细分市场

策略集

Cisco ISE 是基于策略的网络访问控制解决方案，可提供网络访问策略集，允许您管理多个不同的网络访问用例，如无线、有线、访客和客户端调配。通过策略集（网络访问集和设备管理集），您可以对同一集合内的身份验证策略和授权策略进行逻辑分组。您可以基于区域具有若干策略集，例如基于位置、访问类型和类似参数的策略集。安装ISE时，始终有一个定义的策略集，即默认策略集，默认策略集包含预定义和默认的身份验证、授权和例外策略规则。

创建策略集时，可以配置这些规则（使用条件和结果进行配置），以便选择策略集级别的网络访问服务、身份验证策略级别的身份源，以及授权策略级别的网络权限。从适用于各种不同供应商的Cisco ISE 支持的字典中，可以使用任何属性定义一个或多个条件。Cisco ISE 可以让您将条件创建为可重复使用的单个策略元素。

每个策略集用于与网络设备进行通信的网络访问服务是在该策略集的顶层定义的。网络访问服务包括：

- 允许的协议 - 为处理初始请求和协议协商而配置的协议
- 代理服务 - 将请求发送至外部 RADIUS 服务器进行处理

注释 从设备管理工作中心，您还可以为策略集选择相关的 TACACS 服务器序列。使用 TACACS 服务器序列可配置要处理的 TACACS 代理服务器序列。

策略集按层次结构进行配置，其中位于策略集顶层的规则（可从策略集表中查看）适用于整个策略集，并先于其余策略和例外规则进行匹配。此后，按以下顺序应用集合的规则：

1. 身份验证策略规则
2. 本地策略例外
3. 全局策略例外
4. 授权策略规则

注释 对于网络访问和设备管理策略，策略集功能是相同的。在使用网络访问和设备管理工作中心时，可以应用本章中介绍的所有流程。本章专门讨论网络访问工作中心策略集。 在思科 ISE GUI 中，点击 **菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。

ISE 社区资源

有关从 WLC 使用 RADIUS 结果的信息，请参阅 WLC Called-Station-ID（Radius 身份验证和记账配置）。

策略集配置设置

下表介绍**策略集 (Policy Sets)** 窗口中的字段，由此窗口可配置策略集，包括身份验证、例外和授权策略。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**，找到网络访问策略。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**，找到设备管理策略。

表 *1:* 策略集配置设置

字段名称	使用指南
状态	选择此策略的状态。它可以是下列选项之一： • **已启用 (Enabled)**：此策略条件处于活动状态。 • **已禁用 (Disabled)**：此策略条件处于非活动状态，不会被评估。 • **仅监控 (Monitor Only)**：此策略条件不会被评估。
策略集名称	为此策略集输入一个唯一的名称。
条件	在新策略行中，点击加号 (+) 图标，或者在现有策略行中，点击“编辑”(Edit) 图标以打开 Conditions Studio。
说明	输入策略的唯一说明。
允许的协议或服务器序列	选择已创建的允许协议，或点击 (+) 号以**创建新的允许协议**、**创建新的 Radius 序列**或**创建 TACACS 序列**。
条件	在新的例外行中，点击加号 (+) 图标，或者在现有例外行中，点击“编辑”(Edit) 图标以打开 Conditions Studio。
点击数	命中数是一种诊断工具，用于指示条件匹配的次数。将鼠标悬停在该图标上可查看上次更新时间、重置为零和查看更新频率。

字段名称	使用指南
操作	点击“操作”(Actions) 列中的齿轮图标 ⚙，查看并选择不同的操作： • 在上方插入新行 (Insert new row above)：在打开“操作”(Actions) 菜单的策略上方插入新策略。 • 在下方插入新行 (Insert new row below)：在打开“操作”(Actions) 菜单的策略下方插入新策略。 • 在上方复制 (Duplicate above)：在打开“操作”(Actions) 菜单的策略上方插入复制的策略，高于原始集。 • 在下方复制 (Duplicate below)：在打开“操作”(Actions) 菜单的策略下方插入复制的策略，低于原始集。 • 删除 (Delete)：删除策略集。
查看	点击箭头图标可打开特定策略集的集合视图，并查看其身份验证、例外和授权子策略。

身份验证策略

每个策略集可以包含多个身份验证规则，它们共同代表该策略集的身份验证策略。身份验证策略的优先级根据这些策略在策略集本身中的显示顺序来确定（从“身份验证策略”(Authentication Policy) 区域中的“集合视图”(Set view) 页面）。

Cisco ISE 根据策略集级别配置的设置动态选择网络访问服务（允许的协议或服务器序列），然后从身份验证和授权策略级别检查身份源和结果。您可以定义一个或多个使用Cisco ISE 字典中任何属性的条件。Cisco ISE 可以让您将条件单个策略元素，它们可以存储在系统库中，然后重复用于其他基于规则的策略。

身份验证方法是身份验证策略的结果，可以是以下任意一种：

- 拒绝访问 - 系统拒绝用户的访问并且不执行身份验证。
- 身份数据库 - 可以是下述单个身份数据库中的一个：
  - 内部用户
  - 访客用户
  - 内部终端
  - Active Directory

- 轻量级目录访问协议 (LDAP) 数据库
- RADIUS 令牌服务器（RSA 或 SafeWord 服务器）
- 证书身份验证配置文件

- 身份源序列 - 用于身份验证的身份数据库的序列。

初始Cisco ISE 安装时实施的默认策略集包括默认 ISE 身份验证和授权规则。默认策略集还包括用于身份验证和授权的其他灵活内置规则（不是默认规则）。可向这些策略添加其他规则，也可以删除和更改内置规则，但不能删除默认规则，也不能删除默认策略集。

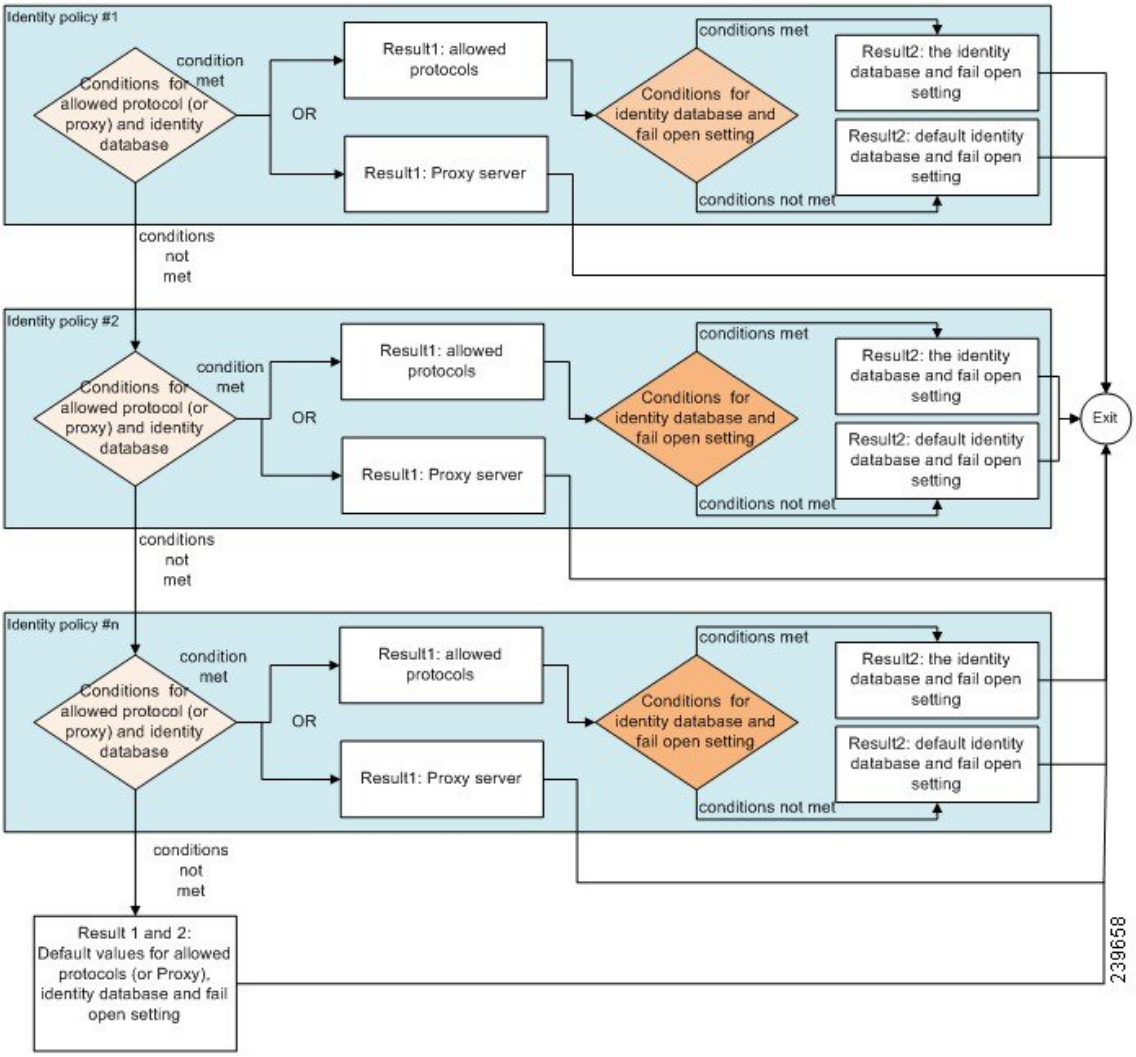
身份验证策略流

在身份验证策略中，可以定义多个由条件和结果组成的规则。ISE 会评估您指定的条件，并根据评估结果分配相应的结果。系统根据匹配条件的第一个规则选择身份数据库。

您还可以定义包括不同数据库的身份源序列。您可以定义您希望Cisco ISE 查询这些数据库的顺序。Cisco ISE 将依次访问这些数据库，直至身份验证成功。如果在外部数据库中同一用户有多个实例，则身份验证失败。身份源中只能有一个用户记录。

我们建议您在身份源序列中仅使用三个，或者最多四个数据库。

图 *1:* 身份验证策略流



身份验证失败 - 策略结果选项

如果您选择的身份方法为拒绝访问，则会发送拒绝消息作为对请求的响应。如果选择身份数据库或身份源序列，并且身份验证成功，则会继续处理为相同策略集配置的授权策略。某些身份验证失败，这些失败情况会按照以下方式分类：

- Authentication failed - 收到身份验证已失败的明确响应，例如错误凭证、禁用的用户等。默认操作是拒绝。
- User not found - 在任何身份数据库中均未找到此用户。默认操作是拒绝。
- Process failed - 无法访问身份数据库。默认操作是丢弃。

Cisco ISE 允许您配置下列任意一条身份验证失败的操作：

- Reject - 发送拒绝响应。
- Drop - 不发送任何响应。
- Continue - Cisco ISE 继续处理授权策略。

即使您选择继续选项，可能会存在一些实例，在这些实例中，由于正在使用的协议受到限制，Cisco ISE 无法继续处理请求。对于使用 PEAP、LEAP、EAP-FAST、EAP-TLS 或 RADIUS MSCHAP 的身份验证，当身份验证失败时或未找到用户时，无法继续处理请求。

当身份验证失败时，可继续处理 PAP/ASCII 和 MAC 身份验证绕行（MAB 或主机查找）的授权策略。对于其他所有身份验证协议，当身份验证失败时将发生以下情况：

- Authentication failed - 发送拒绝响应。
- User or host not found - 发送拒绝响应。
- Process failure - 不发送响应，并丢弃请求。

配置身份验证策略

根据需要，通过配置和维护多个身份验证规则，为每个策略集定义身份验证策略。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)** 可获取网络访问策略。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 可获取设备管理策略。

步骤 2 从要添加或更新身份验证策略的策略集对应的行中，从策略集表中的“视图”列点击 ›，以便访问所有策略集详细信息并创建身份验证和授权策略以及策略例外。

步骤 3 点击页面“身份验证策略”（Authentication Policy）部分旁边的箭头图标，展开并查看表中的所有身份验证策略规则。

步骤 4 在**操作 (Actions)** 列中，点击齿轮图标。从下拉菜单中，根据需要选择任何插入或重复选项来插入新的身份验证策略规则。
身份验证策略表中会显示一个新行。

