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）。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 5 页
配置认知威胁分析适配器，第 6 页
为 CTA 适配器配置授权配置文件，第 8 页
使用操作过程属性配置授权策略，第 8 页
以威胁防护为中心的 NAC 服务，第 1 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 4 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 4 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 4 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 11 页。
- Nexpose 适配器，请参阅配置 Nexpose 适配器， 第 13 页。
- 租户适配器，请参阅。配置 Tenable 适配器， 第 15 页

步骤 3 配置授权配置文件， 第 18 页。

步骤 4 配置隔离易受攻击的终端的例外规则， 第 18 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 5 页
配置认知威胁分析适配器， 第 6 页
为 CTA 适配器配置授权配置文件， 第 8 页
使用操作过程属性配置授权策略， 第 8 页
以威胁防护为中心的 NAC 服务， 第 1 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
思科 ISE 部署术语
配置思科 ISE 节点

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 *1:* 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。 • **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
- 管理节点
- 策略服务节点
- 监控节点
- 思科 pxGrid 节点
- 同步主要和辅助思科 ISE 节点

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

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 *2:* 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

分析服务使用的网络探测功能

在思科 ISE 节点中配置分析服务

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 *3:* 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
- 查看系统证书
- 生成自签证书

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 *4:* 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
- 创建证书签名请求 (CSR) 并将 CSR 提交给证书颁发机构
- 将 CA 签名的证书与 CSR 绑定

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 *5:* 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
- 用户和终端证书续订
- 配置思科 ISE 以使用证书对个人设备进行身份验证
- 将思科 ISE 配置为允许用户续订证书
- 吊销终端证书

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 *6:* 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

添加 OCSP 客户端配置文件

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 *7:* 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
- 查看系统证书
- 导入系统证书

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 *8:* 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
查看受信任证书库证书
更改受信任证书库中的证书状态
在受信任的证书库中添加证书

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 *9:* 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

编辑受信任证书

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 *10:* 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
证书链导入
将根证书导入受信任证书库

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 ***11: 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
- 思科 ISE CA 服务在线证书状态协议响应器
- OCSP 证书状态值
- OCSP 高可用性
- OCSP 故障
- OCSP 统计计数器
- 添加 OCSP 客户端配置文件

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 *12:* 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

配置思科 ISE 以使用证书对个人设备进行身份验证

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 *13:* 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
- 证书模板扩展名
- 配置思科 ISE 以使用证书对个人设备进行身份验证
- 为 pxGrid 控制器部署思科 ISE CA 证书
- 在授权策略条件中使用证书模板

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 *14:* 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
- 思科 ISE 系统日志
- 远程系统日志消息格式
- 思科 ISE 消息目录
- 集合过滤器
- 事件抑制绕行过滤器
- 配置远程系统日志收集位置
- 配置集合过滤器

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 *15:* 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
- 配置远程系统日志收集位置
- 设置消息代码的严重性级别

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 *16:* 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
创建存储库

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 *17:* 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
- 按需备份和计划备份
- 备份历史记录
- 备份失败
- 思科 ISE 恢复操作
- 导出身份验证和授权策略配置
- 在分布式环境中同步主节点和辅助节点
- 执行按需备份

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 *18:* 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
- 按需备份和计划备份
- 备份历史记录
- 备份失败
- 思科 ISE 恢复操作
- 导出身份验证和授权策略配置
- 在分布式环境中同步主节点和辅助节点
- 使用 CLI 备份
- 计划备份

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 *19:* 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 *20:* 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

创建新管理员

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 *21:* 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
- 配置管理员会话超时
- 终止活动管理会话

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
安全评估租约
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
设置网络转换延迟计时器，使客户端实现转换
将登录成功窗口设置为自动关闭
设置非代理设备的终端安全评估状态

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 *22:* 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
- 定期重新评估
- 终端安全状态评估选项
- 安全评估补救选项
- 安全评估的自定义条件
- 自定义安全评估补救措施
- 配置定期重新评估

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 *23:* 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

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 *24:* 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
将 EAP-FAST 用作协议的指南
EAP-FAST 的优势
配置 EAP-FAST 设置

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 *25:* 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
将 EAP-FAST 用作协议的指南
为 EAP-FAST 生成 PAC

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 *26: 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
将 EAP-TTLS 用作身份验证协议
配置 EAP-TTLS 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 *27: 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

配置 EAP-TLS 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 *28: 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

配置 PEAP 设置

使用 PEAP 的优势

PEAP 协议支持的请求方

PEAP 协议流程

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 *29: 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
- 思科 ISE 中的 RADIUS 协议支持
- 配置 RADIUS 设置

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
- TrustSec 组件
- 配置 TrustSec 全局设置

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 *30:* 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
矩阵视图
配置 TrustSec 矩阵

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。

表 *31:* 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
在思科 ISE 中配置第三方网络设备
DHCP 探测功能

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 *32:* 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

使用策略和身份的静态分配创建终端

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 *33*: 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

从 LDAP 服务器导入终端

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 *34:* 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

创建终端身份组

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 *35: 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 *36: 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 *37: 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 *38: 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 *39: 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 *40: 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
- LDAP 用户身份验证
- LDAP 用户查找
- 添加 LDAP 身份源

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 *41: 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

添加 RADIUS 令牌服务器

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 *42: 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 *43: 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
思科 ISE 和 RSA SecurID 服务器集成
添加 RSA 身份源

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 *44:* 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 *45:* 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 *46:* 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 *47:* 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 *48:* 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
思科 ISE 中的第三方网络设备支持
创建网络设备配置文件

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 *49*: 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

配置外部 RADIUS 服务器

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 *50: 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

定义 RADIUS 服务器序列

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 *51: 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
创建授权配置文件
个人设备门户

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
创建 BYOD 门户
移动设备管理门户
创建 MDM 门户
自带设备门户语言文件的 HTML 支持
对移动设备管理门户语言文件的 HTML 支持

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
- 创建 BYOD 门户
- 自带设备门户语言文件的 HTML 支持

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
创建证书调配门户
证书调配门户语言文件的 HTML 支持

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
创建客户端调配门户
客户端调配门户语言文件的 HTML 支持

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
创建 MDM 门户
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

创建我的设备门户

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

创建我的设备门户

监控我的设备门户和终端活动

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

创建我的设备门户

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

创建我的设备门户

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

门户中的 UTF-8 字符支持

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 *52:* 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

我的设备门户

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

创建我的设备门户

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

访问设备门户