 OCSP 服务器对已知证书带来的负载 • 通过缓存已知证书状态提高Cisco ISE 性能 默认情况下，内部 CA 的 OCSP 客户端配置文件的缓存设置为 2 分钟。如果终端在第一次身份验证后 2 分钟内进行第二次验证，将使用 OCSP 缓存，而不查询 OCSP 响应器。如果终端证书在缓存期间内撤销，将使用之前 OCSP 的状态良好 (Good)，身份验证成功。将缓存设置为 0 分钟可阻止所有响应被缓存。此选项可提高安全性，但会降低身份验证性能。
清空缓存 (Clear Cache)	点击**清空缓存 (Clear Cache)** 以清除连接至 OCSP 服务的所有证书颁发机构的条目。 在部署中，**清空缓存 (Clear Cache)** 与所有节点交互并执行此操作。此机制可更新部署中的每个节点。

相关主题

OCSP 服务，第 206 页
思科 ISE CA 服务在线证书状态协议响应器，第 206 页
OCSP 证书状态值，第 207 页
OCSP 高可用性，第 207 页
OCSP 故障，第 207 页
OCSP 统计计数器，第 210 页
添加 OCSP 客户端配置文件，第 208 页

OCSP 统计计数器

Cisco ISE 使用 OCSP 计数器记录并监控 OCSP 服务器的数据和运行状况。日志记录每五分钟记录进行一次。Cisco ISE 将系统日志消息发送到监控节点，并在本地库中进行保存。本地库包含之前五分钟的数据。Cisco ISE 发送系统日志消息后，计数器会重新开始计算下一个间隔。这表示在五分钟后，新的五分钟时间间隔将会启动。

以下表格列出 OCSP 系统日志消息及其说明。

表 *30: OCSP* 系统日志消息

消息	说明
OCSPPrimaryNotResponsiveCount	无响应的主请求数量
OCSPSecondaryNotResponsiveCount	无响应的辅助请求数量
OCSPPrimaryCertsGoodCount	对于使用 OCSP 主服务器的给定 CA 所返回的“good”证书数量
OCSPSecondaryCertsGoodCount	对于使用 OCSP 主服务器的给定 CA 所返回的“good”状态数量
OCSPPrimaryCertsRevokedCount	对于使用 OCSP 主服务器的给定 CA 所返回的“revoked”状态数量
OCSPSecondaryCertsRevokedCount	对于使用 OCSP 辅助服务器的给定 CA 所返回的“revoked”状态数量
OCSPPrimaryCertsUnknownCount	对于使用 OCSP 主服务器的给定 CA 所返回的“Unknown”状态数量
OCSPSecondaryCertsUnknownCount	对于使用 OCSP 辅助服务器的给定 CA 所返回的“Unknown”状态数量
OCSPPrimaryCertsFoundCount	主源缓存中查找到的证书数量
OCSPSecondaryCertsFoundCount	辅助源缓存中查找到的证书数量
ClearCacheInvokedCount	经过间隔时间后触发缓存清理的次数
OCSPCertsCleanedUpCount	经过间隔时间后清除的已缓存条目的数量
NumOfCertsFoundInCache	缓存中已执行的请求数量
OCSPCacheCertsCount	在 OCSP 缓存中查找到的证书数量

配置管理员访问策略

管理员访问权限 (RBAC) 策略以 if-then 的格式表示，其中 if 是 RBAC Admin Group 的值，then 是 RBAC Permissions 的值。

RBAC 策略页面（**管理 (Administration) > 系统 (System) > 管理访问 (Admin Access) > 授权 (Authorization) >RBAC 策略 (Policy)**）包含默认策略列表。您无法编辑或删除这些默认策略。 但是，您可以编辑只读管理员策略的数据访问权限。 通过 RBAC 策略页面，还可以为工作场所的专门管理员组创建自定义 RBAC 策略，并将其应用于个性化管理员组。

分配有限菜单访问权限时，请确保数据访问权限允许管理员访问使用指定菜单时所必需的数据。例如，如果给予对 MyDevices 门户的菜单访问权限，但不允许对终端身份组进行数据访问，则该管理员无法修改该门户。

注释 管理员用户可以将终端 MAC 地址从他们拥有只读访问权限的终端身份组移动到他们拥有完全访问权限的终端身份组。反之则不可能。

开始之前

- 确保您已创建您想要定义 RBAC 策略的所有管理员组。
- 确保这些管理员组映射到各对应的管理员用户。
- 确保您已配置 RBAC 权限，例如菜单访问和数据访问权限。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **RBAC 策略 (RBAC Policy)**。

RBAC Policies 页面包含一系列适用于默认管理员组的现成的预定义策略。您无法编辑或删除这些默认策略。 但是，您可以编辑默认只读管理员策略的数据访问权限。

步骤 2 点击任意默认 RBAC 策略规则旁边的 **Actions**。

在这里，您可以插入新的 RBAC 策略，复制现有 RBAC 策略和删除现有 RBAC 策略。

步骤 3 点击 **Insert new policy**。

步骤 4 为 Rule Name、RBAC Group(s) 和 Permissions 字段输入相应值。

在创建 RBAC 策略时，您不能选择多个菜单访问和数据访问权限。

步骤 5 点击**保存 (Save)**。

管理员访问设置

Cisco ISE 允许为管理员帐户定义某些规则以增强安全性。您可以限制对管理接口的访问，强制管理员使用强密码和定期更改密码等。在Cisco ISE 中的“管理员帐户设置”(Administrator Account Settings) 下定义的密码策略适用于所有管理员帐户。

Cisco ISE 支持包含 UTF-8 字符的管理员密码。

配置最大数量的并发管理会话和登录横幅

您可以配置最大数量的并发管理 GUI 或 CLI (SSH) 会话和登录横幅，它们对访问您的管理 Web 或 CLI 界面的管理员有帮助和指导作用。您可以将登录横幅配置为在管理员登录之前和登录之后显示。默认情况下，这些登录横幅处于禁用状态。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **访问 (Access)** > **会话 (Session)**。

步骤 2 输入您要允许通过 GUI 和 CLI 界面的最大数量的并发管理会话。并发管理 GUI 会话的有效范围为 1 至 20。并发管理 CLI 会话的有效范围为 1 至 10。

步骤 3 如果希望Cisco ISE 在管理员登录之前显示消息，请选中**登录前横幅 (Pre-login banner)** 复选框，然后在文本框中输入消息。

步骤 4 如果希望Cisco ISE 在管理员登录之后显示消息，请选中**登录后横幅 (Post-login banner)** 复选框，然后在文本框中输入消息。

步骤 5 点击**保存 (Save)**。

相关主题

允许从“选择 IP 地址”(Select IP Addresses) 对思科 ISE 进行管理访问 ，第 213 页

允许从“选择 IP 地址”(Select IP Addresses) 对思科 ISE 进行管理访问

Cisco ISE 允许您配置 IP 地址列表，管理员可通过列表中的 IP 地址访问Cisco ISE 管理界面。

管理员访问控制设置仅适用于承担管理、策略服务或监控角色的Cisco ISE 节点。这些限制会从主要节点复制到辅助节点。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **访问 (Access)** > **IP 访问 (IP Access)**。

步骤 2 选择**仅允许连接列出的 IP 地址 (Allow only listed IP addresses to connect)**。

注释 端口 161 上的连接 (SNMP) 用于管理访问。但是，在配置 IP 访问限制时，如果从一个节点执行 snmpwalk 而没有为其配置管理访问，则 snmpwalk 会失败。

步骤 3 在 Configure IP List for Access Restriction 区域中，点击**添加 (Add)**。

步骤 4 在 IP addresses 字段中输入无类域间路由 (CIDR) 格式的 IP 地址。

注释　此 IP 地址的范围可以是 IPv4 和 IPv6。您现在可以为 ISE 节点配置多个 IPv6 地址。

步骤 5 在网络掩码字段中输入 CIDR 格式的子网掩码。

步骤 6 点击**确定 (OK)**。重复此过程在此列表中添加更多 IP 地址范围。

步骤 7 点击**保存 (Save)** 保存所做的更改。

步骤 8 点击**重置 (Reset)** 以刷新 **IP 访问 (IP Access)** 页面。

允许访问思科 ISE 中的 MnT 部分

Cisco ISE 允许您配置节点列表，管理员可从这些节点访问Cisco ISE 中的 MnT 部分。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 从Cisco ISE 主页中，选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **访问 (Access)**。

步骤 2 点击 **MnT 访问 (MnT Access)** 选项卡。

步骤 3 要允许部署内或部署外的节点或实体将系统日志发送到 MnT，请点击**允许任何 IP 地址连接到 MnT (Allow any IP address to connect to MnT)** 单选按钮。要仅允许部署内的节点或实体将系统日志发送到 MnT，请点击**仅允许部署中的节点连接到 MnT (Allow only the nodes in the deployment to connect to MnT)** 单选按钮。

注释　对于 ISE 2.6 P2 及更高版本，默认情况下打开经思科 ISE 消息服务传递的系统日志，此设置不允许来自部署外的任何其他实体的系统日志。

为管理员帐户配置密码策略

Cisco ISE 还允许您为管理员帐户创建密码策略，以增强安全性。您可以定义是使用基于密码的管理员身份验证还是使用基于客户端证书的管理员身份验证。您在此处定义的密码策略将应用于Cisco ISE 中的所有管理员帐户。

注释

- 内部管理员用户的电子邮件通知将发送到 root@host。无法配置电子邮件地址，并且许多 SMTP 服务会拒绝此电子邮件。

  可以遵循开放缺陷 CSCui5583，此增强允许您更改电子邮件地址。

- 思科 ISE 支持包含 UTF-8 字符的管理员密码。

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 如果在部署中启用自动故障切换配置，请务必关闭此配置。当您更改身份验证方法时，需要重新启动应用服务器进程。这些服务重新启动时可能会出现延迟。由于服务重新启动时出现这种延迟，可能会触发辅助管理节点的自动故障切换。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)**。

步骤 2 选择以下身份验证方法之一：

- “基于密码”(Password Based)- 如果想要对管理员登录使用标准用户 ID 和密码凭证，请选择**基于密码 (Password Based)** 选项并指定“内部”(Internal) 或“外部”(External) 身份验证类型。

  注释 如果您已配置外部身份源（如 LDAP）并且想要使用该身份源作为向管理员用户授予访问权限的身份验证源，则必须从“身份源”(Identity Source) 列表框中选择该特定身份源。

- Client Certificate Based - 如果您想要指定基于证书的策略，请选择 **Client Certificate Based** 选项，并选择现有的证书身份验证配置文件。

步骤 3 点击 **Password Policy** 选项卡并输入值。

步骤 4 点击**保存 (Save)** 保存管理员密码策略。

注释 如果在登录时使用外部身份库验证管理员的身份，请记住，即便为应用到该管理员配置文件的密码策略配置了此设置，外部身份库仍会验证管理员的用户名和密码。

相关主题

管理员密码策略设置，第 50 页
为管理员帐户配置帐户禁用策略，第 215 页
为管理员帐户配置锁定或暂停设置，第 216 页

为管理员帐户配置帐户禁用策略

如果在配置的连续几天内，管理员帐户没有通过身份验证，Cisco ISE 允许您禁用该管理员帐户。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)** > **帐户禁用策略 (Account Disable Policy)**。

步骤 2 选中**在 n 天不活跃之后禁用帐户 (Disable account after *n* days of inactivity)** 复选框，并输入天数。

如果管理员帐户在一段连续时间内处于不活跃状态，通过该选项，您可以禁用管理员帐户。但是，您可以使用**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员用户 (Admin Users)** 中提供的**从不禁用不活跃帐户 (Inactive Account Never Disabled)** 选项，从该帐户禁用策略中排除单个管理员帐户。

步骤 3 点击**保存 (Save)** 为管理员配置全局帐户禁用策略。

为管理员帐户配置锁定或暂停设置

Cisco ISE 允许您锁定或暂停失败登录尝试超过指定次数的管理员帐户（包括基于密码的内部管理员帐户和基于证书的管理员帐户）。

步骤 1 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 身份验证 (Authentication) > 锁定/暂停设置 (Lock/Suspend Settings)**。

步骤 2 选中“错误登录尝试之后锁定或暂停帐户”(Account With Incorrect Login Attempts) 复选框，并输入失败尝试次数，在此次数后将采取操作。有效范围为 3 到 20。

- “将帐户暂停 n 分钟”(Suspend Account For n Minutes) - 选择此选项可暂停错误登录尝试超过指定次数的帐户。有效范围为 15 到 1440。
- “锁定帐户”(Lock Account) - 选择此选项可锁定错误登录尝试超过指定次数的帐户。

可以输入自定义电子邮件补救消息，例如请最终用户联系服务中心以解锁帐户。

注释 锁定/暂停设置在思科 ISE 早期版本的“密码策略”(Password Policy) 选项卡中可用。

配置管理员会话超时

在Cisco ISE 中，可以确定管理 GUI 会话处于非活动状态但仍保持连接的时间长度。可以指定Cisco ISE 在注销管理员之前经过的时间（以分钟为单位）。会话超时后，管理员必须重新登录才能访问 Cisco ISE 管理员门户。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 设置 (Settings) > 会话 (Session) > 会话超时 (Session Timeout)**。

步骤 2 输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。

步骤 3 点击**保存 (Save)**。

终止活动管理会话

Cisco ISE 显示所有活动管理会话，您可以从中选择任意会话并在必要时随时终止所选会话。并行管理 GUI 会话的最大数量为 20 个。如果达到 GUI 会话的最大数量，属于超级管理员组的管理员可以登录并阻止某些会话。

开始之前

要执行以下任务，您必须是超级管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)** > **会话信息 (Session Info)**。

步骤 2 选中要终止的会话 ID 旁边的复选框，然后点击**失效 (Invalidate)**。

更改管理员名称

Cisco ISE 允许您从 GUI 更改用户名。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 登录到管理员门户。

步骤 2 点击Cisco ISE UI 右上角显示为链接的用户名。

步骤 3 在显示的 Admin User 页面中输入新用户名。

步骤 4 编辑有关要更改的帐户的任何其他详细信息。

步骤 5 点击**保存 (Save)**。

管理员访问设置

您可以通过这些页面为管理员配置访问设置。

管理员密码策略设置

下表介绍了“管理员密码策略”(Administrator Password Policy) 窗口中的字段，可以使用此窗口定义管理员密码应满足的条件。。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。

表 *31:* 管理员密码策略设置

字段名称	使用指南
最小长度 **(Minimum Length)**	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。
密码不得包含 **(Password must not contain)**	**管理员名称或其反向顺序的字符 (Admin name or its characters in reverse order)**：选中此复选框可限制使用管理员用户名或其反向顺序的字符。
	“cisco”或其反向顺序的字符 ("cisco" or its characters in reverse order)：选中此复选框可限制使用单词“cisco”或其反向顺序的字符。
	此单词或其反向顺序的字符 (This word or its characters in reverse order)：选中此复选框可限制使用您定义的任何单词或其反向顺序的字符。
	连续重复四次或以上的字符 (Repeated characters four or more times consecutively)：选中此复选框可限制使用连续重复四次或以上的字符。
	字典单词、其反向顺序的字符或其替换为其他字符的字母 (Dictionary words, their characters in reverse order or their letters replaced with other characters)：选中此复选框可限制使用字典单词、其反向顺序的字符或其替换为其他字符的字母。 不允许使用“$”替代“s”、“@”替代“a”、“0”替代“o”、“1”替代“l”、“!”替代“i”、“3”替代“e”。例如 Pa$$w0rd • **默认字典 (Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。 默认情况下，此选项已选中。 • **自定义字典 (Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**浏览**选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。

字段名称	使用指南
密码必须包含每个所选类型的至少一个字符 **(Password must contain at least one character of each of the selected types)**	指定管理员密码必须包含从以下选项中选择的类型的至少一个字符： • 小写字母字符 • 大写字母字符 • 数字字符 • 非字母数字字符
密码历史记录 **(Password History)**	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
密码有效期 **(Password Lifetime)**	指定以下选项来强制用户在经过指定时间段后更改密码： • “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。”(Time (in days) before the administrator account is disabled if the password is not changed.)（允许的范围是 0 至 2147483647 天。） • “禁用管理员帐户之前的提醒时间（按天计）。”(Reminder (in days) before the administrator account is disabled.)
显示网络设备敏感数据 **(Display Network Device Sensitive Data)**	
要求管理员密码 **(Require Admin Password)**	如果您希望管理员用户输入登录密码来查看网络设备敏感数据，例如共享密钥和密码，请选中此复选框。
密码缓存用于 **(Password cached for)**	在此段时间内，会对管理员用户输入的密码进行缓存。在此期间，如果管理员用户要查看网络设备敏感数据，系统不会再次提示输入密码。有效范围为 1 至 60 分钟。

相关主题

思科 ISE 管理员，第 3 页
创建新管理员，第 4 页

会话超时和会话信息设置

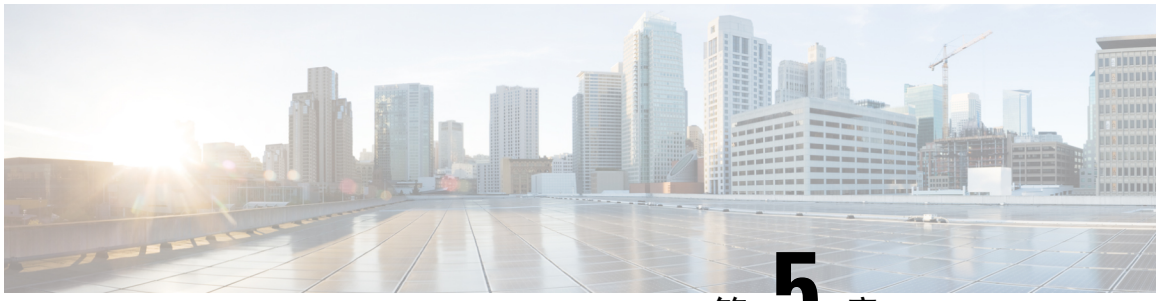
下表介绍**会话 (Session)** 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *32:* 会话超时和会话信息设置

字段名称	使用指南
会话超时 (Session Timeout)	
会话空闲超时 (Session Idle Timeout)	输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。
会话信息 (Session Info)	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后点击**失效 (Invalidate)**。

相关主题

管理员访问设置，第 212 页
配置管理员会话超时，第 216 页
终止活动管理会话，第 217 页



第 5 章

维护和监控

自适应网络控制

自适应网络控制 (ANC) 是一项在管理节点上运行的服务。此服务可监控和控制终端的网络访问。ANC 由 ISE 管理员在管理 GUI 上调用，也可以通过 pxGrid 从第三方系统调用。ANC 支持有线和无线部署，并且需要 Plus 许可证。

您可以使用 ANC 更改授权状态，无需修改系统的总体授权策略。ANC 允许您在隔离终端时设置授权状态。结果会建立授权策略，这些授权策略定义为检查 ANCPolicy 以限制或拒绝网络访问。您可以取消隔离终端，使其获得完整的网络访问权限。您也可以关闭网络连接系统 (NAS) 上的端口，断开终端与网络之间的连接。

一次可以隔离的用户数量没有限制。此外，隔离期长度没有时间限制。

您可以执行以下操作，以便通过 ANC 监控和控制网络访问：

- 隔离 - 允许您使用例外策略（授权策略）限制或拒绝终端接入网络。必须创建例外策略，以根据 ANCPolicy 分配不同的授权配置文件（权限）。设置为隔离状态，本质上是将终端从其默认 VLAN 迁移到指定的隔离 VLAN。您必须提前定义隔离 VLAN，在同一 NAS 上作为终端获得支持。
- 取消隔离 - 允许您解除隔离状态，让终端获得完整的网络访问权限。这是通过使终端返回原 VLAN 实现的。
- 关闭 - 允许您禁用 NAS 上的端口，断开终端与网络之间的连接。当终端连接的 NAS 上的端口关闭后，应重新手动重置 NAS 上的端口。这可以让终端连接到网络（不适用于无线部署）。

隔离和取消隔离操作可以从活动终端的会话目录报告触发。

注释 如果取消隔离已隔离的会话，新取消隔离的会话的发起方法将取决于交换机配置指定的身份验证方法。

注释 从Cisco ISE 1.4 开始，ANC 取代了端点保护服务 (EPS)。ANC 提供额外的分类和性能改进。虽然在策略中使用 ERS 属性有时仍然适用于某些 ANC 操作，但应使用 ANC 属性。

在思科 ISE 中启用自适应网络控制

默认情况下禁用 ANC。只有在启用 pxGrid 时才会启用 ANC，并且它将保持启用状态，直到在管理员门户中手动禁用该服务。

配置网络访问设置

ANC 可以让您重置终端的网络访问状态，以便对端口进行隔离、取消隔离或关闭端口。这些定义了网络中终端的授权程度。

您可以使用终端 IP 地址或 MAC 地址隔离或取消隔离终端抑或关闭终端所连接的网络访问服务器 (NAS) 端口。您可以在同一终端上多次执行隔离和取消隔离操作，但不能同时执行这两种操作。如果在网络上发现恶意终端，可以使用 ANC 关闭 NAS 端口，从而禁止终端访问。

将 ANC 策略分配至终端：

开始之前

- 启用 ANC。
- 为 ANC 创建授权配置文件和例外类型授权策略。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **自适应网络控制 (Adaptive Network Control)** > **策略列表 (Policy List)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入一个 ANC 策略名称并指定 ANC 操作。可提供以下选项：

- 隔离
- Shut_Down
- Port_Bounce

您可以选择一个或多个操作，但是您无法将 Shut_Down 和 Port_Bounce 与其他 ANC 操作结合。

步骤 4 选择**策略 (Policy)** > **策略集 (Policy Sets)**，然后展开策略集。

步骤 5 使用 ANCPolicy 属性将 ANC 策略与相应的授权策略相关联。

步骤 6 选择**操作 (Operations)** > **自适应网络控制 (Adaptive Network Control)** > **终端分配**。

步骤 7 点击**添加 (Add)**。

步骤 8 输入终端的 IP 地址或 MAC 地址，并从**策略分配 (Policy Assignment)** 下拉列表选择策略。

步骤 9 点击**提交 (Submit)**。

通过 ANC 创建网络访问的授权配置文件

您必须创建一个应该与ANC配合使用的授权配置文件。您可以在标准授权配置文件列表中查看该授权配置文件。终端可在网络中进行身份验证和授权，但是限用于接入网络。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为授权配置文件输入唯一名称和说明，并将**访问类型 (Access Type)** 更新为 **ACCESS_ACCEPT**。

步骤 4 选中 **DACL Name** 复选框，然后从下拉列表中选择 **DENY_ALL_TRAFFIC**。

步骤 5 点击**提交 (Submit)**。

例外授权策略用于授权有限访问，满足特殊条件或权限或直接要求。对于ANC授权，需要创建隔离例外策略，该策略先于所有标准授权策略进行处理。您需要使用以下条件创建例外规则：

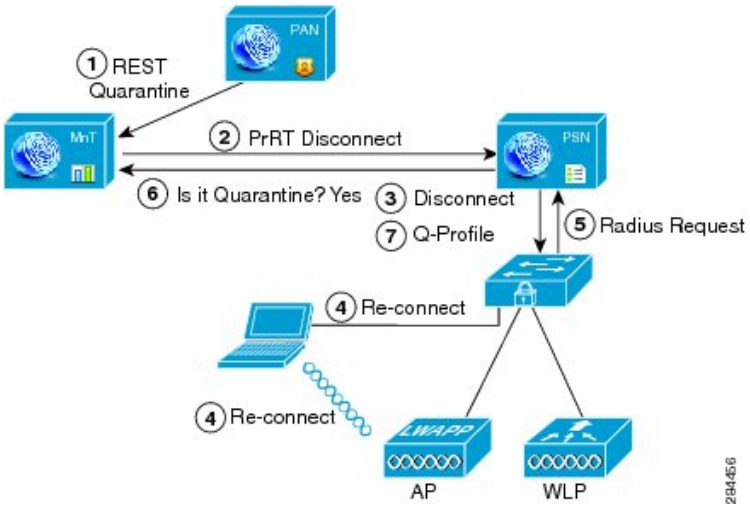
Session:ANCPolicy EQUALS 隔离。

ANC 隔离和取消隔离流程

可以使用ANC隔离所选终端，以限制其对网络的访问。您可以隔离终端并建立根据状态分配不同授权配置文件的例外授权策略。授权配置文件用作您在授权策略中定义的允许访问指定网络服务的权限的容器。当授权完成时，系统会为网络访问请求授予权限。如果之后对终端进行了验证，则可以对终端取消隔离以允许其对网络进行完全访问。

此图显示了隔离流程，它假定已配置授权规则并已建立 ANC 会话。

图 *10: ANC* 隔离流程



1. 客户端设备通过无线设备 (WLC) 登录到网络，并且系统会从管理节点 (PAP) 向监控节点 (MnT) 发出隔离 REST API 调用。
2. 然后，监控节点会通过策略服务Cisco ISE 节点 (PDP) 来调用 PrRT，从而引发授权证书 (CoA)。
3. 客户端设备的连接会断开。
4. 然后，客户端设备会重新进行身份验证并重新连接。
5. 对客户端设备的 RADIUS 请求会发回到监控节点。
6. 在进行检查时，系统将隔离客户端设备。
7. 系统将应用 Q-Profile 授权策略并验证客户端设备。
8. 系统会对客户端设备取消隔离，并向其提供对网络的完全访问权限。

ANC NAS 端口关闭流程

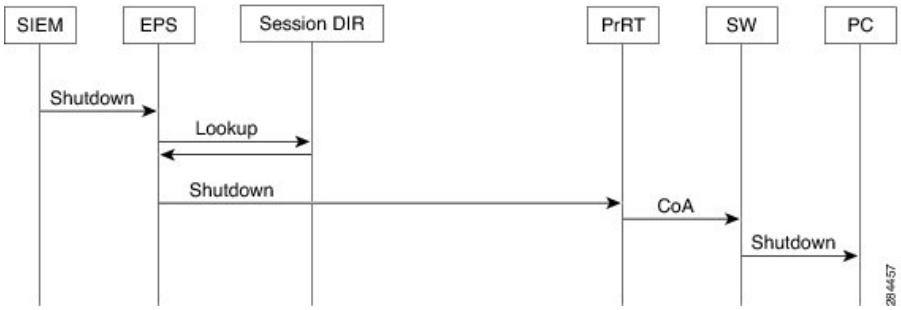
您可以使用终端 IP 地址或 MAC 地址关闭终端所连接的 NAS 端口。

通过此关闭功能您可以根据 MAC 地址的指定 IP 地址关闭 NAS 端口。您必须手动恢复该端口，才能将此终端重新接入网络，这仅对通过有线媒介连接的终端有效。

并非所有设备都支持此关闭功能。不过，大多数交换机应该都支持关闭命令。您可以使用 getResult() 命令验证关闭是否执行成功。

下图说明 ANC 关闭流程。对于客户端设备，关闭操作是在客户端设备用于访问网络的 NAS 上执行的。

图 *11: ANC* 关闭流程



终端清除设置

可以根据身份组和其他条件，通过配置规则来定义终端清除策略。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端清除 (Endpoint Purge)**。您可以选择不清除特定终端以及根据选择的分析条件清除终端。

您可以安排终端清除作业计划。默认情况下，此终端清除计划处于启用状态。默认情况下，Cisco ISE 会删除超出 30 天的终端和已注册设备。系统根据主 PAN 中配置的时区于每日凌晨 1 点（午夜）执行清除作业。

终端清除作业每 3 分钟删除 5000 多个终端。

以下是您可以用于清除终端的一些条件以及示例：

- InactivityDays - 距离终端上最后一次分析活动或更新的天数
  - 此条件用于清除随时间推移累积的陈旧设备，通常是临时访客或个人设备或废弃的设备。在您的部署中，这些终端容易形成干扰，因为它们在网络上不再活动或近期不再可能出现。如果它们偶然再进行连接，系统将在必要的情况下对其进行发现、分析、注册等。
  - 当存在来自端点的更新时，只要启用分析功能，InactivityDays 便会重置为 0。
- ElapsedDays - 创建对象之后经过的天数。
  - 此条件适用于获得特定时间段内未经身份验证或有条件的访问权限的终端，例如访客或承包商终端，或利用 webauth 进行网络访问的员工。在所允许的连接期限到期之后，他们必须重新进行完全身份验证和注册。
- PurgeDate - 要清除终端的日期。
  - 此选项用于在不考虑创建或开始时间的情况下，获得特定时间的访问权限的特殊事件或组。此选项允许同时清除所有终端。例如，贸易展览、会议或每周都有新成员的每周培训课程，在这种情况下，访问权限是根据特定周或月份授予的，而不是绝对的天、周、月。

隔离的终端在策略更改后不会重新进行身份验证

问题

策略或其他身份更改后，身份验证失败，并且系统不会重新进行身份验证。身份验证失败或有问题的终端仍然无法连接网络。根据分配给用户角色的终端安全策略，未能通过安全评估的客户端计算机上经常会出现此问题。

可能的原因

客户端计算机上身份验证计时器的设置不正确，或者交换机上身份验证时间间隔的设置不正确。

解决方案

要解决此问题，有几种可能的办法：

1. 在Cisco ISE 中查看指定 NAD 或交换机的**会话状态摘要 (Session Status Summary)** 报告，确保该界面已配置适当的身份验证间隔。

2. 在NAD/交换机上输入“show running configuration”命令，确保接口已配置适当的“authentication timer restart”设置。（例如，“authentication timer restart 15”和“authentication timer reauthenticate 15”。）
3. 输入“interface shutdown”和“no shutdown”退回NAD/交换机上的端口，并在Cisco ISE 的潜在配置更改后，强制重新进行身份验证。

注释 由于CoA 需要 MAC 地址或会话 ID，因此我们建议您不要退回网络设备 SNMP 报告中显示的端口。

当未找到 IP 地址或 MAC 地址时 ANC 操作失败

当终端的活动会话不包含关于 IP 地址的信息时，在该终端上执行的 ANC 操作会失败。对于该终端的 MAC 地址和会话 ID，也存在这种情况。

注释 如果要通过 ANC 更改终端的授权状态时，则必须提供该终端的 IP 地址或 MAC 地址。如果在终端的活动会话中无法找到 IP 地址或 MAC 地址，则会看到以下错误消息：

```
未找到此 MAC 地址、IP 地址或会话 ID 的活动会话 (No active session found for this MAC
address, IP Address or Session ID)
```

。

通过外部身份验证的管理员无法执行 ANC 操作

如果通过外部身份验证的管理员尝试从实时会话发出 CoA 隔离，Cisco ISE 会返回以下错误消息：

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User
 not found internally. Possible use of unsupported externally authenticated user
```

如果通过外部身份验证的管理员使用终端的IP地址或MAC地址执行ANC操作（从 **操作 (Operations)** ），则Cisco ISE 会显示以下错误消息：

```
Server failure: User not found internally. Possible use of unsupported externally
 authenticated user
```

备份数据类型

Cisco ISE 允许您从主 PAN 和从监控节点备份数据。可以从 CLI 或用户界面完成备份。

Cisco ISE 允许您备份以下类型的数据：

- 配置数据 - 包含应用特定和Cisco ADE 操作系统配置数据。备份可以使用 GUI 或 CLI 通过主 PAN 完成。
- 运行数据 - 包含监控和故障排除数据。备份可以通过主 PAN GUI 或使用监控节点的 CLI 来完成。

当Cisco ISE 在 VMware 上运行时，不支持用 VMware 快照备份 ISE 数据。

注释 VMware 快照用于保存 VM 在给定时间点的状态，因此Cisco ISE 不支持使用 VMware 快照备份 ISE 数据。在多节点Cisco ISE 部署中，所有节点中的数据都与当前数据库信息保持同步。恢复快照可能会导致数据库复制和同步问题。建议您使用Cisco ISE 中包含的备份功能来存档和恢复数据。

使用 VMware 快照或任何第三方备份服务备份Cisco ISE 数据可能会导致Cisco ISE 服务中断。当 VMware 或任何其他第三方备份服务（如 CommVault SAN 级别备份）启动备份时，它会暂停文件系统以保持崩溃一致性，这可能会导致Cisco ISE 功能冻结。您需要重启才能恢复Cisco ISE 部署上的服务。

可以使用更低版本的Cisco ISE 的备份文件执行恢复操作并且可以在更高版本上执行恢复操作。例如，如果您拥有来自Cisco ISE 版本 1.3 或 1.4 的 ISE 节点的备份，您可以在Cisco ISE 版本 2.1 上恢复该备份。

Cisco ISE 版本 2.7 支持从版本 2.2 及更高版本获取的备份恢复。

备份和恢复存储库

Cisco ISE 允许您通过管理员门户创建和删除存储库。您可以创建以下类型的存储库：

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

注释 存储库位于每台设备本地位置。

建议对于所有类型的部署（小型、中型和大型），创建最低 100 GB 大小的存储库。

下表显示了Cisco ISE 操作与外部存储库类型之间的可支持性信息：

表 *33:* 外部存储库的可支持性表格

存储库类型	配置备份	配置恢复	升级	操作备份	运行恢复	支持捆绑包	从用户界面验证	从用户界面导出报告	从用户界面导出策略
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	√	√	√	√	√	√	X	√	√
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

创建存储库

可以使用 CLI 和 GUI 创建存储库。由于以下原因，我们建议您使用 GUI：

- 通过 CLI 创建的存储库保存在本地且不会被复制到其他部署节点。这些存储库不会列于 GUI 的存储库页面。
- 在主 PAN 创建的存储库会被复制到其他部署节点。

在 GUI 中，密钥仅在主 PAN 上生成，因此在升级期间，需要在新的主管理节点的 GUI 中再次生成密钥，并将其导出到SFTP服务器。如果从部署中删除节点，需要在非管理节点的GUI中生成密钥，并将其导出到 SFTP 服务器。

可以在Cisco ISE 中凭借 RSA 公共密钥身份验证配置 SFTP 存储库。您可以选择使用安全密钥的 RSA 公共密钥身份验证来加密数据库和日志，而不必使用管理员创建的密码。对于通过RSA 公共密钥创建的 SFTP 存储库，在 GUI 中创建的存储库不会在 CLI 中复制，在 CLI 中创建的存储库也不会在 GUI 中复制。要在 CLI 和 GUI 中配置相同存储库，请在 CLI 和 GUI 中生成 RSA 公共密钥，并将密钥输出到 SFTP 服务器。

开始之前

- 必须具有超级管理员或系统管理员权限才能执行以下任务。
- 如果要使用 RSA 公共密钥身份验证创建 SFTP 存储库，请执行以下步骤：
  - 在 SFTP 存储库中启用 RSA 公共密钥身份验证。
  - 从Cisco ISE CLI 使用 **crypto host_key add** 命令输入 SFTP 服务器的主机密钥。主机密钥字符串应当与您在存储库配置页面的**路径 (Path)** 字段中输入的主机名匹配。

- 生成密钥对，并从 GUI 将公共密钥导出到您的本地系统。在Cisco ISE CLI 中，使用 **crypto key generate rsa passphrase** *test123* 命令生成密钥对，其中 passphrase 必须超过四个字母，然后将密钥导出到任何存储库（本地磁盘或任何其他配置的存储库）。
- 将导出的 RSA 公共密钥复制到启用 PKI 的 SFTP 服务器并将其添加到“authorized_keys”文件。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

步骤 3 点击**添加 (Add)** 以添加新存储库。

步骤 4 根据需要输入值以设置新存储库。请参阅 存储库设置，第 230 页 以了解字段说明：

步骤 5 点击 **提交 (Submit)** 以创建存储库。

步骤 6 通过点击左侧**操作 (Operations)** 导航窗格中的**存储库 (Repository)** 来验证是否成功创建存储库，或点击**存储库 (Repository)** 窗口顶部的**存储库列表 (Repository List)** 链接以转至存储库列表页面。

下一步做什么

- 确保已创建的存储库有效。可以从**存储库列表 (Repository listing)** 窗口执行此操作。选择对应存储库并点击**验证 (Validate)**。或者，您可以从Cisco ISE 命令行界面执行以下命令：

  show repository *repository_name*

  其中 *repository_name* 是已创建的存储库的名称。

  注释 如果在创建存储库时提供的路径不存在，则会遇到以下错误：

  ```
  %Invalid Directory
  ```

- 运行按需备份或安排备份。

存储库设置

下表介绍了**存储库列表 (Repository List)** 页面上的字段，可以使用此页面创建存储备份文件的存储库。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

表 *34:* 存储库设置

字段	使用指南
存储库 (Repository)	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。
协议 (Protocol)	从可用协议中选择一个您想要使用的协议。
服务器名称 (Server Name)	（对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段）输入您想要在其上创存储库的服务器的主机名或 IP 地址（IPv4 或 IPv6）。 **注释** 如果要添加使用 IPv6 地址的存储库，请确保 ISE eth0 接口配置了 IPv6 地址。
路径 (Path)	输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。 此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。
启用 PKI 身份验证 (Enable PKI authentication)	（可选；仅适用于 SFTP 存储库）如果要在 SFTP 存储库中启用 RSA 公钥身份验证，请选中此复选框。
用户名 (User Name)	（对于 FTP、SFTP 为必填字段）输入对指定服务器拥有写入权限的用户名。只允许使用字母数字字符。
密码 (Password)	（对于 FTP、SFTP 为必填字段）输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、|、@、#、$、%、^、&、*、(、)、+、和 =。

相关主题

备份和恢复存储库，第 228 页
创建存储库，第 229 页

在 SFTP 存储库中启用 RSA 公共密钥身份验证

在 SFTP 服务器中，每个节点必须具有两个 RSA 公共密钥，一个用于 CLI，一个用于 GUI。要在 SFTP 存储库中启用 RSA 公共密钥身份验证，请执行以下步骤：

步骤 1 用有权限编辑 */etc/ssh/sshd_config.file* 的帐户登录 SFTP 服务器。

注释　　*sshd_config* 文件的位置可能根据操作系统安装而有所不用。

步骤 2　输入 **vi /etc/ssh/sshd_config** 命令。

系统列出 sshd_config 文件的内容。

步骤 3　从以下行中删除“#”符号以启用 RSA 公共密钥身份验证：

- RSAAuthentication 是
- PubkeyAuthentication 是

  注释　　如果公共身份验证密钥为“否”(No)，则将其更改为“是”(Yes)。

- AuthorizedKeysFile ~/.ssh/authorized_keys

按需备份和计划备份

您可以配置主 PAN 和主监控节点的按需备份。当您希望立即备份数据时，系统会执行按需备份。

您可以安排一次性、每日、每周或每月运行系统级备份。由于备份操作持续时间较长，您可以将备份操作安排在空闲时间执行。您可以从管理门户安排备份。

注释　　如果使用的是内部 CA，应使用 CLI 导出证书和密钥。在管理门户中使用的备份不会备份 CA 链。

有关详细信息，请参阅《思科身份服务引擎管理员指南》的“基本设置”一章中的“导出思科 ISE CA 证书和密钥”部分。

相关主题

维护设置，第 1106 页

执行按需备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将Cisco ISE 恢复到获取备份时的配置状态。

重要事项 当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构(CA)证书关联的私钥，这一点至关重要。

如果要执行备份并从一个系统恢复到另一个系统，则必须选择以下选项之一以避免错误：

- **选项 1：**

  通过 CLI 从源 ISE 节点导出 CA 证书并将其导入到目标系统。

  优点：从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

- **选项 2：**

  在恢复过程之后，为内部 CA 生成所有新证书。

  优点：推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统颁发的证书将继续受信任。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

开始之前

- 在执行按需备份之前，应对Cisco ISE 中的备份数据类型有基本的了解。
- 确保已创建存储备份文件的存储库。
- 不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。
- 确保在获取备份之前执行所有证书相关的更改。
- 要执行以下任务，您必须是超级管理员或系统管理员。

注释 对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。要恢复备份，请选择存储库，然后点击**恢复 (Restore)**。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 3 选择备份类型：“配置”(Configuration) 或“运行”(Operational)。

步骤 4 点击**立即备份 (Backup Now)**。

步骤 5 根据需要输入值以执行备份。

步骤 6 点击 **备份 (Backup)**。

步骤 7 验证备份是否成功完成。

Cisco ISE 在备份文件名中附加时间戳并将文件存储在指定存储库中。除了时间戳外，Cisco ISE 会为配置备份添加 CFG 标签，为运行备份添加 OPS 标签。确保备份文件位于指定的存储库中。

在分布式部署中，不要在备份运行时更改节点角色或升级节点。如果并发运行备份，则更改节点角色不会关闭所有进程，并可能导致数据不一致。在进行任何节点角色更改之前，请等待备份完成。

备份正在运行时，请勿升级节点。如果并发运行备份，这将关闭所有进程并可能导致数据不一致。在进行任何节点更改之前，请等待备份完成。

注释 备份正在运行时，可能会看到CPU 使用率高并收到平均负载高的警报。备份完成时，CPU 使用率将恢复正常。

相关主题

思科 ISE 恢复操作，第 238 页
导出身份验证和授权策略配置，第 244 页

按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup & Restore)**。

表 *35:* 按需备份设置

字段名称	使用指南
类型	选择以下其中一个选项： • **配置数据备份 (Configuration Data Backup)**：包含应用特定配置数据和Cisco ADE 操作系统配置数据 • **运行数据备份 (Operational Data Backup)**：包含监控和故障排除数据
备份名称 (Backup Name)	输入备份文件的名称。
存储库名称 (Repository Name)	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
加密密钥 (Encryption Key)	此密钥用于加密和解密备份文件。

相关主题

备份数据类型，第 227 页
按需备份和计划备份，第 232 页
备份历史记录，第 237 页
备份失败，第 237 页
思科 ISE 恢复操作，第 238 页
导出身份验证和授权策略配置，第 244 页
在分布式环境中同步主节点和辅助节点，第 245 页
执行按需备份，第 232 页

计划备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将Cisco ISE 恢复到获取备份时的配置状态。

重要事项

当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构(CA)证书关联的私钥，这一点至关重要。

如果要执行备份并从一个系统恢复到另一个系统，则必须选择以下选项之一以避免错误：

- **选项 1：**

  通过 CLI 从源 ISE 节点导出 CA 证书并将其导入到目标系统。

  优点：从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

- **选项 2：**

  在恢复过程之后，为内部 CA 生成所有新证书。

  优点：推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统颁发的证书将继续受信任。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

开始之前

- 在安排备份之前，应对Cisco ISE 中的备份数据类型有基本的了解。
- 确保已配置存储库。
- 不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。
- 要执行以下任务，您必须是超级管理员或系统管理员。

- 如果已从Cisco ISE 1.1 或更低版本升级到Cisco ISE 1.2，应当重新配置已计划的备份。请参见《思科身份服务引擎升级指南》版本 *1.2*“已知升级问题”一节。

注释 对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。

计划备份设置

下表介绍“定期备份”(Scheduled Backup) 窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

表 *36:* 计划备份设置

字段名称	使用指南
类型 (Type)	选择以下其中一个选项： • **配置数据备份 (Configuration Data Backup)**：包含应用特定配置数据和Cisco ADE 操作系统配置数据 • **运行数据备份 (Operational Data Backup)**：包含监控和故障排除数据
名称 (Name)	输入备份文件的名称。您可以输入您所选的描述性名称。Cisco ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup) 列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 **kron** 作业。
说明	输入对备份的说明。
存储库名称 (Repository Name)	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
加密密钥 (Encryption Key)	输入用于加密和解密备份文件的密钥。
计划选项	选择计划备份的频率并相应地填写其他选项。

相关主题

备份数据类型，第 227 页

使用 CLI 备份

虽然可以从 CLI 和 GUI 安排备份，但是建议使用 GUI。不过，只能从 CLI 对辅助监控节点执行操作备份。

备份历史记录

备份历史记录提供关于定时备份和按需备份的基本信息。它会列出备份名称、备份文件大小、存储备份的库以及指明获得备份的时间的时间戳。此信息在操作审核报告以及历史记录表的 Backup and Restore 页面上列出。

对于故障备份，Cisco ISE 将触发警报。备份历史记录页面提供故障原因。操作审核报告也引用故障原因。如果故障原因缺失或不清楚，您可以从Cisco ISE CLI 运行 **backup-logs** 命令，查看 ADE.log 了解更多信息。

在备份操作运行的过程中，您可以使用 **show backup status** CLI 命令查看备份操作的进度。

备份历史记录与Cisco ADE 操作系统配置数据一起存储。甚至在应用升级后历史记录依然存在，只有当您重置 PAN 映像时才能将历史记录删除。

备份失败

如果备份失败，请检查以下事宜：

- 检查是否存在任何 NTP 同步或服务失败问题。如果Cisco ISE 上的 NTP 服务无效，Cisco ISE 将发出 NTP 服务失败警报。当 Cisco ISE 无法与所有配置的 NTP 服务器同步时，Cisco ISE 会发出 NTP 同步失败警报。如果 NTP 服务停止或有任何同步问题，Cisco ISE 备份可能会失败。检查“警报”(Alarms) Dashlet 并修复 NTP 同步或服务问题，然后再重试备份操作。
- 确保没有同时运行任何其他备份。
- 检查已配置存储库的可用磁盘空间。
  - 如果监控数据占用的空间超过所分配的监控数据库大小的 75%，则监控（操作）备份会失败。例如，如果向监控节点分配的空间为 600 GB，而监控数据占用超过 450 GB 的存储空间，则监控备份会失败。

- 如果数据库磁盘使用量超过 90%，系统会执行清除操作，使数据库的大小小于或等于所分配空间的 75%。

- 验证是否正在进行清除。进行清除时，备份和恢复操作不起作用。
- 验证存储库的配置是否正确。

思科 ISE 恢复操作

可以在主管理节点或独立管理节点上恢复配置数据。在主 PAN 上恢复数据后，必须手动将辅助节点与主 PAN 同步。

恢复运营数据的过程根据部署类型而异。

注释 Cisco ISE 中新的备份/恢复用户界面利用备份文件名中的元数据。因此，在备份完成后，不应手动修改备份文件名。如果手动修改备份文件名，则Cisco ISE 备份/恢复用户界面将无法识别备份文件。如果必须修改备份文件名，应使用Cisco ISE CLI 恢复备份。

数据恢复指南

下面提供了恢复Cisco ISE 备份数据时应遵守的指南。

- 利用Cisco ISE，您可以从 ISE 节点 (A) 获取备份并将其存储到另一个 ISE 节点 (B) 上，这两个节点有相同的主机名（但 IP 地址不同）。但是，当您在节点 B 上恢复备份后，不会更改节点 B 的主机名，因为这样做可能会导致证书和门户组标记出现问题。
- 如果在一个时区内从主 PAN 获取备份，并尝试在另一时区中的另一个Cisco ISE 节点上恢复该备份，恢复过程可能失败。如果备份文件中的时间戳晚于恢复备份所在的Cisco ISE 节点上的系统时间，则会发生此故障。如果在获得备份之后一天恢复备份，那么备份文件中的时间戳则为过去时间，恢复过程将成功。
- 当主 PAN 上恢复的备份所使用的主机名不同于获得备份的主机名时，此主 PAN 将成为独立节点。部署已损坏，辅节点将无法运行。您必须使独立节点成为主节点，重置辅节点上的配置，并在主节点上重新注册这些辅节点。要重置Cisco ISE 节点上的配置，请从Cisco ISE CLI 输入以下命令：
  - **application reset-config ise**
- 建议您在初始Cisco ISE 安装和设置之后，不要更改系统时区。
- 如果更改了部署中的一个或多个节点上的证书配置，则必须获得另一个备份才能从独立Cisco ISE 节点或主 PAN 恢复数据。否则，如果您尝试使用旧备份恢复数据，节点之间的通信可能失败。
- 在主 PAN 上恢复配置备份后，可以导入先前导出的Cisco ISE CA 证书和密钥。

注释 如果没有导出思科 ISE CA 证书和密钥，则在主 PAN 上恢复配置备份后，在主 PAN 和策略服务节点 (PSN) 上生成根 CA 和从属 CA。

- 如果尝试恢复白金级数据库而没有使用正确的 FQDN（白金级数据库的 FQDN），则需要重新生成 CA 证书。（ 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)** > **更换 ISE 根 CA 证书链 (Replace ISE Root CA certificate chain)**）。不过，如果使用正确的 FQDN 恢复白金级数据库，请注意 CA 证书将自动重新注册。
- 需要一个数据存储库，供Cisco ISE 保存备份文件。您必须创建一个存储库，然后才能运行按需备份或定期备份。
- 如果有一个独立管理节点发生故障，则必须运行配置备份进行恢复。如果主 PAN 发生故障，则可以使用分布式设置，将辅助管理节点升级为主管理节点。实现之后，可以在主 PAN 上恢复数据。

注释 思科 ISE 还提供 **backup-logs** CLI 命令，可用来收集日志和配置文件以用于故障排除。

从 CLI 恢复配置或监控（操作）备份

要通过Cisco ISE CLI 恢复配置数据，请在 EXEC 模式下使用 **restore** 命令。使用以下命令从配置或操作备份恢复数据：

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

语法说明

restore	键入此命令，从配置或操作备份恢复数据。
filename	驻留在存储库的备份文件的名称。最多支持 120 个字母数字字符。 注释 必须在文件名后面添加 .tar.gpg 扩展名（例如，myfile.tar.gpg）。
repository	指定包含备份的存储库。
repository-name	您想要从其恢复备份的存储库的名称。
encryption-key	（可选）指定用户定义的加密密钥以恢复备份。

hash	恢复备份的散列加密密钥。指定跟随的加密（散列）加密密钥。最多支持 40 个字符。
plain	用于恢复备份的明文加密密钥。指定跟随的未加密密文加密密钥。最多支持 15 个字符。
encryption-key name	输入加密密钥。
include-adeos	（可选，仅适用于配置备份）如果您想要从配置备份恢复 ADE-OS 配置，请输入此命令运算符参数。当您恢复配置备份，如果不包含此参数，Cisco ISE 仅恢复Cisco ISE 应用配置数据。

默认值

无默认行为或值。

命令模式

EXEC

使用指南

在Cisco ISE 中使用 restore 命令时，Cisco ISE 服务器会自动重新启动。

恢复数据时，加密密钥为可选。要在您未提供加密密钥的情况下，支持恢复更早的备份，您可以使用 **restore** 命令，无需加密密钥。

示例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain Lab12345 恢复操作可能需要重新启动应用服务。(Restore may require a restart of application services.) Continue? （是/否）[是]？是 正启动恢复。((yes/no) [yes] ? yes Initiating restore.) 请稍候... ISE 应用恢复正在进行。(ISE application restore is in progress.) This process could take several minutes. Please wait... Stopping ISE Application Server... Stopping ISE Monitoring & Troubleshooting Log Processor... 正停止 ISE 监控并排查日志收集器...(Stopping ISE Monitoring & Troubleshooting Log Collector...) 正停止 ISE 监控并排查警报进程...(Stopping ISE Monitoring & Troubleshooting Alert Process...) 正停止 ISE 监控并排查会话数据库...(Stopping ISE Monitoring & Troubleshooting Session Database...) Stopping ISE Database processes... 正启动 ISE 数据库进程...(Starting ISE Database processes...) 正启动 ISE 监控和排查会话数据库...(Starting ISE Monitoring & Troubleshooting Session Database...) 正启动 ISE 应用服务器...(Starting ISE Application Server...) 正启动 ISE 监控并排查警报进程...(Starting ISE Monitoring & Troubleshooting Alert Process...) 正启动 ISE 监控并排查日志收集器...(Starting ISE Monitoring & Troubleshooting Log Collector...) 正启动 ISE 监控并排查日志处理器...(Starting ISE Monitoring & Troubleshooting Log Processor...) Note: ISE Processes are initializing. 使用“show application status ise”CLI 可确认所有进程全部处于运行状态。ise/admin#
```

相关命令

	说明
backup	执行备份（Cisco ISE 和Cisco ADE OS），并将备份放在存储库中。
backup-logs	备份系统日志。
repository	输入备份配置的存储库子模式。
show repository	显示位于特定存储库上的可用备份文件。
show backup history	显示系统的备份历史记录。
show backup status	显示备份操作的状态。
show restore status	显示恢复操作的状态。

如果任何辅助节点的应用恢复后同步状态和复制状态为 不同步 *(Out of Sync)*，则必须将此辅助节点的证书重新导入主 PAN，执行手动同步。

从 GUI 恢复配置备份

可以从管理门户恢复配置备份。GUI 只列出从当前版本提取的备份。要恢复此版本之前的备份，请从 CLI 使用恢复命令。

开始之前

确保主 PAN 自动故障转移配置（如果已在部署中启用）已关闭。当恢复备份配置时，应用服务器进程会重新启动。这些服务重新启动时可能会出现延迟。由于服务重新启动时出现这种延迟，可能会触发辅助 PAN 的自动故障转移。

在配置备份期间，如果您的部署是双节点部署，请确保满足以下条件：

- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点相同，目标节点可以是独立节点或主节点。
- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点不同，目标节点必须是独立节点。

注释 可以仅在主 PAN 上恢复配置数据库备份和重新生成根 CA。不过，无法恢复注册 PAN 上的配置数据库备份。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 3 从配置备份列表中选择备份名称，然后点击 **Restore**。

步骤 4 输入在备份过程中使用的加密密钥。

步骤 5 点击恢复 **(Restore)**。

下一步做什么

如果使用Cisco ISE CA 服务，必须：

1. 重新生成整个Cisco ISE CA 根链。
2. 从主 PAN 获取Cisco ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助 PAN 可以在主 PAN 故障时用作外部 PKI 的根 CA 或从属 CA，您可将辅助 PAN 升级为主 PAN。

恢复监控数据库

恢复监控数据库的流程因部署类型不同而异。以下各节介绍如何在独立和分布式部署中恢复监控数据库。

必须使用 CLI 从Cisco ISE 的先前版本恢复按需监控数据库备份。不支持跨Cisco ISE 版本恢复定期备份。

注释 如果尝试将数据恢复到调取数据所在节点以外的节点，必须将日志记录目标设置配置为指向新节点。这可以确保监控系统日志发送到正确节点。

在独立环境中恢复监控（运行）备份

GUI 只列出从当前版本提取的备份。要恢复从早期版本获取的备份，请从 CLI 使用恢复命令。

开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

步骤 1 选择 管理 **(Administration)** > 系统 **(System)** > 备份和恢复 **(Backup and Restore)**。

步骤 2 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 系统 **(System)** > 备份和恢复 **(Backup and Restore)**。

步骤 3 从操作备份列表中选择备份的名称，然后点击恢复 **(Restore)**。

步骤 4 输入在备份过程中使用的加密密钥。

步骤 5 点击恢复。

通过管理和监控角色恢复监控备份

您可以使用管理和监控角色在分布式环境中恢复监控备份。

开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

步骤 1 如果使用的是主 PAN 和辅助 PAN，请同步 PAN。

同步 PAN 时，必须选择一个 PAN 并将其升级为活动的主 PAN。

步骤 2 在注销监控节点之前，应将监控角色分配给部署中的其他节点。

每个部署必须至少有一个正常运行的监控节点。

步骤 3 注销监控节点以进行备份。

步骤 4 将监控备份恢复到最近注销的节点。

步骤 5 向当前管理节点注册新恢复的节点。

步骤 6 将新恢复和注册的节点升级为主用监控节点。

通过监控角色恢复监控备份

只能通过监控角色恢复分布式环境中的监控备份。

开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

步骤 1 准备取消注册要恢复的节点。这是通过将监控角色分配给部署中的另一个节点来完成的。

部署必须至少有一个正常运行的监控节点。

步骤 2 取消注册要恢复的节点。

注释 请等待，直到取消注册完成后，再继续执行恢复操作。该节点必须处于独立状态，然后您才能继续执行恢复操作。

步骤 3 将监控备份恢复到最近取消注册的节点。

步骤 4 向当前管理节点注册新恢复的节点。

步骤 5 将新恢复和注册的节点升级为 PAN。

恢复历史记录

可以从**操作审核报告 (Operations Audit Report)** 中获取所有恢复操作、日志事件和状态的相关信息。

注释 但是，**操作审核报告 (Operations Audit Report)** 窗口不提供与之前的恢复操作对应的起始时间信息。

要获得故障排除信息，必须从Cisco ISE CLI 运行 **backup-logs** 命令并查看 ADE.log 文件。

在恢复操作进行过程中，所有Cisco ISE 服务都会停止。您可以使用 **show restore status** CLI 命令查看恢复操作的进度。

导出身份验证和授权策略配置

您可以将身份验证和授权策略配置导出为 XML 文件，您可以离线阅读此文件以识别任何配置错误并用于故障排除。此 XML 文件包括身份验证和授权策略规则、简单和复合策略条件、自主访问控制列表 (dACL) 和授权配置文件。您可以选择以邮件方式发送 XML 文件或将其保存在本地系统中。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup & Restore)**。

步骤 2 点击**策略导出 (Policy Export)**。

步骤 3 根据需要输入值。

步骤 4 点击**导出 (Export)**。

使用文本编辑器，例如 WordPad，查看 XML 文件的内容。

计划策略导出设置

下表对**计划策略导出 (Schedule Policy Export)** 窗口中的字段进行了说明。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)** > **策略导出 (Policy Export)**。

表 *37:* 计划策略导出设置

字段名称	使用指南
加密 (Encryption)	
加密密钥 (Encryption Key)	输入用于加密和解密导出数据的密钥。仅当您选择**使用加密密钥导出 (Export with Encryption Key)** 选项时，才会启用此字段。

字段名称	使用指南
目标 **(Destination)**	
下载文件到本地计算机 **(Download file to local computer)**	可以让您将策略导出文件下载到本地系统。
通过邮件将文件发送到 **(Email file to)**	您可输入多个邮件地址，用逗号分隔。
存储库 **(Repository)**	选择要将策略数据导出到的存储库。无法在此处输入存储库名称。只能从下拉列表选择一个可用存储库。确保在计划策略导出之前创建存储库。
立即导出 **(Export Now)**	点击此选项可将数据导出到本地计算机或作为电子邮件附件发送。您无法导出到存储库；只能计划存储库导出。
时间表 **(Schedule)**	
计划选项	选择导出计划的频率，并相应地输入其他详细信息。

在分布式环境中同步主节点和辅助节点

在分布式环境中，在 PAN 上恢复备份文件之后，主节点和辅助节点中的Cisco ISE 数据库有时不会自动同步。如果发生这种情况，可以手动强制从 PAN 完全复制到辅助 ISE 节点。只能强制从 PAN 同步到辅助节点。在同步操作过程中，无法进行任何配置更改。通过Cisco ISE，只能在同步完成后导航至其他Cisco ISE 管理员门户页面和进行配置更改。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup & Restore)**。

步骤 3 选中处于不同步复制状态的辅助 ISE 节点旁边的复选框。

步骤 4 点击**同步 (Syncup)**，等到节点与 PAN 同步。必须等到此流程完成，然后才能再次访问Cisco ISE 管理员门户。

恢复独立和分布式部署中断开的节点

此部分提供可用于恢复独立和分布式部署中断开的节点的故障排除信息。以下某些用例使用备份和恢复功能，而其他用例则使用复制功能恢复已丢失的数据。

使用现有 IP 地址和主机名恢复分布式部署中断开的节点

场景

在分布式部署中，一场自然灾害导致丢失了所有节点。在恢复之后，您想要使用现有 IP 地址和主机名。

例如，您有两个节点：N1（主策略管理节点，即主PAN）和N2（辅助策略管理节点，即辅助PAN）。可提供在时间 T1 执行的 N1 节点的备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。

假定条件

部署中的所有Cisco ISE 节点都已被破坏。已使用相同的主机名和 IP 地址对新硬件进行映像。

解决步骤

1. 您必须更换 N1 和 N2 节点。N1 和 N2 节点现在具有独立配置。
2. 用 N1 和 N2 节点的 UDI 获取许可证并将其安装在 N1 节点上。
3. 然后，您必须在更换的 N1 节点上恢复备份。恢复脚本将尝试在 N2 上同步数据，但是，N2 现已成为独立节点，所以同步失败。N1 上的数据将重置至时间 T1。
4. 您必须登录 N1 Admin 门户以删除和重新注册 N2 节点。N1 和 N2 节点都将使数据重置至时间 T1。

在分布式部署中使用新 IP 地址和主机名恢复丢失的节点

场景

在分布式部署中，一场自然灾害导致丢失了所有节点。新硬件在新位置进行了重新镜像并且需要新的 IP 地址和主机名。

例如，您有两个 ISE 节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略服务节点）。系统可以提供在时间 T1 执行的 N1 节点备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。Cisco ISE 节点在新位置被替换，新主机名为 N1A（主 PAN）和 N2A（辅助策略服务节点）。此处 N1A 和 N2A 都是独立节点。

假定条件

部署中的所有Cisco ISE 节点都已被破坏。新硬件已使用不同的主机名和 IP 地址在另一位置进行镜像。

解决步骤

1. 获取 N1 备份并在 N1A 上恢复此备份。恢复脚本将识别主机名更改和域名更改，并且将根据当前主机名在部署配置中更新主机名和域名。
2. 您必须生成新的自签证书。

3. 您必须登录到N1A 上的Cisco ISE 管理员门户。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，然后执行以下操作：

   删除旧 N2 节点。

   将新 N2A 节点注册为辅助节点。系统会将 N1A 节点的数据复制到 N2A 节点。

使用现有 IP 地址和主机名恢复独立部署中的节点

场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。已在时间 T1 执行 N1 数据库的备份。N1 节点由于物理故障宕机，必须重置映像此节点或需要使用新的硬件。必须以相同的 IP 地址和主机名恢复 N1 节点。

假定条件

此部署是独立部署，而且新硬件或重置映像的硬件具有相同的 IP 地址和主机名。

解决步骤

N1 节点在重置映像或您采用具有相同 IP 地址和主机名的新Cisco ISE 节点后开始运行时，您必须从旧 N1 节点恢复备份。您无需执行任何角色变更。

使用新 IP 地址和主机名恢复独立部署中的节点

场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。系统可以提供在时间 T1 执行的 N1 数据库备份。N1 节点由于物理故障而宕机，此节点更换为另一位置具有不同 IP 地址和主机名的新硬件。

假定条件

这是独立部署，并且所更换的硬件具有不同的 IP 地址和主机名。

解决步骤

1. 使用新硬件更换 N1 节点。此节点将处于独立状态，主机名为 N1B。
2. 您可以在 N1B 节点恢复备份。不需要更改角色。

配置回滚

问题

有时候，您可能会不小心更改配置，然后您发现所做的更改不正确。例如，您可能会错误地删除几个 NAD 或修改一些 RADIUS 属性，然后在数小时后才发现这个问题。在这种情况下，可以通过恢复您在进行更改之前所做的备份，恢复原来的配置。

可能的原因

有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略管理节点，即辅助 PAN），并且可提供 N1 节点的备份。您在 N1 节点上做了一些错误的配置更改并且想要撤消更改。

解决方案

获取在执行错误的配置更改之前所执行的 N1 节点备份。在 N1 节点上恢复此备份。恢复脚本会将数据从 N1 同步至 N2。

在分布式部署出现故障的情况下恢复主节点

场景

在多节点部署中，PAN 出现故障。

例如，您有两个Cisco ISE 节点：N1 (PAN) 和 N2（辅助管理节点）。由于硬件问题，N1 出现了故障。

假定条件

仅分布式部署中的主节点出现故障。

解决步骤

1. 登录 N2 管理员门户。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，并将 N2 配置为主节点。

   使用新硬件更换 N1 节点，重新镜像此节点并使之处于独立状态。

2. 从 N2 管理员门户，将新的 N1 节点注册为辅助节点。

   现在，N2 节点就成为您的主要节点，而 N1 节点则成为您的辅助节点。

如果您希望重新将 N1 节点设置为主要节点，请登录 N1 Admin 门户并将其设置为主要节点。N2 就自动成为辅助服务器。不会有数据丢失。

在分布式部署出现故障的情况下恢复辅助节点

场景

在多节点部署中，一个辅助节点出现故障。无需恢复。

例如，具有多个节点：N1（主 PAN）、N2（辅助 PAN）、N3（辅助策略服务节点）、N4（辅助策略服务节点）。其中一个辅助节点 N3 出现故障。

解决步骤

1. 将新的 N3A 节点重新映像到默认独立状态。
2. 登录到 N1 管理门户并删除 N3 节点。
3. 重新注册 N3A 节点。

   数据将从 N1 复制到 N3A。无需恢复。

思科 ISE 日志记录机制

Cisco ISE 提供用于审核、故障管理和故障排除的日志记录机制。日志记录机制可以帮助您识别所部署的服务中的故障情况并有效地对相应问题进行故障排除。它还以一致的方式从监控和故障排除主要节点提供日志记录输出。

您可以将Cisco ISE 配置为使用虚拟环回地址在本地系统中收集日志。要从外部收集日志，您可以配置外部系统日志服务器，这些服务器称为目标。日志分为多个预定义的类别。您可以根据各个类别的目标、严重性级别等编辑各个类别，以自定义日志记录输出。

作为最佳实践，请勿将网络设备配置为Cisco ISE 监控和故障排除 (MnT) 节点，因为这会导致一些网络访问设备 (NAD) 系统日志丢失，并使 MnT 服务器过载，进而导致加载问题。如果 NAD 系统日志配置为直接发送至 MnT，会话管理功能可能会中断。NAD 系统日志可定向到外部系统日志服务器以进行故障排除，但不应定向到 MnT。

当 ISE 消息服务在节点上失败时，将不再触发“进程已关闭”(Process Down) 警报。当 ISE 消息服务在节点上失败时，所有系统日志和“进程已关闭”(Process Down) 警报将丢失，直至消息服务在此节点上恢复。

在此情况下，管理员必须查找**队列链接错误 (Queue Link Error)** 警报，此警报将列在Cisco ISE **主页 (Home)** 窗口的**警报 (Alarms)** Dashlet 上。点击此警报，随即将打开包含**建议操作 (Suggested Actions)** 部分的新窗口。请遵循这些说明解决问题。

注释 如果将监控节点配置为网络设备的系统日志服务器，请确保日志记录源使用以下格式发送正确的网络访问服务器 (NAS) IP 地址：

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

否则，这可能会影响依赖 NAS IP 地址的功能。

配置系统日志清除设置

使用此流程可设置本地日志存储期，并可在一定时间后删除本地日志。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **本地日志设置 (Local Log Settings)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **本地日志设置 (Local Log Settings)**。

步骤 3 在 **Local Log Storage Period** 字段中，输入要将日志条目保留在配置源中的最大天数。

如果 localStore 文件夹达到 97 GB，则可能会早于配置的**本地日志存储期 (Local Log Storage Period)** 而删除日志。

步骤 4 点击 **Delete Logs Now** 可在存储期到期前的任何时间删除现有日志文件。

步骤 5 点击**保存 (Save)**。

思科 ISE 系统日志

在Cisco ISE 中，日志记录目标的位置会收集系统日志。目标是指收集和存储日志的服务器的 IP 地址。您可以在本地生成和存储日志，也可以使用 FTP 工具将日志传输至外部服务器。Cisco ISE 具有以下默认目标，在本地系统的环回地址中会动态配置这些目标：

- LogCollector - 日志收集器的系统日志默认目标。
- ProfilerRadiusProbe - 分析器 RADIUS 探测功能的默认系统日志目标。

默认情况下，在执行全新Cisco ISE 安装或升级期间会禁用 AAA 诊断子类别和系统诊断子类别日志记录目标，以减少磁盘空间。您可以为这些子类别手动配置日志记录目标，但这些子类别的本地日志记录始终处于启用状态。

您可以使用在Cisco ISE 安装结束时在本地配置的默认日志记录目标，也可以创建外部目录来存储日志。

注释 如果在分布式部署中配置了系统日志服务器，系统日志消息会直接从进行身份验证的 PSN 发送到系统日志服务器，而不是从 MnT 节点发送。

相关主题

思科 ISE 消息代码，第 252 页

配置远程系统日志收集位置

您可以使用 Web 界面创建向其发送系统日志消息的远程系统日志服务器目标。日志消息根据系统日志协议标准被发送至远程系统日志服务器目标（请参阅 RFC-3164）。系统日志协议为非安全 UDP。

当发生某一事件时，系统会生成消息。事件可能是显示状态的事件，例如当存在某个程序时显示的消息，或报警。诸如内核、电子邮件和用户级别等多个设施会生成不同类型的事件消息。事件消息与严重性级别相关，它允许管理员过滤消息并将其进行优先级排序。数字代码被分配给该设备和严重性级别。系统日志服务器为事件消息收集器并从这些设施收集事件消息。管理员可以基于其严重性级别选择将消息转发至哪个事件消息收集器。

UDP 系统日志（日志收集器）是默认远程日志记录目标。当禁用此日志记录目标时，它不会再充当日志收集器，并且系统会将其从**日志记录类别 (Logging Categories)** 窗口中删除。当启用此日志记录目标时，它会成为**日志记录类别 (Logging Categories)** 窗口中的日志收集器。

注释　对默认远程日志记录目标 **SecureSyslogCollector** 的任何更改都会导致思科 ISE 监控和故障排除日志处理器服务重新启动。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入必要的详细信息。

步骤 4 点击**保存 (Save)**。

步骤 5 转至 Remote Logging Targets 页面，然后验证新的目标是否创建。

然后，可以将日志记录目标映射到下面的每个日志记录类别。PSN 节点根据这些节点上启用的服务将相关日志发送到远程日志记录目标。

- AAA 审核
- AAA 诊断
- 记账
- 外部 MDM
- 被动 ID
- 终端安全评估和客户端调配审核
- 终端安全评估和客户端调配诊断
- Profiler

部署中的所有节点会将以下类别的日志发送到日志记录目标：

- 管理和操作审核
- 系统诊断
- 系统统计项

思科 ISE 消息代码

日志记录类别是用于说明功能、流程或用例的消息代码的捆绑包。在Cisco ISE 中，每条日志根据日志消息内容与日志记录类别所捆绑的消息代码相关联。日志记录类别帮助说明其包含的消息的内容。

日志记录类别可升级日志记录配置。每个类别具有可以根据应用要求进行设置的名称、目标和严重性级别。

Cisco ISE 为可以向其分配日志目标的 Posture、Profiler、Guest、AAA（身份验证、授权和记帐）等服务提供预定义日志记录类别。

对于日志记录类别**通过的身份验证 (Passed Authentications)**，默认情况下禁用允许本地日志记录的选项。启用此类别的本地日志记录将导致操作空间利用率高，并填写 prrt-server.log 与 iseLocalStore.log。

如果您选择为**通过的身份验证 (Passed Authentications)** 启用本地日志记录，请转至 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，从类别部分中点击**通过的身份验证 (Passed Authentications)**，然后选中**本地日志记录 (Local Logging)** 复选框。

相关主题

设置消息代码的严重性级别 ，第 252 页

设置消息代码的严重性级别

您可以设置日志严重性级别，选择存储所选类别的日志的日志记录目标。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

步骤 2 点击想要编辑的类别旁边的单选按钮，点击**编辑 (Edit)**。

步骤 3 修改必填字段值。

步骤 4 点击**保存 (Save)**。

步骤 5 转至“日志记录类别”(Logging Categories) 页面，验证对特定类别所做的配置更改。

思科 ISE 消息目录

您可以使用“消息目录”(Message Catalog) 页面查看所有可能的日志消息和说明。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。

系统将显示“日志消息目录”(Log Message Catalog) 页面，您可以在此查看所有显示在日志文件中可能的日志消息。 依次选择**导出 (Export)** 以 CSV 文件的形式导出所有系统日志消息。

您还可以参阅思科 ISE 系统日志文档，了解Cisco ISE 发送的系统日志消息的综合列表、它们的含义以及它们如何记录在本地和远程目标中。

终端调试日志收集器

要排除特定终端的问题，可以根据其 IP 地址或 MAC 地址为该特定终端下载调试日志。该特定终端专用部署中的各个节点的日志收集在一个文件中，从而帮助您快速、有效地排除问题。一次只能对一个终端运行此故障排除工具。日志文件列于 GUI 中。您可以为部署中的一个节点或所有节点的终端下载日志。

下载特定终端的调试日志

要解决与网络中的特定终端相关的问题，可以从管理员门户使用调试终端工具。或者，可以从 Authentications 页面运行此工具。从 Authentications 页面右键点击 Endpoint ID，然后点击 **Endpoint Debug**。此工具在一个文件中提供关于特定终端的所有服务的所有调试信息。

开始之前

需要准备收集其调试日志的终端的 IP 地址或 MAC 地址。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **端点调试 (Endpoint Debug)**。

步骤 2 点击 **MAC Address** 或 **IP** 单选按钮，输入终端的 MAC 或 IP 地址。

步骤 3 如果想要在指定的时间之后停止日志收集，请选中 **Automatic disable after *n* Minutes** 复选框。如果选中此复选框，必须输入 1 和 60 分钟之间的时间值。

显示以下消息：“Endpoint Debug degrades the deployment performance. Would you like to continue?”

步骤 4 点击 **Continue** 收集日志。

步骤 5 当想要手动停止日志收集时，请点击 **Stop**。

相关主题

终端调试日志收集器，第 253 页

集合过滤器

您可以配置集合过滤器来禁止将系统日志消息发送到监控节点和外部服务器。可以根据不同属性类型在策略服务节点级别执行禁止。您可以使用特定属性类型和对应的值定义多个过滤器。

在将系统日志消息发送到监控节点或外部服务器之前，Cisco ISE 会将这些值与要发送的系统日志消息中的字段进行比较。如果找到任何匹配项，则不会发送对应的消息。

配置集合过滤器

您可以根据各种属性类型配置一系列集合过滤器。建议将过滤器数限制在20个以内。您可以添加、编辑或删除集合过滤器。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **集合过滤器 (Collection Filters)**。

步骤 2 点击**添加 (Add)**。

步骤 3 从以下列表选择 **Filter Type**：

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

步骤 4 为您已选的过滤器类型选择对应的 **Value**。

步骤 5 从下拉列表中选择 **Result**。结果可能是 All、Passed 或 Failed。

步骤 6 点击**提交 (Submit)**。

相关主题

集合过滤器，第 253 页
事件抑制绕行过滤器，第 254 页

事件抑制绕行过滤器

Cisco ISE 允许您设置过滤器，以禁止向监控节点和使用收集过滤器的其他外部服务器发送某些系统日志消息。有时，您需要访问这些禁止发送的日志消息。Cisco ISE 现在为您提供根据特定属性（例如用户名）在可配置的时间内绕过事件抑制的选项。默认值为50分钟，但您可以将持续时间配置为5分钟至480分钟（8小时）。配置事件抑制绕行后，该功能会立即生效。如果您设置的持续时间结束，则绕行抑制过滤器将过期。

您可以在Cisco ISE 用户界面的 Collection Filters 页面中配置抑制绕行过滤器。使用此功能，您现在可以查看某个特定身份（用户）的所有日志并实时解决该身份遇到的问题。

您可以启用或禁用过滤器。如果您在绕行事件过滤器中配置的持续时间结束，则过滤器会自动禁用，直至您再次启用该过滤器。

Cisco ISE 在更改配置审核报告中捕获这些配置更改。此报告提供了事件抑制或绕行抑制配置人员的相关信息，以及抑制事件或绕行抑制的持续时间。

思科 ISE 报告

Cisco身份服务引擎 (ISE) 报告用于监控和故障排除功能分析趋势、和，监控系统性能和网络活动从中心位置。

Cisco ISE 从整个网络收集日志和配置数据。然后，将数据聚合到报告，供您查看和分析。Cisco ISE 提供一套标准的预定义报告，您可以直接使用，也可以自定义以满足自己的需求。

Cisco ISE 报告经过预配置，划分为不同的逻辑类别，包含有关身份验证、会话流量、设备管理、配置和管理以及故障排除的信息。

相关主题

运行并查看报告，第 256 页
导出报告，第 257 页
可用报告，第 261 页

报告过滤器

有两种报告类型：single-section 和 multi-section。Single-section 报告包含单一网格（RADIUS 身份验证报告)，multi-section报告包含多个网格（身份验证摘要报告），并以图表和表格的形式代表数据。单段报告中的过滤器下拉菜单包含**快速过滤器 (Quick Filter)** 和**自定义过滤器 (Custom Filter)**。在多段报告中，仅可以指定高级过滤器。

多段报告可能包含需要您输入的一个或多个必填自定义过滤器。例如，当点击“运行状况摘要”(Health Summary) 报告（**操作 (Operations) > 报告 (Reports) > 诊断 (Diagnostics)** 页面）时，会显示两个必填自定义过滤器：服务器 (Server) 和时间范围 (Time Range)。您必须为这两个过滤器指定操作符命令、服务器名称和所需值，然后点击**开始 (Go)** 生成报告。您可以点击加号 (+) 添加新的高级过滤器。您仅可将 multi-section 导出为 PDF 格式。您不能计划在特定时间或时间间隔运行和重新运行Cisco ISE multi-section 报告。

注释 当点击报告时，默认生成当前日期的数据。但是，除时间范围外，某些多段报告需要用户强制输入。

默认情况下，快速过滤器显示为 single-section 报告的第一行。字段可能是一个包含可选择搜索条件的下拉列表，也可以是一个文本框。

高级过滤器包含一个外部标准，其中含有一个或多个内部标准。外部标准用于指定搜索是否应满足所有或任何指定的内部标准。内部标准包含一个或多个条件，用于指定类别（终端 ID、身份组）、方法（操作符命令，例如包含、不包含)和该条件的时间范围。

使用**快速过滤器 (Quick Filter)** 时，可以从**记录于 (Logged At)** 下拉列表中选择日期或时间，以生成过去 30 天或以内记录的数据集的报告。如果要为 30 天前的日期或时间生成报告，请使用**高级过滤器 (Advanced Filter)**，在下拉列表中**自定义 (Custom)** 选项的**从 (From)** 字段和**到 (To)** 字段中设置所需的时间范围。

创建快速过滤器条件

本节介绍如何创建快速过滤器条件。您只能为单段报告创建快速过滤器条件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** 并点击所需的报告。

步骤 2 从**设置 (Settings)** 下拉列表中选择所需字段。

步骤 3 在必填字段中，您可以从下拉列表中选择或者键入特定字符以过滤数据。搜索使用 Contains 运算符命令。例如，要过滤以“K”开头的文本，请输入K，或者要过滤任意位置包含“geo”的文本，请输入geo。您还可以使用星号 (*)，例如，以 *abc 开头并以 *def 结尾的正则表达式。

快速过滤器使用以下条件：包含、开头为、结尾为、开头为或结尾为，以及使用 OR 运算符的多个值。

步骤 4 按 **Enter** 键。

创建高级过滤条件

本节介绍如何创建高级过滤条件。您可以为单段和多段报告创建高级过滤器。单段报告中的过滤器下拉菜单包含**快速过滤器 (Quick Filter)** 和**自定义过滤器 (Custom Filter)**。在多段报告中，仅可以指定高级过滤器。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** 并点击所需的报告。

步骤 2 在**过滤器 (Filters)** 部分，从**匹配 (Match)** 下拉列表中选择一个选项。

a) 选择**所有 (All)** 以匹配所有指定的条件。

b) 选择**任意 (Any)** 以匹配任意一个指定的条件。

步骤 3 从**时间范围 (Time Range)** 下拉列表中选择所需类别。

步骤 4 从**运算符命令 (Operator Commands)** 下拉列表中，选择所需的命令。例如，可以过滤以特定字符开头的文本（使用“开头为”）或任意位置存在特定字符的文本（使用“包含”）。或者，您可以选择记录时间 (Logged Time) 和对应的自定义 (Custom) 选项并在日历中指定开始和结束的日期和时间以过滤数据。

步骤 5 从**时间范围 (Time Range)** 下拉列表中选择所需选项。

步骤 6 点击 **Go**（**前往**）。

您可以保存已过滤的报告并从**过滤器 (Filters)** 下拉列表中检索该报告以供将来参考。

运行并查看报告

本节描述如何使用报告视图运行、查看并导航报告。默认情况下，当您点击报告时，可生成最近七天的数据。每个报告每页显示 500 行数据。您可以指定报告中所显示数据的时间增量。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **ISE 报告 (ISE Reports)**。

还可以导航至每个工作中心下的**报告 (Reports)** 链接，以查看特定于此工作中心的报告集。

步骤 2 点击 **" 可用报告**页上的类别的报告。

步骤 3 选择一个或多个过滤器以运行报告。每个报告都具有不同的可用过滤器，某些过滤器为必选而某些则为可选。

步骤 4 为过滤器输入适当的值。

步骤 5 点击 **Go**（前往）。

相关主题

导出报告，第 257 页
可用报告，第 261 页

报告导航

您可以从报告输出中获得详细信息。例如，如果您为五个月的一个时间段生成了报告，其图表将按月列出报告的汇总数据。

您可以从表格中点击特定值以查看与此特定字段相关的其他报告。例如，身份验证摘要报告将显示用户或用户组的失败计数。当您点击失败计数时，系统就会打开该特定失败计数的身份验证摘要报告。

导出报告

仅可以导出以下报告的 PDF 文件格式：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要

注释 RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。

- 访客赞助商摘要
- 终端配置文件修改
- 网络设备会话状态

步骤 1 如“运行和查看报告”(Running and Viewing Reports) 一节所述运行报告。

步骤 2 点击报告摘要页面右上角的**导出到 (Export To)**。

步骤 3 选择以下选项之一：

- 存储库 (CSV)：将报告以 CSV 文件格式导出到存储库
- 本地 (CSV)：将报告以 CSV 文件格式导出到本地磁盘
- 本地 (PDF)：将报告以 PDF 文件格式导出到本地磁盘

注释 当选择本地 CSV 或 PDF 选项时，仅会导出前 500 条记录。您可以使用存储库 CSV 选项导出所有记录。

安排和保存思科 ISE 报告

可以自定义报告并将更改另存为新报告，或在报告摘要页面右上角的**我的报告 (My Reports)** 中恢复默认报告设置。

还可以自定义和安排Cisco ISE 报告，以在特定时间或时间间隔运行和重新运行。对于生成的报告，还可以发送和接收电子邮件通知。

以**每小时 (Hourly)** 频率安排报告时，可以让报告运行多天，但时间段不能跨越两天。

例如，在安排从 2019 年 5 月 4 日到 2019 年 5 月 8 日的每小时报告时，可以将时间间隔设置为每天上午 6:00 至晚上 11:00，但不能设置为某日下午 6:00 到次日上午 11:00。Cisco ISE 会显示错误消息，说明在后一种情况下的时间范围无效。

注释 如果外部管理员（例如 Active Directory 管理员）在未填写电子邮件 ID 字段的情况下创建计划报告，则不会发送任何电子邮件通知。

无法安排以下报告：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要
- 访客赞助商摘要
- 终端配置文件更改
- 网络设备会话状态

注释 只能从 PAN 保存或安排（自定义）思科 ISE 报告。

注释 如果主 MnT 关闭，则辅助 MnT 将执行计划的报告作业。计划的报告作业在主 MnT 和辅助 MnT 上运行。在辅助 MnT 上，在运行导出作业之前，它会尝试对主 MnT 执行 ping 操作。如果 ping 操作失败，则它将仅运行导出作业，否则将跳过导出作业。

步骤 1 如“运行和查看报告”一节所述运行报告。

步骤 2 点击报告摘要页面右上角的**我的报告 (My Reports)**。

步骤 3 在对话框中输入所需的详细信息。

步骤 4 点击**另存为新报告 (Save as New)**。

当返回到保存的报告时，所有过滤器选项在默认情况下都处于选中状态。取消选中不想要使用的过滤器。

还可以从**我的报告 (My Reports)** 类别中删除已保存的报告。

思科 ISE 活动 RADIUS 会话

Cisco ISE 为实时会话提供动态的授权更改 (CoA) 功能，通过此功能，可以动态地控制活动 RADIUS 会话。可以将重新验证或断开请求发送到网络接入设备 (NAD) 以执行以下任务：

- 排除与身份验证相关的问题 - 可以使用 Session reauthentication 选项继续尝试重新验证。但是，不能使用此选项来限制访问。要限制访问，请使用 shutdown 选项。
- 阻止有问题主机 - 可以将 Session termination 与 port shutdown 选项一起使用，以阻止在网络上发送大量流量的被感染主机。但是，RADIUS 协议当前不支持重新启用已关闭端口的方法。
- 强制终端重新获取 IP 地址 - 可以将 Session termination 与 port bounce 选项一起使用，以便没有请求方或客户端的终端在 VLAN 更改之后生成 DHCP 请求。
- 将更新的授权策略推送到终端 - 可以使用 Session reauthentication 选项执行更新的策略配置，例如，根据管理员的决定更改现有会话的授权策略。例如，如果启用终端安全评估验证，当终端初次获得访问权限时，通常会被隔离。已知终端的身份和终端安全评估之后，可将 Session reauthentication 命令发送到终端，以便该终端根据其终端安全评估获取实际授权策略。

为了让设备读懂 CoA 命令，应适当地配置选项，这一点非常重要。

为了使 CoA 正常工作，必须为每台需要动态授权更改的设备配置共享密钥。Cisco ISE 使用共享密钥配置向设备请求访问权限并向其发出 CoA 命令。

注释 在此思科 ISE 版本中，可以显示的经过身份验证的最大活动终端会话数限制为 100,000。

相关主题

更改 RADIUS 会话的授权，第 260 页

更改 RADIUS 会话的授权

您网络中的某些网络接入设备可能不会在重新加载后发送 Accounting Stop 或 Accounting Off 数据包。因此，您可能会在 Session Directory 报告中找到两个会话，其中一个已过期。

要动态地更改活动 RADIUS 会话的授权或断开活动 RADIUS 会话的连接，请务必选择最近的会话。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS 实时日志 (RADIUS Livelog)**。

步骤 2 将视图切换到 **Show Live Session**。

步骤 3 点击要发出 CoA 的 RADIUS 会话的 CoA 链接，然后选择以下其中一个选项：

- **SAnet Session Query** - 使用此选项查询有关支持 SAnet 的设备的信息。
- **Session reauthentication** - 重新对会话进行身份验证。如果您为在支持 COA 的 ASA 设备上建立的会话选择此选项，则此操作将会调用 Session Policy Push CoA。
- **Session reauthentication with last** - 为此会话使用最后一个成功身份验证方法。
- **Session reauthentication with rerun** - 从头开始运行配置的身份验证方法。

  注释 思科 IOS 软件中当前不支持**使用上一个方法进行会话重新身份验证 (Session reauthentication with last)** 和**通过重新运行进行会话重新身份验证 (Session reauthentication with rerun)** 选项。

- **Session termination** - 仅终止会话。交换机会在不同的会话中重新对客户端进行身份验证。
- **Session termination with port bounce** - 终止会话并重新启动报告。
- **Session termination with port shutdown** - 终止会话并关闭报告。

步骤 4 点击**运行 (Run)** 使用选定的 reauthenticate 或 terminate 选项发出 CoA。

如果您的 CoA 失败，可能是由于以下其中一个原因引起：

- 设备不支持 CoA。
- 身份或授权策略已发生更改。
- 共享密钥不匹配。

可用报告

下表按照报告类别分组列出系统预配置的报告。此外还提供对报告功能和日志记录类别的说明。

要为日志记录类别生成系统日志，请将其**日志严重性级别 (Log Severity Level)** 设置为**信息 (Info)**：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。
- 点击必须为其生成系统日志的日志记录类别。
- 在**日志严重性级别 (Log Severity Level)** 字段中，从下拉菜单中选择**信息 (Info)**。
- 点击**保存 (Save)**。

注释 在Cisco ISE 版本 2.6 及更高版本中，使用 IPv6 地址的用户将在审核报告中记录以下事件：登录/注销、密码更改和操作更改。在管理员登录、用户更改密码审核和操作审核报告中，您现在可以按IPv4 和 IPv6 记录过滤日志。

报告名称	说明	日志记录类别
审计		
自适应网络控制审计	自适应网络控制审计报告以 RADIUS 计费为基础。它可以显示每个终端所有网络会话的历史报告数据。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“已通过的身份验证”(Passed Authentications) 和“RADIUS 记账”(RADIUS Accounting)。
Administrator Logins	管理员登录报告提供关于所有基于 GUI 的管理员登录事件以及成功的 CLI 登录事件的信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“管理和操作审核”(Administrative and Operational audit)。

报告名称	说明	日志记录类别
更改配置审核	更改配置审核报告提供关于指定时间内配置更改的详细信息。如果需要对某个功能进行故障排除，此报告可以帮助您确定是不是最近的配置更改导致了问题。	
数据清除审核	数据清除审核报告记录何时清除了日志记录数据。 此报告会反映两个数据清除来源。 每天凌晨 4 点，Cisco ISE 会检查是否有任何日志记录文件符合您在“管理”(Administration) > “维护”(Maintenance) > “数据清除”(Data Purging) 页面设置的条件。如有，Cisco ISE 会删除这些文件并将其记录于此报告中。此外，Cisco ISE 继续为日志文件保留最多 80% 的已用存储空间。Cisco ISE 每小时都会检查此百分比并删除最早的数据，直到再次达到此 80% 的阈值。这些信息也会记录于此报告中。 如果磁盘空间利用率高，系统会在达到 80% 阈值时显示一条警报消息，说明 ISE 监控节点即将超过最大分配量 (ISE Monitor node(s) is about to exceed the maximum amount allocated is displayed at the 80 percent threshold)。随后，系统会在达到 90% 阈值显示一条警报消息，说明 ISE 监控节点已超过最大分配量 (ISE Monitor node(s) has exceeded the maximum amount allocated)。	-

报告名称	说明	日志记录类别
终端清除活动	用户可以通过终端清除活动报告查看终端清除活动的历史记录。此报告要求启用“分析器”(Profiler) 日志记录类别。该类别在默认情况下已启用。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“分析器”(Profiler)。
内部管理员摘要	您可以通过内部管理员摘要报告验证管理员用户的注册情况。您还可以从此报告访问管理员登录和更改配置审核报告，从而可以查看每个管理员的此类详细信息。	-
操作审核	操作审核报告提供关于任何操作变更的详细信息，例如运行备份、注册Cisco ISE 节点或重新启动应用。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“管理和操作审核”(Administrative and Operational audit)。
pxGrid Administrator Audit	pxGrid 管理员审核报告提供关于 pxGrid 管理操作的详细信息，例如在主 PAN 上注册客户端、注销客户端、批准客户端、创建主题、删除主题、添加发布者-订用者，以及删除发布者-订用者。 每条记录都会注明在节点上执行相应操作的管理员名称。 您可以根据管理员和消息条件过滤 pxGrid 管理员审核报告。	-
Secure Communications Audit	安全通信审核报告提供关于Cisco ISE 管理员 CLI 中的安全性相关事件的审核详细信息，该管理员 CLI 包括：身份验证失败、可能的入侵尝试、SSH 登录、失效密码、SSH 注销和无效用户帐户等。	-

报告名称	说明	日志记录类别
用户更改密码审核	用户更改密码审核报告显示关于员工密码更改的验证信息。	管理和操作审核
Trustsec 审核	Trustsec 审核日志包含： • 管理（创建、重命名、更新和删除）Trustsec 组件。 • 将 SGACL 和 SGT 部署到启用 Trustsec 的 NAD • Trustsec 会话。 如果Cisco ISE 与Cisco DNA 中心集成，并且 SD 访问由Cisco DNA中心管理，则此日志为空。	-
设备管理		
身份验证摘要	TACACS 身份验证摘要报告会详细说明最常见的身份验证以及身份验证失败的原因。	—
TACACS 计费	TACACS 计费报告为设备会话提供计费的详细信息。它显示用户和设备的生成和日志记录时间的相关信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“TACACS 记账”(TACACS Accounting)。
不同失败原因的前N个身份验证	“不同失败原因的前N个身份验证”(Top N Authentication by Failure Reason) 报告根据所选参数显示特定期间内不同失败原因的身份验证总数。	—
不同网络设备的前N个身份验证	“不同网络设备的前N个身份验证”(Top N Authentication by Network Device) 报告根据所选参数按网络设备名称显示特定期间内已通过和已失败的身份验证数量。	—

报告名称	说明	日志记录类别
不同用户的前 N 个身份验证	“不同用户的前 N 个身份验证”(Top N Authentication by User) 报告根据所选参数按用户名显示特定期间内已通过和失败的身份验证数量。	—
诊断		
AAA 诊断	AAA 诊断报告提供Cisco ISE 和用户之间所有网络会话的详细信息。如果用户无法访问网络，您可查看此报告以确定其动态并明确问题是仅限于特定用户还是普遍存在。 **注释** 有时，如果正在进行用户身份验证，ISE会以静默方式丢弃终端的计费停止 (Accounting Stop) 请求。但是，一旦用户身份验证完成，ISE将开始确认所有计费请求。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择这些日志记录类别：“政策诊断”(Policy Diagnostics)、“身份存储区诊断”(Identity Stores Diagnostics)、“身份验证流程诊断”(Authentication Flow Diagnostics） 和“RADIUS 诊断”(RADIUS Diagnostics)。
AD 连接器操作	AD Connector Operations 报告提供关于 AD 连接器执行的操作的日志，例如Cisco ISE服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理等。 如果遇到某些 AD 故障，您可以在此报告中查看详细信息以确定可能的原因。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“AD 连接器”(AD Connector)。
Endpoint Profile Changes	终端顶级授权（MAC 地址）报告显示Cisco ISE 已授权每个终端 MAC 地址访问网络的次数。	已通过身份验证、失败尝试

报告名称	说明	日志记录类别
运行状况摘要	运行状况摘要报告提供与控制面板类似的详细信息。但是，控制面板仅显示前 24 小时的数据，而您可以使用此报告查看更久之前的历史数据。 您可以评估这些数据，以查看数据中的一致模式。例如，您可能预计当大多数员工都开始工作时，CPU 使用率较高。如果您发现这些趋势存在不一致性，您可以确定潜在的问题。 CPU 使用率表列出不同Cisco ISE功能的 CPU 使用率百分比。此表中提供 **show cpu usage** CLI 命令的输出，您可以将这些值与部署中的问题相关联，从而识别可能的原因。	—
ISE 计数器	ISE 计数器报告列出各种属性的阈值。这些不同的属性值按照不同的时间间隔收集，而数据以表格格式呈现；一个间隔为 5 分钟，另一个间隔大于 5 分钟。 您可以评估这些数据以查看趋势，如果发现高于阈值的值，则可以将此信息与部署中的问题相关联，以确定可能的原因。 默认情况下，Cisco ISE 会收集这些属性值。您可以在Cisco ISE CLI 中使用 **application configure ise** 命令禁用此数据收集操作。选择选项 14 可启用或禁用计数器属性收集。	—
关键性能指标	关键性能指标报告提供有关连接到部署的终端数量以及每个PSN每小时处理的RADIUS请求数量的统计信息。此报告列出服务器上的平均负载、每个请求的平均延迟和每秒的平均事务数。	-

报告名称	说明	日志记录类别
配置有误的 NAS	配置有误的 NAS 报告提供关于记帐频率不正确（通常指频繁地发送记帐信息）的 NAD 的信息。如果您已采取纠正措施并修复配置错误的 NAD，此报告会显示修复确认信息。 **注释** 应启用 RADIUS 抑制才能运行此报告。	-
配置有误的请求方	配置有误的请求方报告提供配置错误的请求方的列表以及对具体请求方执行的失败尝试的统计信息。如果您已采取纠正措施并修复配置错误的请求方，此报告会显示修复确认信息。 **注释** 应启用 RADIUS 抑制才能运行此报告。	-
网络设备会话状态	您可以通过网络设备会话状态摘要报告显示交换机配置，而无需直接登录交换机。 Cisco ISE 使用 SNMP 查询功能获取这些详细信息，而且要求用 SNMP v1/v2c 配置您的网络设备。 如果用户遇到网络问题，此报告可帮助您识别问题是否与交换机配置相关，而与Cisco ISE无关。	-
OCSP 监控	OCSP 监控报告指明在线证书状态协议 (OCSP) 服务的状态。它可以确定Cisco ISE能否成功连接证书服务器并提供证书状态审核，还提供对Cisco ISE执行的所有OCSP证书验证操作的汇总。此外，它可从OCSP服务器检索关于正常和已吊销主要证书与辅助证书的信息。Cisco ISE缓存响应并利用响应生成后续OCSP 监控报告。如果缓存已清除，它将从 OCSP 服务器检索信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“系统诊断”(System Diagnostics)。

报告名称	说明	日志记录类别
RADIUS 错误	您可以通过RADIUS错误报告检查已丢失的RADIUS请求（从未知网络访问设备丢弃的身份验证/记账请求）、EAP连接超时和未知 NAD。 **注释** 您只能查看过去 5 天的报告。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“失败尝试”(Failed Attempts)。
系统诊断	系统诊断报告提供关于Cisco ISE节点的状态的详细信息。如果Cisco ISE节点无法注册，您可查看此报告以对问题进行故障排除。 此报告要求首先启用几个诊断日志记录类别。收集这些日志可能会对Cisco ISE 性能产生负面影响。因此，默认情况下未启用这些类别。如果您启用这些类别，应使其启用持续时间刚好满足收集数据的要求即可。否则，30分钟后系统会自动禁用这些类别。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)** 然后选择以下日志记录类别：“内部操作诊断”(Internal Operations Diagnostics)、“分布式管理”(Distributed Management)、“管理员身份验证”(Administrator Authentication)和“授权”(Authorization)。
Endpoints and Users		
身份验证摘要	身份验证摘要报告以RADIUS身份验证为基础。您可以通过此报告确定最常见的身份验证以及任何身份验证失败的原因。例如，如果一个Cisco ISE服务器处理的身份验证明显多于其他服务器，您可能需要重新将用户分配给其他Cisco ISE服务器，以实现更好的负载均衡。 **注释** 由于身份验证摘要报告或控制面板要收集和显示与失败或成功的身份验证对应的最新数据，所以报告的内容会延迟几分钟才显示。	-
无代理终端安全评估	列出运行无代理终端安全评估的所有终端。	

报告名称	说明	日志记录类别
客户端调配	客户端调配报告显示应用于特定终端的客户端调配代理。您可以使用此报告验证应用于每个终端的策略以确定是否正确调配了终端。 注释 如果终端不与 ISE 连接（未建立会话）或对会话使用网络地址转换 (NAT) 地址，则终端的MAC地址不会显示在“终端ID”(Endpoint ID) 列中。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“终端安全评估和客户端调配审核”(Posture and Client Provisioning Audit) 以及“终端安全评估和客户端调配诊断”(Posture and Client Provisioning Diagnostics)。
当前活动会话	您可以通过当前活动会话报告导出包含关于指定时间内哪些用户正在访问网络的详细信息的报告。 如果用户无法访问网络，您可以查看会话是否经过了身份验证或是否中断，或会话是否存在其他问题。	-
终端脚本调配摘要	**终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)** 窗口显示过去 30 天内通过终端脚本向导运行的作业的详细信息。 有关终端脚本向导和此报告内容的详细信息，请参阅适用于 Windows 和 Macintosh 终端的终端脚本向导，第 679 页。	—
外部移动设备管理	外部移动设备管理报告提供关于 Cisco ISE 与外部移动设备管理 (MDM) 服务器之间的集成的详细信息。 您可以使用此报告查看哪些终端经过了MDM服务器调配，而无需直接登录MDM服务器。此报告还显示注册和MDM合规状态等信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“MDM”。

报告名称	说明	日志记录类别
被动 ID	您可以通过被动 ID (Passive ID) 报告监控与域控制器的 WMI 连接的状态并收集与之相关的统计信息（例如接收的通知数量、每秒钟用户登录/注销的次数等）。 注释 通过此方法进行身份验证的会话在报告中没有身份验证详细信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“身份映射”(Identity Mapping)。
手动证书调配	手动证书调配报告列出所有通过证书调配门户手动调配的证书。	-
按条件进行终端安全评估	通过按条件进行终端安全评估报告，您可以查看 ISE 中配置的基于终端安全评估策略条件的记录，从而对最新安全设置和应用在客户端计算机上的可用性进行验证。	-
按终端进行终端安全评估	“不同终端的终端安全评估”报告提供终端的详细信息，如时间、状态和 PRA 操作。您可以点击**详细信息 (Details)** 以查看终端的更多信息。 注释 “不同终端的终端安全评估”报告不提供终端应用和硬件属性的终端安全评估策略详细信息。您只能在“情景可视性”(Context Visibility) 页面中查看这些信息。	-

报告名称	说明	日志记录类别
已分析终端总结	已分析终端总结报告提供关于正在访问网络的终端的分析详细信息。 注释 对于不注册会话时间的终端（例如思科 IP 电话），“终端会话时间”(Endpoint session time) 字段中会显示“不适用”(Not Applicable)。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“分析器”(Profiler)。
RADIUS 计费	RADIUS 计费报告指出用户访问网络持续的时间。如果用户失去了网络连接，您可以使用此报告确定是不是Cisco ISE 导致的网络连接问题。 注释 如果 RADIUS 记账临时更新包含有关给定会话的 IPv4 或 IPv6 地址更改的信息，则 RADIUS 记账报告中会包含 Radius 记账临时更新。	
RADIUS 身份验证	您可以通过 RADIUS 身份验证报告查看身份验证失败和成功的历史记录。如果用户无法访问网络，您可以在此报告中查看详细信息以确定可能的原因。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择以下日志记录类别：“已通过身份验证”(Passed Authentications) 和“失败尝试”(Failed Attempts)。
注册终端	注册终端报告显示员工注册的所有个人设备。	-
拒绝的终端	“拒绝的终端”(Rejected Endpoints) 报告列出了员工注册的所有被拒绝或放行的个人设备。	—

报告名称	说明	日志记录类别
请求方调配	请求方调配报告提供关于调配至员工个人设备的请求方的详细信息。	终端安全评估和客户端调配审核
按终端查看顶级授权	终端顶级授权（MAC 地址）报告显示Cisco ISE 已授权每个终端 MAC 地址访问网络的次数。	已通过身份验证、失败尝试
按用户查看顶级授权	按用户查看顶级授权报告显示 Cisco ISE 已授权每个用户访问网络的次数。	已通过身份验证、失败尝试
不同访问服务的前N个身份验证	“不同访问服务的前N个身份验证”(Top N Authentication by Access Service) 报告根据所选参数按特定时间段的访问服务类型显示已通过和失败的身份验证数量。	—
不同失败原因的前N个身份验证	“不同失败原因的前N个身份验证”(Top N Authentication by Failure Reason) 报告根据所选参数显示特定期间内不同失败原因的身份验证总数。	—
不同网络设备的前N个身份验证	“不同网络设备的前N个身份验证”(Top N Authentication by Network Device) 报告根据所选参数按网络设备名称显示特定期间内已通过和已失败的身份验证数量。	—
不同用户的前 N 个身份验证	“不同用户的前 N 个身份验证”(Top N Authentication by User) 报告根据所选参数按用户名显示特定期间内已通过和失败的身份验证数量。	—
Guest		

报告名称	说明	日志记录类别
AUP Acceptance Status	AUP Acceptance Status 报告提供从所有 Guest 门户接受的 AUP 的详细信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“访客”(Guest)。
访客计费	访客计费报告是RADIUS计费报告的一部分。此报告中显示分配至激活访客或访客身份组的所有用户。	-
主访客报告	主访客报告综合各个访客接入报告的数据，并且允许您从不同报告来源导出数据。主访客报告还提供关于访客用户正在访问的网站的详细信息。您可以使用此报告进行安全审核，以证明访客用户何时访问了网络以及他们在网络上执行了什么活动。 您还必须在用于访客流量的网络访问设备 (NAD) 上启用 HTTP 检查。这些信息由 NAD 发送回 Cisco ISE。 要检查客户端何时达到最大并行会话限制数，从管理员门户选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)** 并执行以下操作： **1.** 将“身份验证流量诊断”(Authentication Flow Diagnostics) 日志类别的日志级别从警告提高到信息。 **2.** 从 AAA 诊断“日志记录类别”下，将 LogCollector 目标从可用的更改为已选的。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“已通过的身份验证”(Passed Authentications)。

报告名称	说明	日志记录类别
我的设备登录和审核	我的设备登录和审核报告提供关于用户通过设备在“我的设备门户”(My Devices Portal) 中执行的登录活动和操作的详细信息。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“我的设备”(My Devices)。
Sponsor Login and Audit	Sponsor Login and Audit 报告提供关于访客用户的登录、添加、删除、启用、暂停和更新操作以及发起人在发起人门户上的登录活动的详细信息。 如果批量添加访客用户，则“访客用户”(Guest Users) 列下会显示这些用户。此列默认处于隐藏状态。在导出时，这些批量用户也会显示于导出的文件上。	在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“访客”(Guest)。
SXP		
SXP 绑定	SXP 绑定报告提供与通过 SXP 连接进行交换的 IP-SGT 绑定有关的信息。	-
SXP 连接	您可以使用此报告来监控 SXP 连接的状态并收集与之相关的信息，例如对等 IP、SXP 节点 IP、VPN 名称、SXP 模式等。	—
TrustSec		

报告名称	说明	日志记录类别
RBACL 丢包摘要	RBACL 丢包摘要报告专用于 TrustSec 功能，只有在具备Cisco ISE 高级许可证的情况下才可用。 此报告还要求您将网络设备配置为向Cisco ISE 发送关于丢包事件的 NetFlow 事件。 如果用户违反特定策略或访问权限，系统会丢弃数据包并在此报告中指明。 **注释** RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。	-
按用户前 N 个 RBACL 丢包	按用户前 N 个 RBACL 丢包报告专用于 TrustSec 功能，只有在具备Cisco ISE 高级许可证的情况下才可用。 此报告还要求您将网络设备配置为向Cisco ISE 发送关于丢包事件的 NetFlow 事件。 此报告显示特定用户违反策略的情况（依据数据包丢弃情况）。 **注释** RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。	—
TrustSec ACI	此报告列出与 EEPG、终端和 APIC 子网配置同步的 SGT 和 SXP 映射。只有当 TrustSec APIC 集成功能启用时，这些细节才会显示。	-

报告名称	说明	日志记录类别
TrustSec 部署验证		-

报告名称	说明	日志记录类别
	您可以使用此报告验证是否在所有网络设备上部署了最新的 TrustSec 策略，或者在Cisco ISE 中配置的策略与网络设备之间是否存在任何差异。 点击**详细信息 (Details)** 图标以查看验证过程的结果。您可以查看以下详细信息： • 验证过程开始和完成的时间 • 是否在网络设备上成功部署了最新的 TrustSec 策略。您还可以查看部署了最新 TrustSec 策略的网络设备的名称和 IP 地址。 • 在Cisco ISE 中配置的策略与网络设备之间是否存在任何差异。它显示每个策略差异的设备名称、IP地址和相应的错误消息。 您可以在**警报 (Alarms)** Dashlet（在**工作中心 (Work Centers) > TrustSec > 控制板 (Dashboard)** 和**主页 (Home) > 摘要 (Summary)** 下）中查看 TrustSec 部署验证警报。 **注释** • 报告所需的时间取决于部署中的网络设备和 TrustSec 组数量。 • “TrustSec 部署验证”(TrustSec Deployment Verification) 报告中的错误消息长度当前限制为 480 个字符。超过 480 个字符的错误消息将被截断，并且报告中仅显示前 480 个字符。	

报告名称	说明	日志记录类别
Trustsec 策略下载	此报告列出网络设备发出的策略 (SGT/SGACL) 下载请求和 ISE 发出的详细信息。如果启用工作流模式，对于生产或暂存表，可对请求进行过滤。	要查看此报告，必须执行以下操作： 1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。 2. 选择 **AAA 诊断 (AAA Diagnostics)** > **RADIUS 诊断 (RADIUS Diagnostics)**。 3. 将 RADIUS 诊断的日志严重性级别设置为“调试”(DEBUG)。
以威胁防护为中心的 NAC 服务		
适配器状态	适配器状态报告显示威胁和漏洞适配器的状态。	-
COA 事件	当收到某个终端的漏洞事件时，Cisco ISE 对该终端触发 CoA。CoA 事件报告显示这些 CoA 事件的状态。同时显示这些终端的新旧授权规则和配置文件详细信息。	-
威胁事件	“威胁事件”(Threat Events) 报告提供Cisco ISE 从已配置的各种适配器接收的所有威胁事件的列表。	-
漏洞评估	漏洞评估报告为您的终端提供正在进行的评估的信息。您可以查看此报告以确认评估是否以配置策略为基础正在进行。	-

RADIUS 实时日志

下表介绍“实时日志”(Live logs) 窗口中的字段，其中显示最近的 RADIUS 身份验证。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live Logs)**。只能在主 PAN 中查看 RADIUS 实时日志。

表 *38: RADIUS* 实时日志

字段名称	说明描述
时间 (Time)	显示监控和故障排除收集代理接收日志的时间。此列为必选项，无法取消选择。
状态 (Status)	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 (Details)	点击“详细信息”(Details) 列下的图标可在新浏览器窗口中打开**身份验证详细报告 (Authentication Detail Report)**。此报告提供有关身份验证和相关属性以及身份验证流程的信息。在**身份验证详细信息 (Authentication Details)** 框中，**响应时间 (Response Time)** 是Cisco ISE 处理身份验证流程所需的总时间。例如，如果身份验证包含三个往返消息，初始消息花费 300 毫秒，下一条消息花费 150 毫秒，最后一条消息花费 100 毫秒，则**响应时间 (Response Time)** 为 300 + 150 + 100 = 550 毫秒。 注释 您无法查看活动时间超过 48 小时的终端的详细信息。当点击活动时间超过 48 小时的终端的**详细信息 (Details)** 图标时，可能会看到一个包含以下消息的页面：此记录无可用数据。(No Data available for this record.) 数据可能已清除或此会话记录的身份验证发生在一周之前。(Either the data is purged or authentication for this session record happened a week ago.) 或者，如果这是“PassiveID”或“PassiveID 可视性”(PassiveID Visibility) 会话，则不会有 ISE 身份验证详细信息，只有会话。(Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.)

字段名称	说明描述
重复次数 (Repeat Count)	显示过去 24 小时内身份验证请求的重复次数，它们在身份、网络设备和授权方面没有任何变化。
身份 (Identity)	显示与身份验证关联的已登录用户名。 如果用户名不存在于任何 ID 存储区中，则显示为 INVALID。如果身份验证由于任何其他原因而失败，则显示为 USERNAME。 **注释** 这仅适用于用户。这不适用于 MAC 地址。 为了帮助进行调试，可以强制Cisco ISE 显示无效的用户名。为此，请选中位于以下路径下方的**披露无效用户名 (Disclose Invalid Usernames)** 复选框： **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全设置 (Security Settings)**。您还可以将**披露无效用户名 (Disclose Invalid Usernames)** 选项配置为超时，这样就不必手动将其关闭。
终端 ID (Endpoint ID)	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
终端配置文件 (Endpoint Profile)	显示所分析的终端的类型，例如分析为 iPhone、Android、MacBook、Xbox 等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
网络设备 (Network Device)	显示网络访问设备的 IP 地址。
设备端口 (Device Port)	显示终端连接的端口号。
身份组 (Identity Group)	显示分配给生成了日志的用户或终端的身份组。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
服务器 (Server)	指示生成日志的策略服务。
MDM 服务器名称 (MDM Server Name)	显示 MDM 服务器的名称。

字段名称	说明描述
事件 (Event)	显示事件状态。
故障原因 (Failure Reason)	如果身份验证失败，显示失败的详细原因。
身份验证方法 (Auth Method)	显示 RADIUS 协议（例如 Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)、IEEE 802.1x 或 dot1X 等）使用的身份验证方法。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
安全组 (Security Group)	显示由身份验证日志标识的组。
会话 ID (Session ID)	显示会话 ID。

注释 在 **RADIUS 实时日志 (RADIUS Live Logs)** 和 **TACACS+ 实时日志 (TACACS+ Live Logs)** 窗口中，系统会为每个策略授权规则的第一个属性显示一个“已查询 PIP”(Queried PIP) 条目。如果授权规则中的所有属性都与已为之前的规则查询的字典相关，则不会显示其他“已查询 PIP”(Queried PIP) 条目。

您可以在 RADIUS **实时日志 (Live Logs)** 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

身份验证延迟

身份验证延迟是 RADIUS 身份验证程序自身份验证程序启动后的平均响应时间。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**控制板** > **系统摘要 (System Summary)** Dashlet。 查看 Cisco ISE 身份验证延迟。

可以从下拉列表中选择以下身份验证延迟时间：

- **60 分钟 (60 mins)**：此选项对于在前 60 分钟内启动的身份验证提供身份验证延迟。
- **12 小时 (12 hrs)**：此选项对于在前 24 小时内启动的身份验证程序提供身份验证延迟。

显示的响应时间以毫秒 (ms) 为单位。要查看身份验证延迟的详细报告，请点击**实时日志 (Live Logs)** 窗口中的最新日志。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS**。

RADIUS实时会话 (Live Sessions)

下表说明了 RADIUS **实时会话 (Live Sessions)** 窗口中的字段，此窗口显示实时身份验证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择您仅可在主 PAN 上查看 RADIUS 实时会话。

表 *39: RADIUS* 实时会话

字段名称	说明
启动时间 (Initiated)	显示启动会话时的时间戳。
已更新 (Updated)	显示会话上次由于更改而更新时的时间戳。
帐户会话时间 (Account Session Time)	显示用户会话的时间跨度（秒）。
会话状态 (Session Status)	显示终端设备的当前状态。
操作 (Action)	点击**操作 (Actions)** 图标可对活动 RADIUS 会话重新进行身份验证或断开活动 RADIUS 会话连接。
重复次数 (Repeat Count)	显示用户或终端重新进行身份验证的次数。
终端 ID	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 (Identity)	显示终端设备的用户名。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
审核会话 ID (Audit Session ID）	显示唯一会话标识符。
帐户会话 ID (Account Session ID)	显示网络设备提供的唯一 ID。
终端配置文件	显示设备的终端配置文件。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
安全组 (Security Group)	显示由身份验证日志标识的组。

字段名称	说明
服务器 (Server)	指示已从中生成日志的策略服务节点。
身份验证方法 (Auth Method)	显示RADIUS协议使用的身份验证方法，例如密码身份验证协议 (PAP)、质询握手身份验证协议 (CHAP)、IEE 802.1x 或 dot1x 等等。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
NAS IP 地址 (NAS IP Address)	显示网络设备的 IP 地址。
设备端口 (Device Port)	显示网络设备的连接端口。
PRA 操作 (PRA Action)	显示客户端在网络上成功通过合规性验证后，在客户端上采取的定期重评估操作。
ANC 状态 (ANC Status)	设备的自适应网络控制状态，如“隔离”(Quarantine)、“取消隔离”(Unquarantine) 或“关闭”(Shutdown)。
WLC 漫游 (WLC Roam)	显示用于跟踪已在漫游期间从一个 WLC 传递到另一个 WLC 的终端的布尔值 (Y/N)。它的值为 cisco-av-pair=nas-update =Y 或 N。 **注释** Cisco ISE 依靠 WLC 中的 nas-update=true 属性识别会话是否处于漫游状态。当原始 WLC 在 nas-update=true 时发送记账停止属性时，不会在ISE中删除会话，以避免重新进行身份验证。如果漫游失败，ISE 将在会话处于非活动状态五天后清除该会话。
接收的数据包 (Packets In)	显示接收的数据包数量。
发送的数据包 (Packets Out)	显示发送的数据包数量。
接收的字节 (Bytes In)	显示接收的字节数。
发送的字节 (Bytes Out)	显示发送的字节数。

字段名称	说明
会话源 (Session Source)	指示它是 RADIUS 会话还是被动 ID 会话。
用户域名 (User Domain Name)	显示用户的注册 DNS 名称。
主机域名 (Host Domain Name)	显示主机的注册 DNS 名称。
用户 NetBIOS 名称 (User NetBIOS Name)	显示用户的 NetBIOS 名称。
主机 NetBIOS 名称 (Host NetBIOS Name)	显示主机的 NetBIOS 名称。
许可证类型 (License Type)	显示使用的许可证类型。
许可证详细信息 (License Details)	显示许可证详细信息。
提供程序 (Provider)	终端活动获悉自不同的系统日志源。这些系统日志源称为提供程序。 • Windows Management Instrumentation (WMI) - WMI 是一种 Windows 服务，用于提供通用接口和对象模型来访问有关操作系统、设备、应用和服务的管理信息。 • 代理：代表客户端或另一个程序在客户端上运行的程序。 • 系统日志：客户端发送事件消息的日志记录服务器。 • REST：客户端通过终端服务器进行身份验证。对于此系统日志源，将会显示“TS代理ID”、“源端口开始时间”、“源端口结束时间”和“源第一个端口”值。 • SPAN：使用SPAN探测器发现的网络信息。 • DHCP：DHCP 事件。 • 终端 **注释** 从终端会话获悉来自不同提供程序的两个事件后，提供程序在实时会话页面中显示为逗号分隔值。
MAC 地址 (MAC Address)	显示客户端的 MAC 地址。
终端检查时间	显示终端探测器上次检查终端的时间。

字段名称	说明
终端检查结果	显示终端探测的结果。可能的值包括： • 无法接通 • 用户退出 • 活动用户
起始源端口 (Source Port Start)	（仅为 REST 提供程序显示值）显示端口范围中的第一个端口号。
结束源端口	（仅为 REST 提供程序显示值）显示端口范围中的最后一个端口号。
源第一个端口 (Source First Port)	（仅为 REST 提供程序显示值）显示由终端服务器代理分配的第一个端口。 终端服务器指允许多个终端在无需调制解调器或网络接口的情况下连接到其上的服务器或网络设备，可实现多个终端到 LAN 网络的连接。多个终端可能会有相同的 IP 地址，因此难以识别特定用户的 IP 地址。所以，为了识别特定用户，需在服务器上安装终端服务器代理，为每个用户分配一个端口范围。这有助于创建 IP 地址-端口用户映射。
TS 代理 ID (TS Agent ID)	（仅为 REST 提供程序显示值）显示安装在终端上的终端服务器代理的唯一标识。
AD 用户解析的身份 (AD User Resolved Identities)	（仅为 AD 用户显示值）显示匹配的潜在账户。
AD 用户解析的 DN (AD User Resolved DNs)	（仅为 AD 用户显示值）显示 AD 用户的可分辨名称，例如 CN=chris,CN=Users,DC=R1,DC=com

相关主题

更改 RADIUS 会话的授权，第 260 页
思科 ISE 活动 RADIUS 会话，第 259 页

TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 页面的字段，此页面显示 TACACS+ AAA 详细信息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 *40: TACACS* 实时日志

字段名称	使用指南
生成时间 **(Generated Time)**	根据特定事件触发时间显示系统日志生成时间。
日志记录时间 **(Logged Time)**	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态 **(Status)**	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 **(Details)**	在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 **(Session Key)**	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名 **(Username)**	显示设备管理员的用户名。此列为必选项，无法取消选择。
类型 **(Type)**	包括两种类型 - 身份验证和授权。显示身份验证已通过和/或失败的用户名。此列为必选项，无法取消选择。
身份验证策略 **(Authentication Policy)**	显示为特定身份验证选择的策略的名称。
授权策略 **(Authorization Policy)**	显示为特定授权选择的策略的名称。
ISE 节点 **(ISE Node)**	显示处理访问请求的 ISE 节点的名称。
网络设备名称 **(Network Device Name)**	显示网络设备的名称。
网络设备 **IP (Network Device IP)**	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 **(Network Device Groups)**	显示网络设备所属相应网络设备组的名称。
设备类型 **(Device Type)**	显示用于处理来自不同网络设备的访问请求的设备类型。
位置 **(Location)**	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 **(Device Port)**	显示发出访问请求的设备端口号。
故障原因 **(Failure Reason)**	显示拒绝网络设备发出的访问请求的原因。
远程地址 **(Remote Address)**	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。

字段名称	使用指南
匹配的命令集 (Matched Command Set)	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志页面执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

相关主题

TACACS+ 设备管理

配置全局 TACACS+ 设置，第 302 页

导出摘要

您可以查看过去 7 天内所有用户导出的报告的详细信息以及状态。导出摘要包括手动报告和已计划的报告。导出摘要页面每 2 分钟自动刷新一次。点击刷新图标可手动刷新导出摘要页面。

超级管理员可以取消正在进行或处于排队状态的导出进程。其他用户只能取消他们发起的导出进程。

默认情况下，在给定的时间点只能运行 3 次报告手动导出，其余触发的报告手动导出将排队。计划导出的报告没有此类限制。

注释 当思科 ISE 服务器重新启动时，所有处于排队状态的报告都将重新安排，处于正在进行或正在取消状态的报告将标记为失败。

注释 如果主 MnT 节点关闭，则已计划的报告导出作业将在辅助 MnT 节点上运行。

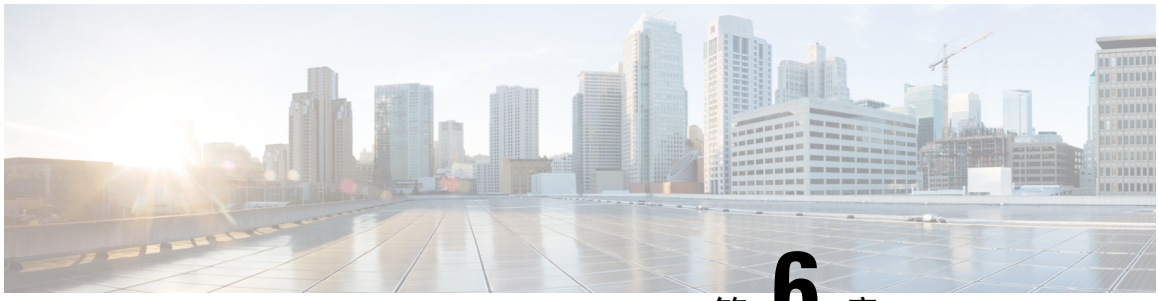
下表列出“导出摘要”(Export Summary) 页面中的字段。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **导出摘要 (Export Summary)**。

表 *41:* 导出摘要

字段名称	说明
报告已导出	显示报告的名称。
导出依据	显示发起导出进程的用户的角色。
已计划	显示报告导出是否为计划性导出。
触发于	显示在系统中触发导出进程的时间。
存储库	显示将存储导出数据的存储库的名称。
过滤器参数	显示导出报告时选择的过滤器参数。
状态	显示导出的报告的状态。它可以是下列类型之一： • 已排队 • 正在进行 • 已完成 • 正在取消 • 已取消 • 失败 • 已跳过 注释 失败状态指示失败的原因。已跳过状态指示当主 MnT 节点关闭时，跳过了计划的报告导出。

您可以在“导出摘要”(Export Summary) 页面中执行以下操作：

- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。



第 6 章

设备管理

TACACS+ 设备管理

Cisco ISE 支持设备管理通过使用终端访问控制器访问控制系统 (TACACS+) 安全协议控制，来控制和审计网络设备的配置。网络设备可以配置为向Cisco ISE 查询对设备管理员操作所进行的身份验证和授权，并发送Cisco ISE 的记账信息以记录操作。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。Cisco ISE 管理员可以创建策略集，允许在设备管理访问服务的授权策略规则中选择 TACACS 结果（如命令集和外壳配置文件）。Cisco ISE 监控节点可提供与设备管理相关的增强型报告。“工作中心”(Work Center) 菜单中包含所有设备管理页面，可作为 ISE 管理员的单一入手点。

Cisco ISE 需要设备管理许可证才能使用 TACACS+。

设备管理中存在两种类型的管理员

- 设备管理员
- Cisco ISE 管理员

设备管理员是指登录到交换机、无线接入点、路由器和网关（一般通过 SSH）等网络设备以执行对所管理设备进行配置和维护的用户。Cisco ISE 管理员可登录Cisco ISE，配置并协调设备管理员所登录的设备。

Cisco ISE 管理员是本文档的目标读者，他们可登录Cisco ISE 以配置相应的设置，控制设备管理员的操作。Cisco ISE 管理员使用设备管理功能（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > 设备管理 (Device Administration)**）来控制和审核网络设备的配置。设备可配置为使用终端访问控制器访问控制系统 (TACACS) 安全协议来查询Cisco ISE 服务器。Cisco ISE 监控节点可提供与设备管理相关的增强型报告。Cisco ISE 管理员可以执行以下任务：

- 配置带有 TACACS+ 详细信息（共享密钥）的网络设备。
- 添加设备管理员为内部用户，并根据需要为其设置启用密码。
- 创建策略集，这些策略集可使得 TACACS 结果（例如，命令集和 shell 配置文件）被选中到设备管理访问服务中的的授权策略规则中。
- 在Cisco ISE 中配置 TACACS 服务器，允许设备管理员基于策略集来访问设备。

设备管理员负责设置设备以与Cisco ISE 服务器进行通信。当设备管理员登录到设备时，设备将查询Cisco ISE 服务器，后者进而查询内部或外部身份存储区，以验证设备管理员的详细信息。当Cisco ISE 服务器完成验证后，设备将通知Cisco ISE 服务器每个会话或用于记账和审核的命令授权操作的最终结果。

Cisco ISE 管理员可以使用 TACACS 和Cisco ISE 2.0 及更高版本来进行设备管理。与设备管理相关的配置也可以从Cisco安全访问控制系统 (ACS) 服务器5.5、5.6、5.7 和 5.8 中迁移。更早期的版本需在迁移之前升级到版本 5.5 或 5.6。

注释 您应选中**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **常规设置 (General Settings)** 页面中的**启用设备管理服务 (Enable Device Admin Service)**，以便启用 TACACS+ 操作。确保部署中每个 PSN 都启用了此选项。

由于已知会限制 TACACS+ 协议在交换机或路由器与思科 ISE 之间创建安全连接，因此，请确保在双方之间部署 IPsec 协议。

ISE 社区资源

有关设备管理属性的信息，请参阅 ISE 设备管理属性。

有关无线局域网控制器、IOS 网络设备、Cisco NX-OS 网络设备和网络设备的 TACACS+ 配置信息，请参阅 ISE 设备管理 (TACACS +)。

设备管理工作中心

“工作中心”(Work Center) 菜单中包含所有设备管理页面，可以作为Cisco ISE 管理员的单一入手点。然而，未指定用于设备管理的页面（例如，“用户”(Users)、“用户身份组”(User Identity Groups)、“网络设备”(Network Devices)、“默认网络设备”(Default Network Devices)、“网络设备组”(Network Device Groups)、“身份验证”(Authentication) 和“授权条件”(Authorization Conditions)）依然可从其原始菜单选项（例如，“管理”(Administration)）访问。仅在获得并安装了正确的 TACACS+ 许可证后，“工作中心”(Work Centers) 选项才可用。

“设备管理菜单”(Device Administration Menu) 包含了以下菜单选项：“概述”(Overview)、“身份”(Identitie)、“用户身份组”(User Identity Groups)，“外部 ID 存储”(Ext ID Stores)、“网络资源”(Network Resources)，“网络设备组”(Network Device Groups)，“策略元素”(Policy Elements)、“设备管理策略集”(Device Admin Policy Sets)、“报告”(Reports) 和“设置”(Settings)。

设备管理部署设置

“设备管理部署”(Device Administration Deployment) 页面（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)** > **部署 (Deployment)**）可供Cisco ISE 管理员集中查看设备管理系统，而无需参考部署部分中的每个节点。

“设备管理部署”(Device Administration Deployment) 页面列出了部署中的 PSN。这简化了在部署中的每个节点中单独启用设备管理服务的任务。您可以通过选择以下任一选项为多个 PSN 集中启用设备管理服务：

选项	说明
无	默认情况下，所有节点的设备管理服务为禁用状态。
所有策略服务节点 (All Policy Service Nodes)	启用所有节点的设备管理服务。通过该选项，在添加新 PSN 时，其设备管理将自动启用。
指定节点 (Specific Nodes)	显示“ISE 节点”(ISE Nodes) 部分，其中列出了部署中的所有节点。您可以选择需要启用设备管理服务的节点。

注释 如果部署未许可用于 TACACS+，以上选项均为禁用状态。

通过“TACACS 端口”(TACACS Ports) 字段，您可以输入最多 4 个 TCP 端口，它们使用逗号隔开，并且端口值范围为 1 至 65535。Cisco ISE 节点及其接口通过指定端口侦听 TACACS+ 请求，而且您需要确保其他服务未使用该指定端口。默认 TACACS+ 端口值为 49。

当您点击**保存 (Save)** 时，所做更改同步到以下位置中指定的节点： **管理 (Administration)** > **系统 (System)** > **部署列表 (Deployment Listing)** 窗口。

设备管理策略集

“设备管理策略集”(Device Admin Policy Sets) 窗口（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **“设备管理”(Device Administration)** > **“设备管理策略集”(Device Admin Policy Sets)**）包含了Cisco ISE 管理员用于控制 TACACS+ 设备管理员的身份验证和授权的策略集列表。每个策略可以为两种模式中的一种：常规和代理顺序模式。

常规策略集包括一个身份验证规则表和一个授权规则表。身份验证规则表包含一组规则，用于选择对网络设备进行身份验证所需的操作。

这些授权规则表由一组规则组成，这些规则用于选择要实施授权业务模式所需的特定授权结果。每个授权规则都包含一个或多个条件（匹配时才能使用该规则）、一组命令集和/或一个外壳配置文件，选中后即可控制授权过程。每个规则表有一个可在特定条件下覆盖这些规则的例外策略，通常在临时情况下使用。

注释 不支持 TACACS + CHAP 出站身份验证。

一个代理策略集包含单个的所选代理顺序。如果策略集处于此模式，则使用一个或多个远程代理服务器处理请求（虽然本地计费可由代理顺序进行配置）。

创建设备管理策略集

创建设置的设备管理策略集：

开始之前

- 确保为 TACACS+ 操作启用**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)** > **部署 (Deployment)** 窗口中的“设备管理”(Device Administration)。
- 确保创建策略所需的用户身份组（例如，System_Admin、帮助台）。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **用户身份组 (User Identity Groups)** 页面）。确保将成员用户（例如，ABC、XYZ）分配给其对应的组。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **身份 (Identities)** > **用户 (Users)** 窗口）。
- 确保在需要管理的设备上配置 TACACS 设置。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框已启用，并且用于 TACACS 和设备的共享密钥相同，以便于设备查询Cisco ISE。）
- 确保网络设备组已根据设备类型和位置创建。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络设备组 (Network Device Groups)** 窗口）

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

步骤 2 从任意行对应的**操作 (Actions)** 列中，点击齿轮图标，然后从下拉菜单中，根据需要通过选择任何插入或重复选项来插入新策略集。
“策略集”(Policy Sets) 表中会显示一个新行。

步骤 3 输入策略集的名称和说明。

步骤 4 如果需要，请从“允许的协议/服务器序列”(Allowed Protocols/Server Sequence) 列中，点击 (+) 符号并选择以下选项之一：

a) 创建新的允许的协议
b) 创建 TACACS+ 服务器序列

步骤 5 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 6 在**Conditions Studio 页面**中创建所需的条件。在**编辑器 (Editor)**部分中，点击**点击以添加属性 (Click To Add an Attribute)** 文本框，然后选择所需的字典和属性（例如，Device-Location Equals Europe）。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 7 点击**使用 (Use)**。

步骤 8 从“视图”(View) 列中，点击 > 以访问所有策略集详细信息，并创建身份验证和授权策略以及策略例外。

步骤 9 创建所需的身份验证策略（例如，规则名称：ATN_Internal_Users，条件：DEVICE： DEVICE:Location EQUALS Location #All Locations#Europe - 该策略仅匹配位于欧洲的设备）。

步骤 10 点击**保存 (Save)**。

步骤 11 创建所需的授权策略。

示例 1：规则名称：Sys_Admin_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8 - 该策略匹配用户名为 ABC 的系统管理员，支持要执行的指定命令，并分配权限级别 8。

示例 2：规则名称：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1 - 该策略匹配用户名为 XYZ 系统管理员，支持要执行的指定命令，并分配权限级别 1。

在上述示例中：

- cmd_Sys_Admin 和 cmd_HDesk 命令集是在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 命令集 (TACACS Command Sets)** > **添加 (Add)** 窗口中创建的。
- TACACS 配置文件 Profile_Priv_1 和 Profile_priv_8 是在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)** > **添加 (Add)** 窗口中创建的。

注释 您可以在身份验证和授权策略中使用的条件中为设备 IP 地址属性添加 IPv4 或 IPv6 单一地址。

步骤 12 点击**保存 (Save)**。

TACACS+ 身份验证设置和共享密钥

下表介绍“网络设备”(Network Device) 窗口中的字段，您可以使用这些字段为网络设备配置 TACACS+ 身份验证设置。导航路径为：

- （适用于网络设备）在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **TACACS 身份验证设置 (TACACS Authentication Settings)**。
- （适用于默认设备）在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **默认设备 (Default Devices)** > **TACACS 身份验证设置 (TACACS Authentication Settings)**。有关详细信息，请参阅在思科 ISE 中定义默认网络设备。

字段名称	使用指南
共享密钥	当 TACACS+ 协议启用时，将文本字符串分配给网络设备。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。此字段为必填字段。
停用的共享密钥处于启用状态	当停用期处于启用状态时显示。
淘汰 (Retire)	停用现有的共享密钥而不是结束它。当您点击“停用”(Retire) 时，系统会显示一个消息框。您可以点击**是**或**否**。
剩余停用期	（仅当在上述消息框中选择**是 (Yes)** 时可用）显示在以下导航路径中指定的默认值： 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。 您可以更改默认值。 这允许您输入新的共享密钥，而且旧共享密钥将在指定天数中保持启用状态。
结束	（只有当您在上述消息框中选择**是**时才可用）结束停用期并终止旧共享密钥。
启用单连接模式	选中该选项以将单一 TCP 连接用于与网络设备之间的所有 TACACS+通信。选择以下其中一个选项： • 传统Cisco设备 (Legacy Cisco Devices) • 或“TACACS+ 草案合规性单连接支持 (TACACS+ Draft Compliance Single Connect Support)。如果禁用单连接模式，ISE 使用新的 TCP 连接以用于每个 TACACS+ 请求。

总而言之，您可以

- 通过指定停用期的天数（范围为 1 至 99）停用旧的共享密钥，同时设置新的共享密钥。
- 在停用期间，使用旧的共享密钥和新的共享密钥。
- 在停用期到期之前，延长停用期。
- 仅在停用期间结束之前使用旧的共享密钥。
- 在停用期到期之前，终止停用期（点击 结束[End] 然后 提交[Submit]）。

注释 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** 窗口，访问“TACACS+ 身份验证设置”(TACACS+ Authentication Settings) 选项。

设备管理 - 授权策略结果

Cisco ISE 管理员可以使用 TACACS+ 命令集和 TACACS+ 配置文件（策略结果）对授予给设备管理员的权限和命令进行控制。策略与网络设备协同工作，从而防止可能发生的意外或恶意配置更改。如果发生此种更改，您可以使用设备管理审计报告对执行特定命令的设备管理员进行跟踪。

FIPS 和非 FIPS 模式支持的 TACACS+ 设备管理协议

Cisco ISE 提供众多可用于创建策略结果的身份认证协议服务。但是，当用于 RADIUS 的Cisco ISE 设备启用 FIPS 模式时，设备会禁用适用于 TACACS+ 协议的身份验证协议服务，例如 PAP/ASCII、CHAP 和 MS-CHAPv1。因此，无法在 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **允许的协议 (Allowed Protocols)** 窗口中启用这些协议来管理设备（当使用启用 FIPS 的 (**管理 (Administration)** > **系统设置 (System Settings)** > **FIPS 模式 (FIPS Mode)**) Cisco ISE 设备时）。

因此，要在设备管理策略结果中为 FIPS 和非 FIPS 模式配置 PAP/ASCII、CHAP 和 MS-CHAPv1 协议，您必须导航至 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **允许的协议 (Allowed Protocols)** 窗口。在启用 FIPS 模式时只会使用默认设备管理支持的协议设置。RADIUS 不支持该选项。

TACACS+ 命令集

命令集实施可由设备管理员执行的指定命令列表。当设备管理员在网络设备上发出操作命令时，查询Cisco ISE 确定管理员是否被授权发出这些命令。这也称为命令授权。

命令集中的通配符和正则表达式

命令行包括命令和零个或多个参数。当Cisco ISE 收到命令行（请求）时，它可以以不同的方式处理命令及其参数：

- 使用通配符匹配模式将请求中的命令与命令集列表中指定的命令进行匹配。

示例：Sh?? or S*

- 使用正则表达式 (regex) 匹配模式将请求中的参数与命令集列表中指定的参数进行匹配。

  示例：Show interface[1-4] port[1-9]:tty*

命令行和命令集列表匹配

将请求的命令行与包含通配符和 Regrex 的命令集列表进行匹配：

1. 循环访问命令集列表以检测匹配的命令。

   通配符匹配允许：

   - 不区分大小写
   - 命令集的命令中的任意字符都可以为“?”，它与请求的命令中必须存在的任意单个字符匹配
   - 命令集的命令中的任意字符都可以为“*”，它与请求的命令中的 0 或多个字符匹配

     示例：

请求	命令集	匹配	备注
show	show	支持	—
show	SHOW	支持	不区分大小写
show	Sh??	支持	匹配任意字符
show	Sho??	N	第二个“?”与不存在的字符相交
show	S*	支持	“*”匹配任意字符
show	S*w	支持	“*”匹配字符“ho”
show	S*p	N	请求中没有字符与字符“p”对应

2. 对于每个匹配的命令，Cisco ISE 会验证参数。

   对于每个命令，命令集列表将包含一组以空格隔开的参数。

   示例：Show interface[1-4] port[1-9]:tty.*

   该命令含有两个参数。

   1. 参数 1：interface[1-4]
   2. 参数 2：port[1-9]:tty.*

对于请求中的命令参数，按照它们在数据包中的位置重要性顺序进行匹配。如果命令定义中的所有参数与请求中的参数匹配，那么该命令/参数可认为是匹配的。注意：请求中的任何外来参数都会被忽略。

注释 在参数中使用标准 Unix 正则表达式。

含多个命令集的处理规则

1. 如果命令集包含命令及其参数的匹配项，并且匹配项具有“始终拒绝”(Deny Always)，则Cisco ISE 会指定该命令集为 Commandset-DenyAlways。
2. 如果命令集中的命令匹配项没有“始终拒绝”(Deny Always)，则Cisco ISE 会依次检查命令集中的所有命令直到找到第一个匹配项。
    1. 如果第一个匹配项具有“允许”(Permit)，则Cisco ISE 会指定命令集为 Commandset-Permit。
    2. 如果第一个匹配项具有“拒绝”(Deny)，则Cisco ISE 会指定命令集为 Commandset-Deny。
3. 在Cisco ISE 分析所有命令集后，它会授权以下命令：
    1. 如果Cisco ISE 指定任何命令集为 Commandset-DenyAlways，则Cisco ISE 拒绝该命令。
    2. 如果没有 Commandset-DenyAlways，且任意命令集为 Commandset-Permit，则Cisco ISE 允许该命令；否则，Cisco ISE 将拒绝该命令。唯一的例外情况是**不匹配 (Unmatched)** 复选框已选中。

创建 TACACS+ 命令集

要使用 TACACS+ 命令集策略结果创建策略集，请按照以下步骤操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 命令集 (TACACS Command Sets)**。

您还可以在以下位置配置 TACACS 命令集： **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 页面。

步骤 2 点击**添加 (Add)**。

步骤 3 输入名称和说明。

步骤 4 点击**添加 (Add)** 指定授予权限、命令和参数。

步骤 5 在**授予 (Grant)** 下拉列表，您可以选择以下选项之一：

- **允许 (Permit)** ：允许指定的命令（例如，permit show, permit con* Argument terminal）。
- **拒绝 (Deny)** ：拒绝指定的命令（例如，deny mtrace）。

- **始终拒绝 (Deny Always)** ：覆盖在其他命令集中允许的命令（例如，clear auditlogs）

注释　点击操作图标以增加或减少“Grant”(授予)、“Command”(命令) 和“参数”(Argument) 字段的列宽。

步骤 6 选中**允许以下未列出的任何命令 (Permit any command that is not listed below)** 复选框允许未在“授予”列中指定为允许、拒绝或始终拒绝的命令和参数。

TACACS+ 配置文件

TACACS+ 配置文件控制设备管理员的初始登录会话。会话是指每个单独的身份验证、授权或记帐请求。对网络设备的会话授权请求会引发Cisco ISE 响应。响应包括由网络设备解释的令牌，限制可能在会话期限执行的命令。用于设备管理访问服务的授权策略可以包含单个外壳配置文件和多个命令集。TACACS+ 配置文件定义分为两个组件：

- 常见任务
- 自定义用户属性

“TACACS+ Profiles (TACACS+ 配置文件)”窗口中有两个视图（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)**）：**任务属性视图 (Task Attribute View)** 和**原始视图 (Raw View)**。可以使用**任务属性视图 (Task Attribute View)** 输入常见任务，且自定义属性可在**任务属性视图 (Task Attribute View)** 和**原始视图 (Raw View)** 中创建。

您可通过**常见任务 (Common Tasks)** 部分为配置文件选择并配置最常用的属性。这里包含的属性为 TACACS+ 协议草案说明定义的那些属性。但是值可用于来自其他服务的请求授权。在**任务属性视图 (Task Attribute View)** 中，Cisco ISE 管理员可以设置分配给设备管理员的权限。常见任务类型如下：

- 外壳
- WLC
- Nexus
- 通用

您可通过**自定义属性 (Custom Attributes)** 部分配置其他属性。它提供不被**常见任务 (Common Tasks)** 部分识别的属性列表。每个定义包括属性名称、该属性是强制还是可选的说明和属性值。

注释　您可以为启用 TACACS 的网络设备定义总共 24 个任务属性。如果定义的任务属性超过 24 个，则不会将这些属性发送到启用 TACACS 的网络设备。

在**原始视图 (Raw View)** 中，可以在属性名称及其值之间使用等号 (=) 输入强制属性，在属性名称及其值之间使用一个星号 (*) 可输入可选属性。**原始视图 (Raw View)** 中输入的属性反映在**任务属性视图 (Task Attribute View)** 中的**自定义属性 (Custom Attributes)** 部分，反之亦然。**原始视图 (Raw View)**

部分也用于将属性列表（例如，另一产品的属性列表）从剪贴板复制并粘贴到Cisco ISE 上。可为非外壳服务定义自定义属性。

创建 TACACS+ 配置文件

要创建 TACACS+ 配置文件：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)**。

还可以在以下位置配置 TACACS 命令集 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 页面。

步骤 2 点击**添加 (Add)**。

步骤 3 在 **TACACS 配置文件 (TACACS Profile)** 部分中，请输入名称和说明。

步骤 4 在**任务属性视图 (Task Attribute View)** 选项卡中，请选中所需的**常见任务 (Common Tasks)**。请参阅常见任务设置，第 299 页页面。

步骤 5 在**任务属性视图 (Task Attribute View)** 选项卡**自定义属性 (Custom Attributes)** 部分中，点击**添加 (Add)** 输入必要的属性。

常见任务设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)** > **添加 (Add)** 以查看常见任务设置窗口。常见任务类型为：外壳、WLC、Nexus 和通用。

Shell

Cisco ISE 管理员可使用以下选项设置设备管理员的权限。

选项	说明
默认权限 (Default Privilege)	为设备管理员启用默认（初始）权限级别，以供其进行外壳授权。请选择以下任意一个选项： • 选择 0 - 15 之间的值。 • 选择所需的“身份存储属性”(Identity Store Attribute)。
最大权限 (Maximum Privilege)	启用“启用身份验证”(Enable authentication) 所需的最大权限级别。您可以选择 0 - 15 之间的值。
访问控制列表 (Access Control List)	选择一个 ASCII 字符串 (1-251*) 或所需的“身份数据库属性”(Identity Store Attribute)。

选项	说明
自动命令 (Auto Command)	选择一个 ASCII 字符串 (1-248*) 或所需的“身份存储属性”(Identity Store Attribute)。
禁用转义 (No Escape)	对于转义字符，选择以下任一选项： • True：说明转义预防已启用。 • False：说明转义预防未启用。 • 选择所需的“身份存储属性”(Identity Store Attribute)。
超时 (Timeout)	选择 0 - 9999 之间的值或所需的“身份存储属性”(Identity Store Attribute)。
空闲时间 (Idle Time)	选择 0 - 9999 之间的值或所需的“身份存储属性”(Identity Store Attribute)。

WLC

Cisco ISE 管理员可使用以下选项控制设备管理员对 WLC 应用选项卡的访问权限。WLC 应用包含以下选项卡：WLAN、“控制器”(Controller)、“无线”(Wireless)、“安全”(Security)、“管理”(Management) 和“命令”(Commands)。

选项	说明
所有 (All)	设备管理员对所有 WLC 应用选项卡均具有完全访问权限。
监控器 (Monitor)	设备管理员对 WLC 应用选项卡仅有只读访问权限。
大厅 (Lobby)	设备管理员仅有部分配置权限。
选中 (Selected)	设备管理员可以访问Cisco ISE管理员从以下复选框中选中的选项卡：WLAN、控制器(Controller)、无线 (Wireless)、安全 (Security)、管理 (Management) 和命令 (Commands)。

Nexus

Cisco ISE 管理员可使用以下选项控制设备管理员对Cisco Nexus 交换机的访问权限。

选项	说明
将属性设置为 (Set Attribute As)	Cisco ISE 管理员可以将常见任务生成的 Nexus 属性指定为“可选”(Optional) 或“必选”(Mandatory)。
网络角色 (Network Role)	将 Nexus 配置为使用Cisco ISE 进行身份验证时，默认情况下，设备管理员拥有只读访问权限。可将设备管理员分配至其中一个角色。每个角色定义允许的操作： • 无 (None)：无权限。 • 操作者（只读）(Operator (Read Only))：对整个 NX-OS 设备有完全的读取访问权限。 • 管理员（读/写）(Administrator (Read/Write))：对整个 NX-OS 设备有完全的读写访问权限。
虚拟设备环境 (VDC) (Virtual Device Context [VDC])	无 (None)：无权限。 操作者（只读）(Operator (Read Only))：仅对 VDC 有读取访问权限 管理员（读/写）(Administrator (Read/Write))：仅对 VDC 有读写访问权限。

通用

Cisco ISE 管理员可使用此选项指定常见任务中不可用的自定义属性。

访问命令行界面以更改启用密码

要更改启用密码，请执行以下步骤：

开始之前

某些命令会分配到特权模式。因此，只能在设备管理员经过身份验证进入此模式时执行它们。

当设备管理员尝试进入特权模式时，设备会发送特殊的启用身份验证类型。Cisco ISE 支持使用单独的启用密码来验证此特殊的启用身份验证类型。当使用内部身份库对设备管理员进行身份验证时，系统将使用单独的启用密码。对于使用外部身份库进行的身份验证，系统将使用相同的密码来进行常规登录。

步骤 1 登录到交换机。

步骤 2 按 Enter 键显示以下提示符：

```
Switch>
```

步骤 3 执行以下命令来配置启用密码。

```
Switch> enable Password:（按 Enter 键可留空密码。）Enter Old Password:（输入旧密码。）Enter New Password:（输入新密码。）Enter New Password Confirmation:（确认新密码。）
```

注释 如果为登录密码和启用密码配置了密码有效期，则在指定时段内未更改密码时，用户帐户将禁用。如果将Cisco ISE 配置为 TACACS+ 服务器，并在网络设备上配置了**启用旁路 (Enable Bypass)** 选项，则无法通过 CLI（通过 telnet）更改启用密码。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**，更改内部用户的启用密码。

配置全局 TACACS+ 设置

配置全局 TACACS+ 设置

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)**。

在**连接设置 (Connection Settings)** 选项卡，您可以更改所需字段的默认值。

- 在**授权缓存超时 (Authorization cache timeout)** 字段中，可以设置生存时间 (TTL) 值，首次授权请求时，系统将在该时间内缓存内部用户的某些属性。缓存的属性包括用户名和用户特定属性，如用户组。“系统管理”（System Administration）“配置”（Configuration）“字典”（Dictionary）“身份”（Identity）“内部用户”（Internal Users）以创建属性。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 默认值为 0，表示禁用授权缓存。
- **单连接支持 (Single Connect Support)**：如果禁用单连接模式，则 ISE 对每个 TACACS+ 请求使用新的 TCP 连接。

步骤 2 在**密码更改控制 (Password Change Control)** 选项卡，定义所需字段以控制是否通过 TACACS+ 允许密码更新。

只有选中此选项，才会启用**启用 Telnet 更改密码 (Enable Telnet Change Password)** 部分中的提示。否则，会启用**禁用 Telnet 更改密码 (Disable Telnet Change Password)** 提示。密码提示可完全自定义，并可根据需要进行修改。

在**密码策略违规消息 (Password Policy Violation Message)** 字段中，如果新密码与指定条件不符，您可以为内部用户设置的密码显示相应的错误消息。

步骤 3 在**会话密钥分配 (Session Key Assignment)** 选项卡，请选择所需的字段以将 TACACS+ 请求链接到会话。

监控节点使用会话密钥来链接来自客户端的AAA请求。默认设置为启用NAS地址、端口、远程地址和用户字段。

步骤 4 点击**保存 (Save)**。

相关主题

TACACS+ 身份验证设置和共享密钥，第 293 页
RADIUS 令牌服务器中的用户属性缓存，第 583 页

从思科安全 ACS 将数据迁移至思科 ISE

您可以使用迁移工具导入来自 ACS 5.5 及更高版本的数据，然后为所有网络设备设置默认 TACACS+ 密钥。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)**，在**准备 (Prepare)** 部分中，点击**下载软件网页**，下载迁移工具。将工具保存到您的 PC，然后在 migTool 文件夹中，运行 migration.bat 文件以开始迁移过程。有关迁移的完整信息，请参阅您的Cisco ISE 版本的迁移指南。

监控设备管理活动

Cisco ISE 提供各种报告和日志，通过这些报告和日志，您可以查看通过 TACACS+ 配置的设备计费、身份验证、授权和命令计费相关的信息。您可以按需或按计划运行这些报告。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **报告 (Reports)** > **报告 (Reports)**。。

您还可以在其他位置查看报告。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** 页面。

步骤 2 在**报告选择器 (Report Selector)** 中，展开**设备管理 (Device Administration)** 以查看**身份验证摘要 (Authentication Summary)**、**TACACS 记账 (TACACS Accounting)**、**TACACS 身份验证 (TACACS Authentication)**、**TACACS 授权 (TACACS Authorization)**、**TACACS 命令记账 (TACACS Command Accounting)**、**不同失败原因的前 N 个身份验证 (Top N Authentication by Failure Reason)**、**不同网络设备的前 N 个身份验证 (Top N Authentication by Network Device)**、 **不同用户的前 N 个身份验证 (Top N Authentication by User)** 报告。

步骤 3 选择报告并选取您想要使用 **Filters** 下拉列表搜索的数据。

步骤 4 在 **Time Range** 中选择您想要查看的数据的时间范围。

步骤 5 点击**运行 (Run)**。

TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 页面的字段，此页面显示 TACACS+ AAA 详细信息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 *42: TACACS* 实时日志

字段名称	使用指南
生成时间 **(Generated Time)**	根据特定事件触发时间显示系统日志生成时间。
日志记录时间 **(Logged Time)**	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态 **(Status)**	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 **(Details)**	在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 **(Session Key)**	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名 **(Username)**	显示设备管理员的用户名。此列为必选项，无法取消选择。
类型 **(Type)**	包括两种类型 - 身份验证和授权。显示身份验证已通过和/或失败的用户名。此列为必选项，无法取消选择。
身份验证策略 **(Authentication Policy)**	显示为特定身份验证选择的策略的名称。
授权策略 **(Authorization Policy)**	显示为特定授权选择的策略的名称。
ISE 节点 **(ISE Node)**	显示处理访问请求的 ISE 节点的名称。
网络设备名称 **(Network Device Name)**	显示网络设备的名称。
网络设备 **IP (Network Device IP)**	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 **(Network Device Groups)**	显示网络设备所属相应网络设备组的名称。
设备类型 **(Device Type)**	显示用于处理来自不同网络设备的访问请求的设备类型。
位置 **(Location)**	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 **(Device Port)**	显示发出访问请求的设备端口号。
故障原因 **(Failure Reason)**	显示拒绝网络设备发出的访问请求的原因。
远程地址 **(Remote Address)**	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。

字段名称	使用指南
匹配的命令集 (Matched Command Set)	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志页面执行以下操作：

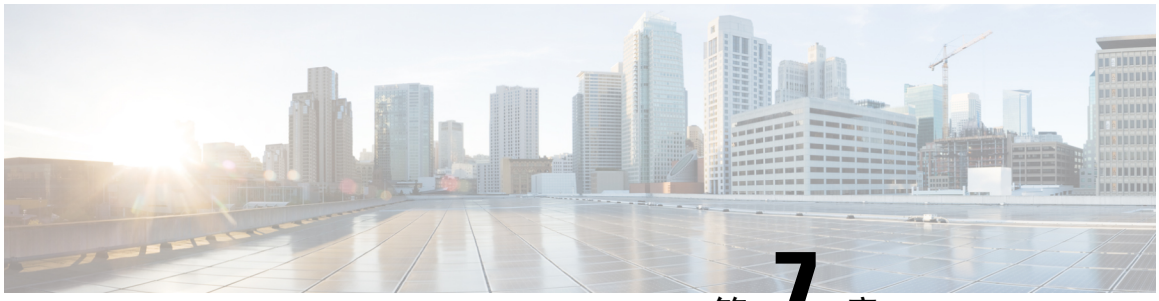
- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

相关主题

TACACS+ 设备管理

配置全局 TACACS+ 设置，第 302 页



第 7 章

访客和安全 WiFi

思科 ISE 访客服务

使用Cisco身份识别服务引擎（Cisco ISE）访客服务，可以提供对访客（例如宾客、承包商、顾问和客户）的安全网络访问。您可以支持具有基本Cisco ISE 许可证的访客，此外，还可以根据公司的基础设施和功能要求，从若干部署选项中选择。

Cisco ISE 提供基于 Web 的门户和移动门户，让访客和员工注册公司的网络以及内部资源和服务。

从 Admin 门户，您可以创建和编辑访客和发起人门户，通过定义访客类型配置访客接入权限，以及分配发起人权限，创建和管理访客帐户。

- 访客门户，第 326 页
- 访客类型和用户身份组，第 309 页
- 发起人门户，第 341 页
- 发起人组，第 342 页

ISE 社区资源

有关 ISE 访客和 Web 身份验证的 ISE 社区资源的完整列表，请参阅 ISE 访客访问 - ISE 访客和 Web 身份验证。

分布式环境中的最终用户访客门户和发起人门户

Cisco ISE 最终用户 Web 门户根据管理、策略服务和监控角色，提供配置、会话支持和报告功能。

- **策略管理节点 (PAN)**：您对用户、设备和最终用户门户所做的配置更改会写入 PAN。
- **策略服务节点 (PSN)**：最终用户门户在 PSN 上运行，后者处理所有会话流量，包括网络访问、客户端调配、访客服务、终端安全评估和分析。如果 PSN 是节点组的一部分，并且一个节点发生故障，则其他节点会检测到故障，并重置任何挂起的会话。
- **监控节点（MnT 节点）**：MnT 节点在我的设备门户、发起人门户和访客门户上收集、聚合和报告有关最终用户和设备活动的数据。如果主 MnT 节点故障，则辅助 MnT 节点自动成为主 MnT 节点。

访客和发起人帐户

- **访客帐户 (Guest Accounts)**：访客通常表示授权访客、承包商、客户，或者需要临时访问网络的其他用户。如果您更愿意使用其中一个访客部署场景以允许员工访问该网络，也可以让员工使用访客帐户。您可以访问发起人门户，查看由发起人和自注册访客创建的访客帐户。
- **发起人帐户 (Sponsor Accounts)**：使用发起人门户为授权访客创建用于安全访问公司网络或互联网的临时帐户。在创建访客帐户后，您还可以使用发起人门户管理这些帐户并向访客提供帐户详细信息。

访客帐户可以通过以下方式创建：

- **发起人 (Sponsors)**：在管理员门户上，您可以为发起人定义访问权限和功能支持，发起人可以访问发起人门户以创建和管理访客帐户。
- **访客 (Guests)**：访客也可以通过自助注册访客门户创建自己的帐户。根据门户配置，自助注册的访客可能需要发起人批准后才能获得登录凭证。

访客还可以使用热点访客门户来访问网络，而无需创建访客帐户及用户名和密码等登录凭证。

- **员工 (Employees)**：包括在身份库（例如 Active Directory、LDAP、内部用户）中的员工同样可以通过已配置的需要凭证的访客门户（发起人管理的和自助注册的访客门户）进行访问。

访客帐户创建完毕后，访客即可使用发起人管理的访客门户进行登录并获得访问网络的权限。

访客类型和用户身份组

每个访客帐户必须与访客类型关联。访客类型允许发起人向访客帐户配分各种访问级别以及不同的网络连接时间。这些访客类型与特定的网络接入策略相关联。Cisco ISE 包括以下默认访客类型：

- 承包商 (Contractor)：需要在长达 1 年时间内访问网络的用户。
- 日 (Daily)：仅需在 1 至 5 天内访问网络资源的访客。
- 周 (Weekly)：需在数周内访问网络的用户。

在创建访客帐户时，可限制某些发起人组使用特定的访客类型。这种组的成员可以创建仅具有针对其访客类型特定功能的访客。例如，发起人组 ALL_ACCOUNTS 可设置为仅使用承包商访客类型，而发起人组 OWN_ACCOUNTS 和 GROUP_ACCOUNTS 则可设置为仅使用每日和每周访客类型。此外，由于使用自助注册访客门户的自助注册访客通常仅需访问一天，因此您可以向其分配每日访客类型。

访客类型定义访客的用户身份组。

有关详情，请参阅：

- 用户身份组，第 455 页
- 创建用户身份组，第 463 页

创建或编辑访客类型

可以编辑默认访客类型及其默认访问权限和设置，或者创建新的访客类型。所做更改将应用到使用此访客类型创建的现有访客帐户。登录的访客用户不会看到这些更改，直到这些用户注销并重新登录为止。还可以复制访客类型，使用相同的访问权限创建其他访客类型。

每个访客类型都有名称、说明以及可以使用此访客类型创建访客帐户的发起人组列表。如下所示，可以按如下方式指定某些访客类型：仅用于自行注册访客，或者不用于（由任何发起人组）创建访客帐户。

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **访客类型 (Guest Types)**。输入必要的详细信息。

使用这些设置可以创建能够访问网络的访客类型及其访问权限。您也可以指定哪些发起人组能够创建此访客类型。

字段名称	使用指南
访客类型名称 (Guest Type Name)	提供一个名称（1 至 256 个字符），将此访客类型与默认访客类型以及您创建的其他访客类型区分开来。
说明	提供有关此访客类型推荐用途的更多信息（最多 2000 个字符），例如：用于自行注册访客，不用于访客帐户创建等等。
语言文件 (Language File)	使用此访客类型导出或导入用于门户的语言文件。
收集其他数据 (Collect Additional Data)	选择自定义字段，从访客收集更多信息。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **访客访问 (Guest Access)** > **设置 (Settings)** > **自定义字段 (Custom Fields)**。
“最长访问时间”(Maximum Access Time) - 帐户持续时间开始	**从首次登录开始 (From First Login)**：当访客用户首次登录访客门户时，即开始计算帐户开始时间，并且帐户结束时间为指定的持续时间。如果访客用户从未登录，帐户会持续处于等待首次登录状态，直至该帐户根据访客帐户清除策略被删除。自注册和由发起人创建的用户帐户在他们创建并登录他们的帐户时开始。 注释 如果使用**仅在这些日期和时间允许访问 (Allow access only on these days and times)**，则在这些时间条件下使用位置。如果不希望“从首次登录开始”(From First Login) 访问基于位置，请勿设置访问的天数和时间。 **从发起人指定的日期开始 (From sponsor-specified date)**：指定此类型的访客能够访问网络和保持网络连接的最大天数、小时数或分钟数，从 1 到 999。 如果更改此设置，您的更改不会应用到使用此访客类型创建的原有访客帐户。
仅在这些日期和时间允许访问 (Allow Access only on these Days and Times)	输入时间范围并选择星期值，以指定此访客类型能够访问网络的时间。如果此访客类型在这些时间参数之外保持连接，他们将被注销。时间范围与使用此访客类型分配给访客的位置所定义的时区有关。 点击 + 或 -，添加或删除访问次数限制。
配置访客帐户清除策略 (Configure guest account Purge Policy)	您可以安排终端清除作业计划。默认情况下会启用终端清除计划，并且Cisco ISE 会删除超过 30 天的终端。有关详细信息，请参阅终端清除设置。
“登录选项”(Login Options) - 最大同时登录数量	输入此访客类型可以同时运行的最大用户会话数。

字段名称	使用指南
当访客超过限制时 **(When Guest Exceeds Limit)**	如果选择**最大同时登录数 (Maximum simultaneous logins)**，还必须同时选择用户在达到限制后连接时要执行的操作。 **当访客超过限度时 (When the guest exceeds limit)** • **断开最早的连接 (Disconnect the oldest connection)** • **断开最近的连接 (Disconnect the newest connection)** • **将用户重定向至显示错误信息的门户 (Redirect user to a portal page showing an error message)**：先显示一条错误消息（持续时间可以配置），然后断开会话，并将用户重定向到访客门户。错误页面的内容在**消息 (Messages) > 错误消息 (Error Messages)** 选项卡上的**门户页面自定义 (Portal Page Customization)** 对话框中进行配置。
访客可以注册的最大设备数 (Maximum Devices Guests can Register)	输入每个访客可以注册的最大设备数。您可以将限制设为小于已为此访客类型的访客注册的设备数的数值。这只会影响新创建的访客帐户。
允许访客绕开访客门户 (Allow Guest to bypass the Guest portal)	允许用户绕过需要提供凭证的访客强制网络门户（Web 身份验证页面），通过向有线和无线 (dot1x) 请求方或 VPN 客户端提供凭证来访问网络。访客帐户进入活动状态，绕过等待初始登录状态和 AUP 页面，即使其是必填项也是如此。 如果不启用此设置，用户必须首先通过需要提供凭证的访客强制网络门户登录，然后才能访问网络的其他部分。
“帐户过期通知”(Account Expiration Notification) - 在帐户过期之前 __ 天，发送帐户过期通知。	在帐户过期之前向访客发送通知，指定距离过期还剩多少天、多少小时或多少分钟。
查看...中的消息 (View messages in)	指定在按照您的设置显示邮件或 SMS 通知时使用的语言。
电子邮件 (Email)	选择邮件作为发送帐户过期通知的方式。
从...使用自定义 (Use customization from)	从另一门户选择邮件自定义。
消息 (Messages)	输入用于帐户过期通知的文本内容。
从...复制文本 (Copy text from)	重复使用您为另一访客类型创建的帐户过期通知邮件文本。
向我发送测试邮件，地址为 (Send test email to me at)	确保邮件通知发送到您的邮件地址后按原样显示。

字段名称	使用指南
SMS	选择文本 (SMS) 作为帐户过期通知的方式。
消息 (Messages)	输入用于帐户过期通知的文本内容。
从...复制文本 (Copy text from)	重复使用您为另一访客类型创建的文本消息。
向我发送测试 SMS，地址为 (Send test SMS to me at)	确保文本通知发送到您的手机后按原样显示。
这些发起人组可以创建该访客类型 (These sponsor groups can create this guest type)	选择哪些发起人组能够使用此访客类型创建访客帐户。 如果想要禁止使用此访客类型，请不要将其分配给任何发起人组。如果想要中断使用此访客类型，请删除列出的发起人组。

下一步做什么

- 创建或修改发起人组，以使用此访客类型。
- 如果适用，请在自行注册访客门户中将此访客类型分配给自行注册访客。

禁用访客类型

您无法删除最后一个剩余的访客类型，或访客帐户正在使用的访客类型。如果您希望删除使用中的访客类型，请首先确保其不再可供使用。禁用访客类型不会影响到使用该访客类型创建的访客帐户。

以下步骤介绍如何准备和禁用目标访客类型。

步骤 1 确定允许发起人使用目标访客类型创建访客的发起人组。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **配置 (Configure)** > **门户和组件 (Portals and Components)** > **发起人组 (Sponsor Groups)**。打开每个发起人组并检查**此发起人组可以使用这些访客类型创建帐户 (This sponsor group can create accounts using these guest types list)** 列表。

步骤 2 确定分配目标访客类型的自注册门户。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **配置 (Configure)** > **门户和组件 (Portals and Components)** > **访客门户 (Guest Portals)**。打开每个自注册访客门户。如果门户使用特定访客类型，请展开**门户设置 (Portal Settings)**，并在**使用此门户的员工作为访客继承登录选项于：(Employees using this portal as guests inherit login options from:)** 字段。

步骤 3 打开要删除的访客类型，并删除您在之前的步骤中确定的所有发起人组。此操作会有效地防止所有发起人使用此访客类型创建新的访客帐户。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **配置 (Configure)** > **门户和组件 (Portals and Components)** > **访客类型 (Guest Type)**。

配置终端用户的最大同时登录数

可以配置针对访客用户允许的最大同时登录数。

当用户登录到访客门户并已成功进行身份验证时，系统会检查该用户的现有登录数，从而查看用户是否已达到最大登录数。如果已达到，则系统会将访客用户重定向到错误页面。系统将显示错误页面，并停止会话。如果此用户尝试再次访问互联网，则系统会将其重定向到访客门户的登录页面。

开始之前

确保您在此门户的授权策略中使用的授权配置文件的**访问类型 (Access Type)** 设置为 *Access_Accept*。如果**访问类型 (Access Type)** 设置为 *Access_Reject*，则不会实施最大同时登录数。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Type)**。在**登录选项 (Login Options)** 下：

a) 选中**最大同时登录数 (Maximum maximum logins)** 复选框，并输入允许的最大同时登录数。

b) 在**访客超出限制时 (When guest exceeds limit)** 下，点击**断开最新连接 (Disconnect the newest connection)** 选项。

c) 选中**将用户重定向至显示错误消息的门户页面 (Redirect user to a portal page showing an error message)** 复选框。

步骤 2 依次选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)**，并创建授权配置文件：

a) 在**常见任务 (Common Tasks)** 下，选中 **Web 重定向 (Web Redirection)** 并执行以下操作：

- 在第一个下拉列表中，选择**集中式 Web 身份验证 (Centralized Web Auth)**。
- 输入已创建的 **ACL** 作为必备条件的一部分。
- 对于**值 (Value)**，选择要重定向到的访客门户。

b) 在**常见任务 (Common Tasks)** 中向下滚动，选中**重新身份验证 (Reauthentication)** 复选框并执行以下操作：

- 在**计时器 (Timer)** 中，输入在将用户重定向到访客门户之前希望错误页面显示的时间量。
- 在 **Maintain Connectivity During Reauthentication** 中，选择 **Default**。

步骤 3 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**。创建授权策略，以便在属性 NetworkAccess.SessionLimitExceeded 为 true 时，将用户重定向到门户。

下一步做什么

可以在“门户页面自定义”(Portal Page Customization) 选项卡上自定义错误页面的文本。依次选择**消息 (Messages)** > **错误消息 (Error Messages)** 并更改错误消息键 *ui_max_login_sessions_exceeded_error* 的文本。

安排清除过期访客帐户的时间

当活动或挂起访客帐户达到其帐户持续时间（按照创建帐户时发起人的定义）结束时，帐户过期。当访客帐户过期时，受影响的访客无法访问网络。发起人可以在清除之前延长到期帐户的期限。然而，帐户清除之后，发起人必须创建新的帐户。

清除过期访客帐户时，关联的终端以及报告和日志记录信息仍然保留。

默认情况下，Cisco ISE 每 15 天自动清除一次过期访客帐户。**Date of next purge** 指示下次清除的时间。您还可以：

- 计划每 X 天执行清除操作。第一次清除会在 X 天之后在指定的**清除时间 (Time of Purge)**进行，然后每 X 天执行一次清除操作。
- 计划每 X 周在指定周的固定某天执行清除操作。第一次清除在下一**周的某天 (Day of Week)** 的指定的**清除时间 (Time of Purge)** 执行，随后清除会每 X 周（X 为设置的周值）在指定的日期和时间进行。例如，如果您在本周的星期一设置每 5 周在星期四执行清除操作，则下次清除将在本周的星期四进行，而不是 5 周之后的星期四。
- 通过点击**立即清除 (Purge Now)** 可立即强制执行清除操作。

如果Cisco ISE 服务器在按计划运行清除时关闭，不会执行清除。假设服务器在下一次计划清除时可以运行，清除进程将在那时再次运行。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问权限 (Guest Access)** > **设置 (Settings)** > **访客帐户清除策略 (Guest Account Purge Policy)**。

步骤 2 选择以下选项之一：

- 点击 **Purge Now**，立即清除过期的访客帐户记录。
- 选中 **Schedule purge of expired guest accounts** 复选框，安排清除。

  注释　每次完成清除后，**下次清除日期 (Date of next purge)** 重置为下一次预定的清除日期。

步骤 3 在**门户用户信息在...后过期 (Expire portal-user information after)** 中指定用户出现不活跃状态多久之后过期。此设置防止从未使用的 LDAP 和 Active Directory 帐户永远保存在 ISE 数据库中。

如果访客未进行首次登录，在指定时间段的到期时，根据配置的清除策略，访客帐户会变为已过期状态，然后被清除。

您还可以指定过期的访客帐户必须清除的频率（以天或周为单位）。如果选择了**每 _ 周清除一次 (Purge occurs every _ weeks)** 选项，还可以指定清除过期帐户的日期和时间。

步骤 4 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

添加用于创建访客帐户的自定义字段

当提供访客接入时，可能不仅仅从访客收集其姓名、邮箱地址和电话号码信息。可以将Cisco ISE 提供的自定义字段用于针对公司需求收集其他访客信息。可以将自定义字段与访客类型，以及自注册的访客门户和发起人门户相关联。Cisco ISE 不提供任何默认自定义字段。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **访客访问 (Guest Access)** > **设置 (Settings)** > **自定义字段 (Custom Fields)**。

步骤 2 输入 **Custom Field Name**，从下拉列表中选取 **Data Type**，然后输入 **Tip Text** 以帮助提供其他有关自定义字段的信息。例如，如果输入 Date of Birth，请选取 Date-MDY，然后输入日期格式提示 MM/DD/YYYY。

步骤 3 点击**添加 (Add)**。

自定义字段按字母顺序显示于列表中或显示于有序排列的情景中。

步骤 4 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

注释 如果删除自定义字段，则无法再在访客类型的**自定义字段 (Custom Fields)** 列表，以及自注册的访客门户和发起人门户设置中供您选择。如果正在使用字段，则**删除 (Delete)** 会被禁用。

下一步做什么

在以下情况下，可以包含所需的自定义字段：

- 当定义访客类型，使得使用该访客类型创建的帐户将包含此信息时。参阅创建或编辑访客类型。
- 当配置发起人门户，供发起人在创建访客帐户的时候使用时。请参阅自定义发起人门户，第350页。
- 当使用自注册的访客门户从自注册访客请求信息时。请参阅创建自注册访客门户，第 334 页。

为邮件通知指定邮箱地址和 SMTP 服务器

通过Cisco ISE，可以将邮件发送到发起人和访客，向他们通知相关信息和说明。可以配置 SMTP 服务器来传送这些邮件通知。还可以指定将通知发送到访客的发件人邮箱地址。

注释 访客通知需要兼容 UTF-8 的邮件客户端。

需要支持 HTML 的邮件客户端（已启用功能）才能使用一键式发起人审批功能。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **设置 (Settings)** > **访客电子邮件设置 (Guest Email Settings)**。

步骤 2 默认情况下，**Enable email notifications to guests** 处于选中状态。如果禁用此设置，访客不会收到邮件通知，不管在配置访客门户和发起人门户时是否已启用任何其他设置。

步骤 3 输入为将邮件通知发送到访客而指定的 **Default “From” email address**。例如，donotreply@ *yourcompany*.com。

步骤 4 执行以下操作之一：

- 如果希望访客从创建其帐户的发起人接收通知，请选中 **Send notifications from sponsor's email address (if sponsored)**。自注册访客将从默认邮箱地址接收通知。
- 如果希望不管是由发起人发起的还是自注册的访客都收到通知，请选中 **Always send notifications from the default email address**。

步骤 5 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

分配访客位置和 SSID

访客位置定义时区的名称，并由 ISE 用于执行已登录访客的时间相关设置。访客位置由创建访客帐户的发起人以及由自行注册的访客分配给访客帐户。默认访客位置为 San Jose。如果未添加其他访客位置，则为所有帐户分配此访客位置。除非您创建一个或多个新位置，否则无法删除 San Jose 访客位置。除非所有访客都将位于与 San Jose 相同的时区中，否则请创建至少一个具有所需时区的访客位置。

注释 访客访问时间基于访客位置的时区。如果访客位置的时区与系统时区不匹配，访客用户可能无法登录。在这种情况下，访客用户可能会收到“身份验证失败”错误。您可能会在调试报告中看到“访客活动时间段未开始 (Guest active time period not yet started)”错误消息。作为解决方法，您可以使用管理帐户 (Manage Accounts) 选项来调整访客接入开始时间，以匹配访客用户的本地时区。

您在此处添加的 SSID 可供发起人门户使用，因此发起人可以告知访客要连接的 SSID。

如果访客位置或 SSID 在发起人门户中进行配置或者分配给访客帐户，则无法删除。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **门户和组件 (Portals & Components)** > **设置 (Settings)** > **访客位置和 SSID (Guest Locations and SSIDs)**。

步骤 2 对于 **Guest Locations**：

a) 对于需要支持的每个时区，请输入 **Location name** 并从下拉列表中选取 **Time zone**。

b) 点击**添加 (Add)**。

注释 在 Guest Location 中，位置的名称、时区的名称和 GMT 时差是静态的；无法对其进行更改。GMT 时差不随夏令时更改而更改。GMT 偏移与列表中显示的相反。例如，*Etc/GMT+3* 实际上是 GMT-3。

注释 对于“从首次登录开始”的访客类型，请确保仅当您要在**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Types)** 页面中配置访问时间限制时配置访客位置（时区）。

步骤 3 对于 **Guest SSIDs**：

a) 输入将可供访客在访客位置使用的网络的 **SSID** 名称。

b) 点击**添加 (Add)**。

步骤 4 点击**保存 (Save)**。要恢复为上次保存的值，请点击**重置 (Reset)**。

下一步做什么

如果您已添加新的访客位置或 SSID，则可以：

- 提供 SSID 以供发起人在创建访客帐户时使用。请参阅发起人门户的门户设置，第 379 页。
- 向发起人组中添加访客位置，以使分配到该组的发起人在创建访客帐户时可以使用这些访客位置。请参阅配置发起人组，第 343 页。
- 使用自行注册的访客门户分配自行注册的访客可用的访客位置。请参阅创建自注册访客门户，第 334 页。
- 对于现有访客帐户，请手动编辑它们以添加 SSID 或位置。

访客密码策略规则

对于访客密码，Cisco ISE 具有以下内置规则：

- 访客密码策略适用于发起人门户、自注册门户、以 CSV 文件格式上传的帐户、使用 ERS API 创建的密码和用户创建的密码。
- 对访客密码策略的更改不会影响现有用户，直到访客密码过期并且需要更改为止。
- 密码区分大小写。
- 不能使用特殊字符 <、>、/、空格、逗号和 %。
- 最低长度和最小字符数要求适用于所有密码。
- 密码不能与用户名一样。
- 新密码不能与当前密码一样。
- 与访客帐户到期情况不一样，访客在密码到期之前不会收到通知。当访客密码到期时，发起人可以将密码重置为随机密码，或者访客也可以使用当前的登录凭证登录，然后更改其密码。

注释 客户默认用户名是四位字母字符，而密码是四位数字字符。简短、易于记忆的用户名和密码适用于短期客户。如果需要，您可以在 ISE 中更改用户名和密码长度。

设置访客密码策略和到期时间

您可以为所有访客门户定义密码策略。访客密码策略决定着如何为所有访客帐户生成密码。密码可以是字母、数字或特殊字符的组合。您还可以设置访客密码到期的天数，使系统在经过这些天之后要求访客重置其密码。

访客密码策略适用于发起人门户、自注册门户、以 CSV 文件格式上传的帐户、使用 ERS API 创建的密码和用户创建的密码。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **访客访问 (Guest Access)** > **设置 (Settings)** > **访客密码策略 (Guest Password Policy)**。

步骤 2 在 **Minimum password length** 字段以字符为单位为访客密码输入最低密码长度值。

步骤 3 指定每个字符集中访客可用于创建密码的字符。

在 **Allowed Characters and Minimums** 下选择以下选项之一以为访客指定密码策略：

- 使用各字符集的所有字符。
- 如要防止使用某些字符，请从下拉菜单选择 **Custom**，然后从预定义的完整字符集中删除这些字符。

步骤 4 输入每个字符集中使用的最低字符数。

全部四个字符集中所需字符的总数不得超出总体**最低密码长度**。

步骤 5 在 **Password Expiration** 下选择以下选项之一：

- 指定访客在首次登录之后必须更改密码的频率（以天为单位）。如果访客在密码到期之前不重置密码，则在下一次使用原始登录凭证登录网络时，系统会提示他们更改密码。
- 将密码设置为永不过期。

步骤 6 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

下一步做什么

您应自定义与密码策略相关的错误消息以提供密码要求。

1. 选择 **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人管理的访客门户或自注册访客门户 (Sponsored-Guest Portals or Self-Registered Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **错误消息 (Error Messages)**。
2. 搜索关键字 policy。

访客用户名策略规则

对于访客用户名策略，Cisco ISE 支持以下内置规则：

- 对访客用户名策略的更改不会影响现有用户，直到访客帐户过期并且需要更改为止。
- 不能使用特殊字符 <、>、/、空格、逗号和 %。
- 最低长度和最小字符数要求适用于所有系统生成的用户名，包括基于邮件地址的用户名。
- 密码不能与用户名一样。

设置访客用户名策略

您可以对访客用户名的创建规则进行配置。生成的用户名可以根据电子邮件地址或基于访客的名字和姓氏创建。当创建多个访客或访客姓名和电子邮件地址不可用时，发起人还可以创建任意数量的访客帐户以节省时间。随机生成的访客用户名由字母、数字和特殊字符组成。这些设置会影响所有访客。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **门户和组件 (Portals & Components)** > **设置 (Settings)** > **访客用户名策略 (Guest Username Policy)**。

步骤 2 在 **Minimum username length** 字段以字符为单位为访客用户名指定最低用户名长度。

步骤 3 在 **Username Criteria for Known Guests** 下选择其中一个选项以指定为已知访客创建用户名的策略。

步骤 4 在 **Characters Allowed in Randomly-Generated Usernames** 下选择其中一个选项以指定为访客创建随机用户名的策略：

- 使用各字符集的所有字符。
- 如要防止使用某些字符，请从下拉菜单选择 **Custom**，然后从预定义的完整字符集中删除这些字符。

步骤 5 输入每个字符集中使用的最低字符数。

从三个字符集中选取的字符总数不得超出 **Minimum username length** 中指定的数值。

步骤 6 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

下一步做什么

您应自定义与用户名策略相关的错误消息以提供用户名要求。

1. 选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人管理的访客门户、自注册访客门户、发起人门户或我的设备门户 (Sponsored-Guest Portals, Self-Registered Guest Portals, Sponsor Portals, or My Devices Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **错误消息 (Error Messages)**。
2. 搜索关键字 `policy`。

SMS 运营商和服务

SMS 服务会向使用需要提供凭证的访客门户的访客发送 SMS 通知。如果计划发送 SMS 消息，请启用此服务。尽可能配置和提供免费的 SMS 服务运营商，以降低您公司的支出。

Cisco ISE 支持向其自己的用户提供免费 SMS 服务的各种移动服务运营商。您可以使用这些运营商，而无需签订服务合同且无需在Cisco ISE 中配置其帐户凭证。其中包括 ATT、Orange、Sprint、T-Mobile 和 Verizon。

您还可以添加其他提供免费 SMS 服务的移动服务运营商或 Click-A-Tell 等全球 SMS 服务运营商。默认全局 SMS 服务运营商要求签订服务合同并且您必须在Cisco ISE 中配置其帐户凭证。

- 如果自行注册访客在 Self-Registration 窗体中选择自己的免费 SMS 服务运营商，系统将免费向他们发送包含其登录凭证的 SMS 通知。如果他们不选择 SMS 服务提供商，则由公司签约的默认全局 SMS 服务提供商发送 SMS 通知。
- 若要允许发起人向他们创建的访客发送SMS通知，应自定义发起人门户并选择所有可用的相应 SMS 服务提供商。如果没有为发起人门户选择任何 SMS 服务提供商，将由公司签约的默认全局 SMS 服务提供商提供 SMS 服务。

在Cisco ISE 中，SMS 提供商配置为 SMS 网关。SMS 网关会将来自Cisco ISE 的电子邮件转换为 SMS。SMS 网关可位于代理服务器之后。

配置 SMS 网关以向访客发送 SMS 通知

您必须在Cisco ISE 中对 SMS 网关进行如下设置：

- 使发起人能够向访客手动发送 SMS 通知以提供访客登录凭证和密码重置说明。
- 使访客能够在成功注册之后使用其登录凭证自动接收 SMS 通知。
- 使访客能够自动接收关于在访客帐户到期之前要采取的操作的 SMS 通知。

当在这些字段输入信息时，您应使用您的SMS运营商帐户的具体信息更新**[ ]**（例如 [USERNAME]、[PASSWORD]、[PROVIDER_ID] 等）中的所有文本。

开始之前

配置用于 SMS Email Gateway 选项的默认 SMTP 服务器。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **SMS 网关 (SMS Gateway)** > **SMS 网关提供商 (SMS Gateway Providers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入以下详细信息以配置 SMS 网关：

表 *43: SMS* 邮件网关的 *SMS* 网关设置

字段名称	使用指南
SMS Gateway Provider Domain	输入作为用于向提供商 SMS/MMS 网关发送消息的邮件地址主机部分的提供商域和作为此地址用户部分的访客帐户移动号码。
Provider account address	（可选） 输入作为电子邮件发件人地址（通常是帐户地址）的帐户地址并覆盖**默认电子邮件地址 (Default Email Address)** 全局设置（ **访客访问 (Guest Access)** > **设置 (Settings)**。

字段名称	使用指南
SMTP API destination address	（可选） 如果您使用的是需要具体帐户收件人地址的 SMTP SMS API（例如 Clickatell SMTP API），请输入 SMTP API 目标地址。 此地址用作邮件的 TO 地址并且系统会将访客帐户的移动号码代入消息的正文模板中。
SMTP API body template	（可选） 如果您使用的是需要使用特定邮件正文模板来发送 SMS 的 SMTP SMS API（例如 SMTP API），请输入 SMTP API 正文模板。 支持的动态替换为 $mobilenumber$、$timestamp$（格式 $YYYYMMDDHHHMISSmimi$）和 $message$。 您可以将 $timestamp$$mobilenumber$ 用于需要 URL 中有唯一标识符的 SMS 网关。

使用以下设置配置通过 HTTP API（GET 或 POST 方法）向访客和发起人发送 SMS 消息。

表 *44: SMS HTTP API* 的 *SMS* 网关设置

字段	使用指南
URL	输入 API 的 URL。 此字段不是 URL 编码的。系统将访客帐户的移动号码代入 URL 中。支持的动态替换为 $mobilenumber$ and $message$。 如果您将 HTTPS 用于 HTTP API，请在 URL 字符串中包含 HTTPS 并将您的提供商的受信任证书上传至Cisco ISE。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。
Data (Url encoded portion)	输入 GET 或 POST 请求的数据（URL 编码部分）。 此字段是 URL 编码的。如果使用默认 GET 方法，此数据附加于上述指定 URL 后面。
Use HTTP POST method for data portion	如果使用 POST 方法，请选中此选项。 上述指定数据用作 POST 请求的内容。
HTTP POST data content type	如果使用 POST 方法，请指定内容类型，例如“plain/text”或“application/xml”。
HTTPS Username HTTPS Password HTTPS Host name HTTPS Port number	输入此信息。

步骤 4

步骤 5 点击**提交 (Submit)**。

下一步做什么

如果您配置了新的 SMS 网关，您可以：

- 选择要在将有关帐户即将到期的 SMS 通知发送到访客时使用的 SMS 运营商。请参阅创建或编辑访客类型。
- 指定哪些已配置的 SMS 运营商应显示在 Self-Registration 表单以供自注册用户选取。请参阅创建自注册访客门户，第 334 页。

用于自行注册访客的社交媒体登录

访客可以选择社交媒体提供商来提供自行注册访客的凭证，而不用在访客门户中输入用户名和密码。要启用此功能，请将社交媒体网站配置为外部身份源，并配置允许用户使用该外部身份的门户（社交媒体提供商）。有关Cisco ISE 的社交媒体登录的其他信息，请参阅此处：
https://community.cisco.com/t5/security-documents/
how-to-configure-amp-use-a-facebook-social-media-login-on-ise/ta-p/3609532

在使用社交媒体进行身份验证后，访客可以编辑从社交媒体网站检索的信息。即便使用社交媒体凭证，社交媒体网站也不知道用户已使用该网站的信息登录。Cisco ISE 仍使用从社交媒体网站内部检索的信息以便日后跟踪。

您可以配置访客门户，以防止用户更改从社交媒体网站检索的信息，甚至阻止显示注册表。

社交登录访客流程

登录流程各不相同，具体取决于您如何配置门户设置。您可以配置无需用户注册、需要用户注册或需要用户注册和发起人批准的社交媒体登录。

1. 用户连接到自行注册门户，选择使用社交媒体登录。如果配置了访问代码，用户还必须在登录页面上输入访问代码。
2. 用户重定向到社交媒体网站进行身份验证。用户必须批准使用其社交媒体网站的基本配置文件信息。
3. 如果成功登录社交媒体网站，Cisco ISE 将从社交媒体网站检索有关用户的其他信息。Cisco ISE 使用社交媒体信息登录用户。
4. 登录后，用户可能必须接受 AUP，具体取决于配置。
5. 登录流程中的下一操作取决于配置：
   - 无注册：注册在后台完成。Facebook 向Cisco ISE 提供用户设备的令牌以供登录。

- 需注册：指示用户填写已使用社交媒体提供商提供的信息预填充的注册表单。这允许用户更正信息和添加缺失的信息，并提交更新的信息以供登录。如果在注册表单设置中配置了注册代码，则用户还必须输入注册代码。
- 需注册和发起人批准：除了允许用户更新社交媒体提供的信息外，还通知用户必须等待发起人批准。发起人收到一封电子邮件，请求批准或拒绝该帐户。如果发起人批准该帐户，则 Cisco ISE 会通过电子邮件告知用户他们已获得权限。用户连接访客门户，并使用社交媒体令牌自动登录。

6. 注册成功。用户将定向到**注册表单设置 (Registration Form Settings)** 上的**提交访客的自我注册表单后将访客定向到 (After submitting the guest form for self-registration, direct guest to)** 中配置的选项。用户帐户添加到为该门户的访客类型配置的终端身份组。
7. 在访客帐户过期或用户断开网络连接之前，用户一直拥有访问权。

   如果帐户过期，用户登录的唯一方法是重新激活帐户或删除该帐户。用户必须再次经历登录流程。

   如果用户断网并重新连接，则Cisco ISE 采取的操作取决于授权规则。如果用户点击类似

   ```
   rule if guestendpoint then permit access
   ```

   的授权，并且用户仍在终端组中，则用户将重定向到登录页面。如果用户仍然具备有效的令牌，则会自动登录。否则，用户必须重新注册一遍。

   如果用户不再位于终端组中，用户将重定向到访客页面，再注册一遍。

社交登录帐户持续时间

帐户的重新授权因连接方法而异：

- 对于 802.1x，默认授权规则

  ```
  if guestendpoint then permit access
  ```

  允许访客在用户设备进入睡眠状态或用户设备漫游到另一座建筑物时重新连接。当用户重新连接时，用户会重定向到访客页面，在该页面上使用令牌自动登录或重新开始注册。

- 对于 MAB，用户每次重新连接时，都会重定向到访客门户，并需要再次点击社交媒体。如果 Cisco ISE 仍具有该用户帐户的令牌（访客帐户尚未过期），则流程会立即成功完成登录，而无需与社交媒体提供商建立连接。

  要防止每次重新连接重定向到另一个社交登录页面，您可以配置一个记住设备的授权规则，并允许在帐户过期前访问。当帐户到期时，它会从终端组中删除，流程将重定向到访客重定向规则。例如：

  ```
  if wireless_mab and guest endpoint then permit access
  ```

  ```
  if wireless_mab then redirect to self-registration social media portal
  ```

报告和用户跟踪

思科 ISE 实时日志和 Facebook

- **身份验证身份存储库 (Authentication Identity Store)**：这是您在社交媒体应用中为Cisco ISE 创建的应用程序的名称。
- **Facebook 用户名 (Facebook username)**：这是 Facebook 报告的用户名。如果允许用户在注册期间更改其用户名，则Cisco ISE 报告的名称为社交媒体用户名。
- **SocialMediaIdentifier**：这是

  `https://facebook.com/<number>`

  ，其中的数字标识社交媒体用户。

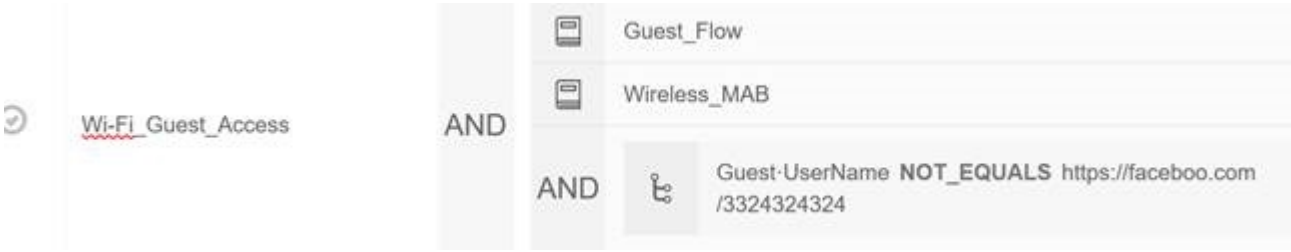
ISE 报告 (ISE Reports)：访客用户名是社交媒体网站上的用户名。

Facebook 分析 (Facebook Analytics)：您可以使用 Facebook 的分析功能通过 Facebook 社交登录查看谁在使用您的访客网络。

无线和 Facebook (Wireless and Facebook)：无线控制器上的**用户名 (User Name)** 是唯一的 Facebook ID，与实时日志上的 **SocialMediaIdentifier** 相同。要查看无线 UI 中的设置，请选择 **监控 (Monitor)** > **客户端 (Clients)** > **详细信息 (Detail)**，然后查看**用户名 (User Name)** 字段。

阻止已通过社交媒体身份验证的访客

您可以创建授权规则来阻止单个社交媒体用户。使用 Facebook 进行身份验证且令牌尚未到期时，此做法非常有用。以下示例显示使用 Facebook 用户名阻止的一个连接 Wi-Fi 的访客用户。



有关为Cisco ISE 配置社交登录的信息，请参阅配置社交媒体登录 ， 第 324 页。

配置社交媒体登录

开始之前

配置社交媒体网站，以便Cisco ISE 可以与之连接。目前仅支持 Facebook。

确保通过您的 NAD 打开以下 HTTPS 443 URL，以便Cisco ISE 可以访问 Facebook：

`facebook.co akamaihd.net akamai.co fbcdn.net`

注释 Facebook 的社交媒体登录 URL 是 HTTPS。并非所有 NAD 都支持重定向到 HTTPS URL。请参阅 https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=true。

步骤 1 在 Facebook 上，创建 Facebook 应用：

a) 登录https://developers.facebook.com并注册为开发者。

b) 在标题中选择**应用 (Apps)**，然后点击**添加新应用 (Add a New App)**。

步骤 2 添加 **Web** 类型的新**产品 Facebook 登录**。点击**设置 (Settings)** 并设置以下值：

- **客户端 OAuth 登录 (Client OAuth Login)**：否
- **Web OAuth 登录 (Web OAuth Login)**：是
- **强制 Web OAuth 重新身份验证 (Force Web OAuth Reauthentication)**：否
- **嵌入式浏览器 OAuth 登录 (Embedded Browser OAuth Login)**：否
- **有效的 OAuth 重定向 URI (Valid OAuth redirect URIs)**：从Cisco ISE 添加自动重定向 URL
- **从设备登录 (Login from Devices)**：否

a) **保存**

步骤 3 点击**应用审核 (App Review)**，然后为您的应用当前处于活动状态且可供公众使用 *(Your app is currently live and available to the public)* 选择**是 (Yes)**。

步骤 4 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **社交媒体登录 (Social Login)**。点击**添加 (Add)** 以创建新的社交媒体登录外部身份源。

- **类型 (Type)**：选择社交媒体登录提供方的类型。Facebook 目前是唯一选择。
- **应用 ID (App ID)**：输入来自 Facebook 应用的应用 ID。
- **应用密钥 (App Secret)**：输入来自 Facebook 应用的应用密钥。

步骤 5 在Cisco ISE 中，在自注册门户中启用**社交媒体登录 (Social Media Login)**。在门户页面上，选择 **门户和页面设置 (Portal & Page Settings)** > **登录页面设置 (Login Page Settings)**，选中**允许社交媒体登录 (Allow Social Login)** 复选框，然后输入以下详细信息：

- **在社交媒体登录后显示注册表 (Show registration form after social login)**：这可以让用户更改 Facebook 提供的信息。
- **要求访客获得批准 (Require guests to be approved)**：这会向用户告知发起人必须批准其帐户，并将向他们发送登录凭证。

步骤 6 选择 **管理 (Administration)** > **外部身份源 (External Identity Sources)**，选择 **Facebook 登录 (Facebook Login)** 窗口，然后编辑 Facebook 外部身份源。
这将创建需要添加到 Facebook 应用的重定向 URI。

步骤 7 在 Facebook 中，将上一步中的 URI 添加到 Facebook 应用。

下一步做什么

在 Facebook 中，可以显示有关应用的数据，其中会显示 Facebook 社交媒体登录的访客活动。

访客门户

当访问公司的人员希望使用公司网络访问互联网或者您的网络上的资源和服务时，您可以通过访客门户为他们提供网络访问权限。在进行配置后，员工可以使用这些访客门户访问您的公司网络。

三种默认访客门户：

- 热点访客门户：授予网络访问权限，而不需要任何凭证。通常，必须在授予网络访问权限之前接受可接受的用户策略 (AUP)。

  对于热点和自注册门户，无线设置支持要求访问代码登录。

- 发起人管理的访客门户：网络访问权限由创建访客帐户的发起人授予，并为访客提供登录凭证。
- 自注册访客门户：访客可以创建自己的帐户和凭证，可能需要发起人批准后才能获得网络访问权限。

Cisco ISE 可托管多个访客门户，包括一组预定义的默认门户。

访客门户的凭证

Cisco ISE 通过要求访客使用各种凭证，提供安全的网络访问。您可以要求访客使用以下一个或多个凭证登录。

- 用户名：必填。适用于使用最终用户门户（热点访客门户除外）的所有访客，系统根据用户名策略派生用户名。用户名策略仅适用于系统生成的用户名，而不适用于使用访客 API 编程接口或自行注册流程指定的用户名。您可以在以下位置配置应用于用户名的策略设置： **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **设置 (Settings)** > **访客用户名策略 (Guest Username Policy)**。可以通过邮件、SMS 或打印形式告知访客其用户名。
- 密码：必填。适用于使用最终用户门户（热点访客门户除外）的所有访客，根据密码策略派生密码。您可以在以下位置配置应用于密码的策略设置： **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **设置 (Settings)** > **访客密码策略 (Guest Password Policy)**。可以通过邮件、SMS 或打印形式告知访客其密码。
- 访问代码：可选。适用于使用热点访客门户和需要提供凭证的访客门户的访客。访问代码主要是提供给实际存在的访客（通过白板以肉眼方式或通过前台接待人员以口头方式）的本地已知代码。不在场的人无法获悉和使用此代码以获得网络访问权限。如果启用了访问代码设置，将出现以下情况：
  - 系统会提示发起人管理的访客在 Login 页面上输入此代码（以及用户名和密码）。
  - 系统会提示使用热点访客门户的访客在可接受使用政策 (AUP) 页面输入此代码。

- 注册码：可选。适用于自行注册访客，在如何向自行注册访客提供此代码方面其类似于访问代码。如果启用注册代码设置，系统会提示自行注册访客在 Self-Registration 窗体上输入此代码。

用户名和密码可由您公司的发起人提供（发起人管理的访客），也可以将需要提供凭证的访客门户配置为允许访客自行注册以获取这些凭证。

相关主题

用户身份验证策略设置

访客类型和用户身份组，第 309 页

访客使用热点访客门户进行访问

Cisco ISE 提供的网络接入功能包括“热点”，访客无需凭证登录即可使用这些接入点访问互联网。当访客使用计算机或任何设备的浏览器连接到热点网络并试图连接到某个网站时，就会被自动重定向至热点访客门户。该功能同时支持有线和无线 (Wi-Fi) 连接。

作为备选访客门户，热点访客门户允许您提供网络接入而无需访客具备用户名和密码，由此可减少对访客帐户进行管理的需求。相反，Cisco ISE 与网络接入设备 (NAD) 和设备注册 Web 身份验证相配合，向访客设备直接提供网络接入。某些情况下，访客可能需要使用访问代码才能登录。通常情况下，该访问代码是本地提供给公司内部实际存在的访客的代码。

如果您支持热点访客门户：

- 根据热点访客门户的配置和设置，如果满足访客访问条件，访客即可访问网络。
- Cisco ISE 为您提供默认访客身份组、访客终端，使您可以密切跟踪访客设备。

访客使用需要提供凭证的访客门户进行访问

您可以使用需要提供凭证的访客门户识别并授权外部用户临时访问内部网络和服务以及互联网。发起人可以为能够通过在门户的 Login 页面中输入这些凭证来访问网络的授权访问者创建临时用户名和密码。

可以设置需要提供凭证的访客门户，以便访客可以使用获取的用户名和密码登录：

- 来自发起人。在此访客流程中，当访客进入公司场地并设置具有单独访客帐户时，发起人（例如前台接待人员）会向其致意。
- 在访客使用可选注册代码或访问代码自行注册后。在此访客流程中，访客可以在没有任何人为交互的情况下访问互联网，并且Cisco ISE 可确保这些访客具有可用于合规的唯一标识符。
- 在访客使用可选注册代码或访问代码自行注册后，但是仅在发起人批准对访客帐户的请求后。在此访客流程中，系统会为访客提供网络访问权限，但是仅在执行额外的筛选后才提供。

您还可以强制用户在登录时输入新密码。

通过Cisco ISE，您可以创建多个需要提供凭证的访客门户，您可以使用这些门户基于不同条件允许进行访客访问。例如，对于每月承包商，您可能具有与用于日常访问者的门户不同的门户。

员工使用需要提供凭证的访客门户进行访问

员工还可以通过使用员工凭证在须提供凭证的访客门户上注册来访问网络，只要为该门户配置的身份源序列可以获取其凭证即可。

访客设备合规性

当访客和非访客通过需要提供凭证的访客门户访问网络时，您可以在允许获得访问权限之前检查其设备的合规性。可以将他们路由至“客户端调配”(Client Provisioning) 窗口，要求他们首先下载终端安全评估代理，查看其终端安全评估配置文件，验证他们的设备是否合规。具体做法是，在需要提供凭证的访客门户的**访客设备合规性设置 (Guest Device Compliance Settings)** 中启用此选项，此门户将在访客流程中显示“客户端调配”(Client Provisioning) 窗口。

注释 访客流程中的客户端终端安全评估仅支持临时代理。

客户端调配服务为访客提供终端安全评估和补救。客户端调配门户只通过中心网络身份验证 (CWA) 访客部署提供。访客登录流程执行CWA，在执行可接受的使用策略和更改密码检查后，需要提供凭证的访客门户被重新定向到客户端调配门户。终端安全评估子系统在网络访问设备上执行授权更改 (CoA)，在终端安全评估后，重新授权客户端连接。

访客门户配置任务

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和Cisco ISE提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

在创建新门户或编辑默认门户后，您必须授权使用该门户。授权使用门户后，您所进行的任何后续配置更改便会立即生效。

如果您选择删除门户，则必须先删除与其关联的任何授权策略规则和授权配置文件，或者将其修改为使用其他门户。

使用以下针对配置不同访客门户相关任务编制的表格。

任务	热点访客门户	发起人管理的访客门户	自注册的访客门户
启用策略服务，第 329 页	必填	必填	必填
为访客门户添加证书，第 329 页	必填	必填	必填
创建外部身份源，第 330 页	不适用	必填	必填

任务	热点访客门户	发起人管理的访客门户	自注册的访客门户
创建身份源序列，第 331 页	不适用	必填	必填
创建终端身份组，第 661 页	必填	不是必填项（由访客类型定义）	不是必填项（由访客类型定义）
创建热点访客门户，第 332 页	必填	不适用	不适用
创建发起人管理的访客门户，第 333 页	不适用	必填	不适用
创建自注册访客门户，第 334 页	不适用	不适用	必填
授权门户，第 338 页	必填	必填	必填
自定义访客门户，第 339 页	可选	可选	可选

启用策略服务

为了支持Cisco ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 点击节点并点击**编辑 (Edit)**。

步骤 3 在**常规设置 (General Settings)** 选项卡下，启用**策略服务 (Policy Service)** 切换按钮。

步骤 4 选中**启用会话服务 (Enable Session Services)** 复选框。

步骤 5 点击**保存 (Save)**。

为访客门户添加证书

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为默认门户证书组。

步骤 1

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 3 添加一个系统证书并将其分配到您希望用于该门户的证书组标签。

在创建或编辑门户期间，此证书组标签可供选择。

步骤 4 选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 访客门户 **(Guest Portals)** > 创建或编辑 **(Create or Edit)** > 门户设置 **(Portal Settings)**。

步骤 5 从与新添加证书关联的 **Certificate group tag** 下拉列表中选择特定的证书组标签。

创建外部身份源

Cisco ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

注释 要使用被动身份服务以接收和共享经过身份验证的用户身份，请参阅其他被动身份服务提供程序，第 522 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅将 Active Directory 用作外部身份源，第 471 页。
- 选择 **LDAP** 以添加 LDAP 身份源。有关详细信息，请参阅LDAP，第 561 页。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关详细信息，请参阅RADIUS 令牌身份源，第 582 页。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关详细信息，请参阅RSA 身份源，第 588 页。
- 选择 **SAML Id 提供程序 (SAML Id Providers)** 添加身份提供程序 (IdP)，例如 Oracle 访问管理器。有关详细信息，请参阅SAMLv2 身份提供者作为外部身份源，第 594 页。
- 选择**社交登录 (Social Login)** 以将社交登录（如 Facebook）设置为外部身份源。请参阅用于自行注册访客的社交媒体登录，第 322 页。

配置访客门户以重定向至 SAML IDP 门户进行身份验证

您可以配置访客门户以允许将用户被重定向至 SAML IDP 门户进行身份验证。

在访客门户（自注册或发起访客）中配置设置允许以下身份提供程序访客门户用于登录 *(Allow the following identity-provider guest portal to be used for login)* 会在该门户中启用新的登录区域。如果用户选择该登录选项，将被重定向至备用身份门户（他们看不到），然后重定向至 SAML IDP 登录门户进行身份验证。

例如访客门户可有员工登录的链接。取代登录现有的门户的操作是，用户点击员工登录链接，并被重定向至 SAML IDP 单一登录门户。员工可使用上次以此 SAML IDP 登录的令牌重新连接，或者在该 SAML 站点登录。这样同一门户可处理来自单一 SSID 的访客和员工。

以下步骤显示如何配置访客门户以调用另一门户，而另一门户配置为使用SAML IDP进行身份验证。

步骤 1 配置外部身份源有关更多详细信息，请参阅 SAMLv2 身份提供者作为外部身份源，第 594 页。

步骤 2 为 SAML 提供程序创建一个访客门户。在“门户设置”(Portal Settings) 中将**身份验证方法 (Authentication method)** 设置为 SAML 提供程序。用户不会看到此门户，它只是一个将用户导向 SAML IDP 登录页面的点位符。其他门户可配置为重定向至此子门户，如下所述。

步骤 3 通过重定向至您刚创建的 SAML 提供程序门户的访客门户选项，创建一个访客门户。这是将重定向至子门户的主门户。

您可能要自定义此门户的外观以使其看起来像 SAML 提供程序。

a) 在主门户的“登录页面设置”(Login Page Settings) 页面，选中**允许以下身份提供程序访客门户用于登录 (Allow the following identity-provider guest portal to be used for login)**。

b) 选择配置为与 SAML 提供程序一起使用的访客门户。

创建身份源序列

开始之前

确保您已经在Cisco ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)** > **添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望Cisco ISE 搜索数据库的顺序。

步骤 6 在 **Advanced Search List** 区域中选择以下选项之一：

- **请勿访问序列中的其他存储区并将 AuthenticationStatus 属性设置为 ProcessError**：如果用户未在第一个选定身份源中找到用户，而您希望Cisco ISE 中止搜索，请选择此选项。
- **视为未找到用户并继续至序列中的下一存储区 (Treat as if the user was not found and proceed to the next store in the sequence)**：如果未在第一个选定身份源中找到用户，而您希望Cisco ISE 仍继续按照序列搜索其他选定身份源，请选择此选项。

  在处理请求时，Cisco ISE 会按照序列搜索这些身份源。确保“选定列表”(Selected list) 字段所列出的身份源的顺序是您希望Cisco ISE 搜索身份源的顺序。

步骤 7 点击**提交 (Submit)** 创建您可以稍后在策略中使用的身份源序列。

创建终端身份组

Cisco ISE 将其所发现的终端划分至相应的终端身份组。Cisco ISE 拥有若干个系统定义的终端身份组。您还从 Endpoint Identity Groups 页面创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为您想要创建的终端身份组输入**名称**（请勿在终端身份组的名称中包含空格）。

步骤 4 为您想要创建的终端身份组输入**说明**。

步骤 5 点击**父级组 (Parent Group)** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

步骤 6 点击**提交 (Submit)**。

创建热点访客门户

您可以提供热点访客门户，以使访客能够在无需用户名和密码进行登录的情况下连接到网络。进行登录可能需要访问代码。

您可以创建新的热点访客门户，也可以编辑或复制现有热点访客门户。您可以删除任何热点访客门户，包括Cisco ISE 提供的默认门户。

您在 **Portal Behavior and Flow Settings** 选项卡上对 Page Settings 进行的任何更改都会反映在访客流程图中的图形流程中。如果您启用某个页面（例如 AUP 页面），则该页面会显示在流程中，并且访客将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除，并为访客显示下一个已启用页面。

所有页面设置（Authentication Success Settings 除外）都可选。

开始之前

- 确保您具有配置用于此门户的所需证书和终端身份组。
- 确保Cisco ISE 支持访客将为热点门户连接到的 WLC。请参阅Cisco ISE 版本对应的《身份服务引擎网络组件兼容性》指南，。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

创建发起人管理的访客门户

您可以提供发起人管理的访客门户，让指定发起人向访客授予访问权限。

您可以创建一个新的发起人管理的访客门户，也可以编辑或复制现有门户。您可以删除任何发起人管理的访客门户，包括Cisco ISE 提供的默认门户。

您在 **Portal Behavior and Flow Settings** 选项卡上对 Page Settings 进行的任何更改都会反映在访客流程图中的图形流程中。如果您启用某个页面（例如AUP页面），则该页面会显示在流程中，并且访客将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除，并为访客显示下一个已启用页面。

通过以下所有页面设置，您可以为访客显示可接受使用政策 (AUP) 并要求访客接受政策：

- 登录页面设置
- 可接受使用政策 (AUP) 页面设置
- BYOD 设置

开始之前

确保您具有为配合此门户使用而配置的所需证书、外部身份源和身份源序列。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 如果创建新门户，请在**创建访客门户 (Create Guest Portal)** 对话框中选择**发起人管理的访客门户 (Sponsored-Guest Portal)** 作为门户类型，然后点击**继续 (Continue)**。

步骤 3 在**访客名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 4 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 5 在**门户设置 (Portal Settings)** 中更新端口、以太网接口、证书组标签、身份源序列、身份验证方法等的默认值，然后定义适用于整个门户的行为。

步骤 6 更新以下适用于每个特定页面的设置：

- **登录页面设置 (Login Page Settings)**：指定访客凭证和登录指南。如果您选择**允许访客创建帐户 (Allow guests to create their accounts)** 选项，用户将能够创建自己的访客帐户。如果未选择此选项，则需要发起人来创建访客帐户。

  注释　如果您已在“身份验证方法”(Authentication Method) 字段选择了身份提供程序 (IdP)，则“登录页面设置”(Login Page Settings) 选项将被禁用。

- **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)**：为访客添加单独的 AUP 页面并定义可接受使用政策行为，包括使用需要提供凭证的访客门户的员工。
- **员工更改密码设置 (Employee Change Password Settings)**：要求访客在第一次登录后更改其密码。
- **访客设备注册设置 (Guest Device Registration Settings)**：选择Cisco ISE 是自动注册访客设备还是显示访客可以手动注册其设备的页面。

- **BYOD 设置 (BYOD Settings)**：允许员工使用个人设备访问网络。
- **登录后横幅页面设置 (Post-Login Banner Page Settings)**：授予访客网络访问权限前向其通知额外信息。
- **访客设备合规性设置 (Guest Device Compliance Settings)**：将访客路由到“客户端调配”(Client Provisioning) 页面并要求其先下载终端安全评估代理。
- **VLAN DHCP 释放页面设置 (VLAN DHCP Release Page Settings)**：从访客 VLAN 释放访客设备 IP 地址并进行续订，以访问网络上的其他 VLAN。
- **身份验证成功设置 (Authentication Success Settings)**：指定访客通过身份验证后应看到的内容。
- **支持信息页面设置 (Support Information Page Settings)**：帮助访客提供信息，以便服务台用于排除网络接入问题。

步骤 7 点击**保存 (Save)**。系统生成的 URL 显示为**门户测试 URL (Portal test URL)**，您可以使用它来访问门户并进行测试。

下一步做什么

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，ISE 会选择第一个活动 PSN。

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

创建自注册访客门户

您可以提供自注册门户以允许访客自行注册并创建自己的帐户，从而可以访问网络。您还可以要求这些帐户须经发起人批准后才能授予访问权限。

您可以创建新的自注册访客门户，也可以编辑或复制现有的门户。您可以删除任何自注册访客门户，包括Cisco ISE 提供的默认门户。

您在 **Portal Behavior and Flow Settings** 选项卡上对 Page Settings 进行的任何更改都会反映在访客流程图中的图形流程中。如果您启用某个页面（例如AUP页面），则该页面会显示在流程中，并且访客将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除，并为访客显示下一个已启用页面。

通过以下所有页面设置，您可以为访客显示可接受使用政策 (AUP) 并要求访客接受政策：

- 登录页面设置
- 自注册页面设置
- 自注册成功页面设置
- 可接受使用政策 (AUP) 页面设置
- BYOD 设置

开始之前

确保您已为该门户配置了必要的证书、外部身份源和身份源序列。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户** > **创建、编辑或复制 (Create, Edit or Duplicate)**。。

步骤 2 如果要创建新门户，请在 **Create Guest Portal** 对话框中选择 **Self-Registered Guest Portal** 作为门户类型，并点击 **Continue**。

步骤 3 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 4 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 5 在**门户设置 (Portal Setting)** 字段，请更新对门户行为进行定义的端口、以太网接口、证书组标记、身份源序列、身份验证方法，以及其他设置的默认值。

有关门户设置字段的详细信息，请参阅 需要提供凭证的访客门户的门户设置，第 365 页。

步骤 6 更新以下适用于每个特定页面的设置：

- **登录页面设置 (Login Page Settings)**：指定访客凭证和登录指南。有关详细信息，请参阅需要提供凭证的访客门户的登录页面设置，第 367 页。
- **自注册页面设置 (Self-Registration Page Settings)**：指定自注册访客将阅读并应输入到自注册表单中的信息，另外还包括访客提交表单后的访客体验。
- **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)**：为访客添加单独的 AUP 页面并定义可接受使用政策行为，包括使用需要提供凭证的访客门户的员工。有关详细信息，请参阅 需要提供凭证的访客门户的可接受使用政策 (AUP) 页面设置，第 372 页。
- **员工更改密码设置 (Employee Change Password Settings)**：要求访客在第一次登录后更改其密码。
- **访客设备注册设置 (Guest Device Registration Settings)**：选择Cisco ISE 是自动注册访客设备还是显示访客可以手动注册其设备的页面。
- **BYOD 设置 (BYOD Settings)**：允许员工使用个人设备访问网络。有关详细信息，请参阅 需要提供凭证的访客门户的 BYOD 设置，第 373 页。有关详细信息，请参阅 需要提供凭证的访客门户的 BYOD 设置，第 373 页。
- **登录后横幅页面 (Include a Post-Login Banner page)**：在用户成功登录后、被授予网络访问权限之前显示其他信息。
- **访客设备合规性设置 (Guest Device Compliance Settings)**：将访客重定向到“客户端调配”(Client Provisioning) 页面以进行终端安全评估。有关详细信息，请参阅需要提供凭证的访客门户的访客设备合规性设置，第 375 页。
- **VLAN DHCP 释放页面设置 (VLAN DHCP Release Page Settings)**：从访客 VLAN 释放访客设备 IP 地址并进行续订，以访问网络上的其他 VLAN。有关详细信息，请参阅 需要提供凭证的访客门户的 BYOD 设置，第 373 页。
- **身份验证成功设置 (Authentication Success Settings)**：指定在对访客进行身份验证后应将其定向至何处。如果您在身份验证后将一个访客重定向到外部URL，可能会在解析URL地址和重定向会话时有延迟。有关详细信息，请参阅访客门户的身份验证成功设置，第 376 页。
- **支持信息页面设置 (Support Information Page Settings)**：帮助访客提供信息，以便服务台用于排除网络接入问题。

步骤 7 点击**保存 (Save)**。系统生成的 URL 显示为**门户测试 URL (Portal test URL)**，您可以使用它来访问门户并进行测试。

下一步做什么

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，ISE 会选择第一个活动 PSN。

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

发起人自注册帐户批准

当您将注册访客配置为需要让其帐户获得批准时，Cisco ISE 会向批准者发送电子邮件以批准帐户。批准者可以是被访问者或发起人用户。

当批准者是发起人时，您可以配置电子邮件以包含用来拒绝或批准帐户的链接。批准链接包含一个令牌，可将批准操作关联到发起人的电子邮件地址。您可以要求发起人进行身份验证，而忽略令牌。令牌也可能超时，这需要发起人在批准帐户之前进行身份验证。

您应在自注册门户的**注册表单设置 (Registration Form Settings)** 中配置帐户批准选项。此功能也称为一键式发起人批准。

当发起人打开电子邮件并点击批准链接时，具体操作因批准者的配置而异。

如果将**批准请求电子邮件收件方 (Email approval request to)** 配置为：

- **被访问者**
  - 访客帐户**不需要**身份验证：一次点击即可批准帐户。
  - 访客帐户**需要**身份验证：系统将发起人定向到发起人门户，发起人必须在这里输入其凭证才能批准帐户。
- **下面列出的发起人邮件地址 (Sponsor email addresses listed below)**：Cisco ISE 将电子邮件发送到所有提供的电子邮件地址。当其中一个发起人点击批准或拒绝链接时，他们会被定向到其发起人门户。该发起人需输入其凭证，系统会对其进行验证。如果他们所属的发起人组允许他们批准访客帐户，则他们可以批准该帐户。如果凭证失败，则Cisco ISE 会通知发起人登录到发起人门户，并手动批准帐户。

考虑因素

- 如果正在从以前版本的Cisco ISE 升级或恢复数据库，则必须手动插入批准或拒绝链接。打开自注册访客门户并选择“门户页面自定义”(Portal Page Customization) 选项卡。向下滚动并选择“批准请求电子邮件”(Approval Request Email) 窗口。点击该窗口**邮件正文**部分中的**插入批准/拒绝链接 (Insert Approve/Deny Links)**。

- 仅支持使用 Active Directory 和 LDAP 进行身份验证的发起人门户。发起人映射到的发起人组必须包含发起人所属的 Active Directory 组。
- 如果存在发起人列表，则使用第一个门户的自定义，即使该门户不是发起人登录的门户也不例外。
- 发起人必须使用支持 HTML 的电子邮件客户端才能使用批准和拒绝链接。
- 如果发起人的电子邮件地址不是有效的发起人，则不会发送批准电子邮件。

有关一键式发起人批准的详细信息，请参阅Cisco ISE 社区资源：**ISE 一键式发起人批准常见问题解答**。本文档还有一个视频链接，其中介绍了整个过程。

配置帐户批准电子邮件链接

您可以要求自注册访客获得批准后才能访问网络。Cisco ISE 使用被访问者的电子邮件地址通知审批者。审批者是被访问者或发起人。有关批准的详细信息，请参阅发起人自注册帐户批准，第 336 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客 (Guest)** > **配置 (Configure)** > **访客门户 (Guest Portals)**。，然后选择要为电子邮件帐户批准链接配置的自注册门户。

步骤 2 展开**自注册页面设置 (Self-Registration Page Settings)** 选项卡。

步骤 3 选中**要求自注册访客获得批准 (Require self-registered guests to be approved)**。

系统将显示**批准/拒绝链接设置 (Approve/Deny Link Settings)** 部分。它还使用批准和拒绝链接填充审批请求电子邮件的电子邮件配置。

输入下列详细信息：

- **要求自注册访客获得批准 (Require self-registered guests to be approved)**：指定使用此门户的自注册访客需要获得获得发起人的批准，才能收到其访客凭证。点击此选项会显示有关发起人如何批准自注册访客的更多选项。
  - 允许访客在获得发起人批准后通过自注册自动登录 (Allow guests to login automatically from self-registration after sponsor's approval)：自注册访客将在发起人批准后自动登录。
  - **批准请求电子邮件收件方 (Email approval request to)** - 如果选择：
    - **下面列出的发起人电子邮件地址 (Sponsor email addresses listed below)**：输入被指定为批准者的发起人的一个或多个电子邮件地址，或邮件收发器，所有访客批准请求都会发送到上述地址。如果电子邮件地址无效，则批准会失败。
    - **被访问者 (Person being visited)**：显示**要求发起人提供身份验证凭证 (Require sponsor to provide credentials for authentication)** 字段，并启用**要包括的字段 (Fields to include)** 中的**必填 (Required)** 选项（如果之前已禁用）。自注册表单上会显示这些字段，要求自注册访客提供这些信息。如果电子邮件地址无效，则批准会失败。
  - **批准/拒绝链接设置 (Approve/Deny Link Settings)** - 此部分可以让您配置：
    - **链接有效期 (Links are valid for)**：您可以设置帐户批准链接的到期期限。

- **要求发起人提供身份验证凭证 (Require sponsor to provide credentials for authentication)**：选中此选项可强制发起人输入凭证以批准帐户（即使此部分中的配置不要求如此）。仅当将**要求自注册访客获得批准 (Require self-registered guests to be approved)** 设置为**被访问者 (person being visited)** 时，此字段才可见。
- **发起人与发起人门户匹配以验证批准权限 (Sponsor is matched to a Sponsor Portal to verify approval privileges)**：点击**详细信息 (Details)** 以选择要搜索的门户，确认发起人是有效的系统用户、发起人组的成员，并且该组的成员有权批准帐户。每个发起人门户都有一个身份源序列，用于标识发起人。门户按其列出的顺序使用。列表中的第一个门户确定发起人门户中使用的样式和自定义。

授权门户

当授权门户时，将会设置网络访问的网络授权配置文件和规则。

开始之前

您必须先创建门户，然后才能对其进行授权。

步骤 1 为门户设置特殊授权配置文件。

步骤 2 为配置文件创建授权策略规则。

创建授权配置文件

各门户要求您为其设置特殊的授权配置文件。

开始之前

如果不打算使用默认门户，您必须先创建门户以便将门户名称与授权配置文件关联。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 使用您希望授权门户使用的名称创建授权配置文件。

下一步做什么

您应当创建门户授权策略规则，用于新创建的授权配置文件。

创建用于热点和 MDM 门户的授权策略规则

要配置供门户在响应用户（访客、发起人、员工）的访问请求时使用的重定向 URL，请为该门户定义授权策略规则。

url-redirect 会根据门户类型采取以下形式，其中：

ip:port：IP 地址和端口号

PortalID：唯一端口名称

对于热点访客门户：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

对于移动设备管理 (MDM) 门户：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)** 以在**标准 (Standard)** 策略下创建新授权策略。

步骤 2 对于**条件 (Conditions)**，请选择要用于门户验证的终端身份组。例如，对于热点访客门户，选择默认的 **GuestEndpoints** 终端身份组；而对于 MDM 门户，选择默认的 **RegisteredDevices** 终端身份组。

注释 由于热点访客门户仅颁发终止 CoA，请不要将 Network Access:UseCase EQUALS Guest Flow 用作热点访客授权策略中的一个验证条件。而是匹配终端归属的身份组用于验证。例如，

- 如果为访客终端 + 无线 MAB，则允许访问
- 如果为无线 MAB，则热点重定向

步骤 3 对于 **Permissions**，请选择创建的门户授权配置文件。

注释 在使用启用了 MAC 选项的字典属性创建授权条件（例如 RADIUS.Calling-Station-ID）时，必须使用 Mac 运算符（例如 Mac_equals）支持不同的 MAC 格式。

自定义访客门户

可以通过自定义门户主题、更改门户页面上的 UI 元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户（访客、发起人，在适当的情况下也可以是员工）体验。有关自定义门户的详细信息，请参阅 自定义最终用户 Web 门户 ，第 391 页。

配置定期 AUP 接受

选择 **策略 (Policy)** > **策略集 (Policy Sets)**，在列表顶部创建新的授权规则，使之在 AUP 期限到期时，将访客用户重定向到需要提供凭证的门户。使用条件比较 LastAUPAcceptanceHours 与需要的最大小时数，例如 LastAUPAcceptanceHours > 8。您可以查找 1 到 999 小时的小时范围。

下一步做什么

要验证终端是否已接收 AUP 设置，请执行以下操作：

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份 (Identities)** > **终端 (Endpoints)**。
2. 点击终端，验证终端是否有 AUP 最后被接受的时间 (*AUPAcceptedTime*)。

强制定期 AUP

可以通过在策略中使用 LastAUPAcceptance 强制用户接受 AUP。

```
If LastAUPAcceptance >= 24: Hotspot Redirect
If LastAUPacceptance < 24: PermitAccess
If Wireless_MAB: Hotspot Redirect
```

此示例显示如何每 24 小时在热点门户上强制执行 AUP。

1. 如果用户在 24 小时之前接受过 AUP，则必须再次接受 AUP（重新开始）。
2. 如果用户在 24 小时之内接受过 AUP，则继续会话。
3. 首次访问网络 (MAB) 时，他们必须接受 AUP。

对于需要提供凭证的门户，只要为此门户启用 AUP，即可使用相同规则。

访客 Remember Me

此功能使Cisco ISE 能够在报告和日志中显示访客的用户名，而不是 MAC 地址。

当访客首次进行身份验证时，用户设备的 MAC 地址保存在终端组中，报告中使用的是用户名。如果用户断开连接，然后重新连接到网络，则 MAC 地址已在终端组中，因此用户不必重新登录（身份验证）。在这种情况下，用户名不可用，因此报告和日志中使用 MAC 地址。

从Cisco ISE 2.3 开始，ISE 会保留门户用户 ID，并将其用于某些报告中，具体取决于版本。

- Cisco ISE 2.3 实施了此功能，但您无法将其关闭。
- Cisco ISE 2.4 添加了禁用此功能的选项，它位于 **访客 (Guest)** > **设置 (Settings)** > **日志记录 (Logging)**。默认情况下，新安装的产品中启用该选项，升级和恢复以前的版本时禁用它。

有关 Remember Me 日志记录问题的详细信息，请参阅以下Cisco ISE 社区资源：ISE 2.3+ Remember Me 访客使用访客终端组日志记录显示 (ISE 2.3+ Remember Me guest using guest endpoint group logging display)。

有关配置 Remember Me 的详细信息，请参阅Cisco ISE 访客访问部署指南：https://communities.cisco.com/docs/DOC-77590

有关每个版本支持的报告方法的详细信息，请参阅该版本的发行说明。

发起人门户

发起人门户是Cisco ISE 访客服务主要的组件之一。使用发起人门户，发起人可以为授权的访客创建和管理临时帐户，以安全地访问公司网络或互联网。创建访客帐户后，发起人还可以使用发起人门户以打印文件、邮件或短信的形式向访客提供帐户详细信息。向自助注册的访客提供对公司网络的访问权限之前，系统可能会通过邮件要求发起人批准其访客帐户。

在发起人门户上管理客户帐户

发起人门户登录流程

发起人组指定分配给发起人用户的一组权限。当发起人登录发起人门户时：

1. ISE 验证发起人的凭证。
2. 如果发起人成功通过身份验证，Cisco ISE 会搜索所有可用发起人组，以查找发起人所属的发起人组。如果符合以下两个条件，则发起人匹配或属于发起人组：
   - 发起人是一个已配置成员组的成员。
   - 如果您使用的是其他条件，则此发起人的所有条件评估为 true。
3. 如果发起人属于发起人组，则发起人将从此组获取权限。发起人可以属于多个发起人组，在此情况下，这些组的权限将合并。如果发起人不属于任何发起人组，则登录发起人门户时将失败。

发起人组及其权限独立于发起人门户。无论发起人登录哪个发起人门户，均使用相同的算法来匹配发起人组。

使用发起人门户

使用发起人门户为授权访问者创建用于安全访问企业网络或互联网的临时访客帐户。在创建访客帐户后，可以使用发起人门户管理这些帐户并向访客提供帐户详细信息。

在发起人门户上，发起人可以单独创建新的访客帐户，或从文件导入一组用户。

注释 从外部身份存储区（例如 Active Directory）授权的 ISE 管理员可以是发起人组的一部分。但是，内部管理员帐户（例如，默认“管理员”帐户）不能是发起人组的一部分。

有多种方法可打开发起人门户：

- 在管理员控制台中，使用**管理帐户 (Manage Accounts)** 链接。在管理员控制台上，点击**访客访问 (Guest Access) > 管理帐户 (Manage Accounts)**。点击**管理帐户 (Manage Accounts)** 时，您将分配到可访问 ALL_ACCOUNTS 的默认发起人组。可以创建新的访客帐户，但无法通知这些访客，因为没有电子邮件地址可用于接收来自访客的帐户激活请求。具有相同权限的发起人在登录发起人门户并搜索这些帐户时，可以发送通知。

此步骤要求您在发起人门户的**门户行为和流程设置 (Portal Behavior and Flow Settings)** 窗口中配置的 FQDN 在 DNS 服务器中。

如果通过 NAT 防火墙访问发起人门户，连接将使用端口 9002。

- 在管理员控制台的“发起人门户配置”(Sponsor Portal configuration) 窗口中。点击 **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)**，打开发起人门户，然后点击**说明 (Description)** 字段右侧的**门户测试 URL (Portal Test URL)** 链接。
- 在浏览器中，打开在发起人门户的**门户设置 (Portal Settings)** 窗口中配置的 URL (FQDN)（必须在 DNS 服务器中定义）。

后续操作

有关如何使用发起人门户的信息，请参阅适用于您的 ISE 版本的《发起人门户用户指南》https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html。

管理发起人帐户

发起人用户是通过发起人门户创建和管理访客用户帐户的组织员工或承包商。Cisco ISE 会通过本地数据库或通过外部轻型目录访问协议 (LDAP)、Microsoft Active Directory 或 SAML 身份库对发起人进行身份验证。如果不使用外部资源，则必须为发起人创建内部用户帐户。

发起人组

在使用任何发起人门户时，发起人组控制对发起人的授权。如果发起人是发起人组的成员，则该发起人拥有在该组中定义的权限。

如果以下两项全都符合，则发起人被视为发起人组的成员：

1. 发起人属于在发起人组中定义的至少一个成员组。成员组可以是用户身份组或从外部身份源中选择的组，例如 Active Directory。
2. 发起人满足在发起人组指定的所有其他条件。其他条件是指字典属性上定义的条件，是可选的。这些条件的行为类似于授权策略中所用的条件。

一个发起人可以是多个发起人组的成员。如果是，该发起人拥有所有这些组的权限，如下所述：

- 如果在任何组中启用了某个权限，例如“删除访客帐户”，则会授权其该权限。
- 发起人可以使用任何组中的访客类型创建访客。
- 发起人可以在任何组中的位置创建访客。
- 对于诸如批次大小限制的数值，将使用各组中的最大值。

如果发起人不是任何发起人组的成员，则不允许该发起人登录任何发起人门户。

- ALL_ACCOUNTS：发起人可以管理所有访客帐户。
- GROUP_ACCOUNTS：发起人可以管理同一发起人组中的发起人创建的访客帐户。
- OWN_ACCOUNTS：发起人只能管理他们创建的访客帐户。

您可以自定义特定发起人组的可用功能，从而限制或扩展发起人门户的功能。

创建发起人帐户并分配到发起人组

要创建内部发起人用户帐户并指定可使用发起人门户的发起人，请执行以下操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。将内部发起人用户帐户分配到适当的用户身份组。

注释　默认身份组 Guest_Portal_Sequence 已分配到默认发起人组。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人组 (Sponsor Groups)** > **创建、编辑或复制 (Create, Edit or Duplicate)**，然后点击**成员 (Members)**。将发起人用户身份组映射到发起人组。

下一步做什么

您还可以创建特定于贵组织的额外用户身份组以用于发起人。选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **用户身份组 (User Identity Groups)**。

配置发起人组

Cisco提供默认发起人组。如果不想使用默认选项，可以创建新的发起人组，或者编辑默认的发起人组，并且更改设置。还可以复制发起人组，以创建更多具有相同设置和权限的发起人组。

可以禁用发起人组，阻止发起人组成员登录发起人门户。可以删除任何发起人组，但Cisco ISE 提供的默认发起人组除外。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals and Components)** > **发起人组 (Sponsor Groups)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 输入 **发起人组名称** 和 **说明**。

步骤 3 在**匹配条件 (Match Criteria)** 部分输入以下详细信息：

- **成员组 (Member Groups)**：点击**成员 (Members)** 以选择一个或多个用户（身份）组以及来自外部身份源的组，然后添加这些组。要成为此发起人组的成员，用户必须属于至少一个已配置的组。
- **其他条件 (Other conditions)**：点击**创建新条件 (Create New Condition)** 可构建要将发起人包括在此发起人组中所必须符合的一个或多个条件。您可以使用来自 Active Directory、LDAP、SAML 和 ODBC 身份存储区的身份验证属性，但不能使用 RADIUS 令牌或 RSA SecurID 存储区的。您也可以使用内部用户属性。条件具有属性、操作符和值。
  - 要使用内部字典属性 *Name* 创建条件，请将用户身份组作为身份组名称前缀。例如：

    InternalUser:Name EQUALS bsmith

    这意味着只有名称为“bsmith”的内部用户才能属于此发起人组。

- 要使用 Active Directory 实例的 ExternalGroups 属性创建条件，请为要匹配的发起人用户选择 AD“Primary Group”。例如，如果用户名是 Smith，则 *AD1:LastName EQUALS Smith* 为 True。

除匹配一个或多个配置的成员组之外，发起人还必须符合您在此处创建的**所有**条件。如果一个进行身份验证的发起人用户符合多个发起人组的匹配条件，则该用户的权限如下：

- 如果在任何匹配组中启用了某个权限，例如删除访客帐户，则会授权其该权限。
- 发起人可以使用任何匹配组中的访客类型创建访客。
- 发起人可以使用任何匹配组中的访客类型创建访客。
- 发起人可以在任何匹配组中的位置创建访客。
- 对于诸如批次大小限制的数值，将使用各匹配组中的最大值。

您可以创建仅包含成员组或仅包含其他条件的匹配条件。如果仅指定其他条件，则发起人组中发起人的成员资格仅由匹配的字典属性确定。

步骤 4 要指定哪些访客类型可由基于此发起人组的发起人创建，请点击**此发起人组可使用以下访客类型创建帐户 (This sponsor group can create accounts using these guest types)**，然后选择一个或多个访客类型。

可以点击**创建访客类型在 (Create Guest Types at)** 下的链接，创建更多访客类型，分配给此发起人组。创建新的访客类型后，必须先保存、关闭并重新打开发起人组，然后才能选择新建的访客类型。

步骤 5 使用**选择访客将访问的位置 (Select the locations that guests will be visiting)** 指定在创建访客帐户时，此发起人组中的发起人可以选择的位置（用于设置访客时区）。

通过点击**配置访问位置在 (Configure guest locations at)** 下方的链接，并且添加访客位置，可以添加更多位置以供选择。创建新的访客位置后，必须先保存、关闭并重新打开发起人组，然后才能选择新建的访客位置。

这不会限制访客从其他位置登录。

步骤 6 如果希望发起人在创建用户后省去点击**通知 (Notify)** 的步骤，则在**自动访客通知 (Automatic guest notification)** 下，选中**如果邮件地址可用，则在创建帐户时自动向访客发送邮件 (Automatically email guests upon account creation if email address is available)**。这会导致弹出一个窗口，说明已发送电子邮件。选中此项还会为发起人门户增加标题行，内容是**自动发送访客通知 (Guest notifications are sent automatically)**。

步骤 7 在**发起人可创建 (Sponsor Can Create)** 下，配置此发起人组中的发起人用来创建访问帐户的选项。

- **分配给特定访客的多个访客帐户（导入）(Multiple guest accounts assigned to specific guests [Import])**：允许发起人通过从文件中导入访客详细信息（例如名字和姓氏）创建多个访客帐户。

  如果启用此选项，则**导入 (Import)** 选项将显示在发起人门户的**创建帐户 (Create Accounts)** 窗口中。Import 选项仅在桌面浏览器（而非移动）上可用，例如 Internet Explorer、Firefox、Safari 等。

- **批处理帐户数限制 (Limit to batch of)**：如果允许此发起人组同时创建多个帐户，请指定在单个导入操作中可以创建的访客帐户数。

  虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

- **分配给任意访客的多个访客帐户（随机）(Multiple guest accounts to be assigned to any guests [Random])**：允许发起人为尚且未知的访客以占位符形式创建多个随机访客帐户，或快速创建多个帐户。

如果启用此选项，则**随机 (Random)** 选项将显示在发起人门户的**创建帐户 (Create Accounts)** 窗口中。

- **默认用户名前缀 (Default username prefix)**：指定发起人在创建多个随机访客帐户时可以使用的用户名前缀。如果指定，则在创建随机访客帐户时，发起人门户中会出现此前缀。此外，如果 **Allow sponsor to specify a username prefix** 的状态为：
  - 已启用 (Enabled)：发起人可以在发起人门户中编辑默认前缀。
  - 未启用 (Not enabled)：发起人无法在发起人门户中编辑默认前缀。

  如果您不指定用户名前缀或者不允许发起人指定用户名前缀，则发起人将无法在发起人门户中分配用户名前缀。
- **允许发起人指定用户名前缀 (Allow sponsor to specify a username prefix)**：如果允许此发起人组同时创建多个帐户，请指定在单个导入操作中可以创建的访客帐户数。

  虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

步骤 8 在**发起人可管理 (Sponsor Can Manage)** 下，可以限制此发起人组的成员可以查看和管理哪些访客帐户。

- **仅发起人创建的帐户 (Only accounts sponsor has created)**：此组中的发起人只能根据发起人的电子邮件帐户，查看和管理他们创建的访客帐户。
- **此发起人组的成员创建的帐户 (Accounts created by members of this sponsor group)**：此组中的发起人可查看和管理此发起人组中任意发起人创建的访客帐户。
- **所有访客帐户 (All guest accounts)**：发起人查看并管理所有待处理访客帐户。

步骤 9 在**发起人可以 (Sponsor Can)** 下，可以向此发起人组的成员提供更多关于访客密码和帐户的权限。

- **更新访客的联系信息（电子邮件、电话号码）(Update guests' contact information (email, Phone Number))**：对于他们可以管理的访客帐户，允许发起人更改访客的联系信息
- **查看/打印访客密码 (View/print guests' passwords)**：启用此选项后，发起人可以打印访客密码。发起人可以在**管理帐户 (Manage Accounts)** 窗口和访客详细信息中查看访客的密码。未选中此选项时，发起人无法打印密码，但用户仍可以通过电子邮件或 SMS（如果已配置）获取密码。
- **发送含访客凭证的 SMS 通知 (Send SMS notifications with guests' credentials)**：对于他们可以管理的访客帐户，允许发起人向访客发送包含其帐户详细信息和登录凭证的 SMS（文本）通知。
- **重置访客帐户密码 (Reset guest account passwords)**：对于他们可以管理的访客帐户，允许发起人将访客的密码重置为由Cisco ISE 生成的随机密码。
- **延长访客帐户有效期 (Extend guests' accounts)**：对于他们可以管理的访客帐户，允许发起人将其延长至到期日期之后。发起人自动复制到发送给访客的、有关帐户到期的邮件通知上。
- **删除访客帐户 (Delete guests' accounts)**：对于他们可以管理的访客帐户，允许发起人删除帐户并阻止访客访问您公司的网络。
- **暂停访客帐户 (Suspend guests' accounts)**：对于他们可以管理的访客帐户，允许发起人暂停其帐户，以阻止访客临时登录。

  此操作还会发出授权变更 (CoA) 终止，以从网络中删除暂停的访客。

- **要求发起人提供原因 (Require sponsor to provide a reason)**：要求发起人提供暂停访客帐户的原因。

- **批准并查看自行注册访客的请求 (Approve and view requests from self-registering guests)**：此发起人组中的发起人可以查看自行注册访客的所有待处理帐户请求（待审批），或仅在用户（作为被访问人）输入发起人电子邮件地址时的请求。此功能要求选中自注册访客使用的门户中的**要求自注册访客需获得批准 (Require self-registered guests to be approved)**，而且列有发起人（作为联系人）的电子邮件。
  - 任何待处理帐户：属于此组的发起人可以批准并审核由任何发起人创建的帐户。
  - 仅分配给此发起人的待处理帐户：属于此组的发起人只能查看和批准自己创建的帐户。

- **使用编程接口（访客 REST API）访问思科 ISE 访客帐户 (Access Cisco ISE guest accounts using the programmatic interface (Guest REST API))**：对于他们可以管理的访客帐户，允许发起人使用访客 REST API 编程接口访问访客帐户。

步骤 10 点击**保存 (Save)**，然后点击**关闭 (Close)**。

为创建发起人帐户配置帐户内容

您可以配置访客和发起人创建新访客帐户时必须提供的用户数据类型。某些字段是识别 ISE 帐户所必需的，但您可以删除其他字段，并添加自己的自定义字段。

配置发起人创建帐户时使用的字段：

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)**，然后编辑发起人门户。
2. 选择**门户页面自定义 (Portal Page Customization)** 选项卡。
3. 向下滚动并选择**为已知访客创建帐户 (Create Account for Known Guests)**。
4. 在右侧的预览屏幕上，选择**设置 (Settings)**。

这些设置决定了在发起人门户上创建访客帐户时显示哪些字段以及哪些是必填字段。此配置适用于“已知”(Known)、“随机”(Random) 和“导入”(Imported) 访客类型。发起人为导入新用户而下载的模板是动态创建的，因此仅包括在已知访客中设置的字段。

导入帐户的用户名和密码

发起人可以导入用户名和密码，但当发起人下载 CSV 模板时，这些行不会添加到模板中。发起人可以添加这些标题。它们必须正确命名，以便 ISE 能够识别列：

- 用户名 - 可以是 *User Name* 或 *UserName*。
- 密码 - 必须是 **`password`**。

发起人门户的特殊设置

以下设置是发起人门户“门户页面自定义”(Portal Page Customization) 选项卡上的“为导入的访客创建帐户”(Create Account for Imported Guest) 页面的独有设置。

- **允许在访客凭证电子邮件中复制发起人 (Allow sponsor to be copied in Guest Credentials email)**：如果启用此选项，则发送到成功导入的访客的每封访客凭证电子邮件也会发送到发起人。默认为不向发起人发送电子邮件。
- **允许发起人接收摘要邮件 (Allow sponsor to receive summary email)**：当发起人导入用户列表时，ISE 会发送一封包含所有导入用户摘要的电子邮件。如果取消选中此选项，发起人会收到每个导入用户的单独电子邮件。

配置发起人门户流

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和Cisco ISE提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

如果贵公司的公司办公室及其零售点拥有不同的品牌，或者贵公司拥有不同产品品牌，或者驻某城市的办公室希望消防、警察和其他部门具有不同主题的门户，则您可能希望创建多个发起人门户。

这些是与配置发起人门户有关的任务。

开始之前

配置或编辑站点的现有发起人组，如配置发起人组，第 343 页中所述。

步骤 1 启用策略服务，第 347 页。
步骤 2 添加用于访客服务的证书，第 348 页。
步骤 3 创建外部身份源，第 348 页。
步骤 4 创建身份源序列，第 349 页。
步骤 5 创建发起人门户，第 349 页。
步骤 6 （可选） 自定义发起人门户，第 350 页。

启用策略服务

为了支持Cisco ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。
步骤 2 点击节点并点击**编辑 (Edit)**。
步骤 3 在**常规设置 (General Settings)** 选项卡下，启用**策略服务 (Policy Service)** 切换按钮。

步骤 4 选中**启用会话服务 (Enable Session Services)** 复选框。

步骤 5 点击**保存 (Save)**。

添加用于访客服务的证书

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为默认门户证书组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 添加一个系统证书并将其分配到您希望用于该门户的证书组标签。

在创建或编辑门户期间，此证书组标签可供选择。

步骤 3 选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建或编辑 (Create or Edit)** > **门户设置 (Portal Settings)**。

步骤 4 从与新添加证书关联的 **Certificate Group Tag** 下拉列表中选择特定的证书组标签。

创建外部身份源

Cisco ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

注释 要使用被动身份服务以接收和共享经过身份验证的用户身份，请参阅其他被动身份服务提供程序，第 522 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅将 Active Directory 用作外部身份源，第 471 页。
- 选择 **LDAP** 以添加 LDAP 身份源。有关详细信息，请参阅LDAP，第 561 页。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关详细信息，请参阅RADIUS 令牌身份源，第 582 页。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关详细信息，请参阅RSA 身份源，第 588 页。
- 选择 **SAML Id 提供程序 (SAML Id Providers)** 添加身份提供程序 (IdP)，例如 Oracle 访问管理器。有关详细信息，请参阅SAMLv2 身份提供者作为外部身份源，第 594 页。

- 选择**社交登录 (Social Login)** 以将社交登录（如 Facebook）设置为外部身份源。请参阅用于自行注册访客的社交媒体登录，第 322 页。

创建身份源序列

开始之前

确保您已经在Cisco ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)** > **添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望Cisco ISE 搜索数据库的顺序。

步骤 6 在 **Advanced Search List** 区域中选择以下选项之一：

- **请勿访问序列中的其他存储区并将 AuthenticationStatus 属性设置为 ProcessError**：如果用户未在第一个选定身份源中找到用户，而您希望Cisco ISE 中止搜索，请选择此选项。
- **视为未找到用户并继续至序列中的下一存储区 (Treat as if the user was not found and proceed to the next store in the sequence)**：如果未在第一个选定身份源中找到用户，而您希望Cisco ISE 仍继续按照序列搜索其他选定身份源，请选择此选项。

  在处理请求时，Cisco ISE 会按照序列搜索这些身份源。确保“选定列表”(Selected list) 字段所列出的身份源的顺序是您希望Cisco ISE 搜索身份源的顺序。

步骤 7 点击**提交 (Submit)** 创建您可以稍后在策略中使用的身份源序列。

创建发起人门户

您可以提供发起人门户，支持发起人为要连接到您的网络访问互联网及内部资源和服务的访客创建、管理和审批帐户。

Cisco ISE 为您提供了默认发起人门户，您可以使用该门户，而不必创建另一个门户。但是，您可以创建新的发起人门户，也可以编辑或复制现有门户。您可以删除上述任何门户，默认发起人门户除外。

您对**门户行为和流程设置 (Portal Behavior and Flow Settings)** 选项卡上的“页面设置”(Page Settings) 所做的任何更改均会反映到发起人流程图中的图形流程中。如果您启用某个页面，例如AUP页面，它会显示在流程中，并且发起人会在门户中看到此页面。如果您禁用某个页面，它会从流程中删除，并且系统会为发起人显示下一个启用的页面。

开始之前

确保您具有为配合此门户使用而配置的所需证书、外部身份源和身份源序列。

步骤 1 配置**门户设置 (Portal Settings)** 页面，如发起人门户的门户设置 ， 第 379 页中所述。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 2 配置**登录设置 (Login Settings)** 页面，如 发起人门户的登录页面设置 ， 第 381 页中所述。

步骤 3 配置**可接受的使用策略 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)** 页面，如 发起人门户的可接受使用政策 (AUP) 页面设置 ， 第 382 页中所述。

步骤 4 配置**发起人更改密码设置 (Sponsor Change Password Settings)** 选项，如 发起人门户的发起人更改密码设置 ， 第 382 页中所述。

步骤 5 配置**登录后横幅页面设置 (Post-Login Banner Page Settings)** 页面，如发起人门户的登录后横幅页面设置 ， 第 382 页中所述。

步骤 6 如果要自定义门户，请点击**发起人门户应用设置 (Sponsor Portal Application Settings)**。

步骤 7 点击**保存 (Save)**。

自定义发起人门户

可以通过自定义门户主题、更改门户页面上的UI元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户体验。有关自定义门户的详细信息，请参阅自定义最终用户 Web 门户 ， 第 391 页。

为创建发起人帐户配置帐户内容

您可以配置访客和发起人创建新访客帐户时必须提供的用户数据类型。某些字段是识别 ISE 帐户所必需的，但您可以删除其他字段，并添加自己的自定义字段。

配置发起人创建帐户时使用的字段：

1. 选择**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)**，然后编辑发起人门户。
2. 选择**门户页面自定义 (Portal Page Customization)** 选项卡。
3. 向下滚动并选择**为已知访客创建帐户 (Create Account for Known Guests)**。

   在右侧的预览屏幕上，选择**设置 (Settings)**。这些设置决定了在发起人门户上创建访客帐户时显示哪些字段，以及哪些是必填字段。

此配置适用于“已知”(Known)、“随机”(Random) 和“导入”(Imported) 访客类型。发起人为导入新用户而下载的模板是动态创建的，因此仅包括在已知访客中设置的字段。

发起人导入帐户的用户名和密码

发起人可以导入用户名和密码，但当发起人下载模板时，这些行不会添加到模板中。发起人可以添加这些标题。它们必须正确命名，以便Cisco ISE 能够识别列：

- **用户名**：可以是 **`User Name`**或 **`UserName`**
- **密码**：必须是密码

配置适用于发起人的时间设置

当发起人创建新的访客帐户时，他们会配置该帐户的活动时间。您可以配置发起人可用的选项，以允许他们设置帐户持续时间以及开始和结束时间。这些选项按访客类型配置。发起人在**访问信息 (Access Information)** 标题下查看结果。

控制发起人门户帐户时间选项的访客类型设置位于标题**最长访问时间 (Maximum Access Time)** 下，如下所述：

- **从首次登录开始 (From first login)**：发起人门户显示首次登录后帐户处于活动状态的持续时间。

  访客类型设置**最长帐户持续时间 (Maximum Account Duration)** 确定发起人可为持续时间输入的值。

- **从发起人指定日期开始（或从自行注册日期开始，如果适用）(From sponsor-specified date (or date of self-registration, if applicable))**：发起人可以选择将持续时间设置为“工作日结束”(End of business day)，或者取消选中该字段并设置持续时间、开始时间和结束时间。

  用于控制持续时间和生效日期的访客类型设置位于标题**仅在这些日期和时间允许访问 (Allow access only on these days and times)** 下。

  - 您选择的星期几限制了在发起人的日历中可选择的日期。
  - 选择持续时间和日期时，发起人门户中将实施最长帐户持续时间。

发起人门户的 Kerberos 身份验证

您可以配置Cisco ISE，使之使用 Kerberos 对登录到 Windows 以访问发起人门户的发起人用户进行身份验证。此过程使用 Kerberos 票证中的已登录发起人用户的 Active Directory 凭证。在浏览器与Cisco ISE 建立 SSL 连接后，系统会在安全隧道内执行 Kerberos SSO。

以下项目必须位于同一 Active Directory 域中：

- 发起人的 PC
- ISE PSN
- 为此发起人门户配置的 FQDN

此要求是因为 Microsoft 不支持跨 Active Directory 林的双向信任 Kerberos SSO。

发起人用户必须登录 Windows。

访客门户不支持 Kerberos 身份验证。

配置 Kerberos

要在发起人门户上启用 Kerberos，请选中**发起人设置和自定义 (Sponsor Settings and Customization)** 窗口中的**允许 Kerberos SSO (Allow Kerberos SSO)** 复选框。

此外，还必须正确配置发起人的浏览器。以下各节介绍如何手动配置每个浏览器。

注释 Active Directory 中的用户名和用户主体名称必须匹配。SSO 将根据用户主体名称来识别用户的会话。

要手动配置 Firefox

1. 在地址栏中输入 `about:config`。
2. 忽略显示的警告，然后点击以继续。
3. 在搜索栏中搜索 `negotiate`。
4. 将 FQDN 添加到 `network.negotiate-auth.delegation-uris` 和 `network.negotiate-auth.trusted-uris`。每个属性的 URL 列表以逗号分隔。
5. 关闭选项卡浏览器已就绪，无需重新启动。

手动配置 Internet Explorer

1. 点击右上角的齿轮，然后选择 **Internet 选项 (Internet Options)**。
2. 点击**安全**选项卡。
3. 点击**本地 Intranet (Local Intranet)**。
4. 点击**站点 (Sites)**，然后点击**高级 (Advanced)**。
5. 添加字符串 `<mydomain>.com`，其中 `<mydomain>` 是发起人门户 FQDN 的通配符，或者可以输入 FQDN。
6. 点击**关闭 (Close)**，然后点击**确定 (OK)**。
7. 点击 **Advanced** 选项卡。
8. 向下滚动到**安全 (Security)** 部分并选中**启用集成 Windows 身份验证 (Enable Integrated Windows Authentication)** 复选框。
9. 重启计算机。

Chrome 可以从 Internet Explorer 获取配置

故障排除

- 在命令提示符下运行 `set user`，验证计算机是否绑定到正确的 AD 域。
- 在命令提示符下运行 `klist`，查看缓存的 Kerberos 票证和主机名列表。
- 查看 SPNEGO 令牌数据。NTLM 密码令牌字符串比 Kerberos 令牌字符串短很多；正确的令牌字符串不应包含在一行中。
- 使用采用过滤器 `kerberos` 的 Wireshark 捕获 Kerberos 请求（如果存在）。

注释 当启用 Kerberos SSO 选项时，用户需要通过节点 FQDN 访问发起人门户，以使 Kerberos SSO 正常运行。如果为发起人门户配置了门户 FQDN，则当用户连接到门户 FQDN 时，用户将通过其节点 FQDN 重定向到门户。

发起人无法登录发起人门户

问题

当发起人尝试登录发起人 门户时，系统显示以下错误消息：

“用户名或密码无效。请重试。”(Invalid username or password. Please try again.)