步骤 5 在**状态 (Status)** 列中，点击当前**状态 (Status)** 图标，然后从下拉列表中根据需要更新策略集的状态。有关状态的详细信息，请参阅身份验证策略配置设置，第 8 页。

步骤 6 对于表中的任何规则，点击**规则名称 (Rule Name)** 或**说明 (Description)** 单元格，可做出任何必要的自由文本更改。

步骤 7 要添加或更改条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击 。Conditions Studio 将打开。有关详细信息，请参阅策略条件，第 25 页。

不是您选择的所有属性都包含“等于”、“不等于”、“位于”、“不位于”、“匹配”、“开头为”或“开头非”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

注释 您必须使用“等于”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。如果是列表，“位于”运算符会检查列表中是否存在特定值。如果是单个字符串，“位于”运算符会检查字符串是否与“等于”运算符相同。

步骤 8 按照检查和匹配策略的顺序来组织表中的策略。要更改规则的顺序，请将这些行拖放到正确位置。

步骤 9 点击**保存 (Save)** 以保存和实施所做的更改。

下一步做什么

1. 配置授权策略

身份验证策略配置设置

下表介绍**策略集 (Policy Sets)** 窗口的**身份验证策略 (Authentication Policy)** 部分中的字段，由此窗口可将身份验证子策略配置为策略集的一部分。对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。从“策略集”(Policy Sets) 页面，选择 **查看 (View)** > **身份验证策略 (Authentication Policy)**。

表 *2:* 身份验证策略配置设置

字段名称	使用指南
状态	选择此策略的状态。它可以是下列选项之一： • **已启用 (Enabled)**：此策略条件处于活动状态。 • **已禁用 (Disabled)**：此策略条件处于非活动状态，不会被评估。 • **仅监控 (Monitor Only)**：此策略条件将被评估，但结果不实施。您可以在 Live Log 身份验证页面查看此策略条件的结果。在此情况下，查看详细报告，了解受监控的步骤和属性。例如，您可能想要添加新策略条件，但不确定此条件是否为您提供正确的结果。在此情况下，您可以在监控模式下创建策略条件来查看结果，如果您对结果满意，可以启用此选项。

字段名称	使用指南
规则名称	输入此身份验证策略的名称。
条件	在新策略行中，点击加号 (+) 图标，或者在现有策略行中，点击“编辑”(Edit) 图标以打开 Condition Studio。
使用	选择要用于身份验证的身份源。如果您配置了身份源序列，也可以选择身份源序列。 您可以编辑在此规则中定义的任何身份源都与请求不匹配时您想要Cisco ISE 使用的默认身份源。
选项	为身份验证失败、未找到用户或进程失败事件定义进一步的操作。您可以选择下面一个选项： • **拒绝 (Reject)**：发送拒绝响应。 • **丢弃 (Drop)**：未发送响应。 • **继续 (Continue)**：Cisco ISE 继续执行授权策略。
点击数	命中数是一种诊断工具，用于指示条件匹配的次数。
操作	点击“操作”(Actions) 列中的齿轮图标 ⚙，查看并选择不同的操作： • 在上方插入新行 (Insert new row above)：在打开“操作”(Actions) 菜单的策略上方插入新的身份验证策略。 • 在下方插入新行 (Insert new row below)：在打开“操作”(Actions) 菜单的策略下方插入新的身份验证策略。 • 在上方复制 (Duplicate above)：在打开“操作”(Actions) 菜单的策略上方插入复制的身份验证策略，高于原始集。 • 在下方复制 (Duplicate below)：在打开“操作”(Actions) 菜单的策略下方插入复制的身份验证策略，低于原始集。 • 删除 (Delete)：删除策略集。

基于密码的身份验证

身份验证对用户信息进行验证，以确认用户身份。传统身份验证使用名称和固定密码。这是最普遍、最简单和最经济的身份验证方法。缺点在于此信息可能会被告知他人、被猜到或捕获。使用简单、未加密用户名和密码的方法不被视为强身份验证机制，但是对于低授权或低权限级别（例如互联网访问）可能已足够。

使用加密密码和加密技术的安全身份验证

应使用加密来降低网络中的密码捕获风险。客户端和服务器访问控制协议（例如 RADIUS）可对密码加密，以防止在网络中捕获密码。但是，RADIUS 仅在身份验证、授权和记账 (AAA) 客户端与 Cisco ISE 之间运行。在身份验证流程中的以下位置点之前，未经授权的人员可以获取明文密码，如以下示例所示：

- 在通过电话线路拨号的最终用户客户端之间的通信中
- 在终止于网络接入服务器的 ISDN 线路上
- 在最终用户客户端与托管设备之间的 Telnet 会话中

安全性较高的方法会采用加密技术，例如，那些用于质询握手身份验证协议 (CHAP)、一次性密码 (OTP) 和基于 EAP 的高级协议中的加密技术。Cisco ISE 支持各种身份验证方法。

身份验证方法和授权权限

身份验证与授权之间存在基本的隐式关系。向用户授予的授权权限越多，身份验证的能力就越强。Cisco ISE 通过提供各种身份验证方法来支持此关系。

身份验证面板

Cisco ISE 控制板会概述网络中和设备发生的全部身份验证。它提供在身份验证 Dashlet 中身份验证和身份验证失败的概览信息。

RADIUS 身份验证 Dashlet 提供以下有关Cisco ISE 已处理身份验证的统计信息：

- Cisco ISE 已处理 RADIUS 身份验证请求的总数，包括已通过的身份验证、已失败的身份验证以及相同用户的同时登录数。
- Cisco ISE 已处理的 RADIUS 已失败的身份验证请求的总数。

您还可以查看 TACACS + 身份验证的摘要。TACACS + 身份验证 Dashlet 提供设备身份验证的统计信息。

有关设备管理身份验证的详细信息，请参阅。TACACS 实时日志有关 RADIUS 实时日志设置的其他信息，请参阅RADIUS 实时日志。

ISE 社区资源

有关如何对失败的身份验证和授权进行故障排除的信息，请参阅如何：对 ISE 失败的身份验证和授权进行故障排除。

查看身份验证结果

Cisco ISE 提供多种方式查看实时身份验证摘要。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 对于网络身份验证 (RADIUS)，请选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)** 或对于设备身份验证 (TACACS)，请选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)** 查看实时身份验证摘要。

步骤 2 您可以通过以下方式查看身份验证摘要：

- 将鼠标悬停在“状态”(Status) 图标上，以查看身份验证的结果和简短摘要。系统将显示一个包含状态详细信息的弹出窗口。
- 在列表顶部显示的任何一个或多个文本框中输入搜索条件，然后按 **Enter** 键以筛选您的结果。
- 点击 Details 列中的放大镜图标以查看详细报告。

  注释 由于身份验证摘要报告或控制板会收集和显示与失败或成功的身份验证对应的最新数据，因此报告内容会延迟几分钟后显示。

身份验证报告和故障排除工具

除身份验证详细信息外，Cisco ISE 还提供各种可用于有效管理网络的报告和故障排除工具。

可以运行各种报告，了解网络中的身份验证趋势和流量。可以生成历史以及当前数据的报告。以下是身份验证报告列表：

- AAA 诊断
- RADIUS 记账
- RADIUS 身份验证
- 身份验证摘要

注释 您必须在 Cisco Catalyst 4000 系列交换机上启用 IPv6 监听，否则 IPv6 地址不会映射到身份验证会话，也不会显示在 show 输出中。使用以下命令可启用 IPv6 监听：

```
vlan config <vlan-number> ipv6 snooping end ipv6 nd raguard policy router device-role router
 interface <access-interface> ipv6 nd raguard interface <uplink-interface> ipv6 nd raguard
 attach-policy router end
```

授权策略

授权策略是Cisco ISE 网络授权服务的组件。此服务允许您为访问网络资源的特定用户和组定义授权策略并配置授权配置文件。

授权策略可包含条件要求，即使用复合条件组合一个或多个身份组，而该复合条件包括可返回一个或多个授权配置文件的授权检查。此外，除了使用特定的身份组外，可能存在条件要求。

在Cisco ISE 中创建授权配置文件时使用授权策略。授权策略包括授权规则。授权规则具有三个元素：名称、属性以及权限。权限元素映射到授权配置文件。

思科 ISE 授权配置文件

授权策略将规则与特定用户和组身份关联以创建相应的配置文件。只要这些规则与已配置的属性匹配，策略就会返回授予权限的相应授权配置文件并且相应地授予网络访问权限。

例如，授权配置文件可以包括以下类型中包含的一系列权限：

- 标准配置文件
- 例外配置文件
- 基于设备的配置文件

配置文件包括从一组资源中选择的属性，这些属性存储于任何可用供应商字典中，并且在满足特定授权策略的条件时就会返回这些属性。由于授权策略可以包括映射到单个网络服务规则的条件，这些策略还可以包括授权检查列表。

这些授权验证都必须符合要返回的授权配置文件。授权验证通常由一个或多个条件组成，包括可添加至库中的用户定义的名称，其他授权策略然后可以重复使用这些条件。

授权配置文件的权限

在开始配置授权配置文件的权限之前，请确保：

- 了解授权策略与配置文件之间的关系
- 熟悉 Authorization Profile 页面
- 知悉在配置策略和配置文件时要遵守的基本规定
- 了解在授权配置文件中构成权限的内容

要使用授权配置文件，请选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)**。从左侧菜单中，选择 **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

使用 Results 导航窗格作为用于显示、创建、修改、删除、复制或搜索网络上不同类型授权配置文件的策略元素权限的过程的起点。Results 窗格初始显示 Authentication、Authorization、Profiling、Posture、Client Provisioning 和 Trustsec 选项。

通过授权配置文件，您可以选择在接受 RADIUS 请求时要返回的属性。Cisco ISE 提供可以通过配置 Common Tasks 设置来支持常用属性的机制。您必须输入 Common Tasks 属性的值，Cisco ISE 会将这些值转换为基础 RADIUS 值。

ISE 社区资源

有关如何在 802.1x 请求方（Cisco AnyConnect 移动安全）和身份验证器（交换机）之间配置媒体访问控制安全 (MACsec) 加密的示例，请参阅使用思科 AnyConnect 和 ISE 配置进行 MACsec 交换机-主机加密示例。

基于位置的授权

Cisco ISE 可与Cisco移动服务引擎 (MSE) 集成以引入基于物理位置的授权。Cisco ISE 使用来自 MSE 的信息基于 MSE 报告的用户实际位置提供差异化网络访问。

通过此功能，您可以使用终端位置信息在用户位于相应区域时提供网络访问。还可以将终端位置作为策略的其他属性添加，以便基于设备位置定义更为细化的策略授权集。您可以在授权规则内配置使用基于位置的属性的条件，例如：

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

您可以定义位置层次结构（园区/建筑物/楼层结构），并使用 Cisco Prime 基础设施应用配置安全区域和不安全区域。定义位置层次结构后，必须将位置层次结构数据与 MSE 服务器同步。有关 Cisco Prime 基础设施的详细信息，请参阅：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html。

您可以添加一个或多个 MSE 实例，以便将基于 MSE 的位置数据集成到授权过程。可以从这些 MSE 检索位置层次结构数据，并使用此数据配置基于位置的授权规则。

要跟踪终端移动，请在创建授权配置文件时选中“跟踪移动”(Track Movement) 复选框。Cisco ISE 将每 5 分钟查询一次相关 MSE 的终端位置，以验证是否更改了位置。

注释 在将 MSE 设备添加到思科 ISE 时，请将证书从 MSE 设备复制到 ISE 以方便授权。

注释 跟踪多个用户将因频繁更新影响性能。“跟踪移动”(Track Movement) 选项可用于安全性较高的位置。

位置树是使用从MSE实例检索的位置数据进行创建的。您可以通过使用位置树选择呈现给授权策略的位置条目。

注释 您将需要思科 ISE Advantage 许可证才能使用位置服务。

添加 MSE 服务器。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration) > 网络资源 (Network Resources) > 位置服务 (Location Services) > 位置服务器 (Location Servers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入 MSE 服务器详细信息，例如服务器名称、主机名/IP 地址、密码等等。

步骤 4 点击**测试 (Test)**可使用您提供的服务器详细信息来测试 MSE 连接。

步骤 5 （可选）在**查找位置 (Find Location)** 字段输入终端的 MAC 地址，并点击**查找 (Find)** 以检查该终端当前已连接到此 MSE。

如果找到终端位置，它显示为以下格式：*Campus:Building:Floor:Zone*。有时，根据位置层次结构和区域设置可显示多个条目。例如，如果一个名为 *Campus1* 中的一栋楼 (*building1*) 的所有楼层定义为非安全区域，一楼的实验区域定义为安全区域，当终端位于实验区域时，将会显示以下条目：

在以下位置查找到终端：

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

步骤 6 点击**提交 (Submit)**。

在新的 MSE 添加后，转到“位置树”(Location Tree) 页面，然后点击**获取更新 (Get Update)** 检索其位置层次结构并将其添加到位置树。如果该树上定义了过滤器，这些过滤器也应用于新的 MSE 条目。

位置树

位置树是通过使用从移动服务引擎 (MSE) 示例中检索的位置数据创建的。要查看位置树 (Location Tree)，请选择**管理 (Administration) > 网络资源 (Network Resources) > 位置服务 (Location Services) > 位置树 (Location Tree)**。

如果建筑物有多个 MSE，Cisco ISE 将收集来自所有 MSE 的详细位置信息并将单个树里呈现这些信息。

您可以通过位置树选择对授权策略可见的位置条目。您还可以根据您的需求隐藏特定位置。建议在隐藏位置之前更新位置树。即使已更新树，隐藏位置仍会保持隐藏状态。

如果与授权规则相关的位置条目已修改或删除，您必须禁用受影响的规则并将这些位置设置为未知，或为每个受影响的规则选择一个替代位置。您必须在应用更改或取消更新之前检验新的树状结构。

点击**获取更新** (Get Update) 从所有 MSE 获取最新位置层次结构。在检验新的树结构后，点击“保存”(Save) 以应用更改。

可下载 ACL

访问控制列表 (ACL) 是访问控制条目 (ACE) 的列表，可由策略实施点（例如，交换机）应用到资源。每个ACE可确定每个用户该对象的允许权限，如读取、写入、执行等。例如，可以为使用网络的销售区域而配置 ACL，同时使用一个 ACE 允许销售部门获得写入权限，并使用单独的 ACE 允许组织的所有其他员工获得读取权限。使用 RADIUS 协议时，ACL 通过过滤源和目标 IP 地址、传输协议和其他参数来进行授权。静态 ACL 驻留在交换机上并直接从交换机配置，可以从 ISE GUI 应用到授权策略中；可下载 ACL (DACL) 可从 ISE GUI 进行配置和管理，并应用到授权策略中。

要在 ISE 中将 DACL 实施到网络授权策略中，请执行以下操作：

1. 从以下位置配置新的或现有的DACL： **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **可下载 ACL (Downloadable ACLs)**。有关详细信息，请参阅为可下载 ACL 配置权限，第 15 页。
2. 从以下位置配置新的或现有的授权配置文件： **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权配置文件 (Authorization Profiles)**，在此期间使用您已配置的任何 DACL。
3. 从以下位置实施在创建和配置新的和现有策略集时配置的授权配置文件： **策略 (Policy)** > **策略集 (Policy Sets)**。

为可下载 ACL 配置权限

借助ISE，可在授权策略中配置和实施可下载ACL (DACL)，以控制不同用户和用户组访问网络的方式。默认授权 DACL 可在安装 ISE 后可用，包括以下默认配置文件：

- DENY_ALL_IPV4_TRAFFIC
- PERMIT_ALL_IPV4_TRAFFIC
- DENY_ALL_IPV6_TRAFFIC
- PERMIT_ALL_IPV6_TRAFFIC

使用 DACL 时，无法更改这些默认值，但可以复制它们以创建其他类似的 DACL。

配置所需的DACL 后，即可将这些DACL 应用于网络上的相关授权策略。将 DACL 应用于授权策略后，就无法再更改其类型或从 ISE 中将其删除。当已在策略中使用 DACL 后，为了更改其类型，可以创建一个重复 DACL，然后更新该重复项，或者，可以从策略中删除该 DACL 以将其更新，然后在相关情况下重新应用。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **可下载 ACL (Downloadable ACLs)**。

步骤 2 点击**可下载 ACL** 表顶部的**添加 (Add)**，或者，选择任何现有的 DACL，然后点击表顶部的**复制 (Duplicate)**。

步骤 3 输入或编辑所需的 DACL 值，牢记以下规则：

- 名称字段支持的字符为：字母数字、连字符 (-)、点号 (.) 和下划线 (_)
- 如下所述，在选择 DACL 类型时，系统会根据所选 IP 版本处理 IP 格式：
  - **IPv4** 仅验证 IPv4 合法 ACE。必须输入有效的 IPv4 格式。

- **IPv6** 仅验证 IPv6 合法 ACE。必须输入有效的 IPv6 格式。
- 从先前版本升级到 2.6 版本的 DACL 会在 **IP 版本 (IP Version)** 字段中显示**无关 (Agnostic)** 以作为 DACL 类型。输入所需的任何格式。使用**无关 (Agnostic)** 可为Cisco不支持的设备创建 DACL。当选择**无关 (Agnostic)** 时，不验证格式，并且您无法检查 DACL 语法。

- 关键字 **Any** 必须是 DACL 中所有 ACE 的源。DACL 推送之后，源中的 **Any** 会被替换为连接到交换机的客户端的 IP 地址。

当将 DACL 映射到任何授权配置文件时，

注释 **IP 版本(IP Version)** 字段不可编辑。在这种情况下，请从**授权配置文件 (Authorization Profiles)** 中删除 DACL 引用，编辑 IP 版本并在**授权配置文件 (Authorization Profiles)** 中重新映射 DACL。

步骤 4 或者，当完成创建完整的 ACE 列表后，点击**检查 DACL 语法 (Check DACL Syntax)** 以验证列表。如果存在验证错误，系统会在自动打开的窗口中显示特定的说明，指明无效的语法。

步骤 5 点击**提交 (Submit)**。

针对 Active Directory 用户授权的设备访问限制

Cisco ISE 包含计算机访问限制 (MAR) 组件，提供另外一种控制 Microsoft Active Directory 身份验证用户授权的方法。此授权形式基于访问Cisco ISE 网络所用的计算机的计算机身份验证。对于每个成功的计算机身份验证，Cisco ISE 会将在 RADIUS Calling-Station-ID 属性（属性 31）中收到的值缓存为成功计算机身份验证的证据。

在达到 Active Directory Settings 页面的“Time to Live”参数中配置的小时数之前，Cisco ISE 会保留缓存中的每个 Calling-Station-ID 属性值。参数过期之后，Cisco ISE 会从参数缓存中删除该参数。

当用户从最终用户客户端进行身份验证时，Cisco ISE 会在缓存中搜索在用户身份验证请求中收到的 Calling-Station-ID 值的成功计算机身份验证的 Calling-Station-ID 值。如果Cisco ISE 在缓存中找到匹配的用户身份验证 Calling-Station-ID 值，这会以如下方式影响Cisco ISE 为请求身份验证的用户分配权限：

- 如果在Cisco ISE 缓存中找到与 Calling-Station-ID 值相匹配的值，则会分配成功授权的授权配置文件。
- 如果在Cisco ISE 缓存中未找到与 Calling-Station-ID 值相匹配的值，则会分配成功用户身份验证（不含计算机身份验证）的授权配置文件。

配置授权策略和配置文件的指南

管理授权策略和配置文件时，请遵循以下规定：

- 您创建的规则名称必须仅使用以下支持的字符：
  - 符号：加号 (+)、连字符 (-)、下划线 (_)、句点 (.) 和空格 ( )。
  - 字母字符：A-Z 以及 a-z。