原因

- 发起人输入了无效凭证。
- 由于数据库（内部用户数据库或 Active Directory）中没有此用户记录，此发起人无效。
- 发起人所属的发起人组已禁用。
- 发起人的用户帐户不属于活动/已启用的发起人组，这意味着发起人用户的身份组不是任何发起人组的成员。
- 发起人的内部用户帐户已禁用（暂停）。

解决方案

- 验证用户的凭证。
- 启用发起人组。
- 如果该用户帐户已禁用，则恢复该用户帐户。
- 将发起人用户的身份组添加为发起人组的成员。

监控访客和发起人活动

Cisco ISE 提供各种报告和日志，您可以通过这些报告和日志查看终端与用户管理信息以及访客与发起人活动。

您可以按需或按计划运行这些报告。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)**。

步骤 2 选择**访客 (Guest)** 或**终端和用户 (Endpoints and Users)** 以查看各种访客、发起人和终端相关报告

步骤 3 选择要使用**过滤器 (Filters)** 下拉列表搜索的数据。

步骤 4 在 **Time Range** 中选择您想要查看的数据的时间范围。

步骤 5 点击**运行 (Run)**。

指标控制面板

Cisco ISE 会在Cisco ISE 主页的指标控制板中提供网络中**经过身份验证的访客 (Authenticated Guests)** 和**活动终端 (Active Endpoints)** 的概览视图。

注释 对于热点流，终端不会显示在**经过身份验证的访客 (Authenticated Guest)** Dashlet 上

AUP 接受状态报告

AUP Acceptance Status 报告访客从所有访客门户对可接受使用政策 (AUP) 的接受状态。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **访客 (Guest)** > **AUP 接受状态 (AUP Acceptance Status)**。

您可以使用此报告跟踪特定时间的所有已接受和已拒绝的 AUP 连接。

访客记账报告

访客记账报告显示指定时间段内的访客登录历史记录。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **访客 (Guest)** > **访客记账 (Guest Accounting)**。

主访客报告

“主访客报告”(Master Guest Report) 将各种报告的数据融入一个视图中，让您可以导出来自不同报告来源的数据。您可以添加更多数据列，删除您不想查看或导出的数据列。要查看此处窗口，请点

击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **访客 (Guest)** > **主访客报告 (Master Guest Report)**。

此报告收集所有访客活动并提供有关访客用户访问的网站的详细信息。您可以使用此报告进行安全审核，以查看访客用户何时访问了网络以及他们在网络上执行了什么活动。要查看访客的互联网活动（例如他们访问的网站的 URL），您必须首先执行以下操作：

- 启用 Passed authentications 日志记录类别。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“已通过的身份验证”(Passed authentications)。
- 在防火墙上启用用于访客流量的以下选项：
  - Inspect HTTP traffic and send data to Cisco ISE Monitoring node. Cisco ISE 仅要求获取 Guest Activity 报告的 IP 地址和已访问 URL；所以，尽可能将数据限制为仅包含这些信息。
  - Send syslogs to Cisco ISE Monitoring node.

发起人登录和审核报告

发起人登录和审核报告是用于跟踪以下内容的组合报告：

- 发起人门户中的发起人登录活动。
- 发起人门户中由发起人执行的访客相关操作。

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **访客访问报告 (Guest Access Reports)** > **发起人登录和审核报告 (Sponsor Login and Audit)**。

访客门户和发起人门户的审核日志记录

在访客门户和发起人门户内执行特定操作的过程中，系统会向基础审核系统发送审核日志消息。默认情况下，这些消息显示在 /opt/CSCOcpm/logs/localStore/iseLocalStore.log 文件中。

您可以将这些消息配置为由系统日志发送到监控和故障排除系统及日志收集器。监控子系统会在相应的发起人和设备审核日志及访客活动日志中提供此信息。

无论访客登录成功还是失败，访客登录流程都会记录在审核日志中。

访客访问 Web 身份验证选项

Cisco ISE 访客和 Web 身份验证服务支持多个部署选项，可实现安全的访客访问。可以使用本地或集中式 Web 身份验证和设备注册 Web 身份验证，提供有线或无线访客连接。

- 集中式 Web 身份验证（集中式 WebAuth）：适用于所有访客门户。对于有线和无线连接请求，将由中央Cisco ISE RADIUS 服务器使用 Web 身份验证。访客通过在热点访客门户上输入可选访问代码，或在需要提供凭证的访客门户上输入用户名和密码来进行身份验证。

注释 在重定向期间，如果浏览器打开多个选项卡，Cisco ISE 会重定向到每个选项卡。用户可以登录到门户，但Cisco ISE 无法授权会话，并且用户无法获得访问权限。要解决此问题，用户必须关闭浏览器上除一个选项卡外的所有选项卡。

- 本地 Web 身份验证（本地 WebAuth）：适用于需要提供凭证的访客门户。访客连接到交换机进行有线连接，或连接到无线 LAN 控制器 (WLC) 进行无线连接。网络接入设备 (NAD) 会将其定向到网页以进行身份验证。访客在需要提供凭证的访客门户上输入用户名和密码以进行身份验证。
- 设备注册 Web 身份验证（设备注册 WebAuth）：仅适用于热点访客门户。Cisco ISE 在 Web 身份验证之前注册并授权访客设备。当访客连接到有线或无线 NAD 时，会定向到热点访客门户。访客无需提供凭证（用户名和密码）即可访问网络。

ISE 社区资源

有关如何使用 Cisco Wireless Controller 配置Cisco ISE 以提供访客访问权限的信息，请参阅《ISE 访客访问规范化部署指南》。

另请参阅以下技术说明：《ISE 无线访客设置指南和向导》。

采用集中式 Web 身份验证流程的 NAD

在此方案中，网络访问设备 (NAD) 从未知终端连接向Cisco ISE RADIUS 服务器发送新的授权请求。然后，终端接收到向Cisco ISE 的 URL 重定向。

注释 仅 IOS XE 3.7E、IOS 15.2(4) E 或更高版本支持 webauth-vrf-aware 命令。其他交换机在虚拟路由和转发 (VRF) 环境中不支持 Web 身份验证 URL 重定向。在这种情况下，作为解决办法，您可以在全局路由表中添加路由，以将流量泄漏回 VRF。

如果访客设备已连接 NAD，则访客服务交互采取 MAC 身份验证绕行 (MAB) 请求的形式，导致访客通过访客门户进行集中式 Web 身份验证登录。以下是对后续集中式 Web 身份验证的概述，此集中式 Web 身份验证适用于无线和有线网络访问设备。

1. 访客设备通过硬线连接方式连接至 NAD。访客设备上无 802.1X 请求方。
2. 包含适用于 MAB 的服务类型的身份验证策略允许在 MAB 失败的情况下继续运行并返回包含集中式 Web 身份验证用户界面的 URL 重定向的受限网络配置文件。
3. NAD 配置为对向Cisco ISE RADIUS 服务器发出的 MAB 请求进行身份验证。
4. Cisco ISE RADIUS 服务器处理 MAB 请求，但找不到适用于访客设备的终端。

   这种 MAB 失败导致产生受限制网络配置文件并且在配置文件中返回指向 access-accept 中 NAD 的 url-redirect 值。要支持此功能，请确保已有授权策略而且其支持相应的有线或无线 MAB（在

复合条件下），此外可以选择使用“Session:Posture Status=Unknown”条件。NAD 使用此值将默认端口 8443 上的所有访客 HTTP 流量重定向至 url-redirect 值。

此案例中标准 URL 值为：

```
https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa
```

5. 访客设备通过 Web 浏览器向重定向 URL 发出 HTTP 请求。
6. NAD 将此请求重定向至从初始 access-accept 返回的 url-redirect 值。
7. 带操作 CWA 的网关 URL 值重定向至访客门户登录页面。
8. 访客输入其登录凭证，然后提交登录窗体。
9. 访客服务器对登录凭证进行身份验证。
10. 根据流量类型，会发生以下情况：
    - 如果为非安全评估流量（无进一步验证的身份验证），其中访客门户未配置为执行客户端调配，访客服务器会向 NAD 发送 CoA。此 CoA 将导致 NAD 使用Cisco ISE RADIUS 服务器对访客设备进行重新身份验证。系统向已配置网络访问权限的NAD返回新的access-accept响应。如果未配置客户端调配并且需要更改 VLAN，则访客门户执行 VLAN IP 更新。访客无需重新输入登录凭证。系统自动使用首次登录时输入的用户名和密码。
    - 如果是安全评估流量，其中访客门户配置为执行客户端调配，访客设备 Web 浏览器显示关于安全评估代理安装和合规性的Client Provisioning 页面。（您也可以配置客户端调配资源策略以设置“NetworkAccess:UseCase=GuestFlow”条件。）

访客门户将重定向至客户端调配门户（因为没有适用于Linux的客户端调配或终端安全评估代理），此门户转而重定向回到访客身份验证 servlet，以执行可选 IP 释放/更新，然后执行 CoA。

重定向至Client Provisioning门户时，客户端调配服务将非永久性Web代理下载至访客设备并对设备执行安全评估检查。或者，还可以配置带有“NetworkAccess:UseCase=GuestFlow”条件的终端安全评估策略。

如果访客设备不合规，请确保已配置带有“NetworkAccess:UseCase=GuestFlow”和“Session:Posture Status=NonCompliant”条件的授权策略。

当访客设备合规时，请确保已配置带有“NetworkAccess:UseCase=GuestFlow”和“Session:Posture Status=Compliant”条件的授权策略。从此处，客户端调配服务向NAD发出CoA。此CoA导致NAD使用Cisco ISE RADIUS 服务器对访客进行重新身份验证。系统向已配置网络访问权限的 NAD 返回新的 access-accept 响应。

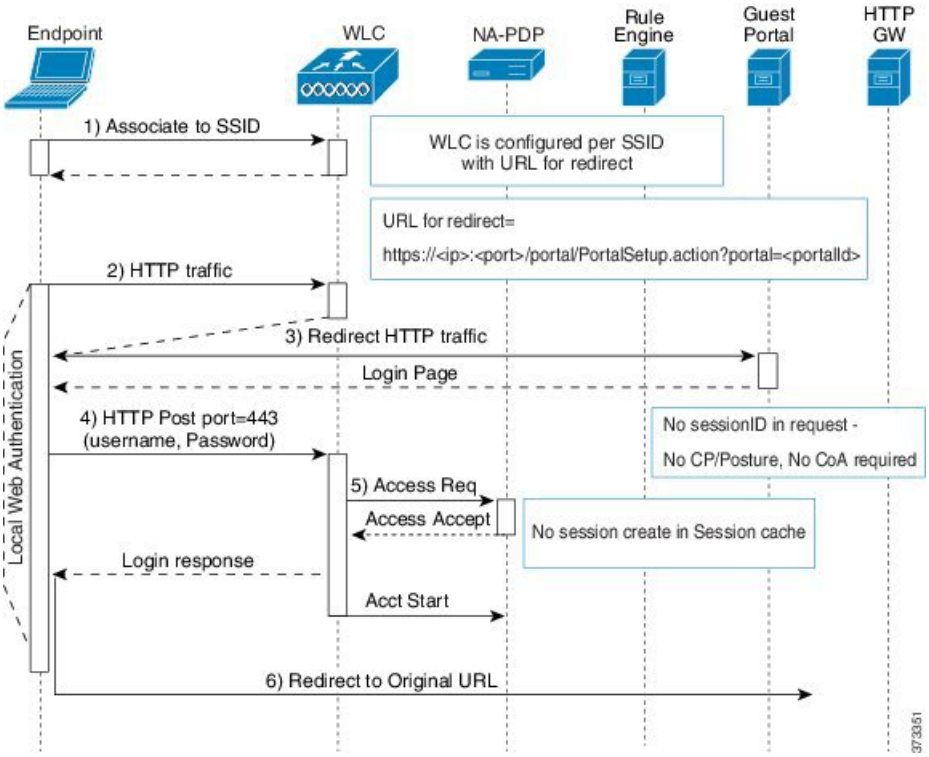
注释 “NetworkAccess:UseCase=GuestFlow”还可应用于 Active Directory 和以访客身份登录的 LDAP 用户。

使用本地 Web 身份验证流程的无线 LAN 控制器

在这种方案下，访客登录并被重定向至无线 LAN 控制器 (WLC)。然后，WLC 将访客重定向到访客门户，在门户中系统会提示访客输入他们的登录凭证，接受可选的可接受使用政策 (AUP) 并可选择更改密码。完成此操作后，访客设备的浏览器将重定向回到 WLC 以通过 POST 提供登录凭证。

现在，WLC 可以通过Cisco ISE RADIUS 服务器让访客登录。完成此操作后，WLC 将客户设备浏览器重定向至原 URL 目标地址。要支持用于访客门户的原 URL 重定向，无线 LAN 控制器 (WLC) 和网络接入设备 (NAD) 要求为运行 IOS-XE 3.6.0.E 和 15.2(2)E 版本的 WLC 5760 与 Cisco Catalyst 3850、3650、2000、3000 和 4000 系列接入交换机。

图 *12:* 使用本地 *Web* 身份验证非安全评估流程的 *WLC*



带本地网络身份验证进程的有线 NAD

在此场景中，访客门户将访客登录请求重定向到交换机（有线 NAD）。登录请求采用 HTTPS URL 形式发布到交换机，并且包含登录凭证。交换机接收访客登录请求，并使用已配置的Cisco ISE RADIUS 服务器验证访客。

1. Cisco ISE 要求将 HTML 重定向的 login.html 文件上传到 NAD。此 login.html 文件返回到访客设备的浏览器，响应任何 HTTPS 请求。
2. 访客设备的浏览器被重定向到访客门户，在此输入访客的登录凭证。
3. 处理可接受使用政策(AUP)和更改密码（两项均可选）后，访客门户重定向访客设备的浏览器，在 NAD 上发布登录凭证。

4. NAD 向Cisco ISE RADIUS 服务器发出 RADIUS 请求，要求对访客进行身份验证和授权。

Login.html 页面所需的 IP 地址和端口值

IP 地址和端口值必须在 login.html 页面的以下 HTML 代码中更改为Cisco ISE 策略服务节点正在使用的值。默认端口为 8443，但是您可以更改此值，以便确保您分配给交换机的值与Cisco ISE 中的设置相匹配。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML> <head> <title>ISE
Guest Portal </title> <meta Http-Equiv="Cache-Control" Content="no-cache"> <meta
Http-Equiv="Pragma" Content="no-cache"> <meta Http-Equiv="Expires" Content="0"> <meta
http-equiv="content-type" content="text/html; charset=UTF-8"> <meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired"> </HEAD> <BODY>
<center> Redirecting ... 登录 <br> <br> <a
href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE 访客门户</a> </center>
</BODY> </HTML>
```

自定义登录页面是公共 Web 表单，因此请考虑以下准则：

- 登录表必须接受用户名和密码的用户条目，并且将它们显示为 **uname** 和 **pwd**。
- 自定义登录页应当遵循 Web 表最佳实践，例如页面超时、隐藏密码和防止冗余提交。

在 NAD 上启用的 HTTPS 服务器

要使用基于 Web 的身份验证，您必须使用 **ip http secure-server** 命令在交换机内启用 HTTPS 服务器。

NAD 自定义身份验证代理 Web 页面的支持

您可以向 NAD 上传自定义的成功、过期和失败页面。Cisco ISE 无需任何特定的自定义，因此您可以根据 NAD 的标准配置说明来创建这些页面。

在 NAD 上配置 Web 身份验证

需要使用自定义文件替换默认 HTML 页面，在 NAD 上完成 Web 身份验证。

开始之前

在基于 Web 的身份验证期间，创建四个替代 HTML 页面，而不使用交换机默认 HTML 页面。

步骤 1 要指定使用自定义身份验证代理 Web 页面，首先在交换机闪存上存储自定义 HTML 文件。要将 HTML 文件复制到交换机闪存中，请在交换机上运行以下命令：

copy tftp/ftp flash

步骤 2 将 HTML 文件复制到交换机之后，在全局配置模式下执行以下命令：

ip admission proxy http login page file device:*login-filename*	指定自定义 HTML 文件在交换机内存文件系统中的位置，替换默认登录页面。设备：为闪存。

ip admission proxy http success page file device:*success-filename*	指定自定义 HTML 文件的位置，替换默认登录成功页面。
ip admission proxy http failure page file device:*fail-filename*	指定自定义 HTML 文件的位置，替换默认登录失败页面。
ip admission proxy http login expired page file device:*expired-filename*	指定自定义 HTML 文件的位置，替换默认登录过期页面。

步骤 3 请遵循交换机提供的指南，配置自定义身份验证代理 Web 页面。

步骤 4 如下列所示，验证自定义身份验证代理 Web 页面的配置：

```
Switch# show ip admission configuration Authentication proxy webpage Login page : flash:login.htm Success
page : flash:success.htm Fail Page : flash:fail.htm Login expired Page : flash:expired.htm Authentication
global cache time is 60 minutes Authentication global absolute time is 0 minutes Authentication global
init state time is 2 minutes Authentication Proxy Session ratelimit is 100 Authentication Proxy Watch-list
is disabled Authentication Proxy Auditing is disabled Max Login attempts per user is 5
```

设备注册 Web 身份验证流程

通过使用设备注册 Web 身份验证和热点访客门户，您可以允许访客设备连接到专用网络，而无需用户名和密码。

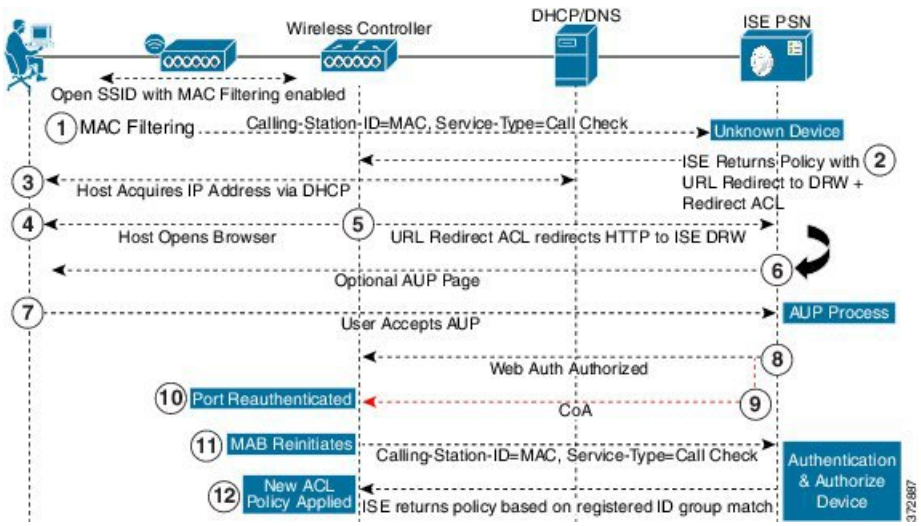
在此场景中，访客使用无线连接来连接到网络。有关设备注册 Web 身份验证流程的示例，请参阅图 13: 无线设备注册 Web 身份验证流。以下是后续设备注册 Web 身份验证过程的概要，此过程与无线和有限连接类似：

1. 网络接入设备 (NAD) 将重定向发送到热点访客门户。
2. 如果访客设备的 MAC 地址不在任何终端身份组中或者未通过将可接受使用政策 (AUP) 接受的属性设置为 true 进行标记，则Cisco ISE 会利用授权配置文件中指定的 URL 重定向进行响应。
3. URL 重定向会在访客尝试访问任何 URL 时向其显示 AUP 页面（如果启用）。
   - 如果访客接受 AUP，则与其设备 MAC 地址关联的终端会分配给已配置的终端身份组。此终端现在通过将 AUP 接受的属性设置为 true 进行标记，从而对访客是否接受 AUP 进行跟踪。
   - 如果客户不接受 AUP 或者如果发生错误（例如，在创建或更新终端时），系统会显示错误消息。
4. 根据热点访客门户配置，可能会出现包含其他信息的访问后横幅页面（如果启用）。
5. 创建或更新终端后，将向 NAD 发送授权变更 (CoA) 终止请求。
6. 在 CoA 后，NAD 会使用新的 MAC 身份验证绕行 (MAB) 请求对访客连接重新进行身份验证。新的身份验证会使用终端的关联终端身份组查找该终端，并且返回对 NAD 的已配置访问。
7. 根据热点访客门户配置，访客会被定向到其请求访问的 URL、管理员指定的自定义 URL 或 Authentication Success 页面。

有线和无线的 CoA 类型均是 Termination CoA。您可以配置热点访客门户来执行 VLAN DHCP Release（和更新），从而将有线与无线的 CoA 类型均重新授权为 Change of Auth。

VLAN DHCP Release 支持仅适用于 Windows 设备。它不适用于移动设备。如果进行注册的设备是移动设备，并且启用了 VLAN DHCP Release 选项，则会请求访客手动更新其 IP 地址。对于移动设备用户，我们建议使用 WLC 上的访问控制列表 (ACL)，而不是使用 VLAN。

图 *13:* 无线设备注册 *Web* 身份验证流



访客门户设置

门户标识设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户或发起人门户 (Guest Portals or Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **访客门户或发起人门户设置和自定义 (Guest Portals or Sponsor Portals Settings and Customization)**。

- **门户名称 (Portal Name)**：输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

  此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述**：可选。

- **门户测试 URL (Portal test URL)**：点击**保存 (Save)** 后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

  点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

- **语言文件 (Language File)**：默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

  语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

  如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

  在**门户页面自定义 (Portal Page Customizations)** 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

热点访客门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：
    - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。

- 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。

- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x**、**x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。

- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。Cisco ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

  选择用于跟踪员工设备的终端身份组。Cisco ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

- **当此身份组中的终端达到 __ 天时将其清除 (Purge Endpoints in this Identity Group when they Reach __ Days)**：指定从Cisco ISE 数据库中清除设备之前应经历的天数。每天都会进行清除，并且清除活动与整体清除时间同步。更改全局应用于此终端身份组。

  如果根据其他策略条件对终端清除策略进行更改，则此设置不可再使用。

- **显示语言**

  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。

  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。

  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

热点访客门户的可接受使用政策 (AUP) 页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)**。

- **包含 AUP (Include an AUP)**：在单独的页面上向用户显示公司的网络使用条款和条件。
- **要求访问代码 (Require an Access Code)**：分配访问代码，作为多个访客在获取网络访问权限时应使用的登录凭证。访问代码主要是提供给实际存在的访客（通过白板以肉眼方式或通过前台接待人员以口头方式）的本地已知代码。它不会被场地外的人员获知和使用以访问网络。

  除作为登录凭证提供给单独访客的用户名和密码以外，您还可以使用此选项。

- **要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)** - 确保用户已完全阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。配置 AUP 何时显示给用户。

配置热点访客门户流时，AUP 访问代码取决于终端身份组设备注册。这意味着无法使用 AUP Last Acceptance 和 Network Access: Use Case EQUALS Guest Flow 标志。当用户的会话从 NAD 中删除时，重新连接后，用户将看到 AUP 页面，但无需输入 AUP 访问代码。

仅在从与热点门户配置绑定的终端身份组中删除 MAC 地址后，才会显示 AUP 访问代码页面。通过 Cisco ISE 上的“情景可视性”(Context Visibility) 页面从数据库中手动删除终端，或者通过终端清除功能和配置的终端清除策略清除终端。

热点门户的访问后横幅页面设置

此页面的导航路径为 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **访问后横幅页面设置 (Post-Access Banner Page Settings)**.

使用此设置可通知访客其访问状态以及任何其他附加操作（如果需要）。

字段	使用指南
包含访问后横幅页面 (Include a Post-Access Banner page)	在对访客成功进行身份验证后并在向其授予网络访问权限之前显示其他信息。

需要提供凭证的访客门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：
    - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
  - 无效组合包括：

- 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
- 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- **身份验证方法 (Authentication Method)**：选择将哪个身份源序列或身份提供程序 (IdP) 用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  Cisco ISE 包含适用于发起人门户的默认身份源序列：Sponsor_Portal_Sequence。

  要配置 IdP，请选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。

  要配置身份源序列，请依次选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)**。

- **使用此门户的员工作为访客继承登录选项自 (Employees Using this Portal as Guests Inherit Login Options from)**：选择员工登录此门户时被分配的访客类型。员工的终端数据存储在终端身份组中，该身份组在属性**在终端身份组中存储设备信息 (Store device information in endpoint identity group)** 的访客类型中进行配置。不会从关联的访客类型继承其他属性。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

需要提供凭证的访客门户的登录页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **登录页面设置 (Login Page Settings)**。

- **要求访问代码 (Require an Access Code)**：分配访问代码，作为多个访客在获取网络访问权限时应使用的登录凭证。访问代码主要是提供给实际存在的访客（通过白板以肉眼方式或通过前台接待人员以口头方式）的本地已知代码。它不会被场地外的人员获知和使用以访问网络。

  除作为登录凭证提供给单独访客的用户名和密码以外，您还可以使用此选项。
- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定Cisco ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts when Rate Limiting)**：设置用户在达到**速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)** 中定义的登录失败次数后，尝试再次登录（限制速率）之前必须等待的时间长度（分钟）。
- **包含 AUP (Include an AUP)**：将可接受使用政策页面添加到流。可以将 AUP 添加到页面，或链接到另一个页面。
- **允许访客创建自己的帐户 (Allow Guests to Create their Own Accounts)**：在此门户的登录页面上为访客提供自行注册的选项。如果未选中此选项，则发起人需创建访客帐户。启用该选项会同时启用该页面中的选项卡以供您配置**自注册页面设置**和**自注册成功页面设置**。

如果访客选择此选项，则为其提供自注册表单，他们可在其中输入请求的信息来创建其自己的访客帐户。

- **允许访客找回密码 (Allow Guests to Recover the Password)**：此选项可在访客门户上为自注册访客启用“重置密码”(Reset Password) 按钮。如果仍然拥有有效帐户的自注册访客连接登录门户并忘记了密码，他们可以点击**重置密码 (Reset Password)**。这会让他们返回自注册页面，在此页面中，他们可以输入自己的（注册时使用的）电话或电子邮件，然后输入新密码。
- **允许社交媒体登录 (Allow Social Login)**：使用社交媒体网站获取此门户用户的登录凭证。选中此选项会显示以下设置：
  - **在社交媒体登录后显示注册表 (Show registration form after social login)**：这可以让用户更改 Facebook 提供的信息。
  - **要求访客获得批准 (Require guests to be approved)**：这会向用户告知发起人必须批准其帐户，并将向他们发送登录凭证。
- **允许访客在登录后更改密码 (Allow guests to change password after login)**：允许访客在成功进行身份验证并接受 AUP 后更改其密码（如果需要）。如果访客更改其密码，则在丢失登录凭证的情况下发起人无法为访客提供其登录凭证。发起人只能将访客的密码重置为随机密码。
- **允许以下身份提供程序访客门户用于登录 (Allow the following identity-provider guest portal to be used for login)**：选中此选项并选择 SAML ID 身份提供程序后，可向此门户添加该 SAML ID 的链接。此子门户可配置为类似于接收用户提供的凭证的 SAML IDP 的门户。
- **允许社交媒体登录 (Allow social login)**：允许此门户将社交媒体类型用于用户登录。有关配置社交媒体登录的详细信息，请参阅用于自行注册访客的社交媒体登录，第 322 页。

自注册页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **自注册页面设置 (Self Registration Page Settings)**。使用这些设置可以让访客能够自行注册，并指定访客必须在自注册表单中提供的信息。

- **将自注册访客分配到访客类型 (Assign self-registered guests to guest type)**：选择应该将使用此门户的所有自注册访客分配到访客类型。
- **帐户有效期 (Account valid for)**：以天、小时或分钟为单位指定帐户的持续时间，经过此时间之后，帐户就会到期，除非您或发起人在发起人门户中延长帐户持续时间。
- **要求用于自注册的注册码 (Require a registration code for self registration)**：为自助注册访客分配成功提交其自注册表单所必须输入的代码。注册代码与接入代码类似，都是通过离线方式提供给访客，以防外部的用户访问系统。
- **要包括的字段 (Fields to include)**：检查要在自注册表单上显示的字段。然后检查哪些字段是访客提交此表单和接收访客帐户必须填写的强制字段。您可能需要强制填写 **SMS Service Provider** 和 **Person being Visited** 等字段，以从自助注册访客收集重要信息。

- **位置 (Location)**：输入自助注册访客在注册时可以使用您所定义的位置列表选择的位置。这将自动分配相关时区，作为这些访客的有效访问时间。应使用明确的位置名称，以免在选择时出现含糊（如波士顿办事处、纽约公园大道 500 号、新加坡）。

  如果计划按一天中的时段来限制访客访问，则时区用来确定该时间。除非所有时间访问受控访客都位于圣荷西时区，否则请为您的区域设置创建时区。如果只有一个位置，系统会将其自动指定为默认位置，并且不在门户中显示此字段以供访客查看。此外，在**要包括的字段 (Fields to include)** 列表中，会禁用**位置 (Location)**。

- **SMS 服务运营商 (SMS Service Provider)** - 在自注册表单上显示 SMS 运营商，使自注册访客可以选择他们自己的 SMS 运营商。然后，可以使用访客的 SMS 服务向他们发送 SMS 通知，这可以最大程度地降低公司开支。如果只选择一个SMS运营商供访客使用，则此字段不会在自注册表单上显示。

- **被访问者 (Person being visited)**- 这是一个文本字段，因此，如果要使用它，请指示访客在此字段中输入哪种类型的信息。

- **自定义字段 (Custom Fields)** - 选择之前为向自注册访客收集更多数据而创建的自定义字段。然后检查哪些字段是访客提交 Self-Registration 表单和接收访客帐户必须填写的字段。系统按名称字母顺序列出这些字段。您可以在 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **设置 (Settings)** > **自定义字段 (Custom Fields)** 上创建这些字段，以便添加更多自定义字段。

- **包含一个 AUP (Include an AUP)** - 显示公司的网络使用条款和条件，可以是当前为用户显示的页面上的文本，或是一个链接，能够打开包含 AUP 文本的新选项卡或窗口。

  - **要求接受 (Require acceptance)** - 确保用户已完整阅读 AUP。这会在自注册页面上配置**接受 (Accept)** 按钮。如果将 AUP 配置为**在页面上**，则还可以禁用“接受”(Accept) 按钮，直到用户滚动到 AUP 的末尾。

- **仅允许电子邮件地址来自以下域的访客 (Only allow guests with an email address from)** - 指定自注册访客可在**电子邮件地址 (Email Address)** 中使用哪些允许的域列表来创建电子邮件地址，例如，cisco.com。

  如果将此字段留空，则任何电子邮件地址均有效，但**不允许电子邮件地址来自以下域的访客 (Do not allow guests with email address from)** 中列出的域除外。

- **不允许电子邮件地址来自以下域的访客 (Do not allow guests with email address from)** - 指定自注册访客不能在**电子邮件地址 (Email Address)** 中用来创建电子邮件地址的阻止域列表，例如，czgtgj.com。

- **要求自注册访客获得批准 (Require self-registered guests to be approved)**：指定使用此门户的自注册访客需要获得获得发起人的批准，才能收到其访客凭证。点击此选项会显示有关发起人如何批准自注册访客的更多选项。

  - 允许访客在获得发起人批准后通过自注册自动登录 (Allow guests to login automatically from self-registration after sponsor's approval)：自注册访客将在发起人批准后自动登录。

  - **批准请求电子邮件收件方 (Email approval request to)** - 如果选择：

- **下面列出的发起人电子邮件地址 (Sponsor email addresses listed below)**：输入被指定为批准者的发起人的一个或多个电子邮件地址，或邮件收发器，所有访客批准请求都会发送到上述地址。如果电子邮件地址无效，则批准会失败。
- **被访问者 (Person being visited)**：显示**要求发起人提供身份验证凭证 (Require sponsor to provide credentials for authentication)** 字段，并启用**要包括的字段 (Fields to include)** 中的**必填 (Required)** 选项（如果之前已禁用）。自注册表单上会显示这些字段，要求自注册访客提供这些信息。如果电子邮件地址无效，则批准会失败。

- **批准/拒绝链接设置 (Approve/Deny Link Settings)** - 此部分可以让您配置：
  - **链接有效期 (Links are valid for)**：您可以设置帐户批准链接的到期期限。
  - **要求发起人提供身份验证凭证 (Require sponsor to provide credentials for authentication)**：选中此选项可强制发起人输入凭证以批准帐户（即使此部分中的配置不要求如此）。仅当将**要求自注册访客获得批准 (Require self-registered guests to be approved)** 设置为**被访问者 (person being visited)** 时，此字段才可见。
  - **发起人与发起人门户匹配以验证批准权限 (Sponsor is matched to a Sponsor Portal to verify approval privileges)**：点击**详细信息 (Details)** 以选择要搜索的门户，确认发起人是有效的系统用户、发起人组的成员，并且该组的成员有权批准帐户。每个发起人门户都有一个身份源序列，用于标识发起人。门户按其列出的顺序使用。列表中的第一个门户确定发起人门户中使用的样式和自定义。

- **提交注册后，将访客定向至 (After registration submission, direct guest to)**：选择在成功注册后将自注册访客定向到什么位置。
  - **自注册成功页面 (Self-Registration Success page)**：将成功自注册的访客定向至**自注册成功 (Self-Registration Success)** 窗口，其中会显示您在**自注册成功页面设置 (Self Registration Success Page Settings)** 中指定的字段和消息。

    可能无需显示所有信息，因为系统可能正在等待批准帐户（如已在此窗口启用该选项）或根据此窗口中指定的允许列表域和组织列表域，向电子邮件地址或电话号码发送登录凭证。

    如果在**自注册成功页面设置 (Self-Registration Success Page Settings)** 中启用了**允许访客直接从自注册成功页面登录 (Allow guests to log in directly from the Self-Registration Success page)**，则自助注册成功的访客可以直接从此窗口登录。如未启用，则在显示**自注册成功 (Self-Registration Success)** 窗口之后，系统会将访客定向至门户的登录窗口。
  - **包含如何获取登录凭证相关说明的登录页面 (Login page with instructions about how to obtain login credentials)**：将成功自注册的访客定向回到门户的登录窗口，并显示一条消息，如“请等待您的访客凭证以电子邮件、短信或打印格式送达，然后再继续登录。(Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in)”。

    要自定义默认消息，请点击**门户页面自定义 (Portal Page Customization)** 选项卡，然后选择**自注册页面设置 (Self-Registration Page Settings)**。

    系统可能正在等待批准帐户（如已在此窗口启用该选项）或根据此窗口中指定的允许列表域和组织列表域，向电子邮件地址或电话号码发送登录凭证。

- **URL**：将自注册成功的访客定向至指定的 URL，同时等待他们的帐户凭证送达。

  系统可能正在等待批准帐户（如已在此窗口启用该选项）或根据此窗口中指定的允许列表域和组织列表域，向电子邮件地址或电话号码发送登录凭证。

- **使用以下方式自动发送凭证通知：**
  - **电子邮件 (Email)**：选择将邮件作为自注册成功的访客用来接收其登录凭证信息的选项。如果您选择此选项，**Email address** 会成为 **Fields to include** 列表中的必填字段，而且您再也无法禁用此选项。
  - **SMS**：选择将 SMS 作为自注册成功的访客用来接收其登录凭证信息的选项。如果您选择此选项，**SMS Service Provider** 会成为 **Fields to include** 列表中的必填字段，而且您再也无法禁用此选项。

自行注册成功页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **自注册成功页面设置 (Self Registration Page Settings)**。使用这些设置可向成功自注册的访客通知他们获取网络访问权限所需的凭证。

字段	使用指南
自注册成功页面中纳入该信息 (Include this information on the Self-Registration Success page)	选中要在“自注册成功”(Self-Registration Success) 页面上为成功自注册访客显示的字段。 如果不需要访客的赞助商审批，请选中**用户名 (Username)** 和 **密码 (Password)**，为访客显示这些凭证。如果需要赞助商审批，则这些字段将被禁用，因为凭证只能在得到批准之后发送到访客。
允许访客通过以下方式向自己发送信息 (Allow guest to send information to self using)	选中成功自注册访客可用于向自己传送凭证信息的方式的选项：**打印 (Print)**、**电子邮件 (Email)** 或 **SMS**。
包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的页面上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。

字段	使用指南
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	如果选择了**页面上的 AUP (AUP on page)** 选项，系统会显示此字段。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。
允许访客直接通过自注册成功页面登录 (Allow guests to log in directly from the Self-Registration Success page)	“自注册成功”(Self-Registration Success) 页面底部显示**登录 (Login)** 按钮。这使得访客能够绕过“登录”(Login) 页面，自动将登录凭证传送到门户并在门户流程中显示下一个页面（例如，AUP 页面）。

需要提供凭证的访客门户的可接受使用政策 (AUP) 页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)**。

- **包含 AUP (Include an AUP)**：在单独的页面上向用户显示公司的网络使用条款和条件。
- **对员工使用不同的 AUP (Use Different AUP for Employees)**：仅为员工显示不同的 AUP 及网络使用条款和条件。如果您选择此选项，则不能同时选择**跳过面向员工的 AUP (Skip AUP for employees)**。
- **对员工跳过 AUP (Skip AUP for Employees)**：员工在访问网络之前无需接受 AUP。如果您选择此选项，则不能同时选择**使用面向员工的不同 AUP (Use different AUP for employees)**。
- **要求滚动至 AUP 末尾 (Require Scrolling to End of AUP)**：此选项仅在已启用**在页面上包含 AUP (Include an AUP on page)** 时显示。

  确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。配置何时向用户显示 AUP。

  - **仅首次登录时 (On First Login only)**：仅在用户首次登录网络或门户时显示 AUP。
  - **每次登录时 (On Every Login)**：每次用户登录网络或门户时都显示 AUP。
  - **每 __ 天（从首次登录算起）(Every __ Days [starting at first login])**：在用户首次登录网络或门户后定期显示 AUP。

需要提供凭证的访客门户的访客更改密码设置

访客更改密码设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **访客更改密码设置 (Guest Change Password Settings)**

- **允许访客在登录后更改密码 (Allow guests to change password after login)**：允许访客在成功进行身份验证并接受AUP后更改其密码（如果需要）。如果访客更改其密码，则在丢失登录凭证的情况下发起人无法为访客提供其登录凭证。发起人只能将访客的密码重置为随机密码。

需要提供凭证的访客门户的访客设备注册设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **访客设备和注册设置 (Guest Device Registration Settings)**。

使用这些设置可确保在登录到访客设备时Cisco ISE 自动注册访客设备，或者允许访客在登录后手动注册其设备。

在以下位置为每个访客类型指定最大设备数量：**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Types)**。

- **自动注册访客设备 (Automatically Register Guest Devices)**：自动为访客用来访问此门户的设备创建终端。此终端将添加到为此门户指定的终端身份组。

  现在，可以创建授权规则来允许访问该身份组中的终端，以便不再需要 Web 身份验证。

  如果达到最大注册设备数，则系统会自动删除第一个注册设备，注册访客尝试登录所使用的设备，并且通知访客。选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Types)** 以更改访客可向其注册的最大设备数量。

- **允许访客注册设备 (Allow Guests to Register Devices)**：访客可以通过提供名称、说明和 MAC 地址手动注册其设备。MAC 地址与终端身份组相关联。

  如果达到最大注册设备数，则访客需要删除至少一个设备，然后才允许其注册其他设备。

需要提供凭证的访客门户的 BYOD 设置

此页面的导航路径为 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **BYOD 设置 (BYOD Settings)**。

使用这些设置为非访客（例如使用需要提供凭证的访客门户访问企业网络的员工）启用自带设备 (BYOD) 功能。

字段	使用指南
允许员工在网络中使用个人设备 (Allow Employees to use Personal Devices on the Network)	向此门户添加“BYOD 注册”(BYOD Registration) 页面，允许员工完成员工设备注册过程，并且可能进行本地请求方和证书调配，具体视员工的个人设备类型（例如，iOS、Android、OSX）对应的客户端调配设置而定。
终端身份组 (Endpoint Identity Group)	选择用于跟踪访客设备的终端身份组。Cisco ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
允许员工选择仅获取方可访问权限 (Allow employees to choose to get guest access only)	使员工可以访问访客网络并避免在访问企业网络时可能需要另行调配和注册。
在注册期间显示设备 ID 字段 (Display Device ID Field During Registration)	在注册过程中向用户显示设备 ID，即使设备 ID 已预配置并在使用 BYOD 门户时无法更改也如此。
原始 URL (Originating URL)	成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示“身份验证成功”(Authentication Success) 页面。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的Cisco ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。 对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。
注册成功页面	显示设备注册成功的页面。
URL	成功对网络进行身份验证后，将用户的浏览器重定向到指定的 URL，例如贵公司的网站。

需要提供凭证的访客门户的登录后横幅页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** 或**发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **登录后横幅页面设置 (Post-Login Banner Page Settings)**.

使用此设置可在用户（适用情况下的访客、发起人或员工）成功登录后向其通知其他信息。

字段	使用指南
包含登录后横幅页面 (Include a Post-Login Banner page)	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

需要提供凭证的访客门户的访客设备合规性设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **访客设备合规性设置 (Guest Device Compliance Settings)**。使用这些设置可要求使用访客门户的访客和员工对其设备进行客户端调配，以便获取对网络的访问权限。

- **需要访客设备合规性 (Require guest device compliance)** - 将访客重定向到“客户端调配”(Client Provisioning) 页面，这会要求其下载终端安全评估代理。这会将客户端调配添加到访客流，您可以在其中配置访客的终端安全评估策略，如检查病毒防护软件。

  如果访客是使用需要提供证书的访客门户来访问网络的员工，并且：

  - 如果您已启用 **BYOD Settings** 中的 **Allow employees to use personal devices on the network**，则员工会被重定向到 BYOD 流程，并且不会进行客户端调配。
  - 如果您同时启用 **BYOD Settings** 中的 **Allow employees to use personal devices on the network** 和 **Allow employees to choose to get guest access only**，并且员工选择访客接入，则他们会被重定向到 Client Provisioning 页面。

访客门户的 VLAN DHCP 释放页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **VLAN DHCP 释放页面设置 (VLAN DHCP Release Page Settings)**。

- **启用 VLAN DHCP 释放 (Enable VLAN DHCP release)**：在有线与无线环境中发生 VLAN 更改后刷新访客的 Windows 设备 IP 地址。

  这会在网络访问将访客 VLAN 更改为新 VLAN 时影响最终授权过程中的集中式 Web 身份验证 (CWA) 流程。在 VLAN 更改之前必须释放访客的旧 IP 地址，并且必须在访客连接新 VLAN 时通过 DHCP 请求新访客 IP 地址。仅在使用 DirectX 控件的 Internet Explorer 浏览器上支持 IP 地址释放和续订操作。

  “VLAN DHCP 释放”(VLAN DHCP Release) 选项不适用于移动设备。相反，系统会请求访客手动重置 IP 地址。此方法因设备而异。例如，在 Apple iOS 设备上，访客可以选择 Wi-Fi 网络并点击 **Renew Lease** 按钮。

- **延迟 __ 秒释放 (Delay to Release __ Seconds)**：输入延迟释放时间。我们建议使用较短的值，因为释放必须紧随在下载小应用程序之后、在Cisco ISE 服务器指示 NAD 对 CoA 请求重新进行身份验证之前发生。
- **延迟 __ 秒执行 CoA (Delay to CoA __ Seconds)**：输入使Cisco ISE 延迟执行 CoA 的时间。提供足够时间（使用默认值作为规定值），以允许下载小程序并在客户端上执行 IP 释放。
- **延迟 __ 秒续订 (Delay to Renew __ Seconds)**：输入延迟续订值。此时间会添加到 IP 释放值，并且在下载控件之前不会开始计时。提供足够时间（使用默认值作为规定值），以便允许 CoA 进行处理并授予新的 VLAN 访问权限。

访客门户的身份验证成功设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **身份验证成功设置 (Authentication Success Settings)**。

这些设置会通知用户（适用的访客、发起人或员工）身份验证成功或显示 URL。在**经过身份验证后将访客转到: (Once authenticated, take guest to:)** 下，配置以下字段：

- **原始 URL (Originating URL)**：成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示 Authentication Success 页面。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。

  对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。
- **身份验证成功 (Authentication Success) 页面**：通知用户身份验证成功。
- **URL**：成功对网络进行身份验证后，将用户的浏览器重定向到指定的 URL，例如您公司的网站。

注释 如果您在身份验证后将一个访客重定向到外部 URL，可能会在解析 URL 地址和重定向会话时有延迟。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。

访客门户的支持信息页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **支持信息页面设置 (Support Information Page Settings)**.

使用这些设置可显示服务中心可用于对用户（适用情况下的访客、发起人或员工）遇到的访问问题进行故障排除的信息。

字段	使用指南
包含支持信息页面 (Include a Support Information Page)	在门户的所有已启用页面上显示指向信息页面（例如**联系我们 [Contact Us]**）的链接。
MAC 地址	在**支持信息 (Support Information)** 窗口上包含设备的 MAC 地址。
IP 地址	在**支持信息 (Support Information)** 窗口上包含设备的 IP 地址。
浏览器用户代理	在**支持信息 (Support Information)** 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 (Policy Server)	在**支持信息 (Support Information)** 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，请选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。
隐藏字段 (Hide Field)	如果字段标签将会包含的信息不存在，请勿在**支持信息 (Support Information)** 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示**故障代码 (Failure code)**，即使已选择故障代码也如此。
显示不含任何值的标签 (Display Label with no Value)	在**支持信息 (Support Information)** 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示**故障代码 (Failure code)**，即使其为空白也如此。
显示含默认值的标签 (Display Label with Default Value)	如果标签将会包含的信息不存在，请在**支持信息 (Support Information)** 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用”(Not Available)，并且故障代码未知，则**故障代码 (Failure Code)** 将显示**不可用 (Not Available)**。

发起人门户应用设置

门户标识设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户或发起人门户 (Guest Portals or Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **访客门户或发起人门户设置和自定义 (Guest Portals or Sponsor Portals Settings and Customization)**。

- **门户名称 (Portal Name)**：输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

  此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述**：可选。

- **门户测试 URL (Portal test URL)**：点击**保存 (Save)** 后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

  点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。

  注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

- **语言文件 (Language File)**：默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

  语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

  如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

  在**门户页面自定义 (Portal Page Customizations)** 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

发起人门户的门户设置

配置这些设置以标识门户并选择要用于所有门户页面的语言文件。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：
    - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
  - 无效组合包括：
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

  注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在 **门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。

- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- 在Cisco ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
- 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**：为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com,sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。

  如果更改默认 FQDN，还需执行以下操作：

  - 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在Cisco ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。

- **身份验证方法 (Authentication Method)**：选择将哪个身份源序列或身份提供程序 (IdP) 用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  Cisco ISE 包含适用于发起人门户的默认身份源序列：Sponsor_Portal_Sequence。

  要配置 IdP，请选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。

  要配置身份源序列，请依次选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)**。

- **空闲超时 (Idle Timeout)**：输入Cisco ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。
- **允许 Kerberos (Allow Kerberos)**：使用 Kerberos 对发起人进行身份验证，用于访问发起人门户。在浏览器与 ISE 建立 SSL 连接后，在安全隧道内执行 Kerberos SSO。

注释 Kerberos 身份验证要求以下项目位于同一域中：

- 发起人的 PC
- ISE PSN
- 为此发起人门户配置的 FQDN

注释 访客门户不支持 Kerberos 身份验证。

- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。
- **发起人的可用 SSID (SSIDs Available to Sponsors)**：输入网络的名称或 SSID（会话服务标识符），发起人可以告知访客该网络是可以连接访问的正确网络。

发起人门户的登录页面设置

发起人门户的登录页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **登录页面设置 (Login Page Settings)**。

- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定Cisco ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts when Rate Limiting)**：设置用户在达到**速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)** 中定义的登录失败次数后，尝试再次登录（限制速率）之前必须等待的时间长度（分钟）。

- **包含 AUP (Include an AUP)**：将可接受使用政策页面添加到流。可以将 AUP 添加到页面，或链接到另一个页面。

发起人门户的可接受使用政策 (AUP) 页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)**.

使用这些设置可定义用户（适用情况下的访客、发起人或员工）的 AUP 体验。

字段	使用指南
包含 AUP 页面 (Include AUP page)	在单独的页面上向用户显示公司的网络使用条款和条件。
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。
仅首次登录时 (On First Login only)	仅在用户首次登录到网络或门户时显示 AUP。
每次登录时 (On Every Login)	每次用户登录到网络或门户时显示 AUP。
每 __ 天（从首次登录算起）(Every __ Days [starting at first login])	在用户首次登录到网络或门户时定期显示 AUP。

发起人门户的发起人更改密码设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **发起人更改密码设置 (Sponsor Change Password Settings)**。这些设置为使用发起人门户的发起人定义密码要求。

字段	使用指南
Allow sponsors to change their own passwords	允许发起人在登录发起人门户后更改密码。此选项仅在发起人在内部用户数据库中时才显示“更改密码”(Change Password) 页面。

发起人门户的登录后横幅页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** 或**发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **登录后横幅页面设置 (Post-Login Banner Page Settings)**.

使用此设置可在用户（适用情况下的访客、发起人或员工）成功登录后向其通知其他信息。

字段	使用指南
包含登录后横幅页面 (Include a Post-Login Banner page)	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

发起人门户的支持信息页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **支持信息页面设置 (Support Information Page Settings)**.

使用这些设置可显示服务中心可用于对用户（适用情况下的访客、发起人或员工）遇到的访问问题进行故障排除的信息。

字段	使用指南
包含支持信息页面 (Include a Support Information Page)	在门户的所有已启用页面上显示指向信息页面（例如**联系我们 [Contact Us]**）的链接。
MAC 地址	在**支持信息 (Support Information)** 窗口上包含设备的 MAC 地址。
IP 地址	在**支持信息 (Support Information)** 窗口上包含设备的 IP 地址。
浏览器用户代理	在**支持信息 (Support Information)** 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 (Policy Server)	在**支持信息 (Support Information)** 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，请选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。
隐藏字段 (Hide Field)	如果字段标签将会包含的信息不存在，请勿在**支持信息 (Support Information)** 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示**故障代码 (Failure code)**，即使已选择故障代码也如此。

字段	使用指南
显示不含任何值的标签 **(Display Label with no Value)**	在**支持信息 (Support Information)** 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示**故障代码 (Failure code)**，即使其为空白也如此。
显示含默认值的标签 **(Display Label with Default Value)**	如果标签将会包含的信息不存在，请在**支持信息 (Support Information)** 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用”(Not Available)，并且故障代码未知，则**故障代码 (Failure Code)** 将显示**不可用 (Not Available)**。

自定义从发起人门户发送至访客的通知

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户页面自定义 (Portal Page Customization)** > **通知访客 (Notify Guests)**。

在 **Page Customizations** 下，您可以自定义发起人从发起人门户发送至访客的通知上显示的消息、标题、内容、说明和字段与按钮标签。

在 **Settings** 下，您可以指定发起人是否可以使用邮件或 SMS 单独向访客发送用户名和密码。您还可以指定发起人是否可以向访客显示 Support Information 页面，以提供技术支持可用于对访问问题进行故障排除的信息。

自定义发起人门户的“管理和审批”选项卡

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户页面自定义 (Portal Page Customization)** > **管理和批准 (Manage and Approve)**。

在 **Page Customizations** 下，您可以自定义发起人门户的 Manage 和 Approve 选项卡上显示的消息、标题、内容、说明以及字段和按钮标签。

其中包括帐户（已注册和待处理）摘要和详细视图、根据发起人对访客帐户执行的操作（例如编辑、扩展、暂停等）显示的弹出对话框，以及常规门户和帐户操作消息。

访客和发起人门户的全局设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **访客访问 (Guest Access)** > **设置 (Settings)**。您可以配置以下常规设置应用于Cisco ISE 的访客和发起人门户、访客类型以及发起人组：

- 清除访客帐户和生成用户名和密码的策略。
- 向访客和发起人发送邮件和 SMS 通知时使用的 SMTP 服务器和 SMS 网关。
- 使用自助注册访客门户创建访客帐户和注册访客时可选择的位置、时区、SSID 和自定义字段。

配置这些全局设置后，在配置特定访客和发起人门户、访客类型和发起人组时，可以根据需要使用这些设置。

“门户设置”(Portal settings) 页面中提供以下选项卡：

- **访客帐户清除策略 (Guest Account Purge Policy)** - 当要清除已过期的访客帐户时安排。有关详细信息，请参阅安排清除过期访客帐户的时间，第 314 页。
- **自定义字段 (Custom Fields)** - 添加用于访客门户的自定义字段，以检索来自用户的其他信息。有关详细信息，请参阅添加用于创建访客帐户的自定义字段，第 315 页。
- **访客邮件设置 (Guest Email Settings)** - 确定是否发送邮件将其帐户的变更通知访客。有关详细信息，请参阅为邮件通知指定邮箱地址和 SMTP 服务器，第 315 页。
- **访客位置和 SSID (Guest Locations and SSIDs)** - 配置位置和访客可以在这些位置中使用的网络服务集标识符 (SSID)。有关详细信息，请参阅分配访客位置和 SSID，第 316 页。
- **访客用户名策略 (Guest Username Policy)** - 配置创建访客用户名的方式。有关详细信息，请参阅设置访客用户名策略，第 319 页和访客密码策略规则，第 317 页。
- **访客密码策略 (Guest Password Policy)** - 定义所有访客和发起人门户的访客密码策略。有关详细信息，请参阅设置访客密码策略和到期时间，第 317 页。
- **日志记录 (Logging)** - 通过用户设备的 MAC 地址跟踪访客用户。当报告中显示访客用户时，用户名为 MAC 地址。如果选择此选项，报告会显示门户用户 ID 作为用户名，而不是 MAC 地址。有关此选项的详细信息，请参阅访客 Remember Me，第 340 页。

访客类型设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Types)**。使用这些设置可以创建能够访问网络的访客类型及其访问权限。您也可以指定哪些发起人组能够创建此访客类型。

- **访客类型名称 (Guest type name)** - 提供一个名称（1 至 256 个字符），将此访客类型与其他访客类型区分开来。
- **说明** - 提供有关此访客类型推荐用途的更多信息（最多 2000 个字符），例如用于自行注册访客。
- **语言文件 (Language File)** - 使用此字段可导出和导入语言文件，文件包含所有受支持语言的电子邮件主题、电子邮件和 SMS 消息的内容。这些语言和内容用于有关过期帐户的通知中，并发送给分配了此访客类型的访客。如果您正在创建新的访客类型，在保存访客类型之前，此功能将被禁用。有关编辑语言文件的详细信息，请参阅门户语言自定义，第 416 页。

- **收集其他数据 (Collect Additional Data)** - 点击**自定义字段 (Custom Fields)** 选项，选择要用于向使用此访客类型的访客收集其他数据的自定义字段。

  要管理自定义字段，请选择 **工作中心 (Work Centers)** > **访客访问权限 (Guest Access)** > **设置 (Settings)** > **自定义字段 (Custom Fields)**。

- **最长接入时间**

  - **帐户持续时间开始 (Account Duration Starts)** - 如果您选中了**从首次登录开始 (From first login)** 选项，当访客用户首次登录访客门户时，即开始计算帐户开始时间，并且帐户结束时间为配置的持续时间。如果访客用户从未登录，帐户会持续处于`等待首次登录 (Awaiting first login)` 状态，直至访客帐户清除策略删除该帐户。

    值的范围为 1 到 999 天、小时或分钟。

    自注册用户的账户在他们创建并登录他们的帐户时开始。

    如果您选择**从发起人指定的日期开始 (From sponsor-specified date)**，输入此类型的访客能够访问网络和保持网络连接的最大天数、小时数或分钟数。

    如果更改这些设置，您的更改不会应用到使用此访客类型创建的原有访客帐户。

  - **最长帐户持续时间 (Maximum account duration)** - 输入分配给此访客类型的访客可以登录的天数、小时数或分钟数。

    注释 帐户清除策略检查过期的访客帐户，并发送过期通知。此策略每 20 分钟运行一次，因此，如果将帐户持续时间设置为少于 20 分钟，则在清除帐户之前可能不会发出过期通知。

    您可以使用**仅在这些日期和时间允许访问 (Allow Access only on these Days and Times)** 选项指定向此类型的访客提供访问权限的持续时间和星期几。

    - 您选择的星期几限制了在发起人的日历中可选择的访问日期。
    - 当发起人选择持续时间和日期时，发起人门户中将实施最长帐户持续时间。

  您在此进行的访问时间设置会影响创建访客帐户时发起人门户上可用的时间设置。有关详细信息，请参阅 配置适用于发起人的时间设置 ， 第 351 页。

- **登录选项**

  - **最大同时登录数 (Maximum simultaneous logins)** - 输入分配此访客类型的用户可以同时运行的最大用户会话数。
  - **当访客超过限制时 (When Guest Exceeds Limit)** - 如果选择**最大同时登录数 (Maximum simultaneous logins)**，还必须同时选择用户在达到最大登录数后连接时要执行的操作。
    - **断开最早的连接 (Disconnect the oldest connection)**

- **断开最近的连接 (Disconnect the newest connection)** - 如果选择**将用户重定向至显示错误信息的门户页面 (Redirect user to a portal page showing an error message)**，错误消息将在配置的时长内显示，然后会话断开，用户重定向到访客门户。错误页面的内容在“门户页面自定义”(Portal Page Customization) 对话框中配置，对话框位于 **消息 (Messages)** > **错误消息 (Error Messages)** 窗口。

- **访客可以注册的最大设备数 (Maximum Devices Guests can Register)** - 输入每个访客可以注册的最大设备数。您可以将限制设为小于已为此访客类型的访客注册的设备数的数值。这只会影响新创建的访客帐户。当添加新设备并达到最大值时，最早的设备将断开连接。
- **用于注册访客设备的终端身份组 (Endpoint identity group for guest device registration)** - 选择要分配访客设备的终端身份组。Cisco ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- **允许访客绕开访客门户 (Allow Guest to bypass the Guest portal)** - 允许用户绕过需要提供凭证的访客类型强制网络门户（Web 身份验证页面），通过向有线和无线 (dot1x) 请求方或 VPN 客户端提供凭证来访问网络。访客帐户进入活动状态，绕过等待初始登录状态和 AUP 页面，即使 AUP 是必填项也是如此。

  如果不启用此设置，用户必须首先通过需要提供凭证的访客强制网络门户登录，然后才能访问网络的其他部分。

- **帐户过期通知**
  - **在帐户过期之前 __ 天，发送帐户过期通知 (Send account expiration notification __ days before account expires)** - 在帐户过期之前向访客发送通知，指定距离过期还剩多少天、多少小时或多少分钟。
  - **查看消息的语言 (View messages in)** - 指定在按照您的设置显示电子邮件或 SMS 通知时使用的语言。
  - **电子邮件 (Email)** - 通过电子邮件发送帐户过期通知。
  - **使用自定义设置源 (Use customization from)** - 将您为所选门户配置的相同自定义设置应用于此访客类型的帐户过期邮件。
  - **复制文本自 (Copy text from)** - 重复使用您为另一访客类型的帐户过期电子邮件而创建的电子邮件文本。
  - **SMS** - 通过 SMS 发送帐户过期通知。

    SMS 的设置与电子邮件通知的设置相同，不同之处在于您选择了**向我发送测试 SMS (Send test SMS to me)** 对应的 SMS 网关。

- **发起人组 (Sponsor Groups)** - 指定成员可以使用此访客类型创建访客帐户的发起人组。删除您不希望访问此访客类型的发起人组。

发起人组设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人组 (Sponsor Groups)**。使用这些设置可向发起人组添加成员，定义访客类型和位置权限，以及设置与创建和管理访客帐户相关的权限。

- **禁止发起人组 (Disable Sponsor Group)**：禁止此发起人组的成员访问发起人门户。

  例如，您可能希望在管理门户中进行配置更改时暂时阻止发起人登录到发起人门户。或者，您可能希望禁用不频繁活动（例如，年度会议的发起访客）中涉及的发起人组，直至其需要再次激活。

- **发起人组名称 (Sponsor group name)**：输入唯一名称（1 至 256 个字符）。

- **说明**：包含有用信息（最多 2000 个字符），例如此发起人组使用的访客类型。

- **配置访客类型 (Configure Guest Types)**：如果所需的访客类型不可用，请点击 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Types)** 并创建新的访客组或编辑现有组。

- 匹配标准

  - **成员 (Members)**：点击显示**选择发起人组成员 (Select Sponsor Group Members)** 复选框，您可在其中选择可用的用户身份组（从内部和外部身份存储区中选择）并将其添加为此发起人组的成员。

    - **发起人组成员 (Sponsor Group Members)**：搜索和筛选所选发起人组的列表，并删除不希望包含的任意组。

  - **其他条件 (Other conditions)**：点击**创建新条件 (Create New Condition)** 可构建要将发起人包括在此发起人组中所必须符合的一个或多个条件。您可以使用来自 Active Directory、LDAP、SAML 和 ODBC 身份库的身份验证属性，但不能使用 RADIUS 令牌或 RSA SecurID 库的。您也可以使用内部用户属性。条件具有属性、操作符和值。

    - 要使用内部字典属性 *Name* 创建条件，请将用户身份组作为身份组名称前缀。例如：

      InternalUser:Name EQUALS bsmith

      这意味着只有名称为“bsmith”的内部用户才能属于此发起人组。

- **此发起人组可以使用这些访客类型创建帐户 (This sponsor group can create accounts using these guest types)**：指定此发起人组的成员在创建访客帐户时可以使用的访客类型。要启用发起人组，该发起人组必须具有至少一个可使用的访客类型。

  如果仅向此发起人组分配一个访客类型，则可以选择不在发起人门户中显示该访客类型，因为它是可供使用的唯一有效访客类型。选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portal)** > **页面自定义 (Page Customization)** > **创建帐户 (Create Accounts)** > **访客类型 (Guest Types)** > **设置 (Settings)**。选中 **Hide guest type if only one is available to sponsor** 复选框可启用此选项。

- **选择访客将访问的位置 (Select the locations that guests will be visiting)**：选择在创建访客帐户时可分配给这些访客的位置。这可帮助定义这些访客帐户的有效时区，并且指定适用于访客的所有时间参数，例如有效访问时间等。这不会阻止访客从其他位置连接到网络。这不会阻止访客从其他位置连接到网络。

  要启用发起人组，该发起人组必须具有至少一个可使用的位置。

  如果您仅向此发起人组分配一个位置，则该位置将是其成员创建的访客帐户的唯一有效时区。默认情况下，该位置不会显示在发起人门户中。

发起人可以创建

- **分配给特定访客的多个访客帐户（导入）(Multiple guest accounts assigned to specific guests (Import))**：允许发起人通过从文件中导入访客详细信息（例如名字和姓氏）创建多个访客帐户。

  如果启用此选项，则**导入 (Import)** 选项将显示在发起人门户的**创建帐户 (Create Accounts)** 页面中。“导入”(Import) 选项仅在桌面浏览器（而非移动浏览器）上可用，例如 Internet Explorer、Firefox、Safari 等。

- **批处理帐户数限制 (Limit to batch of)**：如果允许此发起人组同时创建多个帐户，指定在单个导入操作中可以创建的访客帐户数。

  虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

- **分配给任意访客的多个访客帐户（随机）(Multiple guest accounts to be assigned to any guests (Random))**：允许发起人为尚且未知的访客或在访客需要快速创建许多帐户时将多个随机访客帐户创建为占位符。

  如果启用此选项，则**随机 (Random)** 选项将显示在发起人门户的**创建帐户 (Create Accounts)** 窗口中。

- **默认用户名前缀 (Default username prefix)**：指定发起人在创建多个随机访客帐户时可以使用的用户名前缀。如果指定，则在创建随机访客帐户时，发起人门户中会出现此前缀。此外，如果 **Allow sponsor to specify a username prefix** 的状态为：
  - 已启用：发起人可以在发起人门户中编辑默认前缀。
  - 未启用：发起人无法在发起人门户中编辑默认前缀。

  如果您不指定用户名前缀或者不允许发起人指定用户名前缀，则发起人将无法在发起人门户中分配用户名前缀。

- **允许发起人指定用户名前缀 (Allow sponsor to specify a username prefix)**：如果允许此发起人组同时创建多个帐户，指定在单个导入操作中可以创建的访客帐户数。

  虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

- **开始日期不能超过未来 __ 天 (Start date can be no more than __ days into the future)**：指定天数，在此期间，发起人需为其所创建的多个访客帐户设置开始日期。

发起人可以管理

- **仅发起人创建的帐户 (Only accounts sponsor has created)**：此组中的发起人只能根据发起人的电子邮件帐户，查看和管理他们创建的访客帐户。
- **此发起人组的成员创建的帐户 (Accounts created by members of this sponsor group)**：此组中的发起人可查看和管理此发起人组中任意发起人创建的访客帐户。
- **所有访客帐户 (All guest accounts)**：发起人查看并管理所有待处理访客帐户。

注释 无论组成员身份如何，所有发起人都可以查看所有待处理的帐户，除非您选中**发起人可以 (Sponsor Can)** 下面**批准并查看自行注册访客的请求 (Approve and view requests from self-registering guests)** 的**仅分配给此发起人的待处理帐户 (Only pending accounts assigned to this sponsor)** 选项。

发起人可以

- **更新访客的联系信息（电子邮件、电话号码）(Update guests' contact information (email, Phone Number))**：对于他们可以管理的访客帐户，允许发起人更改访客的联系信息
- **查看/打印访客密码 (View/print guests' passwords)**：启用此选项后，发起人可以打印访客密码。发起人可以在**管理帐户 (Manage Accounts)** 窗口和访客详细信息中查看访客的密码。未选中此选项时，发起人无法打印密码，但用户仍可以通过电子邮件或 SMS（如果已配置）获取密码。
- **发送含访客凭证的 SMS 通知 (Send SMS notifications with guests' credentials)**：对于他们可以管理的访客帐户，允许发起人向访客发送包含其帐户详细信息和登录凭证的 SMS（文本）通知。
- **重置访客帐户密码 (Reset guest account passwords)**：对于他们可以管理的访客帐户，允许发起人将访客的密码重置为由Cisco ISE 生成的随机密码。
- **延长访客帐户有效期 (Extend guests' accounts)**：对于他们可以管理的访客帐户，允许发起人将其延长至到期日期之后。发起人自动复制到发送给访客的、有关帐户到期的邮件通知上。
- **删除访客帐户 (Delete guests' accounts)**：对于他们可以管理的访客帐户，允许发起人删除帐户并阻止访客访问您公司的网络。
- **暂停访客帐户 (Suspend guests' accounts)**：对于他们可以管理的访客帐户，允许发起人暂停其帐户，以阻止访客临时登录。

  此操作还会发出授权变更 (CoA) 终止，以从网络中删除暂停的访客。

  - **要求发起人提供原因 (Require sponsor to provide a reason)**：要求发起人提供暂停访客帐户的原因。

- **批准并查看自行注册访客的请求 (Approve and view requests from self-registering guests)**：此发起人组中的发起人可以查看自行注册访客的所有待处理帐户请求（待审批），或仅在用户（作为被访问人）输入发起人电子邮件地址时的请求。此功能要求选中自注册访客使用的门户中的

要求自注册访客需获得批准 (Require self-registered guests to be approved)，而且列有发起人（作为联系人）的电子邮件。

- 任何待处理帐户：属于此组的发起人可以批准并审核由任何发起人创建的帐户。
- 仅分配给此发起人的待处理帐户：属于此组的发起人只能查看和批准自己创建的帐户。

- **使用编程接口（访客 REST API）访问思科 ISE 访客帐户 (Access Cisco ISE guest accounts using the programmatic interface (Guest REST API))**：对于他们可以管理的访客帐户，允许发起人使用访客 REST API 编程接口访问访客帐户。

最终用户门户

Cisco ISE 为三类主要最终用户提供基于 Web 的门户：

- 需要使用访客门户（热点和有凭证访客门户）临时访问企业网络的访客。
- 被指定为发起人，可以使用 Sponsor 门户创建和管理访客帐户的员工。
- 使用各种非访客门户（例如 Bring Your Own Device (BYOD) 门户、Mobile Device Management (MDM) 门户和 My Devices 门户）在企业网络上使用其个人设备的员工。

自定义最终用户 Web 门户

您可以编辑、复制和创建更多门户。您也可以完全自定义门户外观以及门户体验。您可以单独自定义每个门户，而不影响其他门户。

您可以自定义门户界面的各个要素，这些自定义设置可以适用于整个门户，也可以适用于门户的特定页面，例如：

- 主题、图像、颜色、横幅和页脚
- 用于显示门户文本、错误消息和通知的语言
- 标题、内容、说明以及字段和按钮标签
- 通过邮件、SMS 和打印机发送给访客的通知（仅适用于自行注册访客门户和发起人门户）
- 显示给用户的错误消息和信息性消息
- 对于自注册访客和发起人门户，可以创建自定义字段以搜集特定于您的需求的访客信息

ISE 社区资源

有关自定义 Web 门户的详细信息，请参阅 ISE 门户生成器和操作方法：ISE Web 门户自定义选项。

自定义方法

自定义最终用户门户页面的方法有多种，各自需要不同的知识水平。

- **基本**：您可以修改门户“自定义”页面：
  - 上传条幅和徽标
  - 更改某些颜色（按钮除外）
  - 更改屏幕上的文本以及整个门户上使用的语言
- **中级**
  - 使用迷你编辑器添加 HTML 和 Javascript

    注释 要在迷你编辑器中输入 HTML，需要先点击 HTML 图标。
  - 使用 jQuery 移动主题滚动条可更改所有页面元素的颜色
- **高级**
  - 手动修改属性和 CSS 文件。

自定义门户后，可以通过复制该门户来创建（相同类型的）多个门户。例如，如果已为一家商业实体自定义热点访客门户，则可以复制此门户，稍作更改，为其他商业实体创建自定义热点访客门户。

使用迷你编辑器自定义门户的技巧

- 迷你编辑器框中的长字词可能会滚动出门户的屏幕区域。可以使用 HTML 段落属性 style="word-wrap: break-word" 中断行。例如：

```
 <p style="word-wrap:break-word">
thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure
 </p>
```

- 使用 HTML 或 javascript 自定义门户页面时，应确保使用有效的语法。Cisco ISE 不会验证输入迷你编辑器的标签和代码。无效语法有可能在门户流程中造成问题。

门户内容类型

Cisco ISE 提供一组默认门户主题，您可以“按原样”使用或使用现有 CSS 文件作为模型进行自定义，以创建新的自定义文件。但是，可以在不使用自定义 CSS 文件的情况下修改门户的外观。

例如，如果想要使用唯一的公司徽标和横幅图像，只需上传和使用这些新的图像文件。可以通过更改门户的不同元素和区域的颜色来自定义默认配色方案。甚至可以选择在进行自定义更改时查看更改所要使用的语言。

当设计要替换徽标和横幅的图像时，尽可能让图像接近以下像素大小：

横幅	1724 X 133
桌面徽标	86 X 45
移动徽标	80 X 35

请注意，ISE 会调整图像的大小以适合门户，但过小的图像在调整大小之后可能无法正确显示。

要执行高级自定义，如更改页面布局或在门户页面上添加视频剪辑或广告，可以使用自定义 CSS 文件。

在特定门户内，这些类型的更改会全局应用到该门户的所有页面。对页面布局的更改可以全局应用或只应用到门户中的某个特定页面。

门户页面标题、内容和标签

您可以自定义标题、文本框、说明、字段与按钮标签，以及访客在最终用户 Web 门户页面上查看的其他可视元素。在自定义页面时，甚至可以动态编辑页面设置。

这些更改只适用于您所自定义的特定页面。

门户的基本自定义

选择最适合您的需求的预定义主题，并使用其大多数默认设置。然后，您可以执行基本的自定义，例如：

- 修改门户主题颜色， 第 393 页
- 更改门户图标、图像和徽标， 第 395 页
- 更新门户的横幅和页脚元素， 第 395 页
- 更改门户显示语言， 第 394 页
- 更改标题、说明、按钮和标签文本， 第 396 页
- 格式和样式文本框内容， 第 396 页

提示 您可以在进行更新时 查看您的自定义， 第 400 页。

修改门户主题颜色

可以自定义默认门户主题中的默认配色方案，并更改门户的不同元素和区域的颜色。这些更改将应用于您自定义的所有门户。

如果计划更改门户颜色，请注意以下事项：

- 无法使用此选项更改可能已导入用于此门户的任何自定义门户主题中的配色方案。必须编辑自定义主题 CSS 文件才能更改其颜色设置。

- 更改门户主题中的颜色之后，如果从 **Portal Theme** 下拉菜单中选择其他门户主题，则原始门户主题中的更改将丢失，颜色将恢复到其默认颜色。
- 如果使用已修改的配色方案调整门户主题的颜色，然后在保存方案前重置其颜色，则配色方案将恢复到其默认颜色，且之前所做的所有修改都将丢失。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **配置 (Configure)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** >（任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 从 **Portal Theme** 下拉列表选择一个默认主题。

步骤 3 点击 **Tweaks** 以覆盖选定默认门户主题中的某些颜色设置。

a) 更改横幅和页面背景、文本和标签的颜色设置。
b) 如果要恢复到主题的默认配色方案，请点击**重置颜色 (Reset Colors)**。
c) 如果要在**预览 (Preview)** 中查看颜色更改，请点击**确定 (OK)**。

步骤 4 点击**保存 (Save)**。

更改门户显示语言

您可以选择您想要用于查看您所做的自定义更改的语言。此更改适用于您所自定义的整个门户。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **全局自定义 (Global Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **全局自定义 (Global Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** >（任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **全局自定义 (Global Customization)**。

步骤 2 从 **View In** 下拉列表选择您想要用于在自定义页面时查看文本的语言。

此下拉列表包含与特定门户关联的语言文件中的所有语言。

下一步做什么

确保将您在自定义门户页面期间以所选语言所做的任何更改都更新至所支持的语言属性文件中。

更改门户图标、图像和徽标

如果要使用唯一的公司徽标、图标和横幅图像，只需通过上传自定义图像即可替换现有图像。支持的图像格式包括：.gif、.jpg、.jpeg 和 .png。这些更改将应用于您自定义的所有门户。

开始之前

要在门户的页脚（例如，广告）中包含图像，应该能够访问具有这些图像的外部服务器。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **配置 (Configure)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在 **Images** 下方，点击任意徽标、图标和图像按钮，然后上传自定义图像。

步骤 3 点击**保存 (Save)**。

更新门户的横幅和页脚元素

您可以自定义门户各页面中横幅和页脚部分所显示信息。这些更改将应用于您自定义的所有门户。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** >（任意门户）> **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 更改显示在各门户页面中的**横幅标题 (Banner title)**。

步骤 3 包括这些使用门户的访客链接：

- **帮助 (Help)** - 在线帮助（仅提供给发起人和我的设备门户）。
- **联系方式 (Contact)** - 技术支持（设置支持信息页面以启用它）。

步骤 4 在各门户页面上显示的**页角元素 (Footer Elements)** 中添加免责声明或版权声明。

步骤 5 点击**保存 (Save)**。

更改标题、说明、按钮和标签文本

您可以更新门户中显示的所有文本。您所自定义的页面上的每个UI元素对于您可以输入的字符数都有最高和最低范围限制。有些文本块提供小型编辑器，您可以使用此编辑器将视觉风格应用于相应文本。这些更改只适用于您自定义的特定门户页面。这些页面元素对于邮件、SMS 和打印通知是不同的。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问权限 (Guest Access)** > **门户和组件 (Portals & Components)** > **配置 (Configure)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问权限 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** >（任意门户）> **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。

步骤 2 在 **Pages** 下，选择您想要更改的页面。

步骤 3 在 **Page Customizations** 下，更新任何显示的 UI 元素。所有页面均包含**浏览器页面标题 (Browser Page Title)**、**内容标题 (Content Title)**、**说明文本 (Instructional Text)**、**内容 (Content)** 和两个**可选内容 (Optional Content)** 文本块。**Content** 区域的字段是特定于各页面的。

格式和样式文本框内容

使用**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和 **可选内容 2 (Optional Content 2)** 文本框中可用的小型编辑器对文本执行基本格式处理。这些更改仅用于您自定义的特定门户页面。

使用**切换全屏 (Toggle Full Screen)** 按钮可在使用文本框时缩放其大小。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** >（任意门户）> **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在**页面 (Pages)** 下，选择您想要更改的页面。

步骤 3 在**页面自定义 (Page Customizations)** 下，在**说明文本 (Instructional Text)** 和 **可选文本 (Optional Content)** 文本块中，您可以执行以下操作：

- 更改文本的字体、大小和颜色。
- 将文本样式设置为粗体、斜体或带下划线。
- 创建带项目符号和编号的列表。

注释 可以使用**切换 HTML 源 (Toggle HTML Source)** 按钮查看应用于您使用小型编辑器进行格式设置的文本的 HTML 标签。如果在 **HTML 源 (HTML Source)** 视图中编辑文本，请再次点击**切换 HTML 源 (Toggle HTML Source)** 按钮，然后再在**门户页面自定义 (Portal Page Customization)** 窗口中保存所做更改。

用于门户页面定制的变量

这些门户页面文本框的导航路径为：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** >（任意门户）> **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。

为门户内容和访客通知创建模板时，请使用这些变量，从而确保向门户用户（访客、发起人和员工）显示的信息的一致性。对每个门户，请使用此处列出的变量名称替换**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 文本框中的文本。

表 *45:* 访客门户的变量列表

显示名称	用以下变量名称替换
Access code 用于以电子邮件、文本或打印通知的形式向访客提供访问代码。	ui_access_code
BYOD IOS SSID 用于指定在双 SSID 流程中完成自行激活之后设备应该连接的网络。	ui_byod_success_ios_ssid
Client Provisioning Agent Type 用于指定客户端调配策略中当前配置的代理，例如 AnyConnect 代理。	ui_client_provision_agent_type
Client Provisioning Agent URL 用于指定安全评估代理的下载 URL。	ui_client_provision_agent_url
Client Provisioning agent install minutes 用于向访客通知其必须在多长时间内（由补救计时器设置）按照**客户端调配 (Client Provisioning)** 窗口上的说明完成安装。如果访客未在计时结束前按照说明完成安装，就必须刷新浏览器页面并再次执行登录过程。	ui_client_provision_install_agent_mins
Company	ui_company
Email address	ui_email_address
End date and time	ui_end_date_time
First name	ui_first_name
Last name	ui_last_name
Location name	ui_location_name
Maximum registered devices	ui_max_reg_devices
Maximum simultaneous logins	ui_max_siml_login
Password	ui_password
Person being visited (email)	ui_person_visited

显示名称	用以下变量名称替换
Phone number	ui_phone_number
Reason for visit	ui_reason_visit
SMS Provider	ui_sms_provider
SSID 用于指定访客可用于连接网络的无线网络。	ui_ssid
Start date and time	ui_start_date_time
Time left	ui_time_left
Username	ui_user_name

表 *46:* 发起人门户的变量列表

显示名称	用以下变量名称替换
Guest - Company	ui_guest_company
Guest - Email address	ui_guest_email_address
Guest - End date and time	ui_guest_end_date_time
Guest - First name	ui_guest_first_name
Guest - Last name	ui_guest_last_name
Guest - Location name	ui_guest_location_name
Guest - Maximum registered devices	ui_guest_max_reg_devices
Guest - Maximum simultaneous logins	ui_guest_max_siml_login
Guest - Password	ui_guest_password
Guest - Person being visited (email)	ui_guest_person_visited
Guest - Phone number	ui_guest_phone_number
Guest - Reason for visit	ui_guest_reason_visit
Guest - SMS Provider	ui_guest_sms_provider
Guest - SSID 用于指定访客可用于连接网络的无线网络。	ui_guest_ssid
Guest - Start date and time	ui_guest_start_date_time
Guest - Time left	ui_guest_time_left
Guest - Username	ui_guest_user_name

显示名称	用以下变量名称替换
Username 用于指定登录门户的用户的用户名。	ui_sponsor_user_name
用于显示**访客访问信息 (Guest Access Information)**窗口中的“来自”(From)。	ui_from_label
用于显示**访客访问信息 (Guest Access Information)**窗口中的“首次登录”(First Login)。	ui_first_login_text
用于显示访问时间始于首次登录时的访客帐户通知消息。	ui_notification_first_login_text
表示邮件通知中帐户持续时间的动态变量。	ui_access_duration
显示帐户的动态变量不再可用。对于“开始-结束”(Start-End) 帐户，日期采用结束日期，对于从“首次登录”(From-First-Login) 帐户，日期为帐户创建日期加上清除持续时间日。	ui_account_purge_date
用于当访客用户过去至少登录一次时限制发起人从“从首次登录到开始-结束”(From First Login to Start-End) 状态更改访客类型，反之亦然。显示在通用发起人门户消息中。	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_ startend_ffl_not_allowed_error

表 *47: MDM* 门户的变量列表

显示名称	用以下变量名称替换
MDM - Vendor Name	ui_mdm_vendor_name

表 *48: My Devices* 门户的变量列表

显示名称	用以下变量名称替换
MyDevices - Login Failure Rate Limit	$user_login_failure_rate_limit$
MyDevices - Max Devices to Register	ui_max_register_devices
MyDevices - User Name 用于指定登录门户的用户的用户名。	$session_username$

查看您的自定义

您可以查看自己的自定义向门户用户（访客、发起人或员工）的显示方式。

步骤 1 点击 **Portal test URL** 查看您做出的更改。

步骤 2 （可选）点击**预览 (Preview)** 以动态查看所做的更改如何出现在各类设备上：

- 移动设备 - 在**预览 (Preview)** 下查看做出的更改。
- 桌面设备 - 点击**预览 (Preview)** 并点击**桌面预览 (Desktop Preview)**。

  如果没有显示更改，请点击 **Refresh Preview**。所显示的门户仅用于查看您做出的更改；您无法点击按钮或输入数据。

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

自定义门户文件

通过自定义门户文件菜单，您可以将自己的文件上传到 ISE 服务器，然后用它来自定义所有面向用户的门户（管理员门户除外）。您上传的文件将存储在 PSN 上，并同步到所有 PSN。

支持的文件类型为：

- .png、.gif、.jpg、.jpeg、ico：用作背景、公告和广告
- .htm、.html、.js、.json、.css、.m4a、.m4v、.mp3、.mp4、.mpeg、.ogg、.wav：用于高级自定义（例如，门户构建器）

文件大小限制：

- 每个文件 20 MB
- 所有文件共 200 MB

文件列表中的路径列显示此服务器上的文件的 URL，您可以使用该 URL 在迷你编辑器外部引用该文件。如果是图像文件，则当您点击该链接时，它会打开显示图像的新窗口。

上传的文件可在**门户页面自定义 (Portal Page Customization)** 下的迷你编辑器中被所有门户类型引用，管理员门户除外。要将文件插入迷你编辑器，请点击**插入文件 (Insert File)**。切换到 HTML 源视图，您将看到插入的文件被相应的 HTML 标记包围。

您还可以从 ISE 外部通过浏览器查看可显示的已上传文件，以进行测试。URL 为 https://*ise_ip*:8443/portal/customFiles/*filename*。

门户的高级自定义

如果不想使用Cisco ISE 提供的任一默认门户主题，您可以对门户进行自定义来满足您的需求。为此，您必须熟悉使用 CSS 和 JavaScript 文件以及 jQuery Mobile ThemeRoller 应用。

您不能修改默认门户主题，但可以执行以下操作：

- 导出门户的默认主题 CSS 文件，第 406 页，将其用作创建自定义门户主题的基础。
- 创建自定义门户主题 CSS 文件，第 407 页，方法是编辑默认门户主题并将其另存为新文件。
- 导入自定义门户主题 CSS 文件，第 415 页，并将其应用于门户。

基于您的专业知识程度和具体要求，您可执行各种高级自定义。您可以使用预定义变量来实现显示信息的一致性，在门户页面上添加广告，使用 HTML、CSS 和 Javascript 代码来自定义您的内容，以及修改门户页面布局。

您可以通过将 HMTL、CSS 和 javascript 添加到每个门户的**门户页面定制 (Portal Page Customization)** 选项卡上的内容框中来修改门户。本文档提供使用 HTML 和 CSS 进行定制的示例。使用 javascript 定制的示例位于此处的 ISE 社区：http://cs.co/ise-community。更多 HTML、CSS 和 Javascript 示例位于此处的 ISE 社区：https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042。

注释 TAC 不支持Cisco ISE 门户的 Javascript 定制。如果您在使用 Javascript 定制时遇到问题，请将您的问题发布到 ISE 社区 https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise。

启用高级门户自定义

Cisco ISE 可以让您自定义最终用户门户上显示的内容。在**门户页面自定义 (Portal Page Customization)** 下列出的不同页面上的文本框中输入 HTML、CSS 和 Javascript 代码。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **门户自定义 (Portal Customization)**。

步骤 2 验证在默认情况下是否已选中 **Enable portal customization with HTML**。此设置可以让您在**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段中包含 HTML 标签。

步骤 3 选中**启用 HTML 和 JavaScript 门户自定义 (Enable portal customization with HTML and Javascript)** 后，可以通过包含以下字段进行高级 JavaScript 自定义： <script> tags in the **说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段。

门户的主题和结构 CSS 文件

如果您具有使用 CSS 文件方面的经验，则可以自定义默认门户主题 CSS 文件以修改门户演示和操作页面布局、颜色和字体等元素。自定义 CSS 文件使您在指定演示特征时能够灵活控制，从而使您能够在多个页面上共享格式，并降低结构内容的复杂性和重复性。

Cisco ISE 最终用户门户使用两种不同类型的 CSS 文件：structure.css 和 *theme*.css。每个门户主题都有其自己的 *theme*.css 文件，但每个门户类型只有一个 structure.css 文件；例如，适用于访客门户的

guest.structure.css、适用于发起人门户的 sponsor.structure.css，以及适用于我的设备门户的 mydevices.structure.css。

structure.css 为页面布局和结构提供样式。它定义每个页面上的元素的定位，并且包括 jQuery Mobile 结构样式。只可以查看 structure.css 文件，但不能进行编辑。但是，当更改 *theme*.css 文件中的页面布局时，请将这些文件导入门户，并进行应用，最新更改将优先于 structure.css 样式。

theme.css 文件指定字体、按钮颜色和标题背景等样式。您可以导出 *theme*.css 文件，更改主题设置，然后导入这些设置，用作门户的自定义主题。对 *theme*.css 文件所做的所有页面布局样式更改都将优先于在 structure.css 文件中定义的样式。

无法修改任何Cisco提供的默认门户 *theme*.css 文件。但是，可以编辑文件中的设置并将这些设置保存到新的自定义 *theme*.css*theme*.css 文件。可以对自定义 *theme*.css 文件进行进一步编辑，但将其导入回 Cisco ISE 时，记得要使用与最初所用主题名称相同的名称。无法将两个不同的主题名称用于同一个 *theme*.css 文件。

例如，可以使用默认的 *green theme.css* 文件创建新的自定义 *blue theme.css* 文件并将该文件命名为 *Blue*。之后，可以编辑 *blue theme.css* 文件，但是当您再次导入此文件时，必须重新使用 *Blue* 主题名称。不能将其命名为 *Red*，因为Cisco ISE 会检查文件名与其名称之间的关系，以及主题名称的唯一性。但是，可以编辑 *blue theme.css* 文件，将其另存为 *red theme.css*，导入新文件，然后将其命名为 *Red*。

关于使用 jQuery Mobile 更改主题颜色

Cisco最终用户门户的颜色主题与 jQuery ThemeRoller 兼容。您可以使用 ThemeRoller 网站轻松编辑整个门户的颜色。

ThemeRoller颜色“样本”包含一个独特的颜色主题，用于定义主要UI元素（例如工具栏、内容块、按钮、列表项和字体文本阴影）的颜色、底纹和字体设置。颜色主题还定义按钮各种交互状态设置：正常、悬停和按下。

Cisco使用三种样本：

- 样本 A - 默认样本。
- 样本 B - 定义着重强调的元素，例如 **Accept** 按钮。
- 样本 C - 定义关键元素，例如警告、错误消息、无效输入字段和删除按钮。

您无法应用其他样本，除非您添加包含使用新增样本的元素的 HTML 代码（例如添加至 Optional Content 中）。

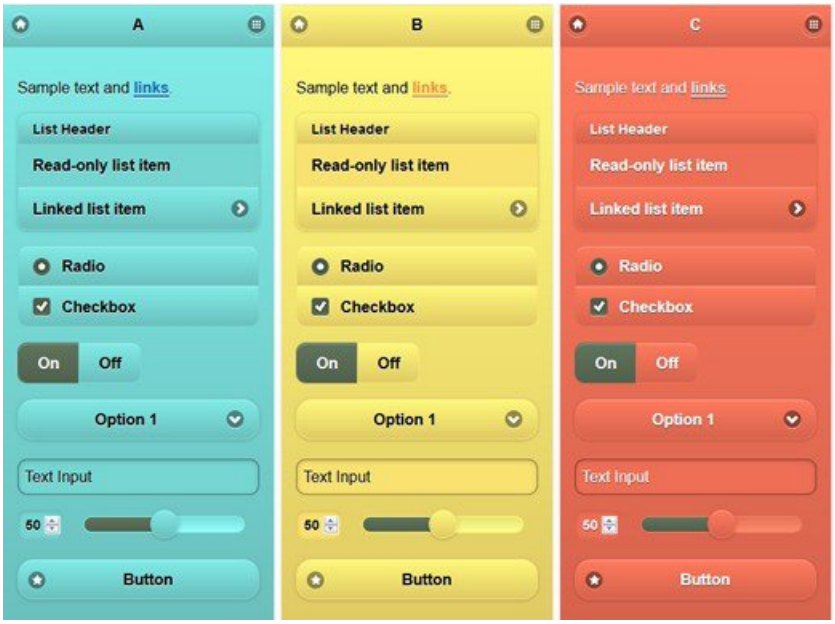
要编辑Cisco提供的默认 CSS 文件或创建基于默认主题中定义的 CSS 类和结构的新文件，请使用规定版本的 jQuery Mobile ThemeRoller（1.3.2 版本）。

有关jQuery Mobile ThemeRoller中样本和主题的更多信息，请参阅使用 ThemeRoller 创建自定义主题中的“创建主题概述”。请使用 jQuery Mobile ThemeRoller 在线帮助了解如何下载、导入和共享您的自定义主题。

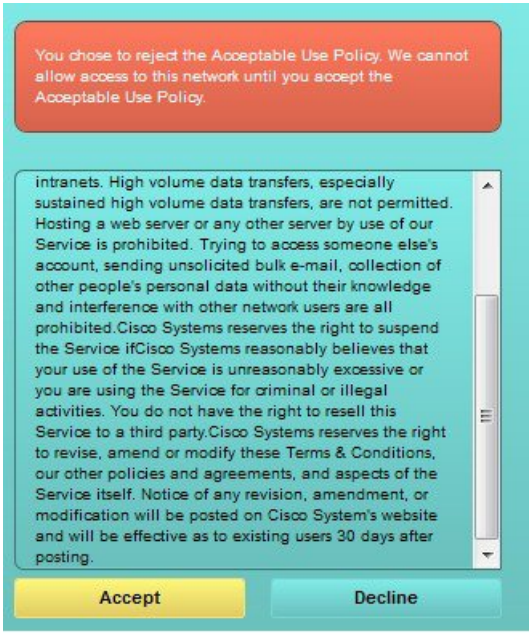
有关如何使用HTML、CSS和Javascript代码自定义在门户页面上显示的文本和内容的教程，请访问 CodeAcademy。

显示思科样本的主题示例

为了演示如何使用样本，我们在 ThemeRoller 中编辑了用于访客门户的默认主题以显示颜色差异。



以下屏幕显示访客门户登录错误（样本 C）以及要求用户操作的按钮（样本 B），屏幕的其余部分为样本 A。



使用 jQuery Mobile 更改主题颜色

开始之前

确保您使用的是 1.3.2 版本的 jQuery Mobile ThemeRoller。屏幕左上角会显示您所使用的版本，如下所示。

步骤 1 在门户上点击**配置 (Configuration)** 选项卡，从门户中导出您想要更改的现有主题。

步骤 2 选择 **高级定制 (Advanced Customization)** > **导出/导入主题 (Export/Import Themes)**。

步骤 3 在**自定义主题 (Custom Theming)** 对话框中，导出您要更新的主题。

步骤 4 在文本编辑器中打开该主题，全选并复制。

步骤 5 将该文本 (CSS) 粘贴到 jQuery 网站的**导入主题 (Import Theme)** 字段。

步骤 6 在 jQuery Mobil Web 版应用中执行更改。

步骤 7 从 jQuery 网站导出更新的主题（导出格式为 ZIP）。

步骤 8 解压缩更新的主题，从主题文件夹中将更新的主题提取至您的 PC。主题名称即您在 jQuery 网站提供的名称。

步骤 9 在门户配置页面的**自定义主题 (Custom Theming)** 对话框中将提取的 CSS 主题文件导入您的门户。

您可以点击**门户配置 (Portal Configuration)** 窗口上的**门户主题 (Portal Theme)** 下拉列表，在新旧主题之间来回切换。

基于位置的自定义

创建访客帐户后，您可以将其与某个位置关联并指定服务集标识符 (SSID) 属性。位置和 SSID 均可用作 CSS 类，您可以将 CSS 类用于根据访客的位置和 SSID 向门户页面应用不同的 CSS 样式。

例如：

- 访客位置 - 当使用 *San Jose* 或 *Boston* 作为位置的帐户的用户登录需要提供凭证的访客门户时，以下一个类可用于每个门户页面：**guest-location-san-jose** 或 **guest-location-boston**。
- 访客 SSID - 对于名称为 *Coffee Shop Wireless* 的 SSID，以下 CSS 类可用于每个门户页面：**guest-ssid-coffee-shop-wireless**。此 SSID 是您在访客帐户上指定的 SSID，而不是访客在登录时连接的 SSID。

注释 此信息仅适用于需要提供凭证的访客门户（在访客登录之后）。

当您向网络添加交换机和无线 LAN 控制器 (WLC) 等设备时，也可以指定位置。此位置还可用作根据网络设备的位置向门户页面应用不同 CSS 样式的 CSS 类。

例如，如果向 *Seattle* 分配 WLC 并且访客从 Seattle-WLC 重定向至Cisco ISE，以下 CSS 类可用于每个门户页面：**device-location-my-locations-usa-seattle**。

相关主题

根据访客位置自定义问候语，第 412 页

基于用户设备类型的自定义

Cisco ISE 会检测用来访问公司网络或最终用户 Web 门户（访客、发起人和设备）的客户端设备类型（访客、发起人或员工）。它会被检测为移动设备（Android、iOS 等）或桌面设备（Windows、MacOS 等）。设备类型可作为 CSS 类，您可以根据用户的设备类型，使用该类将不同的 CSS 样式应用到门户页面。

当用户登录任何Cisco ISE 最终用户 Web 门户时，门户页面上提供以下类：**cisco-ise-mobile** 或 **cisco-ise-desktop**。

相关主题

根据用户设备类型自定义问候语，第 413 页

导出门户的默认主题 CSS 文件

您可以下载Cisco提供的默认门户主题并按照您的需求进行自定义。您可以将其用做执行高级自定义的基础。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。

步骤 2 从**高级自定义 (Advanced Customization)** 下拉列表中，选择**导出/导入主题 (Export/Import Themes)**。

步骤 3 在**自定义主题 (Custom Theming)** 对话框中，使用下拉菜单选择您想要自定义的主题。

步骤 4 点击**导出主题 CSS (Export Theme CSS)** 以下载默认 *theme.css* 文件进行自定义。

步骤 5 点击**保存 (Save)** 将文件保存至您的桌面。

创建自定义门户主题 CSS 文件

通过自定义现有默认门户主题和在新门户 *theme*.css 文件中保存更改，可以创建自定义门户主题。可以修改默认主题设置和样本，对选中的门户进行全局更改。

开始之前

- 将 *theme*.css 文件从想要自定义的门户下载到桌面。
- 此任务需要拥有使用 HTML、CSS 和 Javascript 代码的经验。
- 使用 jQuery Mobile ThemeRoller 版本 1.3.2

步骤 1 将已下载的门户 *theme*.css 文件内容导入 jQuery Mobile ThemeRoller 工具。

提示 可以在更改时查看您的自定义，第 416 页。

步骤 2 （可选）在门户内容中嵌入链接，第 407 页

步骤 3 （可选）插入动态文本更新的变量，第 408 页

步骤 4 （可选）使用源代码设置文本格式和包含链接，第 409 页

步骤 5 （可选）将图像添加为广告，第 410 页

步骤 6 （可选）根据访客位置自定义问候语，第 412 页

步骤 7 （可选）根据用户设备类型自定义问候语，第 413 页

步骤 8 （可选）设置轮播广告，第 411 页

步骤 9 （可选）修改门户页面布局，第 414 页

步骤 10 将自定义文件另存为新的 *theme*.css 文件。

注释 不能将编辑保存到默认 CSS 主题文件。只能使用已进行的任何编辑创建新的自定义文件。

步骤 11 当新 *theme*.css 文件就绪时，可以将其导入Cisco ISE。

在门户内容中嵌入链接

您可以添加链接以使访客可以从门户页面访问各种网站。这些更改仅用于您进行自定义的特定门户页面。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用字段时缩放其大小。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals and Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

- 对于发起人门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals and Components)** > 发起人门户 **(Sponsor Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。
- 对于设备门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 设备门户管理 **(Device Portal Management)** >（任意门户）> 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。
- 对于证书调配门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 设备门户管理 **(Device Portal Management)** > 证书调配 **(Certificate Provisioning)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。

步骤 2 在页面 **(Pages)** 下，选择想要更新的页面。

步骤 3 在页面自定义 **(Page Customizations)** 下，使用带有可选内容 **(Optional Content)** 文本块的小型编辑器向门户页面添加链接。

步骤 4 点击创建链接 **(Create Link)** 按钮。
此时将显示链接属性 **(Link Properties)** 对话框。

步骤 5 输入 **URL** 并且在 URL 的描述 **(Description)** 窗口输入您要添加超链接的文本。

为使链接正常工作，URL 中应包括协议标识符。例如使用 http://www.cisco.com 而不是 www.cisco.com。

步骤 6 点击设置 **(Set)**，然后点击保存 **(Save)**。

可以使用 切换 **HTML** 源 **(Toggle HTML Source)** 选项查看应用于您使用小型编辑器进行格式设置的文本的 HTML 标记。

插入动态文本更新的变量

通过替代动态更新内容的预定义变量 ($variable$)，您可以为显示在门户的文本创建模板。这可以使向访客显示的文本和信息保持一致。这些更改仅用于您自定义的特定门户页面。

使用切换全屏 **(Toggle Full Screen)** 选项可在使用字段时缩放其大小。

步骤 1 导航至以下门户：

- 对于访客门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals and Components)** > 访客门户 **(Guest Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。
- 对于发起人门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals and Components)** > 发起人门户 **(Sponsor Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。
- 对于设备门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 设备门户管理 **(Device Portal Management)** >（任意门户）> 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。

步骤 2 在 **Pages** 下，选择要更新的页面。

步骤 3 在页面定制 **(Page Customizations)** 下，使用说明文本 **(Instructional Text)**、可选内容 **1 (Optional Content 1)** 和可选内容 **2 (Optional Content 2)** 字段随附的小型编辑器创建门户页面的文本模板。

例如，您可以为多个访客创建一个欢迎消息模板，但只有在访客成功登录并连接到网络之后才能看到个性化设置的消息。

步骤 4 像往常一样在字段中输入信息。

例如，您可以为门户输入一条欢迎消息：

```
欢迎来到我们公司的访客门户，
```

步骤 5 如果要用变量替代文本，请点击**插入变量 (Insert Variable)**。
变量列表将显示在弹出菜单中。

步骤 6 选择用于替代文本的变量。

例如，选择**名字 (First name)** 以在欢迎消息中显示每位访客的名字。变量 **ui_first_name** 会插入到光标位置：

```
欢迎来到我们公司的访客门户，$ ui_first_name $。
```

此欢迎消息会 出现在名叫 John 的访客的门户欢迎页面上： **Johen，欢迎访问我们公司的访客门户**。

步骤 7 根据需要继续使用变量列表，直到您在文本框中完成信息输入。

步骤 8 点击**保存 (Save)**。

可以使用 **切换 HTML 源 (Toggle HTML Source)** 选项查看应用于您使用小型编辑器进行格式设置的文本的 HTML 标记。

使用源代码设置文本格式和包含链接

除了可以将小型编辑器的格式设置和链接图标用于纯文本，您还可以使用 HTML、CSS 和 Javascript 代码来自定义在门户页面上显示的文本。这些更改仅用于您自定义的特定门户页面。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用文本框时缩放其大小。

开始之前

在以下路径中，确保默认启用**启用 HTML 门户自定义 (Enable portal customization with HTML)**：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **门户自定义 (Portal Customization)**。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在**页面 (Pages)** 下，选择想要更新的页面。

步骤 3 在**页面定制 (Page Customizations)** 下，使用**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段随附的小型编辑器输入和查看源代码。

步骤 4 点击**切换 HTML 源 (Toggle HTML Source)**。

步骤 5 输入您的源代码。

例如，要为文本添加下划线，请输入：

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

例如，要包含使用 HTML 代码的链接，请输入：

```
<a href="http://www.cisco.com">Cisco</a>
```

重要事项 当在 HTML 代码中插入外部 URL 时，确保您输入的是包括“http”或“https”的绝对（完整）URL 路径。

步骤 6 点击**保存 (Save)**。

相关主题

启用高级门户自定义，第 402 页

将图像添加为广告

您可以加入要在门户页面的特定区域中显示的图像和广告。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用文本框时缩放其大小。

开始之前

确保在以下位置启用**启用 HTML 门户自定义 (Enable portal customization with HTML)**：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **门户自定义 (Portal Customization)**。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在**页面 (Pages)** 下，选择想要更新的页面。

步骤 3 在**页面定制 (Page Customizations)** 下，使用**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段随附的小型编辑器输入和查看源代码。

步骤 4 点击**切换 HTML 源 (Toggle HTML Source)**。

步骤 5 输入您的源代码。

例如，要使用 HTML 代码在热点访客门户访问后横幅上加入产品广告及其图像，请在**访问后横幅 (Post-Access Banner)** 页面上的**可选内容 1 (Optional Content 1)** 文本框中输入以下代码：

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p> <img
src="http://www.static-cisco.com/assets/prod/root/catalyst_6800.jpg" width="100%" />
```

注释 当在 HTML 代码中插入外部 URL 时，确保您输入的是包括“http”或“https”的绝对（完整）URL 路径。

步骤 6 点击**保存 (Save)**。

设置轮播广告

轮播广告是一种广告格式，在一个横幅内显示多个产品图像和文本说明并且重复循环播放。在您的访客门户上使用轮播广告以推广多个相关产品或您公司提供的各种不同产品。

使用 **切换全屏 (Toggle Full Screen)** 选项可在使用文本框时缩放其大小。

开始之前

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **门户定制 (Portal Customization)** 并选中**通过 HTML 和 JavaScript 启用门户定制 (Enable portal customization with HTML and Javascript)**。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问权限 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。

步骤 2 在**页面 (Pages)** 下，选择想要更新的页面。

步骤 3 在**页面定制 (Page Customizations)** 下，使用**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段随附的小型编辑器输入和查看源代码。

步骤 4 点击 **Toggle HTML Source**。

步骤 5 输入您的源代码。

例如，要在访客门户上使用产品图像实施轮播广告，请在**访问后横幅 (Post-Access Banner)**（适用于热点门户）或**登录后横幅 (Post Login Banner)**（适用于需要凭证的访客门户）窗口的**可选内容 1 (Optional Content 1)** 字段中输入以下 HTML 和 Javascript 代码：

```
<script> var currentIndex = 0; setInterval(changeBanner, 5000); function changeBanner(){ var bannersArray
 = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%'/>", "<img
src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />", "<img
src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%'/>" ]; var div =
document.getElementById("image-ads"); if(div){ currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
div.innerHTML = bannersArray[currentIndex]; } } </script> <style> .grey{ color: black; background-color:
 lightgrey; } </style> <div class="grey" id="image-ads"> <img
src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/ content_parsys/overview/layout-
overview/gd12v2/gd12v2-left/n21v1_cq/ n21v1DrawerContainer.img.jpg/1379452035953.jpg'/> </div>
```

例如，要在访客门户上使用文本产品说明实施轮播广告，请在**访问后横幅 (Post-Access Banner)**（适用于热点门户）或**登录后横幅 (Post Login Banner)**（适用于需要凭证的访客门户）窗口的**可选内容 2 (Optional Content 2)** 字段中输入以下 HTML 和 Javascript 代码：

```
<script> var currentIndex = 0; setInterval(changeBanner, 2000); function changeBanner(){ var bannersArray
 = ["Optimize branch services on a single platform while delivering an optimal application experience
across branch and WAN infrastructure", "Transform your Network Edge to deliver high-performance, highly
 secure, and reliable services to unite campus, data center, and branch networks", "Differentiate your
service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware
 services"]; var colorsArray = ["grey", "blue", "green"]; var div = document.getElementById("text-ads");
 if(div){ currentIndex = (currentIndex<2) ? (currentIndex+1) : 0; div.innerHTML =
bannersArray[currentIndex]; div.className = colorsArray[currentIndex]; } } </script> <style> .grey{
color: black; background-color: lightgrey; } .blue{ color: black; background-color: lightblue; } .green{
 color: black; background-color: lightgreen; } </style> <div class="grey" id="text-ads"> 优化单一平台上的
分支机构服务，同时在分支机构和 WAN 基础架构上提供最佳应用体验 </div>
```

注释 当在 HTML 代码中插入外部 URL 时，必须输入包括“http”或“https”的绝对（完整）URL 路径。

步骤 6 点击**保存 (Save)**。

根据访客位置自定义问候语

此示例显示如何根据访客类型中配置的位置，自定义访客在登录需要提供凭证的访客门户（不是热点）后所看到的登录成功的消息。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用字段时缩放其大小。

步骤 1 导航至这些门户之一：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在**页面 (Pages)**中，点击**身份验证成功 (Authentication Success)**。

步骤 3 在**页面自定义 (Page Customizations)** 下，使用**可选内容 1 (Optional Content 1)** 字段随附的小型编辑器输入和查看 HTML 源代码。

步骤 4 点击**切换 HTML 源 (Toggle HTML Source)**。

步骤 5 输入您的源代码。

例如，要包含基于位置的问候语，请在**可选内容 1 (Optional Content 1)** 中输入以下代码：

```
<style> .custom-greeting { display: none; } .guest-location-san-jose .custom-san-jose-greeting { display: block; } .guest-location-boston .custom-boston-greeting { display: block; } </style> <div class="custom-greeting custom-san-jose-greeting">欢迎来到金州！ </div> <div class="custom-greeting custom-boston-greeting">欢迎来到海湾州！ </div>
```

访客将根据其特定位置，在登录成功后看到不同的问候语。

根据用户设备类型自定义问候语

可以根据客户端设备类型（移动设备或桌面设备）自定义在用户登录任何Cisco ISE 最终用户 Web 门户（访客、发起人和设备）之后向其发送的问候语。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用字段时缩放其大小。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在**页面 (Pages)** 下，选择想要更新的页面。

步骤 3 在**页面自定义 (Page Customizations)** 下，使用**可选内容 1 (Optional Content 1)** 字段随附的小型编辑器输入和查看 HTML 源代码。

步骤 4 点击**切换 HTML 源 (Toggle HTML Source)**。

步骤 5 输入您的源代码。

例如，要在 AUP 页面上包含基于设备类型的问候语，请在 AUP 窗口的**可选内容 1 (Optional Content 1)** 字段中输入以下代码：

```
<style> .custom-greeting { display: none; } .cisco-ise-desktop .custom-desktop-greeting { display: block; } .cisco-ise-mobile .custom-mobile-greeting { display: block; } </style> <div class="custom-greeting
```

```
custom-mobile-greeting">尝一下我们的新法式深烘咖啡！完美随身！</div> <div class="custom-greeting
custom-desktop-greeting">我们的三重巧克力玛芬回归了！找个座位品尝一下吧！ </div>
```

用户将在 AUP 页面上看到不同的问候语，视用户用于获取网络或门户访问权限的设备类型而定。

修改门户页面布局

可以操作页面的整体布局；例如，可以将边栏添加到 AUP 页面，以提供其他信息或信息链接。

步骤 1 将以下 CSS 代码添加到创建并计划应用于门户的自定义 *theme*.css 文件的底部。这会更改 AUP 页面布局。**可选内容 1 (Optional Content 1)** 字段在桌面和移动设备模式下显示为侧栏。

```
#page-aup .cisco-ise-optional-content-1 { margin-bottom: 5px; } @media all and ( min-width: 60em ) {
#page-aup .cisco-ise-optional-content-1 { float: left; margin-right: 5px; width: 150px; } #page-aup
.cisco-ise-main-content { float: left; width: 800px; } #page-aup .cisco-ise-main-content h1, #page-aup
.cisco-ise-main-content p { margin-right: auto; margin-left: -200px; } }
```

之后，可以在该门户的 AUP 窗口的**可选内容 1 (Optional Content 1)** 字段中使用 HTML 代码添加链接。

步骤 2 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portal & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问权限 (Guest Access)** > **门户和组件 (Portal & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)**。

步骤 3 在 **Pages** 下，选择要在其中包含边栏的页面。

步骤 4 在**页面定制 (Page Customizations)** 下，使用**可选内容 1 (Optional Content 1)** 字段随附的小型编辑器输入和查看源代码。

步骤 5 点击**切换 HTML 源 (Toggle HTML Source)**。

步骤 6 输入您的源代码。

例如，要为 AUP 窗口添加侧栏，请在 AUP 窗口上的**可选内容 1 (Optional Content 1)** 字段中输入此代码：

```
<ul data-role="listview"> <li>租车 (Rent a Car) </li> <li>排名前十的酒店 (Top 10 Hotels) </li> <li>免费按摩
 (Free Massage) </li> <li>尊巴课 (Zumba Classes)</li> </ul>
```

步骤 7 点击**保存 (Save)**。

下一步做什么

可以通过在**可选内容 (Optional Content)** 字段中输入不同的文本或 HTML 代码来定制其他页面。

导入自定义门户主题 CSS 文件

您可以上传已创建的任何自定义 *theme*.css 文件并将其应用于任何最终用户门户。这些更改将应用于您自定义的所有门户。

任何时候编辑自定义 *theme*.css 文件并将其导入回到Cisco ISE 中时，请记住使用原先对其使用的同一主题名称。无法将两个不同的主题名称用于同一个 *theme*.css 文件。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **配置 (Configure)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portal & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 从**高级自定义 (Advanced Customization)** 下拉列表中，选择**导出/导入主题 (Export/Import Themes)**。

步骤 3 在**自定义主题 (Custom Theming)** 对话框中，点击**浏览 (Browse)** 查找新的 *theme*.css 文件。

步骤 4 输入新文件的**主题名称 (Theme Name)**。

步骤 5 点击**保存 (Save)**。

下一步做什么

您可以将此自定义门户主题应用于要自定义的门户。

1. 从**门户主题 (Portal Themes)** 下拉列表中选择已更新的主题来应用于整个门户。
2. 点击**保存 (Save)**。

删除自定义门户主题

可以删除已导入Cisco ISE 中的任何自定义门户主题，除非某个门户正在使用该主题。不能删除Cisco ISE 提供的任何默认主题。

开始之前

想要删除的门户主题不应被任何门户使用。

步骤 1 导航至以下门户：

- 对于访客门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 访客门户 **(Guest Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。
- 对于发起人门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 发起人门户 **(Sponsor Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。
- 对于设备门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 设备门户管理 **(Device Portal Management)** >（任意门户）> 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)**。

步骤 2 从高级自定义 **(Advanced Customization)** 下拉列表选择 删除主题 **(Delete Themes)**。

步骤 3 从主题名称 **(Theme Name)** 下拉列表选择想要删除的门户主题。

步骤 4 点击删除 **(Delete)**，然后点击保存 **(Save)**。

查看您的自定义

您可以查看自己的自定义向门户用户（访客、发起人或员工）的显示方式。

步骤 1 点击 **Portal test URL** 查看您做出的更改。

步骤 2 （可选）点击预览 **(Preview)** 以动态查看所做的更改如何出现在各类设备上：

- 移动设备 - 在预览 **(Preview)** 下查看做出的更改。
- 桌面设备 - 点击预览 **(Preview)** 并点击桌面预览 **(Desktop Preview)**。

  如果没有显示更改，请点击 **Refresh Preview**。所显示的门户仅用于查看您做出的更改；您无法点击按钮或输入数据。

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

门户语言自定义

访客门户、发起人门户、我的设备门户和客户端调配门户会本地化为所有受支持的语言和区域设置。这包括文本、标签、消息、字段名称和按钮标签。如果客户端浏览器请求未映射到Cisco ISE 中的模板的区域设置，则门户使用英语模板显示内容。

通过使用管理门户，您可以针对每种语言单独修改用于访客门户、发起人门户和我的设备门户的字段，并且可以添加更多语言。当前，您无法自定义客户端调配门户的这些字段。

默认情况下，每种类型的门户都支持 15 种语言。您可以在门户页面自定义 **(Portal Page Customization)** 窗口中选择门户使用的语言，还可以选择更新该语言的页面内容。请注意，如果更改页面上一种语

言的字体和内容，则这些更改不会影响其他语言。导出语言文件时，会包含您在**门户页面自定义 (Portal Page Customization)** 窗口中所做的更改。

支持的语言为：

- 中文（简体）
- 中文（繁体）
- 捷克语
- 荷兰语
- 英语
- 法语
- 德语
- 匈牙利语
- 意大利语
- 日语
- 韩语
- 波兰语
- 葡萄牙语
- 俄语
- 西班牙语

编辑门户使用的语言

1. 打开要编辑的门户。
2. 在**门户页面自定义 (Portal Page Customization)** 选项卡上，从**查看 (view in)** 下拉列表中选择要编辑的语言。
3. 根据需要更改内容、标题和字体。
4. 保存该门户配置，并对要更新的其他语言重复此流程。

要编辑语言文件

每个**门户页面自定义 (Portal Page Customization)** 窗口还提供一个语言文件。语言文件是属性文件的 ZIP 文件，可用于自定义作为门户流程一部分的标题和文本，但不可用来在**门户页面自定义 (Portal Page Customization)** 窗口中自定义。

语言文件还包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点

访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

您可以导出压缩语言文件并对其进行更新，包括添加新语言或删除不需要的现有语言。

有关如何更新语言文件的说明，请参阅：

- 导出语言文件 ， 第 418 页
- 从语言文件添加或删除语言 ， 第 418 页
- 导入更新的语言文件 ， 第 419 页

导出语言文件

可以导出可供每个门户类型使用的语言文件，用以编辑和自定义其中指定的现有值，并添加或删除语言。

注释 语言属性文件中只有部分字典键支持在其值（文本）中使用 HTML。

步骤 1 导航至以下门户：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **编辑 (Edit)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **配置 (Configure)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)**。

步骤 2 点击**语言文件 (Language File)**，然后从下拉列表中选择**导出 (Export)**。

步骤 3 在桌面上保存压缩后的语言文件。

从语言文件添加或删除语言

如果想用于门户类型的语言在该语言文件中不存在，则可以创建新的语言属性文件，并将其添加到压缩语言文件中。如果有不需要的语言，则可以删除其语言属性文件。

开始之前

要添加或删除语言属性文件，请导出适于各个门户类型的压缩语言文件。

步骤 1 使用任何显示 UTF-8 的编辑器（例如 Notepad ++），为想要添加或删除语言的门户类型打开预定义语言文件。

如果想要为多个门户类型添加或删除语言，请使用所有适当的门户属性文件。

步骤 2 要添加新的语言，请将现有语言属性文件另存为新语言属性文件，与压缩语言文件中的其他文件使用相同的命名规范。例如，要创建新的日语语言属性文件，请将该文件另存为 Japanese.properties (*LanguageName*.properties)。

步骤 3 在新语言属性文件的第一行指定浏览器本地值，将新语言与其浏览器区域设置关联起来。例如，LocaleKeys=ja,ja-jp (LocaleKeys=*browser locale value*) 应当是 Japanese.properties 文件的第一行。

步骤 4 更新新语言属性文件中的所有字典键值（文本）。

无法更改字典键。只能更新其值。

注释 仅部分字典键支持在键值（文本）中使用 HTML。

下一步做什么

1. 压缩所有属性文件（新文件和现有文件），创建新的压缩语言文件。不包含任何文件夹或目录。

   注释 使用 Mac 时，解压 zip 文件将生成 DS 存储区。在编辑语言文件后进行压缩时，请勿在 zip 中包含 DS 存储区。要了解提取 DS 存储区的方法，请参阅 https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store。

2. 为压缩语言文件创建新名称或使用其原始名称。
3. 将压缩语言文件导入您从其导出的特定门户。

导入更新的语言文件

可以导入通过添加或删除语言属性文件或通过更新现有属性文件中的文本进行自定义的已编辑语言文件。

注释 确保不从 Word 文件复制和粘贴自定义内容。或者，选择**文件 (File) > 另存为 (Save As)** 并将 Word 文件保存为 HTML 格式。然后，您可以从 HTML 文件复制和粘贴自定义内容。

步骤 1 导航至以下门户：

- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （任意门户） > **编辑 (Edit)**。

步骤 2 点击**语言文件 (Language File)**，然后从下拉列表中选择**导入 (Import)**。

步骤 3 浏览以在桌面上查找新的压缩语言文件。

步骤 4 将语言文件重新导入从其导出文件的门户类型。

下一步做什么

要显示更改的文本或添加的新语言，请从 **View In** 下拉列表中选择特定语言。

自定义访客通知、审批和错误消息

在每个门户中，您可以自定义访客接收通知的方式，可以通过邮件、SMS 文本消息和打印方式。使用这些通知以邮件、文本发送登录凭证或打印登录凭证：

- 当访客使用自注册访客门户且成功进行自注册时。
- 当发起人创建访客帐户且要向访客提供详细信息时。当创建发起人组时，您可以确定是否授权发起人使用 SMS 通知。如果这些设施可用，则发起人总是可以使用邮件发送并打印通知。

您还可以自定义发送给发起人的邮件通知，用于发起人批准尝试获得访问网络权限的自助注册访客的请求。此外，您还可以自定义向访客和发起人显示的默认错误消息。

自定义邮件通知

可以自定义通过邮件发送给访客的信息。

开始之前

- 将 SMTP 服务器配置为启用邮件通知。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **SMTP 服务器 (SMTP Server)**。
- 配置对向访客发送邮件通知的支持。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **设置 (Settings)** > **访客电子邮件设置 (Guest Email Settings)**。选中**对访客启用邮件通知 (Enable email notifications to guests)**。
- 在以下路径中，确保默认启用**启用 HTML 门户自定义 (Enable portal customization with HTML)**：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **门户自定义 (Portal Customization)**。

步骤 1 对于自注册发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **通知访客 (Notify Guests)** > **电子邮件通知 (Email Notification)**。

步骤 2 可以更改在**全局页面自定义 (Global Page Customizations)** 下指定的**徽标 (Logo [Email])** 默认值。

步骤 3 指定**主题 (Subject)**和**邮件主体 (Email body)**。使用预定义变量指定邮件中包含的访客帐户信息。使用小型编辑器和 HTML 标记自定义文本。

步骤 4 在设置 (Settings) 下，可以：

- 选择分别发送用户名和密码 (Send username and password separately)，使用不同的邮件单独发送用户名和密码。如果选择此选项，两个单独的选项卡会显示在页面自定义 (Page Customizations) 中，用于自定义用户名邮件 (Username Email) 和密码邮件 (Password Email) 通知。
- 选择发送测试邮件 (Send Test Email)，将测试邮件发送到邮箱地址，以在所有设备上预览自定义设置，从而确保信息正确显示。

步骤 5 点击保存 (Save)，然后点击关闭 (Close)。

自定义 SMS 文本消息通知

您可以自定义通过 SMS 文本消息发送给访客的信息。

开始之前

- 配置用于将邮件发送到 SMS 网关以传达 SMS 文本消息的 SMTP 服务器。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 系统 (System) > 设置 (Settings) > SMTP 服务器 (SMTP Server)。
- 将发起人组配置为支持 SMS 文本通知。
- 设置具有第三方 SMS 网关的帐户。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择管理 (Administration) > 系统 (Systems) > 设置 (Settings) > SMS 网关 (SMS Gateway)。Cisco ISE 将文本消息作为邮件发送到网关，该网关通过 SMS 运营商将消息转发给指定用户。
- 在以下路径中，确保默认启用启用 HTML 门户自定义 (Enable portal customization with HTML)：管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 设置 (Settings) > 门户自定义 (Portal Customization)。

步骤 1 对于自注册访客或发起人门户，点击菜单 (Menu) 图标 (☰)，然后选择 工作中心 (Work Centers) > 访客访问 (Guest Access) > 门户和组件 (Portals & Components) > 访客或发起人门户 (Guest or Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > SMS 回执或 SMS 通知 (SMS Receipt or SMS Notification)。

步骤 2 使用迷你编辑器和 HTML 标签自定义消息文本 (Message Text)。使用预定义变量指定要在 SMS 文本消息中包含的访客帐户信息。

步骤 3 在设置 (Settings) 下，可以：

- 选择分别发送用户名和密码 (Send username and password separately)，以使用不同文本消息单独发送用户名和密码。如果选择此选项，则在页面自定义 (Page Customizations) 中会出现两个单独的选项卡，用于自定义用户名消息 (Username Message) 和密码消息 (Password Message) 通知。
- 选择发送测试消息 (Send Test Message)，向手机发送文本消息，以预览自定义，确保信息按预期显示。支持的电话号码格式包括：+1 ### ### ####、###-###-####、(###) ### ####、##########、1########## 等。

步骤 4 点击保存 (Save)，然后点击关闭 (Close)。

自定义打印通知

您可以自定义为访客打印的信息。

注释 在每个门户中，打印通知徽标沿用自电子邮件通知徽标设置。

开始之前

在以下路径中，确保默认启用**启用 HTML 门户自定义 (Enable portal customization with HTML)**：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **门户定制 (Portal Customization)**。

步骤 1 对于自行注册的访客和发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客或发起人门户 (Guest or Sponsor Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **打印回执或打印通知 (Print Receipt or Print Notification)**。

步骤 2 指定**打印说明文本 (Print Introduction Text)**。使用预定义变量指定邮件中包含的访客帐户信息。使用小型编辑器和 HTML 标记自定义文本。

步骤 3 在缩略图中预览自定义或点击**打印预览 (Print Preview)**。您无法在缩略图中查看任何 HTML 自定义。
如果选择**打印预览 (Print Preview)** 选项，则会显示一个窗口，从中可以打印帐户详细信息来确保信息按预期显示。

步骤 4 点击**保存 (Save)**，然后点击**关闭 (Close)**。

自定义审批请求邮件通知

您可以要求发起人需要批准自行注册的访客，才能创建访客帐户且访客才可以获取登录凭证。您可以自定义通过邮件发送至发起人，请求发起人批准的信息。只有在您已指定使用 Self-Registered Guest 门户的自行注册的访客必须经过批准才能获得网络访问权限的情况下，才会显示此通知。

开始之前

- 将 SMTP 服务器配置为启用邮件通知。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (Systems)** > **设置 (Settings)** > **SMTP 服务器 (SMTP Server)**。
- 配置对向访客发送邮件通知的支持。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **设置 (Settings)** > **访客电子邮件设置 (Guest Email Settings)**。选中**对访客启用邮件通知 (Enable email notifications to guests)**。
- 如果希望发起人批准自注册帐户请求，请在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡中的**自注册页面设置 (Self-Registration Page Settings)** 下选中**需要批准自注册访客 (Require self-registered guests to be approved)** 复选框。这会启用**门户页面自定义 (Portal Page Customization)** 页面中**通知 (Notifications)** 下方的**请求批准电子邮件 (Approval Request Email)** 选项卡，在这里可以自定义发送给发起人的电子邮件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **配置 (Configure)** > **自注册访客门户 (Self-Registered Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **请求批准电子邮件 (Approval Request Email)**。在此，您可以：

步骤 2 执行以下操作：

a) 在 **Global Page Customizations** 下更改在 **Logo** 中指定的默认标志。

b) 指定 **Subject** 和 **Email body**。使用预定义变量指定邮件中包含的访客帐户信息。使用小型编辑器和 HTML 标记自定义文本。例如，要在请求批准电子邮件中包含指向发起人门户的链接，请点击**创建链接 (Create a Link)** 按钮，然后将 FQDN 添加到发起人门户。

c) 在所有设备上使用 **Send Test Email** 预览您的自定义，确保其显示符合预期。

d) 点击**保存 (Save)**，然后点击 **关闭 (Close)**。

步骤 3 自定义发起人发送的批准电子邮件内容：

a) 选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)**。

b) 点击**门户页面自定义 (Portal Page Customization)**。

c) 点击**电子邮件通知 (Email Notification)** 选项卡并输入所需的详细信息。

编辑错误消息

可以完全自定义为访客、发起人和员工显示在“故障”(Failure) 页面中的错误消息。所有最终用户 Web 门户都具有“故障”(Failure) 页面，但黑名单门户除外。

步骤 1 执行以下操作之一：

- 对于访客门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **消息 (Messages)** > **错误消息 (Error Messages)**。
- 对于发起人门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **消息 (Messages)** > **错误消息 (Error Messages)**。
- 对于设备门户，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （**任何门户 [any Portals]**） > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **消息 (Messages)** > **错误消息 (Error Messages)**。

步骤 2 从**查看语言 (View In)** 下拉列表中选择在自定义消息时查看文本所要使用的语言。

下拉列表包含与特定门户关联的语言文件中的所有语言。确保将自定义门户页面时所做的任何更改更新到支持的语言属性文件中。

步骤 3 更新错误消息文本。可以通过键入 **aup** 等关键字来搜索特定错误消息，以便查找 AUP 相关的错误消息。

步骤 4 点击保存 **(Save)**，然后点击关闭 **(Close)**。

门户页面标题、内容和标签的字符限制

可以在 **Portal Page Customization** 选项卡的标题、文本框、说明、字段和按钮标签以及其他视觉元素中输入的最大和最小字符范围限制。

门户页面标题、内容和标签的字符限制

这些门户页面 UI 元素的导航路径如下：

- 对于访客门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 访客门户 **(Guest Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)** > 页面 **(Pages)**。
- 对于发起人门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 发起人门户 **(Sponsor Portals)** > 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)** > 页面 **(Pages)**。
- 对于设备门户，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 设备门户管理 **(Device Portal Management)** >（任意门户）> 编辑 **(Edit)** > 门户页面自定义 **(Portal Page Customization)** > 页面 **(Pages)**。

在标题、文本框、说明、字段与按钮标签，以及您自定义的其他门户页面可视元素中输入内容时，请使用此信息。这些更新仅适用于您自定义的特定页面。

注释 无论您输入的是单字节还是多字节字符，您最多都只能输入字段指定的最大字符数。多字节字符不影响字符限制。

字段类别	字段	字段标签：最小字符数	字段标签：最大字符数	字段输入值：最小字符数	字段输入值：最大字符数
常见页面元素	横幅标题				256
	页脚元素			0	2000
	浏览器页面标题			0	256
	说明文本			0	2000
	内容标题			0	256
	可选内容 1			0	2000

字段类别	字段	字段标签：最小字符数	字段标签：最大字符数	字段输入值：最小字符数	字段输入值：最大字符数
	可选内容 2			0	2000
	按钮标签	0	64		
	复选框标签	0	64		
	选项卡标签	0	64		
	链接标签	0	256		
AUP	AUP 文本			0	50000
消息文本	消息文本（显示在页面上）			0	2000
	消息文本（显示在弹出窗口中）			0	256
字段标签	所有字段标签	0	256		
字段输入（常规）	一般字段输入（请参阅下面的特殊情况）			0	256
字段输入（特殊情况）	“访问代码”(Access Code) 字段			1	20
	“注册代码”(Registration Code) 字段			1	20
	“用户名”(Username) 字段			1	64
	“密码”(Password) 字段			1	256
	“电话号码”(Phone Number) 字段			0	64
	“设备 ID”(Device ID) 字段			12	17

门户自定义

您可以自定义最终用户 Web 门户的外观和访客体验。如果您熟悉级联样式表 (CSS) 语言和 Javascript，您可以使用 jQuery Mobile ThemeRoller 应用，通过更改门户页面布局来自定义门户主题。

您可以通过从所需门户页面导出 CSS 主题或语言属性查看所有字段。有关详细信息，请参阅导出门户的默认主题 CSS 文件。

最终用户门户页面布局的 CSS 类和说明

使用这些 CSS 类可定义和修改Cisco ISE 最终用户 Web 门户的页面布局。

CSS 类名	说明
cisco-ise-banner	包括徽标、横幅图像和横幅文本。 在发起人门户和我的设备门户上，此类还包含可激活上下文菜单的按钮。例如，菜单可能会显示具有 **Log Out** 和 **Change Password** 等选项的弹出窗口。
cisco-ise-body	包含不属于横幅的一部分的所有页面元素。
cisco-ise-optional-content-1	默认情况下为空。您可以添加文本、链接以及 HTML 和 JavaScript 代码。
cisco-ise-main-content	包含门户页面的主要内容，例如说明性文本、操作按钮和 cisco-ise-footer 容器。
cisco-ise-optional-content-2	默认情况下为空。您可以添加文本、链接以及 HTML 和 JavaScript 代码。
cisco-ise-footer	页脚的一部分，它是 **Contact Support** 和在线 **Help** 等链接的占位符。
cisco-ise-footer-text	默认情况下为空。它是要在门户页面底部显示的任何内容（例如版权声明或免责声明）的占位符。

门户语言文件的 HTML 支持

每个门户的压缩语言文件包含该门户的默认语言属性文件。每个属性文件包含用于定义门户上显示的内容的字典键。

您可以自定义门户上显示的文本，包括**说明文本 (Instructional Text)**、**内容 (Content)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段中的内容。其中一些字段具有默认内容，而有些字段则为空。

其中，只有与这些字段关联的一些字典键在其值（文本）中支持 HTML。

黑名单门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 这是文件中字典键的不完整列表。

- key.blacklist.ui_reject_message

自带设备门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD 门户 (BYOD Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 这是文件中字典键的不完整列表。

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_instruction_message

- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message

证书调配门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配门户 (Certificate Provisioning Portal)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message

- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1
- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1
- key.manualcertprov.ui_post_access_optional_content_2
- key.manualcertprov.ui_landing_instruction_message
- key.manualcertprov.ui_status_page_single_generated_content
- key.manualcertprov.ui_status_generated_content

客户端调配门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message

- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

凭证访客门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.guest.ui_contact_instruction_message
- key.guest.ui_login_optional_content_1
- key.guest.ui_login_optional_content_2
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_device_reg_optional_content_2

- key.guest.ui_device_reg_optional_content_1
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_max_devices_instruction_message
- key.guest.ui_max_devices_optional_content_1
- key.guest.ui_self_reg_results_instruction_message
- key.guest.notification_credentials_email_body
- key.guest.ui_max_devices_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_changepwd_instruction_message
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_aup_instruction_message
- key.guest.ui_changepwd_optional_content_2
- key.guest.ui_changepwd_optional_content_1
- key.guest.ui_self_reg_results_optional_content_2
- key.guest.ui_self_reg_results_optional_content_1
- key.guest.ui_device_reg_instruction_message
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_vlan_execute_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_device_reg_max_reached_message
- key.guest.ui_byod_success_message

- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_aup_employee_text
- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_success_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_self_reg_optional_content_2
- key.guest.ui_self_reg_optional_content_1
- key.guest.ui_byod_reg_limit_message
- key.guest.notification_credentials_print_body
- key.guest.ui_byod_reg_content_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_aup_guest_text
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_self_reg_aup_text
- key.guest.ui_login_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_self_reg_results_aup_text
- key.guest.ui_device_reg_register_message

- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_self_reg_instruction_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_client_provision_posture_agent_scan_message

热点访客门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2

- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message
- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

对移动设备管理门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **MDM 门户 (MDM Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

- key.mdm.ui_contact_instruction_message
- key.mdm.ui_mdm_enrollment_after_message
- key.mdm.ui_error_optional_content_2
- key.mdm.ui_error_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_2
- key.mdm.ui_mdm_enroll_instruction_message
- key.mdm.ui_error_instruction_message
- key.mdm.ui_mdm_enrollment_link_message
- key.mdm.ui_mdm_not_reachable_message
- key.mdm.ui_contact_optional_content_2

- key.mdm.ui_mdm_continue_message
- key.mdm.ui_contact_optional_content_1

我的设备门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.mydevices.ui_add_optional_content_1
- key.mydevices.ui_add_optional_content_2
- key.mydevices.ui_post_access_instruction_message
- key.mydevices.ui_edit_instruction_message
- key.mydevices.ui_contact_optional_content_2
- key.mydevices.ui_contact_optional_content_1
- key.mydevices.ui_changepwd_optional_content_1
- key.mydevices.ui_changepwd_optional_content_2
- key.mydevices.ui_post_access_message
- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1
- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1

- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message
- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message
- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

发起人门户语言文件的 HTML 支持

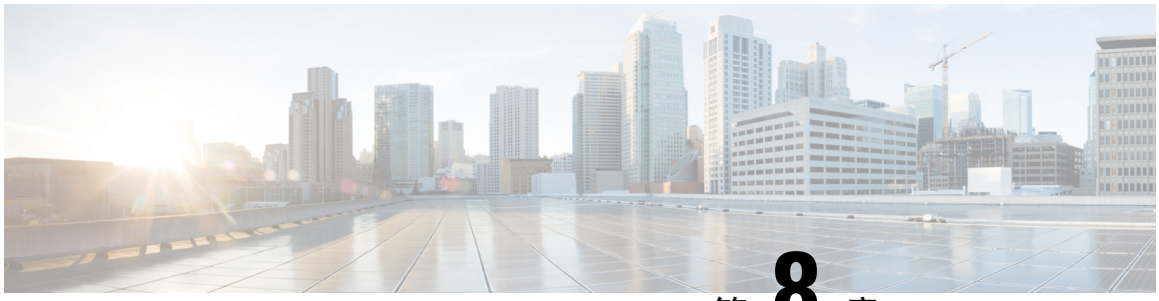
要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
- key.sponsor.ui_home_instruction_message
- key.sponsor.ui_post_access_instruction_message
- key.sponsor.notification_credentials_print_body
- key.sponsor.ui_aup_sponsor_text
- key.sponsor.ui_create_accounts_access_info_instruction_message
- key.sponsor.ui_login_instruction_message
- key.sponsor.notification_credentials_email_body
- key.sponsor.ui_create_known_instruction_message

- key.sponsor.ui_create_import_instruction_message
- key.sponsor.ui_suspend_account_instruction_message
- key.sponsor.ui_post_access_message
- key.sponsor.ui_login_optional_content_2
- key.sponsor.ui_login_optional_content_1
- key.sponsor.notification_credentials_email_password_body
- key.sponsor.ui_contact_optional_content_2
- key.sponsor.ui_contact_optional_content_1
- key.sponsor.ui_login_aup_text
- key.sponsor.ui_changepwd_instruction_message
- key.sponsor.ui_create_accounts_guest_type_instruction_message
- key.sponsor.ui_changepwd_optional_content_1
- key.sponsor.ui_changepwd_optional_content_2
- key.sponsor.notification_credentials_email_username_body
- key.sponsor.ui_aup_optional_content_1
- key.sponsor.ui_aup_optional_content_2
- key.sponsor.ui_post_access_optional_content_1
- key.sponsor.ui_post_access_optional_content_2
- key.sponsor.ui_contact_instruction_message



第 8 章

资产可视性

使用外部身份库对思科 ISE 进行管理访问

在Cisco ISE 中，您可以通过外部身份库（例如，Active Directory、LDAP 或 RSA SecureID）对管理员进行身份验证。您可以使用两种模式，通过外部身份库提供身份验证：

- 外部身份验证和授权：没有在本地Cisco ISE 数据库中为管理员指定的凭证，授权仅基于外部身份库组成员身份。此模式用于 Active Directory 和 LDAP 身份验证。

- 外部身份验证和内部授权：管理员的身份验证凭证来自外部身份源，并使用本地Cisco ISE 数据库分配授权和管理员职责。此模式用于 RSA SecurID 身份验证。此方法要求您同时在外部身份库和本地Cisco ISE 数据库中配置相同的用户名。

在身份验证过程中，如果与外部身份库的通信尚未建立或失败，Cisco ISE 将“后退”，并尝试从内部身份数据库执行身份验证。此外，无论已为其设置外部身份验证的管理员何时启动浏览器和发起登录会话，该管理员都可以从登录对话中的**身份存储区 (Identity Store)** 下拉列表中选择**内部 (Internal)**，请求通过Cisco ISE 本地数据库进行身份验证。

属于超级管理员组且配置为使用外部身份存储区进行身份验证和授权的管理员也可以使用外部身份存储区进行身份验证，以访问命令行界面 (CLI)。

注释 您可以将此方法配置为仅通过 Admin 门户提供外部管理员身份验证。Cisco ISE CLI 不具备这些功能。

如果网络没有一个或多个现有外部身份库，请确保已安装必要的外部身份库，并已将Cisco ISE 配置为访问这些身份库。

外部身份验证和授权

默认情况下，Cisco ISE 提供内部管理员身份验证。要设置外部身份验证，您必须为您在外部身份库中定义的外部管理员帐户创建密码策略。然后，您可以将此策略应用于最终成为外部管理员 RBAC 策略一部分的外部管理员组。

除了通过外部身份库提供身份验证之外，您的网络还可能要求您使用通用访问卡 (CAC) 身份验证设备。

要配置外部身份验证，必须执行以下操作：

- 使用外部身份库，配置基于密码的身份验证。
- 创建外部管理员组。
- 为外部管理员组配置菜单访问和数据访问权限。
- 为外部管理员身份验证创建 RBAC 策略。

使用外部身份库配置基于密码的身份验证

必须先为使用外部身份库（例如 Active Directory 或 LDAP）进行身份验证的管理员配置基于密码的身份验证。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)**。

步骤 2 在**身份验证方式 (Authentication Method)** 选项卡上，选择**基于密码 (Password Based)**，然后选择您应已配置的外部身份源之一。例如，您已创建的 Active Directory 实例。

步骤 3 为使用外部身份库进行身份验证的管理员配置您所需的特定密码策略设置。

步骤 4 点击**保存 (Save)**。

创建外部管理员组

您需要创建一个外部 Active Directory 或 LDAP 管理员组。这可确保Cisco ISE 使用外部 Active Directory 或 LDAP 身份存储区中定义的用户名验证您登录时输入的管理员用户名和密码。

Cisco ISE 将从外部资源导出 Active Directory 或 LDAP 组信息并将其存储为字典属性。然后，在为此外部管理员身份验证方法配置 RBAC 策略时，您可以将该属性指定为策略元素之一。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**

映射的外部组 (External Groups Mapped) 列显示映射到内部 RBAC 角色的外部组数量。您可以点击与管理员角色对应的数字以查看外部组（例如，如果点击超级管理员对应显示的 2，则系统将显示两个外部组的名称）。

步骤 2 点击**添加 (Add)**。

步骤 3 输入名称和可选说明。

步骤 4 点击**外部 (External)**。

如果已连接并加入 Active Directory 域，则**名称 (Name)** 字段中会显示 Active Directory 实例名称。

步骤 5 从**外部组 (External Groups)** 下拉列表框中，选择要为此外部管理员组映射的 Active Directory 组。

点击“+”号以将更多 Active Directory 组映射至此外部管理员组。

步骤 6 点击**保存 (Save)**。

创建内部只读管理员

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **管理员 (Administrators)** > **管理员用户 (Admin Users)** 。

步骤 2 点击**添加 (Add)**，然后选择**创建管理员用户 (Create An Admin User)**。

步骤 3 选中**只读 (Read Only)** 复选框以创建只读管理员。

将外部组映射至只读管理员组

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** 以配置外部身份验证源。

步骤 2 点击需要的外部身份源（例如 Active Directory 或 LDAP），然后从选定身份源检索组。

步骤 3 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)**，将管理员访问权限的身份验证方法映射到身份源。

步骤 4 依次选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **管理员 (Administrators)** > **管理员组 (Admin Groups)**，然后选择**只读管理员 (Read Only Admin)** 组。

步骤 5 选中**外部 (External)** 复选框，并选择您想要为其提供只读权限的所需外部组。

步骤 6 点击**保存 (Save)**。

无法将映射到只读管理员组的外部组分配到任何其他管理员组。

为外部管理员组配置菜单访问和数据访问权限

您必须配置可以分配给外部管理员组的菜单访问和数据访问权限。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **权限 (Permissions)**。

步骤 2 点击以下选项之一：

- **菜单访问 (Menu Access)**：属于外部管理员组的所有管理员都可以获得菜单或子菜单级别的权限。菜单访问权限决定着管理员可以访问的菜单或子菜单。
- **数据访问 (Data Access)**：属于外部管理员组的所有管理员都可以获得数据级别的权限。数据访问权限决定着管理员可以访问的数据。

步骤 3 为外部管理员组指定菜单访问或数据访问权限。

步骤 4 点击**保存 (Save)**。

创建用于外部管理员身份验证的 RBAC 策略

必须配置新的RBAC策略， 以便使用外部身份存储区对管理员进行身份验证，并指定自定义菜单和数据访问权限。此策略必须拥有用于身份验证的外部管理员组以及Cisco ISE 菜单和数据访问权限以管理外部身份验证和授权。

注释 您无法修改现有（系统预设）RBAC 策略以指定这些新外部属性。如果想要将某个现有策略用作模板，则必须复制该策略，为其重命名，然后分配新属性。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **RBAC 策略 (RBAC Policy)**。

步骤 2 指定规则名称、外部管理员组和权限。

请记住，必须向正确的管理员用户 ID 分配相应的外部管理员组。确保管理员与正确的外部管理员组关联。

步骤 3 点击**保存 (Save)**。

如果您以管理员身份登录，而且Cisco ISE RBAC 策略无法验证您的管理员身份，则Cisco ISE 会显示“unauthenticated”消息，而且您无法访问 Admin 门户。

使用外部身份库配置管理员访问权限以使用内部授权进行身份验证

此方法要求您同时在外部身份库和本地Cisco ISE 数据库中配置相同的用户名。当您配置Cisco ISE 使用外部 RSA SecurID 身份库来提供管理员身份验证时，管理员凭证身份验证将由 RSA 身份库执行。但是，授权（策略应用）仍根据Cisco ISE 内部数据库进行。此外，还要记住两个与外部身份和授权不同的重要因素：

- 您不需要为管理员指定任何特定的外部管理员组。
- 您必须同时在外部身份库和本地Cisco ISE 数据库中配置相同的用户名。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **管理员 (Administrators)** > **管理员用户 (Admin Users)**。

步骤 2 确保外部 RSA 身份库中的管理员用户名也存在于Cisco ISE 中。确保点击“密码”(Password) 下的 **外部 (External)** 选项。

注释 您不需要为此外部管理员用户 ID 指定密码，也不需要将任何特殊配置的外部管理员组应用到关联的RBAC策略。

步骤 3 点击**保存 (Save)**。

外部身份验证流程

当管理员登录时，登录会话会完成流程中的以下步骤：

1. 管理员发送 RSA SecurID 质询。
2. RSA SecurID 返回质询响应。
3. 管理员在Cisco ISE 登录对话框中输入用户名和 RSA SecurID 质询响应，就像输入用户 ID 和密码。
4. 管理员确保指定的身份库为外部 RSA SecurID 资源。
5. 管理员点击 **Login**。

登录之后，管理员仅可查看在 RBAC 策略中指定的菜单和数据访问项目。

外部身份源

您可以通过这些页面配置和管理包含Cisco ISE 用于身份验证和授权的用户数据的外部身份源。

LDAP 身份源设置

下表介绍“LDAP 身份源”(LDAP Identity Sources) 窗口上的字段，您可以使用此窗口创建 LDAP 实例并连接该实例。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

LDAP 常规设置

下表介绍**常规 (General)** 选项卡上的字段。

表 *49: LDAP* 常规设置

字段名称	使用指南
名称 (Name)	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
说明	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。
架构 (Schema)	您可以选择以下任一内置架构类型或创建自定义架构： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 您可以点击 Schema 旁边的箭头以查看架构详细信息。 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。
注释 仅当选择自定义架构时，才可以编辑以下字段。	
Subject Objectclass	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
主题名称属性 (Subject Name Attribute)	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。

字段名称	使用指南
组名称属性 **(Group Name Attribute)**	• CN：根据通用名称检索 LDAP 身份存储区组。 • DN：根据可分辨名称检索 LDAP 身份存储区组。
证书属性 **(Certificate Attribute)**	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
Group Objectclass	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。
组映射属性 **(Group Map Attribute)**	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 **(Subject Objects Contain Reference To Groups)**	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 **(Group Objects Contain Reference To Subjects)**	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 **(Subjects in Groups Are Stored in Member Attribute As)**	（仅适用于启用**组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects)** 选项时）指定在组成员属性中如何搜索成员，其默认值为 DN。
用户信息属性	默认情况下，预定义属性用于收集以下内置架构类型的用户信息（例如，名字、姓氏、电子邮件、电话，位置等）： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。 您还可以选择架构 (Schema) 下拉菜单中的定制 (Custom) 选项，根据要求编辑用户信息属性。

LDAP 连接设置

下表介绍**连接设置 (Connection Settings)** 选项卡中的字段。

表 *50: LDAP* 连接设置

字段名称	使用指南
启用辅助服务器 **(Enable Secondary Server)**	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器 **(Primary and Secondary Servers)**	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效IP地址。对于主机名，仅字母数字字符（a 至 z；A 至 Z；0 至 9）、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。
为每个 **ISE** 节点指定服务器	选中此复选框可配置每个PSN的主辅LDAP服务器主机名/IP 及其端口。 启用此选项后，将显示一个表，列出部署中的所有节点。您需要选择节点并配置主要和辅助LDAP服务器主机名/IP 及所选节点的端口。
访问	**匿名访问 (Anonymous Access)**：点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。 **身份验证访问 (Authenticated Access)**：点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员DN”(Admin DN) 字段和“密码”(Password) 字段输入信息。
管理员 **DN (Admin DN)**	输入管理员的DN。管理员DN是有权限搜索“用户目录子树”(User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。

字段名称	使用指南
安全身份验证 (Secure Authentication)	点击此字段以对Cisco ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口”(Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA”(LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 (Server Timeout)	以秒为单位输入Cisco ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 (Max. Admin Connections)	输入利用 LADP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于0）。这些连接用于在“用户目录子树”(User Directory Subtree) 和 “组目录子树”(Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
每 N 秒强制重新连接	选中此复选框并在秒 (Seconds) 字段中输入所需的值可强制服务器按照指定的时间间隔续订 LDAP 连接。有效范围为 1 至 60 分钟。
测试与服务器的绑定 (Test Bind to Server)	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
Failover	
Always Access Primary Server First	如果您希望Cisco ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
...后故障恢复到主服务器 (Failback to Primary Server after)	如果Cisco ISE 尝试连接的主 LDAP 服务器无法访问，Cisco ISE 会尝试连接辅助 LDAP 服务器。如果您希望Cisco ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

LDAP 目录组织设置

下表介绍目录组织 (Directory Organization) 选项卡上的字段。

表 *51: LDAP* 目录组织设置

字段名称	使用指南
主题搜索库 (Subject Search Base)	输入包含所有主题的子树的 DN。例如： o=corporation.com 如果包含主题的树是基本 DN，请输入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
组搜索库 (Group Search Base)	输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com 如果包含组的树是基本 DN，请键入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	输入一个MAC地址格式供Cisco ISE用于在LDAP数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当Cisco ISE 收到主机查找请求时，Cisco ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。 使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <*format*> 可以是以下任何一种格式： • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。

字段名称	使用指南
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	输入适当的文本以删除用户名的域前缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <start_string> 框中指定的多个字符，Cisco ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则Cisco ISE 会向 LDAP 服务器提交 user1。 注释 <start_string> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	输入适当的文本以删除用户名的域后缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，Cisco ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 *user1@domain*，则Cisco ISE 会向 LDAP 服务器提交 *user1*。 注释 *<end_string>* 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *52: LDAP* 组设置

字段名称	使用指南
添加	选择 **Add> 添加组**添加新组或从目录**中选择** Add> 选择 Group 选择组从 LDAP 目录。 如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。点击要选择的组旁边的复选框，然后点击**确定 (OK)**。选中的组将显示在**组 (Groups)** 窗口中。

LDAP 属性设置

表 *53: LDAP* 属性设置

字段名称	使用指南
添加	选择 **Add> 添加属性**添加新属性或从目录**中选择** Add> 选择属性从 LDAP 服务器的属性。 如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击**检索属性 (Retrieve Attributes)** 以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。

LDAP 高级设置

下表介绍“高级设置”(Advanced Settings) 选项卡中的字段。

表 *54: LDAP* 高级设置

字段名称	使用指南
启用密码更改 (Enable Password Change)	在使用 PAP 协议进行设备管理和使用 RADIUS EAP-GTC 协议进行网络访问时，选中此复选框可让用户在密码到期或重置密码的情况下更改密码。对于不受支持的协议，用户身份验证会失败。此选项还可以让用户在下次登录时更改密码。

相关主题

LDAP 目录服务，第 561 页
LDAP 用户身份验证，第 562 页
LDAP 用户查找，第 565 页
添加 LDAP 身份源，第 566 页

RADIUS 令牌身份源设置

下表介绍“RADIUS 令牌身份源”(Token Identity Sources) 窗口上的字段，您可以使用此窗口配置和连接外部 RADIUS 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

表 *55: RADIUS* 令牌身份源设置

字段名称	使用指南
名称	输入 RADIUS 令牌服务器名称。允许的最大字符数为 64。
说明	输入 RADIUS 令牌服务器说明。允许的最大字符数为 1024。

字段名称	使用指南
SafeWord Server	如果 RADIUS 身份源为 SafeWord 服务器，请选中此复选框。
Enable Secondary Server	选中此复选框，为Cisco ISE 启用辅助 RADIUS 令牌服务器，在主要服务器发生故障时用作备份。如果选中此复选框，必须配置辅助 RADIUS 令牌服务器。
Always Access Primary Server First	如果希望Cisco ISE 总是首先访问主服务器，请点击此选项。
Fallback to Primary Server after	点击此选项可指定在无法连接主服务器时，Cisco ISE 能够在多长时间里（分钟）使用辅助 RADIUS 令牌服务器进行身份验证。这段时间过后，Cisco ISE 重新尝试对照主服务器进行身份验证。
主服务器	
Host IP	输入主要 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在主要 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入主要 RADIUS 令牌服务器侦听的端口号。
Server Timeout	指定Cisco ISE 在确定主服务器关闭之前，等待主要 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在迁移到辅助服务器（如果已定义）或放弃请求（如果未定义辅服务器）之前，尝试重新连接到主服务器的次数。
辅助服务器	
Host IP	输入辅助 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在辅助 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入辅助 RADIUS 令牌服务器侦听的端口号。有效值为 1 至 65535。默认值为 1812。
Server Timeout	指定Cisco ISE 在确定辅助服务器关闭之前，等待辅助 RADIUS 令牌服务器发出响应的秒数。

字段名称	使用指南
Connection Attempts	指定Cisco ISE 在放弃请求之前应当尝试重新连接辅助服务器的次数。

相关主题

RADIUS 令牌身份源，第 582 页
添加 RADIUS 令牌服务器，第 587 页

RSA SecurID 身份源设置

下表介绍“RSA SecurID 身份源”(RSA SecurID Identity Sources) 窗口上的字段，您可以使用此窗口创建和连接 RSA SecurID 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 *56: RSA* 提示设置

字段名称	使用指南
Enter Passcode Prompt	输入文本字符串以获取密码。
Enter Next Token Code	输入文本字符串以请求下一个令牌。
Choose PIN Type	输入文本字符串以请求 PIN 类型。
Accept System PIN	输入文本字符串以接受系统生成的 PIN。
Enter Alphanumeric PIN	输入文本字符串以请求字母数字 PIN。
Enter Numeric PIN	输入文本字符串以请求数字 PIN。
Re-enter PIN	输入文本字符串以请求用户重新输入 PIN。

RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 *57: RSA* 消息设置

字段名称	使用指南
Display System PIN Message	输入文本字符串以编辑系统 PIN 消息。
Display System PIN Reminder	输入文本字符串以通知用户记住新 PIN。

字段名称	使用指南
Must Enter Numeric Error	输入一条消息，指导用户仅输入数字作为 PIN。
Must Enter Alpha Error	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
PIN Rejected Message	输入在系统拒绝用户的 PIN 时用户所看到的消息。
User Pins Differ Error	输入在用户输入错误 PIN 时所看到的消息。
System PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
Bad Password Length Error	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

相关主题

RSA 身份源，第 588 页
思科 ISE 和 RSA SecurID 服务器集成，第 589 页
添加 RSA 身份源，第 592 页

思科 ISE 用户

在本章中，“用户”一词是指定期访问网络的员工和承包商，以及发起人和访客用户。发起人用户是通过发起人门户创建和管理访客用户帐户的组织的员工或承包商。访客用户是在一段有限时间内需要访问组织的网络资源的外部访问者。

您必须为任何要获取对Cisco ISE 网络上的资源和服务的访问权限的用户创建帐户。员工、承包商和发起人用户可从管理门户创建。

用户身份

用户身份就像一个容纳关于用户的信息并形成其网络访问凭证的容器。每个用户的身份都由数据定义并且包括：用户名、邮件地址、密码、帐户说明、关联管理组、用户组和角色。

用户组

用户组是单个用户的集合，这些用户拥有一系列允许其访问特定Cisco ISE 服务和功能的相同权限。

用户身份组

用户的组身份包含用于标识和说明属于同一个组的一组特定用户的元素。组名是此组的成员具有的功能角色的说明。组是属于此组的用户的列表。

默认用户身份组

Cisco ISE 提供以下预定义用户身份组：

- Employee - 贵公司的员工属于此组。
- SponsorAllAccount - 可以暂停或恢复Cisco ISE 网络中的所有访客帐户的发起人用户。
- SponsorGroupAccounts - 可以暂停由同一发起人用户组中的发起人用户创建的访客帐户的发起人用户。
- SponsorOwnAccounts - 只能暂停其已创建的访客帐户的发起人用户。
- Guest - 需要临时访问网络中的资源的访问者。
- ActivatedGuest - 其帐户已启用并处于活动状态的访客用户。

用户角色

用户角色是决定用户可以执行什么任务以及可以访问Cisco ISE 网络上的什么服务的一系列权限。用户角色与用户组关联。例如，网络接入用户。

用户帐户自定义属性

Cisco ISE 允许根据用户属性限制网络访问用户和管理员的网络访问。Cisco ISE 具有一系列预定义的用户属性并且允许创建自定义属性。两种属性都可以用于定义身份验证策略的条件中。您还可以为用户帐户定义密码策略，以使密码符合指定的条件。

自定义用户属性

您可以在**用户自定义属性 (User Custom Attributes)** 窗口（**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 用户自定义属性 (User Custom Attributes)**）配置其他用户帐户属性。在此窗口中，您还可以查看预定义用户属性列表。不能编辑预定义用户角色。

在**用户自定义属性 (User Custom Attributes)** 窗格输入必填的详细信息以添加新的自定义属性。在添加或编辑网络访问用户（**管理 [Administration] > 身份管理 [Identity Management] > 身份 [Identities] > 用户 [Users] > 添加/编辑 [Add/Edit]**）或管理员用户（**管理 [Administration] > 系统 [System] > 管理访问 [Admin Access] > 管理员 [Administrators] > 管理员用户 [Admin Users] > 添加/编辑 [Add/Edit]**）时，会显示您在**用户自定义属性 (User Custom Attributes)** 窗口添加的自定义属性和默认值。在添加或编辑网络访问或管理员用户时，您可以更改默认值。

您可以在**用户自定义属性 (User Custom Attributes)** 窗口为自定义属性选择以下数据类型：

- 字符串 (String)：您可以指定最大字符串长度（字符串属性值允许的最大长度）。

- 整数 (Integer)：您可以配置最小和最大值（指定最低和最高的可接受整数值）。
- 枚举 (Enum)：您可以为每个参数指定以下值：
  - 内部使用
  - 显示值

  您还可以指定默认参数。在显示 (Display) 字段中添加的值会在添加或编辑网络访问或管理员用户时显示。
- Float
- 密码 (Password)：您可以指定最大字符串长度。
- 长 (Long)：您可以配置最小和最大值。
- IP：您可以指定默认 IPv4 或 IPv6 地址。
- Boolean：您可以设置 True 或 False 作为默认值。
- 日期(Date)：您可以从日历中选择一个日期并将其设置为默认值。该日期显示格式为 yyyy-mm-dd。

如果要在添加或编辑网络访问或管理员用户时将一个属性设置为强制属性，请选中**强制 (Mandatory)** 复选框。您还可以设置自定义属性的默认值。

自定义属性可在身份验证策略中使用。您为自定义属性设置的数据类型和允许范围将应用于策略条件中的自定义属性值。

用户身份验证设置

并非所有外部身份存储区都允许网络访问用户更改其密码。有关详细信息，请参阅每个身份源对应的部分。

网络使用密码规则是在以下位置配置的： **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **用户身份验证设置 (User Authentication Settings)**。

以下部分提供有关**密码策略 (Password Policy)** 选项卡上某些字段的更多信息。

- **必要字符 (Required Characters)**：如果配置要求使用大写或小写字符的用户密码策略，而用户的语言不支持这些字符，则用户无法设置密码。要支持 UTF-8 字符，请取消选中以下复选框：
  - 小写字母字符。
  - 大写字母字符
- **密码更改增量 (Password Change Delta)**：指定在将当前密码更改为新密码时必须更改的最小字符数。Cisco ISE 不会将字符位置更改视为更改。

  例如，如果密码增量为 3，当前密码为“?Aa1234?”，则“?Aa1567?”（“5”、“6”和“7”是三个新字符）是有效的新密码。“?Aa1562?”失败，因为“?”、“2”和“?”字符包含在当前密码中。“Aa1234??”失败，因为尽管字符位置已更改，但当前密码中的字符是相同的。

密码更改增量也会考虑以前的 X 个密码，其中 X 是**密码必须与以前的版本不同 (Password must be different from the previous versions)** 的值。如果密码增量为 3，密码历史记录为 2，则必须更改未包含在过去 2 个密码中的 4 个字符。

- **字典单词 (Dictionary words)**：选中此复选框可限制使用任何字典单词、它的逆序字符或用其他字符替换的字母。

  不允许用“$”替换“s”、“@”替换“a”、“0”替换“o”、“1”替换“l”、“!”替换“i”、“3”替换“e”。例如，“Pa$$w0rd”。

  - **默认字典 (Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。
  - **自定义字典 (Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**选择文件 (Choose File)** 以选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。

- 最终用户需要定期更改密码，否则用户帐户将被临时禁用。您可以使用**密码生存期 (Password Lifetime)** 部分更新密码重置间隔和提醒。要设置密码的生存期，请选中**若不更改密码则在 __ 天后禁用用户帐户 (Disable user account after __ days if password was not changed)** 复选框，然后在输入框中输入天数。要启用密码重置提醒，请选中**在密码到期前 __ 天显示提醒 (Display reminder __ days prior to password expiration)** 复选框，在输入值中输入天数，以便在密码到期之前向用户发送通知。
- **锁定/暂停帐户前的错误登录尝试数 (Lock/Suspend Account with Incorrect Login Attempts)**：如果登录尝试失败次数超过所指定的值，可以使用此选项暂停或锁定帐户。有效范围为 3 到 20。
- 在**帐户禁用策略 (Account Disable Policy)** 选项卡中，可以配置有关何时禁用现有用户帐户的规则。有关详细信息，请参阅全局禁用用户帐户。

相关主题

用户帐户自定义属性，第 455 页
添加用户，第 458 页

为用户和管理员生成自动密码

Cisco ISE 在用户和管理员创建页面引入了**生成密码 (Generate Password)** 选项，可根据Cisco ISE 密码策略生成即时密码。通过此选项，用户或管理员可使用Cisco ISE 生成的密码，而不用花时间思考需配置的安全密码。

Cisco ISE Web 界面中的以下三个位置可支持**生成密码 (Generate Password)** 选项

- 用户 - **管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)**。
- 管理员 - **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 管理员 (Administrators) > 管理员用户 (Admin Users)**。
- 登录的管理员（当前管理员） - **设置 (Settings) > 帐户设置 (Account Settings) > 更改密码 (Change Password)**。

内部用户操作

添加用户

通过Cisco ISE，您可以查看、创建、修改、复制、删除、导入、导出、搜索Cisco ISE 用户的属性，或更改用户属性的状态。

如果您使用Cisco ISE 内部数据库，则必须为需要访问Cisco ISE 中资源或服务的任何新用户创建帐户。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

您还可以通过访问以下位置来创建用户： **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **身份 (Identities)** > **用户 (Users)** 页面。

步骤 2 点击 **添加 (+) (Add[+])** 以创建新用户。

步骤 3 为字段输入值。

请勿在用户名中包含!、%、:、;、[、{、|、}、]、`、?、=、<、>、\和控制字符。此外，也不允许只包含空格的用户名。如果您使用用于自带设备的Cisco ISE 内部证书授权 (CA)，您在此处提供的用户名会用作终端证书的通用名称。Cisco ISE 内部 CA 的“通用名称”(Common Name) 字段不支持“+”或“*”字符。

步骤 4 点击**提交 (Submit)** 在Cisco ISE 内部数据库中创建新用户。

导出思科 ISE 用户数据

您可能需要从Cisco ISE 内部数据库中导出用户数据。Cisco ISE 允许您以受密码保护的 csv 文件格式导出用户数据。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

步骤 2 选中与要导出其数据的用户对应的复选框。

步骤 3 点击**导出所选 (Export Selected)**。

步骤 4 在 Key 字段中输入加密密码的密钥。

步骤 5 点击**开始导出 (Start Export)** 创建 users.csv 文件。

步骤 6 点击**确定 (OK)** 导出 users.csv 文件。

导入思科 ISE 内部用户

您可以使用 csv 文件将新用户数据导入 ISE 以创建新的内部帐户。可以在可导入用户帐户的页面上下载模板 csv 文件。您可以在以下位置导入用户： **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。 发起人可以在发起人门户上导入用户。“发起人门户指南”可以告诉发起人如何导入访客帐户。 请参阅 为创建发起人帐户配置帐户内容，第 346 页， 了解有关配置发起人访客帐户使用的信息类型的信息。

注释 如果 csv 文件包含自定义属性，则在导入期间，您为自定义属性设置的数据类型和允许范围将应用于自定义属性值。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**。

步骤 2 点击**导入 (Import)**，从逗号隔开的文本文件导入用户。

如果没有逗号分隔的文本文件，请点击**生成模版 (Generate a Template)**，以创建已填充标题行的 csv 文件。

步骤 3 在文件 (File) 文本框中，输入包含要导入的用户的文件名，或者点击**浏览 (Browse)**，导航至文件所在位置。

步骤 4 如果想要创建新的用户和更新现有用户，请选中**以新数据创建新用户和更新现有用户 (Create new user(s) and update existing user(s) with new data)** 复选框。

步骤 5 点击**保存 (Save)**，将更改保存到Cisco ISE 内部数据库。

注释 我们建议您不要一次性删除所有网络访问用户，因为这可能会导致 CPU 使用率达到峰值和服务崩溃，尤其是在使用一个非常大的数据库时。

终端设置

下表介绍**终端 (Endpoints)** 窗口上的字段，您可以使用此窗口创建终端和为终端分配策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *58:* 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的MAC地址以静态创建终端。 MAC 地址是连接到启用Cisco ISE 的网络的接口设备标识符。
Static Assignment	如果您想要在 Endpoints 页面静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。 您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。

字段名称	使用指南
Policy Assignment	（除非选中**静态分配 (Static Assignment)** 复选框，否则会默认禁用此字段）从**策略分配 (Policy Assignment)** 下拉列表选择匹配的终端策略。 您可以执行以下操作之一： • 如果您不选择匹配的终端策略，而是使用默认终端策略 Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。 • 如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中**静态分配 (Static Assignment)** 复选框。
Static Group Assignment	当您想要向身份组静态分配终端时，请选中此复选框。 如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。 如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。

字段名称	使用指南

Identity Group Assignment	选择您要将终端分配至哪个终端身份组。
	当您静态创建终端，或在为某个终端评估终端策略期间不想使用**创建匹配身份组 (Create Matching Identity Group)** 选项时，可将终端分配至身份组。
	Cisco ISE 包括以下系统创建的终端身份组：
	• Blacklist
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 659 页
使用策略和身份的静态分配创建终端，第 655 页

从 LDAP 设置导入终端

下表介绍“从 LDAP 导入”(Import from LDAP) 窗口上的字段，您可以使用此窗口从 LDAP 服务器导入终端。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *59:* 从 *LDAP* 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。 注释 Cisco ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。

字段名称	使用指南
Enable Secure Connection	选中**启用安全连接 (Enable Secure Connection)** 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	点击下拉箭头，查看受信任的 CA 证书。 根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在Cisco ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
Anonymous Bind	您必须选中**匿名绑定 (Anonymous Bind)** 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
Admin DN	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
密码 (Password)	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
Base DN	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
查询设置	
MAC Address objectClass	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
MAC Address Attribute Name	输入导入操作返回的属性名称，例如，macAddress。

字段名称	使用指南
Profile Attribute Name	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置**分析属性名称 (Profile Attribute Name)** 字段时，请考虑以下事项： • 如果未在**分析属性名称 (Profile Attribute Name)** 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知”(Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。 • 如果您在**分析属性名称 (Profile Attribute Name)** 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与Cisco ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。
超时	输入时间（单位：秒），值介于 1 和 60 秒之间。

相关主题

已识别的终端，第 659 页
从 LDAP 服务器导入终端，第 658 页

身份组操作

创建用户身份组

您必须创建用户身份组，才能为其分配用户。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **身份组 (Identity Groups)** > **用户身份组 (User Identity Groups)** > **添加 (Add)**。

您还可以用另一种方法创建用户身份组，访问 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **用户身份组 (User Identity Groups)** > **身份组 (Identity Groups)** > **用户身份组 (User Identity Groups)** > **添加 (Add)** 页面。

步骤 2 在 名称 字段和 描述 字段输入相应值。“名称”(Name) 字段支持的字符为空格 # $ & ‘ ( ) * + - . / @ _。

步骤 3 点击**提交 (Submit)**。

相关主题

用户身份组，第 455 页

导出用户身份组

Cisco ISE 允许您以 csv 文件格式导出本地配置的用户身份组。

步骤 1 选择管理 **(Administration)** > 身份管理 **(Identity Management)** > 组 **(Groups)** > 身份组 **(Identity Groups)** > 用户身份组 **(User Identity Groups)**。

步骤 2 选中想要导出的用户身份组对应的复选框，点击导出 **(Export)**。

步骤 3 点击确定 **(OK)**。

导入用户身份组

Cisco ISE 允许以 CSV 文件的形式导入用户身份组。

步骤 1 选择 管理 **(Administration)** > 身份管理 **(Identity Management)** > 组 **(Groups)** > 身份组 **(Identity Groups)** > 用户身份组 **(User Identity Groups)**。

步骤 2 点击生成模板 **(Generate a Template)** 获取用于导入文件的模板。

步骤 3 点击“导入”(Import)以从逗号分隔的文本文件导入网络访问用户。

步骤 4 如果您想要同时添加新用户身份组并更新现有用户身份组，请选中 用新数据覆盖现有数据 **(Overwrite existing data with new data)** 复选框。

步骤 5 点击导入 **(Import)**。

步骤 6 点击保存 **(Save)** 以将您的更改保存至Cisco ISE 数据库。

终端身份组设置

下表介绍“终端身份组”(Endpoint Identity Groups) 窗口上的字段，您可以使用此窗口创建终端组。要查看此处窗口，请点击菜单 **(Menu)** 图标 (☰)，然后选择管理 **(Administration)** > 身份管理 **(Identity Management)** > 组 **(Groups)** > 终端身份组 **(Endpoint Identity Groups)**。

表 *60*: 终端身份组设置

字段名称	使用指南
名称	输入您要创建的终端身份组的名称。
说明	输入对您要创建的终端身份组的说明。
Parent Group	从 Parent Group 下拉列表选择您要关联新创建的终端身份组的终端身份组。

相关主题

已识别终端划分为终端身份组，第 662 页
创建终端身份组，第 661 页

配置最大并发会话数

为了获得最佳性能，您可以限制并发用户会话的数量。您可以在用户级别或组级别上设置限制。系统根据最大用户会话配置，将会话计数应用于用户。

您可以为每个 ISE 节点的每个用户配置最大并发会话数。超过此限制的会话将被拒绝。

步骤 1 选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 最大会话数 (Max Sessions) > 用户 (User)**。

步骤 2 执行以下操作之一：

- 输入**每个用户最大会话数 (Maximum Sessions per User)** 字段中允许的每个用户的最大并发会话数。

  或

- 如果您希望用户拥有无限会话，请选中**无限会话 (Unlimited Sessions)** 复选框。默认情况下，此选项已选中。

步骤 3 点击**保存 (Save)**。

如果在用户和组级别上配置最大会话数，则较小的值将具有优先级。例如，如果用户的最大会话值设置为 10，用户所属组的最大会话值设置为 5，则用户最多只能有 5 个会话。

组的最大并发会话数

您可以配置身份组的最大并发会话数。

有时，组中的几个用户可以使用所有会话。其他用户创建新会话的请求被拒绝，因为会话数已达到配置的最大值。Cisco ISE 允许您为组中的每个用户配置最大会话限制；属于特定身份组的每个用户能够打开的会话数不可超过该会话限制，无论同一组的其他用户打开了多少会话。当计算特定用户的会话限制时，最低配置值优先 - 无论每个用户的全局会话限制、用户所属的每个身份组的会话限制或组中每个用户的会话限制为何。

要为身份组配置最大并发会话数，请执行以下操作：

步骤 1 请选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 最大会话 (Max Sessions) > 组 (Group)**。

列出所有已配置的身份组。

步骤 2 点击要编辑的组旁边的编辑 (Edit) 图标，然后输入以下内容的值：

- 该组允许的并发会话的最大数。如果一个组的最大会话数设置为 100，则该组的所有成员建立的所有会话总数不能超过 100。

  注释 组级别会话限制基于组层次结构而实施。

- 该组中每个用户允许的最大并发会话数。此选项将覆盖组的最大会话数。

如果要将组的最大并发会话数或组中用户的最大并发会话数设置为无限制，请将**组的最大会话数/组中用户的最大会话数 (Max Sessions for Group/Max Sessions for User in Group)** 字段留空，点击勾选图标，然后点击“保存”(Save)。默认情况下，这两个值都设置为无限制。

步骤 3 点击**保存 (Save)**。

配置计数器时间限制

您可以为并发用户会话配置超时值。

步骤 1 选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 最大会话数 (Max Sessions) > 计数器时间限制 (Counter Time Limit)**。

步骤 2 选择以下选项之一：

- **无限 (Unlimited)**：如果您不想为会话设置任何超时或时间限制，请选中此复选框。
- **删除会话前等待 (Delete sessions after)**：您可以输入并发会话的超时值（分钟、小时或天）。当会话超过时间限制时，Cisco ISE 会从计数器中删除会话，并更新会话计数，从而允许新的会话。用户的会话超过时间限制时，并不会注销用户。

步骤 3 点击**保存 (Save)**。

您可以从 RADIUS 实时日志 (RADIUS Live Logs) 页面重置会话计数。点击身份 (Identity)、身份组 (Identity Group) 或服务器 (Server) 列上显示的操作 (Actions) 图标以重置会话计数。当您重设会话时，会话从计数器中删除（从而允许新的会话）。当会话从计数器中删除时，用户不会断开连接。

帐户禁用策略

Cisco ISE 为用户和管理员引入了帐户禁用策略，以实现与 Cisco Secure ACS 同等的功能。对用户或管理员进行身份验证或查询时，Cisco ISE 会在**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 用户身份验证设置 (User Authentication Settings)** 页面中检查全局帐户禁用策略设置，并根据配置进行身份验证或返回结果。

Cisco ISE 会验证以下三个策略：

- 禁用超过指定日期 (yyyy-mm-dd) 的用户帐户 - 在指定日期禁用用户帐户。但是，在**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users) > 帐户禁用策略 (Account Disable Policy)** 中为单个网络访问用户配置的帐户禁用策略设置优先于全局设置。
- 在帐户创建或最后一次启用 *n* 天后禁用用户帐户 - 在帐户创建或帐户最后一次处于活动状态的日期过去指定天数后禁用用户帐户。您可以在**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users) > 状态 (Status)** 中检查用户状态。

- 处于非活动状态 *n* 天后禁用帐户 - 禁用在配置的连续天数内尚未进行身份验证的管理员和用户帐户。

从Cisco Secure ACS 迁移至Cisco ISE 后，为Cisco安全 ACS 中的网络访问用户指定的帐户禁用策略设置迁移至Cisco ISE。

禁用单个用户帐户

如果禁用帐户日期超过管理员用户指定的日期，Cisco ISE 允许您禁用每个用户的用户帐户。

步骤 1 依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)**。

步骤 2 点击**添加 (Add)** 创建新用户或者选中现有用户旁边的复选框并点击**编辑 (Edit)** 编辑现有用户的详细信息。

步骤 3 选中**禁用帐户，如果日期超出 (Disable account if the date exceeds)** 复选框并选择日期。

此选项允许您在已配置日期超出用户级别时禁用用户帐户。您可以根据需要为不同用户配置不同的到期日期。此选项将否决每个用户的全局配置。已配置日期可以是当前系统日期或未来日期。

注释 不允许输入早于当前系统日期的日期。

步骤 4 点击**提交 (Submit)** 配置个人用户帐户的帐户禁用策略。

全局禁用用户帐户

您可以在特定日期、超过帐户创建日期或最后一次访问日期一定天数后，以及帐户处于非活动状态一定天数后，禁用用户帐户。

步骤 1 依次选择**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 用户身份验证设置 (User Authentication Settings) > 帐户禁用策略 (Account Disable Policy)**。

步骤 2 执行下列操作之一：

- 选定**如果日期超过...则禁用帐户 (Disable account if date exceeds)** 复选框，并按照 yyyy-mm-dd 格式选择合适的日期。通过该选项，您可以在用户帐户超过设定的日期时，禁用该帐户。用户级别的**如果日期超过...则禁用帐户 (Disable account if date exceeds)** 设置优先于此全局配置。
- 选定**在帐户创建 n 天后或最后一次启用后禁用帐户 (Disable account after n days of account creation or last enable)** 复选框，并输入天数。此选项在帐户创建日期或最后一次访问的日期超过指定天数时禁用用户帐户。管理员可以手动启用已禁用的用户帐户，这会重置天数计数。
- 选定**在 n 天不活跃之后禁用帐户**复选框，并输入天数。此选项在帐户不活跃天数超过指定天数时禁用用户帐户。

步骤 3 点击**提交 (Submit)** 配置全局帐户禁用策略。

内部和外部身份源

身份源是存储用户信息的数据库。Cisco ISE 在身份验证期间使用身份源中的用户信息来验证用户凭证。用户信息包括组信息和与用户关联的其他属性。您可以添加、编辑以及从身份源删除用户信息。

Cisco ISE 支持内部和外部身份源。您可以使用两个来源对发起人和访客用户进行身份验证。

内部身份源

Cisco ISE 有一个内部用户数据库，可用来存储用户信息。内部用户数据库中的用户称为内部用户。Cisco ISE 还有一个内部终端数据库，存储关于所有设备以及与其相连的终端的信息。

外部身份源

Cisco ISE 允许您配置包含用户信息的外部身份源。Cisco ISE 连接外部身份源，获取身份验证所需的用户信息。外部身份源还包括Cisco ISE 服务器的证书信息以及证书身份验证配置文件。Cisco ISE 使用身份验证协议与外部身份源进行通信。

为内部用户配置策略时，请注意以下几点：

- 配置身份验证策略，以根据内部身份存储区对内部用户进行身份验证。
- 通过选择以下选项为内部用户组配置授权策略：

  `Identitygroup.Name EQUALS User Identity Groups:` **`Group_Name`**

下表列出了身份验证协议以及它们支持的外部身份源。

表 *61:* 身份验证协议和支持的外部身份源

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	REST
EAP-GTC，PAP（纯文本密码）	支持	支持	支持	支持	支持
MS-CHAP 密码散列： MSCHAPv1/v2 EAP-MSCHAPv2（作为 PEAP、EAP-FAST、EAP-TTLS 或 TEAP 的内部方法） LEAP	支持	支持	不支持	否	否

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	REST
EAP-MD5 CHAP	支持	不支持	否	否	否
EAP-TLS PEAP-TLS （证书检索） 注释 对于 TLS 身份验证（EAP-TLS 和 PEAP-TLS），身份源不是必需的，但是可以选择为授权策略条件添加。	不支持	支持	支持	不支持	否

凭证的存储方式不同，具体取决于外部数据源连接类型和使用的功能。

- 当加入 Active Directory 域（但不用于被动 ID）时，不会保存用于加入的凭证。CiscoISE会创建AD计算机帐户（如果不存在），并使用该帐户对用户进行身份验证。
- 对于 LDAP 和被动 ID，用于连接到外部数据源的凭证也用于对用户进行身份验证。

创建外部身份源

Cisco ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

注释 要使用被动身份服务以接收和共享经过身份验证的用户身份，请参阅其他被动身份服务提供程序，第 522 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅将 Active Directory 用作外部身份源，第 471 页。

- 选择 **LDAP** 以添加 LDAP 身份源。有关详细信息，请参阅 LDAP，第 561 页。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关详细信息，请参阅 RADIUS 令牌身份源，第 582 页。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关详细信息，请参阅 RSA 身份源，第 588 页。
- 选择 **SAML Id 提供程序 (SAML Id Providers)** 添加身份提供程序 (IdP)，例如 Oracle 访问管理器。有关详细信息，请参阅 SAMLv2 身份提供者作为外部身份源，第 594 页。
- 选择**社交登录 (Social Login)** 以将社交登录（如 Facebook）设置为外部身份源。请参阅用于自行注册访客的社交媒体登录，第 322 页。

利用外部身份存储密码验证内部用户

Cisco ISE 允许您利用外部身份存储密码验证内部用户。Cisco ISE 可通过以下页面为内部用户提供选择密码身份存储的选项：**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)** 页面。在“用户”(Users) 页面添加或编辑用户时，管理员可以从Cisco ISE 外部身份源列表中选择身份存储。内部用户的默认密码身份存储为内部身份存储。Cisco Secure ACS 用户在从 Cisco Secure ACS 迁移至Cisco ISE 过程中及之后将会保持相同的密码身份存储。

Cisco ISE 支持以下密码类型的外部身份存储：

- Active Directory
- LDAP
- ODBC
- RADIUS 令牌服务器
- RSA SecurID 服务器

证书身份验证配置文件

对于每个配置文件，必须指定应用作主体用户名的证书字段，以及是否希望对证书进行二进制比较。

添加证书身份验证配置文件

您必须创建证书验证配置文件，如果您想要使用可扩展身份验证协议 - 传输层安全 (EAP-TLS) 基于证书的身份验证方法，即必须创建证书身份验证配置文件。Cisco ISE 不是通过传统的用户名与密码方法进行身份验证，而是将从客户端接收的证书与服务器中的证书进行比较，从而验证用户的身份。

开始之前

您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **证书身份验证配置文件 (Certificate Authentication Profile)** > **添加 (Add)**。

步骤 2 为证书身份验证配置文件输入名称和可选说明。

步骤 3 从下拉列表中选择身份库。

基本证书检查不需要使用身份源。如果希望对证书进行二进制比较，就必须选择身份源。如果您选择 Active Directory 作为身份源，使用者和通用名称以及使用者替代名称（所有值）都可用于查找用户。

步骤 4 从**证书属性**或**证书中的任何主体或备选名称属性**中选择身份的使用。此身份将用于日志以及查找。

如果选择**证书中的任何主体或备选名称属性**，则 Active Directory UPN 将用作日志的用户名，并将尝试使用证书中的所有主体名称和备选名称来查找用户。只有选择 Active Directory 作为身份源时，此选项才可用。

步骤 5 如果您想要将客户端证书与身份库中的证书进行匹配，请选择 **Match Client Certificate Against Certificate In Identity Store**。为此，您必须选择身份源（LDAP 或 Active Directory）。如果您选择 Active Directory，您可以选择仅为解决身份不明情况而匹配证书。

- **从不 (Never)**：此选项从不执行二进制比较。
- **仅用于解决身份模糊 (Only to resolve identity ambiguity)**：此选项仅在遇到身份不明情况时，才将客户端证书与 Active Directory 中帐户的证书进行二进制比较。例如，系统发现若干个 Active Directory 帐户与证书中的身份名称匹配，就属于身份不明情况。
- **始终执行二进制比较 (Always perform binary comparison)**：此选项始终将客户端证书与身份库（Active Directory 或 LDAP）中帐户的证书进行二进制比较。

步骤 6 点击**提交 (Submit)** 以添加证书身份验证配置文件或保存更改。

将 Active Directory 用作外部身份源

Cisco ISE 使用 Microsoft Active Directory 作为外部身份源以访问用户、设备、组和属性等资源。Active Directory 中的用户和设备身份验证仅允许对 Active Directory 中列出的用户和设备进行网络访问。

ISE 社区资源

使用 AD 凭证的 ISE 管理门户访问配置示例

支持 Active Directory 的身份验证协议和功能

Active Directory 支持使用某些协议对用户和设备进行身份验证、更改 Active Directory 用户密码等功能。下表列出了 Active Directory 支持的身份验证协议及相应功能。

表 *62: Active Directory* 支持的身份验证协议

身份验证协议	功能
EAP-FAST 和基于密码的受保护的可扩展身份验证协议 (PEAP)	用户和设备身份验证，能够使用 EAP-FAST 和 PEAP 结合 MS-CHAPv2 和 EAP-GTC 的内部方法更改密码
密码身份验证协议 (PAP)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)	用户和设备身份验证
可扩展身份验证协议 - 通用令牌卡 (EAP-GTC)	用户和设备身份验证
可扩展身份验证协议 - 传输层安全 (EAP-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
可扩展身份验证协议 - 通过安全隧道的灵活身份验证-传输层安全 (EAP-FAST-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
受保护的可扩展身份验证协议 - 传输层安全 (PEAP-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
轻型可扩展身份验证协议 (LEAP)	用户身份验证

用于授权策略的 Active Directory 属性和组检索

Cisco ISE 从 Active Directory 检索用户或设备属性和组以用于授权策略规则。这些属性可用于Cisco ISE 策略并且决定了用户或设备的授权级别。Cisco ISE 在身份验证成功后会检索用户和设备 Active Directory 属性，还可以为与身份验证无关的授权检索属性。

Cisco ISE 可以使用外部身份存储区中的组来为用户或计算机分配权限；例如，将用户映射到发起人组。请注意 Active Directory 中的以下组成员身份限制：

- 策略规则条件可引用以下任意组：用户或计算机的主要组、用户或计算机作为直接成员的组，或者间接（嵌套）组。

- 不支持在用户或计算机的帐户域外的域本地组。

注释 您可以使用 Active Directory 属性 (msRadiusFramedIPAddress) 的值作为 IP 地址。可将此 IP 地址发送给授权配置文件中的网络接入服务器 (NAS)。msRADIUSFramedIPAddress 属性仅支持 IPv4 地址。在进行用户身份验证时，为用户获取的 msRadiusFramedIPAddress 属性值将转换为 IP 地址格式。

系统按加入点检索和管理属性和组。这些属性和组将用于授权策略（方法是首先选择加入点，然后选择属性）。您无法按范围为授权定义属性或组，但可以对身份验证策略使用范围。当您在身份验证策略中使用范围时，可以通过一个加入点对用户进行身份验证，但要通过另一个具有用户帐户域信任路径的加入点检索属性和/或组。您可以使用身份验证域来确保一个范围中的任两个加入点在身份验证域中都没有任何重叠。

注释 在多加入点配置的授权过程中，Cisco ISE 会按照加入点在授权策略中列出的顺序搜索它们，直到找到特定用户才会停止。找到用户后，在加入点中分配给用户的属性和组将用于评估授权策略。

注释 请参阅 Microsoft 对可用 Active Directory 组施加的最大数量限制： http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

如果规则包含带有特殊字符（例如 /、!、@、\、#、$、%、^、&、*、(、)、_、+ 或 ~）的 Active Directory 组名称，则授权策略会失败。

如果管理员用户名包含 $ 字符，则通过 Active Directory 进行的管理员用户登录可能会失败。

使用显式 UPN

要在将用户信息与 Active Directory 的用户主体名称 (UPN) 属性进行匹配时降低模糊性，您必须将 Active Directory 配置为使用显式 UPN。如果两个用户具有相同的 *sAMAccountName* 值，则使用显式 UPN 可能会产生模糊结果。

要在 Active Directory 中设置显式 UPN，请打开**高级调整**页面，并将属性 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* 设置为 1。

支持 Boolean 属性

Cisco ISE 支持从 Active Directory 和 LDAP 身份库中检索 Boolean 属性。

在配置 Active Directory 或 LDAP 的目录属性时，您可以配置 Boolean 属性。一旦使用 Active Directory 或 LDAP 进行身份验证，即可检索这些属性。

Boolean 属性可用于配置策略规则条件。

可从 Active Directory 或 LDAP 服务器抓取作为字符串类型的 Boolean 属性值。Cisco ISE支持以下 Boolean 属性值：

Boolean 属性	支持的值
真	t、T、true、TRUE、True、1
错误	f、F、false、FALSE、False、0

注释 Boolean 属性不支持属性替代。

如果您将 Boolean 属性（例如 msTSAllowLogon）配置为字符串类型，则 Active Directory 或 LDAP 服务器中该属性的 Boolean 值是为Cisco ISE 中字符串属性设置的。您可以将属性类型更改为 Boolean 或将该属性作为 Boolean 类型进行手动添加。

基于证书的身份验证的 Active Directory 证书检索

Cisco ISE 支持为使用 EAP-TLS 协议的用户和设备身份验证检索证书。Active Directory 上的用户或设备记录包括二进制数据类型的证书属性。此证书属性可以包含一个或多个证书。Cisco ISE 将此属性标识为 userCertificate，并且不允许为此属性配置任何其他名称。Cisco ISE 会检索此证书并将其用于执行二进制比较。

证书身份验证配置文件决定从哪个字段（例如 Subject Alternative Name (SAN) 或 Common Name 字段）获取用户名以在 Active Directory 中查找用于检索证书的用户。Cisco ISE 检索到证书后，会将此证书与客户端证书进行二进制比较。当接收到多个证书时，Cisco ISE 会对这些证书进行比较以确定相匹配的证书。找到匹配的证书后，则用户或设备身份验证通过。

Active Directory 用户身份验证流程

当对用户进行身份验证或查询时，Cisco ISE 会检查以下内容：

- MS-CHAP 和 PAP 身份验证会检查用户是否被禁用、锁定、过期或者登录超时，如果上述任一条件为真，则身份验证失败。
- EAP-TLS 身份验证会检查用户是否被禁用或锁定，如果满足上述任一条件，则身份验证失败。

配置资源所有者密码凭证流以使用 Azure Active Directory 对用户进行身份验证

注意 Cisco ISE 中的资源所有者密码凭证 (ROPC) 流是一种受控引入功能。我们建议您在生产环境中使用此功能之前，在测试环境中全面测试此功能。

资源所有者密码凭证 (ROPC) 是一种 OAuth 2.0 授予类型，允许Cisco ISE 使用基于云的身份提供程序在网络中执行授权和身份验证。

通过 ROPC 流，Cisco ISE 使用基于云的身份源验证用户的凭证。ROPC 流支持明文身份验证协议。Cisco ISE 目前通过 ROPC 流支持 Azure Active Directory。

在 Azure Active Directory 中为资源所有者密码凭证流配置应用

步骤 1 登录到 Azure 门户。

步骤 2 点击顶部导航栏中的**目录+应用 (Directory+Application)** 过滤器图标。选择必须向其添加支持 ROPC 的应用的 Azure Active Directory 租户。

步骤 3 使用搜索栏查找并选择**应用注册 (App Registrations)**。

步骤 4 点击 **+ 新注册 (+ New Registration)**。

步骤 5 在显示的**注册应用 (Register an Application)** 窗口中，在**名称 (Name)** 字段中为此应用输入有意义的名称。

步骤 6 在**支持的帐户类型 (Supported account types)** 区域中，点击**仅此组织目录中的帐户 (Accounts in this organizational directory only)**。

步骤 7 点击**注册**。

步骤 8 在显示的新窗口中，点击左侧菜单窗格中的**证书和密钥 (Certificates & Secrets)**。

步骤 9 在**客户端密钥 (Client Secrets)** 区域中，点击 **+ 新客户端密钥 (+ New Client Secret)**。

步骤 10 在显示的**添加客户端密钥 (Add a Client Secret)** 对话框中，在**说明 (Description)** 字段中输入说明。

步骤 11 在**到期 (Expiry)** 区域中，点击**从不 (Never)**。

步骤 12 点击**添加 (Add)**。

步骤 13 点击复制到剪贴板图标以复制共享密钥。在Cisco ISE 中配置 ROPC 流时，需要此值。

步骤 14 点击左侧菜单窗格中的**概述 (Overview)**，然后在配置 ROPC 流时复制以下值以在Cisco ISE 中使用。

- 应用（客户端）ID。
- 目录（租户）ID。

步骤 15 要为此应用启用 ROPC 流，请点击左侧菜单窗格中的**身份验证 (Authentication)**。在**高级设置 (Authentication)** 区域中，确保切换按钮设置为**是 (Yes)**。

步骤 16 要向应用添加组声明，请点击左侧菜单窗格中的**令牌配置 (Token Configuration)**。

步骤 17 点击 **+ 添加组声明 (+ Add Groups Claim)**。

步骤 18 在**编辑组声明 (Edit Groups Claim)** 对话框中，选中**安全组 (Security groups)** 复选框。

步骤 19 点击**保存 (Save)**。

步骤 20 要启用 API 的使用，请点击左侧菜单窗格中的 **API 权限 (API Permissions)**。

步骤 21 点击 **+ 添加权限 (+ Add A Permission)**。

步骤 22 在 **Microsoft API** 区域中，点击 **Microsoft Graph**。

步骤 23 点击**应用权限 (Application Permissions)**。

步骤 24 在**组 (Group)** 下拉区域中，选中 **Group.Read.All** 复选框。

步骤 25 点击**添加权限 (Add Permissions)**。

步骤 26 点击为 **<user>** 授予管理员同意，然后点击是 **(Yes)**。

在思科 ISE 中配置资源所有者密码凭证流

开始之前

在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后依次选择 **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **受信任证书 (Trusted Certificates)**。检查 **DigiCert Global Root G2** 是否显示在受信任证书列表中。

如果此证书在受信任证书存储区中不可用，请将 PEM 格式的公共根证书 DigiCert Global Root G2 导入Cisco ISE 受信任证书存储区。

请参阅 https://www.digicert.com/kb/digicert-root-certificates.htm。

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **REST ID 存储设置 (REST ID Store Settings)**。

步骤 2 点击**已启用 (Enabled)**，然后点击**提交 (Submit)**。

步骤 3 在 ISE 节点中通过以下 CLI 命令验证 REST 身份验证服务的状态：

```
show application status ise
```

如果响应中显示消息 **REST 身份验证服务正在运行 (REST Auth Service running)**，则表明已成功启用 REST ID 存储设置。现在可以继续配置 ROPC 流。

步骤 4 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **REST (ROPC)**。

步骤 5 点击**添加 (Add)**。

步骤 6 在显示的新窗口中，在**名称 (Name)** 字段中输入值。

步骤 7 从 **REST 身份提供程序 (REST Identity Provider)** 下拉列表中，选择要配置的身份源。

步骤 8 对于字段**客户端 ID (Client ID)**、**客户端密钥 (Client Secret)** 和**租户 ID (Tenant ID)**，通过在先前任务中配置 Azure Active Directory 时保存的信息输入所需值。

步骤 9 点击**测试连接 (Test Connection)** 以检查Cisco ISE 能否连接到所选身份源。

步骤 10 点击**加载组 (Load Groups)** 以从连接的身份源导入用户组。然后可以从**组 (Groups)** 下拉列表中选择特定组。

步骤 11 （可选）在**用户名后缀 (Username Suffix)** 字段中输入值，以按用户名对 Azure Active Directory 租户的用户进行身份验证。

例如，如果用户的 Azure Active Directory 用户专用名称 (UPN) 为 *example@myTest.onMicrosoft.com*，则后缀为分隔符，域名为 *@ myTest.onMicrosoft.com*。

步骤 12 点击**提交 (Submit)**。

支持 Active Directory 多域林

Cisco ISE 支持带多域林的 Active Directory。在每个林中，Cisco ISE 连接到单个域，但如果在Cisco ISE 连接到的域与其他域之间建立信任关系，则可从 Active Directory 林中的其他域访问资源。

请参阅Cisco身份服务引擎的版本说明，以获取支持 Active Directory 服务的 Windows 服务器操作系统列表。

注释 思科 ISE 不支持位于网络地址转换器背后并具有网络地址转换 (NAT) 地址的 Microsoft Active Directory 服务器。

Active Directory 与思科 ISE 集成的先决条件

本节介绍配置 Active Directory 以与Cisco ISE 集成所需的手动步骤。但是，在大多数情况下，可以启用Cisco ISE 来自动配置 Active Directory。以下是将 Active Directory 与Cisco ISE 集成的先决条件。

- 确保您拥有对 AD 域配置进行更改所需的 Active Directory 域管理员凭证。
- 确保您在Cisco ISE 中具有超级管理员或系统管理员权限。
- 使用网络时间协议 (NTP) 服务器设置来同步Cisco ISE 服务器和 Active Directory 之间的时间。您可以从Cisco ISE CLI 配置 NTP 设置。
- Cisco ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。如果要从特定加入点查询其他域，请确保加入点和其他具有需要访问的用户和计算机信息的域之间存在信任关系。如果信任关系不存在，您必须为不受信任的域创建另一个加入点。有关建立信任关系的详细信息，请参阅 Microsoft Active Directory 文档。
- 您必须在Cisco ISE 加入到的域中具有至少一个可由Cisco ISE 运行并访问的全局目录服务器。

执行各种操作所需的 Active Directory 帐户权限

加入操作	退出操作	Cisco ISE 机器账户
加入操作需要以下帐户权限： • 搜索 Active Directory（以查看Cisco ISE 机器账户是否存在） • 将Cisco ISE 机器账户创建到域（如果机器账户尚不存在） • 在新机器账户上设置属性（例如，Cisco ISE 机器账户密码、SPN、dnsHostname） 不必是域管理员即可执行加入操作。	退出操作需要以下帐户权限： • 搜索 Active Directory（以查看Cisco ISE 机器账户是否存在） • 从域中删除Cisco ISE 机器帐户 如果执行强制退出（在没有密码的情况下退出），则不会从域中删除计算机帐户。	用于传达到 Active Directory 连接的Cisco ISE 机器帐户需要以下权限： • 更改密码 • 读取与已身份验证的用户和机器对应的用户和机器对象。 • 查询 Active Directory 以获取信息（例如，受信任域和替代 UPN 后缀等） • 读取 tokenGroups 属性 可以在 Active Directory 中预创建机器帐户。如果 SAM 名称与 Cisco ISE 设备主机名匹配，则应在加入操作期间找到该名称并重复使用。 如果具有多个加入操作，则会在 Cisco ISE 中维护多个机器帐户，每个加入操作对应一个账户。

注释 用于加入或退出操作的凭证不存储在Cisco ISE 中。仅存储新创建的Cisco ISE 机器帐户凭证。

Microsoft Active Directory 中的**网络访问权限：限制允许远程调用 SAM 的客户端**安全策略已修改。因此，Cisco ISE 可能无法每 15 天更新一次其机器帐户密码。如果机器帐户密码未更新，Cisco ISE 不会再通过 Microsoft Active Directory 对用户进行身份验证。您将在Cisco ISE 控制板上收到 **AD: ISE 密码更新失败 (AD: ISE password update failed)** 警报，以通知您此事件。

安全策略可使用户枚举本地安全帐户管理器 (SAM) 数据库和 Microsoft Active Directory 中的用户和组。要确保Cisco ISE 可更新其机器帐户密码，请检查 Microsoft Active Directory 中的配置是否正确。有关受影响的 Windows 操作系统和 Windows Server 版本的详细信息，包括这对您的网络意味着什么、可能需要哪些更改，请参阅：

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

必须开放用于通信的网络端口

协议	端口（远程-本地）	目标	已通过身份验证	备注
DNS (TCP/UDP)	随机数大于或等于 49152	DNS 服务器/AD 域控制器	否	-
MSRPC	445	域控制器	支持	-
Kerberos (TCP/UDP)	88	域控制器	是 (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	支持	-
LDAP (GC)	3268	全局目录服务器	支持	-
NTP	123	NTP 服务器/域控制器	否	-
IPC	80	部署中的其他 ISE 节点	是（使用 RBAC 凭证）	-

DNS 服务器

在配置您的 DNS 服务器时，请确保注意以下事项：

- 您在Cisco ISE 中配置的 DNS 服务器必须能够解析要使用的域的所有正向和反向 DNS 查询。
- 建议使用权威 DNS 服务器来解析 Active Directory 记录，因为 DNS 递归可能会导致延迟并对性能造成重大不利影响。
- 所有 DNS 服务器都必须能够对 DC、GC 和 KDC（无论它们是否具有额外的站点信息）的 SRV 查询作出应答。
- Cisco建议向 SRV 响应添加服务器 IP 地址以提高性能。
- 避免使用查询公共互联网的DNS服务器。当必须解析未知名称时，这些服务器可能会泄漏有关网络的信息。

将 Active Directory 配置为外部身份源

在功能部件（例如 Easy Connect 和 被动 ID 工作中心）的配置过程中将 Active Directory 配置为外部身份源。有关这些功能部件的详细信息，请参阅 Easy Connect，第 510 页 和 被动 ID 工作中心，第 514 页。

在您将 Active Directory 配置为外部身份源之前，请确保：

- Microsoft Active Directory 服务器未驻留在网络地址转换器后，并且不具有网络地址转换 (NAT) 地址。

- 用于加入操作的 Microsoft Active Directory 帐户有效，且未配置为下次登录时修改密码。
- 您拥有 ISE 的超级管理员或系统管理员权限。

注释 如果在思科 ISE 连接到 Active Directory 时发现操作问题，请参阅**操作** > **报告** 下的“AD 连接器操作报告”(AD Connector Operations Report)。

您必须执行以下任务，从而将 Active Directory 配置配为外部身份源。

1. 添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点， 第 480 页
2. 配置身份验证域， 第 485 页
3. 配置 Active Directory 用户组， 第 486 页
4. 配置 Active Directory 用户和计算机属性， 第 487 页
5. （选件）修改密码更改、设备身份验证和设备访问限制设置， 第 487 页

添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点

开始之前

确保Cisco ISE 节点可以与NTP 服务器、DNS 服务器、域控制器和全局日志服务器所在的网络通信。您可以通过运行域诊断工具来检查这些参数。

必须创建加入点才能使用 Active Directory 以及使用被动 ID 工作中心的代理、系统日志、SPAN 和终端探测器。

在与 Active Directory 集成时，如果需要使用 IPv6，则必须确保已为相关 ISE 节点配置 IPv6 地址。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击**添加 (Add)** 并从 **Active Directory 加入点名称 (Active Directory Join Point Name)** 设置中输入域名和身份存储库名称。

步骤 3 点击**提交 (Submit)**。

此时将出现弹出窗口，询问您是否要将新创建的加入点加入到域中。如果要立即加入，请点击**是 (Yes)**。

如果已点击**否**，则保存配置将会全局保存 Active Directory 域配置（在主策略服务节点和辅助策略服务节点中），但不会将任何 ISE 节点加入到该域。

步骤 4 选中所创建的新 Active Directory 加入点旁边的复选框并点击**编辑 (Edit)**，或者从左侧的导航窗格中点击新的 Active Directory 加入点。系统将显示部署加入/退出表，其中包含所有Cisco ISE 节点、节点角色及其状态。

步骤 5 如果加入点没有在步骤 3 中加入域，请选中相关Cisco ISE 节点旁边的复选框，然后点击**加入 (Join)** 将Cisco ISE 节点加入到 Active Directory 域。

您必须明确地执行此操作，即使已保存配置。要通过单个操作将多个Cisco ISE 节点加入到域，所要使用的账户的用户名和密码必须对于所有加入操作都相同。如果需要不同的用户名和密码以加入每个Cisco ISE 节点，则应对每个Cisco ISE 节点分别执行加入操作。

步骤 6 在**加入域 (Join Domain)** 对话框中输入 Active Directory 用户名和密码。

强烈建议您选择**存储凭证 (Store credentials)**，在此情况下将会保存管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

用于加入操作的用户本身应存在于域中。如果该用户存在于其他域中或子域中，应使用 UPN 符号注解用户名，如 jdoe@acme.com。

步骤 7 （可选） 选中**指定组织单位 (Specify Organizational Unit)** 复选框。

如果Cisco ISE 节点机器帐户要位于除 CN=Computers,DC=someDomain,DC=someTLD 以外的特定组织单位中，应选中此复选框。Cisco ISE 会在指定的组织单位下创建机器账户，如果该机器账户已存在，则会将该账户移至此位置。如果未指定组织单位，Cisco ISE 将使用默认位置。应以完整可分辨名称 (DN) 格式指定值。语法必须符合 Microsoft 规范。特殊保留字符，例如 /'+,;=<> 换行符、空格和回车符，必须用反斜线 (\) 转义。例如，OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 和 Workstations,DC=someDomain,DC=someTLD。如果计算机帐户已经创建，则您不需要选中此复选框。加入 Active Directory 域之后，您还可以更改计算机帐户的位置。

步骤 8 点击**确定 (OK)**。

您可以选择多个要加入 Active Directory 域的节点。

如果加入操作不成功，则系统会显示失败消息。点击每个节点的失败消息可查看该节点的详细日志。

注释 加入完成后，Cisco ISE 将更新其 AD 组和对应的 SID。Cisco ISE 自动启动 SID 更新过程。您必须确保允许此过程完成。

注释 如果缺少 DNS SRV 记录，您可能无法将Cisco ISE 加入 Active Directory 域（域控制器不会对您尝试加入到的域公告其 SRV 记录）。有关故障排除信息，请参阅以下 Microsoft Active Directory 文档：

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

注释 在 ISE 上最多只能添加 200 个域控制器。如果超出此限制，您将收到错误“创建 <DC FQDN> 时出错 - DC 数超出允许的最大值 200”(Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200)。

下一步做什么

配置 Active Directory 用户组 ， 第 486 页

配置身份验证域。

添加域控制器

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **Active Directory**。

步骤 2 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有Cisco ISE 节点、节点角色及其状态。

步骤 3 **注释** 要为被动身份服务添加新的域控制器 (DC)，需要该 DC 的登录凭证。

转至 PassiveID 选项卡，然后点击**添加 DC (Add DCs)**。

步骤 4 选中要添加到加入点以进行监控的域控制器旁边的复选框，然后点击**确定 (OK)**。
域控制器显示在 PassiveID 选项卡的“域控制器”列表中。

步骤 5 配置域控制器：

a) 选中域控制器，然后点击**编辑 (Edit)**。系统将显示**编辑项目 (Edit Item)** 屏幕。

b) 或者，编辑不同的域控制器字段。有关详细信息，请参阅Active Directory 设置，第 519 页。

c) 如果选择 WMI 协议，请点击**配置 (Configure)**以自动配置 WMI，然后点击**测试 (Test)** 以测试连接。有关自动配置 WMI 的详细信息，请参阅对被动 ID 配置 WMI，第 484 页。

DC 故障转移机制根据 DC 优先级列表进行管理，该列表确定在故障转移情况下选择 DC 的顺序。如果 DC 由于错误而离线或无法访问，则其优先级在优先级列表中会降低。当 DC 恢复在线时，其优先级会在优先级列表中相应地进行调整（提高）。

注释 思科 ISE 不支持将只读域控制器用于身份验证流程。

用于被动 ID 的 MSRPC 协议

从Cisco ISE 版本 3.0 开始，可以将 MS-Eventing API 或 MSRPC（Microsoft 远程过程调用）协议用于被动身份。MSRPC 协议用于在Cisco ISE 中的节点之间建立节点通信并监控心跳。除 WMI 协议外，此选项也可用。

当Cisco ISE 或Cisco ISE-PIC 从多个域控制器收集或监控事件时，MSRPC 协议可提供一种可靠机制。它还可减少 Active Directory 域控制器用户登录事件的延迟。

对于Cisco ISE 3.0 及更高版本，MSRPC 是默认协议。建议您为 MSPRC 的高可用性功能启用主代理和辅助代理，以便在主代理安装的服务器发生故障时，辅助代理变为活动状态并监控域控制器。

也可以在创建代理时选择对 MSPRC 使用独立选项。但是，如果代理故障并且无法监控 DC 事件，辅助代理不会备份独立代理。

从Cisco ISE 2.x 升级到 3.0 版本时，如果使用现有代理更新成员服务器，则代理版本将在**代理 (Agents)** 窗口的**版本 (Version)** 列中显示 2.0.0.1。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **被动 ID (Passive ID)** > **提供程序 (Providers)** > **代理 (Agents)**。

为 MSRPC 部署代理

开始之前

启用被动身份服务。为此：

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，然后选中部署节点旁的复选框。点击**编辑 (Edit)**。在**编辑节点 (Edit Node)** 窗口中，选中**启用被动身份服务 (Enable Passive Identity Service)** 复选框并点击**保存 (Save)**。

在Cisco ISE-PIC GUI 中，选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，然后选中部署节点旁的复选框。点击**编辑 (Edit)**。在**编辑节点 (Edit Node)** 窗口中，选中**启用被动身份服务 (Enable Passive Identity Service)** 复选框并点击**保存 (Save)**。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **被动 ID (Passive ID)** > **提供程序 (Providers)** > **代理 (Agents)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**代理 (Agents)** 窗口中，如果要部署新代理，请点击**部署新代理 (Deploy New Agent)**，或者，如果要注册现有代理，请点击**注册现有代理 (Register Existing Agents)**。

如果选择**注册现有代理 (Register Existing Agent)** 选项，由于协议不受支持，因此可能会丢弃来自受支持注册客户端的请求。在这种情况下，需要使用支持的协议配置Cisco ISE 客户端。

步骤 4 在**名称 (Name)** 字段中输入名称。

步骤 5 在**主机 FQDN (Host FQDN)** 字段中输入主机 FQDN URL。

步骤 6 输入**用户名 (User Name)** 和**密码 (Password)**。

步骤 7 从**协议 (Protocol)** 下拉列表中选择 **MSRPC**。

步骤 8 点击**高可用性设置 (High Availability Settings)** 部分中的 **主 (Primary)**。

成功部署主代理后，应重复上述步骤，通过选择**高可用性设置 (High Availability Settings)** 部分中的**辅助 (Secondary)** 选项来部署辅助代理。在部署辅助代理时，应从**主代理 (Primary Agent)** 下拉列表中选择已配置的主代理。

步骤 9 点击 **Deploy**（部署）。

通过主代理映射域控制器

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **PassiveID** > **提供方 (Providers)** > **Active Directory**。

步骤 2 在 **Active Directory** 窗口中，点击**添加 (Add)**。

步骤 3 在**连接 (Connection)** 部分中，输入域控制器的**加入点名称 (Join Point Name)** 和 **Active Directory 域 (Active Directory Domain)**。

步骤 4 点击**提交 (Submit)**。

系统随即会显示以下消息：

是否要将所有 ISE 节点都加入到此 Active Directory 域？(Would you like to Join all ISE Nodes to this Active Directory Domain?)