- 数字字符：0-9。

- 身份组默认为“Any”（您可以将此全局默认设置应用于所有用户）。
- 您可以通过条件设置一个或多个策略值。但是，条件是可选的，不一定要选择条件才能创建授权策略。以下是创建条件的两种方法：
  - 从供选择的相应字典选择现有条件或属性。
  - 创建允许您选择建议值或使用文本框来输入自定义值的自定义条件。
- 您创建的条件名称必须仅使用以下支持的字符：
  - 符号：连字符 (-)、下划线 (_) 和句点 (.)。
  - 字母字符：A-Z 以及 a-z。
  - 数字字符：0-9。
- 创建或编辑授权配置文件时，如果选择使用除**客户端调配（策略）(Client Provisioning [Policy])**以外的任何其他选项启用 **Web 重定向（CWA、MDM、NSP、CPP）(Web Redirection [CWA, MDM, NSP, CPP])**，则无法将 IPv6 地址配置为该授权策略的**静态 IP/主机名/FDQN**。这是因为集中式 Web 身份验证 (CWA)、移动设备管理 (MDM) 重定向和本机请求方协议 (NSP) 不支持 IPv6 静态 IP/主机名/ FQDN。
- 选择用于策略的授权配置文件时，权限非常重要。权限可以允许访问特定资源或允许您执行特定任务。例如，如果用户属于特定身份组（例如设备管理员组）并且用户符合所定义的条件（例如属于波士顿的某个站点），则此用户可以获得与该身份组关联的权限（例如访问特定网络资源或在设备上执行特定操作的权限）。
- 在授权条件中使用 **radius** 属性 **Tunnel-Private-Group-ID** 时，必须在使用 **EQUALS** 运算符时在条件中同时提及标签和值，例如：

```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

注释 从Cisco ISE 1.4 开始，ANC 取代了端点保护服务 (EPS)。ANC 提供额外的分类和性能改进。虽然在策略中使用 ERS 属性有时仍然适用于某些 ANC 操作，但应使用 ANC 属性。例如，**Session:EPSStatus=Quarantine** 可能会失败。在策略中使用 **Session:ANCPolicy** 作为条件。

配置授权策略

在从策略 (Policy) 菜单为授权策略创建属性和构建块后，从策略集 (Policy Sets) 菜单在策略集中创建授权策略。

开始之前

在开始此程序之前，您应该对用于创建授权策略（如身份组和条件）的不同构建块有基本的了解。

步骤 1 对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

步骤 2 从“视图”(View) 列中，点击 > 以访问所有策略集详细信息，并创建身份验证和授权策略以及策略例外。

步骤 3 点击页面“授权策略”(Authorization Policy) 部分旁的箭头图标以展开并查看授权策略表。

步骤 4 在**操作 (Actions)** 列中，点击齿轮图标。从下拉菜单中，根据需要选择任何插入或重复选项来插入新的授权策略规则。
授权策略表中将显示新行。

步骤 5 要设置策略的状态，请点击当前**状态 (Status)** 图标，然后从下拉列表中选择**状态 (Status)** 列中的必要状态。有关状态的详细信息，请参阅授权策略设置，第 20 页。

步骤 6 对于表中的任何策略，请点击**规则名称 (Rule Name)** 单元格，进行必要的自由文本更改，并创建唯一的规则名称。

步骤 7 要添加或更改条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击  。Conditions Studio 将打开。有关详细信息，请参阅策略条件，第 25 页。

不是您选择的所有属性都包含“等于”、“不等于”、“位于”、“不位于”、“匹配”、“开头为”或“开头非”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

注释 您必须使用“等于”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。如果是列表，“位于”运算符会检查列表中是否存在特定值。如果是单个字符串，“位于”运算符会检查字符串是否与“等于”运算符相同。

步骤 8 对于网络访问结果配置文件，请从**结果配置文件 (Results Profiles)** 下拉列表中选择相关授权配置文件，或者选择或点击 ✚，选择**创建新授权配置文件 (Create a New Authorization Profile)**，然后在**添加新标准配置文件 (Add New Standard Profile)** 屏幕打开时，执行以下步骤：

a) 根据需要输入值以配置新的授权配置文件。请注意以下事项：

- 名称字段中支持的字符包括：空格 ! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {。
- 对于**常见任务**，要输入DACL，请按如下所示选择相关的 **DACL 名称 (ACL Name)** 选项，然后从动态下拉列表中选择必要的 DACL：
  - 要使用 IPv4 DACL，请选中 **DACL 名称 (ACL Name)**。
  - 要输入 IPv6 DACL，请选中 **IPv6 DACL 名称 (IPv6 DACL Name)**。
  - 要输入任何其他 DACL 语法，请选中任一选项。无关 DACL 同时显示在 IPv4 和 IPv6 下拉列表中。

    注释 如果选择 **DACL名称 (DACL Name)**，则 AVP 类型适用于 IPv4（即使 DACL 本身是无关的）。如果为 **IPv6 DACL 名称 (IPv6 DACL Name)** 选择 DACL，则 AVP 类型适用于 IPv6（即使 DACL 本身是无关的）。

- **注释** 如果选择对策略使用ACL，请确保设备与此功能兼容。有关详细信息，请参阅《思科身份识别服务引擎兼容性指南》。

  对于**常见任务**，要输入 ACL，请如下所示选择相关 **ACL（过滤器 ID）(ACL (Filter-ID))** 选项，然后在字段中键入 ACL 名称：

  - 要使用 IPv4 ACL，请选中 **ACL（过滤器 ID）(ACL (Filter-ID))**。
  - 要输入 IPv6 ACL，请选中 **ACL IPv6（过滤器 ID）(ACL IPv6 (Filter-ID))**。

- 要对 Airespace 设备使用 ACL，请根据需要选中 **Airespace ACL 名称 (Airespace ACL Name)** 或 **Airespace IPv6 ACL 名称 (Airespace IPv6 ACL Name)**，然后在字段中键入 ACL 名称。
- 您可以从动态显示在屏幕底部的**属性详细信息 (Attributes Details)** 中仔细检查授权配置文件 RADIUS 语法。

b) 点击**保存 (Save)** 以将所做的更改保存到Cisco ISE 系统数据库，以便创建授权配置文件。

c) 要在策略集区域之外创建、管理、编辑和删除配置文件，请选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 9 对于网络访问结果安全组，请从**结果安全组 (Results Security Groups)** 下拉列表中选择相关安全组，或者点击 ➕，选择**创建新安全组 (Create a New Security Group)**，然后在“创建新安全组”(Create New Security Group) 屏幕打开时，执行以下步骤：

a) 为新安全组输入名称和说明（可选）。

b) 如果要将此 SGT 传播至 Cisco ACI，请选中**传播至 ACI (Propagate to ACI)** 复选框。只有当与此 SGT 相关的 SXP 映射属于在 Cisco ACI“设置”(Settings) 页面中选择的同一 VPN 时，它们才会传播至 Cisco ACI。

默认情况下该选项处于禁用状态。

c) 输入 Tag Value。标签值可以设置为手动输入或自动生成。您还可以为 SGT 保留范围。您可以从以下位置对其进行配置：“通用 TrustSec 设置”(General TrustSec Settings) 页面（**工作中心 (Work Centers)** > **TrustSec** > **设置 (Settings)** > **通用 TrustSec 设置 (General TrustSec Settings)**）。

d) 点击**提交 (Submit)**。

有关详细信息，请参阅 安全组配置，第 111 页。

步骤 10 对于 TACACS+ 结果，请从**结果 (Results)** 下拉列表中选择相关命令集和外壳配置文件，或者点击**命令集 (Command Sets)**或**外壳配置文件 (Shell Profiles)** 列中的 ➕，分别打开**添加命令 (Add Commands)** 屏幕或**添加外壳配置文件 (Add Shell Profile)**。选择**创建新命令集 (Create a New Command Set)** 或**创建新外壳配置文件 (Create a New Shell Profile)**，然后输入字段。

步骤 11 在表中组织用来检查和匹配策略的顺序。

步骤 12 点击**保存 (Save)** 保存您对Cisco ISE 系统数据库所做的更改，并创建这条新的授权策略。

授权策略设置

下表介绍**策略集 (Policy Sets)** 窗口的**身份验证策略 (Authentication Policy)** 部分中的字段，由此窗口可将身份验证子策略配置为策略集的一部分。对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。从“策略集”(Policy Sets) 页面，选择 **查看 (View)** > **授权策略 (Authorization Policy)**。

表 *3:* 身份验证策略配置设置

字段名称	使用指南
状态	选择此策略的状态。它可以是下列选项之一： • **已启用 (Enabled)**：此策略条件处于活动状态。 • **已禁用 (Disabled)**：此策略条件处于非活动状态，不会被评估。 • **仅监控 (Monitor Only)**：将评估此策略条件，但不实施结果。您可以在 Live Log 身份验证页面查看此策略条件的结果。在此情况下，查看详细报告，了解受监控的步骤和属性。例如，您可能想要添加新策略条件，但不确定此条件是否为您提供正确的结果。在此情况下，您可以在监控模式下创建策略条件来查看结果，如果您对结果满意，可以启用此选项。
规则名称	为此策略输入一个唯一的名称。
条件	在新策略行中，点击加号 (+) 图标，或者在现有策略行中，点击“编辑”(Edit) 图标以打开 Condition Studio。
结果或配置文件	选择相关授权配置文件，该配置文件用于确定为配置的安全组提供的不同权限级别。如果尚未配置相关授权配置文件，可以内联配置。
结果或安全组	选择相关安全组，该安全组用于确定与特定规则相关的用户组。如果尚未配置相关安全组，则可以内联配置。
结果或命令集	命令集实施可由设备管理员执行的指定命令列表。当设备管理员在网络设备上发出操作命令时，查询 ISE 确定管理员是否被授权发出这些命令。这也称为命令授权。

字段名称	使用指南
结果或外壳配置文件	TACACS+ 外壳配置文件控制设备管理员的初始登录会话。
点击数	命中数是一种诊断工具，用于指示条件匹配的次数。
操作	点击“操作”(Actions) 列中的齿轮图标 ，查看并选择不同的操作： • 在上方插入新行 (Insert new row above)：在打开“操作”(Actions) 菜单的规则上方插入新的授权规则。 • 在下方插入新行 (Insert new row below)：在打开“操作”(Actions) 菜单的规则下方插入新的授权规则。 • 在上方复制 (Duplicate above)：在打开“操作”(Actions) 菜单的规则上方，插入重复授权规则，高于原集合。 • 在下方复制 (Duplicate below)：在打开“操作”(Actions) 菜单的规则下方，插入重复授权规则，低于原集合。 • 删除 (Delete)：删除规则。

授权配置文件设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 ( )，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**，**授权配置文件 (Authorization Profiles)** 窗口定义网络访问属性。

授权配置文件设置

- **名称 (Name)**：输入此新授权配置文件的名称。
- **说明**：输入此授权配置文件的说明。
- **访问类型 (Access Type)**：选择访问类型：**ACCESS_ACCEPT** 或 **ACCESS_REJECT**。
- **服务模板 (Service Template)**：启用此选项以支持与有 SAnet 功能的设备的会话。Cisco ISE 在授权配置文件中实施服务模板，用一个特殊标志将其标记为兼容服务模板 *(Service Template)*。由于服务模板也是授权配置文件，因此它充当支持 SAnet 和非 SAnet 设备的单个策略。
- **跟踪移动 (Track Movement)**：启用此选项可通过Cisco移动服务引擎 (MSE) 跟踪用户位置。

注释 此选项可能会影响思科 ISE 性能，仅适用于高安全性位置。

- **被动身份跟踪 (Passive Identity Tracking)**：启用此选项可将被动身份的 Easy Connect 功能来实施策略和跟踪用户。

常见任务

常见任务是适用于网络访问的特定权限和操作。

- **DACL 名称 (DACL Name)**：启用此选项可使用可下载的 ACL。您可以使用默认值（**PERMIT_ALL_IPV4_TRAFFIC**、**PERMIT_ALL_IPV6_TRAFFIC**、**DENY_ALL_IPV4_TRAFFIC**、**DENY_ALL_IPV6_TRAFFIC**）或从以下字典中选择属性：
  - 外部身份库（属性）
  - 终端
  - 内部用户
  - 内部终端

  有关添加 DACL 或编辑和管理现有 DACL 的详细信息，请参阅可下载 ACL，第 15 页。
- **ACL (Filter-ID)**：启用此选项可配置 RADIUS filter-ID 属性。filter-ID 指定 NAD 上的 ACL。定义 filter-ID 时，Cisco ISE 会在文件名后附加“.in”。Filter-ID 显示在**属性详细信息 (Attributes Details)** 窗格中。**ACL IPv6 (Filter-ID)** 的工作方式与 NAD 的 IPv6 连接相同。
- **安全组 (Security Group)**：启用此选项可分配授权的安全组 (SGT) 部分。
  - 如果Cisco ISE 未与 Cisco DNA Center 集成，则Cisco ISE 会分配 VLAN ID 1。
  - 如果Cisco ISE 与 Cisco DNA Center 集成，则选择 Cisco DNA Center 与Cisco ISE 共享的虚拟网络 (VN)，选择**数据类型 (Data Type)** 和子网/地址池。

注释 一个安全组任务包括一个安全组和一个 VN。如果配置安全组，则无法配置 VLAN。终端设备只能分配给一个虚拟网络。

- **VLAN**：启用此选项可指定虚拟 LAN (VLAN) ID。您可以为 VLAN ID 输入整数或字符串值。此条目的格式为 `Tunnel-Private-Group-ID:VLANnumber`。
- **语音域权限 (Voice Domain Permission)**：启用此选项可使用可下载的 ACL。供应商专用属性 (VSA) `cisco-av-pair` 与值 `device-traffic-class=voice` 相关联。在多域授权模式下，如果网络交换机收到此 VSA，则授权后终端将连接到语音域。
- **Web 重定向（CWA、DRW、MDM、NSP、CPP）(Web Redirection (CWA, DRW, MDM, NSP, CPP))**：启用此选项可在身份验证后启用 Web 重定向。

- 选择重定向类型。您选择的 Web 重定向类型会显示其他选项，如下所述。
- 输入 ACL 以支持让Cisco ISE 发送到 NAD 的重定向。

  您输入的发送到 NAD 的 ACL 在**属性详细信息 (Attributes Details)** 窗格中显示为 cisco-av pair。例如，输入 **acl119**，它会在**属性详细信息 (Attributes Details)** 窗格中显示为：`cisco-av-pair = url-redirect-acl = acl119`。
- 选择所选 Web 重定向类型的其他设置。

选择以下 Web 重定向类型之一：

- **集中式 Web 身份验证 (Centralized Web Auth)**：重定向到您从**值 (Value)** 下拉列表中选择的门户。
- **客户端调配（安全评估）(Client Provisioning (Posture))**：重定向到您从**值 (Value)** 下拉列表中选择的客户端调配门户，以在客户端上启用安全评估。
- **热点：重定向 (Hot Spot: Redirect)**：重定向到您从**值 (Value)** 下拉列表中选择的热点门户。
- **MDM 重定向 (MDM Redirect)**：重定向到您指定的 MDM 服务器上的 MDM 门户。
- **本地请求方调配 (Native Supplicant Provisioning)**：重定向到您从**值 (Value)** 下拉列表中选择的 BYOD 门户。

在选择 Web 重定向类型并输入所需参数后，配置以下选项：

- **显示证书续约消息 (Display Certificates Renewal Message)**：启用此选项可显示证书续约消息。URL-redirect 属性值改变并且包含证书有效的天数。此选项仅适用于集中式 Web 身份验证重定向。
- **静态 IP/主机名/FQDN (Static IP/Host Name/FQDN)**：启用此选项可将用户重定向到其他 PSN。输入目标 IP 地址、主机名或 FQDN。如果不配置此选项，用户将重定向到收到此请求的策略服务节点的 FQDN。
- **在逻辑配置文件中抑制终端的分析器 CoA (Suppress Profiler CoA for endpoints in Logical Profile)**：启用此选项可取消特定类型终端设备的重定向。

- **自动智能端口 (Auto SmartPort)**：启用此选项可使用自动智能端口功能。输入事件名称，它会创建一个 VSA cisco-av-pair，该值为 `auto-smart-port=event_name`。此值显示在**属性详细信息 (Attributes Details)** 窗格中。
- **访问漏洞 (Access Vulnerabilities)**：启用此选项可作为授权的一部分在此终端上运行以威胁防护为中心的 NAC 漏洞评估。选择适配器以及运行扫描的时间。
- **重新验证身份 (Reauthentication)**：启用此选项可在重新验证身份期间保持终端连接。通过选择使用 **RADIUS-Request** (1)，选择在重新验证身份的过程中保持连接。默认 RADIUS-Request (0) 会断开现有会话。您还可以设置非活动计时器。
- **MACSec 策略**：启用此选项可在启用 MACSec 的客户端连接到Cisco ISE 时使用 MACSec 加密策略。选择以下选项之一：**must-secure**、**should-secure** 或 **must-not-secure**。您的设置在**属性详细信息 (Attributes Details)** 窗格中显示为：`cisco-av-pair = linksec-policy=must-secure`。

- **NEAT**：启用此选项可使用网络边缘接入拓扑 (NEAT)，它能在网络之间扩展身份识别。如果选中此复选框，**属性详细信息 (Attributes Details)** 窗格中将显示 `cisco-av-pair = device-traffic-class=switch`。
- **Web 身份验证（本地 Web 身份验证）(Web Authentication (Local Web Auth))**：启用此选项可对此授权配置文件使用本地 Web 身份验证。通过由Cisco ISE 发送 VSA 以及 DACL，此值使交换机能够识别用于 Web 身份验证的授权。VSA 为 `cisco-av-pair = priv-lvl=15`，显示在**属性详细信息 (Attributes Details)** 窗格中。
- **Airespace ACL名称 (Airespace ACL Name)**：启用此选项可向Cisco Airespace 无线控制器发送 ACL 名称。Airespace VSA 使用此 ACL 向 WLC 上的连接授权本地定义的 ACL。例如，输入 **rsa-1188**，它会在**属性详细信息 (Attributes Details)**窗格中显示为 `Airespace-ACL-Name = rsa-1188`。
- **ASA VPN**：选中此选项可分配自适应安全设备 (ASA) VPN 组策略。从下拉列表中选择一个 VPN 组策略。
- **AVC 配置文件名称 (AVC Profile Name)**：启用此选项可在此终端上运行应用可视性。输入要使用的 AVC 配置文件。
- **UPN 查找 (UPN Lookup)**：待定

高级属性设置

- **目录 (Dictionaries)**：点击向下箭头图标可查看**目录 (Dictionaries)** 窗口中的可用选项。在第一个字段中选择应配置的字典和属性。
- **属性值 (Attribute Values)**：点击向下箭头图标可显示**属性值 (Attribute Values)** 窗口中的可用选项。选择所需的属性组和属性值。此值与第一个字段中选择的值匹配。您配置的任何**高级属性 (Advanced Attributes)** 设置都将显示在**属性详细信息 (Attributes Details)** 面板中。

  注释 字符 % 不能在**高级属性设置 (Advanced Attributes Settings)** 窗格中的**属性值 (Attribute Values)** 字段中使用。

- **属性详细信息 (Attributes Details)**：此窗格显示您为**常见任务 (Common Tasks)** 和**高级属性 (Advanced Attributes)** 设置的已配置属性值。

  属性详细信息 (Attributes Details) 窗格中显示的值是只读的。

  注释 要修改或删除**属性详细信息 (Attributes Details)** 窗格中显示的任何只读值，请在对应的**常见任务 (Common Tasks)** 字段中或在**高级属性设置 (Advanced Attributes Settings)** 窗格的**属性值 (Attribute Values)** 字段中选择的属性中修改或删除这些值。

相关主题

思科 ISE 授权配置文件，第 12 页
授权配置文件的权限，第 12 页
配置用于重定向未注册设备的授权配置文件
创建授权配置文件

授权策略例外

在每个策略集中，您可以定义常规授权策略，以及本地例外规则（从每个策略集的“集”(Set) 视图中的“授权策略本地例外”(Authorization Policy Local Exceptions) 部分定义）和全局例外规则（从每个策略集的“集”(Set) 视图中的“授权策略全局例外”(Authorization Policy Global Exceptions) 部分定义）。

使用全局授权例外策略，可以定义覆盖所有策略集中所有授权规则的规则。配置全局授权例外策略后，系统会将其添加到所有策略集。然后，可以从任何当前配置的策略集中更新全局授权例外策略。每次更新全局授权例外策略时，这些更新都会应用于所有策略集。

本地授权例外规则会覆盖全局例外规则。系统按以下顺序处理授权规则：首先处理本地例外规则，然后处理全局例外规则，最后处理授权策略常规规则。

授权例外策略规则的配置与授权策略规则相同。要配置例外策略，请参阅上述有关配置常规授权策略的说明：配置授权策略，第 17 页

本地和全局例外配置设置

对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。从**策略集 (Policy Sets)** 窗口中，选择 **查看 (View)** > **本地例外策略 (Local Exceptions Policy)** 或**全局例外策略 (Global Exceptions Policy)**。

授权例外设置与授权策略设置相同，如授权策略设置，第 20 页所述。

策略条件

Cisco ISE 使用基于规则的策略提供网络访问。策略是一组规则和结果，其中规则由条件组成。Cisco ISE 可以让您将条件创建为可在系统库中存储的单个策略元素，然后从 Conditions Studio 重复用于其他基于规则的策略。

条件可以很简单，或者，必要时可以使用运算符（等于、不等于、大于，等等）和值，或者通过包含多个属性、运算符和复杂层次结构，使之变得复杂。在运行时，Cisco ISE 会评估策略条件，然后根据策略评估返回的 true 值或 false 值，应用您所定义的结果。

在创建条件并为其分配唯一名称后，可以从 Conditions Studio 库中选择该条件，多次将其重复用于各种规则和策略，例如：

```
Network Conditions.MyNetworkCondition EQUALS true
```

不能从 Condition Studio 中删除策略中使用的条件或作为其他条件组成部分的条件。

每个条件各自定义可包括在策略条件中的对象列表，从而得到与请求中的定义匹配的一组定义。

您可以使用运算符 `EQUALS true` 来检查网络条件是否为 true（无论请求中存在的值是否与网络条件中的至少一个条目匹配）或 `EQUALS false`，以测试网络条件是否为 false（不匹配网络条件中的任何条目）。

CiscoISE还提供预定义的智能条件，您可以在策略中单独使用这些条件，也可以将其作为您自己的自定义条件中的构建块，并且可以根据需要进行更新和更改。

您可以创建以下唯一网络条件以限制对网络的访问：

- 终端站网络条件 - 基于发起和终止连接的终端站。

  Cisco ISE 会评估远程地址 TO 字段（根据它是 TACACS+ 还是 RADIUS 请求而获取），确定它是终端的 IP 地址、MAC 地址、主叫线路标识 (CLI) 还是被叫号码识别服务 (DNIS)。

  在 RADIUS 请求中，标识符在属性 31 (Calling-Station-Id) 中可用。

  在 TACACS+ 请求中，如果远程地址包含斜杠 (/)，则斜杠前的部分作为 FROM 值，斜杠后的部分作为 TO 值。例如，如果请求具有 CLI/DNIS，则 CLI 作为 FROM 值，DNIS 作为 TO 值。如果不包含斜杠，则整个远程地址作为 FROM 值（不论是 IP 地址、MAC 地址或 CLI）。

- 设备网络条件 - 基于处理请求的 AAA 客户端。

  可通过 IP 地址、在网络设备存储库中定义的设备名称或网络设备组确定网络设备。

  在 RADIUS 请求中，如果存在属性 4 (NAS-IP-Address)，Cisco ISE 会从该属性中获取 IP 地址。如果存在属性 32 (NAS-Identifier)，Cisco ISE 将从属性 32 获取 IP 地址。如果未找到这些属性，它将从其接收的数据包获取 IP 地址。

  设备字典（NDG 字典）包含网络设备组属性，如位置、设备类型或其他动态创建的表示 NDG 的属性。反过来，这些属性包含与当前设备相关的组。

- 设备端口网络条件 - 基于设备的 IP 地址、名称、NDG 和端口（终端站连接到的设备物理端口）。

  在 RADIUS 请求中，如果请求中存在属性 5 (NAS-Port)，则Cisco ISE 会从该属性中获取值。如果请求中存在属性 87 (NAS-Port-Id)，Cisco ISE 将从属性 87 获取请求。

  在 TACACS+ 请求中，Cisco ISE 会从（每个阶段的）起始请求的端口字段中获取此标识符。

有关这些独特条件的详细信息，请参阅特殊网络访问条件 ，第 44 页。

字典和字典属性

字典是关于可用于为域定义访问策略的属性和允许值的域特定目录。单个字典是同种属性类型的集合。字典中定义的属性具有相同的属性类型并且其类型会指明特定属性的来源或上下文。

属性类型可以是以下一种类型：

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

除了属性和允许的值之外，字典还包含关于名称与说明、数据类型和默认值等属性的信息。一个属性可以有以下一种数据类型：BOOLEAN、FLOAT、INTEGER、IPv4、IPv6、OCTET_STRING、STRING、UNIT32 和 UNIT64。

Cisco ISE 在安装时会创建系统字典并且允许您创建用户字典。

属性存储在不同的系统词典中。属性用于配置条件。属性可以在多个条件中重复使用。

要在创建策略条件时重复使用某个有效的属性，请从包含支持的属性的词典中选择该属性。例如，Cisco ISE 提供名为 AuthenticationIdentityStore 的属性，该属性位于 Networkaccess 目录中。该属性识别验证用户身份期间访问的最后一个身份源：

- 在身份验证期间使用单个身份源时，该属性包括成功进行身份验证所在的身份库的名称。
- 在身份验证期间使用某个身份源序列时，该属性包括访问的最后一个身份源的名称。

您可以将 AuthenticationStatus 属性与 AuthenticationIdentityStore 属性组合使用，以定义用来识别成功验证某个用户的身份的身份源的条件。例如，要使用授权策略中的 LDAP 目录 (LDAP13) 检查用户通过身份验证的条件，您可以定义下列可重复使用的条件：

```
 If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

注释 AuthenticationIdentityStore 表示允许您输入条件数据的文本字段。确保向该字段中正确输入或复制名称。如果身份源的名称发生更改，您必须确保修改此条件，以与身份源的更改保持一致。

要定义基于之前已进行身份验证的终端身份组的条件，Cisco ISE 支持在终端身份组 802.1X 身份验证状态期间定义的授权。当Cisco ISE 执行 802.1X 身份验证时，它从 RADIUS 请求的“Calling-Station-ID”字段中提取 MAC 地址，并使用该值查找和填充设备终端身份组（被定义为 endpointIDgroup 属性）的会话缓存。此过程使 endpointIDgroup 属性在创建授权策略条件时可供使用，并且允许您根据使用该属性的终端身份组信息（用户信息除外）来定义授权策略。

可以在授权策略配置页面的 ID Groups 列中定义终端身份组的条件。需要在授权策略的“Other Conditions”部分中定义基于用户相关信息的条件。如果用户信息基于内部用户属性，请使用内部用户目录中的 ID 组属性。例如，您可以使用诸如“User Identity Group:Employee:US”等值，在身份组中输入完整的值路径。

支持的网络访问策略词典

Cisco ISE 支持以下系统存储的词典，这些词典包含为身份验证和授权策略构建条件和规则时所需的不同属性：

- 系统定义的字典
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS 供应商字典

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- Network access

对于授权策略类型，条件中配置的验证必须符合要返回的授权配置文件。

验证通常包括一个或更多条件，条件中包含用户定义的名称，可以将这些条件添加到库中并供其他策略重复使用。

以下部分介绍可用于配置条件的受支持属性和词典。

字典支持的属性

此表列出字典支持的固定属性，这些属性可用于策略条件中。并非所有这些属性都可用于创建所有类型的条件。

例如，创建在身份验证策略中选取访问服务的条件时，您将只看到以下网络访问属性：Device IP Address、ISE Host Name、Network Device Name、Protocol 和 Use Case。