步骤 5 点击**是 (Yes)** 以加入所有 ISE 节点。

步骤 6 在**加入域 (Join Domain)** 弹出窗口中，输入 **AD 用户名 (AD User name)** 和**密码 (Password)**。

步骤 7 点击**确定 (OK)**。

步骤 8 点击 **PassiveID** 选项卡。

步骤 9 在 **PassiveID 域控制器 (PassiveID Domain Controllers)** 窗口中，点击要映射的 ISE 域旁的复选框。

对于多个 DC 映射，可以通过**使用现有代理 (Use Existing Agent)** 选项选择现有代理。

步骤 10 点击**编辑 (Edit)**。

步骤 11 在**主机 FQDN (Host FQDN)** 字段中输入主机 FQDN URL。

步骤 12 在 **AD 用户名 (AD User Name)** 和**密码 (Password)** 字段中输入 AD 凭证。

步骤 13 从**协议 (Protocol)** 下拉列表中选择**代理 (Agent)**。

步骤 14 从**代理 (Agent)** 下拉列表中选择相应的代理（满足高可用性需求的**主要 (Primary)** 代理或**独立 (Standlone)** 代理）。

步骤 15 点击**保存 (Save)**。

在**控制板 (Dashboard)** 中可以查看代理映射状态、监控域控制器的代理以及代理角色。（ 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **PassiveID** > **概览 (Overview)**.）

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时会话 (Live Sessions)** 查看域控制器事件日志。

对被动 ID 配置 WMI

开始之前

确保您具有 Active Directory 域管理员凭证，这样才能对任何 AD 域配置进行更改。确保已在**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** 下对此节点启用被动 ID。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

图 ***14:***

步骤 2 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有Cisco ISE 节点、节点角色及其状态。有关详细信息，请参阅表 65: Active Directory 加入/退出窗口，第 520 页。

步骤 3 转至“被动 ID”选项卡，选中相关域控制器旁边的复选框，然后点击**配置 WMI** 以使 ISE 能够自动配置所选的域控制器。

要手动配置 Active Directory 和域控制器或对任何配置问题进行故障排除，请参阅Active Directory 与思科 ISE 集成的先决条件，第 477 页。

退出 Active Directory 域

如果不再需要从此 Active Directory 域或从此加入点对用户或机器进行身份验证，则可以退出 Active Directory 域。

从命令行界面重置Cisco ISE 应用配置或在备份或升级后恢复配置时，它将执行退出操作，从而将 Cisco ISE 节点与 Active Directory 域断开连接（如果已加入该节点）。但是，不会从 Active Directory 域中删除Cisco ISE 节点账户。我们建议您使用 Active Directory 凭证从 Admin 门户执行退出操作，因为这也会从 Active Directory 域删除节点帐户。在更改Cisco ISE 主机名时，也建议您如此操作。

开始之前

如果您退出 Active Directory 域，但是仍然使用 Active Directory 作为身份验证的身份源（直接使用或作为身份源序列的一部分），则身份验证会失败。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有Cisco ISE 节点、节点角色及其状态。

步骤 3 选中Cisco ISE 节点旁边的复选框，然后点击**退出 (Leave)**。

步骤 4 输入 Active Directory 用户名和密码，然后点击**确定 (OK)** 以退出该域并从Cisco ISE 数据库中删除机器账户。

如果输入 Active Directory 凭证，则Cisco ISE 节点将退出 Active Directory 域并从 Active Directory 数据库中删除Cisco ISE 机器账户。

注释 要从 Active Directory 数据库中删除思科 ISE 计算机帐户，此处提供的 Active Directory 凭证必须具有从域中删除计算机帐户的权限。

步骤 5 如果您没有 Active Directory 凭证，请选中**无可用凭证 (No Credentials Available)** 复选框，然后点击**确定 (OK)**。

如果选中**退出没有凭证的域 (Leave domain without credentials)** 复选框，则主Cisco ISE 节点将退出 Active Directory 域。Active Directory 管理员必须手动删除加入期间在 Active Directory 中创建的设备帐户。

配置身份验证域

对于与其有信任关系的其他域，Cisco ISE 加入的域具有可视性。默认情况下，Cisco ISE 设置为允许依据所有可信任域进行身份验证。可以将与 Active Directory 部署的交互限制到身份验证域子集。通过配置身份验证域，可以为每个加入点选择特定域，以便仅对选择的域执行身份验证。身份验证域可以提高安全性，因为这些域指示Cisco ISE 仅对来自所选域（而不是来自加入点信任的所有域）的用户进行身份验证。身份验证域还可改善性能以及身份验证请求处理延迟，因为身份验证域限制搜索区域（即，将搜索帐户与传入用户名或身份匹配的范围）。这在传入用户名或身份不包含域标记（前缀或后缀）时尤为重要。由于上述原因，配置身份验证域是最佳实践，我们强烈推荐此最佳实践。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

步骤 2 点击 Active Directory 加入点。

步骤 3 点击 Authentication Domains 选项卡。

系统会显示一个表，其中包含受信任域列表。默认情况下，Cisco ISE 允许对所有受信任域执行身份验证。

步骤 4 要仅允许指定域，请取消选中 Use all Active Directory domains for authentication 复选框。

步骤 5 选中想要允许对其执行身份验证的域旁边的复选框，并点击 Enable Selected。在身份验证 (Authenticate) 列中，此域的状态会更改为“是”(Yes)。

还可以禁用选定的域。

步骤 6 点击 Show Unusable Domains 以查看无法使用的域的列表。无法使用的域是Cisco ISE 由于单向信任、选择性身份验证等原因而无法用于身份验证的域。

下一步做什么

配置 Active Directory 用户组。

配置 Active Directory 用户组

您必须配置 Active Directory 用户组，使其可以用于授权策略中。在内部，Cisco ISE 使用安全标识符 (SID) 帮助解决组名称不明确问题和增强组映射。SID 提供准确的组分配匹配。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

步骤 2 点击 Groups 选项卡。

步骤 3 执行以下操作之一：

a) 选择 添加 (Add) > 从目录中选择组 (Select Groups From Directory) 以选择现有组。

b) 选择 添加 (Add) > 添加组 (Add Group)以手动添加组。您可以同时提供组名称和 SID，也可以仅提供组名称并按 Fetch SID。

对于用户界面登录，请勿在组名称中使用双引号 (”)。

步骤 4 如果您手动选择组，您可以使用过滤器进行搜索。例如，输入 admin* 作为搜索条件，然后点击 Retrieve Groups，即可查看以 admin 开头的用户组。您还可以输入星号 (*) 通配符过滤结果。一次只能检索 500 个组。

步骤 5 选中想要可用于授权策略的组旁边的复选框，然后点击确定 (OK)。

步骤 6 如果您选择手动添加组，请为新组输入名称和 SID。

步骤 7 点击确定 (OK)。

步骤 8 点击保存 (Save)。

注释　如果删除某个组，然后创建一个与此组相同名称的新组，则必须点击**更新 SID 值 (Update SID Values)** 以向新创建的组分配新 SID。升级之后，SID 会在首次联接之后自动更新。

下一步做什么

配置 Active Directory 用户属性。

配置 Active Directory 用户和计算机属性

必须配置 Active Directory 用户和计算机属性，以便在授权策略的条件中使用这些属性。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Attributes** 选项卡。

步骤 3 选择 **添加 (Add)** > **添加属性 (Add Attribute)** 以手动添加属性，或选择 **添加 (Add)** > **从目录中选择属性 (Select Attributes From Directory)** 以从目录中选择属性列表。

Cisco ISE 允许您在手动添加属性类型 IP 时使用 IPv4 或 IPv6 地址配置 AD 以进行用户身份验证。

步骤 4 如果选择从目录添加属性，请在**示例用户或机器账户**字段中输入用户的名称，然后点击**检索属性**以获取用户属性的列表。例如，输入 **administrator** 以获取管理员属性列表。您还可以输入星号 (*) 通配符过滤结果。

注释　当输入示例用户名时，确保从Cisco ISE 连接到的 Active Directory 域选择用户。当您选择示例计算机获得计算机属性时，请务必在计算机名称前面加上“host/”或使用SAM$格式。例如，可以使用host/myhost。检索属性时显示的示例值仅用于说明，不能存储。

步骤 5 选中想要选择的 Active Directory 的属性旁边的复选框，并且点击**确定 (OK)**。

步骤 6 如果选择手动添加属性，请输入新属性的名称。

步骤 7 点击**保存 (Save)**。

修改密码更改、设备身份验证和设备访问限制设置

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。有关详细信息，请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点，第 480 页。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选中相关Cisco ISE 节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**高级设置 (Advanced Settings)** 选项卡。

步骤 4 根据需要，修改 Password Change、Machine Authentication 和 Machine Access Restrictions (MAR) 设置。

步骤 5 选中**启用拨入检查 (Enable dial-in check)** 复选框以在身份验证或查询期间检查用户的拨入权限。如果拨入权限被拒绝，检查的结果可能导致身份验证被拒绝。

步骤 6 如果您希望在身份验证或查询期间服务器回拨用户，请选中**对拨入客户端启用回拨检查**复选框。服务器使用的 IP 地址或电话号码可以由主叫方或网络管理员来设置。检查结果返回到 RADIUS 响应上的设备。

步骤 7 如果您想要使用 Kerberos 进行纯文本身份验证，请选中 **Use Kerberos for Plain Text Authentications** 复选框。默认和推荐选项为 MS-RPC。

计算机访问限制 (MAR) 缓存

当手动停止应用服务时，Cisco ISE 会将 MAR 缓存内容、主叫站 ID 列表和相应的时间戳存储到其本地磁盘上的文件中。如果意外重新启动应用服务，则Cisco ISE 不会存储实例的 MAR 缓存条目。重新启动应用服务时，Cisco ISE 会根据缓存条目有效时间从其本地磁盘上的文件中读取 MAR 缓存条目。当应用服务在重新启动后出现时，Cisco ISE 会将该实例的当前时间与 MAR 缓存条目时间进行比较。如果当前时间与 MAR 条目时间之间的差大于 MAR 缓存条目有效时间，则Cisco ISE 不会从磁盘中检索该条目。否则，Cisco ISE 将检索该 MAR 缓存条目并更新其 MAR 缓存条目有效时间。

要配置 MAR 缓存

在外部身份源中定义的 Active Directory 的**高级设置 (Advanced Settings)** 选项卡上，验证是否选中了以下选项：

- **启用计算机身份验证 (Enable Machine Authentication)**：启用计算机身份验证。
- **启用计算机访问限制 (Enable Machine Access Restriction)**：在授权之前结合用户和计算机身份验证。

在授权中使用 MAR 缓存

在授权策略中使用 `WasMachineAuthenticated is True`。您可以使用此规则和凭证规则执行双重身份验证。计算机身份验证必须在 AD 凭证之前完成。

如果在**系统 (System) > 部署 (Deployment)** 页面上创建了节点组，请启用 MAR 缓存分布。MAR 缓存分布会将 MAR 缓存复制到同一节点组中的所有 PSN。

有关详细信息，请参阅

请参阅以下Cisco ISE 社区页面：

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

相关主题

将 Active Directory 配置为外部身份源 ， 第 479 页

配置自定义架构

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选择加入点。

步骤 3 点击 **Advanced Settings** 选项卡。

步骤 4 在**架构 (Schema)** 部分下，选择**架构 (Schema)** 下拉列表中的**定制 (Custom)** 选项。您可以根据需要更新用户信息属性。这些属性用于收集用户信息，例如名字、姓氏、电子邮件、电话、地点等。

预定义的属性用于 Active Directory 架构（内置架构）。如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。

对 Active Directory 多加入配置的支持

Cisco ISE 支持对 Active Directory 域执行多加入。Cisco ISE 最多支持 50 个 Active Directory 加入。Cisco ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。Active Directory 多域加入包括一组不同的 Active Directory 域，每个加入均有其自己的组、属性和授权策略。

您可以多次联接同一个域林，也即是说，如有必要，您可以在同一个域林中联接不止一个域。

Cisco ISE 现在允许联接具有单向信任的域。此选项有助于绕过单向信任导致的权限问题。您可以联接以下任一受信任域，因此能够看见这两个域。

- 加入点 - 在Cisco ISE 中，每个到 Active Directory 域的独立加入都叫作一个加入点。Active Directory 加入点是Cisco ISE 身份库，可用于身份验证策略。它有用于属性和组的关联字典，这些属性和组可用于授权条件。
- 范围 - 一部分 Active Directory 加入点组合到一起就叫做范围。您可以在身份验证策略中使用范围代替单个加入点并用作身份验证结果。范围用于按照多个加入点对用户进行身份验证。如果您使用范围，就无需为每个加入点设置多个规则，可以创建只有单个策略的相同策略，节约了 Cisco ISE 用于处理请求的时间并且有助于提高性能。一个加入点可以用于多个范围中。范围可以包含在身份源序列中。因为范围不具有任何关联字典，所以您无法将范围用于授权策略条件中。

  当您执行Cisco ISE 全新安装时，默认情况下并无范围。这称为无范围模式。当您添加范围时，Cisco ISE 进入多范围模式。如果需要，您可以返回无范围模式。所有加入点将移至 Active Directory 文件夹。

  - Initial_Scope 是用于存储在无范围模式中添加的 Active Directory 加入点的隐式范围。当启用多范围模式时，所有 Active Directory 加入点将移至自动创建的 Initial_Scope。您可以重命名 Initial_Scope。

- All_AD_Instances 是在 Active Directory 配置中不显示的一个内置伪范围。它只在策略和身份序列中作为身份验证结果显示。如果您要选择Cisco ISE 中配置的所有 Active Directory 加入点，就可以选择此范围。

创建新范围，添加 **Active Directory** 加入点

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Scope Mode**。
默认情况下，系统创建名为 Initial_Scope 的范围，当前所有加入点都放在此范围中。

步骤 3 要创建更多范围，请点击 **Add**。

步骤 4 输入新范围的名称和说明。

步骤 5 点击**提交 (Submit)**。

身份重写

身份重写是一种定向Cisco ISE 的高级功能，使其在传递至外部 Active Directory 系统之前处理其身份。您可以创建规则以将身份改为包含或排除域前缀和/或后缀或您所选择的其他附加标记的相应格式。

身份重写规则应用于传递至 Active Directory 之前从客户端接收的用于使用者搜索、身份验证和授权查询等操作的用户名或主机名。Cisco ISE 将匹配条件标记，在发现第一个匹配项时，Cisco ISE 停止处理策略并根据结果重写身份字符串。

在重写期间，以方括号"[]"括起来的所有内容（例如 [IDENTITY]）是变量，在评估端不会对其进行评估，但会添加与字符串中该位置匹配的字符串。没有方括号的所有内容在规则的评估端和重写端都会评估为固定字符串。

以下是身份重写的一些示例，假设用户输入的身份是 ACME\jdoe：

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。

  结果是 jdoe。此规则指示Cisco ISE 删掉所有用户名的 ACME 前缀。

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@ACME.com**。

  结果是 jdoe@ACME.com。此规则指示Cisco ISE 将格式从前缀更改为后缀表示法，或从 NetBIOS 格式更改为 UPN 格式。

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **ACME2\[IDENTITY]**。

  结果是 ACME2\jdoe。此规则指示Cisco ISE 将具有特定前缀的所有用户名更改为使用备用前缀。

- 如果身份与 **[ACME]\jdoe.USA** 匹配，则重写为 **[IDENTITY]@[ACME].com**。

结果是jdoe\ACME.com。此规则指示Cisco ISE删掉点后面的领域（在本例中是国家/地区），替换为正确的领域。

- 如果身份与 **E=[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。

  结果是jdoe。如果身份来自证书，字段是邮件地址，而且Active Directory配置为按使用者搜索，则可以创建此示例规则。此规则指示Cisco ISE 删除“E=”。

- 如果身份与 **E=[EMAIL],[DN]** 匹配，则重写为 **[DN]**。

  此规则会将证书使用者从E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com转变为纯DN, CN=jdoe, DC=acme, DC=com。如果身份取自证书使用者，且Active Directory配置为按DN搜索用户，则可以创建此示例规则。此规则指示Cisco ISE 删掉邮件前缀并生成DN。

以下是编写身份重写规则的一些常见错误：

- 如果身份与 **[DOMAIN]\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@DOMAIN.com**。

  结果是 jdoe@DOMAIN.com。此规则在规则的重写端没有用方括号 [] 括起来的 [DOMAIN]。

- 如果身份与 **DOMAIN\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@[DOMAIN].com**。

  同样，结果是jdoe@DOMAIN.com。此规则在规则的评估端没有用方括号[]括起来的[DOMAIN]。

身份重写规则始终应用在 Active Directory 加入点的情景中。即使由于身份验证策略而选择了范围，重写规则也适用于每个Active Directory加入点。如果使用的是EAP-TLS，这些重写规则还适用于取自证书的身份。

启用身份重写

注释 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Advanced Settings** 选项卡。

步骤 3 在 **Identity Rewrite** 部分下，选择是否要应用重写规则来修改用户名。

步骤 4 输入匹配条件和重写结果。您可以删除出现的默认规则并根据要求输入规则。Cisco ISE 按顺序处理规则，并会应用与请求用户名相匹配的第一个条件。您可以使用匹配令牌（方括号中包含的文本）将原始用户名的元素传输到结果。如果无任何规则匹配，则身份名称保持不变。您可以点击 **Launch Test** 按钮预览重写处理。

身份解析设置

某些身份类型包括域标记，如前缀或后缀。例如，在如 ACME\jdoe 这样的 NetBIOS 身份中，“ACME”是域标记前缀，同样在如jdoe@acme.com这样的UPN身份中，“acme.com”是域标记后缀。域前缀应该与组织中 Active Directory 域的 NetBIOS (NTLM) 名称匹配，域后缀应该与组织中 Active Directory 域的 DNS 名称或备选 UPN 后缀匹配。例如，jdoe@gmail.com 会视为没有域标记，因为 gmail.com 不是 Active Directory 域的 DNS 名称。

身份解析设置允许您配置重要设置来调整安全和性能的平衡，以符合您的 Active Directory 部署。您可以使用这些设置来调整没有域标记的用户名和主机名的身份验证。在Cisco ISE 不知道用户域的情况下，可以将其配置为在所有身份验证域中搜索用户。即使在一个域中找到了用户，Cisco ISE 仍将等待所有响应以确保不存在模糊身份。这可能需要较长时间，具体取决于域的数量、网络中的延迟、负载等。

避免身份解析问题

强烈建议在身份验证期间，使用完全限定的用户和主机名称（即，带有域标记的名称）。例如，用户使用 UPN 和 NetBIOS 名称，主机使用 FQDN SPN 名称。这在您频繁遇到模糊错误的情况下尤其重要，例如，多个 Active Directory 帐户匹配传入用户名；例如，jdoe m 匹配 jdoe@emea.acme.com 和 jdoe@amer.acme.com。在某些情况下，使用完全限定名称是解决问题的唯一方法。在其他情况下，保证用户拥有唯一密码即可。因此，如果最初使用唯一身份，则更加高效，而且可以减少密码锁定问题。

配置身份解析设置

注释 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

开始之前

您必须将Cisco ISE 加入到 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Advanced Settings** 选项卡。

步骤 3 在 **Identity Resolution**（身份解析）部分下，对用户名或计算机名称的身份解析定义以下设置。此设置可提供用于用户搜索和身份验证的高级控制。

第一个设置适用于没有标记的身份。在这种情况下，可以选择以下任一选项：

- **拒绝请求 (Reject the request)**：此选项将导致没有任何域标记的用户（例如 SAM 名称）的身份验证失败。如果有多个加入域，而Cisco ISE 必须在所有加入的全局目录中查找身份（这可能不太安全），则此选项非常有用。此选项强制用户使用具有域标记的名称。

- **仅搜索加入的林中的“身份验证域”(Only search in the “Authentication Domains” from the joined forest)**：此选项只在加入点所在林的域（这些域在身份验证域部分中指定）中搜索身份。对于SAM帐户名称，这是默认选项，并且与Cisco ISE 1.2 的行为相同。
- **搜索所有“身份验证域”部分 (Search in all the “Authentication Domains” sections)**：此选项在所有受信任林的所有身份验证域中搜索身份。这可能会增加延迟并影响性能。

根据身份验证域在Cisco ISE 中的配置方式来选择选项。如果只选择特定身份验证域，将只搜索这些域（无论是选择“加入的林”还是“所有林”）。

如果Cisco ISE 无法与它所需的所有全局目录 (GC) 通信，则使用第二个设置，以符合在“Authentication Domains”部分中指定的配置。在这种情况下，可以选择以下任一选项：

- **继续使用可用域 (Proceed with available domains)**：如果在任一可用的域中找到匹配项，此选项将继续执行身份验证。
- **丢弃请求 (Drop the request)**：如果身份解析遇到某些无法访问或不可用的域，此选项将删除身份验证请求。

就 Active Directory 测试用户 (Test Users for Active Directory)身份验证

“测试用户”工具可用于从 Active Directory 验证用户身份验证。您还可以获取组和属性并对其进行检查。您可以对单个加入点或对范围运行测试。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选择以下选项之一：

- 要在所有加入点上运行测试，请选择 **高级工具 (Advanced Tools)** > **就所有加入点测试用户 (Test User for All Join Points)**。
- 要对特定加入点运行测试，请选择该加入点并点击**编辑 (Edit)**。选择Cisco ISE 节点并点击**测试用户**。

步骤 3 在 Active Directory 中输入用户（或主机）的用户名和密码。

步骤 4 选择身份验证类型。如果选择查找 (Lookup) 选项，则无需步骤 3 中的密码输入。

步骤 5 如果您是对所有加入点运行此测试，请选择要对其运行此测试的Cisco ISE 节点。

步骤 6 如果要从 Active Directory 检索组和属性，请选中“检索组”(Retrieve Groups) 和“检索属性”(Retrieve Attributes) 复选框。

步骤 7 点击 **Test**。

系统将显示测试操作的结果和步骤。这些步骤可帮助确定故障原因并进行故障排除。

您还可以查看 Active Directory 执行每个处理步骤（用于身份验证、查找或获取组/属性）所需的时间（以毫秒为单位）。如果操作所需的时间超过阈值，Cisco ISE 将显示警告消息。

删除 Active Directory 配置

如果您不会使用 Active Directory 作为外部身份源，则应删除 Active Directory 配置。如果您希望加入其他 Active Directory 域，则请勿删除该配置。您可以退出当前所加入的域并加入新的域。

开始之前

确保您已退出 Active Directory 域。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 选中已配置的 Active Directory 旁边的复选框。

步骤 3 检查并确保列出的本地节点状态为未加入。

步骤 4 点击 **Delete**。

您已从 Active Directory 数据库中移除该配置。如果希望以后再使用 Active Directory，您可以重新提交有效的 Active Directory 配置。

查看节点的 Active Directory 加入

您可以使用 **Active Directory** 页面上的**节点视图**按钮查看给定Cisco ISE 节点的所有 Active Directory 加入点的状态或所有Cisco ISE 节点上的所有加入点列表。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击 **Node View**。

步骤 3 从 **ISE Node** 下拉列表中选择节点。
表格按节点列出 Active Directory 的状态。如果部署中有多个加入点和多个Cisco ISE 节点，则更新此表可能需要几分钟时间。

步骤 4 点击加入点 **Name** 链接以转至该 Active Directory 加入点页面，然后执行其他特定操作。

步骤 5 点击**诊断摘要**列中的链接以转至**诊断工具**页面来对特定问题进行故障排除。诊断工具显示每个节点的每个加入点的最新诊断结果。

诊断 Active Directory 问题

诊断工具是在每个Cisco ISE 节点上运行的服务。当Cisco ISE 使用 Active Directory 时，通过该工具可自动测试和诊断 Active Directory 部署并执行一组测试，以检测可能导致功能或性能故障的问题。

Cisco ISE 无法加入 Active Directory 或对其进行身份验证有多个原因。此工具帮助确保正确配置用于将Cisco ISE 连接到 Active Directory 的先决条件。该工具有助于检测网络、防火墙配置、时钟同步、用户身份验证等问题。此工具以逐步操作指南的形式工作，并帮助您根据需要解决中间每层的问题。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。

步骤 2 点击**高级工具 (Advanced Tools)** 下拉列表，选择**诊断工具 (Diagnostic Tools)**。

步骤 3 选择要运行诊断的Cisco ISE 节点。

如果未选择Cisco ISE 节点，则在所有节点上运行测试。

步骤 4 选择特定的 Active Directory 加入点。

如果不选择 Active Directory 加入点，则在所有加入点上运行测试。

步骤 5 您可以按需或按计划运行诊断测试。

- 要立即运行测试，请选择**立即运行测试 (Run Tests Now)**。
- 要按计划间隔运行测试，请选中**运行计划测试 (Run Scheduled Tests)** 复选框并指定必须运行测试的开始时间和间隔（以小时、天或周为单位）。启用此选项后，将在所有节点和实例上运行所有诊断测试，并在**主页**控制面板上的**警报** dashlet 中报告故障。

步骤 6 点击 **View Test Details** 查看具有警告或失败状态的测试的详细信息。
下表允许您重新运行特定测试、停止正在运行的测试和查看特定测试的报告。

启用 Active Directory 调试日志

默认情况下，不会记录 Active Directory 调试日志。必须在您的部署中承担策略服务角色的思科 ISE 节点上启用此选项。启用 Active Directory 调试日志可能会影响 ISE 性能。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **调试日志配置 (Debug Log Configuration)**。

步骤 2 点击要从中获取 Active Directory 调试信息的Cisco ISE 策略服务节点旁边的单选按钮，然后点击**编辑 (Edit)**。

步骤 3 点击 **Active Directory** 单选按钮，然后点击**编辑 (Edit)**。

步骤 4 从 Active Directory 旁的下拉列表中选择 **DEBUG**。这将包括错误、警告和 verbose 日志。要获得完整日志，请选择 **TRACE**。

步骤 5 点击**保存 (Save)**。

获取 Active Directory 日志文件来进行故障排除

下载并查看 Active Directory 调试日志，对您可能遇到的问题进行故障排除。

开始之前

必须启用 Active Directory 调试日志记录。

步骤 1 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)**。

步骤 2 点击您要从其获得 Active Directory 调试日志文件的节点。

步骤 3 点击 **Debug Logs** 选项卡。

步骤 4 向下滚动此页面找到 ad_agent.log 文件。点击该文件并下载该文件。

Active Directory 警报和报告

Cisco ISE 提供多种警报和报告，用于对 Active Directory 相关活动进行监控和故障排除。

警报

Active Directory 错误和故障会触发以下警报：

- 配置的名称服务器不可用
- 所加入的域不可用
- 身份验证域不可用
- Active Directory 林不可用
- AD 连接器必须重新启动
- AD：ISE 帐户密码更新失败
- AD：计算机 TGT 刷新失败

报告

您可以通过以下两种报告监控 Active Directory 相关活动：

- RADIUS Authentications Report - 此报告显示 Active Directory 身份验证和授权的详细步骤。您可以在此处查找该报告： **操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **RADIUS 身份验证 (RADIUS Authentications)**。
- AD Connector Operations Report - AD 连接器操作报告提供 AD 连接器所执行后台操作的日志，例如Cisco ISE 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理。如果遇到 Active Directory 失败，您可以查看此报告的详细信息以确定可能的原因。您可以在此处查找该报告： **操作 (Operations)** > **报告 (Reports)** > **诊断 (Diagnostics)** > **AD 连接器操作 (AD Connector Operations)**。

Active Directory 高级调整

高级调整功能提供节点特定的设置，用于在Cisco支持人员指导下的支持操作，更深入地调整系统中的参数。这些设置不适用于正常管理流程，只应在指导下使用。

Active Directory 身份搜索属性

Cisco ISE 使用 SAM、CN 或这两者来识别用户。Cisco ISE 版本 2.2 补丁 5 及更高版本，版本 2.3 补丁 2 及更高版本，将 sAMAccountName 属性用作默认属性。在早期版本中，默认搜索 SAM 和 CN 属性。此行为已在版本 2.2 补丁 5 及更高版本，以及版本 2.3 补丁 2 及更高版本中发生更改，是 CSCvf21978 漏洞修复的组成部分。在这些版本中，仅 sAMAccountName 属性用作默认属性。

如果环境需要，您可以配置Cisco ISE 以使用 SAM、CN 或者这两者。使用 SAM 和 CN 时，SAMAccountName 属性的值不唯一，Cisco ISE 还将比较 CN 属性值。

注释 默认情况下，身份搜索行为已在Cisco ISE 2.4 中更改为仅搜索 SAM 帐户名称。要修改此默认行为，请按照“配置 Active Directory 身份搜索的属性”部分所述更改“IdentityLookupField”标志的值。

配置 Active Directory 身份搜索的属性

1. 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。在 **Active Directory** 窗口中，点击**高级工具 (Advanced Tools)**，然后选择**高级调整 (Advanced Tuning)**。输入下列详细信息：
   - **ISE Node** - 选择连接 Active Directory 的 ISE 节点。
   - **Name** - 输入您正更改的注册表项。要更改 Active Directory 搜索属性，请输入：`REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
   - **Value** - 输入 ISE 用于识别用户的属性：
     - *SAM* - 在查询中仅使用 SAM（此选项为默认选项）。
     - *CN* - 在查询中仅使用 CN。
     - *SAMCN* - 在查询中使用 CN 和 SAM。
   - **Comment** - 说明您正在更改的内容，例如：将默认行为更改为 SAM 和 CN
2. 点击**更新值 (Update Value)** 以更新注册表。

   系统将显示一个弹出窗口。阅读消息并接受更改。ISE 中的 AD 连接器服务重新启动。

搜索字符串示例

在以下示例中，假设用户名为 *userd2only*：

- SAM 搜索字符串—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM 和 CN 搜索字符串—

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

使用 Active Directory 设置思科 ISE 的补充信息

要使用 Active Directory 配置Cisco ISE，必须配置组策略，并配置请求方以对计算机进行身份验证。

在 Active Directory 中配置组策略

有关如何访问组策略管理编辑器的详细信息，请参阅 Microsoft Active Directory 文档。

步骤 1 打开组策略管理编辑器，如下图所示。

239641

组策略对象选择

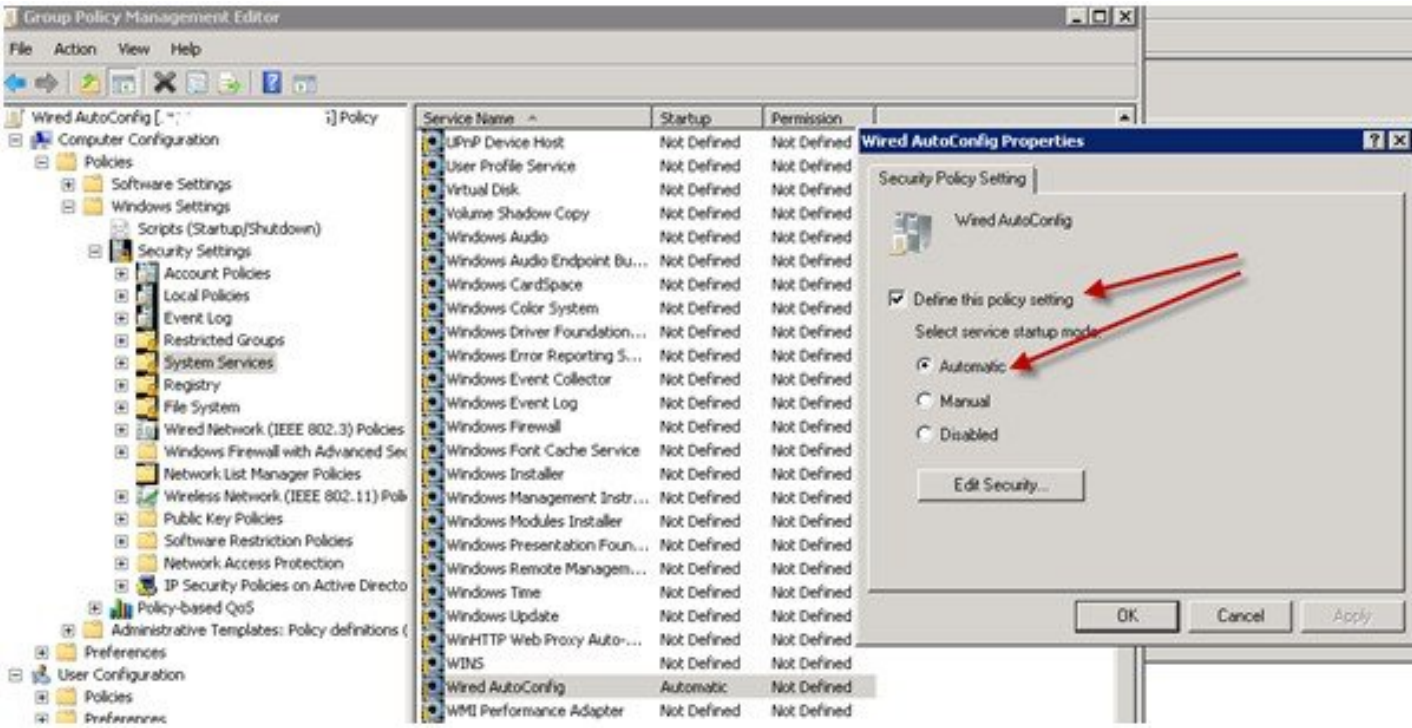
步骤 2 创建新策略并为其输入描述性名称，或者将其添加到现有域策略。

示例：

在以下示例中，使用 Wired Autoconfiguration 作为策略名称。

步骤 3 选中 **Define this policy setting** 复选框，然后针对服务启动模式点击 **Automatic** 单选按钮，如下图所示。

策略属性



步骤 4 在所需的组织单元或域 Active Directory 级别应用策略。

配置 Odyssey 5.X 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证

如果使用 Odyssey 5.x 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证，则必须在请求方进行以下配置。

步骤 1 启动 Odyssey 访问客户端。

步骤 2 从 Tools 菜单选择 **Odyssey Access Client Administrator**。

步骤 3 双击 **Machine Account** 图标。

步骤 4 从**计算机帐户 (Machine Account)** 窗口，必须配置 EAP-TLS 身份验证配置文件：

a) 选择 **配置 (Configuration)** > **配置文件 (Profiles)**。

b) 为 EAP-TLS 配置文件输入名称。

c) 在“身份验证”(Authentication) 选项卡上，选择 **EAP-TLS** 作为身份验证方法。

d) 在“证书”(Certificate) 选项卡上，选中**允许使用我的证书登录 (Permit login using my certificate)** 复选框，然后为请求方计算机选择证书。

e) 在**用户信息 (User Info)** 选项卡上，选中**使用计算机凭证 (Use machine credentials)** 复选框。

如果启用此选项，Odyssey 请求方将以 host\<*machine_name*> 格式发送计算机名称，Active Directory 识别来自计算机的请求，并且查找要执行身份验证的计算机对象。如果禁用此选项，Odyssey 请求方将发送不带 host\ 前缀的计算机名称，Active Directory 将查找用户对象，身份验证失败。

用于计算机身份验证的 AnyConnect 代理

当您为计算机身份验证配置 AnyConnect 代理时，可以执行下列操作之一：

- 使用默认的计算机主机名，包括前缀“host/”。
- 配置新的配置文件，在这种情况下必须包括前缀“host/”，然后是计算机名称。

支持 Easy Connect 和 被动身份服务 的 Active Directory 要求

Easy Connect 和 被动身份服务 使用 Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。必须正确配置 Active Directory 服务器，才能使 ISE 用户能够连接和获取用户登录信息。以下各部分说明如何配置 Active Directory 域控制器（Active Directory 端的配置）以支持 Easy Connect 和 被动身份服务。

要配置 Active Directory 域控制器（Active Directory 端的配置）以支持 Easy Connect 和被动身份服务，请按照以下步骤操作：

注释 必须配置所有域中的所有域控制器。

1. 从 ISE 设置 Active Directory 加入点和域控制器。请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点，第 480 页 和 添加域控制器，第 482 页。
2. 根据域控制器配置 WMI。请参阅对被动 ID 配置 WMI，第 484 页。
3. 从 Active Directory 执行以下步骤：
   - 配置 Active Directory 以服务 被动身份服务，第 501 页
   - 设置 Windows 审核策略，第 503 页
4. （可选）使用以下步骤在 Active Directory 上对 ISE 执行的自动配置进行故障排除：
   - 为域管理员组中的 Microsoft Active Directory 用户设置权限，第 504 页
   - 不在域管理员组中的 Microsoft Active Directory 用户的权限，第 504 页
   - 在域控制器上使用 DCOM 的权限，第 506 页
   - 设置访问 WMI Root/CIMv2 名称空间的权限，第 507 页
   - 授权访问 AD 域控制器上的安全事件日志，第 508 页

配置 Active Directory 以服务 被动身份服务

ISE Easy Connect 和 被动身份服务 使用 Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。ISE 连接到 Active Directory 并获取用户登录信息。

应从 Active Directory 域控制器执行以下步骤：

步骤 1 确保相关 Microsoft 补丁安装在 Active Directory 域控制器上。

a) 需要以下 Windows Server 2008 补丁：

- http://support.microsoft.com/kb/958124

  此补丁可修复 Microsoft WMI 中的内存泄漏，这会阻止 ISE 与域控制器建立成功连接。

- http://support.microsoft.com/kb/973995

  此补丁修复 Microsoft 的 WMI 中的不同的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录事件写入至域控制器的安全日志。

b) Windows Server 2008 R2 需要以下补丁（除非安装 SP1）：

- http://support.microsoft.com/kb/981314

  此补丁修复 Microsoft 的 WMI 中的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录活动事件写入至域控制器的安全日志。

- http://support.microsoft.com/kb/2617858

  此补丁修复 Windows Server 2008 R2 中的启动或登录过程意外缓慢。

c) 需要以下链接中列出的 Windows 平台 WMI 相关问题补丁：

- http://support.microsoft.com/kb/2591403

这些热修复与 WMI 服务及其相关组件的操作和功能相关。

步骤 2 确保 Active Directory 在 Windows 安全日志中记录用户登录事件。

验证“审核策略”(Audit Policy) 设置（“组策略管理” [Group Policy Management] 设置的一部分）支持成功登录在 Windows 安全日志中生成必要事件（这是 Windows 默认设置，但是，您必须明确保证此设置正确）。

步骤 3 您必须拥有具备足够权限的 Active Directory 用户才能将 ISE 连接到 Active Directory。以下说明显示如何为管理域组用户或无管理域组用户定义权限：

- Active Directory 用户为域管理员组成员时需要的权限
- Active Directory 用户不是域管理员组成员时需要的权限

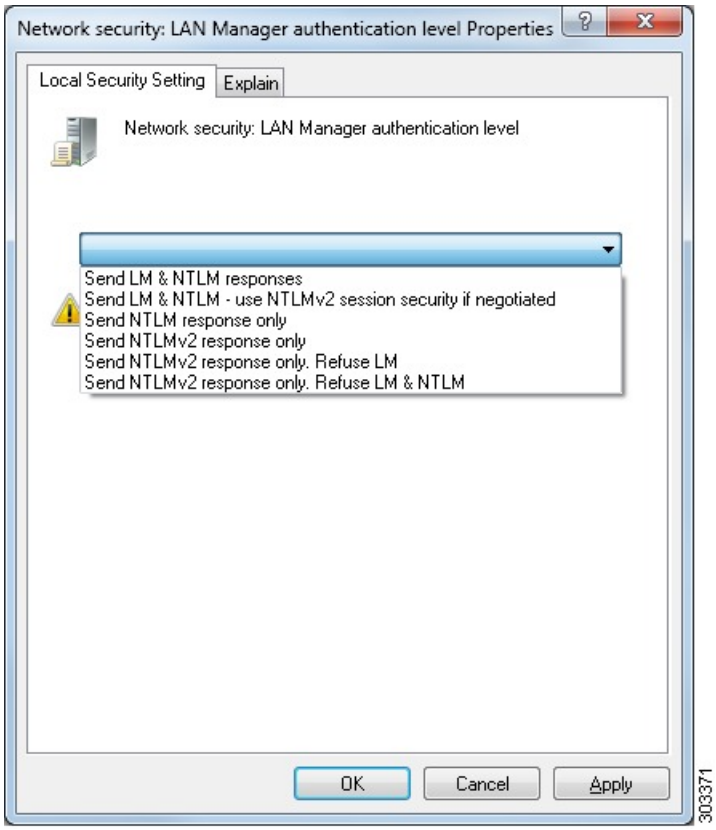
步骤 4 ISE 使用的 Active Directory 用户可以通过 NT LAN Manager (NTLM) v1 或 v2 进行身份验证。您需要验证 Active Directory NTLM 设置是否与 ISE NTLM 设置一致，以确保 ISE 和 Active Directory 域控制器之间的连接成功进行身

份验证。下表显示所有 Microsoft NTLM 选项及支持哪些 ISE NTLM 操作。如果 ISE 设置为 NTLMv2，则支持所述的全部六个选项。如果 ISE 设置为支持 NTLMv1，则仅支持前五个选项。

表 *63:* 基于 *ISE* 和 *AD NTLM* 版本设置的受支持身份验证类型

ISE NTLM 设置选项/Active Directory (AD) NTLM 设置选项 NTLMv1 NTLMv2	NTLMv1	NTLMv2
发送 LM & NTLM 响应	允许连接	允许连接
发送 LM & NTLM - 如果有协商，使用 NTLMv2 会话安全	允许连接	允许连接
仅发送 NTLM 响应	允许连接	允许连接
仅发送 NTLMv2 响应	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM & NTLM	拒绝连接	允许连接

图 *15: MS NTLM* 身份验证类型选项



步骤 5 确保您已创建一个防火墙规则允许流量去往 Active Directory 域控制器中的 `dllhost.exe`。

您可以关闭防火墙，或者允许在特定 IP（ISE IP 地址）访问以下端口：

- TCP 135：通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端为此请求服务的组件使用哪个端口。
- UDP 137：Netbios 名称解析
- UDP 138：Netbios 数据报服务
- TCP 139：Netbios 会话服务
- TCP 445：SMB

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 %SystemRoot%\System32\dllhost.exe 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP (ISE IP)。

设置 Windows 审核策略

确保**审核策略 (Audit Policy)**（**组策略管理 (Group Policy Management)** 设置的一部分）支持成功登录。此为在 AD 域控制器机器的 Windows 安全日志中生成必要事件所需要的。这是 Windows 默认设置，但是，您必须验证此设置的正确性。

步骤 1 选择 **开始 (Start)** > **程序 (Programs)** > **管理工具 (Administrative Tools)** > **组策略管理 (Group Policy Management)**。

步骤 2 在域 (Domain) 下导航至相关的域，并展开导航树。

步骤 3 依次选择**默认域控制器策略 (Default Domain Controller Policy)**，右键点击并选择**编辑 (Edit)**。

组策略管理编辑器 (Group Policy Management Editor) 出现。

步骤 4 选择 **默认域控制器策略 (Default Domain Controllers Policy)** > **计算机配置 (Computer Configuration)** > **策略 (Policies)** > **Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)**。

- 对于 Windows Server 2003 或 Windows Server 2008（非 R2），依次选择 **本地策略 (Local Policies)** > **审核策略 (Audit Policy)**。对于这两个策略项目（**审核帐户登录事件 [Audit Account Logon Events]** 和**审核日志事件 [Audit Logon Events]**），请确保相应的**策略设置 (Policy Setting)** 直接或间接包含**成功 (Success)** 条件。要间接包含成功 (Success) 条件，**策略设置 (Policy Setting)** 必须设置为**未定义 (Not Defined)**，表示有效值将从较高级别的域沿用，并且该高级别域的**策略设置 (Policy Setting)** 必须配置为明确包含**成功 (Success)** 条件。
- 对于 Windows Server 2008 R2 和 Windows 2012，请选择 **高级审核策略配置 (Advanced Audit Policy Configuration)** > **审核策略 (Audit Policies)** > **帐户登录 (Account Logon)**。对于这两个策略项目（**审核 Kerberos 身份验证服务 [Audit Kerberos Authentication Service]** 和**审核 Kerberos 服务申请单操作 [Audit Kerberos Service Ticket Operations]**），请确保相应的“策略设置”(Policy Setting) 直接或间接包括成功 (Success) 如上所述的成功条件。

注释 Cisco ISE 在与 Active Directory 通信时使用 Kerberos 协议中的 RC4 密码（除非在 Active Directory 域控制器配置中禁用此加密类型）。可以使用 Active Directory 中的**网络安全: 配置 Kerberos 允许的加密类型 (Network Security: Configure Encryption Types Allowed for Kerberos)** 选项来配置 Kerberos 协议允许的加密类型。

步骤 5 如果更改了任何“审核策略”(Audit Policy) 项目设置，那么您应运行 `gpupdate /force` 强制新设置生效。

为域管理员组中的 Microsoft Active Directory 用户设置权限

默认情况下，对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，域管理员组对 Windows 操作系统中的某些注册表项没有完全控制权限。Microsoft Active Directory 管理员必须给予 Microsoft Active Directory 用户对以下注册表项的完全控制权限：

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

以下 Microsoft Active Directory 版本不需要对注册表进行更改：

- Windows 2003
- Windows 2003R2
- Windows 2008

要授予完全控制权限，Microsoft Active Directory 管理员必须首先获得注册表项的所有权：

步骤 1 右键点击注册表项图标，然后选择**所有者 (Owner)** 选项卡。

步骤 2 点击 **Permissions**（权限）。

步骤 3 点击 **Advanced**。

不在域管理员组中的 Microsoft Active Directory 用户的权限

对于 Windows Server 2012 R2，授予 Microsoft AD 用户对以下注册表项的完全控制权限：

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

在 Windows PowerShell 中使用以下命令来检查是否提供了对注册表项的完整权限：

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
  ```

- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

当 Microsoft AD 用户不在域管理员组，但在域用户组中时，还需要以下权限：

- 添加注册表项以允许思科 ISE 连接到域控制器。
- 在域控制器上使用 DCOM 的权限，第 506 页
- 设置访问 WMI Root/CIMv2 名称空间的权限，第 507 页

只有以下 Active Directory 版本要求具有这些权限：

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

添加注册表项以允许思科 ISE 连接到域控制器

必须手动将一些注册表项添加到域控制器，以允许思科 ISE 以域用户身份进行连接，并检索登录身份验证事件。域控制器或该域中的任何其他机器都不需要代理。

以下注册脚本显示了要添加的密钥。您可以将其复制并粘贴到一个文本文件，并另存为扩展名为 .reg 的文件，然后双击该文件进行注册更改。要添加注册密钥，用户必须是根秘钥的所有者。

```
Windows 注册表编辑器版本 5.00 [HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
 "AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"="
 "
```

确保DllSurrogate注册表项的值包含两个空格。如果手动更新注册表，必须仅包含两个空格，不包含引号。手动更新注册表时，请确保 AppID、DllSurrogate 及其值中不包含引号。

如前一脚本所示，保留所有空行，包括文件末尾的空行。

在 Windows 命令提示符下使用以下命令，以确认注册表项是否已创建并包含正确值：

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

在域控制器上使用 DCOM 的权限

用于思科 ISE 被动身份服务的 Microsoft Active Directory 用户必须具有在域控制器服务器上使用 DCOM 的权限。通过 **dcomcnfg** 命令行工具配置权限。

步骤 1 从命令行运行 **dcomcnfg** 工具。

步骤 2 扩展组件服务 **(Component Services)**。

步骤 3 扩展 **计算机 (Computers)** > **我的计算机 (My Computer)**。

步骤 4 从菜单栏中选择**操作 (Action)**，点击**属性 (Properties)**，然后点击 **COM 安全性 (COM Security)**。

步骤 5 Cisco ISE 用于访问和启动的帐户必须具有允许权限。将 Microsoft Active Directory 用户添加至所有四个选项（**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)** 的**编辑限制设置 (Edit Limits)** 和**编辑默认设置 (Edit Default)**）。

步骤 6 对于**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)**，允许所有本地和远程访问。

图 ***16:*** 访问权限的本地和远程访问

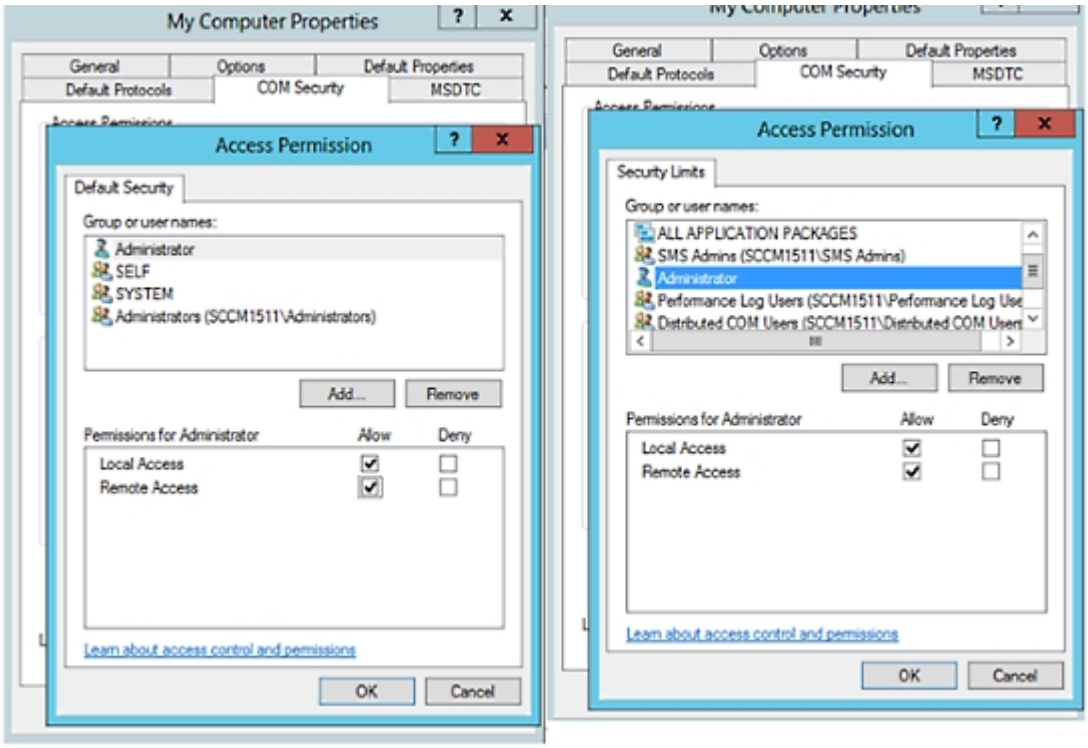
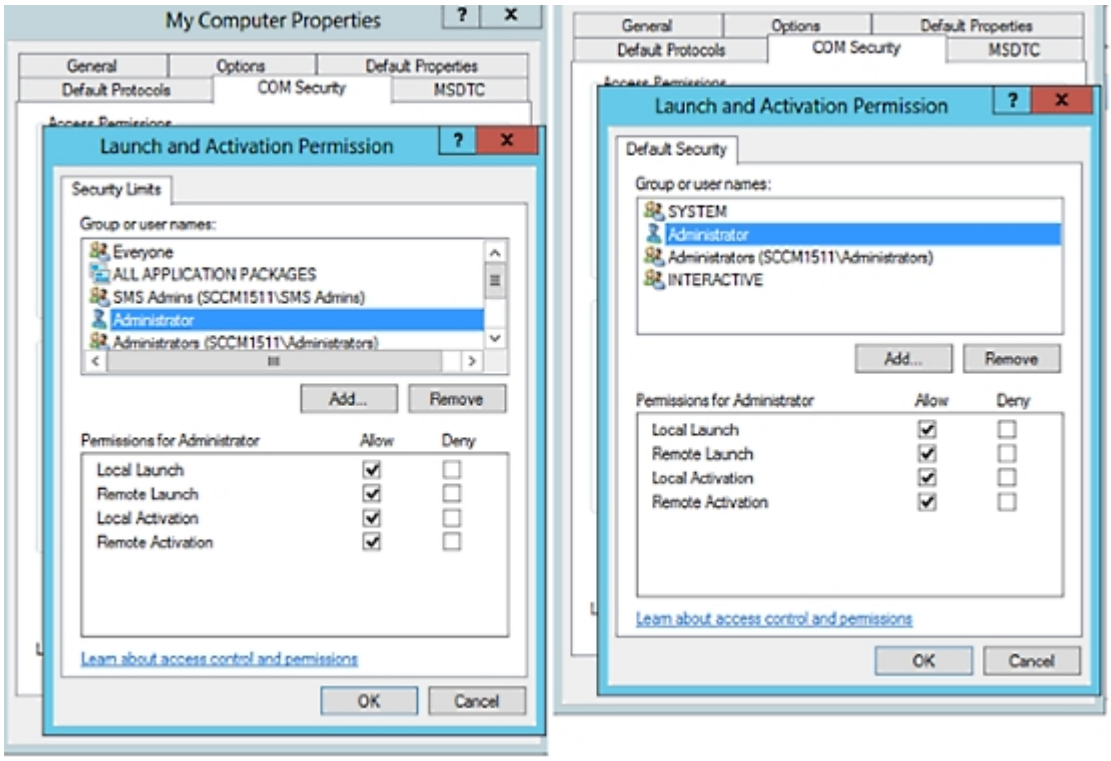


图 *17:* 启动以及激活权限的本地和远程访问



设置访问 WMI Root/CIMv2 名称空间的权限

默认情况下，Microsoft Active Directory 用户没有对“执行方法”(Execute Methods) 和“远程启用”(Remote Enable) 的权限。您可以使用 wmimgmt.msc MMC 控制台授予访问权限。

步骤 1 选择 **开始 (Start)** > **运行 (Run)** 并键入 `wmimgmt.msc`。

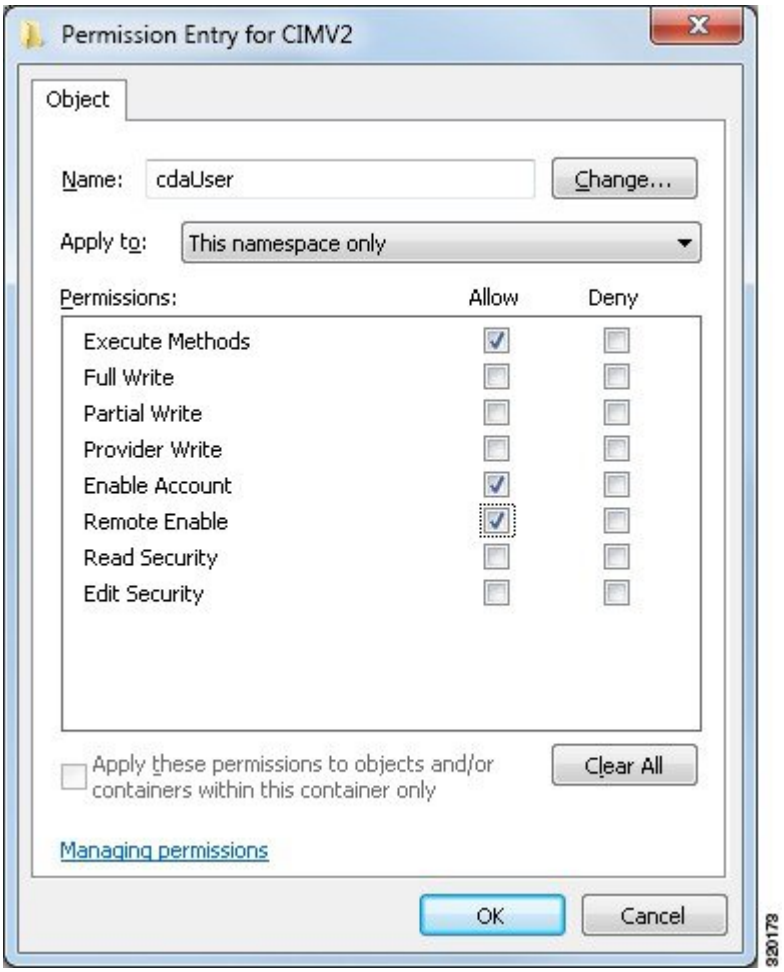
步骤 2 右键点击 **WMI 控制 (WMI Control)** 并点击**属性 (Properties)**。

步骤 3 在**安全 (Security)** 选项卡下，展开**根 (Root)** 并选择 **CIMV2**。

步骤 4 点击 **Security**。

步骤 5 添加 Active Directory 用户，并按如下所示配置所需的权限。

图 *18: WMI Root\CIMv2* 名称空间所需的权限



授权访问 AD 域控制器上的安全事件日志

在 Windows 2008 及更高版本上，您可以通过将 ISE ID 映射用户添加到名为“事件日志读取器”的组中来授予对 AD 域控制器日志的访问权限。

在 Windows 所有旧版本上，您必须编辑一个注册表项，如下所示。

步骤 1 要委托访问至安全事件日志，请查找该帐户的 SID。

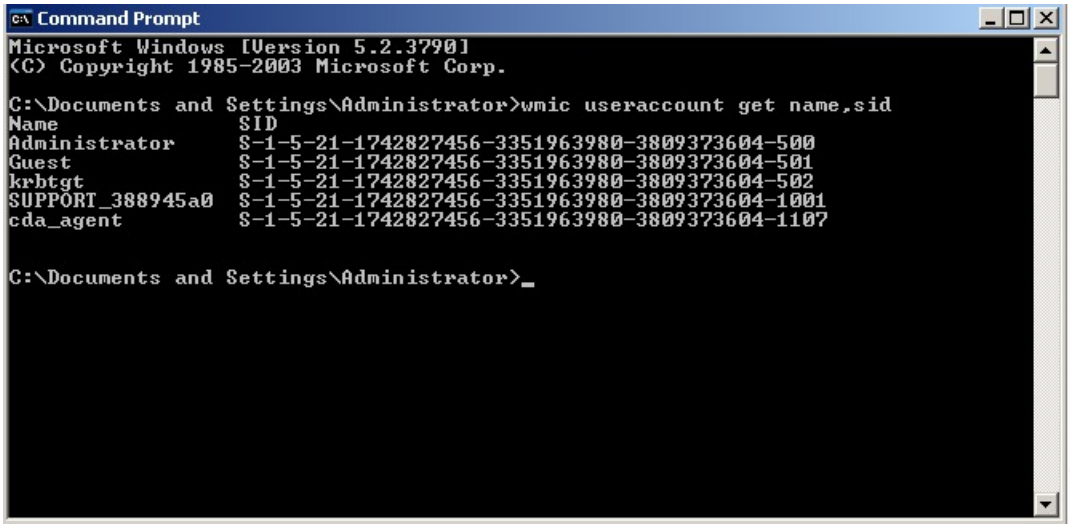
步骤 2 在命令行处使用以下命令，列出所有 SID 帐户，也如下图所示。

```
wmic useraccount get name,sid
```

您可以使用用于特定用户名和域的以下命令：

```
wmic useraccount where name=“iseUser” get domain,name,sid
```

图 *19:* 列出所有 *SID* 帐户



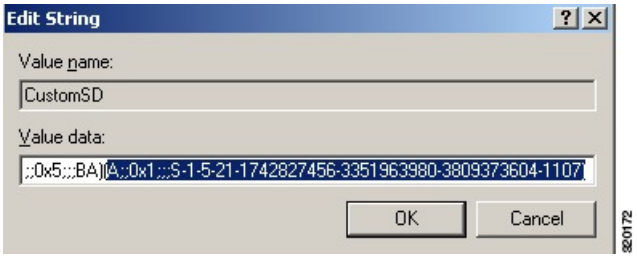
步骤 3 查找 SID，打开“注册表编辑器”(Registry Editor)，并对以下位置进行浏览：

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

步骤 4 点击**安全 (Security)** 和双击 **CustomSD**。

例如，要允许读访问 ise_agent 账户 `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`，请输入 `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`。

图 *20:* 编辑 *CustomSD* 字符串



步骤 5 重启域控制器上的 WMI 服务。您可以通过以下两种方式重启 WMI 服务：

a) 在 CLI 处运行以下命令：

net stop winmgmt

net start winmgmt

b) 运行 `Services.msc`，打开 Windows 服务管理工具。在 Windows 服务管理窗口中，找到 **Windows 管理规范 (Windows Management Instrumentation)** 服务，右键点击，然后选择**重启 (Restart)**。

Easy Connect

使用 Easy Connect，您可以轻松地以安全方式将用户从有线终端连接到网络，并通过 Active Directory 域控制器（而不是通过Cisco ISE）对这些用户进行身份验证，从而监控他们。通过 Easy Connect，Cisco ISE 可以从 Active Directory 域控制器收集用户身份验证信息。Easy Connect 使用 MS WMI 接口连接至 Windows 系统 (Active Directory) 并从 Windows 事件消息查询日志，因此它当前仅支持安装了 Windows 的终端。Easy Connect 使用 MAB 支持有线连接，这与 802.1X 相比更易于配置。与 802.1X 不同的是，使用 Easy Connect 和 MAB：

- 您无需配置请求方
- 您无需配置 PKI
- ISE 会在外部服务器 (AD) 对用户进行身份验证后发出 CoA

Easy Connect 支持以下操作模式：

- 实施模式：ISE 主动将授权策略下载到网络设备，以基于用户凭证进行实施。
- 可视性模式：Cisco ISE 发布从 NAD 设备传感器接收的会话合并和帐户信息，以便将该信息发送至 pxGrid。

在这两种情况下，通过 Active Directory (AD) 进行身份验证的用户会显示在Cisco ISE 实时会话视图中，而且可以使用Cisco pxGrid 接口由第三方应用从会话目录进行查询。已知信息为用户名、IP 地址、AD DC 主机名以及 AD DC NetBios 名称。有关 pxGrid 的详细信息，请参阅思科 pxGrid 节点，第 70 页。

设置 Easy Connect 后，即可根据用户的名称或 IP 地址过滤特定用户。例如，如果 IT 服务中的管理员登录到终端以帮助该终端的常规用户，则可以过滤掉管理员活动，从而在“实时会话”中不显示管理员活动，而是仅显示该终端的常规用户。要过滤被动身份服务，请参阅过滤被动身份服务，第 555 页。

Easy Connect 限制

- MAC 身份验证绕行 (MAB) 支持 Easy Connect。MAB 和 802.1X 可以在同一端口上进行配置，但您必须为每个服务设置不同的 ISE 策略。
- 当前仅支持 MAB 连接。您无需唯一身份验证策略来进行连接，因为将根据授权策略中定义的 Easy Connect 条件来授权连接及授予权限。
- 在高可用性模式下支持 Easy Connect。可以定义多个节点，并使用被动 ID 来启用它们。然后，ISE 会自动激活一个 PSN，而其他节点将保持备用状态。
- 仅支持 Cisco Network Access Devices (NAD)。
- 不支持 IPv6。
- 当前不支持无线连接。

- 系统仅跟踪 Kerberos 身份验证事件，因此 Easy Connect 仅启用用户身份验证，不支持机器身份验证。

Easy Connect 需要 ISE 中的配置，而 Active Directory 域服务器还必须根据 Microsoft 发布的说明和准则进行正确的补丁安装和配置。有关为Cisco ISE 配置 Active Directory 域控制器的信息，请参阅 支持 Easy Connect 和 被动身份服务 的 Active Directory 要求，第 500 页

Easy Connect 实施模式

Easy Connect 允许用户从有线终端（通常为 PC）使用 Windows 操作系统通过以下方式登录到安全网络：使用 MAC 地址绕行 (MAB) 协议并访问 Active Directory (AD) 以进行身份验证。Easy Connect 从 Active Directory 服务器侦听 Windows Management Instrumentation (WMI) 事件，以获取有关已通过身份验证的用户的信息。AD对用户进行身份验证后，域控制器将生成一份事件日志，此日志中包含用户名和为此用户分配的IP地址。Cisco ISE从AD接收登录通知，然后发出RADIUS授权更改(CoA)。

注释 如果将 Radius 服务类型设置为 call-check，则不会对 MAB 请求执行 MAC 地址查找。因此，将针对请求返回 access-accept。这是默认配置。

Easy Connect 实施模式流程

Easy Connect 实施模式流程如下所示：

1. 用户从有线终端（如 PC）连接到 NAD。
2. NAD（为 MAB 所配置）将访问请求发送至Cisco ISE。ISE 根据用户配置使用访问权限进行响应，以允许用户访问 AD。配置必须至少允许访问 DNS、DHCP 和 AD。
3. 用户登录到域，系统将一份安全审核事件发送至Cisco ISE。
4. ISE从RADIUS收集MAC地址以及IP地址和域名，并从安全审核事件收集用户的帐户信息（登录信息）。
5. 将所有数据收集并合并到会话目录中后，Cisco ISE向NAD发出CoA（根据在策略服务节点中管理的相应策略），NAD 根据此策略为用户提供对网络的访问权限。

图 *21: Easy Connect* 实施模式基本流程

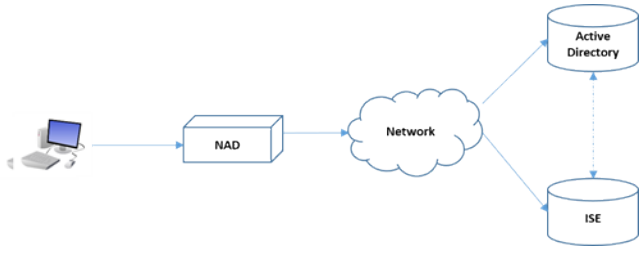
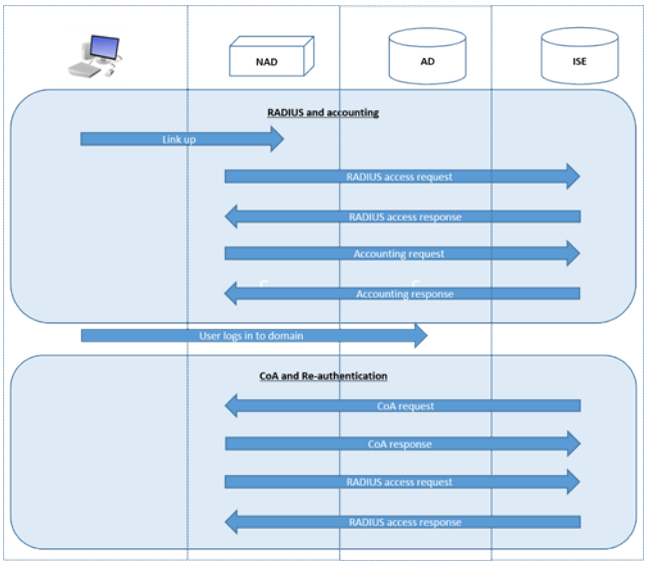


图 *22: Easy Connect* 实施模式详细流程

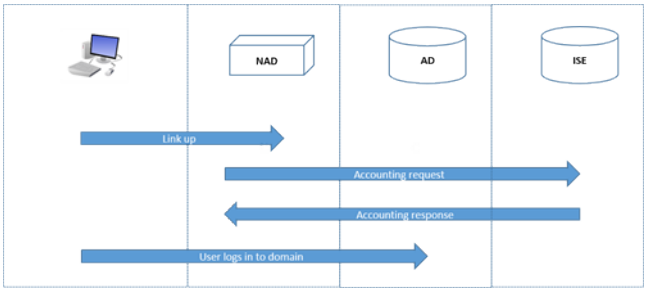


有关配置实施模式的详细信息，请参阅配置 Easy Connect 实施模式，第 512 页。

Easy Connect 可见性模式

对于可视性模式，Cisco ISE 仅从 RADIUS 监控帐户信息（NAD 中设备传感器功能的一部分）且不执行授权。Easy Connect 侦听 RADIUS 帐户和 WMI 事件，并将该信息发布到日志和报告（或者发布到 pxGrid）。设置 pxGrid 时，系统会使用 Active Directory 将用户登录期间的 RADIUS 帐户开始和会话终止信息同时发布到 pxGrid。

图 *23: Easy Connect* 可见性模式流程



有关配置 Easy Connect 可视性模式的详细信息，请参阅配置 Easy Connect 可视性模式，第 513 页。

配置 Easy Connect 实施模式

开始之前

- 为了获得最佳性能，请部署专用的 PSN 来接收 WMI 事件。
- 为接收 AD 登录事件的 WMI 节点创建 Active Directory 域控制器列表。

- 确定Cisco ISE 必须加入的 Microsoft 域以从 Active Directory 中提取用户组。
- 确定在授权策略中用于参考的 Active Directory 组。
- 如果您使用 pxGrid 与其他支持 pxGrid 的系统共享来自网络设备的会话数据，则需要在您的部署中定义 pxGrid 角色。有关 pxGrid 的详细信息，请参阅 思科 pxGrid 节点，第 70 页
- 在 MAB 成功之后，NAD 必须提供一个具有限访问权限的配置文件，该配置文件允许该端口的用户访问 Active Directory 服务器（如概述中所述）。

注释 被动身份服务可在多个节点上启用，但是，Easy Connect 一次只能在一个节点上运行。如果您在多个节点上启用该服务，ISE 会自动确定使用哪个节点用于活动的 Easy Connect 会话。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开一个节点，然后在**常规设置 (General Settings)** 之下，启用**启用被动身份服务 (Enable Passive Identity Service)**。

步骤 2 配置要由 Easy Connect 使用的 Active Directory 加入点和域控制器。有关详细信息，请参阅支持 Easy Connect 和 被动身份服务 的 Active Directory 要求，第 500 页。

步骤 3 （可选）选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory**。点击**组 (Groups)** 选项卡，然后添加您计划在授权策略中使用的 Active Directory 组。
为域控制器映射的 Active Directory 组会在 PassiveID 字典中动态更新，然后可以在您设置策略条件规则时使用。

步骤 4 **注释** 为了便于 Easy Connect 进程正常运行以及使 ISE 能够发出 CoA，必须为所有用于 Easy Connect 授权的配置文件启用**被动身份跟踪 (Passive Identity Tracking)**。

选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。对于所有 Easy Connect 要使用的配置文件，请打开配置文件并启用**被动身份跟踪 (Passive Identify Tracking)** 选项。

步骤 5 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **授权 (Authorization)** > **简单条件 (Simple Conditions)**，为 Easy Connect 创建规则。点击**添加 (Add)** 并定义条件：

a) 输入名称和说明。
b) 从**属性 (Attribute)** 选项，转至 PassiveID 字典并选择 PassiveID_Groups 为域控制器组创建条件或选择 PassiveID_user 为单个用户创建条件。
c) 输入正确的操作。
d) 输入策略中需包含的用户名或组名。

步骤 6 点击**提交 (Submit)**。

配置 Easy Connect 可视性模式

开始之前

- 为了获得最佳性能，请部署专用的 PSN 来接收 WMI 事件。

- 为接收 AD 登录事件的 WMI 节点创建 Active Directory 域控制器列表。
- 确定Cisco ISE 必须加入的 Microsoft 域以从 Active Directory 中提取用户组。
- 如果您使用 pxGrid 与其他支持 pxGrid 的系统共享来自网络设备的会话数据，则需要在您的部署中定义 pxGrid 角色。有关 pxGrid 的详细信息，请参阅 思科 pxGrid 节点，第 70 页

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开一个节点，然后在**常规设置 (General Settings)** 之下，启用**启用被动身份服务 (Enable Passive Identity Service)**。

步骤 2 配置要由 Easy Connect 使用的 Active Directory 加入点和域控制器。有关详细信息，请参阅支持 Easy Connect 和 被动身份服务 的 Active Directory 要求，第 500 页。

被动 ID 工作中心

被动身份连接器(被动ID工作中心)提供集中的一站式安装和实施，使您能够轻松简单地配置网络，以便接收用户身份信息并与各种不同的安全产品用户（例如Cisco Firepower 管理中心 [FMC] 和 Stealthwatch）进行共享。作为用于被动识别的全面代理，被动 ID 工作中心 从不同提供程序源（例如 Active Directory 域控制器 [AD DC]）收集用户身份，将用户登录信息映射到使用中的相关 IP 地址，然后将该映射信息与已配置的任何用户安全产品进行共享。

什么是被动身份？

由思科身份服务引擎 (ISE) 提供的标准流程，用于提供身份验证、授权和记账 (AAA) 服务器，并利用 802.1X 或 Web 身份验证之类的技术，直接与用户或终端进行通信，从而请求访问网络，然后使用其登录凭证来确认其身份并主动进行身份验证。

被动身份服务不直接对用户进行身份验证，而是从 Active Directory 之类的外部身份验证服务器（称为提供程序）收集用户身份和 IP 地址，然后与用户共享该信息。被动 ID 工作中心首先从提供程序接收用户身份信息（通常根据用户登录名和密码），然后执行必要的检查和服务，以便将用户身份与相关 IP 地址进行匹配，从而向用户传送经过身份验证的 IP 地址。

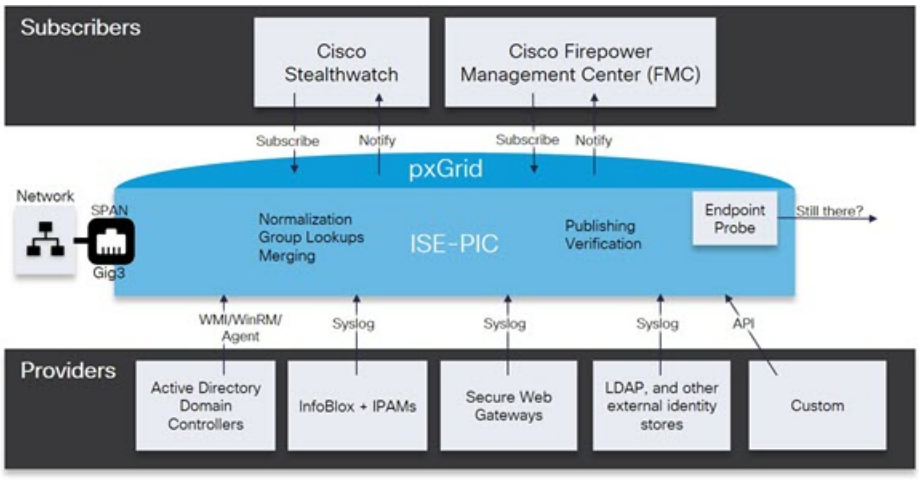
Passive Identity Connector (被动 ID 工作中心) 流程

被动 ID 工作中心 的流程如下：

1. 提供程序对用户或终端执行身份验证。
2. 提供程序将经过身份验证的用户信息发送到Cisco ISE。
3. 思科 ISE 将用户信息规范化，执行查找、合并、解析并将其映射到 IP 地址，然后将映射的详细信息发布到 pxGrid。
4. pxGrid 用户接收映射的用户详细信息。

下图说明了思科 ISE 提供的概要流程。

图 *24:* 概要流程



初始设置和配置

要快速开始使用Cisco 被动 ID 工作中心，请遵循以下流程：

1. 确保您已正确配置 DNS 服务器，包括从Cisco ISE 配置客户端机器的反向查找。有关详细信息，请参阅DNS 服务器，第 479 页。
2. 在您打算用于任何被动身份服务的专用策略服务器 (PSN) 上启用被动身份和 pxGrid 服务。选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开相关节点，并在**常规设置 (General Settings)** 下启用**开启被动身份服务 (Enable Passive Identity Service)** 和 **pxGrid**。
3. 同步 NTP 服务器的时钟设置。
4. 使用 ISE 被动身份设置来配置初始提供程序。有关详细信息，请参阅PassiveID 设置入门，第 517 页
5. 配置单个或多个用户。有关详细信息，请参阅用户，第 558 页

设置初始提供程序和用户后，可以轻松创建其他提供程序（请参阅其他被动身份服务提供程序，第 522 页）并从 被动 ID 工作中心：

- RADIUS实时会话 (Live Sessions)，第 282 页
- 思科 ISE 警报，第 1215 页

被动 ID 工作中心 控制板 (Dashboard)

Cisco被动 ID 工作中心 控制板显示对于有效监控和故障排除很重要的综合性相关摘要和统计数据，并实时更新。Dashlet 显示过去 24 小时的活动，另有说明的情况除外。要访问控制板，请依次选择 **工作中心 (Work Centers)** > **被动 ID (PassiveID)**，然后从左侧面板中选择**控制板 (Dashboard)**。只能在主管理节点 (PAN) 上查看Cisco 被动 ID 工作中心 控制板。

- **主要 (Main)** 视图具有线性指标控制板、饼形图 Dashlet 和列表 Dashlet。在 被动 ID 工作中心 中，Dashlet 不可配置。可用 Dashlet 包括：
  - **被动身份指标 (Passive Identity Metrics)** - 显示当前跟踪的唯一实时会话总数、系统中配置的身份提供程序总数、主动提供身份数据的代理总数，以及当前配置的用户总数。
  - **提供程序** - 提供程序向 被动 ID 工作中心 提供用户身份信息。可以配置 ISE 探测器（从给定源收集数据的机制），并通过此探测器从提供程序源接收信息。例如，Active Directory (AD) 探测器和代理探测器均可帮助 ISE-PIC 从 AD 收集数据（每个采用不同的技术），而系统日志探测器可从读取系统日志消息的解析器收集数据。
  - **用户 (Subscribers)** - 用户连接至 ISE 以解锁用户身份信息。
  - **操作系统类型 (OS Types)** - 可以显示的唯一操作系统类型为 Windows。Windows 类型按 Windows 版本显示。提供程序不报告操作系统类型，但 ISE 可查询 Active Directory 以获取此信息。Dashlet 中最多显示 1000 个条目。
  - **警报 (Alarms)** - 用户身份相关警报。

Active Directory 作为探测器和提供程序

Active Directory (AD) 是一种高度安全且精确的源，可以从中接收用户身份信息，包括用户名、IP 地址和域名。

AD 探测器 (被动身份服务) 通过 WMI 技术从 AD 收集用户身份信息，而其他探测器则通过其他技术和方法将 AD 用作用户身份提供程序。有关 ISE 提供的其他探测器和提供程序类型的详细信息，请参阅其他被动身份服务 提供程序，第 522 页。

通过配置 Active Directory 探测器，您还可以快速配置并启用以下其他探测器（它们也使用 Active Directory 作为源）：

- Active Directory 代理，第 524 页

  注释 仅 Windows Server 2008 及更高版本上支持 Active Directory 代理。

- SPAN，第 533 页
- 终端探测器，第 555 页

此外，配置 Active Directory 探测器，以便在收集用户信息时使用 AD 用户组。您可以对 AD、代理、SPAN 和系统日志探测使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组，第 486 页。

设置 Active Directory (WMI) 探测

要为被动身份服务配置 Active Directory 和 WMI，可以使用被动 ID 工作中心向导（请参阅PassiveID 设置入门 ，第 517 页），也可以遵循如下步骤：

1. 配置 Active Directory 探测器。请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点 ，第 480 页。
2. 为 WMI 配置的用于接收 AD 登录事件的一个或多个节点创建 Active Directory 域控制器列表。请参阅添加域控制器 ，第 482 页。
3. 配置 Active Directory，以使其与 ISE 集成。请参阅对被动 ID 配置 WMI ，第 484 页。
4. （可选）管理 Active Directory 提供程序 ，第 519 页。

有关详细信息，请参阅支持 Easy Connect 和 被动身份服务 的 Active Directory 要求 ，第 500 页。

PassiveID 设置入门

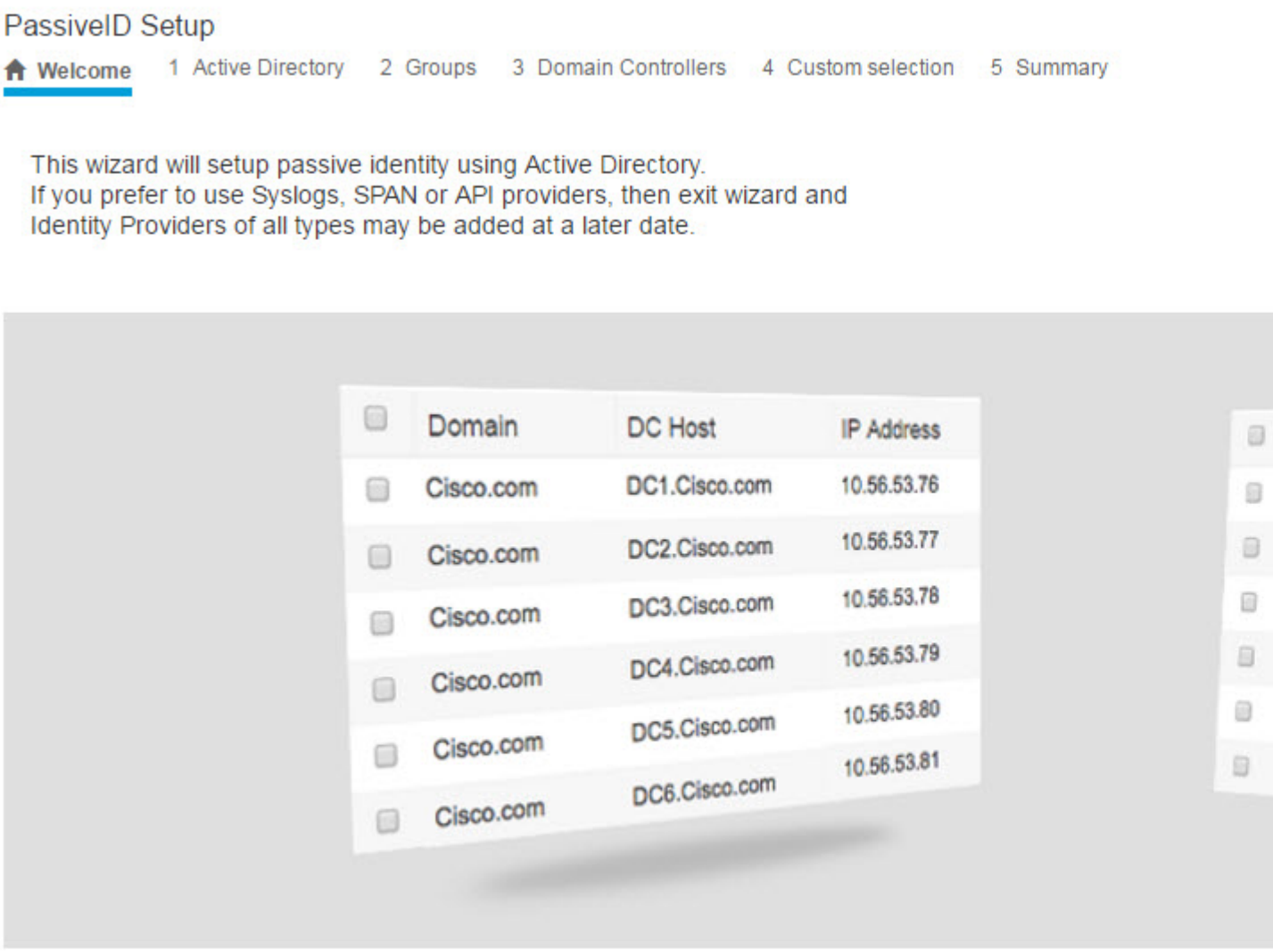
ISE-PIC 提供向导，从中可以轻松快速地将 Active Directory 配置为第一个用户身份提供程序，以便从 Active Directory 接收用户身份。通过为 ISE-PIC 配置 Active Directory，还可以简化稍后配置其他提供程序类型的过程。一旦配置了 Active Directory，就必须配置用户（例如Cisco Firepower 管理中心 (FMC) 或 Stealthwatch），以便定义将要接收用户数据的客户端。有关用户的详细信息，请参阅用户 ，第 558 页。

开始之前

- 确保 Microsoft Active Directory 服务器未驻留在网络地址转换器后，并且不具有网络地址转换 (NAT) 地址。
- 确保旨在用于加入操作的 Microsoft Active Directory 账户有效，并且未配置为下次登录时更改密码。
- 确保您在 ISE 中具有超级管理员或系统管理员权限。
- 在您打算用于任何被动身份服务的专用策略服务器 (PSN) 上启用被动身份和 pxGrid 服务。选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，打开相关节点，并在**常规设置 (General Settings)** 下启用**开启被动身份服务 (Enable Passive Identity Service)** 和 **pxGrid**。
- 确保 ISE 在域名服务器 (DNS) 中具有条目。确保您已从 ISE 正确配置客户端机器的反向查找。有关详细信息，请参阅DNS 服务器 ，第 479 页

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID**。从“被动身份连接器概述”屏幕中，点击**被动身份向导**。

图 *25: PassiveID* 设置



步骤 2 点击**下一步 (Next)**以开始向导。

步骤 3 输入此 Active Directory 加入点的唯一名称。输入此节点连接的 Active Directory 域的域名，然后输入 Active Directory 管理员用户名和密码。有关 Active Directory 设置的详细信息，请参阅Active Directory 设置，第 519 页。

强烈建议您选择**存储凭证 (Store credentials)**，在此情况下将会保存管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

步骤 4 点击**下一步 (Next)**以定义 Active Directory 组并选中要包含和监控的任何用户组。
Active Directory 用户组根据您在上一步中配置的 Active Directory 加入点自动显示。

步骤 5 点击**下一步 (Next)**。选择要监控的 DC。如果选择“自定义”，则从下一个屏幕中选择用于监控的特定 DC。完成后，点击**下一步 (Next)**。

步骤 6 点击**退出 (Exit)** 以完成向导。

下一步做什么

完成将 Active Directory 配置为初始提供程序时，还可以轻松配置其他提供程序类型。有关详细信息，请参阅其他被动身份服务 提供程序，第 522 页。此外，现在还可以配置指定要接收由任何已定义的提供程序收集到的用户身份信息的用户。有关详细信息，请参阅用户，第 558 页。

管理 Active Directory 提供程序

创建并配置 Active Directory 加入点之后，通过以下任务继续管理 Active Directory 探测器：

- 就 Active Directory 测试用户 (Test Users for Active Directory)身份验证，第 493 页
- 查看节点的 Active Directory 加入，第 494 页
- 诊断 Active Directory 问题，第 494 页
- 退出 Active Directory 域，第 485 页
- 删除 Active Directory 配置，第 494 页
- 启用 Active Directory 调试日志，第 495 页

Active Directory 设置

Active Directory AD 是用于从中接收用户信息（包括用户名和 IP 地址）的高度安全且精确的源。

要通过创建和编辑加入点来创建和管理 Active Directory 探测器，请选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)** > **Active Directory**。

有关详细信息，请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点，第 480 页。

表 *64: Active Directory* 加入点名称设置和加入域窗口

字段名称	说明
加入点名称	用于快速轻松地区分此已配置加入点的唯一名称。
Active Directory 域	此节点连接到的 Active Directory 域的域名。
域管理员	这是具有管理员权限的 Active Directory 用户的用户主体名称或用户账户名称。
密码	这是 Active Directory 中配置的域管理员的密码。
指定组织单位	输入管理员的组织单位信息

字段名称	说明
存储凭证 (Store credentials)	强烈建议您选择**存储凭证 (Store credentials)**，在此情况下将会保存管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。 对于终端探测器，必须选择**存储凭证**。

表 *65: Active Directory* 加入/退出窗口

字段名称	说明
ISE 节点 (ISE Node)	安装中的特定节点的 URL。
ISE 节点角色	表示节点是安装中的主节点还是辅助节点。
状态	指示节点是否主动加入 Active Directory 域。
域控制器	对于加入 Active Directory 的节点，此列指示节点在 Active Directory 域中连接到的特定域控制器。
站点	使用 ISE 加入 Active Directory 林时，此字段按照特定 Active Directory 站点在“Active Directory 站点和服务”区域中的显示来指示林中的该站点。

表 *66:* 被动 *ID* 域控制器 *(DC)* 列表

字段	说明
域	域控制器所在的服务器的完全限定域名。
DC 主机	域控制器所在的主机。
站点	使用 ISE 加入 Active Directory 林时，此字段按照特定 Active Directory 站点在“Active Directory 站点和服务”区域中的显示来指示林中的该站点。
IP 地址	域控制器的 IP 地址。
监控方法	通过以下方法之一监控 Active Directory 域控制器的用户身份信息： • WMI：使用 WMI 基础设施直接监控 Active Directory。 • 代理名称：如果已定义代理来监控 Active Directory 的用户信息，请选择“代理”(Agent) 协议，并从下拉列表中选择要使用的代理。有关代理的详细信息，请参阅 Active Directory 代理，第 524 页。

表 *67:* 被动 *ID* 域控制器 *(DC)* 编辑窗口

字段名称	说明
主机 **FQDN**	输入域控制器所在的服务器的完全限定域名。
说明	输入此域控制器的唯一说明，以便轻松标识此域控制器。
用户名	用于访问 Active Directory 的管理员的用户名。
密码	用于访问 Active Directory 的管理员的密码。
协议	通过以下方法之一监控 Active Directory 域控制器的用户身份信息： • WMI：使用 WMI 基础设施直接监控 Active Directory。 • 代理名称：如果已定义代理来监控 Active Directory 的用户信息，请选择“代理”(Agent) 协议，并从下拉列表中选择要使用的代理。有关代理的详细信息，请参阅 Active Directory 代理，第 524 页。

系统从 Active Directory 来定义和管理 Active Directory 组，并且可从此选项卡查看加入此节点的 Active Directory 的组。有关 Active Directory 的详细信息，请参阅 https://msdn.microsoft.com/en-us/library/bb742437.aspx。

表 *68: Active Directory* 高级设置

字段名称	说明
历史记录间隔	被动身份服务 读取已出现的用户登录信息的时间段。启动或重新启动 被动身份服务 以跟进在其不可用情况下生成的事件时需要此项。当终端探测器处于活动状态时，它将保持此间隔的频率。
用户会话老化时间	用户可以登录的时间量。被动身份服务 会识别 DC 中的新用户登录事件，但是 DC 在用户注销时不会进行报告。通过老化时间，思科 ISE 可以确定用户登录的时间间隔。
NTLM 协议设置	您可以选择 NTLMv1 或 NTLMv2 作为思科 ISE 和 DC 之间的通信协议。NTLMv2 是建议默认值。

其他被动身份服务 提供程序

为了使 ISE 能够向订用服务的使用者（用户）提供身份信息（被动身份服务 ），您必须首先配置 ISE 探测器，它连接到身份提供程序。

下表提供了有关 ISE 中所有提供程序和探测类型的详细信息。有关 Active Directory 的详细信息，请参阅 Active Directory 作为探测器和提供程序， 第 516 页。

您可以定义下列提供程序类型：

表 *69:* 提供程序类型

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
Active Directory (AD)	用于从中接收用户信息的高度安全而精确且最常用的源。 作为探测器，AD 运用 WMI 技术传送经过身份验证的用户身份。 此外，AD 本身而不是探测器，而是用作其他探测器从中检索用户数据的源系统（提供程序）。	Active Directory 域控制器	WMI	• 用户名 • IP 地址 • 域 (Domain)	Active Directory 作为探测器和提供程序，第 516 页
代理	Active Directory 域控制器或成员服务器上安装的本地 32 位应用。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。		域控制器或成员服务器上安装的代理。	• 用户名 • IP 地址 • 域 (Domain)	Active Directory 代理，第 524 页
终端	除其他已配置的探测器以外，始终在后台运行，以便验证用户是否仍然处于连接状态。		WMI	用户是否仍然处于连接状态	终端探测器，第 555 页
SPAN	位于网络交换机上，以便侦听网络流量并根据 Active Directory 数据提取用户身份信息。		交换机上安装的 SPAN，以及 Kerberos 消息	• 用户名 • IP 地址 • 域 (Domain)	SPAN，第 533 页

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
API 提供程序	使用 ISE 提供的 RESTful API 服务从编程为与 RESTful API 客户端进行通信的任何系统收集用户身份信息。	编程为与 REST API 客户端进行通信的任何系统。	RESTful API。以 JSON 格式发送到用户的用户身份。	• 用户名 • IP 地址 • 端口范围 • 域	API 提供程序，第 528 页
系统日志	解析系统日志消息和检索用户身份，包括 MAC 地址。	• 常规系统日志消息提供程序 • DHCP 服务器	系统日志消息	• 用户名 • IP 地址 • MAC 地址 • 域	系统日志提供程序，第 534 页

Active Directory 代理

从 被动身份服务 工作中心在 Active Directory (AD) 域控制器 (DC) 或成员服务器上的任意位置（根据配置）安装本地 32 位应用（即域控制器 [DC] 代理），以从 AD 检索用户身份信息，然后将这些身份发送给已配置的用户。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。代理可安装在单独的域中，也可安装在 AD 域中，并且一旦安装，它们就会每分钟提供一次 ISE 的状态更新。

代理可由 ISE 自动安装和配置，您也可以手动对其进行安装。安装时，会发生以下情况：

- 代理及其关联文件安装在以下路径：**`Program Files/Cisco/Cisco ISE PassiveID Agent`**
- 系统将安装一个名为 **`PICAgent.exe.config`** 的配置文件，其中会指示代理的日志记录级别。您可以从该配置文件内手动更改日志记录级别。
- CiscoISEPICAgent.log 文件与所有日志记录消息一起存储。
- nodes.txt 文件包含部署中可与代理进行通信的所有节点的列表。代理会访问列表中的第一个节点。如果无法访问该节点，代理将根据列表中节点的顺序继续尝试通信。对于手动安装，必须打开文件并输入节点 IP 地址。（手动或自动）安装完成后，便只能通过手动更新该文件来对其进行更改。打开文件，然后根据需要添加、更改或删除节点 IP 地址。
- Cisco ISE PassiveID 代理服务在机器上运行，您可从“Windows 服务”对话框管理该机器。
- ISE 最多支持 100 个域控制器，而每个代理最多可以监控 10 个域控制器。

注释 要监控 100 个域控制器，必须配置 10 个代理。

注释 仅 Windows Server 2008 及更高版本上支持 Active Directory 代理。

如果无法安装代理，则对被动身份服务使用 Active Directory 探测器。有关详细信息，请参阅Active Directory 作为探测器和提供程序，第 516 页。

自动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何自动安装并配置代理以监控域控制器。

开始之前

准备工作：

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE 的 DNS 服务器配置要求的详细信息，请参阅DNS 服务器，第 479 页
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅 https://www.microsoft.com/net/framework。
- 活动的被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置，第 515 页。
- 创建AD加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅Active Directory 作为探测器和提供程序，第 516 页。

  对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组，第 486 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**代理 (Agents)**。

步骤 2 要添加新客户端，请从表的顶部点击**添加 (Add)**。

步骤 3 要创建新代理并将其自动安装到您在此配置中指示的主机上，请选择**部署新代理 (Deploy New Agent)**。

步骤 4 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅Active Directory 代理设置，第 527 页。

步骤 5 点击 **Deploy**（部署）。
代理将根据您在配置中指示的域自动安装到主机上，并保存设置。代理现在显示在“Agents”(代理)表格中，并可应用于监控指定域控制器，如以下步骤所述。

步骤 6 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **Active Directory** 以查看当前配置的所有接入点。

步骤 7 点击您要从中启用所创建代理的接入点的链接。

步骤 8 选择**被动 ID (Passive ID)** 选项卡以配置您作为先决条件的一部分而添加的域控制器。

步骤 9 选择您要通过所创建代理来监控的域控制器，然后点击**编辑 (Edit)**。

步骤 10 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。

步骤 11 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您为代理创建的用户名和密码凭证（如果有），然后点击**保存 (Save)**。

手动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何手动安装并配置代理以监控域控制器。

开始之前

准备工作：

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器，第 479 页
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅 https://www.microsoft.com/net/framework。
- 活动的被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置，第 515 页。
- 创建 AD 加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅Active Directory 作为探测器和提供程序，第 516 页。

  对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组，第 486 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**代理 (Agents)**。

步骤 2 点击**下载代理 (Download Agent)** 以下载 **`picagent-installer.zip`** 文件进行手动安装。
此文件将下载至标准 Windows 下载文件夹。

步骤 3 将此 zip 文件置于指定主机并运行安装。

步骤 4 在 ISE GUI 中，再次选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**代理 (Agents)**。

步骤 5 要配置新代理，请从表的顶部点击**添加 (Add)**。

步骤 6 要配置已在主机上安装的代理，请选择**注册现有代理 (Register Existing Agent)**。

步骤 7 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅Active Directory 代理设置，第 527 页。

步骤 8 点击**保存 (Save)**。
系统会保存代理设置。代理现在显示在“Agents”(代理)表格中，并可应用于监控指定域控制器，如以下步骤所述。

步骤 9 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **Active Directory** 以查看当前配置的所有接入点。

步骤 10 点击您要从中启用所创建代理的接入点的链接。

步骤 11 选择**被动 ID (Passive ID)** 选项卡以配置您作为先决条件的一部分而添加的域控制器。

步骤 12 选择您要通过所创建代理来监控的域控制器，然后点击**编辑 (Edit)**。

步骤 13 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。

步骤 14 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您为代理创建的任何用户名和密码凭证，然后点击**保存 (Save)**

卸载代理

可以直接从 Windows 轻松（手动）卸载自动或手动安装的代理。

步骤 1 在 Windows 对话框中，转至**程序和功能**。

步骤 2 在已安装程序的列表中，查找并选择Cisco ISE 被动 ID 代理。

步骤 3 点击**卸载**。

Active Directory 代理设置

允许 ISE 在网络中的指定主机上自动安装代理，以从不同的域控制器 (DC) 检索用户身份信息并向被动身份服务 订户提供此信息。

要创建和管理代理，请选择 **提供程序 (Providers)** > **代理 (Agents)**. 请参阅自动安装并部署 Active Directory 代理，第 525 页。

表 *70:* 代理窗口

字段名称	说明
名称	您配置的代理名称。
主机	安装代理的主机的完全限定域名。
监控	此为指定代理所监控的域控制器的逗号分隔列表。

表 *71:* 新建代理 *(Agents New)*

字段	说明
“部署新代理”(Deploy New Agent) 或“注册现有代理”(Register Existing Agent)	• “部署新代理”(Deploy New Agent)：在指定主机上安装新代理。 • “注册现有代理”(Register Existing Agent)：在主机上手动安装代理，然后从此屏幕为 被动身份服务 配置此代理以启用服务。
名称	输入可用于轻松识别代理的名称。
说明	输入可用于轻松识别代理的说明。
主机 **FQDN**	此为已安装代理（注册现有代理）或将要安装代理（自动部署）的主机的完全限定域名。
用户名	输入用户名以访问要安装代理的主机。 被动身份服务 将使用这些凭证为您安装代理。
密码	输入用户密码以访问要安装代理的主机。 被动身份服务 将使用这些凭证为您安装代理。

API 提供程序

通过Cisco ISE 中的“API 提供程序”功能，可将用户身份信息从自定义程序或从终端服务器 (TS) 代理推送到内置的 ISE 被动身份服务 REST API 服务。通过此方式，可以自定义网络中的可编程客户端，以将从任何网络访问控制 (NAC) 系统收集到的用户身份发送到服务。此外，通过Cisco ISE API 提供程序，还可与网络应用（例如 Citrix 服务器上的 TS 代理，其中所有用户都具有同一 IP 地址但分配有唯一端口）接合。

例如，在 Citrix 服务器上运行的用于为根据 Active Directory (AD) 服务器进行身份验证的用户提供身份映射的代理可向 ISE 发送 REST 请求，请求只要有新用户登录或注销便添加或删除用户会话。然后，ISE 获取从客户端传送的用户身份信息（包括 IP 地址和已分配的端口），并将其发送到预配置用户，例如Cisco Firepower 管理中心 (FMC)。

ISE REST API 框架通过 HTTPS 协议实施 REST 服务（无需客户端证书验证），并以 JSON (JavaScript Object Notation) 格式传送用户身份信息。有关 JSON 的详细信息，请参阅 http://www.json.org/。

ISE REST API 服务会解析用户身份，此外还会将该信息映射到端口范围，以便区分同时登录到一个系统的不同用户。每次将端口分配给用户时，API 都会向 ISE 发送一条消息。

REST API 提供程序流程

配置了从 ISE 到自定义客户端的网桥后（通过将该客户端声明为 ISE 的提供程序，并使该特定自定义程序 (客户端) 能够发送 RESTful 请求），ISE REST 服务便通过以下方式进行工作：

1. 对于客户端身份验证，Cisco ISE 需要身份验证令牌。客户端机器上的自定义程序在发起联系时发送身份验证令牌的请求，然后 ISE 每次都会通知先前令牌已到期。系统会返回令牌以响应请求，从而启用客户端和 ISE 服务之间的持续通信。
2. 用户登录到网络中后，客户端便会检索用户身份信息，并使用 API 添加命令将该信息发布到 ISE REST 服务。
3. Cisco ISE 接收并映射用户身份信息。
4. Cisco ISE 向用户发送已映射的用户身份信息。
5. 只要有必要，自定义机器即可发送用于移除用户信息的请求，方法是发送“删除 API”调用并包含在发送“添加”调用后作为响应接收到的用户 ID。

在 ISE 中使用 REST API 提供程序

按照以下步骤激活 ISE 中的 REST 服务：

1. 配置客户端。有关详细信息，请参阅客户端用户文档。
2. 激活被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置， 第 515 页。
3. 确保您已正确配置 DNS 服务器，包括从 ISE 配置客户端机器的反向查找。有关 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器， 第 479 页
4. 请参阅为 被动身份服务 配置与 ISE REST 服务的桥接， 第 529 页。

注释 要将 API 提供程序配置为使用 TS 代理，请在创建从 ISE 到该代理的网桥时添加 TS 代理信息，然后参考 TS 代理文档以获取有关发送 API 调用的信息。

5. 生成身份验证令牌并向 API 服务发送添加和删除请求。

为 被动身份服务 配置与 ISE REST 服务的桥接

为了使 ISE REST API 服务能够从特定客户端接收信息，必须首先从 ISE 定义该特定客户端。您可以定义多个具有不同 IP 地址的 REST API 客户端。

开始之前

准备工作：

- 确保您已激活被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置， 第 515 页。
- 确保您已正确配置 DNS 服务器，包括从Cisco ISE 配置客户端机器的反向查找。有关Cisco ISE 的 DNS 服务器配置要求的详细信息，请参阅DNS 服务器， 第 479 页

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **API 提供程序 (API Providers)**

系统将显示“API 提供程序”表，包括每个现有客户端的状态信息。

步骤 2 要添加新客户端，请从表的顶部点击**添加**。

步骤 3 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅API 提供程序设置，第 530 页。

步骤 4 点击**提交 (Submit)**。
系统将保存客户端配置，并其屏幕会显示更新后的“API 提供程序”表。客户端现在可以将发布内容发送到 ISE REST 服务。

下一步做什么

设置自定义客户端，以将身份验证令牌和用户身份发布到 ISE REST 服务。请参阅将 API 调用发送到 被动 ID REST 服务，第 530 页。

将 API 调用发送到 被动 ID REST 服务

开始之前

为 被动身份服务 配置与 ISE REST 服务的桥接，第 529 页

步骤 1 在浏览器的地址栏中输入Cisco ISE URL（例如 *https://<ise hostname or ip address>/admin/*）

步骤 2 在以下位置中输入已从“API 提供程序”屏幕中指定并配置的用户名和密码：ISE GUI。有关详细信息，请参阅为 被动身份服务 配置与 ISE REST 服务的桥接，第 529 页。

步骤 3 按 **Enter** 键。

步骤 4 在目标节点的“URL 地址”(URL Address) 字段中输入 API 调用。

步骤 5 点击**发送**以发出 API 调用。

下一步做什么

请参阅 API 调用，第 531 页以获取有关不同 API 调用、其架构及其结果的更多信息和详细信息。

API 提供程序设置

注释 完整 API 定义和对象架构可通过请求调用进行检索，如下所示：

- 对于完整 API 规范 (wadl) - https://YOUR_ISE:9094/application.wadl
- 对于 API 模型和对象方案 - https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *72: API* 提供程序设置

字段	说明
名称 (Name)	输入此客户端的用于快速轻松地将其与其他客户端进行区分的唯一名称。
说明	输入此客户端的明确说明。
状态	选择**已启用 (Enabled)** 以使客户端能够在完成配置时立即与 REST 服务进行交互。
主机/IP	输入客户端主机器的 IP 地址。确保您已正确配置 DNS 服务器，包括从 ISE 配置客户端机器的反向查找。
用户名	创建在发布到REST服务时要使用的唯一用户名。
密码	创建在发布到 REST 服务时要使用的唯一密码。

API 调用

这些 API 调用用于通过Cisco ISE 来管理 被动身份服务 的用户身份事件。

目的：生成身份验证令牌

- **请求**

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  请求应包含 BasicAuth 授权报头。提供先前从 ISE-PIC GUI 创建的 API 提供程序凭证。有关详细信息，请参阅API 提供程序设置，第 530 页。

- **响应报头**

  该报头包含 X-auth-access-token。这是发布其他 REST 请求时要使用的令牌。

- **响应正文**

  HTTP 204 No Content

目的：添加用户

- **请求**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  在发布请求标头中添加 X-auth-access-token，例如，标头：X-auth-access-token，值：f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

  201创建

- 响应正文

  {

  "user": "<username>",

  "srcPatRange": {

  "userPatStart": <user PAT start value>,

  "userPatEnd": <user PAT end value>,

  "patRangeStart": <PAT range start value>

  },

  "srcIpAddress": "<src IP address>",

  "agentInfo": "<Agent name>",

  "timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<domain>"

  }

- 注

  - 可在以上 JSON 中删除 srcPatRange 以创建单个 IP 用户绑定。
  - 响应正文包含“ID”，这是所创建的用户会话绑定的唯一标识符。发送 DELETE 请求时使用此 ID，以指示应删除哪个用户。
  - 此响应还包含自链接，这是此新创建的用户会话绑定的 URL。

目的：删除用户

- 请求

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  在 <id> 中，输入从“添加”响应接收到的 ID。

  在删除请求信头中添加 X-auth-access-token，例如，信头：X-auth-access-token，值：f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

  200 OK

- 响应正文

  响应正文包含有关已删除的用户会话绑定的详细信息。

SPAN

SPAN 是 被动身份服务，可以让您快速轻松地启用Cisco ISE 以侦听网络和检索用户信息，而不必将 Active Directory 配置为直接使用Cisco ISE。SPAN 嗅探网络流量（专门检查 Kerberos 消息），提取 Active Directory 也已存储的用户身份信息，并将该信息发送到 ISE。然后，ISE 解析信息，最终将用户名、IP 地址和域名传送到您也已从 ISE 配置的用户。

为了使 SPAN 侦听网络和提取 Active Directory 用户信息，ISE 和 Active Directory 必须连接到网络上的同一交换机。这样，SPAN 便可以从 Active Directory 复制并镜像所有用户身份数据。

使用 SPAN，将通过以下方式检索用户信息：

1. 用户终端登录网络。
2. 登录和用户数据存储在 Kerberos 消息中。
3. 一旦用户登录且用户数据通过交换机进行传递，SPAN 就会镜像网络数据。
4. Cisco ISE 侦听网络以获取用户信息，并从交换机检索镜像的数据。
5. Cisco ISE 解析用户信息并更新被动 ID 映射。
6. Cisco ISE 将已解析的用户信息传送到用户。

使用 SPAN

开始之前

要使 ISE 从网络交换机接收 SPAN 流量，必须先定义侦听此交换机的节点和节点接口。可以配置 SPAN 以侦听安装的不同 ISE 节点。对于每个节点，只能配置一个接口来侦听网络，用于侦听的接口只能专用于 SPAN。

在开始之前，请确保您已激活被动 ID 和 pxGrid 服务。只有已启用被动 ID 的节点才会显示在可用于配置 SPAN 的接口列表中。有关详细信息，请参阅初始设置和配置，第 515 页。

此外，您必须牢记：

- 确保已在网络上配置 Active Directory。
- 在同样连接至 Active Directory 的网络中的交换机上运行 CLI，以确保交换机可以与 ISE 通信。
- 配置交换机以从 AD 镜像网络。
- 配置专用于 SPAN 的 ISE 网络接口卡 (NIC)。此 NIC 仅用于 SPAN 流量。
- 通过命令行界面，确保激活专用于 SPAN 的 NIC。
- 创建仅将 Kerberos 流量发送到 SPAN 端口的 VACL。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **SPAN** 以配置 SPAN。

步骤 2 注释 建议 GigabitEthernet0 网卡 (NIC) 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

输入有意义的说明（可选），选择状态**已启用 (Enabled)**，并选择将用于侦听网络交换机的节点和相关 NIC。有关详细信息，请参阅SPAN 设置，第 534 页。

步骤 3 点击**保存 (Save)**。
系统将保存 SPAN 配置， ISE-PIC ISE 现在主动侦听网络流量。

SPAN 设置

从已部署的每个节点，通过在客户端网络上安装 SPAN，可快速轻松地配置 ISE 以接收用户身份。

表 *73: SPAN* 设置

字段	说明
说明	输入唯一说明以向您提醒当前启用的节点和接口。
状态	选择**已启用 (Enabled)** 可在完成配置时立即启用客户端。
接口 NIC (Interface NIC)	为 ISE 选择一个或两个节点，然后对于每个选定节点，选择用于侦听网络以获取信息的节点接口。 注释 建议将 GigabitEthernet0 NIC 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

系统日志提供程序

被动身份服务会解析来自任何传送系统日志消息的客户端（身份数据提供程序）的系统日志消息，包括常规系统日志消息（来自 InfoBlox、Blue Coat、BlueCat 和 Lucent 之类的提供程序）以及 DHCP 系统日志消息，并发回用户身份信息，包括 MAC 地址。然后将此映射的用户身份数据传送到用户。

您可以指定接收用户身份数据的系统日志客户端（请参阅配置系统日志客户端，第 535 页）。配置提供程序时，您必须指定连接方法（TCP 或 UDP）以及要用于解析的系统日志模板。

注释 当所配置的连接类型为 TCP 时，如果消息报头存在问题且无法解析主机名，则 ISE 会尝试将数据包中接收到的 IP 地址与已为 ISE 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。要查看此列表，请依次选择**工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)** > **系统日志提供程序 (Syslog Providers)**。建议您检查消息报头并根据需要进行自定义，以便保证解析成功。有关自定义报头的详细信息，请参阅自定义系统日志报头，第 541 页。

系统日志探测器会将接收到的系统日志消息发送到 ISE 解析器，该解析器会映射用户身份信息，并将该信息发布到 ISE。然后， ISE 将已解析和已映射的用户身份信息传送给 被动身份服务用户。

要从 ISE-PIC ISE 解析用户身份的系统日志消息，请执行以下操作：

- 配置要从中接收用户身份数据的系统日志客户端。请参阅配置系统日志客户端，第 535 页。
- 自定义单个消息报头。请参阅自定义系统日志报头，第 541 页。
- 通过创建模板来自定义消息正文。请参阅自定义系统日志消息正文，第 540 页。
- 在将系统日志客户端配置为用于解析的消息模板时使用 ISE 中预定义的消息模板，或者基于这些预定义的模板自定义报头或正文模板。请参阅使用系统日志预定义消息模板，第 544 页。

配置系统日志客户端

为了使Cisco ISE 能够从特定客户端侦听系统日志消息，必须首先从Cisco ISE 定义该特定客户端。您可以使用不同 IP 地址定义多个提供程序。

开始之前

在开始之前，请确保您已激活被动 ID 和 pxGrid 服务。有关详细信息，请参阅初始设置和配置，第 515 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**系统日志提供程序 (Syslog Providers)**。
系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 要配置新系统日志客户端，请从表的顶部点击**添加**。

步骤 3 填写所有必填字段（请参阅系统日志设置，第 535 页以获取更多详细信息），并在必要时创建消息模板（请参阅自定义系统日志消息正文，第 540 页以获取更多详细信息），以便正确配置客户端。

步骤 4 点击**提交 (Submit)**。

系统日志设置

配置Cisco ISE 以通过来自特定客户端的系统日志消息接收用户身份，包括 MAC 地址。您可以使用不同 IP 地址定义多个提供程序。

表 *74:* 系统日志提供程序

字段名称	说明
名称	输入用于快速轻松地区分此已配置客户端的唯一名称。
说明	此系统日志提供程序的有意义说明。
状态	选择**已启用 (Enabled)** 可在完成配置时立即启用客户端。
主机	输入主机器的 FQDN。
连接类型	输入 UDP 或 TCP 以指示 ISE 用于侦听系统日志消息的通道。 注释 当所配置的连接类型为 TCP 时，如果消息信头存在问题且无法解析主机名，则思科 ISE 会尝试将数据包中接收到的 IP 地址与已为思科 ISE 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。 要查看此列表，请依次选择**工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)** > **系统日志提供程序 (Syslog Providers)**。建议您检查消息信头并根据需要进行自定义，以便确保解析成功。有关自定义信头的详细信息，请参阅自定义系统日志报头，第 541 页。

字段名称	说明
模板	

字段名称	说明
	模板指示精确正文消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。 例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。 从此字段中，指示要使用的模板（适用于系统日志消息的正文），以便识别并正确解析系统日志消息。 从预定义下拉列表中进行选择，或者点击**新建**以创建自己的自定义模板。有关创建新模板的详细信息，请参阅自定义系统日志消息正文，第 540 页。大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。 **注释** 只能编辑或删除自定义模板，而无法修改下拉列表中的预定义系统模板。 ISE 当前提供下列预定义 DHCP 提供程序模板： • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP **注释** DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便Cisco ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的DHCP 系统日志消息中列出的IP地址进行匹配，从而正确解析和传送用户身份信息。 如果从DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。 Cisco ISE 提供下列预定义常规系统日志提供程序模板：

字段名称	说明
	• ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN 有关模板的信息，请参阅使用系统日志预定义消息模板，第 544 页。
默认域	如果在特定用户的系统日志消息中未识别域，则会将此默认域自动分配给用户，以便确保为所有用户都分配域。 通过默认域或通过从消息中解析的域，会将用户名附加到 username@domain，从而包含该域，以便获取有关用户和用户组的详细信息。

自定义系统日志消息结构（模板）

模板指示精确消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。模板可确定新增和删除映射消息的受支持结构。

通过Cisco ISE，您可以自定义单个消息报头和多个正文结构以供 被动 ID 解析器使用。

模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 被动 ID 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

自定义消息模板时，可以选择基于 ISE-PIC ISE 中预定义的消息模板进行自定义，参考这些预定义选项中使用的正则表达式和消息结构。有关预定义模板、正则表达式、消息结构、示例等的详细信息，请参阅使用系统日志预定义消息模板，第 544 页。

可以自定义：

- 单个消息报头 -自定义系统日志报头，第 541 页
- 多个消息正文 - 自定义系统日志消息正文，第 540 页。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便Cisco ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

自定义系统日志消息正文

通过Cisco ISE，您可以自定义将由 被动 ID 解析器解析的自有系统日志消息模板（通过自定义消息正文）。模板应包含正则表达式，以定义用户名、IP 地址、MAC 地址和域的结构。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便Cisco ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

从系统日志客户端配置屏幕中创建和编辑系统日志消息正文模板。

注释 您只能编辑自己的自定义模板。无法更改系统提供的预定义模板。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**系统日志提供程序 (Syslog Providers)**。
系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 点击**添加 (Add)**以添加新系统日志客户端，或者点击**编辑 (Edit)**来更新已配置的客户端。有关配置和更新系统日志客户端的详细信息，请参阅配置系统日志客户端，第 535 页。

步骤 3 在**系统日志提供程序 (Syslog Providers)** 窗口中，点击**新建 (New)** 以创建新消息模板。要编辑现有模板，请从下拉列表中选择该模板，然后点击**编辑 (Edit)**。

步骤 4 填写所有必填字段。

有关如何正确输入值的信息，请参阅系统日志自定义模板设置和示例，第 542 页。

步骤 5 点击**测试**以根据所输入的字符串正确解析消息。

步骤 6 点击**保存 (Save)**。

自定义系统日志报头

系统日志报头还包含消息源于的主机名。如果Cisco ISE 消息解析器未识别系统日志消息，则可能需要通过配置前置于主机名的分隔符来自定义消息报头，从而使Cisco ISE 能够正确识别主机名并解析消息。有关此屏幕中的字段的更多详细信息，请参阅系统日志自定义模板设置和示例，第 542 页。只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

注释 只能自定义单个报头。自定义信头后，点击**自定义信头 (Custom Header)** 并创建模板时，仅会保存最新的配置。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**系统日志提供程序 (Syslog Providers)**。
系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 点击**自定义报头**以打开“系统日志自定义报头”屏幕。

步骤 3 在**粘贴示例系统日志 (Paste sample syslog)** 字段中，输入系统日志消息中报头格式的示例。例如，从其中一条消息复制并粘贴以下信头：**<181>Oct 10 15:14:08 Cisco.com**。

步骤 4 在**分隔符 (Separator)** 字段中，指示单词是以空格还是制表符分隔。

步骤 5 在**报头中的主机名位置 (Position of hostname in header)** 字段中，指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。

主机名 (Hostname) 字段根据前三个字段中指示的详细信息来显示主机名。例如，如果**粘贴示例系统日志**中的报头示例如下：

<181>Oct 10 15:14:08 Cisco.com

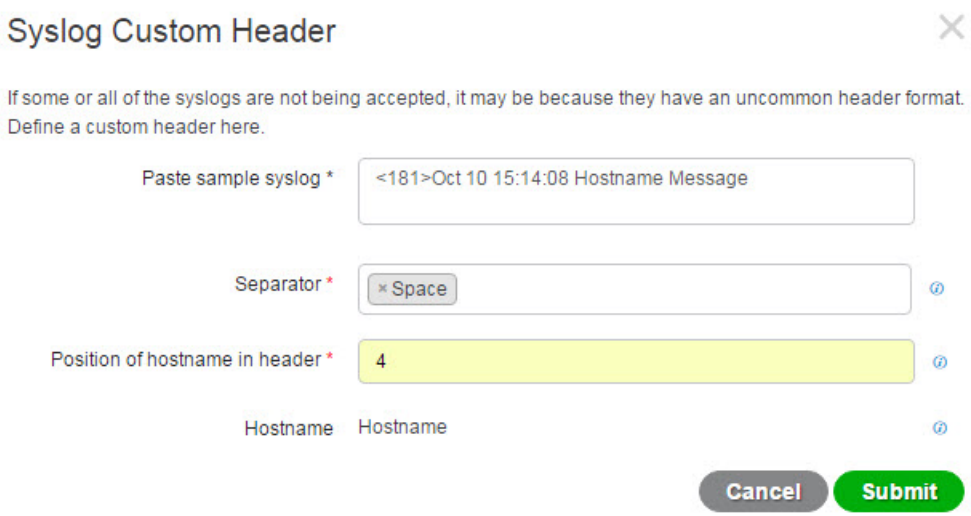
分隔符指示为**空格**，并且**报头中的主机名位置**输入为 4。

主机名将自动显示为 Cisco.com，这是**粘贴示例系统日志**字段中粘贴的报头短语中的第四个单词。

如果未正确显示主机名，请检查您已在**分隔符 (Separator)** 和**报头中的主机名位置 (Position of hostname in header)** 字段中输入的数据。

此示例与以下截屏相同：

图 *26:* 自定义系统日志报头



步骤 6 点击**提交 (Submit)**。

只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

系统日志自定义模板设置和示例

通过Cisco ISE，您可以自定义将由 被动 ID 解析器解析的自有系统日志消息模板。自定义模板确定了新增和删除映射消息的受支持结构。模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 被动 ID 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

注释 大多数预定义模板都使用正则表达式。自定义模板也应使用正则表达式。

系统日志报头部分

您可以通过配置前置于主机名的分隔符来自定义系统日志探测器可识别的单个报头。

下表介绍可在自定义系统日志报头中包含的不同部分和字段。有关正则表达式的详细信息，请参阅表 77: 自定义模板的正则表达式，第 544 页。

表 *75:* 系统日志自定义报头

字段	说明
粘贴示例系统日志	输入系统日志消息中的报头格式的示例。例如，复制并粘贴以下报头： **`<181>Oct 10 15:14:08 Hostname Message`**
分隔符	指示单词是以空格还是制表符分隔。
报头中的主机名位置	指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。
主机名 (Hostname)	根据前三个字段中指示的详细信息来显示主机名。例如，如果**粘贴示例系统日志**中的报头示例如下： <181>Oct 10 15:14:08 Hostname Message 分隔符指示为**空格**，并且**报头中的主机名位置**输入为 4。 **主机名**将自动显示为 Hostname。 如果未正确显示主机名，请检查您已在**分隔符**和**报头中的主机名位置**字段中输入的数据。

消息正文的系统日志模板部分和说明

下表介绍可在自定义系统日志消息模板中包含的不同部分和字段。有关正则表达式的详细信息，请参阅表 77: 自定义模板的正则表达式，第 544 页。

表 *76:* 系统日志模板

部件	字段	说明
	名称 (Name)	用于识别此模板的用途的唯一名称。
映射操作	新映射	描述与此模板配合用于添加新用户的映射类型的正则表达式。例如，在此字段中输入“on from”可指示已登录到 F5 VPN 的新用户。
	已删除的映射	描述与此模板配合用于删除用户的映射类型的正则表达式。例如，在此字段中输入“disconnect”可指示应为 ASA VPN 删除的用户。

部件	字段	说明
用户数据	IP 地址	指示要捕获的 IP 地址的正则表达式。 例如，对于 Bluecat 消息，要捕获此 IP 地址范围内的用户的身份，请输入： (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]
	用户名	指示要捕获的用户名格式的正则表达式。
	域	指示要捕获的域的正则表达式。
	MAC 地址	指示要捕获的 MAC 地址格式的正则表达式。

正则表达式示例

要解析消息，请使用正则表达式。此部分提供正则表达式示例，以便解析 IP 地址、用户名和添加映射消息。

例如，使用正则表达式解析以下消息：

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

正则表达式按下表中进行定义。

表 *77:* 自定义模板的正则表达式

部件	正则表达式
IP 地址	Address <([^\s]+)>|address ([^\s]+)
用户名	User <([^\s]+)>| Username = ([^\s]+)
添加映射消息	(%ASA-4-722051|%ASA-6-713228)

使用系统日志预定义消息模板

系统日志消息具有包含报头和消息正文的标准结构。

本节介绍了Cisco ISE 提供的预定义模板，包括根据消息源支持的报头以及受支持正文结构的内容详细信息。

此外，您可以使用系统中未预定义的源的自定义正文内容来创建自己的模板。本节还介绍了自定义模板的受支持结构。解析消息时，除系统中预定义的报头以外，您还可以配置要使用的单个自定义报头，并且可为消息正文配置多个自定义模板。有关自定义报头的详细信息，请参阅自定义系统日志报头，第 541 页。有关自定义正文的详细信息，请参阅自定义系统日志消息正文，第 540 页。

注释 大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。

消息报头

有两种可由解析器识别的报头类型：适用于所有消息类型（新增和删除）和适用于所有客户端机器。这些报头如下：

- <171>Host message
- <171>Oct 10 15:14:08 Host message

收到后，系统将解析报头以获取主机名，它可以是 IP 地址、主机名或完整 FQDN。

此外，还可以自定义报头。要自定义报头，请参阅自定义系统日志报头，第 541 页。

系统日志 ASA VPN 预定义模板

ASA VPN 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

正文消息	解析示例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 注释 从此消息类型解析的 IP 地址是私有 IP 地址，如消息中所示。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] 注释 从此消息类型解析的 IP 地址是 IPv4 地址。

删除映射正文消息

解析器支持的 ASA VPN 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[UserA,10.1.1.1]

正文消息
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason

正文消息
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

系统日志 Bluecat 预定义模板

支持的系统日志消息格式和 Bluecoat 类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

Bluecat 系统日志的新映射支持的消息如本部分所述。

收到正文消息后，如下解析正文以获取用户详细信息：

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

正文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

删除映射消息

Bluecat 没有已知的删除映射消息。

系统日志 F5 VPN 预定义模板

F5 VPN 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 F5 VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[user=UserA,ip=172.16.0.12]

正文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security [nnnnn]：[UserA @ vendor-abcr] User UserA login on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz \

删除映射消息

目前没有支持的 F5 VPN 删除消息。

系统日志 Infoblox 预定义模板

Infoblox 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

正文消息
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

删除映射消息

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

- 如果包含 MAC 地址：

  [00:0c:29:a2:18:34,10.0.10.100]

- 如果不包含 MAC 地址：

  [10.0.10.100]

正文消息
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

系统日志 Linux DHCPd3 预定义模板

Linux DHCPd3 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射消息

如下表所述，解析器可识别不同的 Linux DHCPd3 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

正文消息
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

删除映射正文消息

解析器支持的 Linux DHCPd3 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[00:0c:29:a2:18:34 ,10.0.10.100]

正文消息
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

系统日志 MS DHCP 预定义模板

MS DHCP 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 MS DHCP 正文消息，如下表所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

[macAddress=000C29912E5D,ip=10.0.10.123]

正文消息
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,,0x4D53465420352E30,MSFT,5.0

删除映射正文消息

解析器解析的 MS DHCP 支持的删除映射消息如此部分所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

[macAddress=000C29912E5D,ip=10.0.10.123]

正文消息
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

系统日志 SafeConnect NAC 预定义模板

SafeConnect NAC 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 SafeConnect NAC 正文消息，如下表所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

正文消息
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

删除映射消息

目前没有 Safe Connect 支持的删除消息。

系统日志 Aerohive 预定义模板

Aerohive 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Aerohive 正文消息。

从正文解析的详细信息包括用户名和 IP 地址。用于解析的正则表达式如以下示例所示：

- 新映射—`auth\:`
- IP—`ip ([A-F0-9a-f:.]+)`
- 用户名—`UserA ([a-zA-Z0-9\_]+)`

收到正文消息后，如下解析正文以获取用户详细信息：

[UserA,10.5.50.52]

正文消息
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

删除映射消息

系统当前不支持从 Aerohive 删除映射消息。

系统日志 Blue Coat 预定义模板 - 主代理、代理 SG、Squid Web 代理

系统支持 Blue Coat 的以下消息类型：

- BlueCoat 主代理
- BlueCoat 代理 SG
- BlueCoat Squid Web 代理

支持的系统日志消息格式和 Bluecoat 消息类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 Blue Coat 正文消息，如下表所述。

收到正文消息后，如下解析正文以获取用户详细信息：

[UserA,192.168.10.24]

正文消息（此示例摘自 **BlueCoat** 代理 **SG** 消息）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

下表介绍了每个客户端用于新映射消息的不同正则表达式结构。

客户端	正则表达式
BlueCoat 主代理	新映射 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4})\s** 用户名 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat 代理 SG	新映射 **(\-\sPROXIED){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4})\s[a-zA-Z0-9_]+\s-** 用户名 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web 代理	新映射 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,2}){1,7}[a-zA-Z0-9]{1,4})\sTCP** 用户名 **\s([a-zA-Z0-9\._]+)\s\-\/**

删除映射消息

Blue Coat 客户端支持删除映射消息，但当前没有提供相关示例。

下表介绍了每个客户端用于删除映射消息的不同的已知正则表达式结构示例。

客户端	正则表达式
BlueCoat 主代理	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat 代理 SG	当前无可用示例。
BlueCoat Squid Web 代理	**(TCP_MISS|TCP_NC_MISS){1}**

系统日志 ISE 和 ACS 预定义模板

侦听 ISE 或 ACS 客户端时，解析器将接收以下消息类型：

- 通过身份验证 - 当用户经 ISE 或 ACS 进行身份验证后，通过身份验证消息将发出以通知身份验证已成功，并包含用户详细信息。系统将解析此消息，并保存此消息中的用户详细信息和会话 ID。
- 记帐启动和记帐更新消息（新映射）- 从 ISE 或 ACS 接收的记帐启动或记帐更新消息将进行解析，并包含在通过身份验证消息中保存的用户详细信息和会话 ID，然后映射用户。
- 记帐停止（删除映射）- 从 ISE 或 ACS 接收后，用户应设将从系统中删除。

ISE 和 ACS 支持的系统日志消息格式与类型如下所述。

通过身份验证消息

通过身份验证类型支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- 解析示例

  仅解析用户名和会话 ID。

  [UserA,5]

记帐启动/更新（新映射）消息

新映射支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- 解析示例

  解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

  [UserA,10.0.0.16]

删除映射消息

删除映射支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- 解析示例

  解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

  [UserA,10.0.0.16]

系统日志 Lucent QIP 预定义模板

Lucent QIP 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 544 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Lucent QIP 正文消息。

这些消息的正则表达式结构如下：

DHCP_GrantLease|:DHCP_RenewLease

收到正文消息后，如下解析正文以获取用户详细信息：

[00:0C:29:91:2E:5D,10.0.0.11]

正文消息
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

删除映射正文消息

这些消息的正则表达式结构如下所示：

删除租约:|DHCP 自动释放:

收到正文消息后，如下解析正文以获取用户详细信息：

[10.0.0.11]

正文消息
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

过滤被动身份服务

您可以根据用户名称或 IP 地址过滤某些用户。例如，如果 IT 服务中的管理员登录到终端以帮助该终端的常规用户，则可以过滤掉管理员活动，从而在“实时会话”中不显示管理员活动，而是仅显示该终端的常规用户。实时会话显示映射过滤器未过滤掉的被动身份服务组件。您可以按照需要添加很多过滤器。“OR”逻辑运算符适用于过滤器之间。如果在单个过滤器中同时指定两个字段，则在这两个字段之间使用“AND”逻辑运算符。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择**映射过滤器 (Mapping Filters)**。

步骤 2 选择 **提供程序 (Providers)** > **映射过滤器 (Mapping Filters)**。

步骤 3 点击 **Add**，输入您想要过滤的用户的用户名和 Ip 地址，然后点击**提交 (Submit)**。

步骤 4 要查看当前已记录到监控会话目录中未过滤用户，请选择 **操作 (Operations)** > **RADIUS 实时日志 (RADIUS Livelog)**。

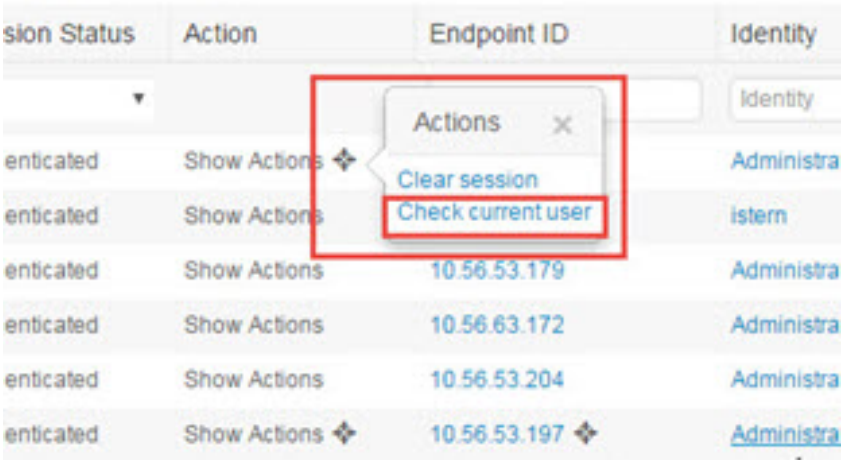
终端探测器

除可以配置的自定义提供程序以外，当激活 被动身份服务 时会在 ISE 中启用终端探测器，并且始终在后台运行。终端探测器会定期检查每个特定用户是否仍已登录到系统。

注释 为了确保终端在后台运行，必须首先配置初始 Active Directory 加入点，并确保选择**存储凭证 (Store Credentials)**。有关配置终端探测器的详细信息，请参阅使用终端探测器，第 556 页。

要手动检查终端状态，请转至**实时会话 (Live Sessions)**，从**操作 (Actions)** 列点击**显示操作 (Show Actions)**，然后选择**检查当前用户 (Check current user)**，如下图所示。

图 *27:* 检查当前用户



有关终端用户状态和手动执行检查的详细信息，请参阅RADIUS实时会话 (Live Sessions)，第 282 页。

当终端探测器识别用户已连接时，如果自上次为特定终端更新会话已经过 4 小时，则它将检查该用户是否仍已登录并收集以下数据：

- MAC 地址
- 操作系统版本

根据此检查，探测器将执行以下操作：

- 当用户仍处于登录状态时，探测器将使用“活动用户”(Active User) 状态更新Cisco ISE。
- 当用户已注销时，会话状态更新为“已终止”，15 分钟后，将从会话目录中删除用户。
- 当无法联系用户时（例如，当防火墙阻止联系或者终端已关闭时），状态更新为“无法访问”，并且用户策略将确定如何处理用户会话。终端将保持处于会话目录中。

使用终端探测器

开始之前

根据子网范围创建并启用终端探测器。每个 PSN 可以创建一个终端探测器。要使用终端探测器，请首先确保您已配置下列各项：

- 终端必须具有与端口 445 的网络连接。
- 从 ISE 配置初始 Active Directory 加入点，并确保在出现提示时选择**选择凭证**。有关加入点的详细信息，请参阅 Active Directory 作为探测器和提供程序，第 516 页。

注释 为了确保终端在后台运行，必须首先配置初始 Active Directory 加入点，通过它可使终端探测器即便在 Active Directory 未完全配置时也能够运行。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **提供程序 (Providers)**，然后选择**终端探测 (Endpoint Probes)**。

步骤 2 点击**添加 (Add)**以创建新终端探测器。

步骤 3 填写必填字段，从而确保您从**状态**字段中选择**启用**，然后点击**提交 (Submit)**。有关详细信息，请参阅终端探测器设置，第 557 页。

终端探测器设置

根据子网范围，为每个 PSN 创建单个终端探测器。如果部署中有多个 PSN，则可以为一组单独的子网分配每个 PSN。

表 *78:* 终端探测器设置

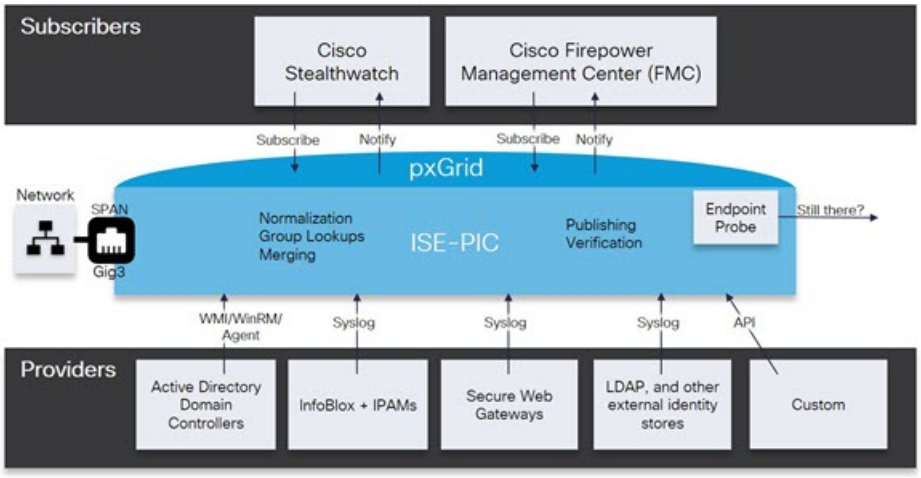
字段名称	说明
名称	输入用于识别此探测器的使用的唯一名称。
说明	输入用于介绍此探测器的使用的唯一说明。
状态	选择**启用 (Enable)** 以激活此探测器。
主机名	从部署中的可用 PSN 的列表中选择此探测器的 PSN。
子网	输入此探测器应检查的终端组的子网范围。使用标准子网掩码范围并以逗号分隔子网地址。 例如：10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 每个范围必须唯一并与所有其他范围分隔开来。例如，不能为同一探测器输入以下范围，因为它们相互重叠：2.2.2.0/16,2.2.3.0/16

用户

被动身份服务 使用Cisco pxGrid 服务，以便将从各种提供程序收集并由Cisco ISE 会话目录存储的经过身份验证的用户身份传送到其他网络系统，例如Cisco Stealthwatch 或Cisco Firepower 管理中心 (FMC)。

在下图中，pxGrid 节点从外部提供程序收集用户身份。这些身份经过解析、映射和设置格式。pxGrid 获取这些设置格式的用户身份，并将其发送到 被动身份服务 用户。

图 *28*: 被动身份服务 流



连接到Cisco ISE 的用户必须注册才能使用 pxGrid 服务。用户应通过 pxGrid SDK 采用思科提供的 pxGrid 客户端库以成为客户端。用户可以使用唯一名称和基于证书的相互身份验证登录 pxGrid。一旦他们发送了有效证书，ISE 便会自动批准Cisco pxGrid 用户。

用户可连接到已配置的 pxGrid 服务器主机名或 IP 地址。我们建议您使用主机名，以避免出现不必要的错误，尤其是为了确保 DNS 查询正常工作。功能是指在 pxGrid 上创建的供用户发布和订用的信息主题或通道。在Cisco ISE 中，仅支持 SessionDirectory 和 IdentityGroup。功能信息可通过发布、定向查询或批量下载查询从发布者获取，并可导航至**功能 (Capabilities)** 选项卡中的**用户 (Subscribers)** 进行查看。

要使用户能够从 ISE 接收信息，必须执行以下操作：

1. 或者，从用户端生成证书。
2. 从 PassiveID 工作中心生成用户的 pxGrid 证书，第 559 页。
3. 启用用户，第 560 页。执行此步骤，或者自动启用批准，以便允许订户从ISE接收用户身份。请参阅 配置用户设置，第 560 页。

生成用户的 pxGrid 证书

开始之前

您可以生成 pxGrid 用户的证书，以便保证 pxGrid 和用户之间的相互信任，从而使用户身份能够从 ISE 传递到用户。要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择**工作中心 (Work Centers)** > **PassiveID** > **订户 (Subscribers)**，然后转至**证书 (Certificates)** 选项卡。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **“生成无证书签名请求的单个证书”(Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。在“通用名称”字段中，输入包含 pxGrid 作为前缀的 pxGrid FQDN。例如，www.pxgrid-ise.ise.net。或者，使用通配符。例如，*.ise.net
- **“生成有证书签名请求的单个证书”(Generate a single certificate with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。
- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载 ISE 公共根证书，以便将其添加到 pxGrid 客户端的受信任证书存储区。ISE pxGrid 节点仅信任新签名的 pxGrid 客户端证书，反之亦然，从而无需外部证书颁发机构。

步骤 3 （可选）您可以输入此证书的说明。

步骤 4 查看或编辑此证书所基于的 pxGrid 证书模板。证书模板包含证书颁发机构 (CA) 基于该模板颁发的所有证书通用的属性。证书模板定义了主题、主题备选名称 (SAN)、密钥类型、密钥大小、必须使用的 SCEP RA 配置文件、证书的有效期以及扩展密钥用法 (EKU)（指定必须将证书用于客户端身份验证、服务器身份验证，还是用于两者）。内部Cisco ISE CA (ISE CA) 使用证书模板颁发基于该模板的证书。要编辑此模板，请选择 **管理 (Administration)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)**。

步骤 5 指定使用者备选名称 (SAN)。可以添加多个 SAN。可提供以下选项：

- **FQDN**：输入 ISE 节点的完全限定域名。例如 www.isepic.ise.net。或者，使用通配符表示 FQDN。例如，*.ise.net

  可以为 FQDN 添加其中还可输入 pxGrid FQDN 的附加行。这应与您在“通用名称”(Common Name) 字段中使用的 FQDN 相同。

- **“IP 地址”(IP address)**：输入将与证书关联的 ISE 节点的 IP 地址。如果用户使用 IP 地址而不是 FQDN，则必须输入此信息。

注释 如果选定“生成批量证书”(Generate Bulk Certificate) 选项，则不会显示此字段。

步骤 6 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE)

----”标签。终端实体的私钥使用 PKCS* PEM 存储。其开头采用“-----加密私钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密私钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。

- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format [including certificate chain; one file for both the certificate chain and key])**：CA 根证书、CA 中间证书以及终端实体的证书和私钥存储在一个加密文件时，所采用的二进制格式。

步骤 7 输入证书密码。

步骤 8 点击**创建**。

启用用户

必须执行此任务，或者自动启用审批，才能允许用户从Cisco ISE 接收用户身份。请参阅配置用户设置，第 560 页。

开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看Cisco pxGrid 客户端发送的请求。
- 启用被动身份服务。有关详细信息，请参阅Easy Connect，第 510 页。

步骤 1 选择 **工作中心 (Work Centers)** > **PassiveID** > **订户 (Subscribers)** 并确保查看的是**客户端 (Clients)** 选项卡。

步骤 2 选中用户旁边的复选框，然后点击**审批**。

步骤 3 点击**刷新 (Refresh)** 查看最新的状态。

从实时日志查看用户事件

“实时日志”(Live Logs) 页面显示所有用户事件。事件信息包括用户和功能名称，以及事件类型和时间戳。

导航至 **用户** 并选择**实时日志 (Live Log)** 选项卡以查看事件列表。您还可以清除日志并重新同步或刷新列表。

配置用户设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **pxGrid服务 (pxGrid Services)** > **设置 (Settings)**。

步骤 2 根据您的需求选择以下选项：

- 自动审批新账户 - 选中此复选框可自动审批来自新 pxGrid 客户端的连接请求。
- 允许基于密码的账户创建 - 选中此复选框可为 pxGrid 客户端启用基于用户名/密码的身份验证。如果启用此选项，系统无法自动审批 pxGrid 客户端。

  pxGrid 客户端可以通过使用 REST API 发送用户名向 pxGrid 控制器注册。在客户端注册时，pxGrid 控制器为 pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。

步骤 3 点击**保存 (Save)**。

中的监控和故障排除服务被动 ID 工作中心

详细了解如何使用监控、故障排除和报告工具来管理 被动 ID 工作中心。

- RADIUS实时会话 (Live Sessions)，第 282 页
- 请参阅 中的“报告”部分 思科 ISE 报告，第 255 页
- 用于验证传入流量的 TCP Dump 实用工具，第 1253 页

LDAP

轻型目录访问协议 (LDAP) 是 RFC 2251 定义用于查询和修改在 TCP/IP 上运行的目录服务的网络协议。LDAP 是用于访问基于 X.500 的目录服务器的轻型机制。

Cisco ISE 使用 LDAP 协议集成 LDAP 外部数据库，此外部数据库也称为身份源。

LDAP 目录服务

LDAP 目录服务以客户端-服务器模式为基础。客户端通过连接至 LDAP 服务器并向服务器发送运行请求，启动 LDAP 会话。然后服务器发送其响应。一个或多个 LDAP 服务器包含来自 LDAP 目录树或 LDAP 后端数据库的数据。

目录服务管理一个目录，此目录是存储信息的一个数据库。目录服务使用分布式模式存储信息，而且通常会在目录服务器之间复制这些信息。

LDAP 目录以简单树状层次结构排列，可以分布在多个服务器中。每台服务器都可包含整个目录的复制版本，系统会定期同步此复制版本。

树中的每个条目都包含一组属性，其中每个属性都有一个名称（属性类型或属性说明）以及一个或多个值。这些属性在架构中定义。

每个条目都有一个唯一标识符：其可分辨名称 (DN)。此名称包含相对可分辨名称 (RDN)，RDN 由条目中的属性，然后加上父条目的 DN 构成。您可以将 DN 视为完整文件名，将 RDN 视为文件夹的相对文件名。

多个 LDAP 实例

通过使用不同的 IP 地址或端口设置创建多个 LDAP 实例，可以将Cisco ISE 配置为使用不同的 LDAP 服务器或同一个 LDAP 服务器中的不同数据库进行身份验证。每个主要服务器 IP 地址和端口配置，以及辅助服务器 IP 地址和端口配置，组成对应于一个Cisco ISE LDAP 身份源实例的一个 LDAP 实例。

Cisco ISE 不要求每个 LDAP 实例都对应一个 LDAP 数据库。可以设置多个 LDAP 实例来访问同一个数据库。当 LDAP 数据库包含多个用户或组子树时，此方法非常有用。由于每个 LDAP 实例仅支持一个用户子树目录和一个组子树目录，因此，必须为每个用户目录和组目录子树组合配置单独的 LDAP 实例，Cisco ISE 为该组合提交身份验证请求。

LDAP 故障转移

Cisco ISE 支持在主要 LDAP 服务器和辅助 LDAP 服务器之间进行故障转移。当 LDAP 服务器宕机或因其他原因而无法访问，导致Cisco ISE 无法连接 LDAP 服务器，从而使得身份验证请求失败时，就会发生故障转移。

如果您建立故障转移设置并且Cisco ISE 尝试连接的第一个 LDAP 服务器无法访问，Cisco ISE 始终会尝试连接第二个 LDAP 服务器。如果您希望Cisco ISE 再次使用第一个 LDAP 服务器，您必须在 Failback Retry Delay 文本框中输入一个值。

注释 Cisco ISE 始终使用主要 LDAP 服务器从 Admin 门户获取用于授权策略的组和属性，因此当您配置这些项目时必须可以访问主要 LDAP 服务器。根据故障转移配置，Cisco ISE 仅将辅助 LDAP 服务器用于运行时的身份验证和授权。

LDAP 连接管理

Cisco ISE 支持多个并行 LDAP 连接。首次进行 LDAP 身份验证时，根据需要打开连接。为每个 LDAP 服务器配置最大连接数。事先打开连接可缩短身份验证时间。可以设置最大连接数以用于并发绑定连接。每台 LDAP 服务器（主要或辅助）的打开连接数量可以不同，此数量根据为每台服务器配置的最大管理连接数来确定。

Cisco ISE 会为Cisco ISE 中配置的每台 LDAP 服务器保留打开的 LDAP 连接列表（包括绑定信息）。在身份验证流程中，连接管理器会尝试从池中查找打开的连接。如果打开的连接不存在，系统会打开新的连接。

如果 LDAP 服务器关闭连接，则连接管理器会在对搜索目录的第一个调用过程中报告错误，并会尝试更新连接。身份验证流程完成之后，连接管理器会发布连接。

LDAP 用户身份验证

您可以将 LDAP 配置为外部身份存储库。Cisco ISE 使用明文密码身份验证。用户身份验证包括：

- 在 LDAP 服务器中搜索与请求中的用户名相匹配的条目。

- 使用 LDAP 服务器中查找到的用户密码检查用户密码。
- 检索用于策略的组成员信息。
- 检索指定属性的值以用于策略和授权配置文件。

若要验证用户，Cisco ISE 会向 LDAP 服务器发送绑定请求。绑定请求会包含明文显示的用户 DN 和密码。如果用户的 DN 和密码与 LDAP 目录中的用户名和密码匹配，则用户通过身份验证。

当 Active Directory 用作 LDAP 时，UPN 名称用于用户身份验证。当 Sun ONE Directory Server 用作 LDAP 时，SAM 名称用于用户身份验证

注释 Cisco ISE 会为每个用户身份验证发送两条 searchRequest 消息。这不会影响Cisco ISE 授权或网络性能。第二个 LDAP 请求用于确保Cisco ISE 与正确的身份通信。

注释 思科 ISE 作为 DNS 客户端，仅使用 DNS 响应中返回的第一个 IP 来执行 LDAP 绑定。

我们建议您使用安全套接字层 (SSL) 保护与 LDAP 服务器的连接。

注释 仅当密码到期后，帐户仍有剩余宽限登录次数时，LDAP才支持密码更改。如果密码更改成功，LDAP 服务器的 bindResponse 应为 LDAP_SUCCESS，且 bindResponse 消息中应包含剩余宽限期登录控制字段。如果 bindResponse 消息包含任何额外的控制字段（除剩余宽限登录外），Cisco ISE 可能无法对消息进行解码。

在授权策略中使用的 LDAP 组和属性检索

Cisco ISE 可以依据 LDAP 身份源验证主题（用户或主机），具体方法是在目录服务器上执行绑定操作，查找和验证主题。成功进行身份验证后，Cisco ISE 可以在必要时检索属于主题的组和属性。可以配置属性以在Cisco ISE 管理员门户中进行检索，方法是选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。Cisco ISE 可以使用这些组和属性授权主题。

要验证用户或查询 LDAP 身份源，Cisco ISE 连接到 LDAP 服务器并维护连接池。

当 Active Directory 配置为 LDAP 存储时，应当注意下列关于组成员身份的限制：

- 用户或计算机必须是策略条件中定义的组的直接成员，才符合策略规则。
- 定义的组可能不是用户或计算机的主组。此限制仅在 Active Directory 配置为 LDAP 存储时适用。

LDAP 组成员身份信息检索

对于用户身份验证、用户查找和 MAC 地址查找，Cisco ISE 必须从 LDAP 数据库检索组成员身份信息。LDAP 服务器通过以下其中一种方式表示使用者（用户或主机）与组之间的关联：

- 组引用使用者 - 组对象包含用于指定使用者的属性。使用者的标识符可以作为以下内容在组中寻源：
  - 可分辨名称
  - 明文用户名
- 使用者引用组 - 使用者对象包含用于指定其所属的组的属性。

LDAP 身份源包含以下用于组成员身份信息检索的参数：

- 引用方向 - 此参数指定在确定组成员身份时要使用的方法（组引用使用者或使用者引用组）。
- 组映射属性 - 此参数指示包含组成员身份信息的属性。
- 组对象类 - 此参数确定特定对象可识别为组。
- 组搜索子树 - 此参数指示用于组搜索的搜索库。
- 成员类型选项 - 此参数指定成员在组成员属性中的存储方式（作为 DN 或明文用户名）。

LDAP 属性检索

针对用户身份验证、用户查找和 MAC 地址查找，Cisco ISE 必须从 LDAP 数据库检索主题属性。对于 LDAP 身份源的每个实例，将创建身份源字典。这些字典支持以下数据类型的属性：

- 字符串
- 无符号整数 32
- IPv4 地址

对于无符号整数和IPv4属性，Cisco ISE会对已检索的相应数据类型的字符串进行转换。如果转换失败或未检索到属性的值，则Cisco ISE 将记录调试消息，但身份验证或查找进程不会失败。

您同样可以配置属性的默认值，当转换失败或Cisco ISE未检索到任何属值时，Cisco ISE即可使用该默认值。

LDAP 证书检索

如果您已将证书检索配置为用户查找的一部分，那么Cisco ISE 必须从 LDAP 检索证书属性值。要从LDAP检索证书属性值，在配置LDAP身份源时，先前必须将属性列表中的证书属性配置为可访问。

LDAP 服务器返回的错误

在身份验证过程中可能会出现以下错误：

- 身份验证错误 - Cisco ISE 会在Cisco ISE 日志文件中记录身份验证错误。

LDAP 服务器返回绑定（身份验证）错误的可能原因如下：

- 参数错误 - 输入了无效的参数
- 用户帐户受限制（已禁用、已锁定、已到期、密码已到期等）
- 初始化错误 - 使用 LDAP 服务器超时设置配置Cisco ISE 在确定该服务器上的连接或身份验证是否已失败之前，应该等待从 LDAP 服务器接收响应的秒数。

  LDAP 服务器返回初始化错误的可能原因如下：

  - 不支持 LDAP。
  - 服务器宕机。
  - 服务器内存不足。
  - 用户无权限。
  - 管理员凭证配置不正确。

以下错误记录为外部资源错误，指示 LDAP 服务器可能有问题：

- 发生连接错误
- 超时到期
- 服务器宕机
- 服务器内存不足

以下错误记录为 Unknown User 错误：

- 用户在数据库中不存在

以下错误记录为 Invalid Password 错误，虽然用户存在，但是发送的密码无效：

- 输入了无效密码

LDAP 用户查找

Cisco ISE 支持 LDAP 服务器的用户查找功能。通过此功能，可以在未经身份验证的情况下在 LDAP 数据库中搜索用户和检索信息。用户查找流程包括以下操作：

- 在 LDAP 服务器中搜索与请求中的用户名相匹配的条目
- 检索要用于策略的用户组成员身份信息
- 检索指定属性的值以用于策略和授权配置文件

LDAP MAC 地址查找

Cisco ISE 支持 MAC 地址查找功能。您可以通过此功能在 LDAP 数据库中搜索 MAC 地址以及在未经身份验证的情况下检索信息。MAC 地址查找过程包括以下操作：

- 在 LDAP 服务器中搜索与设备 MAC 地址匹配的条目
- 为策略中使用的设备检索 MAC 地址组信息
- 为策略中使用的指定属性检索值

添加 LDAP 身份源

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- Cisco ISE 始终使用主要 LDAP 服务器获取用于授权策略的组和属性。因此，当您配置这些项目时，必须可访问您的主要 LDAP 服务器。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP** > **添加 (Add)**。

步骤 2 输入相应值。

步骤 3 点击**提交 (Submit)** 以创建 LDAP 实例。

LDAP 身份源设置

下表介绍“LDAP 身份源”(LDAP Identity Sources) 窗口上的字段，您可以使用此窗口创建 LDAP 实例并连接该实例。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

LDAP 常规设置

下表介绍**常规 (General)** 选项卡上的字段。

表 *79: LDAP* 常规设置

字段名称	使用指南
名称 (Name)	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
说明	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。

字段名称	使用指南
架构 (Schema)	您可以选择以下任一内置架构类型或创建自定义架构： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 您可以点击 Schema 旁边的箭头以查看架构详细信息。 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。
注释　仅当选择自定义架构时，才可以编辑以下字段。	
Subject Objectclass	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
主题名称属性 (Subject Name Attribute)	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。
组名称属性 (Group Name Attribute)	• CN：根据通用名称检索 LDAP 身份存储区组。 • DN：根据可分辨名称检索 LDAP 身份存储区组。
证书属性 (Certificate Attribute)	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
Group Objectclass	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。
组映射属性 (Group Map Attribute)	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 (Subject Objects Contain Reference To Groups)	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 (Group Objects Contain Reference To Subjects)	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 (Subjects in Groups Are Stored in Member Attribute As)	（仅适用于启用**组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects)** 选项时）指定在组成员属性中如何搜索成员，其默认值为 DN。

字段名称	使用指南
用户信息属性	默认情况下，预定义属性用于收集以下内置架构类型的用户信息（例如，名字、姓氏、电子邮件、电话，位置等）： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。 您还可以选择架构 (Schema) 下拉菜单中的定制 (Custom) 选项，根据要求编辑用户信息属性。

LDAP 连接设置

下表介绍**连接设置 (Connection Settings)** 选项卡中的字段。

表 ***80: LDAP*** 连接设置

字段名称	使用指南
启用辅助服务器 (Enable Secondary Server)	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器 (Primary and Secondary Servers)	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效 IP 地址。对于主机名，仅字母数字字符（a 至 z；A 至 Z；0 至 9）、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。
为每个 ISE 节点指定服务器	选中此复选框可配置每个 PSN 的主辅 LDAP 服务器主机名/IP 及其端口。 启用此选项后，将显示一个表，列出部署中的所有节点。您需要选择节点并配置主要和辅助 LDAP 服务器主机名/IP 及所选节点的端口。

字段名称	使用指南
访问	**匿名访问 (Anonymous Access)**：点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。 **身份验证访问 (Authenticated Access)**：点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员 DN”(Admin DN) 字段和“密码”(Password) 字段输入信息。
管理员 DN (Admin DN)	输入管理员的 DN。管理员 DN 是有权限搜索“用户目录子树”(User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。
安全身份验证 (Secure Authentication)	点击此字段以对Cisco ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口”(Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA”(LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 (Server Timeout)	以秒为单位输入Cisco ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 (Max. Admin Connections)	输入利用 LADP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于0）。这些连接用于在“用户目录子树”(User Directory Subtree) 和 “组目录子树”(Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
每 **N** 秒强制重新连接	选中此复选框并在**秒 (Seconds)** 字段中输入所需的值可强制服务器按照指定的时间间隔续订LDAP 连接。有效范围为 1 至 60 分钟。

字段名称	使用指南
测试与服务器的绑定 **(Test Bind to Server)**	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
Failover	
Always Access Primary Server First	如果您希望Cisco ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
...后故障恢复到主服务器 (Failback to Primary Server after)	如果Cisco ISE 尝试连接的主 LDAP 服务器无法访问，Cisco ISE 会尝试连接辅助 LDAP 服务器。如果您希望Cisco ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

LDAP 目录组织设置

下表介绍目录组织 **(Directory Organization)** 选项卡上的字段。

表 ***81: LDAP*** 目录组织设置

字段名称	使用指南
主题搜索库 **(Subject Search Base)**	输入包含所有主题的子树的 DN。例如： o=corporation.com 如果包含主题的树是基本 DN，请输入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
组搜索库 **(Group Search Base)**	输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com 如果包含组的树是基本 DN，请键入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。

字段名称	使用指南
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	输入一个MAC地址格式供Cisco ISE用于在LDAP数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当Cisco ISE 收到主机查找请求时，Cisco ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。 使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <*format*> 可以是以下任何一种格式： • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	输入适当的文本以删除用户名的域前缀。 如果Cisco ISE在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <start_string> 框中指定的多个字符，Cisco ISE会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则Cisco ISE 会向 LDAP 服务器提交 user1。 **注释** <start_string> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

字段名称	使用指南
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	输入适当的文本以删除用户名的域后缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，Cisco ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 *user1@domain*，则Cisco ISE 会向 LDAP 服务器提交 *user1*。 注释 <*end_string*> 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *82: LDAP* 组设置

字段名称	使用指南
添加	选择 **Add> 添加组**添加新组或从目录**中选择** Add> 选择 Group 选择组从 LDAP 目录。 如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。点击要选择的组旁边的复选框，然后点击**确定 (OK)**。选中的组将显示在**组 (Groups)** 窗口中。

LDAP 属性设置

表 *83: LDAP* 属性设置

字段名称	使用指南
添加	选择 **Add> 添加属性**添加新属性或从目录**中选择** Add> 选择属性从 LDAP 服务器的属性。 如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击**检索属性 (Retrieve Attributes)** 以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。

LDAP 高级设置

下表介绍“高级设置”(Advanced Settings) 选项卡中的字段。

表 *84: LDAP* 高级设置

字段名称	使用指南
启用密码更改 (Enable Password Change)	在使用 PAP 协议进行设备管理和使用 RADIUS EAP-GTC 协议进行网络访问时，选中此复选框可让用户在密码到期或重置密码的情况下更改密码。对于不受支持的协议，用户身份验证会失败。此选项还可以让用户在下次登录时更改密码。

相关主题

LDAP 目录服务，第 561 页
LDAP 用户身份验证，第 562 页
LDAP 用户查找，第 565 页
添加 LDAP 身份源，第 566 页

配置 LDAP 方案

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选择 LDAP 实例。

步骤 3 点击**常规**选项卡。

步骤 4 点击**方案 (Schema)** 选项旁的下拉箭头。

步骤 5 从**方案 (Schema)** 下拉列表中选择所需方案。可以根据需要选择**自定义 (Custom)** 选项。

预定义属性用于内置方案，例如 Active Directory、Sun directory Server、Novell eDirectory。如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。

配置主要和辅助 LDAP 服务器

在创建 LDAP 实例之后，您必须为主要 LDAP 服务器配置连接设置。配置辅助 LDAP 服务器为可选操作。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击 **Connection** 选项卡以配置主要和辅助服务器。

步骤 4 输入作为 LDAP 身份源设置中描述的值。

步骤 5 点击**提交 (Submit)** 保存连接参数。

允许思科 ISE 从 LDAP 服务器获取属性

为了让Cisco ISE 从 LDAP 服务器获取用户和组数据，您必须在Cisco ISE 中配置 LDAP 目录详细信息。对于 LDAP 身份源，适用以下三种搜索：

- 搜索组子树中的所有组用于管理
- 搜索主题子树中的用户以定位用户
- 搜索用户在其中为成员的组

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击 **Directory Organization** 选项卡。

步骤 4 输入作为 LDAP 身份源设置中描述的值。

步骤 5 点击**提交 (Submit)** 保存配置。

从 LDAP 服务器检索组成员身份详细信息

您可以添加新组或从 LDAP 目录选择组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击**组 (Groups)** 选项卡。

步骤 4 选择 **添加 (Add)** > **添加组 (Add Group)** 添加新组或选择 **添加 (Add)** > **从目录中选择组 (Select Groups From Directory)** 从 LDAP 目录中选择组。

a) 如果您选择添加组，请输入新组的名称。
b) 如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。搜索条件可以包含星号 (*) 通配符。

步骤 5 点击要选择的组旁边的复选框，然后点击**确定 (OK)**。

选择的组将显示在“组”(Groups) 页面。

步骤 6 点击**提交 (Submit)** 保存组选择。

注释 当 Active Directory 配置为思科 ISE 中的 LDAP 身份存储时，不支持 Active Directory 内置组。

从 LDAP 服务器检索用户属性

可以从 LDAP 服务器获取用户属性，以便在授权策略中使用。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

步骤 3 点击 **Attributes** 选项卡。

步骤 4 选择 **添加 (Add)** > **添加属性 (Add Attribute)** 添加新属性或选择 **添加 (Add)** > **从目录中选择属性 (Select Attributes From Directory)** 从 LDAP 服务器选择属性。

a) 如果选择添加属性，则为新属性输入名称。

b) 如果从目录选择，则输入示例用户，点击**检索属性 (Retrieve Attributes)**，检索用户的属性。可以使用星号 (*) 通配符。

Cisco ISE 允许您在手动添加属性类型 IP 时使用 IPv4 或 IPv6 地址配置 LADP 服务器以进行用户身份验证。

步骤 5 选中想要选择的属性旁边的复选框，然后点击**确定 (OK)**。

步骤 6 点击**提交 (Submit)**，保存属性选择。

使用 LDAP 身份源进行安全身份验证

在“LDAP 配置”(LDAP configuration) 页面上选择“安全身份验证”(Secure Authentication) 选项时，Cisco ISE 使用 SSL 保护与 LDAP 身份源的通信。通过以下方式建立到 LDAP 身份源的安全连接：

- SSL 隧道 - 使用 SSL v3 或 TLS v1（LDAP 服务器支持的最强大的版本）
- 服务器身份验证（LDAP 服务器身份验证）- 基于证书
- 客户端身份验证（Cisco ISE 身份验证）- 无（在 SSL 隧道中使用管理员绑定）
- 密码套件 - Cisco ISE 支持的所有密码套件

我们建议您使用带有Cisco ISE 支持的最强加密和密码的 TLS v1。

要使Cisco ISE 与 LDAP 身份源安全通信，请执行以下操作：

开始之前

- Cisco ISE 必须连接到 LDAP 服务器
- TCP 端口 636 应当开放

步骤 1 将向 LDAP 服务器颁发服务器证书的 CA 的完整证书颁发机构 (CA) 链导入Cisco ISE （**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）。

完整 CA 链指的是根 CA 和中级 CA 证书；不是 LDAP 服务器证书。

步骤 2 将Cisco ISE 配置为在与 LDAP 身份源通信时使用安全身份验证（**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**；务必选中“连接设置”(Connection Settings) 选项卡中的“安全身份验证”(Secure Authentication) 复选框）。

步骤 3 在 LDAP 身份存储区中选择根 CA 证书。

ODBC 身份源

您可以使用符合开放式数据库连接 (ODBC) 的数据库作为外部身份源，以便对用户和终端进行身份验证。ODBC 身份源可在身份存储区序列中使用，用于访客和发起人身份验证。它可以用于 BYOD 流。

支持以下数据库引擎：

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

配置Cisco ISE 对 ODBC 兼容数据库进行身份验证不会影响该数据库的配置。要管理您的数据库，请参阅您的数据库文档。

ODBC 数据库凭证检查

对于 ODBC 数据库，Cisco ISE 支持三种类型的凭证检查。您必须为每种凭证检查类型配置适当的 SQL 已存储程序。Cisco ISE 使用已存储程序在 ODBC 数据库中查询相应的表并接收 ODBC 数据库的输出参数或记录集。在响应 ODBC 查询时，该数据库会返回记录集或一组命名参数。

密码可以明文或加密格式存储在ODBC数据库中。当Cisco ISE 调用密码时，存储程序可以将密码解密为明文。

凭证检查类型	ODBC 输入参数	ODBC 输出参数	凭证检查	身份验证协议
ODBC 数据库中明文密码身份验证	用户名 密码	结果 Group 帐户信息 错误字符串	如果用户名和密码匹配，会返回相关用户信息。	PAP EAP-GTC（作为 PEAP或 EAP-FAST 的内部方法） TACACS

凭证检查类型	ODBC 输入参数	ODBC 输出参数	凭证检查	身份验证协议
从 ODBC 数据库获取明文密码	用户名	结果 Group 帐户信息 错误字符串 Password	如果找到用户名，存储程序会返回其密码和相关用户信息。Cisco ISE 基于身份验证方式计算密码散列值并将其与从客户端收到的值进行比较。	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2（作为 PEAP 或 EAP-FAST 的内部方法） TACACS
查询	用户名	结果 Group 帐户信息 错误字符串	如果找到用户名，则会返回相关用户信息。	MAB PEAP、EAP-FAST 和 EAP-TTLS 快速重连

注释 在Cisco ISE 中没有使用输出参数返回的组。在Cisco ISE 中只使用获取组 (Fetch Groups) 存储程序检索的组。该帐户信息仅包含在身份验证审核日志中。

下表列出了 ODBC 数据库存储过程返回的结果代码和Cisco ISE 身份验证结果代码之间的映射：

结果代码（由存储过程返回）	说明	Cisco ISE 身份验证结果代码
0	CODE_SUCCESS	NA（身份验证已通过）
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	失败
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

注释 思科 ISE 根据此映射的身份验证结果代码执行实际身份验证或查找操作。

您可以使用该存储程序从 ODBC 数据库中获取组和属性。

返回用于明文密码身份验证的记录集的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset] @username varchar(64), @password
 varchar(255) AS BEGIN IF EXISTS( SELECT username FROM NetworkUsers WHERE username = @username
 AND password = @password ) SELECT 0,11,'give full access','No Error' FROM NetworkUsers
WHERE username = @username ELSE SELECT 3,0,'odbc','ODBC Authen Error' END
```

返回用于获取明文密码的记录集的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset] @username varchar(64) AS BEGIN
IF EXISTS( SELECT username FROM NetworkUsers WHERE username = @username) SELECT 0,11,'give
 full access','No Error',password FROM NetworkUsers WHERE username = @username ELSE SELECT
 3,0,'odbc','ODBC Authen Error' END
```

返回用于查找的记录集的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset] @username varchar(64) AS BEGIN IF
EXISTS( SELECT username FROM NetworkUsers WHERE username = @username) SELECT 0,11,'give
full access','No Error' FROM NetworkUsers WHERE username = @username ELSE SELECT
3,0,'odbc','ODBC Authen Error' END
```

返回用于明文密码身份验证的参数的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters] @username varchar(64), @password
 varchar(255), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT,
 @errorString varchar(255) OUTPUT AS BEGIN IF EXISTS( SELECT username FROM NetworkUsers
WHERE username = @username AND password = @password ) SELECT @result=0, @group=11,
@acctInfo='give full access', @errorString='No Error' FROM NetworkUsers WHERE username =
@username ELSE SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen
Error' END
```

返回用于获取明文密码的参数的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters] @username varchar(64), @result
INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString
varchar(255) OUTPUT, @password varchar(255) OUTPUT AS BEGIN IF EXISTS( SELECT username FROM
 NetworkUsers WHERE username = @username) SELECT @result=0, @group=11, @acctInfo='give full
 access', @errorString='No Error', @password=password FROM NetworkUsers WHERE username =
@username ELSE SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen
Error' END
```

返回用于查找的参数的示例程序（适用于 Microsoft SQL Server）

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters] @username varchar(64), @result INT
 OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255)
 OUTPUT AS BEGIN IF EXISTS( SELECT username FROM NetworkUsers WHERE username = @username)
SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error' FROM
NetworkUsers WHERE username = @username ELSE SELECT @result=3, @group=0, @acctInfo='odbc',
 @errorString='ODBC Authen Error' END
```

从 Microsoft SQL Server 获取组的示例程序

```
CREATE PROCEDURE [dbo].[ISEGroupsH] @username varchar(64), @result int output AS BEGIN if
exists (select * from NetworkUsers where username = @username) begin set @result = 0 select
 'accountants', 'engineers', 'sales','test_group2' end else set @result = 1 END
```

当用户名为 "*" 时，获取所有用户的所有组的示例程序（适用于 Microsoft SQL Server）

```
ALTER PROCEDURE [dbo].[ISEGroupsH] @username varchar(64), @result int output AS BEGIN if
@username = '*' begin -- if username is equal to '*' then return all existing groups set
```

```
@result = 0 select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4' end else if exists (select
 * from NetworkUsers where username = @username) begin set @result = 0 select 'accountants'
 end else set @result = 1 END
```

从 Microsoft SQL Server 获取属性的示例程序

```
CREATE PROCEDURE [dbo].[ISEAttrsH] @username varchar(64), @result int output AS BEGIN if
exists (select * from NetworkUsers where username = @username) begin set @result = 0 select
 phone as phone, username as username, department as department, floor as floor, memberOf
as memberOf, isManager as isManager from NetworkUsers where username = @username end else
set @result = 1 END
```

ODBC 配置的其他示例

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

添加 ODBC 身份源

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 点击 **ODBC**。

步骤 3 点击**添加 (Add)**。

步骤 4 在**常规** (General) 选项卡，请输入 ODBC 身份源的名称和说明。

步骤 5 在**连接 (Connection)** 选项卡中，输入以下详细信息：

- ODBC 数据库的主机名或 IP 地址。如果对数据库使用非标准 TCP 端口，则可以使用以下格式指定端口号：主机名或 IP 地址端口:端口
- ODBC 数据库名称
- 管理员用户名和密码（Cisco ISE 使用这些凭证连接到数据库）
- 服务器超时（单位：秒；默认为 5 秒）
- 连接尝试（默认为 1）
- 数据库类型。选择以下其中一个选项：
  - **MySQL**
  - **Oracle**
  - **PostgreSQL**

- **Microsoft SQL Server**
- **Sybase**

步骤 6 点击**测试连接 (Test Connection)** 以检查与 ODBC 数据库的连接，并且对于已配置的使用案例验证是否存在已存储程序。

步骤 7 在已存储程序 (**Stored Procedures**) 选项卡，输入以下详细信息：

- **已存储程序类型 (Stored Procedure Type)**：选择您数据库支持的输出类型。
  - **返回记录集 (Returns Recordset)**：数据库返回记录集以响应 ODBC 查询。
  - **返回参数 (Returns Parameters)**：数据库返回一组具名参数以响应 ODBC 查询。
- **明文密码身份验证 (Plain Text Password Authentication)**：输入在 ODBC 服务器上运行的已存储程序的名称，该已存储程序用于明文密码身份验证。用于 PAP、EAP-GTC 内部方法和 TACACS。
- **明文密码获取 (Plain Text Password Fetching)**：输入在 ODBC 服务器上运行的、用于获取明文密码的已存储程序的名称。用于 CHAP、MS CHAPv1/v2、LEAP、EAP-MD5、EAP-MSCHAPv2 内部方法和 TACACS。
- **检查存在用户名或机器 (Check Username or Machine Exists)**：输入在 ODBC 服务器上运行的、用于用户/MAC 地址查询的已存储程序的名称。用于 MAB 和 PEAP、EAP-FAST和EAP-TTLS 快速重连。
- **获取组 (Fetch Groups)**：输入从 ODBC 数据库中检索组的已存储程序的名称。
- **获取属性 (Fetch Attributes)**：输入从 ODBC 数据库中检索属性及其值的已存储程序的名称。
- **高级设置 (Advanced Settings)**：点击此选项可使用以下字词典下的属性作为**获取属性 (Fetch Attributes)** 已存储程序中的输入参数（除了用户名和密码）：
  - **RADIUS**
  - **设备**
  - **网络接入**

  注释 只能在**网络访问 (Network Access)** 字典中使用以下属性：**AuthenticationMethod**、**设备 IP 地址 (Device IP Address)**、**EapAuthentication**、**EapTunnel**、**ISE 主机名 (ISE Host Name)**、**协议 (Protocol)**、**用户名 (UserName)**、**VN** 和 **WasMachineAuthenticated**。

  在**已存储程序中的属性名称 (Attribute Name in Stored Procedure)** 字段中，指定已存储程序中使用的属性名称。

  您可以将已存储程序配置为从 ODBC 数据库检索以下输出参数：
  - ACL
  - 安全组
  - VLAN（名称或编号）
  - Web 重定向 ACL

- Web 重定向门户名称

您可以使用这些属性配置授权配置文件。这些属性列在**授权配置文件 (Authorization Profiles)** 窗口的**常见任务 (Common Tasks)** 部分中（在**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results)** 下）。以下是一些可以使用这些属性的用例场景：

- 根据指定的输入属性（MAC 地址、用户名、呼叫站 ID 或设备位置），配置授权配置文件以使用从 ODBC 数据库返回的 VLAN，而不是手动为每个授权配置文件指定 VLAN 。
- 配置授权配置文件，阻止在 ODBC 身份存储区中被阻止的呼叫站 ID 的访问。
- 配置授权配置文件，根据 MAC 地址、用户名、呼叫站 ID 或设备位置从 ODBC 数据库检索 Web 重定向 ACL 或 Web 重定向门户名称。

在配置授权策略时，可以在**策略集 (Policy Sets)** 窗口中选择从 ODBC 数据库检索的安全组。

注释 使用**高级设置 (Advanced Settings)** 选项时，会在 ODBC 数据库中创建名为 user_attributes_detail 的新表来存储其他详细信息。您必须将所有输出参数的数据类型设置为 VARCHAR2。否则，已存储程序可能会在合并和编译过程中失败。例如，如果将 SGTNAME 设置为 VARCHAR2 并将 VLANNUMBER 设置为 NUMBER，则编译以下已存储程序时可能会失败：

```
select ATTR_NAME, value from ATTRIBUTES where user_id=userid union select 'SGTNAME', SGTNAME
 from user_attributes_detail where USER_ID = userid and
user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE union select 'VLANNUMBER', VLANNUMBER
 from user_attributes_detail where USER_ID = userid and
user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE;
```

- **搜索格式 MAC 地址 (Search for MAC Address in Format)**：根据所选的 MAC 格式对接收的 MAC 地址进行标准化处理。

步骤 8 在**属性 (Attributes)** 选项卡中，添加所需的属性。在添加属性时，您可以指定属性名称在授权策略规则中的显示方式。

您还可以从 ODBC 数据库获取属性。这些属性可在授权策略中使用。

步骤 9 在**组 (Groups)** 选项卡中，添加用户组。您可以通过指定用户名或 MAC 地址从 ODBC 数据库获取组。这些组可在授权策略中使用。

您可以对组和属性进行重命名。默认情况下，**ISE 中名称 (Name in ISE)** 字段中显示的名称与 ODBC 数据库中的名称相同，但是，您可以修改此名称。此名称在授权策略中使用。

步骤 10 点击**提交 (Submit)**。

有关如何配置 ODBC 身份源的详细信息，请参阅以下链接：

- 在采用 Oracle 数据库的思科 ISE 上配置 ODBC
- 使用 ODBC 配置采用 MS SQL 的思科 ISE
- 在采用 PostgreSQL 的思科 ISE 上配置 ODBC
- 配置思科 ISE 以与 MySQL 服务器集成

注释 如果已配置输入属性，则必须在复制 ODBC 身份存储区时执行以下操作。否则，输入参数可能会在复制的 ODBC 身份存储区中丢失。

1. 点击**高级设置 (Advance Settings)**。
2. 验证输入参数是否设置正确。
3. 点击**确定 (OK)** 以将这些输入参数保存在复制的 ODBC 身份存储区中。

RADIUS 令牌身份源

支持 RADIUS 协议并向用户和设备提供身份验证、授权和记账 (AAA) 服务的服务器称为 RADIUS 服务器。RADIUS 身份源只是一个外部身份源，包含一系列的主题及其凭证，使用 RADIUS 协议进行通信。例如，Safeword 令牌服务器是一个身份源，可以包含若干用户以及作为一次性密码的凭证，提供一个您可以使用 RADIUS 协议查询的界面。

Cisco ISE 支持任何符合 RADIUS RFC 2865 的服务器作为外部身份源。Cisco ISE 支持多个 RADIUS 令牌服务器身份，例如 RSA SecurityID 服务器和 SafeWord 服务器。RADIUS 身份源可以与任何用于验证用户的 RADIUS 令牌服务器配合使用。

注释 必须为 MAB 身份验证启用“处理主机查找”(Process Host Lookup) 选项。我们建议不要为 MAB 身份验证配置用作外部身份源的 RADIUS 令牌服务器，因为使用 MAB 身份验证的设备无法生成 OTP 或 RADIUS 令牌（这是 RADIUS 令牌服务器身份验证所需的）。因此，身份验证将失败。您可以使用外部 RADIUS 服务器选项来处理 MAB 请求。

支持 RADIUS 令牌服务器的身份验证协议

对于 RADIUS 身份源，Cisco ISE 支持以下身份验证协议：

- RADIUS PAP
- 使用内部可扩展身份验证协议 - 通用令牌卡 (EAP-GTC) 的受保护的可扩展身份验证协议 (PEAP)
- 使用内部 EAP-GTC 的 EAP-FAST

RADIUS 令牌服务器用于通信的端口

RADIUS 令牌服务器将 UDP 端口用于身份验证会话。此端口用于所有 RADIUS 通信。为了让Cisco ISE 将 RADIUS 一次性密码 (OTP) 消息发送到已启用 RADIUS 的令牌服务器，必须确保Cisco ISE 和已启用 RADIUS 的令牌服务器之间的网关设备能够通过 UDP 端口进行通信。您可以通过管理员门户配置 UDP 端口。

RADIUS 共享密钥

您在Cisco ISE 中配置 RADIUS 身份源时必须提供共享密钥。此共享密钥应与 RADIUS 令牌服务器上配置的共享密钥相同。

RADIUS 令牌服务器中的故障转移

Cisco ISE 允许您配置多个 RADIUS 身份源。每个 RADIUS 身份源可以使用 RADIUS 主服务器和辅助服务器。当Cisco ISE 无法连接到主服务器时，则会使用辅助服务器。

RADIUS 令牌服务器中的可配置密码提示

RADIUS 身份源允许您配置密码提示。您可以通过管理员门户配置密码提示。

RADIUS 令牌服务器用户身份验证

Cisco ISE 会获取用户凭证（用户名和密码）并将这些凭证发送到 RADIUS 令牌服务器。Cisco ISE 还会将 RADIUS 令牌服务器身份验证处理的结果中继到用户。

RADIUS 令牌服务器中的用户属性缓存

默认情况下，RADIUS 令牌服务器不支持用户查找。但是，用户查找功能对于以下Cisco ISE 功能非常重要。

- PEAP 会话恢复：此功能允许在建立 EAP 会话期间在身份验证成功之后恢复 PEAR 会话。
- EAP/FAST 快速重新连接：此功能允许在建立 EAP 会话期间在身份验证成功之后快速进行重新连接。
- TACACS+ 授权：在 TACACS+ 身份验证成功后发生。

Cisco ISE 缓存成功的身份验证的结果以为这些功能处理用户查找请求。对于每次成功的身份验证，系统会缓存经过身份验证的用户的名称和所检索的属性。失败的身份验证不写入缓存。

在运行时内存中可提供缓存，在分布式部署中不可在Cisco ISE 节点之间进行复制。您可以通过 Admin 门户为缓存配置有效时间 (TTL) 限制。从 ISE 2.6 开始，您可以选择启用身份缓存选项并以分钟为单位设置老化时间。该选项默认被禁用，启用之后，在指定的持续时间里，可在内存中使用缓存。

身份序列中的 RADIUS 身份源

您可以在身份源序列中添加身份验证序列的 RADIUS 身份源。但是，由于您无法查询不带身份验证的 RADIUS 身份源，因此无法添加属性检索序列的 RADIUS 身份源。Cisco ISE 在使用 RADIUS 服务器进行身份验证时无法区分不同的错误。RADIUS 服务器针对所有错误都返回 Access-Reject 消息。例如，当在 RADIUS 服务器中找不到用户时，RADIUS 服务器会返回 Access-Reject 消息，而不是返回 User Unknown 状态。

RADIUS 服务器为所有错误返回相同消息

当在 RADIUS 服务器中未找到某名用户时，RADIUS 服务器会返回一条访问 - 拒绝消息。Cisco ISE 提供一个选项可通过管理员门户配置此消息，显示为身份验证失败或未找到用户的消息。但是，对于用户未知和所有失败的情况，此选项均会返回一条未找到用户的消息。

下表列出 RADIUS 身份服务器可能出现的各种失败情况。

表 *85*: 错误处理

失败情况	失败的原因
身份验证失败	• 用户未知。 • 用户尝试使用错误的验证码登录。 • 用户登录时长过期。
处理失败	• RADIUS 服务器在Cisco ISE 中配置错误。 • RADIUS 服务器不可用。 • 检测到 RADIUS 包错误。 • 发送或接收 RADIUS 服务器包期间出现问题。 • 超时。
未知用户	身份验证失败，并且 Fail on Reject 选项设置为 False。

Safeword 服务器支持特殊用户名格式

Safeword 令牌服务器支持使用以下用户名格式进行身份验证：

Username—Username, OTP

Cisco ISE 一收到身份验证请求，便会解析用户名并将其转换为以下用户名：

Username—Username

SafeWord 令牌服务器同时支持这两种格式。Cisco ISE 适用于各种令牌服务器。在配置 SafeWord 服务器时，您必须选中Cisco ISE 的管理门户中的 SafeWord Server 复选框，以解析用户名并将其转换为指定格式。在将请求发送到 RADIUS 令牌服务器之前，系统会在 RADIUS 令牌服务器身份源中执行此转换。

RADIUS 令牌服务器中的身份验证请求和响应

当Cisco ISE 向支持 RADIUS 的令牌服务器转发身份验证请求时，RADIUS 身份验证请求包含以下属性：

- 用户名（RADIUS 属性 1）
- 用户密码（RADIUS 属性 2）
- NAS IP 地址（RADIUS 属性 4）

Cisco ISE 预期收到以下任一响应：

- 接受访问 - 无需任何属性，但是响应可能包含根据 RADIUS 令牌服务器配置的各种属性。
- 拒绝访问 - 无需任何属性。
- 质询访问 - 每个 RADIUS RFC 所需的属性如下：
  - 状态（RADIUS 属性 24）
  - 回复信息（RADIUS 属性 18）
  - 以下一个或多个属性：供应商特定、空闲超时（RADIUS 属性 28）、会话超时（RADIUS 属性 27）、代理状态（RADIUS 属性 33）

    质询访问中不允许使用任何其他属性。

RADIUS 令牌身份源设置

下表介绍“RADIUS 令牌身份源”(Token Identity Sources) 窗口上的字段，您可以使用此窗口配置和连接外部 RADIUS 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

表 *86: RADIUS* 令牌身份源设置

字段名称	使用指南
名称	输入RADIUS 令牌服务器名称。允许的最大字符数为 64。
说明	输入RADIUS 令牌服务器说明。允许的最大字符数为 1024。
SafeWord Server	如果 RADIUS 身份源为 SafeWord 服务器，请选中此复选框。

字段名称	使用指南
Enable Secondary Server	选中此复选框，为Cisco ISE 启用辅助 RADIUS 令牌服务器，在主要服务器发生故障时用作备份。如果选中此复选框，必须配置辅助 RADIUS 令牌服务器。
Always Access Primary Server First	如果希望Cisco ISE 总是首先访问主服务器，请点击此选项。
Fallback to Primary Server after	点击此选项可指定在无法连接主服务器时，Cisco ISE 能够在多长时间里（分钟）使用辅助 RADIUS 令牌服务器进行身份验证。这段时间过后，Cisco ISE 重新尝试对照主服务器进行身份验证。
主服务器	
Host IP	输入主要 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在主要 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入主要 RADIUS 令牌服务器侦听的端口号。
Server Timeout	指定Cisco ISE 在确定主服务器关闭之前，等待主要 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在迁移到辅助服务器（如果已定义）或放弃请求（如果未定义辅服务器）之前，尝试重新连接到主服务器的次数。
辅助服务器	
Host IP	输入辅助 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在辅助 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入辅助 RADIUS 令牌服务器侦听的端口号。有效值为 1 至 65535。默认值为 1812。
Server Timeout	指定Cisco ISE 在确定辅助服务器关闭之前，等待辅助 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在放弃请求之前应当尝试重新连接辅助服务器的次数。

相关主题

RADIUS 令牌身份源，第 582 页
添加 RADIUS 令牌服务器，第 587 页

添加 RADIUS 令牌服务器

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)** > **添加 (Add)**。

步骤 2 在 **General** 和 **Connection** 选项卡中输入值。

步骤 3 点击 **Authentication** 选项卡。

通过此选项卡，您可以控制 RADIUS 令牌服务器对 Access-Reject 消息的响应。此响应可能意味着凭证无效或用户未知。Cisco ISE 收到以下其中一个响应：Failed authentication 或 User not found。通过此选项卡，您可以启用身份缓存和设置缓存的老化时间。您还可以配置请求密码的提示。

a) 如果您要将从 RADIUS 令牌服务器收到的 Access-Reject 响应处理为失败身份验证，请点击**将拒绝视为“身份验证失败”(Treat Rejects as ‘authentication failed’)** 单选按钮。

b) 如果您要将从 RADIUS 令牌服务器收到的 Access-Reject 响应处理为未知用户失败，请点击**将拒绝视为“未找到用户”(Treat Rejects as ‘user not found’)** 单选按钮。

步骤 4 如果您希望Cisco ISE 在使用 RADIUS 令牌服务器进行首次成功身份验证后将密码存储在缓存中，并为后续身份验证使用缓存的用户凭证（如果它们在配置的时间段内发生），请选中**启用密码缓存 (Enable Passcode Caching)** 复选框。

在**老化时间 (Aging Time)** 字段输入密码必须在缓存中存储的秒数。在此时间段内，用户可以使用同一密码执行多个身份验证。默认值为 30 秒。有效范围是从 1 到 300 秒。

注释 Cisco ISE 在首次身份验证失败后清除缓存。用户必须输入新的有效密码。

注释 我们强烈建议您仅在支持密码加密的协议（例如，EAP-FAST-GTC）中启用此选项。有关 RADIUS 令牌服务器支持的身份验证协议的信息，请参阅 支持 RADIUS 令牌服务器的身份验证协议，第 582 页

步骤 5 如果要允许处理没有在服务器上执行身份验证的请求，请选中**启用身份缓存 (Enable Identity Caching)** 复选框。

您可以启用身份缓存选项并以分钟为单位设置老化时间。默认值为 120 分钟。有效范围为 1 至 1440 分钟。从上次成功的身份验证中获得的结果和属性将在缓存中保留指定的时长。

默认情况下该选项处于禁用状态。

步骤 6 点击 **Authorization** 选项卡。

通过此选项卡，您可以配置该属性的显示名称。该属性是 RADIUS 令牌服务器向Cisco ISE 发送 Access-Accept 响应时返回的属性。此属性可用于授权策略条件。默认值为 CiscoSecure-Group-Id。

注释　如果要从外部 ID 源发送 Access-Accept 中的任何属性，则外部 ID 源需要发送 <ciscoavpair> 作为属性名称，值格式为 ACS:<attrname>=<attrvalue>，其中 <attrname> 是在**授权 (Authorization)** 选项卡中配置的。

步骤 7 点击**提交 (Submit)**。

删除 RADIUS 令牌服务器

开始之前

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 确保您未选择身份源序列中的 RADIUS 令牌服务器。如果您选择身份源序列中的 RADIUS 令牌服务器，删除操作将失败。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

步骤 2 选中要删除的 RADIUS 令牌服务器旁边的复选框，然后点击 **Delete**。

步骤 3 点击**确定 (OK)** 以删除您已选择的 RADIUS 令牌服务器。

如果您选择删除多个RADIUS令牌服务器，且其中一个服务器用于身份源序列，则删除操作将失败，任何RADIUS令牌服务器都不会被删除。

RSA 身份源

Cisco ISE 支持 RSA SecurID 服务器作为外部数据库。RSA SecurID 双因素身份验证由用户的 PIN 和单独注册的 RSA SecurID 令牌组成，该令牌基于时间代码算法生成一次性令牌代码。其他令牌代码按固定时间间隔（通常每 30 或 60 秒）生成。RSA SecurID 服务器会验证此动态身份验证代码。每个 RSA SecurID 令牌都是唯一的，并且无法根据以往令牌预测未来令牌的值。因此，在提供正确的令牌代码与 PIN 时，大致可以确定该人员是有效用户。因此，RSA SecurID 服务器提供的身份验证机制比传统可重用密码更可靠。

Cisco ISE 支持以下 RSA 身份源：

- RSA ACE/Server 6.x 系列
- RSA Authentication Manager 7.x 和 8.0 系列

您可以通过以下任何一种方式与 RSA SecurID 身份验证技术集成：

- 使用 RSA SecurID 代理 - 用户通过 RSA 本地协议使用其用户名和密码进行身份验证。
- 使用 RADIUS 协议 - 用户通过 RADIUS 协议使用其用户名和密码进行身份验证。

Cisco ISE 中的 RSA SecurID 令牌服务器通过使用 RSA SecurID 代理与 RSA SecurID 身份验证技术相连接。

Cisco ISE 仅支持一个 RSA 领域。

思科 ISE 和 RSA SecurID 服务器集成

以下是将Cisco ISE 与 RSA SecurID 服务器连接所涉及的两个管理角色：

- RSA 服务器管理员 - 配置和维护 RSA 系统与集成
- Cisco ISE 管理员 - 将Cisco ISE 配置为连接到 RSA SecurID 服务器并维护配置

本节介绍将Cisco ISE 与 RSA SecurID 服务器连接作为外部身份源所涉及的流程。有关 RSA 服务器的更多信息，请参考 RSA 文档。

思科 ISE 中的 RSA 配置

RSA 管理系统生成 sdconf.rec 文件，RSA 系统管理员将为您提供此文件。您可以通过此文件在领域中添加Cisco ISE 服务器作为 RSA SecurID 代理。您必须浏览至此文件并将其添加至Cisco ISE 中。通过复制过程，主要Cisco ISE 服务器将此文件分发至所有辅助服务器。

针对 RSA SecurID 服务器进行的 RSA 代理身份验证

在所有Cisco ISE 服务器上安装 sdconf.rec 文件之后，RSA 代理模块进行初始化，并且每个Cisco ISE 服务器上都将使用 RSA 生成的凭证进行身份验证。在部署中的每个Cisco ISE 服务器上的代理都成功通过身份验证之后，RSA 服务器和代理模块将一起下载 securid 文件。此文件位于Cisco ISE 文件系统中，而且是在 RSA 代理定义的已知位置。

思科 ISE 分布式环境中的 RSA 身份源

管理分布式Cisco ISE 环境中的 RSA 身份源涉及以下操作：

- 将主服务器上的 sdconf.rec 和 sdopts.rec 文件分布到辅助服务器。
- 删除 securid 和 sdstatus.12 文件。

思科 ISE 部署中的 RSA 服务器更新

在Cisco ISE 中添加 sdconf.rec 文件后，RSA SecurID 管理员可能在停用 RSA 服务器或添加新的 RSA 辅助服务器时更新 sdconf.rec 文件。RSA SecurID 管理员将为您提供更新的文件。您可以使用更新的文件重新配置Cisco ISE。在Cisco ISE 中的复制流程将更新的文件分布到部署中的辅助Cisco ISE 服务器。Cisco ISE 首先更新文件系统中的文件，然后与 RSA 代理模块协调，酌情逐步执行重启流程。更新 sdconf.rec 文件时，将重置（删除）sdstatus.12 和 securid 文件。

覆盖自动 RSA 路由

一个领域中可以有不止一个 RSA 服务器。sdopts.rec 文件执行负载均衡器的职责。Cisco ISE 服务器和 RSA SecurID 服务器通过代理模块运行。位于Cisco ISE 上的代理模块维护一分基于成本的路由表

以充分利用领域中的 RSA 服务器。但是，您可以通过 Admin 门户使用名称为 sdopts.rec 的文本文件为该领域的每个Cisco ISE 服务器进行手动配置，以选择覆盖此路由。有关如何创建此文件的信息，请参阅 RSA 文档。

RSA 节点密钥重置

SecurID 文件是秘密节点密钥文件。RSA 经过初始设置后，会使用密钥验证代理。位于Cisco ISE 中的 RSA 代理第一次成功对 RSA 服务器进行身份验证后，会在客户端计算机上创建一个名为 SecurID 的文件，并会使用该文件确保在设备之间交换的数据有效。有时，可能必须从部署中的特定Cisco ISE 服务器或一组服务器中删除 SecurID 文件（例如，在 RSA 服务器上重置密钥之后）。可以使用 Cisco ISE 管理门户从该领域的Cisco ISE 服务器中删除此文件。Cisco ISE 中的 RSA 代理在下一次成功进行身份验证时，会创建新的 SecurID 文件。

注释 如果在升级到最新版本的思科 ISE 之后，身份验证失败，请重置 RSA 密钥。

RSA 自动可用性重置

sdstatus.12 文件提供有关领域中的 RSA 服务器可用性的信息。例如，它提供有关哪些服务器处于活动状态和哪些已关闭的信息。代理模块与领域中的 RSA 服务器协作维护此可用性状态。此信息在 sdstatus.12 文件中连续列出，此文件位于Cisco ISE 文件系统中的常见位置。有时，此文件会变成旧文件，而当前状态未反映在此文件中。您必须删除此文件，以便可以重新创建当前状态。您可以使用管理门户从特定领域的特定Cisco ISE 服务器中删除此文件。Cisco ISE 与 RSA 代理协调并确保正确的重新启动阶段化。

每当重置 securid 文件或者更新 sdconf.rec 或 sdopts.rec 文件时，便会删除 sdstatus.12 文件。

RSA SecurID 身份源设置

下表介绍“RSA SecurID 身份源”(RSA SecurID Identity Sources) 窗口上的字段，您可以使用此窗口创建和连接 RSA SecurID 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 ***87: RSA*** 提示设置

字段名称	使用指南
Enter Passcode Prompt	输入文本字符串以获取密码。
Enter Next Token Code	输入文本字符串以请求下一个令牌。
Choose PIN Type	输入文本字符串以请求 PIN 类型。

字段名称	使用指南
Accept System PIN	输入文本字符串以接受系统生成的 PIN。
Enter Alphanumeric PIN	输入文本字符串以请求字母数字 PIN。
Enter Numeric PIN	输入文本字符串以请求数字 PIN。
Re-enter PIN	输入文本字符串以请求用户重新输入 PIN。

RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 ***88: RSA*** 消息设置

字段名称	使用指南
Display System PIN Message	输入文本字符串以编辑系统 PIN 消息。
Display System PIN Reminder	输入文本字符串以通知用户记住新 PIN。
Must Enter Numeric Error	输入一条消息，指导用户仅输入数字作为 PIN。
Must Enter Alpha Error	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
PIN Rejected Message	输入在系统拒绝用户的 PIN 时用户所看到的消息。
User Pins Differ Error	输入在用户输入错误 PIN 时所看到的消息。
System PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
Bad Password Length Error	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

相关主题

RSA 身份源， 第 588 页
思科 ISE 和 RSA SecurID 服务器集成， 第 589 页
添加 RSA 身份源， 第 592 页

添加 RSA 身份源

要创建 RSA 身份源，必须导入 RSA 配置文件 (sdconf.rec)。必须从 RSA 管理员那里获取 sdconf.rec 文件。要执行此任务，您必须是超级管理员或系统管理员。

添加 RSA 身份源需要执行以下任务：

导入 RSA 配置文件

必须导入 RSA 配置文件，才能在Cisco ISE 中添加 RSA 身份源。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID** > **添加 (Add)**。

步骤 2 点击**浏览 (Browse)**，从正运行客户端浏览器的系统中选择新建或更新的 sdconf.rec 文件。

首次创建 RSA 身份源时，Import new sdconf.rec file 字段为必填字段。从那以后，可以用更新的 sdconf.rec 文件替换现有的 sdconf.rec 文件，但替换现有文件是可选操作。

步骤 3 以秒为单位输入服务器超时值。在超时之前，Cisco ISE 将在指定的时间内等待 RSA 服务器做出响应。该值可以是 1 至 199 之间的任意整数。默认值为 30 秒。

步骤 4 PIN 发生更改时，选中 **Reauthenticate on Change PIN** 复选框，强制执行重新验证。

步骤 5 点击**保存 (Save)**。

Cisco ISE 也支持以下场景：

- 为Cisco ISE 服务器配置选项文件，重置 SecurID 和 sdstatus.12 文件。
- 为 RSA 身份源配置身份验证控制选项。

为思科 ISE 服务器配置选项文件并重置 SecurID 和 sdstatus.12 文件

步骤 1 登录Cisco ISE 服务器。

步骤 2 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID** > **添加 (Add)**。

步骤 3 点击 **RSA Instance Files** 选项卡。

此页面列出您的部署中所有Cisco ISE 服务器的 sdopts.rec 文件。

当用户经过 RSA SecurID 令牌服务器的身份验证后，节点密钥状态会显示为已创建 *(Created)*。节点密钥状态可为以下其中一种：“已创建”(Created) 或“未创建”(Not Created)。清除节点密钥状态后，它会显示为未创建 *(Not Created)*。

步骤 4 点击特定Cisco ISE 服务器 sdopts.rec 文件旁边的单选按钮，然后点击 **Update Options File**。

Current File 区域会显示现有文件。

步骤 5 选择如下选项之一：

- Use the Automatic Load Balancing status maintained by the RSA agent - 如果希望 RSA 代理自动管理负载均衡，请选择此选项。
- Override the Automatic Load Balancing status with the sdopts.rec file selected below - 如果想要根据您的具体需求手动配置负载均衡，请选择此选项。如果选择此选项，则必须点击**浏览 (Browse)**，然后从运行客户端浏览器的系统选择新的 sdopts.rec 文件。

步骤 6 点击**确定 (OK)**。

步骤 7 点击与Cisco ISE 服务器对应的行以重置该服务器的 securid 和 sdstatus.12 文件：

a) 点击下拉箭头，然后在“重置 securid 文件”(Reset securid File) 列和“重置 sdstatus.12 文件”(Reset sdstatus.12 File) 列中选择**提交时删除 (Remove on Submit)**。

注释 Reset sdstatus.12 File 字段隐藏在您的视线之外。在最内部的框中使用垂直和水平滚动条，向下滚动，然后向右滚动以查看此字段。

b) 在此行中点击**保存 (Save)** 以保存更改。

步骤 8 点击**保存 (Save)**。

为 RSA 身份源配置身份验证控制选项

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID** > **添加 (Add)**。

步骤 2 点击 **Authentication Control** 选项卡。

步骤 3 选择如下选项之一：

- Treat Rejects as "authentication failed" - 如果您希望将拒绝的请求视为失败的身份验证，请选择此选项。
- Treat Rejects as "user not found" - 如果您希望将拒绝的请求视为“未找到用户”错误，请选择此选项。

步骤 4 如果希望Cisco ISE 在第一次身份验证成功后在缓存中存储密码，并为在配置的时间段内发生的后续身份验证使用缓存的用户凭据，请选中**启用密码缓存 (Enable Passcode Caching)** 复选框。

在**老化时间 (Aging Time)** 字段输入密码必须在缓存中存储的秒数。在此时间段内，用户可以使用同一密码执行多个身份验证。默认值为 30 秒。有效范围是从 1 到 300 秒。

注释 Cisco ISE 在首次身份验证失败后清除缓存。用户必须输入新的有效密码。

注释 我们强烈建议您仅在支持密码加密的协议（例如，EAP-FAST-GTC）中启用此选项。

步骤 5 如果要允许处理没有在服务器上执行身份验证的请求，请选中**启用身份缓存 (Enable Identity Caching)** 复选框。

您可以启用身份缓存选项并以分钟为单位设置老化时间。默认值为 120 分钟。有效范围为 1 至 1440 分钟。从上次成功的身份验证中获得的结果和属性将在缓存中保留指定的时长。

默认情况下该选项处于禁用状态。

步骤 6 点击**保存 (Save)** 保存配置。

配置 RSA 提示

Cisco ISE 允许您配置系统在处理发送给 RSA SecurID 服务器的请求时向用户显示的 RSA 提示。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

步骤 2 点击 **Prompts**。

步骤 3 输入“RSA SecurID 身份源设置”中所述的值。

步骤 4 点击**提交 (Submit)**。

配置 RSA 消息

通过Cisco ISE，您可以配置在处理发送到 RSA SecurID 服务器的请求时向用户显示的消息。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

步骤 2 点击 **Prompts**。

步骤 3 点击 **Messages** 选项卡。

步骤 4 输入“RSA SecurID 身份源设置”中所述的值。

步骤 5 点击**提交 (Submit)**。

SAMLv2 身份提供者作为外部身份源

安全断言标记语言 (SAML) 是基于 XML 的开放标准数据格式，可让管理员在登录到其中一个应用后能够无缝访问定义的一组应用。SAML 描述了受信任的业务合作伙伴之间安全相关信息的交换。SAML 实现了身份提供者 (IdP) 和服务提供者（在这里是指 ISE）之间安全身份验证信息的交换。

SAML 单点登录 (SSO) 在调配过程中通过在 IdP 和服务提供者之间交换元数据和证书建立信任圈 (CoT)。服务提供者信任 IdP 的用户信息，提供对各种服务或应用的访问权限。

启用 SAML SSO 可提供以下优势：

- 无需输入不同的用户名和密码组合，降低了密码管理难度。
- 由于重新输入同一身份的凭证所需的时间减少，提高了效率。
- 将身份验证从托管应用的系统转移到第三方系统。
- 降低成本，由于请求重置密码的服务中心呼叫减少，从而节省更多成本。

IdP 是身份验证模块，可以创建、保留并管理用户、系统或服务的身份信息。IdP 存储和验证用户凭证，并生成 SAML 响应以允许用户访问受服务提供者保护的资源。

注释 您必须熟悉自己的 IdP 服务，确保该服务当前已安装并且可以运行。

以下门户支持 SAML SSO：

- 访客门户（发起人管理或自助注册）
- 发起人门户
- 我的设备门户
- 证书调配门户

您不能选择 IdP 作为 BYOD 门户的外部身份源，但可以为访客门户选择 IdP 并启用 BYOD 流程。

Cisco ISE 符合 SAMLv2，支持符合 SAMLv2 且使用 Base64 编码的证书的所有 IdP。下面列出的 IdP 已使用Cisco ISE 进行了测试：

- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP 无法添加到身份源序列。

SSO 会话将终止，并且如果在指定的时间（默认为 5 分钟）内没有任何活动，会显示一条 Session Timeout 错误消息。

如果想要在门户的 Error 页面中添加 Sign On Again 按钮，请在 Portal Error 页面的 Optional Content 字段中添加以下 JavaScript：

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">重新登录</button>
```

在思科 ISE 中配置 SAML 身份提供程序

要在Cisco ISE 中配置 SAML 身份提供程序，请执行以下操作：

- 您必须是Cisco ISE 中的超级管理员或系统管理员。
- 如果要使用的证书不是身份提供程序 (IdP) 自签名的，则将证书颁发机构 (CA) 证书导入受信任证书库。
- 您必须对正在配置的IdP门户具有管理员访问权限。以下任务需要在IdP门户中执行一些步骤。

要在Cisco ISE 中配置 SAML 身份提供程序，请执行以下操作：

1. 将 SAML 身份提供程序添加至Cisco ISE。
2. 添加 SAML 身份提供程序作为门户的身份验证方法。
3. 配置 SAML ID 提供程序。

将 SAML 身份提供程序添加至思科 ISE

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在显示的**SAML 身份提供程序 (SAML Identity Provider)** 窗口中，在**常规 (General)** 选项卡中输入 **ID 提供程序名称 (Id Provider Name)** 和**说明 (Description)**。

步骤 4 点击**提交 (Submit)**。

步骤 5 在**身份提供程序配置 (Identity Provider Config)** 选项卡中，导入相关的 metadata.xml 文件，然后点击**提交 (Submit)**。

将 SAML 身份提供程序添加为门户的身份验证方法

您可以将刚刚创建的 SAML 身份提供程序添加到以下门户：

1. 自注册访客门户和发起的访客门户（**工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)**）
2. 证书调配门户（**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配** > **证书调配门户 (Certificate Provisioning Portal)**

步骤 1 在要配置的门户的门户自定义窗口中，点击**门户设置 (Portal Settings)**。

步骤 2 在显示的下拉部分中，转到**身份验证方法 (Authentication Method)** 部分，然后使用菜单选择所添加的 SAML IP 提供程序。

步骤 3 点击**保存 (Save)**。

配置 SAML ID 提供程序

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。选择刚才链接到门户的 IdP，然后点击**编辑 (Edit)**。

步骤 2 （可选）如果使用负载均衡器来优化Cisco ISE 节点上的负载，则可以在**服务提供商 (Service Provider Info)** 信息选项卡中添加其详细信息，以简化 IdP 的配置。可以添加软件或硬件负载均衡器。

负载均衡器应该能够使用**端口设置 (Portal Settings)** 中指定的端口，将请求转发到部署中的Cisco ISE 节点。

当添加负载均衡器时，在服务提供商元数据文件中只提供其负载均衡器 URL。如果负载均衡器不存在，则在服务提供商元数据文件中会包含多个 **AssertionConsumerService** URL。

注释 我们建议避免在门户 FQDN 设置中使用相同的负载均衡器 IP 地址。

步骤 3 在**服务提供商信息 (Service Provider Info)** 选项卡中，点击**导出 (Export)** 导出服务提供者元数据文件。导出的元数据包括Cisco ISE 的签名证书，与所选门户的证书完全相同。

导出的元数据压缩文件夹包括一个自述文件，其中含有配置每个 IdP （包括 Azure Active Directory、PingOne、PingFederate、SecureAuth 和 OAM）的基本操作说明。

如果以下方面有以下任何更改，则必须重新导出服务提供商元数据：

- 新Cisco ISE 节点的注册。
- 节点的主机名或 IP 地址。
- 我的设备门户、发起人门户或证书调配门户的完全限定域名 (FQDN)。
- 端口和接口设置。
- 关联的负载均衡器。

如果不重新导出更新后的的元数据，则 IdP 可能会拒绝用户身份验证请求。

步骤 4 转到您的 IdP 门户并以管理员用户身份登录，导入刚才从Cisco ISE 导出的服务提供商元数据文件。您需要首先解压导出的文件夹和具有门户名称的元数据文件。该元数据文件包括提供商 ID 和绑定 URI。

步骤 5 返回Cisco ISE 门户。

步骤 6 （可选）在 **SAML 身份提供程序 (SAML Identity Provider)** 窗口的**组 (Groups)** 选项卡中，添加所需的用户组。

输入在**组成员**属性 (Group Membership Attribute) 字段中指定用户组成员的声明属性。

步骤 7 （可选）在**属性 (Attributes)** 选项卡中添加用户属性，以指定属性如何显示在从 IdP 返回的断言中。

您在 **ISE 中名称 (Name in ISE)** 中指定的名称会在策略规则中显示。

对于属性，支持以下的数据类型：

- 字符串
- 整数
- IPv4
- 布尔值

步骤 8 在**高级设置 (Advanced Settings)** 选项卡中，配置以下选项：

选项	描述
身份属性	通过点击显示的选项对应的单选按钮以选择属性，用来指定要进行身份验证的用户身份。 **注释** Cisco ISE 不支持包含临时或永久格式的使用者名称 (NameID) 的 SAML IdP 响应。如果使用这些方法，Cisco ISE 无法从 SAML IdP 响应中检索用户名属性断言，并且身份验证将失败。
电子邮件属性	从下拉列表中，选择返回用户电子邮件地址的断言属性。如果计划过滤（限制）由同一发起人批准的发起访客名单，则必须配置电子邮件属性。
多值属性	选择以下一个选项： • **每个单独 XML 中各一个值 (Each value in a separate XML)**：如果您的 IdP 在不同 XML 元素中返回同一属性的多个值，则点击该选项。 • **单个 XML 中多个值 (Multiple values in a single XML)**：如果您的 IdP 在单个 XML 元素中返回多个值，则点击该选项。在文本框中指定分隔符。
注销设置	如果希望对注销请求进行签名，请选中**签署注销请求 (Sign Logout Requests)** 复选框。如果正在配置的 IdP 是 Oracle Access Manager 或 Oracle Identity Federation，则不会显示此选项。 **注释** SecureAuth 不支持 SAML 注销。 以下选项仅在配置 Oracle Access Manager 或 Oracle Identity Federation IdP 且未配置负载均衡器时显示： • **注销 URL (Logout URL)**：输入一个页面 URL，当用户从发起人门户或我的设备门户注销时，他们将重定向到该页面以终止 SSO 会话。 • **重定向参数名称 (Redirect Parameter Name)**：当 SSO 会话终止时，用户将返回到 IdP 的登录页面。重定向参数名称可能因 IdP 而异，例如，**end_url** 或 **returnURL**。该字段区分大小写。 如果注销操作未按预期运行，请查看 IdP 的文档，了解有关使用注销 URL 和重定向参数名称的详细信息。
身份验证上下文	使用此部分可编辑 SAML IdP 身份验证上下文类引用。Cisco ISE SAML 请求通常在 SAML 请求标题中使用 **PasswordProtectedTransport** 身份验证方法。这导致在使用多因素身份验证的情况下发生身份验证失败。

选项	描述
	要避免这种情况，您可以使用 **AuthnContextClassRef SAML 元素 (AuthnContextClassRef SAML Element)** 部分指定身份验证方法。如果不确定所使用的身份验证方法，我们建议将此部分留空，以避免身份验证失败。

步骤 9 点击**提交 (Submit)**。

删除身份提供者

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

确保您要删除的 IdP 未链接至任何门户。如果 IdP 与任何门户链接，删除操作将失败。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > 网络访问 (Network Access) > 分机 ID 源 (Ext Id Sources) > SAML ID 提供商 (SAML Id Providers)**。

步骤 2 选中您要删除的 IdP 旁边的复选框，然后点击 **删除 (Delete)**。

步骤 3 点击**确定 (OK)** 以删除您所选择的 IdP。

身份验证失败日志

当按照 SAML ID 库进行身份验证失败并且 IdP 将用户重定向回 ISE 门户（通过 SAML 响应），ISE 将在身份验证日志中报告失败原因。对于访客门户（启用或不启用自带设备流量的情况下），您可以检查 RADIUS 实时日志 (RADIUS Livelog)（操作 (Operations) > RADIUS > 实时日志 (Live Log)）了解身份验证失败原因。对于我的设备门户和发起人门户，您可以查看我的设备登录/审计报告和发起人登录/审计报告（操作 (Operations) > 报告 (Reports) > 访客 (Guest)）了解身份验证失败原因。

如果出现注销故障，您可以查看报告，并通过登录了解我的设备、发起人和访客门户出现故障的原因。

身份验证可能由于以下原因而失败：

- SAML 响应解析错误
- SAML 响应验证错误（例如 Wrong Issuer）
- SAML 断言验证错误（例如 Wrong Audience）
- SAML 响应签名验证错误（例如 Wrong Signature）
- IdP 签名证书错误（例如 Certificate Revoked）

注释 Cisco ISE 不支持具有加密断言的 SAML 响应。如果在 IdP 中配置了此选项，您将在 ISE 中看到以下错误消息：`FailureReason = 24803 无法找到“用户名”属性断言 (FailureReason=24803 Unable to find 'username' attribute assertion)`。

如果身份验证失败，我们建议您检查身份验证日志中的“DetailedInfo”属性。此属性提供关于失败原因的更多信息。

身份源序列

身份源序列定义Cisco ISE 在不同数据库中查找用户凭证的顺序。

如果您在多个连接到Cisco ISE 的数据库中有用户信息，您可以定义您希望Cisco ISE 在这些身份源中查找信息的顺序。找到匹配后，Cisco ISE 不会继续查找，而是评估证书，将结果返回给用户。此策略是第一个匹配策略。

创建身份源序列

开始之前

确保您已经在Cisco ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)** > **添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望Cisco ISE 搜索数据库的顺序。

步骤 6 在 **Advanced Search List** 区域中选择以下选项之一：

- **请勿访问序列中的其他存储区并将 AuthenticationStatus 属性设置为 ProcessError**：如果用户未在第一个选定身份源中找到用户，而您希望Cisco ISE 中止搜索，请选择此选项。
- **视为未找到用户并继续至序列中的下一存储区 (Treat as if the user was not found and proceed to the next store in the sequence)**：如果未在第一个选定身份源中找到用户，而您希望Cisco ISE 仍继续按照序列搜索其他选定身份源，请选择此选项。

  在处理请求时，Cisco ISE 会按照序列搜索这些身份源。确保“选定列表”(Selected list) 字段所列出的身份源的顺序是您希望Cisco ISE 搜索身份源的顺序。

步骤 7 点击**提交 (Submit)** 创建您可以稍后在策略中使用的身份源序列。

删除身份源序列

您可以删除不再在策略中使用的身份源序列。

开始之前

- 确保您即将删除的身份源序列未在任何身份验证策略中使用。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)**。

步骤 2 选中要删除的一个或多个身份源序列旁边的复选框，然后点击 **Delete**。

步骤 3 点击**确定 (OK)** 删除一个或多个身份源序列。

报告中的身份源详细信息

Cisco ISE 通过 Authentications dashlet 报告和 Identity Source 报告提供关于身份源的信息。

身份验证面板

在身份验证面板中，您可以逐步向下展开，找到包括故障原因在内的更多信息。

选择操作 (Operations) > RADIUS 实时日志 (RADIUS Livelog) 以查看实时身份验证概述。有关 RADIUS 实时日志的详细信息，请参阅 RADIUS 实时日志，第 279 页。

身份源报告

Cisco ISE 提供包含身份源相关信息的各种报告。有关这些报告的说明，请参阅“可用报告”一节。

网络上已分析的终端

分析器服务可协助识别、查找和确定您的网络上所有终端的功能（在Cisco ISE 中叫作身份），而无论其设备类型如何，从而确保和保持对您的企业网络的适当访问。Cisco ISE 分析器功能使用大量的探测功能收集您的网络上所有终端的属性，并将这些属性传递至分析服务分析器，此分析器根据已知终端的关联策略和身份组给已知终端分类。

分析器源服务允许管理员通过Cisco ISE 中的订用从指定Cisco源服务器检索新的和已更新的终端分析策略以及作为源的已更新 OUI 数据库。

分析器条件设置

下表介绍“分析器条件”(Profiler Condition) 窗口中的字段。此窗口的导航路径是 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **分析 (Profiling)**。

表 *89:* 分析器条件设置

字段名称	使用指南
名称 (Name)	分析器条件的名称。
说明	分析器条件的说明。
类型	选择任何一个预定义类型。
Attribute Name	选择分析器条件所基于的属性。
运算符	选择运算符。
Attribute Value	输入已选择的属性的值。对于包含预定义属性值的属性名称，此选项显示具有预定义值的下拉列表，并且您可以选择值。
System Type	分析条件可以是以下任何一个类型： • **思科提供 (Cisco Provided)**：在部署时由Cisco ISE 提供的分析条件标识为“Cisco提供”(Cisco Provided)。您不能从系统编辑或删除这些条件。 • **管理员创建 (Administrator Created)**：您以Cisco ISE 管理员身份创建的分析条件标识为“管理员创建”(Administrator Created)。

相关主题

思科 ISE 分析服务，第 603 页
分析器条件，第 627 页
分析器源服务，第 664 页
创建分析器条件，第 642 页

思科 ISE 分析服务

Cisco身份服务引擎 (ISE) 中的分析服务能够识别连接到网络的设备及其位置。它根据在Cisco ISE 中配置的终端分析策略来分析终端。然后，Cisco ISE 会根据策略评估的结果，向终端授予访问网络资源的权限。

分析服务：

- 利用 IEEE 802.1X 基于端口的标准身份验证访问控制、MAC 身份验证绕行 (MAB) 身份验证，以及适用于各种规模和复杂性的任何企业网络的网络准入控制 (NAC)，可以实现高效和有效的部署以及对身份验证的持续管理。
- 识别、查找并确定连接的所有网络终端的功能，无论终端类型是什么都如此。
- 防止意外拒绝对某些终端的访问。

ISE 社区资源

ISE 终端配置文件

操作方法：ISE 分析设计指南

分析器工作中心

分析器工作中心菜单（“工作中心”(Work Centers) > “分析器”(Profiler)）包含所有分析器页面，作为 ISE 管理员的单一起点。分析器工作中心菜单包含以下选项：“概述”(Overview)、“外部 ID 库”(Ext ID Stores)、“网络设备”(Network Devices)、“终端分类”(Endpoint Classification)、“节点配置”(Node Config)、“源”(Feeds)、“手动扫描”(Manual Scans)、“策略元素”(Policy Elements)、“分析策略”(Profiling Policies)、“授权策略”(Authorization Policy)、“故障排除”(Troubleshoot)、“报告”(Reports)、“设置”(Settings) 和“字典”(Dictionaries)。

分析器控制面板

分析器控制面板（工作中心 (Work Centers) > 分析器 (Profiler) > 终端分类 (Endpoint Classification)）是一种集中式监控网络中配置文件、终端和资产的工具。该控制面板同时以图形和表格格式展示数据。“配置文件”(Profiles) dashlet 显示当前在网络中处于活动状态的逻辑和终端配置文件。“终端”(Endpoints) dashlet 显示连接到网络的终端的身份组、PSN 和操作系统类型。“资产”(Assets) dashlet 显示访客、自带设备和公司等流程。下表显示了连接的各种终端，您也可以添加新的终端。

使用分析服务的终端资产

您可以使用分析服务发现、找到和确定连接到网络的所有终端的功能。无论设备类型如何，都可以确保和维护终端对企业网络的适当访问。

分析服务从网络设备和网络收集终端属性，根据配置文件将终端归到特定组，以及在Cisco ISE 数据库中存储终端及其匹配的配置文件。分析服务处理的所有属性都需要在分析器字典中定义。

分析服务识别网络上的每个终端，并根据配置文件将这些终端归入系统中的现有终端身份组，或者归入您在系统中创建的新组。通过对终端分组以及将终端分析策略应用到终端身份组，您可以确定终端到相应终端分析策略的映射。

思科 ISE 分析器队列限制配置

Cisco ISE 分析器可在短时间内从网络收集大量终端数据。由于某些速度较慢的Cisco ISE 组件在处理分析器生成的数据时会产生积压（造成性能下降和稳定性问题），因此这将导致 Java 虚拟机 (JVM) 内存使用率增加。

为确保分析器不会增加 JVM 内存使用率并防止 JVM 内存不足和重新启动，系统会对分析器的以下内部组件应用限制：

- 终端缓存 - 内部缓存大小有限，当大小超过限制时，必须定期清除（根据最近最少使用的策略）。
- 转发器 - 分析器收集的终端信息的主入口队列。
- 事件处理程序 - 用于断开快速组件（该组件会向较慢的处理组件 [通常与数据库查询相关] 提供数据）的连接的内部队列。

终端缓存

- maxEndPointsInLocalDb = 100000（缓存中的终端对象数）
- endPointsPurgeIntervalSec = 300（终端缓存清除线程时间间隔，以秒为单位）
- numberOfProfilingThreads = 8（线程数）

限制适用于所有分析器内部事件处理程序。当达到队列大小限制时，会触发监控警报。

思科 ISE 分析器队列大小限制

- forwarderQueueSize = 5000（终端集合事件数）
- eventHandlerQueueSize = 10000（事件数）

事件处理程序

- NetworkDeviceEventHandler - 除筛选已经缓存的重复网络接入设备 (NAD) IP 地址外，还用于处理网络设备事件。
- ARPCacheEventHandler - 用于处理 ARP 缓存事件。

Martian IP 地址

Martian IP 地址不会在 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** 和 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **终端分类 (Endpoint Classification)** 窗口中显示，因为 RADIUS 解析器会在这些

地址到达分析服务之前将其删除。Martian IP 地址容易受到攻击，因此是安全隐患。但是，出于审核目的，MnT 日志中会显示 Martian IP 地址。此行为在组播 IP 地址的情况下也是如此。有关 Martian IP 地址的详细信息，请参阅 https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html

分析转发器持久化队列

分析转发器持久化队列会存储事件，然后再将事件发送到分析器模块进一步处理。此外，还增加了队列容量，以支持增加的事件处理工作。这可以减少因事件数量突然增加而丢失的事件数量。这继而会减少队列达到其最大限制时发出的警报。

默认情况下启用此功能。如果需要，您可以禁用此功能以回退到原始机制，在该机制中，事件直接发送到分析器模块。要启用或禁用此功能，请选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **分析 (Profiling)** 并选中或取消选中**启用分析转发器持久化队列 (Enable Profiler Forwarder Persistence Queue)** 复选框。

在思科 ISE 节点中配置分析服务

可以配置分析服务，该服务为您提供正在任何启用Cisco ISE 的网络中使用网络资源的所有终端的上下文资产。

可以将分析服务配置为在单一Cisco ISE 节点上运行，默认情况下，此节点承担所有管理、监控和策略服务角色。

在分布式部署中，分析服务仅在承担策略服务角色的Cisco ISE 节点上运行，不在承担管理和监控角色的其他Cisco ISE 节点上运行。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选择承担策略服务角色的Cisco ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击**编辑 (Edit)**。

步骤 4 在**常规设置 (General Settings)** 选项卡上，选中**策略服务 (Policy Service)** 复选框。如果取消选中 Policy Service 复选框，会话服务和分析服务复选框均被禁用。

步骤 5 执行以下任务：

a) 选中 **Enable Session Services** 复选框，运行网络访问、终端安全评估、访客和客户端调配会话服务。

b) 选中 **Enable Profiling Services** 复选框，运行分析服务。

c) 选中**启用设备管理服务 (Enable Device Admin Service)** 复选框运行设备管理服务，对企业网络设备进行控制和审计。

步骤 6 点击**保存 (Save)**，保存节点配置。

分析服务使用的网络探测功能

网络探测功能是一种用于从网络上的终端收集属性或属性集的方法。通过探测功能，您可以使用Cisco ISE 数据库中的终端匹配配置文件创建或更新终端。

Cisco ISE 可以使用许多网络探测功能来分析设备，这些网络探测功能会分析网络上设备的行为并确定设备的类型。网络探测功能可帮助您获取更多网络可视性。

IP 地址和 MAC 地址绑定

您只能通过在企业网络中使用终端的 MAC 地址来创建或更新终端。如果您在 ARP 缓存中找不到条目，则可以通过在Cisco ISE 中使用 HTTP 数据包的 L2 MAC 地址和 NetFlow 数据包的 IN_SRC_MAC 来创建或更新终端。当终端只是一个跃点之隔时，分析服务依赖于 L2 邻接。当终端是 L2 邻接时，表明已映射终端的 IP 地址和 MAC 地址，无需进行 IP-MAC 缓存映射。

如果终端不是 L2 邻接并且间隔多个跃点，则映射可能不可靠。您收集的 NetFlow 数据包的一些已知属性包括 PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC 和 OUT_SRC_MAC。当终端不是 L2 邻接并且间隔多个 L3 跃点时，IN_SRC_MAC 属性只能运载 L2 网络设备的 MAC 地址。当在Cisco ISE 中启用 HTTP 探测时，您只能通过使用 HTTP 数据包的 MAC 地址创建终端，因为 HTTP 请求消息在负载数据中不会运载终端的 IP 地址和 MAC 地址。

Cisco ISE 在分析服务中实施 ARP 缓存，以便您能够可靠地映射终端的 IP 地址和 MAC 地址。为使 ARP 缓存正常运行，您必须启用 DHCP 探测或 RADIUS 探测。DHCP 和 RADIUS 探测在负载数据中运载终端的 IP 地址和 MAC 地址。DHCP 探测中的 dhcp-requested 地址属性和 RADIUS 探测中的 Framed-IP-address 属性运载终端的 IP 地址，及其可在 ARP 缓存中映射和存储的 MAC 地址。

NetFlow 探测功能

Cisco ISE 分析器使用Cisco IOS NetFlow 版本 9。我们建议使用 NetFlow 版本 9，因为其具有增强此分析器以支持Cisco ISE 分析服务的更多功能。

您可以从支持 NetFlow 的网络访问设备收集 NetFlow 版本 9 属性以在Cisco ISE 数据库中创建终端或更新现有终端。您可以将 NetFlow 版本 9 配置为连接终端和更新终端的源与目标 MAC 地址。您还可以创建 NetFlow 属性字典以支持基于 NetFlow 的分析。

有关NetFlow版本9记录格式的更多信息，请参阅NetFlow版本9流程-记录格式文档的表6“NetFlow 版本 9 字段类型定义”。

此外，Cisco ISE 支持低于 5 以下的 NetFlow 版本。如果您在网络使用 NetFlow 版本 5，则只能在接入层主要网络访问设备 (NAD) 上使用版本 5，因为此版本在其他位置无法运行。

Cisco IOS NetFlow 版本 5 程序包不包含终端的 MAC 地址。从 NetFlow 版本 5 收集的属性不能直接添加至Cisco ISE 数据库。您可以通过使用终端的 IP 地址发现终端，并且通过将网络访问设备的 IP 地址与从 NetFlow 版本 5 属性获取的 IP 地址组合，将 NetFlow Version 5 属性附加到终端上。但是，之前必须已使用 RADIUS 或 SNMP 探测功能发现这些终端。

在早版 NetFlow 版本 5 中，MAC 地址不是 IP 流的组成部分，这就要求您关联从终端缓存中的网络访问设备收集的属性信息，才能用终端 IP 地址分析终端。

有关 NetFlow 版本 5 记录格式的更多信息，请参阅《NetFlow 服务解决方案指南》中表 2“Cisco ISE NetFlow 流程记录和导出格式内容信息”。

DHCP 探测功能

在Cisco ISE 部署中，动态主机配置协议探测功能允许Cisco ISE 分析服务仅根据 INIT-REBOOT 和 SELECTING 消息类型的新请求，重新分析终端。虽然系统会处理 RENEWING 和 REBINDING 等其他 DHCP 消息类型，但是这些消息类型不会用于分析终端。在 DHCP 数据包之外解析的任何属性都会映射至终端属性。

在 INIT-REBOOT 状态期间生成的 DHCPREQUEST 消息

如果 DHCP 客户端进行检查以验证之前分配和缓存的配置，则客户端不得填写 Server identifier (server-ip) 选项，而应该用之前分配的 IP 地址填写 Requested IP address (requested-ip) 选项，并且在其 DHCPREQUEST 消息中用零填写 Client IP Address (ciaddr) 字段。然后，如果所请求的 IP 地址不正确或客户端位于错误的网络上，则 DHCP 服务器将向该客户端发送 DHCPNAK 消息。

在 SELECTING 状态期间生成的 DHCPREQUEST 消息

DHCP 客户端在 Server identifier (server-ip) 选项中插入所选 DHCP 服务器的 IP 地址，用客户端选择的 DHCPOFFER 的 Your IP Address (yiaddr) 字段的值填写 Requested IP address (requested-ip) 选项，并且在“ciaddr”字段中填写零。

表 *90:* 来自不同状态的 *DHCP* 客户端消息

-	INIT-REBOOT	SELECTING	RENEWING	REBINDING
广播 / 单播	广播	广播	单播	广播
server-ip	不得填写	必须填写	不得填写	不得填写
requested-ip	必须填写	必须填写	不得填写	不得填写
ciaddr	零	零	IP 地址	IP 地址

DHCP 桥接模式下的无线 LAN 控制器配置

我们建议您在动态主机配置协议 (DHCP) 桥接模式下配置无线 LAN 控制器 (WLC)，这样您就可以将所有来自无线客户端的 DHCP 数据包转发至Cisco ISE。您必须在 WLC Web 界面取消选中“启用 DHCP 代理” (Enable DHCP Proxy) 复选框： **控制器 (Controller)** > **高级 (Advanced)** > **DHCP 主控制器模式 (DHCP Master Controller Mode)** > **DHCP 参数 (DHCP Parameters)**。您还必须确保 DHCP IP 帮助程序命令指向Cisco ISE 策略服务节点。

DHCP SPAN 探测功能

当在Cisco ISE 节点中初始化 DHCP 交换端口分析器 (SPAN) 探测功能时，即可监听网络流量，而该网络流量来自特定接口的网络接入设备。您需要对网络接入设备进行配置，从DHCP服务器向Cisco ISE 分析器转发 DHCP SPAN 数据包。分析器接收这些 DHCP SPAN 数据包并对其进行分析以抓取终端的属性，而这些属性可用于分析终端。

例如，

```
switch(config)# monitor session 1 source interface Gi1/0/4 switch(config)# monitor session
1 destination interface Gi1/0/2
```

HTTP 探测功能

在 HTTP 探测中，标识字符串在 HTTP 请求报头字段 User-Agent 中进行传输，该字段是可用于创建 IP 类型的分析条件以及检查 Web 浏览器信息的属性。分析器从 User-Agent 属性以及请求消息中的其他 HTTP 属性捕获 Web 浏览器信息，并将其添加到终端属性列表。

Cisco ISE 同时在端口 80 和端口 8080 上侦听来自 Web 浏览器的通信。Cisco ISE 提供许多默认配置文件，这些配置文件内置到系统中以根据 User-Agent 属性识别终端。

默认情况下，HTTP 探测器处于启用状态。多个 ISE 服务（例如 CWA、热点、BYOD、MDM 和终端安全评估）依赖于客户端 Web 浏览器的 URL 重定向。重定向的流量包括所连接终端的 RADIUS 会话 ID。当 PSN 终止这些 URL 重定向的流时，它对已解密的 HTTPS 数据具有可视性。即使在 PSN 上禁用 HTTP 探测器，节点也会通过 Web 流量来解析浏览器用户代理字符串，并根据其关联的会话 ID 将数据关联到终端。通过此方法收集浏览器字符串时，数据源将列出为访客门户或 CP（客户端调配），而不是 HTTP 探测器。

HTTP SPAN 探测功能

Cisco ISE 部署中的 HTTP 探测功能随交换端口分析器 (SPAN) 探测功能一起启用时，允许分析器从指定的接口捕获 HTTP 数据包。您可以在端口 80 上使用 SPAN 功能，在该端口上Cisco ISE 服务器会侦听来自 Web 浏览器的通信。

HTTP SPAN 收集 HTTP 请求报头消息的 HTTP 属性以及 IP 报头（L3 报头）中的 IP 地址，IP 地址可根据 L2 报头中终端的 MAC 地址与某个终端关联。此信息有助于识别具备 IP 功能的不同的移动和便携式设备（例如 Apple 设备）以及安装不同操作系统的计算机。由于Cisco ISE 服务器在访客登录或下载客户端调配期间会重定向捕获的数据包，因此能够更加可靠地识别具备 IP 功能的不同的移动和便携式设备。这样，分析器就可以从请求消息中收集用户-代理属性和其他 HTTP 属性，然后识别设备，例如 Apple 设备。

无法在 VMware 上运行的思科 ISE 中收集 HTTP 属性

如果您在 ESX 服务器 (VMware) 上部署Cisco ISE，Cisco ISE 分析器会收集动态主机配置协议流量，但由于 vSphere 客户端上的配置问题，它不会收集 HTTP 流量。要在 VMware 设置上收集 HTTP 流量，请将您为Cisco ISE 分析器创建的虚拟交换机的 Promiscuous Mode 从 Reject（默认设置）改为 Accept，配置安全设置。当为 DHCP 和 HTTP 启用交换端口分析器 (SPAN) 探测功能时，Cisco ISE 分析器会同时收集 DHCP 流量和 HTTP 流量。

pxGrid 探测器

pxGrid 探测器利用Cisco pxGrid 从外部源接收终端情景。在早于Cisco ISE 2.4 的版本中，Cisco ISE 仅充当发布程序，并向外部用户共享各种情景信息，例如会话身份和组信息以及配置元素。当在Cisco ISE 2.4 中引入 pxGrid 探测器后，其他解决方案将充当发布程序，Cisco ISE 策略服务节点将成为用户。

pxGrid 探测器基于 pxGrid v2 规范并使用终端资产主题 */topic/com.cisco.endpoint.asset* 和服务名称 *com.cisco.endpoint.asset*。下表显示了主题属性，所有这些属性前面都带有前缀 *asset*。

表 ***91:*** 终端资产主题

属性名称	类型	说明
assetId	长	资产 ID
assetName	字符串	资产名称
assetIpAddress	字符串	IP 地址
assetMacAddress	字符串	MAC 地址
assetVendor	字符串	Manufacturer
assetProductId	字符串	产品代码
assetSerialNumber	字符串	序列号
assetDeviceType	字符串	设备类型
assetSwRevision	字符串	软件修订号
assetHwRevision	字符串	硬件修订号
assetProtocol	字符串	协议
assetConnectedLinks	阵列	网络链接对象阵列
assetCustomAttributes	阵列	自定义名称-值对数组

除了通常用于跟踪网络资产的属性（例如设备 MAC 地址 (assetMacAddress) 和 IP 地址 (assetIpAddress)）之外，该主题还允许供应商将唯一终端信息发布为自定义属性 (assetCustomAttributes)。在Cisco ISE

中使用终端自定义属性，使主题可扩展到各种使用情形，而无需为通过 pxGrid 共享的每组新的唯一供应商属性更新架构。

RADIUS 探测功能

您可以将Cisco ISE配置为使用 RADIUS 进行身份验证，您可以定义在客户端服务器交易中使用的共享密钥。利用从 RADIUS 服务器接收的 RADIUS 请求和响应消息，分析器可以收集 RADIUS 属性，用于分析终端。

Cisco ISE 可以用作 RADIUS 服务器以及其他 RADIUS 服务器的 RADIUS 代理客户端。充当代理客户端时，它可以使用外部 RADIUS 服务器处理 RADIUS 请求和响应消息。

RADIUS 探测还会收集设备传感器在 RADIUS 记账数据包中发送的属性。有关详细信息，请参阅从 IOS 传感器嵌入式交换机收集属性，第 622 页和支持 IOS 传感器的网络访问设备的配置检查表，第 622 页。

默认情况下，即使对于未配置分析服务的系统，RADIUS 探测也会运行，以确保 ISE 可以跟踪终端身份验证和授权详细信息，以便在情景可视性服务中使用。RADIUS 探测和分析服务还用于跟踪已注册终端的创建和更新时间，以进行清除操作。

表 *92*: 使用 *RADIUS* 探测功能收集的常见属性。

User-Name	Calling-Station-Id	Called-Station-Id	Framed-IP-Address
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
设备类型 (NAD)	位置 (NAD)	身份验证策略 (Authentication Policy)	授权策略

注释 收到记账停止消息时，如果最初使用IP地址进行了分析，则会触发Cisco ISE重新分析相应的终端。因此，如果您为使用IP地址分析的终端配置了自定义配置文件，则满足这些配置文件的总确定性因素的唯一方法是匹配相应的 IP 地址。

网络扫描 (NMAP) 探测功能

通过Cisco ISE，您可以使用 NMAP 安全扫描器检测子网中的设备。您可以在已启用运行分析服务的策略服务节点上启用 NMAP 探测功能。可以在终端分析策略中使用该探测的结果。

每个 NMAP 手动子网扫描都有唯一的数字 ID，用于使用该扫描 ID 更新终端源信息。检测终端时，终端源信息也被更新，表示网络扫描探测功能发现此终端。

NMAP 手动子网扫描对于检测持续连接Cisco ISE 网络的设备（例如，已为其分配静态 IP 地址的打印机）很有帮助，因此，这些设备无法被其他探测器发现。

NMAP 扫描限制

扫描子网会耗费大量资源。扫描子网的过程很漫长，具体取决于子网的规模和密度。活动扫描的数量始终限制为一个扫描，这意味着您一次只能扫描一个子网。在子网扫描期间，您可以随时取消子网扫描。您可以使用**点击 (Click)** 查看最新扫描结果链接，查看存储在以下位置的最近网络扫描结果： **工作中心 (Work Centers)** > **分析器 (Profiler)** > **手动扫描 (Manual Scans)** > **手动 NMAP 扫描结果 (Manual NMAP Scan Results)**。

手动 NMAP 扫描

以下 NMAP 命令扫描子网并发送输出至 nmapSubnet.log：

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX - <subnet>
```

表 *93:* 用于手动子网扫描的 *NMAP* 命令

-O	启用操作系统检测
-sU	UDP 扫描
-p <端口范围>	仅扫描指定端口。例如，U:161，162
oN	正常输出
oX	XML 输出

NMAP 手动子网扫描的 SNMP 只读社区字符串

只要 NMAP 手动子网扫描发现 UDP 端口 161 在终端上处于打开状态，该扫描就会使用 SNMP 查询进行扩展，导致收集更多属性。在NMAP手动子网扫描过程中，网络扫描探测功能会检测SNMP端口 161 在设备上是否处于打开状态。如果端口处于打开状态，则系统会使用 SNMP 版本为 2c 的默认社区字符串 (public) 触发 SNMP 查询。

如果设备支持SNMP，并且默认只读社区字符串设置为public，则您可以从MIB值“ifPhysAddress”获取设备的 MAC 地址。

此外，还可以在**分析器配置 (Profiler Configuration)** 窗口中为 NMAP 手动网络扫描配置以逗号分隔的其他 SNMP 只读社区字符串。您也可以为 SNMP 版本为 1 和 2c 的 SNMP MIB walk 指定新的只读社区字符串。有关配置 SNMP 只读社区字符串的信息，请参阅设置 CoA、SNMP RO 社区和终端属性过滤器，第 616 页。

手动 NMAP 扫描结果

最新网络扫描结果存储位置为工作中心 (Work Centers) > 分析器 (Profiler) > 手动扫描 (Manual Scans) > 手动 NMAP 扫描结果 (Manual NMAP Scan Results)。手动 NMAP 扫描结果 (Manual NMAP Scan Results) 页面仅显示检测到的最新终端、其关联终端的配置文件、其 MAC 地址和作为您在任何子网上执行的手动网络扫描结果的静态分配状态。如有必要，您可以通过此页面编辑从终端子网检测的点以实现更好的分类。

Cisco ISE 允许您从已启用运行分析服务的策略服务节点执行手动网络扫描。您必须从您的部署中的主要管理 ISE 节点用户界面选择策略服务节点，才能从策略服务节点运行手动网络扫描。在任何子

网上执行手动网络扫描期间，网络扫描探测功能都会检测指定子网上的终端、其操作系统并检查 UDP 端口 161 和 162 是否在运行 SNMP 服务。

下面提供了与手动 NMAP 扫描结果相关的其他信息：

- 要检测未知终端，NMAP 应能够通过 NMAP 或支持的 SNMP 扫描获知 IP/MAC 绑定。
- ISE 通过 Radius 身份验证或 DHCP 分析了解已知终端的 IP/MAC 绑定。
- IP/MAC 绑定不会跨部署中的 PSN 节点复制。因此，必须从 PSN 触发手动扫描，此 PSN 在其本地数据库中具有 IP/MAC 绑定（例如，上次对其进行 MAC 地址身份验证的 PSN）。
- NMAP 扫描结果不显示与 NMAP 之前手动或自动扫描的终端相关的任何信息。

DNS 探测功能

您的Cisco ISE 部署中的域名服务 (DNS) 探测功能允许分析器查找终端并获取完全限定域名 (FQDN)。在启用Cisco ISE 的网络中检测到终端之后，系统会从 NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP 探测功能收集一系列终端属性。

当您首次在独立环境或分布式环境中部署Cisco ISE 时，系统将提示您运行设置实用程序以配置Cisco ISE 设备。当您运行实用程序设置时，您要配置域名系统 (DNS) 域和主要名称服务器（主要 DNS 服务器），其中您可以配置一个或多个名称服务器。您也可以在部署Cisco ISE 之后，随时使用 CLI 命令更改或添加 DNS 名称服务器。

DNS FQDN 查找

在可执行 DNS 查找前，必须随 DNS 探测功能一起启用以下一个探测功能：DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。这将允许分析器中的 DNS 探测功能对您在Cisco ISE 部署中定义的指定名称服务器执行 DNS 反向查找（FQDN 查找）。系统会为终端在属性列表中添加新属性，可将此属性用于终端分析策略评估。FQDN 是系统 IP 字典中存在的新属性。您可以创建终端分析条件以验证 FQDN 属性及其用于分析的值。以下是 DNS 查找和收集这些属性的探测功能需要的特定终端属性：

- dhcp-requested-address 属性 - DHCP 和 DHCP SPAN 探测功能收集的属性。
- SourceIP 属性 - HTTP 探测功能收集的属性。
- Framed-IP-Address 属性 - RADIUS 探测功能收集的属性
- cdpCacheAddress 属性 - SNMP 探测功能收集的属性

在 WLC Web 界面中配置呼叫站 ID 类型

可以使用 WLC Web 界面配置呼叫站 ID 类型信息。可以转到 WLC Web 界面的 Security 选项卡，在 RADIUS Authentication Servers 页面配置呼叫站 ID。默认情况下，WLC 用户界面中的 MAC Delimiter 字段设置为 Colon。

关于如何在 WLC Web 界面中进行配置的详细信息，请参阅《Cisco无线 LAN 控制器配置指南》7.2 版第 6 章“配置安全解决方案”。

关于如何使用 config radius callStationIdType 命令在 WLC CLI 中进行配置的详细信息，请参阅《Cisco 无线 LAN 控制器命令参考指南》7.2 版第 2 章“控制器命令”。

步骤 1 登录无线 LAN 控制器用户界面。

步骤 2 点击 **Security**。

步骤 3 展开 **AAA**，然后选择 **RADIUS** > **身份验证 (Authentication)**。

步骤 4 从 Call Station ID Type 下拉列表选择 **System MAC Address**。

步骤 5 从 MAC Delimeter 下拉列表选择 **Colon**。

SNMP 查询探测功能

除在“编辑节点”(Edit Node) 页面中配置 SNMP 查询探测以外，还必须在以下位置配置其他简单管理协议设置：**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

您可以在 Network Devices 列表页面中的新网络接入设备 (NAD) 中配置 SNMP 设置。在 SNMP 查询探测中或在网络接入设备中的 SNMP 设置中指定的轮询间隔按定期间隔查询 NAD。

您可以根据以下配置为特定 NAD 打开和关闭 SNMP 查询：

- 在收到表明链路已启动并新增 MAC 的通知时打开或关闭 SNMP 查询
- 针对Cisco发现协议信息，在收到表明链路已启动并新增 MAC 的通知时打开或关闭 SNMP 查询
- 默认情况下，SNMP 查询计时器针对每个交换机每小时进行一次计时

对于 iDevice 和其他不支持 SNMP 的移动设备，可以通过 ARP 表发现 MAC 地址，而该表可由 SNMP 查询探测功能从网络接入设备进行查询。

使用 SNMP 查询的思科发现协议支持

当在网络设备上配置SNMP设置时，必须确保网络设备的所有端口上均启用Cisco发现协议（默认情况下）。如果在网络设备的任意端口上禁用Cisco发现协议，则可能会因为缺少有关所有已连接终端的Cisco发现协议信息而无法进行正确的分析。可以通过在网络设备上使用 cdp run 命令来全局启用Cisco发现协议，或通过在网络接入设备的任意接口上使用 cdp enable 命令来启用Cisco发现协议。要禁用网络设备或接口上的Cisco发现协议，请在命令开头使用 no 关键字。

使用 SNMP 查询的链路层发现协议支持

Cisco ISE 分析器使用 SNMP 查询收集 LLDP 属性。您也可以使用 RADIUS 探测功能从Cisco IOS 传感器（嵌入网络设备中）收集 LLDP 属性。以下是默认 LLDP 配置设置，您可以使用这些设置在网络访问设备上配置 LLDP 全局配置命令和 LLDP 接口配置命令。

表 *94:* 默认 *LLDP* 配置

属性	设置
LLDP 全局状态	已禁用
LLDP 维持时间（丢弃前）	120 秒
LLDP 计时器（数据包更新频率）	30 秒
LLDP 重新初始化延迟	2 秒
LLDP tlv-select	启用，发送和接收所有 TLV。
LLDP 接口状态	已启用
LLDP 接收	已启用
LLDP 传输	已启用
LLDP med-tlv 选择	启用，发送所有 LLDP-MED TLV

以单个字符显示的 CDP 和 LLDP 功能代码

终端的 Attribute List 显示 lldpCacheCapabilities 和 lldpCapabilitiesMapSupported 属性的单一字符值。这些值是对于运行 CDP 和 LLDP 的网络访问设备显示的功能代码。

示例 1

```
lldpCacheCapabilities S lldpCapabilitiesMapSupported S
```

示例 2

```
lldpCacheCapabilities B;T lldpCapabilitiesMapSupported B;T
```

示例 3

```
Switch#show cdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route
 Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M
- Two-port Mac Relay ... Switch# Switch#show lldp neighbors Capability codes: (R) Router,
(B) Bridge, (T) Telephone, (C) DOCSIS Cable Device (W) WLAN Access Point, (P) Repeater, (S)
 Station, (O) Other ... Switch#
```

SNMP 陷阱探测功能

SNMP 陷阱探测功能能够接收来自支持 MAC 通知、LinkUp、LinkDown 和 INFORM 的网络访问设备的信息。SNMP 陷阱探针能够在端口连接或中断以及端点与您的网络断开连接或进行连接时接收来自特定网络访问设备的信息。

要使 SNMP 陷阱探测功能充分运行并创建终端，您必须启用 SNMP 查询，从而在收到陷阱时，使 SNMP 查询探测功能在网络访问设备的特定端口上触发轮询事件。要使此功能充分运行，您应该配置网络访问设备和 SNMP 陷阱。

注释 思科 ISE 不支持从无线 LAN 控制器 (WLC) 和接入点 (AP) 接收的 SNMP 陷阱。

Active Directory 探测

Active Directory (AD) 探测器：

- 提高 WINDOWS 终端操作系统信息的保真度。Microsoft AD 对加入 AD 的计算机操作系统的详细信息进行跟踪，包括版本和服务包级别。AD探测使用AD运行时连接器直接检索此信息，从而提供一个关于客户操作系统信息的高度可靠的来源。
- 帮助区别公司和非公司资产之间的不同之处。AD探测具备的一个基本而重要的属性就是终端是否存在于 AD 中。可使用此信息把 AD 中包含的终端归为受管设备或公司资产类别。

可以在以下位置下启用 AD 探测器 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **分析配置 (Profiling Configuration)**。启用此探测器后，Cisco ISE 在接收到主机名后，将立即获取新终端的 AD 属性。主机名通常是从 DHCP 或 DNS 中获取的。一旦检索成功，直到重新扫描计时器过期，ISE 才会再次尝试对同一个终端进行 AD 查询。这是为了限制 AD 负载，以便于属性查询。重新扫描计时器在**天数之后重新扫描 (Days Before Rescan)** 字段（**管理 [Administration]** > **系统 [System]** > **部署 [Deployment]** > **文件配置 [Profiling Configuration]** > **Active Directory**）中是可配置的。如果终端上有其他配置文件活动，会再次对 AD 进行查询。

可以使用 ACTIVEDIRECTORY 条件，在 **策略 (Policy)** > **策略元素 (Policy Elements)** > **分析 (Profiling)** 匹配以下 AD 探测器属性。使用 AD 探测器收集的 AD 属性在**情景可视性 (Context Visibility)** > **终端 (Endpoints)** 窗口的终端详细信息中通过 "AD" 前缀显示出来。

- AD 主机存在
- AD 连接点
- AD 操作系统
- AD 操作系统版本
- AD 服务包

为每个思科 ISE 节点配置探测功能

您可以在 Profiling Configuration 选项卡上为您的部署中承担策略服务角色的每个Cisco ISE 节点配置一个或多个探测功能，其中节点可能是以下节点：

- 独立节点：如果在默认承担所有管理、监控和策略服务角色的单一节点中部署了Cisco ISE。

- 多个节点：如果在部署中部署了承担策略服务角色的多个节点。

注释 并非全部探测都默认处于启用状态。某些探测器即使未通过复选标记显式启用，也会部分启用。目前，分析配置对于每个 PSN 来说是唯一的。我们建议为部署中的每个 PSN 配置相同的分析器配置设置。

开始之前

您只能从管理节点为每个Cisco ISE 节点配置探测功能，在分布式部署的辅助管理节点上无法执行此配置。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选择承担策略服务角色的Cisco ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击**编辑 (Edit)**。

步骤 4 在**常规设置 (General Settings)** 选项卡上，选中**策略服务 (Policy Service)** 复选框。如果取消选中 Policy Service 复选框，会话服务和分析服务复选框均被禁用。

步骤 5 选中 **Enable Profiling Services** 复选框。

步骤 6 点击 **Profiling Configuration** 选项卡。

步骤 7 为每个探测功能配置相应值。

步骤 8 点击**保存 (Save)** 以保存探测功能配置。

设置 CoA、SNMP RO 社区和终端属性过滤器

Cisco ISE 允许全局配置在 Profiler Configuration 页面中发布授权更改 (CoA)，从而增强分析服务对已通过身份验证的终端的控制。

此外，您还可以在 Profiler Configuration 页面中为 NMAP 手动网络扫描配置以逗号分隔的其他 SNMP 只读社区字符串。SNMP RO 社区字符串使用的顺序与它们在当前自定义 SNMP 社区字符串字段中显示的顺序相同。

您还可以在 Profiler Configuration 页面中配置终端属性筛选。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **分析 (Profiling)**。

步骤 2 选择以下设置之一配置 CoA 类型：

- **No CoA**（默认）- 可以使用此选项禁用 CoA 的全局配置。此设置会根据终端分析策略覆盖任何已配置的 CoA。如果只是为了获得可视性，请保留默认值**无 CoA (No CoA)**。

- **Port Bounce** - 如果交换机端口只存在一个会话，您可以使用此选项。如果端口存在多个会话，则使用 Reauth 选项。如果目标是根据配置文件更改立即更新访问策略，请选择**端口退回 (Port Bounce)** 选项，这将确保重新授权所有无客户端终端，并在需要时刷新 IP 地址。
- **Reauth** - 您可以使用此选项强制重新验证分析时已通过身份验证的终端。如果在重新授权当前会话后预计不会发生 VLAN 或地址更改，请选择**重新验证 (Reauth)** 选项。

  注释　如果一个端口上有多个活动会话，分析服务会通过**重新验证 (Reauth)** 选项发放 CoA，即便您已使用**端口退回 (Port Bounce)** 选项配置了 CoA 也是如此。该功能可避免断开其他会话，而使用**端口退回 (Port Bounce)** 选项就有可能发生这种情况。

步骤 3 在**更改自定义 SNMP 社区字符串 (Change Custom SNMP Community Strings)** 字段中输入新的 SNMP 社区字符串（用逗号分隔）以执行 NMAP 手动网络扫描，然后在**确认自定义 SNMP 社区字符串 (Confirm Custom SNMP Community Strings)** 字段中重新输入字符串进行确认。

默认 SNMP 社区字符串为 *public*。点击**当前自定义 SNMP 社区字符串 (Current Custom SNMP Community Strings)** 部分中的**显示 (Show)** 以验证这一点。

步骤 4 选中 **Endpoint Attribute Filter** 复选框启用终端属性筛选。

启用**终端属性过滤器 (EndPoint Attribute Filter)** 后，Cisco ISE 分析器仅保留重要属性并丢弃所有其他属性。有关详细信息，请参阅过滤器终端属性的全局设置，第 620 页和针对 ISE 数据库持久性和性能的属性过滤器，第 619 页两节。作为最佳实践，我们建议您在生产部署中启用**终端属性过滤器 (EndPoint Attribute Filter)**。

步骤 5 如果您希望Cisco ISE 将终端探测数据发布到需要此数据以对 ISE 上自行激活的终端进行分类的 pxGrid 用户，请选中**启用探测数据发布器 (Enable Probe Data Publisher)** 复选框。在初始部署阶段，pxGrid 用户可以使用批量下载从 Cisco ISE 拉取终端记录。Cisco ISE 会随时将 PAN 中更新的终端记录发送给 pxGrid 用户。默认情况下该选项处于禁用状态。

启用此选项时，请确保在部署中启用 pxGrid 角色。

步骤 6 点击**保存 (Save)**。

对已通过身份验证的终端的授权更改全局配置

您可以使用全局配置功能以通过使用默认的“无 CoA”(No CoA) 选项禁用授权更改 (CoA)，或使用端口退回和重新身份验证选项启用 CoA。如果您在Cisco ISE 中配置了 CoA 的端口回退，则分析服务可能仍会发出“CoA 例外”一节描述的其他 CoA。

所选的全局配置仅在没有更具体的设置的情况下规定默认 CoA 行为。请参阅每个终端分析策略的授权更改配置，第 649 页。

您可以使用 RADIUS 探测或监控角色 REST API 对终端进行身份验证。您可以启用 RADIUS 探测获得更快的性能。如果您已启用 CoA，我们建议您在Cisco ISE 应用中启用 RADIUS 探测时同时启用您的 CoA 配置以获得更快的性能。通过使用已收集的 RADIUS 属性，分析服务可发出终端适当的 CoA。

如果您已在Cisco ISE 应用中禁用 RADIUS 探测，那么您可以通过监控角色 REST API 来发出 CoA。这将允许分析服务支持更多种类的终端。在分布式部署中，您的网络必须至少有一个作为监控角色的Cisco ISE 节点从而通过监控角色 REST API 发出 CoA。

因为主要和次要监控节点都具有相同的会话目录信息，Cisco ISE 会随意指定主要或次要监控节点作为您分布式部署中 REST 查询的默认目标。

发出授权更改的使用案例

分析服务在以下情况下会发出授权更改：

- 删除终端 - 当从 Endpoints 页面删除终端并且从网络上断开或移除该终端时。
- 配置例外操作 - 如果您根据配置文件配置了例外操作，导致该终端出现异常或不可接受的事件。分析服务会通过发出 CoA 将该终端移至相应的静态配置文件。
- 首次分析某个终端 - 当在未静态分配某个终端的情况下首次分析该终端时；例如配置文件从未知配置文件变为已知配置文件。
    - 终端身份组已更改 - 当为授权策略使用的终端身份组添加或删除终端时。

      当某个终端身份组中有任何变更并且在以下情况下将该终端身份组用于授权策略时，分析服务会发出 CoA：

        - 动态分析终端时，终端身份组因这些终端而变更
        - 当某个动态终端的静态分配标志设置为 true 时，终端身份组变更

- 终端身份组策略已变更并且此策略用于授权策略中 - 当终端分析策略变更，并且用于授权策略的逻辑配置文件中包含该策略时。终端分析策略可能因分析策略匹配或终端被静态分配至与逻辑配置文件关联的终端分析策略而改变。在这两种情况下，都只有在将终端分析策略用于授权策略时，分析服务才会发出 CoA。

发出授权更改的豁免

当终端身份组发生更改且静态分配已设置为 true 时，分析服务不会发出 CoA。

出于以下原因，Cisco ISE 不会发出 CoA：

- An Endpoint disconnected from the network - 当发现与网络断开连接的终端时。
- Authenticated wired (Extensible Authentication Protocol) EAP - 当发现支持 EAP 且经过身份验证的有线终端时。
- Multiple active sessions per port - 当一个端口上存在多个活动会话时，分析服务会发出带 Reauth 选项的 CoA，即使您已配置带 Port Bounce 选项的 CoA 亦如此。
- Packet-of-Disconnect CoA (Terminate Session) when a wireless endpoint is detected - 如果发现的终端为无线终端，则分析服务会发出 Packet-of-Disconnect (Terminate-Session)，而不是 Port Bounce CoA。此更改的益处是支持无线 LAN 控制器 (WLC) CoA。

- 当**在逻辑配置文件中抑制终端的分析器 CoA (Suppress Profiler CoA for endpoints in Logical Profile)** 选项用于在授权配置文件中配置的逻辑配置文件时，将抑制分析器 CoA。默认情况下，将为所有其他终端触发分析器 CoA。
- Global No CoA Setting overrides Policy CoA - Global No CoA 设置会覆盖终端分析策略中的所有配置设置，因为不管每个终端分析策略是否配置了 CoA，Cisco ISE 中都不会发出 CoA。

注释 “无 CoA”(No CoA) 和“Reauth CoA”(重新授权 CoA) 配置不受影响，并且分析器服务会为有线和无线终端应用相同的 CoA 配置。

对各类型 CoA 配置发出的授权更改

表 *95:* 对各类型 *CoA* 配置发出的授权更改

情景	No CoA 配置	端口重启配置	Reauth 配置	更多信息
Cisco ISE 中的 CoA 全局配置（典型配置）	No CoA	端口重启	重新身份验证	-
终端与您的网络断开连接	No CoA	No CoA	No CoA	授权更改由 RADIUS 属性 Acct-Status -Type 值停止决定。
支持相同交换机端口上的多个活动的会话	No CoA	重新身份验证	重新身份验证	重新身份验证可避免断开其他会话连接。
无线终端	No CoA	Packet-of-Disconnect CoA（终止会话）	重新身份验证	支持无线局域网控制器。
不完整的 CoA 数据	No CoA	No CoA	No CoA	由于缺少 RADIUS 属性。

针对 ISE 数据库持久性和性能的属性过滤器

Cisco ISE 为动态主机配置协议（DHCP 帮助程序和 DHCP SPAN）、HTTP、RADIUS 和简单网络管理协议探测功能（针对性能下降问题的 NetFlow 探测功能除外）实施过滤器。每个探测功能过滤器都包含与终端分析无关的临时属性的列表，并且会从探测功能收集的属性中移除那些属性。

isebootstrap 日志 (isebootstrap-yyyymmdd-xxxxxx.log) 包含处理字典创建和从字典中过滤属性的消息。您还可以配置在终端经过过滤阶段时记录调试消息以指示已经进行过滤。

Cisco ISE 分析器会调用以下终端属性过滤器：

- 用于 DHCP 帮助程序和 DHCP SPAN 的 DHCP 过滤器包含所有不必要并且在解析 DHCP 数据包后被移除的属性。对于终端，过滤之后的属性会与终端缓存中的现有属性合并。
- 系统使用 HTTP 过滤器从 HTTP 数据包过滤属性，过滤之后属性集中不会有重大变更。
- 系统日志解析完成后会立即使用 RADIUS 过滤器，并且终端属性会并入终端缓存中以进行分析。
- 用于 SNMP 查询的 SNMP 过滤器包括单独的 CDP 过滤器和 LLDP 过滤器，这些过滤器都用于 SNMP-Query 探测功能。

过滤器终端属性的全局设置

您可以通过在收集点减少不会频繁变更的终端属性的数量，减少持久性事件和复制事件的数量。启用**终端属性过滤器 (EndPoint Attribute Filter)** 会使Cisco ISE 分析器仅保留重要属性并丢弃所有其他属性。重要属性是指Cisco ISE 系统使用的属性或特别用于终端分析策略或规则的属性。

要启用**终端属性过滤器 (EndPoint Attribute Filter)**，请参阅设置 CoA、SNMP RO 社区和终端属性过滤器，第 616 页部分。

允许列表是自定义终端分析策略中用于分析终端的一系列属性，这些属性至关重要，关系到授权更改 (CoA)、自带设备 (BYOD)、设备注册 WebAuth (DRW) 等在Cisco ISE 中是否正常运行。允许列表始终用作终端所有权变更时（由多个策略服务节点收集属性时）的标准，即使禁用允许列表也不例外。

默认情况下禁用允许列表，并且只有在启用属性过滤器时才会丢弃属性。当终端分析策略变更（包括数据源变更，以在分析策略中包含新属性）时，允许列表会动态更新。在收集属性时，允许列表中不存在的任何属性会被立即丢弃，并且这些属性不用于分析终端。当与缓冲相结合时，可以减少持久性事件的数量。

您必须确保允许列表包含根据以下两个来源确定的一系列属性：

- 用于默认配置文件中的一系列属性，从而使您可以将终端与配置文件进行匹配。
- 对于使授权更改 (CoA)、自带设备 (BYOD)、设备注册 Web 身份验证 (DRW) 等正常运行很重要的一系列属性。

注释 要向允许列表添加新属性，管理员需要创建使用该属性的新分析器条件和策略。该新属性将自动添加到已存储和复制属性的允许列表。

表 *96:* 允许的属性

AAA-Server	BYODRegistration

Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	说明
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	-
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities

lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	-

从 IOS 传感器嵌入式交换机收集属性

IOS 传感器集成允许Cisco ISE 运行时间和Cisco ISE 分析器收集交换机发送的任何或所有属性。您可以利用 RADIUS 协议，直接从交换机收集 DHCP、CDP 和 LLDP 属性。系统会收集 DHCP、CDP 和 LLDP 的属性，进行解析后，会将其映射至以下位置的分析器词典中的属性：**策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)**。

有关设备传感器支持的 Catalyst 平台的信息，请参阅 https://communities.cisco.com/docs/DOC-72932。

IOS 传感器嵌入式网络接入设备

将 IOS 传感器嵌入式网络接入设备与Cisco ISE 集成涉及以下组件：

- IOS 传感器
- 嵌入在网络接入设备（交换机）中的数据收集器，用于收集 DHCP、CDP 和 LLDP 数据
- 用于处理数据并确定终端的设备类型的分析器

  部署分析器有两种方法，但它们不应相互结合使用：

  - 分析器可以部署在Cisco ISE 中
  - 分析器可以作为传感器嵌入在交换机中

支持 IOS 传感器的网络访问设备的配置检查表

本节概述您必须在支持 IOS 传感器的交换机上和Cisco ISE 中配置的一系列任务，以直接从交换机收集 DHCP、CDP 和 LLDP 属性。

- 确保在Cisco ISE 中启用 RADIUS 探测功能。
- 确保网络访问设备支持用于收集 DHCP、CDP 和 LLDP 信息的 IOS 传感器。
- 确保网络访问设备运行以下 CDP 和 LLDP 命令以从终端捕获 CDP 和 LLDP 信息：

  ```
  cdp enable lldp run
  ```

- 确保通过使用标准 AAA 命令和 RADIUS 命令，单独启用会话记帐。

  例如，使用以下命令：

  ```
  aaa new-model aaa accounting dot1x default start-stop group radius radius-server host
  <ip> auth-port <port> acct-port <port> key <shared-secret> radius-server vsa send
  accounting
  ```

- 确保运行 IOS 传感器特定的命令。
  - 启用计帐扩大

    您必须启用网络访问设备以向 RADIUS 记帐消息添加 IOS 传感器协议数据以及在其检测到新传感器协议数据时生成更多记帐事件。这意味着所有 RADIUS 记帐消息都应包含所有 CDP、LLDP 和 DHCP 属性。

    请输入以下全局命令：

    device-sensor accounting

  - 禁用计帐扩大

    对于在特定端口上托管的会话，要禁用（记帐）网络访问设备和向 RADIUS 记帐消息添加 IOS 传感器协议数据（如果已全局启用记帐功能），请在相应端口输入以下命令：

    no device-sensor accounting

  - TLV 更改跟踪

    默认情况下，对于每个支持的对等协议，只有在传入数据包包含之前在特定会话情景中未接收过的类型、长度和值 (TLV) 时，才会生成客户端通知和记帐事件。

    您必须为所有 TLV 更改（即出现新 TLV，或之前接收的 TLV 拥有不同的值的情况）启用客户端通知和记帐事件。请输入以下命令：

    device-sensor notify all-changes

- 请务必在网络访问设备中禁用 IOS 设备分类器（本地分析器）。

  请输入以下命令：

```
no macro auto monitor
```

注释 此命令可阻止网络访问设备对一项更改发送两个相同的RADIUS记帐消息。

ISE 分析器对思科 IND 控制器的支持

Cisco ISE 可以分析和显示连接到Cisco工业网络设备 (IND) 的设备的状态。PxGrid 连接Cisco ISE 和 Cisco Industrial Network Director 以传送终端（物联网）数据。Cisco ISE 上的 pxGrid 使用Cisco IND 事件，并查询Cisco IND 以更新终端类型。

Cisco ISE 分析器具有物联网设备的词典属性。选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)**，然后从系统词典列表中选择 *IOTASSET* 以查看词典属性。

准则和建议

如果您为分析配置了多个 ISE 节点，我们建议您仅在一个节点上为 Cisco IND 启用 pxGrid。

多个Cisco IND 设备可以连接到单个 ISE。

如果从两个或更多发布者（Cisco IND）收到同一终端信息，则Cisco ISE仅为该终端保留最后一个发布者的数据。

Cisco ISE 从 pxGrid 中的 *com.cisco.endpoint.asset* 和 */topic/com.cisco.endpoint.asset* 服务获取Cisco IND 数据。

思科 IND 分析流程

Cisco IND 资产发现功能查找物联网设备，并将该设备的终端数据发布到 pxGrid。Cisco ISE 看到 pxGrid 上的事件，获取终端数据。Cisco ISE 中的分析器策略将设备数据分配给 ISE 分析器词典中的属性，并将这些属性应用于Cisco ISE 中的终端。

不符合Cisco ISE 中的现有属性的物联网终端数据不会保存。但是，您可以在Cisco ISE 中创建更多属性，并向Cisco IND 注册这些属性。

通过 pxGrid 首次建立与Cisco IND 的连接时，Cisco ISE 会批量下载终端。如果发生网络故障，Cisco ISE 会再次批量下载累积的终端更改。

配置思科 ISE 和思科 IND 进行 IND 分析

注释 您必须在思科 IND 中安装思科 ISE 证书，并在 ISE 中安装思科 IND 证书，然后才能在思科 IND 中激活 pxGrid。

1. 选择 **管理 (Administration)** > **部署 (Deployment)**。编辑您计划用作 pxGrid 使用者的 PSN，并启用 pxGrid。此 PSN 根据Cisco IND 和分析发布的 pxGrid 数据创建终端。
2. 选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** 验证 pxGrid 是否正在运行。然后点击**证书 (Certificates)** 选项卡，并填写证书字段。点击**创建 (Create)** 颁发证书并下载证书。
   - 对于**我想要 (I want to)**，请选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))**，**通用名称 (Common Name)**，并输入要连接的Cisco IND 的名称。
   - 对于**证书下载格式 (Certificate Download Format)**，选择 **PKS12 格式**。
   - 对于**证书密码 (Certificate Password)**，请创建密码。

   注释 必须启用 ISE 内部 CA。如果您的浏览器阻止弹出窗口，您将无法下载证书。解压缩证书，以使 PEM 文件可用于下一步。
3. 在Cisco IND 中，选择 **设置 (Settings)** > **pxGrid**，然后点击**下载 .pem IND 证书 (Download .pem IND certificate)**。保持打开此窗口。
4. 在Cisco ISE 中，选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **所有客户端 (All Clients)**。当您看到Cisco IND pxGrid 客户端时，请批准该客户端。

5. 在Cisco IND 中，移动滑块以启用 pxGrid。系统将打开另一个屏幕，您可以在其中定义 ISE 节点的位置、您在 ISE 中为此 pxGrid 服务器输入的证书的名称以及您提供的密码。点击**上传证书 (Upload Certificate)**，并找到 ISE pxGrid PEM 文件。
6. 在 ISE 中，选择 **管理 (Administration)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。点击**导入 (Import)**，输入从Cisco IND 获取的证书的路径。
7. 在Cisco IND 中，点击**激活 (Activate)**。
8. 在Cisco ISE 中，依次选择**管理 (Adminstration) > 部署 (Deployment)**。选择要用于Cisco IND 连接的 PSN，选择“分析”(Profiling) 窗口，并启用 pxGrid 探测。
9. ISE 与Cisco IND 之间的 pxGrid 连接现在处于活动状态。通过显示Cisco IND 已找到的物联网终端来验证这一点。

添加属性以执行 IND 分析

Cisco IND 可能会返回不在 ISE 词典中的属性。您可以向Cisco ISE 添加更多属性，以便更准确地分析该物联网设备。要添加新属性，请在Cisco ISE 中创建自定义属性，然后通过 pxGrid 将该属性发送到Cisco IND。

1. 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)**，然后选择**终端自定义属性 (Endpoint Custom Attributes)**。创建属性终端属性。
2. 现在，您可以在分析器策略中使用此属性来标识具有新属性的资产。选择 **策略 (Policy)** > **分析 (Profiling)**，并创建新的分析器策略。在**规则 (Rules)** 部分中，创建新规则。添加**属性/值**时，请选择 **CUSTOMATTRIBUTE** 文件夹以及您创建的自定义属性。

ISE 支持 MUD

制造商使用描述符 (MUD) 是一种 IETF 标准，定义了自行激活物联网设备的方式。它提供物联网设备的无缝可视性和分段自动化。MUD 已在 IETF 流程中获得批准，并发布为 RFC8520。有关详细信息，请参阅 https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/。

Cisco ISE 版本 2.6 及更高版本支持识别物联网设备。Cisco ISE 会自动创建分析策略和终端身份组。MUD 支持分析物联网设备，动态创建分析策略，以及自动执行创建策略和终端身份组的整个过程。管理员可以使用这些分析策略手动创建授权策略和配置文件。在 DHCP 和 LLDP 数据包中发送 MUD URL 的物联网设备使用这些配置文件和策略自行激活。

Cisco ISE 对物联网设备执行未签名分类。Cisco ISE 不存储 MUD 属性；属性仅在当前会话中使用。在**情景和可视性 (Context and Visibility)** > **终端 (Endpoints)** 窗口中，可以按**终端配置文件 (Endpoint Profile)** 字段过滤物联网设备。

以下设备支持将 MUD 数据发送到Cisco ISE：

- 运行 Cisco IOS XE 版本 16.9.1 和 16.9.2 的Cisco Catalyst 3850 系列交换机
- 运行 Cisco IOS 版本 15.2(6)E2 的Cisco Catalyst 全数字化楼宇系列交换机

- 运行 Cisco IOS 版本 15.2(6)E2 的Cisco工业以太网 4000 系列交换机
- 具有嵌入式 MUD 功能的物联网 (IoT) 设备

Cisco ISE 支持以下分析协议和分析探测器：

- LLDP 和 Radius - TLV 127
- DHCP - 选项 161

两个字段均可通过 IOS 设备传感器发送到Cisco ISE。

为 MUD 配置 ISE

1. 选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **分析器设置 (Profiler Settings)**，选中**为 MUD 启用分析 (Enable profiling for MUD)** 复选框。
2. 添加可向 ISE 发送 MUD URI 的网络访问设备。要添加网络设备，请选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。
3. 验证 MUD-URL 连接是否正常。
    1. 选择 **情景可视性 (Context Visibility)** > **端点 (Endpoints)**，查找 ISE 成功分类的物联网终端。您可以按终端配置文件名称（以 **IOT-MUD** 开头）过滤物联网设备。
    2. 点击一个物联网设备的终端 MAC 地址，然后选择属性标签。验证属性列表中是否有一个 mud-url。
    3. 选择 **策略 (Policy)** > **分析 (Profiling)** 并在**系统类型 (System Type)** 中选择**物联网创建 (IOT Created)** 以过滤列表。
4. （可选）为新的物联网设备配置调试日志记录。
    1. 选择 **系统 (System)** > **日志记录 (Logging)** > **调试日志配置 (Debug Log Configuration)**，然后选择具有 MUD 配置的 ISE 节点。
    2. 在左侧菜单中选择**调试日志配置 (Debug Log Configuration)**，然后选择**分析器 (profiler)**。

随着分类的物联网设备的增加，MUD-URL 相同的同类别或同组的所有设备都分配到同一终端组。例如，Molex 灯已连接并分类，系统会为该 Molex 灯创建分析器组。随着分类的同类型（有相同的 MUD-URL）的 Molex 灯越来越多，它们会继承相同的分类或终端身份组。

验证 ISE 和交换机中的 MUD 流量

1. 在打开物联网设备之前，请**连接端口**或**取消关闭**接口。
    1. 开始在 ISE 上进行数据包捕获。
    2. 开始在交换端口上进行数据包捕获。
2. 查看交换机上的以下输出。

1. **show device-sensor cache all**
2. **show access-session**
3. **show radius statistics**

3. 打开物联网设备。
4. 每分钟重复以下步骤。
   1. **show device-sensor cache all**
   2. **show access-session**
   3. **show radius statistics**
5. 等待 3 到 5 分钟，以便 ISE 上显示所有设备。
6. 停止 ISE 和交换机的数据包捕获。
7. 每分钟重复以下步骤。
   1. **show device-sensor cache all**
   2. **show access-session**
   3. **show radius statistics**

分析器条件

分析条件是策略元素，而且与其他条件相似。但是不同于身份验证、授权和访客条件，分析条件可以基于有限数量的属性。Profiler Conditions 页面列出Cisco ISE 中可用的属性及其说明。

分析器条件可以是以下任一条件：

- Cisco Provided - Cisco ISE 包含部署时预定义的分析条件，在 Profiler Conditions 页面中标识为 Cisco Provided。您不能删除 Cisco Provided 分析条件。

  您还可以在以下位置在系统分析字典中找到 Cisco Provided 条件：Policy > Policy Elements > Dictionaries > System。

  例如，MAC 字典。对于某些产品，OUI（组织唯一标识符）是您可以首先用于标识设备的生产组织的唯一属性。它是设备 MAC 地址的组成部分。MAC 字典包含 MACAddress 和 OUI 属性。

- Administrator Created - 您以Cisco ISE 管理员的身份创建的分析器条件或复制的预定义分析条件标识为 Administrator Created 条件。您可以使用 Profiler Conditions 页面中的分析字典，创建 DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP 和 NMAP 类型的分析器条件。

虽然建议的分析策略数上限为 1000，但是您可以扩展到多达 2000 个分析策略。

分析网络扫描操作

终端扫描操作是终端分析策略中可以引用的一种可配置操作，当满足与网络扫描操作关联的条件时，就会触发该操作。

终端扫描用于扫描终端，从而限制Cisco ISE 系统中的资源使用。网络扫描操作扫描的是单个终端，而不像涉及整体资源的网络扫描。它可以提高终端的整体分类，并且可以为终端重新定义终端配置文件。一次仅能处理一个终端扫描。

您可以将单个网络扫描操作与终端分析策略关联。Cisco ISE 为网络扫描操作预定义三个扫描类型，一个扫描操作可以包含一个扫描类型，也可以包含全部三个扫描类型：例如 OS 扫描、SNMPPortsAndOS 扫描和 CommonPortsAndOS 扫描。您不能编辑或删除 OS 扫描、SNMPPortsAndOS 扫描和 CommonPortsAndOS 扫描，这些扫描是Cisco ISE 中预定义的网络扫描操作。您还可以创建自己的新网络扫描操作。

正确分析某个终端之后，就无法对该终端使用所配置的网络扫描操作。例如，您可以通过扫描 Apple-Device 将所扫描的终端归类为 Apple 设备。OS 扫描确定了终端运行的操作系统之后，终端就不再与 Apple-Device 配置文件匹配，而是与 Apple 设备的相应配置文件匹配。

创建新的网络扫描操作

与终端分析策略关联的网络扫描操作会扫描终端的操作系统、简单网络管理协议 (SNMP) 端口和通用端口。Cisco为最常见的NMAP扫描提供网络扫描操作，但是您也可以创建自己的网络扫描操作。

当您创建新的网络扫描时，可定义 NMAP 检测要扫描的信息类型。

开始之前

必须首先启用网络扫描 (NMAP) 检测，才能定义规则触发网络扫描操作。关于启用网络扫描检测的操作程序，请参阅为每个思科 ISE 节点配置探测功能。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。或者，您可以选择**工作中心 (Work Centers)** > **分析器 (Profiler)** > **策略元素 (Policy Elements)** > **NMAP 扫描操作 (NMAP Scan Actions)** 。

步骤 2 点击**添加 (Add)**。

步骤 3 输入要创建的网络扫描操作的名称和说明。

步骤 4 当您要对终端扫描以下各项时，请选中一个或多个复选框：

- “扫描操作系统”(Scan OS) - 扫描操作系统
- Scan SNMP Port - 扫描 SNMP 端口（161、162）
- Scan Common Port - 扫描通用端口。
- “扫描自定义端口”(Scan Custom Ports) - 扫描自定义端口。

- “扫描包括业务版本信息”(Scan Include Service Version Information) - 扫描业务版本信息，可能包含设备的详细说明。
- “运行 SMB 发现脚本”(Run SMB Discovery Script) - 扫描 SMB 端口(端口号为：445 和 139）以检索操作系统和计算机名称等信息。
- “跳过 NMAP 主机发现”(Skip NMAP Host Discovery) - 跳过 NMAP 扫描的初始主机发现阶段。

  注释　对于自动 NMAP 扫描，默认选择“跳过 NMAP 主机发现”(Skip NMAP Host Discovery) 选项，但是，必须选择该选项才能运行手动 NAMP 扫描。

步骤 5　点击**提交 (Submit)**。

NMAP 操作系统扫描

操作系统扫描（OS 扫描）类型用于扫描终端运行的操作系统（OS 版本）。这种扫描会占用大量资源。

NMAP 工具对可能导致不可靠的结果的 OS 扫描有限制。例如，当扫描交换机和路由器等网络设备的操作系统时，NMAP 操作系统扫描针对这些设备提供的操作系统数据不正确。即使准确度不是 100%，Cisco ISE 也会显示操作系统属性。

您应将在规则中使用 NMAP 操作系统属性的终端分析策略配置为具有较低的可信度值条件（可信度值）。我们建议，每当您基于 NMAP:operating-system 属性创建终端分析策略时，都应包含 AND 条件以帮助从 NMAP 中过滤掉错误结果。

以下 NMAP 命令用于在您将操作系统扫描与终端分析策略关联时扫描操作系统：

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

以下 NMAP 命令扫描子网并发送输出至 nmapSubnet.log：

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX - <subnet>
```

表 *97:* 用于手动子网扫描的 *NMAP* 命令

-O	启用操作系统检测
-sU	UDP 扫描
-p <端口范围>	仅扫描指定端口。例如，U:161，162
oN	正常输出
oX	XML 输出

操作系统端口

下表列出 NMAP 用于 OS 扫描的 TCP 端口。此外 NMAP 使用 ICMP 和 UDP 端口 51824。

1	3	4	6	7	9	13	17	19

20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407 个	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720

1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972 年	1974	1984	1998-2010	2013	2020 年	2021
2022	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000-4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959

5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774

32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP 端口扫描

SNMPPortsAndOS 扫描类型扫描终端运行的操作系统（和操作系统版本）并在打开 SNMP 端口（161 和 162）时触发 SNMP 查询。其可用于一开始识别为与 Unknown 配置文件匹配的终端，以更好地进行分类。

以下 NMAP 命令用于在将 Scan SNMP 端口与终端分析策略关联时扫描 SNMP 端口（UDP 161 和 162）：

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

表 *98:* 用于终端 *SNMP* 端口扫描的 *NMAP* 命令

-sU	UDP 扫描。
-p <端口范围>	仅扫描指定端口。例如，扫描 UDP 端口 161 和 162。
oN	正常输出。
oX	XML 输出。
IP-address	所扫描终端的 IP 地址。

NMAP 通用端口扫描

CommonPortsAndOS-scan type 扫描终端所运行的操作系统（和操作系统版本）以及通用端口（TCP 和 UDP），但不扫描 SNMP 端口。当您将 Scan Common Port 与终端分析策略关联时，以下 NMAP 命令会扫描通用端口：nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP 地址>

表 *99:* 用于终端通用端口扫描的 *NMAP* 命令

-sTU	TCP 连接扫描和 UDP 扫描。
-p <端口范围>	扫描 TCP 端口：21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080 和 UDP 端口：53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900
oN	正常输出。
oX	XML 输出。
IP 地址	所扫描终端的 IP 地址。

通用端口

下表列出 NMAP 用于扫描的端口。

表 *100:* 通用端口

TCP 端口		**UDP** 端口	
端口	服务	端口	服务
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP 自定义端口扫描

除了通用端口，还可以使用自定义端口（**工作中心 (Work Centers)** > **分析器 (Profiler)** > **策略元素 (Policy Elements)** > **NMAP 扫描操作 (NMAP Scan Actions)** 或 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **网络扫描 (NMAP) 操作 (Network Scan [NMAP]**

Actions)）以指定自动和手动 NMAP 扫描操作。NMAP 探测通过开放的特定自定义端口收集来自终端的属性。这些属性在“ISE 身份”(ISE Identities) 页面中的终端属性列表中进行更新（**工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**）。您最多可以为每项扫描操作指定 10 个 UDP 端口和 10 个 TCP 端口。您无法使用您已指定为常见端口的相同端口号。有关详细信息，请参阅 使用 McAfee ePolicy Orchestrator 配置分析器策略。

NMAP 包括服务版本信息扫描

“包括服务版本信息 NMAP”探测通过收集与在设备上运行的软件相关的信息自动扫描终端，以便更好地对它们进行分类。服务版本选项可与通用端口或自定义端口结合使用。

示例：

CLI 命令：nmap -sV -p T:8083 172.21.75.217

输出：

端口	省/自治区	服务	版本
8083/tcp	open	http	McAfee ePolicy Orchestrator 代理 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {15D79A24-3BAB-A0FA-E76C-2F})

NMAP SMB 发现扫描

NMAP SMB 发现扫描有助于区分 Windows 版本并实现更佳终端分析。您可以配置 NMAP 扫描操作来运行 NMAP 提供的 SMB 发现脚本。

NMAP 扫描操作包含在 Windows 默认策略中，而且当终端与策略和扫描规则匹配时，对终端进行扫描，其结果有助于确定确切的 Windows 版本。策略将在源服务上进行配置，新的预定义 NMAP 扫描通过 SMB 发现选项进行创建。

NMAP 扫描操作通过 Microsoft-Workstation 策略调用，而且扫描结果保存在该操作系统属性下的终端中并应用于 Windows 策略。您还可以通过手动扫描子网找到 SMB 发现脚本选项。

注释 对于 SMB 发现，请务必在终端启用 Windows 文件共享选项。

SMB 发现属性 (SMB Discovery Attributes)

当在终端上执行 SMB 发现脚本时，新的 SMB 发现属性（例如 SMB.Operating-system）被添加到终端。当在源服务上更新 Windows 终端分析策略时会考虑这些属性。当运行 SMB 发现脚本时，SMB 发现属性增加了 SMB 前缀，例如 SMB.operating-system、SMB.lanmanager、SMB.server、SMB.fqdn、SMB.domain、SMB.workgroup 和 SMB.cpe。

跳过 NMAP 主机发现

浏览每个 IP 地址的每各端口是一个耗时的过程。根据扫描的目的，您可以跳过活动终端的 NMAP 主机发现。

如果在终端分类后触发 NMAP 扫描，分析器会始终跳过终端的主机发现。但是，如果在启用“跳过 NMAP 主机发现扫描”(Skip NMAP Host Discovery Scan) 之后手动扫描操作被触发，则跳过主机发现。

NMAP 扫描工作流程

执行 NMAP 扫描应遵循以下步骤：

开始之前

要运行 NMAP SMB 发现脚本，必须在系统中启用文件共享。关于示例，请参阅启用文件共享以运行 NMAP SMB 发现脚本主题。

步骤 1 创建 SMB 扫描操作。

步骤 2 使用 SMB 扫描操作配置分析器策略。

步骤 3 使用 SMB 属性添加新条件。

创建 SMB 扫描操作

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。

步骤 2 输入**操作名称**和**描述** 。

步骤 3 选中**运行 SMB 发现脚本 (Run SMB Discovery Script)** 复选框。

步骤 4 点击**添加 (Add)**，创建网络访问用户。

下一步做什么

应使用 SMB 扫描操作配置分析器策略。

使用 SMB 扫描操作配置分析器策略

开始之前

您必须创建一个新的分析器策略以通过 SMB 扫描操作对终端进行扫描。例如，您可以通过指定一条规则来扫描 Microsoft 工作站，该条规则规定如果 DHCP 类标识符包含 MSFT 属性，则应采取网络操作。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入**名称** 和**描述**。

步骤 3 在下拉列表中，选择您已创建的扫描操作（例如，SMBScanAction）。

下一步做什么

您应该使用 SMB 属性添加新的条件。

使用 SMB 属性添加新条件

开始之前

您应创建新的分析器策略扫描终端版本。例如，您可以在 Microsoft Workstation 父策略下扫描 Windows 7。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入**名称** （例如 Windows 7Workstation）和**说明**。

步骤 3 在**网络扫描 (NMAP) 操作 (Network Scan (NMAP) Action)** 下拉列表中，选择**无 (None)**。

步骤 4 在**父组策略 (Parent Policy)** 下拉列表中选择 Microsoft-Workstation 策略。

启用文件共享以运行 NMAP SMB 发现脚本

以下是在 Windows OS 版本 7 中启用文件共享运行 NMAP SMB 发现脚本的示例。

步骤 1 选择**控制面板 (Control Panel)** > **网络和 Internet (Network and Internet)**。

步骤 2 点击**网络和共享中心**。

步骤 3 点击**更改高级共享设置 (Change Advanced Sharing Settings)**。

步骤 4 点击**打开文件和打印机共享 (Turn on File and Printer Sharing)**。

步骤 5 启用以下选项：**为使用 40 或 56 位加密的设备启用文件共享 (Enable File Sharing for Devices That Use 40- or 56-bit Encryption)** 和**打开密码保护共享 (Turn on Password Protected Sharing)**。

步骤 6 点击**保存更改 (Save Changes)**。

步骤 7 配置防火墙设置。

a) 在控制面板中，导航至 **系统和安全 (System and Security)** > **Windows 防火墙 (Windows Firewall)** > **允许程序通过 Windows 防火墙 (Allow a Program Through Windows Firewall)**。

b) 选中**文件和打印机共享 (File and Printer Sharing)** 复选框。

c) 点击**确定 (OK)**。

步骤 8 配置共享文件夹。

a) 右键点击目标文件夹，并选择**属性 (Properties)**。
b) 点击**共享 (Sharing)** 选项卡，然后点击**共享 (Share)**。
c) 在**文件共享 (File Sharing)** 对话框中，添加所需名称并点击**共享 (Share)**。
d) 在选定文件夹共享后，点击**完成 (Done)**。
e) 点击**高级共享 (Advanced Sharing)**，并选择**共享此文件夹 (Share This Folder)** 复选框。
f) 点击 **Permissions**（权限）。
g) 在**扫描权限 (Permissions for Scans)** 对话框中，选择**所有人 (Everyone)**，并选中**完全控制 (Full Control)** 复选框。
h) 点击**确定 (OK)**。

从 NMAP 扫描中排除子网

您可以执行 NMAP 扫描以识别终端的操作系统或 SNMP 端口。

当执行 NMAP 扫描时，您可以排除不应由 NMAP 扫描的完整子网或 IP 范围。您可以在 **NMAP 扫描子网排除项 (NMAP Scan Subnet Exclusions)** 窗口中配置子网或 IP 范围（**工作中心 (Work Centers) > 分析器 (Profiler) > 设置 (Settings) > NMAP 扫描子网排除 (Settings)**）。这有助于限制网络上的负载并节省大量时间。

要进行手动 NMAP 扫描，您可以使用**运行手动 NMAP 扫描 (Run Manual NMAP Scan)** 窗口（**工作中心 (Work Centers) > 分析器 (Profiler) > 手动扫描 (Manual Scans) > 手动 NMAP 扫描 (Manual NMAP Scan) > 在以下范围配置 NMAP 扫描子网排除项 (Configure NMAP Scan Subnet Exclusions At)**）来指定子网或 IP 范围。

手动 NMAP 扫描设置

您可以使用自动 NMAP 扫描的可用选项，执行手动 NMAP 扫描（**工作中心 (Work Centers)** > **分析器 (Profiler)** > **手动扫描 (Manual Scans)** > **手动 NMAP 扫描 (Manual NMAP Scan)**）。您可以选择扫描选项或预定义选项。

表 *101:* 手动 *NMAP* 扫描设置

字段名称	使用指南
节点	选择 NMAP 扫描可运行的 ISE 节点。
手动扫描子网 (Manual Scan Subnet)	输入您要运行 NMAP 扫描的终端的子网 IP 地址范围。
在...配置 NMAP 扫描子网例外情况 (Configure NMAP Scan Subnet Exclusions At)	您将定向到 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **设置 (Settings)** > **NMAP 扫描子网排除项 (NMAP Scan Subnet Exclusions)** 窗口。指定应排除的 IP 地址和子网掩码。如果匹配，则 NMAP 扫描不运行。

字段名称	使用指南
NMAP 扫描子网	• 指定扫描选项 • 或者选择现有的 NMAP 扫描
指定扫描选项	选择所需的扫描选项：OS、SNMP 端口 (SNMP Port)、通用端口 (Common Ports)、自定义端口 (Custom Ports)、包括服务版本信息 (Include Service Version Information)、运行 SMB 发现脚本 (Run SMB Discovery Script)、跳过 NMAP 主机发现 (Skip NMAP Host Discovery)。有关详细信息，请参阅创建新的网络扫描操作。
选择现有的 NMAP 扫描 (Select an Existing NMAP Scan)	显示会显示默认分析器 NMAP 扫描操作的**现有 NMAP 扫描操作 (Existing NMAP Scan Actions)** 下拉列表。
重置为默认扫描选项	点击此选项可恢复默认设置（选中所有扫描选项）。
保存 NMAP 扫描操作 (Save as NMAP Scan Action)	输入操作名称和说明。

运行手动 NMAP 扫描

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **手动扫描 (Manual Scans)** > **手动 NMAP 扫描 (Manual NMAP Scan)**。

步骤 2 在**节点 (Node)** 下拉列表中，选择要运行 NMAP 扫描的 ISE 节点。

步骤 3 在**手动扫描子网 (Manual Scan Subnet)** 文本框中输入要检查开放端口终端的子网地址。

步骤 4 选择以下一个选项：

a) 选择**指定扫描选项 (Specify Scan Options)**，并且在页面右侧选择必填扫描选项。有关详细信息，请参阅创建新的网络扫描操作 页面。

b) 选择**选择现有 NMAP 扫描操作 (Select An Existing NMAP Scan Action)**，以选择默认 NMAP 扫描操作，如 MCAFeeEPOOrchestratorClientScan。

步骤 5 点击**运行扫描 (Run Scan)**。

使用 McAfee ePolicy Orchestrator 配置分析器策略

Cisco ISE 分析服务可以检测终端上是否存在 McAfee ePolicy Orchestrator (McAfee ePO) 客户端。这有助于确定给定终端是否属于您的组织。

在该流程中涉及的实体如下：

- ISE 服务器
- McAfee ePO 服务器
- McAfee ePO 代理

Cisco ISE 能够提供内置的 NMAP 扫描操作 (MCAFeeEPOOrchestratorClientscan) 以便于在配置的端口上使用 NMAP McAfee 脚本来检查 McAfee 代理是否在终端上运行。您还可以使用自定义端口（例如，8082）创建新的 NMAP 扫描选项。您可以按照以下步骤使用 McAfee ePO 软件配置新的 NMAP 扫描操作：

步骤 1 配置 McAfee ePo NMAP 扫描操作。

步骤 2 配置 McAfee ePO 代理。

步骤 3 使用 McAfee ePO NMAP 扫描操作配置分析器策略。

配置 McAfee ePo NMAP 扫描操作

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **策略元素 (Policy Elements)** > **网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入**操作名称 (Action Name)** 和**说明**。

步骤 4 在**扫描选项 (Scan Options)**中，选择**自定义端口 (Custom Ports)**。

步骤 5 在**自定义端口 (Custom Ports)** 对话框中，添加所需的 TCP 端口。默认情况下，8080 TCP 端口为 McAfee ePO 启用。

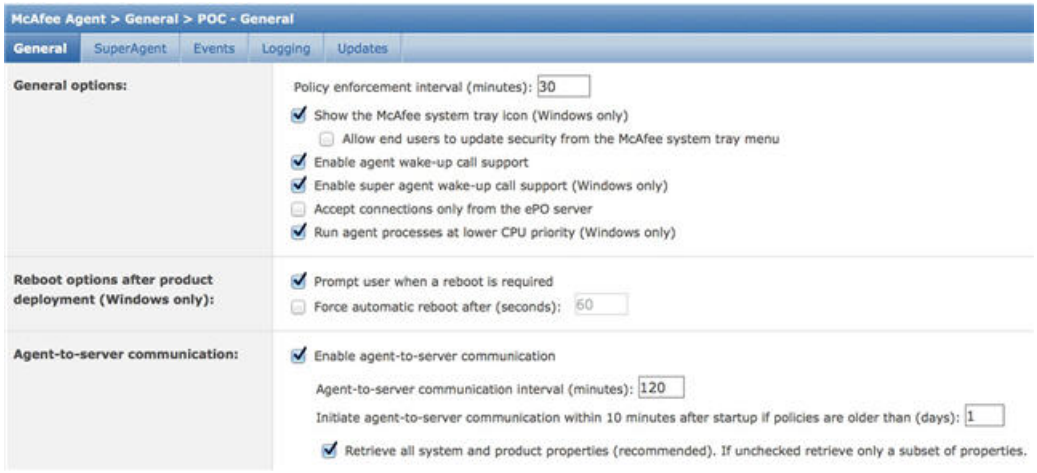
步骤 6 选中**包括服务版本信息 (Include Service Version Information)** 复选框。

步骤 7 点击**提交 (Submit)**。

配置 McAfee ePO 代理

步骤 1 在您的 McAfee ePO 服务器上，选中推荐设置促进 McAfee ePO 代理和 ISE 服务器之间的通信。

图 *29: McAfee ePO* 代理的推荐选项



步骤 2 验证**仅接受来自 ePO 服务器的连接 (Accept Connections Only From The ePO Server)** 已取消选中。

使用 McAfee ePO NMAP 扫描操作配置分析器策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入**名称**和**描述**。

步骤 3 在**网络扫描 (NMAP) 操作 (Network Scan (NMAP) Action)** 下拉列表，请选择所需的操作（例如，MCAFeeEPOOrchestratorClientscan）。

步骤 4 创建父分析器策略（例如，Microsoft 工作站）以包含一条规则用于检查 DHCP 类标识符是否包含 MSFT 属性。

步骤 5 在父 NMAP McAfee ePO 策略（例如，Microsoft 工作站）中创建新策略（例如，CorporateDevice）以检查 McAfee ePO 座席是否在终端上安装。

满足条件的终端作为企业设备进行分析。您可以使用策略将通过 McAfee ePO 代理进行分析的终端移动至新的 VLAN。

分析器终端自定义属性

选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)**，将属性分配给终端，终端通过检测收集的属性除外。终端自定义属性可用于授权策略，以分析终端。

最多可以创建 100 个终端自定义属性。支持的终端自定义属性类型有：Int、String、Long、Boolean 和 Float。

您可以在以下位置添加终端自定义属性的值：**情景目录 (Context Directory)** > **终端 (Endpoints)** > **终端分类 (Endpoint Classification)** 窗口。

终端自定义属性的使用案例包括，基于某些属性允许或阻止设备，或基于授权分配某些权限。

在授权策略中使用终端自定义属性

终端自定义属性部分允许您配置其他属性。每个定义包括属性和类型（String、Int、Boolean、Float、Long)。可以使用终端自定义属性分析设备。

注释 您必须具有思科 ISE Advantage 许可证才能向终端添加自定义属性。

以下步骤演示如何使用终端自定义属性创建授权策略。

步骤 1 创建终端自定义属性并分配值。

a) 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)** 页面。

b) 在**终端客户属性 (Endpoint Custom Attributes)** 区域，输入**属性名称 (Attribute Name)**（例如 deviceType）、数据类型（例如 String）和参数。

c) 点击**保存 (Save)**。

d) 选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **摘要 (Summary)**。

e) 分配自定义属性值。

- 选中所需的 MAC 地址复选框，然后点击**编辑 (Edit)**。
- 或者，点击所需的 MAC 地址，然后在“终端”(Endpoints) 页面上，点击**编辑 (Edit)**。

f) 在**编辑终端 (Edit Endpoint)** 对话框，在**自定义属性 (Custom Attributes)** 区域中输入所需的属性值（例如 deviceType = Apple iPhone ）。

g) 点击**保存 (Save)**。

步骤 2 使用自定义属性和值创建授权策略。

a) 选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

b) 通过从终端词典选择自定义属性创建授权策略（例如规则名称：企业设备，条件：终端：deviceType 包含 Apple-iPhone，权限：则 PermitAccess）。

c) 点击**保存 (Save)**。

相关主题

分析器终端自定义属性 ，第 641 页

创建分析器条件

Cisco ISE 中的终端分析策略允许您对网络上已发现的终端进行分类，并将它们分配到特定的终端身份组。这些终端分析策略由分析条件构成，Cisco ISE 评估这些条件对终端进行分类和分组。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **分析 (Profiling)** > **添加 (Add)**。

步骤 2 输入终端分析策略设置，第 643 页中所描述的字段的值。

步骤 3 点击**提交 (Submit)** 保存分析器条件。

步骤 4 重复此过程创建更多条件。

终端分析策略规则

您可以定义一条规则来允许您从库中选择您之前创建并保存在策略元素库中的一个或多个分析条件，并且允许关联针对每个条件的可信度的整数值，或者为该条件关联例外操作或网络扫描操作。例外操作或网络扫描操作用于触发可配置的操作，而Cisco ISE 则就终端整体分类对分析策略进行评估。

使用 OR 运算符单独评估特定策略中的规则时，每个规则的可信度都会影响终端配置文件与特定终端类别的整体匹配。如果终端分析策略的规则匹配，在您的网络上动态发现分析策略和匹配的策略时，对于该终端分析策略和匹配的策略相同。

规则中的逻辑分组条件

终端分析策略（配置文件）包含单已条件或使用 AND 或 OR 运算符从逻辑上组合的多个单一条件，您可以根据这些条件为策略中的具体规则对终端进行检查、分类和分组。

条件用于按照终端条件中指定的值检查所收集的终端属性值。如果映射不止一个属性，您可以按逻辑给条件分组，这样可以帮助您给您的网络上的终端分类。您可以根据一个或多个条件检查终端，在规则中为其关联相应的可信度指标（即您所定义的整数值），也可以触发与条件关联的例外操作或与条件关联的网络扫描操作。

可信度

分析策略中的最低可信度用于评估终端的匹配配置文件。终端分析策略中每条规则都有一个与分析条件关联的最低可信度指标（一个整数）。可信度指标是为终端分析策略中所有有效规规则增加的一个衡量标准，用于衡量终端分析策略中各个条件对于提高终端整体分类的影响。

各条规则的可信度都会影响终端配置文件与具体终端类别的整体匹配度。所有有效规则的可信度相加形成匹配可信度。它必须超过终端分析策略中定义的最低可信度。默认情况下，所有新分析策略规则和预定义分析策略的最低可信度为 10。

终端分析策略设置

下表列出了**终端策略 (Endpoint Policies)** 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

表 *102:* 终端分析策略设置

字段名称	使用指南
Name	输入要创建的终端分析策略的名称。
Description	输入要创建的终端分析策略的说明。
Policy Enabled	默认情况下，**Policy Enabled** 复选框处于选中状态，以便在您分析终端时关联匹配的分析策略。 如果未选中此复选框，则在您分析终端时会排除终端分析策略。
Minimum Certainty Factor	输入要与分析策略相关联的最小值。默认值为 10。
Exception Action	选择在分析策略中定义规则时要与条件关联的例外操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 例外操作 (Exception Actions)**。
Network Scan (NMAP) Action	从列表中选择在分析策略中定义规则时（如有必要）要与条件关联的网络扫描操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。
Create an Identity Group for the policy	选择以下选项之一以创建终端身份组： • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	选择此选项以使用现有的分析策略。 此选项可为那些终端创建匹配的身份组，当终端配置文件与现有的分析策略相匹配时，身份组将是已分析的终端身份组的子项。 例如，在网络中发现的终端与 Xerox-Device 配置文件相匹配时，系统会在 Endpoints Identity Groups 页面创建 Xerox-Device 终端身份组。

字段名称	使用指南
No, use existing Identity Group hierarchy	选中此复选框可使用分析策略和身份组的层次结构将终端分配给匹配的父终端身份组。 通过此选项，可以使用终端分析策略层次结构将终端分配给其中一个匹配的父终端身份组，以及父身份组的关联终端身份组。 例如，与现有配置文件相匹配的终端会归入相应的父终端身份组中。在本例中，与 Unknown 配置文件相匹配的终端会归入 Unknown 终端身份组中，与现有配置文件相匹配的终端会归入 Profiled 终端身份组中。例如， • 如果终端与 Cisco-IP-Phone 配置文件相匹配，则这些终端会归入 Cisco-IP-Phone 终端身份组中。 • 如果终端与 Workstation 配置文件相匹配，则这些终端会归入 Workstation 终端身份组中。 Cisco-IP-Phone 和 Workstation 终端身份组与系统中的 Profiled 终端身份组相关联。
Parent Policy	选择在系统中定义的、要与新终端分析策略相关联的父分析策略。 可以选择可将规则和条件继承到其子项的父分析策略。
Associated CoA Type	选择以下要与终端分析策略相关联的 CoA 类型之一： • No CoA • Port Bounce • Reauth • Global Settings，该设置是从在 Administration > System > Settings > Profiling 中设置的分析器配置进行应用
Rules	在终端分析策略中定义的一个或多个规则为终端确定了匹配的分析策略，这允许您根据终端配置文件对终端进行分组。 策略要素库中的一个或多个分析条件用于规则，以验证终端属性及其整体分类值。

字段名称	使用指南
Conditions	点击加号 [+] 展开 Conditions 固定重叠，点击减号 [-] 或点击固定重叠的外部可将其折叠。 点击 **从库中选择现有条件 (Select Existing Condition from Library)** 或 **创建新条件（高级选项）(Create New Condition (Advanced Option))**。 **从库中选择现有条件 (Select Existing Condition from Library)**：可以通过从策略元素库中选择Cisco预定义条件来定义表达式。 **创建新条件（高级选项）(Create New Condition (Advanced Option))**：可以通过从各种系统或用户定义的字典中选择属性来定义表达式。 可以将以下其中一项与分析条件相关联： • 每种条件的可信度的整数值。 • 为该条件输入例外操作或网络扫描操作 选择以下其中一个要与分析条件相关联的预定义设置： • “可信度增加”(Certainty Factor Increases)：为每个规则输入可信度值，可以为与整体分类相关的所有匹配规则添加此可信度值。 • “采取例外操作”(Take Exception Action)：触发在此终端分析策略的“例外操作”(Exception Action) 字段中配置的例外操作。 • “采取网络扫描操作”(Take Network Scan Action)：触发在此终端分析策略的“网络扫描 (NMAP) 操作”(Network Scan (NMAP) Action) 字段中配置的网络扫描操作。

字段名称	使用指南
Select Existing Condition from Library	可以执行以下操作： • 可以选择策略要素库中可用的Cisco预定义条件，然后使用 AND 或 OR 运算符添加多个条件。 • 点击 Action 图标，在后续步骤中执行以下操作： • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对 • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件 • **复制 (Duplicate)**：创建选定条件的副本 • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中 • **删除 (Delete)**：删除所选条件。
创建新条件（高级选项）	可以执行以下操作： • 可以将临时属性/值对添加到表达式，然后使用 AND 或 OR 运算符添加多个条件。 • 点击 Action 图标，在后续步骤中执行以下操作： • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对 • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件 • **复制 (Duplicate)**：创建选定条件的副本 • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中 • **删除 (Delete)**：删除所选条件。可以使用 AND 或 OR 运算符

相关主题

思科 ISE 分析服务 ， 第 603 页

创建终端分析策略，第 648 页
使用 UDID 属性的终端情景可视性，第 679 页

创建终端分析策略

您可以通过使用 New Profiler Policy 页面中的以下选项，创建用于分析终端的新分析策略：

- Policy Enabled
- Create an Identity Group，让策略创建匹配的终端身份组或使用终端身份组层次结构
- Parent Policy
- Associated CoA Type

注释 当您选择在**分析策略 (Profiling Policies)** 窗口中创建终端策略时，请勿使用 Web 浏览器中的“停止”(Stop) 按钮。此操作会导致以下结果：停止加载**新分析器策略 (New Profiler Policy)** 窗口、在访问时加载其他列表页面及列表页面内的菜单，以及防止您对列表页面内的所有菜单执行操作，“过滤器”(Filter) 菜单除外。您可能需要注销Cisco ISE，然后重新登录才能对列表菜单内的所有菜单执行操作。

您可以通过复制终端分析策略来创建类似特征的分析策略，这样您就可以修改现有的分析策略，而不是通过重新定义所有条件来创建新分析策略。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入要创建的新终端政策的名称和说明。**Policy Enabled** 复选框在默认情况下处于选中状态，以包含用于在分析终端时进行验证的终端分析策略。

步骤 4 输入最低可信度的值，有效范围为 1 至 65535。

步骤 5 点击 **Exception Action** 下拉列表旁边的箭头以关联例外操作，或点击 **Network Scan (NMAP) Action** 下拉列表旁边的箭头以关联网络扫描操作。

步骤 6 为 **Create an Identity Group for the policy** 选择以下其中一个选项：

- **Yes, create matching Identity Group**
- **No, use existing Identity Group hierarchy**

步骤 7 点击 **Parent Policy** 下拉列表旁边的箭头将父策略关联到新终端策略。

步骤 8 在 **Associated CoA Type** 下拉列表中选择要关联的 CoA 类型。

步骤 9 点击规则以添加条件并为每个条件的可信度关联一个整数值或为该条件关联例外操作或网络扫描操作，以对终端进行整体分类。

步骤 10 在新建分析器策略 (New Profiler Policy) 页面中点击**提交 (Submit)** 以添加终端策略，或点击**分析器策略列表 (Profiler Policy List)** 链接以返回分析策略 (Profiling Policies) 页面。

每个终端分析策略的授权更改配置

除了Cisco ISE 中授权更改 (CoA) 类型的全局配置，您还可以配置为每个终端分析策略发出特定类型的关联 CoA。

全局 No CoA 类型配置会覆盖终端分析策略中配置的每个 CoA 类型。如果全局 CoA 类型设置的不是 No CoA 类型，则系统允许每个终端分析策略覆盖全局 CoA 配置。

当触发 CoA 时，每个终端分析策略都可以决定实际 CoA 类型，如下所示：

- General Setting - 这是适用于所有终端分析策略的根据全局配置发出 CoA 的默认设置。
- No CoA - 此设置会覆盖任何全局配置并为配置文件禁用 CoA。
- Port Bounce - 此设置会覆盖全局 Port Bounce 和 Reauth 配置类型，并发出端口退回 CoA。
- Reauth - 此设置会覆盖全局 Port Bounce 和 Reauth 配置类型，并且发出重新身份验证 CoA。

注释 如果分析器全局 CoA 配置设置为 Port Bounce（或 Reauth），请确保您将相应终端分析策略配置为基于策略的 CoA 选项 No CoA，从而使您的移动设备不会出现自带设备流程中断。

请参阅下表中对所有 CoA 类型和根据全局和终端分析策略设置在每个案例中实际发出的 CoA 类型的配置总结。

表 *103:* 为各种配置组合发出的 *CoA* 类型

全局 **CoA** 类型	根据策略设置的默认 **CoA** 类型	根据策略的 **No CoA** 类型	根据策略的端口退回类型	根据策略的重新身份验证类型
No CoA	No CoA	No CoA	No CoA	No CoA
Port Bounce	Port Bounce	No CoA	Port Bounce	Re-Auth
Reauth	Reauth	No CoA	Port Bounce	Re-Auth

导入终端分析策略

使用可以在导出功能中创建的相同格式，从 XML 文件导入终端分析策略。如果导入已关联父策略的新建分析策略，则必须在定义子策略之前定义父策略。

导入的文件包含终端分析策略层级结构，首先包含父策略，其次是导入的配置文件，然后是在策略中定义的规则和考核。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 点击**导入 (Import)**。

步骤 3 点击**浏览 (Browse)**，找到您之前导出而现在想要导入的文件。

步骤 4 点击**提交 (Submit)**。

步骤 5 点击**分析器策略列表 (Profiler Policy List)** 链接，返回“分析策略”(Profiling Policies) 页面。

导出终端分析策略

您可以将终端分析策略导出到其他Cisco ISE 部署中。或者，您可以使用 XML 文件作为模板创建您自己的策略并导入。您还可以将该文件下载到您系统中的默认位置，以用于日后的导入。

当您导出终端分析策略时会出现一个对话框，提示您使用适当的应用打开 profiler_policies.xml 或将其保存。此文件的格式为 XML，您可以使用网页浏览器打开，也可以用其他适当的应用打开。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 选择**导出 (Export)**，并选择以下一项：

- **导出所选 (Export Selected)**：您仅可以导出在“分析策略”(Profiling Policies) 页面中选择的终端分析策略。
- **导出所选及终端 (Export Selected with Endpoints)**：可以导出所选择的终端分析策略，以及使用所选择的终端分析策略分析的终端。
- **全部导出 (Export All)**：默认情况下，可以导出“分析策略”(Profiling Policies) 页面中的所有分析策略。

步骤 3 点击“确定”(OK) 以在 profiler_policies.xml 文件中导出终端分析策略。

预定义终端分析策略

部署Cisco ISE 时，Cisco ISE 包含预定义的默认分析策略，这些策略的分层结构允许您对网络上的已识别终端进行分类，并将它们分配给匹配的终端身份组。因为终端分析策略采用分层结构，所以您会发现，Profiling Policies 页面显示设备的通用（母）策略列表，Profiling Policies 列表页面显示与母策略关联的子策略。

无论是否启用以用于验证，Profiling Policies 页面都显示终端分析策略及其名称、类型、描述和状态。

终端分析策略类型分类如下：

- Cisco Provided - 在Cisco ISE 中预定义的终端分析策略被识别为 Cisco Provided 类型。
  - Administrator Modified - 修改预定义的终端分析策略时，终端分析策略被识别为 Administrator Modified 类型。Cisco ISE 将在升级过程中覆盖您在预定义终端分析策略中所做的更改。
- Administrator Created - 您创建的终端分析策略或者当您复制Cisco提供的终端分析策略时，被识别为 Administrator Created 类型。

我们建议为一组终端创建通用策略（母策略），其子策略能够继承规则和条件。如果终端必须归类，那么终端配置文件必须首先匹配母策略，当您分析终端时，再匹配后代（子）策略。

例如，Cisco-Device 是一个适用于所有Cisco设备的通用终端分析策略，适用于Cisco设备的其他策略则为 Cisco-Device 的子策略。如果终端必须归类为 Cisco-IP-Phone 7960，那么此终端的终端配置文件必须首先匹配母 Cisco-Device 策略、子 Cisco-IP-Phone 策略，然后匹配 Cisco-IP-Phone 7960 分析策略，以便更好地分类。

注释 Cisco ISE 不会覆盖管理员修改的策略及其子策略，即使这些策略仍标记为Cisco提供。如果管理员修改的策略被删除，它会恢复为以前的Cisco提供的策略。下一次发生源更新时，所有子策略都会更新。

在升级期间覆盖预定义终端分析策略

您可以在 Profiling Policies 页面编辑现有的终端分析策略。此外，当您想要修改预定义终端分析策略时，必须在预定义终端配置文件副本中保存所有配置。

在升级过程中，Cisco ISE 重写您在预定义终端配置文件中保存的任何配置。

无法删除终端分析策略

您可以在**分析策略 (Profiling Policies)** 窗口中删除选定的或所有终端分析策略。默认情况下，可以从**分析策略 (Profiling Policies)** 窗口删除所有终端分析策略。当在**分析策略 (Profiling Policies)** 窗口中选择所有终端分析策略并尝试删除它们时，如果其中有些终端分析策略映射至其他终端分析策略或映射至授权策略，则可能不会删除它们。

- 您无法删除Cisco提供的终端分析策略，
- 当终端配置文件定义为其他终端配置文件的父级时，您无法在**分析策略 (Profiling Policies)** 窗口中删除父配置文件。例如，Cisco-Device 是用于Cisco设备的其他终端分析策略的父级。
- 当某个终端配置文件映射至授权策略时，您无法删除此终端配置文件。例如，Cisco-IP-Phone 映射至 Profiled Cisco IP Phones 授权策略而且是用于Cisco IP 电话的其他终端分析策略的父级。

用于 Draeger 医疗设备的预定义分析策略

Cisco ISE 包含默认终端分析策略，这些策略包括用于 Draeger 医疗设备的通用策略、用于 Draeger-Delta 医疗设备的策略，以及用于 Draeger-M300 医疗设备的策略。两个医疗设备共用端口 2050 和 2150，因此当您使用默认 Draeger 终端分析策略时，您无法给 Draeger-Delta 和 Draeger-M300 医疗设备分类。

如果这些 Draeger 设备在您的环境中共用端口 2050 和 2150，除了在默认 Draeger-Delta 和 Draeger-M300 终端分析策略中检查设备目标 IP 地址之外，您还必须增加一条规则以确保您可以区分这些医疗设备。

Cisco ISE 包括用于 Draeger 医疗设备终端分析策略的以下分析策略：

- 包含端口 2000 的 Draeger-Delta-PortCheck1
- 包含端口 2050 的 Draeger-Delta-PortCheck2
- 包含端口 2100 的 Draeger-Delta-PortCheck3
- 包含端口 2150 的 Draeger-Delta-PortCheck4
- 包含端口 1950 的 Draeger-M300PortCheck1
- 包含端口 2050 的 Draeger-M300PortCheck2
- 包含端口 2150 的 Draeger-M300PortCheck3

用于未知终端的终端分析策略

不匹配现有的配置文件且无法在Cisco ISE 中分析的终端为未知终端。未知配置文件是分配给终端的默认系统分析策略，为此终端收集的一个属性或一组属性与Cisco ISE 中现有的配置文件不匹配。

在以下情境中分配未知配置文件：

- 在Cisco ISE 中动态地发现终端，并且没有适用于此终端的匹配终端分析策略时，将终端分配给未知配置文件。
- 当Cisco ISE 中静态地添加终端，且没有适用于静态添加的终端的匹配终端分析策略时，将终端分配给未知配置文件。

  如果将终端静态地添加到网络，Cisco ISE 中的分析服务不分析静态添加的终端。稍后，您可以将未知配置文件更改为相应的配置文件，Cisco ISE 不会重新分配您已分配的分析策略。

用于静态添加的终端的终端分析策略

对于静态添加以进行分析的终端，分析服务将新的 MATCHEDPROFILE 属性添加到终端，为终端计算配置文件。如果动态分析终端，那么计算的配置文件则是该终端的实际配置文件。这样，您可以发现静态添加的终端的计算配置文件与动态分析的终端的匹配配置文件不匹配的情况。

静态 IP 设备的终端分析策略

如果您的终端拥有静态分配的 IP 地址，则您可以为这些静态 IP 设备创建配置文件。

必须启用 RADIUS 探测功能或 SNMP 查询和 SNMP 陷阱探测功能，分析拥有静态 IP 地址的终端。

终端分析策略匹配

当在分析策略中满足一个或多个规则中定义的分析条件时，Cisco ISE 会始终将终端的所选策略视为匹配策略而不是已评估的策略。此处，该终端的静态分配的状态在系统中设置为 false。但是，通过在终端编辑过程中使用静态分配功能，可以在将该终端重新静态分配给系统中的现有分析策略后将状态设置为 true。

以下操作适用于终端的匹配策略：

- 对于静态分配的终端，分析服务会计算 MATCHEDPROFILE。
- 对于动态分配的终端，MATCHEDPROFILE 与匹配终端配置文件相同。

您可以使用分析策略中定义的一个或多个规则确定动态终端的匹配分析策略，并且相应地分配终端身份组以进行分类。

当终端映射到现有策略时，分析服务会搜索分析策略的层次结构以查找具有匹配策略组的最近父配置文件，并将终端分配给相应的终端策略。

用于授权的终端分析策略

您可以在授权规则中使用终端分析策略，在其中您可以创建作为属性的新条件，使之包含终端分析策略检查，并且该属性以终端分析策略的名称作为属性值。您可以从终端字典选择终端分析策略，其中包含以下属性：PostureApplicable、EndPointPolicy、LogicalProfile 和 BYODRegistration。

PostureApplicable 的属性值根据操作系统自动设置。对于 IOS 和 Android 设备，它设置为否 *(No)*，因为这些平台上不能使用 AnyConnect 支持来执行终端安全评估。对于 Mac OSX 和 Windows 设备，该值设置为是 *(Yes)*。

您可以定义包括 EndPointPolicy、BYODRegistration 和身份组的组合的授权规则。

终端分析策略分组为逻辑配置文件

逻辑配置文件是一类配置文件或相关联配置文件的容器，无需考虑终端分析策略是由Cisco提供还是由管理员创建。终端分析策略可以与多个逻辑配置文件关联。

您可以在授权策略条件中使用逻辑配置文件，来帮助您创建针对某类别配置文件的整体网络接入策略。您可以创建授权的简单条件，该条件可包括在授权规则中。您可以在授权条件中使用的属性-值对是逻辑配置文件（属性）和逻辑配置文件名称（值），该属性-值对位于终端系统字典中。

例如，通过将与移动设备类别匹配的终端分析策略分配至逻辑配置文件，可以为所有移动设备（如安卓、苹果 iPhone 或黑莓）创建一个逻辑配置文件。Cisco ISE 包含 IP 电话，这是一个针对所有 IP

电话的默认逻辑配置文件，包括 IP 电话、Cisco IP 电话、Nortel IP 电话 2000 系列和 AVAYA IP 电话配置文件。

创建逻辑配置文件

您可以创建可用于对某个类别的终端分析策略进行分组的逻辑配置文件，借此可创建整体类别的配置文件或关联配置文件。您还可以从分配的集合中删除终端分析策略，从而将其移回到可用集合。有关逻辑配置文件的详细信息，请参阅终端分析策略分组为逻辑配置文件，第 653 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **逻辑配置文件 (Logical Profiles)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**名称 (Name)** 和**说明 (Description)** 的文本框中输入新逻辑配置文件的名称和说明。

步骤 4 从**可用策略 (Available Policies)** 中选择终端分析策略以在逻辑配置文件中对其进行分配。

步骤 5 点击向右箭头以将所选终端分析策略移至**分配策略 (Assigned Policies)**。

步骤 6 点击**提交 (Submit)**。

分析例外操作

例外操作是终端分析策略中可以引用的一个可配置操作，当符合该操作关联的例外条件时就会触发例外操作。

例外操作可以是以下任一类型：

- Cisco-provided - 您不能删除Cisco提供的例外操作。当您要在Cisco ISE 中分析终端时，Cisco ISE 从系统中触发以下非可编辑的分析例外操作：
  - Authorization Change - 当从授权策略使用的终端身份组添加或删除终端时，此分析服务发出授权更改。
  - Endpoint Delete - 当在 Endpoints 页面从系统中删除终端或在Cisco ISE 网络中从 Edit 页面向已知配置文件分配终端时，在Cisco ISE 中会触发例外操作并且会发出 CoA。
  - FirstTimeProfiled - 当在Cisco ISE 中首次分析某个终端时，如果该终端的配置文件从未知配置文件转变为现有配置文件，但是在Cisco ISE 网络中该终端身份验证未成功，则在Cisco ISE 中会触发例外操作并且会发出 CoA。
- Administrator-created - Cisco ISE 触发您所创建的分析例外操作。

创建例外操作

您可以定义一个或多个例外规则并将其关联到单个分析策略。此关联会在分析策略和至少一个例外规则在Cisco ISE 中的分析终端中匹配时触发例外操作（单个可配置操作）。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **分析 (Profiling)** > **例外操作 (Exception Actions)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在 **名称** 和 **说明** 的文本框中输入例外操作的名称和说明。

步骤 4 选中 **CoA Action** 复选框。

步骤 5 选中 **Policy Assignment** 下拉列表以选择终端策略。

步骤 6 点击**提交 (Submit)**。

使用策略和身份的静态分配创建终端

在终端页面中，您可以使用终端的 MAC 地址静态创建新的终端。在终端页面中，您还可以选择静态分配的终端分析策略和身份组。

常规和移动设备 (MDM) 终端会显示在终端身份列表中。在列表页面中会显示 MDM 终端的属性列，这些属性包括主机名、设备类型、设备标识符。其他列如静态分配和静态组分配在默认情况下不显示。

注释 您无法使用此页面添加、编辑、删除、导入或导出 MDM 终端。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入十六进制格式的终端 MAC 地址，以冒号分隔。

步骤 4 从 **Policy Assignment** 下拉列表中选择一个匹配的终端策略，将其静态分配状态从动态更改为静态。

步骤 5 选中 **Static Assignment** 复选框，将分配到终端的静态分配的状态从动态更改为静态。

步骤 6 从 **Identity Group Assignment** 下拉列表中选择您希望分配到新创建终端的终端身份组。

步骤 7 选中 **Static Group Assignment** 复选框，将终端身份组的动态分配更改为静态。

步骤 8 点击**提交 (Submit)**。

从 CSV 文件导入终端

您可以从已从Cisco ISE 模板创建的 CSV 文件导入终端，并使用终端详细信息进行更新。从 ISE 导出的终端包含约 75 个属性，因此无法直接导入到另一 ISE 部署中。如果 CSV 文件中存在不允许导入的列，则会显示包含列列表的消息。尝试再次导入文件之前，必须删除指定的列。

注释 要导入终端自定义属性，必须使用正确的数据类型在**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)** 页面创建与 CSV 文件中相同的自定义属性。这些属性必须添加“CUSTOM.”前缀以便与终端属性区分。

大约有 30 个可以导入的属性。此列表包括 MACAddress、EndPointPolicy 和 IdentityGroup。可选属性为：

说明	PortalUser	lastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	设备类型	host-name
PortalUser.GuestStatus	StaticAssignment	位置
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<自定义属性名称>	-	-

文件标题行必须是在默认导入模板中指定的格式，使终端列表按以下顺序显示：MACAddress、EndpointPolicy、IdentityGroup <以上作为可选属性的属性列表>。可以创建以下文件模板：

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <以上作为可选属性的属性列表>

所有属性值（MACAddress 除外）对于从 CSV 文件导入终端均是可选的。如果想要导入终端而无需特定值，值依然用逗号分隔。

例如，

- MAC1, Endpoint Policy1, Endpoint Identity Group1

- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, 等

步骤 1 选择 情景可视性 **(Context Visibility)** > 终端 **(Endpoints)** > 导入 **(Import)**。

步骤 2 点击从文件导入 **(Import From File)**。

步骤 3 点击浏览 **(Browse)** 找到您已创建的 CSV 文件。

步骤 4 点击提交 **(Submit)**。

可用于终端的默认导入模板

您可以生成可以在其中更新终端的模板，您可将其用于导入终端。默认情况下，您可以使用 生成模板 链接，在 Microsoft Office Excel 应用中创建 CSV 文件并将文件保存在您的系统本地位置上。文件位于以下位置： **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **导入 (Import)** > **从文件导入 (Import From File)**。您可以使用 生成模板 链接创建模板，并且Cisco ISE 服务器将显示 Opening template.csv 对话框。您可以通过此对话框打开默认 template.csv 文件，或将 template.csv 文件保存在您的系统本地位置上。如果您选择从此对话框打开 template.csv 文件，系统会使用 Microsoft Office Excel 应用打开此文件。默认的 template.csv 文件包含一个标题行，其中显示 MAC 地址、终端策略、终端身份组和其他可选属性。。

您必须更新终端的 MAC 地址、终端分析策略、终端身份组和任何要导入的可选属性值，并使用新文件名保存文件。此文件可用于导入终端。请参阅您使用 生成模板 时创建的 template.csv 文件中的标题行。

表 ***104: CSV*** 模板文件

MAC	EndpointPolicy	IdentityGroup	其他可选属性
11:11:11:11:11:11	Android	Profiled	<空>/<值>

导入过程中重新分析的未知终端

如果用于导入的文件包含具有 MAC 地址的终端，并且其已分配的终端分析策略是 Unknown 配置文件，则这些终端会在Cisco ISE 中立即重新分析到导入过程中的匹配终端分析策略。但是，系统不会将它们静态分配到 Unknown 配置文件。如果终端在 CSV 文件中没有向其分配的终端分析策略，则它们会分配到 Unknown 配置文件，然后重新分析到匹配的终端分析策略。请参阅以下内容，了解 Cisco ISE 如何在导入过程中重新分析与 Xerox_Device 配置文件匹配的 Unknown 配置文件，以及Cisco ISE 如何重新分析未分配的终端。

表 *105: Unknown* 配置文件：从文件导入

MAC 地址	Cisco ISE 中导入前分配的终端分析策略	Cisco ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	Unknown。	Xerox-Device
00:00:00:00:01:03	Unknown。	Xerox-Device
00:00:00:00:01:04	Unknown。	Xerox-Device
00:00:00:00:01:05	如果未向终端分配配置文件，则该终端会分配到 Unknown 配置文件，并且还会重新分析到匹配的配置文件。	Xerox-Device

不导入具有无效属性的终端

如果 CSV 文件中存在的任何终端具有无效属性，则不导入该终端，并显示错误消息。

例如，如果终端被分配至用于导入的文件中的无效配置文件，因为Cisco ISE 中没有匹配的配置文件，所以不会导入这些无效配置文件。请参阅下文，了解当终端被分配至CSV 文件中的无效配置文件时，如何不导入终端。

表 *106:* 无效配置文件：从文件导入

MAC 地址	Cisco ISE 中导入前分配的终端分析策略	Cisco ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	Unknown。	Xerox-Device
00:00:00:00:01:05	如果向无效配置文件而不是向 Cisco ISE 中可用的配置文件分配 00:00:00:00:01:05 等终端，则 Cisco ISE 会显示警告消息，提示此策略名称无效并且将不导入该终端。	因为Cisco ISE 中没有匹配的配置文件，所以不会导入该终端。

从 LDAP 服务器导入终端

可以安全地从 LDAP 服务器导入终端的 MAC 地址、关联的配置文件和终端身份组。

开始之前

在开始导入终端之前，请确保已安装 LDAP 服务器。

必须配置连接设置和查询设置才能从 LDAP 服务器导入。如果Cisco ISE 中的连接设置或查询设置配置不正确，则系统会显示“LDAP import failed:”错误消息。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **导入 (Import)** > **从 LDAP 导入 (Import From LDAP)**。

步骤 2 输入连接设置的值。

步骤 3 输入查询设置的值。

步骤 4 点击**提交 (Submit)**。

使用逗号分隔值文件导出终端

您可以从Cisco ISE 服务器将选定的终端或所有终端导出到 CSV 文件中，其中会列出约 75 个属性以及终端的 MAC 地址、终端分析策略和终端身份组。在Cisco ISE 中创建的自定义属性也会导出到 CSV 文件并增加“CUSTOM.”前缀，以便与其他终端属性区分。

注释 要将从一个部署导出的终端自定义属性导入到另一部署，必须在**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)** 窗口中创建相同的自定义属性，并使用原始部署中指定的相同数据类型。

导出全部 (Export All) 可导出Cisco ISE 中的所有终端，而**导出所选 (Export Selected)** 可仅导出用户选择的终端。默认情况下，profiler_endpoints.csv 是 CSV 文件，而 Microsoft Office Excel 是打开 CSV 文件的默认应用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**。

步骤 2 点击**导出 (Export)**，并选择下列选项之一：

- **导出所选 (Export Selected)**：只能导出在**终端 (Endpoints)** 窗口中选定的终端。
- **全部导出 (Export All)**：默认情况下，可以导出**终端 (Endpoints)** 窗口中的所有终端。

步骤 3 点击**确定 (OK)** 保存 profiler_endpoints.csv 文件。

已识别的终端

Cisco ISE 显示已识别的终端，这些终端在终端页面中连接到您的网络并使用您网络上的资源。终端通常是一个支持网络的设备，该设备通过有线和无线网络接入设备和VPN连接到您的网络。终端可以是个人计算机、笔记本、IP 电话、智能手机、游戏主机、打印机、传真机等等。

以十六进制显示的终端 MAC 地址通常唯一地表示一个终端，但是您也可以使用一组变化的属性以及与这些属性关联的值（属性-值对）来标识终端。您可以根据终端的功能、网络接入设备的配置以及您用于收集这些属性的方法（探测），收集一组变化的终端属性。

已动态分析的终端

当在您的网络上发现终端时，根据已配置的终端分析策略，即可对这些终端进行动态分析，并按照配置文件将这些终端分配到匹配的终端身份组。

已静态分析的终端

当您使用终端的 MAC 地址在Cisco ISE 中创建终端并将配置文件及终端身份组与其关联时，即可静态分析该终端。Cisco ISE 不会重新分配已静态分配终端的分析策略和身份组。

未知终端

如果终端缺少匹配的分析策略，您可以分配一个未知分析策略（未知），而终端则会被分析为未知。由未知终端策略分析的终端需要您使用已收集的一个终端属性或一组终端属性来创建配置文件。与所有配置文件均不匹配的终端会被分组到未知终端身份组中。

策略服务节点数据库中本地存储的已识别终端

Cisco ISE 在本地将已识别的终端写入策略服务节点数据库。将这些终端在本地存储于数据库中之后，只有在终端中重要属性出现变更时，在管理节点数据库中这些终端才可用（远程写入），并且被复制到其他策略服务节点数据库中。

以下是重要属性：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

当您在Cisco ISE 中更改终端配置文件定义时，所有终端都必须重新进行分析。收集终端属性的策略服务节点负责重新分析这些终端。

当策略服务节点开始收集关于某个终端的属性时，如果一开始该终端是由另一个不同的策略服务节点收集其属性，则该终端的所有权就改为属于当前策略服务节点。新策略服务节点会从之前的策略服务节点检索最新属性，并且将所收集的这些属性与已经收集的那些属性进行比较。

当终端中某个重要属性发生变更时，该终端的属性会自动保存在管理节点数据库中，这样您就会获得该终端中最新的重要变更。如果拥有某个终端的策略服务节点由于某些原因不可用，则管理员 ISE 节点将会重新分析失去所有者的终端而且您必须为这些终端配置新的策略服务节点。

集群中的策略服务节点

Cisco ISE 将策略服务节点组用作集群，如果集群中两个或多个节点为同一终端收集属性，集群将允许交换终端属性。我们建议您为负载均衡器后面的所有策略服务节点创建集群。

如果与当前所有者不同的节点接收到同一终端的属性，此节点会在集群中发送一条向当前所有者请求最新属性的消息以合并属性并确定是否需要更改所有权。如果您未在Cisco ISE 中定义节点组，系统会假定所有节点都处于同一集群中。

Cisco ISE 不会更改终端创建和复制，只会根据从静态属性和动态属性构建的用于分析的许可属性列表决定是否更改终端的所有权。

在以后的属性收集中，如果以下任一属性发生更改，管理节点上会更新终端：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

在管理节点中编辑和保存终端时，系统会从当前终端所有者检索属性。

创建终端身份组

Cisco ISE 将其所发现的终端划分至相应的终端身份组。Cisco ISE 拥有若干个系统定义的终端身份组。您还从 Endpoint Identity Groups 页面创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为您想要创建的终端身份组输入**名称**（请勿在终端身份组的名称中包含空格）。

步骤 4 为您想要创建的终端身份组输入**说明**。

步骤 5 点击**父级组 (Parent Group)** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

步骤 6 点击**提交 (Submit)**。

已识别终端划分为终端身份组

Cisco ISE 根据终端分析策略，将已发现的终端划分为对应的终端身份组。分析策略分为不同的层级，在Cisco ISE 中在终端身份组级应用。通过将终端划分为终端身份组，并且将分析策略应用到终端身份组，Cisco ISE 使您能够查看对应的终端分析策略，确定终端到终端配置文件的映射。

默认情况下，Cisco ISE 创建终端身份组集合，允许您创建自己的身份组，动态或静态地向其分配终端。您可以创建终端身份组，将身份组关联到系统创建的身份组之一。此外，您还可以将您创建的终端静态地分配到系统中存在的身份组之一，分析服务不能重新分配身份组。

为终端创建的默认终端身份组

Cisco ISE 创建以下终端身份组：

- “黑名单”(Blacklist) - 此终端身份组包括Cisco ISE 中静态分配给此组的终端和在设备注册门户中列入黑名单的终端。可以在Cisco ISE 中定义授权配置文件以允许或拒绝为该组中的终端提供网络接入。
- GuestEndpoints - 此终端身份组包括访客用户使用的终端。
- “分析”(Profiled) - 此终端身份组包括Cisco ISE 中除Cisco IP 电话和工作站之外与终端分析策略匹配的终端。
- RegisteredDevices - 此终端身份组包括属于员工通过设备注册门户添加的已注册设备的终端。当这些设备分配至该组时，分析服务会继续正常分析这些设备。终端在Cisco ISE 中会静态分配至该组，而且分析服务无法将其重新分配到任何其他身份组。这些设备会像任何其他终端一样显示在终端列表上。您可以在Cisco ISE 中的“终端”(Endpoints) 窗口从终端列表编辑、删除和阻止通过设备注册门户添加的这些设备。您在设备注册门户中阻止的设备会分配至“黑名单”终端身份组，而且Cisco ISE 中存在的一个授权配置文件会将被阻止的设备重定向显示“未授权的网络访问”(Unauthorised Network Access) 的 URL，这是被阻止设备的默认门户页面。
- “未知”(Unknown) - 此终端身份组包括与Cisco ISE 中任何配置文件都不匹配的终端。

除了上述系统创建的终端身份组，Cisco ISE还会创建以下终端身份组，这些身份组与“分析”(Profiled) 身份组关联：父组是系统中存在的默认身份组：

- Cisco-IP-Phone - 此身份组包含您的网络上所有已分析的Cisco IP 电话。
- Workstation - 此身份组包含您的网络上所有已分析的工作站。

为匹配的终端分析策略创建的终端身份组

如果您有终端策略与现有策略匹配，则分析服务可以创建一个匹配的终端身份组。此身份组就成为已分析终端身份组的子级。当您创建终端策略时，您可以在 Profiling Policies 页面选中 Create Matching Identity Group 复选框，以创建匹配的终端身份组。除非删除配置文件的映射，否则无法删除匹配的身份组。

向终端身份组中添加静态终端

您可以在任意终端身份组中添加或移除静态添加的终端。

您仅可从 Endpoints 小组件向特定身份组添加终端。如果您向某个终端身份组添加某个终端，该终端就会从其之前动态分组的终端身份组删除。

在从您最近添加了某个终端的终端身份组删除该终端后，系统会重新分析该终端，使之回到相应身份组。这不会从系统删除终端，而只是从终端身份组删除终端。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 选择终端身份组，然后点击**编辑 (Edit)**。

步骤 3 点击**添加 (Add)**。

步骤 4 在 Endpoints 小组件中选择终端，以将所选终端添加至终端身份组。

步骤 5 点击 **Endpoint Group List** 链接以返回 Endpoint Identity Groups 页面。

在身份组中添加或删除终端后重新分析动态终端

如果终端身份组分配不是静态的，则在终端身份组中添加或删除终端后重新分析终端。由 ISE 分析器动态识别的终端显示在相应的终端身份组中。如果从终端身份组删除动态添加的终端，Cisco ISE 则显示一条消息，指明您已成功从身份组删除终端，但在终端身份组中重新分析这些终端。

用于授权规则的终端身份组

您可以在授权策略中有效地使用终端身份组来向所发现的终端提供相应的网络接入权限。例如，在 Cisco ISE 中，以下位置默认提供适用于所有类型Cisco IP 电话的授权规则： **策略 (Policy)** > **策略集 (Policy Sets)** > **默认 (Default)** > **授权策略 (Authorization Policy)**。

您必须确保终端分析策略为独立策略（而不是其他终端分析策略的父策略），或确保未禁用终端分析策略的父策略。

任意播和分析器服务

任意播是一种网络技术，其中将相同的IP地址分配给两个或更多主机，并允许路由确定接收数据的最适当目标。与提供单一分析数据目标（RADIUS、DHCP中继、SNMP陷阱和NetFlow）的负载均衡器用例类似，任意播允许为源配置单一IP目标，以避免将相同数据发送到多个目标。

任意播IP地址可分配给实际PSN接口IP地址或负载均衡器虚拟IP地址，以支持跨数据中心的冗余。不得将任意播IP地址分配给ISE千兆以太网0管理接口。

用于任意播的接口必须是专供分析器探测器使用的接口。当任意播IP地址分配给负载均衡器虚拟IP地址时，不适用这一要求。

使用任意播时，关键在于自动检测任何节点故障，并从路由表中删除故障节点的对应路由。如果任意播目标是链路或VLAN上的唯一主机，则故障可能会导致自动删除路由。

部署IP任意播时，务必确保通往每个目标的路由度量具有重大的权重或偏重。如果通往任意播目标的路由摆动或导致等价多路径路由(ECMP)场景，则给定服务（RADIUS AAA、DHCP或SNMP陷阱分析、HTTPS门户）的流量可能会分配给每个目标，从而导致流量过多和服务故障（RADIUS AAA和HTTPS门户）或次优分析和数据库复制（分析服务）。

IP任意播的主要优势在于，它可以极大简化接入设备、配置文件数据源和DNS上的配置。它还可以通过确保给定终端的数据仅发送到单个PSN来优化ISE分析。必须仔细规划其他路由配置并使用适当的监控器进行管理。但是，由于没有使用不同的子网和IP地址，所以故障排除可能比较困难。

分析器源服务

分析器条件、例外操作和NMAP扫描操作分类为由Cisco提供或由管理员创建，如“系统类型”(System Type)属性所示。终端分析策略会分类为由Cisco提供、由管理员创建或由管理员修改。这些分类显示在“系统类型”(System Type)属性中。

您可以根据系统类型属性，对分析器条件、例外操作、NMAP操作和终端分析策略执行不同的操作。您无法编辑或删除由Cisco提供的条件、例外操作和NMAP扫描操作。无法删除由Cisco提供的终端策略。编辑策略时，这些策略称为管理员修改的策略。源服务更新策略后，管理员修改的策略将替换为所基于的由Cisco提供的最新版本策略。

可以从Cisco源服务器检索新的和更新后的策略及更新的OUI数据库。必须已订阅Cisco ISE。还可以接收有关已应用、成功和失败消息的电子邮件通知。可以将有关源服务操作的匿名信息发送回Cisco，这有助于Cisco改进源服务。

OUI数据库包含分配给供应商的MAC OUI。以下是OUI列表：http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE会在本地Cisco ISE服务器时区每天凌晨1:00下载策略和OUI数据库更新。Cisco ISE自动应用这些已下载的源服务器策略，其中存储了更改，因此可以将这些更改恢复到先前状态。恢复到先前状态时，将删除新的终端分析策略，而已更新的终端分析策略将恢复到先前状态。此外，分析器源服务将自动禁用。

您还可以在离线模式下手动更新源服务。如果您无法将 ISE 部署连接到Cisco源服务，则可以通过使用此选项手动下载更新。

注释 许可证在 60 天时段内处于不合规 (OOC) 状态 45 天后，不允许来自源服务的更新。当许可证已过期或使用量超过允许的会话数时，许可证即为不合规。

配置分析器源服务

分析器源服务会从Cisco源服务器中检索新的和更新后的终端分析策略及 MAC OUI 数据库更新。如果源服务不可用或发生其他错误，系统会在 Operations Audit 报告中进行报告。

您可以将Cisco ISE 配置为将匿名的馈送服务使用情况报告发回Cisco，这会向Cisco发送以下信息：

- Hostname - Cisco ISE 主机名
- MaxCount - 终端总数
- ProfiledCount - 已分析的终端计数
- UnknownCount - 未知终端计数
- MatchSystemProfilesCount - Cisco提供的配置文件计数
- UserCreatedProfiles - 用户创建的配置文件计数

您可以更改由Cisco提供分析策略中的 CoA 类型。当源服务更新该策略时，CoA 类型不会更改，但该策略的其余属性仍会更新。

Cisco ISE 2.7 及更高版本可以让您手动下载 OUI 更新，而无需下载策略更新。如果您对某些分析器条件进行了自定义以不止更改 CoA 类型，则可能不希望分析器馈送替换这些条件。您可能仍希望更新 OUI，以便分析器可以在制造商添加新设备时识别它们。“馈送服务”(Feed Service) 门户上提供仅下载 OUI 的选项。

开始之前

分析器源服务只可以从分布式部署中的Cisco ISE 管理门户或在独立 ISE 节点中配置。

如果计划从管理员门户发送有关馈送更新的电子邮件通知，请设置简单邮件传输协议 (SMTP) 服务器（**管理 (Administration)** > **系统 (System)** > **设置 (Settings)**）。

在线更新源服务：

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**，然后检查是否已启用 **QuoVadis 根 CA 2 (QuoVadis Root CA 2)**。

步骤 2 选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **馈送 (Feeds)**。
您还可以在以下位置访问该选项： **管理 (Administration)** > **Feed 服务 (FeedService)** > **分析器 (Profiler)** 页面。

步骤 3 点击**在线订用更新 (Online Subscription Update)** 选项卡。

步骤 4 点击 **Test Feed Service Connection** 按钮以验证是否存在到Cisco源服务的连接，以及证书是否有效。

步骤 5 选中**启用临时计费更新 (Enable Interim Accounting Update)** 复选框。

步骤 6 以 HH:MM 格式（Cisco ISE 服务器的本地时区）输入时间。默认情况下，Cisco ISE 源服务安排在每天凌晨 1.00 点运行。

步骤 7 选中**在下载发生时通知管理员 (Notify administrator when download occurs)** 复选框，并在**管理员电子邮件地址 (Administrator email address)** 文本框输入您的电子邮件地址。如果您想要允许Cisco ISE 收集非敏感的信息（用于在将来的版本中提供更好的服务和附加功能），请选中**向思科提供匿名信息以帮助提高分析准确性 (Provide Cisco anonymous information to help improve profiling accuracy)** 复选框。

步骤 8 点击**保存 (Save)**。

步骤 9 点击 **Update Now**。

指示Cisco ISE 联系Cisco源服务对自上次源服务以来创建的新的和更新后的配置文件进行更新。此操作会重新分析系统中的所有终端，这可能导致系统负载增加。由于终端分析策略经过更新，某些当前连接到Cisco ISE 的终端的授权策略可能会发生更改。

当您对自上次源服务以来创建的新的和更新后的配置文件进行更新时，**立即更新 (Update Now)** 按钮会被禁用，并且只会在下载完成后启用。您必须通过导航操作离开分析器源服务的 Configuration 页面，然后返回此页面。

相关主题

离线配置分析器源服务 ， 第 666 页

离线配置分析器源服务

当Cisco ISE 未直接连接到Cisco源服务器时，您可以离线更新源服务。您可以从Cisco源服务器下载离线更新包，并使用离线源更新将其上传到Cisco ISE。您还可以设置关于添加到源服务器的新策略的邮件通知。

离线配置分析器源服务包括以下任务：

1. 下载离线更新包
2. 应用离线源更新

下载离线更新包

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **源 (Feeds)**。
您还可以在以下位置访问该选项： **管理 (Administration)** > **Feed 服务 (FeedService)** > **分析器 (Profiler)** 页面。

步骤 2 点击**离线手动更新 (Offline Manual Update)** 选项卡。

步骤 3 点击**下载更新的配置文件策略 (Download Updated Profile Policies)** 链接。您将被重定向至源服务合作伙伴门户。
您还可以从浏览器转到 https://ise.cisco.com/partner/，直接访问源服务合作伙伴门户。

步骤 4 如果您是新用户，请接受条款和协议。
系统将触发邮件给源服务管理员以便审批您的申请。批准后，您将收到一封确认邮件。

步骤 5 使用您的 Cisco.com 凭证登录合作伙伴门户。

步骤 6 选择**离线源 (Offline Feed) > 下载数据包 (Download Package)**。

步骤 7 点击**生成数据包 (Generate Package)**。

步骤 8 点击**点击以查看离线更新包内容 (Click to View the Offline Update Package contents)** 链接以查看生成的数据包中包含的所有配置文件和 OUI。

- 源分析器 1 和源 OUI 下的策略将下载到所有版本的Cisco ISE 。
- 源分析器 2 下的策略将仅下载到Cisco ISE 版本 1.3 和更高版本。
- 源分析器 3 下的策略将仅下载到Cisco ISE 版本 2.1 和更高版本。

步骤 9 点击**下载数据包 (Download Package)** 并将文件保存到您的本地系统。
您可以将文件上传并保存到Cisco ISE 服务器以应用已下载数据包中的源更新。

应用离线源更新

开始之前

您必须先下载离线更新数据包，才能应用源更新。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **馈送 (Feeds)** 。
您还可以在以下位置访问该选项： **管理 (Administration)** > **FeedService** > **分析器 (Profiler)** 窗口。

步骤 2 点击**离线手动更新 (Offline Manual Update)** 选项卡。

步骤 3 点击**浏览 (Browse)** 并选择已下载的分析器源数据包。

步骤 4 点击**应用更新 (Apply Update)**。

为配置文件和 OUI 更新配置邮件通知

您可以配置您的邮箱地址，以接收有关配置文件和 OUI 更新的通知。

步骤 1 下载离线更新包 部分中执行**第 1 步 (Step 1)** 至**第 5 步 (Step 5)**，转到源服务合作伙伴门户。

步骤 2 选择**离线源 (Offline Feed)** > **邮件首选项 (Email Preferences)**。

步骤 3 选中**启用通知 (Enable notification)** 复选框以接收通知。

步骤 4 从**天数 (days)** 下拉列表中选择天数，以设置您希望接收新更新通知的频率。

步骤 5 输入单个/多个邮箱地址并点击**保存 (Save)**。

撤消源更新

您可以恢复在之前更新中已经更新的终端分析策略，并删除通过之前更新分析器源服务新添加的终端分析策略和 OUI，。

如果在源服务器更新之后修改了终端分析策略，则系统中的终端分析策略不会更改。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **分析器 (Profiler)** > **源 (Feeds)**。

步骤 2 如果想要查看在 Change Configuration Audit 报告中所做的配置更改，请点击**转到更新报告页面 (Go to Update Report Page)**。

步骤 3 点击 **Undo Latest**。

分析器报告

Cisco ISE 为您提供关于终端分析的各种报告，以及可用于管理您的网络的故障排除工具。可以生成历史以及当前数据的报告。您还可以向下钻取报告的某个部分以查看更多详细信息。对于大型报告，您还可以安排报告计划并以各种格式下载这些报告。

您可以从**操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** 为终端运行以下报告：

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

检测终端的异常行为

Cisco ISE 可保护您的网络，避免非法使用 MAC 地址问题。Cisco ISE 可以检测涉及 MAC 地址欺骗的终端，可以让您限制可疑终端的许可。

以下是异常行为的分析器配置页面中的两个选项：

- 启用异常行为检测
- 启用异常行为实施

如果启用异常行为检测，则Cisco ISE 会探测数据，并检查在与 NAS-Port-Type、DHCP 类标识符和终端策略相关的属性更改方面，是否存在与现有数据的任何冲突。如果是，则向终端添加名为

AnomalousBehavior 且设置为 true 的属性，这有助于过滤和查看“可视性情景”（Visibility Context）页面中的终端。系统还会为相应的 MAC 地址生成审核日志。

启用异常行为检测后，Cisco ISE 会检查现有终端的以下属性是否已更改：

1. 端口类型 - 确定终端的访问方法是否已更改。这仅适用于通过有线 Dot1x 连接的同一 MAC 地址用于无线 Dot1x 的情况，反之亦然。
2. DHCP 类标识符 - 确定终端的客户端类型或供应商类型是否已更改。这仅适用于 DHCP 类标识符属性已填充某个值，然后更改为另一个值的情况。如果为终端配置了静态 IP，则Cisco ISE 中的 DHCP 类标识符属性为空。稍后，如果另一台设备伪造此终端的 MAC 地址并使用 DHCP，则类标识符将从空值更改为特定字符串。这不会触发异常行为检测。
3. 终端策略 - 确定是否有重大配置文件更改。这仅适用于终端的配置文件从“电话”或“打印机”更改为“工作站”的情况。

如果启用“异常行为实施”，则在检测到异常行为时会发出 CoA，可根据**分析器配置 (Profiler Configuration)** 窗口中配置的授权规则对可疑终端进行重新授权。

针对带有异常行为的终端设置授权策略规则

可以通过在“授权策略”(Authorization Policy) 页面上设置相应的规则，选择要针对带有异常行为的任何终端执行的操作。

步骤 1 选择**策略 (Policy)** > **策略集 (Policy Sets)**

步骤 2 点击**视图 (View)** 列中与默认策略对应的箭头图标 ，打开“集”(Set) 视图屏幕，然后查看和管理默认授权策略。

步骤 3 在任意行的**操作 (Actions)** 列中，点击齿轮图标，然后从下拉列表中根据需要选择插入或复制选项，插入新的授权规则。
“策略集”(Policy Sets) 表中会显示一个新行。

步骤 4 输入规则名称。

步骤 5 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 6 在**Conditions Studio 页面**中创建所需的条件。在**编辑器 (Editor)**部分中，点击**点击以添加属性 (Click To Add an Attribute)** 文本框，然后选择所需的字典和属性（例如，Endpoints.AnomalousBehaviorEqualsTrue）。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 7 点击**使用 (Use)**，为具有异常行为的终端设置授权策略规则。

步骤 8 点击**完成 (Done)**。

查看带有异常行为的终端

您可以使用以下任一选项查看有异常行为的终端：

- 从**主页 (Home)** > **摘要 (Summary)** > **指标 (Metrics)** 中，点击“异常行为”(Anomalous Behavior)。此操作将打开一个新选项卡，页面底部窗格中有“异常行为”(Anomalous Behavior) 列。
- 依次选择**情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **终端分类 (Endpoint Classification)**。您可以在页面的下方窗格中查看“异常行为”(Anomalous Behavior) 列。
- 您可以在“情景可视性”（Context Visibility）页面的“身份验证”（Authentication）视图或“受危害终端”（Compromised Endpoints）视图中创建新的“异常行为”（Anomarous Behavior）列，如以下步骤所述：

步骤 1 依次选择**情景可视性 (Context Visibility)** > **端点 (Endpoints)** > **身份验证 (Authentication)** 或**情景可视性 (Context Visibility)** > **端点 (Endpoints)** > **受损终端 (Compromised Endpoints)**。

步骤 2 点击页面下方窗格中的“设置”(Settings) 图标，并选中**异常行为 (Anomalous Behavior)** 复选框。

步骤 3 点击 **Go**（前往）。
您可以在身份验证或受损终端视图中查看异常行为列。

客户端设备上的代理下载问题

问题

执行用户身份验证和授权之后，客户端设备浏览器显示“no policy matched”错误消息。此问题适用于身份验证的客户端调配阶段的用户会话。

可能的原因

客户端调配策略缺失必要的设置。

安全评估代理下载问题

请记住，下载安全评估代理安装程序需要满足以下要求：

- 首次在客户端设备上安装代理时，用户必须在浏览器会话中允许 ActiveX 安装程序。（客户端调配下载页面会提示此要求。）
- 客户端设备必须接入互联网。

解决方法

- 确保Cisco ISE 中已有客户端调配策略。如果有，则验证策略中定义的策略身份组、条件和代理类型。（另外，请确认在以下位置是否配置了任何代理配置文件：**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**添加 **(Add)AnyConnect 终端安全评估配置文件 (AnyConnect Posture Profile)**，包括采用所有默认值的配置文件。）

- 尝试在接入交换机上回弹端口，对客户端设备重新执行身份验证。

终端

通过这些页面，您可以配置和管理连接到您的网络的终端。

终端设置

下表介绍**终端 (Endpoints)** 窗口上的字段，您可以使用此窗口创建终端和为终端分配策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *107:* 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的MAC地址以静态创建终端。 MAC 地址是连接到启用Cisco ISE 的网络的接口设备标识符。
Static Assignment	如果您想要在 Endpoints 页面静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。 您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。
Policy Assignment	（除非选中**静态分配 (Static Assignment)** 复选框，否则会默认禁用此字段）从**策略分配 (Policy Assignment)** 下拉列表选择匹配的终端策略。 您可以执行以下操作之一： • 如果您不选择匹配的终端策略，而是使用默认终端策略Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。 • 如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中**静态分配 (Static Assignment)** 复选框。

字段名称	使用指南
Static Group Assignment	当您想要向身份组静态分配终端时，请选中此复选框。 如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。 如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。

Identity Group Assignment	选择您要将终端分配至哪个终端身份组。
	当您静态创建终端，或在为某个终端评估终端策略期间不想使用**创建匹配身份组 (Create Matching Identity Group)** 选项时，可将终端分配至身份组。
	Cisco ISE 包括以下系统创建的终端身份组：
	• Blacklist
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 659 页
使用策略和身份的静态分配创建终端，第 655 页

从 LDAP 设置导入终端

下表介绍“从 LDAP 导入”(Import from LDAP) 窗口上的字段，您可以使用此窗口从 LDAP 服务器导入终端。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *108:* 从 *LDAP* 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。 注释 Cisco ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。
Enable Secure Connection	选中**启用安全连接 (Enable Secure Connection)** 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	点击下拉箭头，查看受信任的 CA 证书。 根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在Cisco ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
Anonymous Bind	您必须选中**匿名绑定 (Anonymous Bind)** 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
Admin DN	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
密码 (Password)	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
Base DN	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
查询设置	
MAC Address objectClass	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
MAC Address Attribute Name	输入导入操作返回的属性名称，例如，macAddress。

字段名称	使用指南
Profile Attribute Name	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置**分析属性名称 (Profile Attribute Name)** 字段时，请考虑以下事项： • 如果未在**分析属性名称 (Profile Attribute Name)** 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知”(Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。 • 如果您在**分析属性名称 (Profile Attribute Name)** 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与Cisco ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。
超时	输入时间（单位：秒），值介于 1 和 60 秒之间。

相关主题

已识别的终端，第 659 页
从 LDAP 服务器导入终端，第 658 页

终端分析策略设置

下表列出了**终端策略 (Endpoint Policies)** 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

表 *109:* 终端分析策略设置

字段名称	使用指南
Name	输入要创建的终端分析策略的名称。
Description	输入要创建的终端分析策略的说明。
Policy Enabled	默认情况下，**Policy Enabled** 复选框处于选中状态，以便在您分析终端时关联匹配的分析策略。 如果未选中此复选框，则在您分析终端时会排除终端分析策略。
Minimum Certainty Factor	输入要与分析策略相关联的最小值。默认值为 10。

字段名称	使用指南
Exception Action	选择在分析策略中定义规则时要与条件关联的例外操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 例外操作 (Exception Actions)**。
Network Scan (NMAP) Action	从列表中选择在分析策略中定义规则时（如有必要）要与条件关联的网络扫描操作。 默认值为 NONE。例外操作在以下位置定义：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)**。
Create an Identity Group for the policy	选择以下选项之一以创建终端身份组： • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	选择此选项以使用现有的分析策略。 此选项可为那些终端创建匹配的身份组，当终端配置文件与现有的分析策略相匹配时，身份组将是已分析的终端身份组的子项。 例如，在网络中发现的终端与 Xerox-Device 配置文件相匹配时，系统会在 Endpoints Identity Groups 页面创建 Xerox-Device 终端身份组。

字段名称	使用指南
No, use existing Identity Group hierarchy	选中此复选框可使用分析策略和身份组的层次结构将终端分配给匹配的父终端身份组。 通过此选项，可以使用终端分析策略层次结构将终端分配给其中一个匹配的父终端身份组，以及父身份组的关联终端身份组。 例如，与现有配置文件相匹配的终端会归入相应的父终端身份组中。在本例中，与Unknown配置文件相匹配的终端会归入 Unknown 终端身份组中，与现有配置文件相匹配的终端会归入Profiled终端身份组中。例如， • 如果终端与Cisco-IP-Phone配置文件相匹配，则这些终端会归入 Cisco-IP-Phone 终端身份组中。 • 如果终端与Workstation配置文件相匹配，则这些终端会归入Workstation终端身份组中。 Cisco-IP-Phone 和 Workstation 终端身份组与系统中的 Profiled 终端身份组相关联。
Parent Policy	选择在系统中定义的、要与新终端分析策略相关联的父分析策略。 可以选择可将规则和条件继承到其子项的父分析策略。
Associated CoA Type	选择以下要与终端分析策略相关联的CoA类型之一： • No CoA • Port Bounce • Reauth • Global Settings，该设置是从在 Administration > System > Settings > Profiling 中设置的分析器配置进行应用
Rules	在终端分析策略中定义的一个或多个规则为终端确定了匹配的分析策略，这允许您根据终端配置文件对终端进行分组。 策略要素库中的一个或多个分析条件用于规则，以验证终端属性及其整体分类值。

字段名称	使用指南
Conditions	点击加号 [+] 展开 Conditions 固定重叠，点击减号 [-] 或点击固定重叠的外部可将其折叠。 点击 **从库中选择现有条件 (Select Existing Condition from Library)** 或 **创建新条件（高级选项）(Create New Condition (Advanced Option))**。 **从库中选择现有条件 (Select Existing Condition from Library)**：可以通过从策略元素库中选择Cisco预定义条件来定义表达式。 **创建新条件（高级选项）(Create New Condition (Advanced Option))**：可以通过从各种系统或用户定义的字典中选择属性来定义表达式。 可以将以下其中一项与分析条件相关联： • 每种条件的可信度的整数值。 • 为该条件输入例外操作或网络扫描操作 选择以下其中一个要与分析条件相关联的预定义设置： • “可信度增加”(Certainty Factor Increases)：为每个规则输入可信度值，可以为与整体分类相关的所有匹配规则添加此可信度值。 • “采取例外操作”(Take Exception Action)：触发在此终端分析策略的“例外操作”(Exception Action) 字段中配置的例外操作。 • “采取网络扫描操作”(Take Network Scan Action)：触发在此终端分析策略的“网络扫描 (NMAP) 操作”(Network Scan (NMAP) Action) 字段中配置的网络扫描操作。

字段名称	使用指南
Select Existing Condition from Library	可以执行以下操作： • 可以选择策略要素库中可用的Cisco预定义条件，然后使用 AND 或 OR 运算符添加多个条件。 • 点击 Action 图标，在后续步骤中执行以下操作： • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对 • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件 • **复制 (Duplicate)**：创建选定条件的副本 • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中 • **删除 (Delete)**：删除所选条件。
创建新条件（高级选项）	可以执行以下操作： • 可以将临时属性/值对添加到表达式，然后使用 AND 或 OR 运算符添加多个条件。 • 点击 Action 图标，在后续步骤中执行以下操作： • **添加属性/值 (Add Attribute/Value)**：可以添加临时属性或值对 • **从库中添加条件 (Add Condition from Library)**：可以添加Cisco预定义条件 • **复制 (Duplicate)**：创建选定条件的副本 • **将条件添加到库 (Add Condition to Library)**：可以将自行创建的临时属性/值对保存到策略元素库中 • **删除 (Delete)**：删除所选条件。可以使用 AND 或 OR 运算符

相关主题

思科 ISE 分析服务，第 603 页

创建终端分析策略，第 648 页
使用 UDID 属性的终端情景可视性，第 679 页

使用 UDID 属性的终端情景可视性

唯一标识符 (UDID) 是终端属性，用于识别特定终端的 MAC 地址。一个终端可以有多个 MAC 地址。例如，一个 MAC 地址用于有线接口，另一个用于无线接口。AnyConnect 代理会为该终端生成 UDID，并将其保存为终端属性。 您可以在授权查询中使用 UDID。 终端的 UDID 保持不变，不会随 AnyConnect 的安装或卸载而更改。使用 UDID 时，**情景可视性 (Context Visibility)** 窗口（**情景可视性 (Context Visibility) > 终端 (Endpoints) > 合规性 (Compliance)**）会为具有多个网卡的终端显示一个条目，而不是多个。您可以确保对特定终端（而不是 MAC 地址）的安全评估控制。

注释 终端必须具有 AnyConnect 4.7 或更高版本才能创建 UDID。

适用于 Windows 和 Macintosh 终端的终端脚本向导

终端脚本向导可以让您在连接的终端上运行脚本，以执行符合组织要求的管理任务。这包括卸载过时软件、启动或终止进程或应用以及启用或禁用特定服务等任务。

终端脚本可通过终端脚本向导在 Windows 终端和 Macintosh 终端上运行。

开始之前

- 您必须具有超级管理员用户角色。
- 为Cisco ISE 配置登录凭证，以便使用管理权限访问 Macintosh 和 Windows 终端。

  在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **终端登录配置 (Endpoint Login Configuration)**，并配置以下内容：

  - Cisco ISE 可用于登录终端的域凭证。
  - 适用于 Windows 和 Macintosh 的本地用户凭证，Cisco ISE 可以使用这些凭证作为本地用户登录到终端。

    域用户优先于本地用户。如果同时配置了两者，并且需要使用本地用户凭证运行脚本，则必须删除域凭证。

- Windows 终端必须安装 Windows PowerShell 5.1 或更高版本。必须启用 PowerShell 远程处理。
- Macintosh 终端必须安装 Bash。
- Windows 终端和 Macintosh 终端都必须安装 cURL 7.34 或更高版本。
- Windows 终端和 Macintosh 终端必须连接到网络并在Cisco ISE 中具有活动会话。

步骤 1 在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**

步骤 2 点击窗口右上角的链接图标，然后从下拉列表中选择**运行终端脚本 (Run Endpoint Scripts)**。

欢迎 (Welcome) 选项卡包含指向**终端登录配置 (Endpoint Login Configuration)** 窗口的链接，用于配置登录凭证（如果尚未配置）。只有在配置登录凭证后，才能点击此选项卡右下角的**开始 (Start)** 按钮。

步骤 3 在**选择类别 (Select Category)** 选项卡中，可以根据终端的操作系统或终端上可用的应用选择终端。点击**按操作系统 (By OS)** 或**按应用 (By Application)** 单选按钮做出选择。点击 **下一步 (Next)** 继续操作。

步骤 4 在**选择终端 (Select Endpoints)** 窗口中，一个 Dashlet 会显示适用于操作系统类型或应用（如适用）的过滤器。在 Dashlet 中，点击要应用的过滤器，该过滤器的所有终端都列在一个表中。

- 要选择选定过滤器的所有终端，请选中表标题行中的复选框。
- 要选择特定终端，请选中表中该条目的复选框。要从表中查找特定终端，请点击表上方的**过滤器 (Filter)** 按钮，然后选择**快速过滤器 (Quick Filter)**。您可以按显示的任何参数进行过滤，以查找所需的终端。

注释　如果在**选择类别**步骤中选择了**按应用 (By Application)**，请记住选择属于该步骤中同一操作系统类型的终端。对于基于应用的脚本，请在终端脚本向导中为每种操作系统类型创建脚本，并为每种操作系统类型设置单独的作业。

步骤 5 选择要运行脚本的终端后，点击**下一步 (Next)**。

步骤 6 在**选择脚本 (Select Scripts)** 选项卡中，点击**添加 (Add)**。

步骤 7 点击**添加脚本 (Add Script)** 以从系统中选择脚本。点击**开始上传 (Start Upload)**，将脚本添加到**选择脚本 (Select Scripts)** 选项卡。

步骤 8 选中要运行的脚本的复选框，然后点击**下一步 (Next)**。

步骤 9 **摘要 (Summary)** 选项卡显示所选择的终端和脚本。在此处检查所做的选择，然后点击**返回 (Back)** 以更改任何详细信息。点击**完成 (Finish)** 以启动脚本运行。

系统将显示名为**终端脚本报告 (Endpoints Script Report)** 的弹出窗口，其中包含此任务的**作业 ID (Job ID)**。点击**终端脚本调配报告 (Endpoint Scripts Provisioning report)** 以重定向到包含此任务详细信息的窗口。

要查看通过终端脚本向导运行的作业报告，请选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)**。

终端脚本调配摘要报告

在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)**

“终端脚本调配摘要”(Endpoint Scripts Provisioning Summary) 窗口显示过去 30 天内通过终端脚本向导运行的作业的详细信息。点击窗口右上角的**计划 (Schedule)**，安排导出报告并跟踪较旧的报告。

点击**导出到 (Export To)** 并从下拉列表中选择一个选项，将报告的 CSV 或 PDF 版本保存到存储库或本地目标。

默认情况下，**终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)** 窗口显示包含以下列的表格：

列的名称	显示的信息
记录时间	提交作业的时间戳。
作业 **ID**	点击作业 ID 条目可查看条目的详细信息。系统将打开一个包含**终端脚本调配详细信息**的新选项卡，其中有时间戳、所选终端的 MAC 地址、每个终端的脚本状态和脚本调配状态、调配作业的 PSN 名称以及作业 ID。 **注释　　注意** ：点击 MAC 地址可查看脚本运行的详细分步信息。
管理员用户名	提交作业的管理员的名称。
操作系统	为其运行所选脚本的操作系统。
总数/成功/失败/正在进行的终端	• 所选终端的总数。 • 成功运行脚本的终端数量。 • 脚本运行失败的终端数量。 • 仍在运行脚本的终端数量。
脚本名称	作业中包含的脚本的名称。

IF-MIB

对象	**OID**
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

对象	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

对象	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

对象	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3

对象	OID
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

对象	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

对象	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

对象	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

对象	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

对象	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9

对象	OID
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

对象	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

对象	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.5

对象	OID
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

对象	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

对象	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

对象	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7

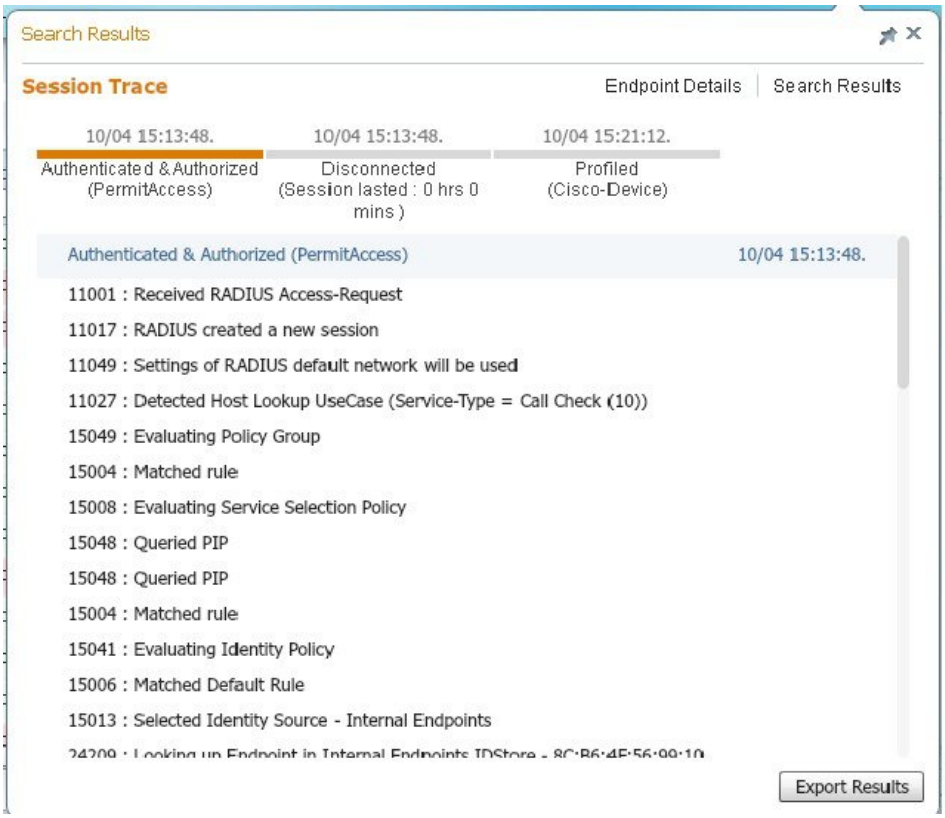
对象	OID
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

终端的会话跟踪

您可以使用Cisco ISE 首页顶部的全局搜索框来获得某个终端的会话信息。当使用条件进行搜索时，您将会看到终端列表。点击其中任意终端以查看该终端的会话跟踪信息。下图所示为终端会话跟踪信息的示例。

注释 用于搜索的数据集基于作为索引的终端 ID。因此，当进行身份验证时，对于包括在搜索结果集中的身份验证，必须具有终端 ID。

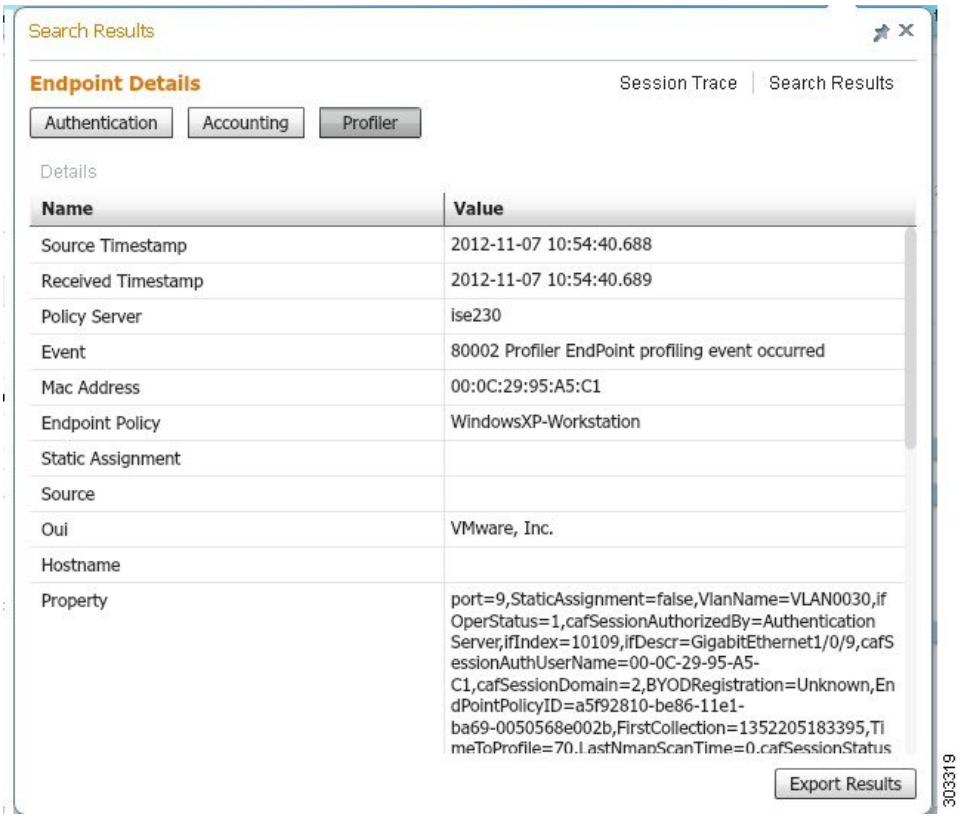
图 *30:* 终端的会话跟踪



您可以使用顶部可点击的时间表来查看主要的授权过渡。还可以使用**导出结果 (Export Results)** 选项导出 .csv 格式的结果。报告会下载到您的浏览器。

可以点击**终端详细信息 (Endpoint Details)** 链接查看特定终端的更多身份验证、记帐和分析器信息。下图所示为所显示的终端详细信息。

图 *31:* 终端详细信息



从目录清除会话

在监控和故障排除节点上，会话按以下方式从会话目录中清除：

- 已终止会话会在终止 15 分钟后清除。
- 如果存在身份验证但无记账，则此类会话将在一个小时后清除。
- 所有非活动会话在五天之后清除。

终端的全局搜索

您可以使用Cisco ISE 首页顶部的全局搜索框搜索终端。您可以使用以下任何条件搜索终端：

- 用户名
- MAC 地址
- IP 地址
- 授权配置文件

- 终端配置文件
- 失败原因
- 身份组
- 身份库
- 网络设备名称
- 网络设备类型
- 操作系统
- 安全评估状态
- 位置
- 安全组
- 用户类型

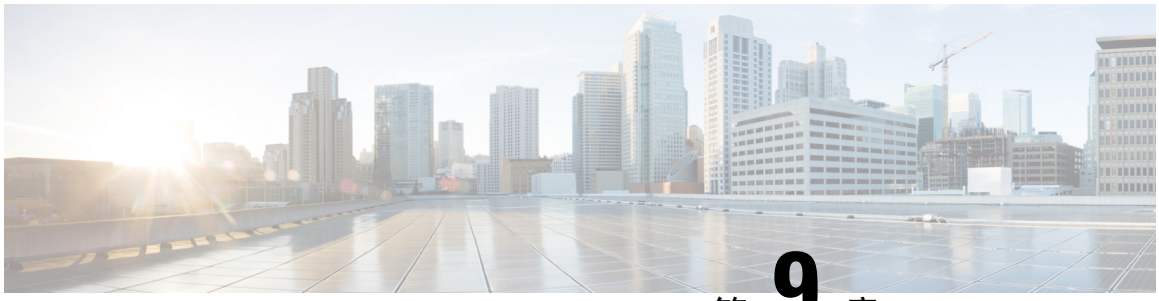
对于任何搜索条件，您应在搜索字段中至少输入三个字符以显示数据。

注释 如果终端已由Cisco ISE 进行身份验证，或其审计更新已收到，则可通过全局搜索找到该终端。搜索结果中不会显示已手动添加但未由Cisco ISE 进行身份验证或未在Cisco ISE 中说明的终端。

搜索结果提供终端当前状态的详细和概览信息，可用于故障排除。搜索结果仅显示前25个条目。建议使用过滤器缩小结果范围。

您可以使用左侧面板中的任何属性过滤结果。您也可以点击任意终端查看该终端的详细信息，例如：

- 跟踪会话
- 身份验证详细信息
- 记帐详细信息
- 安全评估详细信息
- 分析器详细信息
- 客户端调配详细信息
- 访客记帐和活动



第 9 章

自带设备 (BYOD)

公司网络上的个人设备 (BYOD)

支持公司网络上的个人设备时，必须验证和授权用户（员工、承包商和访客）及其设备，保护网络服务和企业数据。Cisco ISE 提供相关工具，允许员工在公司网络上安全地使用个人设备。

登录访客门户时，访客能够自动注册其设备。访客可以注册更多设备，直到达到您为其访客类型定义的最大限制。这些设备会根据门户配置注册到终端身份组中。

访客可以通过运行本地请求方调配（网络设置助手）或通过将其设备添加到“我的设备”(My Devices) 门户，将其个人设备添加到网络。您可以根据操作系统创建本地请求方配置文件，后者决定着应该使用的适当本地请求方调配向导。

因为不是所有设备都能够使用本地请求方配置文件，所以用户可以使用我的设备门户手动添加这些设备；或者您可以配置 BYOD 规则，注册这些设备。

思科 ISE 社区资源

分布式环境中的最终用户设备门户

Cisco ISE 最终用户 Web 门户根据管理、策略服务和监控角色，提供配置、会话支持和报告功能。

- **策略管理节点 (PAN)**：您对用户、设备和最终用户门户所做的配置更改会写入 PAN。
- **策略服务节点 (PSN)**：最终用户门户在 PSN 上运行，后者处理所有会话流量，包括网络访问、客户端调配、访客服务、终端安全评估和分析。如果 PSN 是节点组的一部分，并且一个节点发生故障，则其他节点会检测到故障，并重置任何挂起的会话。

- **监控节点（MnT 节点）**：MnT 节点在我的设备门户、发起人门户和访客门户上收集、聚合和报告有关最终用户和设备活动的数据。如果主 MnT 节点故障，则辅助 MnT 节点自动成为主 MnT 节点。

设备门户的全局设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)**。

您可以为 BYOD 门户和 My Devices 门户配置以下常规设置：

- **员工注册的设备 (Employee Registered Devices)**：在**将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。
- **重试 URL (Retry URL)**：在**重试激活 URL (Retry URL for onboarding)** 中输入可用于将设备重定向至Cisco ISE 的 URL。

当您配置这些常规设置后，它们适用于为您的公司设置的所有 BYOD 门户和 My Devices 门户。

相关主题

限制员工注册的个人设备的数量，第 699 页
提供用于重新连接 BYOD 注册流程的 URL，第 701 页
分布式环境中的最终用户设备门户，第 693 页

个人设备门户

Cisco ISE 提供若干基于 Web 的门户，支持员工自有的个人设备。这些设备门户不参与访客或发起人门户流。

- **黑名单门户 (Blacklist Portal)**：提供关于被列入阻止列表且无法用于获得网络访问权限的个人设备的信息。
- **BYOD 门户 (BYOD Portals)**：使员工能够使用本地请求方调配功能注册其个人设备。
- **证书调配门户 (Certificate Provisioning Portal)**：允许管理员和员工为无法完成 BYOD 流的设备请求用户/设备证书。
- **客户端调配门户 (Client Provisioning Portals)**：强制员工在其设备上下载终端安全评估代理，用来检查合规性。
- **MDM 门户 (MDM Portals)**：使员工能够在外部移动设备管理 (MDM) 系统中登记其移动设备。
- **我的设备门户 (My Devices Portals)**：使员工能够添加和注册个人设备，包括不支持本地请求方调配的个人设备，然后管理这些设备。

通过Cisco ISE，您可以在Cisco ISE 服务器上托管多个设备门户，包括一组预定义的默认门户。默认门户主题具有标准Cisco品牌，您可以通过管理员门户（**管理 (Administration)** > **设备门户管理 (Device**

Portal Management)）对其进行自定义。此外，还可以选择上传组织特有的图片、徽标和级联样式表 (CSS) 文件，进一步自定义门户。

访问设备门户

可以从Cisco ISE GUI 访问任何个人设备门户，如下所示：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)**。

步骤 2 选择您要配置的特定设备门户。

黑名单门户

员工不直接访问该门户，但可被重新定向到该门户。

如果员工丢失个人设备或设备被盗，他们可以在我的设备门户更新设备状态，将设备添加到**黑名单**终端身份组。这可以防止其他人使用该设备进行未经授权的网络访问。如果有人尝试使用黑名单中的某个设备连接网络，他们将被重新定向到 Blacklist 门户，并且被告知该设备禁止接入网络。如果找到设备，员工可以恢复设备（在我的设备门户），在无需重新注册设备的情况下重新获得网络访问权限。根据设备是丢失还是被盗，设备可能需要经过额外调配，才能连接到网络。

您可以为 Blacklist 门户配置端口设置（默认为端口 8444）。如果更改端口号，请确保此端口号未被其他最终用户门户使用。

有关配置黑名单门户的信息，请参阅编辑黑名单门户，第 705 页。

证书调配门户

员工可以直接访问证书调配门户。

通过证书调配门户，员工可以为无法完成自行激活流程的设备请求证书。例如，销售点终端等设备无法完成自带设备流程，需要手动颁发证书。通过证书调配门户，特权用户组可以为此类设备上传证书请求，生成密钥对（如果需要）以及下载证书。

员工可以访问此门户，并使用 CSV 文件请求单个证书或创建批量证书请求。

ISE 社区资源

有关Cisco ISE 证书调配门户的功能和配置的信息，请参阅ISE 2.0：证书调配门户。

自带设备门户

员工无法直接访问该门户。

当员工使用本地请求方注册个人设备时，员工会被重定向至自带设备 (BYOD) 门户。员工首次尝试使用个人设备访问网络时，系统会提示员工手动下载并启动网络设置助理 (NSA) 向导并引导他们完成注册和安装本地请求方。员工注册设备后，就可以使用 My Devices 门户管理设备。

注释 当设备连接到使用 AnyConnect 网络访问管理器 (NAM) 的网络时，不支持 BYOD 流。

相关主题

创建 BYOD 门户，第 707 页
公司网络上的个人设备 (BYOD)，第 693 页

客户端调配门户

员工不直接访问该门户，但可被重新定向到该门户。

客户端调配系统为尝试访问公司网络的设备提供终端安全评估和补救。当员工使用设备请求网络访问时，您可以将他们路由至客户端调配门户，要求他们首先下载终端安全评估代理。终端安全评估代理扫描设备以检查合规性，例如验证设备是否已安装病毒防护软件，操作系统是否受支持。

相关主题

创建客户端调配门户，第 709 页

移动设备管理门户

员工不直接访问该门户，但可被重新定向到该门户。

许多公司使用移动设备管理 (MDM) 系统管理员工的移动设备。

Cisco ISE 允许与外部 MDM 系统集成，员工使用这些系统注册他们的移动设备并访问公司网络。Cisco提供一个外部 MDM 接口，员工可用其注册他们的设备并连接到网络。

MDM 门户允许员工在一个外部 MDM 系统中注册。

员工可使用“我的设备”门户管理他们的移动设备，例如使用PIN码锁定设备、恢复设备出厂设置、或移除注册设备时所安装的应用和设置。

Cisco ISE 允许您为所有外部 MDM 系统设置单个 MDM 门户，或为每个 MDM 系统分别设置一个门户。

有关将 MDM 服务器配置为与Cisco ISE 配合使用的信息，请参阅创建 MDM 门户，第 711 页。

我的设备门户

员工可以直接访问我的设备门户。

某些需要网络接入的网络设备不受本地请求方调配支持，并且无法使用 BYOD 门户进行注册。但是，员工可以使用“我的设备”(My Devices) 门户添加和注册其操作系统不受支持或没有 Web 浏览器的个人设备（例如打印机、互联网广播和其他设备）。

员工可以通过输入设备的 MAC 地址添加和管理新设备。当员工使用“我的设备”(My Devices) 门户添加设备时，Cisco ISE 会将设备添加到“终端”(Endpoints) 窗口（**管理 (Administration)** > **情景可视性 (Context Visibility)** > **终端 (Endpoints)**）作为 **RegisteredDevices** 终端身份组的成员（除非已经静态分配到其他终端身份组）。设备如同Cisco ISE 中的任何其他终端一样进行分析，并且完成注册过程以接入网络。

当用户向“我的设备”(My Devices Portal) 门户中输入一台设备上的两个 MAC 地址时，分析会确定它们具有相同主机名，并在Cisco ISE 中将它们合并为单个条目。例如，用户注册具有有线和无线地址的笔记本电脑。该设备的所有操作（例如删除）对两个地址都会执行。

从门户中删除注册设备时，**DeviceRegistrationStatus** 和 **BYODRegistration** 属性会分别更改为**未注册 (Not Registered)** 和**否 (No)**。但是，当访客（不是员工）使用需要提供凭证的访客门户中的“访客设备注册”(Guest Device Registration) 窗口注册设备时，这些属性保持不变，因为这些 BYOD 属性仅在员工设备注册过程中使用。

无论员工使用 BYOD 门户还是我的设备门户注册其设备，他们都可以使用我的设备门户管理这些设备。

注释 当管理员门户关闭时，“我的设备”(My Devices) 门户不可用。

相关主题

创建我的设备门户 ，第 712 页

BYOD 部署选项和状态流程

支持个人设备的 BYOD 部署流程根据以下因素而略有不同：

- 单或双 SSID：使用单 SSID 时，认证登记、调配和网络访问都使用同一无线本地区域网络 (WLAN)。在双 SSID 部署中，有两个 SSID。一个用来登记和调配，另一个提供安全网络访问。
- Windows、MacOS、iOS 或 Android 设备：无论设备类型如何，本地请求方流程开始时都相似：将使用支持的个人设备的员工重定向至 BYOD 门户以确认其设备信息。此流程因设备类型而异。

员工连接至网络

1. Cisco ISE 根据公司 Active Directory 或其他公司身份存储区对员工的凭证进行身份验证并提供授权策略。
2. 设备被重定向至BYOD门户。设备的MAC地址字段已预配置，用户可以添加设备名称和说明。
3. 已配置本地请求方（MacOS、Windows、iOS、Android），但是此流程因设备而异：
   - MacOS 和 Windows 设备：员工在 BYOD 门户中点击**注册 (Register)** 以下载和安装请求方调配向导（网络设置助理），此向导会配置请求方并提供证书（如果必要），用于基于EAP-TLS 证书的身份验证。颁发的证书嵌有设备的 MAC 地址和员工的用户名。

注释 网络设置助理无法下载到 Windows 设备，除非该设备的用户具有管理权限。如果无法授予最终用户管理权限，则使用组策略对象 (GPO) 将证书推送到用户的设备，而不是使用 BYOD 流。

注释 从 MacOS 10.15 开始，用户必须允许下载请求方调配向导 (SPW)。用户设备上会显示一个窗口，要求他们允许或拒绝从Cisco ISE 服务器下载。

- iOS 设备：Cisco ISE 策略服务器使用 Apple 的 iOS 空中下载功能向 IOS 设备发送新配置文件，其中包括：
  - 颁发的证书（如已配置）嵌有 IOS 设备的 MAC 地址和员工的用户名。
  - 强制使用 EAP-TLS 进行 802.1X 身份验证的 Wi-Fi 请求方配置文件。
- Android 设备：Cisco ISE 会提示并引导员工从 Google Play 商店下载网络设置助理 (NSA)。安装应用后，员工可以打开 NSA 并启动设置向导，该向导会生成请求方配置和用于配置设备的已颁发证书。

4. 在用户完成激活流程后，Cisco ISE 会发起授权更改 (CoA)。这会导致 MacOS、Windows 和 Android 设备重新连接到安全 802.1X 网络。对于单 SSID，iOS 设备也会自动连接；但是对于双 SSID，向导会提示 iOS 用户手动连接新网络。

注释 您可以配置不使用请求方的 BYOD 流。请参阅Cisco ISE 社区文档https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning。

注释 仅在隐藏实际 Wi-Fi 网络时，选中**目标网络隐藏时启用 (Enable if Target Network is Hidden)** 复选框。否则，不能为某些 iOS 设备调配 Wi-Fi 网络配置，尤其是在单 SSID 流中（在这种情况下，激活和连接使用同一个 Wi-Fi 网络或 SSID）。

BYOD 会话终端属性

终端属性 *BYODRegistration* 的状态在 BYOD 流期间更改为以下状态。

- 未知 *(Unknown)*：设备尚未通过 BYOD 流。
- 是 *(Yes)*：设备已通过 BYOD 流，并已注册。
- 否 *(No)*：设备已通过 BYOD 流，但未注册。这意味着设备已删除。

设备注册状态终端属性

终端属性 *DeviceRegistrationStatus* 的状态在设备注册期间更改为以下状态。

- 已注册 *(Registered)*：设备已通过 BYOD 流，并且已注册。属性从待处理状态更改为已注册状态之间有 20 分钟的延迟。
- 待处理 *(Pending)*：设备已通过 BYOD 流，并且已注册。但是，Cisco ISE 尚未在网络上看到它。
- 未注册 *(Not Registered)*：设备尚未通过 BYOD 流。未注册 *(Not Registered)* 是 *DeviceRegistrationStatus* 属性的默认状态。
- 被盗 *(Stolen)*：用户登录我的设备门户，并将当前已激活的设备标记为“被盗”(Stolen)。这会在以下情况下发生：
  - 如果设备是通过调配证书和配置文件激活的，则Cisco ISE 会撤销调配到设备的证书，并将设备的 MAC 地址分配给**黑名单**终端身份组。该设备不再具有网络访问权限。
  - 如果设备是通过调配配置文件（无证书）激活的，则Cisco ISE 会将设备分配到**黑名单**终端身份组。设备仍然具有网络访问权限，除非您为此情况创建授权策略。例如，**IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN DenyAccess**。

  管理员执行能够禁用多个设备的网络访问的操作，如删除或撤销证书。

  如果用户恢复被盗的设备，则状态会恢复为未注册 *(Not Registered)*。用户必须删除该设备，然后重新添加。这会启动激活过程。
- 丢失 *(Lost)*：用户登录“我的设备”门户，并将当前已激活的设备标记为丢失 *(Lost)*，从而导致以下操作：
  - 设备被分配到**黑名单**身份组。
  - 调配到设备的证书不会被撤销。
  - 设备状态更新为丢失 *(Lost)*。
  - *BYODRegistration*状态更新为否 *(No)*。

  除非创建授权策略来阻止丢失的设备，否则丢失的设备仍具有网络访问权限。您可以在规则中使用**黑名单**身份组或 *endpoint:BYODRegistration* 属性。例如，**IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD**。如需更精细的访问，还可以将 *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST”*，*InternalUser:IdentityGroup Equals* <<*group*>> 添加到规则的 IF 部分。

限制员工注册的个人设备的数量

可以允许员工注册 1 至 999 台个人设备。无论员工用于注册个人设备的门户如何，此设置均可定义在所有门户上注册的最大设备数量。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。

步骤 2 在**将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

步骤 3 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

支持使用本地请求方注册设备

您可以创建本地请求方配置文件来支持Cisco ISE 网络上的个人设备。根据您与用户的授权要求相关联的配置文件，Cisco ISE 提供必要的请求方向导来设置用户的个人设备以访问网络。

员工首次尝试使用个人设备访问网络时，系统会自动引导其完成注册和请求方配置。在其注册设备后，可以使用我的设备门户管理其设备。

本地请求方支持的操作系统

以下操作系统支持本地请求方：

- Android（Amazon Kindle 和 B&N Nook 除外）
- Mac OS（适用于 Apple Mac 计算机）
- Apple iOS 设备（Apple iPod、iPhone 和 iPad）
- Microsoft Windows 7 和 8（RT 除外）、Vista 和 10

允许员工使用需要提供凭证的访客门户注册个人设备

使用需要提供凭证的访客门户的员工可以注册其个人设备。员工通过 BYOD 门户提供的自行调配流程可以使用本地请求方（可用于 Windows、MacOS、iOS 和 Android 设备）将设备直接连接至网络。

开始之前

您必须创建本地请求方配置文件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)**。

步骤 2 选择您希望允许员工用于使用本地请求方注册其个人设备的需要提供凭证的访客门户，然后点击 **Edit**。

步骤 3 点击**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡。

步骤 4 在 **BYOD 设置 (BYOD Settings)** 下，选中**允许员工在网络上使用个人设备 (Allow employees to use personal devices on the network)** 复选框。

步骤 5 点击保存 (Save)。

提供用于重新连接 BYOD 注册流程的 URL

您可以提供信息，让使用 BYOD 门户注册其个人设备遇到问题的员工重新连接到注册过程。

步骤 1 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 设备门户管理 (Device Portal Management) > 设置 (Settings) > 重试 URL (Retry URL)。

步骤 2 在重试激活 URL (Retry URL for onboarding) 字段中，输入用于将设备重定向至Cisco ISE 的 URL。

当设备在注册过程中遇到问题时，它将尝试自动重新连接到互联网。此时，您在此处输入的URL 会将设备重定向到Cisco ISE（重新启动激活过程）。默认值为 192.0.2.123。

步骤 3 点击保存 (Save)。

如果不想保存对设置进行的任何更新，请点击重置 (Reset) 以恢复为上次保存的值。

设备门户配置任务

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和Cisco ISE提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

在创建新门户或编辑默认门户后，您必须授权使用该门户。授权使用门户后，您所进行的任何后续配置更改便会立即生效。

不需要授权使用我的设备门户。

如果您选择删除门户，则必须先删除与其关联的任何授权策略规则和授权配置文件，或者将其修改为使用其他门户。

使用以下针对配置不同设备门户相关任务编制的表格。

任务	黑名单门户	BYOD 门户	客户端调配门户	MDM 门户	我的设备门户
启用策略服务，第 702 页	必填	必填	必填	必填	必填
将证书添加到设备门户，第 703 页	必填	必填	必填	必填	必填
创建外部身份源，第 703 页	不是必填项	不是必填项	不是必填项	不是必填项	必填

任务	黑名单门户	BYOD 门户	客户端调配门户	MDM 门户	我的设备门户
创建身份源序列，第 704 页	不是必填项	不是必填项	不是必填项	不是必填项	必填
创建终端身份组，第 704 页	不是必填项	必填	不是必填项	必填	必填
编辑黑名单门户，第 705 页	必填	不适用	不适用	不适用	不适用
创建 BYOD 门户，第 707 页	不适用	必填	不适用	不适用	不适用
创建客户端调配门户，第 709 页	不适用	不适用	必填	不适用	不适用
创建 MDM 门户，第 711 页	不适用	不适用	不适用	必填	不适用
创建我的设备门户，第 712 页	不适用	不适用	不适用	不适用	必填
创建授权配置文件，第 713 页	不适用	必填	必填	必填	不是必填项
自定义设备门户，第 715 页	可选	可选	可选	可选	可选

启用策略服务

为了支持Cisco ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 点击节点并点击**编辑 (Edit)**。

步骤 3 在**常规设置 (General Settings)** 选项卡下，启用**策略服务 (Policy Service)** 切换按钮。

步骤 4 选中**启用会话服务 (Enable Session Services)** 复选框。

步骤 5 点击**保存 (Save)**。

将证书添加到设备门户

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为**默认门户证书组 (Default Portal Certificate Group)**。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 添加一个系统证书并将其分配到您希望用于该门户的证书组标签。

在创建或编辑门户期间，此证书组标签可供选择。

步骤 3 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > （**任意门户**） > **创建或编辑 (Create or Edit)** > **门户设置 (Portal Settings)**。

步骤 4 从与新添加证书关联的 **Certificate Group Tag** 下拉列表中选择特定的证书组标签。

注释

- BYOD 不支持超过三个证书的证书链。
- 在 BYOD 激活期间，系统会为 iOS 设备颁发两次证书。

创建外部身份源

Cisco ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

注释 要使用被动身份服务以接收和共享经过身份验证的用户身份，请参阅其他被动身份服务提供程序，第 522 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅将 Active Directory 用作外部身份源，第 471 页。
- 选择 **LDAP** 以添加 LDAP 身份源。有关详细信息，请参阅LDAP，第 561 页。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关详细信息，请参阅RADIUS 令牌身份源，第 582 页。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关详细信息，请参阅RSA 身份源，第 588 页。

- 选择 **SAML Id 提供程序 (SAML Id Providers)** 添加身份提供程序 (IdP)，例如 Oracle 访问管理器。有关详细信息，请参阅 SAMLv2 身份提供者作为外部身份源，第 594 页。
- 选择**社交登录 (Social Login)** 以将社交登录（如 Facebook）设置为外部身份源。请参阅用于自行注册访客的社交媒体登录，第 322 页。

创建身份源序列

开始之前

确保您已经在Cisco ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)** > **添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望Cisco ISE 搜索数据库的顺序。

步骤 6 在 **Advanced Search List** 区域中选择以下选项之一：

- **请勿访问序列中的其他存储区并将 AuthenticationStatus 属性设置为 ProcessError**：如果用户未在第一个选定身份源中找到用户，而您希望Cisco ISE 中止搜索，请选择此选项。
- **视为未找到用户并继续至序列中的下一存储区 (Treat as if the user was not found and proceed to the next store in the sequence)**：如果未在第一个选定身份源中找到用户，而您希望Cisco ISE 仍继续按照序列搜索其他选定身份源，请选择此选项。

  在处理请求时，Cisco ISE 会按照序列搜索这些身份源。确保“选定列表”(Selected list) 字段所列出的身份源的顺序是您希望Cisco ISE 搜索身份源的顺序。

步骤 7 点击**提交 (Submit)** 创建您可以稍后在策略中使用的身份源序列。

创建终端身份组

Cisco ISE 将其所发现的终端划分至相应的终端身份组。Cisco ISE 拥有若干个系统定义的终端身份组。您还从 Endpoint Identity Groups 页面创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **组 (Groups)** > **终端身份组 (Endpoint Identity Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为您想要创建的终端身份组输入**名称**（请勿在终端身份组的名称中包含空格）。

步骤 4 为您想要创建的终端身份组输入**说明**。

步骤 5 点击**父级组 (Parent Group)** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

步骤 6 点击**提交 (Submit)**。

编辑黑名单门户

Cisco ISE 提供一个黑名单门户，它会在被列入Cisco ISE 阻止列表的丢失或被盗设备试图访问您的公司网络时显示信息。

您只能编辑默认门户设置以及自定义为门户显示的默认消息。您不能创建新的黑名单门户，也不能复制或删除默认门户。

开始之前

确保您具有为配合此门户使用而配置的证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portal)** > **编辑 (Edit)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用 **语言 (Languages)** 菜单导出和导入要与门户一起使用的语言文件。

步骤 4 点击**门户测试 URL** 链接以打开显示此门户 URL 的新浏览器标签页。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

步骤 5 在 **Portal Settings** 中更新证书组标签、语言等的默认值，然后定义适用于整个门户的行为。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释　我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x**、**x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。

- **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。
- **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

步骤 6 在 **Portal Page Customization** 选项卡中，自定义在未授权的设备试图获取网络访问权限时显示在门户中的页面标题和消息文本。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

创建 BYOD 门户

可以提供自带设备 (BYOD) 门户，使员工能够注册其个人设备，以便可在允许访问网络之前完成注册和请求方配置。

您可以创建新 BYOD 门户，也可以编辑或复制现有 BYOD 门户。您可以删除任何 BYOD 门户，包括Cisco ISE 提供的默认门户。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保您具有配置用于此门户的所需证书和终端身份组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新**门户设置 (Portal Settings)** 中的端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新 **Support Information Page Settings** 以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。

步骤 6 在**门户页面自定义 (Portal Page Customization)** 选项卡上，自定义配置过程中在以下页面上显示的**内容区域 (Content Area)** 消息文本。

- **BYOD 欢迎 (BYOD Welcome)** 页面：
  - **需要设备配置 (Device Configuration Required)**：输入当设备首次重定向到 BYOD 门户并需要证书调配时应显示的内容。
  - **证书需要更新 (Certificate Needs Renewal)**：输入当需要更新先前证书时应显示的内容。

- **BYOD 设备信息 (BYOD Device Information)** 页面：
  - **达到最大设备数 (Maximum Devices Reached)**：输入当达到员工可注册的设备的最大限制时应显示的内容。
  - **需要的设备信息 (Required Device Information)**：输入当请求需要的设备信息以使员工能够注册设备时应显示的内容。
- **BYOD 安装 (BYOD Installation)** 页面：
  - **桌面安装 (Desktop Installation)**：输入当提供桌面设备的安装信息时应显示的内容。
  - **iOS 安装 (iOS Installation)**：输入当提供 iOS 移动设备的安装说明时应显示的内容。
  - **Android 安装 (Android Installation)**：输入当提供 Android 移动设备的安装说明时应显示的内容。
- **BYOD 成功 (BYOD Success)** 页面：
  - **成功 (Success)**：输入当设备已配置并自动连接到网络时应显示的内容。
  - **成功：手动说明 (Success: Manual Instructions)**：输入当设备配置成功并且员工必须手动连接到网络时应显示的说明。
  - **成功：不受支持的设备 (Success: Unsupported Device)**：输入当允许不受支持的设备连接到网络时应显示的内容。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

创建证书调配门户

对于无法完成登录流程的设备，Cisco ISE 提供证书调配门户，允许您为其申请证书。例如，销售点终端。使用 CSV 文件，您可以申请单个证书或进行批量证书申请。

您可以编辑默认门户设置以及自定义在门户中显示的消息。您还可以创建、复制和删除证书调配门户。

以下两种类型的用户可以访问证书调配门户：

- 具备管理权限的内部或外部用户：能够为他们自己及其他人生成证书。
- 所有其他用户：只能为自己生成证书。

分配有超级管理员或 ERS 管理员权限的用户（网络访问用户）有权访问该门户，并且可以为其他人申请证书。但是，如果您创建一个新的内部管理员用户，并为其分配超级管理员或 ERS 管理员权限，内部管理员用户将无权访问此门户。您必须首先创建一个网络访问用户，并将该用户添加到超

级管理员或ERS管理员组。添加至超级管理员或ERS管理员组的所有现有网络访问用户可以访问此门户。

对于能够访问该门户并为自己生成证书的其他用户，请配置“证书调配门户”(Certificate Provisioning Portal) 设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配 (Certificate Provisioning)** > **编辑 (Edit)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。确保您在**身份验证方法 (Authentication Method)** 下选择适当的身份源或身份源序列，并且在**配置授权组 (Configure Authorized Groups)** 下选择用户组。属于您所选择用户组的所有用户可以访问该门户，并且可以生成自己的证书。

开始之前

确保您具有为配合此门户使用而配置的证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配 (Certificate Provisioning)** > **创建 (Create)**。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 2 在 **门户名称** 中提供唯一的门户名称，并在 **说明** 中提供门户说明。

步骤 3 使用“**语言文件**”**(Language File)** 菜单导出和导入要与门户一起使用的语言文件。

步骤 4 在 **Portal Settings** 中更新证书组标签、语言等的默认值，然后定义适用于整个门户的行为。

步骤 5 在“**门户页面定制**”**(Portal Page Customization)** 选项卡上，请自定义在门户中显示的页面标题和消息文本。

步骤 6 点击**保存 (Save)**，然后点击**关闭 (Close)**。

创建客户端调配门户

可以提供一个客户端调配门户，使员工可以下载Cisco AnyConnect 终端安全评估组件，此组件或代理将在允许设备访问网络之前验证设备的终端安全评估合规性。

您可以创建新 Client Provisioning 门户，也可以编辑或复制现有 Client Provisioning 门户。您可以删任意 Client Provisioning 门户，包括Cisco ISE 提供的默认门户。

分配有超级管理员或 ERS 管理员权限的用户（网络访问用户）有权访问该门户。但是，如果您创建一个新的内部管理员用户，并为其分配超级管理员或 ERS 管理员权限，内部管理员用户将无权访问此门户。您必须首先创建一个网络访问用户，并将该用户添加到超级管理员或 ERS 管理员组。添加至超级管理员或 ERS 管理员组的所有现有网络访问用户可以访问此门户。

对于能够访问该门户并为自己生成证书的其他用户，请配置“证书调配门户”(Certificate Provisioning Portal) 设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配 (Client Provisioning)** > **编辑 (Edit)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。确保您在**身份验证方法 (Authentication Method)** 下选择适当的身份源或身份源序列，并且在**配置授权组 (Configure**

Authorized Groups) 下选择用户组。属于您所选择用户组的所有用户可以访问该门户，并且可以生成自己的证书。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保已为此门户配置必需的证书和客户端调配策略。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配 (Client Provisioning)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新**门户设置 (Portal Settings)** 中的端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新 **Support Information Page Settings** 以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。

步骤 6 在 **Portal Page Customization** 选项卡上，自定义在调配过程中在 Client Provisioning 门户上显示的 **Content Area** 消息文本：

a) 在**客户端调配门户 (Client Provisioning Portals)** 页面上：

- **未知代理 (Agent Unknown)**：输入当代理未知时应显示的内容。
- **检查、扫描和合规 (Checking, Scanning and Compliant)**：输入当终端安全评估代理已安装成功并且检查、扫描和验证设备是否符合终端安全评估要求时应显示的内容。
- **不合规 (Non-compliant)**： 输入当终端安全评估代理确定设备不符合终端安全评估要求时应显示的内容。

b) 在 Client Provisioning (Agent Not Found) 页面上：

- **未找到代理 (Agent Not Found)**：输入在设备上未检测到终端安全评估代理时应显示的内容。
- **手动安装说明 (Manual Installation Instructions)**：输入当设备上未安装 Java 或 Active X 软件时应显示的内容，说明如何手动下载和安装终端安全评估代理。
- **安装，无 Java/ActiveX (Install, No Java/ActiveX)**：输入当设备上未安装 Java 或 Active X 软件时应显示的内容，说明如何下载和安装 Java 插件。
- **已安装代理 (Agent Installed)**：输入在设备上检测到终端安全评估代理时应显示的内容，说明如何启动终端安全评估代理以检查设备是否符合终端安全评估要求。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

相关主题

授权门户，第 338 页
自定义设备门户，第 715 页

创建 MDM 门户

您可以提供移动设备管理 (MDM) 门户，以使员工能够管理其注册以供在公司网络上使用的移动设备。

您可以创建新 MDM 门户，也可以编辑或复制现有 MDM 门户。您可以为所有 MDM 系统创建单个 MDM 门户，也可以为每个系统创建一个门户。您可以删除任何 MDM 门户，包括Cisco ISE 提供的默认门户。默认门户用于第三方 MDM 提供商。

您可以创建新 MDM 门户，也可以编辑或复制现有 MDM 门户。您可以删除任何 MDM 门户，包括 Cisco ISE 提供的默认门户。默认门户用于第三方 MDM 提供商。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保您具有配置用于此门户的所需证书和终端身份组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **移动设备管理 (Mobile Device Management)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新**门户设置 (Portal Settings)** 中的端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新以下适用于每个特定页面的设置：

- 在**员工移动设备管理设置 (Employee Mobile Device Management Settings)** 中，访问提供用于配置第三方 MDM 提供商的链接，然后使用 MDM 门户定义员工的接受策略行为。
- **支持信息页面设置 (Support Information Page Settings)**，用于帮助访客提供可供服务中心用于对网络访问问题进行故障排除的信息。

步骤 6 在**门户页面自定义 (Portal Page Customization)** 选项卡上，自定义设备注册过程中显示在 MDM 门户中的**内容区域 (Content Area)** 消息。

- **无法接通 (Unreachable)**：输入当无法访问所选 MDM 系统时显示的内容。

- **不合规 (Non-compliant)**：输入当正在注册的设备不符合 MDM 系统要求时显示的内容。
- **继续 (Continue)**：输入当设备在发生连接问题的情况下尝试连接网络时显示的内容。
- **注册 (Enroll)**：输入当设备需要 MDM 代理并需要在 MDM 系统中注册时显示的内容。

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。另请参阅以下主题：

- 将证书添加到设备门户 ， 第 703 页
- 创建终端身份组 ， 第 704 页
- 创建授权配置文件 ， 第 713 页
- 自定义设备门户 ， 第 715 页

创建我的设备门户

您可以提供我的设备门户，以使员工能够添加并注册其个人设备，这些设备不支持本地请求方且无法使用自带设备 (BYOD) 门户进行添加。然后，您可以使用我的设备门户管理已使用任一门户添加的所有设备。

您可以创建新的我的设备门户，也可以编辑或复制现有我的设备门户。您可以删除任何我的设备门户，包括Cisco ISE 提供的默认门户。

您在**门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡下对**门户和页面设置 (Portal & Page Settings)** 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个页面（例如 Support Information 页面），则该页面会显示在流程中，并且员工将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除。

开始之前

确保您具有配置用于此门户的所需证书、外部身份存储区、身份源序列和终端身份组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备 (My Devices)** > **创建、编辑或复制 (Create, Edit or Duplicate)**。

步骤 2 在**门户名称** 中提供唯一的门户名称，并在**说明** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

步骤 3 使用**语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

步骤 4 更新 **Portal Settings** 中的端口、证书组标签、身份源序列、终端身份组等的默认值，然后定义适用于整体门户的行为。

步骤 5 更新以下适用于每个特定页面的设置：

- **登录页面设置 (Login Page Settings)**：指定员工凭证和登录准则。
- **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)**：添加单独的 AUP 页面，并规定员工的可接受使用政策行为。
- **登录后横幅页面设置 (Post-Login Banner Page Settings)**：在员工登录到门户后向其通知其他信息。
- **员工更改密码设置 (Employee Change Password Settings)**：允许员工更改其自己的密码。仅在员工是内部用户数据库的一部分时，才会启用此选项。

步骤 6 在 **Portal Page Customization** 选项卡中，自定义注册和管理过程中显示在我的设备门户中的以下信息：

- 标题、说明、内容、字段和按钮标签
- 错误消息和通知消息

步骤 7 点击**保存 (Save)**，然后点击**关闭 (Close)**。

下一步做什么

如果希望更改门户外观，您可以对其进行自定义。请参阅

相关主题

自定义设备门户，第 715 页
我的设备门户，第 696 页
显示员工添加的设备，第 715 页

创建授权配置文件

当授权门户时，将会设置网络访问的网络授权配置文件和规则。

开始之前

您必须先创建门户，然后才能对其进行授权。

步骤 1 为门户设置特殊授权配置文件。
步骤 2 为配置文件创建授权策略规则。

创建授权配置文件

各门户要求您为其设置特殊的授权配置文件。

开始之前

如果不打算使用默认门户，您必须先创建门户以便将门户名称与授权配置文件关联。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 使用您希望授权门户使用的名称创建授权配置文件。

下一步做什么

您应当创建门户授权策略规则，用于新创建的授权配置文件。

创建授权策略规则

要配置供门户在响应用户（访客、发起人、员工）的访问请求时使用的重定向 URL，请为该门户定义授权策略规则。

url-redirect 会根据门户类型采取以下形式，其中：

ip:port：IP 地址和端口号

PortalID：唯一端口名称

对于热点访客门户：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

对于移动设备管理 (MDM) 门户：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)** 以在**标准 (Standard)** 策略下创建新授权策略。

步骤 2 对于**条件 (Conditions)**，请选择要用于门户验证的终端身份组。例如，对于热点访客门户，选择默认的 **GuestEndpoints** 终端身份组；而对于 MDM 门户，选择默认的 **RegisteredDevices** 终端身份组。

注释 由于热点访客门户仅颁发终止 CoA，请不要将 Network Access:UseCase EQUALS Guest Flow 用作热点访客授权策略中的一个验证条件。而是匹配终端归属的身份组用于验证。例如，

- 如果为访客终端 + 无线 MAB，则允许访问
- 如果为无线 MAB，则热点重定向

步骤 3 对于 **Permissions**，请选择创建的门户授权配置文件。

注释 在使用启用了 MAC 选项的字典属性创建授权条件（例如 RADIUS.Calling-Station-ID）时，必须使用 Mac 运算符（例如 Mac_equals）支持不同的 MAC 格式。

自定义设备门户

可以通过自定义门户主题、更改门户页面上的UI元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户（访客、发起人，在适当的情况下也可以是员工）体验。有关自定义门户的详细信息，请参阅 自定义最终用户 Web 门户 ，第 391 页。

管理员工添加的个人设备

当员工使用自带设备 (BYOD) 或我的设备门户注册设备时，此注册设备将显示在**终端 (Endpoints)** 列表中。虽然员工可以通过删除设备取消该设备与其帐户之间的关联，但设备依然留在Cisco ISE 数据库中。因此，当员工使用自己的设备时，可能需要您协助他们解决遇到的错误。

显示员工添加的设备

您可以使用**终端 (Endpoints)** 列表窗口上显示的**门户用户 (Portal User)** 字段查找特定员工添加的设备。如果需要删除特定用户注册的设备，这可能会有所帮助。默认情况下，此字段不显示，因此在搜索之前必须先将其启用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

步骤 2 在 Dashlet 下方，点击终端列表右上角可用的**设置 (Settings)** 图标。

步骤 3 选中**门户用户 (Portal User)**复选框启用**门户用户 (Portal User)**切换按钮以在终端列表中显示这些信息。

步骤 4 点击 **Go**（前往）。

步骤 5 点击**过滤器 (Filter)** 下拉列表，并选择**快速过滤器 (Quick Filter)**。

步骤 6 在 **Portal User** 字段中输入用户的名称，以仅显示分配给该特定用户的终端。

向我的设备门户添加设备时出错

如果设备已由其他员工添加，并且该设备仍在终端数据库中，则员工无法添加该设备。

如果员工尝试添加Cisco ISE 数据库中已存在的设备：

- 如果设备支持本地请求方调配，则我们建议通过 BYOD 门户添加设备。此操作将覆盖该设备最初添加到网络时创建的任何注册详细信息。
- 如果该设备是 MAC 身份验证绕行 (MAB) 设备，如打印机，则必须先解决设备的所有权。如果适当，您可以使用管理员的门户从终端数据库中删除该设备，以便新的所有者可以使用“我的设备”(My Devices) 门户成功添加该设备。

注释 当管理员门户关闭时，“我的设备”(My Devices) 门户不可用。

从我的设备门户删除的设备仍保留在终端数据库中

当员工从“我的设备”(My Devices) 门户删除设备时，系统会从员工的已注册设备列表删除设备，但是设备仍保留在Cisco ISE 终端数据库中并且显示于**终端 (Endpoints)** 列表上。

您可以从“终端”(Endpoints) 窗口永久删除设备。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

限制员工注册的个人设备的数量

可以允许员工注册 1 至 999 台个人设备。无论员工用于注册个人设备的门户如何，此设置均可定义在所有门户上注册的最大设备数量。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。

步骤 2 在**将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

步骤 3 点击**保存 (Save)**。如果不想保存对设置进行的任何更新，请点击**重置 (Reset)** 以恢复为上次保存的值。

监控我的设备门户和终端活动

Cisco ISE 提供各种报告和日志，您可以通过这些报告和日志查看终端与用户管理信息以及访客与发起人活动。

您可以按需或按计划运行这些报告。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)**。

步骤 2 选择**访客 (Guest)** 或**终端和用户 (Endpoints and Users)** 以查看各种访客、发起人和终端相关报告

步骤 3 选择要使用**过滤器 (Filters)** 下拉列表搜索的数据。

步骤 4 在 **Time Range** 中选择您想要查看的数据的时间范围。

步骤 5 点击**运行 (Run)**。

我的设备登录和审核报告

我的设备登录和审核 (My Devices Login and Audit) 报告是跟踪以下信息的一种综合报告：

- 员工在 My Devices 门户上的登录活动。
- 员工在“我的设备”(My Devices) 门户中执行的与设备相关的操作。

此报告位于： **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **访客 (Guest)** > **我的设备登录和审核 (My Devices Login and Audit)**。

注册的终端报告

注册终端 (Registered Endpoints) 报告提供有关由员工注册的所有终端的信息。此报告位于： **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **注册终端 (Registered Endpoints)**。可以过滤**身份 (Identity)**、**终端 ID (Endpoint ID)**、**身份组 (Identity Group)**、**终端配置文件 (Endpoint Profile)** 等属性并生成报告。

可以查询分配给**注册设备 (Registered Devices)** 终端身份组的终端的终端数据库。还可以为将**门户用户 (Portal User)** 属性设置为非空值的特定用户生成报告。

注册终端 (Registered Endpoints) 报告提供有关选定时间段内由特定用户通过设备注册门户注册的终端列表的信息。

第 10 章

安全有线接入

在思科 ISE 中定义网络设备

网络设备（如交换机或路由器）是一种向Cisco ISE 发送身份验证、授权和记账 (AAA) 服务请求所借助的 AAA 客户端。在Cisco ISE 中定义网络设备，以启用Cisco ISE 与网络设备之间的交互。

可以配置用于 RADIUS 或 TACACS AAA 的网络设备，以及用于分析服务的简单网络管理协议 (SNMP)，以收集Cisco发现协议和链路层发现协议 (LLDP) 属性进行终端分析，以及用于Cisco Trustsec 设备的 Trustsec 属性。未在Cisco ISE 中定义的网络设备无法收到Cisco ISE 的 AAA 服务。

在网络设备定义中：

- 选择适合网络设备的供应商配置文件。配置文件包括设备的预定义配置，如URL 重定向设置和授权变更。
- 配置用于 RADIUS 身份验证的 RADIUS 协议。当Cisco ISE 收到网络设备的 RADIUS 请求时，它会查找相应的设备定义以检索所配置的共享密钥。如果Cisco ISE 找到设备定义，它会获取在设备上配置的共享密钥并将其与请求中的共享密钥进行匹配，对访问权限进行身份验证。如果共享密钥匹配，RADIUS 服务器将进一步根据策略和配置处理该请求。如果共享密钥不匹配，系统会向网络设备发送拒绝响应。并生成一份未通过身份验证的报告，提供失败原因。
- 配置用于进行 TACACS+ 身份验证的 TACACS+ 协议。当Cisco ISE 收到网络设备的 TACACS+ 请求时，它会查找相应的设备定义以检索配置的共享密钥。如果Cisco ISE 找到设备定义，它会获取在设备上配置的共享密钥并将其与请求中的共享密钥进行匹配，对访问权限进行身份验证。如果共享密钥匹配，TACACS+ 服务器将进一步根据策略和配置处理该请求。如果共享密钥不匹配，系统会将拒绝响应发送到网络设备，并生成一份未通过身份验证的报告，提供失败原因。

- 可以在网络设备定义中配置用于分析服务的简单网络管理协议(SNMP)，以便与网络设备进行通信并对连接到网络设备的终端进行分析。
- 必须在Cisco ISE 中定义支持Cisco Trustsec 的设备才能处理来自这类设备的请求，支持 Trustsec 的设备可以是Cisco Trustsec 解决方案的一部分。任何支持Cisco Trustsec 解决方案的交换机都是支持Cisco TrustSec 的设备。

  Cisco Trustsec 设备不使用 IP 地址。相反，必须定义其他设置，以便Cisco Trustsec 设备可与Cisco ISE 通信。

  支持Cisco TrustSec 的设备使用 Trustsec 属性与Cisco ISE 通信。支持Cisco Trustsec 的设备（例如 Nexus 7000 系列交换机、Catalyst 6000 系列交换机、Catalyst 4000 系列交换机和 Catalyst 3000 系列交换机）使用您在添加Cisco Trustsec 设备时定义的 Trustsec 属性进行身份验证。

注释 在Cisco ISE 上配置网络设备时，我们建议不要在共享密钥中包含反斜线 (\)。这是因为，在升级Cisco ISE 时，反斜线不会出现在共享密钥中。但请注意，如果重新映像Cisco ISE 而不是对其进行升级，则共享密钥中会显示反斜线。

在思科 ISE 中定义默认网络设备

Cisco ISE 支持用于 RADIUS 和 TACACS 身份验证的默认设备定义。您可以定义Cisco ISE 在找不到特定 IP 地址的设备定义时可以使用的默认网络设备。此功能允许您为新调配的设备定义一个默认的 RADIUS 或 TACACS 共享密钥和访问权限级别。

注释 我们建议仅为基本 RADIUS 和 TACACS 身份验证添加默认设备定义。对于高级流程，您必须为每个网络设备添加单独的设备定义。

当Cisco ISE 从网络设备接收到 RADIUS 或 TACACS 请求时，Cisco ISE 会查找对应的设备定义，以检索网络设备定义中配置的共享密钥。

当Cisco ISE 收到 RADIUS 或 TACACS 请求时，它执行以下程序：

1. 查找与请求中的地址匹配的具体 IP 地址。
2. 查找范围以了解请求中的 IP 地址是否属于指定的范围。
3. 如果步骤 1 和 2 都失败了，它会使用默认设备定义（如已定义）处理请求。

Cisco ISE 会获取设备定义中为该设备配置的共享密钥并将其与 RADIUS 或 TACACS 请求中的共享密钥进行匹配以执行访问身份验证。如果找不到设备定义，Cisco ISE 会从默认网络设备定义中获取共享密钥并处理 RADIUS 或 TACACS 请求。

网络设备

您可以使用这些窗口在Cisco ISE 中添加和管理网络设备。

网络设备定义设置

下表介绍**网络设备 (Network Devices)** 窗口上的字段，您可以使用该窗口配置Cisco ISE 中的网络访问设备。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**，然后点击**添加 (Add)**。

网络设备设置

下表介绍**新网络设备 (New Network Devices)** 窗口中的字段。

表 *110:* 网络设备设置

字段名称	说明
名称	输入网络设备的名称。 您可以为网络设备提供一个不同于设备主机名的描述性名称。设备名称是一个逻辑标识符。 **注释** 配置设备名称后无法进行编辑。
说明	输入设备的说明。

字段名称	说明
IP 地址或 **IP** 范围	从下拉列表中选择以下选项之一，并在显示的字段中输入所需的值： • **IP 地址**：输入单个 IP 地址（IPv4 或 IPv6 地址）和子网掩码。 • **IP 范围**：输入所需的 IPv4 地址范围。要在身份验证期间排除 IP 地址，请在**排除 (Exclude)** 字段中输入 IP 地址或 IP 地址范围。 以下是定义 IP 地址和子网掩码或 IP 地址范围时必须遵守的准则： • 您可以定义一个特定 IP 地址或具有子网掩码的 IP 地址范围。如果设备 A 定义了 IP 地址范围，则可以使用在设备 A 中定义的 IP 地址范围的某个地址配置另一设备 B。 • 您可以在所有八位组中定义 IP 地址范围。您可以使用连字符 (-) 或使用星号 (*) 作为通配符来指定 IP 地址范围。例如，*.*.*.*、1-10.1-10.1-10.1-10 或 10-11.*.5.10-15。 • 在已添加 IP 地址范围子集的场景中，可以从配置的范围中排除该子集。例如，10.197.65.*/10.197.65.1 或 10.197.65.* 会排除 10.197.65.1。 • 您不能使用相同的特定 IP 地址定义两台设备。 • 您不能使用同一 IP 地址范围定义两台设备。IP 地址范围不得部分或全部重叠。
设备配置文件	从下拉列表中选择网络设备的供应商。 使用下拉列表旁的工具提示可查看选定供应商的网络设备所支持的流和服务。工具提示还显示设备使用的 RADIUS CoA 端口和 URL 重定向类型。这些属性在设备类型的网络设备配置文件中进行定义。
型号名称	从下拉列表中选择设备型号。 在基于规则的策略中查找条件时，可以将型号名称用作其中一个参数。此属性存在于设备字典中。

字段名称	说明
软件版本	从下拉列表中选择在网络设备上运行的软件版本。 在基于规则的策略中查找条件时，您可以将软件版本用作其中一个参数。此属性存在于设备字典中。
网络设备组	在**网络设备组 (Network Device Group)** 区域中，从**位置 (Location)**、**IPSEC** 和**设备类型 (Device Type)** 下拉列表中选择所需的值。 如果未将设备专门分配到组，则设备将加入默认设备组（根网络设备组），位置为**所有位置 (All Locations)**，设备类型为**所有设备类型 (All Device Types)**。

RADIUS 身份验证设置

下表介绍 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 区域中的字段。

表 *111:*“*RADIUS* 身份验证设置”*(RADIUS Authentication Settings)* 区域中的字段

字段名称	使用指南
RADIUS UDP 设置	
协议	显示 **RADIUS** 作为所选协议。
共享密钥	输入网络设备的共享密钥。 共享密钥是使用 **radius-host** 命令和 **pac** 选项在网络设备上配置的密钥。 注释 共享密钥长度必须等于或大于在**设备安全设置 (Device Security Settings)** 窗口（**管理 [Administration] > 网络资源 [Network Resources] > 网络设备 (Network Devices) > 设备安全设置 [Device Security Settings]**）的 **RADIUS 共享密钥最小长度 (Minimum RADIUS Shared Secret Length)** 字段中配置的值。 对于 RADIUS 服务器，长度最好为 22 个字符。对于新安装和升级的部署，默认情况下，共享密钥长度为四个字符。您可以在**设备安全设置 (Device Security Settings)** 窗口中更改此值。

字段名称	使用指南
使用第二个共享密钥	指定网络设备和Cisco ISE 要使用的第二个共享密钥。 注释 虽然Cisco TrustSec 设备可以利用双重共享密钥（密钥），但Cisco ISE 发送的Cisco TrustSec CoA 数据包将始终使用第一个共享密钥（密钥）。要启用第二个共享密钥，请选择必须从哪一个 Cisco ISE 节点向 TrustSec 设备发送 Cisco TrustSec CoA 数据包。在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **高级 TrustSec 设置 (Advanced TrustSec Settings)** 窗口的**发送自 (Send From)** 下拉列表中，配置要用于此任务的Cisco ISE 节点。您可以选择主管理节点 (PAN) 或策略服务节点 (PSN)。如果所选 PSN 节点关闭，PAN 将向Cisco TrustSec 设备发送Cisco TrustSec CoA 数据包。 注释 RADIUS 访问请求的“第二共享密钥”功能仅适用于包含**消息-身份验证器 (Message-Authenticator)** 字段的数据包。

字段名称	使用指南
CoA 端口	指定要用于 RADIUS DTLS CoA 的端口。 设备的默认CoA端口在为网络设备配置的网络设备配置文件中进行定义（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Device Profiles)**）。点击**设置为默认 (Set To Default)** 按钮以使用默认 CoA 端口。 注释 如果修改在 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 下的**网络设备 (Network Devices)** 窗口（**管理 [Administration]** > **网络资源 [Network Resources]** > **网络设备 [Network Devices]**）中指定的 CoA 端口，请确保在**网络设备配置文件 (Network Device Profile)** 窗口（**管理 [Administration]** > **网络资源 [Network Resources]** > **网络设备配置文件 [Network Device Profiles]**）中为相应配置文件指定相同的 CoA 端口。
RADIUS DTLS 设置	
需要 DTLS	如果选中**需要 DTLS (DTLS Required)** 复选框，则Cisco ISE 仅处理来自此设备的 DTLS 请求。如果禁用此选项，则Cisco ISE 会同时处理来自此设备的 UDP 和 DTLS 请求。 RADIUS DTLS 为安全套接字层 (SSL) 隧道建立和 RADIUS 通信提供了更高的安全性。
共享密钥	显示用于 RADIUS DTLS 的共享密钥。此值为固定值，用于计算消息摘要 5 (MD5) 完整性检查。
CoA 端口	指定用于 RADIUS DTLS CoA 的端口。
CoA ISE 证书 CA 颁发者	从下拉列表中选择要用于 RADIUS DTLS CoA 的证书颁发机构。

字段名称	使用指南
DNS 名称	输入网络设备的 DNS 名称。如果在 **RADIUS 设置 (RADIUS Settings)** 窗口下启用**启用 RADIUS/DTLS客户端身份验证选项**（**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **RADIUS**，Cisco ISE会将此DNS名称与客户端证书中指定的DNS名称进行比较，以验证网络设备的身份。
常规设置	
启用 **KeyWrap**	仅当网络设备支持 KeyWrap 算法时，选中**启用 KeyWrap (Enable KeyWrap)** 复选框。此选项用于通过 AES KeyWrap 算法提高 RADIUS 安全性。 **注释** 当在 FIPS 模式下运行思科 ISE 时，必须在网络设备上启用 KeyWrap。
密钥加密密钥	输入用于会话加密（保密）的加密密钥。
消息身份验证器代码密钥	输入用于 RADIUS 消息键控散列消息验证码 (HMAC) 计算的密钥。
密钥输入格式	点击以下格式之一对应的单选按钮： • **ASCII**：在**密钥加密密钥 (Key Encryption Key)** 字段中输入的值的长度必须为 16 个字符（字节），在**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入的值长度必须为 20 个字符（字节）。 • **十六进制 (Hexadecimal)**：在**密钥加密密钥 (Key Encryption Key)** 字段中输入的值的长度必须为32个字符（字节），在**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入的值长度必须为 40 个字符（字节）。 指定想要用于输入Cisco ISE FIPS 加密密钥的密钥输入格式，从而使其与无线 LAN 控制器上的配置一致。您指定的值必须是密钥的正确（完整）长度，不允许使用短于此长度的值。

TACACS 身份验证设置

表 *112: TACACS* 身份验证设置区域中的字段

字段名称	使用指南
共享密钥	当启用 TACACS+ 协议时，会向网络设备分配文本字符串。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。
停用的共享密钥处于启用状态	当停用期处于启用状态时显示。
淘汰	停用现有的共享密钥而不是结束它。点击**停用 (Retire)** 时，系统会显示一个消息框。您可以点击**是 (Yes)** 或**否 (No)**。
剩余停用期	（仅当在**停用 (Retire)** 消息框中选择**是 (Yes)** 时可用）显示在以下导航路径中指定的默认值：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。您可以更改默认值。 这允许输入新的共享密钥。旧共享密钥会在指定天数内保持有效。
结束	（仅当在**停用 (Retire)** 消息框中选择**是 (Yes)** 时可用）结束停用期并终止旧共享密钥。
启用单连接模式	选中**启用单连接模式 (Enable Single Connect Mode)** 复选框，将单一 TCP 连接用于与网络设备之间的所有 TACACS 通信。点击以下选项之一的单选按钮： • **传统思科设备 (Legacy Cisco Devices)** • **TACACS 草案合规性单连接支持** 如果禁用**单连接模式 (Single Connect Mode)**，Cisco ISE 会对每个 TACACS 请求使用新的 TCP 连接。

SNMP 设置

下表介绍 **SNMP 设置 (SNMP Settings)** 部分中的字段。

表 *113: SNMP* 设置区域中的字段

字段名称	使用指南
SNMP 版本	从 **SNMP (SNMP 版本)** 下拉列表中，选择以下选项之一： • **1**：SNMPv1 不支持通知。 • **2c** • **3**：SNMPv3 是最安全的型号，因为当在后续步骤中选择 **Priv** 安全级别时，它允许加密数据包。 注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的**网络设备会话状态 (Network Device Session Status)** 摘要报告（**操作 [Operations]** > **报告 [Reports]** > **诊断 [Diagnostics]** > **网络设备会话状态 [Network Device Session Status]**）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。
SNMP 只读社区	（仅适用于 SNMP 版本 1 和 2c）输入只读社区字符串，为Cisco ISE 提供特殊类型的设备访问权限。 注释 不允许使用插入符号 (circumflex ^)。
SNMP 用户名	（仅适用于 SNMP 版本 3）输入 SNMP 用户名。
安全级别	（仅适用于 SNMP 版本 3）从**安全级别 (Security Level)** 下拉列表中选择以下选项之一： • **身份验证 (Auth)**：启用 MD5 或安全散列算法 (SHA) 数据包身份验证。 • **无身份验证 (No Auth)**：无身份验证，无隐私安全级别。 • **隐私 (Priv)**：启用数据加密标准 (DES) 数据包加密。

字段名称	使用指南
身份验证协议	（选择安全级别**身份验证 [Auth]** 和**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）从**身份验证协议 (Auth Protocol)** 下拉列表中，选择希望网络设备使用的身份验证协议。 • **MD5** • **SHA**
身份验证密码	（选择安全级别**身份验证 [Auth]** 和**隐私 [Priv]** 时，仅适用于SNMP版本3）输入身份验证密钥。密码的长度应至少为 8 个字符。 点击**显示 (Show)**，显示已为设备配置的身份验证密码。 **注释** 不能使用插入符号 (circumflex ^)。
隐私协议	（选择安全级别**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）从**隐私协议 (Privacy Protocol)** 下拉列表中，选择以下选项之一： • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
隐私密码	（选择安全级别**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）输入隐私密钥。 点击**显示 (Show)**，显示已为设备配置的隐私密码。 **注释** 不能使用插入符号 (circumflex ^)。
轮询间隔	输入轮询间隔（秒）。默认值为 3600 秒。
链路陷阱查询	选中**链路陷阱查询 (Link Trap Query)** 复选框，可接收和解析通过SNMP陷阱接收的链路接通和链路断开通知。
MAC 陷阱查询	选中**链路陷阱查询 (Link Trap Query)** 复选框，可接收和解析通过 SNMP 陷阱接收的 MAC 通知。

字段名称	使用指南
原始策略服务节点	从**原始策略服务节点 (Originating Policy Services Node)** 下拉列表中，选择要用于轮询 SNMP 数据的Cisco ISE 服务器。此字段的默认值为**自动 (Auto)**。从下拉列表中选择特定值以覆盖设置。

高级 Trustsec 设置

下表介绍**高级 Trustsec 设置 (Advanced Trustsec Settings)** 部分中的字段。

表 *114:* 高级 *TrustSec* 设置区域中的字段

字段名称	使用指南
设备身份验证设置	
将设备 ID 用于 Trustsec 标识	如果希望在**设备 ID (Device ID)** 字段中将设备名称作为设备标识符列出，请选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框。
设备 ID	仅当未选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框时，才能在此字段中输入设备 ID。
密码	输入在Cisco TrustSec 设备 CLI 中配置的密码，用于对Cisco TrustSec 设备进行身份验证。 点击**显示 (Show)** 可显示密码。
HTTP REST API 设置	
启用 **HTTP REST API (Enable HTTP REST API)**	选中**启用 HTTP REST API (Enable HTTP REST API)** 复选框以使用 HTTP REST API 向网络设备提供所需的Cisco TrustSec 信息。与 RADIUS 协议相比，这提高了在短时间内下载大型配置的效率和能力。它还通过使用 TCP over UDP 提高了可靠性。
用户名	输入在Cisco TrustSec 设备 CLI 中配置的用户名，用于对Cisco TrustSec 设备进行身份验证。用户名不能包含特殊字符，如空格 ! % ^ : ; , [{ | }] ` " = < > ?
密码	输入在Cisco TrustSec 设备 CLI 中配置的密码，用于对Cisco TrustSec 设备进行身份验证。
Trustsec 设备通知和更新	

字段名称	使用指南
设备 ID	仅当未选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框时，才能在此字段中输入设备 ID。
密码	输入在Cisco TrustSec 设备 CLI 中配置的密码，用于对Cisco TrustSec 设备进行身份验证。 点击**显示 (Show)** 可显示密码。
每<...> 下载一次环境数据 (Download Environment Data Every <...>)	通过从此区域的下拉列表中选择所需的值，指定设备从Cisco ISE 下载其环境数据时必须遵守的时间间隔。您可以选择秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。
每 <...>下载一次对等授权策略 (Download Peer Authorization Policy Every <...>)	通过从此区域的下拉列表中选择所需的值，指定设备从Cisco ISE 下载对等授权策略时必须遵守的时间间隔。您可以指定单位为秒、分钟、小时、天或周的时间间隔。默认值为一天。
每 <...>重新进行身份验证 (Reauthentication Every <...>)	通过从此区域的下拉列表中选择所需的值，指定在初始身份验证后设备对照Cisco ISE 重新进行身份验证的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。例如，如果输入 1000 秒，则设备会每 1000 秒对照Cisco ISE 对自身重新进行身份验证。默认值为一天。
每 <...>下载 SGACL 列表 (Download SGACL Lists Every <...>)	通过从此区域的下拉列表中选择所需的值，指定设备从Cisco ISE 下载 SGACL 列表时遵守的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。
其他 **TrustSec** 设备信任该设备（**Trustsec** 信任）	选中**其他 TrustSec 设备信任该设备 (Other TrustSec Devices to Trust This Device)** 复选框，可允许所有对等设备信任此Cisco TrustSec 设备。如果取消选中此复选框，则对等设备不信任此设备，所有从此设备到达的数据包都会相应地标注颜色或进行标记。

字段名称	使用指南
将配置更改发送到设备	如果希望Cisco ISE 使用 CoA 或 CLI (SSH) 将Cisco TrustSec 配置更改发送到Cisco TrustSec 设备，请选中**将配置更改发送到设备 (Send Configuration Changes to Device)** 复选框。根据需要，点击 **CoA** 或 **CLI (SSH)** 的单选按钮。 如果希望Cisco ISE 使用 CoA 将配置更改发送到 Cisco TrustSec 设备，请选择 **CoA** 选项。 如果希望Cisco ISE 使用 CLI（使用 SSH 连接）将配置更改发送到Cisco TrustSec 设备，请选择 **CLI (SSH)** 选项。有关详细信息，请参阅 向不支持 CoA 的设备推送配置更改，第 921 页。
发送自	从下拉列表中选择必须从哪一个Cisco ISE 节点将配置更改发送到Cisco TrustSec 设备。您可以选择 PAN 或 PSN 节点。如果所选择的 PSN 节点关闭，则使用 PAN 将配置更改发送到Cisco TrustSec 设备。
测试连接	您可以使用此选项测试Cisco TrustSec 设备与所选 Cisco ISE 节点（PAN 或 PSN）之间的连接。
SSH 密钥	要使用此功能，请打开从Cisco ISE 到网络设备的 SSHv2 隧道，然后使用设备的 CLI 检索 SSH 密钥。您必须复制此密钥并将其粘贴到 **SSH 密钥 (SSH Key)** 字段中以进行验证。有关详细信息，请参阅《》中的“ SSH 密钥验证”部分请参阅 SSH 密钥验证，第 922 页。
设备配置部署设置	
当部署安全组标签映射更新时纳入该设备	如果希望Cisco TrustSec 设备使用设备接口凭据获取 IP-SGT 映射，请选中**当部署安全组标记映射更新时包含此设备 (Include this device when deploying Security Group Tag Mapping Updates)** 复选框。
EXEC 模式用户名	输入用于登录Cisco TrustSec 设备的用户名。
EXEC 模式密码	输入设备密码。 点击**显示 (Show)** 可查看密码。
启用模式密码	（可选）输入用于在特权模式下编辑Cisco TrustSec 设备配置的启用密码。 点击**显示 (Show)** 可查看密码。

字段名称	使用指南
带外 **Trustsec PAC**	
颁发日期	显示Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发日期。
到期日期	显示Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的到期日期。
颁发者	显示Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发者（Cisco TrustSec 管理员）名称。
生成 **PAC**	点击**生成 PAC (Generate PAC)** 按钮，为Cisco TrustSec 设备生成带外Cisco TrustSec PAC。

相关主题

在思科 ISE 中定义网络设备，第 719 页
思科 ISE 中的第三方网络设备支持，第 740 页
网络设备组，第 748 页
在思科 ISE 中添加网络设备，第 203 页
在思科 ISE 中配置第三方网络设备，第 744 页

默认网络设备定义设置

下表介绍**默认网络设备 (Default Network Device)** 窗口中的字段，该窗口用于配置Cisco ISE 可用于 RADIUS 和 TACACS+ 身份验证的默认网络设备。选择以下导航路径之一：

- **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **默认设备 (Default Device)**
- **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **默认设备 (Default Devices)**

表 ***115:*** **“默认网络设备”*(Default Network Device)* 窗口中的字段**

字段名称	使用指南
默认网络设备状态	从**默认网络设备状态 (Default Network Device Status)** 下拉列表中选择**启用 (Enable)**，以启用默认网络设备定义。 注释 如果默认设备已启用，则必须通过选中窗口中的复选框启用 RADIUS 或 TACACS+ 身份验证设置。
设备配置文件	显示**思科 (Cisco)** 为默认的设备供应商。

字段名称	使用指南
RADIUS 身份验证设置	
启用 **RADIUS**	选中**启用 RADIUS (Enable RADIUS)** 复选框，启用设备的 RADIUS 身份验证。
RADIUS UDP 设置	
共享密钥	输入共享密钥。共享密钥最大长度为 127 个字符。 共享密钥是您使用 **radius-host** 命令和 **pac** 选项在网络设备上配置的密钥。 注释 共享密钥长度必须等于或大于在**设备安全设置 (Device Security Settings)** 窗口的 **RADIUS 共享密钥最小长度 (Minimum RADIUS Shared Secret Length)** 字段中配置的值（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **设备安全设置 (Device Security Settings)**）。默认情况下，对于新安装和升级的部署，此值为 4 个字符。对于 RADIUS 服务器，长度最好为 22 个字符。
RADIUS DTLS 设置	
需要 **DTLS**	如果选中**需要 DTLS (DTLS Required)** 复选框，则Cisco ISE 仅处理来自此设备的 DTLS 请求。如果禁用此选项，则Cisco ISE 会同时处理来自此设备的 UDP 和 DTLS 请求。 RADIUS DTLS 为 SSL 隧道建立和 RADIUS 通信提供了更高的安全性。
共享密钥	显示用于 RADIUS DTLS 的共享密钥。此值为固定值，用于计算 MD5 完整性检查。
CoA ISE 证书 CA 颁发者	从 **CoA ISE 证书 CA 颁发者 (Issuer CA of ISE Certificates for CoA)** 下拉列表中，选择要用于 RADIUS DTLS CoA 的证书颁发机构。
常规设置	

字段名称	使用指南
启用 **KeyWrap**	仅在网络设备支持 KeyWrap 算法时选中**启用 KeyWrap (Enable KeyWrap)** 复选框，这可以通过 AES KeyWrap 算法提高 RADIUS 安全性。
密钥加密密钥	启用 KeyWrap 时，输入用于会话加密（保密）的加密密钥。
消息身份验证器代码密钥	启用 KeyWrap 时，输入对 RADIUS 消息进行键控散列消息身份认证代码 (HMAC) 计算的密钥。
密钥输入格式	通过点击相应的单选按钮选择以下格式之一，并在**密钥加密密钥 (Key Encryption Key)** 和**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入值： • **ASCII**：**密钥加密密钥 (Key Encryption Key)** 长度必须为 16 个字符（字节），而**消息身份验证器代码密钥 (Message Authenticator Code Key)** 长度必须为 20 个字符（字节）。 • **十六进制 (Hexadecimal)**：**密钥加密密钥 (Key Encryption Key)** 长度必须为 32 个字节，而**消息身份验证器代码密钥 (Message Authenticator Code Key)** 长度必须为 40 个字节。
TACACS 身份验证设置	
共享密钥	当 TACACS+ 协议启用时，将文本字符串分配给网络设备。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。
停用的共享密钥处于启用状态	当停用期处于启用状态时显示。
淘汰	停用现有的共享密钥而不是结束它。点击**停用 (Retire)** 时，系统会显示一个消息框。点击**是 (Yes)** 或**否 (No)**。

字段名称	使用指南
剩余停用期	（仅当在上述消息框中选择**是 (Yes)** 时可用）显示在以下导航路径中指定的默认值： **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。 您可以更改默认值。 这允许您输入新的共享密钥，而且旧共享密钥将在指定天数中保持启用状态。
结束	（只有当您在上述消息框中选择**是**时才可用）结束停用期并终止旧共享密钥。
启用单连接模式	选中**启用单连接模式 (Enable Single Connect Mode)** 复选框，将单一 TCP 连接用于与网络设备之间的所有 TACACS+ 通信。点击以下选项之一的单选按钮： • **传统思科设备 (Legacy Cisco Devices)** • **TACACS 草案合规性单连接支持 (TACACS Draft Compliance Single Connect Support)**。 如果禁用此选项，Cisco ISE 会为每个 TACACS+ 请求使用新的 TCP 连接。

网络设备导入设置

下表介绍 Network Device Import 页面上的字段，您可以使用此页面将网络设备详细信息导入Cisco ISE。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

表 *116:* 网络设备导入设置

字段名称	使用指南
生成模板	点击**创建模板 (Generate a Template)** 可创建逗号分隔值 (CSV) 模板文件。 使用相同格式的网络设备信息更新模板，并将其保存在本地。然后，使用编辑的模板将网络设备导入任何Cisco ISE 部署。

字段名称	使用指南
文件	点击**选择文件 (Choose File)**，选择您可能最近创建的或以前从任何Cisco ISE 部署导出的 CSV 文件。 您可以使用**导入 (Import)** 选项将包含新的和更新后的网络设备信息的网络设备导入其他Cisco ISE 部署中。
用新数据覆盖现有数据	选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框可用您的导入文件中的设备取代现有网络设备。 如不选中此复选框，则导入文件中可用的新网络设备定义将添加到网络设备存储库。系统会忽略重复条目。
遇到第一个错误时停止导入	如果您希望Cisco ISE 在导入过程中遇到错误时停止导入，请选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。Cisco ISE 会导入网络设备，直至出现错误。 如未选中此复选框并且遇到错误，系统会报错并且Cisco ISE 会继续导入剩余设备。

相关主题

在思科 ISE 中定义网络设备，第 719 页
思科 ISE 中的第三方网络设备支持，第 740 页
将网络设备导入思科 ISE，第 738 页

在思科 ISE 中添加网络设备

您可以在Cisco ISE 中添加网络设备或使用默认网络设备。

您还可以在**网络设备 (Network Devices)** 窗口（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）中添加网络设备。

开始之前

必须在要添加的网络设备上启用 AAA 功能。请参阅启用 AAA 功能的命令，第 1197 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**名称 (Name)**、**说明** 和 **IP 地址 (IP Address)** 字段中输入相应的值。

步骤 4 从**设备配置文件 (Device Profile)**、**型号名称 (Model Name)**、**软件版本 (Software Version)** 和**网络设备组 (Network Device Group)** 字段的下拉列表中选择所需的值。

步骤 5 （可选）选中 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 复选框以配置用于身份验证的 RADIUS 协议。

步骤 6 （可选）选中 **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框以配置用于身份验证的 TACACS 协议。

步骤 7 （可选）选中 **SNMP 设置 (SNMP Settings)** 复选框以为Cisco ISE 分析服务配置 SNMP，以便从设备收集信息。

步骤 8 （可选）选中**高级 Trustsec 设置 (Advanced Trustsec Settings)** 复选框以配置启用Cisco Trustsec 的设备。

步骤 9 点击**提交 (Submit)**。

将网络设备导入思科 ISE

要使Cisco ISE 能够与网络设备通信，您必须在Cisco ISE 中添加网络设备的设备定义。通过**网络设备 (Network Devices)** 窗口将网络设备的设备定义导入Cisco ISE（从主菜单中，选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）。

使用逗号分隔值 (CSV) 文件，将设备定义列表导入到Cisco ISE 节点中。当您在**网络设备 (Network Devices)** 窗口中点击**导入 (Import)** 时，CSV 模板文件可用。下载此文件，输入所需的设备定义，然后通过**导入 (Import)** 窗口上传编辑的文件。

您不能同时运行同一资源类型的多项导入。例如，不能同时从两个不同的导入文件导入网络设备。

导入设备定义的 CSV 文件时，您可以通过点击**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 选项创建新记录或更新现有记录。

每个Cisco ISE 中的模板导入可能有所不同。请勿导入从其他Cisco ISE 版本导出的网络设备的 CSV 文件。在您的版本的 CSV 模板文件中输入网络设备的详细信息，然后将此文件导入Cisco ISE。

注释 您可以导入 IP 地址在所有八位组的范围内的网络设备。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 点击**导入**。

步骤 3 在显示的**导入网络设备 (Import Network Devices)** 窗口中，点击**生成模板 (Generate A Template)** 下载一个 CSV 文件，您可以编辑它，填好所需的详细信息后导入Cisco ISE。

步骤 4 点击**选择文件 (Choose File)**，从正在运行客户端浏览器的系统中选择该 CSV 文件。

步骤 5 （可选）根据需要，选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 和**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。

步骤 6 点击**导入**。

文件导入完成后，Cisco ISE 会显示摘要消息。摘要消息包括导入状态（成功或不成功）、遇到的错误数（如果有）以及文件导入过程所需的总处理时间。

从思科 ISE 导出网络设备

您可以用 CSV 文件的形式导出Cisco ISE 节点中可用的网络设备的设备定义。然后，您可以将此 CSV 文件导入另一个Cisco ISE 节点，以便设备定义可用于所需的Cisco ISE 节点。

注释 您可以导出 IP 地址在所有八位组中的网络设备。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 点击**导出**。

步骤 3 通过执行以下操作之一，导出添加到Cisco ISE 节点的网络设备的设备定义。

- 选中要导出的设备旁边的复选框，点击**导出 (Export)**，然后从下拉列表中选择**导出所选 (Export Selected)**。
- 点击**导出 (Export)** 并从下拉列表中选择**全部导出 (Export All)**，以便导出添加到Cisco ISE 节点的所有网络设备。

步骤 4 在这两种情况下，设备定义 CSV 文件都会下载到您的系统。

解决网络设备配置问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **评估配置验证器 (Evaluate Configuration Validator)**。

步骤 2 在**网络设备 IP (Network Device IP)** 字段中输入您想要评估其配置的网络设备的 IP 地址。

步骤 3 选中相应复选框，然后点击要与建议模板进行比较的配置选项旁边的单选按钮。

步骤 4 点击**运行 (Run)**。

步骤 5 在显示的**进度详细信息... (Progress Details...)** 区域中，点击**点击此处输入凭证 (Click Here to Enter Credentials)**。在显示的**凭证窗口 (Credentials Window)** 对话框中，输入与网络设备建立连接所需的连接参数和凭证，然后点击**提交 (Submit)**。

要取消工作流程，请在**进度详细信息... (Progress Details...)** 窗口中点击**点击此处取消正在运行的工作流程 (Click Here to Cancel the Running Workflow)**。

步骤 6 选中想要分析的接口旁边的复选框，然后点击**提交 (Submit)**。

步骤 7 点击**显示结果摘要 (Show Results Summary)** 以查看配置评估的详细信息。

执行网络设备命令诊断工具

执行网络设备命令诊断工具允许您在任何网络设备上运行 **show** 命令。

显示的结果与您应在控制台上看到的结果相同。通过此工具，您可以发现设备配置中的任何问题。

使用此工具可验证任何网络设备的配置，也可以使用此工具了解网络设备的配置方式。

要访问执行网络设备命令诊断工具，请选择以下导航路径之一：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **执行网络设备命令 (Execute Network Device Command)**。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **解析器 (Profiler)** > **故障排除 (Troubleshoot)** > **执行网络设备命令 (Execute Network Device Command)**。

在显示的**执行网络设备命令 (Execute Network Device Command)** 窗口中，在相应字段中输入网络设备的 IP 地址和您想要运行的 show 命令。点击**运行 (Run)**。

思科 ISE 中的第三方网络设备支持

Cisco ISE 通过使用网络设备配置文件，支持第三方网络访问设备 (NAD)。不管供应商端实施如何，NAD 配置文件都使用简化的策略配置定义第三方设备的功能。网络设备配置文件包含以下内容：

- 该网络设备支持的协议，例如 RADIUS、TACACS+ 和Cisco TrustSec。可以将任何有关该网络设备的供应商特定的 RADIUS 字典导入到Cisco ISE 中。
- 该设备用于各种身份验证流程的属性和值，例如有线 MAB 和 802.1x。通过这些属性和值，Cisco ISE 可以根据网络设备使用的属性为您的设备检测正确的身份验证流程。
- 网络设备具有的授权更改 (CoA) 功能。虽然 RADIUS 协议 RFC 5176 定义了 CoA 请求，但 CoA 请求中使用的属性因网络设备而异。大多数支持 RFC 5176 的非Cisco设备都会支持“推送”和“断开连接”功能。对于不支持 RADIUS CoA 类型的设备，Cisco ISE 还支持 SNMP CoA。
- 网络设备针对 MAB 流程使用的属性和协议。不同供应商的网络设备采用不同方式执行 MAB 身份验证。
- 设备使用的 VLAN 和 ACL 权限。保存配置文件后，Cisco ISE 为每个配置的权限自动生成授权配置文件。
- URL 重定向技术信息。对于高级流程（如自带设备 (BYOD)、访客访问和终端安全评估服务），URL 重定向是必需的。在网络设备上有两种类型的 URL 重定向：静态和动态。对于静态 URL 重定向，可以复制Cisco ISE 门户 URL 并将其粘贴到配置中。对于动态 URL 重定向，Cisco ISE 会通过 RADIUS 属性告诉网络设备应重定向至哪个地址。

如果网络设备既不支持动态 URL 重定向，也不支持静态 URL 重定向，则Cisco ISE 提供身份验证 VLAN 配置，用于模拟 URL 重定向。身份验证 VLAN 配置基于Cisco ISE 中运行的 DHCP 和 DNS 服务。要创建身份验证 VLAN 配置，请定义 DHCP 和 DNS 服务设置。有关详细信息，请参阅DHCP 和 DNS 服务。

在Cisco ISE 中定义网络设备后，配置这些设备配置文件或使用Cisco ISE 提供的预配置设备配置文件，以定义Cisco ISE用于启用基本身份验证流程以及高级流程（如分析器、访客、BYOD、MAB 和终端安全评估）的功能。

URL 重定向机制和身份验证 VLAN

在网络中使用第三方设备且该设备不支持动态或静态URL 重定向时，ISE将模拟URL 重定向流程。通过在Cisco ISE 上运行 DHCP 或 DNS 服务来运行此类设备的 URL 重定向模拟流程。

有关详细信息，请参阅DHCP 和 DNS 服务。

以下是身份验证 VLAN 流程的示例：

1. 访客终端连接到 NAD。
2. 网络设备将 RADIUS 或 MAB 请求发送至Cisco ISE。
3. Cisco ISE 运行已配置的身份验证和授权策略，并存储用户帐户信息。
4. Cisco ISE 发送 RADIUS 访问-接受消息，其中包含身份验证 VLAN ID。
5. 访客终端接收网络访问。
6. 终端广播 DHCP 请求，并从Cisco ISE DHCP 服务获取客户端 IP 地址和Cisco ISE DNS sinkhole IP 地址。
7. 访客终端打开浏览器，从中发送 DNS 查询并接收Cisco ISE IP 地址。
8. 终端 HTTP 和 HTTPS 请求定向到Cisco ISE。
9. Cisco ISE 使用“HTTP 301 已移动”(HTTP 301 Moved) 消息进行响应并提供访客门户 URL。终端浏览器重定向到访客门户窗口。
10. 访客终端用户登录以进行身份验证。
11. Cisco ISE 验证终端合规性，然后响应 NAD。Cisco ISE 发送 CoA，授权终端并绕过 sinkhole。
12. 访客用户基于 CoA 获得适当访问权限，终端从企业 DHCP 接收 IP 地址。访客用户现在即可使用网络。

可以使身份验证 VLAN 独立于企业网络，以防止访客终端在通过身份验证之前进行未经授权的网络访问。将身份验证 VLAN IP 助手配置为指向Cisco ISE 计算机，或将一个Cisco ISE 网络接口连接到身份验证 VLAN。

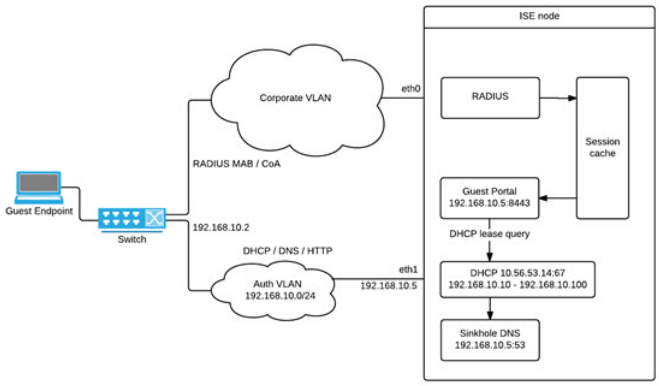
有关VLAN（DHCP和要创建身份验证VLAN配置）设置的详细信息，请参阅 DHCP和DNS服务。

通过从 NAD 配置中配置 VLAN IP 助手可以将多个 VLAN 连接到一个网络接口卡。有关配置 IP 助手的详细信息，请参阅网络设备的管理指南说明。对于包含具有IP助手的VLAN的访客访问流程，

请定义访客门户，并在绑定到MAB授权的授权配置文件中选择此门户。有关访客门户的详细信息，请参阅思科 ISE 访客服务，第 307 页。

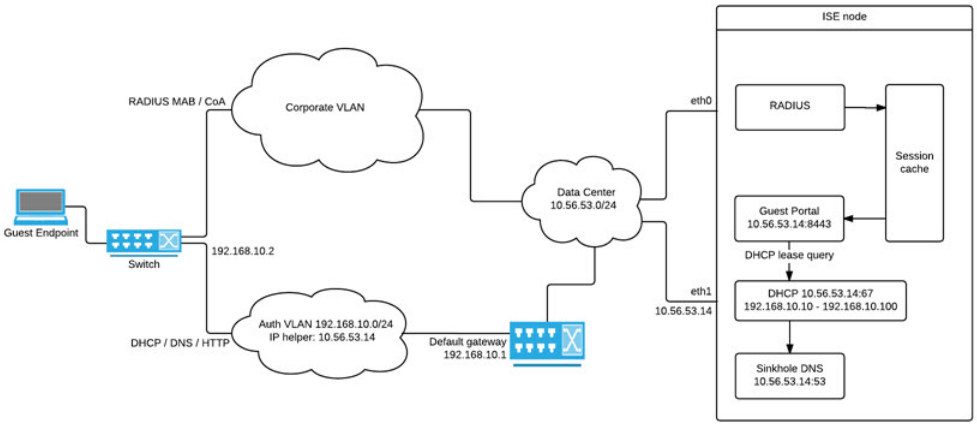
下图显示了定义身份验证VLAN时的基本网络设置（身份验证VLAN直接连接到Cisco ISE节点）。

图 *32:* 连接到思科 *ISE* 节点的身份验证 *VLAN*



下图显示了带有身份验证 VLAN 和 IP 助手的网络：

图 *33:* 配置有 *IP* 助手的身份验证 *VLAN*



CoA 类型

Cisco ISE 同时支持 RADIUS 和 SNMP CoA 类型。必须支持 RADIUS 或 SNMP CoA 类型，NAD 才能在复杂流程中工作，而这对于基本流程不是强制性的。

在从Cisco ISE 中配置 NAD 时定义网络设备支持的 RADIUS 和 SNMP 设置，并在配置 NAD 配置文件时指出要用于特定流程的CoA类型。有关为NAD定义协议的详细信息，请参阅网络设备。在Cisco ISE 中创建设备和 NAD 配置文件之前，请与您的第三方供应商联系，以确认您的 NAD 所支持的 CoA 类型。

网络设备配置文件

Cisco ISE 通过使用网络设备配置文件，支持某些第三方网络访问设备 (NAD)。这些配置文件定义用于启用基本流量和高级流量（如访客、自带设备、MAB 和终端安全评估）的Cisco ISE 功能。

Cisco ISE 包含多个供应商网络设备的预定义配置文件。思科 ISE 2.1 及更高版本已在下表所列的网络设备上测试：

表 *117:* 已经过思科 ***ISE 2.1*** 及更高版本测试的供应商设备

设备类型	供应商	CoA 类型	URL 重定向类型	支持或验证的使用案例				
				802.1X 和 MAB 流	无 CoA 的分析器	带 CoA 的分析器	终端安全评估	访客和 BYOD 流
无线	Aruba 7000，InstantAP	RADIUS	静态 URL	支持	支持	支持	支持	支持
	Motorola RFS 4000	RADIUS	动态 URL	支持	支持	支持	支持	支持
	HP 830	RADIUS	静态 URL	支持	支持	支持	支持	支持
	Ruckus ZD 1200	RADIUS	-	支持	支持	支持	支持	支持
有线	HP A5500	RADIUS	ISE 提供的 Auth VLAN	支持	支持	支持	支持	支持
	HP 3800 和 2920 (ProCurve)	RADIUS	ISE 提供的 Auth VLAN	支持	支持	支持	支持	支持
	Alcatel 6850	SNMP	动态 URL	支持	支持	支持	支持	支持
	Brocade ICX 6610	RADIUS	ISE 提供的 Auth VLAN	支持	支持	支持	支持	支持
	Juniper EX3300-24p	RADIUS	ISE 提供的 Auth VLAN	支持	支持	支持	支持	支持

对于其他第三方 NAD，您必须在Cisco ISE 中确定设备属性和功能并创建自定义 NAD 配置文件。	支持	支持	需要 CoA 支持	需要 CoA 支持。 如果有线设备不支持 URL 重定向，Cisco ISE 将使用 Auth VLAN。尚未使用 Auth VLAN 测试无线设备。