您可以将下表中列出的属性用于策略条件中。

字典	属性	允许的协议规则和代理	身份规则
设备	Device Type（预定义的网络设备组）	支持	支持
	Device Location（预定义的网络设备组）		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	所有属性	支持	支持

字典	属性	允许的协议规则和代理	身份规则
网络接入	ISE Host Name	支持	支持
	AuthenticationMethod	不支持	支持
	AuthenticationStatus	否	否
	CTSDeviceID	否	否
	Device IP Address	支持	支持
	EapAuthentication（设备用户身份验证期间使用的 EAP 方法）	不支持	支持
	EapTunnel（用于建立隧道的 EAP 方法）	不支持	支持
	Protocol	支持	支持
	UseCase	支持	支持
	UserName	不支持	支持
	WasMachineAuthenticated	否	否

字典	属性	允许的协议规则和代理	身份规则
Certificate	Common Name	不支持	支持
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

系统定义的字典和字典属性

Cisco ISE 会在安装期间创建系统字典，您可以在 System Dictionaries 页面找到这些系统字典。系统定义的字典属性为只读属性。由于其性质，您只能查看现有的系统定义的字典。您不能创建、编辑或删除系统定义的值或系统字典中的任何属性。

所显示的系统定义的字典属性会带有属性的描述性名称、域识别的内部名称和允许的值。

IETF RADIUS 属性集也是系统定义的字典的一部分，由互联网工程任务组 (IETF) 定义，Cisco ISE 也会为此属性集创建字典默认设置。您可以编辑除 ID 之外的所有 IETF RADIUS 自由属性字段。

显示系统字典和字典属性

您无法创建、编辑或删除系统字典中的任何系统定义的属性。您只能查看系统定义的属性。您可以执行基于字典名称和说明的快速搜索或基于您所定义的搜索规则的高级搜索。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **系统 (System)**。

步骤 2 在 System Dictionaries页面上选择系统字典，然后点击 **View**。

步骤 3 点击 **Dictionary Attributes**。

步骤 4 从列表中选择系统字典属性，然后点击 **View**。

步骤 5 点击 **Dictionaries** 链接以返回 System Dictionaries 页面。

用户定义的字典和字典属性

Cisco ISE 显示您在 User Dictionaries 页面中创建的用户定义字典。在系统中创建并保存现有用户字典的 Dictionary Name 或 Dictionary Type 值后，将不能修改这些值。

您可以在 User Dictionaries 页面执行以下操作：

- 编辑和删除用户字典。
- 根据名称和说明搜索用户字典。
- 添加、编辑和删除用户字典中的用户定义的字典属性。
- 使用 NMAP 扫描操作删除 NMAP 扩展名字典中的属性。当在“NMAP 扫描操作”(NMAP Scan Actions) 页面中添加或删除自定义端口时，将在字典中添加、删除或更新对应的自定义端口属性。
- 添加或删除允许的字典属性值

创建用户定义的字典

您可以创建、编辑或删除用户定义的字典。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **用户 (User)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为用户字典输入名称、可选说明和用户字典版本。

步骤 4 从 Dictionary Attribute Type 下拉列表选择属性类型。

步骤 5 点击**提交 (Submit)**。

创建用户定义的字典属性

您可以在用户字典中添加、编辑和删除用户定义的字典属性以及添加或删除用于字典属性的允许值。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **用户 (User)**。

步骤 2 从 User Dictionaries 页面选择用户字典，然后点击**编辑 (Edit)**。

步骤 3 点击 **Dictionary Attributes**。

步骤 4 点击**添加 (Add)**。

步骤 5 为字典属性输入属性名称、可选说明和内部名称。

步骤 6 从 Data Type 下拉列表选择数据类型。

步骤 7 点击**添加 (Add)** 以配置名称、允许值，并在 Allowed Values 表中设置默认状态。

步骤 8 点击**提交 (Submit)**。

RADIUS 供应商字典

Cisco ISE 允许您定义一套 RADIUS 供应商字典并且为每个字典定义一系列属性。列表中的每个供应商定义都包含供应商名称、供应商 ID 和扼要说明。

默认情况下，Cisco ISE 为您提供以下 RADIUS 供应商字典：

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUS 协议支持这些供应商字典以及可用于授权策略和策略条件的供应商特定属性。

创建 RADIUS 供应商字典

还可以创建、编辑、删除、导出和导入 RADIUS 供应商字典。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)** > **系统 (System)** > **Radius** > **Radius 供应商 (Radius Vendors)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入 RADIUS 供应商字典的名称、可选说明，以及由互连网号码分配机构 (IANA) 批准的 RADIUS 供应商的供应商 ID。

步骤 4 从 Vendor Attribute Type Field Length 下拉列表中选择从属性值提取用于指定属性类型的字节数。有效值为 1、2 和 4。默认值为 1。

步骤 5 从 Vendor Attribute Size Field Length 下拉列表中选择从属性值提取用于指定属性长度的字节数。有效值为 0 和 1。默认值为 1。

步骤 6 点击**提交 (Submit)**。

创建 RADIUS 供应商字典属性

您可以创建、编辑和删除Cisco ISE 支持的 RADIUS 供应商属性。每个 RADIUS 供应商属性都有名称、数据类型、说明和方向，其指定属性是否仅与请求相关、仅与响应相关，还是与二者都相关。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)** > **系统 (System)** > **Radius** > **Radius 供应商 (Radius Vendors)**。

步骤 2 从 RADIUS 供应商字典列表选择 RADIUS 供应商字典，然后点击**编辑 (Edit)**。

步骤 3 点击**字典属性 (Dictionary Attributes)**，然后点击**添加 (Add)**。

步骤 4 为 RADIUS 供应商属性输入属性名称和可选说明。

步骤 5 从 Data Type 下拉列表选择数据类型。

步骤 6 选中 **启用MAC选项 (Enable MAC option)** 复选框。

步骤 7 从 Direction 下拉列表选择仅应用于 RADIUS 请求、仅应用于 RADIUS 响应或同时应用于二者的方向。

步骤 8 在 ID 字段输入供应商属性 ID。

步骤 9 选中 **允许标记 (Allow Tagging)** 复选框。

步骤 10 选中 **允许配置文件中存在该属性的多个实例 (Allow Multiple Instances of this Attribute in a Profile)** 复选框。

步骤 11 点击**添加 (Add)** 以在“允许的值”(Allowed Values) 表中为供应商属性添加允许的值。

步骤 12 点击**提交 (Submit)**。

HP RADIUS IETF 服务类型属性

Cisco ISE 为 RADIUS IETF 服务类型属性引入两个新值。此 RADIUS IETF 服务类型属性位于**策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > RADIUS > IETF**在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > RADIUS > IETF**。您可在策略条件中使用这两个值。这两个值专为 HP 设备设计，用于了解用户的权限。

列举名称	列举值
HP-Oper	252
HP-User	255

RADIUS 供应商字典属性设置

本节介绍Cisco ISE 中使用的 RADIUS 供应商字典。

下表介绍了 RADIUS 供应商的“字典”(Dictionary) 窗口中的字段，可以通过此窗口为 RADIUS 供应商配置字典属性。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **系统 (System)** > **RADIUS** > **RADIUS 供应商 (RADIUS Vendors)**。

表 *4: RADIUS* 供应商字典属性设置

字段名称	使用指南
属性名称	输入选定 RADIUS 供应商的供应商特定属性名称。
说明	输入供应商特定属性的可选说明。
内部名称	输入数据库内部所称呼的供应商特定属性的名称。
数据类型	为供应商特定属性选择以下其中一种数据类型： • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPv6

字段名称	使用指南
启用MAC选项	选中此复选框可启用将RADIUS属性比作为MAC地址。默认情况下，对于 RADIUS 属性 calling-station-id，此选项标记为启用，您无法禁用此选项。对于 RADIUS 供应商字典中的其他（字符串类型）字典属性，可以启用或禁用此选项。 启用此选项之后，在设置身份验证和授权条件时，可以通过选择Text选项来定义对比是否是明文字符串，或通过选择 MAC address 选项来定义是否是 MAC 地址。
方向	选择一个适用于 RADIUS 消息的选项：
ID	输入供应商属性 ID。有效范围为 0 至 255。
允许标记	根据RFC2868定义，选中该复选框，将属性标记为已被允许带有标签。该标签旨在允许将已建立隧道的用户的属性进行分组。有关详细信息，请参阅 RFC2868。 已标记的属性支持确保有关指定隧道的所有属性在各自的标签字段中包含相同值，并且，每组包含一个 Tunnel-Preference 属性实例。这符合将用于多供应商网络环境中的隧道属性，以此消除不同供应商生产的网络接入服务器 (NAS) 之间的互通性问题。
允许配置文件中存在该属性的多个实例	当希望配置文件中存在此RADIUS供应商特定属性的多个实例时，请选中此复选框。

相关主题

系统定义的字典和字典属性，第 31 页
用户定义的字典和字典属性，第 31 页
RADIUS 供应商字典，第 32 页
创建 RADIUS 供应商字典，第 32 页

浏览 Conditions Studio

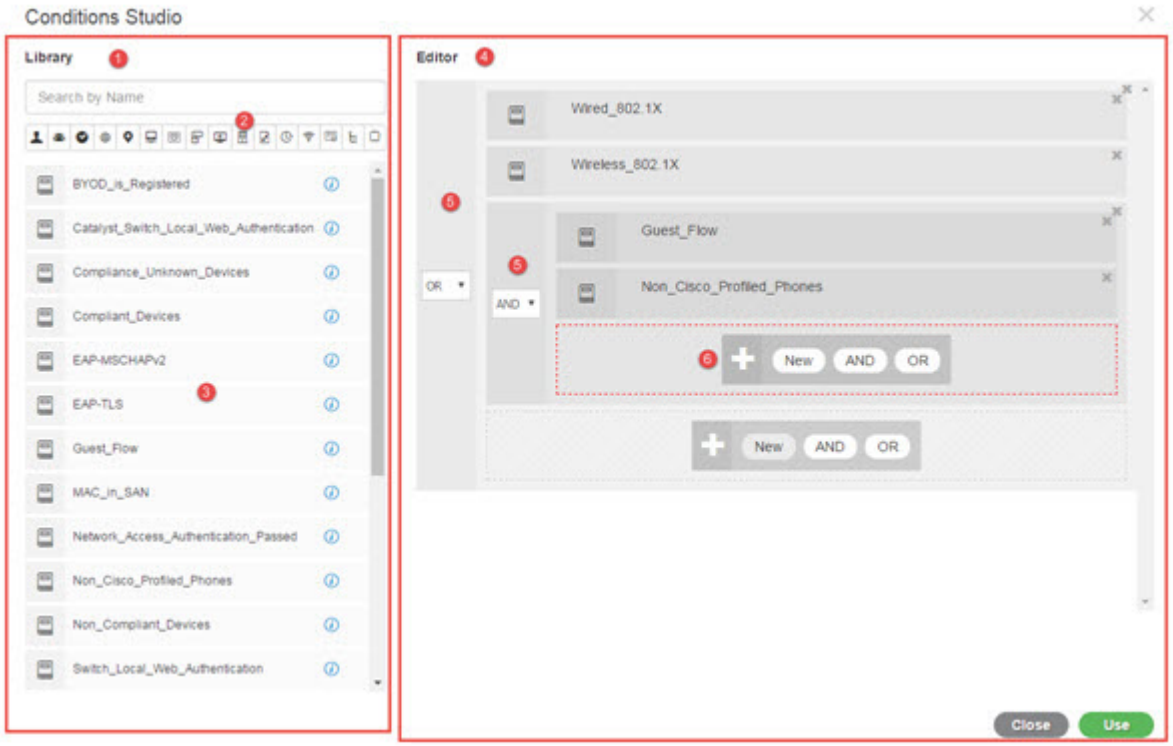
使用 Conditions Studio 创建、管理和重复使用条件。条件可以包括多个规则，并且结构复杂性不限（包括仅一个级别或多个层级）。使用 Conditions Studio 创建新条件时，可以使用已存储在库中的条件块，也可以更新和更改这些存储的条件块。在稍后创建和管理条件时，可以使用快速类别过滤器等轻松查找需要的块和属性。