您必须为没有预定义配置文件的其他第三方网络设备创建自定义NAD配置文件。对于高级流量（例如访客、自带设备和终端安全评估），网络设备必须支持有关 CoA是否支持这些流量取决于 NAD 的功能。请参阅设备的管理指南，了解在Cisco ISE 中创建网络设备配置文件所需的属性的相关信息。

如果从Cisco ISE 版本 2.0 或更低版本升级到Cisco ISE 版本 2.1 或更高版本，则升级后，早期版本中创建的用于与非Cisco NAD 通信的身份验证策略规则和 RADIUS 词典将继续在Cisco ISE 中运行。

> ISE 社区资源
>
> 有关第三方 NAD 配置文件的信息，请参阅 ISE 第三方 NAD 配置文件和配置。

在思科 ISE 中配置第三方网络设备

Cisco ISE 通过使用网络设备配置文件支持第三方 NAD。这些配置文件对Cisco ISE 用于启用流（例如，访客、BYOD、MAB 和安全状态）的功能进行定义。

开始之前

请参阅网络设备配置文件，第 743 页。

步骤 1 在Cisco ISE 中配置第三方网络设备（参阅将网络设备导入思科 ISE，第 738 页。如果要配置访客、BYOD 或终端安全评估工作流程，请确保已定义授权更改(CoA)，并且已将NAD的URL 重定向机制配置为指向相关的Cisco ISE 门户。要配置 URL 重定向，请从门户的登录页面复制Cisco ISE 门户 URL。有关在 ISE 中为 NAD 配置 CoA 类型和 URL 重定向的详细信息，请参阅网络设备，第 721 页。此外，请参阅第三方的设备管理指南以了解有关说明。

步骤 2 确保在 ISE 中可使用设备的适当 NAD 配置文件。要查看现有配置文件，请选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。如果Cisco ISE 中不存在适当的配置文件，请创建自定义配置文件。有关如何创建自定义配置文件的信息，请参阅创建网络设备配置文件，第 745 页。

步骤 3 将 NAD 配置文件分配至您想要配置的 NAD。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。打开您希望为其分配配置文件的设备，从**设备配置文件 (Device Profile)** 下拉列表中，选择正确的配置文件。

步骤 4 当您在配置策略规则时，在第 1 步中应明确地将授权配置文件设置为 NAD 配置文件；或者如果您使用 VLAN 或者 ACL，或者在您的网络中存在不同供应商的不同设备，则设置为“Any”。要设置授权配置文件的NAD配置文件，请选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。打开相关的授权配置文件，从**网络设备配置文件 (Network Device Profile)** 下拉列表中，选择相关的 NAD 配置文件。在对访客流量使用 Auth VLAN 时，象常规的访客流量一样，您还应定义访客门户，

并在绑定至MAB授权的授权配置文件中选择该访客门户。有关访客门户的详细信息，请参阅《》 中的“思科ISE访客服务”部分请参阅思科 ISE 访客服务 ， 第 307 页。

创建网络设备配置文件

开始之前

- 大多数 NAD 都具有供应商特定的 RADIUS 字典，除了提供标准的 IETF RADIUS 属性之外，该字典还提供多个供应商特定属性。如果网络设备有供应商特定的 RADIUS 字典，请将其导入到 Cisco ISE。有关需要哪一个 RADIUS 字典的说明，请参阅第三方设备的管理指南。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **系统 (System)** > **Radius** > **RADIUS 供应商 (RADIUS Vendors)**。要导入 RADIUS 字典，请参阅创建 RADIUS 供应商字典 ， 第 820 页。
- 对于访客和终端安全评估等复杂流，网络设备必须支持 RFC 5176中定义的 CoA 类型。
- 有关创建网络设备配置文件的字段和可能值的信息，请参阅网络设备配置文件设置。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在显示的**新网络设备配置文件 (New Network Device Profile)** 窗口中，在网络设备的**名称 (Name)** 和**说明 (Description)** 字段中输入相应的值。

步骤 4 从**供应商 (Vendor)** 下拉列表中，选择网络设备的供应商。

步骤 5 在**图标 (Icon)** 区域中，点击**更改图标... (Change Icon...)** 按钮，从您的系统上传网络设备的图标。

点击**图标 (Icon)** 区域中的**设置为默认 (Set To Default)** 按钮，使用Cisco ISE 提供的默认图标。

步骤 6 在**支持的协议 (Supported Protocols)** 区域中，选中设备支持的协议所对应的复选框。仅选中要实际使用的协议对应的复选框。如果网络设备支持 RADIUS 协议，请从 **RADIUS 字典 (RADIUS Dictionaries)** 下拉列表中选择要用于设备的 RADIUS 字典。

步骤 7 在**模板 (Templates)** 区域，输入如下相关详细信息：

a) 点击**身份验证/授权 (Authentication/Authorization)** 折叠部分，配置网络设备的默认流类型、属性别名和主机查找设置。在显示的新**流类型条件 (Flow Type Conditions)** 区域中，输入设备用于各种身份验证和授权流（如有线 MAB 和 802.1x）的属性和值。这使Cisco ISE 能够根据它使用的属性为设备检测到正确的流类型。对于MAB没有 IETF 标准，不同的供应商对于 Service-Type 使用不同的值。请参阅设备的用户指南或使用 MAB 身份验证嗅探器跟踪以确定正确的设置。在**属性别名 (Attribute Aliasing)** 区域中，将设备特定的属性名称映射到通用名称以简化策略规则。目前，仅定义服务集标识符 (SSID)。如果网络设备具有无线 SSID 的概念，则将此设置为其使用的属性。在标准化 RADIUS 字典中，Cisco ISE 将它映射至称为 SSID 的属性。您可以在一个规则中引用SSID，并且即使底层属性不同，它也适用于多个设备，因此可简化策略规则配置。在**主机查找 (Host Lookup)** 区域中，选中**处理主机查找 (Process Host Lookup)** 复选框，并根据第三方提供的说明为设备选择相关 MAB 协议和属性。

b) 点击**权限 (Permissions)** 折叠部分，配置网络设备的默认 VLAN 和 ACL 设置。这些设置会根据您在Cisco ISE 中创建的授权配置文件自动映射。
c) 点击**授权更改 (CoA)** 折叠部分以配置网络设备的 CoA 功能。
d) 点击**重定向 (Redirect)** 折叠部分以配置网络设备的 URL 重定向功能。URL 重定向对于访客、BYOD 和终端安全评估服务来说是必需的。

步骤 8 点击**提交 (Submit)**。

相关主题

如何创建 ISE 网络访问设备配置文件

从思科 ISE 导出网络设备配置文件

以 XML 文件的形式导出在Cisco ISE 中配置的单个或多个网络设备配置文件。然后，可以编辑 XML 文件并将其作为新的网络配置文件导入到Cisco ISE 文件中。

开始之前

请参阅如何创建 ISE 网络访问设备配置文件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。
步骤 2 选中您要导出的设备旁边的复选框，然后点击**导出选定对象 (Export Selected)**。
步骤 3 将名为 **DeviceProfiles.xml** 的文件下载到您的本地硬盘。

将网络设备配置文件导入到思科 ISE

可以使用具有Cisco ISE XML 结构的单个 XML 文件将单个或多个网络设备配置文件导入到Cisco ISE。您无法同时导入来自多个导入文件的网络设备配置文件。

通常，您将首先从Cisco ISE 管理员门户导出现有配置文件以用作模板。必要时在文件中输入设备配置文件详细信息，并将其另存为 XML 文件。然后，将编辑后的文件重新导入到Cisco ISE。为了使用多个网络设备配置文件，可将多个构造在一起的配置文件导出为单个 XML 文件，编辑该文件，然后将配置文件一并导入，以便在Cisco ISE 中创建多个配置文件。

在导入网络设备配置文件时，只能创建新记录。您无法覆盖现有的配置文件。要更新现有网络设备配置文件，请从Cisco ISE 导出现有配置文件，从Cisco ISE 删除配置文件，然后在相应编辑后导入配置文件。

开始之前

请参阅如何创建 ISE 网络访问设备配置文件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。

步骤 2 点击**导入**。

步骤 3 点击 **选择文件 (Choose File)**，从正在运行客户端浏览器的系统中选择 XML 文件。

步骤 4 点击**导入**。

管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

网络设备组设置

下表介绍**网络设备组 (Network Device Groups)** 窗口上的字段，您可以使用此窗口创建网络设备组。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **组 (Groups)**。

您还可以在以下位置创建网络设备组：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **所有组 (All Groups)** 窗口。

表 *118*: “网络设备组” *(Network Device Group)* 窗口中的字段

字段名称	使用指南
名称	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。 网络设备组层次结构中最多可以有六个节点，包括根节点。每个网络设备组的名称最多可以包含 32 个字符。
说明	为根网络设备组或子网络设备组输入一段说明。
网络设备数	此列中显示网络组中的网络设备数量。

相关主题

网络设备组，第 748 页
思科 ISE 在策略评估中使用的网络设备属性，第 750 页
在思科 ISE 中添加网络设备，第 203 页

网络设备组导入设置

下表列出了**网络设备组 (Network Device Group)** 窗口上**导入 (Import)** 对话框中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** 。

表 *119:* 网络设备组导入窗口中的字段

字段名称	使用指南
生成模板	点击此链接下载 CSV 模板文件。 以相同格式的网络设备组信息更新模板，并将其保存于本地位置，以将网络设备组导入任何Cisco ISE 部署中。
文件	点击 **选择文件 (Choose File)**，找到您要上传的 CSV 文件的位置。这可能是新创建的文件，也可能是之前从其他Cisco ISE 部署导出的文件。 可以将包含新的和更新后的网络设备组信息的网络设备组从一个Cisco ISE 部署导入另一部署。
用新数据覆盖现有数据	如果想要用您的导入文件中的设备组替换现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。 如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。
遇到第一个错误时停止导入	选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，可在导入期间遇到错误的第一个实例时停止导入。 如果未选中此复选框并且遇到错误，Cisco ISE 将报告错误，并继续导入剩余设备组。

相关主题

网络设备组 ，第 748 页
思科 ISE 在策略评估中使用的网络设备属性 ，第 750 页
将网络设备组导入思科 ISE ，第 750 页

网络设备组

Cisco ISE 支持创建分层网路设备组。使用网络设备组根据不同的条件（例如地理位置、设备类型或其在网络中的相对位置 [例如，“接入层”或“数据中心”等]）对网络设备进行逻辑分组。

要查看网络设备组窗口，请点击**菜单 (Menu)** 图标 (☰) 并选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

例如，要按地理位置组织网络设备，可以按大洲、区域和国家/地区将设备进行分组：

- 非洲 > 南部 > 纳米比亚
- 非洲 > 南部 > 南非
- 非洲 > 南部 > 博茨瓦纳

根据设备类型对网络设备进行分组：

- 非洲 > 南部 > 博茨瓦纳 > 防火墙
- 非洲 > 南部 > 博茨瓦纳 > 路由器
- 非洲 > 南部 > 博茨瓦纳 > 交换机

将网络设备分配给一个或多个分层网络设备组。当Cisco ISE 通过已配置的网络设备组的有序列表确定要分配给特定设备的适当组时，它可能会发现同一设备配置文件适用于多个设备组。在这种情况下，Cisco ISE 将应用匹配的第一个设备组。

对可创建的网络设备组的最大数量没有限制。您可以为网络设备组创建最多六个层级（包括父级组）。

设备组层级以两种视图显示：**树表 (Tree Table)** 和**平面表 (Flat Table)**。点击网络设备组列表上方的 **树表 (Tree Table)** 或**平面表 (Flat Table)**，按所需视图组织列表。

在**树表 (Tree Table)** 视图中，根节点显示在树顶部，下面是按层级顺序排列的子组。点击**全部展开 (Expand All)** 以查看每个根组中的所有设备组。点击**全部折叠 (Collapse All)** 以查看仅含根组的列表。

在**平面表 (Flat Table)** 视图中，**组层次结构 (Group Hierarchy)** 列中显示每个设备组的层次结构。

在两个视图中，分配给每个子组的网络设备的数量显示在相应的**网络设备数量 (No. of Network Devices)** 列中。点击数字可启动一个对话框，其中列出了分配给该设备组的所有网络设备。显示的对话框还包含两个按钮，可将网络设备从一个组移动到另一个组。点击**将设备移动到另一个组 (Move Devices to Another Group)** 按钮，可将网络设备从当前组移动到另一个组。点击**将设备添加到组 (Add Devices to Group)** 按钮，可将网络设备移至所选网络设备组。

要在**网络设备组 (Network Device Groups)** 窗口中添加网络设备组，请点击**添加 (Add)**。在**父级组 (Parent Group)** 下拉列表中，选择网络设备组必须添加到的父级组，或选择**添加为根组 (Add As Root Group)** 选项将新网络设备组添加为父级组。

注释 如果已向设备组分配了任何设备，则无法删除该设备组。在删除设备组之前，您必须将所有现有设备移动到另一个设备组。

根网络设备组

Cisco ISE 包含两个预定义的根网路设备组：**所有设备类型 (All Device Types)** 和**所有位置 (All Locations)**。无法编辑、复制或删除这些预定义的网路设备组，但可以在这些组中添加新设备组。

您可以创建根网络设备组（网络设备组），然后在**网络设备组 (Network Device Groups)** 窗口中的根组下创建子网络设备组，如上一节所述。

思科 ISE 在策略评估中使用的网络设备属性

创建新网络设备组时，新网络设备属性将添加至**系统字典 (System Dictionaries)** 中的**设备 (Device)** 字典（**策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)**）。添加的设备属性随后将在策略定义中使用。

Cisco ISE 允许您使用**设备 (Device)** 字典属性（例如设备类型、位置、型号名称或网络设备上运行的软件版本）配置身份验证和授权策略。

将网络设备组导入思科 ISE

您可以使用逗号分隔值 (CSV) 文件将网络设备组导入到Cisco ISE 节点。您不能同时从两个不同的导入文件导入网络设备组。

从Cisco ISE 管理员门户下载 CSV 模板，在模板中输入网络设备组详细信息，并将模板另存为 CSV 文件，然后将编辑的文件导入到Cisco ISE。

导入设备组时，您可以创建新记录或更新现有记录。导入设备组时，您还可以定义在Cisco ISE 遇到第一个错误时希望Cisco ISE 使用新组覆盖现有设备组还是停止导入过程。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

步骤 2 点击**导入**。

步骤 3 在显示的对话框中，点击**选择文件 (Choose File)**，从正在运行客户端浏览器的系统中选择 CSV 文件。

要下载用于添加网络设备组的 CSV 模板文件，请点击**生成模板 (Generate a Template)**。

步骤 4 要覆盖现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。

步骤 5 选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。

步骤 6 点击**导入**。

从思科 ISE 导出网络设备组

您可以用 CSV 文件的形式导出在Cisco ISE 中配置的网络设备组。然后，您可以将这些网络设备组导入另一个Cisco ISE 节点。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **组 (Groups)**。

步骤 2 要导出网络设备组，可以执行以下操作之一：

- 选中要导出的组旁的复选框，然后选择 **导出 (Export)** > **导出所选 (Export Selected)**。
- 选择 **导出 (Export)** > **全部导出 (Export All)**，导出已定义的所有网络设备组。

步骤 3 一个 CSV 文件会下载到您的本地硬盘。

管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

网络设备组设置

下表介绍**网络设备组 (Network Device Groups)** 窗口上的字段，您可以使用此窗口创建网络设备组。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **组 (Groups)**。

您还可以在以下位置创建网络设备组：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **所有组 (All Groups)** 窗口。

表 *120:* “网络设备组” *(Network Device Group)* 窗口中的字段

字段名称	使用指南
名称	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。 网络设备组层次结构中最多可以有六个节点，包括根节点。每个网络设备组的名称最多可以包含 32 个字符。
说明	为根网络设备组或子网络设备组输入一段说明。
网络设备数	此列中显示网络组中的网络设备数量。

相关主题

网络设备组，第 748 页
思科 ISE 在策略评估中使用的网络设备属性，第 750 页
在思科 ISE 中添加网络设备，第 203 页

网络设备组导入设置

下表列出了**网络设备组 (Network Device Group)** 窗口上**导入 (Import)** 对话框中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

表 *121:* 网络设备组导入窗口中的字段

字段名称	使用指南
生成模板	点击此链接下载 CSV 模板文件。 以相同格式的网络设备组信息更新模板，并将其保存于本地位置，以将网络设备组导入任何Cisco ISE 部署中。
文件	点击 **选择文件 (Choose File)**，找到您要上传的 CSV 文件的位置。这可能是新创建的文件，也可能是之前从其他Cisco ISE 部署导出的文件。 可以将包含新的和更新后的网络设备组信息的网络设备组从一个Cisco ISE 部署导入另一部署。
用新数据覆盖现有数据	如果想要用您的导入文件中的设备组替换现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。 如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。
遇到第一个错误时停止导入	选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，可在导入期间遇到错误的第一个实例时停止导入。 如果未选中此复选框并且遇到错误，Cisco ISE 将报告错误，并继续导入剩余设备组。

相关主题

网络设备组，第 748 页
思科 ISE 在策略评估中使用的网络设备属性，第 750 页
将网络设备组导入思科 ISE，第 750 页

在思科 ISE 中导入模板

Cisco ISE 可以让您使用 CSV 文件导入大量网络设备和网络设备组。模板包含用于定义字段格式的标题行。不得编辑此信头行。

在网络设备和网络设备组的相关导入流中，可以使用**生成模板 (Generate a Template)** 链接将 CSV 文件下载到本地系统。

网络设备导入模板格式

下表列出了重要网络设备 CSV 模板文件标题中的字段，并进行了说明。

表 *122:* 网络设备的 *CSV* 模板字段和说明

字段	说明
Name:String(32)	（必填）此字段是网络设备名称。这是一个最大长度为 32 个字符的字母数字字符串。
说明:String(256)	此字段是网络设备的说明。这是一个最大长度为 256 个字符的字符串。
IP Address:Subnets(a.b.c.d/m|...)	（必填）此字段是网络设备的 IP 地址和子网掩码。它可以包含多个使用竖线“|”符号分隔的值。 网络设备（TACACS 和 RADIUS）配置以及外部 RADIUS 服务器配置支持 IPv4 和 IPv6。 输入 IPv4 地址时，可以使用地址范围和子网掩码。
Model Name:String(32)	（必填）此字段是网络设备的型号名称。这是一个最大长度为 32 个字符的字符串。
Software Version:String(32)	（必填）此字段是网络设备的软件版本。这是一个最大长度为 32 个字符的字符串。
Network Device Groups:String(100)	（必填）此字段是现有的网络设备组。如果是子组，必须同时包含由空格分隔的父组和子组。这是一个最大长度为 100 个字符的字符串。例如，位置 *(Location)* > 所有位置 *(All Location)* > 美国 *(US)*
Authentication:Protocol:String(6)	此字段是要使用的身份验证协议。唯一有效的值为“ RADIUS”（不区分大小写）。
Authentication:Shared Secret:String(128)	（如果在身份验证协议字段中输入一个值，则此字段为必填字段）此字段是一个最大长度为 128 个字符的字符串。
EnableKeyWrap:Boolean(true|false)	它仅在网络设备上支持此字段时才启用。有效值为“true”和“false”。

字段	说明
EncryptionKey:String(ascii:16|hexa:32)	（如果启用 KeyWrap，则此字段为必填字段）此字段是用于会话加密的加密密钥。 ASCII 值 - 长度为 16 个字符（字节） 十六进制值 - 长度为 32 个字符（字节）。
AuthenticationKey:String(ascii:20|hexa:40)	（如果启用 KeyWrap，则此字段为必填字段）。此字段表示基于 RADIUS 消息的键控散列消息验证码 (HMAC) 计算。 ASCII 值 - 长度为 20 个字符（字节） 十六进制值 - 长度为 40 个字符（字节）。
InputFormat:String(32)	此字段是加密和身份验证密钥输入格式。接受 ASCII 和十六进制值。
SNMP:Version:Enumeration (|2c|3)	此字段由分析器服务使用。它是 SNMP 协议的版本 1、2c 或 3。
SNMP:RO Community:String(32)	（如果为 SNMP 版本字段输入一个值，则此字段为必填字段）SNMP 只读社区。此字段是一个最大长度为 32 个字符的字符串。
SNMP:RW Community:String(32)	（如果为 SNMP 版本字段输入一个值，则此字段为必填字段）SNMP 读写社区。此字段是一个最大长度为 32 个字符的字符串。
SNMP:Username:String(32)	此字段是一个最大长度为 32 个字符的字符串。
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)	（如果选择 SNMP 版本 3，则此字段为必填字段）此字段接受的值为“Auth”、“No Auth”或“Priv”。
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	（如果已输入“Auth”或“Priv”作为 SNMP 安全级别，则此字段为必填字段）此字段接受的值为“MD5”或“SHA”。
SNMP:Authentication Password:String(32)	（如果已输入 Auth 作为 SNMP 安全级别，则此字段为必填字段）此字段是一个最大长度为 32 个字符的字符串。
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	（如果已输入“Priv”作为 SNMP 安全级别，则此字段为必填字段）此字段接受的值为“DES”、“AES128”、“AES192”、“AES256”或“3DES”。

字段	说明
SNMP:Privacy Password:String(32)	（如果已输入 Auth 作为 SNMP 安全级别，则此字段为必填字段）此字段是一个最大长度为 32 个字符的字符串。
SNMP:Polling Interval:Integer:600-86400 seconds	此字段用于设置 SNMP 轮询间隔。有效值为介于 600 和 86400 之间的整数。
SNMP:Is Link Trap Query:Boolean(true|false)	此字段用于启用或禁用 SNMP 链路陷阱。有效值为“true”或“false”。
SNMP:Is MAC Trap Query:Boolean(true|false)	此字段用于启用或禁用 SNMP MAC 陷阱。有效值为“true”或“false”。
SNMP:Originating Policy Services Node:String(32)	此字段用于指示必须用于轮询 SNMP 数据的Cisco ISE 服务器。它默认情况下是自动的，但可以通过在此字段中分配不同的值来覆盖该设置。
Trustsec:Device Id:String(32)	此字段为Cisco Trustsec 设备 ID，是最大长度为 32 个字符的字符串。
Trustsec:Device Password:String(256)	（如果已输入Cisco Trustsec 设备 ID，则此字段为必填字段）此字段为Cisco Trustsec 设备密码，是最大长度为 256 个字符的字符串。
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	此字段是Cisco Trustsec 环境数据下载间隔。有效值为介于 1 和 24850 之间的整数。
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	此字段用于设置Cisco Trustsec 对等体授权策略下载间隔。有效值为介于 1 和 24850 之间的整数。
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	此字段用于设置Cisco Trustsec 重新身份验证间隔。有效值为介于 1 和 24850 之间的整数。
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	此字段用于设置Cisco TrustSec 安全组 ACL 列表下载间隔。有效值为介于 1 和 24850 之间的整数。
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	此字段用于指示Cisco TrustSec 设备是否受信任。有效值为“true”或“false”。
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	此字段用于向Cisco Trustsec 设备通知Cisco Trustsec 配置更改。有效值为 **ENABLE_ALL** 或 **DISABLE_ALL**。
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	此字段指示Cisco TrustSec 设备是否包含在安全组标签中。有效值为“true”或“false”。

字段	说明
Deployment:Execution Mode Username:String(32)	此字段是有权编辑设备配置的用户名。这是一个最大长度为 32 个字符的字符串。
Deployment:Execution Mode Password:String(32)	此字段为设备密码，是最大长度为 32 个字符的字符串。
Deployment:Enable Mode Password:String(32)	此字段是设备的密码，可以让您编辑设备的配置。这是一个最大长度为 32 个字符的字符串。
Trustsec:PAC issue date:Date	此字段是Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发日期。
Trustsec:PAC expiration date:Date	此字段是Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的到期日期。
Trustsec:PAC issued by:String	此字段是Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发者（Cisco TrustSec 管理员）名称。它是一个字符串值。

网络设备组导入模板格式

下表列出模板标题中的字段并提供网络设备组 CSV 文件中的字段描述。

表 *123:* 网络设备组的 *CSV* 模板字段和描述

字段	说明
Name:String(100):	（必填）此字段为网络设备组的名称。它是长度最大为 100 个字符的字符串。NDG 全名的长度最大为 100 个字符。例如，如果您要在父组 Global > Asia 下创建子组 India，则您创建的 NDG 的全名为 Global#Asia#India，并且该全名的长度不得超过 100 个字符。如果 NDG 的全名超过 100 个字符，则 NDG 将无法创建。
说明:String(1024)	这是可选的网络设备组说明。它是长度不超过 1024 个字符的字符串。
Type:String(64):	（必填）此字段为网络设备组的类型。它是长度最大为 64 个字符的字符串。
Is Root:Boolean(true|false):	（必填）此字段用于确定特定的网络设备组是否为根组。有效值为 true 或 false。

IPsec 安全保护思科 ISE 与 NAD 间的通信

IPsec 是为 IP 提供安全保护的一组协议。AAA、RADIUS 和 TACACS + 协议使用 MD5 散列算法。为了提高安全性，Cisco ISE 提供 IPsec 功能。IPsec 通过对发送方进行身份验证，发现数据在传输过程中的任何变化以及对发送的数据进行加密来保证安全通信。

Cisco ISE 在隧道及传输模式下支持 IPSec。当在Cisco ISE 接口上启用 IPsec 并配置对等体时，会在 Cisco ISE 和 NAD 之间创建 IPsec 隧道以保护通信。

可以定义预共享密钥或使用 X.509 证书进行 IPsec 身份验证。可以在千兆以太网 1 到千兆以太网 5 接口上启用 IPsec。每个 PSN 仅可以在一个Cisco ISE 接口上配置 IPSec。

由于智能许可证默认处于启用状态 (e0/2—> eth2)，因此无法在千兆以太网2上启用IPsec。但是，如果需要启用 IP 安全，需要为智能许可选择其他接口。

注释 千兆以太网 0 和绑定 0（当千兆以太网 0 和千兆以太网 1 接口绑定时）是Cisco ISE CLI 中的管理接口。千兆以太网 0 和绑定 0 不支持 IPsec。

所需组件包括：

- Cisco ISE 2.2 和更高版本。
- Cisco IOS 软件、C5921 ESR 软件 (C5921_I86-UNIVERSALK9-M)：默认情况下，ESR 5921 配置在隧道及传输模式下支持 IPsec。支持 Diffie-Hellman 组 15 和组 16。

注释 C5921 ESR 软件与 Cisco ISE 2.2 及更高版本捆绑在一起。您需要 ESR 许可证才能将其启用。请参阅《Cisco 5921 嵌入式服务路由器集成指南》，了解 ESR 许可信息。

在思科 ISE 上配置 RADIUS IPSec

要在Cisco ISE 上配置 RADIUS IPsec，您必须：

步骤 1 从Cisco ISE CLI 配置接口上的 IP 地址。

千兆以太网 1 至千兆以太网 5 接口（绑定 1 和绑定 2）支持 IPsec。但是，只能在Cisco ISE 节点的一个接口上配置 IPSec。

步骤 2 将直连网络设备添加到 IPsec 网络设备组。

注释 RADIUS IPsec 需要通过设备的接口直接连接静态路由网关。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。
b) 在**网络设备 (Network Devices)** 窗口中，点击**添加 (Add)**。
c) 在相应字段中输入要添加的网络设备的名称、IP 地址和子网。
d) 从 IPSEC 下拉列表中，选择**是 (Yes)**。
e) 选中 **RADIUS Authentication Settings** 复选框。
f) 在**共享密钥 (Shared Secret)** 字段中，输入您在网络设备上配置的共享密钥。
g) 点击**保存 (Save)**。

步骤 3 添加单独的管理界面，以与Cisco Smart Software Manager (CSSM) 交互。有关嵌入式服务路由器 (ESR) 的信息，请参阅 Smart Software Manager satellite。要执行此操作，请从Cisco ISE CLI 运行以下命令以选择相应的管理接口（千兆以太网 1 至 5 或绑定 1 或 2）：

ise/admin# **license esr smart** {*interface*}

此接口必须能够连通 Cisco.com 才能访问Cisco在线许可服务器。

步骤 4 从Cisco ISE CLI 将网络设备添加到直连网关。

ip route [*destination network*] [*network mask*] **gateway** [*next-hop address*]

步骤 5 在Cisco ISE 节点上激活 IPsec。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **IPSec**。

此窗口中列出了部署中的所有Cisco ISE 节点。

b) 选中要激活 IPsec 的Cisco ISE 节点旁边的复选框，然后点击**启用 (Enable)** 单选按钮。
c) 从**所选节点的 IPSec 接口：(IPSec Interface for selected nodes:)** 下拉列表中选择要用于 IPsec 通信的接口。
d) 点击所选Cisco ISE 节点的以下身份验证类型之一的单选按钮：

- **预共享密钥 (Pre-shared Key)**：如果选择此选项，必须输入预共享密钥并在网络设备上配置相同的密钥。预共享密钥需使用字母数字字符。不支持特殊字符。有关如何在网络设备上配置预共享密钥的说明，请参阅网络设备文档。有关预共享密钥配置输出的示例，请参阅示例：思科 Catalyst 3850 系列交换机上预共享密钥配置的输出 ，第 762 页。
- **X.509 证书 (X.509 Certificates)**：如果您选择此选项，请从Cisco ISE CLI 转到 ESR shell 并为 ESR 5921 配置和安装 X.509 证书。然后，为 IPsec 配置网络设备。有关说明，请参阅在 ESR-5921 上配置和安装 X.509 证书 ，第 760 页。

e) 点击**保存 (Save)**。

注释 不能直接修改 IPsec 配置。要在启用 IPsec 时修改 IPsec 隧道或身份验证，请禁用当前 IPsec 隧道，修改 IPsec 配置，然后重新启用不同配置的 IPsec 隧道。

注释 启用后，IPsec 将从Cisco ISE 接口删除 IP 地址并关闭该接口。当用户从Cisco ISE CLI 登录时，接口显示为无 IP 地址且处于关闭状态。此 IP 地址将在 ESR-5921 接口上配置。

步骤 6 键入 **esr** 进入 ESR shell。

```
ise/admin# esr % Entering ESR 5921 shell % Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M),
 Version 15.5(2)T2, RELEASE SOFTWARE (fc3) % Technical Support: http://www.cisco.com/techsupport %
Copyright (c) 1986-2015 Cisco Systems, Inc. Press RETURN to get started, CTRL-C to exit ise-esr5921>
ise-esr5921>
```

注释 对于 FIPS 合规性，必须配置长度至少为八个字符的加密密码。输入 **Enable secret level 1** 命令以指定密码：

```
ise-esr5921(config)#enable secret level 1 ? 0 Specifies an UNENCRYPTED password will follow 5
Specifies a MD5 HASHED secret will follow 8 Specifies a PBKDF2 HASHED secret will follow 9
Specifies a SCRYPT HASHED secret will follow LINE The UNENCRYPTED (cleartext) 'enable' secret
```

注释 如果从 GUI 配置自定义 RADIUS 端口（除 1645、1646、1812 和 1813 之外），您必须在 ESR shell 中输入以下 CLI 命令以接受配置的 RADIUS 端口：

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

步骤 7 验证 IPsec 隧道和经由 IPsec 隧道的 RADIUS 身份验证。

a) 在Cisco ISE 中添加用户并将用户分配到用户组（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰) 并选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**）。

b) 执行以下步骤，验证是否已在Cisco ISE 和 NAD 之间建立 IPsec 隧道：

1. 使用 **ping** 命令测试Cisco ISE 和 NAD 之间的连接是否已建立。
2. 从 ESR shell 或 NAD CLI 运行以下命令，验证连接是否处于活动状态：

   show crypto isakmp sa

   ```
   ise-esr5921#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id status 192.168.30.1
    192.168.30.3 QM_IDLE 1001 ACTIVE
   ```

3. 从 ESR shell 或 NAD CLI 运行以下命令，验证隧道是否已建立：

   show crypto ipsec sa

   ```
   ise-esr5921#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: radius, local addr
   192.168.30.1 protected vrf: (none) local ident (addr/mask/prot/port):
   (192.168.30.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port):
   (192.168.30.2/255.255.255.255/0/0) current_peer 192.168.30.2 port 500 PERMIT, flags={} #pkts
   encaps: 52, #pkts encrypt: 52, #pkts digest: 52 #pkts decaps: 57, #pkts decrypt: 57, #pkts verify:
    57 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto
    endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2 plaintext mtu 1438, path mtu 1500, ip
   mtu 1500, ip mtu idb Ethernet0/0 current outbound spi: 0x393783B6(959939510) PFS (Y/N): N, DH
   group: none inbound esp sas: spi: 0x8EA0F6EE(2392913646) transform: esp-aes esp-sha256-hmac , in
    use settings ={Tunnel, } conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
    sa timing: remaining key lifetime (k/sec): (4237963/2229) IV size: 16 bytes replay detection
   support: Y Status: ACTIVE(ACTIVE) inbound ah sas: inbound pcp sas: outbound esp sas: spi:
   0x393783B6(959939510) transform: esp-aes esp-sha256-hmac , in use settings ={Tunnel, } conn id:
   100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius sa timing: remaining key lifetime
    (k/sec): (4237970/2229) IV size: 16 bytes replay detection support: Y Status: ACTIVE(ACTIVE)
   outbound ah sas: outbound pcp sas:
   ```

c) 使用以下方法之一验证 RADIUS 身份验证：

- 使用您在步骤 8 (a) 中创建的用户的凭证登录网络设备。RADIUS 身份验证请求将发送到Cisco ISE 节点。在**实时身份验证 (Live Authentications)** 窗口中查看详细信息。

- 将终端主机连接到网络设备并配置 802.1X 身份验证。使用您在步骤 8 (a) 中创建的用户的凭证登录终端主机。RADIUS 身份验证请求将发送到Cisco ISE 节点。在**实时身份验证 (Live Authentications)** 窗口中查看详细信息。

在 ESR-5921 上配置和安装 X.509 证书

步骤 1 键入 **esr** 进入 ESR shell。

```
ise/admin# esr % Entering ESR 5921 shell % Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M),
 Version 15.5(2)T2, RELEASE SOFTWARE (fc3) % Technical Support: http://www.cisco.com/techsupport %
Copyright (c) 1986-2015 Cisco Systems, Inc. Press RETURN to get started, CTRL-C to exit ise-esr5921>
ise-esr5921>
```

注释　对于 FIPS 合规性，必须配置长度至少为八个字符的加密密码。输入 **Enable secret level 1** 命令以指定密码：

```
ise-esr5921(config)#enable secret level 1 ? 0 Specifies an UNENCRYPTED password will follow 5
Specifies a MD5 HASHED secret will follow 8 Specifies a PBKDF2 HASHED secret will follow 9
Specifies a SCRYPT HASHED secret will follow LINE The UNENCRYPTED (cleartext) 'enable' secret
```

注释　如果从 GUI 配置自定义 RADIUS 端口（除 1645、1646、1812 和 1813 之外），必须在 ESR shell 中输入以下 CLI 命令以接受配置的 RADIUS 端口：

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

步骤 2 使用以下命令生成 RSA 密钥对：

示例：

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

步骤 3 使用以下命令创建信任点：

示例：

```
crypto pki trustpoint trustpoint-name enrollment terminal serial-number none fqdn none ip-address none
subject-name cn=networkdevicename.cisco.com revocation-check none rsakeypair rsa2048
```

步骤 4 使用以下命令生成证书签名请求：

示例：

```
crypto pki enroll rsaca-mytrustpoint Display Certificate Request to terminal? [yes/no]: yes
```

步骤 5 将证书签名请求的输出复制到文本文件，将其提交到外部 CA 进行签名，然后获取签名证书和 CA 证书。

步骤 6 使用以下命令导入证书颁发机构 (CA) 证书：

示例：

```
crypto pki authenticate rsaca-mytrustpoint
```

复制并粘贴 CA 证书的内容，包括“—**BEGIN**—”和“—**-End**—”行。

步骤 7 使用以下命令导入签名证书：

示例：

```
crypto pki import rsaca-mytrustpoint
```

复制并粘贴签名证书的内容，包括“—**BEGIN**—”和“—**-End**—”行。

以下是在Cisco 5921 ESR 上配置和安装 X.509 证书时显示的输出示例：

```
ise-esr5921#show running-config ! hostname ise-esr5921 ! boot-start-marker boot host unix:default-config
 boot-end-marker ! no aaa new-model bsd-client server url https://cloudsso.cisco.com/as/token.oauth2 mmi
 polling-interval 60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180 call-home ! 如果 call-home 中
的联系电子邮件地址配置为 sch-smart-licensing@cisco.com ! 将使用Cisco智能许可证门户中配置的电子邮件地址作为发送 SCH
通知的联系电子邮件地址。contact-email-addr sch-smart-licensing@cisco.com profile "CiscoTAC-1" active
destination transport-method http no destination transport-method email ! ip cef no ipv6 cef ! multilink
 bundle-name authenticated ! crypto pki trustpoint SLA-TrustPoint enrollment pkcs12 revocation-check crl
 ! crypto pki trustpoint rsaca-mytrustpoint enrollment terminal serial-number none fqdn none ip-address
 none subject-name cn=ise-5921.cisco.com revocation-check none rsakeypair rsa2048 ! crypto pki certificate
 chain SLA-TrustPoint certificate ca 01 30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101
0B050030 32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73
696E6720 526F6F74 20434130 1E170D31 33303533 30313934 3834375A 170D3338 30353330 31393438 34375A30
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A6BCBD96
131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A
9CAE6388 8A38E520 1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE 4AA4E80D
DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC 7390A3EB 2B5436AD C847A2C5 DAB553EB
69A9A535 58E9F3E3 C0BD23CF 58BD7188 68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B
42C68BB7 C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191 C55F0D76 61F9A4CD
3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44 DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06
03551D0F 0101FF04 04030201 06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500 03820101 00507F24 D3932A66
86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905 604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB
9093D3B1 6C9E3D8B D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8 467A3DF4
4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C 7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB
E973DE7F 5BDDEB86 C71E3B49 1765308B 5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69
39F08678 80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB 418616A9 4093E049
4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0 D697DF7F 28 quit crypto pki certificate chain
rsaca-mytrustpoint certificate 39 30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
 61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06 03550407 0C035254 50310E30
0C060355 040A0C05 43495343 4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
65726368 616F2E63 6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734 335A301D
311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F 6D308201 22300D06 092A8648 86F70D01
01010500 0382010F 00308201 0A028201 0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536
BF1EBBD3 73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617 194AF1B0 7F04B4EA
B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F 8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A
C2BB3174 361B13FA 2CB7BDFE 22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0 F9A21FFB 3C3C507A 20B924F7
E0125D60 6552321C 35736079 42449401 15E68DA6 B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69
A46173B6 96CC84FB 5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801 86F84201
0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469 66696361 7465301D 0603551D 0E041604
146DD31C 03690B98 330B67FA 6EDC7B20 F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690
423599CC EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D 01010B05 00038201
0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965 1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36
236F528E E30C921C 81DA29E1 EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1 2CFDDBE3 EA9D407C 8D1B0F49
BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27 69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC
7BDCC1BB 61F69B31 BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D CD2E1A95
7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585 89AE82F6 A37E51D6 EECD quit certificate
ca 008DD3A81106B14664 308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886 F70D0101
05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06 03550407 0C035254
50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273
6163612E 65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531 30313832 31313534
335A3061 310B3009 06035504 06130255 53310B30 09060355 04080C02 4E43310C 300A0603 5504070C 03525450
310E300C 06035504 0A0C0543 4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
```

```
0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190 16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085
6FAC5425 14AFE225 0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11 B4C32D38
AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B D985703D F3BB9ED1 7DE99614 422D765C
86AB25CD E80008C5 22049BE8 66D1CA27 E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929
D22E2C42 B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B DFBE6EA7 56EBE30B
D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A A196DA5A 1B525175 C26B3581 EA4B0203 010001A3
5D305B30 1D060355 1D0E0416 0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405 30030101 FF300B06 03551D0F
04040302 02A4300D 06092A86 4886F70D 01010505 00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3
05B7D05F 926CC863 220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354 86C6D9DF
D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D 43B80E44 AE69C164 2C9F41A2 8284F577
21FFAB8E A6771A5E DD34EBE4 A0DC2EAD 95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1
DEE50B07 12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3 60E2ED42 7F10D1A6
F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5 3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B
437D82DD D74A4A9F 3557B3D9 D0BD055F 65A8 quit license udi pid CISCO5921-K9 sn 9XG4481W768 username lab
password 0 lab ! redundancy ! crypto keyring MVPN-spokes rsa-pubkey address 0.0.0.0 address 0.0.0.0
key-string quit ! crypto isakmp policy 10 encr aes hash sha256 group 16 ! crypto isakmp policy 20 encr
aes hash sha256 group 14 crypto isakmp profile MVPN-profile description LAN-to-LAN for spoke router(s)
connection keyring MVPN-spokes match identity address 0.0.0.0 ! crypto ipsec transform-set radius esp-aes
 esp-sha256-hmac mode tunnel crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac mode transport
 ! crypto dynamic-map MVPN-dynmap 10 set transform-set radius radius-2 ! crypto map radius 10 ipsec-isakmp
 dynamic MVPN-dynmap ! interface Ethernet0/0 description e0/0->connection to external NAD ip address
192.168.20.1 255.255.255.0 ip nat outside ip virtual-reassembly in no ip route-cache crypto map radius
! interface Ethernet0/1 description e0/1->tap0 internal connection to ISE ip address 10.1.1.1
255.255.255.252 ip nat inside ip virtual-reassembly in no ip route-cache ! interface Ethernet0/2 no ip
address shutdown ! interface Ethernet0/3 no ip address shutdown ! ip forward-protocol nd ! no ip http
server no ip http secure-server ip nat inside source list 1 interface Ethernet0/0 overload ip nat inside
 source static udp 10.1.1.2 1645 interface Ethernet0/0 1645 ip nat inside source static udp 10.1.1.2
1646 interface Ethernet0/0 1646 ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
 ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813 ! access-list 1 permit 10.1.1.0
 0.0.0.3 ! control-plane ! line con 0 logging synchronous line aux 0 line vty 0 4 login transport input
 none ! end
```

以下是在Cisco Catalyst 3850 系列交换机上配置和安装 X.509 证书时显示的输出示例：

```
cat3850#show running-config enable password lab ! username lab password 0 lab aaa new-model ! aaa group
 server radius ise server name ise-vm deadtime 60 ! aaa authentication login default group radius local
 aaa authentication enable default group radius enable ! crypto isakmp policy 10 encr aes hash sha256
authentication rsa-sig group 16 ! crypto ipsec security-association lifetime seconds 86400 ! crypto ipsec
 transform-set radius esp-aes esp-sha256-hmac mode tunnel ! crypto ipsec profile radius-profile ! crypto
 map radius 10 ipsec-isakmp set peer 192.168.20.1 set transform-set radius match address 100 ! interface
 GigabitEthernet1/0/1 no switchport ip address 192.168.20.2 255.255.255.0 crypto map radius ! access-list
 100 permit ip host 192.168.20.2 host 192.168.20.1 ! snmp-server community public RO snmp-server community
 private RW ! radius server rad-ise address ipv4 192.168.20.1 auth-port 1645 acct-port 1646 key secret
```

示例：思科 Catalyst 3850 系列交换机上预共享密钥配置的输出

以下是在Cisco Catalyst 3850 系列交换机上配置预共享密钥时显示的输出示例：

```
cat3850#show running-config enable password lab ! username lab password 0 lab aaa new-model
 ! aaa group server radius ise server name ise-vm deadtime 60 ! aaa authentication login
default group radius local aaa authentication enable default group radius enable ! crypto
isakmp policy 10 encr aes hash sha256 authentication pre-share group 16 crypto isakmp key
123456789 address 0.0.0.0 ! crypto ipsec security-association lifetime seconds 86400 !
crypto ipsec transform-set radius esp-aes esp-sha256-hmac mode tunnel ! crypto ipsec profile
 radius-profile ! crypto map radius 10 ipsec-isakmp set peer 192.168.20.1 set transform-set
 radius match address 100 ! interface GigabitEthernet1/0/1 no switchport ip address
192.168.20.2 255.255.255.0 crypto map radius ! access-list 100 permit ip host 192.168.20.2
```

```
 host 192.168.20.1 ! snmp-server community public RO snmp-server community private RW !
radius server rad-ise address ipv4 192.168.20.1 auth-port 1645 acct-port 1646 key secret
```

移动设备管理器与思科 ISE 的互操作性

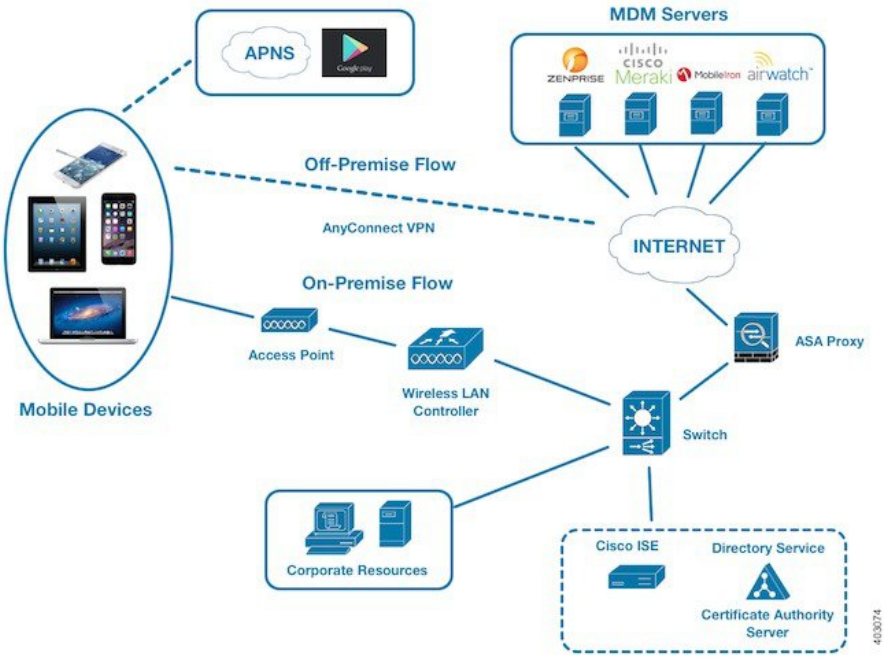
移动设备管理(MDM)服务器保护、监控、管理和支持跨移动运营商、服务提供商和企业部署的移动设备。MDM服务器作为策略服务器运行，用于控制移动设备上的某些应用（例如，电子邮件应用）在部署环境中的使用。但是，网络是基于访问控制列表(ACL)提供精细终端访问的唯一实体。Cisco ISE 会在 MDM 服务器上查询所需的设备属性，以创建为这些设备提供网络访问控制的 ACL。

您可以在网络上运行多个活动 MDM 服务器，包括来自不同供应商的 MDM 服务器。这样，您就可以根据位置或设备类型等设备因素，将不同的终端路由到不同的 MDM 服务器。

Cisco ISE 还使用Cisco MDM 服务器信息 API 版本 2 与 MDM 服务器集成，以便允许设备通过Cisco AnyConnect 4.1 和Cisco自适应安全设备 9.3.2 或更高版本，利用 VPN 访问网络。

在此示例图中，Cisco ISE 是执行点，而 MDM 策略服务器是策略信息点。Cisco ISE 从 MDM 服务器获取数据，以提供完整的解决方案。

图 *34: MDM* 与思科 *ISE* 的互通性



您可以配置Cisco ISE，使其与一个或多个外部移动设备管理器(MDM)服务器进行互操作。通过设置此类第三方连接，您可以使用 MDM 数据库中的详细信息。Cisco ISE 使用 REST API 调用，从外部 MDM 服务器检索信息。Cisco ISE 将相应的访问控制策略应用到交换机、接入路由器、无线接入点和其他网络接入点。策略可以让您能够更好地控制访问支持Cisco ISE 的网络的远程设备。

有关Cisco ISE 支持的 MDM 供应商的列表，请参阅支持的移动设备管理服务器，第 765 页。

支持的移动设备管理使用情形

Cisco ISE 与外部 MDM 服务器联合执行以下功能：

- 管理设备注册：访问网络的未注册终端会重定向到 MDM 服务器上托管的注册页面。设备注册包括用户角色、设备类型等。
- 处理设备补救 ：在补救期间向终端授予有限访问权限。
- 增强终端数据：使用来自 MDM 服务器的信息更新终端数据库，这些信息是无法使用Cisco ISE 分析服务收集的。Cisco ISE 使用可在**终端 (Endpoints)** 窗口中查看的六个设备属性。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

  以下是可用设备属性的示例。

  - MDMImei: 99 000100 160803 3
  - MDMManufacturer: Apple
  - MDMModel: iPhone
  - MDMOSVersion: iOS 6.0.0
  - MDMPhoneNumber: 9783148806
  - MDMSerialNumber: DNPGQZGUDTF9

- 每 4 小时轮询一次 MDM 服务器，获取设备合规性数据。在**外部 MDM 服务器 (External MDM Servers)** 窗口中配置轮询间隔。（要查看此窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **网络资源 (Network Resources)** > **外部 MDM 服务器 (External MDM Servers)**。
- 通过 MDM 服务器发出设备指示：Cisco ISE 通过 MDM 服务器发出针对用户设备的远程操作。通过**终端 (Endpionts)** 窗口从Cisco ISE 管理门户发起远程操作。要查看此窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**。选中 MDM 服务器旁的复选框，然后点击**MDM 操作 (MDM Actions)**。从显示的下拉列表中选择所需的操作。

供应商 MDM 属性

在Cisco ISE 中配置 MDM 服务器时，供应商的属性会添加到Cisco ISE 系统字典中名为 **mdm** 的新条目。以下属性用于注册状态，通常受 MDM 供应商支持。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus

- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- 无法
- MDMServerName
- MDMServerReachable
- MEID
- Model
- UDID

如果不支持供应商的唯一属性，可以使用 ERS API 来交换供应商特定属性。请查阅供应商的文档，了解有关支持的 ERS API 的信息。

新 MDM 字典属性可以在授权策略中使用。

支持的移动设备管理服务器

支持的 MDM 服务器包括来自以下供应商的产品：

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki 系统管理器
- Citrix Endpoint Management（之前称为 Xenmobile）
- Globo
- IBM MaaS360
- JAMF Casper Suite
- Microsoft Intune（用于移动设备）
- Microsoft SCCM（用于桌面设备）
- MobileIron UEM

注释 某些版本的 MobileIron 不适用于Cisco ISE。MobileIron 已了解此问题，并已修复。请联系 MobileIron 了解更多信息。

- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE（之前称为 AirWatch）
- 42 Gears

ISE 社区资源

何操作方法：Meraki EMM/MDM 与 ISE 集成

移动设备管理服务器使用的端口

下表列出Cisco ISE 和 MDM 服务器之间要相互通信必须打开的端口。有关必须在 MDM 代理和服务器上打开的端口的列表，请参阅 MDM 供应商的文档。

表 *124: MDM* 服务器使用的端口

MDM 服务器	端口
MobileIron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 和 443
Microsoft SCCM	80 和 443

移动设备管理集成流程

1. 用户将设备与 SSID 关联。
2. ISE 向 MDM 服务器发出 API 调用。
3. 此 API 调用会返回用户的设备列表和这些设备的终端安全评估状态。

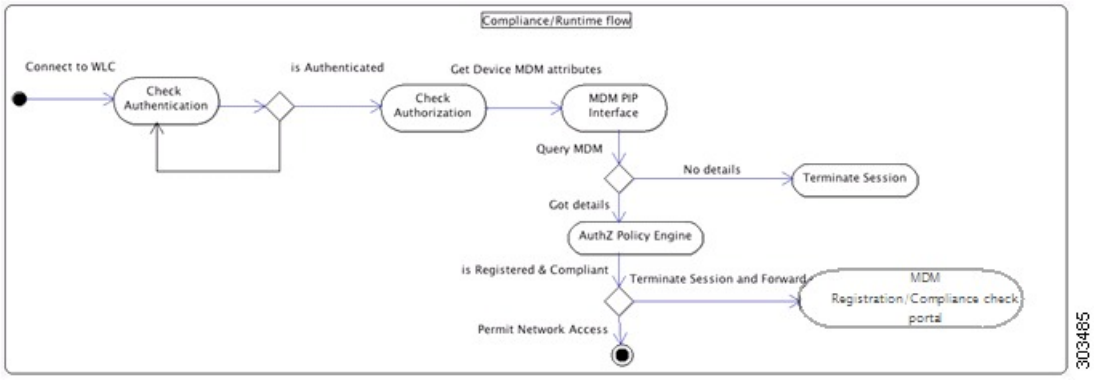
   注释 输入参数是终端设备的 MAC 地址。对于异地 Apple iOS 设备（通过 VPN 连接到思科 ISE 的任何设备），输入参数为 UDID。

4. 如果用户的设备不在此列表中，意味着该设备未注册。Cisco ISE 向 NAD 发送授权请求以重定向至Cisco ISE。系统会向用户显示 MDM 服务器页面。

   注释 对于在Cisco ISE 网络之外注册到 MDM 服务器上的设备，必须通过 MDM 门户对其进行注册。这适用于Cisco ISE 1.4 及更高版本。在之前的Cisco ISE 版本中，如果在启用Cisco ISE 的网络外部注册的设备符合终端安全评估策略，将自动对其进行注册。

5. Cisco ISE 使用 MDM 调配设备并向用户显示相应的页面供其注册设备。
6. 用户在 MDM 服务器中注册设备，然后 MDM 服务器通过自动重定向或手动刷新浏览器将此请求重定向至Cisco ISE。
7. Cisco ISE 重新查询 MDM 服务器获取安全评估状态。
8. 如果用户的设备不符合 MDM 服务器上配置的终端安全评估（合规性）策略，系统会向用户告知设备不合规。用户必须采取必要的措施来确保设备合规。
9. 用户设备合规后，MDM 服务器会在其内部表中更新设备状态。
10. 如果用户现在刷新浏览器，Cisco ISE 将恢复控制。
11. Cisco ISE 每四小时轮询 MDM 服务器一次，以获取合规性信息并发出适当的授权更改 (CoA)。您可以配置轮询间隔。Cisco ISE 还会每五分钟检查一次 MDM 服务器以确保其可用。

下图说明 MDM 流程。



注释 一个设备一次只能向一台 MDM 服务器注册。如果您要向其他供应商的 MDM 设备注册同一设备，用户必须删除设备上的前供应商的配置文件。MDM 服务通常提供“公司擦除”功能，仅删除设备的供应商配置（而不是整个设备）。用户还可以删除文件。例如，在iOS设备上，用户可以转到“设置”(Settings) > “常规”(General) > “设备管理”(Device management) 窗口，然后点击**移除管理 (Remove Management)**。或者，用户可以转到Cisco ISE 中的我的设备门户，然后点击**公司擦除 (Corporate Wipe)**。

使用思科 ISE 设置移动设备管理服务器

要使用Cisco ISE 设置 MDM 服务器，您必须执行以下高级任务：

步骤 1 将 MDM 服务器证书导入Cisco ISE，但 Intune 除外，后者需将策略管理节点 (PAN) 的证书导入 Azure。

步骤 2 创建移动设备管理器定义。

步骤 3 在无线 LAN 控制器上配置 ACL。

步骤 4 配置将非注册设备重定向到 MDM 服务器的授权配置文件。

步骤 5 如果网络上有多个 MDM 服务器，请为每个供应商配置单独的授权配置文件。

步骤 6 为 MDM 使用案例配置授权策略规则。

将移动设备管理服务器证书导入思科 ISE

要使Cisco ISE 连接 MDM 服务器，您必须将 MDM 服务器证书导入Cisco ISE 受信任证书库。如果您的 MDM 服务器有一个 CA 签名的证书，您必须将根证书导入Cisco ISE 受信任证书库。

注释 对于 Microsoft Azure，请将Cisco ISE 证书导入 Azure。请参阅将 Microsoft Intune 配置为移动设备管理服务器，第 772 页。

步骤 1 从您的 MDM 服务器导出 MDM 服务器证书并将其保存至您的本地计算机上。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificate)** > **导入 (Import)**。

步骤 3 在**将新证书导入证书库 (Import a new Certificate into the Certificate Store)** 窗口中，点击**选择文件 (Choose File)**，选择从 MDM 服务器获取的 MDM 服务器证书。

步骤 4 在**友好名称 (Friendly Name)** 字段中，输入证书名称。

步骤 5 选中**信任 ISE 中的身份验证 (Trust for authentication within ISE)** 复选框。

步骤 6 点击**提交 (Submit)**。

步骤 7 确认**信任证书 (Trust Certificates)** 窗口列出新添加的 MDM 服务器证书。

下一步做什么

在 ISE 中定义移动设备管理服务器，第 769 页

。

在 ISE 中定义移动设备管理服务器

您可以为外部 MDM 服务器创建一个或多个 MDM 和桌面设备管理器 (SCCM) 定义。

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)**。
2. 点击**添加 (Add)**。
3. 在相应的字段中输入要添加的 MDM 服务器的名称和说明。
4. 从**服务器类型 (Server Type)** 下拉列表中，选择**移动设备管理器 (Mobile Device Manager)** 或**桌面设备管理器 (Desktop Device Manager)**。您在此做出的选择决定了您在下一步能够看到的字段。要配置桌面设备管理器服务器，请参阅桌面设备管理 (Desktop Device Management)，第 771 页。要配置移动设备管理器服务器，请继续执行此步骤列表。
5. 从**身份验证类型 (Authentication Type)** 下拉列表中，选择**基础 (Basic)** 或 **OAuth-客户端凭证 (OAuth - Client Credentials)**。要为 Microsoft Intune 服务器配置 **OAuth-客户端凭证 (OAuth - Client Credentials)**，请参阅移动设备管理（采用 OAuth-客户端凭证身份验证类型），第 770 页。要配置**基础 (Basic)** 身份验证类型，请继续执行此步骤列表。
6. 所有界面都要求名称并描述此MDM服务器定义。下节基于服务器和身份验证类型介绍其他字段和步骤。

移动设备管理（采用基本身份验证类型）

- **主机名/IP 地址 (Host Name/IP Address)**：输入 MDM 服务器主机名或 IP 地址。
- **端口 (Port)**：输入连接至 MDM 服务器时要使用的端口，通常为 443。

- **实例名称 (Instance Name)**：如果此 MDM 服务器有多个实例，应输入要连接到的实例。
- **轮询间隔 (Polling Interval)**：输入Cisco ISE 轮询 MDM 服务器以获取合规性检查信息的轮询间隔（以分钟为单位）。此值应与MDM服务器上的轮询间隔相同。有效范围为15至1440分钟。默认值为 240 分钟。我们建议仅在网络上测试若干活动客户端时将轮询间隔设置为小于 60 分钟。如果为具有许多活动客户端的生产环境将此值设置为小于60分钟，则系统的负载会显著增加并可能对性能造成不利影响。

  如果将轮询间隔设置为 0，则Cisco ISE 会禁用与 MDM 服务器的通信。
- **合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)**：当终端通过身份验证或重新进行身份验证时，Cisco ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)** 值，则Cisco ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则Cisco ISE 会触发相应的 CoA。

  有效范围为 1 至 1440 分钟。默认值为 1 分钟。

移动设备管理（采用 OAuth-客户端凭证身份验证类型 ）

要使用 OAuth 身份验证类型，请按照将 Microsoft Intune 配置为移动设备管理服务器，第 772 页中所述配置 OAuth 服务器。

- **自动发现 URL (Auto Discovery URL)**：输入 Microsoft Azure 管理门户中的 *Microsoft Azure AD* 图形 *API* 终端 *(Microsoft Azure AD Graph API Endpoint)* 值。此 URL 是应用可使用图形 API 访问 Microsoft Azure AD 中的目录数据的终端。URL 格式为：`https://<hostname>/<tenant id>`

  例如，`https://graph.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329`。

  此 URL 的扩展版本也在属性文件中，格式为：
  `https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>`。
- **客户端 ID (Client ID)**：应用的唯一标识符。如果应用访问其他应用中的数据，如 Microsoft Azure AD Graph API、Microsoft Intune API 等，则需要使用此属性。
- **颁发令牌的 URL (Token Issuing URL)**：输入上一步中的 *Oauth2.0* 授权终端 *(Oauth2.0 Authorization Endpoint)* 值。在该终端上，应用可以使用 OAuth2.0 获得访问令牌。在对应用进行身份验证后，Microsoft Azure AD 会为应用（Cisco ISE）颁发一个访问令牌，允许应用调用图形 API/Intune API。
- **令牌受众 (Token Audience)**：令牌面向的接收资源，通常为指向 Microsoft Intune API 的公共知名 **APP ID URL**。
- **轮询间隔 (Polling Interval)**：输入Cisco ISE 轮询 MDM 服务器以获取合规性检查信息的轮询间隔（以分钟为单位）。此值应与MDM服务器上的轮询间隔相同。有效范围为15至1440分钟。默认值为 240 分钟。我们建议仅在网络上测试若干活动客户端时将轮询间隔设置为小于 60 分钟。如果为具有许多活动客户端的生产环境将此值设置为小于60分钟，则系统的负载会显著增加并可能对性能造成不利影响。

  如果将轮询间隔设置为 0，则Cisco ISE 会禁用与 MDM 服务器的通信。

- **合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)**：当终端通过身份验证或重新进行身份验证时，Cisco ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)** 值，则Cisco ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则Cisco ISE 会触发相应的 CoA。

  有效范围为 1 至 1440 分钟。默认值为 1 分钟。

桌面设备管理 (Desktop Device Management)

以下设置要求您在 SCCM 服务器上配置 WMI，以便它能够与Cisco ISE 通信。请参阅为思科 ISE 配置 Microsoft System Center Configuration Manager Server，第 776 页。

- **主机名/IP 地址 (Host Name/IP Address)**：输入 MDM 服务器主机名或 IP 地址。
- **站点或实例名称 (Site or Instance Name)**：输入站点名称，或者在 MDM 服务器有多个实例的情况下输入实例名称。

针对 Microsoft Intune 和 Microsoft System Center Configuration Manager 的思科 ISE 移动设备管理支持

- **Microsoft Intune**：Cisco ISE 支持 Microsoft Intune 设备管理，将其作为伙伴 MDM 服务器来管理移动设备。

  在管理移动设备的 Microsoft Intune 服务器上配置Cisco ISE 作为 OAuth 2.0 客户端应用。Cisco ISE 从 Azure 获取令牌，以便与Cisco ISE Intune 应用建立会话。

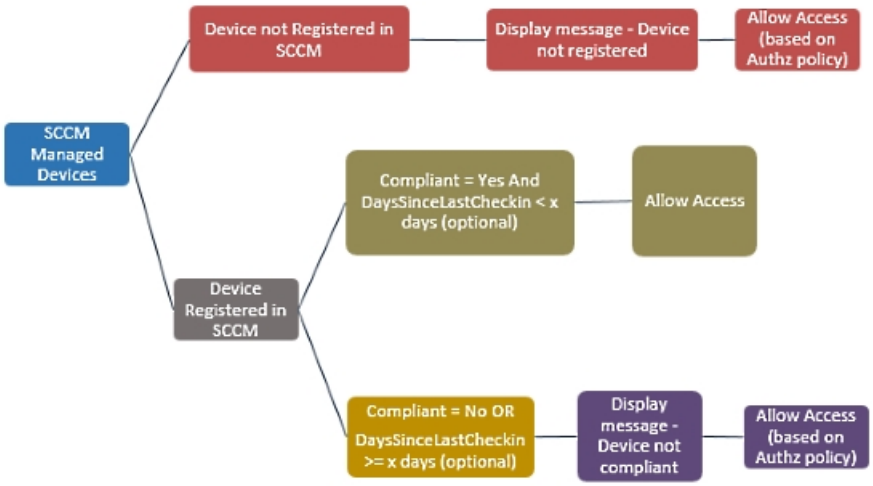
  有关 Microsoft Intune 如何与客户端应用通信的信息，请参阅 https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx。

- **桌面设备管理器 (Microsoft SCCM)**：Cisco ISE 支持 Microsoft System Center Configuration Manager (SCCM)，将其作为伙伴 MDM 服务器来管理 Windows 计算机。Cisco ISE 使用 WMI 从 Microsoft SCCM 服务器检索合规性信息，并使用该信息向用户 Windows 设备授予或拒绝网络访问权限。

Microsoft SCCM 工作流程

Cisco ISE 会从 Microsoft SCCM 服务器检索有关设备是否注册的信息，如果设备已注册，则检索其是否合规的信息。下图显示了 Microsoft SCCM 管理的设备的工作流程。

图 *35: SCCM* 工作流程



当设备连接网络并且与 Microsoft SCCM 策略匹配时，Cisco ISE 会查询在授权策略中指定的 SCCM 服务器，以检索合规性和最后登录（签入）时间。借助这些信息，Cisco ISE 可在**终端 (Endpoint)** 列表中更新设备合规状态和 lastCheckinTimeStamp。

如果设备不合规或未在 Microsoft SCCM 上注册，且授权策略中使用了重定向配置文件，则系统会向用户显示一则消息，说明该设备不合规或未在 Microsoft SCCM 上注册。在用户确认该消息后，Cisco ISE 会向 Microsoft SCCM 注册站点发出 CoA。可根据授权策略和配置文件授予用户访问权限。

Microsoft SCCM 服务器连接监控

您无法为 Microsoft SCCM 配置轮询间隔。

Cisco ISE 运行 MDM 心跳作业以验证与 Microsoft SCCM 服务器的连接，如果Cisco ISE 断开了与 Microsoft SCCM 服务器的连接，则会发出警报。无法配置心跳作业间隔。

将 Microsoft Intune 配置为移动设备管理服务器

配置 Microsoft Intune 作为Cisco ISE 的 MDM 服务器的过程与配置其他 MDM 服务器的过程略有不同。以下步骤可帮助您配置Cisco ISE 和 Microsoft Azure 之间的连接。

1. 从 Microsoft Intune 或 Azure Active Directory 租户获取公共证书，并将其导入Cisco ISE 中以支持 SSL 握手。
    1. 登录到 Microsoft Intune 或 Microsoft Azure 的管理员控制台（如适用）。
    2. 使用浏览器获取证书详细信息。例如，使用 Internet Explorer：
        1. 点击浏览器工具栏中的锁定符号，然后点击**查看证书 (View Certficates)**。
        2. 在**证书 (Certificate)** 窗口中，点击**证书路径 (Certification Path)**。
        3. 找到 **Baltimore Cyber Trust Root**，然后导出此根证书。

3. 登录Cisco ISE。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。点击**添加 (Add)** 并导入您保存的根证书。为证书指定一个有意义的名称，例如“Azure MDM”。

2. 从Cisco ISE 导出自签证书，并准备用于 Microsoft InTune 或 Azure。
   1. 在 PAN 的管理员门户中，在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。在显示的证书列表中，选择**默认自签名服务器证书 (Default Self-Signed Server Certificate)** 复选框，然后点击**导出 (Export)**。
   2. 在显示的新对话框中，点击**仅导出证书 (Export Certificate Only)** 单选按钮，然后点击**导出 (Export)**

      。

   在导出的证书文件上运行以下 PowerShell 脚本：

   ```
   $cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
   $cer.Import(“mycer.cer”) $bin = $cer.GetRawCertData() $base64Value =
   [System.Convert]::ToBase64String($bin) $bin = $cer.GetCertHash() $base64Thumbprint =
   [System.Convert]::ToBase64String($bin) $keyid = [System.Guid]::NewGuid().ToString()
   ```

   记下 **$base64Thumbprint**、**$base64Value** 和 **$keyid** 的值。这些值将在以后使用。

3. 在 Microsoft Intune 中创建一个Cisco ISE 应用。
   1. 在 Microsoft Azure 管理门户 (https://manage.windowsazure.com) 中登录到您的客户域。选择 **目录 (Directory)** > **应用 (Applications)** > **添加应用 (Add an Application)**，然后选择**添加我的组织正在开发的应用 (Add an application my organization is developing)**。
   2. 在 Microsoft Azure 中使用以下参数配置Cisco ISE 应用：
      - **应用名称 (Application Name)**：输入 **`CiscoISE`**。
      - 选择 **WEB 应用和/或 WEB APP (WEB APPLICATION AND/OR WEB APP)**。
      - **登录 URL 和应用 ID URL (SIGN-ON URL and APP ID URL)**：添加任何有效的 URL，Cisco ISE 不使用这些值。

4. 从 Microsoft Azure 获取该清单文件，添加Cisco ISE 证书信息，然后将更新后的清单上传至 Microsoft Azure。
   1. 在Microsoft Azure管理门户中，打开AAD管理单元，然后导航至创建的“CiscoISE”应用。

   从**管理清单 (Manage Manifest)** 菜单下载应用清单文件。

5. 更新清单 JSON 文件中的 **keyCredentials** 字段，如以下示例所示。将 *Base64 Encoded String of ISE PAN cert* 替换为从Cisco ISE 导出且经过编辑的证书文件，即 PowerShell 脚本中的 $base64Value：

   ```
   "keyCredentials": [ { “customKeyIdentifier“: “$base64Thumbprint_from_above”, “keyId“:
    “$keyid_from_above“, "type": "AsymmetricX509Cert", "usage": "Verify", "value": "Base64
    Encoded String of ISE PAN cert" } ]
   ```

注释 请勿更改清单文件的名称。

KeyCredentials 复合类型在以下位置记录：
http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx。

6. 将更新后的清单文件上传至 Microsoft Azure。
7. 在 Microsoft Azure 管理门户，导航至**应用终端 (App Endpoints)** 列表。您将使用以下终端属性的值在Cisco ISE 中配置 MDM：
   - **MICROSOFT AZURE AD GRAPH API ENDPOINT**
   - **OAUTH 2.0 TOKEN ENDPOINT**
8. 在Cisco ISE 中，配置 Microsoft Intune 服务器。有关配置外部 MDM 服务器的详细信息，请参阅在 ISE 中定义移动设备管理服务器，第 769 页。以下字段对于配置 Microsoft Intune 很重要：
   - **自动发现 URL (Auto Discovery URL)**：输入 Microsoft Azure 管理门户中的 *Microsoft Azure AD* 图形 *API* 终端 *(Microsoft Azure AD Graph API Endpoint)* 值。此 URL 是应用可使用图形 API 访问 Microsoft Azure AD 中的目录数据的终端。URL 格式为：`https://<hostname>/<tenant id>`

     例如，`https://graph.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329`。

     此 URL 的扩展版本也在属性文件中，格式为：`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>`。
   - **客户端 ID (Client ID)**：应用的唯一标识符。如果应用访问其他应用中的数据，如 Microsoft Azure AD Graph API、Microsoft Intune API 等，则需要使用此属性。
   - **颁发令牌的 URL (Token Issuing URL)**：输入上一步中的 *Oauth2.0* 授权终端 *(Oauth2.0 Authorization Endpoint)* 值。在该终端上，应用可以使用 OAuth2.0 获得访问令牌。在对应用进行身份验证后，Microsoft Azure AD 会为应用（Cisco ISE）颁发一个访问令牌，允许应用调用图形 API/Intune API。
   - **令牌受众 (Token Audience)**：令牌面向的接收资源，通常为指向 Microsoft Intune API 的公共知名 **APP ID URL**。

有关 Microsoft Intune 应用的详细信息，请参阅：

- https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest

Microsoft System Center Configuration Manager 策略集示例

以下新字典条目在策略中用于支持 Microsoft SCCM。

- **MDM.DaysSinceLastCheckin**：自用户最后使用 Microsoft SCCM 签入或同步设备以来的天数。此值可以介于 1 至 365 天之间。
- **MDM.UserNotified**：有效值为 **Y** 或 **N**。该值指示是否通知用户其设备未注册。然后，您可以允许用户有限地访问网络，然后将他们重定向到注册门户，或者拒绝他们访问网络。
- **MDM.ServerType**：有效值为 **MDM**，表示 MDM 服务器，以及 **DM**，表示桌面设备管理。

以下是支持 Microsoft SCCM 的策略集示例。

策略名称	如果	过去
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCM_Redirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCM_Redirect

策略名称	如果	过去
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

为思科 ISE 配置 Microsoft System Center Configuration Manager Server

Cisco ISE 使用 Windows 管理规范 (WMI) 与 Microsoft SCCM 服务器通信。在运行 Microsoft SCCM 的 Windows 服务器上配置 WMI。

注释 用于思科 ISE 集成的用户帐户必须符合以下条件之一：

- 成为 SMS 管理员用户组的成员。
- 具有与 WMI 命名空间下的 SMS 对象相同的权限：

  `root\sms\site_<sitecode>`

  ，其中 *sitecode* 是 Microsoft SCCM 站点。

为域管理员组中的 Microsoft Active Directory 用户设置权限

默认情况下，对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，域管理员组对 Windows 操作系统中的某些注册表项没有完全控制权限。Microsoft Active Directory 管理员必须给予 Microsoft Active Directory 用户对以下注册表项的完全控制权限：

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

以下 Microsoft Active Directory 版本不需要对注册表进行更改：

- Windows 2003
- Windows 2003R2
- Windows 2008

要授予完全控制权限，Microsoft Active Directory 管理员必须首先获得注册表项的所有权：

步骤 1 右键点击注册表项图标，然后选择**所有者 (Owner)** 选项卡。

步骤 2 点击 **Permissions**（权限）。

步骤 3 点击 **Advanced**。

不在域管理员组中的 Microsoft Active Directory 用户的权限

对于 Windows Server 2012 R2，授予 Microsoft AD 用户对以下注册表项的完全控制权限：

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

在 Windows PowerShell 中使用以下命令来检查是否提供了对注册表项的完整权限：

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

当 Microsoft AD 用户不在域管理员组，但在域用户组中时，还需要以下权限：

- 添加注册表项以允许思科 ISE 连接到域控制器。
- 在域控制器上使用 DCOM 的权限，第 506 页
- 设置访问 WMI Root/CIMv2 名称空间的权限，第 507 页

只有以下 Active Directory 版本要求具有这些权限：

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

添加注册表项以允许思科 ISE 连接到域控制器

必须手动将一些注册表项添加到域控制器，以允许思科 ISE 以域用户身份进行连接，并检索登录身份验证事件。域控制器或该域中的任何其他机器都不需要代理。

以下注册脚本显示了要添加的密钥。您可以将其复制并粘贴到一个文本文件，并另存为扩展名为 .reg 的文件，然后双击该文件进行注册更改。要添加注册密钥，用户必须是根秘钥的所有者。

```
Windows 注册表编辑器版本 5.00 [HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
 "AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"="
 "
```

确保DllSurrogate注册表项的值包含两个空格。如果手动更新注册表，必须仅包含两个空格，不包含引号。手动更新注册表时，请确保 AppID、DllSurrogate 及其值中不包含引号。

如前一脚本所示，保留所有空行，包括文件末尾的空行。

在 Windows 命令提示符下使用以下命令，以确认注册表项是否已创建并包含正确值：

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

在域控制器上使用 DCOM 的权限

用于思科 ISE 被动身份服务的 Microsoft Active Directory 用户必须具有在域控制器服务器上使用 DCOM 的权限。通过 **dcomcnfg** 命令行工具配置权限。

步骤 1 从命令行运行 **dcomcnfg** 工具。

步骤 2 扩展**组件服务 (Component Services)**。

步骤 3 扩展 **计算机 (Computers)** > **我的计算机 (My Computer)**。

步骤 4 从菜单栏中选择**操作 (Action)**，点击**属性 (Properties)**，然后点击 **COM 安全性 (COM Security)**。

步骤 5 Cisco ISE 用于访问和启动的帐户必须具有允许权限。将 Microsoft Active Directory 用户添加至所有四个选项（**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)** 的**编辑限制设置 (Edit Limits)** 和**编辑默认设置 (Edit Default)**）。

步骤 6 对于**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)**，允许所有本地和远程访问。

图 ***36:*** 访问权限的本地和远程访问

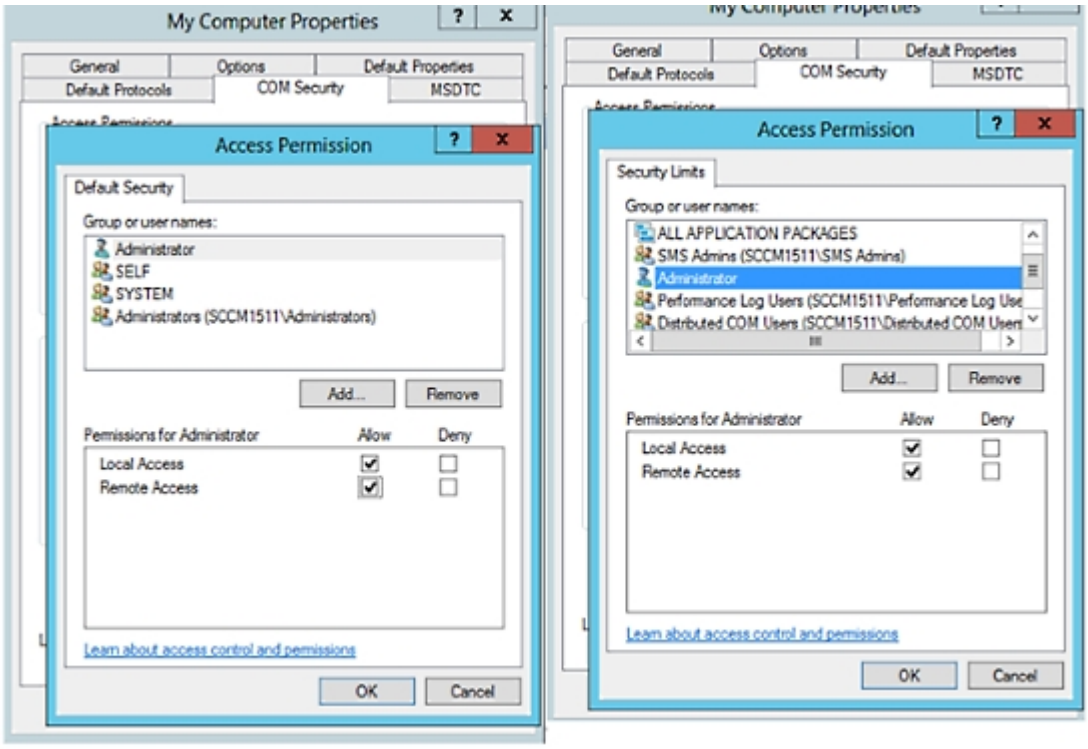
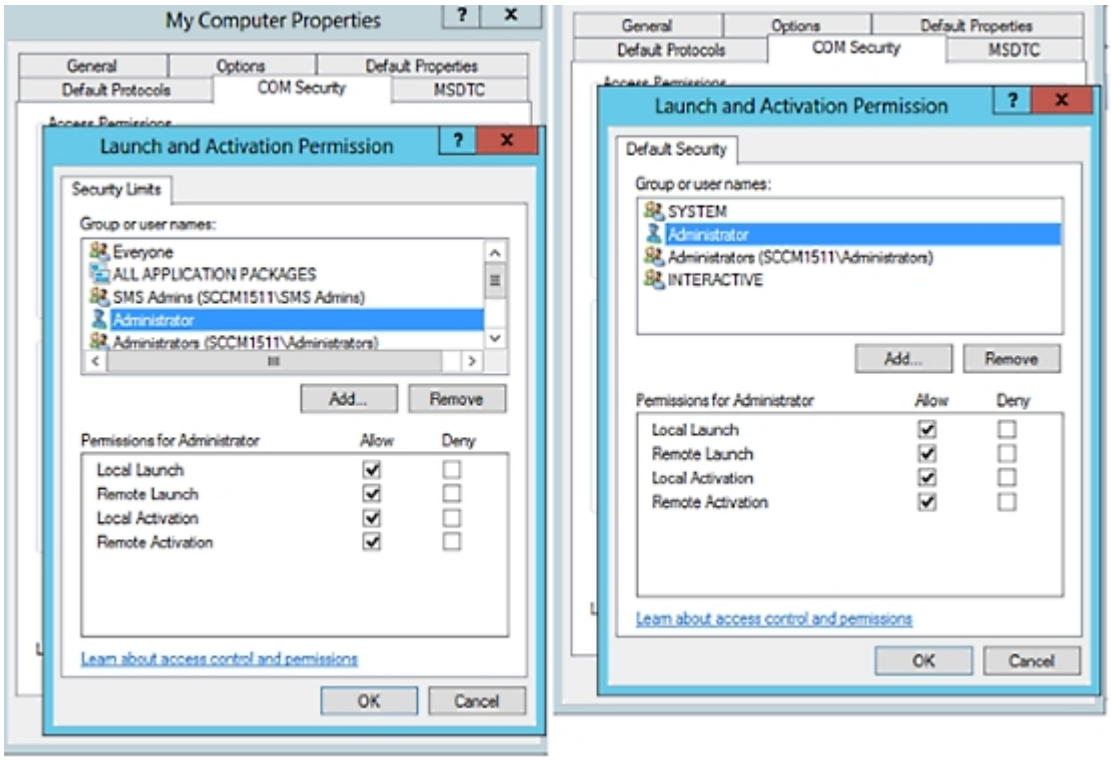


图 *37:* 启动以及激活权限的本地和远程访问



设置访问 WMI Root/CIMv2 名称空间的权限

默认情况下，Microsoft Active Directory 用户没有对“执行方法”(Execute Methods) 和“远程启用”(Remote Enable) 的权限。您可以使用 wmimgmt.msc MMC 控制台授予访问权限。

步骤 1 选择 **开始 (Start)** > **运行 (Run)** 并键入 `wmimgmt.msc`。

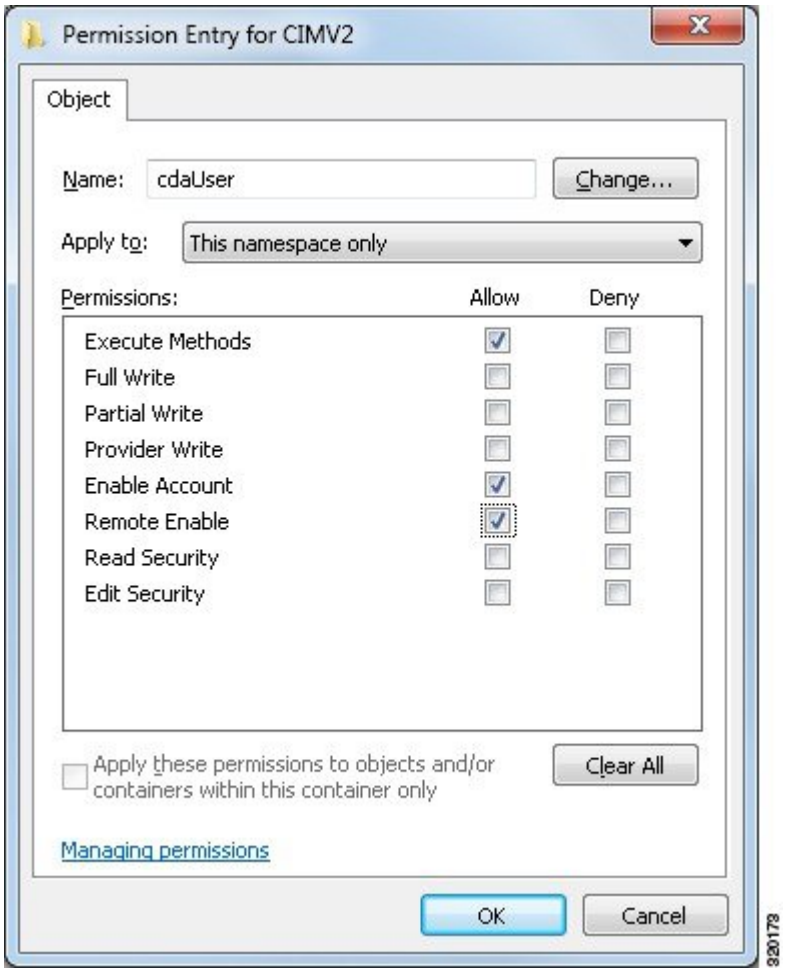
步骤 2 右键点击 **WMI 控制 (WMI Control)** 并点击**属性 (Properties)**。

步骤 3 在**安全 (Security)** 选项卡下，展开**根 (Root)** 并选择 **CIMV2**。

步骤 4 点击 **Security**。

步骤 5 添加 Active Directory 用户，并按如下所示配置所需的权限。

图 *38: WMI Root\CIMv2* 名称空间所需的权限



为 WMI 访问开放防火墙端口

Microsoft Active Directory 域控制器上的防火墙软件可能会阻止对 WMI 的访问。您可以关闭防火墙，或者允许在特定 IP 地址（Cisco ISE IP 地址）访问以下端口：

- TCP 135：通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端处理此请求的组件使用哪个端口。
- UDP 138：NetBIOS 数据报服务
- TCP 139：NetBIOS 会话服务
- TCP 445：SMB

注释 思科 ISE 支持 SMB 2.0。

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 *%SystemRoot%\System32\dllhost.exe* 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP 地址（Cisco ISE IP）。

在思科 ISE 中配置移动设备管理服务器

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)**。

步骤 2 点击。

步骤 3 为以下字段输入所需的值：**名称 (Name)**、**主机名/IP 地址 (Host Name/IP Address)**、**端口 (Port)**、**实例名称 (Instance Name)**、**用户名 (Username)**、**密码 (Password)**、**说明 (Description)**、**轮询间隔 (Polling Interval)** 和**合规设备重新身份验证查询的时间间隔 (Time Interval for Compliance Device ReAuth Query)**。

步骤 4 从**服务器类型 (Server Type)** 下拉列表选择**移动设备管理器 (Mobile Device Manager)** 或**桌面设备管理器 (Desktop Device Manager)**。

步骤 5 从**身份验证类型 (Authentication type)** 下拉列表中选择身份验证。

步骤 6 从**状态 (Status)** 下拉列表中选择**启用 (Enabled)** 或**禁用 (Disabled)**。

步骤 7 要验证 MDM 服务器是否已连接到Cisco ISE，请点击**测试连接 (Test Connection)**。**测试连接 (Test Connection)** 并非旨在检查所有使用案例的权限（获取基准、获取设备信息等）。这些在服务器添加到Cisco ISE 时进行验证。

步骤 8 在配置**桌面设备管理器**服务器时，点击**保存并继续 (Save & Continue)**；在配置**移动设备管理器**服务器时，点击**保存 (Save)**。

从桌面设备管理器服务器选择用于终端合规性的配置基准策略

您可以查看添加到Cisco ISE 的桌面设备管理器服务器（例如，Microsoft SCCM 服务器）中可用的基准策略，并选择特定基准策略以检查网络访问的终端合规性。可以在Cisco ISE 管理门户中查看在桌面设备管理器服务器中启用和部署的配置基准策略。

注释 检查您的桌面设备管理服务器中的用户权限，确保您拥有所需的安全权限，允许将基准策略和合规性信息发送到Cisco ISE。必须在桌面设备管理器的“**安全**”**(Security)** > “**管理员用户**”**(Administrator Users)** 文件夹中添加管理员。

要在Cisco ISE GUI 中查看桌面设备管理器服务器中的基准策略，请点击**菜单 (Menu)** 图标（☰），然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)** > **MDM 服务器 (MDM Servers)**。

向思科 ISE 添加新的桌面设备管理器服务器，然后选择配置基准策略

在 **MDM 服务器 (MDM Servers)** 窗口中，点击**添加 (Add)** 以添加新的桌面设备管理器服务器。

要验证服务器是否已连接到Cisco ISE，请点击**测试连接 (Test Connection)** 按钮。要查看此服务器中可用的配置基准策略，请点击**保存并继续 (Save & Continue)**。系统将显示一个新窗口，其中包含基准策略的名称和 ID 列表。

从现有桌面设备管理器服务器中选择配置基准策略

在 **MDM 服务器 (MDM Servers)** 窗口中，选中所需服务器的复选框，然后点击**编辑 (Edit)**。点击**配置基准 (Configuration Baselines)** 选项卡，获取此服务器中可用的基准策略列表。

默认情况下，系统会选择所有基准策略。取消选中**名称 (Name)** 旁的复选框，以取消选择所有基准策略。通过选中基准策略名称旁的复选框，选择所需的基准策略。点击**保存 (Save)**。

根据所选配置基准策略检查终端合规性。

如果桌面设备管理器服务器中的配置基准策略有任何更改，请点击**配置基准 (Configuration Baselines)** 选项卡中的**立即更新 (Update Now)** 按钮，以在Cisco ISE 中更新更改。

配置 Windows 终端的设备标识符

桌面设备管理器服务器使用某些属性作为标识符来验证连接到网络的终端。终端 MAC 地址是最常用的标识符。但是，当使用加密狗、扩展坞或 MAC 地址随机化技术时，MAC 地址不是最可靠的标识符。

您现在可以选择使用主机名作为标识符。主机名派生自证书中可用的通用名称 (CN) 或 SAN-DNS 属性。对于使用主机名检查基准策略合规性来说，基于证书的终端身份验证是强制的。

要配置桌面设备管理器服务器的设备标识符，请转至其**服务器配置 (Server Configuration)** 选项卡。从主菜单中选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)** > **MDM 服务器 (MDM Servers)** > **编辑 (Edit)**。

在**设备标识符配置 (Device Identifier Configurations)** 部分中，默认情况下按如下顺序启用以下标识符：

1. **旧版 MAC 地址**
2. **证书 - CN、主机名**
3. **证书 - SAN-DNS、主机名**

要取消选择标识符，请取消选中该标识符对应的复选框。可以拖动属性以重新排列服务器用于验证的顺序。

验证设备标识符的配置

当使用主机名进行验证时，Cisco ISE 会为终端分配一个 GUID。请参阅**实时日志 (Live Logs)** 窗口（在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)**），并检 GUID 条目以了解详细信息。

配置用于重定向未注册设备的授权配置文件

您必须在Cisco ISE 中配置授权配置文件来重定向每个外部 MDM 服务器的非注册设备。

开始之前

- 确保您已在Cisco ISE 中创建 MDM 服务器定义。只有在成功将Cisco ISE 与 MDM 服务器集成之后，才会填充 MDM 字典，您才可以使用 MDM 字典属性创建授权策略。
- 在无线 LAN 控制器上配置用于重定向未注册设备的 ACL。
- 如果使用代理进行互联网连接，并且 MDM 服务器是内部网络的一部分，则必须将 MDM 服务器名称或其 IP 地址置于代理绕行列表中。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **代理 (Proxy)** 以执行此操作。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)** > **添加 (Add)**。

步骤 2 创建用于重定向不合规或未注册的非注册设备的授权配置文件。

步骤 3 在**名称 (Name)** 字段中，为授权配置文件输入与 MDM 服务器名称匹配的名称。

步骤 4 从**访问类型 (Access Type)** 下拉列表中，选择 **ACCESS_ACCEPT**。

步骤 5 在**常见任务 (Common Tasks)** 部分中，选中 **Web 重定向 (Web Redirection)** 复选框，然后从下拉列表中选择 **MDM 重定向 (MDM Redirect)**。

步骤 6 从 **ACL** 下拉列表中，选择输入您在无线 LAN 控制器上配置的 ACL 的名称。

步骤 7 从**值 (Value)** 下拉列表中，选择 MDM 门户。

步骤 8 从 **MDM 服务器 (MDM Server)** 下拉列表中，选择要使用的 MDM 服务器。

步骤 9 点击**提交 (Submit)**。

下一步做什么

为移动设备管理用例配置授权策略规则。

为移动设备管理用例配置授权策略规则

您必须在Cisco ISE 中配置授权策略规则才能完成 MDM 配置。

开始之前

- 将 MDM 服务器证书添加到Cisco ISE 证书库。
- 确保您已在Cisco ISE 中创建了 MDM 服务器定义。只有在成功将Cisco ISE 与 MDM 服务器集成之后，才会填充 MDM 字典，您才可以使用 MDM 字典属性创建授权策略。
- 在无线 LAN 控制器上配置 ACL 以重定向未注册或不合规设备。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开策略集以查看授权策略规则。

步骤 2 添加以下规则：

- **MDM_Un_Registered_Non_Compliant**：适用于尚未向 MDM 服务器注册或不符合 MDM 策略的设备。请求与此规则匹配之后，系统会显示Cisco ISE MDM 窗口，其中包含有关向 MDM 注册设备的信息。

  注释　请勿在此策略中使用 **MDM.MDMServerName** 条件。使用此条件时，仅当终端注册到 MDM 服务器注册后，才与策略匹配。

- **PERMIT**：如果设备已注册到Cisco ISE、MDM，并符合Cisco ISE 和 MDM 策略，则系统将根据Cisco ISE 中配置的访问控制策略向它授予网络访问权限。

步骤 3 点击**保存 (Save)**。

在无线 LAN 控制器上配置 ACL 以实现移动设备管理互操作

必须在无线 LAN 控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备和证书调配。ACL 必须采用以下顺序。

步骤 1 允许所有从服务器到客户端的出站流量。

步骤 2 （可选）允许从客户端到服务器的 ICMP 入站流量以进行故障排除。

步骤 3 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。

步骤 4 允许从客户端到服务器再到 ISE 的所有入站流量以执行 Web 门户和请求方以及证书调配流程。

步骤 5 允许从客户端到服务器的入站 DNS 流量以进行名称解析。

步骤 6 允许从客户端到服务器的入站 DHCP 流量以获取 IP 地址。

步骤 7 拒绝所有从客户端到服务器再到企业资源的入站流量，以重定向至Cisco ISE（根据公司策略）。

步骤 8 （可选）允许其余流量。

示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，Cisco ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 *39:* 用于重定向未注册设备的 *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

擦除或锁定设备

Cisco ISE 可以让您擦除已丢失的设备或打开其 pin 锁。您可以从**终端 (Endpoints)** 窗口配置此特性。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

步骤 2 选中您想要擦除或锁定的设备旁边的复选框。

步骤 3 从 **MDM 操作(MDM Actions)** 下拉列表中，选择以下选项之一：

- **完全擦除 (Full Wipe)**：此选项会删除公司应用或将设备重置为出厂设置，具体取决于 MDM 供应商。
- **企业擦除 (Corporate Wipe)**：此选项会删除您在 MDM 服务器策略中配置的应用。
- **PIN 锁定**：此选项会锁定设备。

步骤 4 点击**是 (Yes)** 擦除或锁定设备。

查看移动设备管理报告

Cisco ISE 记录 MDM 服务器定义的所有添加、更新和删除操作。可以在**更改配置审核 (Change Configuration Audit)** 报告中查看这些事件，该报告显示选定时段内任何系统管理员的全部配置更改。

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。检查您要查看的 MDM 服务器的**对象类型 (Object Type)** 和**对象名称 (Object Name)** 列中的条目，然后点击相应的**事件 (Event)** 值以查看配置事件的详细信息。

查看移动设备管理日志

您可以使用**调试向导 (Debug Wizard)** 窗口查看移动设备管理日志消息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)**。点击Cisco ISE 节点旁的单选按钮，然后点击**编辑 (Edit)**。在显示的新窗口中，点击组件名称 **external-mdm** 旁的单选按钮，然后点击**编辑 (Edit)**。此组件的默认日志级别为**信息 (INFO)**。从相应的**日志级别 (Log Level)** 下拉列表中，选择**调试 (DEBUG)** 或**跟踪 (TRACE)**，然后点击**保存 (Save)**。

第 11 章

细分市场

策略集

Cisco ISE 是基于策略的网络访问控制解决方案，可提供网络访问策略集，允许您管理多个不同的网络访问用例，如无线、有线、访客和客户端调配。通过策略集（网络访问集和设备管理集），您可以对同一集合内的身份验证策略和授权策略进行逻辑分组。您可以基于区域具有若干策略集，例如基于位置、访问类型和类似参数的策略集。安装ISE时，始终有一个定义的策略集，即默认策略集，默认策略集包含预定义和默认的身份验证、授权和例外策略规则。

创建策略集时，可以配置这些规则（使用条件和结果进行配置），以便选择策略集级别的网络访问服务、身份验证策略级别的身份源，以及授权策略级别的网络权限。从适用于各种不同供应商的Cisco ISE 支持的字典中，可以使用任何属性定义一个或多个条件。Cisco ISE 可以让您将条件创建为可重复使用的单个策略元素。

每个策略集用于与网络设备进行通信的网络访问服务是在该策略集的顶层定义的。网络访问服务包括：

- 允许的协议 - 为处理初始请求和协议协商而配置的协议
- 代理服务 - 将请求发送至外部 RADIUS 服务器进行处理

注释 从设备管理工作中心，您还可以为策略集选择相关的 TACACS 服务器序列。使用 TACACS 服务器序列可配置要处理的 TACACS 代理服务器序列。

策略集按层次结构进行配置，其中位于策略集顶层的规则（可从策略集表中查看）适用于整个策略集，并先于其余策略和例外规则进行匹配。此后，按以下顺序应用集合的规则：

1. 身份验证策略规则
2. 本地策略例外
3. 全局策略例外
4. 授权策略规则

注释 对于网络访问和设备管理策略，策略集功能是相同的。在使用网络访问和设备管理工作中心时，可以应用本章中介绍的所有流程。本章专门讨论网络访问工作中心策略集。 在思科 ISE GUI 中，点击 **菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。

ISE 社区资源

有关从 WLC 使用 RADIUS 结果的信息，请参阅 WLC Called-Station-ID（Radius 身份验证和记账配置）。

策略集配置设置

下表介绍**策略集 (Policy Sets)** 窗口中的字段，由此窗口可配置策略集，包括身份验证、例外和授权策略。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**，找到网络访问策略。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**，找到设备管理策略。

表 *125:* 策略集配置设置

字段名称	使用指南
状态	选择此策略的状态。它可以是下列选项之一： • **已启用 (Enabled)**：此策略条件处于活动状态。 • **已禁用 (Disabled)**：此策略条件处于非活动状态，不会被评估。 • **仅监控 (Monitor Only)**：此策略条件不会被评估。
策略集名称	为此策略集输入一个唯一的名称。
条件	在新策略行中，点击加号 (+) 图标，或者在现有策略行中，点击“编辑”(Edit) 图标以打开 Conditions Studio。
说明	输入策略的唯一说明。
允许的协议或服务器序列	选择已创建的允许协议，或点击 (+) 号以**创建新的允许协议**、**创建新的 Radius 序列**或**创建 TACACS 序列**。
条件	在新的例外行中，点击加号 (+) 图标，或者在现有例外行中，点击“编辑”(Edit) 图标以打开 Conditions Studio。
点击数	命中数是一种诊断工具，用于指示条件匹配的次数。将鼠标悬停在该图标上可查看上次更新时间、重置为零和查看更新频率。

字段名称	使用指南
操作	点击“操作”(Actions) 列中的齿轮图标 ⚙，查看并选择不同的操作： • 在上方插入新行 (Insert new row above)：在打开“操作”(Actions) 菜单的策略上方插入新策略。 • 在下方插入新行 (Insert new row below)：在打开“操作”(Actions) 菜单的策略下方插入新策略。 • 在上方复制 (Duplicate above)：在打开“操作”(Actions) 菜单的策略上方插入复制的策略，高于原始集。 • 在下方复制 (Duplicate below)：在打开“操作”(Actions) 菜单的策略下方插入复制的策略，低于原始集。 • 删除 (Delete)：删除策略集。
查看	点击箭头图标可打开特定策略集的集合视图，并查看其身份验证、例外和授权子策略。

身份验证策略

每个策略集可以包含多个身份验证规则，它们共同代表该策略集的身份验证策略。身份验证策略的优先级根据这些策略在策略集本身中的显示顺序来确定（从“身份验证策略”(Authentication Policy) 区域中的“集合视图”(Set view) 页面）。

Cisco ISE 根据策略集级别配置的设置动态选择网络访问服务（允许的协议或服务器序列），然后从身份验证和授权策略级别检查身份源和结果。您可以定义一个或多个使用Cisco ISE 字典中任何属性的条件。Cisco ISE 可以让您将条件单个策略元素，它们可以存储在系统库中，然后重复用于其他基于规则的策略。

身份验证方法是身份验证策略的结果，可以是以下任意一种：

- 拒绝访问 - 系统拒绝用户的访问并且不执行身份验证。
- 身份数据库 - 可以是下述单个身份数据库中的一个：
  - 内部用户
  - 访客用户
  - 内部终端
  - Active Directory

- 轻量级目录访问协议 (LDAP) 数据库
- RADIUS 令牌服务器（RSA 或 SafeWord 服务器）
- 证书身份验证配置文件

- 身份源序列 - 用于身份验证的身份数据库的序列。

初始Cisco ISE 安装时实施的默认策略集包括默认 ISE 身份验证和授权规则。默认策略集还包括用于身份验证和授权的其他灵活内置规则（不是默认规则）。可向这些策略添加其他规则，也可以删除和更改内置规则，但不能删除默认规则，也不能删除默认策略集。

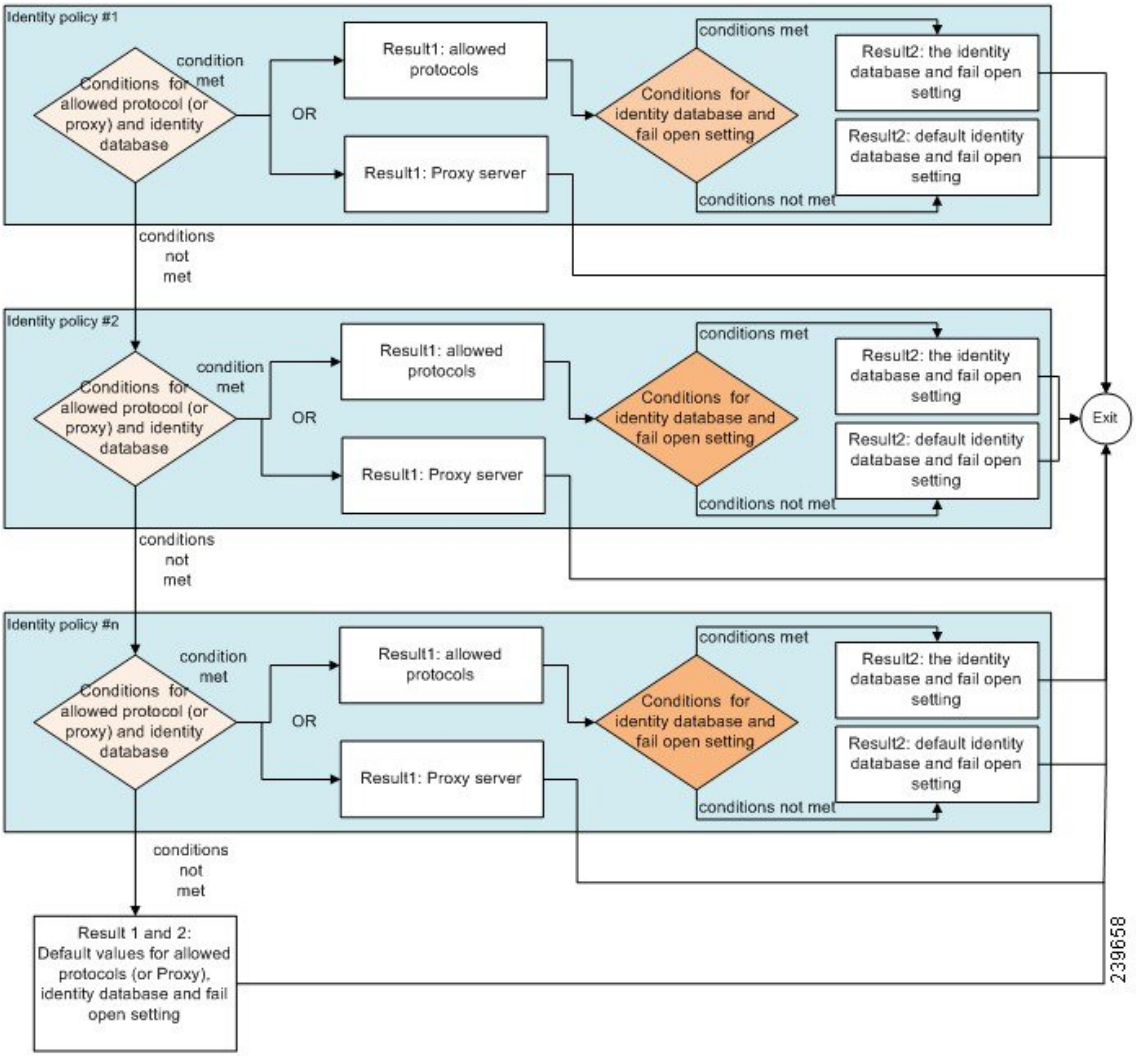
身份验证策略流

在身份验证策略中，可以定义多个由条件和结果组成的规则。ISE 会评估您指定的条件，并根据评估结果分配相应的结果。系统根据匹配条件的第一个规则选择身份数据库。

您还可以定义包括不同数据库的身份源序列。您可以定义您希望Cisco ISE 查询这些数据库的顺序。Cisco ISE 将依次访问这些数据库，直至身份验证成功。如果在外部数据库中同一用户有多个实例，则身份验证失败。身份源中只能有一个用户记录。

我们建议您在身份源序列中仅使用三个，或者最多四个数据库。

图 *40:* 身份验证策略流



身份验证失败 - 策略结果选项

如果您选择的身份方法为拒绝访问，则会发送拒绝消息作为对请求的响应。如果选择身份数据库或身份源序列，并且身份验证成功，则会继续处理为相同策略集配置的授权策略。某些身份验证失败，这些失败情况会按照以下方式分类：

- Authentication failed - 收到身份验证已失败的明确响应，例如错误凭证、禁用的用户等。默认操作是拒绝。
- User not found - 在任何身份数据库中均未找到此用户。默认操作是拒绝。
- Process failed - 无法访问身份数据库。默认操作是丢弃。

Cisco ISE 允许您配置下列任意一条身份验证失败的操作：

- Reject - 发送拒绝响应。
- Drop - 不发送任何响应。
- Continue - Cisco ISE 继续处理授权策略。

即使您选择继续选项，可能会存在一些实例，在这些实例中，由于正在使用的协议受到限制，Cisco ISE 无法继续处理请求。对于使用 PEAP、LEAP、EAP-FAST、EAP-TLS 或 RADIUS MSCHAP 的身份验证，当身份验证失败时或未找到用户时，无法继续处理请求。

当身份验证失败时，可继续处理 PAP/ASCII 和 MAC 身份验证绕行（MAB 或主机查找）的授权策略。对于其他所有身份验证协议，当身份验证失败时将发生以下情况：

- Authentication failed - 发送拒绝响应。
- User or host not found - 发送拒绝响应。
- Process failure - 不发送响应，并丢弃请求。

配置身份验证策略

根据需要，通过配置和维护多个身份验证规则，为每个策略集定义身份验证策略。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)** 可获取网络访问策略。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 可获取设备管理策略。

步骤 2 从要添加或更新身份验证策略的策略集对应的行中，从策略集表中的“视图”列点击 ›，以便访问所有策略集详细信息并创建身份验证和授权策略以及策略例外。

步骤 3 点击页面“身份验证策略”（Authentication Policy）部分旁边的箭头图标，展开并查看表中的所有身份验证策略规则。

步骤 4 在**操作 (Actions)** 列中，点击齿轮图标。从下拉菜单中，根据需要选择任何插入或重复选项来插入新的身份验证策略规则。
身份验证策略表中会显示一个新行。

步骤 5 在**状态 (Status)** 列中，点击当前**状态 (Status)** 图标，然后从下拉列表中根据需要更新策略集的状态。有关状态的详细信息，请参阅身份验证策略配置设置，第 796 页。

步骤 6 对于表中的任何规则，点击**规则名称 (Rule Name)** 或**说明 (Description)** 单元格，可做出任何必要的自由文本更改。

步骤 7 要添加或更改条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击 。Conditions Studio 将打开。有关详细信息，请参阅策略条件，第 813 页。

不是您选择的所有属性都包含“等于”、“不等于”、“位于”、“不位于”、“匹配”、“开头为”或“开头非”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

注释　您必须使用“等于”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。如果是列表，“位于”运算符会检查列表中是否存在特定值。如果是单个字符串，“位于”运算符会检查字符串是否与“等于”运算符相同。

步骤 8 按照检查和匹配策略的顺序来组织表中的策略。要更改规则的顺序，请将这些行拖放到正确位置。

步骤 9 点击**保存 (Save)** 以保存和实施所做的更改。

下一步做什么

1. 配置授权策略

身份验证策略配置设置

下表介绍**策略集 (Policy Sets)** 窗口的**身份验证策略 (Authentication Policy)** 部分中的字段，由此窗口可将身份验证子策略配置为策略集的一部分。对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。从“策略集”(Policy Sets) 页面，选择 **查看 (View)** > **身份验证策略 (Authentication Policy)**。

表 *126:* 身份验证策略配置设置

字段名称	使用指南
状态	选择此策略的状态。它可以是下列选项之一： • **已启用 (Enabled)**：此策略条件处于活动状态。 • **已禁用 (Disabled)**：此策略条件处于非活动状态，不会被评估。 • **仅监控 (Monitor Only)**：此策略条件将被评估，但结果不实施。您可以在 Live Log 身份验证页面查看此策略条件的结果。在此情况下，查看详细报告，了解受监控的步骤和属性。例如，您可能想要添加新策略条件，但不确定此条件是否为您提供正确的结果。在此情况下，您可以在监控模式下创建策略条件来查看结果，如果您对结果满意，可以启用此选项。

字段名称	使用指南
规则名称	输入此身份验证策略的名称。
条件	在新策略行中，点击加号 (+) 图标，或者在现有策略行中，点击“编辑”(Edit) 图标以打开 Condition Studio。
使用	选择要用于身份验证的身份源。如果您配置了身份源序列，也可以选择身份源序列。 您可以编辑在此规则中定义的任何身份源都与请求不匹配时您想要Cisco ISE 使用的默认身份源。
选项	为身份验证失败、未找到用户或进程失败事件定义进一步的操作。您可以选择下面一个选项： • **拒绝 (Reject)**：发送拒绝响应。 • **丢弃 (Drop)**：未发送响应。 • **继续 (Continue)**：Cisco ISE 继续执行授权策略。
点击数	命中数是一种诊断工具，用于指示条件匹配的次数。
操作	点击“操作”(Actions) 列中的齿轮图标 ⚙，查看并选择不同的操作： • 在上方插入新行 (Insert new row above)：在打开“操作”(Actions) 菜单的策略上方插入新的身份验证策略。 • 在下方插入新行 (Insert new row below)：在打开“操作”(Actions) 菜单的策略下方插入新的身份验证策略。 • 在上方复制 (Duplicate above)：在打开“操作”(Actions) 菜单的策略上方插入复制的身份验证策略，高于原始集。 • 在下方复制 (Duplicate below)：在打开“操作”(Actions) 菜单的策略下方插入复制的身份验证策略，低于原始集。 • 删除 (Delete)：删除策略集。

基于密码的身份验证

身份验证对用户信息进行验证，以确认用户身份。传统身份验证使用名称和固定密码。这是最普遍、最简单和最经济的身份验证方法。缺点在于此信息可能会被告知他人、被猜到或捕获。使用简单、未加密用户名和密码的方法不被视为强身份验证机制，但是对于低授权或低权限级别（例如互联网访问）可能已足够。

使用加密密码和加密技术的安全身份验证

应使用加密来降低网络中的密码捕获风险。客户端和服务器访问控制协议（例如 RADIUS）可对密码加密，以防止在网络中捕获密码。但是，RADIUS 仅在身份验证、授权和记账 (AAA) 客户端与 Cisco ISE 之间运行。在身份验证流程中的以下位置点之前，未经授权的人员可以获取明文密码，如以下示例所示：

- 在通过电话线路拨号的最终用户客户端之间的通信中
- 在终止于网络接入服务器的 ISDN 线路上
- 在最终用户客户端与托管设备之间的 Telnet 会话中

安全性较高的方法会采用加密技术，例如，那些用于质询握手身份验证协议 (CHAP)、一次性密码 (OTP) 和基于 EAP 的高级协议中的加密技术。Cisco ISE 支持各种身份验证方法。

身份验证方法和授权权限

身份验证与授权之间存在基本的隐式关系。向用户授予的授权权限越多，身份验证的能力就越强。Cisco ISE 通过提供各种身份验证方法来支持此关系。

身份验证面板

Cisco ISE 控制板会概述网络中和设备发生的全部身份验证。它提供在身份验证 Dashlet 中身份验证和身份验证失败的概览信息。

RADIUS 身份验证 Dashlet 提供以下有关Cisco ISE 已处理身份验证的统计信息：

- Cisco ISE 已处理 RADIUS 身份验证请求的总数，包括已通过的身份验证、已失败的身份验证以及相同用户的同时登录数。
- Cisco ISE 已处理的 RADIUS 已失败的身份验证请求的总数。

您还可以查看 TACACS + 身份验证的摘要。TACACS + 身份验证 Dashlet 提供设备身份验证的统计信息。

有关设备管理身份验证的详细信息，请参阅。TACACS 实时日志，第 285 页有关 RADIUS 实时日志设置的其他信息，请参阅RADIUS 实时日志，第 279 页。

ISE 社区资源

有关如何对失败的身份验证和授权进行故障排除的信息，请参阅如何：对 ISE 失败的身份验证和授权进行故障排除。

查看身份验证结果

Cisco ISE 提供多种方式查看实时身份验证摘要。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 对于网络身份验证 (RADIUS)，请选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)** 或对于设备身份验证 (TACACS)，请选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)** 查看实时身份验证摘要。

步骤 2 您可以通过以下方式查看身份验证摘要：

- 将鼠标悬停在“状态”(Status) 图标上，以查看身份验证的结果和简短摘要。系统将显示一个包含状态详细信息的弹出窗口。
- 在列表顶部显示的任何一个或多个文本框中输入搜索条件，然后按 **Enter** 键以筛选您的结果。
- 点击 Details 列中的放大镜图标以查看详细报告。

  注释 由于身份验证摘要报告或控制板会收集和显示与失败或成功的身份验证对应的最新数据，因此报告内容会延迟几分钟后显示。

身份验证报告和故障排除工具

除身份验证详细信息外，Cisco ISE 还提供各种可用于有效管理网络的报告和故障排除工具。

可以运行各种报告，了解网络中的身份验证趋势和流量。可以生成历史以及当前数据的报告。以下是身份验证报告列表：

- AAA 诊断
- RADIUS 记账
- RADIUS 身份验证
- 身份验证摘要

注释 您必须在 Cisco Catalyst 4000 系列交换机上启用 IPv6 监听，否则 IPv6 地址不会映射到身份验证会话，也不会显示在 show 输出中。使用以下命令可启用 IPv6 监听：

```
vlan config <vlan-number> ipv6 snooping end ipv6 nd raguard policy router device-role router
 interface <access-interface> ipv6 nd raguard interface <uplink-interface> ipv6 nd raguard
 attach-policy router end
```

授权策略

授权策略是Cisco ISE 网络授权服务的组件。此服务允许您为访问网络资源的特定用户和组定义授权策略并配置授权配置文件。

授权策略可包含条件要求，即使用复合条件组合一个或多个身份组，而该复合条件包括可返回一个或多个授权配置文件的授权检查。此外，除了使用特定的身份组外，可能存在条件要求。

在Cisco ISE 中创建授权配置文件时使用授权策略。授权策略包括授权规则。授权规则具有三个元素：名称、属性以及权限。权限元素映射到授权配置文件。

思科 ISE 授权配置文件

授权策略将规则与特定用户和组身份关联以创建相应的配置文件。只要这些规则与已配置的属性匹配，策略就会返回授予权限的相应授权配置文件并且相应地授予网络访问权限。

例如，授权配置文件可以包括以下类型中包含的一系列权限：

- 标准配置文件
- 例外配置文件
- 基于设备的配置文件

配置文件包括从一组资源中选择的属性，这些属性存储于任何可用供应商字典中，并且在满足特定授权策略的条件时就会返回这些属性。由于授权策略可以包括映射到单个网络服务规则的条件，这些策略还可以包括授权检查列表。

这些授权验证都必须符合要返回的授权配置文件。授权验证通常由一个或多个条件组成，包括可添加至库中的用户定义的名称，其他授权策略然后可以重复使用这些条件。

授权配置文件的权限

在开始配置授权配置文件的权限之前，请确保：

- 了解授权策略与配置文件之间的关系
- 熟悉 Authorization Profile 页面
- 知悉在配置策略和配置文件时要遵守的基本规定
- 了解在授权配置文件中构成权限的内容

要使用授权配置文件，请选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)**。从左侧菜单中，选择 **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

使用 Results 导航窗格作为用于显示、创建、修改、删除、复制或搜索网络上不同类型授权配置文件的策略元素权限的过程的起点。Results 窗格初始显示 Authentication、Authorization、Profiling、Posture、Client Provisioning 和 Trustsec 选项。

通过授权配置文件，您可以选择在接受 RADIUS 请求时要返回的属性。Cisco ISE 提供可以通过配置 Common Tasks 设置来支持常用属性的机制。您必须输入 Common Tasks 属性的值，Cisco ISE 会将这些值转换为基础 RADIUS 值。

ISE 社区资源

有关如何在 802.1x 请求方（Cisco AnyConnect 移动安全）和身份验证器（交换机）之间配置媒体访问控制安全 (MACsec) 加密的示例，请参阅使用思科 AnyConnect 和 ISE 配置进行 MACsec 交换机-主机加密示例。

基于位置的授权

Cisco ISE 可与Cisco移动服务引擎 (MSE) 集成以引入基于物理位置的授权。Cisco ISE 使用来自 MSE 的信息基于 MSE 报告的用户实际位置提供差异化网络访问。

通过此功能，您可以使用终端位置信息在用户位于相应区域时提供网络访问。还可以将终端位置作为策略的其他属性添加，以便基于设备位置定义更为细化的策略授权集。您可以在授权规则内配置使用基于位置的属性的条件，例如：

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

您可以定义位置层次结构（园区/建筑物/楼层结构），并使用 Cisco Prime 基础设施应用配置安全区域和不安全区域。定义位置层次结构后，必须将位置层次结构数据与 MSE 服务器同步。有关 Cisco Prime 基础设施的详细信息，请参阅：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html。

您可以添加一个或多个 MSE 实例，以便将基于 MSE 的位置数据集成到授权过程。可以从这些 MSE 检索位置层次结构数据，并使用此数据配置基于位置的授权规则。

要跟踪终端移动，请在创建授权配置文件时选中“跟踪移动”(Track Movement) 复选框。Cisco ISE 将每 5 分钟查询一次相关 MSE 的终端位置，以验证是否更改了位置。

注释 在将 MSE 设备添加到思科 ISE 时，请将证书从 MSE 设备复制到 ISE 以方便授权。

注释 跟踪多个用户将因频繁更新影响性能。“跟踪移动”(Track Movement) 选项可用于安全性较高的位置。

位置树是使用从MSE实例检索的位置数据进行创建的。您可以通过使用位置树选择呈现给授权策略的位置条目。

注释 您将需要思科 ISE Advantage 许可证才能使用位置服务。

添加 MSE 服务器。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration) > 网络资源 (Network Resources) > 位置服务 (Location Services) > 位置服务器 (Location Servers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入 MSE 服务器详细信息，例如服务器名称、主机名/IP 地址、密码等等。

步骤 4 点击**测试 (Test)**可使用您提供的服务器详细信息来测试 MSE 连接。

步骤 5 （可选）在**查找位置 (Find Location)** 字段输入终端的 MAC 地址，并点击**查找 (Find)** 以检查该终端当前已连接到此 MSE。

如果找到终端位置，它显示为以下格式：*Campus:Building:Floor:Zone*。有时，根据位置层次结构和区域设置可显示多个条目。例如，如果一个名为 *Campus1* 中的一栋楼 (*building1*) 的所有楼层定义为非安全区域，一楼的实验区域定义为安全区域，当终端位于实验区域时，将会显示以下条目：

在以下位置查找到终端：

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

步骤 6 点击**提交 (Submit)**。

在新的 MSE 添加后，转到“位置树”(Location Tree) 页面，然后点击**获取更新 (Get Update)** 检索其位置层次结构并将其添加到位置树。如果该树上定义了过滤器，这些过滤器也应用于新的 MSE 条目。

位置树

位置树是通过使用从移动服务引擎 (MSE) 示例中检索的位置数据创建的。要查看位置树 (Location Tree)，请选择**管理 (Administration) > 网络资源 (Network Resources) > 位置服务 (Location Services) > 位置树 (Location Tree)**。

如果建筑物有多个 MSE，Cisco ISE 将收集来自所有 MSE 的详细位置信息并将单个树里呈现这些信息。

您可以通过位置树选择对授权策略可见的位置条目。您还可以根据您的需求隐藏特定位置。建议在隐藏位置之前更新位置树。即使已更新树，隐藏位置仍会保持隐藏状态。

如果与授权规则相关的位置条目已修改或删除，您必须禁用受影响的规则并将这些位置设置为未知，或为每个受影响的规则选择一个替代位置。您必须在应用更改或取消更新之前检验新的树状结构。

点击**获取更新** (Get Update) 从所有 MSE 获取最新位置层次结构。在检验新的树结构后，点击“保存”(Save) 以应用更改。

可下载 ACL

访问控制列表 (ACL) 是访问控制条目 (ACE) 的列表，可由策略实施点（例如，交换机）应用到资源。每个ACE可确定每个用户该对象的允许权限，如读取、写入、执行等。例如，可以为使用网络的销售区域而配置 ACL，同时使用一个 ACE 允许销售部门获得写入权限，并使用单独的 ACE 允许组织的所有其他员工获得读取权限。使用 RADIUS 协议时，ACL 通过过滤源和目标 IP 地址、传输协议和其他参数来进行授权。静态 ACL 驻留在交换机上并直接从交换机配置，可以从 ISE GUI 应用到授权策略中；可下载 ACL (DACL) 可从 ISE GUI 进行配置和管理，并应用到授权策略中。

要在 ISE 中将 DACL 实施到网络授权策略中，请执行以下操作：

1. 从以下位置配置新的或现有的DACL： **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **可下载 ACL (Downloadable ACLs)**。有关详细信息，请参阅为可下载 ACL 配置权限，第 803 页。
2. 从以下位置配置新的或现有的授权配置文件： **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权配置文件 (Authorization Profiles)**，在此期间使用您已配置的任何 DACL。
3. 从以下位置实施在创建和配置新的和现有策略集时配置的授权配置文件： **策略 (Policy)** > **策略集 (Policy Sets)**。

为可下载 ACL 配置权限

借助ISE，可在授权策略中配置和实施可下载ACL (DACL)，以控制不同用户和用户组访问网络的方式。默认授权 DACL 可在安装 ISE 后可用，包括以下默认配置文件：

- DENY_ALL_IPV4_TRAFFIC
- PERMIT_ALL_IPV4_TRAFFIC
- DENY_ALL_IPV6_TRAFFIC
- PERMIT_ALL_IPV6_TRAFFIC

使用 DACL 时，无法更改这些默认值，但可以复制它们以创建其他类似的 DACL。

配置所需的DACL 后，即可将这些DACL 应用于网络上的相关授权策略。将 DACL 应用于授权策略后，就无法再更改其类型或从 ISE 中将其删除。当已在策略中使用 DACL 后，为了更改其类型，可以创建一个重复 DACL，然后更新该重复项，或者，可以从策略中删除该 DACL 以将其更新，然后在相关情况下重新应用。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **可下载 ACL (Downloadable ACLs)**。

步骤 2 点击**可下载 ACL** 表顶部的**添加 (Add)**，或者，选择任何现有的 DACL，然后点击表顶部的**复制 (Duplicate)**。

步骤 3 输入或编辑所需的 DACL 值，牢记以下规则：

- 名称字段支持的字符为：字母数字、连字符 (-)、点号 (.) 和下划线 (_)
- 如下所述，在选择 DACL 类型时，系统会根据所选 IP 版本处理 IP 格式：
  - **IPv4** 仅验证 IPv4 合法 ACE。必须输入有效的 IPv4 格式。

- **IPv6** 仅验证 IPv6 合法 ACE。必须输入有效的 IPv6 格式。
- 从先前版本升级到 2.6 版本的 DACL 会在 **IP 版本 (IP Version)** 字段中显示**无关 (Agnostic)** 以作为 DACL 类型。输入所需的任何格式。使用**无关 (Agnostic)** 可为Cisco不支持的设备创建 DACL。当选择**无关 (Agnostic)** 时，不验证格式，并且您无法检查 DACL 语法。

- 关键字 **Any** 必须是 DACL 中所有 ACE 的源。DACL 推送之后，源中的 **Any** 会被替换为连接到交换机的客户端的 IP 地址。

当将 DACL 映射到任何授权配置文件时，

注释 **IP 版本(IP Version)** 字段不可编辑。在这种情况下，请从**授权配置文件 (Authorization Profiles)** 中删除 DACL 引用，编辑 IP 版本并在**授权配置文件 (Authorization Profiles)** 中重新映射 DACL。

步骤 4 或者，当完成创建完整的 ACE 列表后，点击**检查 DACL 语法 (Check DACL Syntax)** 以验证列表。如果存在验证错误，系统会在自动打开的窗口中显示特定的说明，指明无效的语法。

步骤 5 点击**提交 (Submit)**。

针对 Active Directory 用户授权的设备访问限制

Cisco ISE 包含计算机访问限制 (MAR) 组件，提供另外一种控制 Microsoft Active Directory 身份验证用户授权的方法。此授权形式基于访问Cisco ISE 网络所用的计算机的计算机身份验证。对于每个成功的计算机身份验证，Cisco ISE 会将在 RADIUS Calling-Station-ID 属性（属性 31）中收到的值缓存为成功计算机身份验证的证据。

在达到 Active Directory Settings 页面的“Time to Live”参数中配置的小时数之前，Cisco ISE 会保留缓存中的每个 Calling-Station-ID 属性值。参数过期之后，Cisco ISE 会从参数缓存中删除该参数。

当用户从最终用户客户端进行身份验证时，Cisco ISE 会在缓存中搜索在用户身份验证请求中收到的 Calling-Station-ID 值的成功计算机身份验证的 Calling-Station-ID 值。如果Cisco ISE 在缓存中找到匹配的用户身份验证 Calling-Station-ID 值，这会以如下方式影响Cisco ISE 为请求身份验证的用户分配权限：

- 如果在Cisco ISE 缓存中找到与 Calling-Station-ID 值相匹配的值，则会分配成功授权的授权配置文件。
- 如果在Cisco ISE 缓存中未找到与 Calling-Station-ID 值相匹配的值，则会分配成功用户身份验证（不含计算机身份验证）的授权配置文件。

配置授权策略和配置文件的指南

管理授权策略和配置文件时，请遵循以下规定：

- 您创建的规则名称必须仅使用以下支持的字符：
  - 符号：加号 (+)、连字符 (-)、下划线 (_)、句点 (.) 和空格 ( )。
  - 字母字符：A-Z 以及 a-z。

- 数字字符：0-9。

- 身份组默认为“Any”（您可以将此全局默认设置应用于所有用户）。
- 您可以通过条件设置一个或多个策略值。但是，条件是可选的，不一定要选择条件才能创建授权策略。以下是创建条件的两种方法：
  - 从供选择的相应字典选择现有条件或属性。
  - 创建允许您选择建议值或使用文本框来输入自定义值的自定义条件。
- 您创建的条件名称必须仅使用以下支持的字符：
  - 符号：连字符 (-)、下划线 (_) 和句点 (.)。
  - 字母字符：A-Z 以及 a-z。
  - 数字字符：0-9。
- 创建或编辑授权配置文件时，如果选择使用除**客户端调配（策略）(Client Provisioning [Policy])**以外的任何其他选项启用 **Web 重定向（CWA、MDM、NSP、CPP）(Web Redirection [CWA, MDM, NSP, CPP])**，则无法将 IPv6 地址配置为该授权策略的**静态 IP/主机名/FDQN**。这是因为集中式 Web 身份验证 (CWA)、移动设备管理 (MDM) 重定向和本机请求方协议 (NSP) 不支持 IPv6 静态 IP/主机名/ FQDN。
- 选择用于策略的授权配置文件时，权限非常重要。权限可以允许访问特定资源或允许您执行特定任务。例如，如果用户属于特定身份组（例如设备管理员组）并且用户符合所定义的条件（例如属于波士顿的某个站点），则此用户可以获得与该身份组关联的权限（例如访问特定网络资源或在设备上执行特定操作的权限）。
- 在授权条件中使用 **radius** 属性 **Tunnel-Private-Group-ID** 时，必须在使用 **EQUALS** 运算符时在条件中同时提及标签和值，例如：

```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

注释 从Cisco ISE 1.4 开始，ANC 取代了端点保护服务 (EPS)。ANC 提供额外的分类和性能改进。虽然在策略中使用 ERS 属性有时仍然适用于某些 ANC 操作，但应使用 ANC 属性。例如，**Session:EPSStatus=Quarantine** 可能会失败。在策略中使用 **Session:ANCPolicy** 作为条件。

配置授权策略

在从策略 (Policy) 菜单为授权策略创建属性和构建块后，从策略集 (Policy Sets) 菜单在策略集中创建授权策略。

开始之前

在开始此程序之前，您应该对用于创建授权策略（如身份组和条件）的不同构建块有基本的了解。

步骤 1 对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

步骤 2 从“视图”(View) 列中，点击 > 以访问所有策略集详细信息，并创建身份验证和授权策略以及策略例外。

步骤 3 点击页面“授权策略”(Authorization Policy) 部分旁的箭头图标以展开并查看授权策略表。

步骤 4 在**操作 (Actions)** 列中，点击齿轮图标。从下拉菜单中，根据需要选择任何插入或重复选项来插入新的授权策略规则。
授权策略表中将显示新行。

步骤 5 要设置策略的状态，请点击当前**状态 (Status)** 图标，然后从下拉列表中选择**状态 (Status)** 列中的必要状态。有关状态的详细信息，请参阅授权策略设置，第 808 页。

步骤 6 对于表中的任何策略，请点击**规则名称 (Rule Name)** 单元格，进行必要的自由文本更改，并创建唯一的规则名称。

步骤 7 要添加或更改条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击  。Conditions Studio 将打开。有关详细信息，请参阅策略条件，第 813 页。

不是您选择的所有属性都包含“等于”、“不等于”、“位于”、“不位于”、“匹配”、“开头为”或“开头非”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

注释 您必须使用“等于”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。如果是列表，“位于”运算符会检查列表中是否存在特定值。如果是单个字符串，“位于”运算符会检查字符串是否与“等于”运算符相同。

步骤 8 对于网络访问结果配置文件，请从**结果配置文件 (Results Profiles)** 下拉列表中选择相关授权配置文件，或者选择或点击 ✚，选择**创建新授权配置文件 (Create a New Authorization Profile)**，然后在**添加新标准配置文件 (Add New Standard Profile)** 屏幕打开时，执行以下步骤：

a) 根据需要输入值以配置新的授权配置文件。请注意以下事项：

- 名称字段中支持的字符包括：空格 ! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {。
- 对于**常见任务**，要输入DACL，请按如下所示选择相关的 **DACL 名称 (ACL Name)** 选项，然后从动态下拉列表中选择必要的 DACL：
  - 要使用 IPv4 DACL，请选中 **DACL 名称 (ACL Name)**。
  - 要输入 IPv6 DACL，请选中 **IPv6 DACL 名称 (IPv6 DACL Name)**。
  - 要输入任何其他 DACL 语法，请选中任一选项。无关 DACL 同时显示在 IPv4 和 IPv6 下拉列表中。

    注释 如果选择 **DACL名称 (DACL Name)**，则 AVP 类型适用于 IPv4（即使 DACL 本身是无关的）。如果为 **IPv6 DACL 名称 (IPv6 DACL Name)** 选择 DACL，则 AVP 类型适用于 IPv6（即使 DACL 本身是无关的）。

- **注释** 如果选择对策略使用ACL，请确保设备与此功能兼容。有关详细信息，请参阅《思科身份识别服务引擎兼容性指南》。

  对于**常见任务**，要输入 ACL，请如下所示选择相关 **ACL（过滤器 ID）(ACL (Filter-ID))** 选项，然后在字段中键入 ACL 名称：

  - 要使用 IPv4 ACL，请选中 **ACL（过滤器 ID）(ACL (Filter-ID))**。
  - 要输入 IPv6 ACL，请选中 **ACL IPv6（过滤器 ID）(ACL IPv6 (Filter-ID))**。

- 要对 Airespace 设备使用 ACL，请根据需要选中 **Airespace ACL 名称 (Airespace ACL Name)** 或 **Airespace IPv6 ACL 名称 (Airespace IPv6 ACL Name)**，然后在字段中键入 ACL 名称。
- 您可以从动态显示在屏幕底部的**属性详细信息 (Attributes Details)** 中仔细检查授权配置文件 RADIUS 语法。

b) 点击**保存 (Save)** 以将所做的更改保存到Cisco ISE 系统数据库，以便创建授权配置文件。

c) 要在策略集区域之外创建、管理、编辑和删除配置文件，请选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 9 对于网络访问结果安全组，请从**结果安全组 (Results Security Groups)** 下拉列表中选择相关安全组，或者点击 ➕，选择**创建新安全组 (Create a New Security Group)**，然后在“创建新安全组”(Create New Security Group) 屏幕打开时，执行以下步骤：

a) 为新安全组输入名称和说明（可选）。

b) 如果要将此 SGT 传播至 Cisco ACI，请选中**传播至 ACI (Propagate to ACI)** 复选框。只有当与此 SGT 相关的 SXP 映射属于在 Cisco ACI“设置”(Settings) 页面中选择的同一 VPN 时，它们才会传播至 Cisco ACI。

默认情况下该选项处于禁用状态。

c) 输入 Tag Value。标签值可以设置为手动输入或自动生成。您还可以为 SGT 保留范围。您可以从以下位置对其进行配置：“通用 TrustSec 设置”(General TrustSec Settings) 页面（**工作中心 (Work Centers)** > **TrustSec** > **设置 (Settings)** > **通用 TrustSec 设置 (General TrustSec Settings)**）。

d) 点击**提交 (Submit)**。

有关详细信息，请参阅 安全组配置，第 899 页。

步骤 10 对于 TACACS+ 结果，请从**结果 (Results)** 下拉列表中选择相关命令集和外壳配置文件，或者点击**命令集 (Command Sets)**或**外壳配置文件 (Shell Profiles)** 列中的 ➕，分别打开**添加命令 (Add Commands)** 屏幕或**添加外壳配置文件 (Add Shell Profile)**。选择**创建新命令集 (Create a New Command Set)** 或**创建新外壳配置文件 (Create a New Shell Profile)**，然后输入字段。

步骤 11 在表中组织用来检查和匹配策略的顺序。

步骤 12 点击**保存 (Save)** 保存您对Cisco ISE 系统数据库所做的更改，并创建这条新的授权策略。

授权策略设置

下表介绍**策略集 (Policy Sets)** 窗口的**身份验证策略 (Authentication Policy)** 部分中的字段，由此窗口可将身份验证子策略配置为策略集的一部分。对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。从“策略集”(Policy Sets) 页面，选择 **查看 (View)** > **授权策略 (Authorization Policy)**。

表 *127:* 身份验证策略配置设置

字段名称	使用指南
状态	选择此策略的状态。它可以是下列选项之一： • **已启用 (Enabled)**：此策略条件处于活动状态。 • **已禁用 (Disabled)**：此策略条件处于非活动状态，不会被评估。 • **仅监控 (Monitor Only)**：将评估此策略条件，但不实施结果。您可以在 Live Log 身份验证页面查看此策略条件的结果。在此情况下，查看详细报告，了解受监控的步骤和属性。例如，您可能想要添加新策略条件，但不确定此条件是否为您提供正确的结果。在此情况下，您可以在监控模式下创建策略条件来查看结果，如果您对结果满意，可以启用此选项。
规则名称	为此策略输入一个唯一的名称。
条件	在新策略行中，点击加号 (+) 图标，或者在现有策略行中，点击“编辑”(Edit) 图标以打开 Condition Studio。
结果或配置文件	选择相关授权配置文件，该配置文件用于确定为配置的安全组提供的不同权限级别。如果尚未配置相关授权配置文件，可以内联配置。
结果或安全组	选择相关安全组，该安全组用于确定与特定规则相关的用户组。如果尚未配置相关安全组，则可以内联配置。
结果或命令集	命令集实施可由设备管理员执行的指定命令列表。当设备管理员在网络设备上发出操作命令时，查询 ISE 确定管理员是否被授权发出这些命令。这也称为命令授权。

字段名称	使用指南
结果或外壳配置文件	TACACS+ 外壳配置文件控制设备管理员的初始登录会话。
点击数	命中数是一种诊断工具，用于指示条件匹配的次数。
操作	点击“操作”(Actions) 列中的齿轮图标 ，查看并选择不同的操作： • 在上方插入新行 (Insert new row above)：在打开“操作”(Actions) 菜单的规则上方插入新的授权规则。 • 在下方插入新行 (Insert new row below)：在打开“操作”(Actions) 菜单的规则下方插入新的授权规则。 • 在上方复制 (Duplicate above)：在打开“操作”(Actions) 菜单的规则上方，插入重复授权规则，高于原集合。 • 在下方复制 (Duplicate below)：在打开“操作”(Actions) 菜单的规则下方，插入重复授权规则，低于原集合。 • 删除 (Delete)：删除规则。

授权配置文件设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**，**授权配置文件 (Authorization Profiles)** 窗口定义网络访问属性。

授权配置文件设置

- **名称 (Name)**：输入此新授权配置文件的名称。
- **说明**：输入此授权配置文件的说明。
- **访问类型 (Access Type)**：选择访问类型：**ACCESS_ACCEPT** 或 **ACCESS_REJECT**。
- **服务模板 (Service Template)**：启用此选项以支持与有 SAnet 功能的设备的会话。Cisco ISE 在授权配置文件中实施服务模板，用一个特殊标志将其标记为兼容服务模板 *(Service Template)*。由于服务模板也是授权配置文件，因此它充当支持 SAnet 和非 SAnet 设备的单个策略。
- **跟踪移动 (Track Movement)**：启用此选项可通过Cisco移动服务引擎 (MSE) 跟踪用户位置。

注释 此选项可能会影响思科 ISE 性能，仅适用于高安全性位置。

- **被动身份跟踪 (Passive Identity Tracking)**：启用此选项可将被动身份的 Easy Connect 功能来实施策略和跟踪用户。

常见任务

常见任务是适用于网络访问的特定权限和操作。

- **DACL 名称 (DACL Name)**：启用此选项可使用可下载的 ACL。您可以使用默认值（**PERMIT_ALL_IPV4_TRAFFIC**、**PERMIT_ALL_IPV6_TRAFFIC**、**DENY_ALL_IPV4_TRAFFIC**、**DENY_ALL_IPV6_TRAFFIC**）或从以下字典中选择属性：
  - 外部身份库（属性）
  - 终端
  - 内部用户
  - 内部终端

  有关添加 DACL 或编辑和管理现有 DACL 的详细信息，请参阅可下载 ACL，第 803 页。
- **ACL (Filter-ID)**：启用此选项可配置 RADIUS filter-ID 属性。filter-ID 指定 NAD 上的 ACL。定义 filter-ID 时，Cisco ISE 会在文件名后附加“.in”。Filter-ID 显示在**属性详细信息 (Attributes Details)** 窗格中。**ACL IPv6 (Filter-ID)** 的工作方式与 NAD 的 IPv6 连接相同。
- **安全组 (Security Group)**：启用此选项可分配授权的安全组 (SGT) 部分。
  - 如果Cisco ISE 未与 Cisco DNA Center 集成，则Cisco ISE 会分配 VLAN ID 1。
  - 如果Cisco ISE 与 Cisco DNA Center 集成，则选择 Cisco DNA Center 与Cisco ISE 共享的虚拟网络 (VN)，选择**数据类型 (Data Type)** 和子网/地址池。

注释 一个安全组任务包括一个安全组和一个 VN。如果配置安全组，则无法配置 VLAN。终端设备只能分配给一个虚拟网络。

- **VLAN**：启用此选项可指定虚拟 LAN (VLAN) ID。您可以为 VLAN ID 输入整数或字符串值。此条目的格式为 `Tunnel-Private-Group-ID:VLANnumber`。
- **语音域权限 (Voice Domain Permission)**：启用此选项可使用可下载的 ACL。供应商专用属性 (VSA) `cisco-av-pair` 与值 `device-traffic-class=voice` 相关联。在多域授权模式下，如果网络交换机收到此 VSA，则授权后终端将连接到语音域。
- **Web 重定向（CWA、DRW、MDM、NSP、CPP）(Web Redirection (CWA, DRW, MDM, NSP, CPP))**：启用此选项可在身份验证后启用 Web 重定向。

- 选择重定向类型。您选择的 Web 重定向类型会显示其他选项，如下所述。
- 输入 ACL 以支持让Cisco ISE 发送到 NAD 的重定向。

  您输入的发送到 NAD 的 ACL 在**属性详细信息 (Attributes Details)** 窗格中显示为 cisco-av pair。例如，输入 **acl119**，它会在**属性详细信息 (Attributes Details)** 窗格中显示为：`cisco-av-pair = url-redirect-acl = acl119`。
- 选择所选 Web 重定向类型的其他设置。

选择以下 Web 重定向类型之一：

- **集中式 Web 身份验证 (Centralized Web Auth)**：重定向到您从**值 (Value)** 下拉列表中选择的门户。
- **客户端调配（安全评估）(Client Provisioning (Posture))**：重定向到您从**值 (Value)** 下拉列表中选择的客户端调配门户，以在客户端上启用安全评估。
- **热点：重定向 (Hot Spot: Redirect)**：重定向到您从**值 (Value)** 下拉列表中选择的热点门户。
- **MDM 重定向 (MDM Redirect)**：重定向到您指定的 MDM 服务器上的 MDM 门户。
- **本地请求方调配 (Native Supplicant Provisioning)**：重定向到您从**值 (Value)** 下拉列表中选择的 BYOD 门户。

在选择 Web 重定向类型并输入所需参数后，配置以下选项：

- **显示证书续约消息 (Display Certificates Renewal Message)**：启用此选项可显示证书续约消息。URL-redirect 属性值改变并且包含证书有效的天数。此选项仅适用于集中式 Web 身份验证重定向。
- **静态 IP/主机名/FQDN (Static IP/Host Name/FQDN)**：启用此选项可将用户重定向到其他 PSN。输入目标 IP 地址、主机名或 FQDN。如果不配置此选项，用户将重定向到收到此请求的策略服务节点的 FQDN。
- **在逻辑配置文件中抑制终端的分析器 CoA (Suppress Profiler CoA for endpoints in Logical Profile)**：启用此选项可取消特定类型终端设备的重定向。

- **自动智能端口 (Auto SmartPort)**：启用此选项可使用自动智能端口功能。输入事件名称，它会创建一个 VSA cisco-av-pair，该值为 `auto-smart-port=event_name`。此值显示在**属性详细信息 (Attributes Details)** 窗格中。
- **访问漏洞 (Access Vulnerabilities)**：启用此选项可作为授权的一部分在此终端上运行以威胁防护为中心的 NAC 漏洞评估。选择适配器以及运行扫描的时间。
- **重新验证身份 (Reauthentication)**：启用此选项可在重新验证身份期间保持终端连接。通过选择使用 **RADIUS-Request** (1)，选择在重新验证身份的过程中保持连接。默认 RADIUS-Request (0) 会断开现有会话。您还可以设置非活动计时器。
- **MACSec 策略**：启用此选项可在启用 MACSec 的客户端连接到Cisco ISE 时使用 MACSec 加密策略。选择以下选项之一：**must-secure**、**should-secure** 或 **must-not-secure**。您的设置在**属性详细信息 (Attributes Details)** 窗格中显示为：`cisco-av-pair = linksec-policy=must-secure`。

- **NEAT**：启用此选项可使用网络边缘接入拓扑 (NEAT)，它能在网络之间扩展身份识别。如果选中此复选框，**属性详细信息 (Attributes Details)** 窗格中将显示 `cisco-av-pair = device-traffic-class=switch`。
- **Web 身份验证（本地 Web 身份验证）(Web Authentication (Local Web Auth))**：启用此选项可对此授权配置文件使用本地 Web 身份验证。通过由Cisco ISE 发送 VSA 以及 DACL，此值使交换机能够识别用于 Web 身份验证的授权。VSA 为 `cisco-av-pair = priv-lvl=15`，显示在**属性详细信息 (Attributes Details)** 窗格中。
- **Airespace ACL名称 (Airespace ACL Name)**：启用此选项可向Cisco Airespace 无线控制器发送 ACL 名称。Airespace VSA 使用此 ACL 向 WLC 上的连接授权本地定义的 ACL。例如，输入 **rsa-1188**，它会在**属性详细信息 (Attributes Details)**窗格中显示为 `Airespace-ACL-Name = rsa-1188`。
- **ASA VPN**：选中此选项可分配自适应安全设备 (ASA) VPN 组策略。从下拉列表中选择一个 VPN 组策略。
- **AVC 配置文件名称 (AVC Profile Name)**：启用此选项可在此终端上运行应用可视性。输入要使用的 AVC 配置文件。
- **UPN 查找 (UPN Lookup)**：待定

高级属性设置

- **目录 (Dictionaries)**：点击向下箭头图标可查看**目录 (Dictionaries)** 窗口中的可用选项。在第一个字段中选择应配置的字典和属性。
- **属性值 (Attribute Values)**：点击向下箭头图标可显示**属性值 (Attribute Values)** 窗口中的可用选项。选择所需的属性组和属性值。此值与第一个字段中选择的值匹配。您配置的任何**高级属性 (Advanced Attributes)** 设置都将显示在**属性详细信息 (Attributes Details)** 面板中。

  注释 字符 % 不能在**高级属性设置 (Advanced Attributes Settings)** 窗格中的**属性值 (Attribute Values)** 字段中使用。

- **属性详细信息 (Attributes Details)**：此窗格显示您为**常见任务 (Common Tasks)** 和**高级属性 (Advanced Attributes)** 设置的已配置属性值。

  属性详细信息 (Attributes Details) 窗格中显示的值是只读的。

  注释 要修改或删除**属性详细信息 (Attributes Details)** 窗格中显示的任何只读值，请在对应的**常见任务 (Common Tasks)** 字段中或在**高级属性设置 (Advanced Attributes Settings)** 窗格的**属性值 (Attribute Values)** 字段中选择的属性中修改或删除这些值。

相关主题

思科 ISE 授权配置文件，第 800 页
授权配置文件的权限，第 800 页
配置用于重定向未注册设备的授权配置文件，第 784 页
创建授权配置文件，第 338 页

授权策略例外

在每个策略集中，您可以定义常规授权策略，以及本地例外规则（从每个策略集的“集”(Set) 视图中的“授权策略本地例外”(Authorization Policy Local Exceptions) 部分定义）和全局例外规则（从每个策略集的“集”(Set) 视图中的“授权策略全局例外”(Authorization Policy Global Exceptions) 部分定义）。

使用全局授权例外策略，可以定义覆盖所有策略集中所有授权规则的规则。配置全局授权例外策略后，系统会将其添加到所有策略集。然后，可以从任何当前配置的策略集中更新全局授权例外策略。每次更新全局授权例外策略时，这些更新都会应用于所有策略集。

本地授权例外规则会覆盖全局例外规则。系统按以下顺序处理授权规则：首先处理本地例外规则，然后处理全局例外规则，最后处理授权策略常规规则。

授权例外策略规则的配置与授权策略规则相同。要配置例外策略，请参阅上述有关配置常规授权策略的说明：配置授权策略，第 805 页

本地和全局例外配置设置

对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。从**策略集 (Policy Sets)** 窗口中，选择 **查看 (View)** > **本地例外策略 (Local Exceptions Policy)** 或**全局例外策略 (Global Exceptions Policy)**。

授权例外设置与授权策略设置相同，如授权策略设置，第 808 页所述。

策略条件

Cisco ISE 使用基于规则的策略提供网络访问。策略是一组规则和结果，其中规则由条件组成。Cisco ISE 可以让您将条件创建为可在系统库中存储的单个策略元素，然后从 Conditions Studio 重复用于其他基于规则的策略。

条件可以很简单，或者，必要时可以使用运算符（等于、不等于、大于，等等）和值，或者通过包含多个属性、运算符和复杂层次结构，使之变得复杂。在运行时，Cisco ISE 会评估策略条件，然后根据策略评估返回的 true 值或 false 值，应用您所定义的结果。

在创建条件并为其分配唯一名称后，可以从 Conditions Studio 库中选择该条件，多次将其重复用于各种规则和策略，例如：

```
Network Conditions.MyNetworkCondition EQUALS true
```

不能从 Condition Studio 中删除策略中使用的条件或作为其他条件组成部分的条件。

每个条件各自定义可包括在策略条件中的对象列表，从而得到与请求中的定义匹配的一组定义。

您可以使用运算符 `EQUALS true` 来检查网络条件是否为 true（无论请求中存在的值是否与网络条件中的至少一个条目匹配）或 `EQUALS false`，以测试网络条件是否为 false（不匹配网络条件中的任何条目）。

CiscoISE还提供预定义的智能条件，您可以在策略中单独使用这些条件，也可以将其作为您自己的自定义条件中的构建块，并且可以根据需要进行更新和更改。

您可以创建以下唯一网络条件以限制对网络的访问：

- 终端站网络条件 - 基于发起和终止连接的终端站。

  Cisco ISE 会评估远程地址 TO 字段（根据它是 TACACS+ 还是 RADIUS 请求而获取），确定它是终端的 IP 地址、MAC 地址、主叫线路标识 (CLI) 还是被叫号码识别服务 (DNIS)。

  在 RADIUS 请求中，标识符在属性 31 (Calling-Station-Id) 中可用。

  在 TACACS+ 请求中，如果远程地址包含斜杠 (/)，则斜杠前的部分作为 FROM 值，斜杠后的部分作为 TO 值。例如，如果请求具有 CLI/DNIS，则 CLI 作为 FROM 值，DNIS 作为 TO 值。如果不包含斜杠，则整个远程地址作为 FROM 值（不论是 IP 地址、MAC 地址或 CLI）。

- 设备网络条件 - 基于处理请求的 AAA 客户端。

  可通过 IP 地址、在网络设备存储库中定义的设备名称或网络设备组确定网络设备。

  在 RADIUS 请求中，如果存在属性 4 (NAS-IP-Address)，Cisco ISE 会从该属性中获取 IP 地址。如果存在属性 32 (NAS-Identifier)，Cisco ISE 将从属性 32 获取 IP 地址。如果未找到这些属性，它将从其接收的数据包获取 IP 地址。

  设备字典（NDG 字典）包含网络设备组属性，如位置、设备类型或其他动态创建的表示 NDG 的属性。反过来，这些属性包含与当前设备相关的组。

- 设备端口网络条件 - 基于设备的 IP 地址、名称、NDG 和端口（终端站连接到的设备物理端口）。

  在 RADIUS 请求中，如果请求中存在属性 5 (NAS-Port)，则Cisco ISE 会从该属性中获取值。如果请求中存在属性 87 (NAS-Port-Id)，Cisco ISE 将从属性 87 获取请求。

  在 TACACS+ 请求中，Cisco ISE 会从（每个阶段的）起始请求的端口字段中获取此标识符。

有关这些独特条件的详细信息，请参阅特殊网络访问条件 ，第 832 页。

字典和字典属性

字典是关于可用于为域定义访问策略的属性和允许值的域特定目录。单个字典是同种属性类型的集合。字典中定义的属性具有相同的属性类型并且其类型会指明特定属性的来源或上下文。

属性类型可以是以下一种类型：

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

除了属性和允许的值之外，字典还包含关于名称与说明、数据类型和默认值等属性的信息。一个属性可以有以下一种数据类型：BOOLEAN、FLOAT、INTEGER、IPv4、IPv6、OCTET_STRING、STRING、UNIT32 和 UNIT64。

Cisco ISE 在安装时会创建系统字典并且允许您创建用户字典。

属性存储在不同的系统词典中。属性用于配置条件。属性可以在多个条件中重复使用。

要在创建策略条件时重复使用某个有效的属性，请从包含支持的属性的词典中选择该属性。例如，Cisco ISE 提供名为 AuthenticationIdentityStore 的属性，该属性位于 Networkaccess 目录中。该属性识别验证用户身份期间访问的最后一个身份源：

- 在身份验证期间使用单个身份源时，该属性包括成功进行身份验证所在的身份库的名称。
- 在身份验证期间使用某个身份源序列时，该属性包括访问的最后一个身份源的名称。

您可以将 AuthenticationStatus 属性与 AuthenticationIdentityStore 属性组合使用，以定义用来识别成功验证某个用户的身份的身份源的条件。例如，要使用授权策略中的 LDAP 目录 (LDAP13) 检查用户通过身份验证的条件，您可以定义下列可重复使用的条件：

```
 If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

注释 AuthenticationIdentityStore 表示允许您输入条件数据的文本字段。确保向该字段中正确输入或复制名称。如果身份源的名称发生更改，您必须确保修改此条件，以与身份源的更改保持一致。

要定义基于之前已进行身份验证的终端身份组的条件，Cisco ISE 支持在终端身份组 802.1X 身份验证状态期间定义的授权。当Cisco ISE 执行 802.1X 身份验证时，它从 RADIUS 请求的“Calling-Station-ID”字段中提取 MAC 地址，并使用该值查找和填充设备终端身份组（被定义为 endpointIDgroup 属性）的会话缓存。此过程使 endpointIDgroup 属性在创建授权策略条件时可供使用，并且允许您根据使用该属性的终端身份组信息（用户信息除外）来定义授权策略。

可以在授权策略配置页面的 ID Groups 列中定义终端身份组的条件。需要在授权策略的“Other Conditions”部分中定义基于用户相关信息的条件。如果用户信息基于内部用户属性，请使用内部用户目录中的 ID 组属性。例如，您可以使用诸如“User Identity Group:Employee:US”等值，在身份组中输入完整的值路径。

支持的网络访问策略词典

Cisco ISE 支持以下系统存储的词典，这些词典包含为身份验证和授权策略构建条件和规则时所需的不同属性：

- 系统定义的字典
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS 供应商字典

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- Network access

对于授权策略类型，条件中配置的验证必须符合要返回的授权配置文件。

验证通常包括一个或更多条件，条件中包含用户定义的名称，可以将这些条件添加到库中并供其他策略重复使用。

以下部分介绍可用于配置条件的受支持属性和词典。

字典支持的属性

此表列出字典支持的固定属性，这些属性可用于策略条件中。并非所有这些属性都可用于创建所有类型的条件。

例如，创建在身份验证策略中选取访问服务的条件时，您将只看到以下网络访问属性：Device IP Address、ISE Host Name、Network Device Name、Protocol 和 Use Case。

您可以将下表中列出的属性用于策略条件中。

字典	属性	允许的协议规则和代理	身份规则
设备	Device Type（预定义的网络设备组）	支持	支持
	Device Location（预定义的网络设备组）		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	所有属性	支持	支持

字典	属性	允许的协议规则和代理	身份规则
网络接入	ISE Host Name	支持	支持
	AuthenticationMethod	不支持	支持
	AuthenticationStatus	否	否
	CTSDeviceID	否	否
	Device IP Address	支持	支持
	EapAuthentication（设备用户身份验证期间使用的 EAP 方法）	不支持	支持
	EapTunnel（用于建立隧道的 EAP 方法）	不支持	支持
	Protocol	支持	支持
	UseCase	支持	支持
	UserName	不支持	支持
	WasMachineAuthenticated	否	否

字典	属性	允许的协议规则和代理	身份规则
Certificate	Common Name	不支持	支持
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

系统定义的字典和字典属性

Cisco ISE 会在安装期间创建系统字典，您可以在 System Dictionaries 页面找到这些系统字典。系统定义的字典属性为只读属性。由于其性质，您只能查看现有的系统定义的字典。您不能创建、编辑或删除系统定义的值或系统字典中的任何属性。

所显示的系统定义的字典属性会带有属性的描述性名称、域识别的内部名称和允许的值。

IETF RADIUS 属性集也是系统定义的字典的一部分，由互联网工程任务组 (IETF) 定义，Cisco ISE 也会为此属性集创建字典默认设置。您可以编辑除 ID 之外的所有 IETF RADIUS 自由属性字段。

显示系统字典和字典属性

您无法创建、编辑或删除系统字典中的任何系统定义的属性。您只能查看系统定义的属性。您可以执行基于字典名称和说明的快速搜索或基于您所定义的搜索规则的高级搜索。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **系统 (System)**。

步骤 2 在 System Dictionaries页面上选择系统字典，然后点击 **View**。

步骤 3 点击 **Dictionary Attributes**。

步骤 4 从列表中选择系统字典属性，然后点击 **View**。

步骤 5 点击 **Dictionaries** 链接以返回 System Dictionaries 页面。

用户定义的字典和字典属性

Cisco ISE 显示您在 User Dictionaries 页面中创建的用户定义字典。在系统中创建并保存现有用户字典的 Dictionary Name 或 Dictionary Type 值后，将不能修改这些值。

您可以在 User Dictionaries 页面执行以下操作：

- 编辑和删除用户字典。
- 根据名称和说明搜索用户字典。
- 添加、编辑和删除用户字典中的用户定义的字典属性。
- 使用 NMAP 扫描操作删除 NMAP 扩展名字典中的属性。当在“NMAP 扫描操作”(NMAP Scan Actions) 页面中添加或删除自定义端口时，将在字典中添加、删除或更新对应的自定义端口属性。
- 添加或删除允许的字典属性值

创建用户定义的字典

您可以创建、编辑或删除用户定义的字典。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **用户 (User)**。
步骤 2 点击**添加 (Add)**。
步骤 3 为用户字典输入名称、可选说明和用户字典版本。
步骤 4 从 Dictionary Attribute Type 下拉列表选择属性类型。
步骤 5 点击**提交 (Submit)**。

创建用户定义的字典属性

您可以在用户字典中添加、编辑和删除用户定义的字典属性以及添加或删除用于字典属性的允许值。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **用户 (User)**。
步骤 2 从 User Dictionaries 页面选择用户字典，然后点击**编辑 (Edit)**。
步骤 3 点击 **Dictionary Attributes**。
步骤 4 点击**添加 (Add)**。
步骤 5 为字典属性输入属性名称、可选说明和内部名称。
步骤 6 从 Data Type 下拉列表选择数据类型。
步骤 7 点击**添加 (Add)** 以配置名称、允许值，并在 Allowed Values 表中设置默认状态。
步骤 8 点击**提交 (Submit)**。

RADIUS 供应商字典

Cisco ISE 允许您定义一套 RADIUS 供应商字典并且为每个字典定义一系列属性。列表中的每个供应商定义都包含供应商名称、供应商 ID 和扼要说明。

默认情况下，Cisco ISE 为您提供以下 RADIUS 供应商字典：

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUS 协议支持这些供应商字典以及可用于授权策略和策略条件的供应商特定属性。

创建 RADIUS 供应商字典

还可以创建、编辑、删除、导出和导入 RADIUS 供应商字典。

步骤 1 选择 策略 (Policy) > 策略元素 (Policy Elements) > 词典 (Dictionaries) > 系统 (System) > Radius > Radius 供应商 (Radius Vendors)。

步骤 2 点击添加 (Add)。

步骤 3 输入 RADIUS 供应商字典的名称、可选说明，以及由互连网号码分配机构 (IANA) 批准的 RADIUS 供应商的供应商 ID。

步骤 4 从 Vendor Attribute Type Field Length 下拉列表中选择从属性值提取用于指定属性类型的字节数。有效值为 1、2 和 4。默认值为 1。

步骤 5 从 Vendor Attribute Size Field Length 下拉列表中选择从属性值提取用于指定属性长度的字节数。有效值为 0 和 1。默认值为 1。

步骤 6 点击提交 (Submit)。

创建 RADIUS 供应商字典属性

您可以创建、编辑和删除Cisco ISE 支持的 RADIUS 供应商属性。每个 RADIUS 供应商属性都有名称、数据类型、说明和方向，其指定属性是否仅与请求相关、仅与响应相关，还是与二者都相关。

步骤 1 选择 策略 (Policy) > 策略元素 (Policy Elements) > 词典 (Dictionaries) > 系统 (System) > Radius > Radius 供应商 (Radius Vendors)。

步骤 2 从 RADIUS 供应商字典列表选择 RADIUS 供应商字典，然后点击编辑 (Edit)。

步骤 3 点击字典属性 (Dictionary Attributes)，然后点击添加 (Add)。

步骤 4 为 RADIUS 供应商属性输入属性名称和可选说明。

步骤 5 从 Data Type 下拉列表选择数据类型。

步骤 6 选中 启用MAC选项 (Enable MAC option) 复选框。

步骤 7 从 Direction 下拉列表选择仅应用于 RADIUS 请求、仅应用于 RADIUS 响应或同时应用于二者的方向。

步骤 8 在 ID 字段输入供应商属性 ID。

步骤 9 选中 允许标记 (Allow Tagging) 复选框。

步骤 10 选中 允许配置文件中存在该属性的多个实例 (Allow Multiple Instances of this Attribute in a Profile) 复选框。

步骤 11 点击添加 (Add) 以在“允许的值”(Allowed Values) 表中为供应商属性添加允许的值。

步骤 12 点击提交 (Submit)。

HP RADIUS IETF 服务类型属性

Cisco ISE 为 RADIUS IETF 服务类型属性引入两个新值。此 RADIUS IETF 服务类型属性位于**策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > RADIUS > IETF**在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > RADIUS > IETF**。您可在策略条件中使用这两个值。这两个值专为 HP 设备设计，用于了解用户的权限。

列举名称	列举值
HP-Oper	252
HP-User	255

RADIUS 供应商字典属性设置

本节介绍Cisco ISE 中使用的 RADIUS 供应商字典。

下表介绍了 RADIUS 供应商的“字典”(Dictionary) 窗口中的字段，可以通过此窗口为 RADIUS 供应商配置字典属性。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **系统 (System)** > **RADIUS** > **RADIUS 供应商 (RADIUS Vendors)**。

表 ***128: RADIUS*** 供应商字典属性设置

字段名称	使用指南
属性名称	输入选定 RADIUS 供应商的供应商特定属性名称。
说明	输入供应商特定属性的可选说明。
内部名称	输入数据库内部所称呼的供应商特定属性的名称。
数据类型	为供应商特定属性选择以下其中一种数据类型： • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPv6

字段名称	使用指南
启用MAC选项	选中此复选框可启用将RADIUS属性比作为MAC地址。默认情况下，对于 RADIUS 属性 calling-station-id，此选项标记为启用，您无法禁用此选项。对于 RADIUS 供应商字典中的其他（字符串类型）字典属性，可以启用或禁用此选项。 启用此选项之后，在设置身份验证和授权条件时，可以通过选择Text选项来定义对比是否是明文字符串，或通过选择 MAC address 选项来定义是否是 MAC 地址。
方向	选择一个适用于 RADIUS 消息的选项：
ID	输入供应商属性 ID。有效范围为 0 至 255。
允许标记	根据RFC2868定义，选中该复选框，将属性标记为已被允许带有标签。该标签旨在允许将已建立隧道的用户的属性进行分组。有关详细信息，请参阅 RFC2868。 已标记的属性支持确保有关指定隧道的所有属性在各自的标签字段中包含相同值，并且，每组包含一个 Tunnel-Preference 属性实例。这符合将用于多供应商网络环境中的隧道属性，以此消除不同供应商生产的网络接入服务器 (NAS) 之间的互通性问题。
允许配置文件中存在该属性的多个实例	当希望配置文件中存在此RADIUS供应商特定属性的多个实例时，请选中此复选框。

相关主题

系统定义的字典和字典属性，第 819 页
用户定义的字典和字典属性，第 819 页
RADIUS 供应商字典，第 820 页
创建 RADIUS 供应商字典，第 820 页

浏览 Conditions Studio

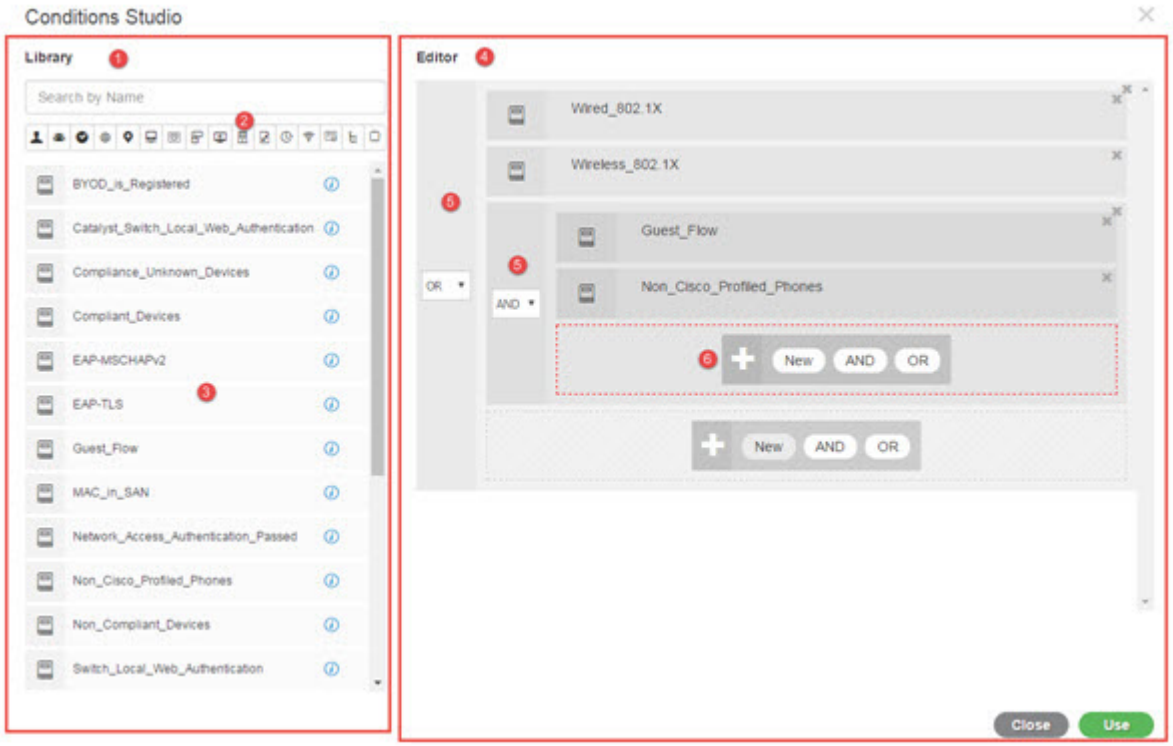
使用 Conditions Studio 创建、管理和重复使用条件。条件可以包括多个规则，并且结构复杂性不限（包括仅一个级别或多个层级）。使用 Conditions Studio 创建新条件时，可以使用已存储在库中的条件块，也可以更新和更改这些存储的条件块。在稍后创建和管理条件时，可以使用快速类别过滤器等轻松查找需要的块和属性。

对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

要编辑或更改已应用于任何策略集中的特定规则的条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击，或者从策略集表中的**条件 (Conditions)** 列点击加号 以创建新列，随后可以立即将其应用于同一策略集，也可以将其保存在库中以供将来使用。

下图显示 Conditions Studio 的主要元素。

图 *41: Conditions Studio*



Condition Studio 分为两个主要部分：库和编辑器。库可以存储条件块以供重复使用，而编辑器可以让您编辑这些已保存的块和创建新的块。

下表介绍了 Condition Studio 的不同部分：

字段	使用指南
库	显示已创建并保存在 ISE 数据库中以供重复使用的所有条件块的列表。若要在当前编辑的条件中使用这些条件块，请将其从库中拖放到编辑器中的相关级别，必要时更新运算符。 存储在库中的条件全部用库图标  表示，原因是条件可以与多个类别相关联。 在库中的每个条件旁，也可以找到该图标。将鼠标悬停在此图标上可查看条件的完整说明，查看其关联的类别，还可以从库中彻底删除条件。如果条件被策略使用，则无法删除这些条件。 将任何库条件拖放到编辑器中，以便将其单独用于当前编辑的策略，或作为更复杂条件的构建块，以便在当前策略中使用或在库中另存为新条件。您还可以在编辑器中拖放条件，以便对该条件进行更改，然后在库中以相同名称或新名称保存该条件。 安装后还有预定义条件。这些条件也可以更改和删除。
搜索和过滤	按名称搜索条件或按类别过滤条件。以类似的方式，还可以从编辑器中的**点击以添加属性 (Click to add an attribute)** 字段搜索和过滤属性。工具栏上的图标代表不同的属性类别，如主题、地址等。点击图标可查看与特定类别相关的属性，而点击类别工具栏中的突出显示图标可取消选择该类别，从而删除过滤器。
条件列表	库中所有条件的完整列表，或库中基于搜索或过滤结果而显示的条件列表。
编辑人	创建要立即使用的新条件，以及要保存在系统库中以供将来使用的新条件，然后编辑现有条件并将这些更改保存在库中以供立即使用和将来使用。 当打开 Conditions Studio 以创建新条件时（点击任意策略集表中的加号），会显示只包含一个空行的编辑器，您可以在其中添加第一个规则。 当编辑器打开并显示空字段时，不会显示任何运算符图标

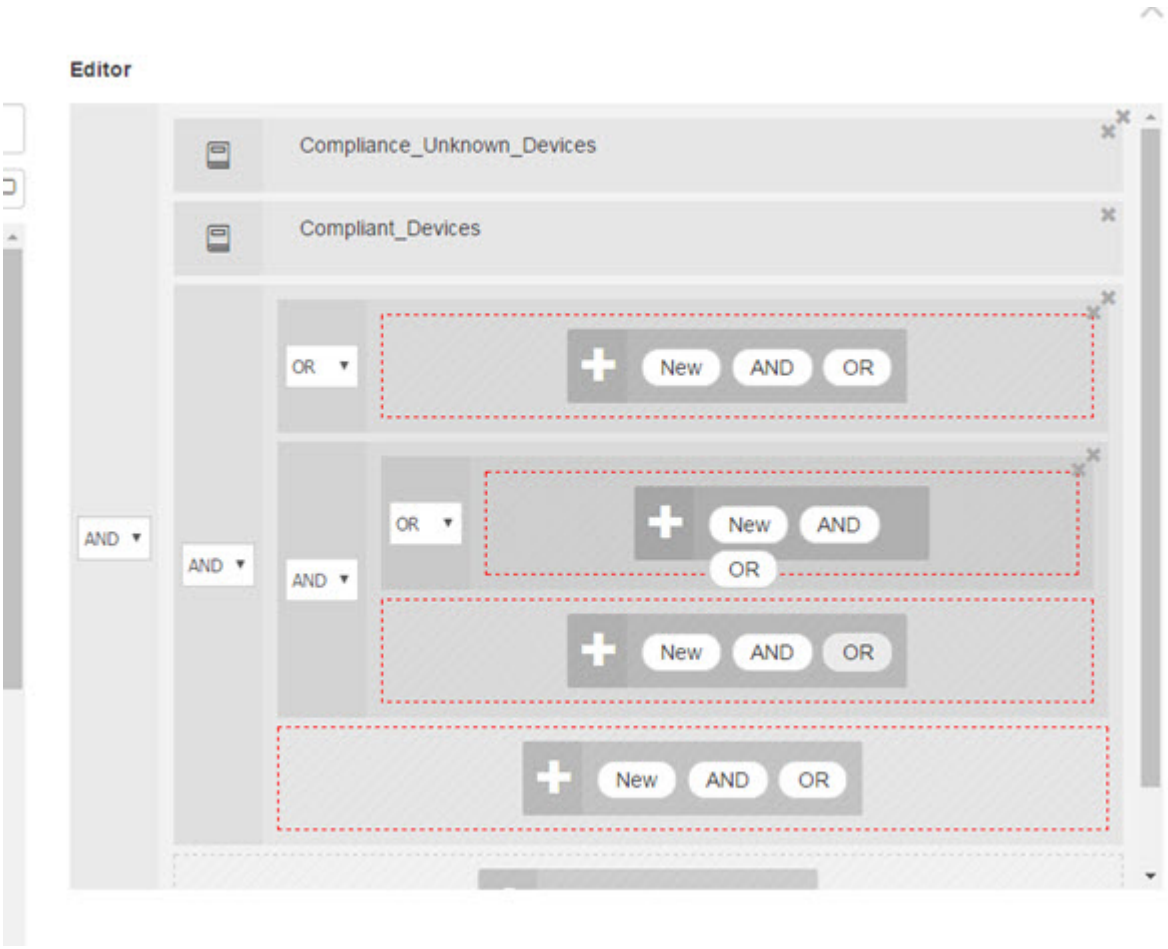
字段	使用指南
	编辑器分为不同的虚拟列和行。 列表示不同的层次结构级别，每列根据其在层次结构中的位置缩进；行代表单个规则。您可以为每个级别创建单个或多个规则，并且可以包含多个级别。 上图中的示例显示了正在构建或编辑的条件，包括规则层次结构，图中的第一级和第二级均标有数字 5。顶级父级别的规则使用运算符 OR。 要在选择运算符并创建层次结构级别后更改该运算符，只需从此列中显示的下拉列表中选择相关选项。 除了运算符下拉列表之外，每个规则在此列中都有一个相关图标，指示其所属的类别。如果将鼠标悬停在图标上，工具提示会指示类别的名称。 一旦保存到库中，系统将为所有条件块分配库图标，替换编辑器中显示的类别图标。 最后，如果将规则配置为**排除**所有相关的匹配项目，则此列中也会显示“不是”(Is-Not) 标志。例如，如果将值为 London 的位置属性设置为“不是”(Is-Not)，则来自伦敦的所有设备都将被拒绝访问。

字段	使用指南
	此区域显示使用层次结构级别以及同一条件中的多个规则时可用的选项。 当将鼠标悬停在任何列或行上时，会显示相关操作。选择操作时，该操作会应用于该部分和所有子部分。例如，当层次结构 A 中有五个级别时，如果从第三级中的任何规则中选择“和”(AND)，则会在原规则下创建新的层次结构 B，以便原规则成为层次结构 B 的父规则，嵌入在层次结构 A 中。 当首次打开 Condition Studio 以从头创建新条件时，编辑器区域仅包含一行（用于您可配置的单个规则），以及用于选择相关运算符或从库中拖放相关条件的选项。 使用**和 (AND)** 和**或 (OR)** 运算符选项可以向条件中添加其他级别。选择**新建 (New)**，可在点击选项的同一级别创建新规则。只有在层次结构的顶层配置至少一个规则后，**新建 (New)** 选项才会显示。

配置、编辑和管理策略条件

使用 Conditions Studio 创建、管理和重复使用条件。条件可以包括多个规则，并且结构复杂性不限（包括仅一个级别或多个层级）。从 Conditions Studio 的编辑器侧管理条件层次结构，如下图所示：

图 42: 编辑器 - 条件层次结构



创建新条件时，可以使用已存储在库中的条件块，也可以更新和更改这些存储的条件块。在创建和管理条件时，可以使用快速类别过滤器等工具轻松找到所需的块和属性。

在创建和管理条件规则时，请使用属性、运算符和值。

Cisco ISE 包含一些最常见用例的预定义复合条件。您可以编辑这些预定义条件来满足您的要求。为重用而保存的条件（包括即用型块）存储在 Condition Studio 的库中，如本任务中所述。

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 访问“策略集”(Policy Sets) 区域。选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

步骤 2 访问 Conditions Studio 以创建新条件并编辑现有条件块，以便随后将这些条件纳入您为特定策略集（及其关联策略和规则）配置的规则中，或保存到库以供将来使用：

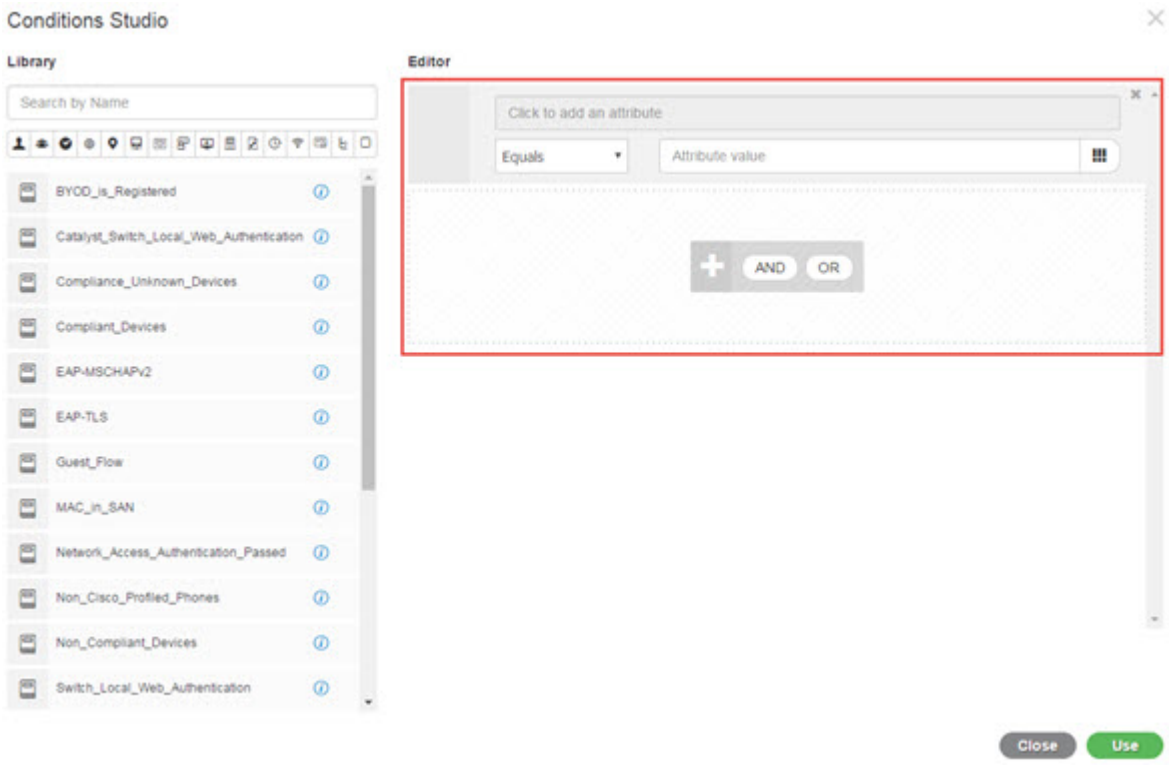
a) 从“策略集”(Policy Set) 主页面上的“策略集”(Policy Set) 表的“**条件**”**(Conditions)** 列中点击 ✚，以创建与整个策略集相关的条件（在匹配身份验证策略规则之前检查的条件）。

b) 或者，从特定策略集行点击 ，以查看“设置”(Set) 视图，包括所有身份验证和授权规则。在“设置”(Set) 视图中，将鼠标悬停在任何规则表的**条件 (Conditions)** 列中的单元格上，然后点击 打开 Conditions Studio。

c) 如果您正在编辑已应用于策略集的条件，请点击 以访问 Conditions Studio。

Conditions Studio 将打开。如果您已打开它来创建新条件，则如下图所示。若要查看字段的说明，以及打开 Conditions Studio 后如何编辑策略集已应用的条件的示例，请参阅浏览 Conditions Studio，第 823 页。

图 *43: Conditions Studio* - 创建新条件



步骤 3 使用库中的现有条件块作为您正在创建或编辑的条件中的规则。

a) 通过从类别工具栏中选择相关类别进行过滤 - 库中显示包含所选类别的属性的所有块。此外，还会显示包含多个规则但至少一个规则中使用了所选类别的属性的条件块。如果添加了其他过滤器，则显示的结果仅包括符合该特定过滤器而且与包含的其他过滤器也匹配的条件块。例如，从工具栏中选择“端口”(Ports) 类别，并在**按名称搜索 (Search by Name)** 字段中输入自由文本“auth”，就会显示与名称中包含“auth”的端口相关的所有块。再次点击类别工具栏中突出显示的图标，取消选择它，从而删除该过滤器。

b) 使用自由文本搜索条件块 - 在**按名称搜索 (Search by Name)** 自由文本字段中，输入要搜索的块名称中出现的任何术语或部分术语。在您键入内容时，系统会实时动态搜索相关结果。如果未选择类别（未突出显示任何图标），则结果包括来自所有类别的条件块。如果已选择类别图标（显示的列表已过滤），则显示的结果仅包括该特定类别中使用特定文本的块。

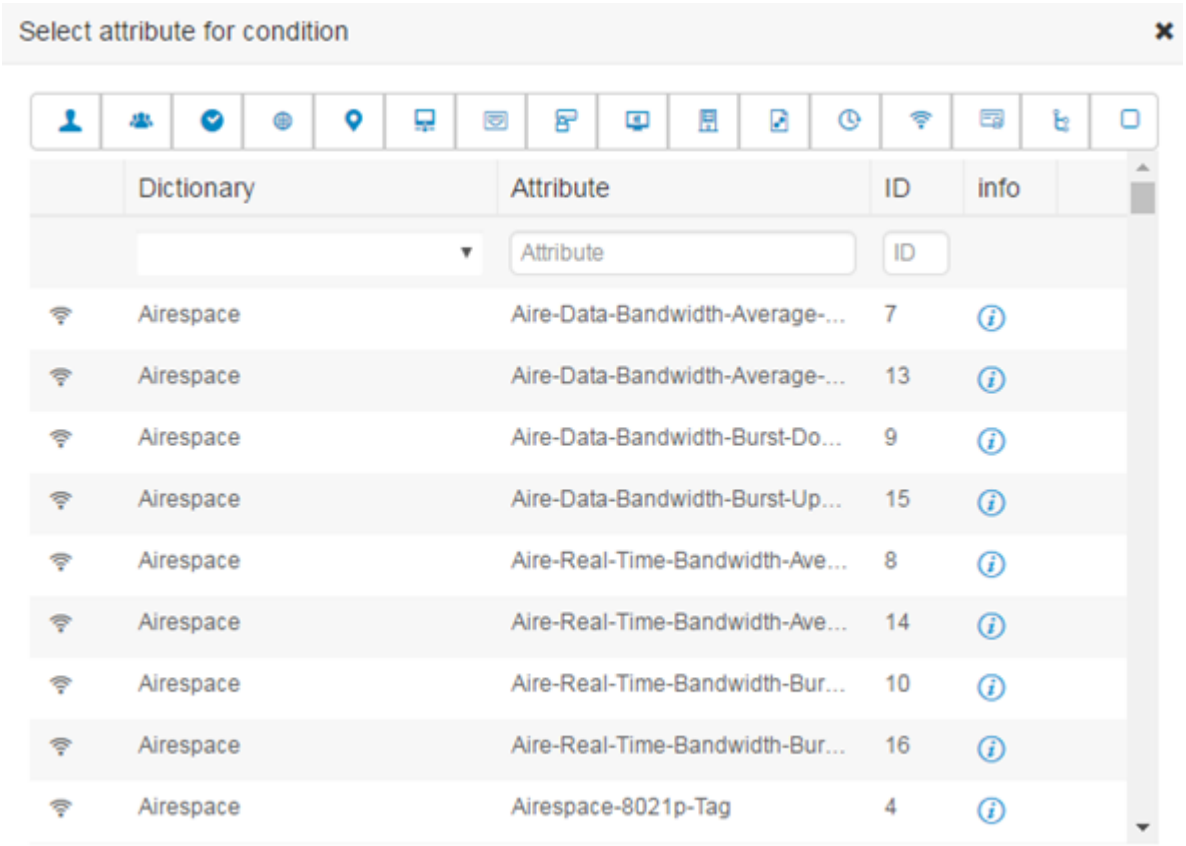
c) 找到条件块后，将其拖到编辑器中，放到要构建的块的正确级别上。如果放置的位置不正确，您可以在编辑器中再次拖放，直至放置正确。

d) 将鼠标悬停在编辑器中的条件块上，然后点击**编辑 (Edit)** 更改规则，以便对处理的条件做出相关的更改，用这些更改覆盖库中的规则，或者在库中将规则另存为新块。

放入编辑器时为只读状态的块现在可以编辑了，并且与编辑器中的所有其他自定义规则具有相同的字段、结构、列表和操作。继续执行后续步骤，了解有关编辑此规则的更多信息。

步骤 4 向当前级别添加运算符，以便随后在同一级别添加其他规则 - 选择 **AND**、**OR** 或 **Set to 'Is not'**。**Set to 'Is not'** 也可应用于单个规则。

步骤 5 使用属性词典创建和编辑规则 - 点击**点击以添加属性**字段。属性选择器随即打开，如下图所示：



属性选择器的各部分如下表所述：

字段	使用指南
属性类别工具栏	包含每个不同属性类别的唯一图标。选择任何属性类别图标，按类别过滤视图。 点击突出显示的图标可取消选择它，从而删除过滤器。
字典	表示存储属性的词典的名称。从下拉列表中选择特定词典，以便按供应商词典过滤属性。
属性	表示属性的名称。在可用字段中为属性名称键入自由文本来过滤属性。在您键入内容时，系统会实时动态搜索相关结果。

字段	使用指南
ID	表示唯一属性标识号。在可用字段中键入 ID 号来过滤属性。在您键入内容时，系统会实时动态搜索相关结果。
信息	将鼠标悬停在相关属性行上的信息图标上可查看有关属性的额外详细信息。

a) 从属性选择器的搜索框中，过滤并搜索所需的属性。在属性选择器的任何部分过滤或输入自由文本时，如果未激活其他过滤器，则结果仅包括与所选过滤器相关的所有属性。如果使用多个过滤器，则显示的搜索结果与所有过滤器匹配。例如，点击工具栏中的“端口”(Port) 图标并在“属性”(Attribute) 列中键入“auth”，则仅显示端口类别中名称含“auth”的属性。选择类别时，工具栏中的图标以蓝色突出显示，并显示过滤后的列表。再次点击类别工具栏中突出显示的图标，取消选择它，从而删除过滤器。

b) 选择相关属性，将其添加到规则中。
属性选择器关闭，您选择的属性会添加到**点击以添加属性 (Click to add an attribute)** 字段。

c) 从**等于 (Equals)** 下拉列表中，选择相关运算符。

不是您选择的所有属性都包含“Equals”、“Not Equals”、“Matches”、“Starts With”或“Not Starts With”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

您必须使用“equals”运算符进行直接比较。“Contains”运算符可用于多值属性。“Matches”运算符应用于正则表达式比较。当使用“Matches”运算符时，将解译正则表达式中的静态值和动态值。

d) 在**属性值 (Attribute value)** 字段中，执行以下操作之一：

- 在字段中键入自由文本值
- 从列表中选择一个动态加载的值（相关时 - 取决于上一步中选择的属性）
- 使用其他属性作为条件规则的值 - 选择字段旁边的表图标以打开属性选择器，然后搜索、过滤并选择相关属性。属性选择器关闭，您选择的属性会添加到**属性值 (Attribute value)** 字段。

步骤 6 在库中将规则另存为条件块。

a) 将鼠标悬停在要在库中另存为块的规则或规则的层次结构上。任何可另存为单个条件块的规则或规则组都将显示**复制 (Duplicate)** 和**保存 (Save)** 按钮。如果要将一组规则另存为块，请在整个层次结构的阻止区域中从整个层次结构的底部选择操作按钮。

b) 点击**保存 (Save)**。系统将弹出“保存条件”(Save condition) 屏幕。

c) 选择:

- 保存到现有库条件 - 选择此选项可使用您创建的新规则覆盖库中的现有条件块，然后在**从列表中选择 (Select from list)** 下拉列表中选择要覆盖的条件块。
- 另存为新库条件 - 在块的“条件名称”(Condition Name) 字段中键入唯一名称。

d) （可选）在**说明 (Description)** 字段中输入说明。当您将鼠标悬停在库中任何条件块的信息图标上时，系统会显示此说明，使您能够快速识别不同的条件块及其用途。

e) 点击**保存 (Save)** 在库中保存条件块。

步骤 7 在新的子级别上创建新规则 - 请点击 **AND** 或 **OR**，在现有父层级和您创建的子层级之间应用正确的运算符。新部分与所选运算符一起添加到编辑器层次结构中，作为提供所选运算符的规则或层次结构的子项。

步骤 8 在当前现有级别上创建新规则 - 从相关级别点击**新建 (New)**。在您开始的同一级别中，将显示新规则的一个空行。

步骤 9 点击 **X** 从编辑器中删除任何条件及其所有子项。

步骤 10 点击**复制 (Duplicate)** 可自动复制并粘贴层次结构中的特定条件，从而在同一级别创建其他相同的子项。您可以复制有或无子项的单个规则，具体取决于您点击**复制 (Duplicate)** 按钮的级别。

步骤 11 点击页面底部的**使用 (Use)** 保存在编辑器中创建的条件，并在策略集中实施该条件。

特殊网络访问条件

本部分说明了在创建策略集时有用的独特条件。这些条件无法从条件 Studio 创建，因此具有其自己的唯一进程。

配置设备网络条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 设备网络条件 (Device Network Conditions)**

步骤 2 点击**添加 (Add)**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 - 您可以添加 IP 地址或子网列表，每行一个。IP 地址/子网可以采用 IPV4 或 IPV6 格式。
- 设备名称 - 您可以添加设备名称列表，每行一个。必须输入在网络设备对象中配置的相同设备名称。
- 设备组 - 可以添加元组列表（按以下顺序）：根 NDG、逗号、（在根 NDG 下的）NDG。必须每行一个元组。

步骤 5 点击**提交 (Submit)**。

配置设备端口网络条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 设备端口网络条件 (Device Port Network Conditions)**

步骤 2 点击**添加 (Add)**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 (IP Addresses) - 按以下顺序输入详细信息：IP 地址或子网、逗号和（设备使用的）端口。必须每行一个元组。
- 设备 (Devices) - 按以下顺序输入详细信息：设备名称、逗号和端口。必须每行一个元组。您必须输入在网络设备对象中配置的相同设备名称。
- 设备组 (Device Groups) - 按以下顺序输入详细信息：根 NDG、逗号、（在根下的）NDG 和端口。必须每行一个元组。

步骤 5 点击**提交 (Submit)**。

配置终端站网络条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 终端站网络条件 (Endstation Network Conditions)**

步骤 2 点击**添加 (Add)**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 - 您可以添加 IP 地址或子网列表，每行一个。IP 地址/子网可以采用 IPV4 或 IPV6 格式。
- MAC 地址 - 您可以输入终端 MAC 地址和目标 MAC 地址的列表，用逗号分隔。每个 MAC 地址必须包含 12 个十六进制数字，且必须为以下格式之一：nn:nn:nn:nn:nn:nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn 或 nnnnnnnnnnnn。

  如果不需要终端站 MAC 或目标 MAC，请使用令牌“-ANY-”代替。
- CLI/DNIS - 您可以添加主叫方 ID (CLI) 和被叫方 ID (DNIS) 的列表，用逗号分隔。如果不需要主叫方 ID (CLI) 或被叫方 ID (DNIS)，请使用令牌“-ANY-”代替。

步骤 5 点击**提交 (Submit)**。

创建时间和日期条件

使用 Policy Elements Conditions 页面显示、创建、修改、删除、复制以及搜索时间和日期策略元素条件。策略元素是共享的对象，定义一个基于您所配置的特定时间和日期属性设置的条件。

使用时间和日期条件，使您可以按照您做出属性设置所指定的特定时间和日期来设置或限制访问Cisco ISE 系统资源的权限。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **通用 (Common)** > **时间和日期 (Time and Date)** > **添加 (Add)**

步骤 2 在字段中输入适当的值。

- 在 Standard Settings 区域中，指定提供访问的时间和日期。
- 在 Exceptions 区域中，指定限制访问的时间和日期。

步骤 3 点击**提交 (Submit)**。

在授权策略中使用 IPv6 条件属性

Cisco ISE 可以检测、管理和保护来自终端的 IPv6 流量。

当一个支持 IPv6 的终端连接至Cisco ISE 网络时，它通过 IPv6 网络与 NAD 通信。NAD 通过 IPv4 网络将来自终端的计费和分析信息（包括 IPv6 值）发送至Cisco ISE。您可以使用规则条件中的 IPv6 属性在Cisco ISE 中配置授权配置文件和策略，以处理来自支持 IPv6 终端的这些请求，并且确保终端合规。

您可以在 IPv6 前缀和 IPv6 接口值中使用通配符。例如：2001:db8:1234::/48。

支持的 IPv6 地址格式包括：

- 完整表示法：冒号分隔的八组四个十六进制数字。例如，2001:0db8:85a3:0000:0000:8a2e:0370:7334
- 缩短表示法：去除组中的前导零；使用两个连续的冒号替换零值组。例如：2001:db8:85a3::8a2e:370:7334
- 点分四组表示法（IPv4 映射和兼容 IPv4 的 Ipv6 地址）：例如，::ffff:192.0.2.128

支持的 IPv6 属性包括：

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address

- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

下表列出了受支持的Cisco属性-值对及其等效 IETF 属性：

Cisco属性值对	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

RADIUS 实时日志页面、RADIUS 身份验证报告、RADIUS 记账报告、当前活动会话报告、RADIUS 错误报告、错误配置的 NAS 报告、、自适应网络控制审核和错误配置的请求方客户端报告均支持 IPv6 地址。您可以从 RADIUS 实时日志页面或通过任何这些报告查看有关这些会话的详细信息。您可以根据 IPv4、IPv6 或 MAC 地址来过滤记录。

注释 如果将一个 Android 设备连接至支持 IPv6 的 DHCPv6 网络，它从 DHCP 服务器仅接收本地链路 IPv6 地址。因此，全局 IPv6 地址不在实时日志和终端页面（**工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**）中显示。

以下步骤描述了如何在授权策略中配置 IPv6 属性。

开始之前

确保在您的部署中网络接入设备 (NAD) 支持具备 IPv6 的 AAA。有关如何在 NAD 上启用 AAA IPv6 支持的信息，请参阅 **AAA IPv6 支持**。

步骤 1 对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

步骤 2 创建授权规则。

步骤 3 创建授权规则时，请从 Conditon Studio 创建条件。在 Condition Studio 中，从 RADIUS 字典中选择 RADIUS IPv6 属性、运算符和值。

步骤 4 点击**保存 (Save)** 以将授权规则保存在策略集中。

策略集用于身份验证的

必须先在Cisco ISE 中定义全局协议设置，然后才能使用这些协议创建、保存和实施策略集。您可以使用 Protocol Settings 页面为 Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 和 Protected Extensible Authentication Protocol (PEAP) 协议定义全局选项，这些协议可以与网络中的其他设备进行通信。

支持的网络访问策略集协议

以下是您在定义网络访问策略集策略时可以选择的协议的列表：

- 密码身份验证协议 (PAP)
- 受保护的可扩展身份验证协议 (PEAP)
- Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)
- 可扩展身份验证协议消息摘要 5 (EAP-MD5)
- 可扩展身份验证协议-传输层安全 (EAP-TLS)
- 可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST)
- 可扩展的身份验证协议-基于隧道的传输层安全 (EAP-TTLS)
- 受保护的可扩展身份验证协议-传输层安全 (PEAP-TLS)

将 EAP-FAST 用作协议的指南

将 EAP-FAST 用作身份验证协议时，请遵循以下规定：

- 在经过身份验证的调配中启用 EAP-FAST 接受客户端证书时，强烈建议启用 EAP-TLS 内部方法。经过身份验证的调配中的 EAP-FAST 接受客户端证书不是一个单独的身份验证方法，而是一种更简短的客户端证书身份验证形式，它使用相同的证书凭证类型来对用户进行身份验证，但是不需要运行内部方法。
- 经过身份验证的调配中的接受客户端证书适用于无PAC完全握手和经过身份验证的PAC调配。它不适用于无 PAC 会话恢复、匿名 PAC 调配和基于 PAC 的身份验证。
- EAP属性按身份显示（所以在EAP链中会显示两次），即使身份验证按照不同的顺序进行，在监控工具的身份验证详细信息中仍然会按照先用户后设备的顺序显示。
- 当使用 EAP-FAST 授权 PAC 时，实时日志中显示的 EAP 身份验证方法等于用于完全身份验证（如在 PEAP 中）而非用于查找的身份验证方法。
- 在 EAP 链接模式中，当隧道 PAC 到期，然后 ISE 退回调配且 AC 请求用户和设备授权 PAC 时 - 无法调配设备授权 PAC。当 AC 请求时，它将在后续基于 PAC 的身份验证对话中进行调配。

- 当为链接配置Cisco ISE 并且为单一模式配置 AC 时，则 AC 使用身份类型 TLV 向 ISE 做出响应。但是，第二个身份的身份验证会失败。您可以通过此对话看到客户端适合执行链接，但当前未为单一模式执行配置。
- Cisco ISE 支持在仅适用于 AD 的 EAP-FAST 链中检索设备和用户的属性与组。对于 LDAP 和内部数据库，ISE 仅使用最后的身份属性。

注释 如果 EAP-FAST 身份验证协议用于 High Sierra、Mojave 或 Catalina MAC OSX 设备，可能会看到“EAP-FAST 加密绑定验证失败”(EAP-FAST cryptobinding verification failed) 消息。我们建议您配置“允许的协议”(Allowed Protocols) 页面中的“首选 EAP 协议”(Preferred EAP Protocol) 字段，以使这些 MAC OSX 设备使用 PEAP 或 EAP-TLS 而非 EAP-FAST。

配置 EAP-FAST 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP Fast 设置 (EAP Fast Settings)**。

步骤 2 按需输入详细信息，定义 EAP-FAST 协议。

步骤 3 如果要调用以前生成的所有主密钥和 PAC，请点击**撤销 (Revoke)**。

步骤 4 点击**保存 (Save)**，保存 EAP-FAST 设置。

为 EAP-FAST 生成 PAC

您可以使用Cisco ISE 中的 Generate PAC 选项为 EAP-FAST 协议生成隧道或计算机 PAC。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)**。

步骤 2 从左侧的 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **EAP-FAST** > **生成 PAC (Generate PAC)**。

步骤 4 根据需要输入用于为 EAP-FAST 协议生成计算机 PAC 的详细信息。

步骤 5 点击**生成 PAC (Generate PAC)**。

EAP-FAST 设置

下表介绍“协议设置”(Protocol Settings) 窗口中的字段，您可以使用此窗口配置 EAP-FAST、EAP-TLS 和 PEAP 协议。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP-FAST 设置 (EAP-FAST Settings)**。

表 *129:* 配置 *EAP-FAST* 设置

字段名称	使用指南
Authority Identity Info Description	输入用于说明向客户端发送凭证的Cisco ISE 节点的用户友好字符串。客户端可以在类型、长度和值 (TLV) 的受保护访问凭证 (PAC) 信息中发现此字符串。默认值为 Identity Services Engine。
Master Key Generation Period	指定主键生成期（以秒、分钟、小时、天或周为单位）。值必须是范围在 1 至 2147040000 秒内的正整数。默认值为 604800 秒，相当于一周。
Revoke all master keys and PACs	点击“撤销”(Revoke) 可撤销所有主键和 PAC。
Enable PAC-less Session Resume	如果您要在没有 PAC 文件的情况下使用 EAP-FAST，请选中此复选框。
PAC-less Session Timeout	指定无 PAC 会话恢复超时的时间（以秒为单位）。默认值为 7200 秒。

相关主题

策略集用于身份验证的，第 836 页
将 EAP-FAST 用作协议的指南，第 836 页
EAP-FAST 的优势，第 879 页
配置 EAP-FAST 设置，第 837 页

PAC 设置

下表介绍“生成 PAC”(Generate PAC) 窗口上的字段，您可以使用此窗口为 EAP-FAST 身份验证配置受保护的访问凭证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **生成 PAC (Generate PAC)**。

表 *130:* 为 *EAP-FAST* 设置生成 *PAC*

字段名称	使用指南
Tunnel PAC	点击此单选按钮生成隧道 PAC。
Machine PAC	点击此单选按钮生成设备 PAC。

字段名称	使用指南
Trustsec PAC	点击此单选按钮生成 Trustsec PAC。
Identity	（针对 Tunnel 和 Machine PAC 身份字段）指定 EAP-FAST 协议显示为“内部用户名”的用户名或设备名称。如果身份字符串与该用户名不匹配，则身份验证失败。 这是主机定义在自适应安全设备 (ASA) 上定义的主机名。身份字符串必须与 ASA 主机名匹配，否则 ASA 无法导入生成的 PAC 文件。 如果生成的是 Trustsec PAC，则 Identity 字段指定 Trustsec 网络设备的设备 ID 并且由 EAP-FAST 协议提供发起方 ID。如果在此处输入的 Identity 字符串与该设备 ID 不匹配，则身份验证失败。
PAC Time to Live	（对于隧道和设备 PAC）请以秒为单位输入 PAC 的到期时间。默认值为 604800 秒，相当于一周。该值必须是介于 1 和 157680000 秒之间的正整数。对于 Trustsec PAC，请以天、周、月或年为单位输入一个值。默认情况下，该值为一年。最小值为一天，最大值为 10 年。
Encryption Key	输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。
Expiration Data	（仅对于 Trustsec PAC）到期日期根据 PAC Time to Live 计算。

相关主题

策略集用于身份验证的，第 836 页
将 EAP-FAST 用作协议的指南，第 836 页
为 EAP-FAST 生成 PAC，第 837 页

将 EAP-TTLS 用作身份验证协议

EAP-TTLS 是对 EAP-TLS 协议功能进行了扩展的两阶段协议。第 1 阶段建立安全隧道，并获取用于在第 2 阶段安全地在服务器与客户端之间隧道化属性的会话密钥。您可以使用在第 2 阶段隧道化的属性通过多种不同机制执行其他身份验证。

Cisco ISE 能够处理各种 TTLS 请求方的身份验证包括：

- Windows 系统上的 AnyConnect 网络访问管理器 (NAM)
- Windows 8.1 本地请求方

- Secure W2（在 MultiOS 上也称为 JoinNow）
- MAC OS X 本地请求方
- IOS 本地请求方
- 基于 Android 的本地请求方
- Linux WPA 请求方

注释 如果需要加密绑定，则必须使用 EAP-FAST 作为内部方法。

配置 EAP-TTLS 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-TTLS**。

步骤 2 在“EAP-TTLS 设置”(EAP-TTLS Settings) 页面输入所需的详细信息。

步骤 3 点击**保存 (Save)**。

EAP-TTLS 设置

下表介绍“EAP-TTLS 设置”(EAP-TTLS Settings) 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-TTLS**。

表 *131: EAP-TTLS* 设置

字段名称	使用指南
Enable EAP-TTLS Session Resume	如果您选中此复选框，Cisco ISE 将缓存在 EAP-TTLS 身份验证第一阶段创建的 TLS 会话，前提是用户在 EAP-TTLS 第二阶段成功通过身份验证。如果用户需要重新连接而且原来的 EAP-TTLS 会话尚未超时，Cisco ISE 使用缓存的 TLS 会话，从而加快 EAP-TTLS 性能、降低 AAA 服务器负载。 注释 当 EAP-TTLS 会话恢复时，跳过内部验证方法。

字段名称	使用指南
EAP-TTLS Session Timeout	指定 EAP-TTLS 会话在多少秒的时间后超时。默认值为 7200 秒。

相关主题

策略集用于身份验证的，第 836 页
将 EAP-TTLS 用作身份验证协议，第 839 页
配置 EAP-TTLS 设置，第 840 页

配置 EAP-TLS 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-TLS**。

步骤 2 根据需要输入详细信息可定义 EAP-TLS 协议。

步骤 3 点击**保存 (Save)** 保存 EAP-TLS 设置。

EAP-TLS 设置

下表介绍了“EAP-TLS 设置”(EAP-TLS Settings) 窗口上的字段，可以使用此窗口配置 EAP-TLS 协议设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-TLS**。

表 *132: EAP-TLS* 设置

字段	使用指南
Enable EAP-TLS Session Resume	选中此复选框可通过完全 EAP - TLS 认证用户的行为。此功能仅使用安全套接字层(SSL)握手（而不使用证书）对用户提供重新身份验证。只有在 EAP-TLS 会话未超时的情况下，EAP-TLS 会话才会重新运行。
EAP-TLS Session Timeout	指定 EAP-TLS 会话在多少秒的时间后超时。默认值为 7200 秒。
无状态会话恢复	
Master Key Generation Period	输入主键重新生成前经过的时间。此值确定主键保持活动的持续时间。您可以输入以秒、分钟、小时、天或周为单位的值。

字段	使用指南
Revoke	点击**撤销 (Revoke)** 以取消以前生成的所有主键和票证。此选项在辅助节点上禁用。

相关主题

策略集用于身份验证的，第 836 页
配置 EAP-TLS 设置，第 841 页

配置 PEAP 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)**。

步骤 2 从左侧的 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **PEAP**。

步骤 4 根据需要，输入详细信息以定义 PEAP 协议。

步骤 5 点击**保存 (Save)** 以保存 PEAP 设置。

PEAP 设置

下表列出“PEAP 设置”(PEAP Settings) 窗口上的字段，您可以使用此窗口配置 PEAP 协议设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **PEAP**。

表 *133: PEAP* 设置

字段名称	使用指南
Enable PEAP Session Resume	选中此复选框，使Cisco ISE 缓存在 PEAP 身份验证的第一阶段创建的 TLS 会话，前提是用户在 PEAP 的第二阶段成功通过身份验证。如果用户需要重新连接，原始 PEAP 会话尚未超时，Cisco ISE 使用缓存的 TLS 会话，从而加快 PEAP 性能、降低的 AAA 服务器的负载。您必须指定 PEAP 会话恢复功能的 PEAP 会话超时值可以工作。
PEAP Session Timeout	指定 PEAP 会话超时的时间（单位：秒）。默认值为 7200 秒。

字段名称	使用指南
Enable Fast Reconnect	选中此复选框，允许在Cisco ISE 中恢复 PEAP 会话，而无需在启用会话恢复功能时检查用户凭证。

相关主题

策略集用于身份验证的，第 836 页
配置 PEAP 设置，第 842 页
使用 PEAP 的优势，第 878 页
PEAP 协议支持的请求方，第 878 页
PEAP 协议流程，第 878 页

配置 RADIUS 设置

您可以配置 RADIUS 设置，以检测未能通过身份验证的客户端，并禁止重复报告成功的身份验证。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)**。

步骤 2 在 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **RADIUS**。

步骤 4 输入定义 RADIUS 设置所需的详细信息。

步骤 5 点击**保存 (Save)**，保存设置。

RADIUS 设置

下表介绍“RADIUS 设置”(RADIUS Settings) 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **RADIUS**。

如果启用**抑制重复失败的客户端 (Suppress Repeated Failed Clients)** 选项，系统会从审核日志中抑制身份验证重复失败的客户端，并在指定的时间段内自动拒绝来自这些客户端的请求。您还可以指定身份验证失败的次数，在此之后应拒绝来自这些客户端的请求。例如，如果此值配置为 5，当客户端身份验证失败五次时，将在配置的时间段内拒绝从该客户端收到的所有请求。

注释 如果身份验证失败的原因是输入了错误的密码，则不会抑制客户端。

注释 如果配置RADIUS失败抑制，则在配置RADIUS日志抑制后，仍可能会收到错误“5440终端已放弃会话并启动了新会话”(5440 Endpoint Abandoned EAP Session and started a new one)。有关详细信息，请参阅以下 ISE 社区帖子：

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

。

表 *134: RADIUS* 设置

字段名称	使用指南
抑制重复失败的客户端 (Suppress Repeated Failed Clients)	
抑制重复失败的客户端 (Suppress Repeated Failed Clients)	选中此复选框可抑制因相同原因导致身份验证重复失败的客户端。系统会从审核日志中抑制这些客户端，如果已启用**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 选项，还会在指定时间段内拒绝来自这些客户端的请求。
检测两次失败的时间范围 (Detect Two Failures Within)	输入以分钟为单位的时间间隔。如果客户端在该时间段内因相同原因导致两次身份验证失败，则系统会从审核日志中将其抑制，并且，如果已启用**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 选项，还会拒绝来自此客户端的请求。
每几分钟报告一次故障 (Report Failures Once Every)	以分钟为单位输入报告失败身份验证的时间间隔。例如，如果此值设置为 15 分钟，则每 15 分钟在审核日志中仅报告一次重复身份验证失败的客户端，从而防止过度报告。
拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)	选中此复选框可自动拒绝来自身份验证重复失败的客户端的RADIUS请求。您可以启用此选项，以避免Cisco ISE进行不必要的处理，并防范潜在的拒绝服务攻击。
自动拒绝前的失败次数 (Failures Prior to Automatic Rejection)	输入身份验证失败次数，超过此次数后，会自动拒绝来自重复失败客户端的请求。在配置的时间段内（在**持续拒绝请求的时长 (Continue Rejecting Requests for)** 字段中指定），系统会自动拒绝从这些客户端收到的所有请求。在该间隔到期后，系统会处理来自这些客户端的身份验证请求。
持续拒绝请求的时长 (Continue Rejecting Requests for)	输入一个时间间隔（分钟），在此间隔内会拒绝来自重复失败客户端的请求。

字段名称	使用指南
忽略重复记账更新的时间范围 **(Ignore Repeated Accounting Updates Within)**	在此期间内发生的重复记账更新将被忽略。
抑制成功报告 **(Suppress Successful Reports)**	
Suppress Repeated Successful Authentications	选中此复选框以防重复报告前 24 小时内在身份情景、网络设备和授权方面没有变更的成功身份验证。
身份验证详细信息 **(Authentications Details)**	
突出显示长于该值的步骤 **(Highlight Steps Longer Than)**	以毫秒为单位输入时间间隔。如果单个步骤的执行超出指定阈值，则在身份验证详细信息页面中使用时钟图标来标记此步骤。
检测 **RADIUS** 请求的高速率 **(Detect High Rate of RADIUS Requests)**	
检测 **RADIUS** 请求的稳定高速率 **(Detect Steady High Rate of Radius Requests)**	选中此复选框可在超过 **RADIUS 请求持续时间 (Duration of RADIUS requests)** 字段和 **RADIUS 请求总数 (Total number of RADIUS requests)** 字段中指定的限制时，发出高 RADIUS 请求负载警报。
RADIUS 请求持续时间 **(Duration of RADIUS Requests)**	输入将用于计算 RADIUS 速率的时间段（以秒为单位）。默认值为 60 秒。有效范围为 20 至 86400 秒。
RADIUS 请求总数 **(Total Number of RADIUS Requests)**	输入将用于计算 RADIUS 速率的请求限制。默认为 72000 个请求。有效范围为 24000 到 103680000 个请求。
RADIUS UDP 端口 **(RADIUS UDP Ports)**	
身份验证端口 **(Authentication Ports)**	指定将用于 RADIUS UDP 身份验证流程的端口。您可以指定最多 4 个端口号（用逗号分隔）。默认情况下，使用端口 1812 和端口 1645。有效范围为 1024 到 65535。
记帐端口 **(Accounting Ports)**	指定将用于 RADIUS UDP 记帐流程的端口。您可以指定最多 4 个端口号（用逗号分隔）。默认情况下，使用端口 1813 和端口 1646。有效范围为 1024 到 65535。 注释　确保其他服务未使用这些端口。
RADIUS DTLS	

字段名称	使用指南
身份验证和记账端口 (Authentication and Accounting Port)	指定将用于 RADIUS DTLS 身份验证和记帐流程的端口。默认情况下，使用端口 2083。有效范围为 1024 到 65535。 **注释** 确保其他服务未使用此端口。
空闲超时 （Idle Timeout）	如果没有从网络设备收到数据包，请输入希望 Cisco ISE 在关闭 TLS 会话之前等待的时间（以秒为单位）。默认值为 120 秒。有效范围为 60 至 600 秒。
启用 RADIUS/DTLS 客户端身份验证 (Enable RADIUS/DTLS Client Identity Verification)	如果希望Cisco ISE 在 DTLS 握手期间验证 RADIUS/DTLS 客户端的身份，请选中此复选框。如果客户端身份无效，则Cisco ISE 握手失败。默认网络设备会跳过身份检查（如果已配置）。身份检查按以下顺序执行： **1.** 如果客户端证书包含使用者备用名称 (SAN) 属性： • 如果 SAN 包含 DNS 名称，则证书中指定的 DNS 名称会与为Cisco ISE 中的网络设备配置的 DNS 名称进行比较。 • 如果 SAN 包含 IP 地址（且不包含 DNS 名称），则证书中指定的 IP 地址会与 Cisco ISE 中配置的所有设备 IP 地址进行比较。 **2.** 如果证书不包含 SAN，则使用者 CN 会与为 Cisco ISE 中的网络设备配置的 DNS 名称进行比较。如果不匹配，则Cisco ISE 握手失败。

相关主题

策略集用于身份验证的 ， 第 836 页
思科 ISE 中的 RADIUS 协议支持 ， 第 852 页
配置 RADIUS 设置 ， 第 843 页

配置安全设置

要配置安全设置：

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全设置 (Security Settings)**。

步骤 2 在“安全设置”(Security Settings) 页面上，选择所需的选项：

- **Allow TLS 1.0 (允许 TLS 1.0)**：在以下工作流程中允许 TLS 1.0 用于与以下传统对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端
- **Allow TLS 1.1 (允许 TLS 1.1)**：在以下工作流程中允许 TLS 1.1 用于与以下传统对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端
- **允许 SHA1 密码 (Allow SHA1 Ciphers)**：在以下工作流程中允许 SHA-1 密码用于与对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 配置为 RADIUS DTLS 服务器
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

  您可以选择以下其中一个选项：
  - **允许所有 SHA-1 密码**
  - **仅允许 TLS_RSA_with_AES_128_CBC_SHA**

  注释 我们建议使用 SHA-256 或 SHA-384 密码以增强安全性。
- **允许 ECDHE-RSA 密码 (Allow ECDHE-RSA Ciphers)**：在以下工作流程中允许 ECDHE-RSA 密码用于与对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 配置为 RADIUS DTLS 服务器
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端

- Cisco ISE 配置为安全 LDAP 客户端

- **允许 3DES 密码 (Allow 3DES Ciphers)**：在以下工作流程中允许 3DES 密码用于与对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 配置为 RADIUS DTLS 服务器
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

- **接受证书而不验证用途 (Accept Certificates without Validating Purpose)**：当 ISE 充当 EAP 或 RADIUS DTLS 服务器时，系统会接受客户端证书，而不检查密钥使用扩展是否包含用于 ECDHE-ECDSA 密码的 keyAgreement 位或用于其他密码的 keyEncipherment 位。

- **允许 DSS 密码用于作为客户端的 ISE (Allow DSS ciphers for ISE as a client)**：当Cisco ISE 充当客户端时，在以下工作流程中允许使用 DSS 密码与服务器通信：
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

- **允许传统的不安全 TLS 重新协商用于作为客户端的 ISE (Allow Legacy Unsafe TLS Renegotiation for ISE as a Client)**：在以下工作流程中允许与不支持安全 TLS 重新协商的传统 TLS 服务器通信：
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

步骤 3 **披露无效用户名 (Disclose invalid usernames)**：默认情况下，对于因用户名不正确而导致的身份验证失败，ISE 会显示无效。为了帮助进行调试，此选项会强制 ISE 在报告中披露（显示）用户名，而不是无效。无论是否选中此选项，对于因用户名不正确而导致的身份验证失败，始终会显示用户名。

当启用**披露无效用户名 (Disclose invalid usernames)** 时，必须选择**始终显示无效用户名 (Always show invalid usernames)**或**在特定时间内显示无效用户名 (Show invalid usernames for a specific time)**。当选择时间选项时，请以分钟为单位选择时间，最多一个月（43,200 分钟）。

此功能适用于 Active Directory、内部用户、LDAP 和 ODBC 身份源。其他身份存储库（如 RADIUS 令牌、RSA 或 SAML）不支持此功能。对于这些身份库，错误输入的用户名始终报告为“无效”。

步骤 **4** 点击**保存 (Save)**。

支持的密码套件

Cisco ISE 支持 TLS 版本 1.0、1.1 和 1.2。

Cisco ISE 支持 RSA 和 ECDSA 服务器证书。支持以下椭圆曲线：

- secp256r1
- secp384r1
- secp521r1

下表列出了支持的密码套件：

密码套件	当思科 **ISE** 配置为 **EAP** 服务器时 当思科 **ISE** 配置为 **RADIUS DTLS** 服务器时	当思科 **ISE** 从 **HTTPS** 或安全 **LDAP** 服务器下载 **CRL** 时 当思科 **ISE** 配置为安全系统日志客户端或安全 **LDAP** 客户端时 当思科 **ISE** 配置为 **CoA** 的 **RADIUS DTLS** 客户端时
TLS 1.0 支持	当允许 TLS 1.0 时 （DTLS 服务器仅支持 DTLS 1.2） 默认情况下，在Cisco ISE 2.3 及更高版本中，“允许 TLS 1.0”选项 (Allow TLS 1.0) 选项处于禁用状态。当禁用此选项时，基于 TLS 的 EAP 身份验证方法（EAP-TLS、EAP-FAST/TLS）和 802.1X 请求方不支持 TLS 1.0。如果要在 TLS 1.0 中使用基于 TLS 的 EAP 身份验证方法，请选中**安全设置 (Security Settings)**窗口中的“允许 TLS 1.0”(Allow TLS 1.0) 复选框。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **安全设置 (Security Settings)**。	当允许 TLS 1.0 时 （DTLS 客户端仅支持 DTLS 1.2）
TLS 1.1 支持	当允许 TLS 1.1 时	当允许 TLS 1.1 时

ECC DSA 密码		
ECDHE-ECDSA-AES256-GCM-SHA384	支持	支持
ECDHE-ECDSA-AES128-GCM-SHA256	支持	支持
ECDHE-ECDSA-AES256-SHA384	支持	支持
ECDHE-ECDSA-AES128-SHA256	支持	支持
ECDHE-ECDSA-AES256-SHA	当允许 SHA-1 时	当允许 SHA-1 时
ECDHE-ECDSA-AES128-SHA	当允许 SHA-1 时	当允许 SHA-1 时
ECC RSA 密码		
ECDHE-RSA-AES256-GCM-SHA384	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES128-GCM-SHA256	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES256-SHA384	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES128-SHA256	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES256-SHA	当允许 ECDHE-RSA/SHA-1 时	当允许 ECDHE-RSA/SHA-1 时
ECDHE-RSA-AES128-SHA	当允许 ECDHE-RSA/SHA-1 时	当允许 ECDHE-RSA/SHA-1 时
DHE RSA 密码		
DHE-RSA-AES256-SHA256	不支持	支持
DHE-RSA-AES128-SHA256	不支持	支持
DHE-RSA-AES256-SHA	否	当允许 SHA-1 时
DHE-RSA-AES128-SHA	否	当允许 SHA-1 时
RSA 密码		
AES256-SHA256	支持	支持
AES128-SHA256	支持	支持
AES256-SHA	当允许 SHA-1 时	当允许 SHA-1 时
AES128-SHA	当允许 SHA-1 时	当允许 SHA-1 时
3DES 密码		

DES-CBC3-SHA	当允许 3DES / SHA-1 时	当启用 3DES/DSS 和 SHA-1 时
DSS 密码		
DHE-DSS-AES256-SHA	否	当启用 3DES/DSS 和 SHA-1 时
DHE-DSS-AES128-SHA	否	当启用 3DES/DSS 和 SHA-1 时
EDH-DSS-DES-CBC3-SHA	否	当启用 3DES/DSS 和 SHA-1 时
弱 RC4 密码		
RC4-SHA	当“允许的协议”（Allowed Protocols）页面中启用“允许弱密码”（Allow weak ciphers）选项且允许 SHA-1 时	否
RC4-MD5	当“允许的协议”（Allowed Protocols）页面中启用“允许弱密码”（Allow weak ciphers）选项时	否
仅 EAP-FAST 匿名调配： ADH-AES-128-SHA	支持	不支持
对等证书限制		
验证 KeyUsage	对于以下密码，客户端证书应具有 KeyUsage=密钥协议和 ExtendedKeyUsage=客户端身份验证： • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

验证 ExtendedKeyUsage	对于以下密码，客户端证书应具有 KeyUsage=密钥加密和 ExtendedKeyUsage=客户端加密： • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	服务器证书应具有 ExtendedKeyUsage=服务器身份验证

思科 ISE 中的 RADIUS 协议支持

RADIUS 是一个客户端/服务器协议，通过该协议，远程访问服务器与中央服务器发生通信，对拨入用户进行身份验证，并对拨入用户所请求的系统或服务的访问进行授权。您可以在所有远程服务器可共享的中央数据库中使用 RADIUS 维护用户配置文件。此协议提供更高的安全性，并且您可以使用它来设置策略以应用于单个管理的网络点。

RADIUS 还可以在Cisco ISE 中用作 RADIUS 客户端以代理远程 RADIUS 服务器的请求，并且它还可在活动会话期间提供授权更改 (CoA)。

Cisco ISE 依据 RFC 2865 对 RADIUS 协议流程提供支持，并广泛支持所有 RADIUS 常规属性（如 RFC 2865 及其扩展中所描述）。Cisco ISE 支持仅解析在Cisco ISE 字典中定义的供应商特定属性。

RADIUS 接口支持下述在 RFC 2865 中定义的属性数据类型：

- 文本（Unicode 转换格式 [UTF]）
- 字符串（二进制）
- 地址 (IP)
- 整数
- 时间

ISE 社区资源

有关Cisco ISE 支持的网络访问属性的信息，请参阅 ISE 网络访问属性。

允许的协议

下表介绍**允许的协议 (Allowed Protocols)** 窗口中的字段，您可以使用此窗口配置身份验证过程中要使用的协议。 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)**。

表 *135:* 允许的协议

字段名称	使用指南
允许的协议 > 身份验证旁路	
流程主机查找	如果希望Cisco ISE 处理主机查询请求，请选中此复选框。当 RADIUS 服务类型等于 10 (呼叫-检查）且用户名等于呼叫 - 站 - ID 时，对于 PAP/CHAP 协议，会对主机查询请求进行处理。当服务类型等于 1（框到的）且用户名等于呼叫 - 站 - ID 时，对于 EAP-MD5 协议，会对主机查询请求进行处理。如果您希望Cisco ISE 忽略主机查找请求并使用系统用户名属性的原始值进行身份验证，请取消选中此复选框。当取消选中时，系统会根据协议（例如 PAP）进行消息处理。 注释 禁用此选项可能会导致现有 MAB 身份验证失败。
允许的协议 > 身份验证协议	
Allow PAP/ASCII	此选项可启用 PAP/ASCII。PAP 使用明文密码（即，未加密的密码），并且是最不安全的身份验证协议。
允许 **CHAP (Allow CHAP)**	此选项可启用 CHAP 身份验证。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。
允许 **MS-CHAPv1 (Allow MS-CHAPv1)**	选中此复选框可启用 MS-CHAPv1。
允许 **MS-CHAPv2 (Allow MS-CHAPv2)**	选中此复选框可启用 MS-CHAPv2。
允许 **EAP-MD5 (Allow EAP-MD5)**	选中此复选框可启用基于 EAP 的 MD5 密码散列身份验证。

字段名称	使用指南
允许 EAP-TLS (Allow EAP-TLS)	选中此复选框可启用EAP-TLS身份验证协议并配置 EAP-TLS 设置。您可以指定Cisco ISE 将如何按照来自最终用户客户端的EAP身份响应中的说明对用户身份进行验证。用户身份根据最终用户客户端提供的证书中的信息进行验证。在Cisco ISE 与最终用户客户端之间建立 EAP-TLS 隧道后，会发生此比较。 **注释** EAP-TLS是基于证书的身份验证协议。仅在您已完成配置证书的所需步骤后，才能发生 EAP-TLS 身份验证。 • **在授权策略中允许过期证书的身份验证以允许证书续订 (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy)** 复选框：如果要允许用户续订证书，请选中此复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。 • **启用无状态会话恢复 (Enable Stateless Session Resume)**：选中此复选框可允许恢复EAP-TLS会话，而无需将会话状态存储在服务器上。Cisco ISE 支持 RFC 5077 中所述的会话票证扩展。Cisco ISE创建一个票证并将其发送到EAP-TLS客户端。客户端向ISE提供票证以恢复会话。 • **主动会话票证更新 (Proactive Session Ticket update)**：输入一个百分比值，以表示会话票证更新之前必须经过的有效时间 (TTL)。例如，如果您输入的值为 60，则在经过 TTL 的 60% 后更新会话票证。 • **会话票证有效时间 (Session ticket Time to Live)**：输入会话票证过期前所经过的时间。此值可确定会话票证保持活动状态的持续时间。您可以输入以秒、分钟、小时、天或周为单位输入值。
允许 LEAP (Allow LEAP)	选中此复选框可启用轻量级可扩展身份验证协议 (LEAP) 身份验证。

字段名称	使用指南
允许 **PEAP (Allow PEAP)**	

字段名称	使用指南

	选中此复选框可启用PEAP身份验证协议和PEAP设置。默认内部方法为 MS-CHAPv2。
	
	当选中“允许 PEAP”(Allow PEAP) 复选框时，您可以配置以下 PEAP 内部方法：
	
	• **允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE支持密码更改。
	  • **重试尝试数 (Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。
	
	• **允许 EAP-GTC (Allow EAP-GTC)**：选中此复选框可使用 EAP-GTC 作为内部方法。
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE支持密码更改。
	  • **重试尝试数 (Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效范围为 0 到 3。
	
	• **允许 EAP-TLS (Allow EAP-TLS)**：选中此复选框可使用 EAP-TLS 作为内部方法。
	
	如果要允许用户更新证书，请选中**允许过期证书的身份验证以允许身份验证策略中的证书更新 (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy)** 复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。
	
	• **需要加密的 TLV (Require Cryptobinding TLV)**：如果希望 EAP 对等体和 EAP 服务器都参与 PEAP 身份验证的内部和外部 EAP 身份验证，则选中此复选框。
	
	• **仅对传统客户端允许 PEAPv0 (Allow PEAPv0 Only for Legacy Clients)**：选中此复选框可

字段名称	使用指南
	允许 PEAP 请求方使用 PEAPv0 进行协商。某些传统客户端不符合 PEAPv1 协议标准。要确保不丢弃此类 PEAP 对话，请选中此复选框。

字段名称	使用指南
允许 **EAP-FAST (Allow EAP-FAST)**	

字段名称	使用指南

	选中此复选框可启用 EAP-FAST 身份验证协议和 EAP-FAST 设置。EAP-FAST 协议可以在同一服务器上支持多个内部协议。默认内部方法为 MS-CHAPv2。
	
	当选中“允许 EAP-FAST”(Allow EAP-FAST) 复选框时，您可以将 EAP-FAST 配置为内部方法：
	
	• **允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE 支持密码更改。
	  • **重试尝试数 (Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。
	
	• **Allow EAP-GTC**
	
	允许密码更改 (Allow Password Change)：选中此复选框可使Cisco ISE 支持密码更改。
	
	重试尝试数 (Retry Attempts)：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。
	
	• **使用 PAC (Use PACs)**：选中此选项可配置 Cisco ISE 以便为 EAP-FAST 客户端调配授权受保护访问凭证 (PAC)。系统显示其他 PAC 选项。
	
	• **不使用 PAC (Don't Use PACs)**：选择此选项可配置Cisco ISE 以使用 EAP-FAST，而不发出或接受任何隧道或计算机 PAC。系统会忽略对 PAC 的所有请求，并且Cisco ISE 会在没有 PAC 的情况下使用 Success-TLV 进行响应。
	
	当选择此选项时，您可以将Cisco ISE 配置为执行计算机身份验证。
	
	• **允许 EAP-TLS (Allow EAP-TLS)**：选中此复选框可使用 EAP-TLS 作为内部方法。
	
	如果要允许用户更新证书，请选中**允许过期证书的身份验证以允许身份验证策略中的证书更新 (Allow authentication of expired**

字段名称	使用指南
	certificates to allow certificate renewal in Authorization Policy) 复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。 • **启用 EAP 链接 (Enable EAP Chaining)**：选中此复选框可启用 EAP 链接。 EAP 链接允许Cisco ISE 将用户和计算机身份验证的结果相关联，并且使用 EAPChainingResult 属性应用相应的授权策略。 EAP 链接要求请求方在客户端设备上支持 EAP 链接。选择请求方中的“用户和计算机身份验证”(User and Machine Authentication) 选项。 当选择 EAP-FAST 协议（二者均处于基于 PAC 的模式和无 PAC 模式下）时，EAP 链接可用。 对于基于 PAC 的身份验证，您可以使用用户授权 PAC 和/或计算机授权 PAC 跳过内部方法。 对于基于证书的身份验证，如果您为 EAP-FAST 协议启用“接受客户端调配证书”(Accept Client Certificate for Provisioning) 选项（在允许的协议服务中），并且如果终端 (AnyConnect) 配置为在隧道内发送用户证书，则在隧道建立过程中，ISE 会使用证书对用户进行身份验证（跳过内部方法），而计算机身份验证会通过内部方法来完成。如果未配置这些选项，则 EAP-TLS 会用作用于进行用户身份验证的内部方法。 在您启用 EAP 链接后，使用 NetworkAccess:EapChainingResult 属性更新授权策略并添加条件，然后分配相应的权限。