对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

要编辑或更改已应用于任何策略集中的特定规则的条件，请将鼠标悬停在**条件 (Conditions)** 列中的单元格上，然后点击，或者从策略集表中的**条件 (Conditions)** 列点击加号 以创建新列，随后可以立即将其应用于同一策略集，也可以将其保存在库中以供将来使用。

下图显示 Conditions Studio 的主要元素。

图 *2: Conditions Studio*



Condition Studio 分为两个主要部分：库和编辑器。库可以存储条件块以供重复使用，而编辑器可以让您编辑这些已保存的块和创建新的块。

下表介绍了 Condition Studio 的不同部分：

字段	使用指南
库	显示已创建并保存在 ISE 数据库中以供重复使用的所有条件块的列表。若要在当前编辑的条件中使用这些条件块，请将其从库中拖放到编辑器中的相关级别，必要时更新运算符。 存储在库中的条件全部用库图标  表示，原因是条件可以与多个类别相关联。 在库中的每个条件旁，也可以找到该图标。将鼠标悬停在此图标上可查看条件的完整说明，查看其关联的类别，还可以从库中彻底删除条件。如果条件被策略使用，则无法删除这些条件。 将任何库条件拖放到编辑器中，以便将其单独用于当前编辑的策略，或作为更复杂条件的构建块，以便在当前策略中使用或在库中另存为新条件。您还可以在编辑器中拖放条件，以便对该条件进行更改，然后在库中以相同名称或新名称保存该条件。 安装后还有预定义条件。这些条件也可以更改和删除。
搜索和过滤	按名称搜索条件或按类别过滤条件。以类似的方式，还可以从编辑器中的**点击以添加属性 (Click to add an attribute)** 字段搜索和过滤属性。工具栏上的图标代表不同的属性类别，如主题、地址等。点击图标可查看与特定类别相关的属性，而点击类别工具栏中的突出显示图标可取消选择该类别，从而删除过滤器。
条件列表	库中所有条件的完整列表，或库中基于搜索或过滤结果而显示的条件列表。
编辑人	创建要立即使用的新条件，以及要保存在系统库中以供将来使用的新条件，然后编辑现有条件并将这些更改保存在库中以供立即使用和将来使用。 当打开 Conditions Studio 以创建新条件时（点击任意策略集表中的加号），会显示只包含一个空行的编辑器，您可以在其中添加第一个规则。 当编辑器打开并显示空字段时，不会显示任何运算符图标

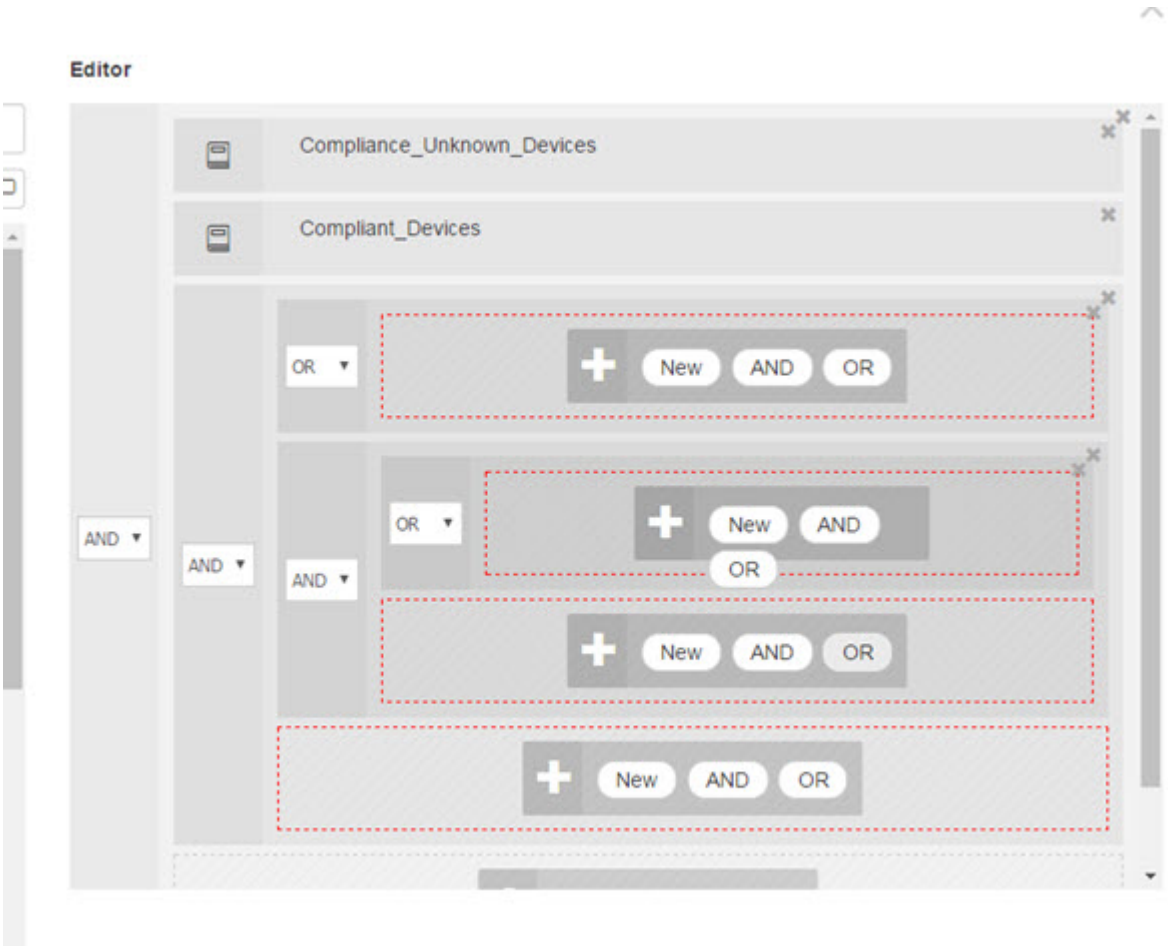
字段	使用指南
	编辑器分为不同的虚拟列和行。 列表示不同的层次结构级别，每列根据其在层次结构中的位置缩进；行代表单个规则。您可以为每个级别创建单个或多个规则，并且可以包含多个级别。 上图中的示例显示了正在构建或编辑的条件，包括规则层次结构，图中的第一级和第二级均标有数字 5。顶级父级别的规则使用运算符 OR。 要在选择运算符并创建层次结构级别后更改该运算符，只需从此列中显示的下拉列表中选择相关选项。 除了运算符下拉列表之外，每个规则在此列中都有一个相关图标，指示其所属的类别。如果将鼠标悬停在图标上，工具提示会指示类别的名称。 一旦保存到库中，系统将为所有条件块分配库图标，替换编辑器中显示的类别图标。 最后，如果将规则配置为**排除**所有相关的匹配项目，则此列中也会显示“不是”(Is-Not) 标志。例如，如果将值为 London 的位置属性设置为“不是”(Is-Not)，则来自伦敦的所有设备都将被拒绝访问。

字段	使用指南
	此区域显示使用层次结构级别以及同一条件中的多个规则时可用的选项。 当将鼠标悬停在任何列或行上时，会显示相关操作。选择操作时，该操作会应用于该部分和所有子部分。例如，当层次结构 A 中有五个级别时，如果从第三级中的任何规则中选择“和”(AND)，则会在原规则下创建新的层次结构 B，以便原规则成为层次结构 B 的父规则，嵌入在层次结构 A 中。 当首次打开 Condition Studio 以从头创建新条件时，编辑器区域仅包含一行（用于您可配置的单个规则），以及用于选择相关运算符或从库中拖放相关条件的选项。 使用**和 (AND)** 和**或 (OR)** 运算符选项可以向条件中添加其他级别。选择**新建 (New)**，可在点击选项的同一级别创建新规则。只有在层次结构的顶层配置至少一个规则后，**新建 (New)** 选项才会显示。

配置、编辑和管理策略条件

使用 Conditions Studio 创建、管理和重复使用条件。条件可以包括多个规则，并且结构复杂性不限（包括仅一个级别或多个层级）。从 Conditions Studio 的编辑器侧管理条件层次结构，如下图所示：

图 *3:* 编辑器 - 条件层次结构



创建新条件时，可以使用已存储在库中的条件块，也可以更新和更改这些存储的条件块。在创建和管理条件时，可以使用快速类别过滤器等工具轻松找到所需的块和属性。

在创建和管理条件规则时，请使用属性、运算符和值。

Cisco ISE 包含一些最常见用例的预定义复合条件。您可以编辑这些预定义条件来满足您的要求。为重用而保存的条件（包括即用型块）存储在 Condition Studio 的库中，如本任务中所述。

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 访问“策略集”(Policy Sets) 区域。选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

步骤 2 访问 Conditions Studio 以创建新条件并编辑现有条件块，以便随后将这些条件纳入您为特定策略集（及其关联策略和规则）配置的规则中，或保存到库以供将来使用：

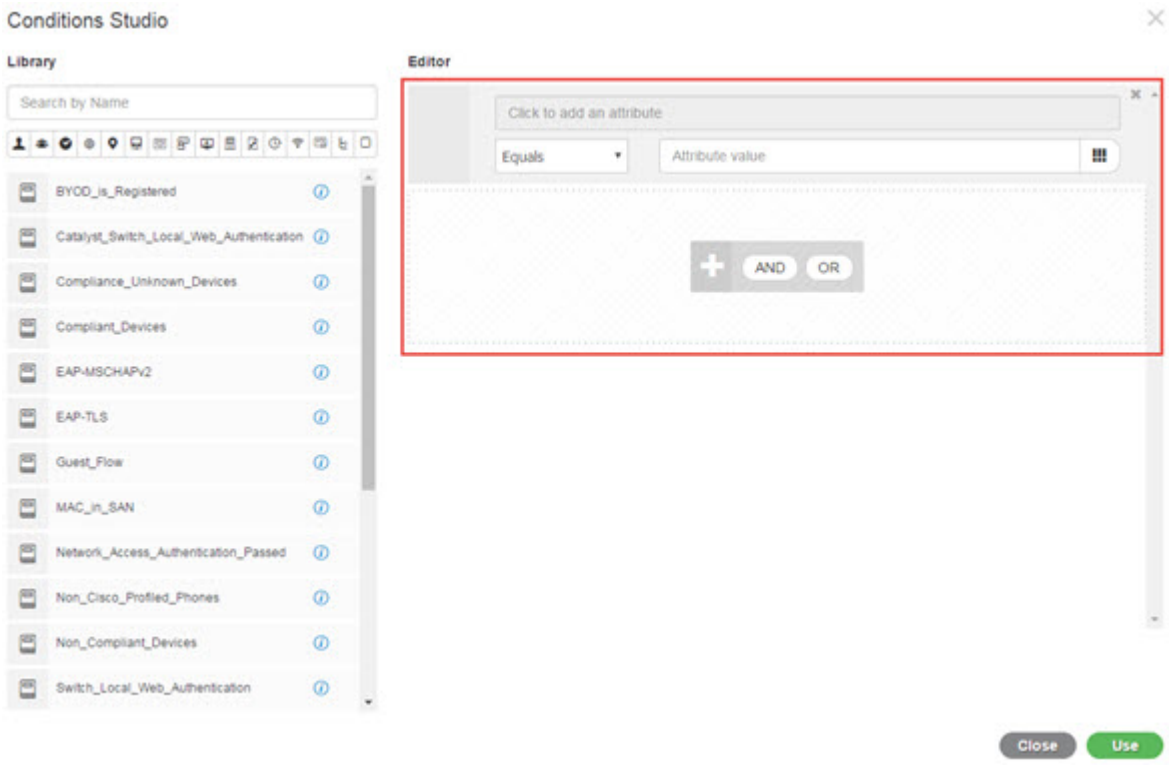
a) 从“策略集”(Policy Set) 主页面上的“策略集”(Policy Set) 表的“**条件**”**(Conditions)** 列中点击 ✚，以创建与整个策略集相关的条件（在匹配身份验证策略规则之前检查的条件）。

b) 或者，从特定策略集行点击 ，以查看“设置”(Set) 视图，包括所有身份验证和授权规则。在“设置”(Set) 视图中，将鼠标悬停在任何规则表的**条件 (Conditions)** 列中的单元格上，然后点击 打开 Conditions Studio。

c) 如果您正在编辑已应用于策略集的条件，请点击 以访问 Conditions Studio。

Conditions Studio 将打开。如果您已打开它来创建新条件，则如下图所示。若要查看字段的说明，以及打开 Conditions Studio 后如何编辑策略集已应用的条件的示例，请参阅浏览 Conditions Studio，第 35 页。