字段名称	使用指南

允许 **EAP-TTLS (Allow EAP-TTLS)**	选中此复选框可启用 EAP-TTLS 协议。
	您可以配置以下内部方法：
	• 允许 **PAP/ASCII (Allow PAP/ASCII)**：选中此复选框可使用 PAP/ASCII 作为内部方法。可以使用 EAP-TTLS PAP 进行基于令牌和基于 OTP 的身份验证。
	• 允许 **CHAP (Allow CHAP)**：选中此复选框可使用 CHAP 作为内部方法。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。
	• 允许 **MS-CHAPv1 (Allow MS-CHAPv1)**：选中此复选框可使用 MS-CHAPv1 作为内部方法。
	• 允许 **MS-CHAPv2 (Allow MS-CHAPv2)**：选中此复选框可使用 MS-CHAPv2 作为内部方法。
	• 允许 **EAP-MD5 (Allow EAP-MD5)**：选中此复选框可使用 EAP-MD5 作为内部方法。
	• 允许 **EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。
	  • 允许密码更改 **(Allow Password Change)**：选中此复选框可使Cisco ISE 支持密码更改。
	  • 重试尝试数 **(Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。

字段名称	使用指南
允许 **TEAP (Allow TEAP)**	

字段名称	使用指南

	选中此复选框可启用隧道可扩展身份验证协议 (TEAP) 并配置 TEAP 设置。TEAP 是一种基于隧道的 EAP 方法，可通过使用传输层安全 (TLS) 协议建立隧道，实现对等体和服务器之间的安全通信。类型长度值 (TLV) 对象在 TEAP 隧道内用于在 EAP 对等体和 EAP 服务器之间传输与身份验证相关的数据。
	
	您可以为 TEAP 配置以下内部方法：
	
	• **允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。
	
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE 支持密码更改。
	
	  • **重试次数 (Retries)**：输入Cisco ISE 在显示登录失败消息之前允许用户输入凭证的次数。有效范围为 0 到 3。
	
	• **允许 EAP-TLS (Allow EAP-TLS)**：选中此复选框可使用 EAP-TLS 作为内部方法。
	
	  • **在授权策略中允许过期证书的身份验证以允许证书续订 (Allow Authentication of Expired Certificates to Allow Certificate Renewal in Authorization Policy)**：如果要允许用户续订证书，请选中此复选框。如果启用此选项，请确保配置相应的授权策略规则，确认在进一步处理请求之前是否已续订证书。
	
	• **允许降级到 MSK (Allow Downgrade to MSK)**：如果内部方法支持扩展主会话密钥 (EMSK)，但客户端设备仅提供主会话密钥 (MSK)，请选中此复选框。请注意，虽然 EMSK 比 MSK 更安全，但某些客户端设备可能不支持 EMSK。
	
	• **在隧道建立期间接受客户端证书 (Accept Client Certificate during Tunnel Establishment)**：如果希望Cisco ISE 在 TEAP 隧道建立期间请求客户端证书，请选中此复选框。如果未提供证书，则Cisco ISE 使用所配置的内部方法进行身份验证。

字段名称	使用指南
	• **启用 EAP 链接 (Enable EAP Chaining)**：选中此复选框可启用 EAP 链接。EAP 链接允许Cisco ISE 在同一 TEAP 隧道内同时运行用户和计算机身份验证的内部方法。这可以让 Cisco ISE 使用 EAPChainingResult 属性关联身份验证结果，并应用相应的授权策略。 在启用 EAP 链接后，应使用 NetworkAccess:EapChainingResult 属性更新授权策略并添加条件，然后分配相应的权限。 **注释** 启用 EAP 链接时，如果要同时执行用户和计算机身份验证，请确保在请求方中复制用户和计算机证书。 **注释** • 如果在思科 ISE 中启用了 EAP 链接，则必须为 Microsoft 请求方同时配置主身份验证方法和辅助身份验证方法。 • 如果在思科 ISE 中禁用了 EAP 链接，则必须仅为 Microsoft 请求方配置主身份验证方法。 • 如果主身份验证方法和辅助身份验证方法均配置为“无”，则 EAP 协商可能会失败，并显示以下消息： `请求方已停止响应ISE (Supplicant stopped responding to ISE)`
Preferred EAP Protocol	选中此复选框可从以下任一选项中选择首选EAP协议：EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS 和 EAP-MD5。如果没有指定首选协议，则默认情况下使用 EAP - TLS。
“EAP-TLS L-位”(EAP-TLS L-bit)	选中此复选框可支持传统EAP请求方，后者默认情况下期望来自 ISE 的 TLS 更改密码规格报文和加密握手报文中具有长度包含标志（L位标志）。

字段名称	使用指南
允许 EAP 的弱密码 (Allow Weak Ciphers for EAP)	如果启用了此选项，会允许传统客户端使用弱密码协商（例如：RSA_RC4_128_SHA, RSA_RC4_128_MD5）。我们建议仅在您的传统客户端只支持弱密码时启用此选项。 默认情况下该选项处于禁用状态。 注释 思科 ISE 不支持 EDH_RSA_DES_64_CBC_SHA 和 EDH_DSS_DES_64_CBC_SHA。
所有 RADIUS 请求均需要消息身份验证器 (Require Message Authenticator for all RADIUS Requests)	如果启用此选项，Cisco ISE 验证 RADIUS 消息中是否存在 RADIUS 消息身份验证器 (RADIUS Message Authenticator) 属性。如果消息身份验证器属性不存在，则 RADIUS 消息将被丢弃。 启用此选项可提供保护,免受欺骗性访问请求消息和篡改 RADIUS 消息的威胁。 RADIUS 消息身份验证器 (RADIUS Message Authenticator) 属性是整个 RADIUS 消息的消息摘要 5 (MD5) 散列。 注释 EAP 默认使用消息身份验证器属性，不要求您将其启用。

相关主题

FIPS 和非 FIPS 模式支持的 TACACS+ 设备管理协议 ，第 295 页
为网络访问定义允许的协议，第 873 页

PAC 选项

下表介绍了在**允许协议服务列表 (Allowed Protocols Services List)** 窗口中选择了“使用 PAC”(Use PACs) 后显示的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)**。

表 *136: PAC* 选项

字段名称	使用指南
使用 **PAC (Use PAC)**	

字段名称	使用指南
	• “隧道 PAC 存活时间”(Tunnel PAC Time To Live)：存活时间 (TTL) 值限制 PAC 的生存期。指定生存期值和单位。默认值为 90 天。时间范围为 1 至 1825 天。 • “当剩下 <n%> 的 PAC TTL 时主动进行 PAC 更新”(Proactive PAC Update When: <n%> of PAC TTL is Left)：更新值确保客户端拥有有效的 PAC。首次成功通过身份验证后，但在 TTL 设置的到期时间前，Cisco ISE 启动更新。更新值是指 TTL 中的剩余时间百分比。默认为 90%。 • “允许匿名带内 PAC 调配”(Allow Anonymous In-band PAC Provisioning)：选中此复选框，使Cisco ISE 与客户端建立安全的匿名 TLS 握手，并使用 EAP-FAST 的零阶段和 EAP-MSCHAPv2，通过 PAC 调配客户端。要启用匿名 PAC 调配，必须选择这两种内部方法：EAP-MSCHAPv2 和 EAP-GTC。 • “允许经验证的带内 PAC 调配 ”(Allow Authenticated In-band PAC Provisioning)：Cisco ISE 使用 SSL 服务器侧身份验证，在 EAP-FAST 的零阶段期间通过 PAC 调配客户端。此选项比匿名调配的安全性更高，但要求在Cisco ISE 上安装服务器证书和受信任的根 CA。 如果您选中此选项，可将Cisco ISE 配置为在成功对 PAC 调配进行身份验证后将 Access-Accept 消息传送至客户端。 • “服务器在对调配进行身份验证后返回 Access-Accept 消息”(Server Returns Access Accept After Authenticated Provisioning)：如果希望Cisco ISE 在成功对 PAC 调配进行身份验证后传送 Access-Accept 消息，请选中此复选框。 • “允许机器身份验证”(Allow Machine Authentication)：选中此复选框，使Cisco ISE 使用计算机 PAC 调配最终用户客户端，并执行计算机身份验证（适用于没有计算机凭证的最终用户客户端）。可以通过请求（频内）或管理员（频外）将计算机 PAC 调配至

字段名称	使用指南
	客户端。当Cisco ISE 收到最终用户客户端发送的有效计算机 PAC 时，会从 PAC 提取计算机身份详细信息，并在Cisco ISE 外部身份源中进行验证。Cisco ISE 只支持 Active Directory 作为计算机身份验证的外部身份源。正确验证这些详细信息后，不会再执行进一步的身份验证。 如果您选中此选项，可以输入接受使用计算机 PAC 的时间值。当Cisco ISE 收到过期的计算机 PAC 时，会自动使用新的计算机 PAC 重新调配最终用户客户端（无需等待最终用户客户端发送新的计算机 PAC 请求）。 • “启用无状态会话恢复”(Enable Stateless Session Resume)：选中此复选框后，Cisco ISE 会为 EAP-FAST 客户端调配授权 PAC，并跳过 EAP-FAST 的第二阶段（默认为启用）。 在下列情况下取消选中此复选框： • 如果您不希望Cisco ISE 为 EAP-FAST 客户端调配授权 PAC • 要始终执行 EAP-FAST 的第二阶段 如果您选中此选项，可以输入用户授权 PAC 的授权时间段。在此时间段后，PAC 过期。当Cisco ISE 收到过期的授权 PAC 时，会执行执行 EAP-FAST 身份验证的第二阶段。

相关主题

OOB TrustSec PAC，第 896 页
为 EAP-FAST 生成 PAC，第 837 页

将思科 ISE 用作 RADIUS 代理服务器

Cisco ISE 可用作 RADIUS 服务器和 RADIUS 代理服务器。用作代理服务器时，Cisco ISE 从网络接入服务器 (NAS) 接受身份验证和记帐请求并将这些请求转发至外部 RADIUS 服务器。Cisco ISE 接受请求的结果并将结果返回至 NAS。

Cisco ISE 可以同时用作多个外部 RADIUS 服务器的代理服务器。您可以在 RADIUS 服务器序列中使用此处配置的外部 RADIUS 服务器。External RADIUS Server 页面会列出您已在Cisco ISE 中定义的所有外部 RADIUS 服务器。您可以使用过滤器选项，根据名称或说明或同时根据名称和说明搜索

具体 RADIUS 服务器。在简单身份验证策略和基于规则的身份验证策略中，您都可以使用 RADIUS 服务器序列来代理对 RADIUS 服务器的请求。

RADIUS 服务器序列从 RADIUS-Username 属性删除域名以进行 RADIUS 身份验证。这种域名删除操作不适用于使用 EAP-Identity 属性的 EAP 身份验证。RADIUS 代理服务器从 RADIUS-Username 属性获取用户名并从您配置 RADIUS 服务器序列时指定的字符删除用户名。对于 EAP 身份验证，RADIUS 代理服务器从 EAP-Identity 属性获取用户名。只有在 EAP-Identity 和 RADIUS-Username 值相同时，使用 RADIUS 服务器序列的 EAP 身份验证才会成功。

配置外部 RADIUS 服务器

您必须在Cisco ISE 中配置外部 RADIUS 服务器，使其向外部 RADIUS 服务器转发请求。您可以定义超时时间和连接尝试的次数。

开始之前

- 您无法单独使用您在本节中创建的外部 RADIUS 服务器，而必须创建 RADIUS 服务器序列并将其配置为使用您在本节创建的RADIUS服务器。然后，您就可以在身份验证策略中使用RADIUS服务器序列。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 RADIUS 服务器 (External RADIUS Servers)**。

系统将显示 RADIUS Servers 页面，其中包含已在Cisco ISE 中定义的外部 RADIUS 服务器的列表。

步骤 2 点击**添加 (Add)** 以添加外部 RADIUS 服务器。

步骤 3 根据要求输入相应值。

步骤 4 点击**提交 (Submit)** 以保存外部 RADIUS 服务器配置。

定义 RADIUS 服务器序列

Cisco ISE 中的 RADIUS 服务器序列允许您将 NAD 发送的请求代理到外部 RADIUS 服务器，此外部 RADIUS 服务器会处理该请求并将结果返回至Cisco ISE，随后Cisco ISE 会将响应转发至 NAD。

RADIUS Server Sequences 页面列出您在Cisco ISE 中定义的所有 RADIUS 服务器序列。在此页面上，您可以创建、编辑或复制 RADIUS 服务器序列。

开始之前

- 在开始此程序之前，您应该基本了解代理服务，并且必须成功完成相关链接的第一个条目中的任务。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 管理 **(Administration)** > 网络资源 **(Network Resources)** > **RADIUS** 服务器序列 **(RADIUS Server Sequences)**。

步骤 2 点击添加 **(Add)**。

步骤 3 根据要求输入相应值。

步骤 4 点击提交 **(Submit)** 以保存要用于策略的 RADIUS 服务器序列。

思科 ISE 充当 TACACS+ 代理客户端

Cisco ISE 可以充当外部 TACACS+ 服务器的代理客户端。当用作代理客户端时，Cisco ISE 接收来自网络接入服务器 (NAS) 的身份验证、授权和计费请求并将这些请求转发至外部 TACACS+ 服务器。Cisco ISE 接受请求的结果并将结果返回至 NAS。

“外部 TACACS+ 服务器”(TACACS+ External Servers) 页面列出了您已在Cisco ISE 中定义的所有外部 TACACS+ 服务器。您可以使用过滤器选项来根据名称和/或说明搜索具体的 TACACS+ 服务器。

Cisco ISE 可以同时充当多台外部 TACACS+ 服务器的代理客户端。要配置多台外部服务器，您可以使用 TACACS+ 服务器序列页面。有关更多详细信息，请参阅TACACS+ 服务器序列设置页面。

配置外部 TACACS+ 服务器

您必须在Cisco ISE 中配置外部 TACACS 服务器，使其向外部 TACACS 服务器转发请求。您可以定义超时时间和连接尝试的次数。

开始之前

- 您不能在策略中直接使用在本节中创建的外部 TACACS 服务器。而必须创建 TACACS 服务器序列并将其配置为使用您在本节创建的 TACACS 服务器。然后，您就可以在策略集中使用 TACACS 服务器序列。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 工作中心 **(Work Centers)** > 设备管理 **(Device Administration)** > 网络资源 **(Network Resources)** > **TACACS** 外部服务器 **(TACACS External Servers)**。
系统将显示**TACACS** 外部服务器 **(TACACS External Servers)** 页面，其中包含已在Cisco ISE 中定义的外部 TACACS 服务器的列表。

步骤 2 点击添加 **(Add)** 以添加外部 TACACS 服务器。

步骤 3 根据要求输入相应值。

步骤 4 点击提交 **(Submit)** 以保存外部 TACACS 服务器配置。

TACACS+ 外部服务器设置

下表列出“TACACS 外部服务器”(TACACS External Servers) 页面中的字段。导航路径为 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **TACACS 外部服务器 (TACACS External Servers)** 页面。

表 *137: TACACS+* 外部服务器设置

字段	使用指南
名称 (Name)	输入 TACACS+ 外部服务器的名称。
说明	输入 TACACS+ 外部服务器设置的说明。
Host IP	输入远程 TACACS+ 外部服务器的 IP 地址（IPv4 或 IPv6 地址）。
连接端口	输入远程 TACACS+ 外部服务器的端口号。端口号为 49。
Timeout	指定Cisco ISE 等待外部 TACACS+ 服务器响应的秒数。默认值为 5 秒。有效值范围为 1 至 120。
共享密钥	文本字符串用于获得与 TACACS+ 外部服务器的连接。如果配置不正确，则连接将被 TACACS+ 外部服务器拒绝。
使用单连接	TACACS 协议支持两种将会话与连接关联的模式：单连接和非单连接。单连接模式重复使用用于客户端可能发起的多个 TACACS+ 会话的单 TCP 连接。非单连接打开一个用于客户端发起的每个 TACACS+ 会话的新 TCP 连接。TCP 连接在每个会话之后关闭。 对于高流量环境，您可以选中使用单连接 (Use Single Connect) 复选框，对于低流量环境可取消选中。

定义 TACACS+ 服务器序列

Cisco ISE 中的 TACACS+ 服务器序列允许您将 NAD 发送的请求代理到外部 TACACS+ 服务器，此外部 TACACS+ 服务器会处理该请求并将结果返回至Cisco ISE，随后Cisco ISE 会将响应转发至 NAD。TACACS+ 服务器序列页面列出您在Cisco ISE 中定义的所有 TACACS+ 服务器序列。在此页面上，您可以创建、编辑或复制 TACACS+ 服务器序列。

开始之前

- 您应该对代理服务、Cisco ISE 管理员组、访问级别、权限和限制有一个基本了解。

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 确保您希望在 TACACS+ 服务器序列中使用的外部 TACACS+ 服务器已定义。

步骤 1 选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **TACACS 外部服务器 (TACACS External Servers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入所需的值。

步骤 4 点击**提交 (Submit)** 以保存用于策略的 TACACS+ 服务器序列。

TACACS+ 服务器序列设置

下表介绍“TACACS 服务器序列”页面中的字段。导航路径为 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **TACACS 服务器序列 (TACACS Server Sequence)** 页面。

表 *138: TACACS+* 服务器序列设置

字段	使用指南
名称 (Name)	输入 TACACS 代理服务器序列的名称。
说明	输入 TACACS 代理服务器序列的说明。
服务器列表	从可用列表中选择所需的TACACS代理服务器。可用列表包含在“外部 TACACS+ 服务”(TACACS External Services) 页面配置的 TACACS 代理服务器列表中。
日志记录控制 (Logging Control)	选中此复选框以启用日志记录控制： • “本地计费”(Local Accounting)：计费消息由处理设备请求的服务器记录。 • “远程计费”(Remote Accounting)：计费消息由处理设备请求的代理服务器记录。

字段	使用指南
“用户名剥离”(Username Stripping)	用户名前缀/后缀剥离： • “前缀剥离”(Prefix Strip)：选中此复选框以删除用户名的前缀。例如，如果主题名称是 acme\smith，分隔符为 \，则用户名变成 smith。默认分隔符为 \。 • “后缀剥离”(Suffix Strip)：选中此复选框以删除用户名的后缀。例如，如果主题名称是 smith@acme.com，分隔符为 @，则用户名变成 smith。默认分隔符为 @。

网络访问服务

网络访问服务包含请求的身份验证策略条件。可以为不同的使用案例创建单独的网络访问服务，例如，有线 802.1X、有线 MAB 等。要创建网络访问服务，请配置允许的协议或服务器序列。然后，从“策略集”(Policy Sets) 页面配置网络访问策略的网络访问服务。

为网络访问定义允许的协议

允许的协议定义了Cisco ISE 可以用于与请求访问网络资源的设备通信的协议集。允许的协议访问服务是一个您应在配置身份验证策略前创建的独立实体。允许的协议访问服务是一个包含特定使用案例的选定协议的对象。

Allowed Protocols Services 页面列出了您创建的所有允许的协议服务。Cisco ISE 中预定义了默认网络访问服务。

开始之前

在开始此程序之前，您应该具备用于身份验证的协议服务的基本知识。

- 请查看本章节中的“Cisco ISE 身份验证策略”部分，以了解身份验证类型和各种数据库支持的协议。
- 查看“PAC 选项”，了解每种协议服务的功能和选项，以便您可以做出适合您的网络的选择。
- 确保您已定义全局协议设置。

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入所需信息。

步骤 4 为您的网络选择适当的身份验证协议和选项。

步骤 5 如果您选择使用 PAC，请进行适当的选择。

要启用 Anonymous PAC Provisioning，您必须同时选择以下两个内部方法：EAP-MSCHAPv2 和可扩展身份验证协议-通用令牌卡 (EAP-GTC)。另请注意，Cisco ISE 只支持 Active Directory 作为计算机身份验证的外部身份源。

步骤 6 点击**提交 (Submit)** 保存允许的协议服务。

允许的协议服务在简单和基于规则的身份验证策略页面中显示为独立对象。您可以将此对象用于不同的规则。

您现在可以创建简单或基于规则的身份验证策略。

如果禁用 EAP-MSCHAP 作为内部方法并为 PEAP 或 EAP-FAST 启用 EAP-GTC 和 EAP-TLS 内部方法，则 ISE 会在内部方法协商过程中启动 EAP-GTC 内部方法。在第一个 EAP-GTC 消息发送到客户端之前，ISE 会执行身份选择策略以从身份库获取 GTC 密码。在执行此策略的过程中，EAP 身份验证等于 EAP-GTC。如果 EAP-GTC 内部方法被客户端拒绝且 EAP-TLS 已经过协商，则系统不会再次执行身份库策略。如果身份库策略基于 EAP 身份验证属性，则它可能会出现意外结果，因为实时 EAP 身份验证基于 EAP-TLS，但设置于身份策略评估之后。

用户的网络接入

对网络接入，主机会连接至网络设备并且请求使用网络资源。网络设备识别新连接的主机，并且将 RADIUS 协议用作传输机制，向Cisco ISE 请求对用户进行身份验证和授权。

Cisco ISE 根据基于 RADIUS 协议传输的协议支持网络接入流程。

不使用 EAP 的基于 RADIUS 的协议

不包含 EAP 的基于 RADIUS 的协议包含以下协议：

- 密码身份验证协议 (PAP)
- CHAP
- Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)
- MS-CHAP 版本 2 (MS-CHAPv2)

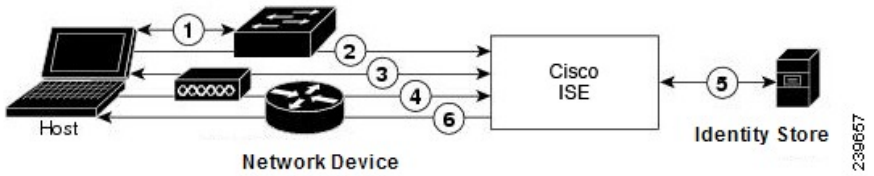
基于 RADIUS 的非 EAP 身份验证流程

本节介绍不使用 EAP 的基于 RADIUS 的身份验证。使用 PAP 身份验证的基于 RADIUS 的流程按以下程序进行：

1. 主机连接至网络设备。
2. 网络设备向Cisco ISE 发送包含适用于所用具体协议（PAP、CHAP、MS-CHAPv1 或 MS-CHAPv2）的 RADIUS 属性的 RADIUS 请求。
3. Cisco ISE 使用身份存储区验证用户凭证。
4. Cisco ISE 向网络设备发送 RADIUS 响应（Access-Accept 或 Access-Reject），然后网络设备将应用此响应决策。

下图显示不使用 EAP 的基于 RADIUS 的身份验证。

图 *44:* 不使用 *EAP* 的基于 *RADIUS* 的身份验证



Cisco ISE 支持的非 EAP 协议如下：

密码身份验证协议

PAP 使用双向握手为用户提供建立其身份的简单方法。PAP 密码使用共享密钥加密，是最简单的身份验证协议。PAP 不是强大的身份验证方法，因为其几乎无法抵御反复试错攻击。

思科 *ISE* 中基于 *RADIUS* 的 *PAP* 身份验证

Cisco ISE 根据身份存储区检查用户名和密码对，直到其最终确认身份验证或终止连接。

您可以同时将不同安全级别应用于Cisco ISE 以满足不同要求。PAP 使用二次握手过程。如果身份验证成功，Cisco ISE 返回确认信息；否则，Cisco ISE 将停止连接或向发起方提供第二次机会。

发起方完全控制尝试的频率和计时。因此，可以使用更强的身份验证方法的任意服务器都可以在PAP之前主动协商该方法。RFC 1334 定义 PAP。

Cisco ISE 支持基于 RADIUS UserPassword 属性的标准 RADIUS PAP 身份验证。RADIUS PAP 身份验证与所有身份存储区都兼容。

RADIUS PAP 身份验证流程包括记录成功和失败的尝试。

质询握手身份验证协议

CHAP 使用质询响应机制，其中会对响应进行单向加密。CHAP 使Cisco ISE 可以从最安全的加密机制向下协商到最不安全的加密机制，并且会保护流程中传输的密码。CHAP 密码可重复使用。如果使用Cisco ISE 内部数据库进行身份验证，您可以使用 PAP 或 CHAP。CHAP 不适用于 Microsoft 用户数据库。与 RADIUS PAP 相比，CHAP 可在从最终用户客户端到 AAA 客户端的通信期间为密码加密实现更高的安全性。

Cisco ISE 支持基于 RADIUS ChapPassword 属性的标准 RADIUS PAP 身份验证。Cisco ISE 仅支持使用内部身份库进行 RADIUS CHAP 身份验证。

Microsoft 质询握手身份验证协议版本 *1*

Cisco ISE 支持 RADIUS MS-CHAPv1 身份验证和更改密码功能。RADIUS MS-CHAPv1 包含两个版本的更改密码功能：Change-Password-V1 和 Change-Password-V2。Cisco ISE 不支持基于 RADIUS MS-CHAP-CPW-1 属性的 Change-Password-V1，仅支持基于 MS-CHAP-CPW-2 属性的 Change-Password-V2。以下身份源支持 RADIUS MS-CHAPv1 身份验证和更改密码功能：

- 内部身份库

- Microsoft Active Directory 身份库

Microsoft 质询握手身份验证协议版本 *2*

RADIUS MS - CHAPv2 身份验证和更改密码功能受以下身份来源支持：

- 内部身份库
- Microsoft Active Directory 身份库

基于 RADIUS 的 EAP 协议

EAP 提供了可扩展的框架，支持各种身份验证类型。本节介绍Cisco ISE 支持的 EAP 方法，包含下列主题：

简单的 EAP 方法

- EAP 消息摘要 5
- 轻型 EAP

使用思科 ISE 服务器证书进行身份验证的 EAP 方法

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

除了上面列出的方法，还有使用证书进行服务器和客户端身份验证的 EAP 方法。

基于 RADIUS 的 EAP 身份验证流程

只要身份验证流程中涉及 EAP，则开始此流程之前都要执行 EAP 协商以确定应该使用哪个具体的 EAP 方法（以及在适当的情况下使用内部方法）。基于 EAP 的身份验证按照以下程序进行：

1. 主机连接至网络设备。
2. 网络设备向主机发送 EAP 请求。
3. 主机向网络设备回复 EAP 响应。
4. 网络设备将其从主机接收的 EAP 响应封装入 RADIUS 访问请求（使用 EAP-Message RADIUS 属性）并将此 RADIUS 访问请求发送至Cisco ISE。
5. Cisco ISE 从此 RADIUS 数据包提取 EAP 响应，并且创建新 EAP 请求，将其封装入 RADIUS 访问质询（也是使用 EAP-Message RADIUS 属性），然年后将其发送至网络设备。
6. 网络设备提取 EAP 请求并将其发送至主机。

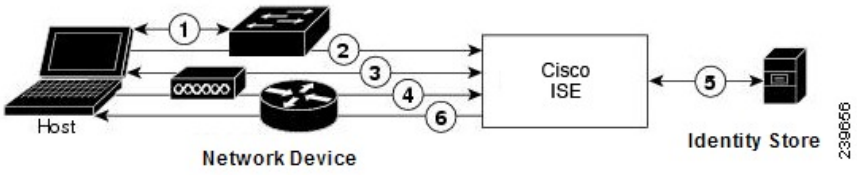
这样，主机和Cisco ISE 就间接地交换 EAP 消息（通过 RADIUS 传输并穿过网络设备）。以此方式交换的首批 EAP 消息会协商以后用于执行身份验证的具体 EAP 方法。

之后交换的 EAP 消息就用于传输执行实际身份验证所需的数据。如果所协商的具体 EAP 身份验证方法需要，Cisco ISE 会使用身份库来验证用户凭证。

Cisco ISE 确定身份验证成功还是失败之后，会向网络设备（而且最终也向主机）发送封装入 RADIUS Access-Accept 或 Access-Reject 消息的 EAP-Success 或 EAP-Failure 消息。

下图显示使用 EAP 的基于 RADIUS 的身份验证。

图 *45:* 使用 *EAP* 的基于 *RADIUS* 的身份验证



可扩展身份验证协议-消息摘要 *5*

可扩展身份验证协议-消息摘要 5 (EAP - MD5) 提供单向客户端身份验证。服务器向客户端发送随机质询。客户端在响应中通过使用 MD5 加密质询及密码证明其身份。由于人为截取可看到质询和响应，所以在开放式媒体上使用时，EAP-MD5 容易遭受字典攻击。由于不发生服务器验证，所以也很容易遭受欺骗。Cisco ISE 支持Cisco ISE 内部身份库的 EAP-MD5 身份验证。在使用 EAP-MD5 协议时，还支持主机查找。

轻型可扩展身份验证协议

目前，Cisco ISE 仅将轻型可扩展身份验证协议 (LEAP) 用于Cisco Aironet 无线网络。如果不启用此选项，配置为执行 LEAP 身份验证的Cisco Aironet 最终用户客户端就无法访问网络。如果所有Cisco Aironet 最终用户客户端都使用不同的身份验证协议（例如，可扩展身份验证协议-传输层安全 [EAP-TLS]），我们建议您禁用此选项。

注释 如果用户使用网络设备 *(Network Devices)* 部分中定义的 AAA 客户端作为 RADIUS（思科 Aironet）设备访问您的网络，您必须启用 LEAP、EAP-TLS 或同时启用这两项；否则思科 Aironet 用户将无法进行身份验证。

受保护的可扩展身份验证协议

受保护的可扩展身份验证协议 (PEAP) 提供相互身份验证，确保易受攻击的用户凭证的机密性和完整性，保护其自身抵御被动（窃听）和主动（中间人）攻击，以及安全地生成加密密钥材料。PEAP 与 IEEE 802.1X 标准和 RADIUS 协议兼容。Cisco ISE 使用可扩展身份验证协议-Microsoft 质询握手身份验证协议 (EAP-MS-CHAP)、可扩展身份验证协议-通用令牌卡 (EAP-GTC) 和 EAP-TLS 内部方法支持 PEAP 版本 0 (PEAPv0) 和 PEAP 版本 1 (PEAPv1)。Cisco安全服务客户端 (SSC) 请求方支持Cisco ISE 支持的所有 PEAPv1 内部方法。

使用 *PEAP* 的优势

使用 PEAP 有这些优势：PEAP 以 TLS 为基础，而 TLS 实施广泛，经过了大量安全审查；它为不派生密钥的方法建立密钥；它在隧道内发送身份；它保护内部方法交换和结果消息；它支持分段。

PEAP 协议支持的请求方

PEAP 支持这些请求方：

- Microsoft 内置客户端 802.1X XP
- Microsoft 内置客户端 802.1X Vista
- Cisco安全服务客户端 (SSC)，4.0 版
- Cisco SSC，5.1 版
- Funk Odyssey 访问客户端，4.72 版
- Intel，12.4.0.0 版

PEAP 协议流程

PEAP 会话可以分为三部分：

1. Cisco ISE 和对等体建立 TLS 隧道。Cisco ISE 提供其证书，但对等体不提供。对等体和Cisco ISE 创建密钥以加密隧道内的数据。
2. 内部方法确定隧道内的数据流：
   - EAP-MS-CHAPv2 内部方法 - EAP-MS-CHAPv2 数据包在不带报头的情况下在隧道内传输。报头的第一个字节包含类型字段。EAP-MS-CHAPv2 内部方法支持更改密码功能。可以配置用户可以尝试通过管理门户更改密码的次数。用户身份验证尝试次数受此数值限制。
   - EAP-GTC 内部方法 - PEAPv0 和 PEAPv1 均支持 EAP-GTC 内部方法。支持的请求方不支持使用 EAP-GTC 内部方法的 PEAPv0。EAP-GTC 支持更改密码功能。可以配置用户可以尝试通过管理门户更改密码的次数。用户身份验证尝试次数受此数值限制。
   - EAP-TLS 内部方法 - Windows 内置请求方不支持在建立隧道后对消息分段，这会影响 EAP-TLS 内部方法。在建立隧道后，Cisco ISE 不支持外部 PEAP 消息分段。在建立隧道时，分段会按照 PEAP 文档中的规定进行工作。在 PEAPv0 中，系统将删除 EAP-TLS 数据包信头，而在 PEAPv1 中， EAP-TLS 数据包在传输时保持不变。
   - 可扩展身份验证协议类型、长度、值 (EAP-TLV) 扩展 - EAP TLV 数据包在传输时保持不变。EAP-TLV 数据包在带标头的情况下在隧道内传输。
3. 如果会话已达到内部方法，会以一种受保护的方式确认成功和失败。

   客户端 EAP 消息始终载于 RADIUS Access-Request 消息中，而服务器 EAP 消息始终载于 RADIUS Access-Challenge 消息中。EAP-Success 消息始终载于 RADIUS Access-Accept 消息中。EAP-Failure 消息始终载于 RADIUS Access-Reject 消息中。丢弃客户端 PEAP 消息会导致丢弃 RADIUS 客户端消息。

注释 Cisco ISE 要求在 PEAPv1 通信期间确认 EAP-成功或 EAP-失败消息。对等体必须发送回带有空 TLS 数据字段的 PEAP 数据包，以确认收到成功或失败消息。

可扩展身份验证协议-通过安全隧道的灵活身份验证 *(EAP-FAST)*

可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST) 是提供相互身份验证和使用共享密钥建立隧道的一种身份验证协议。隧道用于保护基于密码的弱身份验证方法。共享密钥称为受保护的访问凭证 (PAC) 密钥，用于为客户端和服务器进行相互身份验证，同时保护隧道安全。

EAP-FAST 的优势

EAP-FAST 相比其他身份验证协议提供以下优势：

- 相互身份验证 - EAP 服务器必须能够验证对等体的身份和真实性，而且对等体必须能够验证 EAP 服务器的真实性。
- 抵抗被动字典式攻击 - 许多身份验证协议要求对等体向 EAP 服务器明确地提供纯文本或散列形式密码。
- 抵抗中间人攻击 - 建立相互验证保护隧道时，协议必须阻止敌对者在对等体和 EAP 服务器之间的对话中成功插入信息。
- 确保支持许多不同的密码身份验证接口的灵活性，例如 MS-CHAPv2、通用令牌卡 (GTC) 及其他 - EAP-FAST 是一个扩展框架，允许同一服务器支持多个内部协议。
- 提高效率 - 使用无线介质时，对等体的计算资源和电力资源有限。EAP-FAST 使网络访问通信能够减少计算资源占用。
- 最大限度减少身份验证服务器的每用户身份验证状态要求 - 对于大型部署，通常有许多服务器充当多个对等体的身份验证服务器。此外，非常理想的情况是，对等体使用同一共享秘钥保护隧道的方式，与它使用用户名和密码获得网络访问权限的方式基本相同。EAP-FAST 促进对等体使用一个强大的共享秘钥，同时使服务器最大限度减少它必须缓存和管理的每用户和设备状态。

EAP-FAST 流程

EAP-FAST 协议流程始终由以下阶段组成：

1. 调配阶段 - 此阶段是 EAP-FAST 的初始阶段。在此阶段，系统使用Cisco ISE 和对等体之间共享的叫作 PAC 的唯一强密钥调配对等体。
2. 建立隧道阶段 - 客户端和服务器通过使用 PAC 建立全新隧道密钥相互进行身份验证。系统然后使用隧道密钥保护其余对话并实现消息机密性和可靠性。
3. 身份验证阶段 - 身份验证在隧道内部处理，其包含生成会话密码和受保护的终止。Cisco ISE 支持 EAP-FAST 版本 1 和 1a。

从非思科设备启用 MAB

按顺序配置以下设置，可从非Cisco设备配置 MAB。

步骤 1 确保终端数据库中具有要进行身份验证的终端的 MAC 地址。可以添加这些终端或由分析器服务自动分析这些终端。

步骤 2 根据非Cisco设备（PAP、CHAP 或 EAP-MD5）使用的 MAC 身份验证类型创建网络设备配置文件。

a) 选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备配置文件 (Network Device Profiles)**。

b) 点击**添加 (Add)**。

c) 输入网络设备配置文件的名称和描述。

d) 从**供应商 (Vendor)** 下拉列表中选择供应商名称。

e) 选中设备支持的协议所对应的复选框。如果设备支持 RADIUS，请选择 RADIUS 字典与网络设备配合使用。

f) 扩展**身份验证/授权 (Authentication/Authorization)** 部分，对设备的数据流类型、属性别名和主机查找进行默认设置。

g) 在**主机查找 (MAB)** （**Host Lookup (MAB))**部分，请执行以下操作：

- 处理主机查找 - 选中此复选框以定义网络设备配置文件在主机查找时使用的协议。

  不同供应商的网络设备采用不同方式执行 MAB 身份验证。根据设备类型，为您使用的协议选中**检查密码 (Check Password)** 复选框和/或**检查呼叫站 ID 等于 MAC 地址 (Check Calling-Station-Id equals MAC Address)** 复选框。

- 通过 PAP/ASCII (Via PAP/ASCII) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的 PAP 请求作为一个主机查找请求进行检测

- 通过 CHAP (Via CHAP) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的此类请求作为一个主机查找请求进行检测

- 通过 EAP MD5 (Via EAP-MD5) - 选中启用网络设备配置文件基于 EAP 的 MD5 散列身份验证。

h) 在“权限”(Permissions)、“授权更改 (CoA)”(Change of Authorization (CoA)) 和“重定向”(Redirect) 部分输入所需的详细信息，然后点击**提交 (Submit)**。

有关如何创建自定义 NAD 配置文件的信息，请参阅支持思科身份服务引擎的网络接入设备配置文件。

步骤 3 选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**。

步骤 4 选择要启用 MAB 的设备，然后点击**编辑 (Edit)**。

步骤 5 在“网络设备”(Network Device) 页面，在**设备配置文件 (Device Profile)** 下拉列表中选择在步骤 2 中创建的网络设备配置文件。

步骤 6 点击**保存 (Save)**。

注释 对于Cisco NAD，MAB 和网络/用户身份验证使用的服务类型值不同。这样在使用Cisco NAD 时，ISE 可将 MAB 身份验证与网络身份验证区分开来。在某些非Cisco NAD 中，MAB 身份验证与网络/用户身份验证使用相同的服务类型属性值；这可能会导致您的访问策略出现安全问题。如果您在非Cisco 设备上使用 MAB，我们建议您配置其他的授权策略规则，以确保您的网络安全不受影响。例如，如果一台打印机使用了 MAB，您可以配置授权策略规则，以便于在 ACL 中将 MAB 限制在打印机协议端口。

从思科设备启用 MAB

按顺序配置以下设置从Cisco设备配置 MAB。

步骤 1 确保终端数据库中具有要进行身份验证的终端的 MAC 地址。可以添加这些终端或由分析器服务自动分析这些终端。

步骤 2 根据Cisco设备（PAP、CHAP 或 EAP-MD5）使用的 MAC 身份认证类型创建网络设备配置文件。

a) 依次选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备配置文件 (Network Device Profiles)**。

b) 点击**添加 (Add)**。

c) 输入网络设备配置文件的名称和描述。

d) 选中设备支持的协议的复选框。如果设备支持 RADIUS，请选择 RADIUS 字典与网络设备配合使用。

e) 扩展**身份验证/授权 (Authentication/Authorization)** 部分，对设备的数据流类型、属性别名和主机查找进行默认设置。

f) 在**主机查找 (MAB)** （**Host Lookup (MAB))**部分，请执行以下操作：

- 处理主机查找 - 选中此复选框以定义网络设备配置文件在主机查找时使用的协议。

  根据设备类型，为您使用的协议选中**检查密码 (Check Password)** 复选框和/或**检查呼叫站 ID 等于 MAC 地址 (Check Calling-Station-Id equals MAC Address)** 复选框。

- 通过 PAP/ASCII (Via PAP/ASCII) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的 PAP 请求作为一个主机查找请求进行检测

- 通过 CHAP (Via CHAP) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的此类请求作为一个主机查找请求进行检测

- 通过 EAP MD5 (Via EAP-MD5) - 选中启用网络设备配置文件基于 EAP 的 MD5 散列身份验证。

g) 在“权限”(Permissions)、“授权更改 (CoA)”(Change of Authorization (CoA)) 和“重定向”(Redirect) 部分输入所需的详细信息，然后点击**提交 (Submit)**。

有关如何创建自定义 NAD 配置文件的信息，请参阅支持思科身份服务引擎的网络接入设备配置文件。

步骤 3 选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**。

步骤 4 选择要启用 MAB 的设备，然后点击**编辑 (Edit)**。

步骤 5 在“网络设备”(Network Device) 页面，在**设备配置文件 (Device Profile)** 下拉列表中选择在步骤 2 中创建的网络设备配置文件。

步骤 6 点击**保存 (Save)**。

ISE 社区资源

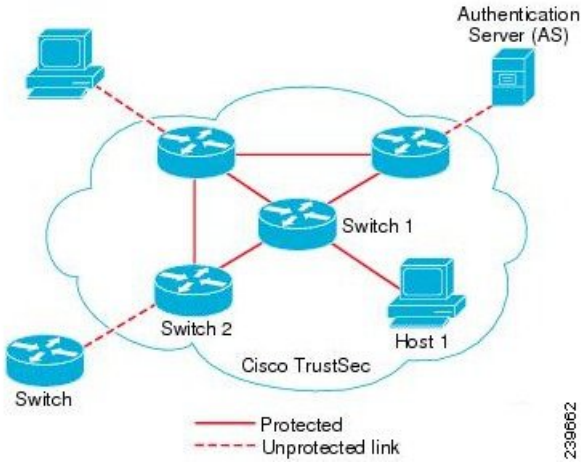
有关 IP 电话身份验证功能的信息，请参阅电话身份验证功能。

TrustSec 架构

Cisco TrustSec 解决方案可建立受信任的网络设备云以构建安全网络。Cisco TrustSec 云中的每个设备都由其相邻设备（对等体）进行身份验证。TrustSec 云中设备之间的通信由加密、消息完整性检查和数据路径重放保护机制进行保护。TrustSec 解决方案使用在身份验证期间获取的设备和用户身份信息来在数据包进入网络时给数据包进行分类或确定颜色。此数据包分类在数据包进入 TrustSec 网络时由标记数据包进行维护，从而可以正确识别数据包，以沿着数据路径应用安全性和其他策略条件。此标签也称为安全组标签 (SGT)，Cisco ISE 可通过此标签使终端设备在 SGT 上执行操作以过滤流量，从而实施访问控制策略。

下图显示 TrustSec 网络云的一个示例。

图 *46: TrustSec* 架构



ISE 社区资源

有关如何使用Cisco TrustSec 简化网络分段并提高安全性的信息，请参阅使用思科 TrustSec 简化网络分段和基于策略的软件定义分段和思科 TrustSec 提高安全性白皮书。

有关CiscoTrustSec平台支持矩阵的完整列表，请参阅CiscoTrustSec平台支持表。http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

有关适用于 TrustSec 的支持文档的完整列表，请参阅思科 TrustSec。

有关 TrustSec 社区资源的完整列表，请参阅 TrustSec 社区。

TrustSec 组件

TrustSec 的重要组件包括：

- 网络设备准入控制 (NDAC) - 在受信任网络中，在身份验证期间，TrustSec 云上的每个网络设备（例如以太网交换机）都由其对等体设备对其凭证和可信度进行验证。NDAC 使用基于 IEEE 802.1X 端口的身份验证并且将可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST) 用作其可扩展身份验证协议 (EAP) 方法。如果在 NDAC 流程中身份验证和授权成功，则系统将为 IEEE 802.1AE 加密执行安全关联协议协商。
- 终端准入控制 (EAC) - 对连接 TrustSec 云的终端用户或设备执行的身份验证流程。EAC 通常发生于访问级别交换机上。如果在 EAP 流程中身份验证和授权成功，系统将向用户或设备分配 SGT。用于身份验证和授权的 EAC 访问方法包括：
  - 基于 802.1X 端口的身份验证
  - MAC 身份验证绕行 (MAB)
  - Web 身份验证 (WebAuth)
- 安全组 (SG) - 共用访问控制策略的一组用户、终端设备和资源。SG 由Cisco ISE 中的管理员定义。当向 SGA 域添加新用户和设备时，Cisco ISE 将这些新的实体分配到相应的安全组。
- 安全组标签 (SGT) - TrustSec 服务向每个安全组分配一个唯一 16 位安全组编号，其范围为 TrustSec 域内的全局范围。交换机内安全组的数量限制为已通过身份验证的网络实体的数量。您无需手动配置安全组数量。它们是自动生成的，但是您可以选择将一系列 SGT 保留用于 IP 到 SGT 的映射。
- 安全组访问控制列表 (SGACL) - SGACL 允许您根据所分配的 SG 控制访问和权限。将权限归入角色可以简化安全策略的管理。当您添加设备时，只需分配一个或多个安全组，这些安全组就会立即获得相应权限。您可以修改安全组以引入新的权限或限制当前权限。
- 安全交换协议 (SXP) - SGT 交换协议 (SXP) 是为 TrustSec 服务开发的一种协议，将整个不具有支持 SGT 的硬件的网络设备上的 IP 到 SGT 绑定表传送至支持 SGT/SGACL 的硬件。
- 环境数据下载 - TrustSec 设备在首次联接受信任网络时从Cisco ISE 获取其环境数据。您也可以在设备上手动配置某些数据。设备必须在到期之前刷新环境数据。TrustSec 设备从Cisco ISE 获取以下环境数据：
  - 服务器列表 - 列出客户端可以用于以后的 RADIUS 请求的服务器列表（适用于身份验证和授权）
  - 设备 SG - 设备自身所属的设备组
  - 过期超时 - 控制 TrustSec 设备应该多久下载或更新一次其环境变量的时间间隔
- 身份到端口的映射 - 交换机在终端所连接的端口上定义身份以及将身份用于在Cisco ISE 服务器中查找特定 SGT 值所使用的方法。

TrustSec 术语

下表列出某些用于 TrustSec 解决方案的常用术语及其在 TrustSec 环境中的含义。

表 *139: TrustSec* 术语

术语	含义
请求方	尝试加入受信任网络的设备。
身份验证	在允许每台设备加入受信任网络之前验证设备身份的过程。
授权	根据已经过身份验证的设备身份决定请求访问受信任网络上的资源的设备的访问级别的过程。
访问控制	根据分配给每个数据包的SGT对每个数据包应用访问控制的过程。
安全通信	为保护流经受信任网络中的每条链路的数据包进行加密、完整性和数据路径重放保护的过程。
TrustSec 设备	支持 TrustSec 解决方案的任何Cisco Catalyst 6000 系列或 Cisco Nexus 7000 系列交换机。
支持 TrustSec 的设备	支持 TrustSec 的设备将具有支持 TrustSec 的硬件和软件。例如，带 Nexus 操作系统的 Nexus 7000 系列交换机。
TrustSec 种子设备	直接对Cisco ISE 服务器进行身份验证的 TrustSec 设备。此设备同时用作验证器和请求方。
入口	当数据包首次遇到支持 TrustSec 的设备时，这些数据包会被标上SGT标记。该设备已加入启用了Cisco TrustSec 解决方案的网络。进入受信任网络的这个点称为入口。
出口	当数据包通过最后一台支持 TrustSec 的设备时，这些数据包会被取消标记。该设备已加入启用了Cisco TrustSec 解决方案的网络。退出受信任网络的这个点称为出口。

TrustSec 支持的交换机和需要的组件

要设置启用Cisco TrustSec 解决方案的Cisco ISE 网络，您需要支持 TrustSec 解决方案的交换机和其他组件。除交换机外，您还需要其他组件用于基于身份的用户访问控制（使用 IEEE 802.1X 协议）。有关支持 Trustsec 的Cisco交换机平台和必要组件的完整的最新列表，请参阅启用 TrustSec 的思科基础设施。

与思科 DNA 中心的集成

Cisco ISE 是Cisco全数字化网络架构 (DNA) 的主要部分。Cisco DNA 中心可使您实现网络自动化以提供业务灵活性。集成Cisco ISE 和Cisco DNA 中心时，Cisco ISE 为Cisco DNA 中心提供终端身份验证。

将思科 DNA 中心连接到思科 ISE

请参阅《DNAC 用户指南》https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html 中有关配置Cisco DNA 中心和Cisco ISE 的要求与说明。

本部分提供有关适于Cisco DNA 中心的Cisco ISE 配置的其他信息。

- 密码：Cisco DNA 中心在连接到Cisco ISE 时使用Cisco ISE 管理员用户名和密码来验证对Cisco ISE 的访问权限。有关系统密码的详细信息，请参阅对思科 ISE 的管理访问 ，第 15 页。

  注释 在早于 2.2.1.0 的Cisco DNA 中心版本中，Cisco ISE CLI 用于执行初始集成步骤，因此Cisco ISE CLI 以及管理员用户名和密码必须相同。从Cisco DNA 中心版本 2.2.1.0 开始，不再使用Cisco ISE CLI，因此Cisco ISE CLI 以及管理员用户名和密码无需相同。

- API：Cisco DNA 中心通过调用 ISE API 配置 ISE 的某些部分。在Cisco ISE 中启用 API 访问，但不启用 CSRF。有关详细信息，请参阅 启用外部 RESTful 服务 API ，第 113 页

- pxGrid：Cisco ISE 是 pxGrid 控制器，Cisco DNA 中心是用户。Cisco ISE 和Cisco DNA 中心均监控 Trustsec (SD-Access) 内容，其中包含 SGT 和 SGACL 信息。同步Cisco ISE 与Cisco DNA 中心之间的系统时钟。Cisco ISE 使用证书连接到 pxGrid，Cisco DNA 中心将其配置为用于连接。有关Cisco ISE 中 pxGrid 的详细信息，请参阅 中的“pxGrid 节点”部分请参阅思科 pxGrid 节点，第 70 页。

  注释 Cisco ISE 2.4 及更高版本支持 pxGrid 2.0 和 pxGrid 1.0。虽然 pxGrid 2.0 允许Cisco ISE 部署中有最多 4 个 pxGrid 节点，但是 Cisco DNA 中心目前不支持两个以上 pxGrid 节点。

- Cisco ISE IP 地址：Cisco ISE PAN 与Cisco DNA 中心之间的连接必须是直接连接。不能通过代理、负载均衡器或虚拟 IP 地址进行连接。Cisco ISE 和Cisco DNA 中心会互相配置静态地址。

  验证Cisco ISE 是否未使用代理。如果使用代理，请从代理中排除Cisco DNA 中心 IP。

  以下功能支持 IPv4 和 IPv6 IP 地址：

  - 外部 RESTful 服务 (ERS) API
  - 管理 REST API

- Secure Shell (SSH) 协议

- SXP：DNA 中心不需要 SXP。您可能希望在将Cisco ISE 连接到 DNA 托管网络时启用 SXP，以便Cisco ISE 与没有 Trustsec (SD-Access) 硬件支持的网络设备进行通信。

  注释 将 ISE 部署配置为支持 Trustsec 时，或者当 ISE 与Cisco DNA 中心集成时，请勿将 ISE 策略服务节点配置为仅 SXP。SXP 是 Trustsec 与非 Trustsec 设备之间的接口。它不与启用了 Trustsec 的网络设备通信。

- Cisco ISE 连接的证书：
  - Cisco ISE 管理员证书必须在使用者名称或 SAN 中包含Cisco ISE IP 或 FQDN。
  - SSH 密钥、ISE SSH 访问或Cisco DNA 中心与Cisco ISE 连接证书不支持 ECDSA。
  - Cisco DNA 中心上的自签名证书必须具有 cA:TRUE 的基本约束扩展（RFC5280 部分 4.2.19）。

注释 在早于 2.2.1.0 的Cisco DNA 中心版本中，需要启用 SSH。从Cisco DNA 中心版本 2.2.1.0 开始，不再使用 SSH，因此无需启用 SSH。

TrustSec 控制面板

TrustSec 控制面板是 TrustSec 网络中的一个集中式监控工具。

TrustSec 控制面板包含以下面板：

- **指标 (Metrics)**：“指标”(Metrics) Dashlet 显示与 TrustSec 网络行为有关的统计信息。
- **活动 SGT 会话 (Active SGT Sessions)**：“活动 SGT 会话”(Active SGT Sessions) Dashlet 显示网络中当前活动的 SGT 会话。“警报”(Alarms) Dashlet 显示与 TrustSec 会话相关的警报。
- **警报**
- **NAD/SGT/ACI 快速查看 (NAD / SGT/ACI Quick View)**：“快速查看” (Quick View) Dashlet 显示 NAD 和 SGT 的 TrustSec 相关信息。
- **TrustSec 会话/ NAD 活动/ACI 终端活动实时日志 (TrustSec Sessions / NAD Activity/ACI endpoint Activity Live Log)**：在“实时日志”(Live Log) Dashlet 中，点击“TrustSec 会话”(TrustSec Sessions) 链接可查看活动的 TrustSec 会话。您还可以查看有关 TrustSec 协议数据请求的信息，以及 NAD 发给Cisco ISE 的响应的信息。

指标

本节显示有关TrustSec网络行为的统计信息。您可以选择时间段（例如，过去2小时、过去2天等）和图表类型（例如，条形图、折线图、样条曲线图）。

图中显示了最新的数据条值。它还显示了相对于之前数据条的变化百分比。如果数据条值增加，则它将显示为绿色并带一个加号。如果值有所下降，则它将显示为红色并带一个减号。

将光标置于图形的数据条上，可查看该值的计算时间及其确切值，格式如下：<Value:xxxx Date/Time: xxx>

您可以查看以下指标：

SGT 会话	显示在所选时间段内创建的 SGT 会话总数。 **注释** SGT 会话是在授权流中接收 SGT 的用户会话。
正在使用的 SGT	显示在所选时间段内使用的唯一 SGT 总数。例如，如果在一个小时内有 200 个 TrustSec 会话，但在授权响应中 ISE 仅以 6 种类型的 SGT 进行响应，则图形将针对该小时显示值 6。
警报	显示在所选时间段内发生的警报和错误总数。错误以红色显示，而警报以黄色显示。
正在使用的 NAD	显示在所选时间段内参与 TrustSec 身份验证的唯一 NAD 数。

当前网络状态

控制面板的中间部分显示有关TrustSec网络当前状态的信息。在加载页面时，图中显示的值会更新，且可使用“刷新控制面板”(Refresh Dashboard) 选项刷新这些值。

活动 SGT 会话

此dashlet显示当前在网络中处于活动状态的SGT会话。您可以查看使用最多或最少的前10个SGT。X 轴显示 SGT 使用情况，Y 轴显示 SGT 的名称。

要查看 SGT 的 TrustSec 会话详细信息，请点击与该 SGT 对应的条形。与该 SGT 相关的 TrustSec 会话的详细信息显示在“实时日志”(Live Log) dashlet 中。

警报

此 dashlet 显示与 TrustSec 会话相关的警报。您可以查看以下详细信息：

- 警报严重性 - 显示一个表示警报严重性级别的图标。
  - 高 - 包括指示 TrustSec 网络中出现故障的警报（例如，设备无法刷新其 PAC）。用红色图标标记。
  - 中 - 包括指示网络设备配置错误的警告（例如，设备无法接受 CoA 消息）。用黄色标记。
  - 低 - 包括有关网络行为的一般信息和更新（例如，TrustSec 中的配置更改）。用蓝色标记。

- 警报说明
- 自上次重置此警报计数器以来发生的警报次数。
- 最后一次发生警报的时间

快速查看

“快速查看”(Quick View) 面板显示网络接入设备 (NAD) 的 TrustSec 相关信息。还可以查看 SGT 的 TrustSec 相关信息。

NAD 快速查看

在搜索框中输入您想要查看其详细信息的 TrustSec 网络设备的名称并按 **Enter**。搜索框提供自动填写功能，当用户在文本框中输入时，它可过滤设备名称并在下拉框中显示匹配的设备名称。

此 Dashlet 会显示以下信息：

- **NDG**：列出此网络设备所属的网络设备组 (NDG)。
- **IP 地址 (IP Address)**：显示网络设备的 IP 地址点击此链接可在“实时日志”(Live Logs) Dashlet 中查看 NAD 活动详细信息。
- **活动会话 (Active sessions)**：连接到此设备的活动 TrustSec 会话数。
- **PAC 有效期 (PAC expiry)**：显示 PAC 的到期日期。
- **上次策略更新时间 (Last Policy Refresh)**：显示策略的上次下载日期。
- **上次身份验证时间 (Last Authentication)**：显示此设备上次身份验证报告的时间戳。
- **活动 SGT (Active SGTs)**：列出在与此网络设备相关的活动会话中使用的 SGT。方括号中显示的数字表示当前正在使用该 SGT 的会话的数量。点击 SGT 链接，在“实时日志”(Live Log) Dashlet 中查看 TrustSec 会话的详细信息。

您可以使用“显示最新日志”(Show Latest Logs) 选项查看该设备的 NAD 活动实时日志。

SGT 快速查看

在搜索框中输入您想要查看详细信息的 SGT 的名称并按 **Enter**。

此 Dashlet 会显示以下信息：

- **值 (Value)**：显示 SGT 值（十进制和十六进制）。
- **图标 (Icon)**：显示分配给该 SGT 的图标。
- **活动会话 (Active sessions)**：列出当前正在使用该 SGT 的活动会话的数量。
- **唯一用户 (Unique users)**：列出在活动会话中持有该 SGT 的唯一用户的数量。
- **已更新的 NAD (Updated NADs)**：列出已下载用于该 SGT 的策略的 NAD 数量。

ACI 快速查看

此 Dashlet 会显示以下信息：

- **SDA SGTs**：列出Cisco ISE 发送到Cisco SD-Access 的 SGT 数量。
- **ACI EPGs**：列出Cisco ISE 从Cisco ACI 获取的 EPG 数量。
- **SDA 绑定 (SDA Bindings)**：列出Cisco ISE 发送到Cisco SD-Access 的绑定数量。
- **ACI 绑定 (ACI Bindings)**：列出Cisco ISE 从Cisco ACI 获知的绑定数量。
- **SDA VNs**：列出Cisco ISE 从Cisco SD-Access 获知的虚拟网络数量。
- **ACI VNs**：列出Cisco ISE 从Cisco ACI 获知的虚拟网络数量。
- **SDA 扩展 VN (SDA Extended VNs)**：列出从Cisco SD-Access 域发送到Cisco ACI 域的扩展虚拟网络数量。
- **SDA 租户 (SDA Tenant)**：显示Cisco SD-Access 与Cisco ISE 共享的租户的名称。
- **ACI 租户 (ACI Tenants)**：列出Cisco ACI 与Cisco SD-Access 共享的租户的数量。
- **SDA 域 ID (SDA Domain ID)**：显示Cisco SD-Access 的域 ID 编号。
- **ACI 域 ID (ACI Domain ID)**：显示Cisco ACI 的域 ID 编号。
- **对等状态 (Peering State)**：显示Cisco SD-Access 域与Cisco ACI 域之间对等关系的当前状态。

要了解有关Cisco软件定义接入（Cisco SD-Access）和Cisco以应用为中心的基础设施（Cisco ACI）的详细信息，请参阅TrustSec-思科 ACI 集成，第 932 页和思科 ACI 和思科 SD-Access 与虚拟网络感知的集成，第 935 页。

实时日志

点击 **TrustSec 会话 (TrustSec Sessions)** 链接查看活跃的 TrustSec 会话（响应中包含 SGT 的会话）。

点击 **NAD 活动 (NAD Activity)** 链接查看有关 TrustSec 协议数据请求和 NAD 对Cisco ISE 的响应的信息。

点击 **ACI 终端活动 (ACI endpoint Activity)** 链接，查看Cisco ISE 向Cisco ACI 学习的 IP-SGT 信息。

配置 TrustSec 全局设置

为了让Cisco ISE 充当 TrustSec 服务器并提供 TrustSec 服务，必须定义某些全局 TrustSec 设置。

开始之前

- 配置全局 TrustSec 设置之前，确保已定义全局 EAP-FAST 设置（依次选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP-FAST 设置 (EAP-FAST Settings)**）。

可以将 Authority Identity Info Description 更改为Cisco ISE 服务器名称。此说明是用户友好字符串，描述向终端客户端发送凭证的Cisco ISE 服务器。Cisco TrustSec 架构中的客户端可以是运行 EAP-FAST 作为其 EAP 方法进行 IEEE 802.1X 身份验证的终端，也可以是执行网络设备访问控制 (NDAC) 的请求方网络设备。客户端可以在受保护的访问凭证 (PAC) 类型长度值 (TLV) 信息中发现此字符串。默认值为 Identity Services Engine。应该更改此值，以便可以在 NDAC 身份验证时在网络设备上唯一识别Cisco ISE PAC 信息。

- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 通用 TrustSec 设置 (General TrustSec Settings)**

步骤 2 在字段中输入值。有关这些字段的信息，请参阅 常规 TrustSec 设置，第 890 页

步骤 3 点击**保存 (Save)**。

下一步做什么

- 配置 TrustSec 设备，第 895 页

常规 TrustSec 设置

定义全局 TrustSec 设置，以便Cisco ISE 作为 TrustSec 服务器运行。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 常规 TrustSec 设置 (General TrustSec Settings)**。

验证 Trustsec 部署 (Verify Trustsec Deployment)

此选项可帮助验证所有网络设备上是否部署了最新的 TrustSec 策略。如果在Cisco ISE 和网络设备上配置的策略之间存在任何差异，“警报”(Alarms) Dashlet 中会显示警报，该 Dashlet 位于**工作中心 (Work Centers) > TrustSec > 控制板和主页 (Dashboard and Home) > 摘要 (Summary)** 下。TrustSec 控制板中会显示以下警报：

- 每当验证过程开始或完成时，系统都会显示带有**信息 (Info)** 图标的警报。
- 如果由于新的部署请求而取消验证过程，则会显示带有**信息 (Info)** 图标的警报。
- 如果验证过程因错误而失败，则会显示带有**警告 (Warning)** 图标的警报。例如，无法打开与网络设备的 SSH 连接，或当网络设备不可用，或当Cisco ISE 和网络设备上配置的策略之间存在任何差异。

验证部署 (Verify Deployment) 选项也可从以下窗口选择。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择：

- **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)**
- **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**

- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 源树 (Source Tree)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 目标树 (Destination Tree)

每次部署后自动验证 (Automatic Verification After Every Deploy)：如果希望Cisco ISE 在每次部署后验证所有网络设备上的更新，请选中此复选框。部署过程完成后，经过您在**部署过程后的时间 (Time after Deploy Process)** 字段中指定的时间后，验证过程开始。

部署过程后的时间 (Time After Deploy Process)：指定您希望Cisco ISE 在部署过程完成后等待多长时间，然后再开始验证过程。有效范围为 10 – 60 分钟。

如果在等待期间收到新的部署请求或正在进行其他验证，则会取消当前验证过程。

立即验证 (Verify Now)：点击此选项可立即开始验证过程。

受保护的访问凭证 (PAC)

- **隧道 PAC 生存时间 (Tunnel PAC Time to Live)**：

  指定 PAC 的到期时间。隧道 PAC 为 EAP-FAST 协议生成隧道。您可以秒、分钟、小时、天或周为单位指定时间。默认值为 90 天。以下是有效范围：

  - 1 – 157680000 秒
  - 1 – 2628000 分钟
  - 1 – 43800 小时
  - 1 – 1825 天
  - 1 – 260 周

- **进行主动 PAC 更新前所经历的时间 (Proactive PAC Update Will Occur After)**：当剩余的隧道 PAC TTL 百分比达到设定值时，Cisco ISE 会在成功身份验证后主动向客户端提供新 PAC。如果第一次成功身份验证发生在 PAC 到期之前，则服务器会启动隧道 PAC 更新。此机制会为客户端更新有效的 PAC。默认值为 10%。

安全组标签编号

- **系统将分配 SGT 编号 (System will Assign SGT Numbers)**：如果希望Cisco ISE 自动生成 SGT 编号，请选择此选项。
- **除范围内的编号外 (Except Numbers in Range)**：选择此选项可保留一系列 SGT 编号以进行手动配置。Cisco ISE 在生成 SGT 时不会使用此范围的值。
- **用户必须手动输入 SGT 编号 (User Must Enter SGT Numbers Manually)**：选择此选项可手动定义 SGT 编号。

APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)

APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)：选中此复选框，指定编号范围以用于根据从 APIC 获取的 EPG 创建的 SGT。

自动创建安全组

创建授权规则时自动创建安全组 (Auto Create Security Groups When Creating Authorization Rules)：选中此复选框可在创建授权策略规则时自动创建 SGT。

如果选中此选项，**授权策略 (Authorization Policy)** 窗口顶部会显示以下消息：`开启自动安全组创建 (Auto Security Group Creation is On)`。

系统会根据规则属性命名自动创建的 SGT。

注释 当删除相应的授权策略规则时，不会删除自动创建的 SGT。

默认情况下，此选项在全新安装或升级后会被禁用。

- **自动命名选项 (Automatic Naming Options)**：使用此选项可定义自动创建的 SGT 的命名约定。

  （必填）**名称将包括 (Name Will Include)**：选择以下选项之一：

  - **规则名称**
  - **SGT 号**
  - **规则名称 (Rule name) 和 SGT 编号 (SGT number)**

  默认选中**规则名称 (Rule name)** 选项。

  或者，可以将以下信息添加到 SGT 名称：

  - **策略集名称 (Policy Set Name)**（此选项仅在已启用**策略集 (Policy Sets)** 时可用）
  - **前缀 (Prefix)**（最多 8 个字符)
  - **后缀 (Suffix)**（最多 8 个字符)

  根据您的选择，Cisco ISE 会在**示例名称 (Example Name)** 字段中显示一个 SGT 名称示例。

  如果存在名称相同的 SGT，ISE 会在 SGT 名称上附加 *_x*，其中 *x* 是从1（如果当前名称中未使用 1）开始的第一个值。如果新名称大于 32 个字符，Cisco ISE 会截取前 32 个字符。

IP SGT 主机名静态映射

IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames)：如果使用 FQDN 和主机名，则Cisco ISE 会在部署映射和检查部署状态的同时在 PAN 和 PSN 节点中查找对应的 IP 地址。您可以使用此选项指定为 DNS 查询返回的 IP 地址创建的映射数。您可以选择以下其中一个选项：

- **为 DNS 查询返回的所有 IP 地址创建映射 (Create mappings for all IP addresses returned by a DNS query)**

- **仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射 (Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query)**

用于网络设备的 TrustSec HTTP 服务

- **启用 HTTP 服务 (Enable HTTP Service)**：使用 HTTP 通过端口 9063 将 Trustsec 数据传输到网络设备。
- **在审核中包括整个响应负载正文 (Include entire response payload body in Audit)**：启用此选项可在审核日志中显示整个 TrustSec HTTP 响应负载正文。此选项可能会显着降低性能。当禁用此选项时，仅会记录 HTTP 信头、状态和身份验证信息。

相关主题

TrustSec 架构，第 882 页
TrustSec 组件，第 883 页
配置 TrustSec 全局设置，第 889 页

配置 TrustSec 矩阵

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**工作站 (Work Centers) > TrustSec >设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

步骤 3 在“TrustSec 矩阵设置”(TrustSec Matrix Settings) 页面输入所需的详细信息。

步骤 4 点击**保存 (Save)**。

TrustSec 表格设置

下表介绍“TrustSec 矩阵设置”(TrustSec Matrix Settings) 窗口上的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

表 *140:* 配置 *TrustSec* 表格设置

字段名称	使用指南
允许多个 SGACL (Allow Multiple SGACLs)	如果要在一个单元格中允许多个 SGACL 请选中此复选框。如果未选择此选项，Cisco ISE 只允许每个单元格一个 SGACL。 默认情况下，此选项在全新安装时禁用。 升级后，Cisco ISE 将扫描出口单元格，因此，如果识别到至少一个被分配多个 SGACL 的单元格，将允许管理员在单元格中添加多个 SGACL。否则，它仅允许每个单元格一个 SGACL。 **注释** 在禁用的多个 SGACL 之前，您必须编辑包含多个 SGACL 的单元格仅包含一个 SGACL。
允许监控 (Allow Monitoring)	选中此复选框可启用对表格中所有单元格的监控。如果禁用监控，“监控全部”(Monitor All) 图标会灰显，“编辑单元格”(Edit Cell) 对话中的“监控”(Monitor) 选项被禁用。 默认情况下，监控在全新安装禁用。 **注释** 在禁用表格级别的监控之前，必须禁用对当前接受监控的单元格的监控。
显示 SGT 数量 (Show SGT Numbers)	使用此选项可显示或隐藏表格单元格中 SGT 值（十进制和十六进制）。 默认情况下，SGT 值在单元格中显示。
外观设置 (Appearance Settings)	可提供以下选项： • **自定义设置 (Custom settings)**：最初显示默认主题（有颜色无图案）。您可以自主设置颜色和图案。 • **默认设置 (Default settings)**：预定义的有颜色无图案列表（不可编辑）。 • **辅助功能设置 (Accessibility settings)**：预定义的有颜色有图案列表（不可编辑）。

字段名称	使用指南
颜色/图案 (Color/Pattern)	要使表格更易读，可根据单元格颜色将颜色和图案应用于表格单元格。 提供以下显示类型： • **允许 IP/允许 IP 日志 (Permit IP/Permit IP Log)**：单元格内已配置 • **拒绝 IP/拒绝 IP 日志 (Deny IP/Deny IP Log)**：单元格内已配置 • **SGACL**：用于单元格内已配置的 SGACL • **允许 IP/允许 IP日志（沿用）(Permit IP/Permit IP Log (Inherited))**：从（非已配置单元格）默认策略中获取 • **拒绝 IP/拒绝 IP 日志（沿用）(Deny IP/Deny IP Log (Inherited))**：从（非已配置单元格）默认策略中获取 • **SGACL（沿用）(SGACLs (Inherited))**：从（非已配置单元格）默认策略中获取

相关主题

出口策略，第 906 页
矩阵视图，第 907 页
配置 TrustSec 矩阵，第 893 页

配置 TrustSec 设备

为了让Cisco ISE 处理来自启用 TrustSec 的设备的请求，您必须在Cisco ISE 中定义这些启用 TrustSec 的设备。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 网络设备 (Network Devices)**

步骤 2 点击**添加 (Add)**。

步骤 3 在 **Network Devices** 部分中输入所需信息。

步骤 4 选中 **Advanced Trustsec Settings** 复选框以配置支持 Trustsec 的设备。

步骤 5 点击**提交 (Submit)**。

OOB TrustSec PAC

所有 TrustSec 网络设备都将 TrustSec PAC 视为 EAP-FAST 协议的一部分。安全 RADIUS 协议也使用此 TrustSec PAC，其中 RADIUS 共享密钥是根据 PAC 携带的参数推导而来。这些参数中的 Initiator-ID 参数包含 TrustSec 网络设备身份，即设备 ID。

如果使用 TrustSec PAC 识别设备，并且在Cisco ISE 上为该设备配置的设备 ID 和 PAC 上的 Initiator-ID 之间不匹配，则身份验证失败。

有些 TrustSec 设备（例如Cisco防火墙 ASA）不支持 EAP-FAST 协议。因此，Cisco ISE 无法通过 EAP-FAST 使用 TrustSec PAC 调配这些设备。系统会在Cisco ISE 上生成 TrustSec PAC 并且需要手动将其复制到设备上，所以这又称为带外 (OOB) TrustSec PAC 生成。

当从Cisco ISE 生成 PAC 时，系统会生成使用加密密钥加密的 PAC 文件。

本节介绍以下主题：

从设置屏幕生成 TrustSec PAC

可以从设置屏幕生成 TrustSec PAC。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)**

步骤 2 从左侧的 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **EAP-FAST** > **生成 PAC (Generate PAC)**。

步骤 4 生成 TrustSec PAC。

从网络设备屏幕生成 TrustSec PAC

您可以从网络设备 屏幕生成 TrustSec PAC。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **TrustSec** > **组件 (Components)** > **网络设备 (Network Devices)**

步骤 2 点击**添加 (Add)**。您还可以从网络设备 导航窗格的操作图标上点击 **添加新设备 (Add new device)**。

步骤 3 如果要添加新设备，请提供设备名称。

步骤 4 选中**TrustSec 高级设置 (Advanced TrustSec Settings)** 复选框以配置 TrustSec 设备。

步骤 5 在**带外 (OOB) TrustSec PAC (Out of Band (OOB) TrustSec PAC)** 子部分下，点击**生成 PAC (Generate PAC)**。

步骤 6 提供以下详细信息：

- PAC Time to Live - 输入值（单位：天、周、月或年）。默认情况下，该值为一年。最小值为一天，最大值为十年。
- Encryption Key - 输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。

加密密钥用于对生成的文件中的 PAC 进行加密。此密钥也用于解密该设备上的 PAC 文件。因此，建议管理员保存加密密钥以供日后使用。

“身份”(Identity) 字段指定 TrustSec 网络设备的设备 ID，并且 EAP-FAST 协议会提供发起方 ID。如果此处输入的身份字符串与“网络设备创建”(Network Device creation) 页面中 TrustSec 部分下定义的设备 ID 不匹配，那么身份验证将会失败。

根据 PAC 存活时间 (PAC Time to Live) 计算到期日期。

步骤 7 点击**生成 PAC (Generate PAC)**。

从网络设备 列表屏幕生成 TrustSec PAC

您可以从网络设备 列表屏幕生成 TrustSec PAC。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 网络设备 (Network Devices)**

步骤 2 点击**网络设备 (Network Devices)**。

步骤 3 选中要为其生成 TrustSec PAC 的设备旁边的复选框，然后点击**生成 PAC (Generate PAC)**。

步骤 4 在字段中提供详细信息。

步骤 5 点击**生成 PAC (Generate PAC)**。

按钮

出口策略中的 Push 选项可以启动 CoA 通知，告知 Trustsec 设备立即从Cisco ISE 请求关于出口策略中的配置更改的更新。

配置 TrustSec AAA 服务器

可以在 AAA 服务器列表中配置启用了 Trustsec 的Cisco ISE 服务器列表。TrustSec 设备向其中任意服务器进行身份验证。点击“推送”(Push)时，此列表中的新服务器将下载到TrustSec 设备。当TrustSec 设备尝试进行身份验证时，它会从此列表中选择任意Cisco ISE 服务器。如果第一台服务器关闭或繁忙，TrustSec 设备可以向此列表中的任何其他服务器自行进行身份验证。默认情况下，主要Cisco ISE 服务器是 TrustSec AAA 服务器。建议您配置更多Cisco ISE 服务器，以获得更可靠的 Trustsec 环境。

此页面列出了部署中您已配置为 TrustSec AAA 服务器的Cisco ISE 服务器。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > TrustSec AAA 服务器 (TrustSec AAA Servers)**

步骤 2 点击**添加 (Add)**。

步骤 3 按如下所述输入值：

- “名称”(Name) - 要分配至此 AAA 服务器列表中的Cisco ISE 服务器的名称。此名称可与Cisco ISE 服务器的主机名不同。
- 说明 - 可选说明。
- IP - 您正添加到 AAA 服务器列表的Cisco ISE 服务器的 IP 地址。
- “端口”(Port) - TrustSec 设备与服务器之间进行通信所在的端口。默认值为 1812。

步骤 4 点击**推送**。

下一步做什么

配置安全组。

TrustSec HTTPS 服务器

默认情况下，Cisco ISE 使用 RADIUS 在Cisco ISE 和 Trustsec NAD 之间交换 Trustsec 环境数据。您可以将Cisco ISE 配置为使用 HTTPS，它比 RADIUS 更快、更可靠。Cisco ISE 使用 REST API 实施 HTTP 传输。

HTTPS 传输要求：

- 端口 9603 必须在 HTTPS 服务器和 Trustsec 网络设备之间开放。
- 连接到 PSN 的每个网络设备上的 HTTPS 服务器凭证必须是唯一的。
- Cisco交换机运行 16.12.2、17.1.1 或更高版本。

要配置 HTTPS 传输，请执行以下操作：

1. 在每个网络设备上，启用 HTTP 文件传输，并要求凭证。
2. 在Cisco ISE 中，在**常规 Trustsec 设置 (General Trustsec Settings)** 中启用**网络设备的 Trustsec REST API 服务 (Trustsec REST API Service for Network Devices)**。
3. 在Cisco ISE 中，编辑每个 PSN 的网络设备定义，选中**启用 HTTP REST API (Enable HTTP REST API)** 并输入网络设备的 HTTP 服务器的凭证。
4. 在Cisco ISE 中，将该网络设备作为 Trustsec HTTPs 服务器添加到 **Trustsec > 组件 (Components)** 下。

注释 如果仅为 HTTPS 配置一个节点，则未为 HTTPS 配置的 Trustsec 服务器不会显示在 Trustsec 服务器列表中。您必须在 HTTPS 部署中配置所有其他启用 Trustsec 的节点。如果未为 HTTPS 配置 PSN，则使用 RADIUS，并且所有Cisco ISE 都会列出此 Trustsec 部署中的所有 PSN 节点。

配置完成后，Cisco ISE 会在 **Trustsec > 网络设备 (Network Devices)** 下的 TrustSec 环境数据中返回已配置服务器的列表。

调试

在调试中启用 ERS。此设置记录所有 ERS 流量。请勿将此设置保持启用状态超过 30 分钟，以避免日志文件过载。

您可以通过选中 **Trustsec > 设置 (Settings) > 常规 TrustSec 设置 (General Trustsec Settings)** 上**网络设备的 Trustsec REST API 服务 (Trustsec REST API Service for Network Devices)** 下的**包括请求负载正文 (Include request payload body)**，启用其他审核信息。常规 TrustSec 设置

安全组配置

安全组 (SG) 或安全组标签 (SGT) 是在 TrustSec 策略配置中用到的元素。在可信任的网络中移动时，SGT连接到数据包。这些数据包在进入可信任的网络（入口）时被标记，离开可信任的网络（出口）时被取消标记。

SGT 按顺序生成，但您可以选择为 IP 到 SGT 映射保留一些 SGT。生成 SGT 时，Cisco ISE 跳过保留的编号。

TrustSec 服务使用这些 SGT 在出口实施 TrustSec 策略。

您可以在 Admin 门户从以下页面配置安全组：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)**
- 直接从出口策略页面： **配置 (Configure)** > **创建新安全组 (Create New Security Group)**。

更新多个 SGT 后，点击 **Push** 按钮，发起环境 CoA 通知。此环境 CoA 通知转至全部 TrustSec 网络设备，强迫它们开始策略/数据刷新请求。

在思科 ISE 中管理安全组

必备条件

要创建、编辑或删除安全组，您必须是超级管理员或系统管理员。

添加安全组

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components)> 安全组 (Security Groups)**。
2. 点击**添加 (Add)** 以添加新安全组。
3. 为新安全组输入名称和说明（可选）。
4. 如果要将此 SGT 传播至 Cisco ACI，请选中**传播至 ACI (Propagate to ACI)** 复选框。只有当与此 SGT 相关的 SXP 映射属于在 Cisco ACI“设置”(Settings) 页面中选择的同一 VPN 时，它们才会传播至 Cisco ACI。

   默认情况下该选项处于禁用状态。
5. 输入 Tag Value。标签值可以设置为手动输入或自动生成。您还可以为 SGT 保留范围。您可以从以下位置对其进行配置：“通用 TrustSec 设置”(General TrustSec Settings) 页面（**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 通用 TrustSec 设置 (General TrustSec Settings)**）。
6. 点击**保存 (Save)**。

删除安全组

您无法删除源或目标仍在使用的安全组。这包括映射到Cisco ISE 中的功能的默认组：

- 自带设备
- 访客
- TrustSec 设备
- 未知

将安全组导入思科 ISE

您可以使用逗号分隔值 (CSV) 文件将安全组导入Cisco ISE 节点。您必须在更新模板之后才能将安全组导入Cisco ISE。您不能同时运行同一资源类型的导入。例如，您无法同时导入来自两个不同导入文件的安全组。

您可以从管理员门户下载 CSV 模板，在模板中输入您的安全组详细信息，并将该目标保存为 CSV 文件，接着您就可以将此文件导入回Cisco ISE。

在导入安全组的过程中，您可以在Cisco ISE 遇到第一个错误时停止导入过程。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components)> 安全组 (Security Groups)**。

步骤 2 点击**导入 (Import)**。

步骤 3 点击**浏览 (Browse)** 从正在运行客户端浏览器的系统选择 CSV 文件。

步骤 4 选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。

步骤 5 点击**导入 (Import)**。

从思科 ISE 导出安全组

您可以将Cisco ISE 中配置的安全组导出为 CSV 文件，您可以使用此文件将这些安全组导入到其他 Cisco ISE 节点中。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**。

步骤 2 点击**导出 (Export)**。

步骤 3 要导出安全组，您可以执行下述操作中的一项：

- 选中要导出的组旁的复选框，然后选择 **导出 (Export) > 导出所选 (Export Selected)**。
- 选择 **导出 (Export) > 全部导出 (Export All)**以导出所有定义的安全组。

步骤 4 将 export.csv 文件保存到您的本地硬盘中。

添加 IP SGT 静态映射

您可以使用 IP-SGT 静态映射在 TrustSec 设备和 SXP 域上以统一的方式部署映射。当创建新的 IP-SGT 静态映射时，您可以指定要部署此映射的 SXP 域和设备。也可以将 IP - SGT 映射关联到一个映射组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在显示的**新 (New)** 区域中，从下拉列表中选择 **IP 地址 (IP Address)** 或**主机名 (Hostname)**，并在其旁边的字段中输入相应的值。

在后续步骤的**单独映射到 SGT (Map to SGT individually)** 选项中，可以指定要映射到的 SXP 域。但是，如果在此步骤中选择**主机名 (Hostname)**，则无法访问**发送到 SXP 域 (Send to SXP Domain)** 字段。要在下一步中添加 SXP 域，必须在此处选择 **IP 地址 (IP Address)**。

步骤 4 如果要使用现有映射组，点击**添加至映射组 (Add to a Mapping Group)**，并从**映射组 (Mapping Group)** 选择所需的组。

如果要将此 IP 地址/主机名单独映射到 SGT，请点击**单独映射到 SGT (Map to SGT Individually)** 并执行以下操作：

- 从 SGT 下拉列表中选择一个 SGT。
- 从下拉列表中选择用于映射的虚拟网络。
- 选择须部署映射的 SXP VPN 组。

- 指定要部署此映射的设备。您可以在所有 Trustsec 设备、选定的网络设备组或选定的网络设备上部署该映射。

步骤 5 点击**保存 (Save)**。

部署 IP SGT 静态映射

添加映射后，使用**部署 (Deploy)** 选项在目标网络设备上部署映射。即使您之前保存了这些映射，也必须明确地执行此操作。点击**检查状态 (Check Status)** 检查设备的配置状态。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**

步骤 2 选中要部署的映射旁边的复选框。如果要部署所有映射，请选中顶部的复选框。

步骤 3 点击 **Deploy**（部署）。

所有 TrustSec 设备都列在**部署 IP SGT 静态映射 (Deploy IP SGT Static Mapping)** 窗口中。

步骤 4 选中所选映射必须部署到的设备或设备组旁边的复选框。

- 如果要选择所有设备，请选中顶部的复选框。
- 使用过滤选项搜索特定的设备。
- 如果不选择任何设备，则所选映射将部署在所有 TrustSec 设备上。
- 选择要部署新映射的设备时，ISE 会选择将受新映射影响的**所有**设备。

步骤 5 点击 **Deploy**（部署）。部署按钮会更新受新映射影响的所有设备上的映射。

部署状态 (Deployment Status) 窗口显示设备更新顺序以及由于错误或设备无法访问而未更新的设备。部署完成后，窗口会显示已成功更新的设备总数和未更新的设备数量。

使用 **IP SGT 静态映射 (IP SGT Static Mapping)** 页面中的**检查状态 (Check Status)** 选项检查是否为特定设备的同一 IP 地址分配了不同的 SGT。您可以使用此选项查找映射冲突的设备、映射到多个 SGT 的 IP 地址以及分配到同一 IP 地址的 SGT。即使在部署中使用了设备组、FQDN、主机名或 IPv6 地址，也可以使用**检查状态 (Check Status)** 选项。在部署这些映射之前，必须删除冲突的映射或修改部署范围。

IPv6 地址可用于 IP SGT 静态映射。这些映射可以使用 SSH 或 SXP 传播到特定网络设备或网络设备组。

如果使用 FQDN 和主机名，Cisco ISE 会在部署映射和检查部署状态时查找 PAN 和 PSN 节点中对应的 IP 地址。

使用**常规 TrustSec 设置 (General TrustSec Settings)** 窗口中的 **IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames)** 选项可指定为 DNS 查询返回的 IP 地址创建的映射数。选择以下选项之一：

- 为 DNS 查询返回的所有 IP 地址创建映射。
- 仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射

将 IP SGT 静态映射导入到思科 ISE

您可以使用 CSV 文件导入 IP SGT 映射。

您还可以从管理门户下载 CSV 模板，输入您的映射详细信息，将该模板另存为 CSV 文件，然后将其导回Cisco ISE。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**

步骤 2 点击**导入 (Import)**。

步骤 3 点击**浏览 (Browse)** 从正在运行客户端浏览器的系统选择 CSV 文件。

步骤 4 点击**上传**。

从思科 ISE 导出 IP SGT 静态映射

您可以 CSV 文件的形式导出 IP SGT 映射。您可以使用此文件将这些映射导入到另一个Cisco ISE 节点。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**。

步骤 2 执行以下操作之一：

- 选中要导出的映射旁的复选框，然后选择**导出 (Export) > 已选择 (Selected)**。
- 选择**导出 (Export) > 所有 (All)** 导出所有映射。

步骤 3 将 mappings.csv 文件保存到您的本地硬盘中。

添加 SGT 映射组

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping) > 管理组 (Manage Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入映射组的名称和说明。

步骤 4 执行以下操作：

- 从 **SGT** 下拉列表中选择一个 SGT。
- 从下拉列表中选择映射的虚拟网络。
- 选择映射必须在其之上部署的 SXP VPN 组。
- 指定要部署映射的设备。您可以在所有 Trustsec 设备、选定的网络设备组或选定的网络设备上部署该映射。

步骤 5 点击**保存 (Save)**。

您可以将 IP SGT 映射从一个映射组移至到另一个映射组。

您还可以更新或删除映射和映射组。要更新一个映射或映射组，请选中要更新的映射或映射组旁边的复选框，然后点击**编辑 (Edit)**。要删除映射或映射组，请选中要删除的映射或映射组旁边的复选框，然后点击**垃圾 (Trash) > 选定 (Selected)**。当删除映射组时，该组内的 IP SGT 映射也会删除。

添加安全组访问控制列表

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**。

步骤 2 添加**添加 (Add)** 创建新安全组 ACL。

步骤 3 输入以下信息：

- Name - SGACL 的名称
- 说明 - SGACL 的可选说明
- IP Version - 此 SGACL 支持的 IP 版本：
  - IPv4 - 支持 IP 版本 4 (IPv4)
  - IPv6 - 支持 IP 版本 6 (IPv6)
  - Agnostic - 同时支持 IPv4 和 IPv6
- Security Group ACL Content - 访问控制列表 (ACL) 命令。例如：

  permit icmp

  deny ip

在ISE中未检查SGACL输入的语法。确保使用正确的语法，以便交换机、路由器和接入点可以正确无误地应用它们。默认策略可以配置为 **permit IP**、**permit ip log**、**deny ip** 或 **deny ip log**。TrustSec 网络设备将默认策略附加到特定信元策略的末尾。

以下是两个指导性的 SGACL 示例。两者都包含一个 final catch all 规则。第一个拒绝为 final catch all 规则，第二个则允许。

Permit_Web_SGACL

```
permit tcp dst eq 80 permit tcp dst eq 443 deny ip
```

Deny_JumpHost_Protocols

```
deny tcp dst eq 23 deny tcp dst eq 23 deny tcp dst eq 3389 permit ip
```

下表列出适用于 IOS、IOS XE 和 NS-OS 操作系统的 SGACL 语法。

SGACL CLI 和 ACE	**IOS、IOS XE 和 NX-OS 通用的语法**
config acl	deny, exit, no, permit
deny permit	ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp
deny tcp deny tcp src deny tcp dst	dst, log, src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst, log, src
deny tcp dst eq www deny tcp src eq www	range 0 65535

注释 某些Cisco交换机不允许使用连字符。所以 `permit dst eq 32767-65535` 无效。请使用 `permit dst eq range 32767 65535`。

步骤 4 点击**推送**。

“推送”(Push) 选项可启动 CoA 通知，告知 Trustsec 设备立即向Cisco ISE 请求关于配置更改的更新。

注释 Cisco ISE 具有以下预定义的 SGACL：Permit IP、Permit IP Log、Deny IP 和 Deny IP Log。您可以使用这些 SGACL 通过 GUI 或 ERS API 配置 TrustSec 矩阵。虽然这些 SGACL 未在 GUI 的“安全组 ACL”(Security Group ACLs) 列表页面中列出，但当您使用 ERS API 列出可用的 SGACL（ERS getAll 调用）时，这些 SGACL 将列出。

出口策略

出口表列出已保留和未保留的源和目标 SGT。此页还允许您过滤出口表以查看特定策略并保存这些预设过滤器。当源 SGT 尝试到达目标 SGT时，基于出口策略中定义的 TrustSec 策略，支持 TrustSec 的设备会执行 SGACL。Cisco ISE 创建并调配策略。

SGT 和 SGACL 是创建 TrustSec 策略的基础，在您创建 SGT 和 SGACL 后，通过将 SGACL 分配至源和目标 SGT，您就可以在二者之间建立起关系。

每个源 SGT 到目标 SGT 的组合即为出口策略中的一个信元。

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**

有三种方式查看出口策略：

- 源树视图
- 目标树视图
- 矩阵视图

源树视图

源树视图以折叠状态列出源 SGT 紧凑而且组织有序的视图。您可以展开任意源 SGT 以查看列出与所选源 SGT 相关的所有信息的内部表。该视图仅显示映射至目标 SGT 的源 SGT。如果您展开具体源 SGT，其将在表中列出映射至此源 SGT 的所有目标 SGT 和相应的策略 (SGACL)。

您会在某些字段旁边看到三个点 (...)。这表示此单元格包含更多信息。您可以将光标放在这三个点上以在快速视图弹出窗口中查看其余信息。当您将光标放在 SGT 名称或 SGACL 名称上时，系统会打开一个快速查看弹出窗口，显示该具体 SGT 或 SGACL 的内容。

目标树视图

目标树视图以折叠状态列出目标 SGT 的精简和组织视图。可以展开任意目标 SGT，以查看列出所有与该选定目标 SGT 相关的信息的内部表。此视图仅显示映射到源 SGT 的目标 SGT。如果展开特定目标 SGT，该 SGT 会在表中列出映射到此目标 SGT 的所有源 SGT，以及对应的策略 (SGACL)。

您会在某些字段旁边看到三个点(...)。这表示此单元格包含更多信息。您可以将光标放在这三个点上以在快速视图弹出窗口中查看其余信息。当您将光标放在 SGT 名称或 SGACL 名称上时，系统会打开一个快速查看弹出窗口，显示该具体 SGT 或 SGACL 的内容。

矩阵视图

出口策略的矩阵视图与电子表格类似。它包含两个轴：

- 源轴 - 此垂直轴列出所有源 SGT。
- 目标轴 - 此水平轴列出所有目标 SGT。

源 SGT 到目标 SGT 的映射以单元格表示。如果某个单元格包含数据，则表示对应的源 SGT 和目标 SGT 之间有一个映射。此矩阵视图中有两类单元格：

- 有映射的单元格 - 源和目标 SGT 对与一组有序的 SGACL 关联并且具有指定的状态。
- 无映射的单元格 - 源和目标 SGT 对不与任何 SGACL 关联并且不具有指定的状态。

出口策略单元格显示源 SGT、目标 SGT 和在 SGACL 下作为单独列表的 Final Catch All Rule，以逗号隔开。如果 Final Catch All Rule 设置为 None，则不显示。矩阵中空单元格表示无映射的单元格。

在出口策略矩阵视图中，您可以滚动浏览矩阵以查看所需单元格集。浏览器不会一次性加载全部矩阵数据。浏览器会请求服务器加载属于您所滚动浏览区域的数据。这样可以防止内存溢出和性能问题。

您可使用**视图 (View)** 下拉列表中的以下选项更改表格视图。

- 带 SGACL 名称压缩 - 如果选择此选项，空单元格会被隐藏，且单元格中显示 SGACL 名称。
- 不带 SGACL 名称压缩 - 空单元格会被隐藏，且单元格中不显示 SGACL 名称。当您要查看更多表格单元格和使用颜色、图案和图标（单元格状态）区分单元格时，此视图非常有用。
- 带 SGACL 名称全屏 - 如果选择此选项，左侧与上面的菜单会被隐藏，且单元格中显示 SGACL 名称。
- 不带 SGACL 名称全屏 - 选中此选项时，表格以全屏模式显示，且单元格中不显示 SGACL 名称。

ISE 允许您创建、命名并保存自定义视图。要创建自定义视图，请选择**显示 (Show) > 创建自定义视图 (Create Custom View)**。您还可以更新视图标准或删除未使用的视图。

此表格视图的 GUI 元素与源视图及目标视图的相同。但是，它还包括以下其他元素：

矩阵维度

通过 Matrix 视图中的 **Dimension** 下拉列表，可以设置矩阵的维度。

导入/导出矩阵

使用**导入 (Import)** 和**导出 (Export)** 按钮，您可以导入或导出矩阵。

创建自定义视图

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在矩阵视图 (Matrix View) 页面，从**显示 (Show)** 下拉列表中选择**创建自定义视图 (Create Custom View)** 选项。

步骤 2 在**编辑视图 (Edit View)** 对话框中，输入以下详细信息：

- “视图名称”(View Name) - 输入自定义视图的名称。
- “源安全组”(Source Security Groups) - 将要纳入自定义视图的 SGT 移至“显示”(Show) 转发框。
- “显示与目标相关”(Show Relevant for Destination) - 如果要覆盖您在“源安全组显示”(Source Security Group Show) 转发框中的选择，并复制“目标安全组隐藏”(Destination Security Group Hide) 转发框中的所有条目，选中此复选框。如果条目超过 200 个，将不能对数据进行复制，并且会显示警告消息。
- “目标安全组”(Destination Security Groups) - 将要纳入自定义视图的 SGT 移至“显示”(Show) 转发框。
- “显示与源相关”(Show Relevant for Source) - 如果要覆盖您在“目标安全组显示”(Destination Security Group Show) 转发框中的选择，并复制“源安全组隐藏”(Source Security Group Hide) 转发框中的所有条目，选中此复选框。
- “通过…排序矩阵”(Sort Matrix By) - 您可以选择以下其中一个选项：
  - “手动顺序”(Manual Order)
  - “标签号”(Tag Number)
  - “SGT 名称”(SGT Name)

步骤 3 点击**保存 (Save)**。

矩阵操作

通过矩阵进行导航

您可以通过矩阵进行导航，方法是使用光标拖曳矩阵内容区域，或者使用水平和垂直滚动条。您可以点击并按住某个单元格，沿任何方向拖曳该单元格以及整个矩阵内容。源栏和目标栏随单元格一起移动。选中某个单元格时，矩阵视图突出显示该单元格以及相应的行（源 SGT）和列（目标 SGT）。选定单元格的坐标（源 SGT 和目标 SGT）显示在矩阵内容区域的下方。

选中矩阵中的单元格

要选中矩阵视图中的某个单元格，请点击该单元格。选定的单元格会显示不同的颜色，并且源 SGT 和目标 SGT 会突出显示。要取消选中某个单元格，只需再次点击该单元格或者选中另一个单元格即可。不允许在矩阵视图中选中多个单元格。双击单元格以编辑单元格的配置。

从出口策略配置 SGACL

您可以直接从“出口策略”(Egress Policy) 页面创建安全组 ACL。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**。

步骤 2 从“源或目标树视图”(Source or Destination Tree View) 页面，选择**配置 (Configure) > 创建新的安全组 ACL (Create New Security Group ACL)**。

步骤 3 输入所需的详细信息，并点击**提交 (Submit)**。

配置工作进程设置

开始之前

要执行以下任务，您必须是超级管理员。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 工作流程设置 (Work Process Settings)**。

步骤 2 选择以下选项之一：

- 单个矩阵 (Single Matrix) - 如果要仅为 TrustSec 网络中的所有设备创建一个策略矩阵，请选择此选项。
- 多个矩阵 (Multiple Matrices) - 允许您为不同场景创建多个策略矩阵。您可以使用这些矩阵将不同的策略部署到不同的网络设备。

  注释 矩阵是独立的，并且每个网络设备只能分配给一个矩阵。

- 具有批准进程的生产和暂存矩阵 (Production and Staging Matrices with Approval Process) - 如果要启用工作流模式，请选择此选项。选择分配给编辑和审批人角色的用户。您可以仅从策略管理员和超级管理员组中选择用户。用户不能同时分配给编辑和审批人角色。

  对于已分配给编辑和审批人角色的用户，确保其电子邮件地址已配置，否则有关工作流程进程的电子邮件通知不会发送给这些用户。

  启用工作流模式后，分配到编辑器角色的用户可以创建暂存矩阵，选择要在其上部署暂存策略的设备，并将暂存策略提交给批准人以供批准。指定为审批人角色的用户可以审核暂存策略，并批准或拒绝请求。暂存策略只有经审批人审核并批准后，才可以在选择的网络设备上进行部署。

步骤 3 如果要创建 DEFCON 矩阵，请选中**使用 DEFCONS (Use DEFCONS)** 复选框。

DEFCON 矩阵是备用策略矩阵，可以在出现网络安全漏洞时轻松部署。

您可以创建以下严重性级别的 DEFCON 矩阵：Critical、Severe、Substantial 和 Moderate。

当激活 DEFCON 矩阵时，相应的 DEFCON 策略将立即部署在所有 TrustSec 网络设备上。您可以使用禁用 (Deactivate) 选项从网络设备中删除 DEFCON 策略。

步骤 4 点击保存 (Save)。

矩阵列表页面

TrustSec 策略矩阵和 DEFCON 矩阵列于矩阵列表 (Matrices Listing) 页面中。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵列表 (Matrices List)。您还可以查看分配给每个矩阵的设备数量。

注释 当启用单个矩阵模式并禁用 DEFCON 矩阵选项时，不会显示“矩阵列表”(Matrices Listing) 页面。

您可以在矩阵列表 (Matrices Listing) 页面执行以下操作：

- 添加新矩阵
- 编辑现有矩阵
- 删除矩阵
- 复制现有矩阵
- 将 NAD 分配到矩阵

通过使用分配 NAD (Assign NAD) 选项，可以将 NAD 分配到矩阵。为此：

1. 在“分配网络设备”(Assign Network Devices) 窗口中，选择要分配到矩阵的网络设备。还可以使用过滤器选项选择网络设备。
2. 从矩阵下拉列表中选择矩阵。所有现有矩阵和默认矩阵均列于此下拉列表中。

在向矩阵分配设备后，点击“推送”(Push) 向相关网络设备通知 TrustSec 配置更改。

在对矩阵列表 (Matrices Listing) 页面进行操作时，请注意以下问题：

- 您无法编辑、删除或重命名默认矩阵。
- 在创建新的矩阵时，您可以从空白矩阵开始，也可以从复制现有矩阵的策略开始。
- 如果删除矩阵，分配给该矩阵的 NAD 会自动移动到默认矩阵。
- 当您复制现有矩阵时，系统将创建矩阵副本，但不会自动将设备分配给此副本矩阵。
- 在多矩阵模式下，所有设备将在初始阶段分配到默认矩阵。
- 在多矩阵模式下，某些 SGACL 可能在矩阵之间共享。在这种情况下，更改 SGACL 内容将影响一个单元格中包含此 SGACL 的所有矩阵。
- 如果正在进行暂存，则无法启用多矩阵。
- 当您从多矩阵模式迁移到单个矩阵模式时，所有 NAD 将自动分配到默认矩阵。

- 如果当前已激活某个 DEFCON 矩阵活动，则无法删除该矩阵。

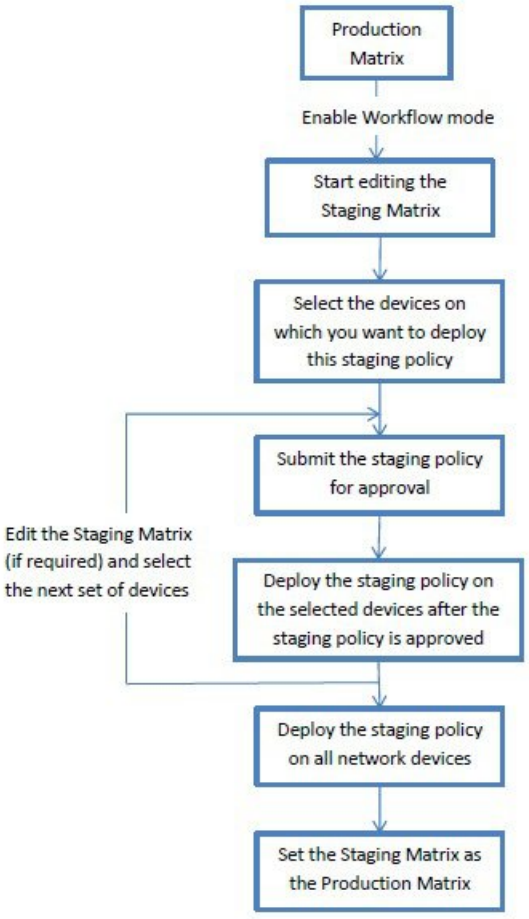
TrustSec 表格工作流过程

通过“表格工作流”(Matrix Workflow) 功能，您可以在所有网络设备上部署策略之前，使用该表格的草稿版（称为暂存表格）在一组有限的设备上测试该新策略。您可以提交暂存策略以供批准，并在获得批准后在选择的网络设备上部署该暂存策略。此功能可帮助您在有限数量的设备上部署新策略，检查是否工作正常，并在需要的时候做出更改。您可以继续在下一组设备或所有设备上部署该策略。当在所有的网络设备上部署暂存策略时，暂存表格可设置为新的生产表格。

启用工作流模式时，指定为编辑人角色的用户可以创建暂存表格，以及编辑表格中的单元格。该暂存表格是目前在 TrustSec 网络中部署的生产表格的副本。编辑人可以选择其希望部署暂存策略的设备，并提交暂存策略给审批人进行批准。指定为审批人角色的用户可以审核暂存策略，并批准或拒绝请求。暂存策略只有经审批人审核并批准后，才可以在选择的网络设备上进行部署。

下图中描述了工作流过程。

图 *47:* 表格工作流过程



超级管理员用户可以在**工作流过程设置 (Workflow Process Settings)** 页面中选择分配到编辑器和批准者角色的用户。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 工作流程 (Workflow Process)**。

在所选设备上部署暂存策略后，您将无法编辑 SGT 和 SGACL，但可以编辑表格中的单元格。您可以使用“配置 Delta”(Configuration Delta) 报告来跟踪生产表格和暂存表格之间的区别。您也可以点击单元格上 Delta 图标，查看暂存过程期间对单元格所做的更改。

下表介绍了工作流的不同阶段：

阶段	说明
编辑状态 (Staging in Edit)	当编辑人开始编辑暂存表格时，该表格将移至编辑状态。编辑完暂存表格后，编辑人可以选择其希望部署新的暂存策略的设备。
等待审批状态 (Staging Awaiting Approval)	编辑完表格后，编辑人提交暂存表格给审批人进行审核和批准。 提交有待审批的暂存表格时，编辑人可以添加评论，这些评论会通过邮件一起发送给审批人。 审批人可以审核暂存策略，并批准或拒绝请求。审批人还可以查看所选网络设备和配置 Delta 报告。在批准或拒绝请求时，审批人可以添加评论，这些评论会通过邮件一起发送给编辑人。 只要暂存策略没有在任何网络设备上部署，编辑人就可以取消审批请求。
部署已批准 (Deploy Approved)	当审批人批准请求时，暂存表格将移至部署已批准状态。当审批人拒绝请求时，表格则移回编辑状态。 只有在审批人批准了暂存策略后，编辑人才能将其部署在所选的网络设备上。
部分已部署 (Partially Deployed)	当在所选设备上部署暂存表格后，表格将移至部分已部署状态。直到暂存策略部署于所有的网络设备之前，该表格将维持在部分已部署状态。 在该阶段，您无法编辑 SGT 和 SFACL，但可以编辑表格中的单元格。 在网络设备部署 (Network Device Deployment) 窗口中，未部署最新策略的设备（不同步设备）显示为橙色（斜体）。配置进程状态栏中也会显示为该状态。编辑人可以选择这些设备，并请求批准对不同部署周期中更新的设备进行同步。

阶段	说明
已完全部署 (Fully Deployed)	直到暂存策略部署于所有的网络设备之前，系统将重复上述流程。当暂存策略部署于所有的网络设备后，审批人可以将暂存表格设置为生产表格。 由于在暂存表格替代生产表格后，您将无法回滚至先前的生产表格版本，因此我们建议您在设置暂存表格为生产表格之前，保留一个生产表格副本。

“工作流”(Workflow) 下拉列表中显示的选项会根据工作流状态和用户角色（编辑人或审批人）出现变化。下表中列出了编辑人和审批人界面显示的菜单选项：

工作流状态	编辑人视图显示的菜单	审批人视图显示的菜单
编辑状态	• 选择网络设备 网络设备配置窗口中提供以下选项： • 请求批准所选设备 • 请求批准所有/过滤的暂存列表 • 请求批准所有/过滤的生产列表 • 请求批准所有/过滤的设备 • 请求批准所有设备 • 丢弃暂存 • 查看 deltas	• 查看网络设备 • 查看 deltas
等待审批阶段 (Staging Awaiting Approval)	• 取消审批请求 • 查看网络设备 网络设备配置窗口中提供以下选项： • 取消审批请求 • 查看 deltas	• 批准部署 • 拒绝部署 • 查看网络设备 网络设备配置窗口中提供以下选项： • 批准部署 • 拒绝部署 • 查看 deltas

工作流状态	编辑人视图显示的菜单	审批人视图显示的菜单
已批准 - 部署就绪	• 部署 • 取消审批请求 • 查看网络设备 网络设备配置窗口中提供以下选项： • 部署 • 取消审批请求 • 查看 deltas	• 拒绝部署 • 查看网络设备 网络设备配置窗口中提供以下选项： • 拒绝部署 • 查看 deltas
部分已部署 (Partially deployed)	• 选择网络设备 网络设备配置窗口中提供以下选项： • 请求批准所选设备 • 请求批准所有/过滤的暂存列表 • 请求批准所有/过滤的生产列表 • 请求批准所有/过滤的设备 • 请求批准所有设备 • 查看 deltas	• 查看网络设备 • 查看 deltas

工作流状态	编辑人视图显示的菜单	审批人视图显示的菜单
已完全部署 (Fully deployed)	• 选择网络设备 网络设备配置窗口中提供以下选项： • 请求批准所选设备 • 请求批准所有/过滤的暂存列表 • 请求批准所有/过滤的生产列表 • 请求批准所有/过滤的设备 • 请求批准所有设备 • 查看 deltas	• 设置为生产 • 查看网络设备 • 查看 deltas

源和目的树视图中也提供这些工作流选项。

您可以使用 TrustSec 策略下载报告（“工作中心”[Work Centers] > TrustSec > “报告”[Reports]）查看下载了暂存/生产策略的设备。TrustSec 策略下载报告列出了网络设备发送的策略 (SGT/SGACL) 下载请求，以及 ISE 发送的详细信息。如果启用工作流模式，对于生产或暂存表，可对请求进行过滤。

出口策略表单元格配置

通过Cisco ISE，可以使用工具栏中可用的各种选项配置单元格。如果所选源和目标 SGT 与映射的单元格相同，则Cisco ISE 不允许进行单元格配置。

添加出口策略单元格映射

您可以从 Policy 页面添加出口策略的映射单元格。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**。

步骤 2 要选择矩阵单元格，请执行以下操作：

- 在矩阵视图中，点击某个单元格将其选定。
- 在 Source 和 Destination 树状视图中，选中内部表中某一行的对应复选框以选定该行。

步骤 3 点击**添加 (Add)** 以添加新映射单元格。

步骤 4 选择下列各项的相应值：

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

步骤 5 点击**保存 (Save)**。

导出出口策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix) > 导出 (Export)**。

步骤 2 如果要在导出文件中包括空信元（没有任何已配置 SGACL），请选中**包括空信元 (Include Empty Cells)** 复选框。

启用此选项后，整个矩阵会导出，空信元会在 SGACL 列中标有“空”关键字。

注释 确保导出文件不超过 500000 行，否则导出可能会失败。

步骤 3 选择以下选项之一：

- “本地磁盘”(Local Disk) - 如果要导出文件至本地驱动器，请选择此选项。
- “存储库”(Repository) - 如果要导出文件至远程存储库，请选择此选项。

  您必须在导出文件之前配置存储库。要配置存储库，请依次选择**管理 (Administration) > 维护 (Maintenance) > 存储库 (Repository)**。确保已授予选定存储库读取和写入权限。

  通过使用加密密钥，您可以加密导出文件。

  您可以更改文件名称。文件名不应超过 50 个字符。默认情况下，文件名包括当前时间，但是，如果远程存储库存在相同的文件名，则文件会被覆盖。

步骤 4 点击**导出 (Export)**。

导入出口策略

您可以离线创建出口策略，然后将该策略导入Cisco ISE。如果具有大量的安全组标记，那么逐个创建安全组 ACL 映射可能需要一些时间。相反，离线创建出口策略并将该策略导入Cisco ISE 可节省时间。在导入过程中，Cisco ISE 会将 CSV 文件中的条目附加到出口策略矩阵，并且不会覆盖数据。

如果出现以下情况，出口策略导入会失败：

- 源或目标 SGT 不存在
- SGACL 不存在
- 监控状态与当前在Cisco ISE 中为该信元配置的状态不同

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **TrustSec 策略 (TrustSec Policy)** > **出口策略 (Egress Policy)** > **矩阵 (Matrix)** > **导入 (Import)**。

步骤 2 点击**生成模版 (Generate a Template)**。

步骤 3 从“出口策略”(Egress Policy) 页面下载模板（CSV 文件），然后在 CSV 文件中输入以下信息：

- 源 SGT
- 目标 SGT
- SGACL
- 监控状态（启用、禁用或监控）

步骤 4 如果您要以正在导入的策略覆盖现有策略，请选中**用新数据覆盖现有数据 (Overwrite existing data with new data)** 复选框。如果导入文件中包括空信元（SGACL 列中标有“空”关键字的信元），相应矩阵信元中现有策略将被删除。

导出出口策略时，如果要包括空信元，请选中**包括空信元 (Include Empty Cells)** 复选框。有关详细信息，请参阅导出出口策略，第 916 页。

步骤 5 点击**验证文件 (Validate File)** 验证已导入的文件。Cisco ISE 会在导入文件之前验证 CSV 结构、SGT 名称、SGACL 和文件大小。

步骤 6 请选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，使Cisco ISE 在遇到任何错误时取消导入。

步骤 7 点击**导入**。

从出口策略配置 SGT

您可以直接从“出口策略”(Egress Policy) 页面创建安全组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **TrustSec 策略 (TrustSec Policy)** > **出口策略 (Egress Policy)**。

步骤 2 从“源或目标树视图”(Source or Destination Tree View) 页面，选择**配置 (Configure)** > **创建新的安全组 (Create New Security Group)**。

步骤 3 输入所需的详细信息，并点击**提交 (Submit)**。

监控模式

只需点击一下，您就可以通过出口策略中的 Monitor All 选项将整个出口策略配置状态改为监控模式。在出口策略页面，选中**Monitor All** 复选框，将所有单元的出口策略配置状态改为监控模式。选中 Monitor All 复选框后，配置状态中会发生以下更改：

- 状态为 Enabled 的单元将显示受监控行为，但看起来仍然像处于启用状态一样。
- 状态为 Disable 的单元不受影响。

- 状态为 Monitored 的单元仍保持 Monitored 状态。

取消选中**Monitor All**复选框即可恢复原始配置状态。这不会更改数据库中单元的实际状态。如果您取消选择 **Monitor All**，出口策略中的每个单元将恢复原配置状态。

监控模式功能

监控模式的监控功能可帮助您：

- 知悉已筛选但受监控模式监控的流量
- 知悉 SGT-DGT 对是处于监控模式还是执行模式，并且观察网络中是否在发生任何异常丢包
- 了解 SGACL 丢弃实际是由执行模式执行还是由监控模式允许
- 根据监控类型（监控和/或执行）创建自定义报告
- 标识在 NAD 上已应用的 SGACL 并显示差异（如有）

未知安全组

未知安全组是一个无法修改、使用标签值 0 表示 Trustsec 的预配置安全组。

当Cisco安全组网络设备没有来源或目标的 SGT 时，这些设备会请求引用未知 SGT 的信元。如果仅来源未知，则请求适用于 <unknown, Destination SGT> 信元。如果仅目标未知，则请求适用于 <source SGT, unknown> 信元。如果来源和目标均未知，则请求适用于 <Unknown, Unknown> 信元。

默认策略

默认策略是指 <ANY,ANY> 信元。所有源 SGT 均映射到所有目标 SGT。此处，ANY SGT 不可修改，且未在任何源或目标 SGT 中列出。ANY SGT 仅可与 ANY SGT 配对。ANY SGT 无法与其他任何 SGT 配对。TrustSec 网络设备将默认策略附加到特定信元策略的末尾。

- 如果信元为空，则意味着该信元仅包含默认策略。
- 如果信元包含某种策略，则生成的策略为信元特定策略与默认策略的组合。

根据Cisco ISE，信元策略和默认策略为两套独立的 SGACL，由设备分别获取以响应两个独立的策略查询。

默认策略的配置与其他信元不同：

- 状态仅可为两个值，启用或监控。
- 安全组 ACL 是默认策略的可选字段，因此可留空。
- 最终抓取所有规则可为以下任意项：允许 IP、拒绝 IP、允许 IP 日志或拒绝 IP 日志。显然此处 None 选项不可用，因为默认策略之外无安全网。

SGT 分配

如果您知道设备主机名或 IP 地址，Cisco ISE 允许向 TrustSec 设备分配 SGT。当具有特定主机名或 IP 地址的设备加入网络时，Cisco ISE 会在对其进行身份验证之前分配 SGT。

默认情况下将创建以下 SGT:

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

有时需要手动将设备配置为将安全组标签映射至终端。您可以从 Security Group Mappings 页面创建此映射。在执行此操作前，请确保您保留了一系列 SGT。

ISE 允许创建最多 10000 个 IP 到 SGT 映射。您可以创建 IP 到 SGT 映射组，从逻辑上将这些大规模的映射进行分组。每组 IP 到 SGT 映射都包含一个 IP 地址列表，其要映射的单个安全组，以及作为这些映射的部署目标的网络设备或网络设备组。

NDAC 授权

您可以通过向设备分配 SGT 配置 TrustSec 策略。您可以根据 TrustSec 设备 ID 属性向设备分配安全组。

配置 NDAC 授权

开始之前

- 确保创建用于策略中的安全组。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 网络设备授权 (Network Device Authorization)**。

步骤 2 点击 Default Rule 行右侧的 **Action** 图标，然后点击 **Insert New Row Above**。

步骤 3 为此规则输入名称。

步骤 4 点击 **Conditions** 旁边的加号 (+) 以添加策略条件。

步骤 5 您可以点击 **创建新条件（高级选项）**，然后创建新条件。

步骤 6 从**安全组 (Security Group)** 下拉列表中，选择在此条件评估为 true 的情况下要分配的 SGT。

步骤 7 在此行中点击 **Action** 图标，根据设备属性在当前规则上方或下方添加更多的规则。您可以重复此过程，为 TrustSec 策略创建所需的所有规则。您可以通过点击  图标，拖放规则以为其重新排序。您还可以复制现有条件，但请确保更改策略名称。

评估为 true 的第一条规则决定评估的结果。如果没有匹配的规则，则将应用默认规则；您可以编辑默认规则以指定在没有匹配的规则的情况下必须应用的 SGT。

步骤 8 点击**保存 (Save)** 以保存您的 TrustSec 策略。

如果在您配置了网络设备策略后 SGA 设备尝试进行身份验证，设备将获取其 SGT 及其对等设备的 SGT 并且将可以下载所有相关的详细信息。

注释 默认情况下，默认**网络设备授权 (Network Device Authorization)** 策略的结果设置为 **TrustSec_Devices**。

配置最终用户授权

Cisco ISE 允许您分配安全组作为授权策略评估的结果。使用此选项，您可以将安全组分配到用户和终端。

开始之前

- 请参阅授权策略的信息。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **授权策略 (Authorization Policy)**。

步骤 2 创建新的授权策略。

步骤 3 选择安全组的权限。

如果在此授权策略中指定的条件对用户或终端为真，则此安全组会被分配到该用户或终端，且该用户或终端所发送的所有数据包会标记为此特定的 SGT。

TrustSec 配置和策略推送

Cisco ISE 支持授权更改 (CoA)，通过 CoA Cisco ISE 可以通知 TrustSec 设备 TrustSec 配置和策略更改，这样设备就可以用获取相关数据的请求作为回复。

CoA 通知可以触发 TrustSec 网络设备发送环境 CoA 或策略 CoA。

您可以向本身不支持 TrustSec CoA 功能的设备推送对设备的配置更改。

支持 CoA 的网络设备

Cisco ISE 可向以下网络设备发送 CoA 通知：

- 具有单个 IP 地址的网络设备（不支持子网）
- 配置为 TrustSec 设备的网络设备
- 设置为支持 CoA 的网络设备

在有多个辅助设备与很多不同的设备互操作的分布式环境中部署Cisco ISE 时，CoA 请求从Cisco ISE 主节点发送至所有网络设备。因此，TrustSec 网络设备需要配置为将Cisco ISE 主节点作为 CoA 客户端。

设备向Cisco ISE 主节点返回 CoA NAK 或 ACK。但是，来自网络设备的以下 TrustSec 会话会发送至接收网络设备发送的所有其他 AAA 请求的Cisco ISE 节点，而不一定会发送至主节点。

向不支持 CoA 的设备推送配置更改

某些平台不支持Cisco ISE 的更改授权 (CoA)“推送”功能，例如：Nexus 网络设备的某些版本。对于这种情况，ISE 将连接到网络设备，使该设备触发对 ISE 的更新配置请求。为此，ISE 对网络设备开放 SSHv2 隧道，Cisco ISE 发送触发刷新 TrustSec 策略矩阵的命令。此方法也可以在支持 CoA 推送的网络平台上实施。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 选中所需网络设备旁边的复选框，然后点击**编辑 (Edit)**。

验证网络设备的名称、IP 地址、RADIUS 和 TrustSec 设置是否已正确配置。

步骤 3 向下滚动至 **TrustSec 高级设置 (Advanced TrustSec Settings)**，在 **TrustSec 通知和更新 (TrustSec Notifications and Updates)** 部分，选中**发送配置更改至设备 (Send configuration changes to device)** 复选框，点击 **CLI (SSH)** 单选按钮。

步骤 4 （可选） 提供 SSH 密钥。

步骤 5 选中**当部署安全组标记影射更新时包含此设备 (Include this device when deploying Security Group Tag Mapping Updates)** 复选框，使此 SGA 设备使用设备接口凭据获取 IP-SGT 映射。

步骤 6 输入拥有在执行模式下编辑设备配置的权限的用户的用户名和密码。

步骤 7 （可选） 输入密码，对设备启用执行模式密码，将允许编辑设备配置。可以点击**显示 (Show)**，显示已为此设备配置的执行模式密码。

步骤 8 点击页面底部的**提交 (Submit)**。

现在，网络设备已配置为推送 Trustsec 更改。更改Cisco ISE 策略后，点击**推送 (Push)**，让新配置在网络设备上体现出来。

SSH 密钥验证

可能想要使用 SSH 密钥增强安全性。Cisco ISE 利用其 SSH 密钥验证功能支持此操作。

要使用此功能，请打开从Cisco ISE 到网络设备的 SSHv2 隧道，然后使用网络设备的 CLI 检索 SSH 密钥。然后，复制此密钥，并将其粘贴到Cisco ISE 中进行验证。如果 SSH 密钥错误，Cisco ISE 将终止连接。

限制：目前，Cisco ISE 只能验证一个 IP（而不是 IP 范围，或者 IP 内的子网）

开始之前

您将需要：

- 登录凭证
- 检索 SSH 密钥的 CLI 命令

希望Cisco ISE 与其安全通信的网络设备。

步骤 1 在网络设备上：

a) 登录想要Cisco ISE 使用 SSH 密钥验证与其通信的网络设备。

b) 使用设备的 CLI 显示 SSH 密钥。

示例：

对于 Catalyst 设备，命令是：`sho ip ssh`。

c) 复制显示的 SSH 密钥。

步骤 2 从Cisco ISE 用户界面：

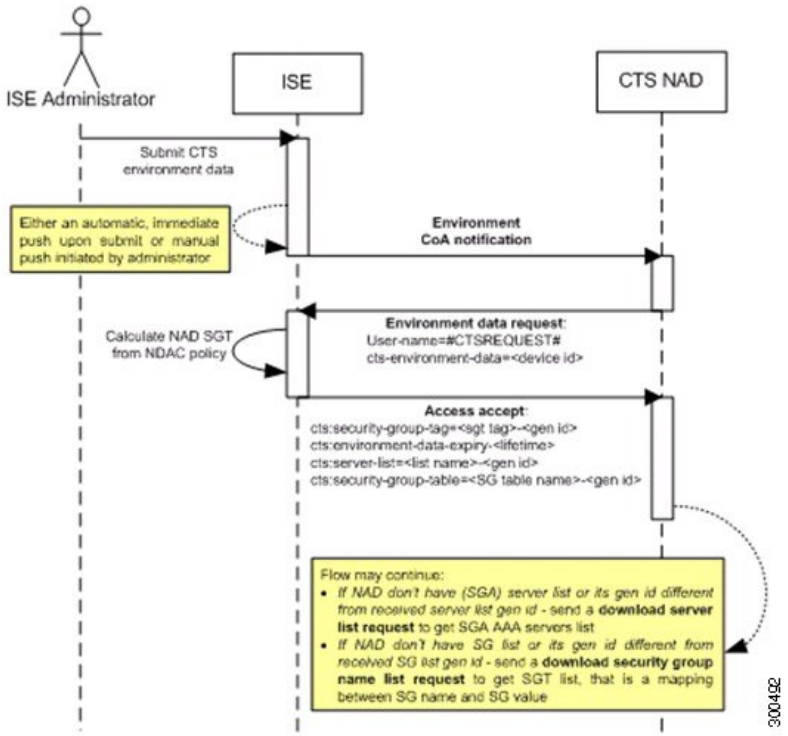
a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**，然后验证所需的网络设备名称、IP 地址、RADIUS 和 TrustSec 设置是否已正确配置。
b) 向下滚动至 **TrustSec 高级设置 (Advanced TrustSec Settings)**，在 **TrustSec 通知和更新 (TrustSec Notifications and Updates)** 部分，选中**发送配置更改到设备 (Send configuration changes to device)** 复选框，点击 **CLI (SSH)** 单选按钮。
c) 在 **SSH 密钥 (SSH Key)** 字段中，粘贴之前从网络设备检索的 SSH 密钥。
d) 点击页面底部的**提交 (Submit)**。

现在，网络设备可以使用 SSH 密钥验证与Cisco ISE 的通信。

环境 CoA 通知流程

下图显示环境 CoA 通知流程。

图 *48:* 环境 *CoA* 通知流程



1. Cisco ISE 向 TrustSec 网络设备发送环境 CoA 通知。
2. 设备返回环境数据请求。
3. Cisco ISE 返回以下数据以响应环境数据请求：

发送请求的设备的环境数据 - 这包括 TrustSec 设备的 SGT（根据 NDAC 策略推断）和下载环境 TTL。

TrustSec AAA 服务器列表的名称和生成 ID。

SGT 表（可能有多个）的名称和生成 ID - 这些表列出 SGT 名称和 SGT 值，并且这些表共同提供 SGT 的完整列表。

4. 如果设备不包含 TrustSec AAA 服务器列表，或者生成 ID 与所接收的生成 ID 不同，设备会再发送另一个请求以获取 AAA 服务器列表内容。
5. 如果设备不包含响应中列出的 SGT 表，或生成 ID 不同于所接收的生成 ID，则设备会发送另一个请求以获取该 SGT 表的内容。

环境 CoA 触发器

系统可以为以下因素触发环境 CoA：

- 网络设备
- 安全组
- AAA 服务器

为网络设备触发环境 CoA

要为网络设备触发环境 CoA，请完成以下步骤：

步骤 1 依次选择在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 添加或编辑网络设备。

步骤 3 更新 Advanced TrustSec Settings 部分下的 TrustSec Notifications 和 Updates 参数。

只有发生更改的特定 TrustSec 网络设备会收到更改环境属性的通知。

由于只有一个设备受到影响，环境 CoA 通知会在提交后立即发送。所产生的结果是对设备的环境属性进行更新。

为安全组触发环境 CoA

要为安全组触发环境 CoA，请完成以下步骤。

步骤 1 **工作中心 (Work Centers) > TrustSec > 组件 (Components)> 安全组 (Security Groups)**。

步骤 2 在 Security Group 页面中，更改 SGT 的名称，此操作将更改该 SGT 的映射值的名称。这会触发环境更改。

步骤 3 点击 **Push** 按钮，以在更改多个 SGT 的名称后发起环境 CoA 通知。此环境 CoA 通知会转至所有 TrustSec 网络设备并提供已更改的所有 SGT 的更新。

为 TrustSec AAA 服务器触发环境 CoA

要为 TrustSec AAA 服务触发环境 CoA，请完成以下步骤。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > TrustSec AAA 服务器 (TrustSec AAA Servers)**。

步骤 2 在 TrustSec AAA Servers 页面可以创建、删除或更新 TrustSec AAA 服务器的配置。这会触发环境更改。

步骤 3 在配置多个 TrustSec AAA 服务器之后，点击 **推送 (Push)** 按钮发起环境 CoA 通知。此环境 CoA 通知将发送到所有 TrustSec 网络设备并提供已更改的所有 TrustSec AAA 服务器的更新。

为 NDAC 策略触发环境 CoA

要为 NDAC 策略触发环境 CoA，请完成以下步骤。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > 策略 (Policy) > 网络设备授权 (Network Device Authorization)**。

在“NDAC 策略”(NDAC policy) 页面，您可以创建、删除或更新 NDAC 策略的规则。系统会向所有网络设备通知这些环境更改。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 网络设备授权 (Network Device Authorization)**。

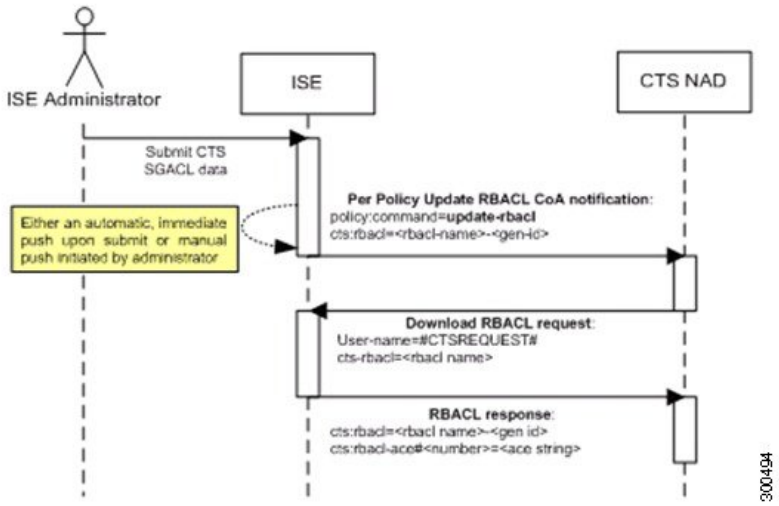
在“NDAC 策略”(NDAC policy) 页面，您可以创建、删除或更新 NDAC 策略的规则。系统会向所有网络设备通知这些环境更改。

步骤 3 您可以点击“NDAC 策略”(NDAC policy) 页面中的 **推送 (Push)** 按钮，发起环境 CoA 通知。此环境 CoA 通知将发送至所有 TrustSec 网络设备并更新网络设备自身 SGT。

更新 SGACL 内容流程

下图显示更新 SGACL 内容流程。

图 *49:* 更新 *SGACL* 内容流程



1. Cisco ISE 将更新 RBACL 命名列表 CoA 通知发送到 TrustSec 网络设备。通知包含 SGACL 名称和生成 ID。
2. 如果满足以下两个条件，设备可能会根据 SGT 数据请求进行重放：

   如果 SGACL 是设备所载出口信元的一部分。设备载有一个出口策略数据子集，这些数据是与相邻设备和终端的 SGT 相关的信元（选定目标 SGT 的出口策略列）。

   CoA 通知中的生成 ID 与设备为此 SGACL 保留的生成 ID 不同。
3. 为了响应 SGACL 数据请求，Cisco ISE 会返回 SGACL 的内容 (ACE)。

启动更新 SGACL 命名的列表 CoA

要触发更新 SGACL 命名的列表 CoA，请完成以下步骤：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **组件 (Components)** > **安全组 ACL (Security Group ACLs)**。

步骤 2 更改 SGACL 的内容。在您提交 SGACL 后，它会提高 SGACL 的生成 ID。

步骤 3 点击**推送 (Push)** 按钮以在您更改多个 SGACL 的内容之后发起更新 SGACL 命名的列表 CoA 通知。此通知将发送至所有 TrustSec 网络设备，并且在相关设备上提供该 SGACL 内容的更新。

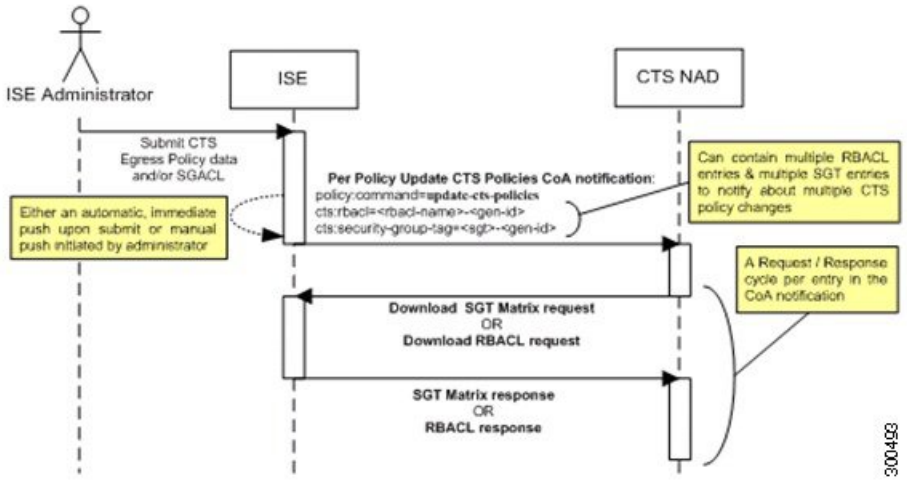
更改 SGACL 的名称或 IP 版本不会更改其生成 ID；因此不需要发送更新 RBACL 命名的列表 CoA 通知。

但是，如果更改出口策略中当前使用的 SGACL 的名称或 IP 版本，则会相应地更改包含该 SGACL 的单元格，并且这会更改该单元格目标 SGT 的生成 ID。

策略更新 CoA 通知流程

下图显示了策略 CoA 通知流程。

图 *50:* 策略 *CoA* 通知流程

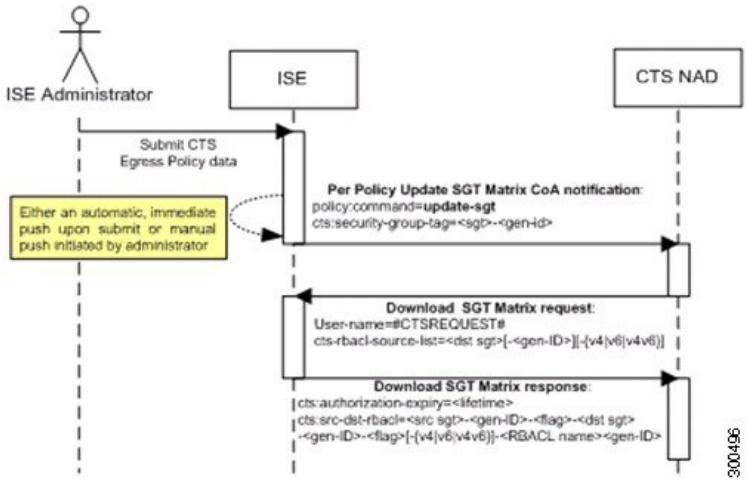


1. Cisco ISE 向 TrustSec 网络设备发送更新策略 CoA 通知。通知可以包含多个 SGACL 名称及其生成 ID，以及多个 SGT 值及其生成 ID。
2. 设备可能重放多个 SGACL 数据请求和/或多个 SGT 数据。
3. 作为对 SGACL 数据请求或 SGT 数据请求的响应，Cisco ISE 返回相关数据。

更新 SGT 矩阵 CoA 流程

下图显示了更新 SGT 矩阵 CoA 的流程。

图 *51:* 更新 *SGT* 矩阵 *CoA* 流程



1. Cisco ISE 将更新的 SGT 矩阵 CoA 通知发送到 TrustSec 网络设备。通知包含 SGT 值和生成 ID。
2. 如果满足以下两个条件，设备可以重放 SGT 数据请求：

   如果 SGT 是毗邻设备或终端的 SGT，设备将下载并保留与毗邻设备和终端的 SGT（目标 SGT）相关的信元。

   CoA 通知中的生成 ID 不同于设备为 SGT 保留的生成 ID。
3. 作为对 SGT 数据请求的响应，Cisco ISE 返回所有出口信元的数据，例如源 SGT 和目标 SGT、信元状态以及在此信元中配置的 SGACL 名称的顺序列表。

发起从出口策略更新 SGT 矩阵 CoA

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**。

步骤 2 在“出口策略”(Egress Policy) 页面，更改单元格的内容（状态、SGACL）。

步骤 3 在提交更改后，系统会提高该单元格目标 SGT 的生成 ID。

步骤 4 点击**推送 (Push)** 按钮以在您更改多个出口单元格的内容之后发起更新 SGACL 命名的列表 CoA 通知。此通知将发送至所有 TrustSec 网络设备，并且在相关设备上提供该单元格内容的更新。

TrustSec CoA 摘要

下表汇总了可能要求发起 TrustSec CoA 的各种场景、每个场景中使用的 CoA 的类型以及相关 UI 页面。

表 *141: TrustSec CoA* 摘要

UI 页面	触发 CoA 的操作	触发方式	CoA 类型	发送到
Network Device	更改页面的 TrustSec 部分中的环境 TTL	在成功提交 TrustSec 网络设备后	环境	特定网络设备
TrustSec AAA Server	TrustSec AAA 服务器中的任何更改（创建、更新、删除、重新排序）	可以通过点击 TrustSec AAA 服务器列表页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
Security Group	SGT 中的任何更改（创建、重命名、删除）	可以通过点击 SGT 列表页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备

UI 页面	触发 CoA 的操作	触发方式	CoA 类型	发送到
NDAC Policy	NDAC 策略中的任何更改（创建、更新、删除）	可以通过点击 NDAC 策略页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
SGACL	更改 SGACL ACE	可以通过点击 SGACL 列表页面中的 Push 按钮推送累积更改。	更新 RBACL 命名列表	所有 TrustSec 网络设备
	更改 SGACL 名称或 IP 版本	可以通过点击 SGACL 列表页面中的 Push 按钮或 Egress 表中的 Policy Push 按钮推送累积更改。	更新 SGT 矩阵	所有 TrustSec 网络设备
Egress Policy	用于更改 SGT 的生成 ID 的操作。	可以通过点击 Egress Policy 页面中的 Push 按钮推送累积更改。	更新 SGT 矩阵	所有 TrustSec 网络设备

安全组标记交换协议

安全组标记 (SGT) 交换协议 (SXP) 用于在所有不具备 TrustSec 硬件支持的网络设备中传播 SGT。SXP 可用于将终端的 SGT 和 IP 地址从一个可感知 SGT 的网络传输设备到另一个此类设备。SXP 传输的数据称为 IP-SGT 映射。属于终端的 SGT 可通过静态或动态的方式进行分配，并且 SGT 可在网络策略中用作分类器。

要在节点上启用 SXP 服务，请在“通用节点设置”(General Node Settings) 页面选中“启用 SXP 服务”(Enable SXP Service) 复选框。您还必须指定 SXP 服务使用的接口。

SXP 使用 TCP 作为传输协议，用于在两个单独的网络设备间建立 SXP 连接。每对 SXP 连接中，一个对等设备被指定为 SXP 发言者，另一个对等设备被指定为 SXP 倾听者。这两个对等设备也可在双向模式中进行配置，此类配置中两个对等设备都可作为发言者和倾听者。任一对等设备都可发起连接，但映射信息总是从发言者传播给倾听者。

注释 始终在默认 SXP 域中传播会话绑定。

下表列出了在 SXP 环境中的一些常用术语：

IP-SGT 映射	通过 SXP 连接交换的 IP 地址到 SGT 的映射。 要查看 SXP 设备学习到的所有映射（包括静态映射和会话映射），请选择**工作中心 (Work Centers) > TrustSec > SXP > 所有 SXP 映射 (All SXP Mappings)**。
SXP 发言者	通过 SXP 连接发送 IP-SGT 映射的对等设备。
SXP 倾听者	通过 SXP 连接接受 IP-SGT 映射的对等设备。

要查看添加到Cisco ISE 的 SXP 对等设备，请选择**工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices)**。

注释 我们建议您在独立节点上运行 SXP 服务。

使用 SXP 服务时,请注意以下几点：

- Cisco ISE 不支持具有相同 IP 地址的多个 SXP 会话绑定。
- 如果 RADIUS 计费更新太过频繁（例如，几秒钟内有大约 6 至 8 次计费更新），计费更新数据包可能会丢失，并且 SXP 可能未收到 IP-SGT 绑定。
- 从先前版本的 ISE 升级后，SXP 不会自动启动。在升级后，必须更改 SXP 密码并重新启动 SXP 过程。

添加 SXP 设备

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择**工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入设备详细信息：

- 点击**从 CSV 文件上传 (Upload from a CSV file)** 使用 CSV 文件添加 SXP 设备。浏览并选择 CSV 文件，然后点击**上传 (Upload)**。

  您也可以下载 CSV 模板文件，填写要添加设备的详细信息，并上传 CSV 文件。

- 点击**添加单个设备 (Add Single Device)** 为每个 SXP 设备手动添加设备的详细信息。

  输入名称、IP 地址、SXP 角色（侦听程序、扬声器或两者）、密码类型、SXP 版本和用于对等设备的连接 PSN。您还必须指定对等设备连接的 SXP 域。

步骤 4 (可选)点击**高级设置 (Advanced Settings)**，然后输入以下详细信息：

- “最短可接受保持时间”(Minimum Acceptable Hold Timer) - 指定时间（以秒为单位），扬声器将发送保持连接存活的保持存活消息。有效范围为 1 到 65534。
- “保持存活计时器”(Keep Alive Timer) - 在没有其他信息通过更新消息导出的间隔，扬声器用其触发保持连接消息的调度。有效范围为 0 到 64000。

步骤 5 点击**保存 (Save)**。

添加 SXP 域过滤器

可以查看 SXP 设备学习的所有映射（包括静态映射和会话映射）。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > SXP > 所有 SXP 映射 (All SXP Mappings)**

默认情况下，从网络设备学习的会话映射仅会发送到默认 VPN 组。您可以创建 SXP 域过滤器，以便将映射发送到不同的 SXP 域 (VPN)。

您将在此窗口中找到根据 IP-SGT 映射中配置的虚拟网络自动创建的映射。

注释 从思科 ISE 3.0 开始，网络设备可以属于多个 SXP 域。

要添加 SXP 域过滤器，请执行以下操作：

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > SXP > 所有 SXP 映射 (All SXP Mappings)**。

步骤 2 点击**添加 SXP 域过滤器 (Add SXP Domain Filter)**。

步骤 3 执行以下操作：

- 输入子网详细信息。具有来自此子网的 IP 地址的网络设备的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域 (VPN)。
- 从 SGT 下拉列表中选择一个 SGT。与此 SGT 相关的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域。

  如果已同时指定子网和 SGT，则与此过滤器匹配的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域。
- 从下拉列表中选择虚拟网络。与此虚拟网络相关的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域。

- 选择必须将映射发送到的 SXP 域。

步骤 4 点击**保存 (Save)**。

您还可以更新或删除 SXP 域过滤器。要更新过滤器，请点击**管理 SXP 域过滤器 (Manage SXP Domain Filter)**，选中要更新的过滤器旁的复选框，然后点击**编辑 (Edit)**。要删除过滤器，请选中要删除的过滤器旁的复选框，然后点击**回收站 (Trash) > 所选项 (Selected)**。

配置 SXP 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > SXP 设置**。

步骤 2 在“SXP 设置”(SXP Settings) 页面输入所需的详细信息。

如果您取消选中**发布 PxGrid 上 SXP 绑定**复选框，IP - SGT 映射不会在网络设备间传播。

步骤 3 点击**保存 (Save)**。

注释 当 SXP 设置更改时，SXP 服务重新启动。

TrustSec-思科 ACI 集成

Cisco ISE 可以将 SGT 和 SXP 映射与内部终端组 (IEPG)、外部终端组 (EEPG) 和Cisco以应用为中心的基础设施（Cisco ACI）的终端 (EP) 配置同步。

Cisco ISE 可通过同步 IEPG，并在 ISE 中创建关联的只读 SGT，支持将数据包从Cisco ACI 域发送到 TrustSec 域。这些 SGT 对Cisco ACI 中配置的终端进行映射，并在 ISE 中创建关联的 SXP 映射。这些 SGT 会显示在“安全组”(Security Group) 页面（“获知源”(Learned From) 字段的值为“Cisco ACI”(Cisco ACI)）。您可以在“所有 SXP 映射” (All SXP Mappings) 页面查看 SXP 映射。只有在已选择“策略平面”(Policy Plane) 选项（在“思科 ACI 设置”(Cisco ACI Settings) 页面中）且 SXP 设备属于您在“Cisco ACI 设置”(Cisco ACI Settings) 页面上设置的 SXP 域时，才会将这些映射发送到Cisco ACI。

注释 在 IP-SGT 映射、映射组和 SXP 本地映射中无法使用只读 SGT。

添加安全组时，可以通过启用**传播到 ACI (Propagate to ACI)** 选项指定是否将 SGT 发送到Cisco ACI。启用此选项后，与此 SGT 相关的 SXP 映射将发送到Cisco ACI。但是，只有在已选择“策略平面”(Policy Plane) 选项（在“思科 ACI 设置”(Cisco ACI Settings) 页面中）且 SXP 设备属于您在“Cisco ACI 设置”(Cisco ACI Settings) 页面上设置的 SXP 域时，才会发送这些映射。

Cisco ACI 可通过同步 SGT，并创建关联的 EEPG，支持将数据包从 TrustSec 域发送到Cisco ACI 域。Cisco ACI 根据来自Cisco ISE 的 SXP 映射在 EEPG 下创建子网。当在Cisco ISE 中删除了相应的 SXP 映射时，这些子网不会从Cisco ACI 中删除。

在Cisco ACI 中更新 IEPG 后，Cisco ISE 中的相应 SGT 配置也会更新。在Cisco ISE 中添加 SGT 后，Cisco ACI 中会创建新的 EEPG。删除 SGT 后，相应的 EEPG 也会在Cisco ACI 中删除。在Cisco ACI 中对终端进行更新后，Cisco ISE 中相应的 SXP 映射也会更新。

如果与Cisco ACI 服务器的连接丢失，则Cisco ISE 会在重新建立连接后重新同步数据。

注释 必须启用 SXP 服务，才能使用思科 ACI 集成功能。

可以在**所有 ACI 映射 (All ACI Mappings)** 窗口中查看Cisco ISE 与Cisco ACI 之间收发的所有绑定。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **TrustSec** > **ACI**。从Cisco ACI 获知绑定时，**获知者 (Learned By)** 列显示 **ACI**，并且**涉及的 PSN (PSNs involved)** 列为空。而当绑定从Cisco ISE 发送到Cisco ACI 时，**获知者 (Learned By)** 列将显示绑定类型（例如静态、SXP 或会话），**涉及的 PSN (PSNs involved)** 列显示所涉及的 PSN 的 FQDN。使用窗口中的过滤器选项可以监控完整列表中的特定映射。

注释 要成功集成Cisco ISE 和Cisco ACI，签名证书应具有适当的 SAN 字段。Cisco ISE 将使用 APIC 服务器提供的证书的 SAN 扩展属性中指定的值。

配置 ACI 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)**。

步骤 2 导入Cisco ACI 证书。有关详细信息，请参阅将根证书导入受信任证书库，第 154 页。

步骤 3 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **TrustSec** > **设置 (Settings)** > **ACI 设置 (ACI Settings)**。

步骤 4 选中**启用 ACI 集成 (Enable ACI Integration)** 复选框，向Cisco ACI 学习终端并使用 SXP 传播它们。

步骤 5 选择以下选项之一：

- 数据平面/硬件集成
- 策略平面/API 集成

注释　如果选择**数据平面/硬件集成 (Data Plane / Hardware Integration)**，则Cisco ISE 必须与Cisco DNA 中心集成。如果选择**策略平面/API 集成 (Policy Plane / API Integration)**，则在没有活动 SXP 服务的情况下无法进行 SXP 传播。在选择此选项之前，在**部署 (Deployment)** 窗口中激活 SXP 服务。

步骤 6 如果选择**数据平面/硬件集成 (Data Plane / Hardware Integration)**，请输入以下详细信息

- **IP 地址 (IP address)**：输入Cisco ACI 服务器的 IP 地址或主机名。可以输入三个 IP 地址或主机名，用逗号分隔。
- **用户名 (Username)**：输入Cisco ACI 管理员用户的用户名。
- **密码 (Password)**：输入Cisco ACI 管理员用户的密码。
- **租户名称 (Tenant name)**：输入在Cisco ACI 上配置的租户名称。
- **测试与 ACI 的连接 (Test Connection to ACI)**：点击此按钮可检查与Cisco ACI 服务器的连接。
- **续订证书 (Renew Certificate)**：点击此按钮可执行域管理器刷新。证书的有效期通常为 10 年。在续订证书之前，系统中应能成功进行对等互连。续订证书后，需要从部署中所有节点的 CLI 重新启动Cisco ISE 应用。续订证书的大概时间为 5 分钟。
- **新 SGT 后缀 (New SGT Suffix)**：此后缀将添加至根据从Cisco ACI 学习的 EPG 新创建的 SGT。

  注释　如果超过 32 个字符，EPG 名称会被截断。但是，您可以在“安全组”(Security Groups) 列表页面的“说明”(Description) 字段 查看 EPG 的全称，应用配置文件名称和 SGT 后缀详细信息。

- **新 EPG 后缀 (New EPG Suffix)**：此后缀将添加至Cisco ACI 中根据从Cisco ISE 学习的 SGT 新创建的 EPG。
- **启用数据平面 (Enable Data Plane)**：选中此复选框可下载边界路由器的转换表。如果启用此复选框，则必须为无法与任何其他现有 SGT 匹配的数据包选择默认 SGT 名称。
  - **默认 SGT 名称 (Default SGT name)**：从下拉列表中选择 SGT 的默认名称。
- **启用元素限制 (Enable Elements Limit)**：仅当启用数据平面时，此选项才可用。
  - **IEPG 的最大数量 (Max number of IEPGs)**：指定要转换为 SGT 的 IEPG 的最大数量。系统将按字母顺序转换 IEPG。默认值为 1000。
  - **SGT 的最大数量 (Max number of SGTs)**：指定将转换为 IEPG 的 SGT 的最大数量。系统将按字母顺序转换 SGT。默认值为 500。

步骤 7 如果选择了**策略平面 (Policy Plane)** 选项，则输入以下详细信息：

- **IP 地址/主机名 (IP address / Hostname)**：输入Cisco ACI 服务器的 IP 地址或主机名。可以输入三个 IP 地址或主机名，用逗号分隔。
- **管理员名称 (Admin name)**：输入Cisco ACI 管理员用户的用户名。
- **管理员密码 (Admin password)**：输入Cisco ACI 管理员用户的密码。

- **租户名称 (Tenant name)**：输入在Cisco ACI 上配置的租户名称。
- **L3 路由网络名称 (L3 Route network name)**：输入在Cisco ACI 上为同步策略元素而配置的第 3 层路由网络的名称。
- **测试设置 (Test Settings)**：点击此按钮检查与Cisco ACI 服务器的连接。
- **新 SGT 后缀 (New SGT Suffix)**：此后缀将添加至根据从Cisco ACI 学习的 EPG 新创建的 SGT。
- **新 EPG 后缀 (New EPG Suffix)**：此后缀将添加至Cisco ACI 中根据从Cisco ISE 学习的 SGT 新创建的 EPG。
- 在 **SXP 传播 (SXP Propagation)** 区域，可以选择所有 SXP 域或指定与Cisco ACI 共享映射的 SXP 域。
- **启用数据平面 (Enable Data Plane)**：选中此复选框可下载边界路由器的转换表。如果启用此复选框，则必须为无法与任何其他现有 SGT 匹配的数据包选择默认 SGT 名称。
  - **未标记数据包的 EEPG 名称 (EEPG name for untagged packets)**：未转换为 EEPG 的Cisco TrustSec 数据包在Cisco ACI 中使用此名称进行标记。
  - **默认 SGT 名称 (Default SGT name)**：从下拉列表中选择 SGT 的默认名称。
- **启用元素限制 (Enable Elements Limit)**：仅当启用数据平面时，此选项才可用。
  - **IEPG 的最大数量 (Max number of IEPGs)**：指定要转换为 SGT 的 IEPG 的最大数量。系统将按字母顺序转换 IEPG。默认值为 1000。
  - **SGT 的最大数量 (Max number of SGTs)**：指定将转换为 IEPG 的 SGT 的最大数量。系统将按字母顺序转换 SGT。默认值为 500。

步骤 8 点击**保存 (Save)**。

思科 ACI 和思科 SD-Access 与虚拟网络感知的集成

Cisco ISE 版本 2.7 中有一种基本的实施机制，可以将 SGT 和 SXP 映射同步到内部终端组 (IEPG)、外部终端组 (EEPG) 和Cisco ACI 的终端配置。

Cisco ISE 版本 3.0 支持一种额外的实施机制，为具有Cisco ACI 基础设施的Cisco软件定义接入 (SD-Access) 交换矩阵提供信息交换和跨域自动化的增强型转化。此实施机制在以下方面提供支持：

- 交换和转换 EPG 和 SGT 信息
- 将Cisco SD-Access 虚拟网络扩展到Cisco ACI 交换矩阵
- Cisco SD-Access 和Cisco ACI 交换矩阵数据平面自动化
- IP-SGT 绑定交换
- 将绑定发送到 pxGrid 和 SXP 域

Cisco ISE 从 RADIUS 绑定或Cisco ACI 绑定获知虚拟网络信息，并为特定虚拟网络提供本地静态映射。虚拟网络可用于增强 SXP 过滤器逻辑，利用该逻辑可协调与Cisco ACI 的 IP-SGT 绑定共享。请注意，因为扩展到Cisco ACI 的虚拟网络是与Cisco ACI 共享 IP-SGT 绑定的唯一结构，所以在这个意义上 SXP 域和虚拟网络是紧密关联的。因此，特定 SXP 域（以 SD-Access- 前缀表示）映射到Cisco ISE 中的等效虚拟网络（SXP 域减去 SD-Access- 前缀）。

为了让Cisco SD-Access 边界节点能了解Cisco ACI 绑定，Cisco ACI 绑定在复制之后再通过 SXP 过滤器逻辑发送出去，仿佛它们源自所有扩展的虚拟网络。例如，Cisco SD-Access 虚拟网络 1、虚拟网络 2 和虚拟网络 3 扩展到Cisco ACI，则Cisco ACI 与原始Cisco ACI 虚拟网络的绑定会通过 SXP 过滤器发送四次。这个完全相同的绑定将通过所有四个虚拟网络的过滤器。可以根据特定部署要求修改和自定义过滤器。但是，面向所有扩展虚拟网络的复制始终会发生。

Cisco ISE 尽可能从Cisco ACI 获知 IP-SGT、EPG 绑定。但是，Cisco ISE 无法强制Cisco ACI 获知任何绑定。Cisco ACI 必须明确向Cisco ISE 请求绑定信息。

下表列出了Cisco ISE 中 IP-SGT 或 IP-EPG 绑定可能存在的源和目标组合。

源域	目标域名	源分组	目标分组	注
Cisco ACI	SXP	Cisco ACI 虚拟网络	SXP 域	Cisco ACI 虚拟网络可用作 SXP 过滤器中的密钥，以与一个或多个 SXP 域共享绑定。
Cisco ACI	pxGrid	Cisco ACI 虚拟网络	PxGrid 上的 VPN for SXP 主题	Cisco ACI 虚拟网络可用作 SXP 过滤器中的密钥，以与 pxGrid 上的一个或多个 SXP VPN 共享绑定。
Cisco ACI	Cisco SD-Access 边界节点	Cisco SD-Access 扩展虚拟网络	SXP 域	Cisco ACI 绑定分享给为边界节点虚拟网络信息交换而自动创建的所有 SXP 域（有“SD-Access-”前缀的域）。
Cisco ISE 静态映射	SXP	Cisco SD-Access 虚拟网络或现有 SXP 域	SXP 域	静态绑定可以直接发送到 SXP 域（在静态映射中指定 SXP 域）或通过 SXP 过滤器发送（连同虚拟网络信息）。如果未指定虚拟网络，则 SXP 过滤器使用虚拟网络 DEFAULT_VN。
Cisco ISE 静态映射	pxGrid	Cisco SD-Access 虚拟网络	SXP 域	静态绑定可以直接发送到 SXP 域（在静态映射中指定 SXP 域）或通过 SXP 过滤器发送（连同虚拟网络信息）。如果未指定虚拟网络，则 SXP 过滤器使用虚拟网络 DEFAULT_VN。
Cisco ISE 静态映射	Cisco ACI	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络必须扩展到Cisco ACI (mdpExtendvirtual networkReq)，并且绑定使用 SXP 过滤器中的虚拟网络发送到 Cisco ACI，同时 SXP 域映射到虚拟网络。
SXP	pxGrid	SXP 域	SXP 域	SXP 域在 pxGrid 上的 SXP 主题中显示为 VPN。

SXP	Cisco ACI	SXP 域	Cisco SD-Access 虚拟网络	在Cisco ACI 设置下选择 SXP 域共享。 仅共享由Cisco SD-Access 虚拟网络自动创建的 SXP 域（虚拟网络等效 SXP 域）。 Cisco SD-Access 虚拟网络应扩展到Cisco ACI，以使虚拟网络有机会共享绑定。 绑定必须包含在让Cisco ACI 请求终端数据的消费者服务中。
SXP	SXP	SXP 域	SXP 域	通过优先级排序实现的 SXP 绑定是共享的。
RADIUS 绑定	Cisco ACI	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络	RADIUS 绑定通过 SXP 过滤器（连同虚拟网络信息）发送。如果未为绑定指定虚拟网络，则 SXP 过滤器使用虚拟网络 DEFAULT_VN。
RADIUS 绑定	pxGrid	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络	RADIUS 绑定进入 pxGrid 上的会话目录主题，虚拟网络字段也添加到该主题。
RADIUS 绑定	SXP	Cisco SD-Access 虚拟网络	SXP 域	Cisco SD-Access 虚拟网络可用作 SXP 过滤器中的密钥，以选择要与之共享绑定的 SXP 域。

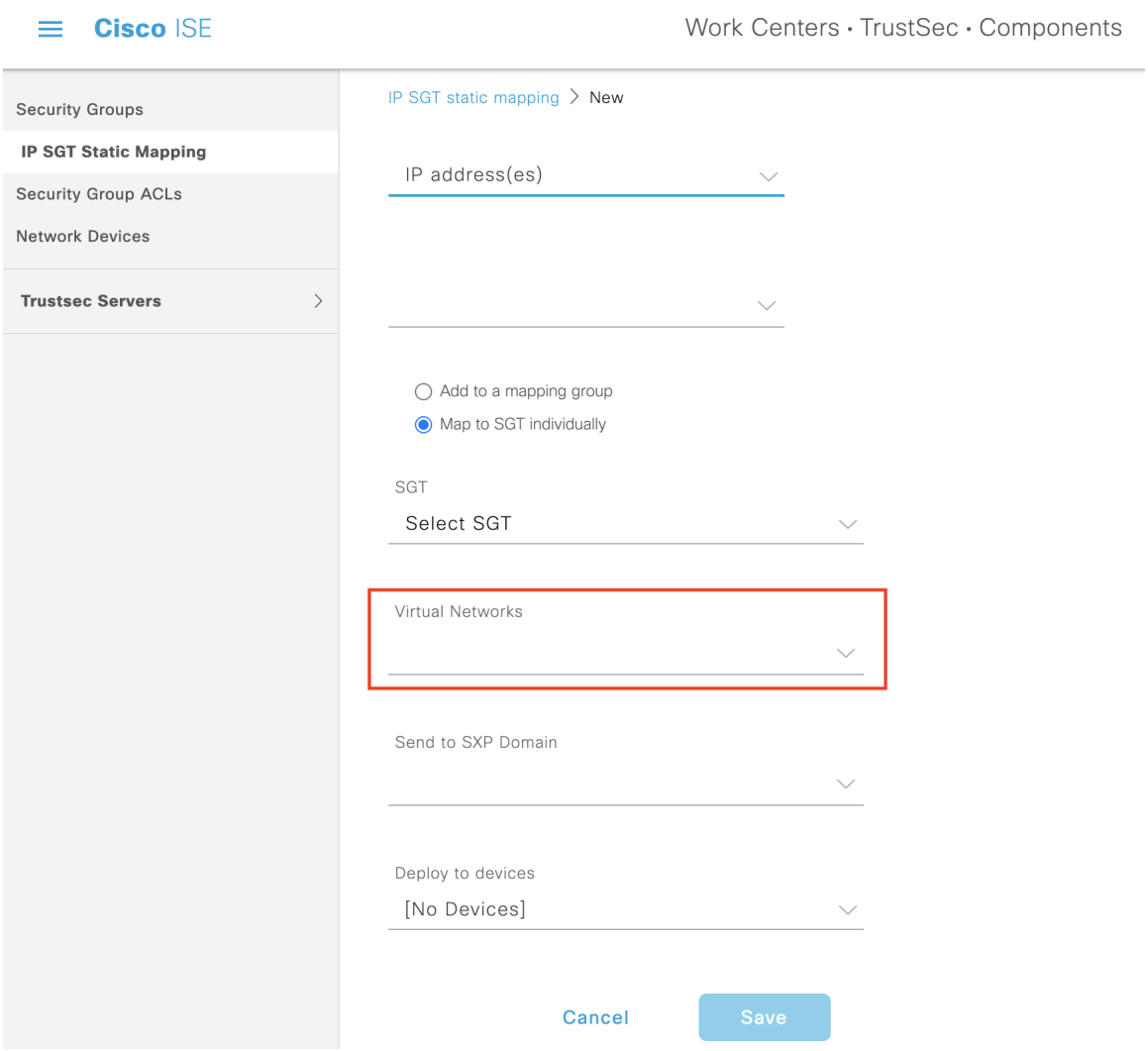
要促进跨域支持，您必须能够在两个策略域（或一个策略域内的转发域）之间交换和过滤各种网络转发域，例如 IP 地址、子网掩码、安全组标记、EPG、虚拟网络、虚拟路由和转发 (VRF)。当策略域（例如Cisco SD-Access、Cisco ACI、SD-WAN、CPC 和 Meraki）有多个转发域时，这一点尤其重要。

您可以识别、捕获和存储策略域的网络特定转发域以及从其他策略域获取的所有会话和绑定的域特定属性。策略管理员将使用这些属性将会话和绑定过滤到特定 SXP 域。此外，管理员还能创建策略，仅将特定绑定从一个转发域映射或过滤到另一个转发域。

从Cisco ISE 3.0 开始，在Cisco ISE 从 Cisco DNA Center 获知的每个虚拟网络中，您将在“SXP 设备”(SXP Devices) 窗口中找到自动创建的 SXP 过滤器和 SXP 域。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices)**。这些 SXP 域将用于在与Cisco ACI 共享的绑定中设置虚拟网络。

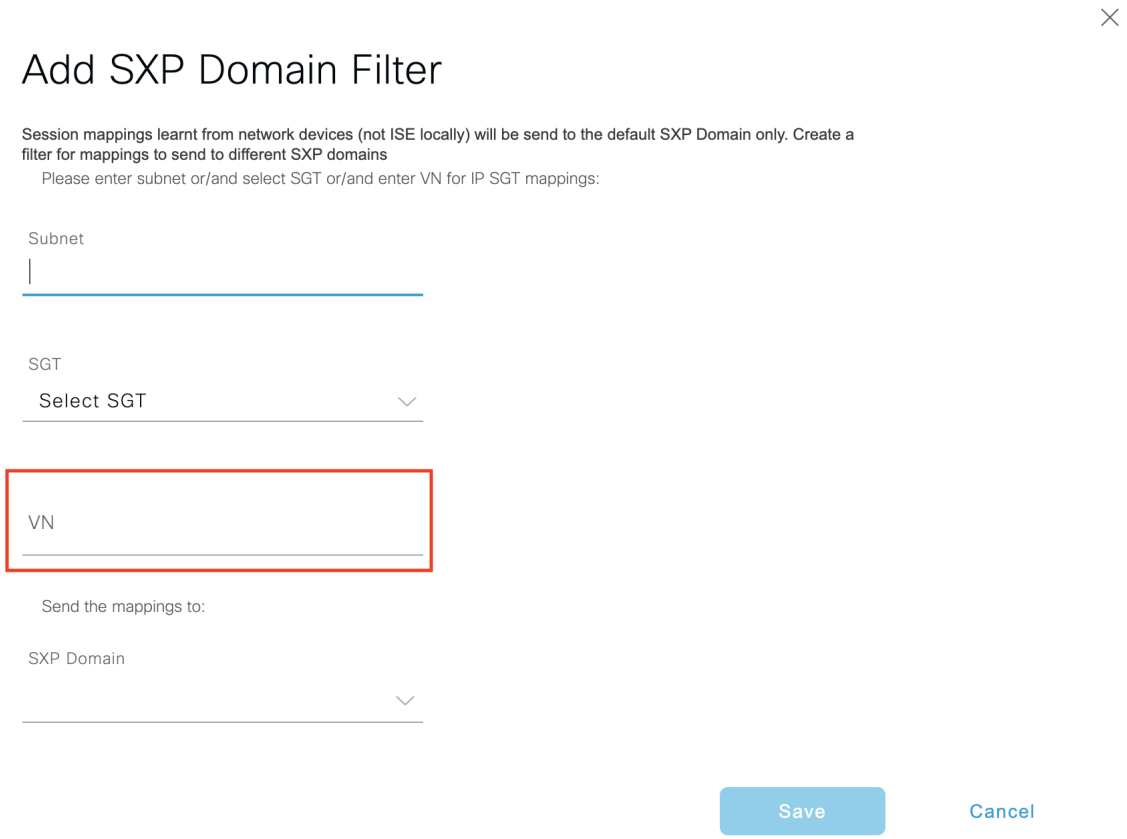
您可以在“IP-SGT 静态映射”(IP-SGT Static mapping) 窗口中向 IP-SGT 静态映射添加虚拟网络并编辑虚拟网络。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**。点击**添加 (Add)** 添加新映射，或点击**编辑 (Edit)** 修改现有映射。

图 *52*: 在 ***IP SGT*** 静态映射中添加虚拟网络



您还可以在 SXP 域过滤器中包含虚拟网络，以指定当Cisco ISE 收到的映射被映射到特定虚拟网络时将映射发送到哪个 SXP 域。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices) > 所有 SXP 映射 (All SXP Mappings)** 并点击**添加 SXP 域过滤器 (Add SXP Domain Filter)**。Cisco ACI 获知的绑定有原始Cisco ACI 虚拟网络，这些绑定发送到过滤器中配置的 SXP 域。此过滤器还会影响绑定发送到Cisco ACI 的方式。

图 *53:* 在 ***SXP*** 设备过滤器中添加虚拟网络信息



配置思科 ISE 以支持思科 ACI 和思科 SD-Access 集成

此任务可帮助您配置Cisco ISE 以支持Cisco ACI 和Cisco SD-Access 集成。

开始之前

确保Cisco ISE 与 Cisco DNA Center 的最新版本集成，并且使用的 APIC 版本为 5.1 或更高版本。

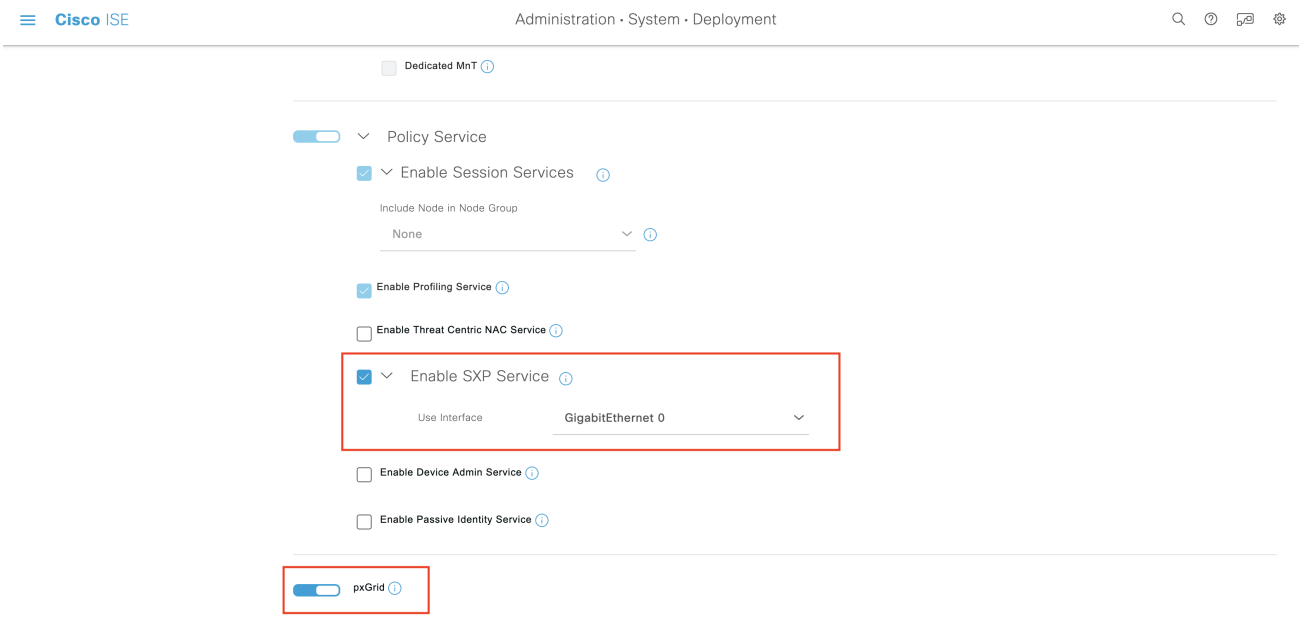
步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 从节点列表中，选中您想要启用 SXP 和 pxGrid 服务的节点旁边的复选框。

步骤 3 向下滚动到**策略服务 (Policy Service)** 部分并启用 pxGrid 和 SXP 服务，如下图所示。

如果您在Cisco ISE 上启用了多个接口，请在**启用 SXP 服务 (Enable SXP Service)** 区域中指定哪个接口将保持 SXP 连接。

图 *54:* 启用 ***SXP*** 和 ***pxGrid*** 服务



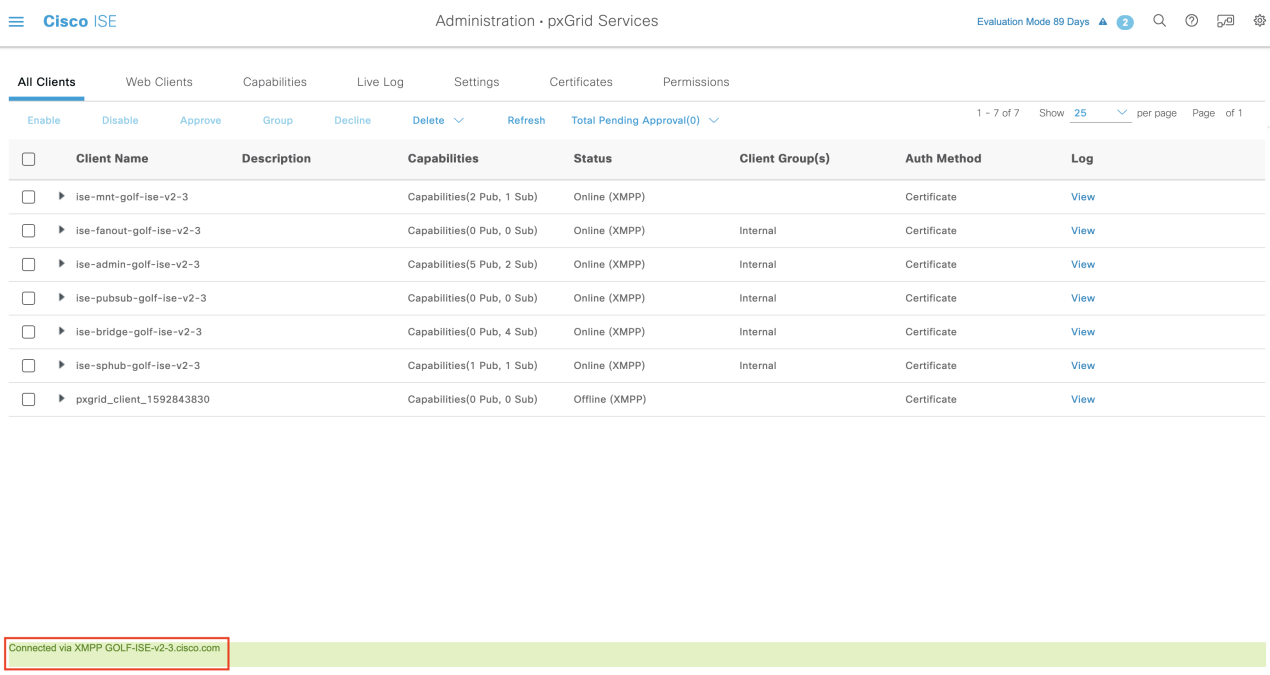
步骤 4 点击**保存 (Save)**。

步骤 5 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **所有客户端 (All Clients)**。

步骤 6 验证 pxGrid 服务是否已启动并正常运行。

连接成功的通知显示在窗口的左下角，如下图所示：

图 *55:* 验证与 *pxGrid* 服务的连接



步骤 7 从 APIC 控制器浏览器下载 APIC 证书。点击浏览器地址栏中的锁定图标，查看证书并将其下载为 PEM 文件。

步骤 8 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 9 在**受信任证书 (Trusted Certificates)** 窗口中导入下载的 APIC 证书文件。

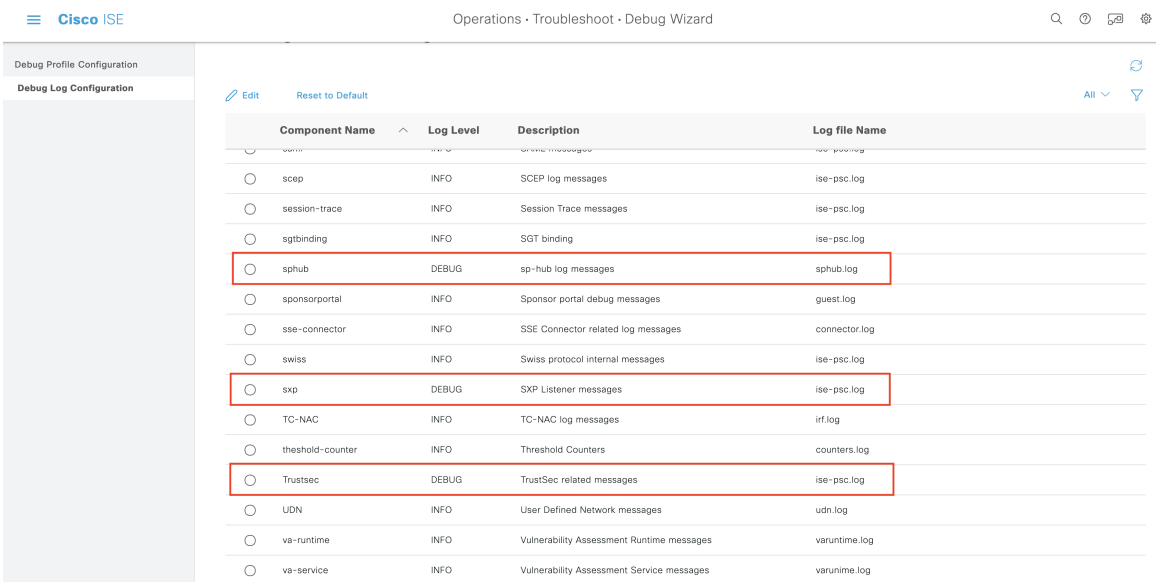
步骤 10 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centres)** > **TrustSec** > **设置 (Settings)** > **ACI 设置 (ACI Settings)**。

步骤 11 根据需要配置 ACI 设置。有关详细信息，请参阅配置 ACI 设置，第 933 页

验证思科 ACI 与思科 SD-Access 的集成

要获取Cisco ACI 和Cisco SD-Access 连接之间的详细信息，请选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)**。选择启用了 SXP 和 pxGrid 服务的Cisco ISE 节点，然后点击“编辑”(Edit)。如下图所示，将 **spbhub**、**sxp** 和 **TrustSec** 组件的日志级别设置为“调试”(DEBUG)。

图 *56:* 启用调试记录



这些日志可从**下载日志 (Dowload Logs)** 窗口下载。（要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)**.) 您可以选择从**支持捆绑包 (Support Bundle)** 选项卡下载支持捆绑包，也可以从**调试日志 (Debug Logs)** 选项卡下载特定调试日志。

此外，还可以使用从Cisco ACI 集成中吸取的信息增强TrustSec 控制面板，第 886 页，这对于排除 Cisco ACI 相关问题非常有用。

在Cisco DNA 中心发出域通告后，应同时在Cisco ISE 的**受信任证书 (Trusted Certificates)** 窗口和**系统证书 (System Certificates)** 窗口中确认 APIC 证书是否是从 APIC 域管理器获取的。

图 *57:* 在“系统证书”*(System Certificates)* 窗口中验证证书

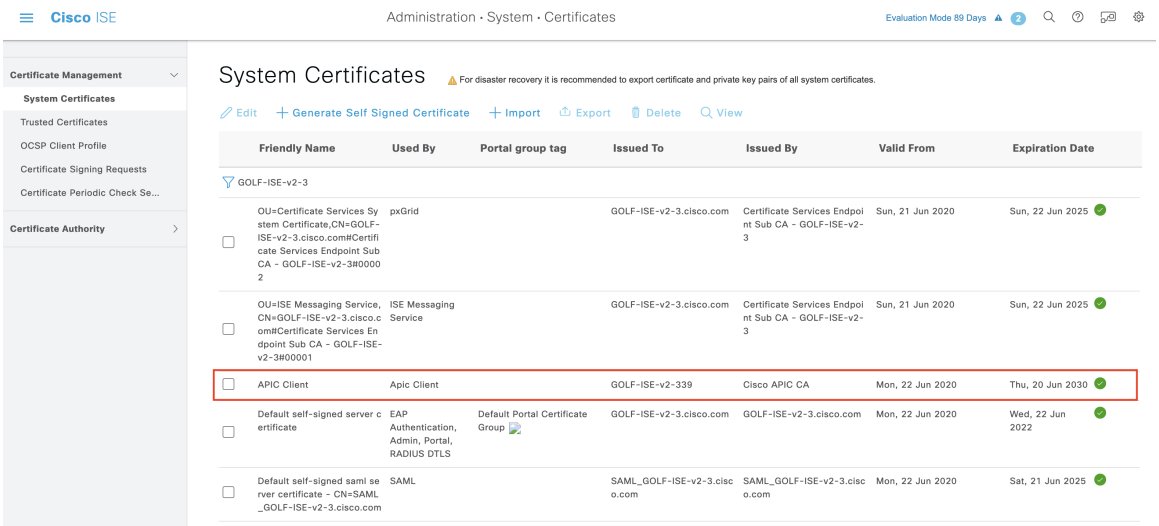
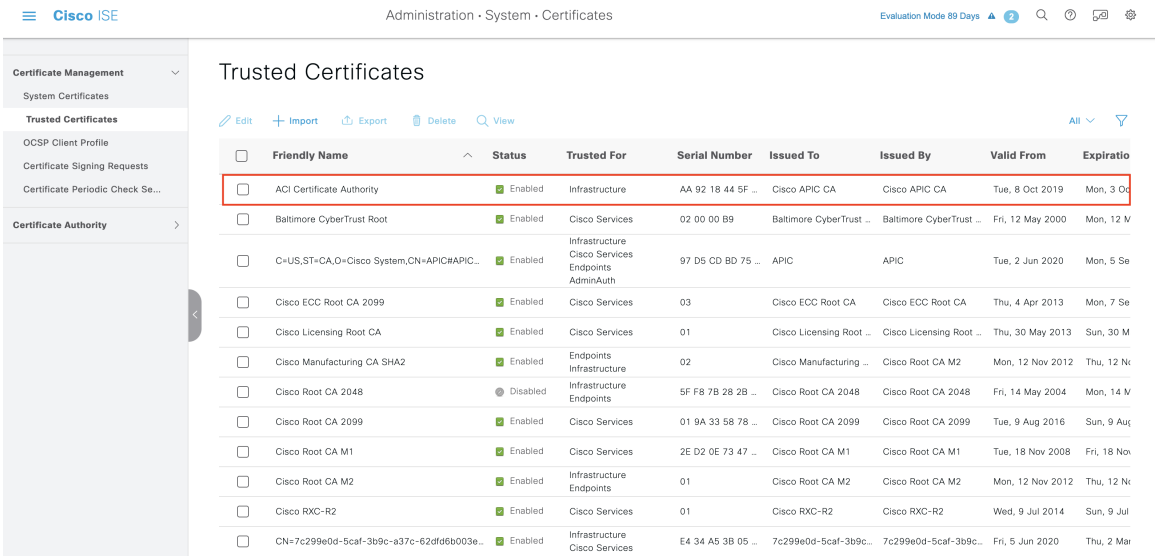


图 *58:* 在“受信任证书”*(Trusted Certificates)* 窗口中验证证书



按用户报告运行前 N 个 RBACL 丢包

可以按用户报告运行前 N 个 RBACL 丢包，以便按特定用户查看策略违规（基于丢包）。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**操作 (Operations)** > **报告 (Reports)** > **TrustSec**。

步骤 2 点击 **Top N RBACL Drops by User**。

步骤 3 从 **Filters** 下拉菜单中添加所需的监控模式。

步骤 4 相应地输入选定参数的值。可以从 Enforcement mode 下拉列表中将模式指定为 Enforce、Monitor 或 Both。

步骤 5 从 **Time Range** 下拉菜单中选择将收集报告数据的时间段。

步骤 6 点击**运行 (Run)** 在特定时间段内运行报告，以及选定的参数。

第 12 章

合规性

终端安全评估类型

以下终端安全评估代理可监控和实施Cisco ISE 终端安全评估策略：

- **AnyConnect**：部署 AnyConnect 代理以监控和实施需要客户端交互的Cisco ISE 策略。AnyConnect 代理留在客户端上。有关在Cisco ISE 中使用 AnyConnect 的详细信息，请参阅思科 AnyConnect 安全移动， 第 1043 页。

- **AnyConnect Stealth**：作为服务运行终端安全评估，没有用户界面。代理留在客户端上。

  当在终端安全评估要求中选择 AnyConnect Stealth 终端安全评估类型时，某些条件、补救或条件中的属性会被禁用（显示为灰色）。例如，当启用 AnyConnect Stealth 要求时，手动补救类型会被禁用（显示为灰色），因为此操作需要客户端交互。

  将终端安全评估配置文件映射到 AnyConnect 配置，然后将 AnyConnect 配置映射到 AnyConnect Stealth 模式部署的客户端调配 (Client Provisioning) 窗口，可支持：

  - AnyConnect 可以读取终端安全评估配置文件并将其设置为目标模式。
  - AnyConnect 可以在初始终端安全评估请求期间将与所选模式的相关信息发送到Cisco ISE。
  - Cisco ISE 可以根据模式和其他因素匹配正确的策略，如身份组、操作系统和合规性模块。

注释 AnyConnect Stealth 模式需要 AnyConnect 4.4 及更高版本。

有关在Cisco ISE 中配置 AnyConnect Stealth 的详细信息，请参阅配置 AnyConnect 隐身模式工作流程，第 1013 页。

- **临时代理**：当客户端尝试访问受信任网络时，Cisco ISE 会打开“客户端调配”(Client Provisioning) 门户。门户会指示用户下载并安装代理，然后运行代理。临时代理会检查合规性状态，并将状态发送到Cisco ISE。Cisco ISE 会根据结果采取行动。在合规性处理完成后，临时代理会将自身从客户端中删除。临时代理不支持自定义补救。默认补救仅支持消息文本。

  临时代理不支持以下条件：

  - 服务条件 macOS - 系统后台守护程序检查
  - 服务条件 macOS - 后台守护程序或用户代理检查
  - PM - 最新检查
  - PM - 已启用检查
  - DE - 加密检查
  - 使用**终端安全评估类型 (Posture Types)** **临时代理 (Temporal Agent)** 和**合规性模块 (Compliance Module) 4.x 或更高版本 (4.x or later)** 配置终端安全评估策略。请勿将合规性模块配置为 **3.x 或更低版本**或**任何版本**。
  - 对于临时代理，只能在**要求 (Requirements)** 窗口中查看包含**安装 (Installation)** 检查类型的补丁管理条件。
  - Cisco ISE 不支持使用 Mac OSX 临时代理的 VLAN 控制终端安全评估。当您将网络访问从现有 VLAN 更改为新 VLAN 时，用户的 IP 地址会在 VLAN 更改之前释放。当用户连接到新 VLAN 时，客户端通过 DHCP 获取新 IP 地址。识别新 IP 地址需要根权限，但临时代理作为用户进程运行。
  - Cisco ISE 支持 ACL 控制的终端安全评估环境，后者不需要刷新终端 IP 地址。
  - 有关在Cisco ISE 中配置临时代理的详细信息，请参阅配置思科临时代理工作流程，第 1018 页。

- **AMP 启用程序**：AMP 启用程序从托管在企业本地的服务器将面向终端软件的 AMP 推送到一部分终端，并将 AMP 服务安装到现有用户群中。此处介绍 AMP 分析器AMP 启用程序配置文件设置，第 1028 页。

- **无代理终端安全评估**：无代理终端安全评估提供来自客户的终端安全评估信息，并在完成后完全删除自身。最终用户无需执行任何操作。与临时代理不同，无代理终端安全评估以管理用户身份连接到客户端。有关在Cisco ISE 中使用无代理终端安全评估的详细信息，请参阅无代理终端安全评估 ，第 948 页。

“客户端调配”(Client Provisioning) 页面（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)**）和“终端安全评估要求”（Posture Requires）窗口（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)**）使用终端安全评估类型。最佳实践是在“客户端调配”(Client Provisioning) 窗口中调配终端安全评估配置文件。

相关主题

配置 AnyConnect 隐身模式工作流程，第 1013 页
配置思科临时代理工作流程，第 1018 页

无代理终端安全评估

无代理终端安全评估从客户端提供终端安全评估信息，并在完成后完全删除自身。最终用户无需执行任何操作。

要求

- 客户端必须可通过其 IP 地址访问，并且此 IP 地址必须在 RADIUS 记帐中可用。
- 目前支持 Windows 和 Mac 客户端。
  - 对于 Windows 客户端，必须打开访问客户端上 Powershell 的端口 5985。Powershell 必须为版本 5.1 或更高版本。
  - 对于 Mac OSX 客户端，必须打开访问 SSH 的端口 22 才能访问客户端。客户端必须具有 curl 版本 7.34 或更高版本。
- 用于外壳登录的客户端凭证必须具有本地管理员权限。
- 运行终端安全评估源更新以获取最新客户端，如配置步骤中所述。
- 确保在 sudoers 文件中更新以下条目，以避免在终端安装证书时失败：

  ```
  <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
  ```

- 对于 Mac OSX，配置的用户帐户必须是管理员帐户。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端脚本 (Endpoint Scripts)** > **登录配置 (Login Configuration)** > **MAC 登录用户 (MAC Local User)**。Mac OSX 的无代理终端安全评估不适用于任何其他帐户类型，即使您授予更多权限也是如此。

支持的终端安全评估条件

- 文件条件
- 服务条件
- 应用条件
- 外部数据源条件
- 复合条件

- 防恶意软件条件
- 补丁管理条件
- 防火墙条件
- 磁盘加密条件

不支持的终端安全评估条件

- 补救
- 宽限期
- 定期重新评估
- 可接受使用策略

支持的客户端操作系统

- Microsoft Windows 版本：10
- Mac OSX 版本：10.13、10.14、10.15

无代理终端安全评估流程

1. 客户端连接到网络。
2. Cisco ISE 检测是否已在客户端使用的授权配置文件中启用了无代理终端安全评估。
3. 如果是，Cisco ISE 会向Cisco ISE 消息队列发送无代理终端安全评估作业请求。
4. Cisco ISE 从消息队列获取作业，并启动无代理终端安全评估流程。
5. Cisco ISE 通过 Power Shell 或 SSH 连接到客户端。
6. 如果证书不在客户端的信任证书颁发机构存储区中，Cisco ISE 将推送证书。
7. Cisco ISE 运行客户端调配策略。
8. Cisco ISE 将无代理插件推送到客户端并启动该插件。
9. 终端安全评估在客户端上运行，并将状态发送到Cisco ISE。
10. Cisco ISE 从客户端删除无代理插件。终端安全评估流程的日志在客户端上保留 24 小时，或保留到客户端将其删除。

无代理终端安全评估配置

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)**，创建一个或多个使用无代理终端安全评估来标识要求的终端安全评估要求。

2. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > 终端安全评估 (Posture) > 终端安全评估策略 (Posture Policy)**，创建一个或多个使用无代理终端安全评估来标识终端安全评估要求的受支持终端安全评估策略规则。可以复制计划使用的规则，并将终端安全评估类型更改为“Agentless”(无代理)。

3. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authoriation) > 授权配置文件 (Authorization Profiles)**，创建从无代理终端安全评估来评估结果的授权配置文件。

   - 在授权配置文件中启用无代理终端安全评估。
   - 仅将此配置文件用于无代理终端安全评估。请勿将其用于其他终端安全评估类型。
   - CWA 和重定向 ACL 不是无代理终端安全评估所必需的。可以将 VLAN、DACL 或 ACL 用作分段规则的一部分。

4. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 客户端调配 (Client Provisioning)**，添加客户端调配策略。对于Cisco代理配置，选择适于您配置的操作系统的无代理插件。对于 Windows，此插件为 CiscoAgentlessWindows 4.9.01095。对于 MacOS，此插件为 CiscoAgentlessOSX 4.9.01095。选择此规则检查的终端安全评估条件。请注意，如果您使用的是 Active Directory，可以在策略中使用 Active Directory 组。

   注释 只有在更新终端安全状态源之后，适于 MACOSX 10.14 和 10.15 版本的无代理终端安全评估配置才可用。请先更新终端安全评估 URL，然后才能运行终端安全评估源。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **设置 (Settings)** > **软件更新 (Software Updates)** > **终端安全评估更新 (Posture Updates)**。在**终端安全评估更新 (Posture Updates)** 窗口中，在**更新源 URL (Update Feed URL)** 字段中输入 URL (https://www.cisco.com/web/secure/spa/posture-update.xml)，然后点击**立即更新 (Update Now)**。

5. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略集 (Policy Sets)**，展开“授权策略”(Authorization Policy)。启用并配置以下三个授权策略：

   - **Unknown_Compliance_Redirect**：使用结果“无代理终端安全评估”(Agentless Posture) 配置条件 Network_Access_Authentication_Passed 和 Compliance_Unknown_Devices。
   - **NonCompliant_Devices_Redirect**：使用结果“DenyAccess”配置条件 Network_Access_Authentication_Passed 和 Non_Compliant_Devices。
   - **Compliant_Devices_Access**：使用结果“PermitAccess”配置条件 Network_Access_Authentication_Passed 和 Compliant_Devices。

6. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration) > 设置 (Settings) > 终端脚本 (Endpoint Scripts) > 终端登录配置 (Endpoint Login Configuration)**，配置客户端凭证以登录客户端。这些相同凭证由终端脚本使用。有关详细信息，请参阅 <<Link to Endpoint Scripts topic>>。

7. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration) > 设置 (Settings) > 终端脚本 (Endpoint Scripts) > 设置 (Settings)**，并配置**操作系统标识的最大重试次数 (Max retry attempts for OS identification)** 和**操作系统标识重试之间的延迟 (Delay between retries for OS identification)**。这些设置决定了确认连接问题的速度。例如，表明 PowerShell 端口未打开的错误仅在所有重试未用尽后才会显示在日志中。
8. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings)**，配置“无代理终端安全评估”(Agentless Posture) 设置。请参阅安全评估常规设置，第 959 页。
9. 当客户端与无代理终端安全评估连接时，可以在实时日志中进行查看。

调试和故障排除

为以下项启用调试日志级别：

- 基础设施
- 客户端调配
- 终端安全评估

调试日志位于 *ise-psc.log* 中

无代理终端安全评估故障排除在以下位置提供：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 实时日志 (Live Logs)** - “终端安全评估状态”(Posture Status) 列下的三个点将打开无代理终端安全评估故障排除
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断 (Diagnostic) > 常规工具 (General Tools)**

有关无代理终端安全评估故障排除的详细信息，请参阅维护和监控 一章。

无代理终端安全状态故障排除

“无代理终端安全评估”(Agentless Posture) 报告是当无代理终端安全评估未按预期工作时使用的主要故障排除工具。此报告显示无代理流的各个阶段，包括脚本上传完成、脚本上传失败、脚本执行完成等事件，以及任何已知的失败原因。

您可以从两个位置访问无代理终端安全评估故障排除：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 实时日志 (Live Logs)**：在要进行故障排除的客户端的“终端安全评估状态”(Posture Status) 列上，点击三个竖点。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断 (Diagnostic) > 常规工具 (General Tools) > 无代理终端安全评估故障排除 (Agentless Posture Troubleshooting)**。

无代理终端安全评估故障排除工具会收集指定客户端的无代理终端安全评估活动。**无代理终端安全评估流 (Agentless Posture Flow)** 会启动终端安全评估并显示当前活动客户端与Cisco ISE 之间的所有交互。**仅下载客户端日志 (Only Download Client Logs)** 会创建一些日志，其中包含最长过去 24 小时的客户端终端安全评估流。客户端可以随时删除日志。收集完成后，可以导出日志的 ZIP 文件。

报告

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 终端和用户 (Endpoints and Users) > 无代理终端安全评估 (Agentless Posture)**，查看运行无代理终端安全评估的所有终端。

安全评估管理设置

您可以从全局为 Admin 门户配置安全评估服务。您可以从Cisco通过 Web 将更新自动下载至Cisco ISE 服务器。之后您还可以离线手动更新Cisco ISE。此外，如果已在客户端上安装 AnyConnect或 Web 代理之类的代理，则可以为客户端提供终端安全评估和补救服务。客户端代理定期向Cisco ISE 更新客户端的合规性状态。登录并成功完成安全状态要求评估之后，客户端代理显示带有一个链接的对话框，要求最终用户遵守网络使用的条款和条件。您可以使用此链接为您的企业网络定义最终用户在可以访问您的网络之前必须接受的网络使用信息。

客户端安全评估要求

要创建终端安全评估要求，请执行以下操作：

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)**。
2. 从任何要求行末尾处的**编辑 (Edit)** 下拉列表中，选择**插入新要求 (Insert New Requirement)**。
3. 输入所需的详细信息，并点击**完成 (Done)**。

下表介绍**客户端终端安全评估要求 (Client Posture Requirements)** 窗口中的字段。

表 *142:* 终端安全评估要求

字段名称	使用指南
Name	输入要求名称。
Operating Systems	选择操作系统。 点击加号 [+]，将多个操作系统关联到策略。 点击减号 [-]，从策略删除操作系统。

字段名称	使用指南
合规性模块	从**合规性模块 (Compliance Module)** 下拉列表中，选择所需的合规性模块： • 4.x 或更高版本：支持反恶意软件、磁盘加密、补丁管理和 USB 条件。 • 3.x 或更低版本：支持防病毒、反间谍软件、磁盘加密和补丁管理条件。 • 任意版本：支持文件、服务、注册、应用和复合条件。 有关合规性模块的详细信息，请参阅合规性模块，第 967 页。
终端安全评估类型	从**终端安全评估类型 (Posture Type)** 下拉列表中，选择所需的终端安全评估类型。 • AnyConnect：部署 AnyConnect 代理以监控和实施需要客户端交互的Cisco ISE 策略。 • AnyConnect 隐身：部署 AnyConnect 代理以监控和实施Cisco ISE 安全评估策略，无需任何客户端交互。 • 临时代理：在客户端运行的临时可执行文件，用于检查合规性状态。
Conditions	从列表中选择一个条件。 您也可以点击 Action 图标，将其与要求关联起来，创建任何用户定义的条件。创建用户定义的条件时，不能编辑已关联的母操作系统。 pr_WSUSRule 是虚拟的复合条件，在终端安全评估要求中与已关联的 Windows Server Update Services (WSUS) 补救一起使用。您必须使用严重性级别选项，将已关联的WSUS 补救操作配置为验证 Windows 更新。当此要求无法满足时，Windows 客户端上的代理会根据您在 WSUS 补救中定义的严重性级别执行 WSUS 补救操作。 pr_WSUSRule 在复合条件列表页面看不到。您只能从条件构件选择 pr_WSUSRule。

字段名称	使用指南
Remediation Actions	从列表中选择一个补救操作。 您也可以创建补救操作，并将其与要求相关联。 您可以在文本框中写下所有补救类型，传达给代理用户。除了补救操作，还可以向代理用户传达关于客户端不合规的消息。 **Message Text Only** 选项可以向代理用户传达不合规的信息。它还提供可选说明，让用户联系服务中心获得详细信息，或者手动修复客户端。在这种情况下，代理不会触发任何补救操作。

相关主题

配置安全评估的可接受使用政策，第 963 页
创建客户端安全评估要求，第 1009 页

客户端的计时器设置

您可以为用户设置计时器，用于进行补救、从一个状态过渡到另一个状态，以及控制登录成功屏幕。

我们建议配置具有补救计时器和网络过渡延迟计时器的代理配置文件，以及用于控制客户端计算机登录成功屏幕的计时器，以便这些设置以策略为基础。您可以在 **AnyConnect 终端安全评估配置文件 (AnyConnect Posture Profile)** 窗口的客户端调配资源中为代理配置所有这些计时器（该窗口位于在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Resilts)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)** > **添加 (Add)** > **AnyConnect 终端安全评估配置文件 (AnyConnect Posture Profile)**）。

但是，当没有任何配置为与客户端调配策略相匹配的代理配置文件时，您可以使用**常规设置 (General Settings)** 配置窗口中的设置（该窗口位于在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**）。

设定补救计时器，使客户端在指定时间内补救

您可以配置计时器，使客户端在指定时间内补救。在初始评估期间，客户端不符合配置的终端安全评估策略，代理将等待客户端在补救计时器中配置的时间内补救。如果客户端无法在指定时间内补救，则客户端代理将向终端安全评估运行服务发送报告，然后，客户端过渡到不合规状态。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

步骤 2 在**补救计时器 (Remediation Timer)** 字段中，以分钟为单位输入时间值。

默认值为 4 分钟。有效范围为 1 至 300 分钟。

步骤 3 点击**保存 (Save)**。

设置网络转换延迟计时器，使客户端实现转换

可以为客户端配置计时器，使客户端在指定的时间内，使用网络过渡延迟计时器从一种状态过渡到另一种状态，这是完成授权更改 (CoA) 所必需的操作。当客户端在终端安全评估成功和失败期间需要获得新的 VLAN IP 地址时，可能需要更长的延迟时间。终端安全评估成功时，Cisco ISE 允许客户端在使用网络过渡延迟计时器指定的时间内从未知模式过渡为合规模式。终端安全评估失败时，Cisco ISE 允许客户端在计时器指定的时间内从未知模式过渡为非合规模式。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

步骤 2 以秒为单位，在 **Network Transition Delay** 字段中输入时间值。

默认值为 3 秒。有效范围为 2 至 30 秒。

步骤 3 点击**保存 (Save)**。

将登录成功窗口设置为自动关闭

成功完成安全状态评估之后，客户端代理会显示一个临时网络访问屏幕。用户需要点击登录窗口中的**确定 (OK)** 按钮将其关闭。您可以设置计时器以在指定时间之后自动关闭此登录屏幕。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

步骤 2 选中**后自动关闭 Telnet 成功界面 (Automatically Close Login Success Screen After)** 复选框。

步骤 3 在**后自动关闭 Telnet 成功界面 (Automatically Close Login Success Screen After)** 复选框旁边的字段中以秒为单位输入时间值。

有效范围为 0 至 300 秒。如果时间设置为零，则 AnyConnect 不显示登录成功界面。

步骤 4 点击**保存 (Save)**。

设置非代理设备的终端安全评估状态

您可以配置在 Linux 或 iDevices 等非代理设备上运行的终端的安全评估状态。当 Android 设备和 Apple 设备（如 iPod、iPhone 或 iPad）连接到支持Cisco ISE 的网络时，这些设备采用默认安全评估状态设置。

安全评估运行期间找不到匹配策略时，还可以将这些设置应用到在 Windows 和 Macintosh 操作系统中运行的终端。

开始之前

要在一个终端上强制实施策略，必须配置相应的客户端调配策略（代理安装包）。否则，该终端的安全评估状态会自动反映默认设置。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

步骤 2 从**默认终端安全评估 (Default Posture Status)** 下拉列表中， 选择**合规 (Compliant)** 或**不合规 (Noncompliant)** 选项。

步骤 3 点击**保存 (Save)**。

安全评估租约

您可以将Cisco ISE 配置为在每次用户登录您的网络时执行安全评估或按指定的间隔执行安全评估。有效范围为 1 至 365 天。

此配置仅适用于使用 AnyConnect 代理进行安全评估的用户。

当终端安全评估租约处于活动状态时，Cisco ISE 将使用上次已知的终端安全评估状态，并且不会连接到终端以检查合规性。但是，当终端安全评估租约到期时，Cisco ISE 不会自动触发终端的重新身份验证或终端安全评估。因为正在使用相同的会话，所以终端将保持相同的合规性状态。当终端重新进行身份验证时，将运行终端安全评估，并重置终端安全评估租用时间。

使用案例场景示例：

- 用户登录终端，使其终端安全评估符合设置为一天的终端安全评估租约。
- 四小时后，用户从终端注销（终端安全评估租约现在还剩 20 小时）。
- 一小时后，用户再次登录。现在，终端安全评估租约还剩19小时。最后已知的终端安全评估状态为合规。因此为用户提供访问权限，无需在终端上运行终端安全评估。
- 四小时后，用户注销（终端安全评估租约现在还剩 15 小时）。
- 14 小时后，用户登录。终端安全评估租约还剩一个小时。最后已知的终端安全评估状态为合规。系统会为用户提供访问权限，无需在终端上运行终端安全评估。
- 一小时后，终端安全评估租约到期。用户仍连接到网络，因为正在使用同一用户会话。
- 一小时后，用户注销（会话与用户绑定，但不与计算机绑定，因此计算机可以留在网络上）。
- 一小时后，用户登录。由于终端安全评估租约已到期且已启动新的用户会话，因此计算机会执行终端安全评估，结果会发送到Cisco ISE，在此使用案例中，终端安全评估租约计时器会重置为一天。

定期重新评估

只有成功完成合规性安全评估的客户端才可以执行定期重新评估 (PRA)。如果您网络上的客户端不合规，则不会执行 PRA。

只有在终端处于合规状态下，PRA 才有效和适用。策略服务节点检查相关策略，根据配置中定义的客户端角色编制实施 PRA 的要求。如果找到 PRA 配置匹配项，策略服务节点在发出 CoA 请求之前会用 PRA 配置中为客户端定义的 PRA 属性对客户端代理做出响应。客户端代理根据配置中指定的间隔定期发送 PRA 请求。如果 PRA 成功或继续执行 RPA 配置中配置的操作，客户端会保持合规状态。如果客户端未能满足 PRA 要求，则客户端会从合规状态变为不合规状态。

即使是安全评估状态重新评估请求，PostureStatus 属性也会在 PRA 请求中将当前安全状态显示为合规状态而不是未知状态。监控报告中也会更新 PostureStatus。

当终端安全评估租约未到期时，终端根据访问控制列表 (ACL) 变为合规，并启动 PRA。如果 PRA 失败，终端视为不合规，并重置终端安全评估租约。

配置定期重新评估

您可以配置仅定期重新评估已成功通过合规性安全状态评估的客户端。您可以为系统中定义的用户身份组配置各项 PRA。

开始之前

- 确保每个定期重新评估 (PRA) 配置都有分配给该配置的唯一组或用户身份组的唯一组合。
- 您可以分配 role_test_1 和 role_test_2，这是 PRA 配置独有的两个角色。您可以使用逻辑运算符组合这两个角色并将 PRA 配置分配为两个角色的唯一组合。例如，role_test_1 OR role_test_2。
- 确保两个 PRA 配置没有相同的用户身份组。
- 如果已有用户身份组为任何 *(Any)* 的 PRA 配置，您就无法创建其他 PRA 配置，除非您执行以下操作之一：
  - 用 Any 用户组更新现有 PRA 配置以反映 *Any* 之外的用户身份组。
  - 删除“*Any*”用户身份组的现有 PRA 配置。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **重新评估 (Reassessments)**。

步骤 2 点击**添加 (Add)**。

步骤 3 修改**新重新评估配置 (New Reassessment Configuration)** 窗口中的值以创建新 PRA。

步骤 4 点击**提交 (Submit)** 以创建 PRA 配置。

安全评估故障排除设置

下表介绍“终端安全评估故障排除”(Posture troubleshooting) 窗口上的字段，您可以使用该窗口查找并解决网络中的终端安全评估问题。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools** > **终端安全评估故障排除 (Posture Troubleshooting)**。

表 *143:* 终端安全评估故障排除设置

字段名称	使用指南
搜索并选择一个需要进行故障排除的安全评估事件	
Username	输入要过滤的用户名。
MAC Address	输入要过滤的 MAC 地址，请使用格式：xx-xx-xx-xx-xx-xx
Posture Status	选择要过滤的身份验证状态：
Failure Reason	输入故障原因，或者点击 **Select** 以从列表中选择故障原因。点击 **Clear** 以清除故障原因。
Time Range	选择时间范围。使用在此时间范围内创建的 RADIUS 身份验证记录。
Start Date-Time:	（仅当您选择自定义时间范围时可用）输入开始日期和时间，或点击日历图标选择开始日期和时间。日期应为 *mm/dd/yyyy* 格式，而时间应为 *hh:mm* 格式。
End Date-Time:	（仅当您选择自定义时间范围时可用）输入结束日期和时间，或点击日历图标选择结束日期和时间。日期应为 *mm/dd/yyyy* 格式，而时间应为 *hh:mm* 格式。
Fetch Number of Records	选择要显示的记录数：10、20、50、100、200、500
Search Result	
Time	事件时间
Status	终端安全评估状态
Username	与事件关联的用户名
MAC Address	系统的 MAC 地址
Failure Reason	事件的失败原因

相关主题

排除终端安全评估故障，第 1250 页
安全评估故障排除工具，第 1020 页

安全评估常规设置

下表介绍“终端安全评估常规设置”(Posture General Settings) 窗口中的字段，可以使用此窗口配置补救时间和终端安全评估状态等常规终端安全评估设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

常规终端安全评估设置

- **补救计时器 (Remediation Timer)**：输入开始补救前等待的时间。默认值为 4 分钟。有效范围为 1 至 300 分钟。
- **网络过渡延迟 (Network Transition Delay)**：以秒为单位输入时间值。默认值为 3 秒。有效范围为 2 至 30 秒。
- **默认终端安全评估状态 (Default Posture Status)**：选择“合规”(Compliant) 或“不合规”(Noncompliant)。在连接到网络时，非代理设备（诸如 Linux）会处于此状态。
- **自动关闭登录成功屏幕前等待 (Automatically Close Login Success Screen After)**：选中此复选框可在指定的时间过后自动关闭成功登录屏幕。可以配置计时器以自动关闭登录屏幕。有效范围为 0 至 300 秒。如果将时间设置为零，则客户端上的代理不会显示成功登录屏幕。
- **连续监控间隔 (Continuous Monitoring Interval)**：指定 AnyConnect 开始发送监控数据之前的时间间隔。对于应用和硬件条件，默认值为 5 分钟。
- **无代理终端安全评估客户端超时**：指定在终端安全评估检查被视为失败之前等待的时间。
- **每次运行后删除无代理插件 (Remove Agentless Plugin)**：启用此设置可在运行无代理终端安全评估后从客户端删除代理。我们强烈禁用此功能，以便下载的插件可以重复使用，直到有新版本可用。禁用此选项有助于减少网络流量。
- **隐身模式下的可接受使用策略 (Acceptable Use Policy)**：如果不符合贵公司的网络使用条款和条件，请在隐身模式下选择**阻止 (Block)** 以将客户端转移到不合规的终端安全评估状态。

安全评估租约

- **每当用户连接到网络时执行终端安全评估 (Perform posture assessment every time a user connects to the network)**：选择此选项可在用户每次连接网络时启动终端安全评估
- **每 n 天执行一次终端安全评估 (Perform posture assessment every n days)**：选择此选项可在指定天数过后启动终端安全评估，即使客户端的状态已评估为“合规”也是如此。

- **缓存最后已知终端安全评估合规状态 (Cache Last Known Posture Compliant Status)**：选中此复选框可使Cisco ISE 缓存终端安全评估的结果。默认情况下，此字段处于禁用状态。
- **最后已知终端安全评估合规状态 (Last Known Posture Compliant Status)**：仅当已选中**缓存最后已知终端安全评估合规状态 (Cache Last Known Posture Compliant Status)** 时，此设置才适用。Cisco ISE 会在此字段中指定的时间量内缓存终端安全评估结果。有效值为 1 到 30 天，或 1 到 720 小时，或 1 到 43200 分钟。

相关主题

安全评估服务
安全评估管理设置，第 952 页
安全评估租约，第 956 页
在思科 ISE 中启用安全评估会话服务
设定补救计时器，使客户端在指定时间内补救，第 954 页
设置网络转换延迟计时器，使客户端实现转换，第 955 页
将登录成功窗口设置为自动关闭，第 955 页
设置非代理设备的终端安全评估状态，第 955 页

将安全评估更新下载至思科 ISE

安全评估更新包括针对适用于 Windows 和 Macintosh 操作系统的防病毒和反间谍软件的一系列预定义的检查、规则和支持图表，以及Cisco支持的操作系统信息。您还可以从您包含最新更新档案的本地系统上的文件离线更新Cisco ISE。

当您首次在您的网络上部署Cisco ISE 时，您可以从 Web 下载安全评估更新。此过程通常大约需要 20 分钟。初次下载后，您可以将Cisco ISE 配置为自动验证和下载增量更新。

在初始安全评估更新期间，Cisco ISE 仅创建一次默认安全评估策略、要求和补救。如果您删除所创建的这些内容，在后续手动或计划更新期间Cisco ISE 不会再进行创建。

开始之前

要确保能够访问合适的远程位置以便将安全评估资源下载至CiscoISE，您可能需要验证您已按照“在 Cisco ISE 中指定代理设置”的说明为您的网络配置了正确的代理设置。

您可以使用“安全评估更新”(Posture Update) 窗口从 Web 动态下载更新。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **更新 (Updates)**。

步骤 2 选择 **Web** 选项以动态地下载更新。

步骤 3 点击**设置为默认值 (Set to Default)** 为**更新源 URL (Update Feed URL)** 字段设置Cisco默认值。

如果您的网络限制 URL 重定向功能（例如通过代理服务器）而且您在访问上述 URL 时遇到了问题，请尝试将您的Cisco ISE 也指向相关主题中的备选 URL。

步骤 4 在**安全评估更新 (Posture Updates)** 窗口更改相应值。

步骤 5 点击**现在更新 (Update Now)** 以从Cisco下载更新。

更新后，“安全评估更新”(Posture Updates) 窗口显示当前Cisco更新版本信息，作为对“安全评估更新”(Posture Updates) 窗口“更新信息”(Update Information) 部分下的更新的验证。

步骤 6 点击**是 (Yes)** 以继续操作。

自动下载安全评估更新

在初始更新后，您可以将Cisco ISE 配置为检查更新并自动下载这些更新。

开始之前

- 您起初应已下载安全评估更新来将Cisco ISE 配置为检查更新并自动下载这些更新。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **更新 (Updates)**。

步骤 2 在**终端安全评估更新 (Posture Updates)** 窗口中，选中**从初始延迟开始自动检查更新 (Automatically check for updates starting from initial delay)** 复选框。

步骤 3 以 hh:mm:ss 格式输入初始延迟时间。

Cisco ISE 在初始延迟时间结束后开始检查更新。

步骤 4 输入时间间隔（以小时为单位）。

Cisco ISE 从初始延迟时间起按指定间隔将更新下载到部署。

步骤 5 点击**保存 (Save)**。

安全评估可接受使用政策配置设置

下表介绍了“终端安全评估可接受使用策略配置”(Posture Acceptable Use Policy Configurations) 窗口中的字段，可以使用此窗口为终端安全评估配置可接受使用策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **可接受使用策略 (Acceptable Use Policy)**。

表 ***144:*** 安全评估 ***AUP*** 配置设置

字段名称	使用指南
配置名称	输入要创建的 AUP 配置的名称。

字段名称	使用指南
配置说明	输入要创建的 AUP 配置的说明。
“向代理用户显示 AUP”(Show AUP to Agent users)（仅适用于 Windows）	选中后，系统会在身份验证和终端安全评估成功后，向用户显示您的网络的网络使用条款和条件的链接。
为 AUP 消息使用 URL (Use URL for AUP message)	选中后，必须在“AUP URL”字段中输入 AUP 消息的 URL。
为 AUP 消息使用文件 (Use file for AUP message)	选中后，必须浏览至文件位置并以压缩格式上传文件。此文件必须在顶层包含 index.html。 除 index.html 文件以外，该 .zip 文件还可包含其他文件和子目录。这些文件可以使用 HTML 标签相互引用。
AUP URL	输入 AUP 的 URL，用户必须在身份验证和安全评估成功后访问该 URL。
AUP File	浏览至文件并将其上传到Cisco ISE 服务器。它应是压缩文件，并且应在顶层包含 index.html 文件。
选择用户身份组 (Select User Identity Groups)	针对 AUP 配置选择唯一用户身份组或用户身份组的唯一组合。 创建 AUP 配置时，请注意以下事项： • 安全评估 AUP 不适用于访客流程 • 两个配置不会共同具有任何用户身份组 • 如果您要使用用户身份组“Any”创建 AUP 配置，则要先删除所有其他 AUP 配置 • 如果使用用户身份组“Any”创建 AUP 配置，则无法使用唯一用户身份组或用户身份组的唯一组合创建其他 AUP 配置。要使用除 Any 以外的用户身份组创建 AUP 配置，请先删除具有用户身份组“Any”的现有 AUP 配置，或者使用唯一用户身份组或用户身份组的唯一组合更新具有用户身份组“Any”的现有 AUP 配置。
可接受使用策略配置 - 配置清单 (Acceptable use policy configurations—Configurations list)	列出现有 AUP 配置以及与 AUP 配置关联的最终用户身份组。

相关主题

安全评估服务

配置安全评估的可接受使用政策，第 963 页

配置安全评估的可接受使用政策

登录并对客户端成功完成安全状态评估之后，客户端代理会显示一个临时网络访问屏幕。此屏幕包含可接受使用政策 (AUP) 的链接。当用户点击此链接时，系统会将用户重定向至显示网络使用条款和条件的页面，用户必须阅读并理解这些条款和条件。

每个可接受使用政策配置都必须具有唯一的用户身份组或唯一的用户身份组组合。Cisco ISE 找到第一个匹配的用户身份组，然后与显示 AUP 的客户端代理通信。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **可接受使用政策 (Acceptable Use Policy)**。

步骤 2 点击**添加 (Add)**。

步骤 3 修改**新可接受使用政策配置 (New Acceptable Use Policy Configuration)** 窗口中的值。

步骤 4 点击**提交 (Submit)**。

安全评估条件

安全评估条件可以是以下任何一个简单条件：文件、注册表、应用、服务或字典条件。这些简单条件中的一个或多个条件构成可与安全评估要求相关联的复合条件。

当您首次在您的网络上部署Cisco ISE时，您可以从 Web 下载安全评估更新。此过程称为初始安全评估更新。

在初始安全评估更新后，Cisco ISE 还会创建Cisco定义的简单条件与复合条件。Cisco定义的简单条件以 pc_ 作为前缀，复合条件以 pr_ 作为前缀。

您也可以将Cisco ISE 配置为由于通过 Web 进行动态安全评估更新而定期下载Cisco定义的条件。您不能删除或编辑Cisco定义的安全评估条件。

用户定义的条件或Cisco定义的条件同时包含简单条件与复合条件。

简单安全评估条件

您可以使用**安全评估导航 (Posture Navigation)** 窗格管理以下简单条件：

- 文件条件：在客户端上检查文件的存在性、文件的日期以及文件的版本的条件。
- 注册条件：在客户端上检查注册表项的存在性或注册表项的值的条件。
- 应用条件：在客户端上检查应用（进程）是否在运行的条件。

注释 如果进程已安装并正在运行，则用户合规。但是，应用条件的逻辑正好相反；如果应用未安装且未运行，则最终用户合规。如果应用已安装并正在运行，则最终用户不合规。

- 服务条件：检查服务是否在客户端上运行的条件。
- 词典条件：检查带某个值的词典属性的条件。
- USB 条件：检查 USB 大量存储设备是否存在的条件。

创建简单安全评估条件

可以创建文件、注册表、应用、服务和字典简单条件，在终端安全评估策略或其他复合条件中可以使用这些条件。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)**。

步骤 2 选择以下任意一项：**文件 (File)**、**注册表 (Registry)**、**应用 (Application)**、**服务 (Service)** 或**字典简单条件 (Dictionary Simple Condition)**。

步骤 3 点击**添加 (Add)**。

步骤 4 在字段中输入适当的值。

步骤 5 点击**提交 (Submit)**。

复合安全评估条件

复合条件由一个或多个简单条件或复合条件组成。您可以利用以下复合条件定义安全评估策略。

- 复合条件：包含一个或多个简单条件或文件、注册表、应用或服务条件类型的复合条件
- 防病毒复合条件：包含一个或多个 AV 条件或 AV 复合条件
- 反间谍软件复合条件：包含一个或多个 AS 条件或 AS 复合条件
- 字典复合条件：包含一个或多个字典简单条件或字典复合条件
- 防恶意软件条件：包含一个或多个 AM 条件。

创建复合安全评估条件

您可以创建复合条件用于安全评估和验证的状态策略。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **复合条件 (Compound Condition)** > **添加 (Add)**。

步骤 2 输入适当的字段值。

步骤 3 点击 **Validate Expression** 验证条件。

步骤 4 点击**提交 (Submit)**。

字典复合条件设置

表 *145:* 字典复合条件设置

字段名称	使用指南
Name	输入要创建的字典复合条件的名称。
Description	输入要创建的字典复合条件的说明。
从库中选择现有条件	通过从策略要素库选择预定义的条件来定义表达式，或在后续步骤中将临时属性/值对添加到表达式中。
条件名称	选择已从策略要素库中创建的字典简单条件。
表达式	Expression 会根据从 Condition Name 下拉列表选择的选项进行更新。
AND 或 OR 运算符	选择 AND 或 OR 运算符可逻辑组合可从策略要素库添加的字典简单条件。 点击 **Action** 图标可执行以下操作： • Add Attribute/Value • Add Condition from Library • Delete
创建新条件（高级选项）	从各种系统或用户定义的字典中选择属性。 还可以在后续步骤中从策略要素库中添加预定义条件。

字段名称	使用指南
条件名称	选择已创建的字典简单条件。
表达式	从 Expression 下拉列表可以创建字典简单条件。
运算符	选择要将值关联到属性的运算符。
Value	输入要关联到字典属性的值，或者从下拉列表中选择一个值。

相关主题

字典和字典属性
简单和复合条件
复合安全评估条件，第 964 页
创建复合安全评估条件，第 965 页

用于在 Windows 客户端中启用自动更新的预定义条件

pr_AutoUpdateCheck_Rule 是Cisco预定义条件，会下载至“复合条件”(Compound Conditions) 窗口。您可以通过此条件检查在 Windows 客户端上是否启用了自动更新功能。如果 Windows 客户端未满足此要求，则网络访问控制 (NAC) 代理会强制 Windows 客户端启用（补救）自动更新功能。这种补救完成后，Windows 客户端就符合安全评估。如果在 Windows 客户端上未启用自动更新功能，您在安全评估策略中关联的 Windows 更新会覆盖 Windows 管理员设置。

预配置的防病毒和反间谍软件条件

Cisco ISE 在“AV 复合条件”(AV Compound Condition) 和“AS 复合条件”(AS Compound Condition) 窗口加载预配置的防病毒和反间谍软件复合条件（在适用于 Windows 和 Macintosh 操作系统的防病毒和反间谍软件支持图表中定义）。如果指定的防病毒和反间谍软件产品存在于全部客户端，则这些复合条件则可以选中。此外，您还可以在Cisco ISE 中创建新的防病毒和反间谍软件复合条件。

防病毒和反间谍软件支持图表

Cisco ISE 使用防病毒和反间谍软件支持图表，此图表在各供应商产品的定义文件中提供最新版本和日期。用户必须定期访问防病毒和反间谍软件支持图表来查看更新。防病毒和反间谍软件供应商会经常更新防病毒和反间谍软件定义文件，请在各供应商产品的定义文件中查找最新版本和日期。

每次系统更新防病毒和反间谍软件支持图表来反映对新防病毒和反间谍软件供应商、产品及其发行版本的支持时，NAC 代理都会收到新的防病毒和反间谍软件库。这可以帮助 NAC 代理支持新增的防病毒和反间谍软件。NAC 代理检索到此支持信息后，会从定期更新的 se-checks.xml 文件（此文件随 se-templates.tar.gz 档案中的 se-rules.xml 文件一起发布）检查最新定义信息，然后确定客户端是否符合安全评估策略。根据防病毒和反间谍软件库对于特定防病毒或反间谍软件产品的支持情况，系统会向 NAC 代理发送相应的要求，在安全评估验证过程中来验证客户端上具体的防病毒和反间谍软件产品是否存在。

有关 ISE 终端安全评估代理支持的防病毒和防恶意软件产品的详细信息，请参阅Cisco AnyConnect ISE 终端安全评估支持图表：思科 ISE 兼容性指南。

您可以在创建防恶意软件终端安全评估条件时验证最低合规性模块版本。更新终端安全评估源后，请选择**工作中心 (Work Centers) > 终端安全评估 (Posture) > 策略元素 (Policy Elements) > 防恶意软件条件 (Anti-Malware Condition)**，然后选择**操作系统 (Operating System)** 和**供应商 (Vendor)** 以查看支持图表。

注释 某些防恶意软件终端安全解决方案（如 FireEye、Cisco AMP、Sophos 等）需要通过网络访问各自的集中服务才能正常运行。对于此类产品，AnyConnect ISE 终端安全评估模块（或 OESIS 库）要求终端能够连接互联网。建议在这些在线代理的终端安全评估预评估期间允许此类终端访问互联网（如果未启用离线检测）。签名定义条件可能不适用于此类情况。

合规性模块

合规性模块包含一个字段列表，例如由支持Cisco ISE 安全评估条件的 OPSWAT 提供的供应商名称、产品版本、产品名和属性。

供应商会经常更新定义文件中的产品版本和日期，因此，您必须频繁轮询合规性模块的新情况，以找到每个供应商产品的定义文件中的最新版本和日期。每次更新合规性模块以反映对新供应商、产品和版本的支持时，AnyConnect 代理都会收到一个新库。从而使 AnyConnect 代理可支持新增产品。AnyConnect 代理检索到此支持信息后，会从定期更新的 se-checks.xml 文件（此文件随 se-templates.tar.gz 档案中的 se-rules.xml 文件一起发布）检查最新定义信息，然后确定客户端是否符合安全评估策略。根据库文件对于特定防病毒、反间谍软件、防恶意软件、磁盘加密或补丁管理产品的支持情况，系统会向 AnyConnect 代理发送相应的要求，在安全评估验证过程中验证客户端上是否存在这些产品以及它们的状态。

合规性模块可从 Cisco.com 获取。

下表列出了支持和不支持 ISE 终端安全评估策略的 OPSWAT API 版本。对于支持版本 3 和 4 的代理，存在不同的策略规则。

表 *146: OPSWAT API* 版本

终端安全评估条件	合规性模块版本
OPSWAT	
防病毒软件	3.x 或更低版本
反间谍软件	3.x 或更低版本
反恶意软件	4.x 或更高版本
磁盘加密	3.x 或更低版本以及 4.x 或更高版本
补丁管理	3.x 或更低版本以及 4.x 或更高版本

终端安全评估条件	合规性模块版本
USB	4.x 或更高版本
非 OPSWAT	
文件	任何版本
应用	任何版本
复合	任何版本
注册表	任何版本
服务	任何版本

注释

- 请务必为版本 3.x 或更低版本以及版本 4.x 或更高版本创建单独的终端安全评估策略，因为预计客户端可能已安装以上任何一个版本。
- 为合规性模块 4.x 和 Cisco AnyConnect 4.3 及更高版本提供了 OESIS 版本 4 支持。但是，AnyConnect 4.3 同时支持 OESIS 版本 3 和版本 4 策略。
- ISE 2.1 和更高版本支持第 4 版合规性模块。

检查安全评估合规性

步骤 1 登录Cisco ISE 并访问控制板。

步骤 2 在**安全评估合规性 (Posture Compliance)** Dashlet 中，将光标悬停于堆积条形图或迷你图上。

工具提示提供详细的信息。

步骤 3 展开数据类别，了解更多信息。

步骤 4 展开 **Posture Compliance** dashlet。

系统将显示详细的实时报告。

注释　您可以在情景可视性 **(Context Visibility)** 窗口中查看终端安全评估合规报告。导航至情景可视性 **(Context Visibility)** > 终端 **(Endpoints)** > 合规 **(Compliance)**。此窗口根据合规状态 **(Compliance Status)**、位置 **(Location)**、终端 **(Endpoints)** 和应用（按类别）**(Applications by Categories)** 显示不同的图表。

您可能会看到没有任何活动会话的终端的安全评估状态。例如，如果终端的上一已知安全评估状态为合规 **(Compliant)**，即使终端会话已终止，在收到终端的下一次更新之前，情景可视性 **(Context Visibility)** 窗口中的状态仍然保持为合规 **(Compliant)**。在终端被删除或清除之前，安全评估状态始终保留在情景可视性 **(Context Visibility)** 窗口中。

创建补丁管理条件

可以创建用于检查选定供应商的补丁管理产品状态的策略。

例如，可以创建一个条件，用以检查微软系统中心配置管理器 (SCCM) 客户端版本 4.x 软件产品是否安装在终端上。

注释　支持的思科 ISE 和 AnyConnect 版本 (Supported versions of Cisco ISE and AnyConnect)：

- 思科 ISE 版本 1.4 及更高版本
- AnyConnect 版本 4.1 及更高版本

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1　在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 策略 **(Policy)** > 策略元素 **(Policy Elements)** > 条件 **(Conditions)** > 终端安全评估 **(Posture)** > 补丁管理条件 **(Patch Management Condition)**。

步骤 2　点击添加 **(Add)**。

步骤 3　在名称 **(Name)** 和说明 **(Description)** 字段中输入条件名称和说明。

步骤 4　从操作系统 **(Operating System)** 下拉字段中选择适当的操作系统。

步骤 5　从下拉列表中选择合规性模块 **(Compliance Module)**。

步骤 6　从下拉列表中选择供应商名称 **(Vendor Name)**。

步骤 7　选择检查类型 **(Check Type)**。

步骤 8　从检查已安装的补丁 **(Check patches installed)** 下拉列表中选择适当的补丁。

步骤 9　点击提交 **(Submit)**。

相关主题

补丁管理条件设置，第 988 页

添加补丁管理补救，第 1005 页

创建磁盘加密条件

您可以创建一个策略以检查终端是否与指定的数据加密软件兼容。

例如，您可以创造条件检查 C 盘是否在终端加密。如果 C 盘没有加密，终端会收到一个非合规性通知，同时 ISE 会记录一条消息。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。只有当您使用AnyConnect ISE终端安全评估代理时，您才可以将磁盘加密条件与终端安全评估需求进行关联。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **磁盘加密条件 (Disk Encryption Condition)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**磁盘加密条件 (Disk Encryption Condition)** 窗口中，在字段中输入适当的值。

步骤 4 点击**提交 (Submit)**。

安全评估条件设置

本节介绍用于安全评估的简单条件和复合条件。

文件条件设置

下表介绍“文件条件”(File Conditions) 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **文件条件 (File Condition)**。

表 *147:* 文件条件设置

字段名称	Windows 操作系统使用指南	Mac OSX 使用指南
名称	输入文件条件的名称。	输入文件条件的名称。
说明	输入文件条件的说明。	输入文件条件的说明。
操作系统	选择应向其应用文件条件的 Windows 操作系统。	选择应向其应用文件条件的 Mac OSX。

字段名称	Windows 操作系统使用指南	Mac OSX 使用指南
文件类型	选择以下预定义设置之一： • **FileDate**：检查系统中是否存在带有特定文件创建或文件修改日期的文件。 • **FileExistence**：检查系统中是否存在文件。 • **FileVersion**：检查系统中是否存在特定版本的文件。 • **CRC32**：使用校验和函数检查文件的数据完整性。 • **SHA-256**：使用哈希函数检查文件的数据完整性。	选择以下预定义设置之一： • **FileDate**：检查系统中是否存在带有特定文件创建或文件修改日期的文件。 • **FileExistence**：检查系统中是否存在文件。 • **CRC32**：使用校验和函数检查文件的数据完整性。 • **SHA-256**：使用哈希函数检查文件的数据完整性。 • **PropertyList**：检查 plist 文件（例如，loginwindow.plist）中的属性值。

字段名称	**Windows** 操作系统使用指南	**Mac OSX** 使用指南
数据类型和运算符	NA	（仅当您选择的文件类型为 **PropertyList** 时可用）选择要在 plist 文件中搜索的数据类型或密钥值。每种数据类型包含一组运算符。 • **未指定**：检查是否存在指定的密钥。输入一个运算符 (Exists, DoesNotExist)。 • **数字**：检查数字数据类型的指定密钥。输入运算符（等于、不等于、大于、小于、大于或等于和小于或等于）和值。 • **字符串**：检查字符串数据类型的指定密钥。输入运算符（等于、不等于、等于（忽略大小写）、以其开始、不以其开始、包含、不包含、以其结尾和不以其结尾）和值。 • **版本**：检查作为版本字符串的指定密钥的值。输入运算符（低于、高于、等与）和值。
属性名称	NA	（仅当您选择的文件类型为 **PropertyList** 时可用）输入密钥名称，例如，BuildVersionStampAsNumber

字段名称	Windows 操作系统使用指南	Mac OSX 使用指南
文件路径	选择以下预定义设置之一： • **ABSOLUTE_PATH**：检查文件的完全限定路径中的文件。例如，C:\<directory>\file name。对于其他设置，请仅输入文件名。 • **SYSTEM_32**：检查 C:\WINDOWS\system32 目录中的文件。输入文件名。 • **SYSTEM_DRIVE**：检查 C:\ 驱动器中的文件。输入文件名。 • **SYSTEM_PROGRAMS**：检查 C:\Program Files 中的文件。输入文件名。 • **SYSTEM_ROOT**：检查 Windows 系统的根路径中的文件。输入文件名。 • **USER_DESKTOP**：检查指定的文件是否显示在 Windows 用户的桌面上。输入文件名。 • **USER_PROFILE**：检查文件是否显示在 Windows 用户的本地配置文件目录中。输入文件路径。	选择以下预定义设置之一： • **Root**：检查根 (/) 目录中的文件。输入文件路径。 • **Home**：检查主 (~) 目录中的文件。输入文件路径。
文件日期类型	（仅当您选择的文件类型为 **FileDate** 时可用）选择**创建日期 (Creation Date)** 或**修改日期 (Modification Date)**。	（仅当您选择的文件类型为 **FileDate** 时可用）选择**创建日期 (Creation Date)** 或**修改日期 (Modification Date)**。

字段名称	**Windows** 操作系统使用指南	**Mac OSX** 使用指南
文件操作符	File Operator 选项会根据在 File Type 中选择的设置而更改。选择适当的设置： FileDate • EarlierThan • LaterThan • EqualTo • Within：最近 *n* 天。有效值为 1 到 300 天。 FileExistence • Exists • DoesNotExist FileVersion • EarlierThan • LaterThan • EqualTo	File Operator 选项会根据在 File Type 中选择的设置而更改。选择适当的设置： FileDate • EarlierThan • LaterThan • EqualTo • Within：最近 *n* 天。有效值为 1 到 300 天。 FileExistence • Exists • DoesNotExist
文件 **CRC** 数据	（仅当您选择的文件类型为 **CRC32** 时可用）您可以输入校验和值（例如，0x3c37fec3）来检查文件完整性。校验和值应以 0x（一个十六进制整数）开头。	（仅当您选择的文件类型为 **CRC32** 时可用）您可以输入校验和值（例如，0x3c37fec3）来检查文件完整性。校验和值应以 0x（一个十六进制整数）开头。
文件 **SHA-256** 数据	（仅当您选择的文件类型为 **SHA-256** 时可用）您可以可以输入 64 字节十六进制哈希值来检查文件完整性。	（仅当您选择的文件类型为 **SHA-256** 时可用）您可以可以输入 64 字节十六进制哈希值来检查文件完整性。
日期和时间	（仅当您选择的文件类型为 **FileDate** 时可用）以 mm/dd/yyyy 和 hh:mm:ss 格式输入客户端系统的日期和时间。	（仅当您选择的文件类型为 **FileDate** 时可用）以 mm/dd/yyyy 和 hh:mm:ss 格式输入客户端系统的日期和时间。

相关主题

简单安全评估条件，第 963 页
复合安全评估条件，第 964 页
创建终端安全评估条件，第 1016 页

防火墙条件设置

防火墙条件检查终端上是否运行有特定防火墙产品。支持的防火墙产品列表基于 OPSWAT 支持图表。在初始安全评估和定期重新评估 (PRA) 期间，您可以实施策略。

Cisco ISE 为 Windows 和 Mac OS 提供默认防火墙条件。默认情况下会禁用这些条件。

字段名称	使用指南
名称	输入防火墙条件的名称。
说明	输入对防火墙条件的说明。
合规性模块	选择所需的合规性模块。 • 4.x 或更高版本 • 3.x 或更高版本 • 任何版本
操作系统	检查终端上是否安装有必需的防火墙产品。您可以选择 Windows OS 或 Mac OSX。
供应商	从下拉列表中选择一个供应商名称。供应商的防火墙产品，及其检查类型显示于**所选供应商的产品 (Products for Selected Vendor)** 表中，可从该表检索。表中所列内容根据所选操作系统而变化。
检查类型	已启用 (Enabled)：检查终端上是否运行了特定防火墙。通过参考 **Products for Selected Vendor** 列表，验证供应商产品是否支持所选检查类型。

注册表条件设置

下表介绍了“注册表条件”(Registry Conditions) 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **注册表条件 (Registry Condition)**。

表 ***148:*** 注册表条件设置

字段名称	使用指南
名称	输入注册表条件的名称。
说明	输入对注册表条件的说明。
作为	选择一个预定义设置作为注册表类型。

字段名称	使用指南
注册表根项	选择一个预定义设置作为注册表根项。
子项	输入不带反斜杠的子项（“\”）以检查在 注册表根项 (Registry Root Key) 中指定的路径中的注册表项。 例如，SOFTWARE\Symantec\Norton AntiVirus\version 将检查以下路径中的注册表项： HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
值名称	（仅在选择 **RegistryValue** 或 **RegistryValueDefault** 作为 Registry Type 的情况下可用）为 **RegistryValue** 输入要检查的注册表项名称值。 这是 **RegistryValueDefault** 的默认字段。
值 数据类型	（仅在选择 **RegistryValue** 或 **RegistryValueDefault** 作为 Registry Type 的情况下可用）选择一个以下设置： • **未指定 (Unspecified)**：检查注册表项值是否存在。此选项仅可用于 **RegistryValue**。 • **数值 (Number)**：检查注册表项值中指定的数值 • **字符串 (String)**：检查注册表项值中的字符串 • **版本 (Version)**：检查注册表项值中的版本
值运算符	选择相应的设置。
值 数据	（仅在选择**RegistryValue** 或 **RegistryValueDefault** 作为 Registry Type 的情况下可用）根据您在 **值数据类型** 中选择的数据类型输入注册表项的值。
操作系统	选择应该应用此注册表条件的操作系统。

相关主题

简单安全评估条件，第 963 页
复合安全评估条件，第 964 页

连续的终端属性监控

可以使用Cisco AnyConnect 代理连续监控不同终端属性，以确保在安全评估期间观察动态变化。这会提高终端的整体可视性，并帮助您根据其行为创建安全评估策略。Cisco AnyConnect 代理监控安装并运行在终端上的应用。您可以打开和关闭此功能，并配置应监控数据的频率。默认情况下，每5分钟收集一次数据，并存储在数据库中。在初始安全评估过程中，Cisco AnyConnect报告正在运行和已安装的应用的完整列表。在初始安全评估后，Cisco AnyConnect 代理每 X 分钟扫描一次应用，并将其与最后一次扫描的差异发送到服务器。服务器显示正在运行和已安装的应用的完整列表。

应用条件设置

安装在终端上的应用的应用条件查询。这有助于您了解终端上分布的软件的汇聚可视性。例如，根据此信息，您可以创建策略并与桌面团队合作以减少软件许可证。

下表说明**应用条件 (Application Conditions)** 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **策略元素 (Policy Elements)** > **应用条件 (Application Condition)** > **添加 (Add)**.

字段名称	使用指南
名称	输入应用条件的名称。
说明	输入应用条件的说明。
操作系统	选择应用条件适用的 Windows OS 或 MAC OSX。
合规性模块	支持 OESIS 4.x 或更高版本、3.x 或更低版本，或任何版本。
检查方式	选择以下其中一个选项： • **进程 (Process)**：选中此选项可检查进程是否正在终端上运行。 • **应用 (Application)**：选中此选项可检查应用是否正在终端上运行。
进程名称	（当选择**进程 (Process)** 作为**检查方式 (Check By)** 选项时可用）输入所需的进程名称。
应用运算符	（当选择**进程 (Process)** 作为**检查方式 (Check By)** 选项时可用）选择以下选项之一： • **正在运行 (Running)**：选中该选项可检查某应用是否正在终端上运行。 • **未在运行 (Not Running)**：选中该选项可检查某应用是否未在终端上运行。

字段名称	使用指南
应用状态	（当选择**应用 (Application)** 作为**检查方式 (Check By)** 选项时可用）选择以下选项之一： • **已安装 (installed)**：选中此选项可检查客户端系统中是否安装了恶意应用。如果找到恶意应用，则触发补救操作。 • **正在运行 (Running)**：选中此选项可检查应用是否正在终端上运行。
调配分类依据	（当选择**应用 (Application)** 作为**检查方式 (Check By)** 选项时可用）选择以下选项之一： • **一切 (Everything)**：您可以选择所有列出的类别，如浏览器、补丁管理等。 • **名称 (Name)**：您应至少选择一个类别。例如，如果选择**浏览器 (Browser)** 类别，则会在**供应商 (Vendor)** 下拉列表中显示相应的供应商。 • **类别 (Category)**：您可以选中一个或多个类别，如防恶意软件、备份、浏览器或数据存储。 **注释** 类别会通过 OPSWAT 库动态更新。

您可以在以下位置查看每个终端的已安装和运行中应用的数量：**情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **合规 (Compliance)** 窗口。

在传出数据包通过以太网微处理器退出前，此 **主页 (Home)** > **摘要 (Summary)** > **合规 (Compliance)** 窗口显示接受终端安全状态评估并且合规的终端百分比。

服务条件设置

下表介绍**服务条件 (File Conditions)** 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **服务条件 (Service Condition)**。

表 ***149:*** 服务条件设置

字段名称	使用指南
名称	输入服务条件的名称。
说明	输入对服务条件的说明。

字段名称	使用指南
操作系统	选择应该应用此服务条件的操作系统。您可以选择不同 Windows OS 或 Mac OSX 版本。
服务名称	输入以 root 身份运行的后台守护程序或用户代理服务的名称，例如，com.apple.geod。AnyConnect 代理使用 **sudo launchctl list** 命令验证服务条件。
服务类型	选择 AnyConnect 应检查的服务类型以确保客户端合规性： • **后台守护程序 (Daemon)**：检查客户端中后台守护程序的指定列表中是否存在特定服务，例如扫描客户端设备中的恶意软件。 • **用户代理 (User Agent)**：检查客户端中用户服务的指定列表中是否存在特定服务，例如当检测到恶意软件时运行的服务。 • **后台守护程序或用户代理 (Daemon or User Agent)**：检查后台守护程序或用户代理服务列表中是否存在特定服务。
服务算符	选择您希望在客户端中检查的服务状态： • **Windows OS**：检查服务**正在运行 (Running)** 还是**未运行 (Not Running)**。 • **Mac OSX**：检查服务**已加载 (Loaded)**、**未加载 (Not Loaded)**、**已加载并运行 (Loaded and Running)**、**已加载并含有退出代码 (Loaded with Exit Code)** 还是**已加载并运行或含有退出代码 (Loaded & running or with Exit code)**。

相关主题

简单安全评估条件，第 963 页
复合安全评估条件，第 964 页

安全评估复合条件设置

下表介绍**复合条件 (Compound Conditions)** 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **复合条件 (Compound Condition)**。

表 *150:* 安全评估复合条件设置

字段名称	使用指南
名称	输入您要创建的复合条件的名称。
说明	输入对您要创建的复合条件的说明。
操作系统	选择一个或多个 Windows 操作系统。这允许关联应用该条件的 Windows 操作系统。
括号 ( )	点击此括号以将以下简单条件类型的两个简单条件组合起来：文件、注册表、应用和服务条件。
(&)：AND 运算符（用“&”表示 AND 运算符，不需要加引号）	您可以在复合条件中使用 AND 运算符（与号 [&]）。例如，输入 **Condition1 & Condition2**。
(|)：OR 运算符（用“|”表示 OR 运算符，不需要加引号）	您可以在复合条件中使用 OR 运算符（小竖线 [|]）。例如，输入 **Condition1 & Condition2**。
(!)：NOT 运算符（用“!”表示 NOT 运算符，不需要加引号）	您可以在复合条件中使用 NOT 运算符（感叹号 [!]）。例如，输入 **Condition1 & Condition2**。
简单条件	从以下类型的简单条件列表中选择：文件、注册表、应用和服务条件。 您还可以从对象选择器创建文件、注册表、应用和服务条件的简单条件。 在**操作 (Action)** 按钮上点击快速选择器（向下箭头）以创建文件、注册表、应用和服务条件的简单条件。

相关主题

安全评估条件，第 963 页
创建复合安全评估条件，第 965 页

防病毒条件设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **防病毒条件 (Anti-Virus Condition)**。

字段名称	使用指南
名称	输入要创建的防病毒条件的名称。
说明	输入要创建的防病毒条件的说明。

字段名称	使用指南
操作系统	选择用于检查客户端的防病毒程序安装情况，或检查条件所适用的最新防病毒定义文件更新的操作系统。
供应商	从下拉列表中选择供应商。通过选择供应商，系统会检索供应商的防病毒产品和版本，这些信息显示在 Products for Selected Vendor 表中。
检查类型	选择是检查客户端的防恶意软件程序安装情况，还是检查最新定义文件更新。
安装	选择此选项，只检查客户端的防病毒程序安装情况。
定义	选择此选项，只检查客户端的防病毒产品的最新定义文件更新。

所选供应商的产品

从表中选择防病毒产品。根据在“新防病毒条件”(New Anti-virus Condition) 页面中选择的供应商，此表会检索有关供应商的防病毒产品和版本、其提供的补救支持、最新定义文件日期及其版本的信息。

通过从表中选择产品，可以检查防病毒程序的安装情况，或检查最新防病毒定义文件日期，及其最新版本。

注释 从**基准条件 (Baseline Condition)** 或**高级条件 (Advanced Condition)** 中，只能为每个防病毒产品配置一个条件。

基准条件

字段名称	使用指南
最小版本	（仅当您更新操作系统和供应商时可用）从下拉列表中选择防病毒程序的最小版本。 该检查会在网络上的所有终端上实施网络策略，以符合防病毒程序的最小版本条件。
最大版本	当您更新终端安全评估源时，系统会自动修订防病毒程序的最大版本。
最低合规性模块版本	最低合规性模块版本会从 AnyConnect 更新。

高级条件

字段名称	使用指南
针对最新防病毒定义文件版本进行检查（如适用）	（仅当选择“定义”(Definition) 检查类型时可用）如果最新防病毒定义文件版本由于Cisco ISE中的终端安全评估更新变为可用，则选择此选项以针对最新防病毒定义文件版本，来检查客户端的防病毒定义文件版本。否则，此选项使您可以针对Cisco ISE 中的最新定义文件日期检查客户端的定义文件日期。
允许病毒定义文件 （已启用）	（仅当选择“定义”(Definition) 检查类型时可用）选择此选项，检查客户端上的防病毒定义文件版本和最新防病毒定义文件日期。最新定义文件日期不能早于在下一个字段（days older than 字段）定义的产品的最新防病毒定义文件日期或当前系统日期。 如果未选中，则思科 ISE 使您可以使用 Check against latest AV definition file version, if available 选项，只检查防病毒定义文件的版本。
早于的天数	定义客户端的最新防病毒定义文件日期可以早于产品的最新防病毒定义文件日期或当前系统日期的天数。默认值为零 (0)。
最新文件日期	选择此选项，检查客户端的防病毒定义文件日期，该日期早于产品最新防病毒定义文件日期的天数可以是在“早于的天数”(Days Older Than) 字段中定义的天数。 如果将天数设置为默认值(0)，则客户端的防病毒定义文件日期不应早于产品的最新防病毒定义文件日期。
当前系统日期	选择此选项，检查客户端的防病毒定义文件日期，该日期早于产品最新防病毒定义文件日期的天数可以是在“早于的天数”(Days Older Than) 字段中定义的天数。 如果将天数设置为默认值(0)，则客户端的防病毒定义文件日期不应早于当前系统日期。

相关主题

复合安全评估条件，第 964 页
预配置的防病毒和反间谍软件条件，第 966 页
防病毒和反间谍软件支持图表，第 966 页

反间谍软件复合条件设置

下表介绍**作为复合条件 (AS Compound Conditions)** 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **作为复合条件 (AS Compound Condition)**。

表 ***151:*** 反间谍软件复合条件设置

字段名称	使用指南
名称	输入您要创建的反间谍软件复合条件的名称。
说明	输入对您要创建的反间谍软件复合条件的说明。
操作系统	选择一个操作系统，该操作系统应允许检查客户端上的反间谍软件程序的安装，或检查应用该条件的最新反间谍软件定义文件更新。
供应商	从下拉列表中选择供应商。选择供应商会检索其反间谍软件产品和版本，这些信息显示于Products for Selected Vendor 表中。
检查类型	选择您是想要在客户端上检查安装，还是检查最新定义文件更新。
安装	选择您是否只想检查客户端上的反间谍软件程序的安装。
定义	选择您是否只想检查客户端上的反间谍软件软件的最新定义文件更新。
允许病毒定义文件 **(Allow virus definition file to be)**（已启用）	当您创建的是反间谍软件定义检查类型时，请选中此复选框；当您创建的是反间谍软件安装检查时，请禁用此复选框。 如果选中此复选框，系统将允许您在客户端上检查反间谍软件定义文件版本和最新反间谍软件定义文件日期。最新的定义文件日期不能早于您在 days older than 字段中定义的距离当前系统日期的天数。 如果未选中此复选框，您就只能选择反间谍软件定义文件的版本，因为未选中 允许病毒定义文件 (Allow virus definition file to be) 复选框。
早于的天数 **(Days Older Than)**	定义在客户端上最新的反间谍软件定义文件日期可以早于当前系统日期的天数。默认值为零 (0)。

字段名称	使用指南
当前系统日期 (Current System Date)	选择在客户端上检查反间谍软件定义文件日期，此日期可以早您在 days older than 字段中定义的天数。 如果您将此天数设置为默认值(0)，则客户端上的反间谍软件定义文件日期不得早于当前系统日期。
所选供应商的产品	从表中选择反间谍软件产品。根据您在 New Anti-spyware Compound Condition 页面选择的供应商，此表检索关于其反间谍软件产品及版本的信息、其所提供的补救支持、最新定义文件日期及其版本。 您可以通过从表中选择产品，检查反间谍软件程序的安装，或检查最新反间谍软件定义文件日期，及其最新版本。

相关主题

复合安全评估条件，第 964 页
预配置的防病毒和反间谍软件条件，第 966 页
防病毒和反间谍软件支持图表，第 966 页

防恶意软件条件设置

防恶意软件条件是反间谍软件和防病毒条件的组合，由OESIS版本4.x或更高版本合规性模块支持。

在思科ISE GUI中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **防恶意软件条件 (Antimalware Conditions)**。

注释 建议您手动更新已安装的防恶意软件产品，使其至少有一次最新的定义。否则，使用AnyConnect对防恶意软件定义的安全评估检查将失败。

字段名称	使用指南
名称	输入防恶意软件条件的名称。
说明	输入防恶意软件条件的说明。
合规性模块	支持 OESIS 版本 4.x 或更高版本。

字段名称	使用指南
操作系统	选择一操作系统，以检查客户端的防恶意软件程序安装情况，或检查条件所适用的最新防恶意软件定义文件更新。它支持 MAC 和 Windows 操作系统。
供应商	从下拉列表中选择供应商。**所选供应商的产品 (Products for Selected Vendor)** 列表会显示该供应商提供的防恶意软件产品、版本、最新定义日期、最新定义版本和最低合规性模块版本。
检查类型	选择是检查客户端的防恶意软件程序安装情况，还是检查最新定义文件更新。
安装	选择此选项，只检查客户端的防恶意软件程序安装情况。
定义	选择此选项，只检查客户端防恶意软件产品的最新定义文件更新。

所选供应商的产品

从表中选择一款防恶意软件产品。根据在“新的防恶意软件条件”(New Antimalware Condition) 页面中选择的供应商，此表会检索有关供应商的防恶意软件产品和版本、其提供的补救支持、最新定义文件日期及其版本的信息。

通过从表中选择一款产品，可以检查防恶意软件程序的安装情况，或检查最新防恶意软件定义文件日期，及其最新版本。

注释 从**基准条件 (Baseline Condition)** 或**高级条件 (Advanced Condition)** 中，只能为每个防恶意软件产品配置一个条件。

基准条件

字段名称	使用指南
最小版本	（仅当您更新操作系统和供应商时可用）从下拉列表中选择防恶意软件的最小版本。 该检查会在网络上的所有终端上实施网络策略，以符合反恶意软件的最小版本条件。
最大版本	当您更新终端安全评估源时，系统会自动修订防恶意软件的最大版本。
最低合规性模块版本	最低合规性模块版本会从 AnyConnect 更新。

高级条件

字段名称	使用指南
针对最新 AV 定义文件版本进行检查（如适用）	（仅当选择“定义”(Definition) 检查类型时可用）如果最新防恶意软件定义文件版本由于Cisco ISE 中的终端安全评估更新变为可用，则选择此选项以针对最新防恶意软件定义文件版本，来检查客户端的防恶意软件定义文件版本。否则，此选项使您可以针对Cisco ISE中的最新定义文件日期检查客户端的定义文件日期。 只有在Cisco ISE 中所选产品的“最新定义日期”(Latest Definition Date) 或“最新定义版本”(Latest Definition Version) 字段内列有数值，该检查才有效。否则，必须使用“当前系统日期”(Current System Date) 字段。
允许病毒定义文件 （已启用）	（仅当选择“定义”(Definition) 检查类型时可用）选择此选项，检查客户端上的防恶意软件定义文件版本和最新防恶意软件定义文件日期。最新定义文件日期不能早于在下一个字段（“早于的天数”(Days Older Than) 字段）定义的产品最新防恶意软件定义文件日期或当前系统日期。 如果未选中，则思科 ISE 允许您使用“请针对最新 AV 定义文件版本进行检查，如适用”(Check against latest AV definition file version, if available) 选项，只检查防恶意软件定义文件的版本。
早于的天数	定义客户端的最新防恶意软件定义文件日期可以早于产品的最新防恶意软件定义文件日期或当前系统日期的天数。默认值为零 (0)。
最新文件日期	选择此选项，检查客户端的防恶意软件定义文件日期，该日期早于产品最新防恶意软件定义文件日期的天数可以是在“早于的天数”(Days Older Than) 字段中定义的天数。 如果将该天数设置为默认值(0)，则客户端的防恶意软件定义文件日期不应早于产品的最新防恶意软件定义文件日期。 只有在Cisco ISE 中所选产品的“最新定义日期”(Latest Definition Date) 字段列有数值，该检查才有效。否则，必须使用“当前系统日期”(Current System Date) 字段。

字段名称	使用指南
当前系统日期	选择此选项，检查客户端的防恶意软件定义文件日期，该日期早于产品最新防恶意软件定义文件日期的天数可以是在“早于的天数”(Days Older Than) 字段中定义的天数。 如果将天数设置为默认值(0)，则客户端的防恶意软件定义文件日期不应早于当前系统日期。

相关主题

复合安全评估条件，第 964 页

字典简单条件设置

下表介绍了**字典简单条件 (Dictionary Simple Conditions)** 窗口上的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **字典简单条件 (Dictionary Simple Condition)**。

表 *152:* 字典简单条件设置

字段名称	使用指南
名称	输入您要创建的字典简单条件的名称。
说明	输入对您要创建的字典简单条件的说明。
属性	从字典选择属性。
运算符	选择将值与您所选择的属性关联的运算符。
Value	输入您想要与字典属性关联的值，或从下拉列表选择预定义值。

相关主题

字典和字典属性
简单和复合条件
简单安全评估条件，第 963 页
创建简单安全评估条件，第 964 页

字典复合条件设置

表 *153:* 字典复合条件设置

字段名称	使用指南
Name	输入要创建的字典复合条件的名称。

字段名称	使用指南
Description	输入要创建的字典复合条件的说明。
从库中选择现有条件	通过从策略要素库选择预定义的条件来定义表达式，或在后续步骤中将临时属性/值对添加到表达式中。
条件名称	选择已从策略要素库中创建的字典简单条件。
表达式	Expression 会根据从 Condition Name 下拉列表选择的选项进行更新。
AND 或 OR 运算符	选择 AND 或 OR 运算符可逻辑组合可从策略要素库添加的字典简单条件。 点击 **Action** 图标可执行以下操作： • Add Attribute/Value • Add Condition from Library • Delete
创建新条件（高级选项）	从各种系统或用户定义的字典中选择属性。 还可以在后续步骤中从策略要素库中添加预定义条件。
条件名称	选择已创建的字典简单条件。
表达式	从 Expression 下拉列表可以创建字典简单条件。
运算符	选择要将值关联到属性的运算符。
Value	输入要关联到字典属性的值，或者从下拉列表中选择一个值。

相关主题

字典和字典属性
简单和复合条件
复合安全评估条件，第 964 页
创建复合安全评估条件，第 965 页

补丁管理条件设置

下表介绍了**补丁管理条件** (Patch Management Conditions) 窗口上的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **补丁管理条件 (Patch Management Condition)**。

表 *154:* 补丁管理条件

字段名称	使用指南
名称	输入补丁管理条件的名称。
说明	输入对补丁管理条件的说明。
操作系统	选择操作系统以检查终端上补丁管理软件的安装，或检查应用该条件的最新补丁管理定义文件更新。您可以选择 Windows OS 或 Mac OSX。您还可以选择不止一个版本的操作系统以创建补丁管理条件。
供应商名称	从下拉列表中选择一个供应商名称。供应商的补丁管理产品及其支持的版本、检查类型和最低合规模块显示在**选定供应商产品 (Products for Selected Vendor)** 表中，可从该表检索。表中所列内容根据所选操作系统而变化。

字段名称	使用指南
检查类型	请选择以下任意一个选项： • **安装 (Installation)**：检查是否在终端上安装了所选产品。所有供应商均支持此检查类型。 注释 对于思科临时代理，只能在**要求 (Requirements)** 页面中查看包含**安装 (Installation)** 检查类型的补丁管理条件。 • **已启用 (Enabled)**：检查是否在终端上启用了所选产品。通过参考 **Products for Selected Vendor** 列表，验证供应商产品是否支持所选检查类型。 • **最新 (Up to Date)**：检查所选产品是否缺失补丁。通过参考 **Products for Selected Vendor** 列表，验证供应商产品是否支持所选检查类型。 点击 **Products for Selected Vendor** 下拉箭头，以查看您在 **Vendor Name** 中指定的供应商支持的产品列表。例如，如果您选择了供应商 A，该供应商有两个产品，分别是为产品 1 和产品 2。产品 1 可能会支持 Enabled 选项，而产品 2 可能不支持此选项。或者，如果产品 1 不支持任何一个检查类型，它将灰显。 注释 （适用于Cisco ISE 2.3 及更高版本以及 AnyConnect 4.5 及更高版本）如果在 SCCM 的补丁管理条件中选择“最新”(Up to Date) 检查类型，Cisco ISE 1. 将使用 Microsoft API 检查指定严重性级别的当前安全补丁。 2. 触发对于此缺失安全补丁的补丁管理补救。

字段名称	使用指南
检查已安装的补丁	（仅当您选择“最新”(Up To Date) 检查类型时可用。）可以为缺失的补丁配置严重性级别，然后根据严重性进行部署。选择以下任一严重性级别： • **仅严重级别 (Critical Only)**：检查部署中的终端上是否安装了严重级别软件补丁。 • **重要和严重级别 (Important and Critical)**：检查部署中的终端上是否安装了重要和严重级别软件补丁。 • **中级、重要和严重级别 (Moderate, Important, & Critical)**：检查部署中的终端上是否安装了中级、重要和严重级别软件补丁。 • **低级到严重级别 (Low To Critical)**：检查部署中的终端上是否安装了低级、中级、重要和严重级别软件补丁。 • **全部 (All)**：安装所有严重性级别的缺失补丁。

相关主题

安装软件补丁

回滚软件补丁

查看补丁安装和回滚更改

创建补丁管理条件，第 969 页

磁盘加密条件设置

下表介绍了**磁盘加密条件 (Disk Encryption Condition)** 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **磁盘加密条件 (Disk Encryption Condition)**。

表 ***155:*** 磁盘加密条件设置

字段名称	使用指南
名称	输入要创建的磁盘加密条件的名称。
说明	输入对磁盘加密条件的说明。

字段名称	使用指南
操作系统	选择要进行磁盘加密检查的终端的一个操作系统。您可以选择 Windows OS 或 Mac OSX。您还可以选择一个操作系统的多个版本，以创建磁盘加密条件。
供应商名称	从下拉列表中选择一个供应商名称。**所选供应商的产品 (Products for Selected Vendor)** 表中检索并显示供应商的数据加密产品、其支持的版本、加密状态检查和最低的兼容性模块支持。表中所列内容根据所选操作系统而变化。

位置	仅当**所选供应商的产品 (Products for Selected Vendor)**部分有项目被勾选时才启用。请选择以下任意一个选项：
	• **特定位置 (Specific Location)**：检查指定的磁盘驱动器是否已在终端加密（例如，Windows 操作系统的 C:），或指定的卷标是否已加密（例如，Mac OSX 的 Mackintosh HD）。
	• **系统位置 (System Location)**：检查默认的 Windows 操作系统驱动器或 Mac OSX 硬盘驱动器是否已在终端加密。
	• **所有内部驱动器 (All Internal Drives)**：检查内部驱动器。包括已挂载和加密的所有硬盘以及所有内部分区。不包括只读驱动器、系统恢复磁盘/分区、引导分区、网络分区和终端外部的不同物理磁盘驱动器（包括但不限于通过 USB 和 Thunderbolt 连接的磁盘驱动器）。经过验证的加密软件产品包括：
	  • Bit-locker-6.*x*/10.*x*
	  • Windows 7 上的 Checkpoint 80.*x*

字段名称	使用指南
加密状态	当所选的产品不支持加密状态检查时，“加密状态”(Encryption State) 复选框为禁用状态。仅该复选框被选中时，才会显示中继器。您可以选择“完全加密”(Fully Encrypted) 选项来检查客户端的磁盘驱动器是否为完全加密。 如果您创建一个条件（例如，TrendMicro），并选择两个供应商，其中一个的加密状态为“是”，另一个的加密状态为“否”，则“加密状态”(Encryption State) 将被禁用，因为其中有一个供应商的加密状态为“否”。 注释 您可以点击中继器以添加更多位置，并且每个位置之间的关系为逻辑“和”(AND) 运算符。

相关主题

创建磁盘加密条件，第 970 页

USB 条件设置

下表介绍了 **USB 条件 (USB Condition)** 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **策略元素 (Policy Elements)** > **USB**。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **USB 条件 (USB Condition)**

USB 检查是一个预定义条件且仅支持 Windows 操作系统。

表 *156: USB* 条件设置

字段名称	使用指南
名称 **(Name)**	USB_Check
说明	Cisco预定义检查
操作系统	Windows
合规性模块	用于版本 4.x（及更高版本）的支持 ISE 终端安全评估状态合规性模块的只显示字段。

相关主题

简单安全评估条件，第 963 页

硬件属性条件设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **硬件属性条件 (Hardware Attributes Condition)** 访问**硬件属性条件 (Hardware Attributes Condition)** 窗口。下表介绍了**硬件属性条件 (Hardware Attributes Condition)** 窗口中的字段。

字段名称	使用指南
名称	Hardware_Attributes_Check：分配给条件的默认名称。
说明	从客户端收集硬件属性的Cisco预定义检查。
操作系统	Windows 或 Mac OS
合规性模块	4.x 或更高版本

相关主题

硬件控制板 ，第 94 页

终端安全评估外部数据源条件

您可以配置条件，将终端 UDID 与外部数据源进行匹配。目前，仅支持 Active Directory。ISE 不包括终端安全评估代理将 UDID 发送到 Active Directory 所需的脚本。

配置安全评估策略

安全评估策略是与一个或多个身份组和操作系统关联的安全评估要求的集合。词典属性是可与身份组和操作系统一起使用以便为设备定义不同策略的可选条件。

Cisco ISE 提供一个为不合规的设备配置宽限时间的选项。如果发现设备不合规，Cisco ISE 会在安全评估结果缓存中查找之前已知的良好状态，并为设备提供相应的宽限时间。在宽限期内，设备将获得网络访问权限。您可以按分钟、小时或天（最多 30 天）配置宽限时段。

有关详细信息，请参阅《ISE 安全评估规范性部署指南》中的“安全评估策略”一节。

注释

- 当宽限期延长或缩短时，如果设备再次经历安全评估流程（例如，如果启用了**延迟通知 (Delayed Notification)** 选项，选择了**重新扫描 (Re-Scan)** 选项，则设备将断网或重新连网），新宽限期和延迟通知将应用。
- 宽限期不适用于临时代理。
- 当设备匹配多个终端安全评估策略（每个策略有不同的宽限期）时，设备将获取在不同策略中配置的最大宽限期。
- 设备处于宽限期时，不会显示“可接受使用政策”(AUP)。

开始之前

- 您必须了解可接受使用政策 (AUP)。
- 您必须了解定期重新评估 (PRA)。
- 您必须使用 AnyConnect 代理 4.7 或更高版本才能查看与合规性相关的通知。有关配置 AnyConnect 代理的详细信息，请参阅创建 AnyConnect 配置，第 1044 页。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **安全评估 (Posture)** 或**工作中心 (Work Centers)** > **安全评估 (Posture)** > **安全评估策略 (Posture Policy)**。

步骤 2 使用下拉箭头添加新策略。

步骤 3 要编辑配置文件，请双击策略或点击行末的“编辑”(Edit)。

步骤 4 从**规则状态 (Rule Status)** 下拉列表中，选择**已启用 (Enabled)**或**已禁用 (Disabled)**。

步骤 5 选择**策略选项 (Policy Options)** 下的下拉列表，并以分钟，小时或天为单位指定**宽限期设置 (Grace Period Settings)**。

有效值为：

- 1 到 30 天
- 1 到 720 小时
- 1 到 43200 分钟

默认情况下，此设置处于禁用状态。

注释 即使终端安全评估结果不合规，如果发现设备之前已合规且缓存尚未过期，则系统会在**宽限期设置 (Grace Period Settings)** 中指定的时间段内授予设备访问权限。

步骤 6 （可选）拖动名为**延迟通知 (Delayed Notification)** 的滑块延迟宽限期提示，直到宽限期消耗特定百分比后再显示给用户。例如，通知延迟期设置为 50% 且配置的宽限期为 10 分钟，则Cisco ISE 将在 5 分钟后检查安全评估状态，如果发现终端不合规，则显示宽限期通知。如果终端状态为合规，则不会显示宽限期通知。如果通知延迟时间设置为 0%，系统会在宽限期开始时立即提示用户以解决问题。但在宽限期过期之前，终端会被授予访问权限。此字段的默认值为 0%。有效范围为 0 到 95%。

步骤 7 在**规则名称 (Rule Name)** 字段中，输入策略的名称。

注释 最好将每项要求作为单独的规则来配置安全评估策略，以避免意外结果。

步骤 8 从**身份组 (Identity Groups)** 列中，选择所需的身份组。

您可以根据用户或终端身份组来创建安全评估策略。

步骤 9 从**操作系统 (Operating Systems)** 列中，选择操作系统。

步骤 10 从**合规性模块 (Compliance Module)** 列中，选择所需的合规性模块：

- **4.x 或更高版本 (4.x or Later)**：支持反恶意软件、磁盘加密、补丁管理和 USB 条件。
- **3.x 或更低版本 (3.x or Earlier)**：支持防病毒、反间谍软件、磁盘加密和补丁管理条件

- **任何版本 (Any Version)**：支持文件、服务、注册表、应用和复合条件。

步骤 11 从**终端安全评估类型 (Posture Type)** 列中，选择终端安全评估类型 (Posture Type)。

- **AnyConnect** - 部署 AnyConnect 代理以监视和实施需要客户端干预的Cisco ISE 策略。
- **AnyConnect Stealth** - 部署 AnyConnect 代理以监控和实施Cisco ISE 安全评估策略，而无需任何客户端干预。
- **临时代理 (Temporal Agent)** - 在客户端上运行以检查合规性状态的临时可执行文件。

步骤 12 在 **Other Conditions** 中，您可以添加一个或多个词典属性，然后以简单或复合条件的方式将它们保存到词典中。

注释 您在**安全评估策略 (Posture Policy)** 窗口中创建的词典简单条件和复合条件在配置授权策略时不显示。

步骤 13 在**要求 (Requirements)** 字段中指定要求。

步骤 14 点击**保存 (Save)**。

配置 AnyConnect 工作流程

要配置 AnyConnect 代理，请在Cisco ISE 中执行以下步骤：

步骤 1 创建 AnyConnect 代理配置文件

步骤 2 为 AnyConnect 包创建 AnyConnect 配置。

步骤 3 创建客户端调配策略。

步骤 4 （可选）创建自定义终端安全评估条件。

步骤 5 （可选）创建自定义补救操作。

步骤 6 （可选）创建自定义终端安全评估要求。

步骤 7 创建终端安全评估策略。

步骤 8 配置客户端调配策略。

步骤 9 创建授权配置文件。

步骤 10 配置授权策略。

注释 Cisco ISE 不支持 ARM64 版本的 AnyConnect 用于 AnyConnect 终端安全评估流程。确保不要在客户端调配策略中使用 ARM64版本的 AnyConnect，否则可能会导致客户端故障。如果 Anyconnect 由于此问题无法正常工作，请重新启动客户端。

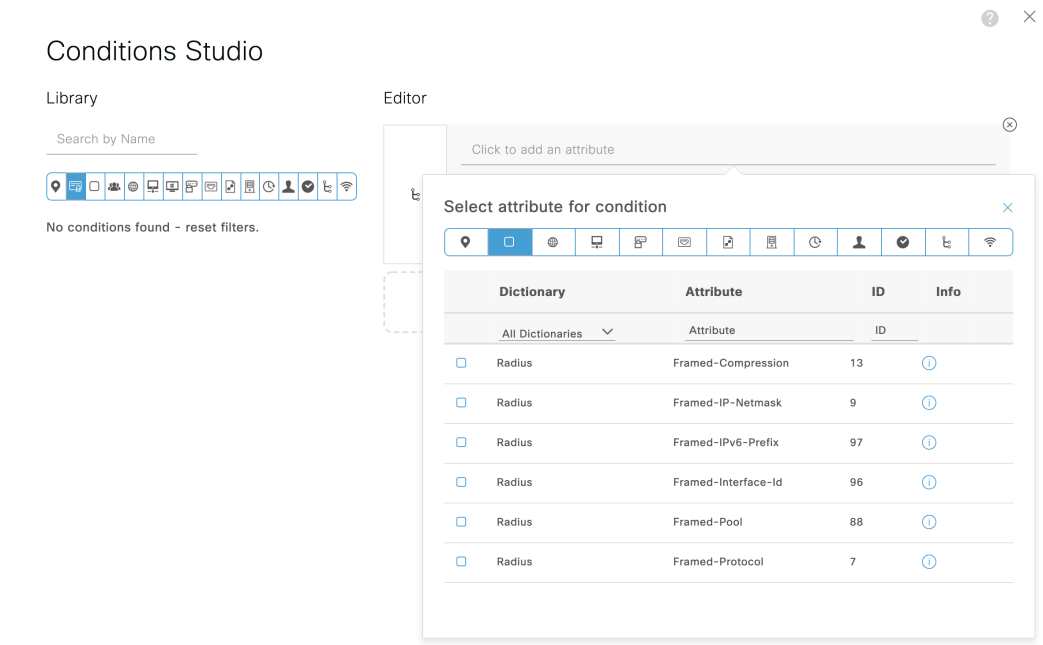
基于证书的条件的先决条件

客户端调配和终端安全评估策略规则可能包括基于证书属性的条件。客户端调配或终端安全评估策略中基于证书的条件的先决条件是为了确保存在基于同一证书属性的匹配授权策略规则。

例如，您应使用图中所示的相同属性，Issuer - Common Name 属性同时用于客户端调配或终端安全评估和授权策略。

图 *59:* 思科调配策略

图 *60: Conditions Studio*



注释 ISE 服务器证书必须在 AnyConnect 4.6 MR2 及更高版本的系统证书库中受信任。如果服务器不受信任，则需要提升权限的终端安全评估检查和补救都不会起作用。

- Windows 操作系统：必须将服务器证书添加到系统证书存储区。
- MAC 操作系统：必须将服务器证书添加到系统密钥链。建议使用命令行实用程序信任证书。如果登录密钥链中已存在证书，则可能无法使用密钥链访问应用将证书添加到系统密钥链。

默认终端安全评估策略

Cisco ISE 软件随附许多预先配置的安全评估策略（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **安全评估 (Posture)**），让您更轻松地创建终端安全评估策略和配置文件。默认情况下，这些策略处于禁用状态。您可以根据要求启用这些策略。以下是一些默认的安全评估策略。

规则名称	说明	要求
Default_Antimalware_Policy_Mac	检查终端是否已在设备中安装并运行任何支持的供应商的防恶意软件（AnyConnect 能识别）。	Any_AM_Installation
Default_Antimalware_Policy_Win	检查终端是否已在设备中安装并运行任何支持的供应商的防恶意软件（AnyConnect 能识别）。	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	收集信息并报告给定终端上安装的所有应用。	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	收集信息并报告给定终端上安装的所有应用。	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	检查终端是否安装了任何支持的供应商的防火墙程序（AnyConnect 能识别）。	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	检查终端是否安装了任何支持的供应商的防火墙程序（AnyConnect 能识别）。	Default_Firewall_Requirement_Win
Default_USB_Block_Win	确保终端设备未连接任何 USB 存储设备。	USB_Block

客户端安全评估

为确保已应用的网络安全措施保持相关和有效，Cisco ISE 使您能够在任何可访问受保护网络的客户端计算机上验证和维护安全功能。通过应用旨在确保最新安全设置或应用在客户端计算机上可用的终端安全评估策略，Cisco ISE 管理员可以确保任何访问网络的客户端都符合并且继续符合为企业网络访问定义的安全标准。终端安全评估合规性报告在用户登录时以及在周期性再评估发生时，为Cisco ISE 提供客户端计算机合规性级别快照。

使用Cisco ISE 中提供的下列代理类型之一，终端安全评估和合规性会发生：

- AnyConnect ISE 代理：持久代理，可以安装在 Windows 或 Mac OS X 客户端计算机上执行终端安全评估合规性功能。
- Cisco临时代理：在客户端运行的临时可执行文件，用于检查合规性状态。登录会话终止后，将从客户端计算机中删除代理。默认情况下，代理位于Cisco ISE ISO 映像中，并在安装期间上传到Cisco ISE。

终端安全状态评估选项

下表提供适用于 Windows 和 Macintosh 的Cisco ISE 终端安全评估代理以及适用于 Windows 的 Web 代理支持的终端安全状态评估（终端安全评估条件）选项的列表。

表 *157:* 终端安全状态评估选项

适用于 **Windows** 的 **ISE** 终端安全评估代理	适用于**Windows**的**Cisco**临时代理	适用于 **Macintosh OS X** 的 **ISE** 终端安全评估代理	适用于 **Macintosh OS X** 的**Cisco**临时代理
操作系统/服务包/修补程序	-	-	-
服务检查	服务检查（临时代理4.5 和 ISE 2.3）	服务检查（AC 4.1 和 ISE 1.4）	不支持后台守护程序检查
注册表检查	注册表检查（临时代理 4.5 和 ISE 2.3）	-	-
文件检查	文件检查（临时代理4.5 和 ISE 2.3）	文件检查（AC 4.1 和 ISE 1.4）	文件检查（临时代理4.5 和 ISE 2.3）
应用检查	应用检查（临时代理4.5 和 ISE 2.3）	应用检查（AC 4.1 和 ISE 1.4）	应用检查（临时代理4.5 和 ISE 2.3）
防病毒软件安装	防恶意软件安装	防病毒软件安装	防恶意软件安装
防病毒软件版本/防病毒软件定义日期	正使用 OPSWAT 版本 4，因此不支持防病毒/反间谍软件；仅支持防恶意软件	防病毒软件版本/防病毒软件定义日期	正使用 OPSWAT 版本 4，因此不支持防病毒/反间谍软件；仅支持防恶意软件
反间谍软件安装	正使用 OPSWAT 版本 4，因此不支持防病毒/反间谍软件；仅支持防恶意软件	反间谍软件安装	正使用 OPSWAT 版本 4，因此不支持防病毒/反间谍软件；仅支持防恶意软件
反间谍软件版本/反间谍软件定义日期	正使用 OPSWAT 版本 4，因此不支持防病毒/反间谍软件；仅支持防恶意软件	反间谍软件版本/反间谍软件定义日期	正使用 OPSWAT 版本 4，因此不支持防病毒/反间谍软件；仅支持防恶意软件
补丁管理检查（AC 4.1 和 ISE 1.4）	仅补丁管理安装检查	补丁管理检查（AC 4.1 和 ISE 1.4）	-
Windows 更新运行	-	-	-

适用于 **Windows** 的 **ISE** 终端安全评估代理	适用于 **Windows** 的**Cisco** 临时代理	适用于 **Macintosh OS X** 的 **ISE** 终端安全评估代理	适用于 **Macintosh OS X** 的**Cisco**临时代理
Windows 更新配置	-	-	-
WSUS 合规性设置	-	-	-

安全评估补救选项

下表列出了Cisco ISE 终端安全评估代理（适用于 Windows 和 Macintosh）和 Web 代理（适用于 Windows）支持的终端安全评估补救选项列表。

表 *158:* 终端安全评估补救选项

ISE 终端安全评估代理（适用于 **Windows**	适用于 **Macintosh OS X**）
消息文本（本地检查）	消息文本（本地检查）
URL 链路（链路分布）	URL 链路（链路分布）
文件分发	-
启动计划	-
防病毒定义更新	防病毒实时更新
反间谍程序定义更新	反间谍程序实时更新
补丁修复检查（AC 4.1 - 和 ISE 1.4）	-
Windows 更新	-
WSUS	-

ISE 社区资源

思科 ISE 与 SCCM 集成参考指南

安全评估的自定义条件

安全评估条件可以是以下任何一个简单条件：文件、注册表、应用、服务或字典条件。这些简单条件中的一个或多个条件构成可与安全评估要求相关联的复合条件。

在初始安全评估更新后，Cisco ISE 还会创建Cisco定义的简单条件与复合条件。Cisco定义的简单条件使用 pc_ 作为前缀，复合条件使用 pr_ 作为前缀。

用户定义的条件或Cisco定义的条件同时包含简单条件与复合条件。

安全评估服务基于防病毒和反间谍软件 (AV/AS) 复合条件利用内部检查。因此，安全评估报告不会反映您已创建的精确 AV/AS 复合条件名称。报告仅显示 AV/AS 复合条件的内部检查名称。

例如，如果您已创建名为“MyCondition_AV_Check”的 AV 复合条件来检查任何供应商与任何产品，则安全评估报告会将内部检查（即“av_def_ANY”）显示为条件名称，而不是显示“MyCondition_AV_Check”。

终端安全评估终端自定义特性

您可以使用终端安全评估终端自定义属性创建客户端调配和终端安全评估策略。最多可以创建 100 个终端自定义属性。支持以下终端自定义属性类型：Int、String、Long、Boolean 和 Float。

终端自定义属性可用于根据某些属性允许或阻止设备，或根据安全评估或客户端调配策略分配特定权限。

使用终端自定义属性创建终端安全评估策略

要使用终端自定义属性创建终端安全评估策略，请执行以下操作：

步骤 1 创建终端自定义属性。

a)

b) 在**终端自定义属性 (Endpoint Custom Attributes)** 区域，输入**属性名称 (Attribute Name)**（例如，deviceType）和“数据类型”（例如，字符串）。

c) 点击**保存 (Save)**。

步骤 2 为自定义属性分配值。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**。

b) 分配自定义属性值。

- 选中所需的 MAC 地址复选框，然后点击**编辑 (Edit)**。
- 或者，点击所需的 MAC 地址，然后点击**终端 (Endpoints)** 页面中的**编辑 (Edit)** 。

c) 确保您创建的自定义属性显示在**编辑终端 (Edit Endpoint)** 对话框的**自定义属性 (Custom Attributes)** 区域中。

d) 点击**编辑 (Edit)**并输入所需的属性值（例如，deviceType = Apple-iPhone）。

e) 点击**保存 (Save)**。

步骤 3 使用自定义属性和值创建授权策略。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **安全评估 (Posture)** > **终端安全评估策略 (Posture Policy)**。

b) 创建所需的策略。通过点击**其他条件 (Other Conditions)** 选择自定义属性，然后选择所需的字典，例如，选择“终端”(Endpoints) > “设备类型”(deviceType)，即您在第 1 步中创建的自定义属性。有关详细信息，请参阅配置思科临时代理工作流程 ，第 1018 页。

c) 点击**保存 (Save)**。

要使用终端自定义属性创建客户端调配策略，请执行以下操作：

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **客户端调配 (Client Provisioning)** > **客户端调配策略 (Client Provisioning Policy)**。
2. 创建所需的策略。
   - 创建所需的规则（例如，Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。
   - 点击**其他条件 (Other Conditions)** 并选择所需的字典，选择自定义属性。

自定义安全评估补救措施

自定义安全评估补救措施是文件、链接、防病毒或反间谍软件定义更新、启动程序、Windows 更新或 Windows Server Update Services (WSUS) 补救类型。

添加文件补救

客户端可以通过文件补救下载实现合规性所需的文件版本。客户端代理可以利用客户端或合规性要求的文件对终端进行补救。

您可以在“文件补救”(File Remediations) 窗口过滤、查看、添加或删除文件补救，但无法编辑文件补救。“文件补救”(File Remediations) 窗口显示所有文件补救及其名称与说明，还有补救所需的文件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **File Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 在**名称** 和**说明** 字段中输入文件补救的名称和说明。

步骤 6 在**新建文件补救 (New File Remediation)** 窗口中修改值。

步骤 7 点击**提交 (Submit)**。

添加链接补救

客户端可以通过链接补救点击URL以访问补救窗口或资源。客户端代理用此链接打开浏览器，并且允许客户端执行进行合规性补救。

“链接补救”(Link Remediation) 窗口显示所有链接补救及其名称与说明和补救模式。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Link Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 在**新建链接补救 (New Link Remediation)** 窗口修改相应值。

步骤 6 点击**提交 (Submit)**。

添加补丁管理补救

您可以创建补丁管理补救，在补救完成后，用最新的合规性文件定义更新客户端。

“补丁管理补救”(Patch Management Remediation) 窗口显示补救类型、补丁管理供应商名称和各种补救选项。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Patch Mangement Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 修改**补丁管理补救 (Patch Management Remediation)** 窗口中的值。

步骤 6 点击**提交 (Submit)**，将补救操作添加到**补丁管理补救 (Patch Management Remediation)** 页面。

相关主题

补丁管理补救

添加防病毒软件补救

您可以创建防病毒软件补救，在补救完成后，用最新的合规性文件定义更新客户端。

“AV 补救”(AV Remediations) 窗口显示所有防病毒软件补救以及补救的名称、说明和模式。

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **AV Remediation**。

步骤 4 点击添加 **(Add)**。

步骤 5 修改新 **AV** 补救 **(New AV Remediation)** 窗口中的值。

步骤 6 点击提交 **(Submit)**。

添加反间谍程序补救

可以创建反间谍程序补救，从而在补救之后使用最新文件定义更新客户端以确保合规。

“AS 补救”(AS Remediations) 窗口显示所有防病毒软件补救以及补救的名称、说明和模式。

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **AS Remediation**。

步骤 4 点击添加 **(Add)**。

步骤 5 修改新 **AS** 补救 **(New AS Remediations)** 窗口中的值。

步骤 6 点击提交 **(Submit)**。

相关主题

反间谍程序补救

添加启动程序补救

您可以创建启动程序补救，其中客户端代理将通过启动一个或多个合规性应用来补救客户端。

Launch Program Remediations 页面显示所有启动程序补救，以及它们的名称和说明及补救模式。

步骤 1 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Launch Program Remediation**。

步骤 4 点击添加 **(Add)**。

步骤 5 在新启动程序补救 **(New Launch Program Remediation)** 页面中修改值。

步骤 6 点击**提交 (Submit)**。

排除启动程序补救故障

问题

当应用作为使用启动计划修复的补救措施启动时，应用成功启动（可在 Windows 任务管理器观察到），但是应用 UI 不可见。

解决方案

启动计划 UI 应用在系统权限运行，并会显示在交互式服务检测 (ISD) 窗口中。要查看启动计划 UI 应用，以下操作系统应启用 ISD：

- Windows Vista：默认情况下 ISD 处于停止状态。通过启动 services.msc 中的 ISD 服务启用 ISD。
- Windows 7：默认情况下启用 ISD 服务。
- Windows 8/8.1：通过在注册表中将 " NoInteractiveServices " 从 1 更改为 0 启用 ISD：\HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Windows。

添加 Windows 更新补救

Windows Update Remediations 页面显示所有 Windows 更新补救及其名称和说明与补救模式。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > > **终端安全评估 (Posture)**。。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Windows Update Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 修改**新建 Windows 更新补救 (New Windows Update Remediation)** 窗口中的值。

步骤 6 点击**提交 (Submit)**。

添加 Windows 服务器更新服务补救

您可以将 Windows 客户端配置为从本地管理或 Microsoft 管理的 WSUS 服务器接收最新的 WSUS 更新，以实现合规性。Windows 服务器更新服务 (WSUS) 补救安装来自本地管理的 WSUS 服务器或 Microsoft 管理的 WSUS 服务器的 Windows 服务包、热补救和补丁。

在客户端代理与本地 WSUS 代理相集成的情况下，您可以创建 WSUS 补救，以检查终端是否安装最新的 WSUS 更新。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Windows Server Update Services Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 修改**新 Windows 服务器更新服务补救 (New Windows Server Update Services Remediation)** 窗口中的值。

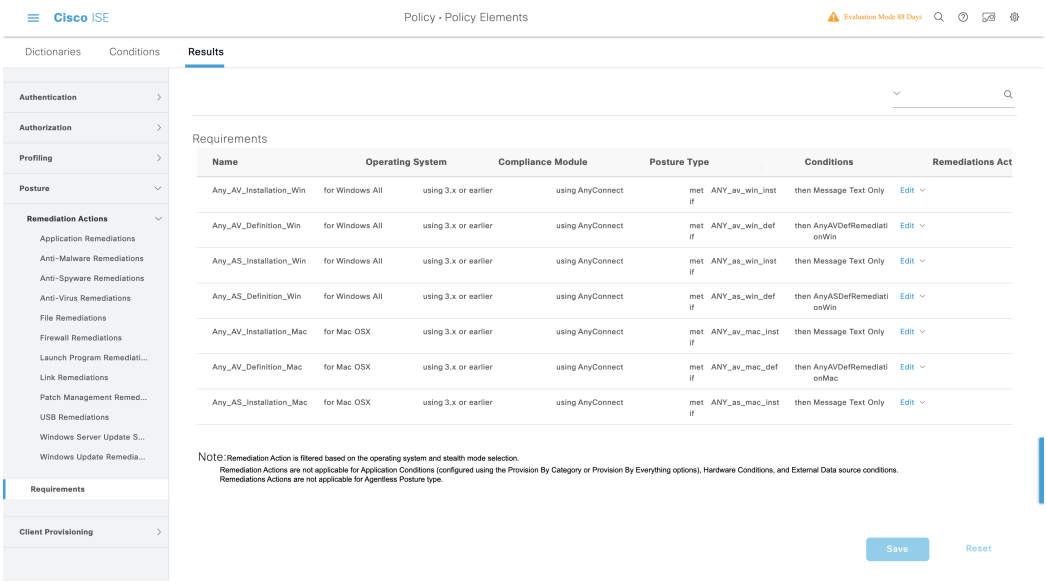
步骤 6 点击**提交 (Submit)**。

终端安全评估要求

终端安全评估要求是一组具有关联补救操作的复合条件，可与角色和操作系统相关联。连接到网络的所有客户端必须在安全评估过程中满足强制性要求才能在网络上达到合规状态。

安全评估策略要求可在安全评估策略中设置为强制性、可选或审核类型。如果要求为可选类型且客户端未能满足这些要求，则客户端可选择继续对终端进行安全评估。

图 *61:* 终端安全评估策略要求类型



强制性要求

在策略评估期间，代理对未能满足终端安全评估策略中定义的强制性要求的客户端提供补救选项。最终用户必须在补救计时器设置中指定的时间内进行补救以满足要求。

例如，您已通过一个用户定义条件指定强制性要求以检查绝对路径中 C:\temp\text.file 的存在。如果该文件不存在，则强制性要求未通过，用户将会被移至非合规状态。

可选要求

在策略评估期间，当无法满足终端安全评估策略中指定的可选要求时，代理会为客户端提供一个选项继续。允许最终用户跳过指定可选要求。

例如，您通过一个用户定义条件指定一个可选要求以检查在客户端机器上运行的应用，例如Calc.exe。虽然客户端未能满足该条件，但代理会提示一个继续后续操作的选项，以便跳过可选要求并将最终用户移至合规状态。

审核要求

审核要求指定用于内部目的，代理不提示任何消息或来自最终用户的四输入，无论策略评估期间状态是失败还是通过。

例如，您在创建一个强制性策略条件以检查最终用户是否拥有防病毒程序的最新版本的过程中。如果要在将其作为策略条件实际实施前找出非合规的最终用户，您可以将其指定为审核要求。

可视性要求

在策略评估期间时，代理每五到十分钟报告一次可视性要求的合规性数据。

客户端系统处于不合规状态

如果客户机无法通过修复符合强制性要求，则安全评估状态会更改为“不合规”，且代理会话会被隔离。若要使客户机通过此“不合规”状态，则需要重启安全评估会话从而使代理再次启动客户机上的安全评估。您可以按以下方法重启安全评估会话：

- 在 802.1X 的有线和无线授权更改 (CoA) 环境下：
  - 当您在新授权策略页面中新建授权配置文件时，您可以配置特定授权策略的重新验证计时器。更多信息请参阅 20-11 页中的“配置可下载 ACL 的权限”一节。
  - 一旦断开并重新连接到网络时，有线用户即可离开隔离状态。在无线环境中，用户必须断开与无线局域网控制器 (WLC) 的连接并等待用户空闲超时过期后才能尝试重新连接到网络。
- 在 VPN 环境中 - 断开并重新连接 VPN 隧道。

创建客户端安全评估要求

可以在“要求”(Requirements) 窗口创建要求，可以通过此窗口将用户定义的条件和Cisco定义的条件与补救操作关联起来。在“要求”(Requirements) 窗口创建并保存用户定义的条件和补救操作后，可以从各自的列表窗口查看这些条件和操作。

开始之前

- 必须了解适用于安全评估的可接受使用政策 (AUP)。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)** > **要求 (Requirements)**。

步骤 2 在**要求 (Requirements)** 窗口中输入值。

步骤 3 点击**完成 (Done)**，在只读模式下保存终端安全评估要求。

步骤 4 点击**保存 (Save)**。

重新进行安全评估配置设置

下表列出“终端安全再评估配置”(Posture Reassessment Configurations) 窗口中的字段，您可以使用此窗口配置终端安全再评估。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **重新评估 (Reassessments)**。

表 *159:* 重新进行安全评估配置设置

字段名称	使用指南
配置名称	输入 PRA 配置的名称。
配置说明	输入 PRA 配置的说明。
Use Reassessment Enforcement?	选中此复选框，将 PRA 配置应用到用户身份组。

字段名称	使用指南
Enforcement Type	选择要执行的操作： • **继续 (Continue)**：用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。 • **注销 (Logoff)**：如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。 • **补救 (Remediate)**：如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送 PRA 报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。 如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的 RADIUS 会话，才能再次布置客户端。 如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续”(Continue) 选项。用户可以继续停留在当前的网络中，不受任何限制。
Interval	输入第一次成功登录后在客户端上启动 PRA 的时间间隔分钟数。 默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。
Grace time	输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于 PRA 间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。 最小值为 5 分钟，最大值为 60 分钟。 **注释** 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。
选择用户身份组	为 PRA 配置选择唯一组或唯一组组合。
PRA configurations	显示现有的 PRA 配置以及关联到 PRA 配置的用户身份组。

相关主题

安全评估租约，第 956 页
定期重新评估，第 957 页
终端安全状态评估选项
安全评估补救选项，第 1002 页
安全评估的自定义条件，第 1002 页
自定义安全评估补救措施，第 1004 页
配置定期重新评估，第 957 页

自定义安全评估权限

自定义权限是一个在Cisco ISE 中定义的标准授权配置文件。标准授权配置文件根据终端的匹配合规性状态设置访问权限。终端安全评估服务将终端安全评估广泛地划分为未知、合规和不合规的配置文件。终端安全评估策略和终端安全评估要求确定终端的合规性状态。

您必须为终端的未知、合规和不合规安全评估状态创建三种不同的授权配置文件，这些终端可以具有不同的 VLAN、DACL 和其他属性值对集合。这些配置文件可与三种不同的授权策略相关联。为了区分这些授权策略，可以使用 Session:PostureStatus 属性以及其他条件。

未知的配置文件

如果没有为终端定义匹配的终端安全评估策略，则终端的终端安全评估合规性状态可能设置为未知。未知的终端安全评估合规性状态也可适用于匹配的终端安全评估策略已启用但其终端安全评估评估尚未进行的终端，因此，客户端代理尚未提供合规性报告。

合规的配置文件

如果已为终端定义匹配的终端安全评估策略，则终端的终端安全评估合规性状态会设置为合规。当进行终端安全评估时，终端会满足匹配的终端安全评估策略中定义的所有强制性要求。对于终端安全评估合规的终端，可以向其授予对网络的网络访问权限。

不合规的配置文件

当为某个终端定义匹配的终端安全评估策略，但该策略在终端安全评估过程中未能满足所有强制性要求时，该终端的终端安全评估合规性状态会设置为不合规。终端安全评估不合规的终端会将终端安全评估要求与补救操作匹配，并且应对该终端授予对补救资源的有限网络访问权限以便自行补救。

配置标准授权策略

您可以在“授权策略”(Authorization Policy) 窗口中定义两种类型的授权策略：标准策略和例外授权策略。特定于安全评估的标准授权策略用于根据终端的合规性状态制定策略决策。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

步骤 2 在**视图 (View)** 列中，点击相应默认策略旁边的箭头图标。

步骤 3 在**操作 (Actions)** 列中，点击齿轮图标，然后从下拉列表中选择新的授权策略。
新行将显示在**策略集 (Policy Sets)** 表中。

步骤 4 输入规则名称。

步骤 5 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 6 在 **Conditions Studio** 页面上创建所需的条件。在**编辑器 (Editor)** 部分中，点击**点击以添加属性 (Click To Add an Attribute)** 文本框，然后选择所需的字典和属性。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 7 点击**使用 (Use)** 以在只读模式下创建新的标准授权策略。

步骤 8 点击**保存 (Save)**。

使用终端安全评估进行网络驱动器映射的最佳实践

在 Windows 终端安全评估期间，终端用户可能会在访问桌面时遇到延迟。这可能是由于 Windows 向用户提供桌面访问权限之前尝试恢复文件服务器的驱动盘号映射。避免在安全评估期间出现延迟的最佳做法是：

- 终端应能够访问 Active Directory 服务器，因为文件服务器驱动盘号无法在不访问 AD 的情况下进行映射。当触发终端安全评估（使用 AnyConnect ISE 终端安全评估代理）时，它会阻止对 AD 的访问，导致登录延迟。在终端安全评估完成之前，使用安全评估补救 ACL 来访问 AD 服务器。
- 您应为登录脚本设置一个延迟，直到终端安全评估完成为止，然后您必须将“持久性”(Persistence) 属性设置为“否”(NO)。Windows 会在登录期间尝试重新连接所有网络驱动器，只有在 AnyConnect ISE 终端安全评估代理获得完全网络访问权限后才能执行此操作。

配置 AnyConnect 隐身模式工作流程

在隐身模式下配置 AnyConnect 的过程涉及一系列步骤。您可以在Cisco ISE 中执行以下步骤。

步骤 1 创建 AnyConnect 代理配置文件，请参阅创建 AnyConnect 代理配置文件。

步骤 2 为 AnyConnect 软件包创建 AnyConnect 配置，请参阅 为 AnyConnect 软件包创建 AnyConnect 配置。

步骤 3 在Cisco ISE 中上传开放式 DNS 配置文件，请参阅 在思科 ISE 中上传开放式 DNS 配置文件。

步骤 4 创建客户端调配策略，请参阅 创建客户端调配策略。

步骤 5 创建终端安全评估条件，请参阅 创建终端安全评估条件。

步骤 6 创建终端安全评估补救，请参阅创建终端安全评估补救。

步骤 7 在无客户端模式下创建终端安全评估要求，请参阅在隐身模式下创建终端安全评估要求。

步骤 8 创建终端安全评估策略，请参阅创建终端安全评估策略。

步骤 9 配置授权配置文件

a)

b) 点击**添加 (Add)** 并输入配置文件的**名称 (Name)**。

c) 在“常见任务”(Common Tasks) 中，启用 **Web 重定向（CWA、MDM、NSP、CPP）(Web Redirection (CWA, MDM, NSP, CPP))** 并从下拉列表中选择**客户端调配（终端安全评估）(Client provisioning (Posture))**，然后输入重定向 **ACL** 名称并选择客户端调配门户**值 (Value)**。您可以在以下位置编辑或创建新的客户端调配门户 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **客户端调配 (Client Provisioning)** > **客户端调配门户 (Client Provisioning Portal)**。

步骤 10 配置授权策略。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**

b) 点击 **>**，然后选择**授权策略 (Authorization Policy)**，然后点击 **+** 图标以创建新的授权规则，该规则采用 **Session:Posture Status EQUALS Unknown** 条件和之前配置的授权文件。

c) 在上一个规则之上，创建新的授权规则，该规则采用 **Session:Posture Status EQUALS NonCompliant** 条件，另一个采用 **Session:Posture Status EQUALS Compliant** 条件。

创建 AnyConnect 代理配置文件

开始之前

必须上传 MAC 和 Windows 操作系统的 AnyConnect Cisco软件包以及 AnyConnect 合规性模块。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 从**添加 (Add)** 下拉列表中，选择 **AnyConnect 终端安全评估配置文件 (AnyConnect Posture Profile)**。

步骤 3 从**安全评估代理配置文件设置 (Posture Agent Profile Settings)** 下拉列表中，选择 **AnyConnect**。

步骤 4 在**名称 (Name)** 字段中，键入所需的名称（例如，AC_Agent_Profile）。

步骤 5 在**代理行为 (Agent Behavior)** 部分，选择**隐藏模式 (Stealth Mode)** 参数为**已启用 (Enabled)** 。

步骤 6 点击**保存 (Save)**。

下一步做什么

应当为 AnyConnect 软件包创建 AnyConnect 配置。

为 AnyConnect 软件包创建 AnyConnect 配置

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 从添加 (Add) 下拉列表中，选择 AnyConnect 配置 (AnyConnect Configuration)。

步骤 3 从选择 AnyConnect 软件包 (Select AnyConnect Package) 下拉列表中，选择所需的 AnyConnect 软件包（例如，AnyConnectDesktopWindows 4.4.117.0）。

步骤 4 在配置名称 (Configuration Name) 文本框中，键入所需的名称（例如，AC_Win_44117）。

步骤 5 在合规性模块 (Compliance Module) 下拉列表中，选择所需的合规性模块（例如，AnyConnectComplianceModuleWindows 4.2.437.0）。

步骤 6 在AnyConnect 模块选择 (AnyConnect Module Selection) 部分，选中ISE 终端安全评估 (ISE Posture) 和网络访问管理器 (Network Access Manager) 复选框。

步骤 7 在配置文件选择 (Profile Selection) 部分，从ISE 终端安全评估 (ISE Posture) 下拉列表中选择 AnyConnect 代理配置文件（例如，AC_Agent_Profile）。

步骤 8 从网络访问管理器 (Network Access Manager) 下拉列表中，选择所需的 AnyConnect 代理配置文件（例如，AC_Agent_Profile）。

下一步做什么

应上传将推送到客户端的开放式 DNS 配置文件。

在思科 ISE 中上传开放式 DNS 配置文件

开放式 DNS 配置文件会被推送到客户端。

步骤 1 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。

步骤 2 从添加 (Add) 下拉列表中，选择来自本地磁盘的代理资源 (Agent Resources From Local Disk)。

步骤 3 从类别 (Category) 下拉列表中选择客户创建的数据包 (Customer Created Packages)。

步骤 4 从类型 (Type) 下拉列表中，选择 AnyConnect 配置文件 (AnyConnect Profile)。

步骤 5 在名称 (Name) 文本框中，键入所需的名称（例如，OpenDNS）。

步骤 6 点击浏览 (Browse) 并从本地磁盘上找到 JSON 文件。

步骤 7 点击提交 (Submit)。

下一步做什么

您应创建客户端调配策略。

创建客户端调配策略

步骤 1 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 策略 (Policy) > 客户端调配 (Client Provisioning)。

步骤 2 创建所需的规则（例如，Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。

下一步做什么

您应创建终端安全评估条件。

创建终端安全评估条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **文件条件 (File Condition)**。

步骤 2 输入所需的名称（例如，filechk）。

步骤 3 从**操作系统 (Operating Systems)** 下拉列表中，选择 Windows 7 (All)。

步骤 4 从**文件类型 (File Type)** 下拉列表中，选择 FileExistence。

步骤 5 从**文件路径 (File Path)** 下拉列表中，选择 ABSOLUTE_PATH C:\test.txt。

步骤 6 从**文件运算符 (File Operator)** 下拉列表中，选择 DoesNotExist。

下一步做什么

您应创建终端安全评估补救。

创建终端安全评估补救

文件条件检查终端上是否存在 test.txt 文件。如果不存在，则补救方法是屏蔽 USB 端口并阻止使用 USB 设备安装该文件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **补救措施 (Remediation Actions)** > **USB 补救 (USB Remediations)**。

步骤 2 输入所需的名称（例如，clientless_mode_block）。

步骤 3 点击**提交 (Submit)**。

下一步做什么

您应创建终端安全评估要求。

在隐身模式下创建终端安全评估要求

在“要求”(Requirements) 页面中创建补救操作时，仅显示适用于隐身模式的补救：防恶意软件、启动程序、补丁管理、USB、Windows 服务器更新服务和 Windows Update。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 创建所需的终端安全评估要求（例如，Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block）。

下一步做什么

您应创建终端安全评估策略。

创建终端安全评估策略

开始之前

确保终端安全评估策略要求和策略是在无客户端模式下创建的。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **终端安全评估 (Posture)**

步骤 2 创建所需的规则。例如，if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=AnyConnect Stealth then Requirements=win7Req。

注释 对于没有 URL 重定向的客户端调配，使用网络访问或 Radius 的特定属性配置条件将不起作用，并且，由于Cisco ISE 服务器中特定用户的会话信息不可用，因此客户端调配策略的匹配可能会失败。但是，Cisco ISE 允许为外部添加的身份组配置条件。

启用 AnyConnect Stealth 模式通知

Cisco ISE 为 AnyConnect 隐身模式部署提供多个新的故障通知。在隐身模式下启用故障通知可帮助您识别有线、无线或 VPN 连接问题。要在隐身模式下启用通知，请执行以下操作：

注释 AnyConnect 版本 4.5.0.3040 及更高版本支持隐身模式通知。

开始之前

在隐身模式下配置 AnyConnect。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择依次选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 依次选择**添加 (Add)** > **AnyConnect ISE 终端安全评估配置文件 (AnyConnect ISE Posture Profile)**。

步骤 3 从**选择一个类别**下拉列表中，选择 **AnyConnect**。

步骤 4 从**代理行为 (Agent Behavior)** 部分，对**在隐身模式下启用通知 (Enable notifications in stealth mode)** 选项选择**已启用 (Enabled)**。

配置思科临时代理工作流程

配置Cisco临时代理的过程涉及一系列步骤。您可以在Cisco ISE 中执行以下步骤。

步骤 1 创建终端安全评估条件

步骤 2 创建终端安全评估要求

步骤 3 创建终端安全评估策略

步骤 4 配置客户端调配策略

步骤 5 配置授权配置文件

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

b) 点击**添加 (Add)** 并输入配置文件的**名称 (Name)**。

c) 在“常见任务”(Common Tasks) 中，启用 **Web 重定向（CWA、MDM、NSP、CPP）(Web Redirection (CWA, MDM, NSP, CPP))** 并从下拉列表中选择**客户端调配（终端安全评估）(Client provisioning (Posture))**，然后输入重定向 **ACL** 名称并选择客户端调配门户**值 (Value)**。您可以在以下位置编辑或创建新的客户端调配门户：**工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **客户端调配 (Client Provisioning)** > **客户端调配门户 (Client Provisioning Portal)**。

步骤 6 配置授权策略。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

b) 点击 >，然后选择**授权策略 (Authorization Policy)**，然后点击 + 图标以创建新的授权规则，该规则采用 **Session:Posture Status EQUALS Unknown** 条件和之前配置的授权文件。

c) 在上一个规则之上，创建新的授权规则，该规则采用 **Session:Posture Status EQUALS NonCompliant** 条件，另一个采用 **Session:Posture Status EQUALS Compliant** 条件。

步骤 7 下载并启动思科临时代理

创建终端安全评估条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **文件条件 (File Condition)**。

步骤 2 输入所需的名称（例如 filecondwin）。

步骤 3 从**操作系统 (Operating Systems)** 下拉列表中，选择 Windows 7 (All)。

步骤 4 从**文件类型 (File Type)** 下拉列表中，选择 FileExistence。

步骤 5 从**文件路径 (File Path)** 下拉列表中，选择 ABSOLUTE_PATH C:\test.txt。

步骤 6 从**文件运算符 (File Operator)** 下拉列表中，选择 DoesNotExist。

创建终端安全评估要求

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)** > **要求 (Requirements)**。

步骤 2 从**编辑 (Edit)** 下拉列表中，选择**插入新要求 (Insert New Requirement)**。

步骤 3 输入**名称**、**操作系统**和**合规性模块**（例如，名称为 filereqwin，操作系统为 Windows All，合规性模块为 4.x 或更高版本）。

步骤 4 在**终端安全评估类型 (Posture Type)** 下拉列表中，选择**临时代理 (Temporal Agent)**。

步骤 5 选择所需条件（例如 filecondwin）。

注释　对于思科临时代理，只能在**要求 (Requirements)** 页面中查看包含**安装 (Installation)** 检查类型的补丁管理条件。

步骤 6 选择**仅消息文本 (Message Text Only)** 补救操作。

注释　AnyConnect 4.x 或更高版本支持临时代理。

创建终端安全评估策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **安全评估 (Posture)**。

步骤 2 创建所需的规则（例如，Name=filepolicywin, Identity Groups=Any, Operating Systems=Windows All, Compliance Module=4.x or later, Posture Type=Temporal Agent, and Requirements=filereqwin）。

配置客户端调配策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 创建所需规则（例如 Rule Name=Win、Identity Groups=Any、Operating Systems=Windows All、Other Conditions=Conditions、Results=CiscoTemporalAgentWindows4.5）。

下载并启动思科临时代理

步骤 1 连接到 SSID。

步骤 2 启动浏览器，您将重定向至客户端调配门户。

步骤 3 点击**开始**。这将检查Cisco临时代理是否已安装并正在运行。

步骤 4 点击**这是我第一次访问 (This Is My First Time Here)**。

步骤 5 选择**点击此处下载并启动思科临时代理 (Click Here to Download and Launch Cisco Temporal Agent)**。

步骤 6 分别保存适用于 Windows 或 Mac OSX 的Cisco临时代理 .exe 或 .dmg 文件。对于 Windows，请运行 .exe 文件；对于 Mac OSX，请双击 .dmg 文件并运行 acisetempagent 应用。
Cisco临时代理会扫描客户端并显示结果，例如不合规检查的红色叉号标记。

安全评估故障排除工具

安全评估故障排除工具可帮助您查找安全状态检查失败的原因，以确定以下事项：

- 在安全评估检查中哪些终端成功，哪些终端失败。
- 如果终端在安全评估检查中失败，则确定安全评估流程中哪些步骤失败。
- 哪些强制检查和可选检查成功，哪些强制检查和可选检查失败。

您可以根据用户名、MAC 地址和安全评估状态等参数过滤请求，确定这些信息。

终端登录配置

此页面用于配置登录凭证，以便Cisco ISE 可以登录客户端。它用于：

- 终端脚本向导
- 无代理终端安全评估

为以下项配置登录凭证：

- **Windows 域用户 (Windows Domain User)**：用于通过 SSH 登录客户端的域凭证。您可以根据需要输入任意数量的 Windows 登录。如果配置了域用户，则会忽略本地用户配置。
- **Windows 本地用户 (Windows Local User)**：Cisco ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。
- **MAC 本地用户 (MAC Local User)**：Cisco ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。

终端脚本设置

此页面配置终端脚本和无代理终端安全评估的选项。

- **将终端脚本执行日志上传到 ISE (Upload endpoint script execution logs to ISE)**：默认情况下已启用，可以将终端脚本上传到Cisco ISE。禁用此选项将禁用终端脚本，无法上传或运行终端脚本。
- **终端脚本执行详细日志记录 (Endpoint script execution verbose logging)**：启用详细日志记录以进行调试。
- **终端处理器批处理大小 (Endpoints processor batch size)**：可以根据网络负载和系统性能进行调整。
- **适用于 MAC 的终端处理并发**
- **适用于 Windows 的终端处理并发**
- **操作系统标识的最大重试次数 (Maximum retry attempts for OS identification)**
- **操作系统标识重试之间的延迟（毫秒）(Delay between retries for OS identification (msec))**
- **终端分页批处理大小**
- **终端上的日志保留期（天）)**
- **连接超时（秒）(Connection Time out (sec))**
- **连接的最大重试次数 (Max-retry attempts for Connection)**
- **Powershell 的端口号 (Port Number for Powershell)**：将它更改为使用非标准端口号。
- **SSH 的端口号 (Port Number for SSH)**：将它更改为使用非标准端口号。

在思科 ISE 中配置客户端调配

启用客户端调配以允许用户下载客户端调配资源并配置代理配置文件。您可以配置 Windows 客户端、Mac OS X 客户端的代理配置文件，并可配置个人设备的本地请求方文件。如果禁用客户端调配，则尝试访问网络的用户会收到警告消息，表明他们无法下载客户端调配资源。

开始之前

如果使用代理并在远程系统上托管客户端调配资源，请验证代理是否允许客户端访问该远程位置。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **客户端调配 (Client Provisioning)** 或 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **设置 (Settings)** > **软件更新 (Software Updates)** > **客户端调配 (Client Provisioning)**。

步骤 2 从**启用调配 (Enable Provisioning)** 下拉列表中，选择**启用 (Enable)** 或**禁用 (Disable)**。

步骤 3 从 **Enable Automatic Download** 下拉列表中选择 **Enable**。

源下载包括所有可用的客户端调配资源。其中一些资源可能与部署无关。Cisco建议尽可能手动下载资源，而不是设置此选项。

步骤 4 **更新源 URL (Update Feed URL)**：在“更新源 URL”(Update Feed URL) 文本框中指定Cisco ISE 从哪一个 URL 搜索系统更新。例如，用于下载客户端调配资源的默认 URL 是 https://www.cisco.com/web/secure/spa/provisioning-update.xml。

步骤 5 **本地请求方调配策略不可用 (Native Supplicant Provisioning Policy Unavailable)**：当没有设备的客户端调配资源时，请在此处决定如何在流程中继续：

- **允许网络访问 (Allow Network Access)**：用户可以在网络上注册其设备，而不必安装和启动本地请求方向导。
- **应用定义的授权策略 (Apply Defined Authorization Policy)**：用户必须尝试通过标准身份验证和授权策略应用访问Cisco ISE 网络（在本地请求方配置过程之外）。如果您启用了此选项，则用户设备会根据应用于用户 ID 的任何客户端调配策略进行标准注册。如果用户的设备需要证书才能访问Cisco ISE 网络，则还必须向用户提供详细说明，介绍如何使用面向用户的可自定义文本字段获取和应用有效证书。

步骤 6 点击**保存 (Save)**。

下一步做什么

配置客户端调配资源策略

客户端调配资源

在终端连接到网络后，客户端调配资源将会下载到终端。客户端调配资源包括适用于台式电脑的合规性和终端安全评估代理，以及适用于手机和平板电脑的本地请求方配置文件。客户端调配策略将这些调配资源分配给终端，以开始网络会话。

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。可以通过点击**添加 (Add)** 按钮将以下资源类型添加到列表中：

- **思科站点中的代理资源 (Agent resources from Cisco Site)**：选择要使其可用于客户端调配策略的 AnyConnect 和请求方调配向导。Cisco会定期更新该资源列表，以便添加新资源和更新现有资源。还可以将 ISE 设置为自动下载所有Cisco资源和资源更新，请参阅在思科 ISE 中配置客户端调配 ， 第 1021 页了解详细信息。

- **本地磁盘中的代理资源 (Agent resources from local disk)**：在 PC 中选择要上传到 ISE 的资源，请参阅从本地计算机添加思科提供的客户端调配资源，第 1024 页。
- **AnyConnect 配置 (AnyConnect Configuration)** - 选择要使其可用于客户端调配的 AnyConnect PC 客户端。有关详细信息，请参阅创建 AnyConnect 配置。
- **本地请求方配置文件 (Native Supplicant Profile)**：为手机和平板电脑配置一个包含网络设置的请求方配置文件。有关详细信息，请参阅创建本地请求方配置文件。
- **AnyConnect ISE 终端安全评估配置文件 (AnyConnect ISE Posture Profile)**：当您不希望创建和分配代理 XML 配置文件时，请在此配置 AnyConnect ISE 终端安全评估。有关 AnyConnect ISE 终端安全评估代理和 ISE 终端安全评估配置文件编辑器的详细信息，请参阅适用于您的 AnyConnect 版本的《AnyConnect 管理员指南》https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html。

在创建客户端调配资源后，请创建客户端调配策略，以便将客户端调配资源应用于终端。请参阅配置客户端调配资源策略，第 1048 页。

相关主题

在思科 ISE 中配置客户端调配，第 1021 页
从思科添加客户端调配资源，第 1023 页
自动下载客户端调配资源
从本地计算机添加思科提供的客户端调配资源，第 1024 页
从本地计算机添加 AnyConnect 的客户创建资源，第 1024 页

从思科添加客户端调配资源

可以从 Cisco.com 添加适用于 AnyConnect（Windows 和 MAC OS x 客户端）以及Cisco Web 代理的客户端调配资源。根据您选择的资源和可用网络带宽，Cisco ISE 会用几分钟时间，将客户端调配资源下载到Cisco ISE。

开始之前

- 确保已在Cisco ISE 中配置正确的代理设置。
- 在Cisco ISE 中启用客户端调配。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**

步骤 2 选择 **添加 (Add)** > **思科站点的代理资源 (Agent resources from Cisco site)**。

步骤 3 从 Download Remote Resource 对话框中的可用列表选择一个或多个所需的客户端调配资源。

步骤 4 点击**保存 (Save)**。

下一步做什么

在成功将客户端调配资源添加到Cisco ISE 之后，您可以开始配置客户端调配资源策略。

从本地计算机添加思科提供的客户端调配资源

您可以从本地磁盘添加之前从Cisco下载的客户端调配资源。

开始之前

请确保仅向Cisco ISE 上传支持的最新资源。较旧且不受支持的资源可能会导致客户端访问出现严重问题。

如果要从 Cisco.com 手动下载资源文件，请参阅思科 ISE 发行说明中的“Cisco ISE 离线更新”部分。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**

步骤 2 选择 **添加 (Add)** > **来自本地磁盘的代理资源 (Agent resources from local disk)**。

步骤 3 从**类别 (Category)** 下拉列表中，选择**思科提供的软件包 (Cisco Provided Packages)**。

步骤 4 点击**浏览 (Browse)** 以浏览要下载到Cisco ISE 的资源文件所在的本地计算机上的目录。

您可以添加之前从Cisco下载到本地计算机的 AnyConnect 或Cisco Web 代理资源。

步骤 5 点击**提交 (Submit)**。

下一步做什么

在成功将客户端调配资源添加到Cisco ISE 之后，即可开始配置客户端调配资源策略。

从本地计算机添加 AnyConnect 的客户创建资源

从本地计算机将 AnyConnect 自定义和本地化包及 AnyConnect 配置文件等客户创建资源添加到Cisco ISE。

开始之前

确保 AnyConnect 的客户创建资源是压缩的文件且在您的本地磁盘中可用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 依次选择**添加 (Add)** > **来自本地磁盘的代理资源 (Agent Resources from local disk)**。

步骤 3 从**类别 (Category)** 下拉列表中，选择**客户创建的包 (Customer Created Packages)**。

步骤 4 输入 AnyConnect 资源的名称和说明。

步骤 5 点击**浏览 (Browse)** 以浏览要下载到Cisco ISE 的资源文件所在的本地计算机上的目录。

步骤 6 选择以下要上传到Cisco ISE 的 AnyConnect 资源：

- AnyConnect 自定义捆绑包
- AnyConnect 本地化捆绑包
- AnyConnect 配置文件
- 高级恶意软件防护 (AMP) 启用程序配置文件

步骤 7 点击**提交 (Submit)**。
Uploaded AnyConnect Resources 表会显示您添加到Cisco ISE 的 AnyConnect 资源。

下一步做什么

创建 AnyConnect 代理配置文件

创建本地请求方配置文件

您可以创建本地请求方配置文件来允许用户将其自己的设备带入Cisco ISE 网络。当用户登录时，Cisco ISE 使用与该用户的权限要求相关的配置文件选择必要的请求方调配向导。向导运行并设置用户的个人设备以访问网络。

注释 调配向导仅配置活动接口。因此，除非两个接口都是活动状态，具有有线和无线连接的用户不会为两个接口进行调配。

开始之前

- 打开 TCP 端口 8905 以支持安装Cisco AnyConnect 代理、Cisco Web 代理和请求方调配向导。有关端口用法的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“Cisco ISE 设备端口参考”附录。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 选择 **添加 (Add)** > **本地请求方配置文件 (Native Supplicant Profile)**。

步骤 3 创建配置文件，按照所述说明 本地请求方配置文件设置，第 1026 页

下一步做什么

按照“对多个访客门户的支持”部分所述，启用自助调配功能，允许员工直接将其个人设备连接到网络。

本地请求方配置文件设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配资源 (Client Provisioning Resources)**，然后添加本地请求方配置文件，您将看到以下设置。

- **名称 (Name)**：您将创建的本地请求方配置文件的名称，并选择此配置文件适用的操作系统。每个配置文件定义 ISE 将应用于客户端本地请求方的网络连接的设置。

无线配置文件

配置一个或多个无线配置文件，用于客户端可用的每个 SSID。

- **SSID 名称 (SSID Name)**：客户端将连接的 SSID 的名称。
- **代理自动配置文件 URL (Proxy Auto-Config File URL)**：如果客户端将连接到代理以获取用于其请求方的网络配置，请输入该代理服务器的 URL。
- **代理 Host/IP**
- **Proxy Port**
- **安全 (Security)**：配置客户端以使用 WPA 或 WPA2。
- **允许协议 (Allowed Procotol)**：配置客户端用于连接到身份验证服务器的协议；PEAP 或 EAP-TLS。
- **证书模板 (Certificate Template)**：对于 TLS，选择定义的一个证书模板 **管理 (Administration)** > **系统证书 (System Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)**。

可选设置如可选设置 - *Windows (Optional Settings - for Windows)* 中所述。

iOS 设置

- **目标网络已隐藏时启用**

有线配置文件

- **允许协议 (Allowed Protocol)**：配置客户端用于连接到身份验证服务器的协议；PEAP 或 EAP-TLS。
- **证书模板 (Certificate Template)**：对于 TLS，选择在“管理”(Administration)、“系统证书”(System Certificates)、“证书颁发机构”(Certificate Authority)、“证书模板”(Certificate Templates) 上定义的一个证书模板。

可选设置 - Windows

如果展开**可选 (Optional)**，以下字段对 Windows 客户端可用。

- **身份验证模式 (Authentication Mode)**：确定是否使用用户和/或计算机作为进行授权的凭证。

- **自动使用登录名和密码（和域，如果有）(Automatically use logon name and password (and domain if any))**：如果选择了用于身份验证模式的用户，若信息可用，请使用登录名和密码，而无需提示用户。
- **启用快速重新连接 (Enable Fast Reconnect)**：当 PEAP 协议选项中的会话恢复功能启用时，允许 PEAP 会话恢复，而不检查用户凭据，该功能在以下位置配置 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **PEAP**。
- **启用隔离检查 (Enable Quarantine Checks)**：检查客户端是否已隔离。
- **服务器不存在加密绑定 TLV 时断开 (Disconnect if server does not present cryptobinding TLV)**：网络连接不支持加密绑定 TLV 时断开。
- **不提示用户授权新服务器或受信任的证书颁发机构 (Do not prompt user to authorize new servers or trusted certification authorities)**：自动接收用户证书；不提示用户。
- **网络不广播其名称 (SSID) 时也连接 (Connect even if the network is not broadcasting its name (SSID))**：仅适用无线配置文件。

无面向不同网络的 URL 重定向的客户端调配

当第三方 NAC 不支持 CoA 时，需要无 URL 重定向的客户端调配。您可以在有无 URL 重定向的情况下执行客户端调配。

注释 对于有 URL 重定向的客户端调配，如果客户端计算机配置了代理设置，请确保将Cisco ISE 添加到浏览器设置中的例外列表。此设置适用于所有使用 URL 重定向的流、BYOD、MDM、访客和终端安全评估。例如，在 Windows 计算机上，执行以下操作：

1. 从控制面板中，点击 **Internet 属性 (Internet Properties)**。
2. 选择**连接 (Connections)** 选项卡。
3. 点击 **LAN 设置 (LAN settings)**。
4. 从代理服务器区域点击**高级 (Advanced)**。
5. 在**例外 (Exceptions)** 框中输入思科 ISE 节点的 IP 地址。
6. 点击**确定 (OK)**。

以下是您在不重定向不同网络的情况下调配终端的步骤。

Dot1X EAP-TLS

1. 将Cisco ISE 网络与已调配证书连接起来。
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户。

AnyConnect 会执行终端安全评估。终端会根据安终端全评估合规性转移至正确的网络。

Dot1X PEAP

1. 通过 NSP 将Cisco ISE 网络与用户名和密码连接起来
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户

   AnyConnect 会执行终端安全评估。终端会根据安终端全评估合规性转移至正确的网络。

MAB (有线网络)

1. 连接Cisco ISE 网络。
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户。

   AnyConnect 会执行终端安全评估。终端会根据安终端全评估合规性转移至正确的网络。

MAB (无线网络)

1. 连接Cisco ISE 网络
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户。

   AnyConnect 会执行终端安全评估。系统仅为无线 802.1X 启动终端安全评估。

AMP 启用程序配置文件设置

下表介绍了“高级恶意软件防护 (AMP) 启用程序配置文件”(Advanced Malware Protection (AMP) Enabler Profile) 窗口中的字段。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

点击**添加 (Add)** 下拉箭头，选择 **AMP 启用程序配置文件 (AMP Enabler Profile)**。

表 ***160: AMP Enabler Profile*** 页面

字段名称	使用指南
名称	输入想要创建的AMP启用程序配置文件的名称。
说明	输入 AMP 启用程序配置文件的说明。

字段名称	使用指南
Install AMP Enabler	• **Windows 安装程序 (Windows Installer)**：指定托管 AMP for Windows OS 软件的本地服务器的 URL。AnyConnect 模块使用此 URL 将 .exe 文件下载到终端。文件大小大约为 25 MB。 • **Mac 安装程序 (Mac Installer)**：指定托管 AMP for Mac OSX 软件的本地服务器的 URL。AnyConnect 模块使用此 URL 将 .pkg 文件下载到终端。文件大小大约为 6 MB。 **Check** 按钮与服务器进行通信，验证 URL 是否有效。如果 URL 有效，则显示“File found”消息，否则显示错误消息。
Uninstall AMP Enabler	从终端卸载终端软件的 AMP。
Add to Start Menu	在终端上安装终端软件的 AMP 后，将终端软件 AMP 的快捷方式添加到终端的 Start 菜单中。
Add to Desktop	在终端上安装终端软件的 AMP 后，将终端软件的 AMP 图标添加到终端桌面上。
Add to Context Menu	在终端上安装终端软件的 AMP 后，将 Scan Now 选项添加到终端右键点击情景菜单中。

使用嵌入式配置文件编辑器创建 AMP 启用程序配置文件

使用 ISE 嵌入式配置文件编辑器或独立编辑器创建 AMP 启用程序配置文件。

要使用 ISE 嵌入式配置文件编辑器创建 AMP 启用程序配置文件，请执行以下操作：

开始之前

- 从 SOURCEfire 门户下载终端软件的 AMP，在本地服务器上托管 AMP。
- 将托管终端软件 AMP 的服务器的证书导入 ISE 证书存储区。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。
- 确保在 **AnyConnect 配置 (AnyConnect Configuration)** 窗口的 **AnyConnect 模块选择 (AnyConnect Module Selection)** 和**配置文件选择 (Profile Selection)** 部分中选中 **AMP 启用程序 (AMP Enabler)** 选项（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client provisioning)** > **资源 (Resources)** > **添加 (Add)** > **AnyConnect 配置 (AnyConnect Configuration)** > **选择 AnyConnect 软件包 (Select AnyConnect Package)**）。

- 必须登录 SOURCEfire 门户，为终端组创建策略，为终端软件下载 AMP。该软件使用您选择的策略进行了预配置。您必须下载两个映像，即，为 Windows OS 的终端软件下载 AMP 的可再分发版本，为 Mac OSX 的终端软件下载 AMP。已下载的软件托管在一台可从企业网络访问的服务器上。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provision)** > **资源 (Resources)**。

步骤 2 点击**添加 (Add)** 下拉列表。

步骤 3 选择**AMP 启用程序配置文件 (AMP Enabler Profile)**，创建新的 AMP 启用程序配置文件。

步骤 4 在字段中输入适当的值。

步骤 5

使用独立编辑器创建 AMP 启用程序配置文件

要使用 AnyConnect 独立编辑器创建 AMP 启用程序配置文件，请执行以下步骤。

开始之前

您可以使用 AnyConnect 4.1 独立编辑器通过上传 XML 格式的配置文件来创建 AMP 启用程序配置文件。

- 从 Cisco.com 下载适用于 Windows 和 Mac OS 的 AnyConnect 独立配置文件编辑器。
- 启动独立配置文件编辑器，并输入 AMP 启用程序配置文件设置 中指定的字段。
- 在您的本地磁盘上将配置文件保存为 XML 文件。
- 确保在 **AnyConnect 配置 (AnyConnect Configuration)** 窗口的 **AnyConnect 模块选择 (AnyConnect Module Selection)** 和**配置文件选择 (Profile Selection)** 部分中选中 **AMP 启用程序 (AMP Enabler)** 选项（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client provisioning)** > **资源 (Resources)** > **添加 (Add)** > **AnyConnect 配置 (AnyConnect Configuration)** > **选择 AnyConnect 软件包 (Select AnyConnect Package)**）。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**

步骤 2 点击**添加 (Add)**。

步骤 3 选择 **Agent resources from local disk**。

步骤 4 从 **Category** 下拉列表中选择 **Customer Created Packages**。

步骤 5 从 **Type** 下拉列表中选择 **AMP Enabler Profile**。

步骤 6 输入 **Name** 和 **说明**。

步骤 7 点击**浏览 (Browse)** 并从本地磁盘选择已保存的配置文件（XML 文件）。以下示例显示一个自定义安装文件。

```
<?xml version="1.0" encoding="UTF-8"?> <FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <FAConfiguration> <Install>
<WindowsConnectorLocation> https://fa_webserver/ACFA_Mac_FireAMPSetup.exe </WindowsConnectorLocation>
<MacConnectorLocation> https://fa_webserver/ACFA_Mac_FireAMPSetup.exe </MacConnectorLocation>
<StartMenu>true</StartMenu> <DesktopIcon>false</DesktopIcon> <ContextIcon>true</ContextIcon> </Install>
 </FAConfiguration> </FAProfile>
```

以下示例显示一个自定义卸载文件。

```
<?xml version="1.0" encoding="UTF-8"?> <FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <FAConfiguration> <Uninstall> </Uninstall>
</FAConfiguration> </FAProfile>
```

步骤 8 点击**提交 (Submit)**。
新创建的 AMP 启用程序配置文件显示在**资源 (Resources)** 页面中。

常见 AMP 启用程序安装错误故障排除

当您在 Windows or MAC Installer 文本框中输入 SOURCEfire URL 并点击 **Check** 时，您可能会遇到下述错误中的一种：

- 错误消息：The certificate for the server containing the Mac/Windows installer file is not trusted by ISE。Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.

  如果您未将 SOURCEfire 受信任证书导入Cisco ISE 证书库，系统会显示此错误消息。获取一个 SOURCEfire 受信任证书并将其导入Cisco ISE 受信任证书库 (Administration > Certificates > Trusted Certificates)。

- 错误消息：The installer file is not found at this location, this may be due to a connection issue. Enter a valid path in the Installer text box or check your connection.

  当承载 AMP 或终端软件的服务器宕机或 Windows Installer or MAC Installer 文本框中有排字错误时，系统会显示此错误消息。

- 错误消息：The Windows/Mac installer text box does not contain a valid URL.

  当您输入语法上不正确的 URL 格式时，系统会显示此错误消息。

思科 ISE 支持登录 Chromebook 设备

不同于其他设备 (Apple、Windows、Android)，Chromebook 设备是受管设备（由 Google 域托管），且只提供有限的登录支持。Cisco ISE 可支持网络上的 Chromebook 设备的登录。登录是指将所需的设置和文件传输至一个终端，由该终端在通过Cisco ISE 身份验证后连接到一个安全网络的过程。该过程包括证书调配和/或本地请求方调配。但在 Chromebook 设备中，您只能执行证书调配。本机请求方调配通过 Google 管理员控制台完成。

非托管 Chromebook 设备无法登录到安全网络中。

Chromebook 登录过程中涉及的实体如下：

- Google 管理员
- ISE 管理员
- Chromebook 用户/设备
- Google 管理控制台（由 Google 管理员管理）

Google 管理员：

- 获得以下许可证：
  1. Google 管理控制台配置所需的 Google Apps 管理员许可证 - URL: https://admin.google.com。管理员可使用 Google 管理控制台管理为某组织中的人员提供的 Google 服务。
  2. Chromebook 设备管理许可证 - URL: https://support.google.com/chrome/a/answer/2717664?hl=en。Chromebook 设备管理许可证可用于配置设置，以及在特定 Chromebook 设备上执行策略。它可以让Google管理员访问设备设置，进而控制用户访问、自定义功能和配置网络访问等。
- 使用 Google 设备许可证实现 Chromebook 设备的调配和注册。
- 通过 Google 管理控制台管理 Chromebook 设备。
- 为每个 Chromebook 用户设置和管理 Wi-Fi 网络配置。
- 通过配置要安装在 Chromebook 设备上的应用和强制扩展程序，实现对 Chromebook 设备的管理。要登录 Chromebook 设备，需在 Chromebook 设备上安装 Cisco Network Setup Assistant 扩展程序。这样 Chromebook 设备可连接到Cisco ISE，并安装 ISE 证书。由于只有受管设备才能执行安装证书操作，因此需强制安装扩展程序。
- 确保 Google 管理控制台上安装了Cisco ISE 证书，以提供服务器验证和安全连接。Google 管理员可以决定是否应为某设备或用户生成证书。Cisco ISE 提供以下选项：
  - 为不共享 Chromebook 设备的单个用户生成证书。
  - 为多名用户共享的 Chromebook 设备生成证书。要查看所需的其他配置，请参阅 在 Google 管理控制台中配置网络与强制扩展 章节中的步骤 5。

  Google 管理员安装 ISE 服务器证书后，ISE 便可以受信任地在 Chromebook 设备上执行证书调配，并支持基于证书的 EAP-TLS 身份验证。Google Chrome 37 及以上版本的支持 Chromebook 设备使用基于证书的身份验证。Google 管理员需在 Google 管理控制台中加载 ISE 调配，并使其适用于 Chromebook 设备，以便从 ISE 获取证书。
- 确保建议的 Google 主机名能够列在为实现 SSL 安全连接而在 WLC 中配置的 ACL 定义列表中。请参阅 Google 支持页面中建议和允许的主机名。

ISE 管理员：

- 定义包括了证书模板结构的 Chromebook 操作系统的本地请求者配置文件。
- 在Cisco ISE 中为 Chromebook 用户创建必要的授权规则和客户端调配策略。

Chromebook 用户：

- 消除 Chromebook 设备，并将其登记至 Google 域，以便确保 Google 管理员定义的实施策略的安全。

- 接收 Chromebook 设备策略以及由 Google 管理控制台安装的 Cisco Network Setup Assistant 扩展程序。
- 连接到调配的 SSID（根据 Google 管理员的定义），打开浏览器，打开自带设备页面，并开始登录流程。
- Cisco Network Setup Assistant 在 Chromebook 设备上安装客户端证书，利用该证书，设备可以执行基于证书的 EAP-TLS 身份验证。

Google 管理控制台:

Google 管理控制台支持 Chromebook 设备管理，同时也支持配置安全网络并推送 Cisco Network Setup Assistant 证书管理扩展程序到 Chromebook。该扩展程序发送 SCEP 请求至Cisco ISE，并安装客户端证书，用于支持安全连接和网络访问。

在共享环境中使用 Chromebook 设备的最佳实践

在共享的环境（如学校和图书馆）中使用 Chromebook 设备时，该 Chromebook 设备在不同的用户之间共享。Cisco建议的一些最佳实践包括：

- 当登录具有特定用户（学生或教授）名称的 Chromebook 设备时，用户名会填充在证书的主题 (Subject) 字段的通用名称 (CN) 中。此外，共享的 Chromebook 列于特定用户下的我的设备 (My Devices) 门户中。因此，建议共享设备在登录时使用共享凭证，以便设备仅在特定用户的我的设备 (My Devices) 门户列表下显示。该共享帐户可由管理员或教授作为单独帐户管理，以控制共享设备。
- Cisco ISE 管理员可以为共享的 Chromebook 设备创建自定义证书模板，并在策略中使用。例如，不使用与主题通用名称 (CN) 值匹配的标准证书模板，而可以在凭证中指定一个名称（例如，chrome-shared-grp1），同一名称也可以分配给 Chromebook 设备。策略可设计为与该名称匹配，以允许或拒绝对 Chromebook 设备的访问。
- Cisco ISE 管理员可以创建一个终端组，其中包含完成 Chromebook 登录所需的所有 Chromebook 设备的 MAC 地址（需要为其限制访问的设备）。授权规则应将其与设备类型 Chromebook 一起调用，这将允许访问重定向到 NSP。

Chromebook 登录过程

Chromebook 登录过程包括一系列步骤：

步骤 1 在 Google 管理控制台中配置网络与强制扩展 。

步骤 2 配置思科 ISE 以支持 Chromebook 登录。

步骤 3 擦除 Chromebook 设备。

步骤 4 注册 Chromebook 到 Google 管理控制台。

步骤 5 将 Chromebook 连接到思科 ISE 网络以实现 BYOD 入网。

在 Google 管理控制台中配置网络与强制扩展

Google 管理员执行以下步骤。

步骤 1 登录到 Google 管理员控制台。

a) 在浏览器输入以下 URL：https://admin.google.com。
b) 输入所需的用户名和密码。
c) 在**欢迎使用管理控制台 (Welcome to Admin Console)** 窗口中，请点击**设备管理 (Device Management)**。
d) 在**设备管理 (Device Management)** 窗口中，请点击**网络 (Network)**。

步骤 2 为受管设备创建 Wi-Fi 网络。

a) 在**网络 (Networks)** 窗口中，点击 **Wi-Fi**。
b) 点击**添加 Wi - Fi (Add Wi - Fi)** 以添加所需的 SSID。有关详细信息，请参阅 Google 管理控制台 - Wi-Fi 网络设置。

对于MAB流，请创建两个SSID，一个用于开放网络，另一个用于证书身份验证。当连接至开放网络时，Cisco ISE ACL 将您重定向至信任的访客门户，进行身份验证。成功进行身份验证后，ACL 会将您重定向到 BYOD 门户。

如果 ISE 证书由中间 CA 颁发，则必须将中间证书映射到“服务器证书颁发机构”，而不是根 CA。

c) 点击**添加 (Add)**。

步骤 3 创建强制扩展程序。

a) 在**设备管理 (Device Management)** 窗口的**设备设置 (Device Settings)** 区域中，点击 **Chrome 管理 (Chrome Management)**。
b) 点击**用户设置 (User Settings)**。
c) 向下滚动，在**应用和扩展程序 (Apps and Extensions)** 部分的**强制安装的应用和扩展程序 (Force-Installed Apps and Extensions)** 选项中，点击**管理强制安装的应用 (Manage Force-Installed Apps)**。

步骤 4 安装强制的扩展程序。

a) 在**强制安装的应用和扩展程序 (Force-Installed Apps and Extensions)** 窗口中，点击 **Chrome Web Store**。
b) 在**搜索 (Search)** 文本框，输入“Cisco网络设置助手”(Cisco Network Setup Assistant) 以定位扩展程序。

Chromebook 设备的强制Cisco网络设置助手扩展程序向Cisco ISE 请求证书，并且在 Chromebook 设备上安装 ISE 证书。因为证书安装仅允许在受管设备上进行，所以扩展程序必须配置为强制安装。如果在注册过程中扩展程序未安装，则无法安装Cisco ISE 证书。

请参阅思科 ISE 国际化和本地化中有关扩展程序支持的语言的详细信息。

c) 点击**添加 (Add)** 以强制安装应用。
d) 点击**保存 (Save)**。

步骤 5 （可选）定义配置文件，以在由多个用户共享的 Chromebook 设备中安装证书。

a) 将以下代码复制并粘贴在记事本文件，然后将其保存到您的本地磁盘。

```
{ "certType": { "Value": "system" } }
```

b) 选择 **设备管理 (Device Management)** > **Chromebook 管理 (Chromebook Management)** > **应用管理 (App Management)**。
c) 点击**思科网络设置助手 (Cisco Network Setup Assistant)** 扩展程序。
d) 点击**用户设置 (User Settings)** 并选择您的域。
e) 点击**上传配置文件 (Upload Configuration File)** 并选择您在本地磁盘保存的 .txt 文件。

注释 要使用Cisco网络设置助手为多个用户共享的设备创建证书，您必须在Google管理控制台中添加记事本文件。否则，Cisco NSA 为单个用户创建证书。

f) 点击**保存 (Save)**。

步骤 6 （可选）为不共享 Chromebook 的单个用户安装证书。

a) 选择 **设备管理 (Device Management)** > **网络 (Network)** > **证书 (Certificates)**。
b) 在**证书 (Certificates)** 窗口中，点击**添加证书 (Add Certificate)** 并上传Cisco ISE 证书文件。

下一步做什么

配置Cisco ISE 以支持 Chromebook 登录。

配置思科 ISE 以支持 Chromebook 登录

开始之前

Cisco ISE 管理员必须创建所需的策略。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)** 窗口。

以下是授权策略的示例：

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess 是一种配置的授权结果。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)** 窗口。

步骤 1 在Cisco ISE 上配置的本地请求方配置文件 (NSP)。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

Chromebook 设备会显示在客户端调配 (Client Provisioning) 页面中，以便进行全新的Cisco ISE 安装。但是，对于升级，您应下载终端安全评估更新。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **更新 (Updates)** 窗口。

b) 点击 **添加 (Add)** > **本地请求方配置文件 (Native Supplicant Profile)**。

c) 输入**名称 (Name)** 和**说明**。
d) 在**操作系统 (Operating System)** 字段，选择**Chrome OS 全部 (Chrome OS All)**。
e) 在**证书模版 (Certificate Template)** 字段，选择所需的证书模板。
f) 点击**提交 (Submit)**。请注意 SSID 是通过 Google 管理控制台而不是本地请求方调配流程进行调配。

步骤 2 映射“客户端调配”(Client Provisioning) 页面的 NSP。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**策略 (Policy)** > **客户端调配 (Client Provisioning)**。
b) 定义结果。

- 在客户端调配策略的**结果 (Results)** 中选择内置本地请求方配置（Cisco ISE Chrome NSP）。
- 或者可以创建一个新规则，并确保选择为 Chromebook 设备创建的**结果 (Result)**。

擦除 Chromebook 设备

Google 管理控制台由 Google 管理员进行配置后，必须擦除 Chromebook 设备。Chromebook 用户必须擦除该设备（这是一个一次性过程）以强制分机和配置网络设置。有关详细信息，您可以参阅以下 URL：https://support.google.com/chrome/a/answer/1360642。

Chromebook 用户执行以下步骤：

步骤 1 按 **Esc-刷新-电源**按键组合。屏幕显示黄色感叹号 (!)。
步骤 2 按 **Ctrl -D** 按键组合启动设备模式，然后按 **Enter** 键。屏幕显示红色感叹号。
步骤 3 按 **Ctrl -D** 按键组合。Chromebook 删除其本地数据，返回初始状态。删除大约需要 15 分钟。
步骤 4 在过渡完成时，按**空格 (Spacebar)** 键，然后按 **Enter** 键返回已验证模式。
步骤 5 在登录前请注册 Chromebook。

下一步做什么

向 Google 管理控制台注册 Chromebook。

注册 Chromebook 到 Google 管理控制台

为调配 Chromebook 设备，Chromebook 用户必须首先在 Google 管理控制台页面注册，并接收设备策略和强制的扩展程序。

步骤 1 请启动 Chromebook 设备并按照屏幕上的说明进行操作，直到您在屏幕上看到登录窗口。现在先不要登录。
步骤 2 在登录到 Chromebook 设备之前，请按 **Ctrl-Alt-E** 组合键。系统将显示**企业注册 (Enterprise Enrolment)** 屏幕。
步骤 3 输入您的电子邮件地址，然后点击**下一步 (Next)**。
您将会收到以下消息：您的设备已成功登记企业管理。

步骤 4 点击 **Done**。

步骤 5 输入您 Google 管理员欢迎函中的用户名和密码，或您的有注册资格的账号上现有 Google 应用用户的用户名和密码。

步骤 6 点击**注册设备 (Enroll Device)**。您将收到一条设备已成功注册的确认消息。

注意：Chromebook 设备注册是一次性的。

将 Chromebook 连接到思科 ISE 网络以实现 BYOD 入网

该程序适用于双 SSID - 要使用 EAP-TLS 协议连接到 802.x 网络，Chromebook 用户需要执行以下步骤：

注释 如果使用双 SSID - 当从 802.x PEAP 连接 EAP-TLS 网络时，应在网络请求方（不是 Web 浏览器）中输入凭证以连接到网络。

步骤 1 在 Chromebook 中，点击**设置 (Settings)**。

步骤 2 在**互联网连接 (Internet Connection)** 部分，点击**调配 Wi-Fi 网络 (Provisioning Wi-Fi Network)**，然后点击您的网络。

步骤 3 此时会打开需要提供凭证的访客门户。

1. 在“登录”(Sign On) 页面，输入**用户名 (Username)** 和**密码 (Password)**。
2. 点击**登录 (Sign On)**。

步骤 4 在 BYOD 欢迎页面，请点击**开始 (Start)**。

步骤 5 在**设备信息 (Device Information)** 字段中，为设备输入名称和说明。例如，“个人设备：Jane 的学校用 Chromebook 或共享设备：图书馆 Chromebook 1 或教室 1 Chromebook 1”。

步骤 6 点击**继续 (Continue)**。

步骤 7 在**思科网络设置助手 (Cisco Network Setup Assistant)** 对话框中，点击**是 (Yes)** 以安装证书访问安全网络。

如果 Google 管理员配置了安全 Wi-Fi，则应该会自动建立网络连接。如果没有，请从可用网络列表中选择安全 SSID。

已在域中登记并且装有Cisco网络设置助手扩展程序的Chromebook用户可以更新该扩展程序，无需等待自动更新。通过执行以下步骤手动更新扩展程序。

1. 在 Chromebook 上，打开浏览器并输入以下 **URL**：**chrome://Extensions**。
2. 选中开发人员模式 (**Developer Mode**) 复选框。
3. 点击**立即更新扩展程序 (Update Extensions Now)**。

4. 检查并验证Cisco网络设置助手扩展程序版本为 2.1.0.35 和更高版本。

Google 管理控制台 - Wi-Fi 网络设置

Wi-Fi 网络配置用于配置客户网络中的 SSID 或使用证书属性与证书匹配（用于 EAP-TLS）。当证书安装于 Chromebook 时，它与 Google 管理设置同步。仅在其中一个已定义的证书属性与 SSID 配置匹配时方可建立连接。

下列为必填字段，专用于 EAP-TLS、PEAP 和开放网络流，由 Google 管理员配置，以在 Google 管理控制台 (Google Admin Console) 页面中为每位 Chromebook 用户建立 Wi-Fi 网络（**设备管理 [Device Management] > 网络 [Network] > Wi-Fi > 添加 Wi-Fi [Add Wi-Fi]**）。

字段	EAP-TLS	PEAP	开放
名称 (Name)	输入网络连接的名称。	输入网络连接的名称。	输入网络连接的名称。
服务集标识符 (SSID)	输入 SSID（例如，tls_ssid）。	输入 SSID（例如，tls_ssid）。	输入 SSID（例如，tls_ssid）。
不广播该 SSID (This SSID Is Not Broadcast)	选择相应选项。	选择相应选项。	选择相应选项。
自动连接 (Automatically Connect)	选择相应选项。	选择相应选项。	选择相应选项。
安全类型 (Security Type)	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	开放
可扩展身份验证协议	EAP-TLS	PEAP	—
内部协议 (Inner Protocol)	—	• Automatic • MSCHAP v2（选择相应选项） • MD5 • PAP • MSCHAP • GTC	—
外部身份 (Outer Identity)	-	-	-

字段	EAP-TLS	PEAP	开放
用户名	在用户登录时设置固定值或使用变量（可选）：${LOGIN_ID} 或 ${LOGIN_EMAIL}。	输入 PEAP 凭证以对 ISE（内部 ISE 用户/AD/其他 ISE 身份）和“密码”(Password) 字段进行身份验证。	—
服务器证书颁发机构 (Server Certificate Authority)	选择 ISE 证书（自“设备管理”[Device Management] > “网络”[Network] > “证书”[Certificates] 导入）。	选择 ISE 证书（自“设备管理”[Device Management] > “网络”[Network] > “证书”[Certificates] 导入）。	—
限制通过平台接入此 Wi-Fi 网络 (Restrict Access to this Wi-Fi Network by Platform)	• 选择移动设备。 • 选择 Chromebook。	• 选择移动设备。 • 选择 Chromebook。	—
客户端注册 URL (Client Enrollment URL)	输入一个 URL，当用户未注册时，Chromebook 设备浏览器为该用户重定向至此 URL。在无线局域网控制器上配置用于为未注册用户重定向的 ACL。	-	-

字段	EAP-TLS	PEAP	开放
颁发者模式 (Issuer Pattern)	证书中的一个属性。至少选择一个来自颁发者模式或主题模式的属性，而且这两个模式需与安装的证书属性匹配。指定要与 Chromebook 设备匹配的证书属性，用于接收证书。 • 通用名称 (Common Name)：指证书的“主题”(Subject) 字段或指证书的“主题”(Subject) 字段中的通配符域，它必须与节点的 FQDN 匹配。 • 位置 (Locality)：指与证书主题相关的测试位置（城市）。 • 组织 (Organization)：指与证书主题相关的组织名称。 • 组织单位 (Organizational Unit)：指与证书主题相关的组织单位名称。	-	-

字段	EAP-TLS	PEAP	开放
主题模式 (Subject Pattern)	证书中的一个属性。至少选择一个来自颁发者模式或主题模式的属性，而且这两个模式需与安装的证书属性匹配。指定要与 Chromebook 设备匹配的证书属性，用于接收证书。 • 通用名称 (Common Name)：指证书的“主题”(Subject) 字段或指证书的“主题”(Subject) 字段中的通配符域，它必须与节点的 FQDN 匹配。 • 位置 (Locality)：指与证书主题相关的测试位置（城市）。 • 组织 (Organization)：指与证书主题相关的组织名称。 • 组织单位 (Organizational Unit)：指与证书主题相关的组织单位名称。	-	-

字段	EAP-TLS	PEAP	开放
代理设置	• 直接互联网接入 (Direct Internet Connection)（已选） • 手动代理配置 (Manual Proxy Configuration) • 自动代理配置 (Automatic Proxy Configuration)	• 直接互联网接入 (Direct Internet Connection)（已选） • 手动代理配置 (Manual Proxy Configuration) • 自动代理配置 (Automatic Proxy Configuration)	—
应用网络 (Apply Network)	按用户 (By User)	按用户 (By User)	-

监控思科 ISE 中的 Chromebook 设备活动

Cisco ISE 提供多种报告和日志以查看 Chromebook 设备身份验证和授权的相关信息。您可以按需或定期运行这些报告。可以查看身份验证方法（例如 802.1x）和身份验证协议（例如 EAP-TLS）。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live Logs)** 窗口。还可以确定归类为 Chromebook 设备的终端数量。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)** 窗口

排除 Chromebook 设备登录故障

本节介绍在登录 Chromebook 设备时您可能会遇到的问题。

- 错误：无法从应用商店安装扩展名 - 您无法安装从 Webstore 安装扩展名。将由网络管理员自动安装在您的 Chromebook 设备上。
- 错误：证书安装完成，但是无法连接到安全网络 - 在管理控制台上验证已安装证书与定义的颁发者/主题属性模式匹配。您可以从此处获取有关安装证书的信息：chrome://settings/certificates
- 错误：当尝试手动连接到 Chromebook 的安全网络时，显示错误消息“获取网络证书”- 点击“获取新证书”(Get New Certificate)，浏览器打开并将您重定向到 ISE 自带设备流程安装证书。但是，如果您无法连接到安全网络，请在管理控制台上验证已安装证书与定义的颁发者/主题属性模式匹配。
- 错误：点击“获取新证书”(Get New Certificate)，但会转至 www.cisco.com 网站 - 为了被重定向到 ISE 并开始证书安装过程，用户需要连接到调配 SSID。请确保已为此网络定义正确的访问列表。
- 错误：显示错误消息“仅受管设备可使用此扩展名。请联系服务中心或网络管理员”-Chromebook 是一个受管设备，扩展名必须配置为强制安装以获得 Chrome 操作系统 API 访问权限在设备上

安装证书。虽然扩展名可通过从 Google Webstore 下载手动安装，但是未注册的 Chromebook 用户无法安装该证书。

如果用户属于域用户组，未注册 Chromebook 设备可以获得证书。扩展名跟踪所有设备的域用户。但是域用户可以为未注册设备的生成基于用户的身份验证密钥。

- 错误：Google 管理控制台中 SSID 连接的顺序不明 -
  - 如果 Google 管理控制台配置了多个 SSID （PEAP 和 EAP-TLS）在，在安装证书且匹配属性后，Chrome 操作系统会通过基于证书的身份验证自动连接到 SSID，无论 SSID 以什么顺序配置。
  - 如果两个 EAP-TLS SSID 匹配相同的属性，则连接取决于无法通过用户或管理员控制的其他因素（例如信号强度和其他网络级别信号）。
  - 如果 Chromebook 设备上安装多个 EAP-TLS 证书，并且它们全部与管理控制台上已配置的证书模式匹配，则最新的证书将用于连接。

思科 AnyConnect 安全移动

Cisco ISE 使用Cisco AnyConnect 中的集成模块来满足Cisco ISE 终端安全评估要求。

注释 Cisco AnyConnect 不支持 CWA 流 。无法通过访客门户使用**工作中心 (Work Centers)**>**访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **访客设备合规性设置 (Guest Device Compliance Settings)** 窗口中的**要求访客设备合规 (Require guest device compliance)** 字段来调配 Cisco AnyConnect。相反，应在客户端调配门户上调配Cisco AnyConnect。该方法会导致按照授权权限中的配置进行重定向。

注释 在切换网络介质时，必须更改默认网关，以便思科 AnyConnect ISE 终端安全评估模块能够检测网络更改并重新评估客户端。

当将Cisco ISE 与Cisco AnyConnect 代理集成时，Cisco ISE 会：

- 充当暂存服务器以部署Cisco AnyConnect 4.0 版本及其未来版本
- 与 AnyConnect 终端安全评估组件进行交互以满足Cisco ISE 终端安全评估要求
- 支持部署Cisco AnyConnect 配置文件、自定义及语言包，以及 Windows 和 Mac OS x 操作系统的 OPSWAT 库更新
- 同时支持Cisco AnyConnect 和传统代理

创建 AnyConnect 配置

AnyConnect 配置包括 AnyConnect 软件及其相关的配置文件。可在允许用户下载 AnyConnect 资源并将其安装到客户端上的客户端调配策略中使用此配置。如果您使用 ISE 和 ASA 部署 AnyConnect，则头端的配置必须相匹配。

要在连接到 VPN 时推送 ISE 终端安全评估模块，Cisco建议您通过使用Cisco自适应安全设备管理器 (ASDM) GUI 工具的Cisco自适应安全设备 (ASA) 安装 AnyConnect 代理。ASA 使用 VPN 下载程序执行安装。在下载后，将通过 ASA 推送 ISE 终端安全评估配置文件，并在 ISE 终端安全评估模块联系 ISE 之前提供随后调配该配置文件所需的发现主机。而对于 ISE，ISE 终端安全评估模块只会在发现 ISE 后获取该配置文件，这有可能导致错误。因此，在连接到 VPN 时，建议使用 ASA 推送 ISE 终端安全评估模块。

注释 当Cisco ISE 与 ASA 集成时，请确保在 ASA 中将记帐模式设置为**单一 (Single)**。记帐数据在“单一”(Single) 模式下仅发送到一个记帐服务器。

开始之前

在配置 AnyConnect 配置对象之前，必须：

1. 从思科软件下载页面下载 AnyConnect 前端部署数据包和合规性模块。
2. 将这些资源上传到Cisco ISE（请参阅从本地计算机添加思科提供的客户端调配资源，第 1024 页）。
3. （可选）添加自定义和本地化捆绑包（请参阅从本地计算机添加 AnyConnect 的客户创建资源，第 1024 页）。
4. 配置AnyConnect终端安全评估代理配置文件（请参阅创建终端安全评估代理配置文件，第 1045 页）。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provision)** > **资源 (Resources)**。

步骤 2 点击**添加 (Add)** 创建 AnyConnect 配置。

步骤 3 选择 **AnyConnect Configuration**。

步骤 4 选择您之前上传的 AnyConnect 软件包。例如，AnyConnectDesktopWindows xxx.x.xxxxx.x。

步骤 5 输入当前 AnyConnect 配置的名称。例如，AC Config xxx.x.xxxxx.x。

步骤 6 选择您之前上传的合规性模块。例如，AnyConnectComplianceModulewindows x.x.xxxx.x

步骤 7 选中一个或多个 AnyConnect 模块复选框。例如，从下列软件中选择一个或多个模块：ISE Posture、VPN、网络访问管理器、网络安全、AMP 启用程序、ASA Posture、Start Before Log on（仅适用于 Windows OS）以及诊断和报告工具。

注释　取消选中 AnyConnect Module Selection 下的 VPN 模块，不会在调配的客户端禁用 VPN 磁贴。您必须配置 VPNDisable_ServiceProfile.xml，才能在 AnyConnect GUI 上禁用 VPN 磁贴。在将 AnyConnect 安装到默认位置的系统中，可以在 C:\Program Files\Cisco 下找到此文件。如果 AnyConnect 安装到不同位置，则此文件将位于 <AnyConnect Installed path>\Cisco 下。

步骤 8　为选定的 AnyConnect 模块选择 AnyConnect 配置文件。例如，ISE Posture、VPN、NAM 和网络安全模块。

步骤 9　选择 AnyConnect 自定义和本地化捆绑包。

步骤 10　点击**提交 (Submit)**。

创建终端安全评估代理配置文件

按照此程序创建 AnyConnect 终端安全评估代理配置文件，您可以在其中指定参数以定义终端安全评估协议的代理行为。

步骤 1　在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2　点击**添加 (Add)**。

步骤 3　选择 **AnyConnect 终端安全评估配置文件 (AnyConnect Posture Profile)**。

步骤 4　输入配置文件的**名称**。

步骤 5　配置以下各项的参数：

- Cisco ISE 终端安全评估代理行为
- 客户端 IP 地址更改
- Cisco ISE 安全评估协议

步骤 6　点击**提交 (Submit)**。

客户端 IP 地址刷新配置

下表描述“NAC AnyConnect 终端安全评估配置文件”(NAC AnyConnect Posture Profile) 窗口中的字段，您可以通过此窗口为客户端配置在 VLAN 更改之后要更新或刷新其 IP 地址的参数。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Resilts)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)** > **添加 (Add)** > **NAC 或 AnyConnect 终端安全评估配置文件 (NAC or AnyConnect Posture Profile)**。

字段名称	默认值	使用指南
“VLAN 检测时间间隔”(VLAN detection interval)	0, 5	此设置是代理检查 VLAN 更改的时间间隔。 对于 Mac OS X 代理，默认值为 5。默认情况下，已启用访问身份验证 VLAN 更改功能，对于 Mac OS X，VlanDetectInteval 为 5 秒。有效范围为 5 至 900 秒。 0 - 禁用访问身份验证 VLAN 更改功能。 1 至 5 - 代理每隔 5 秒发送一个互联网控制消息协议 (ICMP) 或地址解析协议 (ARP) 查询。 6 至 900 - 每隔 x 秒发送一个 ICMP 或 ARP 查询。
Enable VLAN detection without UI（不适用于 Mac OS X 客户端）	否	即使用户未登录，此设置仍可启用或禁用 VLAN 检测。 “否” - 禁用 VLAN 检测功能。 “是” - 启用 VLAN 检测功能。
“重试检测计数”(Retry detection count)	3	如果互联网控制消息协议(ICMP)或地址解析协议 (ARP) 轮询失败，此设置将代理配置为重试 x 次再刷新客户端 IP 地址。
“Ping 命令或 ARP”(Ping 命令或 ARP)	0 有效范围为 0 至 2。	此设置指定用于检测客户端 IP 地址更改的方法。 0 - 使用 ICMP 轮询 1 - 使用 ARP 轮询 2 - 首先使用 ICMP 轮询，然后（如果 ICMP 失败）使用 ARP 轮询
“ping 命令最长超时时间”(Maximum timeout for ping)	1 有效范围为 1 至 10 秒。	使用 ICMP 轮询，并且如果在指定时间内没有响应，则宣布 ICMP 轮询失败。
“启用代理 IP 地址刷新”(Enable agent IP refresh)	“是”（默认值）	指定在交换机（或 WLC）更改相应交换机端口上客户端登录会话的 VLAN 之后客户端设备是否更新或刷新其 IP 地址。

字段名称	默认值	使用指南
“DHCP 更新延迟”(DHCP renew delay)	0 有效范围为 0 至 60 秒。	此设置指定客户端设备在尝试向网络 DHCP 服务器请求新 IP 地址之前等待的时间。
“DHCP 释放延迟”(DHCP release delay)	0 有效范围为 0 至 60 秒。	此设置指定客户端设备在释放当前 IP 地址之前等待的秒数。

注释 将参数值与现有代理配置文件设置合并或覆盖这些设置，从而相应地配置 Windows 客户端和 Mac OS X 客户端以刷新 IP 地址。

安全评估协议设置

下表介绍“AnyConnect 终端安全评估配置文件”(AnyConnect Posture Profile) 页面上的字段，您可以在Cisco ISE 中通过此页面配置终端安全评估协议设置。有关 Anyconnect 终端安全评估协议设置中其他字段的信息，请参阅 AnyConnect 版本对应的《思科 AnyConnect 安全移动客户端管理员指南》。

字段名称	默认值	使用指南
Call Home 列表	—	输入逗号分隔的 IP 地址和端口列表，在 IP 地址和端口之间输入冒号。
回退计时器	30 秒	使用此设置，Anyconnect 代理能够通过发送发现数据包持续到达发现目标（重定向目标和之前连接的 PSN），直到达到此最大时间限制为止。有效范围为 10 到 600 秒。

连续的终端属性监控

可以使用Cisco AnyConnect 代理连续监控不同终端属性，以确保在安全评估期间观察动态变化。这会提高终端的整体可视性，并帮助您根据其行为创建安全评估策略。Cisco AnyConnect 代理监控安装并运行在终端上的应用。您可以打开和关闭此功能，并配置应监控数据的频率。默认情况下，每 5 分钟收集一次数据，并存储在数据库中。在初始安全评估过程中，Cisco AnyConnect 报告正在运行和已安装的应用的完整列表。在初始安全评估后，Cisco AnyConnect 代理每 X 分钟扫描一次应用，并将其与最后一次扫描的差异发送到服务器。服务器显示正在运行和已安装的应用的完整列表。

思科 Web 代理

Cisco Web 代理为客户端设备提供临时安全评估。

用户可以启动Cisco Web 代理可执行文件，此文件会通过 ActiveX 控件或 Java 小应用程序在客户端设备上的临时目录中安装 Web 代理文件。

用户登录Cisco Web 代理后，Web 代理会从Cisco ISE 服务器获取为用户角色和操作系统配置的要求，检查主机注册表、进程、应用和服务以获取所需的数据包，并向Cisco ISE 服务器发回报告。如果客户端设备满足这些要求，用户就可以访问网络。如果不满足这些要求，Web 代理会向用户显示对话框，指出没有满足的各项要求。此对话框会为用户提供让客户端设备满足要求的说明和应执行的操作。或者，如未满足指定的要求，用户可以选择接受有限网络访问，同时尝试对客户端系统进行补救以满足对用户登录角色的要求。

注释 仅 32 位版本的 Internet Explorer 支持 ActiveX。无法安装在 Firefox Web 浏览器或 64 位版本的 Internet Explorer 上安装 ActiveX。

思科 Web 代理

Cisco Web 代理为客户端设备提供临时安全评估。

用户可以启动Cisco Web 代理可执行文件，此文件会通过 ActiveX 控件或 Java 小应用程序在客户端设备上的临时目录中安装 Web 代理文件。

用户登录Cisco Web 代理后，Web 代理会从Cisco ISE 服务器获取为用户角色和操作系统配置的要求，检查主机注册表、进程、应用和服务以获取所需的数据包，并向Cisco ISE 服务器发回报告。如果客户端设备满足这些要求，用户就可以访问网络。如果不满足这些要求，Web 代理会向用户显示对话框，指出没有满足的各项要求。此对话框会为用户提供让客户端设备满足要求的说明和应执行的操作。或者，如未满足指定的要求，用户可以选择接受有限网络访问，同时尝试对客户端系统进行补救以满足对用户登录角色的要求。

注释 仅 32 位版本的 Internet Explorer 支持 ActiveX。无法安装在 Firefox Web 浏览器或 64 位版本的 Internet Explorer 上安装 ActiveX。

配置客户端调配资源策略

对于客户端，客户端调配资源策略确定在登录和用户会话启动时哪些用户会从Cisco ISE 收到哪个（或哪些）版本的资源（代理、代理合规性模块和/或代理自定义包/配置文件）。

对于 AnyConnect，可以从客户端调配资源页面选择资源，创建可在客户端调配策略页面中使用的 AnyConnect 配置。AnyConnect 配置是 AnyConnect 软件及其与不同配置文件的关联，其中包括

Windows 和 Mac OS X 客户端的 AnyConnect 二进制包、合规性模块、模块配置文件以及 AnyConnect 的自定义包和语言包。

开始之前

- 请确保您已将资源添加到Cisco ISE，然后才能创建有效的客户端调配资源策略。当您下载代理合规性模块时，它始终会覆盖系统中可用的现有模块（如果有）。
- 检查客户端配置中使用的原生 Supplicant 客户端配置文件，并确保无线 SSID 是正确的。对于 iOS 设备，如果您尝试连接到的网络已隐藏，请从 iOS 设置 (iOS Settings) 区域中选中**目标网络已隐藏时启用 (Enable if target network is hidden)** 复选框。
- 有关基于证书属性包含条件的客户端调配规则，请参阅基于证书的条件的先决条件部分。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 从行为下拉列表中依次选择 **Enable**、**Disable** 或 **Monitor**：

- **Enable** - 确保Cisco ISE 使用此策略，以在用户登录到网络时帮助实现客户端调配功能，并帮助遵守客户端调配策略规定。
- **Disable** - Cisco ISE 不使用指定的资源策略来实现客户端调配功能。
- **Monitor** - 禁用策略并“观察”客户端调配会话请求，以查看Cisco ISE 尝试根据“受监控”策略进行调用的次数。

步骤 3 在 Rule Name 文本框中输入新资源策略的名称。

步骤 4 指定登录到Cisco ISE 的用户可能所属的一个或多个身份组。

您可以选择指定 Any 身份组类型，或者从已配置的现有身份组列表中选择一个或多个组。

步骤 5 使用 Operating Systems 字段指定可能在用户登录到Cisco ISE 所通过的客户端计算机或设备上运行的一个或多个操作系统。

您可以选择指定单个操作系统，例如“Android”、“Mac iOS”和“Mac OS X”，或者指定用于处理多个客户端计算机操作系统的伞操作系统，例如“Windows XP (All)”或“Windows 7 (All)”。

注释 虽然在思科 ISE GUI 的客户端调配策略页面中提供了选择 MAC OS 10.6/10.7/10.8 的选项，但 AnyConnect 不支持这些版本。

步骤 6 在 Other Conditions 字段中，指定要为此特定资源策略创建的新表达式。

步骤 7 对于客户端计算机，使用 **Agent Configuration** 指定将在客户端计算机上供使用和进行调配的代理类型、合规性模块、代理自定义包和/或配置文件。

必须在授权策略中包含客户端调配 URL，以使代理能够在客户端计算机中弹出。这会阻止来自任何随机客户端的请求，并且确保只有具有正确重定向 URL 的客户端可以请求安全状态评估。

步骤 8 点击 **保存 (Save)**。

下一步做什么

您已成功配置一个或多个客户端调配资源策略后，即可开始配置Cisco ISE，以在登录过程中在客户端计算机上执行安全评估。

在客户端调配策略中配置思科 ISE 安全评估代理

对于客户端计算机，请配置代理类型、合规性模块、代理自定义包和/或配置文件，使之可供使用和调配，以便用户下载和安装到客户端计算机。

开始之前

您必须在Cisco ISE 中为 AnyConnect 客户端添加调配资源。

步骤 1 从 **Agent** 下拉列表中选择可用代理，并根据需要启用或禁用 **Is Upgrade Mandatory** 选项来指定此处定义的代理升级（下载）对于客户端设备而言是否为强制性的。

Is Upgrade Mandatory 设置仅适用于代理下载。代理配置文件、合规性模块和代理自定义包更新始终为强制性的。

步骤 2 从 **Profile** 下拉列表中选择现有的代理配置文件。

步骤 3 使用 **Compliance Module** 下拉列表选择要下载到客户端设备的可用合规性模块。

步骤 4 从 **Agent Customization Package** 下拉列表中选择用于客户端设备的可用代理自定义包。

为个人设备配置本地请求方

员工可以直接使用本地请求方将个人设备连接至网络，本地请求方可用于 Windows、Mac OS、iOS 和 Android 设备。对于个人设备，请指定在所注册的个人设备上提供和调配哪个本地请求方配置。

开始之前

创建本地请求方配置文件，使Cisco ISE 在用户登录时根据您为用户授权要求关联的配置文件提供必要的请求方调配向导，以将用户个人设备设置为接入网络。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 从行为下拉列表中依次选择 **Enable**、**Disable** 或 **Monitor** ：

步骤 3 在 Rule Name 文本框中输入新资源策略的名称。

步骤 4 指定以下项：

- 使用 Identity Groups 字段指定登录Cisco ISE 的用户可能隶属的一个或多个身份组。
- 使用 操作系统 (Operating System) 字段指定用户个人设备上可能运行的、用户借以登录Cisco ISE 的一个或多个操作系统。
- 使用 Other Conditions 字段指定想要为此特定资源策略创建的新表达式。

步骤 5 对于个人设备，请使用 **Native Supplicant Configuration** 以选择向这些个人设备分发的具体 **Configuration Wizard**。

步骤 6 为特定个人设备类型指定适用的 **Wizard Profile**。

步骤 7 点击**保存 (Save)**。

客户端调配报告

可以访问Cisco ISE 监控和故障排除功能，以检查成功或失败的用户登录会话的整体趋势，收集有关在指定时间段登录网络的客户端计算机的数量和类型的统计信息，或检查客户端调配资源中的所有最新配置更改。

客户端调配请求

操作 (Operations) > **报告 (Reports)** > **ISE 报告 (ISE Reports)** > **终端和用户 (Endpoints and Users)** > **客户端调配 (Client Provisioning)** 报告显示有关成功和失败的客户端调配请求的统计信息。当选择**运行 (Run)** 并指定其中一个预设时间段时，Cisco ISE 会梳理数据库并显示产生的客户端调配数据。

请求方调配请求

在传出数据包通过以太网微处理器退出前，此 **操作 (Operations)** > **报告 (Reports)** > **ISE 报告 (ISE Reports)** > **终端和用户 (Endpoints and Users)** > **请求方调配 (Supplicant Provisioning)** 窗口显示有关最近成功和失败的用户设备注册和请求方调配请求的信息。当选择**运行 (Run)** 并指定其中一个预设时间段时，Cisco ISE 会梳理数据库并显示产生的请求方调配数据。

Supplicant Provisioning 报告提供有关特定时间段内通过设备注册门户注册的终端列表的信息，包括登录日期和时间、身份（用户 ID）、IP 地址、MAC 地址（终端 ID）、服务器、配置文件、终端操作系统、SPW 版本、故障原因（如有）和注册状态等数据。

客户端调配事件日志

您可以搜索事件日志条目，帮助诊断客户端登录行为可能存在的问题。例如，您网络上的客户端设备在登录后无法获取客户端调配资源更新，您可能需要确定问题的原因。您可以将日志条目用于安全评估和客户端调配审核以及安全评估和客户端调配诊断。

客户端调配门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)**。

门户设置

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果您已使用此范围外的端口值进行升级，则在

对此页面进行任何更改之前会遵循这些设置。如果您对此页面进行任何更改，则必须更新端口设置以遵守此限制。

- **允许接口 (Allowed interfaces)**：选择可以运行门户的 PSN 接口。仅配备了允许接口的 PSN 可以创建门户。您可以配置物理接口和绑定接口的任意组合。这是整个 PSN 的配置；所有门户只能在这些接口上运行，这些接口配置被推送到所有节点。
  - 您必须使用不同子网上的 IP 地址配置以太网接口。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书主题名称/备用主题名称必须解析到接口 IP。
  - 在 ISE CLI 中配置 ip host x.x.x、x yyy.domain.com 以将辅助接口 IP 映射到 FQDN，FQDN 将用于匹配证书主题名称/备用主题名称。
  - 如果仅选定绑定 NIC - 当 PSN 尝试配置其首次尝试配置该绑定接口的门户时。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。它不会尝试在物理接口上启动门户。
  - **NIC 结合 (NIC Teaming)** 或绑定是一个 O/S 配置选项，通过该选项可以配置两个独立的 NIC 以实现高可用性（容错能力）。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据门户设置配置为门户选定一个 NIC：
    - 如果物理 NIC 和相应的绑定 NIC 均已配置 - 当 PSN 尝试配置门户时会首先尝试连接到绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。
- **证书组标签 (Certificate Group Tag)**：选择要用于门户 HTTPS 流量的证书组的组标签。
- **身份验证方法 (Authentication Method)**：选择用于用户身份验证的身份源序列 (ISS) 或身份提供程序 (IdP)。ISS 是按顺序搜索验证用户凭证的身份库的列表。一些示例包括：内部访客用户、内部用户、Active Directory 和 LDAP 目录。

  Cisco ISE 包含客户端调配门户的默认客户端调配身份源序列，Sponsor_Portal_Sequence。
- **完全限定域名 (Fully Qualified Domain Name [FQDN])**：为客户端调配门户输入至少一个唯一 FQDN 和/或主机名。例如，您可以输入 provisionportal.yourcompany.com，以便在用户将其中任一名称输入到浏览器中时，可以访问客户端调配门户。
  - 更新 DNS，以确保新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在Cisco ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。

注释 对于没有 URL 重定向的客户端调配，必须在 DNS 配置中配置完全限定域名 (FQDN) 字段中输入的门户名称。此 URL 必须传达给用户，以在没有 URL 重定向的情况下启用客户端调配。

- **空闲超时 (Idle Timeout)**：输入Cisco ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。

注释 在客户端调配门户中，可以定义端口号和证书，以便主机允许您为客户端调配和终端安全评估下载相同的证书。如果门户证书由官方证书颁发机构签名，您将不会收到任何安全警告。如果证书是自签证书，您将收到门户和Cisco AnyConnect 终端安全评估组件二者的同一安全警告。

登录页面设置

- 启用登录 (Enable Login)：选择此复选框可在客户端调配门户中启用登录步骤
- 速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)：指定在 Cisco ISE 开始人为减缓可进行登录尝试的速率（从而防止更多登录尝试）之前，单个浏览器会话的失败登录尝试次数。在 **Time between login attempts when rate limiting** 中指定了达到此失败登录次数后，前后两次尝试之间的间隔时间。
- 限制速率时登录尝试之间的间隔时间 (Time between login attempts when rate limiting)：设置用户在达到**速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)** 中定义的登录失败次数后，尝试再次登录之前必须等待的时间长度（以分钟为单位）。
- 包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])：显示公司的网络使用条款和条件，可以是当前为用户显示的页面上的文本，或是一个链接，能够打开包含 AUP 文本的新选项卡或窗口。
- 要求接受 (Require acceptance)：要求用户必须接受 AUP，然后才能访问门户。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，便无法访问该门户。
- 要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)：此选项仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 时显示。确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。

可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)

- 包含一个 AUP (Include an AUP)：在单独的页面上向用户显示公司的网络使用条款和条件。
- 要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)：确保用户已完全阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活“接受”(Accept) 按钮。
- 仅在首次登录时 (On first login only)：仅在用户首次登录到网络或门户时显示 AUP。
- 在每次登录时 (On every login)：每次用户登录到网络或门户时都显示 AUP。

- 每 __ 天（从首次登录算起）(Every __ days [starting at first login])：在用户首次登录到网络或门户后定期显示 AUP。

登录后横幅页面设置

包含登录后横幅页面 (Include a Post-Login Banner page)：在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

更改密码设置 (Change Password Settings)

允许内部用户更改其密码 (Allow internal users to change their own passwords)：允许内部用户在登录到客户端调配门户后更改其密码。这仅适用于帐户存储于Cisco ISE 数据库中的员工，不适用于帐户存储于外部数据库（例如 Active Directory 或 LDAP）的员工。

相关主题

客户端调配门户，第 696 页
创建客户端调配门户，第 709 页
客户端调配门户语言文件的 HTML 支持，第 429 页

客户端调配门户语言文件的 HTML 支持

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在您的内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message

- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

第 13 章

威胁控制

以威胁防护为中心的 NAC 服务

凭借以威胁防护为中心的网络访问控制 (TC-NAC) 功能，您可依据接收自威胁和漏洞适配器的威胁和漏洞属性创建授权策略。威胁严重级别和漏洞评估结果可用于动态控制终端或用户的访问级别。

您可以配置漏洞和威胁适配器来向Cisco ISE 发送高保真危害表现 (IoC)、检测到威胁事件和 CVSS 分数，以便创建以威胁防护为中心的访问策略来相应地更改终端的授权和情景。

Cisco ISE 支持以下适配器：

- Sourcefire FireAMP
- 感知威胁分析 (CTA) 适配器
- Qualys

注释 TC-NAC 流目前仅支持 Qualys 企业版。

- Rapid7 Nexpose
- Tenable 安全中心

当检测到终端威胁事件时，可以在**受到危害的终端 (Compromised Endpoints)** 窗口选择该终端的 MAC 地址并应用一个 ANC 策略，例如隔离。Cisco ISE 对该终端触发 CoA 并应用相应的 ANC 策略。如果 ANC 策略不可用，则Cisco ISE 对该终端触发 CoA 并应用原始的授权策略。可以使用**受到危害的终端 (Compromised Endpoints)** 窗口上的**清除威胁和漏洞 (Clear Threat and Vulnerabilities)** 选项来（从Cisco ISE 系统数据库）清除与某终端关联的威胁和漏洞。

以下属性列在威胁 (Threat) 字典下：

- CTA-Course_Of_Action（值可以是内部屏蔽 [Internal Blocking]、清除 [Eradication] 或监控 [Monitoring]）
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

基础评分 (Base Score) 和临时分数 (Temporal Score) 属性的有效范围均为 0 至 10。

当收到某个终端的漏洞事件时，Cisco ISE 对该终端触发 CoA。但是，在收到威胁事件时不会触发 CoA。

您可以通过使用漏洞属性来创建授权策略，从而基于属性值自动隔离易受攻击的终端。例如：

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

要查看在 CoA 事件期间自动隔离的终端的日志，请选择 **操作 (Operations)** > **以威胁防护为中心的 NAC 实时日志 (Threat-Centric NAC Live Logs)**。要查看手动隔离的终端的日志，请选择 **操作 (Operations)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。

启用以威胁防护为中心的 NAC 服务时，请注意以下几点：

- 以威胁防护为中心的 NAC 服务需要Cisco ISE Advantage 许可证。
- 在一个部署中，只能在一个节点上启用以威胁防护为中心的 NAC 服务。
- 对于漏洞评估服务，每个供应商只能添加一个适配器实例。但是，您可以添加多个 FireAMP 适配器实例。
- 可以停止并重新启动适配器，而不会丢失其配置。配置适配器之后，您可以随时停止适配器。即使重新启动 ISE 服务，适配器也将保持此状态。选择适配器并点击**重新启动 (Restart)** 以重新启动适配器。

注释 当适配器处于“停止”(Stopped) 状态时，只能编辑适配器实例的名称；无法编辑适配器配置或高级设置。

以威胁防护为中心的 NAC 实时日志 (Threat Centric NAC Live Logs) 窗口（**操作 (Operations)** > **以防护为中心的 NAC 实时日志 (Threat-Centric NAC Live Logs)**）列出了所有威胁和漏洞事件。它显

示终端的事故类型、适配器名称、授权匹配规则和授权配置文件（旧的和新的）。您还可以查看事件的详细信息。

您可以在以下页面上查看终端的威胁信息：

- **主页 (Home page) > 威胁控制面板 (Threat dashboard)**
- **情景可视性 (Context Visibility) > 终端 (Endpoints) > 受到危害的终端 (Compromised Endpoints)**

以下警报由以威胁防护为中心的 NAC 服务触发：

- 无法访问适配器（系统日志 ID：91002）：表示适配器无法访问。
- 适配器连接失败（系统日志 ID：91018）：表示适配器可访问，但是适配器和源服务器之间的连接已中断。
- 适配器因出错而停止工作（系统日志 ID：91006）：如果适配器未处于所需状态，则触发此警报。如果显示此警报，请检查适配器配置和服务器连接。有关详细信息，请参阅适配器日志。
- 适配器错误（系统日志 ID：91009）：表示 Qualys 适配器无法与 Qualys 站点建立连接或通过其下载信息。

以下报告可用于以威胁防护为中心的 NAC 服务：

- **适配器状态 (Adapter Status)**：适配器状态报告显示威胁和漏洞适配器的状态。
- **COA 事件 (COA Events)**：当收到某个终端的漏洞事件时，Cisco ISE 对该终端触发 CoA。CoA 事件报告显示这些 CoA 事件的状态。同时显示这些终端的新旧授权规则和配置文件详细信息。
- **威胁事件 (Threat Events)**：威胁事件报告提供Cisco ISE 从已配置的各种适配器接收的所有威胁事件的列表。此报告不包括漏洞评估事件。
- **漏洞评估 (Vulnerability Assessment)**：漏洞评估报告提供您的终端正在进行的评估的信息。您可以查看此报告以确认评估是否以配置策略为基础正在进行。

可以在**操作 (Operations) > 报告 (Reports) > 诊断 (Diagnostics) > ISE 计数器 (ISE Counters) > 阈值计数器趋势 (Threshold Counter Trends)** 位置查看以下信息：

- 收到事件的总数
- 威胁事件的总数
- 漏洞事件的总数
- 发出（到 PSN）的 CoA 的总数

系统每 5 分钟收集一次这些属性的值，因此，这些值表示最近 5 分钟的计数。

威胁 (Threat) 控制面板包含以下 Dashlet：

- **受到危害的终端总数 (Total Compromised Endpoints)** Dashlet 显示当前网络中受影响的终端总数（包括连接和断开连接的终端）。

- **特定时段受危害的终端 (Compromised Endpoints Over Time)** Dashlet 显示特定时间段内对终端影响的历史视图。
- **首要威胁 (Top Threats)** Dashlet 显示基于受影响的终端数量和威胁的严重程度的首要威胁。
- 可以使用**威胁关注列表 (Threats Watchlist)** Dashlet 分析所选事件的趋势。

首要威胁 (Top Threats) Dashlet 中的气泡大小表示受影响终端的数量，而浅色面积表示断开连接终端的数量。颜色和垂直刻度表示威胁的严重程度。威胁分为两类 - 指标和事故。指标的严重程度属性是“Likely_Impact”，而事故的严重程度属性是“Impact_Qualification”。

受到危害的终端 (Compromised Endpoint) 页面显示受影响终端的矩阵视图以及各个威胁类别的影响严重程度。您可以点击设备链接以查看某终端的详细威胁信息。

“操作过程”(Course Of Action) 图表显示根据从 CTA 适配器收到的 CTA-Course_Of_Action 属性，对威胁事件执行的操作（内部屏蔽、根除或监控）。

在主页 (Home) 上的漏洞 (Vulnerability) 控制面板包含以下 Dashlet：

- **易受攻击的终端总数 (Total Vulnerable Endpoints)** Dashlet 显示 CVSS 分数大于指定值的终端总数。此外，还显示 CVSS 分数大于指定值的连接和断开连接的终端总数。
- **首要漏洞 (Top Vulnerability)** Dashlet 显示基于受影响的终端数量或漏洞的严重程度的首要漏洞。首要漏洞 (Top Vulnerability) Dashlet 中的气泡大小表示受影响终端的数量，而浅色面积表示断开连接终端的数量。颜色和垂直刻度表示漏洞的严重程度。
- 可以使用**漏洞关注列表 (Vulnerability Watchlist)** Dashlet 分析一段时间内所选漏洞的趋势。点击 Dashlet 中的搜索图标并输入供应商特定 ID（Qualys ID 号码为“qid”）以选择和查看该特定 ID 号码的趋势。
- **特定时段易受攻击终端 (Vulnerable Endpoints Over Time)** Dashlet 显示一段时间内对终端的影响的历史视图。

易受攻击的终端 (Vulnerable Endpoints) 窗口上的“按 CVSS 排序的终端数”(Endpoint Count By CVSS) 图表显示受影响终端的数量及其 CVSS 分数。在**易受攻击的终端 (Vulnerable Endpoints)** 窗口，还可以查看受影响的终端列表。可以点击设备链接以查看各个终端的详细漏洞信息。

支持捆绑包中包含以威胁防护为中心的NAC服务日志（请参阅下载思科ISE日志文件，第1258页）。以威胁防护为中心的 NAC 服务日志位于 support/logs/TC-NAC/

启用威胁中心 NAC 服务

要配置漏洞和威胁适配器，您必须首先启用威胁中心NAC服务。此服务只可在您部署中的一个策略服务节点上启用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选中要启用威胁中心 NAC 服务的 PSN 旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 选中**启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)** 复选框。

步骤 4 点击保存 (Save)。

相关主题

添加 Sourcefire FireAMP 适配器，第 1061 页
配置认知威胁分析适配器，第 1062 页
为 CTA 适配器配置授权配置文件，第 1064 页
使用操作过程属性配置授权策略，第 1064 页
以威胁防护为中心的 NAC 服务，第 1057 页

添加 Sourcefire FireAMP 适配器

开始之前

- 您必须有一个配有 SourceFire FireAMP 的账户。
- 您需要在所有终端部署 FireAMP 客户端。
- 您需要在部署节点上启用以威胁防护为中心的 NAC 服务（请参阅启用威胁中心 NAC 服务，第 1060 页）。
- FireAMP 适配器使用 SSL 进行 REST API 调用（对于 AMP 云），并使用 AMQP 接收事件。它还支持使用代理。FireAMP 适配器使用端口 443 进行通信。

步骤 1 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择管理 (Administration) > 以威胁防护为中心的 NAC (Threat Centric NAC) > 第三方供应商 (Third Party Vendors)。

步骤 2 点击添加 (Add)。

步骤 3 从提供商 (Vendor)下拉列表中选择 AMP：威胁防护 (AMP : Threat)。

步骤 4 输入适配器实例的名称。

步骤 5 点击保存 (Save)。

步骤 6 刷新“供应商实例列表”(Vendor Instances listing) 页面。在“供应商实例列表”(Vendor Instances listing) 页面中，仅在适配器状态变为配置就绪 (Ready to Configure) 之后，您才可配置适配器。

步骤 7 点击准备配置 (Ready to Configure) 链接。

步骤 8 （可选）如果您配置了 SOCKS 代理服务器用于路由所有流量，请输入主机名和该代理服务器的端口号。

步骤 9 选择您想要连接的云。您可以选择 US 云或 EU 云。

步骤 10 选择要订阅的事件源。可提供以下选项：

- 仅 AMP 事件
- 仅 CTA 事件
- CTA 和 AMP 事件

步骤 11 点击 FireAMP 链路并以管理员的身份登录 FireAMP。点击**应用 (Applications)** 窗格中的**允许 (Allow)**，以授权流事件导出请求。
您将被重定向回到Cisco ISE。

步骤 12 选择您要监控的事件（例如，可疑下载、连接到可疑域、已执行恶意软件、Java 威胁）。

当更改高级设置或重新配置适配器时，如果向 AMP 云中添加了任何新事件，则这些事件也会列在**事件列表 (Events Listing)** 窗口中。

可以为适配器选择一种日志级别。可用选项为：**错误 (Error)** 、**信息 (Info)** 和**调试 (Debug)**。

适配器实例配置摘要将在**配置摘要 (Configuration Summary)** 页面中显示。

配置认知威胁分析适配器

开始之前

- 您需要在部署节点上启用以威胁防护为中心的 NAC 服务（请参阅启用威胁中心 NAC 服务，第 1060 页）。
- 通过 http://cognitive.cisco.com/login 登录到Cisco感知威胁分析 (CTA) 门户并请求 CTA STIX/TAXII 服务。有关详细信息，请参阅 Cisco ScanCenter 管理员指南。
- 感知威胁分析 (CTA) 适配器使用含 SSL 的 TAXII 协议轮询 CTA 云是否有检测到的威胁。它还支持使用代理。
- 将适配器证书导入到受信任证书库。依次选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)** 导入证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **威胁中心 NAC (Threat Centric NAC)** > **第三方供应商 (Third Party Vendors)**。

步骤 2 点击**添加 (Add)**。

步骤 3 从**提供商 (Vendor)** 下拉列表中选择 **CTA：威胁 (CTA : Threat)**。

步骤 4 输入适配器实例的名称。

步骤 5 点击**保存 (Save)**。

步骤 6 刷新“供应商实例列表”(Vendor Instances listing) 页面。在“供应商实例列表”(Vendor Instances listing) 页面中，仅在适配器状态变为**配置就绪 (Ready to Configure)** 之后，您才可配置适配器。

步骤 7 点击**准备配置 (Ready to Configure)** 链接。

步骤 8 输入下列详细信息：

- **CTA STIX/TAXII 服务 URL (CTA STIX/TAXII service URL)**：CTA 云服务的 URL。默认情况下，使用以下 URL：https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/
- **CTA 源名称 (CTA feed name)**：输入 CTA 云服务的源名称。

- **CTA 用户名和密码 (CTA username and password)**：输入 CTA 云服务的用户名和密码。
- **代理主机和端口 (Proxy host and port)**（可选）：如果您已配置代理服务器用于路由所有流量，请输入主机名和该代理服务器的端口号。
- **轮询间隔 (Polling interval)**：每次轮询之间的时间间隔。默认值为 30 分钟。
- **首次轮询持续时间（按小时）(First Poll Duration in hours)**：在首次轮询中提取的数据的期限。默认值为 2 小时。最大值为 12 小时。
- **事故类型 (Incident Type)**：可提供以下选项：
  - **仅 CTA 事件**
  - **仅 AMP 事件**
  - **CTA 和 AMP 事件**

步骤 9 点击 **下一步 (Next)**。

步骤 10 点击**高级设置 (Advanced Settings)** 配置以下选项：

- **影响限定条件 (Impact Qualification)**：选择要轮询的事件的严重程度。可提供以下选项：
  - **1 - 不重要 (Insignificant)**
  - **2 - 干扰 (Distracting)**
  - **3 - 痛苦 (Painful)**
  - **4 - 破坏 (Damaging)**
  - **5 - 灾难 (Catastrophic)**

  例如，如果您选择了“3-痛苦”(3-Painful)，则轮询达到此严重程度（3-痛苦）及更高程度（在本例中为 4-破坏和 5-灾难）的事件。
- **日志记录级别 (Logging level)**：选择适配器的日志级别。可用选项为：错误 (Error)、信息 (Info) 和调试 (Debug)。

步骤 11 点击**完成 (Finish)**。

注释 CTA 使用 Web 代理日志中作为 IP 地址或用户名列出的用户身份。具体而言，在使用 IP 地址的情况下，通过代理日志可用的设备的 IP 地址可能与内部网络上另一台设备的 IP 地址冲突。例如，通过 AnyConnect 和分割隧道直接连接到互联网的漫游用户可以获取本地 IP 范围地址（例如，10.0.0.X 地址），该地址可能与内部网络中使用的重叠私用 IP 范围中的地址冲突。我们建议您在定义策略时考虑逻辑网络架构，以避免对不匹配的设备应用隔离操作。

为 CTA 适配器配置授权配置文件

对于每个威胁事件，CTA 适配器会返回行动方案属性的以下值之一：内部阻止、监控或根除。您可以根据这些值创建授权配置文件。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**策略 (Policy) > 策略元素 (Policy Elements) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)** 。

步骤 2 点击**添加 (Add)**。

步骤 3 输入授权配置文件的名称和描述。

步骤 4 选择访问类型。

步骤 5 输入所需的详细信息，并点击**提交 (Submit)**。

使用操作过程属性配置授权策略

您可以使用 CTA-Course_Of_Action 属性为报告威胁事件的终端配置授权策略。此属性在“威胁”(Threat) 目录下可用。

您还可以根据 CTA-Course_Of_Action 属性创建例外规则。

步骤 1 选择**策略 (Policy) > 策略集 (Policy Sets)**
您可以为有威胁事件的终端编辑现有策略规则或创建新例外规则。

步骤 2 创造一个条件检查 CTA-Course_Of_Action 属性值并分配合适的授权配置文件。例如：

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

注释 “Internal Blocking”是建议用于隔离终端的操作过程属性。

步骤 3 点击**保存 (Save)**。

当收到终端的威胁事件时，Cisco ISE 会检查该终端是否有任何匹配的授权策略，并仅在终端处于活动状态时触发 CoA。如果终端处于离线状态，威胁事件详细信息会添加到“威胁事件”(Threat Events) 报告（“操作”(Operations)>“报告”(Reports)>“以威胁防护为中心的 NAC”(Threat Centralic NAC)>“威胁事件”(Threat Events)）。

注释 有时，CTA 会在一个事件中发送多个风险及其关联的操作过程属性。例如，它可以在一个事件中发送“内部阻断”(Internal Blocking) 和“监控”(Monitoring)（操作过程属性）。在这种情况下，如果您已使用“equals”运算符配置隔离终端的授权策略，则不会隔离终端。例如：

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization profile)
```

在这种情况下，必须在授权策略中使用“contains”运算符来隔离终端。例如：

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

思科 ISE 中的漏洞评估支持

Cisco ISE 与以下漏洞评估 (VA) 生态系统合作伙伴集成，以获取连接到Cisco ISE 网络的终端漏洞结果：

- Qualys：Qualys 是一种基于云的评估系统，在网络中部署有扫描设备。Cisco ISE 允许您配置与 Qualys 通信并获取 VA 结果的适配器。您可以从管理门户配置适配器。您需要具有超级管理员权限的Cisco ISE 管理员帐户来配置适配器。Qualys 适配器使用 REST API 与 Qualys 云服务进行通信。您需要 Qualys 中具有管理器权限的用户帐户来访问 REST API。Cisco ISE 使用以下 Qualys REST API：
  - 托管检测列表 API：用于检查终端的最后扫描结果
  - 扫描 API：用于触发终端的按需扫描

  Qualys 对已订阅用户可进行的 API 调用数量实施限制。默认速率限制数为每 24 小时 300 次。Cisco ISE 使用 Qualys API 版本 2.0 连接到 Qualys。请参阅 Qualys API V2 用户指南，以了解这些 API 功能的详细信息。
- Rapid7 Nexpose：Cisco ISE 与漏洞管理解决方案 Rapid7 Nexpose 集成，以帮助检测漏洞，使您能够快速响应此类威胁。Cisco ISE 从 Nexpose 接收漏洞数据，并根据在 ISE 中配置的策略隔离受影响的终端。从Cisco ISE 控制板，可以查看受影响的终端并采取适当的操作。

  Cisco ISE 已经过 Nexpose 版本 6.4.1 测试。
- Tenable SecurityCenter（Nessus 扫描程序）：Cisco ISE 与 Tenable SecurityCenter 集成并从 Tenable Nessus 扫描程序（由 Tenable SecurityCenter 管理）接收漏洞数据，然后，系统根据您在 ISE 中配置的策略来隔离受影响的终端。从Cisco ISE 控制板，可以查看受影响的终端并采取适当的操作。

  Cisco ISE 已经过 Tenable SecurityCenter 5.3.2 测试。

来自生态系统合作伙伴的结果被转换为结构化威胁信息表达式 (STIX)表示，然后基于该值根据需要触发授权更改 (CoA)，并授予终端相应的访问权限级别。

评估终端漏洞所需的时间取决于多种因素，因此无法实时执行 VA。影响评估终端漏洞所需时间的因素包括：

- 漏洞评估生态系统

- 扫描的漏洞类型
- 启用的扫描类型
- 生态系统为扫描设备分配的网络和系统资源

在此版本的Cisco ISE 中，仅对采用 IPv4 地址的终端进行漏洞评估。

启用并配置漏洞评估服务

要启用和配置Cisco ISE 的漏洞评估服务，请执行以下任务：

步骤 1 启用威胁中心 NAC 服务， 第 1060 页。

步骤 2 若要配置以下项：

- Qualys 适配器，请参阅配置 Qualys 适配器， 第 1067 页。
- Nexpose 适配器，请参阅配置 Nexpose 适配器， 第 1069 页。
- 租户适配器，请参阅。配置 Tenable 适配器， 第 1071 页

步骤 3 配置授权配置文件， 第 1074 页。

步骤 4 配置隔离易受攻击的终端的例外规则， 第 1074 页。

启用威胁中心 NAC 服务

要配置漏洞和威胁适配器，您必须首先启用威胁中心NAC服务。此服务只可在您部署中的一个策略服务节点上启用。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选中要启用威胁中心 NAC 服务的 PSN 旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 选中**启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)** 复选框。

步骤 4 点击**保存 (Save)**。

相关主题

添加 Sourcefire FireAMP 适配器， 第 1061 页
配置认知威胁分析适配器， 第 1062 页
为 CTA 适配器配置授权配置文件， 第 1064 页
使用操作过程属性配置授权策略， 第 1064 页
以威胁防护为中心的 NAC 服务， 第 1057 页

配置 Qualys 适配器

Cisco ISE 支持 Qualys 漏洞评估生态系统。您必须创建一个 Qualys 适配器供Cisco ISE 与 Qualys 通信和获取 VA 结果。

开始之前

- 您必须拥有以下用户帐户：
  - 带可配置供应商适配器的超级管理员权限的Cisco ISE 的管理员用户帐户。
  - 带管理器权限的 Qualys 用户帐户
- 确保您拥有适当的 Qualys 许可证订用。您需要 Qualys 报告中心、知识库 (KBX) 和 API 的访问权限。有关详细信息，请联系您的 Qualys 客户经理。
- 将 Qualys 服务器证书导入Cisco ISE 的受信任证书库（**管理 (Administration) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates) > 导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）Cisco ISE 受信任证书库中。
- 请参阅《Qualys API 指南》以了解以下配置：
  - 确保已启用 Qualys CVSS 评分（**报告 (Reports) > 设置 (Setup) > CVSS 评分 (CVSS Scoring) > 启用 CVSS 评分 (Enable CVSS Scoring)**）。
  - 确保添加了 IP 地址和 Qualys 终端子网掩码（**资产 (Assets) > 主机资产 (Host Assets)**）。
  - 确保拥有 Qualys 选项配置文件的名称。选项配置文件是 Qualys 用于扫描的扫描器模板。我们建议您使用包括身份验证扫描的选项配置文件（此选项也检查终端的 MAC 地址）。
- Cisco ISE 通过 HTTPS/SSL （端口443）与 Qualys 通信。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **威胁中心 NAC (Threat Centric NAC)** > **第三方供应商 (Third Party Vendors)**。

步骤 2 点击**添加 (Add)**。

步骤 3 从**供应商 (Vendor)** 下拉列表中选择**Qualys:VA**。

步骤 4 输入适配器实例的名称。例如，Qualys_Instance。

系统会显示一个列表页面，其中包含配置的适配器实例列表。

步骤 5 刷新“供应商实例列表”(Vendor Instances listing) 页面。新添加的 Qualys_Instance 适配器的状态应更改为**准备配置 (Ready to Configure)**。

步骤 6 点击**准备配置 (Ready to Configure)** 链接。

步骤 7 在 Qualys 配置屏幕输入以下值并点击**下一步 (Next)**。

字段名称	说明
REST API 主机	托管 Qualys 云的服务器的主机名。请联系 Qualys 代表以获得此信息。

字段名称	说明
REST API 端口	443
用户名	具有管理器权限的 Qualys 用户帐户。
密码	Qualys 帐户的密码。
HTTP 代理主机	如果您拥有配置为路由所有 Internet 流量的代理服务器，输入该代理服务器的主机名。
HTTP 代理端口	输入代理服务器使用的端口号。

如果与 Qualys 服务器建立了连接，将显示“扫描仪映射”(Scanner Mappings) 页面，页面包含 Qualys 扫描仪列表。您网络中的 Qualys 扫描仪将显示在此页面中。

步骤 8 选择Cisco ISE 用于按需扫描的默认扫描仪。

步骤 9 在 **PSN 到扫描仪映射 (PSN to Scanner Mapping)** 区域中，选择一个或多个到 PSN 节点的 Qualys 扫描仪设备，然后点击**下一步 (Next)**。

系统将显示**高级设置 (Advanced Settings)** 窗口。

步骤 10 在**高级设置 (Advanced Settings)** 窗口中输入以下值。此页面上的设置确定按需扫描是否会触发或最后扫描结果将用于 VA。

字段名称	说明
选项配置文件	选择要 Qualys 用于端口的选项配置文件。您可以选择默认选项配置文件初始选项。
最后扫描结果 - 检查设置	
最后扫描结果检查间隔（按分钟计）	（影响主机检测列表 API 的接入速率）时间间隔（按分钟计），该时间后会再次检查最后扫描结果。有效范围为 1 到 2880。
检查最后扫描结果之前的最大结果数	（影响主机检测列表 API 的接入速率）如果队列扫描请求数超过此处指定的最大数量，最后扫描结果会在**最后扫描结果检查间隔（按分钟计）(Last scan results check interval in minutes)** 之前接受检查。有效范围为 1 到 1000。
验证 **MAC** 地址	正确还是错误？当设置为 true 时，Qualys 的最后扫描结果只会在春包括终端的 MAC 地址时使用。
扫描设置	
扫描触发间隔（按分钟计）	（影响扫描 API 接入速率）时间间隔（按分钟计），该时间后按需扫描会触发。有效范围为 1 到 2880。
在扫描触发之前的最大请求数	（影响扫描 API 的接入速率）如果队列扫描请求数超过此处指定的最大数量，按需扫描会在**扫描触发间隔（按分钟计）(Scan trigger interval in minutes)** 字段中的指定时间间隔之前被触发。有效范围为 1 到 1000。
扫描状态检查间隔（按分钟计）	Cisco ISE 与 Qualys 通信以检查扫描状态的时间间隔（按分钟计）。有效范围为 1 到 60。

字段名称	说明
可同时触发的扫描数量	（此选项取决于您映射到在扫描仪映射屏幕的每个节点的扫描仪数量）每个扫描仪每次只能处理一个请求。如果映射了一个以上扫描仪到 PSN，则可以根据选定的扫描仪数量增加此值。有效范围为 1 到 200。
扫描超时（按分钟计）	时间（按分钟计），该时间后扫描请求将超时。如果扫描请求超时，将生成警报。有效范围为 20 到 1440。
每个扫描仪将提交的IP地址最大数量	指示可排列为一个请求以发送到 Qualys 进行处理的请求数。有效范围为 1 到 1000。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG)和“跟踪”(TRACE)。

步骤 11 点击**下一步 (Next)** 以审核配置设置。

步骤 12 点击**完成 (Finish)**。

配置 Nexpose 适配器

必须创建一个 Nexpose 适配器，供Cisco ISE 与 Nexpose 通信和获取 VA 结果。

开始之前

- 确保已在Cisco ISE 中启用以威胁防护为中心的 NAC 服务。
- 登录 Nexpose 安全控制台并创建具有以下权限的用户帐户：
  - 管理站点
  - 创建报告
- 将 Nexpose 服务器证书导入Cisco ISE 中的受信任证书存储区（**管理 (Administration)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）Cisco ISE 受信任证书库中。
- Cisco ISE 通过 HTTPS/SSL（端口 3780）与 Nexpose 通信。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **以威胁防护为中心的 NAC (Threat Centric NAC)** > **第三方供应商 (Third Party Vendors)**。

步骤 2 点击**添加 (Add)**。

步骤 3 从**供应商 (Vendor)** 下拉列表中，选择 **Rapid7 Nexpose:VA**。

步骤 4 输入适配器实例的名称。例如，Nexpose。

系统会显示一个列表页面，其中包含配置的适配器实例列表。

步骤 5 刷新“供应商实例列表”(Vendor Instances listing) 页面。新添加的 Nexpose 适配器的状态应该会更改为**准备配置 (Ready to Configure)**。

步骤 6 点击**准备配置 (Ready to Configure)** 链接。

步骤 7 在 Nexpose 配置屏幕输入以下值并点击**下一步 (Next)**。

字段名称	说明
Nexpose 主机 (Nexpose Host)	Nexpose 服务器的主机名。
Nexpose 端口 (Nexpose Port)	3780。
用户名 (Username)	Nexpose 管理员用户帐户。
密码 (Password)	Nexpose 管理员用户帐户的密码。
HTTP 代理主机	如果您拥有配置为路由所有 Internet 流量的代理服务器，输入该代理服务器的主机名。
HTTP 代理端口	输入代理服务器使用的端口号。

步骤 8 点击**下一步 (Next)** 以配置高级设置。

步骤 9 在**高级设置 (Advanced Settings)** 窗口中输入以下值。此页面上的设置确定按需扫描是否会触发或最后扫描结果将用于 VA。

字段名称	说明
用于检查最新扫描结果的设置	
检查最新扫描结果之间的间隔（分钟）(Interval between checking the latest scan results in minutes)	必须再次检查最后扫描结果之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
可以触发检查最新扫描结果的待处理请求数 (Number of pending requests that can trigger checking the latest scan results)	如果队列中的扫描请求数超过此处指定的最大数量，则系统会在检查最新扫描结果之间的间隔（分钟）(Interval between checking the latest scan results in minutes) 字段中指定的时间间隔之前检查最后扫描结果。有效范围为 1 到 1000。
验证 MAC 地址	正确还是错误？当设置为 true 时，Nexpose 的最后扫描结果只会在其包括终端 MAC 地址时使用。
扫描设置	

字段名称	说明
用于检查最新扫描结果的设置	
每个站点的扫描触发间隔（分钟）**(Scan trigger interval for each site in minutes)**	触发扫描之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
各站点触发扫描之前待处理请求的数量 **(Number of pending requests before a scan is triggered for each site)**	如果队列扫描请求数超过此处指定的最大数量，则会在**扫描超时（分钟）(Scan timeout in minutes)** 字段中的指定时间间隔之前触发扫描。有效范围为 1 到 1000。
扫描超时（按分钟计）	时间（按分钟计），该时间后扫描请求将超时。如果扫描请求超时，将生成警报。有效范围为 20 到 1440。
可以并行触发扫描的站点数量 **(Number of sites for which scans could be triggered concurrently)**	可同时对其运行扫描的站点数。有效范围为 1 到 200。
时区	根据 Nexpose 服务器中配置的时区选择时区。
Http 超时（秒）(Http timeout in seconds)	Cisco ISE 等待来自 Nexpose 的响应的时间间隔（秒）。有效范围为 5 到 1200。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG)和“跟踪”(TRACE)。

步骤 10 点击**下一步 (Next)** 以审核配置设置。

步骤 11 点击**完成 (Finish)**。

配置 Tenable 适配器

必须创建一个 Tenable 适配器，供Cisco ISE 与 Tenable SecurityCenter（Nessus 扫描器）通信和获取 VA 结果。

开始之前

注释 必须在 Tenable SecurityCenter 中配置以下内容，然后才能在Cisco ISE 中配置 Tenable 适配器。请参阅 Tenable SecurityCenter 文档以了解这些配置。

- 您必须安装 Tenable Security Center 和 Tenable Nessus 漏洞扫描器。在注册 Tenable Nessus 扫描器时，请确保在**注册 (Registration)** 字段中选择**由 SecurityCenter 管理 (Managed by SecurityCenter)**。
- 在 Tenable SecurityCenter 中创建具有安全管理器权限的用户帐户。
- 在 SecurityCenter 中创建存储库（使用管理员凭证登录到 Tenable SecurityCenter 并选择**存储库 (Repository) > 添加 (Add)**）。
- 在存储库中添加要扫描的终端 IP 范围。
- 添加 Nessus 扫描器。
- 创建扫描区域，并向扫描区域和映射到这些扫描区域的扫描器分配 IP 地址。
- 为 ISE 创建扫描策略。
- 添加活动扫描并将其与 ISE 扫描策略关联。配置设置和目标（IP/DNS 名称）。
- 从 Tenable SecurityCenter 导出系统和根证书，并将其导入Cisco ISE 中的受信任证书存储区（**管理 (Administration) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates) > 导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）Cisco ISE 受信任证书库中。
- Cisco ISE 通过 HTTPS/SSL （端口 443）与 Tenable SecurityCenter 通信。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration) > 以威胁防护为中心的 NAC (Threat Centric NAC) > 第三方供应商 (Third Party Vendors)**。

步骤 2 点击**添加 (Add)**。

步骤 3 从**供应商 (Vendor)** 下拉列表，选择 **Tenable Security Center:VA**。

步骤 4 输入适配器实例的名称。例如，Tenable。

系统会显示一个列表页面，其中包含配置的适配器实例列表。

步骤 5 刷新“供应商实例列表”(Vendor Instances listing) 页面。新添加的 Tenable 适配器的状态应更改为**准备配置 (Ready to Configure)**。

步骤 6 点击**准备配置 (Ready to Configure)** 链接。

步骤 7 在 Tenable SecurityCenter 配置窗口中输入以下值并点击**下一步 (Next)**。

字段名称	说明
Tenable SecurityCenter 主机	Tenable SecurityCenter 的主机名。
Tenable SecurityCenter 端口	443
用户名	在 Tenable SecurityCenter 中具有安全管理器权限的用户帐户的用户名。
密码	在 Tenable SecurityCenter 中具有安全管理器权限的用户帐户的密码。
HTTP 代理主机	如果您拥有配置为路由所有 Internet 流量的代理服务器，输入该代理服务器的主机名。
HTTP 代理端口	输入代理服务器使用的端口号。

步骤 8 点击**下一步 (Next)**。

步骤 9 在**高级设置 (Advanced Settings)** 窗口中输入以下值。此页面上的设置确定按需扫描是否会触发或最后扫描结果将用于 VA。

字段名称	说明
存储库	选择您在 Tenable SecurityCenter 中创建的存储库。
扫描策略	选择您在 Tenable SecurityCenter 中为 ISE 创建的扫描策略。
用于检查最新扫描结果的设置	
检查最新扫描结果之间的间隔（分钟）	必须再次检查最后扫描结果之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
可以触发检查最新扫描结果的待处理请求数	如果队列中的扫描请求数超过此处指定的最大数量，则系统会在**检查最新扫描结果之间的间隔（分钟）** 字段中指定的时间间隔之前检查最后扫描结果。有效范围为 1 到 1000。默认值为 10。
验证 MAC 地址	正确还是错误？当设置为 true 时，Tenable SecurityCenter 的最后扫描结果只会在其包括终端 MAC 地址时使用。
扫描设置	
每个站点的扫描触发间隔（分钟）	触发按需扫描之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
触发扫描之前待处理请求的数量	如果队列扫描请求数超过此处指定的最大数量，则会在**每个站点的扫描触发间隔（分钟）** 字段中的指定时间间隔之前触发按需扫描。有效范围为 1 到 1000。

字段名称	说明
扫描超时（按分钟计）	扫描请求超时之前所经历的时间（分钟）。如果扫描请求超时，将生成警报。有效范围为 20 到 1440。
可以并行运行的扫描数	可同时运行的扫描数量。有效范围为 1 到 200。
Http 超时（秒）	Cisco ISE 等待来自 Tenable SecurityCenter 的响应的时间间隔（秒）。有效范围为 5 到 1200。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG)和“跟踪”(TRACE)。

步骤 10 点击**下一步 (Next)** 以审核配置设置。

步骤 11 点击**完成 (Finish)**。

配置授权配置文件

Cisco ISE 中的授权配置文件现在包括扫描漏洞终端的选项。您可以选择定期运行扫描，并指定这些扫描的时间间隔。定义授权配置文件后，可以将其应用于现有授权策略规则，或创建新的授权策略规则。

开始之前

您必须已启用以威胁防护为中心的 NAC 服务，并且已配置供应商适配器。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 创建新授权配置文件或编辑现有配置文件。

步骤 3 从**常见任务 (Common Tasks)** 区域中，选中**评估漏洞 (Assess Vulnerabilities)** 复选框。

步骤 4 从**适配器实例 (Adapter Instance)** 下拉列表中，选择已配置的供应商适配器。例如，Qualys_Instance。

步骤 5 如果上一次扫描的时间大于文本框中的时间，请在触发扫描字段中输入以小时为单位的扫描间隔。有效范围为 1 到 9999。

步骤 6 勾选**按上述间隔定期评估 (Assess periodically using above internval)** 复选框。

步骤 7 点击**提交 (Submit)**。

配置隔离易受攻击的终端的例外规则

您可以使用以下漏洞评估 (Vulnerability Assessment) 属性来配置一个例外规则，并提供对以下易受攻击终端的有限访问权限：

- Threat:Qualys-CVSS_Base_Score

- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

这些属性在威胁目录下可用。有效值范围为 0 到 10。

您可以选择隔离终端，提供有限访问权限（重定向至不同的门户）或拒绝请求。

步骤 1 选择 **策略 (Policy)** > **策略集 (Policy Sets)**。
您可以编辑现有策略规则或创建新例外规则，以检查 VA 属性。

步骤 2 创造条件检查 Qualys 评分并分配正确的授权配置文件。例如：

任何身份组和 Threat:Qualys-CVSS_Base_Score (Any Identity Group & Threat:Qualys-CVSS_Base_Score) > 5 -> 隔离（授权配置文件）(Quarantine (authorization profile))

步骤 3 点击**保存 (Save)**。

漏洞评估日志

Cisco ISE 为故障排除 VA 服务提供以下日志。

- vaservice.log - 包含 VA 核心信息，在运行 TC-NAC 服务的节点上可用。
- varuntime.log - 包含终端和 VA 流程的信息；在监控节点和运行 TC-NAC 服务的节点上可用。
- vaaggregation.log - 包含终端漏洞的每小时汇聚详细信息，在主管理节点上可用。

部署和节点设置

您可以通过**部署节点 (Deployment Nodes)** 窗口配置Cisco ISE（PAN、PSN 和 MnT）节点并设置部署。

部署节点列表 窗口

下表介绍了**部署节点列表** 窗口上的字段，您可以使用此窗口在部署中配置Cisco ISE 节点。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**.

字段名称	使用指南
主机名 (Hostname)	显示节点的主机名。

字段名称	使用指南
相关角色 (Personas)	（只有在节点类型为Cisco ISE 时才显示）列出 Cisco ISE 节点承担的角色。 例如，**管理 (Administration)**、**策略服务 (Policy Service)**、**监控 (Monitoring)** 或 **pxGrid**。
角色 (Rol)e	如果在此节点上启用了管理和监控角色，则指示管理和监控角色承担的职责（主要、辅助或独立职责）。职责可以是以下一项或多项： • **PRI(A)**：指主 PAN • **SEC(A)**：指辅助 PAN • **PRI(M)**：指主 MnT • **SEC(M)**：指辅助 MnT
服务 (Services)	（只有在启用策略服务角色时才显示）列出此 Cisco ISE 节点上运行的服务。服务可包括以下任意一项： • **身份映射** • **会话** • **剖析** • **全部**
节点状态	指示部署中每个Cisco ISE 节点的数据复制状态。 • 绿色（已连接）：表示部署中已注册的Cisco ISE 节点与主 PAN 处于同步状态。 • 红色（断开）：表示Cisco ISE 节点无法到达、已断开或未进行数据复制。 • 橙色（处理中）：表示向主PAN新注册了新 Cisco ISE 节点、您已执行手动同步操作或 Cisco ISE 节点与主 PAN 不同步。 有关详细信息，请点击**节点状态 (Node Status)** 列中每个Cisco ISE 节点的快速查看图标。

相关主题

思科 ISE 分布式部署，第 35 页
思科 ISE 部署术语，第 32 页
配置思科 ISE 节点，第 32 页

注册辅助思科 ISE 节点

常规节点设置

下表说明Cisco ISE 节点的**常规设置 (General Settings)** 窗口中的字段。在此窗口中，可以将角色分配给节点并配置要在其上运行的服务。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **部署节点 (Deployment Node)** > **编辑 (Edit)** > **常规设置 (General Settings)**。

表 *161:* 常规节点设置

字段名称	使用指南
主机名 (Hostname)	显示Cisco ISE 节点的主机名。
FQDN	显示Cisco ISE 节点的完全限定域名。例如 ise1.cisco.com。
IP 地址 (IP Address)	显示Cisco ISE 节点的 IP 地址。
节点类型 (Node Type)	显示节点类型。
相关角色 (Personas)	
管理 (Administration)	如果Cisco ISE 节点承担管理角色，请启用此切换按钮。只有在受许可提供管理服务的节点上才可以启用 Administration 角色。 **角色 (Role)** - 显示管理角色在部署中承担的职责。角色可以采用以下任一值：**独立 (Standalone)**、**主 (Primary)** 或**辅助 (Secondary)**。 **设为主要 (Make Primary)** - 选择此按钮可使该节点成为主Cisco ISE 节点。在部署中您只能有一个主要Cisco ISE 节点。当您将此节点设置为主要节点之后，此页面的其他选项将进入活动状态。在部署中您只能有两个 Administration 节点。如果节点具有**独立 (Standalone)** 角色，则旁边会显示**设为主要 (Make Primary)** 按钮。如果节点具有**辅助 (Secondary)** 角色，则旁边会显示**升级为主要 (Promote to Primary)** 按钮。如果节点具有**主要 (Primary)** 角色，并且没有其他节点注册到该节点，则旁边会显示**设为独立 (Make Standalone)** 按钮。您可以点击此按钮以使您的主要节点成为独立节点。

字段名称	使用指南
监控 **(Monitoring)**	如果要Cisco ISE 节点承担监控角色并充当日志收集器，请启用此切换按钮。分布式部署中必须至少有一个监控节点。配置主 PAN 时，必须启用监控角色。在部署中注册辅助监控节点之后，如有必要，可以编辑主 PAN 和禁用监控角色。 要在 VMware 平台上将Cisco ISE 节点配置为您的日志收集器，请使用以下规定确定您所需要的最低磁盘空间：您的网络中每天每个终端 180 KB，您的网络中每天每个Cisco ISE 节点 2.5 MB。 您可以根据您想要将多少个月的数据至于监控模式下，计算您所需的最大磁盘空间。如果您的部署中只有一个监控节点，则该节点会承担独立职责。如果在部署中有两个监控节点，Cisco ISE 会显示另一个监控节点的名称以供您配置主要/辅助角色。要配置这些职责，请选择以下选项之一： • **主 (Primary)**：使当前节点成为主监控节点。 • **辅助 (Secondary)**：使当前节点成为辅助监控节点。 • **无 (None)** - 如果要使监控节点不承担主要-辅助角色。 如果您将您的一个监控节点配置为主要或辅助节点，另一个监控节点相应地自动成为辅助或主要节点。主要监控节点和辅助监控节点都接收管理和策略服务日志。如果将一个监控节点的角色改为**无 (None)**，则另一个监控节点的角色也会成为**无 (None)**，从而会在您将某个节点指定为监控节点之后取消高可用性对。您会在**远程日志记录目标 (Remote Logging Targets)** 窗口中发现此节点被列为系统日志目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

字段名称	使用指南
策略服务 **(Policy Service)**	

字段名称	使用指南
	启用此切换按钮可启用以下任一或所有服务： • **启用会话服务 (Enable Session Services)**：选中此复选框可启用网络访问、终端安全评估、访客和客户端调配服务。从**在节点组中包含节点 (Include Node in Node Group)** 下拉列表中选择此策略服务节点所属的组。请注意，证书颁发机构 (CA) 和安全传输注册 (EST) 服务只能在已启用会话服务的策略服务节点上运行。 对于**在节点组中包含节点 (Include Node in Node Group)**，如果不希望此策略服务节点加入任何组，请选择**无 (None)**。 同一个节点组中的所有节点都应在网络接入设备上配置为 RADIUS 客户端，并获 CoA 授权，因为这些节点中的任何一个节点均可为通过节点组中的任何节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，则节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或作为 RADIUS 服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。 虽然可以使用多个Cisco ISE 节点将单个 NAD 配置为 RADIUS 服务器和动态授权客户端，但并不要求所有节点都属于同一个节点组。 一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。有关详细信息，请参阅《》中的“创建策略服务节点组”部分请参阅创建策略服务节点组，第 78 页。 • **启用分析服务 (Enable Profiling Service)**：选中此复选框可启用分析服务。如果启用分析服务，必须点击**分析配置 (Profiling Configuration)** 选项卡并根据要求输入详细信息。当您启用或禁用策略服务节点上运行的任意服务或对此节点做任何更改时，您将重新启动运行这些服务的应用服务器进程。这些服务重新启动时预计会有延迟。您可以从 CLI 使用 *show application status ise* 命令，确定何时在节点上重新启动了应用服务器。

字段名称	使用指南
	• **启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)**：选中此复选框可启用威胁中心网络访问控制 (TC-NAC) 功能。通过此功能，您可依据威胁和漏洞适配器发送的威胁和漏洞属性创建授权策略。威胁严重级别和漏洞评估结果可用于动态控制终端或用户的访问级别。 • **启用 SXP 服务 (Enable SXP Service)**：选中此复选框可在节点上启用SXP服务。您还必须指定 SXP 服务使用的接口。 如果已配置NIC绑定或组合，则还会在使用**接口 (Use Interface)** 下拉列表中列出绑定接口以及物理接口。 • **启用设备管理员服务 (Enable Device Admin Service)**：选中此复选框可创建 TACACS 策略集和策略结果等，以便控制和审计网络设备的配置。 • **启用被动身份服务 (Enable Passive Identity Service)**：选中此复选框可启用身份映射功能。通过此功能，您可以监控通过域控制器 (DC)（而不是Cisco ISE）进行身份验证的用户。在Cisco ISE不主动对用户进行网络访问身份验证的网络中，您可以使用身份映射功能从 Active Directory (AD) 域控制器收集用户身份验证信息。
pxGrid	选中此复选框可启用 pxGrid 角色。Cisco pxGrid 用于将来自Cisco ISE会话目录区分上下文的信息共享给Cisco自适应安全设备 (ASA)。此 pxGrid 框架还可用于在节点之间交换策略和配置数据，例如在Cisco ISE和第三方供应商之间共享标签和策略对象，以及交换威胁信息等非Cisco ISE相关信息。

相关主题

分布式思科 ISE 部署中的角色，第 32 页
管理节点，第 53 页
策略服务节点，第 60 页
监控节点，第 63 页
思科 pxGrid 节点，第 70 页
同步主要和辅助思科 ISE 节点，第 77 页

创建策略服务节点组，第 78 页
部署思科 pxGrid 节点，第 71 页
更改节点角色和服务，第 77 页
配置用于自动故障切换的监控节点，第 69 页

分析节点的设置

下表介绍“分析配置”(Profiling Configuration) 窗口上的字段，您可以使用此窗口为分析器服务配置探测功能。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **ISE 节点 (ISE Node)** > **编辑 (Edit)** > **分析配置 (Profiling Configuration)**。

表 *162:* 分析节点的设置

字段名称	使用指南
NetFlow	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 NetFlow，以便接收从路由器发送的 NetFlow 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入从路由器接收 NetFlow 导出数据的 NetFlow 侦听器端口号。默认端口为 9996。
DHCP	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入 DHCP 服务器 UDP 端口号。默认端口为 67。
DHCP SPAN	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 DHCP，以便收集 DHCP 数据包。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。

字段名称	使用指南
HTTP	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。
RADIUS	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 RADIUS，以便收集 RADIUS 会话属性，以及来自已启用 IOS 传感器的设备的 Cisco设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
网络扫描 (NMAP) (Network Scan [NMAP])	启用此切换按钮可启用 NMAP 探测。
DNS	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 DNS，以便对 FQDN 执行 DNS 查找。以秒为单位输入**超时 (Timeout)** 期间。 注释 要使 DNS 探测功能在分布式部署中特定Cisco ISE 节点上运行，您必须启用以下任一探测功能：DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用上述另一个探测功能。
SNMP 查询 (SNMP Query)	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。为以下字段输入值：**重试次数 (Retries)**、**超时 (Timeout)**、**事件超时 (Event Timeout)**和可选的**说明 (Description)**。 注释 除配置 SNMP 查询探测功能之外，还必须在以下位置配置其他SNMP 设置：**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。当在网络设备上配置 SNMP 设置时，请确保在网络设备上全局启用 CDP 和 LLDP。

字段名称	使用指南
SNMP 陷阱 (SNMP Trap)	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 SNMP 陷阱探测，以便从网络设备接收链路接通、链路断开和MAC通知陷阱。为以下选项输入所需的值： • **链路陷阱查询 (Link Trap Query)**：启用此切换按钮可接收和解释通过 SNMP 陷阱接收的链路接通和链路断开通知。 • **MAC 陷阱查询 (MAC Trap Query)**：启用此切换按钮可接收和解释通过 SNMP 陷阱接收的 MAC 通知。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入要使用的主机UDP端口。默认端口为 162。
Active Directory	启用此切换按钮可扫描所定义的 Active Directory 服务器，以获取有关 Windows 用户的信息。 • **重新扫描前的天数 (Days before rescan)**：选择您希望经过多少天后再次进行扫描。
pxGrid	启用此切换按钮可允许Cisco ISE 通过 pxGrid 收集（配置文件）终端属性。

相关主题

思科 ISE 分析服务，第 603 页
分析服务使用的网络探测功能，第 606 页
在思科 ISE 节点中配置分析服务，第 605 页

证书存储设置

通过 Certificate Store 页面，您可以在Cisco ISE 中配置可用于身份验证的证书。

自签证书设置

下表介绍“生成自签证书”(Generate Self Signed Certificate) 页面上的字段。您可以通过此页面为节点间通信、EAP-TLS 身份验证、Cisco ISE Web 门户创建系统证书以及与 pxGrid 控制器通信。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)** > **生成自签名证书 (Generate Self Signed Certificate)**。

表 *163:* 自签证书设置

字段名称	使用指南
选择节点 (Select Node)	（必填）您要生成系统证书的节点。
公共名称 (CN) (Common Name [CN])	（如果您不指定 SAN，则此字段必填）默认情况下，Common Name 为您要生成自签证书的 ISE 节点的完全限定域名。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
主体可选名称 (SAN) (Subject Alternative Name [SAN])	与该证书关联的 IP 地址、DNS 名称或统一资源标识符 (URI)。
密钥类型 (Key Type)	指定要用于创建公共密钥的算法：RSA 或 ECDSA。

字段名称	使用指南
密钥长度 (Key Length)	指定公共密钥的位大小。以下选项可用于 RSA： • 512 • 1024 • 2048 • 4096 以下选项可用于 ECDSA： • 256 • 384 注释 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。 如果您计划获得公共 CA 签名的证书或将思科 ISE 部署为符合 FIPS 的策略管理系统，请选择 2048。
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。
过期 TTL (Expiration TTL)	指定证书到期之前的天数。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，Cisco ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
允许通配符证书 (Allow Wildcard Certificates)	如果要生成自签名通配符证书，请选中此复选框。通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。

字段名称	使用指南
使用情况 (Usage)	选择应使用此系统证书的服务： • **管理 (Admin)**：用于确保与部署中的管理员门户和 ISE 节点之间安全通信的服务器证书。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL/TLS 隧道的身份验证的服务器证书。 • **RADIUS DTLS**：用于 RADIUS DTLS 身份验证的服务器证书。 • **pxGrid**：用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务器证书。 • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **门户 (Portal)**：用于确保与所有Cisco ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书，第 138 页
查看系统证书，第 139 页
生成自签证书，第 142 页

证书签名请求设置

通过Cisco ISE，只需一个请求即可从管理员门户为部署中的所有节点生成 CSR。此外，还可以选择为部署中的单个节点或多个两个节点生成 CSR。如果选择为单个节点生成 CSR，则 ISE 会自动在证书使用者的 CN= 字段中替换特定节点的完全限定域名 (FQDN)。如果选择在证书的“主体可选名称 (SAN)”(Subject Alternative Name (SAN)) 字段中包含某个条目，则除了其他 SAN 属性之外，还必须输入 ISE 节点的 FQDN。如果选择为部署中的所有节点生成 CSR，请选中“允许通配符证书”(Allow Wildcard Certificates) 复选框，然后在 SAN 字段（“DNS 名称”(DNS name)）中输入通配符 FQDN 符号，例如，*.amer.example.com。如果计划对 EAP 身份验证使用证书，请不要在 CN= 字段中输入通配符值。

通过使用通配符证书，不再需要为每个Cisco ISE 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的多个两个节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个Cisco ISE 节点分配唯一服务器证书的安全性低。

下表列出 Certificate Signing Request (CSR) 页面中的字段，可以使用此页面生成可由证书颁发机构 (CA) 签名的 CSR。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书签名请求 (Certificate Signing Request)**。

表 *164:* 证书签名请求设置

字段	使用指南
证书将用于 **(Certificate(s) will be used for)**	

字段	使用指南
	选择即将对其使用证书的服务： **思科 ISE 身份证书** • **多用途 (Multi-Use)**：用于多种服务（管理员、EAP-TLS 身份验证、pxGrid 和门户）。多用途证书同时使用客户端和服务器密钥用法。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) • **管理 (Admin)** - 用于服务器身份验证（以确保与管理员门户之间的安全通信，以及部署中 ISE 节点之间的安全通信）。签名 CA 的证书模板通常称为 Web 服务器证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **EAP 身份验证 (EAP Authentication)**：用于服务器身份验证。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 注释 EAP-TLS 客户端证书需要使用数字签名密钥。 • **RADIUS DTLS**：用于 RADIUS DTLS 服务器身份验证。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **ISE 消息服务 (ISE Messaging Service)**：用于“经Cisco ISE 消息传递的系统日志”功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **门户 (Portal)**：用于服务器身份验证（以确保与所有 ISE Web 门户之间的

字段	使用指南
	安全通信）。签名CA的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **pxGrid** - 同时用于客户端和服务器身份验证（以确保 pxGrid 客户端与服务器之间的安全通信）。签名CA的证书模板通常称为计算机证书模板。此模板具有以下属性： • **Key Usage (密钥使用)**：数字签名（签名） • **Extended Key Usage (扩展密钥使用)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **Key Usage (密钥使用)**：数字签名（签名） • **扩展密钥使用 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 注释 建议您不要将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符。如果将包含值 2.5.29.37.0 的证书用于“扩展密钥使用”(Extended Key Usage) 属性中的任意用途对象标识符，系统会将此证书视为无效，并显示以下错误消息： `source=local type=fatal message="unsupported certificate"` **思科 ISE 证书颁发机构颁发的证书**

字段	使用指南
	• **ISE 根 CA (ISE Root CA) -**（仅适用于内部 CA 服务）用于重新生成整个内部 CA 证书链，包括主 PAN 上的根 CA 和 PSN 上的辅助 CA。 • **ISE 中间 CA (ISE Intermediate CA)**：（仅适用于当 ISE 用作外部 PKI 的中间 CA 时的内部 CA 服务）用于在主 PAN 上生成中间 CA 证书，在 PSN 上生成从属 CA 证书。签名 CA 的证书模板通常称为辅助证书颁发机构。此模板具有以下属性： • **基本约束 (Basic Constraints)**：关键、是证书颁发机构 • **密钥使用 (Key Usage)**：证书签名、数字签名 • **扩展密钥使用 (Extended Key Usage)**：OCSP 签名 (1.3.6.1.5.5.7.3.9) • **更新 ISE OCSP 响应方证书 (Renew ISE OCSP Responder Certificates)**：（仅适用于内部 CA 服务）用于更新整个部署的 ISE OCSP 响应方证书（不是证书签名请求）。出于安全原因，建议您每六个月更新一次 ISE OCSP 响应方证书。
允许通配符证书 (Allow Wildcard Certificates)	选中此复选框以在 CN 中和/或证书的 SAN 字段的 DNS 名称中使用通配符 (*)。如果选中此复选框，系统会自动选择部署中的所有节点。必须在最左侧的标签位置使用星号 (*) 通配符。如果使用通配符证书，我们建议您对域名空间进行分区以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，可能会导致安全问题。
为这些节点生成 CSR (Generate CSRs for these Nodes)	选中要为其生成证书的节点旁边的复选框。要为部署中的选定节点生成CSR，必须取消 Allow Wildcard Certificates 选项。
公共名称 (CN) (Common Name [CN])	默认情况下，公用名是您正为其生成 CSR 的 ISE 节点的 FQDN。$FQDN$ 表示ISE 节点的FQDN。当为部署中的多个节点生成CSR时，CSR 中的Common Name 字段会替换为各个 ISE 节点的 FQDN。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。

字段	使用指南
主体可选名称 (SAN) (Subject Alternative Name [SAN])	“IP 地址”(IP address)、“DNS 名称”(DNS name)、“统一资源标识符”(Uniform Resource Identifier, URI) 或与证书关联的“目录名称”(Directory Name)。 • **DNS 名称 (DNS name)**：如果选择“DNS 名称”(DNS name)，请输入 ISE 节点的完全限定域名。如果已启用 Allow Wildcard Certificates 选项，请指定通配符符号（域名前的星号和句号）。例如：*.amer.example.com。 • **IP 地址 (IP address)**：将与证书关联的 ISE 节点的 IP 地址。 • **统一资源标识符 (Uniform Resource Identifier)**：您希望与证书关联的 URI。 • **目录名称 (Directory Name)**：根据 RFC 2253 定义的可区分名称 (DN) 的字符串表示。使用逗号 (,) 隔开多个 DN。对于“dnQualifier”RDN，避免使用逗号而是使用反斜杠“\”作为分隔符。例如，CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
密钥类型 (Key Type)	指定要用于创建公共密钥的算法：RSA 或 ECDSA。
密钥长度 (Key Length)	指定公共密钥的位大小。 以下选项可用于 RSA： • 512 • 1024 • 2048 • 4096 以下选项可用于 ECDSA： • 256 • 384 **注释** 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。 如果计划获取公共的 CA 签名证书，请选择 2048 或更大长度。
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。

相关主题

证书签名请求，第 160 页
创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构，第 160 页
将 CA 签名的证书与 CSR 绑定，第 160 页

颁发及撤销的证书

下表介绍颁发及撤销的证书概述页面中的字段。您的部署中的PSN节点会向终端发出证书。此页面向您提供关于您的部署中每个PSN节点发出的终端证书的信息。要查看此处窗口，请点击**菜单 (Menu)**图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificate)** > **概述 (Overview)**。

表 *165:* 颁发及撤销的证书

字段	使用指南
Node name	发出证书的策略服务节点 (PSN) 的名称。
颁发的证书 (Certificates Issued)	PSN 节点发出的终端证书的数量。
撤销的证书 (Certificates Revoked)	已吊销的证书的数量（已由 PSN 节点发出的证书）。
证书请求 (Certificates Requests)	PSN 节点处理的基于证书的身份验证请求数量。
失败的证书 (Certificates Failed)	PSN 节点处理的失败身份验证请求数量。

相关主题

已颁发的证书，第 185 页
用户和终端证书续订，第 170 页
配置思科 ISE 以使用证书对个人设备进行身份验证，第 189 页
将思科 ISE 配置为允许用户续订证书，第 171 页
吊销终端证书，第 206 页

证书定期检查设置

Cisco ISE 定期检查证书撤销列表 (CRL)。使用此页面，您可以对Cisco ISE 进行配置以对照自动下载的 CRL 检查正在进行的会话。您可以指定一天中的某个时间作为 CRL 或 OCSP 每天应当开始检查的时间和Cisco ISE 需要等待的时间间隔（按小时计），在此间隔之后再次对 OCSP 服务器或 CRL 进行检查。

下表列出“证书定期检查设置”(Certificate Periodic Check Settings) 窗口中的字段，可以使用该窗口来指定检查证书（OCSP 或 CRL）状态时的时间间隔。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书定期检查设置 (Certificate Periodic Check Settings)**。

表 *166:* 证书定期检查设置

字段名称	使用指南
证书检查设置	
“对照自动撤销的 CRL 检查正在进行的会话”**(Check ongoing sessions against automatically retrieved CRL)**	如果您希望Cisco ISE 对照自动下载的 CRL 检查正在进行的会话，选中此复选框。
CRL/OCSP 定期检查证书	
首先检查	指定一天中的某个时间作为 CRL 或 OCSP 每天应当开始检查的时间。输入 00:00 和 23:59 小时之间的数值
检查每	指定Cisco ISE 需要等待的时间间隔（按小时计），在此间隔之后再次对 CRL 或 OCSP 服务器进行检查。

相关主题

OCSP 服务，第 206 页
添加 OCSP 客户端配置文件，第 208 页

系统证书导入设置

下表介绍可用于导入服务器证书的“导入系统证书”(Import System Certificate) 窗口上的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)** > **导入 (Import)**。

表 *167:* 系统证书导入设置

字段名称	说明
选择节点 (Select Node)	（必填）选择您要导入系统证书的Cisco ISE 节点。
证书文件 (Certificate File)	（必填）点击**浏览 (Browse)**，从本地系统中选择证书文件。
私钥文件 (Private Key File)	（必填）点击 **浏览 (Browse)** 选择私钥文件。
密码 (Password)	（必填）输入密码以解密私钥文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，Cisco ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。

字段名称	说明
允许通配符证书 (Allow Wildcard Certificates)	如果要导入通配符证书，请选中此复选框。通配符证书使用通配符表示法（在域名前使用一个星号和句点）并且允许在组织中的多个主机之间共享该证书。 如果选中此复选框，Cisco ISE 会将此证书导入到部署中的所有其他节点。
验证证书扩展名 (Validate Certificate Extensions)	如果希望Cisco ISE 验证证书扩展，请选中此复选框。如果选中此复选框，并且要导入的证书包含 CA 标志设为 true 的基本限制扩展，请确保密钥用法扩展存在，并且设置了 keyEncipherment 位和/或 keyAgreement 位。
使用情况 (Usage)	选择应使用此系统证书的服务： • **管理员 (Admin)**：用于确保与部署中的管理员门户和 ISE 节点之间安全通信的服务器证书 **注释** 在主 PAN 上更改管理员角色证书时会在所有其他节点上重新启动服务。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL/TLS 隧道的身份验证的服务器证书 • **RADIUS DTLS**：用于 RADIUS DTLS 身份验证的服务器证书 • **pxGrid**：用于确保pxGrid客户端和服务器之间的安全通信的客户端和服务器证书。 • **ISE 消息服务 (ISE Messaging Service)**：用于**经思科 ISE 消息传递的系统日志 (Syslog Over Cisco ISE Messaging)** 功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **SAML**：用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 • **门户 (Portal)**：用于确保与所有Cisco ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书，第 138 页
查看系统证书，第 139 页
导入系统证书，第 140 页

受信任证书库页面

下表介绍“受信任证书库页面”(Trusted Certificates Store) 窗口上的字段，您可以使用此页面查看添加到管理节点的证书。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

表 *168:* 证书库页面

字段名称	使用指南
友好名称 **(Friendly Name)**	显示证书的名称。
状态 **(Status)**	“启用”(Enabled) 或“禁用”(Disabled)。如果选择“禁用”(Disabled)，ISE 将不使用此证书建立信任。
信任范围 **(Trusted for)**	显示使用此证书的服务。
颁发给 **(Issued To)**	证书使用者的通用名称 (CN)。
颁发者 **(Issued By)**	证书颁发者的通用名称 (CN)。
生效日期 **(Valid From)**	“开始时间”证书属性。
到期日期 **(Expiration Date)**	“截止时间”证书属性。
到期状态 **(Expiration Status)**	提供有关证书到期状态的信息。此列显示五个图标和提示消息类别： • 绿色：距到期还有 90 天以上 • 蓝色：距到期还有 90 天或更短 • 黄色：距到期还有 60 天或更短 • 橙色：距到期还有 30 天或更短 • 红色：已到期

相关主题

受信任证书库，第 147 页
查看受信任证书库证书，第 150 页
更改受信任证书库中的证书状态，第 151 页
在受信任的证书库中添加证书，第 151 页

编辑证书设置

下表介绍了“证书存储区编辑证书”(Certificate Store Edit Certificate) 窗口上的字段，可以使用此窗口编辑证书颁发机构 (CA) 证书属性。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **证书 (Certificate)** > **编辑 (Edit)**。

表 *169:* 证书库编辑设置

字段名称	使用指南
证书颁发者 (Certificate Issuer)	
友好名称 (Friendly Name)	输入证书的友好名称。
状态 (Status)	选择“启用”(Enabled) 或“禁用”(Disabled)。如果选择“禁用”(Disabled)，ISE 将不使用此证书建立信任。
说明	输入可选的说明。
使用情况 (Usage)	
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您想要使用此证书验证服务器证书（从其他 ISE 节点或 LADP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅适用于选中“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框的情况）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部Cisco服务，请选中此复选框。
证书状态验证 (Certificate Status Validation)	ISE 支持使用两种方法检查特定 CA 颁发的客户端或服务器证书的吊销状态。第一种方法是使用在线证书状态协议 (OCSP) 验证证书，其将向 CA 维护的 OCSP 服务发送请求。第二种方法是按照从 CA 下载至 ISE 的证书吊销列表 (CRL) 验证证书。可以同时启用这两种方法，在这种情况下首先使用 OCSP 方法，只有在无法确定证书状态时，才会使用 CRL 方法。
验证 OCSP 服务 (Validate Against OCSP Service)	选中此复选框以按照 OCSP 服务验证证书。您必须先创建 OCSP 服务才能选中此复选框。
如果 OCSP 返回未知状态则拒绝请求 (Reject the request if OCSP returns UNKNOWN status)	如果 OCSP 无法确定证书状态，则选中此复选框以拒绝请求。在选中此复选框的情况下，如果 OCSP 服务返回未知状态值，此服务将导致 ISE 拒绝当前评估的客户端或服务器证书。

字段名称	使用指南
OCSP 响应器无法访问时拒绝请求 (Reject the request if OCSP Responder is unreachable)	选中此复选框供 ISE 在 OCSP 响应器无法访问时拒绝请求。
下载 CRL (Download CRL)	选中此复选框以使Cisco ISE 下载 CRL。
CRL 分类的 URL (CRL Distribution URL)	输入用于从 CA 下载 CRL 的 URL。如果在证书颁发机构证书中指定了URL，则系统会自动填写此字段。URL 必须以“http”、“https”或“ldap”开头。
检索 (Retrieve CRL)	可以自动或定期下载 CRL。请配置下载时间间隔。
如果下载失败，请稍候 (If download failed, wait)	配置在Cisco ISE 再次尝试下载 CRL 之前等待的时间间隔。
如果 CRL 没有收到，绕过此 CRL 验证 (Bypass CRL Verification if CRL is not Received)	选中此复选框，以使系统在收到CRL之前接受客户端请求。如果取消选中此复选框，Cisco ISE 会拒绝使用选定CA签名的证书的所有客户端请求，直到收到 CRL 文件为止。
忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)	如果您希望Cisco ISE 忽略开始日期和到期日期并继续使用非活动或已过期 CRL 以及根据 CRL 内容允许或拒绝 EAP-TLS 身份验证，请选中此复选框。 如果您希望Cisco ISE 在 Effective Date 字段指定的开始日期和 Next Update 字段指定的到期日期检查CRL 文件，请取消选中此复选框。如果CRL尚未激活或已到期，Cisco ISE 会拒绝使用此 CA 签名的证书的所有身份验证。

相关主题

受信任证书库，第 147 页
编辑受信任证书，第 151 页

受信任证书导入设置

下表说明了“受信任证书导入”(Trusted Certificate Import) 窗口上的字段，可以使用此窗口将证书颁发机构 (CA) 证书添加到Cisco ISE。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)**。

表 *170:* 受信任证书导入设置

字段名称	说明
证书文件 (Certificate File)	点击**浏览 (Browse)** 从运行浏览器的计算机选择证书文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果不指定名称，Cisco ISE 会自动按照 <通用名称>#<颁发者>#<nnnnn> 的格式创建名称，其中 <nnnnn> 为唯一的五位数编号。
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您希望将此证书用于验证服务器证书（从其他 ISE 节点或 LDAP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅在选中了“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部Cisco服务，请选中此复选框。
验证证书扩展名 (Validate Certificate Extensions)	（仅适用于同时选中“信任客户端身份验证和系统日志”(Trust for client authentication and Syslog) 选项和“证书扩展上启用验证”(Enable Validation of Certificate Extensions) 选项的情况下）确保有“keyUsage”扩展并且设置了“keyCertSign”位，而且有将 CA 标志设置为 true 的基本限制扩展。
说明	输入可选的说明。

相关主题

受信任证书库，第 147 页
证书链导入，第 156 页
将根证书导入受信任证书库，第 154 页

OCSP 客户端配置文件设置

下表介绍了“OCSP 客户端配置文件”(OCSP Client Profile) 窗口上的字段，可以使用此窗口配置 OCSP 客户端配置文件。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理**

(Administration) > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **OCSP 客户端配置文件 (OCSP Client Profile)**。

表 *171: OCSP* 客户端配置文件设置

字段名称	使用指南
名称 (Name)	OCSP 客户端配置文件的名称。
说明	输入可选的说明。
配置 OCSP 响应器 (Configure OCSP Responder)	
启用辅助服务器 (Enable Secondary Server)	选中此复选框来以启用高可用性辅助 OCSP 服务器。
始终先访问主服务器 (Always Access Primary Server First)	使用此选项以在尝试移至辅助服务器之前先检查主要服务器。即使之前已检查主要服务器并且发现主服务器无响应，Cisco ISE 在移至辅助服务器之前仍会尝试向主要服务器发送请求。
在 *n* 分钟后回退至主服务器 (Fallback to Primary Server After Interval n Minutes)	当您希望Cisco ISE 移至辅助服务器，然后再回退到主服务器时，请使用此选项。在这种情况下，系统将跳过所有其他请求，并按照该文本框中配置的时间使用辅助服务器。允许的时间范围是 1 至 999 分钟。
主服务器和辅助服务器 (Primary and Secondary Servers)	
URL	输入主要和/或辅助 OCSP 服务器的 URL。
启用 Nonce 扩展支持 (Enable Nonce Extension Support)	您可以配置一个作为 OCSP 请求的一部分发送的 Nonce。Nonce 会在 OCSP 请求中包含一个伪随机数。系统会验证在响应中接收的数值是否与请求中包含的此数相同。此选项可确保重放攻击无法利用旧通信数据。
验证响应签名 (Validate Response Signature)	OCSP 响应器用以下一个证书为响应签名： • CA 证书 • 与 CA 证书不同的证书 为了使Cisco ISE 验证响应签名，OCSP 响应器需要连同该证书一起发送响应，否则响应验证会失败，而且证书状态不可靠。根据 RFC，OCSP 可以使用不同的证书给响应签名。只要 OCSP 发送给响应签名的证书以供Cisco ISE 进行验证，就会如此。如果 OCSP 使用Cisco ISE 中未配置的其他证书给响应签名，响应验证将失败。
使用授权信息访问 (AIA) 中指定的 OCSP URL。(Use OCSP URLs specified in Authority Information Access [AIA])	点击单选按钮以使用授权信息访问扩展名中指定的 OCSP URL。

字段名称	使用指南
响应缓存 (Response Cache)	
缓存条目生存时间 *n* 分钟 (Cache Entry Time To Live n Minutes)	以分钟为单位输入缓存项目在多长时间之后过期。来自 OCSP 服务器的每个响应都有一个 nextUpdate 值。此值显示服务器上接下来将于何时更新证书的状态。缓存 OCSP 响应时，系统会比较两个值（一个是来自配置的值，另一个是来自响应的值），系统会按照这两个值中最低的值将响应缓存相应的时间。如果 nextUpdate 值为 0，则根本不缓存响应。Cisco ISE 将 OCSP 响应缓存所配置的时间。缓存不复制，也不是持久性的，所以当Cisco ISE 重新启动时，系统会清除缓存。使用 OCSP 缓存是为了保持 OCSP 响应以及出于以下原因： • 减少网络流量和降低 OCSP 服务器对已知证书带来的负载 • 通过缓存已知证书状态提高Cisco ISE 性能 默认情况下，内部 CA 的 OCSP 客户端配置文件的缓存设置为 2 分钟。如果终端在第一次身份验证后 2 分钟内进行第二次验证，将使用 OCSP 缓存，而不查询 OCSP 响应器。如果终端证书在缓存期间内撤销，将使用之前 OCSP 的状态良好 (Good)，身份验证成功。将缓存设置为 0 分钟可阻止所有响应被缓存。此选项可提高安全性，但会降低身份验证性能。
清空缓存 (Clear Cache)	点击**清空缓存 (Clear Cache)** 以清除连接至 OCSP 服务的所有证书颁发机构的条目。 在部署中，**清空缓存 (Clear Cache)** 与所有节点交互并执行此操作。此机制可更新部署中的每个节点。

相关主题

OCSP 服务，第 206 页
思科 ISE CA 服务在线证书状态协议响应器，第 206 页
OCSP 证书状态值，第 207 页
OCSP 高可用性，第 207 页
OCSP 故障，第 207 页
OCSP 统计计数器，第 210 页
添加 OCSP 客户端配置文件，第 208 页

内部 CA 设置

下表介绍“内部 CA 设置 (Internal CA Settings)”窗口中的字段。您可以查看内部 CA 设置和从该页面禁用内部 CA 服务。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **内部 CA 设置 (Internal CA Settings)**。

表 *172:* 内部 *CA* 设置

字段名称	使用指南
禁用证书权限 (Disable Certificate Authority)	点击此按钮以禁用内部 CA 服务。
主机名 (Host Name)	运行 CA 服务的Cisco ISE 节点的主机名。
相关角色 (Personas)	在运行 CA 服务的节点上启用的Cisco ISE 节点角色。例如管理角色、策略服务角色等。
角色 [Role(s)]	运行 CA 服务的Cisco ISE 节点承担的职责。例如，独立、主要或辅助职责。
CA、EST 和 OCSP 响应方状态 (CA, EST & OCSP Responder Status)	启用或禁用
OCSP 响应者 URL (OCSP Responder URL)	Cisco ISE 节点用于访问 OCSP 服务器的 URL。
SCEP URL	Cisco ISE 节点用来访问 OCSP 服务器的 URL。

相关主题

思科 ISE CA 服务，第 174 页
配置思科 ISE 以使用证书对个人设备进行身份验证，第 189 页

证书模板设置

下表介绍“CA 证书模板”(CA Certificate Template) 窗口中的字段，您可以使用此窗口定义将由客户端调配策略使用的 SCEP RA 配置文件。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统证书 (System Certificates)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)** > **添加 (Add)**。

注释 在证书模板字段（“组织单位”[Organizational Unit]、“企业”[Organization]、“城市”[City]、“省”[State] 和“国家/地区”[Country]）中不支持 UTF-8 字符。如果在证书模板中使用 UTF-8 字符，则证书调配将会失败。

表 *173:* 证书模板设置

字段名称	使用指南
名称	（必填）输入证书模板的名称。例如，Internal_CA_Template。

字段名称	使用指南
说明	（可选）输入说明。
Common Name (CN)	（仅显示）公用名自动填充为用户名。
Organizational Unit (OU)	组织单位名称。例如，Engineering。
Organization (O)	组织名称。例如，Cisco。
City (L)	（请勿缩写）城市名称。例如，圣何塞。
State (ST)	（请勿缩写）省/自治区/直辖市名称。例如，加州。
Country (C)	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
Subject Alternative Name (SAN)	（仅显示）终端的 MAC 地址。
密钥类型 **(Key Type)**	RSA 或 ECC
Key Size	（只有当您选择 RSA 时适用）指定密钥大小为 1024 或更大数字。
曲线类型	（只有当您选择 ECC 时适用）指定曲线类型（默认值为 P-384）。
SCEP RA Profile	选择 ISE Internal CA 或您已创建的外部 SCEP RA 配置文件。
Valid Period	输入证书的到期天数。
扩展密钥使用	
客户端身份验证	如果您要使用此证书用于客户端身份验证，请选中此复选框。
服务器身份验证	如果您要使用此证书用于服务器身份验证，请选中此复选框。

相关主题

证书模板，第 183 页
证书模板扩展名，第 184 页
配置思科 ISE 以使用证书对个人设备进行身份验证，第 189 页
为 pxGrid 控制器部署思科 ISE CA 证书，第 184 页
在授权策略条件中使用证书模板，第 184 页

日志记录设置

下面的小节解释了如何配置调试日志的严重性、创建外部日志目标，并使Cisco ISE 能够将日志消息发送到这些外部日志目标。

远程日志记录目标设置

下表介绍“远程日志记录目标”(Remote Logging Targets) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

表 *174:* 远程日志记录目标设置

字段名称	使用指南
名称 (Name)	输入新目标的名称。
目标类型 (Target Type)	选择目标类型。默认情况下设置为 UDP Syslog。
说明	输入新目标的简短说明。
IP 地址 (IP Address)	输入要存储日志的目标计算机的 IP 地址或主机名。 思科 ISE 支持 IPv4 和 IPv6 格式的日志记录。
端口 (Port)	输入目标计算机的端口号。
设备代码 (Facility Code)	选择要用于日志记录的系统日志设备代码。有效选项为 Local0 至 Local7。
最大长度 (Maximum Length)	输入远程日志目标消息的最大长度。有效选项为 200 至 1024 字节。
服务器关闭时缓冲消息 (Buffer Message When Server is Down)	如果希望Cisco ISE 在 TCP 系统日志目标和安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。Cisco ISE 会在连接恢复时重新尝试将消息发送到目标。连接恢复后，消息按从最旧到最新的顺序进行发送，并且缓冲消息始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
缓冲区大小 (MB) (Buffer Size [MB])	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。

字段名称	使用指南
重新连接超时（秒）**(Reconnect Timeout [Sec])**	输入时间（以秒为单位），提及在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
选择 CA 证书 **(Select CA Certificate)**	选择客户端证书。
忽略服务器证书验证 **(Ignore Server Certificate Validation)**	如果希望 ISE 忽略服务器证书身份验证并接受任何系统日志服务器，请选中此复选框。

相关主题

思科 ISE 日志记录机制，第 249 页
思科 ISE 系统日志，第 250 页
远程系统日志消息格式
思科 ISE 消息目录，第 252 页
集合过滤器，第 253 页
事件抑制绕行过滤器，第 254 页
配置远程系统日志收集位置，第 250 页
配置集合过滤器，第 254 页

日志记录类别设置

下表介绍了**日志记录类别 (Logging Categories)** 窗口中的字段，可以使用此窗口配置日志严重性级别，并为要存储的所选类别的日志选择日志记录目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

表 *175:* 日志记录类别设置

字段名称	使用指南
名称 **(Name)**	显示日志记录类别的名称。

字段名称	使用指南
日志严重性级别 **(Log Severity Level)**	允许您从以下选项中选择诊断日志记录类别的严重性级别： • **严重 (FATAL)**：紧急情况。此选项意味着无法使用Cisco ISE，并且必须立即采取操作。 • **错误 (ERROR)**：此选项表示严重或错误情况。 • **警告 (WARN)**：此选项表示正常但值得注意的情况。这是默认情况。 • **信息 (INFO)**：此选项表示信息性消息。 • **调试 (DEBUG)**：此选项表示诊断错误消息。
本地日志记录 **(Local Logging)**	选中此复选框可为本地节点上的类别启用日志记录事件。
目标 **(Targets)**	允许使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 框之间转移目标来更改类别的目标。**可用 (Available)** 框包含本地（预定义）和外部（用户定义）的现有日志记录目标。初始为空的**所选 (Selected)** 框包含特定类别的选定目标。

相关主题

远程系统日志消息格式
思科 ISE 消息代码，第 252 页
配置远程系统日志收集位置，第 250 页
设置消息代码的严重性级别，第 252 页

维护设置

使用备份、恢复和数据清除功能，这些页面可帮助您管理数据。

存储库设置

下表介绍了**存储库列表 (Repository List)** 页面上的字段，可以使用此页面创建存储备份文件的存储库。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

表 *176:* 存储库设置

字段	使用指南
存储库 (Repository)	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。
协议 (Protocol)	从可用协议中选择一个您想要使用的协议。
服务器名称 (Server Name)	（对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段）输入您想要在其上创存储库的服务器的主机名或 IP 地址（IPv4 或 IPv6）。 注释 如果要添加使用 IPv6 地址的存储库，请确保 ISE eth0 接口配置了 IPv6 地址。
路径 (Path)	输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。 此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。
启用 PKI 身份验证 (Enable PKI authentication)	（可选；仅适用于 SFTP 存储库）如果要在 SFTP 存储库中启用 RSA 公钥身份验证，请选中此复选框。
用户名 (User Name)	（对于 FTP、SFTP 为必填字段）输入对指定服务器拥有写入权限的用户名。只允许使用字母数字字符。
密码 (Password)	（对于 FTP、SFTP 为必填字段）输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、|、@、#、$、%、^、&、*、(、)、+、和 =。

相关主题

备份和恢复存储库，第 228 页
创建存储库，第 229 页

按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup & Restore)**。

表 *177:* 按需备份设置

字段名称	使用指南
类型	选择以下其中一个选项： • **配置数据备份 (Configuration Data Backup)**：包含应用特定配置数据和Cisco ADE 操作系统配置数据 • **运行数据备份 (Operational Data Backup)**：包含监控和故障排除数据
备份名称 (Backup Name)	输入备份文件的名称。
存储库名称 (Repository Name)	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
加密密钥 (Encryption Key)	此密钥用于加密和解密备份文件。

相关主题

备份数据类型，第 227 页
按需备份和计划备份，第 232 页
备份历史记录，第 237 页
备份失败，第 237 页
思科 ISE 恢复操作，第 238 页
导出身份验证和授权策略配置，第 244 页
在分布式环境中同步主节点和辅助节点，第 245 页
执行按需备份，第 232 页

计划备份设置

下表介绍“定期备份”(Scheduled Backup) 窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

表 *178:* 计划备份设置

字段名称	使用指南
类型 (Type)	选择以下其中一个选项： • **配置数据备份 (Configuration Data Backup)**：包含应用特定配置数据和Cisco ADE 操作系统配置数据 • **运行数据备份 (Operational Data Backup)**：包含监控和故障排除数据
名称 (Name)	输入备份文件的名称。您可以输入您所选的描述性名称。Cisco ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup) 列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 **kron** 作业。
说明	输入对备份的说明。
存储库名称 (Repository Name)	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
加密密钥 (Encryption Key)	输入用于加密和解密备份文件的密钥。
计划选项	选择计划备份的频率并相应地填写其他选项。

相关主题

备份数据类型，第 227 页
按需备份和计划备份，第 232 页
备份历史记录，第 237 页
备份失败，第 237 页
思科 ISE 恢复操作，第 238 页
导出身份验证和授权策略配置，第 244 页
在分布式环境中同步主节点和辅助节点，第 245 页
使用 CLI 备份，第 237 页
计划备份，第 235 页

计划策略导出设置

下表对**计划策略导出 (Schedule Policy Export)** 窗口中的字段进行了说明。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)** > **策略导出 (Policy Export)**。

表 *179:* 计划策略导出设置

字段名称	使用指南
加密 (Encryption)	
加密密钥 (Encryption Key)	输入用于加密和解密导出数据的密钥。仅当您选择**使用加密密钥导出 (Export with Encryption Key)** 选项时，才会启用此字段。
目标 (Destination)	
下载文件到本地计算机 (Download file to local computer)	可以让您将策略导出文件下载到本地系统。
通过邮件将文件发送到 (Email file to)	您可输入多个邮件地址，用逗号分隔。
存储库 (Repository)	选择要将策略数据导出到的存储库。无法在此处输入存储库名称。只能从下拉列表选择一个可用存储库。确保在计划策略导出之前创建存储库。
立即导出 (Export Now)	点击此选项可将数据导出到本地计算机或作为电子邮件附件发送。您无法导出到存储库；只能计划存储库导出。
时间表 (Schedule)	
计划选项	选择导出计划的频率，并相应地输入其他详细信息。

管理员访问设置

您可以通过这些页面为管理员配置访问设置。

管理员密码策略设置

下表介绍了“管理员密码策略”(Administrator Password Policy) 窗口中的字段，可以使用此窗口定义管理员密码应满足的条件。。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。

表 *180:* 管理员密码策略设置

字段名称	使用指南
最小长度 **(Minimum Length)**	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。
密码不得包含 **(Password must not contain)**	管理员名称或其反向顺序的字符 **(Admin name or its characters in reverse order)**：选中此复选框可限制使用管理员用户名或其反向顺序的字符。
	“**cisco**”或其反向顺序的字符 **("cisco" or its characters in reverse order)**：选中此复选框可限制使用单词“cisco”或其反向顺序的字符。
	此单词或其反向顺序的字符 **(This word or its characters in reverse order)**：选中此复选框可限制使用您定义的任何单词或其反向顺序的字符。
	连续重复四次或以上的字符 **(Repeated characters four or more times consecutively)**：选中此复选框可限制使用连续重复四次或以上的字符。
	字典单词、其反向顺序的字符或其替换为其他字符的字母 **(Dictionary words, their characters in reverse order or their letters replaced with other characters)**：选中此复选框可限制使用字典单词、其反向顺序的字符或其替换为其他字符的字母。 不允许使用“$”替代“s”、“@”替代“a”、“0”替代“o”、“1”替代“l”、“!”替代“i”、“3”替代“e”。例如 Pa$$w0rd • 默认字典 **(Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。 默认情况下，此选项已选中。 • 自定义字典 **(Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**浏览**选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。

字段名称	使用指南
密码必须包含每个所选类型的至少一个字符 **(Password must contain at least one character of each of the selected types)**	指定管理员密码必须包含从以下选项中选择的类型的至少一个字符： • 小写字母字符 • 大写字母字符 • 数字字符 • 非字母数字字符
密码历史记录 **(Password History)**	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
密码有效期 **(Password Lifetime)**	指定以下选项来强制用户在经过指定时间段后更改密码： • “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。”(Time (in days) before the administrator account is disabled if the password is not changed.)（允许的范围是 0 至 2147483647 天。） • “禁用管理员帐户之前的提醒时间（按天计）。”(Reminder (in days) before the administrator account is disabled.)
显示网络设备敏感数据 **(Display Network Device Sensitive Data)**	
要求管理员密码 **(Require Admin Password)**	如果您希望管理员用户输入登录密码来查看网络设备敏感数据，例如共享密钥和密码，请选中此复选框。
密码缓存用于 **(Password cached for)**	在此段时间内，会对管理员用户输入的密码进行缓存。在此期间，如果管理员用户要查看网络设备敏感数据，系统不会再次提示输入密码。有效范围为 1 至 60 分钟。

相关主题

思科 ISE 管理员，第 3 页
创建新管理员，第 4 页

会话超时和会话信息设置

下表介绍**会话 (Session)** 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *181:* 会话超时和会话信息设置

字段名称	使用指南
会话超时 (Session Timeout)	
会话空闲超时 (Session Idle Timeout)	输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。
会话信息 (Session Info)	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后点击**失效 (Invalidate)**。

相关主题

管理员访问设置，第 212 页
配置管理员会话超时，第 216 页
终止活动管理会话，第 217 页

设置

通过这些页面，您可以配置各种服务的常规设置。

安全评估常规设置

下表介绍“终端安全评估常规设置”(Posture General Settings) 窗口中的字段，可以使用此窗口配置补救时间和终端安全评估状态等常规终端安全评估设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

常规终端安全评估设置

- **补救计时器 (Remediation Timer)**：输入开始补救前等待的时间。默认值为 4 分钟。有效范围为 1 至 300 分钟。
- **网络过渡延迟 (Network Transition Delay)**：以秒为单位输入时间值。默认值为 3 秒。有效范围为 2 至 30 秒。

- **默认终端安全评估状态 (Default Posture Status)**：选择“合规”(Compliant) 或“不合规”(Noncompliant)。在连接到网络时，非代理设备（诸如 Linux）会处于此状态。
- **自动关闭登录成功屏幕前等待 (Automatically Close Login Success Screen After)**：选中此复选框可在指定的时间过后自动关闭成功登录屏幕。可以配置计时器以自动关闭登录屏幕。有效范围为 0 至 300 秒。如果将时间设置为零，则客户端上的代理不会显示成功登录屏幕。
- **连续监控间隔 (Continuous Monitoring Interval)**：指定 AnyConnect 开始发送监控数据之前的时间间隔。对于应用和硬件条件，默认值为 5 分钟。
- **无代理终端安全评估客户端超时**：指定在终端安全评估检查被视为失败之前等待的时间。
- **每次运行后删除无代理插件 (Remove Agentless Plugin)**：启用此设置可在运行无代理终端安全评估后从客户端删除代理。我们强烈禁用此功能，以便下载的插件可以重复使用，直到有新版本可用。禁用此选项有助于减少网络流量。
- **隐身模式下的可接受使用策略 (Acceptable Use Policy)**：如果不符合贵公司的网络使用条款和条件，请在隐身模式下选择**阻止 (Block)** 以将客户端转移到不合规的终端安全评估状态。

安全评估租约

- **每当用户连接到网络时执行终端安全评估 (Perform posture assessment every time a user connects to the network)**：选择此选项可在用户每次连接网络时启动终端安全评估
- **每 n 天执行一次终端安全评估 (Perform posture assessment every n days)**：选择此选项可在指定天数过后启动终端安全评估，即使客户端的状态已评估为“合规”也是如此。
- **缓存最后已知终端安全评估合规状态 (Cache Last Known Posture Compliant Status)**：选中此复选框可使Cisco ISE 缓存终端安全评估的结果。默认情况下，此字段处于禁用状态。
- **最后已知终端安全评估合规状态 (Last Known Posture Compliant Status)**：仅当已选中**缓存最后已知终端安全评估合规状态 (Cache Last Known Posture Compliant Status)** 时，此设置才适用。Cisco ISE 会在此字段中指定的时间量内缓存终端安全评估结果。有效值为 1 到 30 天，或 1 到 720 小时，或 1 到 43200 分钟。

相关主题

安全评估服务
安全评估管理设置，第 952 页
安全评估租约，第 956 页
在思科 ISE 中启用安全评估会话服务
设定补救计时器，使客户端在指定时间内补救，第 954 页
设置网络转换延迟计时器，使客户端实现转换，第 955 页
将登录成功窗口设置为自动关闭，第 955 页
设置非代理设备的终端安全评估状态，第 955 页

重新进行安全评估配置设置

下表列出“终端安全再评估配置”(Posture Reassessment Configurations) 窗口中的字段，您可以使用此窗口配置终端安全再评估。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **重新评估 (Reassessments)**。

表 *182:* 重新进行安全评估配置设置

字段名称	使用指南
配置名称	输入 PRA 配置的名称。
配置说明	输入 PRA 配置的说明。
Use Reassessment Enforcement?	选中此复选框，将PRA配置应用到用户身份组。
Enforcement Type	选择要执行的操作： • **继续 (Continue)**：用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。 • **注销 (Logoff)**：如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。 • **补救 (Remediate)**：如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送 PRA 报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。 如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的RADIUS会话，才能再次布置客户端。 如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续”(Continue) 选项。用户可以继续停留在当前的网络中，不受任何限制。
Interval	输入第一次成功登录后在客户端上启动PRA的时间间隔分钟数。 默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。

字段名称	使用指南
Grace time	输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于PRA间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。 最小值为 5 分钟，最大值为 60 分钟。 注释 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。
选择用户身份组	为 PRA 配置选择唯一组或唯一组组合。
PRA configurations	显示现有的 PRA 配置以及关联到 PRA 配置的用户身份组。

相关主题

安全评估租约，第 956 页
定期重新评估，第 957 页
终端安全状态评估选项
安全评估补救选项，第 1002 页
安全评估的自定义条件，第 1002 页
自定义安全评估补救措施，第 1004 页
配置定期重新评估，第 957 页

安全评估可接受使用政策配置设置

下表介绍了“终端安全评估可接受使用策略配置”(Posture Acceptable Use Policy Configurations) 窗口中的字段，可以使用此窗口为终端安全评估配置可接受使用策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **可接受使用策略 (Acceptable Use Policy)**。

表 *183:* 安全评估 *AUP* 配置设置

字段名称	使用指南
配置名称	输入要创建的 AUP 配置的名称。
配置说明	输入要创建的 AUP 配置的说明。
“向代理用户显示 AUP”**(Show AUP to Agent users)**（仅适用于 **Windows**）	选中后，系统会在身份验证和终端安全评估成功后，向用户显示您的网络的网络使用条款和条件的链接。

字段名称	使用指南
为 AUP 消息使用 URL (Use URL for AUP message)	选中后，必须在“AUP URL”字段中输入 AUP 消息的 URL。
为 AUP 消息使用文件 (Use file for AUP message)	选中后，必须浏览至文件位置并以压缩格式上传文件。此文件必须在顶层包含 index.html。 除 index.html 文件以外，该 .zip 文件还可包含其他文件和子目录。这些文件可以使用 HTML 标签相互引用。
AUP URL	输入 AUP 的 URL，用户必须在身份验证和安全评估成功后访问该 URL。
AUP File	浏览至文件并将其上传到Cisco ISE 服务器。它应是压缩文件，并且应在顶层包含 index.html 文件。
选择用户身份组 (Select User Identity Groups)	针对 AUP 配置选择唯一用户身份组或用户身份组的唯一组合。 创建 AUP 配置时，请注意以下事项： • 安全评估 AUP 不适用于访客流程 • 两个配置不会共同具有任何用户身份组 • 如果您要使用用户身份组“Any”创建 AUP 配置，则要先删除所有其他 AUP 配置 • 如果使用用户身份组“Any”创建 AUP 配置，则无法使用唯一用户身份组或用户身份组的唯一组合创建其他 AUP 配置。要使用除 Any 以外的用户身份组创建 AUP 配置，请先删除具有用户身份组“Any”的现有 AUP 配置，或者使用唯一用户身份组或用户身份组的唯一组合更新具有用户身份组“Any”的现有 AUP 配置。
可接受使用策略配置 - 配置清单 (Acceptable use policy configurations—Configurations list)	列出现有 AUP 配置以及与 AUP 配置关联的最终用户身份组。

相关主题

安全评估服务

配置安全评估的可接受使用政策，第 963 页

EAP-FAST 设置

下表介绍“协议设置”(Protocol Settings) 窗口中的字段，您可以使用此窗口配置 EAP-FAST、EAP-TLS 和 PEAP 协议。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP-FAST 设置 (EAP-FAST Settings)**。

表 *184:* 配置 *EAP-FAST* 设置

字段名称	使用指南
Authority Identity Info Description	输入用于说明向客户端发送凭证的Cisco ISE 节点的用户友好字符串。客户端可以在类型、长度和值 (TLV) 的受保护访问凭证 (PAC) 信息中发现此字符串。默认值为 Identity Services Engine。
Master Key Generation Period	指定主键生成期（以秒、分钟、小时、天或周为单位）。值必须是范围在 1 至 2147040000 秒内的正整数。默认值为 604800 秒，相当于一周。
Revoke all master keys and PACs	点击“撤销”(Revoke) 可撤销所有主键和 PAC。
Enable PAC-less Session Resume	如果您要在没有 PAC 文件的情况下使用 EAP-FAST，请选中此复选框。
PAC-less Session Timeout	指定无 PAC 会话恢复超时的时间（以秒为单位）。默认值为 7200 秒。

相关主题

策略集用于身份验证的，第 836 页
将 EAP-FAST 用作协议的指南，第 836 页
EAP-FAST 的优势，第 879 页
配置 EAP-FAST 设置，第 837 页

PAC 设置

下表介绍“生成 PAC”(Generate PAC) 窗口上的字段，您可以使用此窗口为 EAP-FAST 身份验证配置受保护的访问凭证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **生成 PAC (Generate PAC)**。

表 *185:* 为 *EAP-FAST* 设置生成 *PAC*

字段名称	使用指南
Tunnel PAC	点击此单选按钮生成隧道 PAC。
Machine PAC	点击此单选按钮生成设备 PAC。

字段名称	使用指南
Trustsec PAC	点击此单选按钮生成 Trustsec PAC。
Identity	（针对 Tunnel 和 Machine PAC 身份字段）指定 EAP-FAST 协议显示为“内部用户名”的用户名或设备名称。如果身份字符串与该用户名不匹配，则身份验证失败。 这是主机定义在自适应安全设备 (ASA) 上定义的主机名。身份字符串必须与 ASA 主机名匹配，否则 ASA 无法导入生成的 PAC 文件。 如果生成的是 Trustsec PAC，则 Identity 字段指定 Trustsec 网络设备的设备 ID 并且由 EAP-FAST 协议提供发起方 ID。如果在此处输入的 Identity 字符串与该设备 ID 不匹配，则身份验证失败。
PAC Time to Live	（对于隧道和设备 PAC）请以秒为单位输入 PAC 的到期时间。默认值为 604800 秒，相当于一周。该值必须是介于 1 和 157680000 秒之间的正整数。对于 Trustsec PAC，请以天、周、月或年为单位输入一个值。默认情况下，该值为一年。最小值为一天，最大值为 10 年。
Encryption Key	输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。
Expiration Data	（仅对于 Trustsec PAC）到期日期根据 PAC Time to Live 计算。

相关主题

策略集用于身份验证的，第 836 页
将 EAP-FAST 用作协议的指南，第 836 页
为 EAP-FAST 生成 PAC，第 837 页

EAP-TTLS 设置

下表介绍“EAP-TTLS 设置”(EAP-TTLS Settings) 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-TTLS**。

表 *186: EAP-TTLS* 设置

字段名称	使用指南
Enable EAP-TTLS Session Resume	如果您选中此复选框，Cisco ISE 将缓存在 EAP-TTLS 身份验证第一阶段创建的 TLS 会话，前提是用户在 EAP-TTLS 第二阶段成功通过身份验证。如果用户需要重新连接而且原来的 EAP-TTLS 会话尚未超时，Cisco ISE 使用缓存的 TLS 会话，从而加快 EAP-TTLS 性能、降低 AAA 服务器负载。 注释 当 EAP-TTLS 会话恢复时，跳过内部验证方法。
EAP-TTLS Session Timeout	指定 EAP-TTLS 会话在多少秒的时间后超时。默认值为 7200 秒。

相关主题

策略集用于身份验证的，第 836 页
将 EAP-TTLS 用作身份验证协议，第 839 页
配置 EAP-TTLS 设置，第 840 页

EAP-TLS 设置

下表介绍了“EAP-TLS 设置”(EAP-TLS Settings) 窗口上的字段，可以使用此窗口配置 EAP-TLS 协议设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-TLS**。

表 *187: EAP-TLS* 设置

字段	使用指南
Enable EAP-TLS Session Resume	选中此复选框可通过完全 EAP - TLS 认证用户的行为。此功能仅使用安全套接字层(SSL)握手（而不使用证书）对用户提供重新身份验证。只有在 EAP-TLS 会话未超时的情况下，EAP-TLS 会话才会重新运行。
EAP-TLS Session Timeout	指定 EAP-TLS 会话在多少秒的时间后超时。默认值为 7200 秒。
无状态会话恢复	
Master Key Generation Period	输入主键重新生成前经过的时间。此值确定主键保持活动的持续时间。您可以输入以秒、分钟、小时、天或周为单位的值。

字段	使用指南
Revoke	点击**撤销 (Revoke)** 以取消以前生成的所有主键和票证。此选项在辅助节点上禁用。

相关主题

策略集用于身份验证的，第 836 页
配置 EAP-TLS 设置，第 841 页

PEAP 设置

下表列出“PEAP 设置”(PEAP Settings) 窗口上的字段，您可以使用此窗口配置 PEAP 协议设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **PEAP**。

表 *188: PEAP* 设置

字段名称	使用指南
Enable PEAP Session Resume	选中此复选框，使Cisco ISE 缓存在 PEAP 身份验证的第一阶段创建的 TLS 会话，前提是用户在 PEAP 的第二阶段成功通过身份验证。如果用户需要重新连接，原始PEAP会话尚未超时，Cisco ISE 使用缓存的TLS会话，从而加快PEAP性能、降低的 AAA 服务器的负载。您必须指定 PEAP 会话恢复功能的 PEAP 会话超时值可以工作。
PEAP Session Timeout	指定 PEAP 会话超时的时间（单位：秒）。默认值为 7200 秒。
Enable Fast Reconnect	选中此复选框，允许在Cisco ISE 中恢复 PEAP 会话，而无需在启用会话恢复功能时检查用户凭证。

相关主题

策略集用于身份验证的，第 836 页
配置 PEAP 设置，第 842 页
使用 PEAP 的优势，第 878 页
PEAP 协议支持的请求方，第 878 页
PEAP 协议流程，第 878 页

RADIUS 设置

下表介绍“RADIUS 设置”(RADIUS Settings) 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **RADIUS**。

如果启用**抑制重复失败的客户端 (Suppress Repeated Failed Clients)** 选项，系统会从审核日志中抑制身份验证重复失败的客户端，并在指定的时间段内自动拒绝来自这些客户端的请求。您还可以指定身份验证失败的次数，在此之后应拒绝来自这些客户端的请求。例如，如果此值配置为 5，当客户端身份验证失败五次时，将在配置的时间段内拒绝从该客户端收到的所有请求。

注释 如果身份验证失败的原因是输入了错误的密码，则不会抑制客户端。

注释 如果配置 RADIUS 失败抑制，则在配置 RADIUS 日志抑制后，仍可能会收到错误“5440 终端已放弃会话并启动了新会话”(5440 Endpoint Abandoned EAP Session and started a new one)。有关详细信息，请参阅以下 ISE 社区帖子：

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

。

表 *189: RADIUS* 设置

字段名称	使用指南
抑制重复失败的客户端 (Suppress Repeated Failed Clients)	
抑制重复失败的客户端 (Suppress Repeated Failed Clients)	选中此复选框可抑制因相同原因导致身份验证重复失败的客户端。系统会从审核日志中抑制这些客户端，如果已启用**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 选项，还会在指定时间段内拒绝来自这些客户端的请求。
检测两次失败的时间范围 (Detect Two Failures Within)	输入以分钟为单位的时间间隔。如果客户端在该时间段内因相同原因导致两次身份验证失败，则系统会从审核日志中将其抑制，并且，如果已启用**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 选项，还会拒绝来自此客户端的请求。
每几分钟报告一次故障 (Report Failures Once Every)	以分钟为单位输入报告失败身份验证的时间间隔。例如，如果此值设置为 15 分钟，则每 15 分钟在审核日志中仅报告一次重复身份验证失败的客户端，从而防止过度报告。

字段名称	使用指南
拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)	选中此复选框可自动拒绝来自身份验证重复失败的客户端的RADIUS请求。您可以启用此选项，以避免Cisco ISE进行不必要的处理，并防范潜在的拒绝服务攻击。
自动拒绝前的失败次数 (Failures Prior to Automatic Rejection)	输入身份验证失败次数，超过此次数后，会自动拒绝来自重复失败客户端的请求。在配置的时间段内（在**持续拒绝请求的时长 (Continue Rejecting Requests for)** 字段中指定），系统会自动拒绝从这些客户端收到的所有请求。在该间隔到期后，系统会处理来自这些客户端的身份验证请求。
持续拒绝请求的时长 (Continue Rejecting Requests for)	输入一个时间间隔（分钟），在此间隔内会拒绝来自重复失败客户端的请求。
忽略重复记账更新的时间范围 (Ignore Repeated Accounting Updates Within)	在此期间内发生的重复记账更新将被忽略。
抑制成功报告 (Suppress Successful Reports)	
Suppress Repeated Successful Authentications	选中此复选框以防重复报告前 24 小时内在身份情景、网络设备和授权方面没有变更的成功身份验证。
身份验证详细信息 (Authentications Details)	
突出显示长于该值的步骤 (Highlight Steps Longer Than)	以毫秒为单位输入时间间隔。如果单个步骤的执行超出指定阈值，则在身份验证详细信息页面中使用时钟图标来标记此步骤。
检测 RADIUS 请求的高速率 (Detect High Rate of RADIUS Requests)	
检测 RADIUS 请求的稳定高速率 (Detect Steady High Rate of Radius Requests)	选中此复选框可在超过 **RADIUS 请求持续时间 (Duration of RADIUS requests)** 字段和 **RADIUS 请求总数 (Total number of RADIUS requests)** 字段中指定的限制时，发出高RADIUS请求负载警报。
RADIUS 请求持续时间 (Duration of RADIUS Requests)	输入将用于计算RADIUS速率的时间段（以秒为单位）。默认值为60秒。有效范围为20至86400秒。
RADIUS 请求总数 (Total Number of RADIUS Requests)	输入将用于计算RADIUS速率的请求限制。默认为72000个请求。有效范围为24000到103680000个请求。
RADIUS UDP 端口 (RADIUS UDP Ports)	

字段名称	使用指南
身份验证端口 (Authentication Ports)	指定将用于RADIUS UDP身份验证流程的端口。您可以指定最多 4 个端口号（用逗号分隔）。默认情况下，使用端口 1812 和端口 1645。有效范围为 1024 到 65535。
记帐端口 (Accounting Ports)	指定将用于RADIUS UDP记帐流程的端口。您可以指定最多 4 个端口号（用逗号分隔）。默认情况下，使用端口 1813 和端口 1646。有效范围为 1024 到 65535。 **注释** 确保其他服务未使用这些端口。
RADIUS DTLS	
身份验证和记账端口 (Authentication and Accounting Port)	指定将用于 RADIUS DTLS 身份验证和记帐流程的端口。默认情况下，使用端口 2083。有效范围为 1024 到 65535。 **注释** 确保其他服务未使用此端口。
空闲超时 （Idle Timeout）	如果没有从网络设备收到数据包，请输入希望 Cisco ISE 在关闭 TLS 会话之前等待的时间（以秒为单位）。默认值为 120 秒。有效范围为 60 至 600 秒。
启用 RADIUS/DTLS 客户端身份验证 (Enable RADIUS/DTLS Client Identity Verification)	如果希望Cisco ISE 在 DTLS 握手期间验证RADIUS/DTLS客户端的身份，请选中此复选框。如果客户端身份无效，则Cisco ISE握手失败。默认网络设备会跳过身份检查（如果已配置）。身份检查按以下顺序执行： **1.** 如果客户端证书包含使用者备用名称 (SAN) 属性： • 如果 SAN 包含 DNS 名称，则证书中指定的DNS名称会与为Cisco ISE中的网络设备配置的 DNS 名称进行比较。 • 如果 SAN 包含 IP 地址（且不包含 DNS 名称），则证书中指定的 IP 地址会与Cisco ISE 中配置的所有设备 IP 地址进行比较。 **2.** 如果证书不包含 SAN，则使用者 CN 会与为Cisco ISE中的网络设备配置的DNS名称进行比较。如果不匹配，则Cisco ISE 握手失败。

相关主题

策略集用于身份验证的，第 836 页
思科 ISE 中的 RADIUS 协议支持，第 852 页
配置 RADIUS 设置，第 843 页

常规 TrustSec 设置

定义全局 TrustSec 设置，以便Cisco ISE 作为 TrustSec 服务器运行。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 常规 TrustSec 设置 (General TrustSec Settings)**。

验证 Trustsec 部署 (Verify Trustsec Deployment)

此选项可帮助验证所有网络设备上是否部署了最新的 TrustSec 策略。如果在Cisco ISE 和网络设备上配置的策略之间存在任何差异，“警报”(Alarms) Dashlet 中会显示警报，该 Dashlet 位于**工作中心 (Work Centers) > TrustSec > 控制板和主页 (Dashboard and Home) > 摘要 (Summary)** 下。TrustSec 控制板中会显示以下警报：

- 每当验证过程开始或完成时，系统都会显示带有**信息 (Info)** 图标的警报。
- 如果由于新的部署请求而取消验证过程，则会显示带有**信息 (Info)** 图标的警报。
- 如果验证过程因错误而失败，则会显示带有**警告 (Warning)** 图标的警报。例如，无法打开与网络设备的 SSH 连接，或当网络设备不可用，或当Cisco ISE 和网络设备上配置的策略之间存在任何差异。

验证部署 (Verify Deployment) 选项也可从以下窗口选择。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择：

- **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)**
- **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**
- **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix)**
- **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 源树 (Source Tree)**
- **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 目标树 (Destination Tree)**

每次部署后自动验证 (Automatic Verification After Every Deploy)：如果希望Cisco ISE 在每次部署后验证所有网络设备上的更新，请选中此复选框。部署过程完成后，经过您在**部署过程后的时间 (Time after Deploy Process)** 字段中指定的时间后，验证过程开始。

部署过程后的时间 (Time After Deploy Process)：指定您希望Cisco ISE 在部署过程完成后等待多长时间，然后再开始验证过程。有效范围为 10 – 60 分钟。

如果在等待期间收到新的部署请求或正在进行其他验证，则会取消当前验证过程。

立即验证 (Verify Now)：点击此选项可立即开始验证过程。

受保护的访问凭证 (PAC)

- **隧道 PAC 生存时间 (Tunnel PAC Time to Live)**：

  指定 PAC 的到期时间。隧道 PAC 为 EAP-FAST 协议生成隧道。您可以秒、分钟、小时、天或周为单位指定时间。默认值为 90 天。以下是有效范围：

  - 1 – 157680000 秒
  - 1 – 2628000 分钟
  - 1 – 43800 小时
  - 1 – 1825 天
  - 1 – 260 周

- **进行主动 PAC 更新前所经历的时间 (Proactive PAC Update Will Occur After)**：当剩余的隧道 PAC TTL 百分比达到设定值时，Cisco ISE 会在成功身份验证后主动向客户端提供新 PAC。如果第一次成功身份验证发生在 PAC 到期之前，则服务器会启动隧道 PAC 更新。此机制会为客户端更新有效的 PAC。默认值为 10%。

安全组标签编号

- **系统将分配 SGT 编号 (System will Assign SGT Numbers)**：如果希望Cisco ISE 自动生成 SGT 编号，请选择此选项。
- **除范围内的编号外 (Except Numbers in Range)**：选择此选项可保留一系列 SGT 编号以进行手动配置。Cisco ISE 在生成 SGT 时不会使用此范围的值。
- **用户必须手动输入 SGT 编号 (User Must Enter SGT Numbers Manually)**：选择此选项可手动定义 SGT 编号。

APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)

APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)：选中此复选框，指定编号范围以用于根据从 APIC 获取的 EPG 创建的 SGT。

自动创建安全组

创建授权规则时自动创建安全组 (Auto Create Security Groups When Creating Authorization Rules)：选中此复选框可在创建授权策略规则时自动创建 SGT。

如果选中此选项，**授权策略 (Authorization Policy)** 窗口顶部会显示以下消息：`开启自动安全组创建 (Auto Security Group Creation is On)`。

系统会根据规则属性命名自动创建的 SGT。

注释 当删除相应的授权策略规则时，不会删除自动创建的 SGT。

默认情况下，此选项在全新安装或升级后会被禁用。

- **自动命名选项 (Automatic Naming Options)**：使用此选项可定义自动创建的 SGT 的命名约定。

  （必填）**名称将包括 (Name Will Include)**：选择以下选项之一：

  - **规则名称**
  - **SGT 号**
  - **规则名称 (Rule name) 和 SGT 编号 (SGT number)**

  默认选中**规则名称 (Rule name)** 选项。

  或者，可以将以下信息添加到 SGT 名称：

  - **策略集名称 (Policy Set Name)**（此选项仅在已启用**策略集 (Policy Sets)** 时可用）
  - **前缀 (Prefix)**（最多 8 个字符)
  - **后缀 (Suffix)**（最多 8 个字符)

  根据您的选择，Cisco ISE 会在**示例名称 (Example Name)** 字段中显示一个 SGT 名称示例。

  如果存在名称相同的 SGT，ISE 会在 SGT 名称上附加 *_x*，其中 *x* 是从1（如果当前名称中未使用 1）开始的第一个值。如果新名称大于 32 个字符，Cisco ISE 会截取前 32 个字符。

IP SGT 主机名静态映射

IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames)：如果使用 FQDN 和主机名，则Cisco ISE 会在部署映射和检查部署状态的同时在 PAN 和 PSN 节点中查找对应的 IP 地址。您可以使用此选项指定为 DNS 查询返回的 IP 地址创建的映射数。您可以选择以下其中一个选项：

- **为 DNS 查询返回的所有 IP 地址创建映射 (Create mappings for all IP addresses returned by a DNS query)**
- **仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射 (Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query)**

用于网络设备的 TrustSec HTTP 服务

- **启用 HTTP 服务 (Enable HTTP Service)**：使用 HTTP 通过端口 9063 将 Trustsec 数据传输到网络设备。
- **在审核中包括整个响应负载正文 (Include entire response payload body in Audit)**：启用此选项可在审核日志中显示整个 TrustSec HTTP 响应负载正文。此选项可能会显着降低性能。当禁用此选项时，仅会记录 HTTP 信头、状态和身份验证信息。

相关主题

TrustSec 架构，第 882 页
TrustSec 组件，第 883 页
配置 TrustSec 全局设置，第 889 页

TrustSec 表格设置

下表介绍“TrustSec 矩阵设置”(TrustSec Matrix Settings) 窗口上的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

表 *190:* 配置 *TrustSec* 表格设置

字段名称	使用指南
允许多个 SGACL (Allow Multiple SGACLs)	如果要在一个单元格中允许多个 SGACL 请选中此复选框。如果未选择此选项，Cisco ISE 只允许每个单元格一个 SGACL。 默认情况下，此选项在全新安装时禁用。 升级后，Cisco ISE 将扫描出口单元格，因此，如果识别到至少一个被分配多个 SGACL 的单元格，将允许管理员在单元格中添加多个 SGACL。否则，它仅允许每个单元格一个 SGACL。 **注释** 在禁用的多个 SGACL 之前，您必须编辑包含多个 SGACL 的单元格仅包含一个 SGACL。
允许监控 (Allow Monitoring)	选中此复选框可启用对表格中所有单元格的监控。如果禁用监控，“监控全部”(Monitor All) 图标会灰显，“编辑单元格”(Edit Cell) 对话中的“监控”(Monitor) 选项被禁用。 默认情况下，监控在全新安装禁用。 **注释** 在禁用表格级别的监控之前，必须禁用对当前接受监控的单元格的监控。
显示 SGT 数量 (Show SGT Numbers)	使用此选项可显示或隐藏表格单元格中 SGT 值（十进制和十六进制）。 默认情况下，SGT 值在单元格中显示。

字段名称	使用指南
外观设置 (Appearance Settings)	可提供以下选项： • 自定义设置 (Custom settings)：最初显示默认主题（有颜色无图案）。您可以自主设置颜色和图案。 • 默认设置 (Default settings)：预定义的有颜色无图案列表（不可编辑）。 • 辅助功能设置 (Accessibility settings)：预定义的有颜色有图案列表（不可编辑）。
颜色/图案 (Color/Pattern)	要使表格更易读，可根据单元格颜色将颜色和图案应用于表格单元格。 提供以下显示类型： • 允许 IP/允许 IP 日志 (Permit IP/Permit IP Log)：单元格内已配置 • 拒绝 IP/拒绝 IP 日志 (Deny IP/Deny IP Log)：单元格内已配置 • SGACL：用于单元格内已配置的 SGACL • 允许 IP/允许 IP日志（沿用）(Permit IP/Permit IP Log (Inherited))：从（非已配置单元格）默认策略中获取 • 拒绝 IP/拒绝 IP 日志（沿用）(Deny IP/Deny IP Log (Inherited))：从（非已配置单元格）默认策略中获取 • SGACL（沿用）(SGACLs (Inherited))：从（非已配置单元格）默认策略中获取

相关主题

出口策略，第 906 页
矩阵视图，第 907 页
配置 TrustSec 矩阵，第 893 页

DHCP 和 DNS 服务

要查看此处窗口，请点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 系统 (System) > 设置 (Settings) > DHCP & DNS 服务 (DHCP & DNS Services) 。

使用这些设置配置 DHCP，也可选择配置 DNS，以便启用身份验证 VLAN URL 重定向模拟。您可以创建多个范围并将其应用于不同的 ISE 节点。如果您将多个范围应用于一个 ISE 节点，那么它们需在同一网络接口进行配置。

注释 对于“分析”(Profiling)，您可能需要 DHCP 探测。ISE DHCP 探测与身份验证 VLAN DHCP 服务使用相同的 UDP 端口 67。因此该 DHCP 探测需在不同的接口上进行配置或可以在该 ISE 节点上被禁用。有关 DHCP 探测的详细信息，请参阅DHCP 探测功能， 第 607 页。

表 *191:* 身份验证 *VLAN URL* 重定向模拟 *DHCP* 和 *DNS* 服务设置

字段名称	使用指南
范围名称 (Scope Name)	输入一个便于您记住该范围的用途的名称。
状态	选择**启用 (Enabled)** 或**禁用 (Disabled)**。范围在启用后仅可用于一个 ISE 节点。
ISE 节点 (ISE Node)	应用一个 ISE 节点，将其用作 DHCP/DNS 服务器。在下拉列表中，选择使用该范围的 ISE 节点。身份验证 VLAN 是针对每个 ISE 节点或网络接口定义的，任何两个接口或两个节点均不可共享同一个 VLAN。
Network Interface	根据您所选的 ISE 节点，用于该 ISE 节点的网络接口会动态出现在下拉列表中。选择用于 DHCP/DNS 服务器侦听的接口。可通过在 NAD 上配置一个 VLAN IP 助手将多个 VLAN 连接到一个网络接口卡。
域名	输入用于该范围的 DHCP 服务器的域名。
DHCP 地址范围 (DHCP Address range)	根据您的网络定义，选择可用于该范围的 DHCP 地址范围。
子网掩码	根据您的网络定义，选择可用于该范围的网络掩码。
网络 ID	网络 ID 由Cisco ISE 基于您输入的 DHCP 属性自动确定。
排除地址范围 (Exclusion address range)	根据您的网络定义，选择不应用于该范围的DHCP地址范围。
Default gateway	输入默认网关的 IP 地址。
DHCP 租用时间 (DHCP lease time)	定义 DHCP 租用时间。

字段名称	使用指南
DHCP 选项	（可选）DHCP 选项是 DCHP 服务器发送到 DHCP 客户端的附加配置参数。DHCP选项为需要选项值中指示的信息才能访问网络的设备（例如摄像头、接入点或电话）提供支持，或作为在最终授权之前引导设备的方法。当 DHCP 服务器收到客户端的 DHCP 请求消息时，服务器（通常）通过向客户端发送DHCP ACK数据包做出响应。此时，服务器会转发 DHCP ACK 数据包中的所有已配置选项。 有关详细信息，请参阅此表下方的“DHCP选项”部分。
外部 **DNS** 服务器 **(External DNS servers)**	如果您想要允许用户在收到访问整个公司网络的身份验证之前能够访问身份验证 VLAN 之外的外部域名，请输入 DNS 服务器的 IP 地址以解析外部 DNS 名称。
外部域名 **(External Domains)**	如果您希望用户在收到访问整个公司网络的身份验证之前能够访问特定网站，请在这些字段中输入域名。 输入除父域外，用户可能需要访问的所有子域的名称。

DHCP 选项

在 ISE 中配置 DHCP 服务时，可以为连接到身份验证 VLAN 的客户端分配特定 DHCP 选项。您可以向定义的每个域添加多个 DHCP 选项。

下拉列表中提供的选项取自 RFC 2132。您还可以从下拉列表中选择**自定义 (Custom)** 并输入选项代码，添加额外的自定义选项。

通常，有几个 DHCP 选项往往最常用。常见选项包括：

- 选项 12（主机名）(Option 12 (Hostname))：用于承载节点的完全限定域名的“主机名”部分。例如，mail.ise.com 的“mail”。
- 选项 42（NTP 服务器）(Option 42 (NTP Servers))：承载网络上使用的 NTP 服务器。
- 选项 66（TFTP 服务器）(Option 66 (TFTP Server))：用于承载 IP 地址或主机名。此选项在下拉列表中可用。
- 选项 82（DHCP 中继代理）(Option 82 (DHCP Relay Agent))：用于承载服务器端 DHCP 中继服务器信息的其他子选项。

如要定义选项值，请从下拉列表中选择一个选项。如果选择预定义的**选项 (Option)**，会自动填充代码和类型。

如果选择**自定义 (Custom)**，请输入**代码 (Code)** 和**值 (Value)**。**类型 (Type)** 字段会自动更新。

例如：

- 要设置主机名，请执行以下操作：从**选项 (Option)** 下拉列表中，选择**自定义 (Custom)**。在**代码 (Code)** 字段中输入代码（例如，15）。**类型 (Type)** 字段中会自动填充文本。在**值 (Value)** 名字段中输入主机名。
- 要设置 TFTP 服务器名称，请执行以下操作：从**选项 (Option)** 下拉列表中，选择 TFTP 服务器名称。**代码 (Code)** 和**类型 (Type)** 字段会自动更新。在**值 (Value)** 字段中，键入 TFTP 服务器主机名。

注释 有些 DHCP 选项无法手动输入，因为它们是为 ISE 自动定义的。

如要输入多个选项，请点击**操作 (Actions)** 下面的加号。

相关主题

思科 ISE 中的第三方网络设备支持，第 740 页
在思科 ISE 中配置第三方网络设备，第 744 页
DHCP 探测功能，第 607 页

身份管理

您可以使用这些页面在Cisco ISE 中配置和管理身份。

终端

通过这些页面，您可以配置和管理连接到您的网络的终端。

终端设置

下表介绍**终端 (Endpoints)** 窗口上的字段，您可以使用此窗口创建终端和为终端分配策略。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *192:* 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的MAC地址以静态创建终端。 MAC 地址是连接到启用Cisco ISE 的网络的接口设备标识符。

字段名称	使用指南
Static Assignment	如果您想要在 Endpoints 页面静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。 您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。
Policy Assignment	（除非选中**静态分配 (Static Assignment)** 复选框，否则会默认禁用此字段）从**策略分配 (Policy Assignment)** 下拉列表选择匹配的终端策略。 您可以执行以下操作之一： • 如果您不选择匹配的终端策略，而是使用默认终端策略 Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。 • 如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中**静态分配 (Static Assignment)** 复选框。
Static Group Assignment	当您想要向身份组静态分配终端时，请选中此复选框。 如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。 如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。

字段名称	使用指南

Identity Group Assignment	选择您要将终端分配至哪个终端身份组。
	当您静态创建终端，或在为某个终端评估终端策略期间不想使用**创建匹配身份组 (Create Matching Identity Group)** 选项时，可将终端分配至身份组。
	Cisco ISE 包括以下系统创建的终端身份组：
	• Blacklist
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端，第 659 页
使用策略和身份的静态分配创建终端，第 655 页

从 LDAP 设置导入终端

下表介绍“从 LDAP 导入”(Import from LDAP) 窗口上的字段，您可以使用此窗口从 LDAP 服务器导入终端。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

表 *193:* 从 *LDAP* 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。 注释 Cisco ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。

字段名称	使用指南
Enable Secure Connection	选中**启用安全连接 (Enable Secure Connection)** 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	点击下拉箭头，查看受信任的 CA 证书。 根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在Cisco ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
Anonymous Bind	您必须选中**匿名绑定 (Anonymous Bind)** 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
Admin DN	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
密码 (Password)	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
Base DN	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
查询设置	
MAC Address objectClass	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
MAC Address Attribute Name	输入导入操作返回的属性名称，例如，macAddress。

字段名称	使用指南
Profile Attribute Name	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置**分析属性名称 (Profile Attribute Name)** 字段时，请考虑以下事项： • 如果未在**分析属性名称 (Profile Attribute Name)** 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知”(Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。 • 如果您在**分析属性名称 (Profile Attribute Name)** 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与Cisco ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。
超时	输入时间（单位：秒），值介于 1 和 60 秒之间。

相关主题

已识别的终端，第 659 页
从 LDAP 服务器导入终端，第 658 页

终端身份组设置

下表介绍“终端身份组”(Endpoint Identity Groups) 窗口上的字段，您可以使用此窗口创建终端组。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)**。

表 *194:* 终端身份组设置

字段名称	使用指南
名称	输入您要创建的终端身份组的名称。
说明	输入对您要创建的终端身份组的说明。
Parent Group	从 Parent Group 下拉列表选择您要关联新创建的终端身份组的终端身份组。

相关主题

已识别终端划分为终端身份组，第 662 页
创建终端身份组，第 661 页

外部身份源

您可以通过这些页面配置和管理包含Cisco ISE 用于身份验证和授权的用户数据的外部身份源。

LDAP 身份源设置

下表介绍“LDAP 身份源”(LDAP Identity Sources) 窗口上的字段，您可以使用此窗口创建 LDAP 实例并连接该实例。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **LDAP**。

LDAP 常规设置

下表介绍**常规 (General)** 选项卡上的字段。

表 *195: LDAP* 常规设置

字段名称	使用指南
名称 (Name)	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
说明	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。
架构 (Schema)	您可以选择以下任一内置架构类型或创建自定义架构： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 您可以点击 Schema 旁边的箭头以查看架构详细信息。 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。
注释 仅当选择自定义架构时，才可以编辑以下字段。	
Subject Objectclass	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
主题名称属性 (Subject Name Attribute)	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。

字段名称	使用指南
组名称属性 **(Group Name Attribute)**	• CN：根据通用名称检索 LDAP 身份存储区组。 • DN：根据可分辨名称检索 LDAP 身份存储区组。
证书属性 **(Certificate Attribute)**	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
Group Objectclass	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。
组映射属性 **(Group Map Attribute)**	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 **(Subject Objects Contain Reference To Groups)**	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 **(Group Objects Contain Reference To Subjects)**	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 **(Subjects in Groups Are Stored in Member Attribute As)**	（仅适用于启用**组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects)** 选项时）指定在组成员属性中如何搜索成员，其默认值为 DN。
用户信息属性	默认情况下，预定义属性用于收集以下内置架构类型的用户信息（例如，名字、姓氏、电子邮件、电话，位置等）： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 如果您编辑该预定义架构的属性，Cisco ISE 会自动创建自定义架构。 您还可以选择架构 (Schema) 下拉菜单中的定制 (Custom) 选项，根据要求编辑用户信息属性。

LDAP 连接设置

下表介绍**连接设置 (Connection Settings)** 选项卡中的字段。

表 *196: LDAP* 连接设置

字段名称	使用指南
启用辅助服务器 **(Enable Secondary Server)**	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器 **(Primary and Secondary Servers)**	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效IP地址。对于主机名，仅字母数字字符（a 至 z；A 至 Z；0 至 9）、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。
为每个 **ISE** 节点指定服务器	选中此复选框可配置每个PSN的主辅LDAP服务器主机名/IP 及其端口。 启用此选项后，将显示一个表，列出部署中的所有节点。您需要选择节点并配置主要和辅助LDAP服务器主机名/IP 及所选节点的端口。
访问	**匿名访问 (Anonymous Access)**：点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。 **身份验证访问 (Authenticated Access)**：点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员DN”(Admin DN) 字段和“密码”(Password) 字段输入信息。
管理员 **DN (Admin DN)**	输入管理员的DN。管理员DN是有权限搜索“用户目录子树”(User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该LDAP服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。

字段名称	使用指南
安全身份验证 **(Secure Authentication)**	点击此字段以对Cisco ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口”(Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“**LDAP 服务器根 CA**”**(LDAP Server Root CA)**	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 **(Server Timeout)**	以秒为单位输入Cisco ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 **(Max. Admin Connections)**	输入利用 LADP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于0）。这些连接用于在“用户目录子树”(User Directory Subtree) 和 “组目录子树”(Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
每 **N** 秒强制重新连接	选中此复选框并在**秒 (Seconds)** 字段中输入所需的值可强制服务器按照指定的时间间隔续订 LDAP 连接。有效范围为 1 至 60 分钟。
测试与服务器的绑定 **(Test Bind to Server)**	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
Failover	
Always Access Primary Server First	如果您希望Cisco ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
...后故障恢复到主服务器 **(Failback to Primary Server after)**	如果Cisco ISE 尝试连接的主 LDAP 服务器无法访问，Cisco ISE 会尝试连接辅助 LDAP 服务器。如果您希望Cisco ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

LDAP 目录组织设置

下表介绍**目录组织 (Directory Organization)** 选项卡上的字段。

表 *197: LDAP* 目录组织设置

字段名称	使用指南
主题搜索库 (Subject Search Base)	输入包含所有主题的子树的 DN。例如： o=corporation.com 如果包含主题的树是基本 DN，请输入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
组搜索库 (Group Search Base)	输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com 如果包含组的树是基本 DN，请键入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	输入一个MAC地址格式供Cisco ISE用于在LDAP数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当Cisco ISE 收到主机查找请求时，Cisco ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。 使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <*format*> 可以是以下任何一种格式： • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。

字段名称	使用指南
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	输入适当的文本以删除用户名的域前缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <start_string> 框中指定的多个字符，Cisco ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则Cisco ISE 会向 LDAP 服务器提交 user1。 **注释** <start_string> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	输入适当的文本以删除用户名的域后缀。 如果Cisco ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，Cisco ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 *user1@domain*，则Cisco ISE 会向 LDAP 服务器提交 *user1*。 **注释** *<end_string>* 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。Cisco ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *198: LDAP* 组设置

字段名称	使用指南
添加	选择 **Add> 添加组**添加新组或从目录**中选择** Add> 选择 Group 选择组从 LDAP 目录。 如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。点击要选择的组旁边的复选框，然后点击**确定 (OK)**。选中的组将显示在**组 (Groups)** 窗口中。

LDAP 属性设置

表 *199: LDAP* 属性设置

字段名称	使用指南
添加	选择 **Add> 添加属性**添加新属性或从目录**中选择** Add> 选择属性从 LDAP 服务器的属性。 如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击**检索属性 (Retrieve Attributes)** 以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。

LDAP 高级设置

下表介绍“高级设置”(Advanced Settings) 选项卡中的字段。

表 *200: LDAP* 高级设置

字段名称	使用指南
启用密码更改 (Enable Password Change)	在使用 PAP 协议进行设备管理和使用 RADIUS EAP-GTC 协议进行网络访问时，选中此复选框可让用户在密码到期或重置密码的情况下更改密码。对于不受支持的协议，用户身份验证会失败。此选项还可以让用户在下次登录时更改密码。

相关主题

LDAP 目录服务，第 561 页
LDAP 用户身份验证，第 562 页
LDAP 用户查找，第 565 页
添加 LDAP 身份源，第 566 页

RADIUS 令牌身份源设置

下表介绍“RADIUS 令牌身份源”(Token Identity Sources) 窗口上的字段，您可以使用此窗口配置和连接外部 RADIUS 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)**。

表 *201: RADIUS* 令牌身份源设置

字段名称	使用指南
名称	输入 RADIUS 令牌服务器名称。允许的最大字符数为 64。
说明	输入 RADIUS 令牌服务器说明。允许的最大字符数为 1024。

字段名称	使用指南
SafeWord Server	如果 RADIUS 身份源为 SafeWord 服务器，请选中此复选框。
Enable Secondary Server	选中此复选框，为Cisco ISE 启用辅助 RADIUS 令牌服务器，在主要服务器发生故障时用作备份。如果选中此复选框，必须配置辅助 RADIUS 令牌服务器。
Always Access Primary Server First	如果希望Cisco ISE 总是首先访问主服务器，请点击此选项。
Fallback to Primary Server after	点击此选项可指定在无法连接主服务器时，Cisco ISE 能够在多长时间里（分钟）使用辅助 RADIUS 令牌服务器进行身份验证。这段时间过后，Cisco ISE 重新尝试对照主服务器进行身份验证。
主服务器	
Host IP	输入主要 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在主要 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入主要 RADIUS 令牌服务器侦听的端口号。
Server Timeout	指定Cisco ISE 在确定主服务器关闭之前，等待主要 RADIUS 令牌服务器发出响应的秒数。
Connection Attempts	指定Cisco ISE 在迁移到辅助服务器（如果已定义）或放弃请求（如果未定义辅服务器）之前，尝试重新连接到主服务器的次数。
辅助服务器	
Host IP	输入辅助 RADIUS 令牌服务器的 IP 地址。此字段可用来输入以字符串表示的有效 IP 地址。此字段中允许输入的有效字符为数字和句点 (.)。
共享密钥	输入在辅助 RADIUS 令牌服务器上为此连接配置的共享密钥。
身份验证端口	输入辅助 RADIUS 令牌服务器侦听的端口号。有效值为 1 至 65535。默认值为 1812。
Server Timeout	指定Cisco ISE 在确定辅助服务器关闭之前，等待辅助 RADIUS 令牌服务器发出响应的秒数。

字段名称	使用指南
Connection Attempts	指定Cisco ISE 在放弃请求之前应当尝试重新连接辅助服务器的次数。

相关主题

RADIUS 令牌身份源，第 582 页
添加 RADIUS 令牌服务器，第 587 页

RSA SecurID 身份源设置

下表介绍“RSA SecurID 身份源”(RSA SecurID Identity Sources) 窗口上的字段，您可以使用此窗口创建和连接 RSA SecurID 身份源。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **RSA SecurID**。

RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 *202: RSA* 提示设置

字段名称	使用指南
Enter Passcode Prompt	输入文本字符串以获取密码。
Enter Next Token Code	输入文本字符串以请求下一个令牌。
Choose PIN Type	输入文本字符串以请求 PIN 类型。
Accept System PIN	输入文本字符串以接受系统生成的 PIN。
Enter Alphanumeric PIN	输入文本字符串以请求字母数字 PIN。
Enter Numeric PIN	输入文本字符串以请求数字 PIN。
Re-enter PIN	输入文本字符串以请求用户重新输入 PIN。

RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 *203: RSA* 消息设置

字段名称	使用指南
Display System PIN Message	输入文本字符串以编辑系统 PIN 消息。
Display System PIN Reminder	输入文本字符串以通知用户记住新 PIN。

字段名称	使用指南
Must Enter Numeric Error	输入一条消息，指导用户仅输入数字作为 PIN。
Must Enter Alpha Error	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
PIN Rejected Message	输入在系统拒绝用户的 PIN 时用户所看到的消息。
User Pins Differ Error	输入在用户输入错误 PIN 时所看到的消息。
System PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
Bad Password Length Error	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

相关主题

RSA 身份源，第 588 页
思科 ISE 和 RSA SecurID 服务器集成，第 589 页
添加 RSA 身份源，第 592 页

网络资源

对会话感知网络 (SAnet) 的支持

Cisco ISE 为会话感知网络 (SAnet) 提供有限支持。SAnet 是在许多Cisco交换机上运行的会话管理框架。SAnet 管理访问会话，包括可视性、身份验证和授权。SAnet 使用服务模板，其中包含 RADIUS 授权属性。Cisco ISE 在授权配置文件中包含服务模板。Cisco ISE 在授权配置文件中使用标志来标识服务模板，该标志会将配置文件标识为兼容“服务模板”。

Cisco ISE 授权配置文件包含转换为属性列表的 RADIUS 授权属性。SAnet 服务模板还包含 RADIUS 授权属性，但这些属性不会转换为列表。

对于 SAnet 设备，Cisco ISE 会发送服务模板的名称。设备会下载服务模板的内容，除非该内容已存在于缓存或静态定义的配置中。当服务模板更改 RADIUS 属性时，Cisco ISE 会向设备发送 CoA 通知。

网络设备配置文件设置

下表介绍了“网络设备配置文件”(Network Device Profiles) 窗口上的字段，您可以用其为特定供应商的一种网络设备配置默认设置，例如设备的协议支持、重定向 URL 和 CoA 设置。然后使用配置文件定义特定网络设备。

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。

网络设备配置文件设置

下表列出“网络设备配置文件”(Network Device Profile) 部分的字段。

表 *204:* 网络设备配置文件设置

字段名称	说明
名称	输入网络设备配置文件的名称。
说明	输入网络设备配置文件的说明。
图标	选择要用于网络设备配置文件的图标。此图标将默认为您选择的供应商的图标。 您选择的图标必须是 16 x 16 PNG 文件。
供应商	选择网络设备配置文件的供应商。
支持的协议	
RADIUS	如果此网络设备配置文件支持 RADIUS，请选中此复选框。
TACACS+	如果此网络设备配置文件支持 TACACS+，请选中此复选框。
TrustSec	如果此网络设备配置文件支持 TrustSec，请选中此复选框。
RADIUS 字典	选择此配置文件支持的一个或多个 RADIUS 字典。在创建配置文件之前，请导入所有供应商特定 RADIUS 字典。

身份验证/授权模版设置

下表列出“身份验证/授权”(Authentication/Authorization) 部分的字段。

表 *205:* 身份验证/授权设置

字段名称	说明
流量类型条件 **(Flow Type Conditions)**	Cisco ISE 支持 802.1X、MAC 身份验证绕行 (MAB) 和基于浏览器的 Web 身份验证登录，通过有线和无线网络为用户提供基本身份验证和访问。 对于此类型网络设备支持的身份验证登录选中此复选框。可以是下面的一项或多项： • 有线 MAC 身份验证绕行 (MAB) • 无线 MAB • 有线 802.1X • 无线 802.1X • 有线 Web 身份验证 • 无线 Web 身份验证 在查看网络设备配置文件支持的身份验证登录后，指定用于登录的条件。
属性别名 **(Attribute Aliasing)**	选中 SSID 复选框可将设备的服务集标识符 (SSID) 用作策略规则中的友好名称。这样您可创建一个在策略规则中使用的一致名称。
主机查找 **(MAB)**	
Process Host Lookup	选中此复选框可定义网络设备配置文件使用的主机查找的协议。 来自不同供应商的网络设备以不同的方式执行 MAB 身份验证。根据设备类型，为您使用的协议选中**检查密码 (Check Password)** 或检查**呼叫站 ID 等于 MAC 地址 (Checking Calling-Station-Id equals MAC Address)** 复选框。
通过 **PAP/ASCII (Via PAP/ASCII)**	选中此复选框可配置Cisco ISE检测作为主机查找请求的来自网络设备配置文件的 PAP 请求。
通过 **CHAP**	选中此复选框可配置Cisco ISE检测作为主机查找请求的来自网络设备配置文件这种请求类型。 此选项可启用 CHAP 身份验证。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。

字段名称	说明
通过 EAP-MD5 (Via EAP-MD5)	选中此复选框可启用用于网络设备配置文件的基于 EAP 的 MD5 散列身份验证。

权限

您可以定义用于此网络设备配置文件的 VLAN 和 ACL 权限。保存配置文件后，Cisco ISE 为每个配置权限的授权配置文件自动生成授权配置文件。

表 ***206:*** 权限

字段名称	说明
设置 VLAN	选中此复选框可为此网络设备配置文件设置VLAN权限。选择以下其中一个选项： • IETF 802.1X 属性。这是一组由 Internet 工程工作小组定义的 RADIUS 默认属性。 • 唯一属性您可以指定多个 RADIUS 属性值对。
设置 ACL	选中此复选框可选择为网络设备配置文件上的 ACL 设置的 RADIUS 属性。

授权更改 (CoA) 模板设置

此模板定义如何将 CoA 发送至此类网络设备。下表列出“授权更改”(CoA) 部分的字段。

表 ***207:*** 授权更改 ***(CoA)*** 设置

字段名称	定义
CoA 发送协议	选择以下选项之一： • RADIUS • SNMP • 不支持
通过 RADIUS 发送 CoA	
默认 CoA 端口	发送 RADIUS CoA 的端口。默认情况下，端口 1700 用于Cisco设备，端口 3799 用于非Cisco供应商的设备。 您可以在“网络设备”(Network Device) 窗口对此进行覆盖。

字段名称	定义
超时间隔 **(Timeout Interva**l)	Cisco ISE 在发送 WLAN 后等待响应的秒数。
Retry Count	Cisco ISE 在首次超时后尝试发送 CoA 的次数。
Disconnect	选择如何将断开请求发送至这些设备。 • **RFC 5176**：为标准会话终止选中此复选框并使端口准备好新会话，如 RFC 5176 中所定义。 • **端口退回 (Port Bounce)**：选中此复选框可终止会话并重新启动端口。 • **端口关闭 (Port Shutdown)**：选中此复选框可终止会话并关闭端口。
重新进行身份验证	选择如何发送重新进行身份验证请求至网络设备。当前仅Cisco设备支持此功能。 • **基本 (Basic)**：为标准会话重新进行身份验证选中此复选框。 • **重新运行 (Rerun)**：选中此复选框可从一开始运行身份验证方法。 • **上次 (Last)**：为会话使用上次成功的身份验证方式。
CoA 推送	如果网络设备不支持Cisco的 TrustSec CoA 功能，请选择此选项允许Cisco ISE 推送配置更改至设备。
通过 **SNMP 发送 CoA**	
超时间隔	Cisco ISE 在发送 WLAN 后等待响应的秒数。
Retry Count	Cisco ISE 尝试发送 CoA 的次数。
NAD 端口检测	相关 RADIUS 属性是当前唯一选项。
相关 RADIUS 属性	选择如何检测 NAD 端口： • Nas-Port • NAS-Port-Id

字段名称	定义
Disconnect	选择如何将断开请求发送至这些设备： • **重新验证 (Reauthenticate)**：选中此复选框可终止会话并重新启动端口。 • **端口退回 (Port Bounce)**：选中此复选框可终止会话并重新启动端口。 • **端口关闭 (Port Shutdown)**：选中此复选框可终止会话并关闭端口。

重定向模版设置

如果 HTTP 请求配置为授权配置文件的一部分，网络设备可重定向客户端的 HTTP 请求。此模板指定此网络设备配置文件是否支持 URL 重定向。您将使用指定给设备类型的 URL 参数名称。

下表列出“重定向”(Redirect) 部分的字段。

表 *208:* 重定向设置

字段名称	定义
类型	选择网络设备配置文件是否支持静态或动态URL重定向。 如果设备两者都不支持，请选择**不支持 (Not Supported)** 并从以下位置设置 VLAN： **设置 (Settings)** > **DHCP 和 DNS 服务 (DHCP & DNS Services)** 。
重定向 URL 参数名称 (Redirect URL Parameter Names)	
客户端 IP 地址	输入网络设备用于客户端的IP地址的参数名称。
客户端 MAC 地址 (Client MAC Address)	输入网络设备用于客户端MAC地址的参数名称。
Originating URL	输入网络设备用于原始 URL 的参数名称。
Session ID	输入网络设备用于会话 ID 的参数名称。
SSID	输入网络设备用于服务集标识符 (SSID) 的参数名称。
动态 URL 参数 (Dynamic URL Parameters)	
参数	当您选择使用动态URL用于重定向时，您需要指定这些网络设备如何创建重定向URL。您还可以指定重定向URL是否使用会话ID或客户端MAC地址。

高级设置

您可以使用网络设备配置文件生成大量策略要素以方便在策略规则中使用网络设备。这些元素包括复合条件、授权配置文件和允许协议。

点击**生成策略元素 (Generate Policy Elements)** 创建这些元素。

相关主题

网络设备配置文件，第 743 页
思科 ISE 中的第三方网络设备支持，第 740 页
创建网络设备配置文件，第 745 页

外部 RADIUS 服务器设置

下表介绍“外部 RADIUS 服务器”(External RADIUS Server) 窗口上的字段，您可以使用此窗口配置 RADIUS 服务器。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 RADIUS 服务器 (External RADIUS Servers)**。

表 *209:* 外部 *RADIUS* 服务器设置

字段名称	使用指南
名称	输入外部 RADIUS 服务器的名称。
说明	输入外部 RADIUS 服务器的说明。
Host IP	输入外部 RADIUS 服务器的 IP 地址。输入 IPv4 地址时，可以使用地址范围和子网掩码。IPv6 不支持地址范围。
共享密钥	输入Cisco ISE 和外部 RADIUS 服务器之间用于对外部 RADIUS 服务器进行身份验证的共享密钥。共享密钥是用户必须提供的预期文本字符串，使网络设备能够验证用户名和密码。在用户提供共享密钥之前，连接始终被拒绝。共享密钥最大长度为 128 个字符。
启用 **KeyWrap**	启用此选项，通过 AES KeyWrap 算法增加 RADIUS 协议安全性。
密钥加密密钥)	（仅当选中启用密钥封装 (Enable Key Wrap) 复选框时）输入要用于会话加密（保密）的密钥。
消息身份验证器代码密钥	（仅当选中启用密钥封装 (Enable Key Wrap) 复选框时）输入用于基于 RADIUS 消息的键控 HMAC 计算的密钥。

字段名称	使用指南
密钥输入格式	指定要在输入Cisco ISE 加密密钥时使用的格式，使其匹配 WLAN 控制器上可用的配置。您指定的值必须是密钥的正确（完整）长度，符合下方的定义（不允许使用短于此长度的值）。 • ASCII：“密钥加密密钥”(Key Encryption Key) 长度必须为 16 个字符（字节），“消息身份验证器代码密钥”(Message Authenticator Code Key) 长度必须为 20 个字符（字节）。 • 十六进制 (Hexadecimal)：“密钥加密密钥”(Key Encryption Key) 长度必须为 32 个字节，“消息身份验证器代码密钥”(Message Authenticator Code Key) 长度必须为 40 个字节。
身份验证端口	输入 RADIUS 身份验证端口号。有效范围为 1 至 65535。默认值为 1812。
Accounting Port	输入 RADIUS 记账端口号。有效范围为 1 至 65535。默认值为 1813。
Server Timeout	输入Cisco ISE 等待外部 RADIUS 服务器响应的秒数。默认值为 5 秒。有效值为 5 至 120。
Connection Attempts	输入Cisco ISE 尝试连接到外部 RADIUS 服务器的次数。默认值为 3 次。有效值为 1 至 9。
RADIUS 代理故障转移到期	输入连接失败后到再次尝试连接此服务器之前经过的时间。有效范围为 1 到 600。 配置此参数可跳过服务器超时，直接进行故障转移。

相关主题

将思科 ISE 用作 RADIUS 代理服务器，第 868 页
配置外部 RADIUS 服务器，第 869 页

RADIUS 服务器序列

下表介绍“RADIUS 服务器序列”(RADIUS Server Sequences) 窗口上的字段，它可以用来创建 RADIUS 服务器序列。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **RADIUS 服务器序列 (RADIUS Server Sequences)** > **添加 (Add)**。

表 *210: RADIUS* 服务器序列

字段名称	使用指南
Name	输入 RADIUS 服务器序列的名称。
说明	输入可选的说明。
Host IP	输入外部 RADIUS 服务器的 IP 地址。
User Selected Service Type	从 Available 列表框选择您要用作策略服务器的外部 RADIUS 服务器，并将其移入 Selected 列表框。
Remote Accounting	选中此复选框以在远程策略服务器上启用记账功能。
Local Accounting	选中此复选框以在Cisco ISE 上启用记帐功能。
高级属性设置	
Strip Start of Subject Name up to the First Occurrence of the Separator	选中此复选框以删除用户名的前缀。例如，如果主题名称是 acme\userA，分隔符为 \，则用户名成为 userA。
Strip End of Subject Name from the Last Occurrence of the Separator	选中此复选框以删除用户名的后缀。例如，如果主题名称是 userA@abc.com，分隔符为 @，则用户名成为 userA。 • 您必须启用这些删除选项以从 NetBIOS 或用户主体名称 (UPN) 格式用户名（@domain.com 或 /domain/user）提取用户名，因为系统向 RADIUS 服务器仅传递用户名以对用户进行身份验证。 • 如果您同时激活 \ 和 @ 删除功能，而且您使用的是Cisco AnyConnect，则Cisco ISE 会从字符串中准确地删除第一个 \。但是，每个单独使用的剥离功能都按照设计与Cisco AnyConnect 配合运行。

字段名称	使用指南
Modify Attributes in the Request to the External RADIUS Server	选中此复选框以允许Cisco ISE 修改往来于经过身份验证的 RADIUS 服务器的属性。 属性修改操作包括以下选项： • **添加 (Add)** - 向整体 RADIUS 请求/响应添加其他属性。 • **更新 (Update)** - 更改属性值（固定或静态）或将一个属性值替代为另一个属性值（动态）。 • **删除 (Remove)** - 删除属性或属性-值对。 • **删除所有 (RemoveAny)** - 删除所有出现的属性。
Continue to Authorization Policy	选中此复选框以将代理流程转为运行授权策略，从而根据身份库组和属性检索结果执行进一步决策。如果启用此选项，来自外部 RADIUS 服务器的响应的属性将适用于身份验证策略选择。上下文中已有的属性将根据 AAA 服务器 accept response 属性的相应值进行更新。
Modify Attributes before send an Access-Accept	选中此复选框以在快要向设备发回响应之前修改属性。

相关主题

将思科 ISE 用作 RADIUS 代理服务器，第 868 页
定义 RADIUS 服务器序列，第 869 页

NAC 管理器设置

下表介绍“新 NAC 管理器”(New NAC Managers) 页面上的字段，您可以使用这些字段添加 NAC 管理器。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **NAC 管理器 (NAC Managers)**。

表 *211: NAC* 管理器设置

字段	使用指南
名称 (Name)	输入Cisco接入管理器 (CAM) 的名称。
Status	点击 Status 复选框，启用从验证连接的Cisco ISE 分析器到 CAM 的 REST API 通信。
说明	输入 CAM 的说明。

字段	使用指南
IP Address	输入 CAM 的 IP 地址。在Cisco ISE 中创建和保存 CAM 后，无法编辑 CAM 的 IP 地址。 您不能使用 0.0.0.0 和 255.255.255.255，因为在 Cisco ISE 中验证 CAM 的 IP 地址时，这些 IP 地址被排除在外。因此，它们不是您可以在 CAM 的 IP Address 字段中使用的有效 IP 地址。 注释 您可以使用一对 CAM 在高可用性配置中共享的虚拟服务 IP 地址。这允许在高可用性配置中支持 CAM 故障转移。
Username	输入允许您登录 CAM 用户界面的 CAM 管理员的用户名。
Password	输入允许您登录 CAM 用户界面的 CAM 管理员的密码。

设备门户管理

配置设备门户设置

设备门户的门户标识设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portal)**、**客户端调配门户 (Client Provisioning Portals)**、**BYOD 门户 (BYOD Portals)**、**MDM 门户 (MDM Portals)** 或**我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)**。

- **门户名称 (Portal Name)**：输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

  此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述**：可选。

- **门户测试 URL (Portal test URL)**：点击**保存 (Save)** 后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

  点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，Cisco ISE 会选择第一个活动 PSN。

- **语言文件 (Language File)**：默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

  语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

  如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

  在**门户页面自定义 (Portal Page Customizations)** 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

相关主题

创建授权策略规则，第 714 页
创建授权配置文件，第 713 页
个人设备门户，第 694 页

BYOD 和 MDM 门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD 门户或 MDM 门户 (BYOD Portals or MDM Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

配置这些设置以定义门户页面操作。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：

- 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
- 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
- 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。

- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x**、**x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。Cisco ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

  选择用于跟踪员工设备的终端身份组。Cisco ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

相关主题

自带设备门户，第 695 页
创建 BYOD 门户，第 707 页
移动设备管理门户，第 696 页
创建 MDM 门户，第 711 页
自带设备门户语言文件的 HTML 支持，第 427 页
对移动设备管理门户语言文件的 HTML 支持，第 434 页

BYOD 门户的 BYOD 设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD 门户 (BYOD Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **BYOD 设置 (BYOD Settings)**。

使用这些设置为想要使用个人设备访问您的公司网络的员工启用自带设备 (BYOD) 功能。

字段名称	使用指南
包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的页面上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。

字段名称	使用指南
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。
在注册期间显示设备 ID 字段 (Display Device ID Field During Registration)	在注册过程中向用户显示设备 ID，即使设备 ID 已预配置并在使用 BYOD 门户时无法更改也如此。
原始 URL (Originating URL)	成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示“身份验证成功”(Authentication Success) 页面。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的Cisco ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。 对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。
注册成功页面	显示设备注册成功的页面。
URL	成功对网络进行身份验证后，将用户的浏览器重定向到指定的 URL，例如贵公司的网站。

注释 如果在身份验证后将访客重定向到外部 URL，可能会在解析 URL 地址和重定向会话时存在延迟。

相关主题

自带设备门户，第 695 页
创建 BYOD 门户，第 707 页
自带设备门户语言文件的 HTML 支持，第 427 页

证书调配门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **证书调配门户 (Certificate Provisioning Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在 **门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。

- 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。

- **身份验证方法 (Authentication Method)**：选择将哪个身份源序列或身份提供程序 (IdP) 用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  Cisco ISE 包含适用于发起人门户的默认身份源序列：Sponsor_Portal_Sequence。

  要配置 IdP，请选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。

  要配置身份源序列，请依次选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)**。

- **配置授权组 (Configure authorized groups)**：选择要为其授予权限以生成证书并将证书移至“已选”(Chosen) 框的用户身份组。

- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**：为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com,sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。

  如果更改默认 FQDN，还需执行以下操作：

  - 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在Cisco ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。

- **空闲超时 (Idle Timeout)**：输入Cisco ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。

登录页面设置

- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定Cisco ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。

- **包含 AUP (Include an AUP)**：将可接受使用政策页面添加到流。可以将 AUP 添加到页面，或链接到另一个页面。

可接受使用政策 (AUP) 页面设置

- **包含 AUP (Include an AUP)**：在单独的页面上向用户显示公司的网络使用条款和条件。
- **对员工使用不同的 AUP (Use Different AUP for Employees)**：仅为员工显示不同的 AUP 及网络使用条款和条件。如果您选择此选项，则不能同时选择**跳过面向员工的 AUP (Skip AUP for employees)**。
- **对员工跳过 AUP (Skip AUP for Employees)**：员工在访问网络之前无需接受 AUP。如果您选择此选项，则不能同时选择**使用面向员工的不同 AUP (Use different AUP for employees)**。
- **要求接受 (Require Acceptance)**：在完全启用用户的帐户之前要求用户接受 AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
- **要求滚动至 AUP 末尾 (Require Scrolling to End of AUP)**：此选项仅在已启用**在页面上包含 AUP (Include an AUP on page)** 时显示。

  确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。配置何时向用户显示 AUP。

  - **仅首次登录时 (On First Login only)**：仅在用户首次登录网络或门户时显示 AUP。
  - **每次登录时 (On Every Login)**：每次用户登录网络或门户时都显示 AUP。
  - **每 __ 天（从首次登录算起）(Every __ Days [starting at first login])**：在用户首次登录网络或门户后定期显示 AUP。

相关主题

证书调配门户，第 695 页
创建证书调配门户，第 708 页
证书调配门户语言文件的 HTML 支持，第 428 页

客户端调配门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)**。

门户设置

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果您已使用此范围外的端口值进行升级，则在对此页面进行任何更改之前会遵循这些设置。如果您对此页面进行任何更改，则必须更新端口设置以遵守此限制。
- **允许接口 (Allowed interfaces)**：选择可以运行门户的 PSN 接口。仅配备了允许接口的 PSN 可以创建门户。您可以配置物理接口和绑定接口的任意组合。这是整个 PSN 的配置；所有门户只能在这些接口上运行，这些接口配置被推送到所有节点。
  - 您必须使用不同子网上的 IP 地址配置以太网接口。

- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书主题名称/备用主题名称必须解析到接口 IP。
- 在 ISE CLI 中配置 ip host x.x.x、x yyy.domain.com 以将辅助接口 IP 映射到 FQDN，FQDN 将用于匹配证书主题名称/备用主题名称。
- 如果仅选定绑定 NIC - 当 PSN 尝试配置其首次尝试配置该绑定接口的门户时。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。它不会尝试在物理接口上启动门户。
- **NIC 结合 (NIC Teaming)** 或绑定是一个 O/S 配置选项，通过该选项可以配置两个独立的 NIC 以实现高可用性（容错能力）。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据门户设置配置为门户选定一个 NIC：
  - 如果物理 NIC 和相应的绑定 NIC 均已配置 - 当 PSN 尝试配置门户时会首先尝试连接到绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group Tag)**：选择要用于门户 HTTPS 流量的证书组的组标签。
- **身份验证方法 (Authentication Method)**：选择用于用户身份验证的身份源序列 (ISS) 或身份提供程序 (IdP)。ISS 是按顺序搜索验证用户凭证的身份库的列表。一些示例包括：内部访客用户、内部用户、Active Directory 和 LDAP 目录。

  Cisco ISE 包含客户端调配门户的默认客户端调配身份源序列，Sponsor_Portal_Sequence。
- **完全限定域名 (Fully Qualified Domain Name [FQDN])**：为客户端调配门户输入至少一个唯一 FQDN 和/或主机名。例如，您可以输入 provisionportal.yourcompany.com，以便在用户将其中任一名称输入到浏览器中时，可以访问客户端调配门户。
  - 更新 DNS，以确保新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在Cisco ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。

  注释 对于没有 URL 重定向的客户端调配，必须在 DNS 配置中配置完全限定域名 (FQDN) 字段中输入的门户名称。此 URL 必须传达给用户，以在没有 URL 重定向的情况下启用客户端调配。
- **空闲超时 (Idle Timeout)**：输入Cisco ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。

注释 在客户端调配门户中，可以定义端口号和证书，以便主机允许您为客户端调配和终端安全评估下载相同的证书。如果门户证书由官方证书颁发机构签名，您将不会收到任何安全警告。如果证书是自签证书，您将收到门户和Cisco AnyConnect 终端安全评估组件二者的同一安全警告。

登录页面设置

- 启用登录 (Enable Login)：选择此复选框可在客户端调配门户中启用登录步骤
- 速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)：指定在 Cisco ISE 开始人为减缓可进行登录尝试的速率（从而防止更多登录尝试）之前，单个浏览器会话的失败登录尝试次数。在 **Time between login attempts when rate limiting** 中指定了达到此失败登录次数后，前后两次尝试之间的间隔时间。
- 限制速率时登录尝试之间的间隔时间 (Time between login attempts when rate limiting)：设置用户在达到**速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)** 中定义的登录失败次数后，尝试再次登录之前必须等待的时间长度（以分钟为单位）。
- 包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])：显示公司的网络使用条款和条件，可以是当前为用户显示的页面上的文本，或是一个链接，能够打开包含 AUP 文本的新选项卡或窗口。
- 要求接受 (Require acceptance)：要求用户必须接受 AUP，然后才能访问门户。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，便无法访问该门户。
- 要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)：此选项仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 时显示。确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。

可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)

- 包含一个 AUP (Include an AUP)：在单独的页面上向用户显示公司的网络使用条款和条件。
- 要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)：确保用户已完全阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活“接受”(Accept) 按钮。
- 仅在首次登录时 (On first login only)：仅在用户首次登录到网络或门户时显示 AUP。
- 在每次登录时 (On every login)：每次用户登录到网络或门户时都显示 AUP。
- 每 __ 天（从首次登录算起）(Every __ days [starting at first login])：在用户首次登录到网络或门户后定期显示 AUP。

登录后横幅页面设置

包含登录后横幅页面 (Include a Post-Login Banner page)：在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

更改密码设置 (Change Password Settings)

允许内部用户更改其密码 (Allow internal users to change their own passwords)：允许内部用户在登录到客户端调配门户后更改其密码。这仅适用于帐户存储于Cisco ISE 数据库中的员工，不适用于帐户存储于外部数据库（例如 Active Directory 或 LDAP）的员工。

相关主题

客户端调配门户，第 696 页
创建客户端调配门户，第 709 页
客户端调配门户语言文件的 HTML 支持，第 429 页

MDM 门户的员工移动设备管理设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **MDM 门户 (MDM Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流设置 (Portal Behavior and Flow Settings)** > **员工移动设备管理密码 (Employee Mobile Device Management Settings)**。

使用这些设置为使用 MDM 门户的员工启用移动设备管理 (MDM) 功能，定义他们的 AUP 体验。

字段名称	使用指南
包含一个 AUP（在页面上/作为链接） (Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的页面上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。

相关主题

移动设备管理门户，第 696 页
创建 MDM 门户，第 711 页
移动设备管理器与思科 ISE 的互操作性

我的设备门户的门户设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此页面之前会遵循这些设置。如果修改此页面，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在 **门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在Cisco ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。

- 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
- 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**：为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com,sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。

  如果更改默认 FQDN，还需执行以下操作：

  - 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在Cisco ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。

- **身份验证方法 (Authentication Method)**：选择将哪个身份源序列或身份提供程序 (IdP) 用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  Cisco ISE 包含适用于发起人门户的默认身份源序列：Sponsor_Portal_Sequence。

  要配置 IdP，请选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **SAML ID 提供程序 (SAML Id Providers)**。

  要配置身份源序列，请依次选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份源序列 (Identity Source Sequences)**。

- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。Cisco ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

  选择用于跟踪员工设备的终端身份组。Cisco ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

- **当此身份组中的终端达到 __ 天时将其清除 (Purge Endpoints in this Identity Group when they Reach __ Days)**：指定从Cisco ISE 数据库中清除设备之前应经历的天数。每天都会进行清除，并且清除活动与整体清除时间同步。更改全局应用于此终端身份组。

  如果根据其他策略条件对终端清除策略进行更改，则此设置不可再使用。

- **空闲超时 (Idle Timeout)**：输入Cisco ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。

- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果Cisco ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或Cisco ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

相关主题

我的设备门户，第 696 页
创建我的设备门户，第 712 页

我的设备门户的登录页面设置

- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定Cisco ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定Cisco ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **包含 AUP (Include an AUP)**：将可接受使用政策页面添加到流。可以将 AUP 添加到页面，或链接到另一个页面。

相关主题

我的设备门户，第 696 页
创建我的设备门户，第 712 页
监控我的设备门户和终端活动，第 716 页

我的设备门户的可接受使用策略页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)**.

使用这些设置可定义用户（适用情况下的访客、发起人或员工）的 AUP 体验。

字段	使用指南
包含 AUP 页面 (Include AUP page)	在单独的页面上向用户显示公司的网络使用条款和条件。

字段	使用指南
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。
仅首次登录时 (On First Login only)	仅在用户首次登录到网络或门户时显示 AUP。
每次登录时 (On Every Login)	每次用户登录到网络或门户时显示 AUP。
每 __ 天（从首次登录算起）(Every __ Days [starting at first login])	在用户首次登录到网络或门户时定期显示 AUP。

相关主题

我的设备门户，第 696 页
创建我的设备门户，第 712 页

我的设备门户的登录后横幅页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **登录后横幅页面设置 (Post-Login Banner Page Settings)**.

使用此设置可在用户（适用情况下的访客、发起人或员工）成功登录后向其通知其他信息。

字段名称	使用指南
包含登录后横幅页面 (Include a Post-Login Banner page)	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

相关主题

我的设备门户，第 696 页
创建我的设备门户，第 712 页

我的设备门户的员工更改密码设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **员工更改密码设置 (Employee Change Password Settings)**。这些设置用于为使用 My Devices 门户的员工定义密码要求。

要设置员工密码策略，请选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **用户密码策略 (User Password Policy)**.

字段名称	使用指南
Allow internal users to change password	在员工登录My Devices门户后，允许员工更改其密码。 这仅适用于帐户存储于Cisco ISE 数据库中的员工，不适用于帐户存储于外部数据库（例如Active Directory 或 LDAP）的员工。

相关主题

创建我的设备门户 ，第 712 页
门户中的 UTF-8 字符支持 ，第 106 页

管理我的设备门户的设备设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户页面定制 (Portal Page Customization)** > **管理设备 (Manage Devices)**。

在**页面定制 (Page Customizations)** 下，您可以定制“我的设备”(My Devices) 门户的**管理帐户 (Manage Accounts)** 选项卡上显示的消息、标题、内容、说明和字段与按钮标签。

在**设置 (Settings)** 下，您可以指定使用此门户的员工可以在其已注册的个人设备上执行的操作。

表 *212:* 管理我的设备门户的设备设置

字段名称	使用指南
Lost	使员工可以指示其设备已丢失。此操作会将 My Devices 门户中的设备状态更新为 Lost 并将该设备添加至 Blacklist 终端身份组。
Reinstate	此操作可恢复列入黑名单、已丢失或被盗的设备并将其状态重置为上一次的已知值。此操作会将被盗设备的状态重置为 Not Registered，因为它要经过额外调配才能连接网络。 如果您要阻止员工恢复您已列入黑名单的设备，请勿在“我的设备”(My Devices) 门户中启用此选项。

字段名称	使用指南
删除	使员工在已注册设备达到最大数量时，可以从“我的设备”(My Devices)门户删除已注册设备或删除未使用的设备和添加新设备。此操作会将设备从 My Devices 门户中显示的设备列表上删除，但是设备仍保留在Cisco ISE 数据库中并继续列于 Endpoints 列表上。 要定义员工可以使用 BYOD 门户或“我的设备”(My Devices) 门户注册的个人设备最大数量，请依次选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。 要从Cisco ISE 数据库中永久删除设备，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。
Stolen	使员工可以指示其设备已被盗。此操作会将 My Devices 门户中的设备状态更新为 Stolen 并将该设备添加至 Blacklist 终端身份组，然后删除其证书。
Device lock	仅适用于已向 MDM 注册的设备。 在员工设备丢失或被盗的情况下，使员工可以立即从 My Devices 门户远程锁定其设备。此操作可防止他人未经授权而使用设备。 但是，在 My Devices 门户中无法设置 PIN 而且员工应已提前在其移动设备上配置 PIN。
Unenroll	仅适用于已向 MDM 注册的设备。 如果员工在工作中不再需要使用其设备，则可以选择此选项。此操作仅删除您公司安装的那些应用和设置，其他应用和数据仍会保留在员工的移动设备上。
Full wipe	仅适用于已向 MDM 注册的设备。 使员工丢失其设备或换成使用新设备的情况下可以选择此选项。此操作会将员工的移动设备重置为其默认出厂设置，删除所安装的应用和数据。

相关主题

管理员工添加的个人设备，第 715 页
我的设备门户，第 696 页

为我的设备门户自定义添加、编辑和定位设备

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户页面自定义 (Portal Page Customization)** > **添加设备、编辑设备或定位设备 (Add Devices, Edit Devices or Locate Devices)**。

在 **Page Customizations** 下，您可以自定义显示在我的设备门户的添加、编辑和定位选项卡中的消息、标题、内容、说明以及字段和按钮标签。

相关主题

我的设备门户，第 696 页
创建我的设备门户，第 712 页

设备门户的支持信息页面设置

要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD 门户 (BYOD Portals)**、**客户端调配门户 (Client Provisioning Portals)**、**MDM 门户 (MDM Portals)** 或**我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流程设置 (Portal Behavior and Flow Settings)** > **支持信息页面设置 (Support Information Page Settings)**.

使用这些设置可显示服务中心可用于对用户（适用情况下的访客、发起人或员工）遇到的访问问题进行故障排除的信息。

字段名称	使用指南
包含支持信息页面 (Include a Support Information Page)	在门户的所有已启用页面上显示指向信息页面（例如**联系我们 [Contact Us]**）的链接。
MAC 地址	在**支持信息 (Support Information)** 窗口上包含设备的 MAC 地址。
IP 地址	在**支持信息 (Support Information)** 窗口上包含设备的 IP 地址。
浏览器用户代理	在**支持信息 (Support Information)** 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 (Policy Server)	在**支持信息 (Support Information)** 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，请选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。
隐藏字段 (Hide Field)	如果字段标签将会包含的信息不存在，请勿在**支持信息 (Support Information)** 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示**故障代码 (Failure code)**，即使已选择故障代码也如此。
显示不含任何值的标签 (Display Label with no Value)	在**支持信息 (Support Information)** 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示**故障代码 (Failure code)**，即使其为空白也如此。

字段名称	使用指南
显示含默认值的标签 (Display Label with Default Value)	如果标签将会包含的信息不存在，请在**支持信息 (Support Information)** 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用”(Not Available)，并且故障代码未知，则**故障代码 (Failure Code)** 将显示**不可用 (Not Available)**。

相关主题

监控我的设备门户和终端活动，第 716 页
访问设备门户，第 695 页

第 14 章

pxGrid

pxGrid 和思科 ISE

Cisco pxGrid 是一个开放且可扩展的安全产品集成框架 (SPIF)，允许任意合作伙伴平台双向集成。

pxGrid 1.0 使用传统可扩展消息传送和网真协议 (XMPP) 实施方法。pxGrid 1.0 处于维护模式，很快将被删除。Cisco pxGrid 1.0 需要客户端 SDK 库（Java 或 C）才能使用 pxGrid。

pxGrid 2.0 使用 REST 和 WebSocket 接口。客户端使用 REST 处理控制消息、查询和应用数据，并使用 WebSocket 推送事件。有关 pxGrid 2.0 的详细信息，请参阅**欢迎学习思科平台交换网格 (pxGrid)**。

Cisco pxGrid 可以：

- 与其他网络系统（例如 ISE 生态系统合作伙伴系统）和其他Cisco平台共享Cisco ISE 会话目录中的情景相关信息。
- 让第三方系统能调用自适应网络控制操作隔离用户和设备以应对网络或安全事件。标签定义、值和说明等 TrustSec 信息通过 TrustSec 主题从Cisco ISE 传输到其他网络。
- 通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从Cisco ISE 发送到其他网络。
- 批量下载标签和终端配置文件。
- 通过 pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅《思科 ISE 管理员指南》中“分段”一章中的安全组标签交换协议部分。
- Cisco pxGrid Context-in 使生态系统合作伙伴能够将主题信息发布到Cisco ISE。因此Cisco ISE 能够根据生态系统中识别的资产采取行动。有关 Cisco pxGrid Context-in 的详细信息，请参阅 pxGrid Context-In。

注释 pxGrid 1.0 处于维护模式，很快将被弃用。我们在 ISE 2.4 中引入了 pxGrid 2.0。我们强烈建议合作伙伴将其 pxGrid 客户端实施切换到 pxGrid 2.0。

pxGrid 概述

pxGrid 具有以下组件：

- 控制器：处理发现、身份验证和授权。
- 提供程序：返回查询结果或发布。
- Pubsub：为提供程序和使用者提供 pxGrid 服务。
- 用户：获得授权后，用户会从订阅的主题获取情景信息和警报。

pxGrid 提供以下功能：

- 发现：根据服务名称发现服务属性。当提供程序要求向 pxGrid 控制器“注册服务”时，流程开始。注册后，消费者使用“查找服务”发现提供商的位置。
- 身份验证：pxGrid 控制器验证 pxGrid 客户端有否有权访问服务。凭证为用户名和密码或证书（首选）。
- 授权：当 pxGrid 收到操作请求时，它会与 pxGrid 控制器协商以授权请求。pxGrid 将客户端分配到预定义的组。

pxGrid 1.0 的高可用性

使用 pxGrid 1.0 时，您可以配置两个在主/备模式下运行 pxGrid 角色的节点。Cisco pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 断开连接时，pxGrid 服务器会停止处理客户端注册和订用。您必须手动升级 PAN 才能激活 pxGrid 服务器。

您可以使用 CLI 命令 **show application status ise** 查看 pxGrid 进程。以下与 pxGrid 1.0 相关的进程是：

- pxGrid Infrastructure Service
- pxGrid Publisher Subscriber Service
- pxGrid Connection Manager
- pxGrid 控制器

在活动 pxGrid 1.0 节点上，这些进程显示为“正在运行”(Running)。在备用 pxGrid 1.0 节点上，它们显示为“已禁用”(Disabled)。如果活动 pxGrid 1.0 **show logging application pxgrid.state**节点关闭，备用 pxGrid 节点会检测到此丢失情况，并启动四个 pxGrid 进程。在几分钟内，这些进程显示为“正在运行”(Running)，并且备用节点变为活动节点。您可以通过运行 CLI 命令 **show logging application pxgrid** 验证此节点上的 pxGrid 是否处于备用状态。

Cisco ISE 会自动故障转移到辅助 pxGrid 节点。如果您将原始主 pxGrid 节点重新连接到网络，原始主 pxGrid 节点将继续担当辅助角色，并且不会升级回主角色，除非您关闭当前的主节点。

pxGrid 2.0 的高可用性

pxGrid 2.0 节点在主动/主动配置下运行。为实现高可用性，部署中应至少有两个 pxGrid 节点。大型部署最多可以有四个节点，以增加规模和冗余。我们建议您为所有节点配置 IP 地址，以便在一个节

点关闭时，该节点的客户端连接到工作节点。当 PAN 关闭时，pxGrid 服务器会停止处理激活。手动升级 PAN 才能激活 pxGrid 服务器。有关 pxGrid 部署的详细信息，请参阅 **ISE 性能和扩展**。

所有 pxGrid 服务提供商客户端会在 7.5 分钟内定期向 pxGrid 控制器重新注册。如果客户端未重新注册，PAN 节点会认定它处于非活动状态，并删除该客户端。如果 PAN 节点关闭超过 7.5 分钟，当它恢复正常运行时，它将删除时间戳值早于 7.5 分钟的所有客户端。所有这些客户端都必须再次向 pxGrid 控制器注册。

pxGrid 2.0 客户端使用 WebSocket 和基于 REST 的 API 进行发布/订阅和查询。这些 API 由端口 8910 上的 ISE 应用服务器提供。通过 **show logging application pxgrid** 显示的 pxGrid 进程不适用于 pxGrid 2.0。

丢失检测

在Cisco ISE 3.0 中，我们向 pxGrid 主题添加了序列 ID。如果传输中断，用户可以通过检查 ID 序列中的缺口来识别这种情况。用户注意到主题序列 ID 发生变化，根据最后一个序列号的日期请求数据。如果发布者关闭，则当它恢复时，主题序列从 0 开始。当用户看到序列 0 时，必须清除缓存并开始批量下载。如果用户关闭，发布者会继续分配顺序 ID。当用户重新连接后发现序列 ID 出现缺口时，用户会从最后一个序列号的时间开始请求数据。丢失检测配合 Session Directory 和 TrustSec 配置运行。对于 Session Directory，当客户端检测到丢失时，必须清除缓存并开始批量下载。

如果您现有的应用不使用序列ID，则不必使用它们。但是，使用它们有助于检测丢失情况并从丢失中恢复。

Session Directory 会话是批处理的，在每个通知间隔内由 MnT 异步发布到 `/topic/com.cisco.ise.session`。

Trust Sec Config Security Group 安全组的更改将发布到 `/topic/com.cisco.ise.config.trustsec.security.group`。

丢失检测仅受 pxGrid 2.0 支持，默认情况下处于启用状态。

要查看使用丢失检测的代码示例，请参阅https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise。

监控和调试

以下日志可用于 pxGrid：

- pxgrid.log：pxGrid 1.0 进程活动
- pxgrid-server.log：pxGrid 2.0 活动和错误
- pxgrid-cm.log：pxGrid 1.0 连接日志
- pxgrid-controller.log：pxGrid 1.0 控制消息日志
- pxgrid-jabberd.log：pxGrid 1.0 XMPP 服务器日志
- pxgrid-pubsub.log：pxGrid 1.0 XMPP Pubsub 日志

日志 (Log) 页面显示所有 pxGrid 2.0 管理事件。事件信息包括客户端和功能名称，以及事件类型和时间戳。导航至**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > 日志 (Log)** 以查看事件列表。您还可以清除日志并重新同步或刷新列表。

pxGrid 摘要页面

“摘要”(Summary) 页面显示当前 pxGrid 2.0 环境的统计信息。

- 当前连接 (Current Connections)：列出与控制器的连接
- 控制消息 (Control Messages)：身份验证、授权和服务发现
- REST API：使用 WebSocket 或 XMPP 连接的客户端数量
- Pubsub 吞吐量 (Pubsub Throughput)：发布到客户端的数据量
- 客户端 (Clients)：通过 REST 或 WebSocket 连接的客户端
- 错误数 (Errors)：导致客户端请求重新启动数据传输的传输错误数

pxGrid 客户端管理

当新客户端连接到 pxGrid 时，管理员必须访问此页面以批准客户端，然后客户端才能参与网格。但是，如果在**设置 (Settings)** 页面上启用了自动批准基于证书的帐户，则无需手动审批。

- **客户端 (Clients)**：同时列出 pxGrid 1.0 和 2.0 的外部客户端帐户。
- **pxGrid 策略 (pxGrid Policy)**：列出客户端可以订阅的可用服务。您可以编辑策略以更改哪些组可以访问该策略。您还可以为尚无策略的服务创建新策略。
- **组 (Groups)**：默认组为 EPS 或 ANC。您可以添加更多组，并使用它们限制对服务的访问。

  pxGrid 客户端可以通过使用 REST API 发送用户名向 pxGrid 控制器注册。在客户端注册时，pxGrid 控制器为 pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。
- **证书 (Certificates)**：您可以生成新证书以使用Cisco ISE 内部证书颁发机构。

  有关为 pxGrid 创建证书的信息，请参阅：
  - 随思科 pxGrid 部署证书 - 使用自签证书和思科 ISE 2.0/2.1/2.2 更新
  - 随思科 pxGrid 部署证书 - 使用外部 CA 和思科 ISE 2.0/2.1/2.2 更新

控制 pxGrid 策略

您可以创建 pxGrid 授权策略来控制对 pxGrid 客户端可访问服务的访问。这些策略控制哪些服务可供 pxGrid 客户端使用。

您可以创建不同类型的组，并将 pxGrid 客户端的可用服务映射到这些组。使用**客户端管理 > 组 (Client Management > Groups)** 窗口中的**管理组 (Manage Groups)** 选项添加新组。您可以在“策略”(Policies) 窗口中查看使用预定义组（例如 EPS 和 ANC）的预定义授权策略。

要为 pxGrid 客户端创建授权策略，请执行以下操作：

SUMMARY STEPS

1. 从**管理 (Administration)** 中选择 **pxGrid 服务 (pxGrid Services) > 客户端管理 (Client Management) > 策略 (Policy)**，并点击**添加 (Add)** 按钮。
2. 从**服务 (Service)** 下拉列表中选择服务：
3. 从**操作 (Operation)** 下拉列表中，选择以下选项之一：
4. 从**组 (Groups)** 下拉列表中，选择要映射到此服务的组。
5. 点击**提交 (Submit)**。

DETAILED STEPS

步骤 1 从**管理 (Administration)** 中选择 **pxGrid 服务 (pxGrid Services) > 客户端管理 (Client Management) > 策略 (Policy)**，并点击**添加 (Add)** 按钮。

步骤 2 从**服务 (Service)** 下拉列表中选择服务：

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc
- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

步骤 3 从**操作 (Operation)** 下拉列表中，选择以下选项之一：

- <ANY>
- 发布

- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM> - 如果选择此选项，可以指定自定义操作。

步骤 4 从**组 (Groups)** 下拉列表中，选择要映射到此服务的组。

预定义组（例如 EPS 和 ANC）和手动添加的组列在此下拉列表中。

步骤 5 点击**提交 (Submit)**。

启用 pxGrid 服务

开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看Cisco pxGrid 客户端发送的请求。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)**。

步骤 2 选中该客户端旁边的复选框，然后点击**通过 (Approve)**。

步骤 3 点击**刷新 (Refresh)** 查看最新的状态。

步骤 4 选择要启用的功能，并点击**启用 (Enable)**。

步骤 5 点击**刷新 (Refresh)** 查看最新的状态。

pxGrid 诊断

- XMPP：**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > XMPP** 页面列出了外部和内部 pxGrid 1.0 客户端。此外还列出了功能。
- Websocket：**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > Websocket** 页面列出了外部和内部 pxGrid 2.0 客户端。它还列出了可用 pxGrid 2.0 主题，以及发布或订阅每个主题的客户端。
- 日志：**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > 实时日志 (Live Logs)** 页面列出了管理事件。
- 测试：在**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > 测试 (Tests)** 页面上，运行状况监控测试将验证客户端能否访问会话目录服务。点击**开始测试 (Start Test)** 按钮时，我们将创建一个内部 pxGrid 2.0 客户端。此客户端会查询批量会话下载 REST API，然后订阅会话主题。它侦听该主题几分钟，然后终止。测试完成后，可以显示测试活动的日志。

pxGrid 设置

- **自动批准新的基于证书的帐户 (Automatically approve new certificate-based accounts)**：默认情况下关闭，可以让您控制与 pxGrid 服务器的连接。仅当您信任环境中的所有客户端时，才选中此设置。
- **允许创建基于密码的帐户 (Allow password based account creation)**：选中此复选框可为 pxGrid 客户端启用基于用户名/密码的身份验证。如果启用此选项，系统不会自动批准 pxGrid 客户端。

生成思科 pxGrid 证书

开始之前

某些版本的Cisco ISE 具有使用 NetscapeCertType 的Cisco pxGrid 证书。建议您生成新证书。

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 必须从主 PAN 生成Cisco pxGrid 证书。
- 如果Cisco pxGrid 证书使用了使用者替代名称 (SAN) 扩展名，请确保将使用者身份的 FQDN 包含为 DNS 名称条目。
- 创建使用数字签名用法的证书模板，并使用该模板生成新的Cisco pxGrid 证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **客户端管理 (Client Management)** > **证书 (Certificates)**。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **生成无证书签名请求的单个证书 (Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。
- **生成单个证书（带证书签名请求）Generate a single certificate (with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。
- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载根证书，并将其添加到受信任证书存储区。必须指定主机名和证书的下载格式。

步骤 3 **通用名称 (CN) (Common Name (CN))**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入 pxGrid 客户端的 FQDN。

步骤 4 **证书签名请求详细信息 (Certificate Signing Request Details)**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入完整的证书签名请求详细信息。

步骤 5 **说明**：（可选）可以输入此证书的说明。

步骤 6 **证书模板 (Certificate Template)**：点击 **pxGrig_Certificate_Template** 链接可下载证书模板，并根据您的要求进行编辑。

步骤 7 **使用者备用名称 (SAN) (Subject Alternative Name (SAN))**：可以添加多个 SAN。可提供以下选项：

- **IP 地址 (IP address)**：输入要与证书关联的Cisco pxGrid 客户端的 IP 地址。
- **FQDN**：输入 pxGrid 客户端的完全限定域名。

注释 如果选定**生成批量证书 (Generate Bulk Certificate)** 选项，则不会显示此字段。

步骤 8 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE) ----”标签。终端实体的私钥使用 PKCS* PEM 存储。其开头采用“-----加密私钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密私钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。
- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format (including certificate chain; one file for both the certificate chain and key))**：CA 根证书、CA 中间证书以及终端实体的证书和私钥存储在一个加密文件时，所采用的二进制格式。

步骤 9 **证书密码 (Certificate Password)**：输入证书的密码，并在下一字段中再次输入以确认密码。

步骤 10 点击**创建 (Create)**。

您创建的证书在Cisco ISE 的**已颁发证书 (Issued Certificates)** 窗口中可见。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发证书 (Issued Certificates)**。证书也会下载到浏览器的“下载”目录中。

注释 从Cisco ISE 2.4 补丁 13 开始，pxGrid 服务的证书要求变得更加严格。如果您使用Cisco ISE 默认自签名证书作为 pxGrid 证书，则Cisco ISE 可能会在应用Cisco ISE 2.4 补丁 13 或更高版本后拒绝此证书。这是因为此证书的旧版本具有指定为 **SSL 服务器 (SSL Server)** 的 **Netscape 证书类型 (Netscape Cert Type)** 扩展，此扩展现在会失败（现在还需要客户端证书）。

任何具有不合规证书的客户端都无法与Cisco ISE 集成。使用内部 CA 颁发的证书或生成具有正确使用扩展名的新证书：

- 证书中的**密钥使用 (Key Usage)** 扩展必须包含**数字签名 (Digital Signature)** 和**密钥加密 (Key Encipherment)** 字段。
- 证书中的**扩展密钥使用 (Extended Key Usage)** 扩展必须包含**客户端身份验证 (Client Authentication)** 和**服务器身份验证 (Server Authentication)** 字段。
- 不需要 **Netscape 证书类型 (Netscape Certificate Type)** 扩展。如果要包含此扩展，则必须在扩展中同时添加 **SSL 客户端 (SSL Client)** 和 **SSL 服务器 (SSL Server)**。
- 如果使用的是自签名证书，则**基本约束 CA (Basic Constraints CA)** 字段必须设置为 True，并且**密钥使用 (Key Usage)** 扩展必须包含**密钥证书签名 (Key Cert Sign)** 字段。

第 15 章

集成

• 在无线 LAN 控制器上配置 ACL 以实现移动设备管理互操作 ， 第 1203 页

什么是无线设置

无线设置为设置 802.1x、访客和 BYOD 无线流提供了一种简单的方法。适当情况下，它还提供一些工作流程，用于为访客和 BYOD 配置和自定义每个门户。这些工作流程提供最常见的建议设置，要比在 ISE 中配置关联门户流程简单得多。无线设置会代为执行原本您需要在 ISE 和 WLC 中自己完成的许多步骤，以便您能够快速创建工作环境。

您可以使用无线设置创建的环境来测试和开发自己的流程。无线设置环境正常运行后，您可能希望切换到 ISE，以便支持更高级的配置。有关在 ISE 中配置访客的详细信息，请参阅 ISE 版本对应的《 ISE 管理员指南》和Cisco社区站点https://community.cisco.com/t5/security-documents/ise-guest-amp-web-authentication/ta-p/3657224。有关为 ISE 配置和使用无线设置的详细信息，请参阅 https://community.cisco.com/t5/security-documents/cisco-ise-secure-access-wizard-saw-guest-byod-and-secure-access/ta-p/3636602。

注释 ISE 无线设置为测试版软件，请勿在生产网络中使用。

- 全新安装Cisco ISE 后，**无线设置默认被禁用**。您可以在 ISE CLI 中使用 **application configure ise** 命令（选择选项 17）或使用 ISE GUI 主页中的无线设置选项启用无线设置。
- 如果从以前的版本升级 ISE，无线设置将不起作用。只有新安装的 ISE 才支持无线设置。
- 无线设置仅适用于独立节点。
- 一次仅运行一个无线设置实例；一次只能一人运行无线设置。
- 无线设置需要打开端口 9103 和 9104。要关闭这些端口，请使用 CLI 禁用无线设置。
- 如果要在运行某些流程后开始全新安装无线设置，可以使用 CLI 命令 **application reset-config ise**。此命令会重置 ISE 配置并清除 ISE 数据库，但保留网络定义。因此，您可以重置 ISE 和无线设置，而无需重新安装 ISE 并运行设置。

  如果要从无线设置重新开始，可以通过以下步骤同时重置 ISE 和无线设置的配置：

  - 在 CLI 中，运行 **application reset-config** 以重置所有 ISE 配置。如果您在全新安装中测试无线设置，此命令会删除无线设置在 ISE 中完成的配置。
  - 在 CLI 中，运行 **application configure ise**，然后选择 **[18]重置配置 Wi-Fi 设置**。这将清理无线设置配置数据库。
  - 在 WLC 上，删除无线设置在 WLC 上添加的配置。有关无线设置在 WLC 上的配置的信息，请参阅通过无线设置对 ISE 和 WLC 所做的更改 ， 第 1194 页。

  您可以在完成 ISE 全新安装后为虚拟机创建快照，以便避免这些步骤。

  有关 CLI 的详细信息，请参阅 ISE 版本对应的《思科身份服务引擎 CLI 参考指南》。
- 您必须是 ISE 超级管理员用户才能使用无线设置。

- 无线设置需要至少两个 CPU 核心和 8 GB 内存。
- 仅支持 Active Directory 组和用户。在无线配置中创建一个或多个流后，其他类型的用户、组和授权将可用于无线设置，但必须在 ISE 上进行配置。
- 如果已在 ISE 中定义 Active Directory，并计划将此 AD 用于无线设置，则：
  - 加入名称和域名必须相同。如果名称不同，请在 ISE 中使之相同，然后在无线设置中使用该 AD。
  - 如果已在 ISE 上配置 WLC，则必须为 WLC 配置共享密钥。如果 WLC 定义没有共享密钥，请添加共享密钥或从 ISE 中删除 WLC，然后在无线设置中配置该 WLC。
- 无线设置可以配置 ISE 组件，但在流程启动后无法删除或修改这些组件。有关无线设置在 ISE 中配置的所有项目的列表，请参阅 ISE 版本对应的《思科身份服务引擎 CLI 参考指南》。
- 启动流程时，必须完成该流程。点击流程中的痕迹可停止流程。当您逐步完成流程时，系统会动态更改 ISE 配置。无线设置会提供配置更改列表，以便您可以手动恢复。您无法在流程中后退以进行额外的更改，只有一个例外。您可以返回以更改访客或 BYOD 门户自定义。
- 支持多个 WLC 和 Active Directory 域，但每个流程只能支持一个 WLC 和一个 Active Directory。
- 无线设置需要Cisco ISE Essentials 许可证才能运行。BYOD 需要Cisco ISE Premier许可证。
- 如果在配置无线设置之前配置了 ISE 资源，则无线设置可能与现有策略存在冲突。如果发生这种情况，无线设置会建议您在运行该工具后查看授权策略。我们建议在运行无线设置时从干净设置 ISE 开始。对无线设置和 ISE 混合配置的支持有限。
- 无线设置支持英语，但不支持其他语言。如果要在门户中使用其他语言，请在运行无线设置后在 ISE 中配置。
- BYOD 支持双 SSID。由于冲突，此配置中使用的开放 SSID 不支持访客访问。如果需要同时支持访客和 BYOD 的门户，则无法使用无线设置，并且不在本文档的讨论范围之内。
- **电子邮件和 SMS 通知**
  - 对于自注册访客，支持 SMS 和电子邮件通知。这些通知应在门户自定义通知部分进行配置。您必须将 SMTP 服务器配置为支持 SMS 和电子邮件通知。ISE 中内置的蜂窝服务提供方（包括 AT&T、T Mobile、Sprint、Orange 和 Verizon）已预先配置，是免费的邮件短信网关。
  - 访客可以在门户中选择其蜂窝网络提供方。如果其提供方不在列表中，则他们无法接收消息。您还可以配置全局提供方，但这不属于本指南的范围。如果访客门户配置了 SMS 和电子邮件通知，则必须为这两项服务输入值。
  - 发起的访客流程不会在无线设置中提供 SMS 或电子邮件通知配置。对于该流程，必须在 ISE 中配置通知服务。
  - 为门户配置通知时，请勿选择 SMS 提供方 *Global Default*。未配置此提供方（默认情况下）。

- 无线设置仅支持无 HA 的独立设置。如果决定使用额外的 PSN 进行身份验证，请将这些 PSN 的 ISE IP 地址添加到 WLC 的 RADIUS 配置。

无线设置对 Apple 迷你浏览器（强制网络助理）的支持

- **访客流**- Apple 伪浏览器的自动弹出功能适用于所有访客流。访客可以使用 Apple 的强制网络助理浏览器完成整个流程。当 Apple 用户连接到 OPEN 网络时，迷你浏览器会自动弹出，可以让他们接受 AUP（热点），或者完成自我注册或使用其凭证登录。
- **自带设备**
  - **单 SSID** - ISE 2.2 增加了对 Apple 迷你浏览器的支持。但是，为了限制 Apple 设备上潜在的 SSID 流问题，我们向重定向 ACL 中添加了 captive.apple.com，以便抑制迷你浏览器。这会导致 Apple 设备认为它可以访问互联网。用户必须手动启动 Safari，才能重定向到门户以进行 Web 身份验证或设备激活。
  - **双 SSID** - 对于从初始 OPEN 网络 WLAN 开始，然后启动访客访问，或允许员工经过设备激活 (BYOD) 并重定向到安全 SSID 的双 SSID 流，迷你浏览器也会被抑制。

有关 Apple CAN 迷你浏览器的详细信息，请参阅https://communities.cisco.com/docs/DOC-71122。

在无线网络中配置 WLC

首次登录无线设置并选择流时，系统会要求您配置无线控制器。无线设置会将必要的设置推送到 WLC，以支持您正在配置的流类型。

- WLC 必须是运行 AireOS 8.x 或更高版本的Cisco WLC。
- vWLC 不支持基于 DNS 的 ACL
- 为计划在无线设置部署中使用的接口 VLAN（网络）配置 WLC。默认情况下，WLC 具有管理接口，但建议您为访客和安全访问（员工）网络配置其他接口。
- 对于访客流，ACL_WEBAUTH_REDIRECT ACL 用于将访客设备重定向到热点或需要提供凭证的门户，以接受 AUP（热点）、登录或创建凭证。访客获得授权后，系统将允许他们访问 (ACCESS-ACCEPT)。可以在 WLC 上使用 ACL 来限制访客权限：在 WLC 上创建 ACL，然后在访客权限授权配置文件中使用此ACL。要允许访问ISE成功页面，请将此ACL添加到WLC。有关创建限制性 ACL 的详细信息，请参阅 https://communities.cisco.com/docs/DOC-68169。
- 无线设置为每个流配置 WLAN。为流配置 WLAN 后，此 WLAN 便无法用于任何其他流。如果您为自行注册流配置了 WLAN，并且稍后决定将此 WLAN 用于发起的访客流以同时处理访客的自行注册和发起，此情况为唯一例外情况。

  如果在生产环境中运行无线设置，您的配置可能会与某些现有用户断开连接。
- 如果在无线设置中使用 WLC 配置流，请勿在 ISE 中删除此 WLC。
- 如果已在ISE中配置了WLC，但未在RADIUS选项中配置共享密钥，则必须先添加共享密钥，然后才能在无线设置中使用此 WLC。

- 如果已在 ISE 中配置了 WLC，并且配置了共享密钥，则请勿使用无线设置配置其他共享密钥。无线设置和 ISE 加密密码必须匹配。您选择的 WLAN 在整个流中处于禁用状态，但可以在流结束时通过点击**上线 (Go Live)** 按钮将其重新启用。
- **远程 LAN (Remote LAN)** - 如果网络具有远程 LAN，则当无线设置尝试使用已分配给此远程 LAN 的VLAN ID 时将失败。要解决此问题，请在运行无线设置之前删除远程 LAN，或者创建您计划在 WLC 上使用的 VLAN。在无线设置中，可以为流启用这些现有 VLAN。
- **FlexConnect** - Flexconnect 本地交换机和 Flexconnect ACL 由无线设置进行配置，但不会使用或支持它们。无线设置仅适用于 Flexconnect 集中式或本地模式无线接入点和 SSID。

无线配置示例

以下 WLC 日志提取内容显示了无线设置在您配置流时执行的配置示例。

```
"config radius auth add 1 192.168.201.228 1812 ascii cisco" "config radius auth disable 1"
 "config radius auth rfc3576 enable 1" "config radius auth management 1 disable" "config
radius auth enable 1" "config radius acct add 1 192.168.201.228 1813 ascii cisco" "config
radius acct enable 1" "config acl create ACL_WEBAUTH_REDIRECT" "config acl rule add
ACL_WEBAUTH_REDIRECT 1" "config acl rule action ACL_WEBAUTH_REDIRECT 1 permit" "config acl
 rule source port range ACL_WEBAUTH_REDIRECT 1 53 53" "config acl rule protocol
ACL_WEBAUTH_REDIRECT 1 17" "config acl rule add ACL_WEBAUTH_REDIRECT 1" "config acl rule
action ACL_WEBAUTH_REDIRECT 1 permit" "config acl rule destination port range
ACL_WEBAUTH_REDIRECT 1 53 53" "config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17" "config
 acl rule add ACL_WEBAUTH_REDIRECT 1" "config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
 "config acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl rule add ACL_WEBAUTH_REDIRECT 1" "config acl rule action ACL_WEBAUTH_REDIRECT
1 permit" "config acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255" "config acl apply ACL_WEBAUTH_REDIRECT" "show flexconnect acl summary"
"config flexconnect acl create ACL_WEBAUTH_REDIRECT" "config flexconnect acl rule add
ACL_WEBAUTH_REDIRECT 1" "config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
 "config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53" "config
flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17" "config flexconnect acl rule add
ACL_WEBAUTH_REDIRECT 1" "config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
 "config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53" "config
 flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17" "config flexconnect acl rule add
 ACL_WEBAUTH_REDIRECT 1" "config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
 "config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255" "config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1" "config flexconnect
 acl rule action ACL_WEBAUTH_REDIRECT 1 permit" "config flexconnect acl rule destination
address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255" "config flexconnect acl
apply ACL_WEBAUTH_REDIRECT"
```

带无线设置的 Active Directory

需要 Active Directory 域才能创建发起人访客、802.1x 和 BYOD 流。Active Directory 可以识别发起人组的用户，以访问发起人门户、802.1x 安全访问和关联的 VLAN，以及 BYOD 和设备激活。在无线设置中配置其中任何流之后，可以选择进入 ISE 身份并添加：

- 映射到发起人组的内部发起人帐户，如 ALL_ACCOUNTS。如果使用的是 Active Directory，则不需要执行此操作。
- 属于 ISE 内部员工组的员工。确保将内部员工组添加到授权策略和 ISE 内部员工组。

无线设置中的访客门户

当访问公司的人员希望使用公司网络访问互联网或者您的网络上的资源和服务时，您可以通过访客门户为他们提供网络访问权限。在进行配置后，员工可以使用这些访客门户访问您的公司网络。

三种默认访客门户：

- 热点访客门户：授予网络访问权限，而不需要任何凭证。通常，必须在授予网络访问权限之前接受可接受的用户策略 (AUP)。

  对于热点和自注册门户，无线设置支持要求访问代码登录。

- 发起人管理的访客门户：网络访问权限由创建访客帐户的发起人授予，并为访客提供登录凭证。
- 自注册访客门户：访客可以创建自己的帐户和凭证，可能需要发起人批准后才能获得网络访问权限。

Cisco ISE 可托管多个访客门户，包括一组预定义的默认门户。

访客门户工作流程

1. 选择门户类型后，系统会询问您使用哪个控制器。为每个流配置新的无线网络。您可以选择尚未在无线设置中使用的现有 WLAN，或创建新的 WLAN。

   需要重定向的流可以选择将用户重定向到原始 URL、成功页面或特定 URL（例如，www.cisco.com）。原始 URL 需要 WLC 的支持。

   注释 直到 WLC 8.4 版本后才支持原始 URL。

2. 自定义外观并更改门户的基本设置。
3. 完成自定义后，遵循 URL 链接以测试门户。测试门户会向您显示门户测试版本的预览。您可以继续进行此流程，需要时可做出更多更改。请注意，这是唯一能够转到“成功”(Success) 页面的成功重定向。原始 URL 和静态 URL 不起作用，因为它们需要无线会话来支持重定向。测试门户不支持 RADIUS 会话，因此您将无法看到整个门户流。如果有多个 PSN，ISE 会选择第一个活动 PSN。
4. 配置完成。您可以下载并查看无线设置在 ISE 中为您执行的步骤以及工作流程期间的 WLC。

注释 位置在无线设置中不用于基本访客访问。如果要根据本地时间控制访问，则需要位置。有关在 ISE 中配置时区的信息，请参阅 SMS 运营商和服务，第 319 页。

无线网络自行注册门户

自行注册门户让访客能自行注册并创建自己的帐户，以便访问网络。

我们建议您不要选择登录成功页面，它会在屏幕上向用户显示登录凭证。最佳实践是要求用户通过电子邮件或 SMS 获取凭证，如此可将其与审核用的特定内容相关联。

无线网络发起的访客流

发起人可以使用发起人门户为授权的访客创建和管理临时帐户，以安全地访问企业网络或互联网。创建访客帐户后，发起人还可以使用发起人门户以打印文件、邮件或短信的形式向访客提供帐户详细信息。向自助注册的访客提供对企业网络的访问权限之前，系统可能会通过邮件要求发起人批准其访客帐户。

无线设置在发起流量期间配置发起人门户和发起访客门户。

无线设置不支持审批流程。

您可以在工作流程中将 Active Directory 组映射到发起人组。工作流程会将您选择的 AD 组映射到 ALL_ACCOUNTS 发起人组。它不会配置 GROUP 或 OWN 帐户发起人组。（可选）如果要添加其他身份源（如内部或 LDAP 设置），可以在 ISE 管理员 UI 中执行此操作。有关详细信息，请参阅发起人组。

无线设置 BYOD 流程 - 用于本地请求方和证书调配

自带设备 (BYOD) 门户使员工能够注册其个人设备。可以在允许访问网络之前完成本地请求方和证书调配。员工不直接访问 BYOD 门户，而是在注册个人设备时重定向到此门户。员工首次尝试使用个人设备访问网络时，系统会提示员工手动下载并启动网络设置助理 (NSA) 向导。NSA 会指导他们注册和安装本地请求方。员工注册设备后，就可以使用 My Devices 门户管理设备。

无线设置可以为本地请求方和证书调配配置 ISE 和控制器。用户与控制器建立 PEAP 连接，提供凭证，然后连接切换到 EAP-TLS（证书）。

无线设置支持以下设备：Apple 设备（Mac 和 iOS）、Windows 桌面操作系统（但不支持移动设备）和 Android。无线设置不支持 Chrome 操作系统激活。

如果是 Android 设备，请确保已启用基本身份验证访问策略，以使单个或两个基于 EAP-TLS 的 BYOD 流成功。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)** > **默认 (Default)** > **授权策略 (Authorization Policy)**，并确保 **Basic_Authenticated_Access** 规则处于活动状态。

注释 双 SSID 流包括用于激活的开放网络和用于身份验证访问的基于 TLS 证书的安全网络。设备可以连接到安全网络，而无需激活。这是因为 basic_authenticated_access 默认规则允许任何有效的身份验证通过。当设备连接到安全网络时，它们与 BYOD 受保护的授权规则不匹配，匹配项将落到 basic_authenticated_access 列表的底部。

解决方法是禁用授权策略下的 Basic_Authenticated_Access 规则，或者编辑规则以匹配特定 SSID (WLAN)。两种更改均会阻止 PEAP 连接，阻止不应允许的连接。

注释 无线设置没有授权规则来重定向标记为丢失的设备。此操作通过阻止列表完成，该列表由黑名单门户管理。有关管理丢失和被盗设备的信息，请参阅 http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf。

无线设置中的 BYOD 流程

无线设置中的 BYOD 配置包括以下步骤：

1. 选择或注册无线 LAN 控制器
2. 添加无线网络：对于双 SSID，此步骤运行两次。

   注释 新的 ISE 安装包括默认无线网络。如果是双 SSID BYOD，当用户重定向到第二个 SSID 时，还将在其网络配置文件中看到默认网络 SSID。您可以删除默认 SSID，或告诉用户忽略它。

3. 选择或加入 Active Directory (AD)：您可以覆盖激活 VLAN 和最终访问 VLAN 二者的默认 VLAN 设置。最终访问 VLAN 会映射到 Active Directory 组。
4. 自定义 BYOD 门户：您可以在此处自定义 BYOD 和“我的设备”(My Devices) 门户。您可以在此步骤中自定义 ISE 支持的所有页面。在此步骤中，提交所有门户自定义，创建策略，并将配置文件链接到相应的策略。

   注释 “我的设备”(My Devices) 门户使用 BYOD 门户自定义中的基本自定义；您无法在无线设置中自定义“我的设备”(My Devices) 门户。

5. 预览所做的配置更改，然后选择完成。

对于双 SSID BYOD

必须启用快速 SSID 以支持双 SSID BYOD。启用快速 SSID 更改后，无线控制器允许客户端在 SSID 间更快速移动。启用快速 SSID 时，不会清除客户端条目，也不会强制执行延迟。有关在Cisco WLC 上配置快速 SSID 的详细信息，请参阅《Cisco Wireless Controller 配置指南》。

建议的 WLC 计时器设置

我们建议在计划用于无线设置的 WLC 上设置以下计时器。这些设置显示在 CLI 中。

```
config radius auth retransmit-timeout {SERVER_INDEX} 5 config radius aggressive-failover
disable config radius fallback-test mode passive config wlan exclusionlist {WLAN ID} 180
config wlan exclusionlist {WLAN ID} enabled
```

802.1X 无线流

无线设置流使用 PEAP（用户名和密码凭证）配置 802.1x 无线局域网控制器。

部分流会要求您指定 Active Directory (AD)。您可以将员工 AD 组映射到 VLAN。如果要按 VLAN 划分组，可以将不同的员工组配置到不同的 VLAN。点击**访问 (Access)** 旁的下拉列表，可查看所配置的 AD 中可用的 AD 组。

如果在无线设置中选择 AD 组，则每个组都映射到 VLAN。如果 AD 组未映射到 VLAN，则用户匹配基本访问策略，该策略允许任何有效的 AD 用户登录。

员工连接至网络

1. **对员工凭证进行身份验证 (Employee Credentials Are Authenticated)** - Cisco ISE 对照公司 Active Directory 对员工进行身份验证并提供授权策略。
2. **设备重定向到 BYOD 门户 (Device Is Redirected to the BYOD Portal)** - 设备会重定向到 BYOD 门户。系统会填充设备的 MAC 地址字段，用户可以添加设备名称和说明。
3. **配置本地请求方（MacOS、Windows、iOS、Android）(Native Supplicant Is Configured [MacOS, Windows, iOS, Android])** - 配置本地请求方；但此过程因设备而异：
   - MacOS 和 Windows 设备 - 员工在 BYOD 门户中点击**注册 (Register)** 以下载和安装请求方调配向导。此向导会配置请求方，并安装用于基于 EAP-TLS 证书的身份验证的证书。颁发的证书嵌有设备的 MAC 地址和员工的用户名。

     注释 对于 MacOS，除 Apple 证书外，证书在 Mac 上显示为“未签名”(unsigned)。这不会影响 BYOD 流。

   - iOS 设备 - Cisco ISE 策略服务器使用 Apple 的 iOS 空中下载功能向 IOS 设备发送新配置文件，其中包括：
     - 颁发的证书随 IOS 设备的 MAC 地址和员工的用户名一起存储。
     - Wi-Fi 请求方配置文件，其强制使用 MSCHAPv2 或 EAP-TLS 进行 802.1X 身份验证。

- Android 设备 - Cisco ISE 会提示并引导员工从 Google Play 下载Cisco网络设置助理 (NSA)。安装应用后，员工可以打开 NSA 并启动设置向导。启动向导会生成请求方配置和已使用的颁发证书，用于配置设备。

- **发出授权更改** - 用户完成激活流程后，Cisco ISE 会发起授权更改 (CoA)。这会导致 MacOS X、Windows 和 Android 设备使用 EAP-TLS 重新连接到安全 802.1X 网络。对于单 SSID，iOS 设备也会自动连接；但是对于双 SSID，向导会提示 iOS 用户手动连接新网络。

以下操作系统支持本地请求方：

- Android（Amazon Kindle 和 B&N Nook 除外）
- Mac OS（适用于 Apple Mac 计算机）
- Apple iOS 设备（Apple iPod、iPhone 和 iPad）
- Microsoft Windows 7 和 8（RT 除外）、Vista 和 10

通过无线设置对 ISE 和 WLC 所做的更改

无线设置会在您逐步执行流程时配置 ISE 和控制器。无线设置将列出它在每个流程结束时所做的更改。此处列出了每个流程的更改以作参考，帮助您查找无线设置对 ISE 进行的所有更改，以进行查看或更改。

- **热点**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **热点门户 (Hotspot Portal)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权配置文件 (Authorization Profiles)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **策略集 (Policy Sets)**

- **自行注册**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客门户 (Guest Portals)** > **自行注册门户 (Self-reg Portal)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **门户和组件 (Portals & Components)** > **访客类型 (Guest Types)** > **访客类型 (Guest Types)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**

- 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 策略集 **(Policy Sets)**
- 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 系统 **(System)** > 设置 **(Settings)** > **SMTP** 服务器 **(SMTP Server)**
- 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 管理 **(Administration)** > 系统 **(System)** > 设置 **(Settings)** > **SMTP** 网关 **(SMTP Gateway)**

- 已发起
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 访客门户 **(Guest Portals)** > 发起的访客门户 **(Sponsored Guest Portal)** >
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 发起人门户 **(Sponsor Portals)** > > **Sponsor Portal (**发起人门户**)** >
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 策略 **(Policy)** > 策略元素 **(Policy Elements)** > 授权 **(Authorization)** > 授权配置文件 **(Authorization Profiles)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 授权策略 **(Authorization Policy)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 发起人组 **(Sponsor Groups)** > **Sponsor Groups (**发起人组**)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 门户和组件 **(Portals & Components)** > 访客类型 **(Guest Types)** > 访客类型 **(Guest Types)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > 访客访问 **(Guest Access)** > 外部 **ID** 源 **(Ext ID Sources)** > **Active Directory**

- 自带设备
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > **BYOD** > 门户和组件 **(Portals & Components)** > **BYOD** 门户 **(BYOD Portals)** > **BYOD** 门户 **(BYOD Portal)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > **BYOD** > 门户和组件 **(Portals & Components)** > 我的设备门户 **(My Devices Portals)** > 我的设备门户 **(My Devices Portal)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > **BYOD** > 策略元素 **(Policy Elements)** > 授权 **(Authorization)** > 授权配置文件 **(Authorization Profiles)**
  - 在思科 ISE GUI 中，点击菜单 **(Menu)** 图标 (☰)，然后选择 工作中心 **(Work Centers)** > **BYOD** > 授权策略 **(Authorization Policy)**

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **BYOD** > **外部 ID 源 (Ext ID Sources)** > **Active Directory**
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **BYOD** > **外部 ID 源 (Ext ID Sources)** > **Active Directory**，然后选择 AD，再选择**组 (Groups)** 选项卡。

- 安全接入
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **访客访问 (Guest Access)** > **外部 ID 源 (Ext ID Sources)** > **Active Directory**，然后选择 AD，再选择**组 (Groups)** 选项卡。

- 无线 **LAN** 控制器
  - **WLAN**
  - 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **安全 (Security)** > **访问控制列表 (Access Control Lists)**- 无线设置将创建以下 ACL：
    - 为访客和 BYOD 重定向 ACL
  - 无线设置还会创建条目。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **安全 (Security)** > **AAA** > **身份验证与记帐 (Authentication and Accounting)**

使交换机能够支持标准 Web 身份验证

请确保在交换机配置中包含以下命令，以为Cisco ISE 启用标准 Web 身份验证功能，包括身份验证后的 URL 重定向调配：

```
ip classless  ip route 0.0.0.0 0.0.0.0 10.1.2.3  ip http server ! 必须在端口 80/443
 ip http secure-server
```

上为 URL 重定向启用 HTTP/HTTPS

用于综合 RADIUS 事务的本地用户名和密码定义

输入以下命令以使交换机像该网络的 RADIUS 一样与Cisco ISE 节点通信：

```
username test-radius password 0 abcde123
```

用于确保准确日志和记账时间戳的 NTP 服务器配置

确保指定的 NTP 服务器与Cisco ISE 中设置的服务器相同。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **系统时间 (System Time)**，方法是输入以下命令：

```
ntp server <IP_address>|<domain_name>
```

启用 AAA 功能的命令

输入以下命令可启用交换机与Cisco ISE 之间的各种 AAA 功能，包括 802.1X 和 MAB 身份验证功能：

```
aaa new-model ! 创建 802.1X 基于端口的身份验证方法列表 aaa authentication dot1x default
 group radius ! VLAN/ACL 分配所必需 aaa authorization network default group
radius ! 用于 WebAuth 事务的身份验证和授权 aaa authorization auth-proxy default group
 radius ! 为 802.1X 和 MAB 身份验证启用记账 aaa accounting dot1x default start-stop
 group radius ! aaa session-id common ! aaa accounting update periodic 5 !
 每 5 分钟定期更新 AAA 记账信息 aaa accounting system default start-stop group
radius !
```

交换机上的 RADIUS 服务器配置

输入以下命令，将交换机配置为与用作 RADIUS 源服务器的Cisco ISE 进行互操作：

```
! radius-server <ISE 名称> ! ISE 名称是 ISE PSN 的名称 address ipv4 <ip address>
 auth-port 1812 acct-port 1813 ! IP 地址是 PSN 的地址。此示例使用标准 RADIUS 端口。key
<passwd> ! 密码是在Cisco ISE 中配置的密码 exit
```

注释 我们建议将死亡标准时间配置为 30 秒，期间允许 3 次重试，为使用 Active Directory 进行身份验证的 RADIUS 请求提供更长的响应时间。

用于启用 RADIUS 授权更改 (CoA) 的命令

请通过输入以下命令，指定设置以确保交换机能够相应地处理 RADIUS 授权更改，支持Cisco ISE 的安全状态功能：

```
aaa server radius dynamic-author 客户端 <ISE-IP> server-key 0 abcde123
```

注释

- Cisco ISE 使用端口 1700（Cisco IOS 软件默认值）进行 CoA，而不是 RFC 默认端口 3799。现有 Cisco Secure ACS 5.x 客户如果将 CoA 作为现有 ACS 实施的环节，则可能已将此端口设置为 端口 3799。
- 共享密钥应与添加网络设备时在思科 ISE 上配置的密钥相同，并且IP地址应为 PSN IP 地址。

启用设备跟踪和 DHCP 监听的命令

为了帮助提供Cisco ISE 面向安全的可选功能，您可以在交换机端口动态 ACL 中针对 IP 替代启用设备跟踪和 DHCP 监听，您可输入以下命令：

```
! 可选 ip dhcp snooping ！必填！！配置设备跟踪策略！device-tracking policy
<DT_POLICY_NAME> no protocol ndp tracking enable ！绑定到接口！interface
<interface_id> device-tracking attach-policy<DT_POLICY_NAME>
```

在 RADIUS 记帐中，即便已启用 DHCP 监听，DHCP 属性也不会通过 IOS 传感器发送到Cisco ISE。在这种情况下，则应启用 VLAN 的 DHCP 监听使 DHCP 成为活动状态。

使用以下命令启用 VLAN 的 DHCP 监听：

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 1-100
```

（应包括 VLAN 范围用于数据和 VLAN ）

启用基于 802.1X 端口的身份验证的命令

输入以下命令可为交换机端口全局开启 802.1X 身份验证：

```
dot1x system-auth-control
```

用于为临界身份验证启用 EAP 的命令

要支持局域网上的请求方身份验证请求，请输入以下命令，为临界身份验证（不可访问的身份验证绕行）启用 EAP：

```
dot1x critical eapol
```

使用恢复延迟限制 AAA 请求的命令

当发生关键身份验证恢复事件时，通过输入以下命令，您可以配置交换机自动引入延迟（以毫秒为单位）以确保Cisco ISE 能够在恢复后再次启动服务：

身份验证关键恢复延迟 *1000*

根据实施状态定义 VLAN

输入以下命令，根据网络中已知的实施状态，定义 VLAN 名称、编号和 SVI。创建单独的 VLAN 接口，实现网络间路由。这尤其有助于处理流经相同网段的多个流量源，例如，来自两台 PC 的流量以及通过其使 PC 连接网络的 IP 电话的流量。

vlan *<VLAN_number>* **name** *ACCESS*! **vlan** *<VLAN_number>* **name** *VOICE* ! **interface** *<VLAN_number>* **description** *ACCESS* **ip address** *10.1.2.3 255.255.255.0* **ip helper-address** *<DHCP_Server_IP_address>* **ip helper-address** *<Cisco_ISE_IP_address>* ! **interface** *<VLAN_number>* **description** *VOICE* **ip address** *10.2.3.4 255.255.255.0* **ip helper-address** *<DHCP_Server_IP_address>*

交换机上的本地（默认）ACL 定义

通过输入以下命令，在较低版本的交换机（使用低于 12.2(55)SE 版本的Cisco IOS 软件的交换机）上启用这些功能，确保Cisco ISE 能够执行进行身份验证和授权所需的动态 ACL 更新。

ip access-list extended ACL-ALLOW permit ip any any ! ip access-list extended ACL-DEFAULT remark DHCP permit udp any eq bootpc any eq bootps remark DNS permit udp any any eq domain remark Ping permit icmp any any remark Ping permit icmp any any remark PXE / TFTP permit udp any any eq tftp remark Allow HTTP/S to ISE and WebAuth portal permit tcp any host *<Cisco_ISE_IP_address>* **eq www permit tcp any host** *<Cisco_ISE_IP_address>* **eq 443 permit tcp any host** *<Cisco_ISE_IP_address>* **eq 8443 permit tcp any host** *<Cisco_ISE_IP_address>* **eq 8905 permit udp any host** *<Cisco_ISE_IP_address>* **eq 8905 permit udp any host** *<Cisco_ISE_IP_address>* **eq 8906 permit tcp any host** *<Cisco_ISE_IP_address>* **eq 8080 permit udp any host** *<Cisco_ISE_IP_address>* **eq 9996 remark Drop all the rest deny ip any any log** ! ! 此 ACL 允许 URL 重定向以用于 WebAuth **ip access-list extended ACL-WEBAUTH-REDIRECT permit tcp any any eq www permit tcp any any eq 443**

注释 WLC 上的该配置可能会增加 CPU 利用率，提高系统不稳定风险。这是 IOS 问题，不会对Cisco ISE 产生不利影响。

对 802.1X 和 MAB 启用交换机端口

要为 802.1X 和 MAB 启用交换机端口，请执行以下操作：

步骤 1 使所有接入交换机端口进入配置模式：
interface range FastEthernet0/1-8

步骤 2 启用交换机端口的接入模式（而不是中继模式）：

switchport mode access

步骤 3 静态配置接入 VLAN。这样，即可在本地调配接入 VLAN，这也是开放模式身份验证所要求的：

switchport access vlan <*VLAN_number*>

步骤 4 静态配置语音 VLAN：

switchport voice vlan <*VLAN_number*>

步骤 5 启用开放模式身份验证。身份验证完成之前，开放模式允许将流量桥接至数据和语音VLAN。我们强烈建议您在生产环境中使用基于端口的 ACL，以防止进行未经授权的访问。

! AAA 响应前启用身份预验证访问；具体取决于端口 ACL

authentication open

步骤 6 应用基于端口的 ACL，确定默认情况下应将哪些流量从未经授权的终端桥接至接入 VLAN。由于您应首先允许所有访问，然后再实施策略，因此您应当应用 ACL-ALLOW，以允许所有流量都流经交换机端口。您已创建默认的ISE授权，允许到目前为止的所有流量，这是因为我们希望实现完全可见性，并且不希望影响到现有最终用户的体验。

! 必须配置 ACL 才能从 AAA 服务器预设定 dACL。

ip access-group ACL-ALLOW in

注释 在 DSBU 交换机上的Cisco IOS 软件版本 12.2(55)SE 之前，需要端口 ACL 才能应用来自 RADIUS AAA 服务器的动态 ACL。如果未能设置默认 ACL，交换机将忽略分配的 dACL。使用Cisco IOS 软件版本 12.2(55)SE 时，系统会自动生成并应用默认 ACL。

注释 目前，我们在实验室中使用 ACL-ALLOW，这是因为我们想要启用 802.1X 基于端口的身份验证，却不希望对现有网络造成任何影响。在稍后的练习中，我们将应用不同的 ACL-DEFAULT，以阻止生产环境中产生不需要的流量。

步骤 7 启用多身份验证主机模式。多身份验证可以说是多域身份验证 (MDA) 的超集。MDA 只允许数据域中有一个终端。当配置多身份验证时，语音域中只允许有一个身份验证电话（和MDA一样），但在数据域中却可以对不限数量的数据设备进行身份验证。

! 允许在同一个物理接入端口上使用语音和多个终端。

authentication host-mode multi-auth

注释 IP 电话背后的多台数据设备（无论是虚拟化设备还是连接到集线器的物理设备）都可以增强接入端口的物理链路状态感知能力。

步骤 8 启用各种身份验证方法的选项：

! 启用重新进行身份验证

authentication periodic

! 通过 RADIUS 会话超时启用重新进行身份验证

authentication timer reauthenticate server

authentication event fail action next-method

! 配置服务器故障情况下的关键身份验证 VLAN 方法

authentication event server dead action reinitialize vlan <*VLAN_number*>

authentication event server alive action reinitialize

! IOS Flex-Auth 身份验证 802.1X 和 MAB

authentication order dot1x mab

authentication priority dot1x mab

步骤 9 在交换机端口上启用 802.1X 端口控制：

! 在接口上启用基于端口的身份验证

authentication port-control auto

authentication violation restrict

步骤 10 启用 MAC 身份验证绕行 (MAB)：

! 启用 MAC 身份验证绕行 (MAB)

mab

步骤 11 在交换机端口上启用 802.1X

! 在接口上启用 802.1X 身份验证

dot1x pae authenticator

步骤 12 将重传时间设置为 10 秒：

dot1x timeout tx-period *10*

注释 dot1x tx-period 超时应设置为 10 秒。除非您了解影响，否则请勿更改此值。

步骤 13 启用 portfast 功能：

spanning-tree portfast

在基于身份的网络服务上启用基于 802.1X 的命令

以下示例显示一项控制策略，该策略可配置为允许使用 802.1X、MAB 和 Web 身份验证的顺序身份验证方法。

```
class-map type control subscriber match-all DOT1X match method dot1x ! class-map type control
 subscriber match-all DOT1X_FAILED match method dot1x match result-type method dot1x
authoritative ! class-map type control subscriber match-all DOT1X_NO_RESP match method dot1x
 match result-type method dot1x agent-not-found ! class-map type control subscriber match-all
 MAB match method mab ! class-map type control subscriber match-all MAB_FAILED match method
 mab match result-type method mab authoritative ! ! policy-map type control subscriber
DOT1XMAB event session-started match-all 10 class always do-until-failure 10 authenticate
using dot1x retries 2 retry-time 0 priority 10 event authentication-failure match-first 10
 class DOT1X_NO_RESP do-until-failure 10 terminate dot1x 20 authenticate using mab priority
 20 20 class DOT1X_FAILED do-until-failure 10 terminate dot1x 20 authenticate using mab
priority 20 30 authorize 40 class always do-until-failure 10 terminate dot1x 20 terminate
mab 30 authentication-restart 60 event agent-found match-all 10 class always do-until-failure
 10 terminate mab 20 authenticate using dot1x retries 2 retry-time 0 priority 10 !
```

以下示例显示一项控制策略，该策略可配置为允许使用 MAB、802.1X 和 Web 身份验证的顺序身份验证方法。

```
policy-map type control subscriber MABDOT1X event session-started match-all 10 class always
 do-until-failure 10 authenticate using mab priority 20 20 authenticate using dot1x priority
```

```
 10 event authentication-failure match-first 10 class ALL_FAILED do-until-failure 10
authentication-restart 60 event authentication-success match-all 10 class DOT1X
do-until-failure 10 terminate mab event agent-found match-all 10 class always do-until-failure
 10 authenticate using dot1x priority 10 Applying the service policy on the interface
interface GigabitEthernet1/0/4 switchport mode access device-tracking attach-policy pol1
ip access-group sample in authentication timer reauthenticate server access-session
port-control auto mab dot1x pae authenticator dot1x timeout tx-period 10 dot1x timeout
auth-period 10 spanning-tree portfast service-policy type control subscriber DOT1XMAB
```

用于启用 EPM 日志记录的命令

在交换机上设置标准日志记录功能，以支持对Cisco ISE 功能进行可能的故障排除/记录：

epm logging

支持 SNMP 陷阱的命令

确保交换机能够通过网段中的适当 VLAN，从Cisco ISE 接收 SNMP 陷阱传输：

snmp-server community public RO snmp-server trap-source *<VLAN_number>*

为分析启用 SNMP v3 查询的命令

配置交换机，确保按预期执行 SNMP v3 轮询以支持Cisco ISE 分析服务。首先，在Cisco ISE 中配置 SNMP 设置。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add) | 编辑 (Edit)** > **SNMP 设置 (SNMP Settings)**。

Snmp-server user *<name> <group>* **v3 auth md5** *<string>* **priv des** *<string>*
snmp-server group *<group>* **v3 priv snmp-server group** *<group>* **v3 priv context** *vlan-1*

注释 必须为每个上下文分别配置 **snmp-server group** *<group>* **v3 priv context** *vlan-1* 命令。**snmp show context** 命令会列出所有上下文信息。

如果 SNMP 请求超时并且不存在连接问题，则可以提高 Timeout 值。

启用分析器的 MAC 通知陷阱进行收集的命令

配置您的交换机以传送适当的 MAC 通知陷阱，这样Cisco ISE 分析器功能就可以收集网络终端上的信息：

mac address-table notification change mac address-table notification mac-move snmp trap mac-notification change added snmp trap mac-notification change removed

交换机上的 RADIUS 空闲超时配置

要在交换机上配置 RADIUS 空闲超时，请使用以下命令：

```
Switch(config-if)# authentication timer inactivity
```

其中 *inactivity* 是以秒为单位的非活动时间间隔，这个时间之后，客户端活动将被视为未授权。

在Cisco ISE 中，可以为这类会话非活动计时器应用到的任何授权策略启用此选项。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

用于 iOS 请求方调配的无线 LAN 控制器配置

对于单 SSID

要支持基于 Apple iOS 的设备 (iPhone/iPad) 从一个 SSID 切换至同一无线接入点的另一个 SSID，请将无限局域网控制器 (WLC) 配置为启用“快速 SSID 更改”(FAST SSID change) 功能。此功能有助于确保基于 IOS 的设备能够在 SSID 之间快速切换。

对于双 SSID BYOD

必须启用快速 SSID 以支持双 SSID BYOD。启用快速 SSID 更改后，无线控制器允许客户端在 SSID 间更快速移动。启用快速 SSID 时，不会清除客户端条目，也不会强制执行延迟。有关在Cisco WLC 上配置快速 SSID 的详细信息，请参阅《Cisco Wireless Controller 配置指南》。

WLC 配置示例

```
WLC (config)# 快速 SSID 更改
```

当您尝试在某些基于 Apple iOS 的设备中连接无线网络时，您可以会看到以下错误信息：

```
Could not scan for Wireless Networks.
```

您可以忽略该错误消息，因为这不会影响设备的身份验证。

在无线 LAN 控制器上配置 ACL 以实现移动设备管理互操作

必须在无线 LAN 控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备和证书调配。ACL 必须采用以下顺序。

步骤 1 允许所有从服务器到客户端的出站流量。

步骤 2 （可选）允许从客户端到服务器的 ICMP 入站流量以进行故障排除。

步骤 3 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。

步骤 4 允许从客户端到服务器再到 ISE 的所有入站流量以执行 Web 门户和请求方以及证书调配流程。

步骤 5 允许从客户端到服务器的入站 DNS 流量以进行名称解析。

步骤 6 允许从客户端到服务器的入站 DHCP 流量以获取 IP 地址。

步骤 7 拒绝所有从客户端到服务器再到企业资源的入站流量，以重定向至Cisco ISE（根据公司策略）。

步骤 8 （可选）允许其余流量。

示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，Cisco ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 *62:* 用于重定向未注册设备的 *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

第 16 章

故障排除

思科 ISE 中的监控和故障排除服务

监控和故障排除 (MnT) 服务是所有Cisco ISE 运行时服务的综合身份解决方案。**操作 (Operations)** 菜单包含以下组件，并且只能从主策略管理节点 (PAN) 查看。请注意，**操作 (Operations)** 菜单不会显示在主监控节点中。

- 监控：实时呈现代表网络上的访问活动状态的有意义数据。通过查看展示，您可以轻松地解释并影响操作条件。
- 故障排除：提供用来解决网络上的访问问题的上下文指导。然后，您可以解决用户的问题并及时提供解决方案。

- 报告：提供标准报告的目录，这些报告可用来分析趋势和监控系统性能以及网络活动。您可以用各种方式自定义这些报告，并可保存这些报告以供将来使用。您可以在所有报告中针对以下字段使用通配符和多个值搜索记录：**身份 (Identity)**、**终端 ID (Endpoint ID)** 和 **ISE 节点 (ISE Node)**（**运行状况摘要 (Health Summary)** 报告除外）。

ISE 社区资源

有关故障排除技术说明的完整列表，请参阅 ISE 故障排除技术说明。

运行状况检查

Cisco ISE 版本 3.0 引入了按需运行状况检查选项，用于诊断Cisco ISE 部署中的所有节点。执行任何操作之前，先在所有节点上进行运行状况检查有助于减少停机时间，并通过发现关键问题改善Cisco ISE 系统的整体功能。运行状况检查会提供组件的工作状态，如有任何Cisco ISE 组件损坏，将提供即时故障排除建议。

注释 在运行状况检查期间，如果任何节点在15分钟内没有发回响应，则该特定节点的运行状况检查会超时。

执行运行状况检查

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **运行状况检查 (Health Checks)**。

步骤 2 点击**启动运行状况检查 (Start health checks)**。

信息弹出窗口将显示以下消息：

已触发健康状况检查 (Health Checks triggered)。

步骤 3 点击**确定 (Ok)** 查看状态。

步骤 4 在**运行状况检查 (Health Checks)** 窗口中，您将能够查看每个组件的运行状况。以下颜色用于指示Cisco ISE 组件的运行状况：

颜色	运行状况	操作
红色	不佳	点击下拉选项查看框中提供的故障排除建议。解决问题，然后点击刷新图标。
橙色	良好 **注释** 组件的运行状况良好，可以执行操作。但是，存在的问题可能会在将来影响某些功能。	点击下拉选项查看框中提供的故障排除建议。

颜色	运行状况	操作
绿色	良好	无需任何操作。
蓝色	良好	点击信息图标查看关于功能的关键信息。

步骤 5 点击**下载报告 (Download report)**。

HealthChecksReport.json 文件将保存在本地系统中，其中包含Cisco ISE 部署的详细运行状况信息。

触发运行状况检查后，状态将在**运行状况检查 (Health Check)** 窗口中保留三小时。在**运行状况检查 (Health Check)** 窗口刷新/过期前，将无法运行健康状况检查。

网络权限框架事件流程

网络权限框架 (NPF) 身份验证和授权事件流程使用下表列出的过程：

流程阶段	说明
1	网络访问设备 (NAD) 执行正常授权或 Flex 授权。
2	使用 Web 授权分析无代理的未知身份。
3	RADIUS 服务器进行身份验证和授权。
4	在端口配置身份的授权。
5	丢弃未经授权的终端通信。

用于监控和故障排除功能的用户角色和权限

监控和故障排除功能与默认用户角色相关联。允许您执行的任务与分配给您的用户角色直接相关。

有关为每个用户角色设置的权限和限制的信息，请参阅思科 ISE 管理员组 ， 第 5 页。

注释 不支持在没有思科 TAC 监管的情况下使用根 shell 访问思科 ISE，并且思科不对由此导致的任何服务中断负责。

监控数据库中存储的数据

Cisco ISE 监控服务会收集数据并将所收集的数据存储于专用监控数据库中。根据用于监控网络功能的数据速率和数据量，可能需要将某个节点专用于监控。如果Cisco ISE 网络以高速率从策略服务节点或网络设备收集日志数据，则我们建议将某个Cisco ISE 节点专用于监控。

要管理监控数据库中存储的信息，需要对数据库执行完整备份和增量备份。这包括清除不需要的数据，然后还原数据库。

思科 ISE 遥感勘测

遥测会监控网络中的系统和设备，向Cisco提供有关您如何使用产品的反馈。Cisco将这些信息用于改进产品。

遥测默认处于启用状态。要禁用此功能，请执行以下操作：

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **网络成功诊断 (Network Success Diagnostics)** > **遥测 (Telemetry)**
2. 取消选中**启用遥测 (Enable Telemetry)** 复选框以禁用遥测。

- **思科帐户 (Cisco Account)**：输入您的Cisco帐户，以便您可以通过遥测获取电子邮件。如果遥测发现任何可能影响您的严重问题，我们也可能使用此 ID 与您联系。
- **传输网关 (Transport Gateway)**：您可以在Cisco ISE 和Cisco外部遥测服务器之间使用代理，提供额外的安全性。要执行此操作，请选中此复选框并输入代理服务器的 FQDN。遥测不需要代理。

  Cisco提供传输网关软件。您可以从 Cisco.com 下载。此软件在 Linux 服务器上运行。有关如何在 RHEL 服务器上部署传输网关软件的信息，请参阅 Smart Call Home 部署指南。如果使用此 Cisco软件，则 URL 值为 **<FQDN of proxyserver>/ Transportgateway / services / DeviceRequestHandler**。您也可以使用此网关连接到智能许可服务器。从传输网关版本 3.5 开始，无法更改端口，但可以输入 IP 地址而不是 FQDN。

遥测收集的信息

遥测会将以下信息发送给Cisco。

节点：

对于每个策略管理节点 (PAN)

- 当前经过终端安全评估的终端数量
- 当前的 PxGrid 客户端数量
- 当前由 MDM 管理的终端数量
- 当前访客用户数
- 此遥测记录的开始和结束日期
- FIPS 状态

对于每个策略服务节点 (PSN)

- 分析器探测数
- 节点服务类型
- 已用的被动 ID

对于所有节点

- 总计和活动 NAD 数
- CPU 核心数量
- 虚拟机可用磁盘空间
- 虚拟机内存和 CPU 设置
- 系统名称
- 序列号
- VID 和 PID
- 正常运行时间
- 上次 CLI 登录

MnT 节点计数

pxGrid 节点计数

许可证

- 是否有许可证已到期？
- 可用的Cisco ISE Essentials 许可证数量、曾使用的最大数量
- 可用的Cisco ISE Advantage 许可证数量、曾使用的最大数量
- 可用的Cisco ISE Premier 许可证数量、曾使用的最大数量
- 小型、中型和大型虚拟机许可证的数量
- 是否正在使用评估许可证？
- 智能账户的名称
- TACACS 设备数量
- 到期日期、剩余天数、许可证期限
- 服务类型、主要和辅助 UDI

终端安全评估

- 非活动策略的数量
- 最后终端安全评估源更新

- 活动策略的数量
- 终端安全评估源更新

访客用户

- 当天经过身份验证的访客的最大数量
- 当天活动访客的最大数量
- 当天 BYOD 用户的最大数量
- 经过身份验证的访客的外部 ID 信息

网络访问设备 (NAD)

- 授权：激活的 ACL 数、VLAN 数、策略大小
- NDG 映射和 NAD 层次结构
- 身份验证：
  - RADIUS、RSA ID、LDAP、ODBC 和 Active Directory ID 存储区的数量
  - 本地（非管理员）用户数
  - NDG 映射和 NAD 映射
  - 策略行数

对于授权，包括活动 VLAN 数、策略计数、已激活的 ACL 数量：

- 状态，VID，PT
- 平均负载，内存使用量
- PAP、MnT、pxGrid 和 PIC 节点的数量
- 名称、配置文件名称、配置文件 ID

NAD 配置文件

对于每个 NAD 配置文件：

- 名称和 ID
- Cisco设备
- TACACS 支持
- RADIUS 支持
- TrustSec SXP 支持
- 默认配置文件

Profiler

- 最后源更新的日期
- 是否已启用自动更新？
- 已分析的终端数、终端类型、未知终端数、未知百分比和终端总数
- 自定义配置文件数量
- 序列号、范围、终端类型、自定义配置文件

移动设备管理 (MDM)

- MDM 节点列表
- 对于日期范围，包括当前 MDM 终端计数、当前访客用户计数、当前已经过终端安全评估的用户计数
- pxGrid 客户端计数
- 节点计数

SNMP 陷阱监控思科 ISE

思科 ISE 中的通用 SNMP 陷阱

SNMP 陷阱可帮助您监控Cisco ISE 的状态。如果要在不访问Cisco ISE 服务器的情况下监控Cisco ISE，可以在Cisco ISE 中将 MIB 浏览器配置为 SNMP 主机。然后您可以在 MIB 浏览器中监控Cisco ISE 的状态。

有关 **snmp-server host** 和 **snmp-server trap** 命令的信息，请参阅《思科身份服务引擎 CLI 参考指南》。

Cisco ISE 支持 SNMPv1、SNMPv2c 和 SNMPv3。

如果您在 CLI 中配置了 SNMP 主机，Cisco ISE 将发送以下通用系统陷阱：

- 冷启动：当设备重新引导时。
- Linkup：当以太网接口打开时。
- Linkdown：当以太网接口关闭时。
- 身份验证故障：当社区字符串不匹配时。

下表列出了Cisco ISE 中默认生成的通用 SNMP 陷阱。

OID	说明	陷阱示例
.1.3.6.1.4.1.8072.4.0.3 \n NET-SNMP-AGENT-MIB::nsNotifyRestart	表示代理已重新启动。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET-SNMP-AGENT-MIB::nsNotifyShutdown	表示代理正在关闭。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	表示 SNMP 实体（充当代理角色）检测到其中一条通信链路的 ifOperStatus 对象已从“关闭”(Down) 状态转换为其他状态（但不是“不存在”(notPresent) 状态）。其他状态由包含的 ifOperStatus 值表示。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

OID	说明	陷阱示例
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	表示 SNMP 实体（充当代理角色）检测到其中一条通信链路的 ifOperStatus 对象即将从其他状态（但不是“不存在”(notPresent) 状态）进入“关闭”(Down) 状态。其他状态由包含的 ifOperStatus 值表示。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	表示支持通知发起方应用的 SNMP 实体正在重新初始化自身，并且其配置可能已更改。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

思科 ISE 中的进程监控 SNMP 陷阱

如果从Cisco ISE CLI 配置 SNMP 主机，则Cisco ISE 允许将Cisco ISE 进程状态的 hrSWRunName 陷阱发送到 SNMP 管理器。Cisco ISE 使用时钟守护作业 (cron job) 来触发这些陷阱。Cron 作业会从 Monit 检索Cisco ISE 进程状态。当在 CLI 中配置 **SNMP-服务器主机** 命令后，cron 作业会每五分钟运行一次，并监控Cisco ISE。

注释 当 ISE 进程由管理员手动停止时，该进程的监控也会停止，并且系统不会向 SNMP 管理器发送陷阱。仅当进程意外关闭并且不自动恢复时，系统才会向 SNMP 管理器发送进程停止 SNMP 陷阱。

以下是Cisco ISE 中进程监控 SNMP 陷阱的详尽列表。

OID	说明	陷阱示例
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	此运行软件的文本说明，包括制造商、版本和通常所知的名称。如果此软件是在本地安装的，则此字符串必须与相应的 hrSWInstalledName 中使用的字符串相同。所考虑的服务包括 app-server、rsyslog、redis-server、ad-connector、mnt-collector、mnt-processor、ca-server est-server 和 elasticsearch。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

发生以下状况时，Cisco ISE 会向配置的 SNMP 服务器发送相应的陷阱：

- 进程开始（受监控状态）
- 进程停止（不受监控状态）
- 执行失败：当进程状态从“受监控”(Monitored) 变为“执行失败”(Execution Failed) 时，发送陷阱。
- 不存在：当进程状态从“受监控”(Monitored) 变为“不存在”(Does Not Exist) 时，发送陷阱。

在 SNMP 服务器中，会为每个对象生成唯一的对象 ID (OID)，并为 OID 分配一个值。您可以通过 OID 值在 SNMP 服务器查找对象。正在运行的陷阱的 OID 值为 *running*，不受监控的、不存在的和执行失败的陷阱的 OID 值为 *stopped*。

Cisco ISE 使用属于 HOST-RESOURCES MIB 的 hrSWRunName 的 OID 发送陷阱，并将 OID 值设置为 <进程名称> - <进程状态>，例如，runtime - running。

要终止Cisco ISE 发送 SNMP 陷阱至 SNMP 服务器，需在Cisco ISE CLI 中删除 SNMP 配置。此操作将终止来自 SNMP 管理器的 SNMP 陷阱和轮询。

思科 ISE 中的磁盘利用率 SNMP 陷阱

当Cisco ISE 分区达到利用率限制阈值时并且达到所配置的可用空间量时，将发送一个陷阱。

以下是可在Cisco ISE 中配置的磁盘利用率 SNMP 陷阱的详尽列表：

OID	说明	陷阱示例
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	磁盘上已用空间的百分比。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	磁盘的挂载路径。 dskPath 可以为 ISE 管理命令 **show disks** 输出中的所有挂载点发送陷阱。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

思科 ISE 警报

警报显示在 Alarms dashlet 中，通知您网络中的严重情况。警报还会提供关于系统活动的信息，如数据清除事件。可以配置要接收系统活动通知的方式，或完全禁用警报。还可以为某些警报配置阈值。

大多数警报没有关联的计划，会在事件发生后立即发送。在任何给定时间点，系统只会保留最新的 15,000 个警报。

如果事件再次发生，则系统会在约一个小时内抑制相同的警报。在事件再次发生期间，可能需要经过一个小时，警报才会再次出现（取决于触发器）。

下表列出所有Cisco ISE 警报、说明及其解决方法。

表 *213:* 思科 *ISE* 警报

警报名称	警报说明	警报解决方法
管理和操作审核管理		
部署升级失败	ISE 节点升级失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
升级捆绑包下载失败	ISE 节点升级捆绑包下载失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
SXP 连接失败	SXP 连接失败。	验证 SXP 服务正在运行。检查对等兼容性。

警报名称	警报说明	警报解决方法
应用于所有设备的Cisco配置文件	网络设备配置文件定义网络接入设备的功能，如MAB、Dot1X、CoA 和网络重定向。作为 ISE 2.0 升级的一部分，默认Cisco网络设备配置文件应用于所有网络设备。	编辑非Cisco网络设备的配置，以分配适当的配置文件。
由于CRL查找到已吊销的证书，安全 LDAP 连接重新连接	CRL 检查结果是用于 LDAP 连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在 LDAP 服务器上。
由于 OCSP 查找到已吊销的证书，安全 LDAP 连接重新连接	OCSP 检查结果是用于 LDAP 连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在 LDAP 服务器上。
由于CRL查找到已吊销的证书，安全系统日志连接重新连接	CRL 检查结果是用于系统日志连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在系统日志服务器上。
由于 OCSP 查找到已吊销的证书，安全系统日志连接重新连接	OCSP 检查结果是用于系统日志连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在系统日志服务器上。
管理员帐户已锁定/禁用	由于密码过期或登录尝试不正确，系统锁定或禁用管理员帐户。有关详细信息，请参阅管理员密码策略。	管理员密码可以由其他管理员使用 GUI 或 CLI 进行重置。
ERS 识别已弃用的 URL	ERS 识别已弃用的 URL	请求 URL 已弃用，建议避免使用此 URL
ERS 识别过时的 URL	ERS 识别过时的 URL	请求的 URL 已过时，建议使用更新的URL。未来的版本不会删除此 URL。

警报名称	警报说明	警报解决方法
ERS请求的内容类型信头已过时	ERS请求的内容类型信头已过时	在请求的内容类型信头内指定的请求资源版本已过时。这表明资源方案已被修改。可能已添加或删除一个或多个属性。为使用过时的方案解决这一问题，ERS引擎将使用默认值。
ERS XML 输入有 XSS 或注入攻击的嫌疑	ERS XML 输入有 XSS 或注入攻击的嫌疑。	请检查您的 XML 输入。
备份失败	ISE 备份操作失败。	检查Cisco ISE与存储库之间的网络连接性。确保： • 用于存储库的凭证是正确的。 • 存储库中有足够的磁盘空间。 • 存储库用户具有写入权限。
CA 服务器已关闭	CA 服务器已关闭。	检查以确保 CA 服务已启动并正在 CA 服务器上运行。
CA 服务器已启动	CA 服务器已启动。	通知管理员 CA 服务器已启动。
证书到期	此证书即将到期。证书到期时，Cisco ISE可能无法与客户端建立安全通信。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用Cisco ISE延长有效期。如果不再使用证书，可将其删除。
证书被吊销	管理员已撤销由内部 CA 颁发给终端的证书。	从头完成 BYOD 流程以提供新证书。
证书调配初始化错误	证书调配初始化失败	在主题中找到多个具有相同 CN (CommonName) 属性值的证书。无法构建证书链。检查系统中的所有证书，包括 SCEP 服务器中的证书。

警报名称	警报说明	警报解决方法
证书复制失败	到辅助节点的证书复制失败	证书在辅助节点上无效，或存在某些其他永久错误条件。检查辅助节点是否有预先存在的冲突证书。如果找到，请删除辅助节点上预先存在的证书，然后在主要节点上导出新证书，删除证书，然后将其导入以重新尝试复制。
证书复制暂时失败	到辅助节点的证书复制暂时失败	由于网络故障等临时条件，证书未复制到辅助节点。系统将重试复制，直至成功。
证书已过期	此证书已过期。Cisco ISE 可能无法与客户端建立安全通信。节点到节点通信可能也会受到影响。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用Cisco ISE 延长有效期。如果不再使用证书，可将其删除。
证书请求转发失败	证书请求转发失败。	确保传入的认证请求与发件人的属性相匹配。
配置已更改	Cisco ISE 配置已更新。系统没有为任何用户和终端的配置更改触发此警报。	检查是否应存在配置更改。
CRL 检索失败	无法从服务器检索 CRL。如果指定的 CRL 不可用，就可能会出现这种情况。	确保下载 URL 正确且可用于服务。
DNS 解析失败	节点上的 DNS 解析失败。	检查是否可访问使用 **ip name-server** 命令配置的 DNS 服务器。 如果您收到的警报为 **DNS Resolution failed for CNAME <hostname of the node>**，则确保为每个Cisco ISE 节点创建 CNAME RR 以及 A 记录。
需要进行固件更新	需要在此主机上进行固件更新。	联系Cisco TAC 以获取固件更新。

警报名称	警报说明	警报解决方法
虚拟机资源不足	此主机上的虚拟机 (VM) 资源（如 CPU、RAM、磁盘空间或 IOPS）不足。	确保 VM 主机达到《Cisco ISE 硬件安装指南》中指定的最低要求。
NTP 服务故障	此节点上的 NTP 服务已关闭。	这可能是因为 NTP 服务器与 Cisco ISE 节点之间存在较大的时间差异（超过 1000s）。确保 NTP 服务器正常工作并使用 **ntp server <servername>** CLI 命令重新启动 NTP 服务并修复时间差。
NTP 同步失败	在此节点配置上的所有 NTP 服务器均无法访问。	从 CLI 执行 **show ntp** 命令，进行故障排除。确保可从Cisco ISE访问 NTP 服务器。如果已配置 NTP 身份验证，请确保密钥 ID 和值与服务器的相匹配。
未安排配置备份	未安排Cisco ISE 配置备份。	创建配置备份计划。
操作数据库清除失败	无法从操作数据库中清除较旧的数据。这会在 MnT 节点忙碌时发生。	检查数据清除审核报告并确保 used_space 小于 threshold_space。使用 CLI 登录 MnT 节点，手动执行清除操作。
分析器 SNMP 请求失败	SNMP 请求超时或 SNMP 社区或用户身份验证数据不正确。	确保 SNMP 正在 NAD 上运行并验证Cisco ISE 上的 SNMP 配置是否与 NAD 匹配。
复制失败	辅助节点无法使用复制的消息。	登录到Cisco ISE GUI 并从部署页面执行手动同步。取消注册并重新注册受影响的Cisco ISE 节点。
恢复失败	Cisco ISE 恢复操作失败。	确保Cisco ISE 与存储库之间存在网络连接。确保用于存储库的凭证正确。确保备份文件未损坏。从 CLI 执行 **reset-config** 命令并恢复已知的最后一次有效备份。
补丁失败	服务器上的补丁进程失败。	在服务器上重新安装补丁进程。
补丁成功	服务器上的补丁进程成功。	-

警报名称	警报说明	警报解决方法
外部 MDM 服务器 API 版本不匹配	外部 MDM 服务器 API 版本与 Cisco ISE 中配置的版本不匹配。	确保 MDM 服务器 API 版本与 Cisco ISE 中配置的版本相同。如有需要，更新Cisco ISE MDM 服务器配置。
外部 MDM 服务器连接失败	到外部 MDM 服务器的连接失败。	确保MDM服务器已启动且Cisco ISE-MDM API 服务正在 MDM 服务器上运行。
外部 MDM 服务器响应错误	外部 MDM 服务器响应错误。	确保Cisco ISE-MDM API 服务在 MDM 服务器上正常运行。
复制已停止	ISE 节点无法从 PAN 复制配置数据。	登录Cisco ISE GUI 以从部署页面执行手动同步，或取消注册并重新注册带必填字段的受影响 ISE 节点。
终端证书已过期	终端证书已由每天安排的作业标记为过期。	重新注册终端设备，获取新的终端证书。
终端证书已清除	过期的终端证书已由每天安排的作业清除。	无需执行任何操作。这是管理员发起的清理操作。
终端清除活动	清除终端上过去 24 小时的活动。此警报在午夜触发。	查看清除活动，方法是选择**操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端清除活动 (Endpoint Purge Activities)**。
复制减慢错误	系统检测到复制减慢或停滞。	验证节点是否可访问并且是部署的一部分。
复制减慢信息	系统检测到复制减慢或停滞。	验证节点是否可访问并且是部署的一部分。
复制减慢警告	系统检测到复制减慢或停滞。	验证节点是否可访问并且是部署的一部分。
PAN 自动故障转移 - 故障转移失败	到辅助管理节点的升级请求失败。	有关进一步操作，请参阅警报详细信息。
PAN 自动故障转移 - 故障转移已触发	已成功触发辅助管理节点到主要角色的故障转移。	等待辅助 PAN 完成升级，并调用旧的主 PAN。
PAN 自动故障转移 - 运行状况检查处于非活动状态	PAN 未收到指定监控节点的运行状况检查监控请求。	验证报告的监控节点是否关闭或不同步，如有需要，请触发手动同步。

警报名称	警报说明	警报解决方法
PAN 自动故障转移 - 无效的运行状况检查	收到无效的运行状况检查监控请求，无法进行自动故障转移。	验证运行状况检查监控节点是否不同步，如有需要，请触发手动同步。
PAN 自动故障转移 - 主管理节点已关闭	主管理节点已关闭或无法从监控节点访问。	调用 PAN 或等待进行故障转移。
PAN 自动故障转移 - 故障转移尝试被拒绝	辅助管理节点已拒绝运行状况检查监控节点提出的升级请求。	有关进一步操作，请参阅警报详细信息。
EST 服务已停止	EST 服务已停止。	确保 CA 和 EST 服务正常运行，且证书服务终端从属 CA 证书链完整。
EST 服务已启动	EST 服务已启动。	通知管理员 EST 服务已启动。
Smart Call Home 通信故障	Smart Call Home 消息未成功发送。	确保Cisco ISE 和Cisco系统之间存在网络连接。
遥测通信故障	遥测消息未成功发送。	确保Cisco ISE 和Cisco系统之间存在网络连接。
适配器不可访问。	Cisco ISE 无法连接到适配器。	有关故障的详细信息，请查看适配器日志。
适配器错误	适配器出错。	查看警报说明。
适配器连接失败	适配器无法连接到源服务器。	确保源服务器可访问。
适配器因错误已停止工作	适配器出错，且未处于预期状态。	确保适配器配置正确，且源服务器可访问。有关错误详细信息，请参阅适配器日志。
服务组件错误	服务组件遇到一个错误。	查看警报说明。
服务组件信息	服务组件已发送通知。	无。
ISE 服务		
TACACS 身份验证尝试次数过多	ISE 策略服务节点遇到的 TACACS 身份验证次数超过了预期次数。	• 检查网络设备的重新验证计时器。 • 检查 ISE 基础设施的网络连接。

警报名称	警报说明	警报解决方法
TACACS 身份验证失败次数过多	ISE 策略服务节点遇到的 TACACS 身份验证失败次数超过了预期次数。	• 检查身份验证步骤，找出根本原因。 • 检查 ISE/NAD 配置，确定身份与密钥是否不匹配。
可重新访问 MSE 位置服务器	可重新访问 MSE 位置服务器。	无。
无法访问 MSE 位置服务器。	无法访问 MSE 位置服务器或 MSE 位置服务器已关闭。	请检查 MSE 位置服务器是否正在运行且是否可从 ISE 节点访问该服务器。
AD 连接器必须重新启动	AD 连接器意外停止，必须重新启动。	如果此问题仍然存在，请联系 Cisco TAC 寻求帮助。
Active Directory 林不可用	Active Directory 林全局目录不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份验证域不可用	身份验证域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
ISE 身份验证处于非活动状态	Cisco ISE 策略服务节点未收到网络设备的身份验证请求。	• 检查 ISE/NAD 配置。 • 检查 ISE/NAD 基础设施的网络连接。
ID 映射。身份验证处于非活动状态	身份映射服务在过去 15 分钟未收集任何用户身份验证事件。	如果应在此时间内进行用户身份验证（例如工作时间），请检查到 Active Directory 域控制器的连接。
CoA 失败	网络设备已拒绝Cisco ISE 策略服务节点发出的授权更改 (CoA) 请求。	确保网络设备已配置为接受Cisco ISE 的 CoA 请求。请检查是否在有效会话中发出 CoA。
配置的名称服务器已关闭	配置的名称服务器已关闭或不可用。	检查 DNS 配置和网络连接。

警报名称	警报说明	警报解决方法
请求方已停止响应	Cisco ISE 在 120 秒前向客户端发送了最后一条消息，但客户端未响应。	• 验证请求方是否正确配置为与Cisco ISE 进行完整的 EAP 会话。 • 验证 NAS 是否正确配置为与请求方之间互相传输EAP消息。 • 验证请求方或 NAS 是否不会对 EAP 会话执行短时间超时。
身份验证尝试次数过多	Cisco ISE 策略服务节点进行的身份验证次数超过了预期次数。	检查网络设备的重新验证计时器。检查Cisco ISE 基础设施的网络连接。 达到阈值后，系统会触发“身份验证尝试次数过多”警报和“失败尝试次数过多”警报。显示在**说明** 列旁边的数字是在过去 15 分钟针对Cisco ISE 进行的身份验证成功或失败的总数。
失败尝试次数过多	Cisco ISE 策略服务节点遇到的身份验证失败次数超过了预期次数。	检查身份验证步骤，找出根本原因。检查Cisco ISE/NAD 配置，确定身份与密钥是否不匹配。 达到阈值后，系统会触发“身份验证尝试次数过多”警报和“失败尝试次数过多”警报。显示在**说明 (Description)** 列旁边的数字是在过去 15 分钟针对Cisco ISE 进行的身份验证成功或失败的总数。
AD：计算机 TGT 刷新失败	ISE 服务器票证授予票证 (TGT) 刷新失败。TGT 用于 AD 连接和服务。	检查 ISE 计算机帐户是否存在且有效。另请检查是否存在时钟偏差、复制、Kerberos 配置和/或网络错误。
AD：ISE 帐户密码更新失败	ISE 服务器未能更新其 AD 计算机帐户密码。	检查 ISE 计算机帐户密码是否未更改，计算机帐户是否未禁用或限制。检查到 KDC 的连接。

警报名称	警报说明	警报解决方法
所加入的域不可用	所加入的域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份库不可用	Cisco ISE 策略服务节点无法访问配置的身份库。	检查Cisco ISE 与身份存储库之间的网络连接。
已检测到网络设备配置错误	Cisco ISE 已检测到 NAS 的 RADIUS 记帐信息过多。 默认情况下，禁用此警报。要启用此警报，请参阅启用和配置警报。	NAS 已向 ISE 发送过多的重复 RADIUS 记账信息。为 NAS 配置准确的记账频率。
已检测到请求方配置错误	Cisco ISE 已检测到网络上的请求方配置错误。 默认情况下，禁用此警报。要启用此警报，请参阅启用和配置警报。	确保请求方的配置正确。
记账未启动	Cisco ISE 策略服务节点已授权会话，但未收到网络设备的记帐启动请求。	确保在网络设备上已配置 RADIUS 记账。检查网络设备配置的本地授权情况。
NAD 未知	Cisco ISE 策略服务节点收到未配置在Cisco ISE 中的网络设备的身份验证请求。	检查网络设备是否为真实请求，然后将其添加到配置中。确保密钥匹配。
SGACL 丢包	发生安全组访问 (SGACL) 丢包。如果支持 Trustsec 的设备因 SGACL 策略违规丢包，就会出现这种情况。	运行 RBACL 丢包摘要报告并查看导致 SGACL 丢包的源。向违规的源发出 CoA 以重新授权或断开会话连接。
RADIUS 请求已丢弃	NAD 的身份验证/记账请求已以静默方式丢弃。这可能是由于 NAD 未知、共享密钥不匹配或依照 RFC 数据包的内容无效。 默认情况下，禁用此警报。要启用此警报，请参阅启用和配置警报。	检查 NAD/AAA 客户端是否在 Cisco ISE 中存在有效配置。检查 NAD/AAA 客户端和Cisco ISE 上的共享密钥是否匹配。确保AAA 客户端和网络设备没有硬件问题或 RADIUS 兼容性问题。此外，请确保用于将设备连接到Cisco ISE 的网络没有硬件问题。
EAP 会话分配失败	由于达到 EAP 会话限制，RADIUS 请求已丢弃。此情况可能是由并行 EAP 身份验证请求过多导致。	在调用包含新 EAP 会话的其他 RADIUS 请求之前，请等待几秒钟。如果继续出现系统过载，请尝试重新启动 ISE 服务器。

警报名称	警报说明	警报解决方法
RADIUS 情景分配失败	由于系统过载，RADIUS 请求已丢弃。此情况可能是由并行身份验证请求过多导致。	在调用新 RADIUS 请求之前，请等待几秒钟。如果继续出现系统过载，请尝试重新启动 ISE 服务器。
AD：ISE 计算机帐户没有获取组所需的权限。	Cisco ISE 计算机帐户没有获取组所需的权限。	检查Cisco ISE 计算机帐户是否有权限获取 Active Directory 中的用户组。
系统运行状况		
高磁盘 I/O 利用率	Cisco ISE 系统遇到高磁盘 I/O 利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高磁盘空间利用率	Cisco ISE 系统遇到高磁盘空间利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高平均负载	Cisco ISE 系统遇到高平均负载。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。 如果主 MNT 节点和辅助 MNT 节点的凌晨 2:00 时间戳出现对应的高平均负载警报，请注意，CPU 使用率可能由于在该小时运行 DBMS 统计信息而较高。当 DBMS 统计信息运行完成时，CPU 使用率将恢复正常。 高平均负载警报在每个星期日的凌晨 1:00 由每周维护任务触发。此维护任务将重新构建所有占用 1 GB 以上空间的索引。可以忽略此警报。
高内存利用率	Cisco ISE 系统遇到高内存利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高操作数据库使用率	Cisco ISE 监控节点遇到的系统日志数据量高于预期数据量。	检查并缩小操作数据的清除配置窗口。

警报名称	警报说明	警报解决方法
高身份验证延迟	Cisco ISE 系统遇到高身份验证延迟。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
运行状态不可用	监控节点未收到Cisco ISE 节点的运行状态。	确保Cisco ISE 节点正常运行，并能与监控节点通信。
进程已关闭	其中一个Cisco ISE 进程未运行。	重新启动Cisco ISE 应用。
已达到分析器队列大小限制	已达到 ISE 分析器队列大小限制。在达到队列大小限制后，收到的时间将被丢弃。	检查系统是否有足够的资源，并确保已启用终端属性过滤器。
已达到 OCSP 事务阈值	已达到OCSP 事务阈值。当内部 OCSP 服务达到较高流量时触发此警报。	检查系统是否有足够的资源。
许可		
许可证即将到期	Cisco ISE 节点上安装的许可证即将到期。	查看Cisco ISE 中的**许可 (Licencing)** 页面，可查看许可证使用情况。
许可证已过期	Cisco ISE 节点上安装的许可证已过期。	联系Cisco客户团队购买新许可证。
许可证违规	Cisco ISE 节点已检测到您超出或即将超出允许的许可证计数。	联系Cisco客户团队购买额外许可证。
智能许可授权已过期	智能许可的授权已过期。	请参阅**思科 ISE 许可管理 (Cisco ISE License Administration)** 窗口手动更新智能许可的注册，或检查与Cisco智能软件管理器的网络连接。如果问题仍然存在，请联系您的Cisco合作伙伴。
智能许可授权续订故障	从Cisco智能软件管理器更新授权失败。	请参阅**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，使用**许可证 (Licenses)** 表中的**刷新 (Refresh)** 按钮手动更新Cisco智能软件管理器的授权。如果问题仍然存在，请联系您的Cisco合作伙伴。

警报名称	警报说明	警报解决方法
智能许可授权续订成功	从Cisco智能软件管理器更新授权成功。	通知Cisco ISE 的Cisco智能软件管理器授权续订已成功。
智能许可通信故障	Cisco ISE 与Cisco智能软件管理器的通信失败。	检查与Cisco智能软件管理器的网络连接。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可通信已恢复	Cisco ISE 与Cisco智能软件管理器的通信已恢复。	通知与Cisco智能软件管理器的网络连接已恢复。
智能许可取消注册失败	从Cisco智能软件管理器取消注册Cisco ISE 失败。	请查看**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可取消注册成功	从Cisco智能软件管理器取消注册Cisco ISE 成功。	通知从Cisco智能软件管理器取消注册Cisco ISE 成功。
智能许可已禁用	Cisco ISE 上的智能许可已禁用，正在使用传统许可。	请参阅**许可证管理 (License Administration)** 窗口以再次启用智能许可。请参阅《Cisco ISE 管理指南》或联系您的Cisco合作伙伴，以了解如何使用Cisco ISE 上的智能许可。
智能许可评估期已过期	智能许可的评估期已过期。	请参阅**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，以从Cisco智能软件管理器注册Cisco ISE。
智能许可 HA 角色已更改	在使用智能许可时已发生高可用性角色更改。	通知Cisco ISE 的高可用性角色已更改。
智能许可 Id 证书已过期	智能许可证书已过期。	请查看**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，以手动更新智能许可的注册。如果问题仍然存在，请联系您的Cisco合作伙伴。

警报名称	警报说明	警报解决方法
智能许可 Id 证书续签失败	在Cisco智能软件管理器上续签智能许可的注册失败。	请参阅**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，以手动更新智能许可的注册。如果问题仍然存在，请联系您的Cisco合作伙伴。
智能许可 Id 证书续签成功	在Cisco智能软件管理器上续签智能许可的注册成功。	通知Cisco智能软件管理器的注册续签成功。
智能许可无效请求	对Cisco智能软件管理器的请求无效。	请查看**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可不合规	Cisco ISE 许可证不合规。	请查看 **ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。联系您的合作伙伴或Cisco客户团队购买新许可证。
智能许可注册失败	将Cisco ISE 注册到Cisco智能软件管理器失败。	请查看 **ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可注册成功	将Cisco ISE 注册到Cisco智能软件管理器成功。	通知将Cisco ISE 注册到Cisco智能软件管理器成功。
系统错误		
日志收集错误	Cisco ISE 监控收集器进程无法留存从策略服务节点生成的审核日志。	这不会影响策略服务节点的实际功能。如需进一步解决问题，请联系Cisco TAC。
计划的报告导出失败	无法将导出的报告（CSV 文件）复制到配置的存储库。	验证配置的存储库。如果存储库已删除，请重新添加存储库。如果存储库不可用或不可访问，请将其重新配置为有效存储库。
TrustSec		

警报名称	警报说明	警报解决方法
已调配未知 SGT	已调配未知 SGT。	ISE 将未知 SGT 调配为授权流程的一部分。不应将未知 SGT 分配为已知流程的一部分。
部分 TrustSec 网络设备没有最新的 ISE IP-SGT 映射配置	部分 TrustSec 网络设备没有最新的 ISE IP-SGT 映射配置。	ISE 识别出部分网络设备带有不同的 IP-SGT 映射集。使用 **IP-SGT 映射部署 (IP-SGT Mapping Deploy)** 选项更新这些设备。
TrustSec SSH 连接失败	TrustSec SSH 连接失败。	ISE 无法建立与网络设备的 SSH 连接。在**网络设备 (Network Device)** 窗口检查网络设备 SSH 凭证是否与在网络设备上配置的凭证类似。检查网络设备是否已启用从 ISE（IP 地址）进行 SSH 连接。
TrustSec 识别出 ISE 被设置为与版本 1.0 以外的 TLS 版本配合使用	TrustSec 识别出 ISE 设置为与版本 1.0 以外的 TLS 版本配合使用。	TrustSec 仅支持 TLS 版本 1.0。
TrustSec PAC 验证失败	TrustSec PAC 验证失败。	ISE 无法验证网络设备发送的 PAC。在**网络设备 (Network Device)** 窗口以及设备 CLI 检查 Trustsec 设备凭证。确保设备使用由 ISE 服务器调配的有效 PAC。
TrustSec 环境数据下载失败	Trustsec 环境数据下载失败。	Cisco ISE 收到非法的环境数据请求。 请验证以下项目： • PAC 存在于该请求中且有效。 • 所有属性均存在于该请求中。
已忽略 TrustSec CoA 消息	已忽略 TrustSec CoA 消息。	Cisco ISE 已发送 TrustSec CoA 信息，但尚未收到响应。验证网络设备是否支持 CoA。查看网络设备配置。

警报名称	警报说明	警报解决方法
TrustSec 默认出口策略被更改	TrustSec 默认出口策略被更改。	TrustSec 默认出口策略单元格被更改。请确保它与您的安全策略一致。

注释 当您将用户或终端添加到思科 ISE 时，系统不会触发警报。

警报设置

下表说明了**警报设置 (Alarm Settings)** 窗口（ 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)** > **警报配置 (Alarm Configuration)** > **添加 (Add)**）

字段名称	说明
警报类型	警报类型。
警报名称	警报的名称。
说明	警报说明。
建议的操作	触发警报时要执行的操作。
状态	启用或禁用警报规则。
严重性	选择警报的严重性级别。有效的选项包括： • “严重”(Critical)：指示严重错误情况。 • “警告”(Warning)：指示正常但重要的情况。这是默认情况。 • “信息”(Info)：指示信息性的消息。
发出系统日志消息	为Cisco ISE 生成的每个系统警报发送系统日志消息。
输入以逗号分隔的多个电子邮件 **(Enter multiple e-mails separated with comma)**	电子邮件地址或 ISE 管理员名称（或二者）的列表。
电子邮件中的备注（**0** 到 **4000** 个字符）	您希望与系统警报关联的自定义文本消息。

添加自定义报警

Cisco ISE 包含 12 个默认报警类型，例如高内存利用率和配置更改。Cisco定义的系统警报列在**警报设置 (Alarm Settings)** 窗口（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)**）。您只能编辑系统报警。

除现有系统警报外，还可以在现有警报类型下添加、编辑或删除自定义警报。

对于每种警报类型，最多可以创建五个警报。警报总数限制为 200。

在**警报设置 (Alarm Settings)** 窗口的**警报配置 (Alarm Configuration)** 选项卡中，**条件 (Conditions)** 列显示以下四个警报的详细信息：高身份验证延迟 (High Authentication Latency)、高磁盘 I/O 利用率 (High Disk I/O Utilization)、高磁盘空间利用率 (High Disk Space Utilization) 和高内存利用率 (High Memory Utilization)。其中，每个警报都有一个可配置的阈值。但是，即使已配置阈值，**条件 (Conditions)** 列也可能不显示详细信息。在这种情况下，请重新编辑警报的相关阈值字段，以查看**条件 (Conditions)** 列中的详细信息。

要添加报警，请按以下步骤操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)**

步骤 2 在**报警配置 (Alarm Configuration)** 选项卡中，点击**添加 (Add)**。

步骤 3 输入必要的详细信息。请参阅警报设置部分了解详细信息。

基于报警类型（高内存利用率 (High Memory Utilization)、RADIUS 身份验证尝试次数过多 (Excessive RADIUS Authentication Attempts)、TACACS 身份验证尝试次数过多 (Excessive TACACS Authentication Attempts) 等），**警报配置 (Alarm Configuration)** 窗口中会显示其他属性。例如，会为“配置更改”(Configuration Change) 警报显示**对象名称 (Object Name)** 和**对象类型 (Object Type)** 和**管理员名称 (Admin Name)** 字段。您可以为规定不同条件的相同报警添加多个实例。

步骤 4 点击**提交 (Submit)**。

思科 ISE 警报通知和阈值

您可以启用或禁用Cisco ISE 警报，并且配置警报通知行为以通知紧急状况。对于某些警报，您可以配置阈值，如“尝试失败次数过多”(Excessive Failed Attempts) 警报的最大失败尝试次数或“磁盘利用率高”(High Disk Utilization)警报的最大磁盘利用率。

您可以针对每个警报分别配置通知设置。可以输入每个警报（系统定义警报和用户定义警报）所需要通知的用户的电子邮件 ID。

注释 在警报规则级别指定的收件人邮件地址会覆盖全局收件人邮件地址设置。

启用和配置警报

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)**。

步骤 2 从默认警报列表选择警报，点击**编辑 (Edit)**。

步骤 3 选择 **Enable** 或 **Disable**。

步骤 4 如果适用，则配置警报阈值。

步骤 5 点击**提交 (Submit)**。

用于监控的思科 ISE 警报

Cisco ISE 提供系统警报以通知您所发生的各种严重系统状况。由Cisco ISE 生成的警报在 Alarm dashlet 中显示。Alarm dashlet 中自动显示这些通知。

Alarm dashlet 显示最近警报的列表，您可以从列表中选择查看警报详细信息。您可以通过邮件和系统日志消息接收警报通知。

查看监控警报

步骤 1 转至Cisco ISE **Dashboard**。

步骤 2 在**警报 (Alarms)** Dashlet 中点击警报。系统会打开一个新窗口，其中显示警报详细信息和建议的措施。

步骤 3 点击 **Refresh** 以刷新警报。

步骤 4 将警报标记为已读以确认警报，减少警报计数（发出警报的次数）。可以通过选中时间戳旁边的复选框来选择要确认的警报。

从**确认 (Acknowledge)** 下拉列表中选择**确认所选 (Acknowledge Selected)**，将当前显示在窗口中的所有警报标记为已读。默认情况下，窗口中显示 100 行。可以通过从**行数/页数 (Rows/Page)** 下拉列表中选择所需的值来选择要显示的不同行数。

从**确认 (Acknowledge)** 下拉列表中选择**全部确认 (Acknowledge All)**，将列表中的所有警报标记为已读（无论这些警报当前是否显示在窗口中）。

注释　选中标题行中**时间戳 (Time Stamp)** 旁边的复选框后，将选择窗口中显示的所有警报。但是，如果之后取消选中一个或多个所选警报的复选框，则全选功能将失效。此时**时间戳 (Time Stamp)** 旁的复选框处于取消选中状态。

步骤 5 点击与您所选择的警报对应的 **Details** 链接。系统将打开一个新窗口，其中显示与所选警报对应的详细信息。

注释　与在角色更改之前生成的警报对应的**详细信息 (Details)** 链接不显示任何数据。

日志收集

监控服务收集日志和配置数据，存储数据，然后处理数据，以生成报告和警报。您可以查看从部署中的任何服务器收集的日志详情。

警报系统日志收集位置

如果将监控功能配置为将警报通知作为系统日志消息发送，您需要提供一个接收通知的系统日志目标。警报系统目标即发送警报系统日志消息的目标位置。

注释 Cisco ISE 监控要求日志记录源接口配置使用网络接入服务器 (NAS) IP 地址。您必须为Cisco ISE 监控配置交换机。

您还必须有一个配置为系统日志服务器的系统，才能接受系统日志消息。您可以创建、编辑和删除警报系统日志目标。

要将远程日志记录目标配置为警报目标，请执行此程序。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**新建日志记录目标 (New Logging Target)** 窗口中，提交日志记录目标所需的详细信息，并选中**包括此目标的警报 (Include Alarms for this Target)** 复选框。

RADIUS 实时日志

下表介绍“实时日志”(Live logs) 窗口中的字段，其中显示最近的 RADIUS 身份验证。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live Logs)**。只能在主 PAN 中查看 RADIUS 实时日志。

表 *214: RADIUS* 实时日志

字段名称	说明描述
时间 (Time)	显示监控和故障排除收集代理接收日志的时间。此列为必选项，无法取消选择。
状态 (Status)	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。

字段名称	说明描述
详细信息 **(Details)**	点击“详细信息”(Details) 列下的图标可在新浏览器窗口中打开**身份验证详细报告 (Authentication Detail Report)**。此报告提供有关身份验证和相关属性以及身份验证流程的信息。在**身份验证详细信息 (Authentication Details)** 框中，**响应时间 (Response Time)** 是Cisco ISE 处理身份验证流程所需的总时间。例如，如果身份验证包含三个往返消息，初始消息花费 300 毫秒，下一条消息花费 150 毫秒，最后一条消息花费 100 毫秒，则**响应时间 (Response Time)** 为 300 + 150 + 100 = 550 毫秒。 **注释** 您无法查看活动时间超过 48 小时的终端的详细信息。当点击活动时间超过 48 小时的终端的**详细信息 (Details)** 图标时，可能会看到一个包含以下消息的页面：此记录无可用数据。(No Data available for this record.) 数据可能已清除或此会话记录的身份验证发生在一周之前。(Either the data is purged or authentication for this session record happened a week ago.) 或者，如果这是“PassiveID”或“PassiveID 可视性”(PassiveID Visibility) 会话，则不会有 ISE 身份验证详细信息，只有会话。(Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.)
重复次数 (Repeat Count)	显示过去 24 小时内身份验证请求的重复次数，它们在身份、网络设备和授权方面没有任何变化。

字段名称	说明描述
身份 (Identity)	显示与身份验证关联的已登录用户名。 如果用户名不存在于任何 ID 存储区中，则显示为 INVALID。如果身份验证由于任何其他原因而失败，则显示为 USERNAME。 **注释** 这仅适用于用户。这不适用于 MAC 地址。 为了帮助进行调试，可以强制Cisco ISE 显示无效的用户名。为此，请选中位于以下路径下方的**披露无效用户名 (Disclose Invalid Usernames)** 复选框： **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全设置 (Security Settings)**。您还可以将**披露无效用户名 (Disclose Invalid Usernames)** 选项配置为超时，这样就不必手动将其关闭。
终端 ID (Endpoint ID)	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
终端配置文件 (Endpoint Profile)	显示所分析的终端的类型，例如分析为 iPhone、Android、MacBook、Xbox 等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
网络设备 (Network Device)	显示网络访问设备的 IP 地址。
设备端口 (Device Port)	显示终端连接的端口号。
身份组 (Identity Group)	显示分配给生成了日志的用户或终端的身份组。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
服务器 (Server)	指示生成日志的策略服务。
MDM 服务器名称 (MDM Server Name)	显示 MDM 服务器的名称。
事件 (Event)	显示事件状态。
故障原因 (Failure Reason)	如果身份验证失败，显示失败的详细原因。

字段名称	说明描述
身份验证方法 (Auth Method)	显示 RADIUS 协议（例如 Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)、IEEE 802.1x 或 dot1X 等）使用的身份验证方法。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
安全组 (Security Group)	显示由身份验证日志标识的组。
会话 ID (Session ID)	显示会话 ID。

注释 在 **RADIUS 实时日志 (RADIUS Live Logs)** 和 **TACACS+ 实时日志 (TACACS+ Live Logs)** 窗口中，系统会为每个策略授权规则的第一个属性显示一个“已查询 PIP”(Queried PIP) 条目。如果授权规则中的所有属性都与已为之前的规则查询的字典相关，则不会显示其他“已查询 PIP”(Queried PIP) 条目。

您可以在 RADIUS **实时日志 (Live Logs)** 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 页面的字段，此页面显示 TACACS+ AAA 详细信息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 ***215: TACACS*** 实时日志

字段名称	使用指南
生成时间 (Generated Time)	根据特定事件触发时间显示系统日志生成时间。

字段名称	使用指南
日志记录时间 **(Logged Time)**	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态 **(Status)**	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 **(Details)**	在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 **(Session Key)**	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名 **(Username)**	显示设备管理员的用户名。此列为必选项，无法取消选择。
类型 **(Type)**	包括两种类型 - 身份验证和授权。显示身份验证已通过和/或失败的用户名。此列为必选项，无法取消选择。
身份验证策略 **(Authentication Policy)**	显示为特定身份验证选择的策略的名称。
授权策略 **(Authorization Policy)**	显示为特定授权选择的策略的名称。
ISE 节点 **(ISE Node)**	显示处理访问请求的 ISE 节点的名称。
网络设备名称 **(Network Device Name)**	显示网络设备的名称。
网络设备 **IP (Network Device IP)**	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 **(Network Device Groups)**	显示网络设备所属相应网络设备组的名称。
设备类型 **(Device Type)**	显示用于处理来自不同网络设备的访问请求的设备类型。
位置 **(Location)**	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 **(Device Port)**	显示发出访问请求的设备端口号。
故障原因 **(Failure Reason)**	显示拒绝网络设备发出的访问请求的原因。
远程地址 **(Remote Address)**	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。

字段名称	使用指南
匹配的命令集 (Matched Command Set)	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志页面执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

相关主题

TACACS+ 设备管理

配置全局 TACACS+ 设置，第 302 页

实时身份验证

您可以在**实时身份验证 (Live Authentications)** 窗口实时监控最近发生的 RADIUS 身份验证。此窗口显示最近 24 小时内发生的前 10 项 RADIUS 身份验证。此节说明**实时身份验证 (Live Authentications)** 窗口的功能。

实时身份验证 (Live Authentications) 窗口显示与所发生的身份验证事件对应的实时身份验证条目。除了身份验证条目之外，此窗口还显示与这些事件对应的实时会话条目。您还可以向下钻取会话，查看与该会话对应的详细报告。

此**实时身份验证 (Live Authentications)** 窗口提供一个按所发生时间排序的最近 RADIUS 身份验证的表格说明。**实时身份验证 (Live Authentications)** 窗口底部显示的最近更新会显示服务器日期、时间和时区。

注释 如果 Access-Request 数据包中的密码属性为空，则会触发错误消息，访问请求将失败。

一个终端身份验证成功时，**实时身份验证 (Live Authentications)** 窗口会显示两个条目：一个条目对应身份验证记录，另一个条目对应会话记录（从会话实时视图下拉）。随后，当设备进行其他身份验证成功时，与会话记录对应的重复次数计数器会递增其次数。在**实时身份验证 (Live Authentications)** 窗口显示的重复次数计数器会显示所抑制的重复 RADIUS 身份验证成功消息的数量。

请参阅默认情况下显示的实时身份验证数据类别。“最近的 RADIUS 身份验证”(Recent RADIUS Authentications) 部分中说明了这些类别。

您可以选择查看所有列，也可以只显示所选择的数据列。在选择您想要显示的列之后，您可以保存您的选择。

监控实时身份验证

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)**

步骤 2 从**刷新 (Refresh)** 下拉列表中，选择更改数据刷新率的间隔。

步骤 3 点击**刷新 (Refresh)** 图标手动更新数据。

步骤 4 从**显示 (Show)** 下拉列表中，选择一个选项以更改显示的记录数量。

步骤 5 从**时间范围 (Within)** 下拉列表中，选择一个选项以指定时间间隔。

步骤 6 点击**添加或删除列 (Add or Remove Columns)** 并从下拉列表中选择选项以更改所显示的列。

步骤 7 点击下拉列表底部的**保存 (Save)** 以保存您的修改。

步骤 8 点击**显示实时会话 (Show Live Sessions)** 以查看实时 RADIUS 会话。

您可以使用实时会话的动态授权更改 (CoA) 功能，使您可以动态控制活动的 RADIUS 会话。您可以向网络接入设备 (NAD) 发送重新身份验证或断开连接请求。

在 实时身份验证 页面过滤数据

使用实时身份验证页面中的过滤器，可以过滤出您需要的信息，快速排除网络身份验证问题。您可以在身份验证（实时日志）页面筛选记录，只查看那些您感兴趣的记录。身份验证日志包含许多详细信息，过滤特定用户或位置的身份验证信息有助于您快速扫描数据。您可以使用实时身份验证页面的字段中可用的若干运算符，根据搜索条件筛选记录。

- “abc”：包含“abc”
- “!abc”：不包含“abc”
- “{}”：为空
- “!{}”：不为空
- “abc*”：以“abc”开头
- “*abc”：以“abc”结束
- “\!”、“*”、“\{”、“\\”：转义

通过 Escape 选项，您可以筛选包含特殊字符的文本（包括用作过滤器的特殊字符）。您必须将反斜线 (\) 放在特殊字符的前面。例如，如果您要查看身份为“Employee!”的用户的身份验证记录，请在**身份过滤器 (Identity Filter)** 文本框中输入“Employee\!”。在此例中，Cisco ISE 考虑将感叹号 (!) 作为文字字符，而不是作为特殊字符。

此外，使用**状态 (Status)** 字段您可以筛选出仅成功的身份验证记录、失败的身份验证、实时会话，等等。绿色复选标记会筛选过去发生的所有成功身份验证。红色十字标记会筛选所有失败身份验证。蓝色 i 图标会筛选所有实时会话。您还可以选择查看这些选项的组合。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)**

步骤 2 根据 Show Live Authentications 页面中的任意字段筛选数据。

您可以根据成功或失败身份验证，或实时会话筛选结果。

RADIUS实时会话 (Live Sessions)

下表说明了 RADIUS **实时会话 (Live Sessions)** 窗口中的字段，此窗口显示实时身份验证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择您仅可在主 PAN 上查看 RADIUS 实时会话。

表 ***216: RADIUS*** 实时会话

字段名称	说明
启动时间 (Initiated)	显示启动会话时的时间戳。
已更新 (Updated)	显示会话上次由于更改而更新时的时间戳。
帐户会话时间 (Account Session Time)	显示用户会话的时间跨度（秒）。
会话状态 (Session Status)	显示终端设备的当前状态。
操作 (Action)	点击**操作 (Actions)** 图标可对活动 RADIUS 会话重新进行身份验证或断开活动 RADIUS 会话连接。
重复次数 (Repeat Count)	显示用户或终端重新进行身份验证的次数。
终端 ID	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 (Identity)	显示终端设备的用户名。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
审核会话 ID (Audit Session ID）	显示唯一会话标识符。

字段名称	说明
帐户会话 ID (Account Session ID)	显示网络设备提供的唯一 ID。
终端配置文件	显示设备的终端配置文件。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
安全组 (Security Group)	显示由身份验证日志标识的组。
服务器 (Server)	指示已从中生成日志的策略服务节点。
身份验证方法 (Auth Method)	显示RADIUS协议使用的身份验证方法，例如密码身份验证协议 (PAP)、质询握手身份验证协议 (CHAP)、IEE 802.1x 或 dot1x 等等。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
NAS IP 地址 (NAS IP Address)	显示网络设备的 IP 地址。
设备端口 (Device Port)	显示网络设备的连接端口。
PRA 操作 (PRA Action)	显示客户端在网络上成功通过合规性验证后，在客户端上采取的定期重评估操作。
ANC 状态 (ANC Status)	设备的自适应网络控制状态，如“隔离”(Quarantine)、“取消隔离”(Unquarantine) 或“关闭”(Shutdown)。
WLC 漫游 (WLC Roam)	显示用于跟踪已在漫游期间从一个 WLC 传递到另一个 WLC 的终端的布尔值 (Y/N)。它的值为 cisco-av-pair=nas-update =Y 或 N。 **注释** Cisco ISE 依靠 WLC 中的 nas-update=true 属性识别会话是否处于漫游状态。当原始 WLC 在 nas-update=true 时发送记账停止属性时，不会在ISE中删除会话，以避免重新进行身份验证。如果漫游失败，ISE 将在会话处于非活动状态五天后清除该会话。

字段名称	说明
接收的数据包 (Packets In)	显示接收的数据包数量。
发送的数据包 (Packets Out)	显示发送的数据包数量。
接收的字节 (Bytes In)	显示接收的字节数。
发送的字节 (Bytes Out)	显示发送的字节数。
会话源 (Session Source)	指示它是 RADIUS 会话还是被动 ID 会话。
用户域名 (User Domain Name)	显示用户的注册 DNS 名称。
主机域名 (Host Domain Name)	显示主机的注册 DNS 名称。
用户 NetBIOS 名称 (User NetBIOS Name)	显示用户的 NetBIOS 名称。
主机 NetBIOS 名称 (Host NetBIOS Name)	显示主机的 NetBIOS 名称。
许可证类型 (License Type)	显示使用的许可证类型。
许可证详细信息 (License Details)	显示许可证详细信息。
提供程序 (Provider)	终端活动获悉自不同的系统日志源。这些系统日志源称为提供程序。 • Windows Management Instrumentation (WMI) - WMI 是一种 Windows 服务，用于提供通用接口和对象模型来访问有关操作系统、设备、应用和服务的管理信息。 • 代理：代表客户端或另一个程序在客户端上运行的程序。 • 系统日志：客户端发送事件消息的日志记录服务器。 • REST：客户端通过终端服务器进行身份验证。对于此系统日志源，将会显示“TS代理ID”、“源端口开始时间”、“源端口结束时间”和“源第一个端口”值。 • SPAN：使用 SPAN 探测器发现的网络信息。 • DHCP：DHCP 事件。 • 终端 **注释** 从终端会话获悉来自不同提供程序的两个事件后，提供程序在实时会话页面中显示为逗号分隔值。

字段名称	说明
MAC 地址 (MAC Address)	显示客户端的 MAC 地址。
终端检查时间	显示终端探测器上次检查终端的时间。
终端检查结果	显示终端探测的结果。可能的值包括： • 无法接通 • 用户退出 • 活动用户
起始源端口 (Source Port Start)	（仅为 REST 提供程序显示值）显示端口范围中的第一个端口号。
结束源端口	（仅为 REST 提供程序显示值）显示端口范围中的最后一个端口号。
源第一个端口 (Source First Port)	（仅为 REST 提供程序显示值）显示由终端服务器代理分配的第一个端口。 终端服务器指允许多个终端在无需调制解调器或网络接口的情况下连接到其上的服务器或网络设备，可实现多个终端到 LAN 网络的连接。多个终端可能会有相同的 IP 地址，因此难以识别特定用户的 IP 地址。所以，为了识别特定用户，需在服务器上安装终端服务器代理，为每个用户分配一个端口范围。这有助于创建 IP 地址-端口用户映射。
TS 代理 ID (TS Agent ID)	（仅为 REST 提供程序显示值）显示安装在终端上的终端服务器代理的唯一标识。
AD 用户解析的身份 (AD User Resolved Identities)	（仅为 AD 用户显示值）显示匹配的潜在账户。
AD 用户解析的 DN (AD User Resolved DNs)	（仅为 AD 用户显示值）显示 AD 用户的可分辨名称，例如 CN=chris,CN=Users,DC=R1,DC=com

相关主题

更改 RADIUS 会话的授权，第 260 页
思科 ISE 活动 RADIUS 会话，第 259 页

导出摘要

您可以查看过去 7 天内所有用户导出的报告的详细信息以及状态。导出摘要包括手动报告和已计划的报告。导出摘要页面每 2 分钟自动刷新一次。点击刷新图标可手动刷新导出摘要页面。

超级管理员可以取消正在进行或处于排队状态的导出进程。其他用户只能取消他们发起的导出进程。

默认情况下，在给定的时间点只能运行 3 次报告手动导出，其余触发的报告手动导出将排队。计划导出的报告没有此类限制。

注释 当思科 ISE 服务器重新启动时，所有处于排队状态的报告都将重新安排，处于正在进行或正在取消状态的报告将标记为失败。

注释 如果主 MnT 节点关闭，则已计划的报告导出作业将在辅助 MnT 节点上运行。

下表列出“导出摘要”(Export Summary) 页面中的字段。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **导出摘要 (Export Summary)**。

表 *217:* 导出摘要

字段名称	说明
报告已导出	显示报告的名称。
导出依据	显示发起导出进程的用户的角色。
已计划	显示报告导出是否为计划性导出。
触发于	显示在系统中触发导出进程的时间。
存储库	显示将存储导出数据的存储库的名称。
过滤器参数	显示导出报告时选择的过滤器参数。

字段名称	说明
状态	显示导出的报告的状态。它可以是下列类型之一： • 已排队 • 正在进行 • 已完成 • 正在取消 • 已取消 • 失败 • 已跳过 注释 失败状态指示失败的原因。已跳过状态指示当主 MnT 节点关闭时，跳过了计划的报告导出。

您可以在“导出摘要”(Export Summary) 页面中执行以下操作：

- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。

身份验证摘要报告

您可以根据与身份验证请求相关的属性，针对具体用户、设备或搜索条件对网络接入进行故障排除。您可以通过运行“身份验证摘要”(Authentication Summary) 报告实现此目标。

网络接入问题故障排除

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **设备管理 (Device Administration)** > **身份验证摘要报告 (Authentication Summary Report)**。

步骤 2 过滤报告以了解故障原因。

步骤 3 查看报告中 Authentication by Failure Reasons 部分的数据以对您的网络访问问题进行故障排除。

注释 由于身份验证摘要报告会收集和显示与失败或成功的身份验证对应的最新数据，所以报告内容会延迟几分钟后显示。

部署和支持信息的思科支持诊断

概述

Cisco Support Diagnostics Connector 是一项新功能，可帮助Cisco技术支持中心 (TAC) 和Cisco支持工程师从主管理节点获取部署信息。TAC 可以通过连接器获取部署中任何特定节点的支持信息。这些数据有助于更快、更准确地进行故障排除。

您可以通过Cisco ISE 管理门户启用 Cisco Support Diagnostics Connector。利用安全服务交换 (SSE) 云门户，此功能允许在部署中的主策略管理节点与 Cisco Support Diagnostics 之间建立双向连接。

前提条件

- 您必须具有超级管理员或系统管理员角色才能启用或禁用 Cisco Support Diagnostics。

配置 Cisco Support Diagnostics Connector

启用 Cisco Support Diagnostics 功能：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **网络成功诊断 (Network Success Diagnostics)** > **Cisco Support Diagnostics** > **Cisco Support Diagnostics 设置 (Cisco Support Diagnostics Setting)**。
- 默认情况下会禁用此功能。否则，请选中**启用 Cisco Support Diagnostics (Enable Cisco Support Diagnostics)** 复选框以激活 Cisco Support Diagnostics。

验证 Cisco Support Diagnostics 双向连接

要验证Cisco ISE 是否已成功注册/注册 Cisco Support Diagnostics，以及是否已通过安全服务交换门户建立双向连接，请执行以下操作：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。
- 查找以下事件报告：
  1. Cisco Support Diagnostics 已启用。
  2. ISE 服务器已注册到 Cisco Support Diagnostics。
  3. ISE SSE 服务已登记到 Cisco Support Diagnostics。
  4. Cisco Support Diagnostics 双向连接已启用。
- 您还可以转到“操作审核”(Operations Audit) 窗口 （在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **操作审核 (Operations Audit)**），了解作为 Cisco Support Diagnostics 组成部分启用、禁用、注册、取消注册、登记或取消登记的服务的详细信息。

故障排除信息。

如果 Cisco Support Diagnostics 双向连接显示为断开，请检查以下项目：

- **智能许可**：禁用智能许可会自动禁用 Cisco Support Diagnostics。重新启用智能许可以启用连接器。
- **与安全服务交换云的连接**：启用 Cisco Support Diagnostics 后，Cisco ISE 会持续检查与安全服务交换门户建立的持久连接。如果发现此连接断开，则会触发以下严重警报：“警报：Cisco Support Diagnostics 双向连接断开”(Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken)。使用前面提供的配置步骤重新启用该功能。
-

相关信息

管理员可以使用 ERS API 执行以下特定任务：

- 触发特定节点上的支持信息。
- 获取已触发的支持捆绑包的状态。
- 下载支持捆绑包。
- 提取部署信息。

有关使用情况和其他信息，请参阅 ERS SDK 页面。

故障排除诊断工具

诊断工具可帮助您诊断Cisco ISE 网络上的问题并进行故障排除，同时提供关于如何解决问题的详细说明。您可以使用这些工具对身份验证进行故障排除并评估您网络上包括 Trustsec 设备在内的任何网络设备的配置。

RADIUS 身份验证故障排除工具

当身份验证结果不是预期结果时，可使用此工具搜索并选择 RADIUS 身份验证或与 RADIUS 身份验证相关的 Active Directory，以进行故障排除。如果希望通过身份验证但却未通过，或者希望用户或计算机具有特定级别的权限但用户或计算机没有这些权限，请使用此工具。

- 根据用户名、终端 ID、网络访问服务 (NAS) IP 地址和身份验证失败原因搜索 RADIUS 身份验证以排除故障时，Cisco ISE 只显示系统（当前）日期的身份验证。
- 根据 NAS 端口搜索 RADIUS 身份验证以排除故障时，Cisco ISE 显示自上个月初至当前日期的所有 NAS 端口值。

注释 根据 NAS IP 地址和终端 ID 字段搜索 RADIUS 身份验证时，先在操作数据库中执行搜索，然后在配置数据库中执行搜索。

对意外 RADIUS 身份验证结果进行故障排除

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools** > **RADIUS 身份验证故障排除 (RADIUS Authentication Troubleshooting)**。

步骤 2 根据需要在字段中指定搜索条件。

步骤 3 点击 **Search** 以显示与您的搜索条件匹配的 RADIUS 身份验证。

如果要搜索 AD 相关的身份验证，但在部署中未配置 Active Directory 服务器，则系统将显示消息：“未配置 AD”(AD not configured)。

步骤 4 从表格中选择 RADIUS 身份验证记录，并点击 **Troubleshoot**。

如果需要对 AD 相关的身份验证进行故障排除，请访问**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory** > **AD 节点 (AD node)** 下的“诊断工具”(Diagnostics Tool)。

步骤 5 点击**需要用户输入 (User Input Required)**，根据需要修改字段，然后点击**提交 (Submit)**。

步骤 6 点击 **Done**。

步骤 7 故障排除完成后，点击 **Show Results Summary**。

步骤 8 若要查看诊断、为解决问题而采取的步骤以及故障排除摘要，请点击**完成 (Done)**。

执行网络设备命令诊断工具

执行网络设备命令诊断工具允许您在任何网络设备上运行 **show** 命令。

显示的结果与您应在控制台上看到的结果相同。通过此工具，您可以发现设备配置中的任何问题。

使用此工具可验证任何网络设备的配置，也可以使用此工具了解网络设备的配置方式。

要访问执行网络设备命令诊断工具，请选择以下导航路径之一：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **执行网络设备命令 (Execute Network Device Command)**。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **解析器 (Profiler)** > **故障排除 (Troubleshoot)** > **执行网络设备命令 (Execute Network Device Command)**。

在显示的**执行网络设备命令 (Execute Network Device Command)** 窗口中，在相应字段中输入网络设备的 IP 地址和您想要运行的 show 命令。点击**运行 (Run)**。

执行思科 IOS show 命令以检查配置

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **执行网络设备命令 (Execute Network Device Command)**。

步骤 2 在相应字段中输入信息。

步骤 3 点击**运行 (Run)** 以在指定网络设备上执行此命令。

步骤 4 点击**需要用户输入 (User Input Required)**，必要时修改字段。

步骤 5 点击 **提交 (Submit)** 以在网络设备上运行命令，然后查看输出。

评估配置验证程序工具

可以使用此诊断工具评估网络设备的配置并确定配置问题（如果有）。Expert Troubleshooter 会将设备的配置与标准配置进行比较。

无代理终端安全状态故障排除

“无代理终端安全评估”(Agentless Posture) 报告是当无代理终端安全评估未按预期工作时使用的主要故障排除工具。此报告显示无代理流的各个阶段，包括脚本上传完成、脚本上传失败、脚本执行完成等事件，以及任何已知的失败原因。

您可以从两个位置访问无代理终端安全评估故障排除：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **实时日志 (Live Logs)**：在要进行故障排除的客户端的“终端安全评估状态”(Posture Status) 列上，点击三个竖点。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断 (Diagnostic)** > **常规工具 (General Tools)** > **无代理终端安全评估故障排除 (Agentless Posture Troubleshooting)**。

无代理终端安全评估故障排除工具会收集指定客户端的无代理终端安全评估活动。**无代理终端安全评估流 (Agentless Posture Flow)** 会启动终端安全评估并显示当前活动客户端与Cisco ISE 之间的所有交互。**仅下载客户端日志 (Only Download Client Logs)** 会创建一些日志，其中包含最长过去 24 小时的客户端终端安全评估流。客户端可以随时删除日志。收集完成后，可以导出日志的 ZIP 文件。

报告

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **无代理终端安全评估 (Agentless Posture)**，查看运行无代理终端安全评估的所有终端。

解决网络设备配置问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **评估配置验证器 (Evaluate Configuration Validator)**。

步骤 2 在**网络设备 IP (Network Device IP)** 字段中输入您想要评估其配置的网络设备的 IP 地址。

步骤 3 选中相应复选框，然后点击要与建议模板进行比较的配置选项旁边的单选按钮。

步骤 4 点击**运行 (Run)**。

步骤 5 在显示的**进度详细信息... (Progress Details...)** 区域中，点击**点击此处输入凭证 (Click Here to Enter Credentials)**。在显示的**凭证窗口 (Credentials Window)** 对话框中，输入与网络设备建立连接所需的连接参数和凭证，然后点击**提交 (Submit)**。

要取消工作流程，请在**进度详细信息... (Progress Details...)** 窗口中点击**点击此处取消正在运行的工作流程 (Click Here to Cancel the Running Workflow)**。

步骤 6 选中想要分析的接口旁边的复选框，然后点击**提交 (Submit)**。

步骤 7 点击**显示结果摘要 (Show Results Summary)** 以查看配置评估的详细信息。

排除终端安全评估故障

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools** > **终端安全评估故障排除 (Posture Troubleshooting)**。

步骤 2 在相应字段中输入信息。

步骤 3 点击 **Search**。

步骤 4 要查找说明和确定事件的解决方法，请在列表中选择事件，点击 **Troubleshoot**。

会话跟踪测试案例

此工具用于以一种可预测的方式测试策略流，以检查和验证策略的配置方式，而无需让实际流量源自实际设备。

您可以配置测试案例中使用的属性和值的列表。这些详细信息用于执行与策略系统的交互，以模拟对策略的运行时调用。

可通过使用词典配置属性。适用于简单 RADIUS 身份验证的所有词典都列在**属性 (Attributes)** 字段中。

注释 您可以配置仅适用于简单 RADIUS 身份验证的测试案例。

配置会话跟踪测试用例

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 会话跟踪测试用例 (Session Trace Test Cases)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**测试详细信息 (Test Details)** 选项卡中，输入测试用例的名称和描述。

步骤 4 选择一个预定义的测试用例或配置必填属性及其值。可提供以下预定义的测试案例：

- 基本身份验证访问
- 已分析的Cisco电话
- 兼容设备访问
- Wi-Fi 访客（重定向）
- Wi-Fi 访客（访问）

当您选择预定义的测试案例时，Cisco ISE 会自动填充测试案例的相关属性。您可以使用这些属性的默认值，或从显示的选项中选择所需的值。您还可以向测试用例添加其他自定义属性。

添加到测试用例的属性和值会列在“文本”(Text) 字段（“自定义属性”(Custom Attributes) 字段下方）中。当您在文本 (Text) 字段中编辑内容时，Cisco ISE 会检查更新内容的有效性和语法。

您可以在测试详细信息 (Test Details) 页面底部查看所有属性的摘要。

步骤 5 点击**提交 (Submit)**。

Cisco ISE 验证属性及其值，并在保存测试详细信息之前指示任何错误。

步骤 6 在**测试可视化工具 (Test Visualizer)** 选项中，选择要运行此测试用例的节点。

注释 仅具有策略服务角色的节点显示在 **ISE 节点**下拉列表中。

点击**用户组/属性 (User Groups/Attributes)**，从外部身份库检索用户的组和属性。

步骤 7 点击**执行 (Execute)**

Cisco ISE 执行测试案例，并以表格格式显示测试案例的逐步结果。它显示策略阶段、匹配规则和结果对象。点击绿色图标可查看每个步骤的详细信息。

步骤 8 点击**先前测试执行 (Previous Test Executions)** 选项卡查看先前测试执行的结果。您还可以选择和比较任意两个测试案例。Cisco ISE 以表格格式显示每个测试案例的属性的比较视图。

您可以从“RADIUS 实时日志”(RADIUS Live Logs) 页面启动会话跟踪测试用例工具。您可以在“实时日志”(Live Logs) 页面上选择一个条目，然后点击“操作”(Actions) 图标（在“详细信息”(Details) 列中），启动会话跟踪测试用例工具。Cisco ISE 会从相应的日志条目中提取相关属性及其值。如果需要，可以修改这些属性和值，并执行测试用例。

用于高级故障排除的技术支持隧道

Cisco ISE 使用 Cisco IronPort Tunnel 基础设施为Cisco技术支持工程师创建了一个安全隧道，可以通过该系统连接到 ISE 服务器并进行故障排除。Cisco ISE 使用 SSH 通过该隧道创建安全连接。

作为管理员，您可以控制对隧道的访问；您可以选择允许支持工程师访问隧道的时间和期限。没有您的参与，Cisco客户支持无法建立隧道。您将收到有关服务登录的通知。您可以随时禁用隧道连接。默认情况下，技术支持隧道保持开放72小时。我们建议您或技术支持工程师在完成所有故障排除工作后关闭隧道。如有需要，您可以选择将隧道开放时间延长 72 小时。

使用 **tech support-tunnel enable** 命令发起隧道连接。

通过 **tech support-tunnel status** 命令可使系统显示连接状态。该命令提供关于是否已建立连接、身份验证是否失败，或是否无法访问服务器的信息。如果隧道服务器可访问，但ISE无法进行身份验证，ISE 会每隔 5 分钟再次尝试进行身份验证，如此持续 30 分钟，之后隧道会被禁用。

您可以使用 **tech support-tunnel disable** 命令禁用隧道连接。即使当前有技术支持工程师登录时，该命令也会断开现有的隧道。

如果您已从 ISE 服务器建立隧道连接，则生成的 SSH 密钥可在 ISE 服务器上使用。当您在较晚的时间点尝试启用支持隧道时，系统会提示您重新使用之前生成的 SSH 密钥。您可以选择使用相同的密钥或生成新密钥。您还可以使用 **tech support-tunnel resetkey** 命令手动重置密钥。如果您在隧道连接处于启用状态时执行该命令，系统会提示您需先禁用该连接。如果您选择保持现有的连接而不禁用该连接，则系统会在禁用现有连接后重置密钥。如果您选择禁用连接，则系统会断开隧道连接，并立即重置密钥。

在建立隧道连接后，您可以使用 **tech support-tunnel extend** 命令延长连接的持续时间。

有关 **tech support-tunnel** 命令的使用指南，请参阅《Cisco身份服务引擎 CLI 参考指南》。

建立一个技术支持隧道

您可以通过Cisco ISE 命令行界面 (CLI) 建立一个安全隧道。

步骤 1 在Cisco ISE CLI 上输入以下命令：

技术支持隧道启用

系统会提示您输入该隧道的密码和昵称。

步骤 2 输入密码。

步骤 3 （可选）输入隧道昵称。

系统生成一个 SSH 密钥并显示密码、设备序列号和 SSH 密钥。您必须向Cisco客户支持传输这些信息以供支持工程师连接到您的系统。

步骤 4 复制密码、设备序列号和 SSH 密钥并将其发送给Cisco客户支持。

支持工程师现在可以安全地连接到您的 ISE 服务器。您将收到有关服务登录的定期通知。

用于验证传入流量的 TCP Dump 实用工具

TCP 转储实用工具嗅探数据包，可以使用此实用工具验证预计数据包是否已到达节点。例如，当报告中没有显示传入身份验证或日志时，您可能会怀疑没有传入流量或传入流量无法到达Cisco ISE。在这种情况下，您可以运行此工具进行验证。

可以配置 TCP 转储选项，然后从网络流量收集数据以帮助您对网络问题进行故障排除。

使用 TCP Dump 监控网络流量

“TCP 转储”(TCP Dump) 页面列出了您创建的 TCP 转储进程文件。可以创建不同文件以用于不同目的，根据需要运行这些文件，然后在不需要这些文件时将其删除。

通过指定大小、文件数量以及进程运行时间来控制收集的数据。如果进程在时间限制之前完成，并且文件小于最大大小，并且您启用了多个文件，则进程会继续并创建另一个转储文件。

可以对更多接口运行 TCP 转储，包括绑定接口。

不再提供人可读格式选项，转储文件始终为原始格式。

支持与存储库的 IPv6 连接。

开始之前

TCP Dump 页面中的 Network Interface 下拉列表仅显示已配置 IPv4 或 IPv6 地址的网络接口卡 (NIC)。在 VMware 中，默认情况下将连接所有 NIC，因此，所有 NIC 均具有 IPv6 地址，并显示在“网络接口”(Network Interface) 下拉列表中。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **TCP 转储 (TCP Dump)**。

步骤 2 选择 **Host Name** 作为 TCP Dump 实用程序源。

步骤 3 从下拉列表中选择要监控的**网络接口 (Network Interface)**。

步骤 4 在“过滤器”(Filter) 字段中，输入要对其进行过滤的布尔表达式。

系统支持以下标准 tcpdump 过滤器表达式：

- ip host 10.77.122.123
- ip host ISE123

- ip host 10.77.122.123 and not 10.77.122.119

步骤 5 输入此 TCP 转储进程的**文件名 (File Name)**。

步骤 6 选择用于存储 TCP 转储日志文件的**存储库 (Repository)**。

步骤 7 **文件大小 (File Size)** - 选择最大文件大小。

如果转储超出此文件大小，则一个新文件将打开以继续转储。转储可通过新文件继续的次数受**限制为 (Limit to)** 设置的限制。

步骤 8 **限制为 (Limit to)** - 限制转储可扩展到的文件数。

步骤 9 **时间限制 (Time Limit)** - 配置转储在运行多长时间后结束。

步骤 10 通过点击单选按钮，将 Promiscuous Mode 设置为 On 或 Off。默认值为 On。

混合模式为默认包嗅探模式，在此模式下，网络接口将所有流量都传输到系统的 CPU。我们建议将该选项设置为 On。

注释 思科 ISE 不支持大于1500 MTU 的帧（巨帧）。

保存 TCP Dump 文件

开始之前

您应按照“使用 TCP Dump 文件监控网络流量”一节中所描述的内容成功完成任务。

注释 还可以通过Cisco ISE CLI 访问 TCP 转储。有关详细信息，请参阅《思科身份识别服务引擎 *CLI* 参考指南》。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **TCP 转储 (TCP Dump)**。

步骤 2 从**格式 (Format)** 下拉列表中选择选项。默认设置为**人可读 (Human Readable)**。

步骤 3 点击**下载 (Download)**，导航至所需位置，并点击**保存 (Save)**。

步骤 4 若要清除以前的转储文件而无需事先保存，请点击**删除 (Delete)**。

比较终端或用户的意外 SGACL

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec 工具 (Trustsec Tools)** > **出口 (SGACL) 策略 (Egress (SGACL) Policy)**。

步骤 2 输入想要比较其 SGACL 策略的 Trustsec 设备的网络设备 IP 地址。

步骤 3 点击**运行 (Run)**。

步骤 4 点击 **User Input Required**，按需修改字段。

步骤 5 点击**提交 (Submit)**。

步骤 6 点击 **Show Results Summary**，查看诊断和建议的解决步骤。

出口策略诊断流程

出口策略诊断工具 使用下表中介绍的流程进行比较：

流程阶段	说明
1	使用您所提供的IP地址连接设备，然后获取每个源和目标 SGT 对的访问控制列表 (ACL)。
2	检查并确保已在Cisco ISE 中配置出口策略并为每个源和目标 SGT 对获取 ACL。
3	将从网络设备获取的 SGACL 策略与从Cisco ISE 获取的 SGACL 策略进行比较。
4	如果存在不匹配情况，则显示源和目标SGT对。此外，作为额外的信息，系统会显示匹配的条目。

使用 SXP-IP 映射排除支持 TrustSec 的网络中的连接问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec 工具 (Trustsec Tools)** > **SXP-IP 映射 (SXP-IP Mappings)**。

步骤 2 输入网络设备的 IP 地址。

步骤 3 点击**选择**。

步骤 4 点击**运行 (Run)**，然后点击 **User Input Required** 并修改必要字段。

专业的故障排除人员从网络设备检索 Trustsec SXP 连接，并提示您再次选择 SXP 对等设备。

步骤 5 点击 **User Input Required**，然后输入必要信息。

步骤 6 选中您要用于对比 SXP 映射的 SXP 对等设备的复选框，然后输入通用连接参数。

步骤 7 点击**提交 (Submit)**。

步骤 8 点击 **Show Results Summary** 查看诊断和解决步骤。

通过 IP-SGT 映射解决支持 TrustSec 的网络中的连接问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec Tools (Trustsec 工具)** > **IP 用户 SGT (IP User SGT)**。

步骤 2 根据需要在字段中输入信息。

步骤 3 点击**运行 (Run)**。

系统会提示您输入其他信息。

步骤 4 点击**需要用户输入 (User Input Required)**，必要时修改字段。

步骤 5 点击**提交 (Submit)**。

步骤 6 点击 **Show Results Summary** 查看诊断和解决步骤。

设备 SGT 工具

对于启用 Trustsec 解决方案的设备，每个网络设备都会通过 RADIUS 身份验证分配到一个 SGT 值。设备 SGT 诊断工具连接至网络设备（使用您提供的 IP 地址）并获取网络设备 SGT 值，然后检查 RADIUS 身份验证记录以确定最近分配的最新 SGT 值。最后，它会用表格格式显示设备-SGT 对，并确定 SGT 值为相同还是不同。

通过在启用 Trustsec 的网络中比较设备 SGT 映射对连通性问题进行故障排除

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec 工具 (Trustsec Tools)** > **设备 SGT (Device SGT)**。

步骤 2 根据需要在字段中输入信息。

Telnet 的默认端口号为 23，SSH 的默认端口号为 22。

步骤 3 点击**运行 (Run)**。

步骤 4 点击 **Show Results Summary** 查看设备 SGT 的比较结果。

获取其他故障排除信息

通过Cisco ISE，可以从管理员门户下载支持和故障排除信息。可以使用支持捆绑包为Cisco技术支持中心 (TAC) 准备诊断信息来对Cisco ISE 的问题进行故障排除。

注释 支持捆绑包和调试日志为 TAC 提供高级故障排除信息，并且难以解释。可以使用Cisco ISE 提供的各种报告和故障排除工具对在网络中面临的问题进行诊断和故障排除。

思科 ISE 支持捆绑包

您可以配置日志，使其成为支持捆绑包的一部分。例如，您可以配置来自特定服务的日志，使其成为调试日志的一部分。此外，您还可以根据日期过滤日志。

您可以下载的日志分类如下：

- 完整配置数据库：包含可读 XML 格式的Cisco ISE 配置数据库。当您尝试解决问题时，可以将此数据库配置导入另一个Cisco ISE 节点，以便重新创建场景。
- 调试日志： 捕获引导程序、应用配置、运行时、部署、公共密钥基础设施 (PKI) 信息以及监控和报告。

  调试日志为特定的Cisco ISE 组件提供故障排除信息。要启用调试日志，请参阅第 11 章，“日志记录”。如果不启用调试日志，所有信息消息 (INFO) 将包含在支持捆绑包中。有关详细信息，请参阅思科 ISE 调试日志 ，第 1259 页。
- 本地日志：包含来自Cisco ISE 上运行的各种进程的系统日志消息。
- 核心文件 - 包含有助于识别突发事件的原因的重要信息。这些日志在应用发生崩溃并且包含大量转储时创建。
- 监控和报告日志：包含关于警报和报告的信息。
- 系统日志 - 包含Cisco应用部署引擎 (ADE) 相关信息。
- 策略配置：包含在Cisco ISE 中配置的可读格式的策略。

使用 **backup-logs** 命令，您可以从Cisco ISE CLI 下载这些日志。有关详细信息，请参阅思科身份服务引擎 *CLI* 参考指南。

注释 对于 Inline Posture 节点，您不能从 Admin 门户下载支持捆绑包。必须从Cisco ISE CLI 中使用 **backup-logs** 命令。

如果选择从 Admin 门户下载这些日志，您可以执行以下操作：

- 根据日志类型（例如调试日志或系统日志），仅下载日志子集。

- 对于所选日志类型，仅下载最新的 *n* 个文件。此选项允许您控制支持捆绑包的大小以及下载所需的时间。

监控日志提供关于监控、报告和故障排除功能的信息。有关下载日志的详细信息，请参阅 下载思科 ISE 日志文件，第 1258 页。

支持捆绑包

您可以将支持捆绑包以简单 tar.gpg 文件的形式下载至您的本地计算机。支持捆绑包将按照 ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg 的格式用日期和时间戳命名。浏览器会提示您将支持捆绑包保存至适当的位置。您可以提取支持捆绑包的内容并查看 README.TXT 文件，此文件介绍该支持捆绑包的内容，以及在支持捆绑包包含 ISE 数据库内容的情况下如何导入 ISE 数据库内容。

下载思科 ISE 日志文件

在对网络中的问题进行故障排除时，可以下载Cisco ISE 日志文件，以查找更多信息。

您也可以下载包含 ADE-OS 和其他日志文件的系统日志来排除安装和升级方面的问题。

在下载支持捆绑包时，现在可以选择一个公共加密密钥，而无需手动输入加密密钥。如果选择此选项，会使用Cisco PKI 对支持捆绑包进行加密和解密。Cisco TAC 负责维护公钥和私钥。Cisco ISE 使用公钥来加密支持捆绑包。Cisco TAC 可使用私钥解密支持捆绑包。如果您想要提供支持捆绑包到 Cisco TAC 以进行故障排除，请使用此选项。如果您要在现场排除故障，请使用共享密钥加密。

开始之前

- 您必须具有超级管理员或系统管理员权限才能执行以下任务。
- 应已配置调试日志和调试日志级别。

步骤 1 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 3 点击要从其下载支持捆绑包的节点。

步骤 4 在**支持捆绑包 (Support Bundle)** 选项卡中，选择要填充在您的支持捆绑包中的参数。

如果您将所有日志包含在内，则您的支持捆绑包会非常大，下载会需要较长时间。要优化下载流程，请选择只下载最新的 *n* 个文件。

步骤 5 输入生成支持捆绑包的起始日期和结束日期。

步骤 6 选择以下其中一个选项：

- “公共密钥加密”(Public Key Encryption)：如果您想要向Cisco TAC 提供支持捆绑包以进行故障排除，请选择此选项。

- “共享密钥加密”(Shared Key Encryption)：如果您希望在现场排除故障，请选择此选项。如果选择此选项，您必须输入支持捆绑包的加密密钥。

步骤 7 输入支持捆绑包的加密密钥，并重新输入加以确认。

步骤 8 点击 **Create Support Bundle**。

步骤 9 点击**下载 (Download)** 以下载新创建的支持捆绑包。

支持捆绑包是下载到正在运行您的应用浏览器的客户端系统的一个 tar.gpg 文件。

下一步做什么

下载特定组件的调试日志。

思科 ISE 调试日志

调试日志为各种Cisco ISE 组件提供故障排除信息。调试日志包含过去 30 天生成的紧急和警告警报以及在过去 7 天生成的信息警报。报告问题时，可能会要求您启用并发送这些调试日志，以便诊断和解决问题。

注释 启用具有高负载的调试日志（例如监控调试日志）可能会生成有关高负载的警报。

获取调试日志

步骤 1 配置您希望获取调试日志的组件。

步骤 2 下载调试日志。

思科 ISE 组件和相应的调试日志

表 *218:* 组件和相应的调试日志

组件	调试日志
Active Directory	ad_agent.log
缓存跟踪器	tracking.log
实体定义框架 (EDF)	edf.log
JMS	ise-psc.log
许可证	ise-psc.log
通知跟踪器	tracking.log

组件	调试日志
复制部署	replication.log
Replication-JGroup	replication.log
复制跟踪器	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
开机启动向导	ise-psc.log
cisco-mnt	ise-psc.log
客户端	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
访客访问权限管理	guest.log
访客访问权限	guest.log
MyDevices	guest.log
门户	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log

组件	调试日志
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

配置调试向导（按功能）

调试向导包含调试模板，可用于对Cisco ISE 节点问题进行故障排除。可以配置调试配置文件和调试日志。

在**调试配置文件配置 (Debug Profile Configuration)** 窗口中，可以为模板中的各个组件配置调试日志严重性级别。

在**调试日志配置 (Debug Log Configuration)** 窗口中，可以配置调试日志的严重性级别。调试日志可捕获引导程序 (bootstrap)、应用配置、运行时间、部署、监控、报告和公钥基础设施 (PKI) 信息。

注释

- 每节点日志级别优先于调试向导配置文件。
- 当启用多个配置文件来编辑同一组件时，较高的日志级别优先，其中跟踪日志具有最高优先级。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试配置文件配置 (Debug Profile Configuration)** 配置调试配置文件。

步骤 2 要创建新配置文件，请点击**添加 (Add)**。

步骤 3 输入新配置文件的**名称**和**描述**。

选中要包含在配置文件中的组件旁边的复选框，并为每个组件设置相应的**日志级别**。

步骤 4 要保存此配置文件，请点击**保存 (Save)**。

步骤 5 要立即启用 ISE 节点，请点击**启用 (Enable)**。否则，请点击**稍后执行 (Do it Later)**。

步骤 6 如果点击**启用 (Enable)**，请选中要为其启用配置文件的 ISE 节点旁边的复选框。

步骤 7 点击**保存 (Save)**。

步骤 8 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)** 配置调试日志。

步骤 9 点击单选按钮以选择节点。

步骤 10 点击单选按钮以选择组件，然后点击**编辑 (Edit)** 以更改**组件名称**、**日志级别**、**说明**和组件的**日志文件名称**。

步骤 11 点击**保存 (Save)**。

下载调试日志

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 3 在“设备节点”(Appliance node) 列表中，点击您希望下载调试日志的节点。

步骤 4 点击 **Debug Logs** 选项卡。

系统会显示调试日志类型和调试日志的列表。此列表显示的内容取决于您的调试日志配置。

步骤 5 点击您希望下载的日志文件并将其保存到正在运行客户端浏览器的系统中。

您可以根据需要重复此过程下载其他日志文件。可以从**调试日志 (Debug Logs)** 页面下载以下额外的调试日志：

- isebootstrap.log：提供引导日志消息
- monit.log：提供监视程序消息
- pki.log：提供第三方加密库日志
- iseLocalStore.log：提供本地存储文件相关日志
- ad_agent.log：提供 Microsoft Active Directory 第三方库日志
- catalina.log：提供第三方日志