图 *4: Conditions Studio* - 创建新条件



步骤 3 使用库中的现有条件块作为您正在创建或编辑的条件中的规则。

a) 通过从类别工具栏中选择相关类别进行过滤 - 库中显示包含所选类别的属性的所有块。此外，还会显示包含多个规则但至少一个规则中使用了所选类别的属性的条件块。如果添加了其他过滤器，则显示的结果仅包括符合该特定过滤器而且与包含的其他过滤器也匹配的条件块。例如，从工具栏中选择“端口”(Ports) 类别，并在**按名称搜索 (Search by Name)** 字段中输入自由文本“auth”，就会显示与名称中包含“auth”的端口相关的所有块。再次点击类别工具栏中突出显示的图标，取消选择它，从而删除该过滤器。

b) 使用自由文本搜索条件块 - 在**按名称搜索 (Search by Name)** 自由文本字段中，输入要搜索的块名称中出现的任何术语或部分术语。在您键入内容时，系统会实时动态搜索相关结果。如果未选择类别（未突出显示任何图标），则结果包括来自所有类别的条件块。如果已选择类别图标（显示的列表已过滤），则显示的结果仅包括该特定类别中使用特定文本的块。

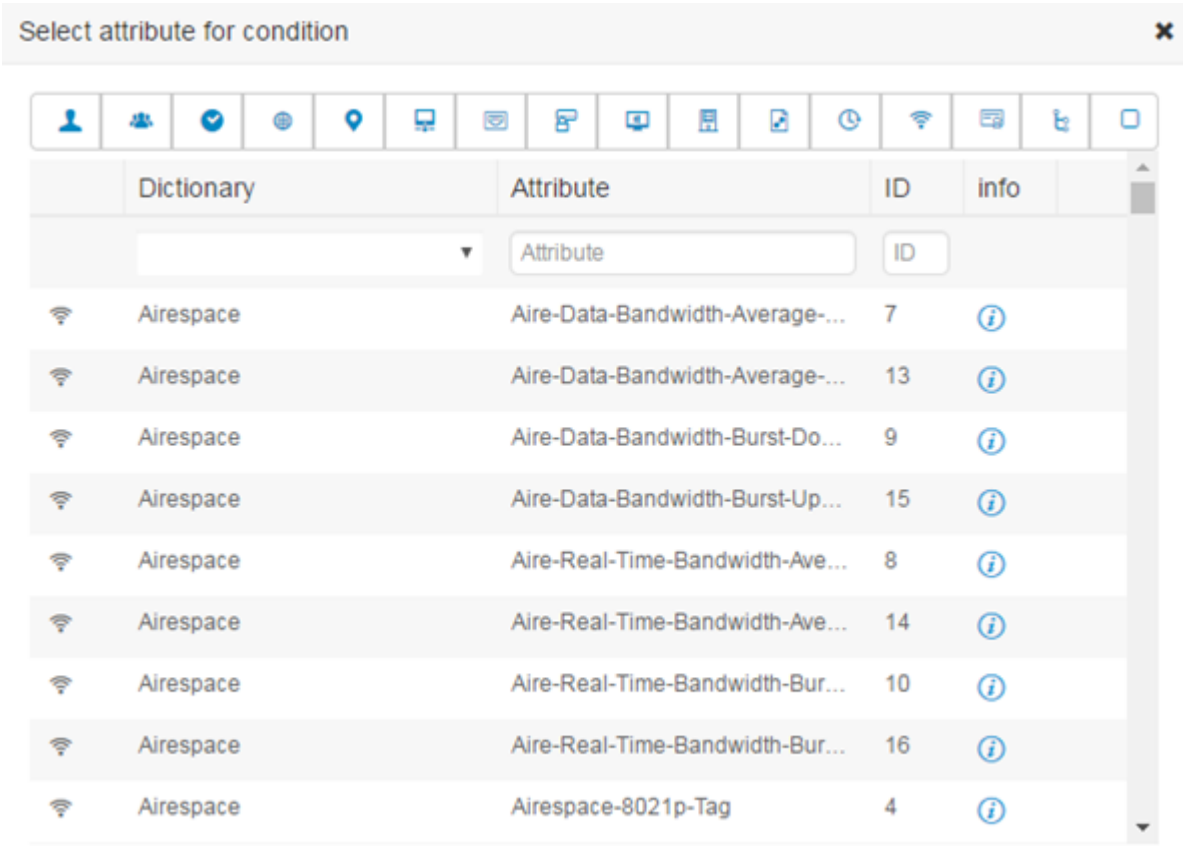
c) 找到条件块后，将其拖到编辑器中，放到要构建的块的正确级别上。如果放置的位置不正确，您可以在编辑器中再次拖放，直至放置正确。

d) 将鼠标悬停在编辑器中的条件块上，然后点击**编辑 (Edit)** 更改规则，以便对处理的条件做出相关的更改，用这些更改覆盖库中的规则，或者在库中将规则另存为新块。

放入编辑器时为只读状态的块现在可以编辑了，并且与编辑器中的所有其他自定义规则具有相同的字段、结构、列表和操作。继续执行后续步骤，了解有关编辑此规则的更多信息。

步骤 4 向当前级别添加运算符，以便随后在同一级别添加其他规则 - 选择 **AND**、**OR** 或 **Set to 'Is not'**。**Set to 'Is not'** 也可应用于单个规则。

步骤 5 使用属性词典创建和编辑规则 - 点击**点击以添加属性**字段。属性选择器随即打开，如下图所示：



属性选择器的各部分如下表所述：

字段	使用指南
属性类别工具栏	包含每个不同属性类别的唯一图标。选择任何属性类别图标，按类别过滤视图。 点击突出显示的图标可取消选择它，从而删除过滤器。
字典	表示存储属性的词典的名称。从下拉列表中选择特定词典，以便按供应商词典过滤属性。
属性	表示属性的名称。在可用字段中为属性名称键入自由文本来过滤属性。在您键入内容时，系统会实时动态搜索相关结果。

字段	使用指南
ID	表示唯一属性标识号。在可用字段中键入 ID 号来过滤属性。在您键入内容时，系统会实时动态搜索相关结果。
信息	将鼠标悬停在相关属性行上的信息图标上可查看有关属性的额外详细信息。

a) 从属性选择器的搜索框中，过滤并搜索所需的属性。在属性选择器的任何部分过滤或输入自由文本时，如果未激活其他过滤器，则结果仅包括与所选过滤器相关的所有属性。如果使用多个过滤器，则显示的搜索结果与所有过滤器匹配。例如，点击工具栏中的“端口”(Port) 图标并在“属性”(Attribute) 列中键入“auth”，则仅显示端口类别中名称含“auth”的属性。选择类别时，工具栏中的图标以蓝色突出显示，并显示过滤后的列表。再次点击类别工具栏中突出显示的图标，取消选择它，从而删除过滤器。

b) 选择相关属性，将其添加到规则中。
属性选择器关闭，您选择的属性会添加到**点击以添加属性 (Click to add an attribute)** 字段。

c) 从**等于 (Equals)** 下拉列表中，选择相关运算符。

不是您选择的所有属性都包含“Equals”、“Not Equals”、“Matches”、“Starts With”或“Not Starts With”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

您必须使用“equals”运算符进行直接比较。“Contains”运算符可用于多值属性。“Matches”运算符应用于正则表达式比较。当使用“Matches”运算符时，将解译正则表达式中的静态值和动态值。

d) 在**属性值 (Attribute value)** 字段中，执行以下操作之一：

- 在字段中键入自由文本值
- 从列表中选择一个动态加载的值（相关时 - 取决于上一步中选择的属性）
- 使用其他属性作为条件规则的值 - 选择字段旁边的表图标以打开属性选择器，然后搜索、过滤并选择相关属性。属性选择器关闭，您选择的属性会添加到**属性值 (Attribute value)** 字段。

步骤 6 在库中将规则另存为条件块。

a) 将鼠标悬停在要在库中另存为块的规则或规则的层次结构上。任何可另存为单个条件块的规则或规则组都将显示**复制 (Duplicate)** 和**保存 (Save)** 按钮。如果要将一组规则另存为块，请在整个层次结构的阻止区域中从整个层次结构的底部选择操作按钮。

b) 点击**保存 (Save)**。系统将弹出“保存条件”(Save condition) 屏幕。

c) 选择:

- 保存到现有库条件 - 选择此选项可使用您创建的新规则覆盖库中的现有条件块，然后在**从列表中选择 (Select from list)** 下拉列表中选择要覆盖的条件块。
- 另存为新库条件 - 在块的“条件名称”(Condition Name) 字段中键入唯一名称。

d) （可选）在**说明 (Description)** 字段中输入说明。当您将鼠标悬停在库中任何条件块的信息图标上时，系统会显示此说明，使您能够快速识别不同的条件块及其用途。

e) 点击**保存 (Save)** 在库中保存条件块。

步骤 7 在新的子级别上创建新规则 - 请点击 **AND** 或 **OR**，在现有父层级和您创建的子层级之间应用正确的运算符。新部分与所选运算符一起添加到编辑器层次结构中，作为提供所选运算符的规则或层次结构的子项。

步骤 8 在当前现有级别上创建新规则 - 从相关级别点击**新建 (New)**。在您开始的同一级别中，将显示新规则的一个空行。

步骤 9 点击 **X** 从编辑器中删除任何条件及其所有子项。

步骤 10 点击**复制 (Duplicate)** 可自动复制并粘贴层次结构中的特定条件，从而在同一级别创建其他相同的子项。您可以复制有或无子项的单个规则，具体取决于您点击**复制 (Duplicate)** 按钮的级别。

步骤 11 点击页面底部的**使用 (Use)** 保存在编辑器中创建的条件，并在策略集中实施该条件。

特殊网络访问条件

本部分说明了在创建策略集时有用的独特条件。这些条件无法从条件 Studio 创建，因此具有其自己的唯一进程。

配置设备网络条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 设备网络条件 (Device Network Conditions)**

步骤 2 点击**添加 (Add)**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 - 您可以添加 IP 地址或子网列表，每行一个。IP 地址/子网可以采用 IPV4 或 IPV6 格式。
- 设备名称 - 您可以添加设备名称列表，每行一个。必须输入在网络设备对象中配置的相同设备名称。
- 设备组 - 可以添加元组列表（按以下顺序）：根 NDG、逗号、（在根 NDG 下的）NDG。必须每行一个元组。

步骤 5 点击**提交 (Submit)**。

配置设备端口网络条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 设备端口网络条件 (Device Port Network Conditions)**

步骤 2 点击**添加 (Add)**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 (IP Addresses) - 按以下顺序输入详细信息：IP 地址或子网、逗号和（设备使用的）端口。必须每行一个元组。
- 设备 (Devices) - 按以下顺序输入详细信息：设备名称、逗号和端口。必须每行一个元组。您必须输入在网络设备对象中配置的相同设备名称。
- 设备组 (Device Groups) - 按以下顺序输入详细信息：根 NDG、逗号、（在根下的）NDG 和端口。必须每行一个元组。

步骤 5 点击**提交 (Submit)**。

配置终端站网络条件

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 终端站网络条件 (Endstation Network Conditions)**

步骤 2 点击**添加 (Add)**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 - 您可以添加 IP 地址或子网列表，每行一个。IP 地址/子网可以采用 IPV4 或 IPV6 格式。
- MAC 地址 - 您可以输入终端 MAC 地址和目标 MAC 地址的列表，用逗号分隔。每个 MAC 地址必须包含 12 个十六进制数字，且必须为以下格式之一：nn:nn:nn:nn:nn:nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn 或 nnnnnnnnnnnn。

  如果不需要终端站 MAC 或目标 MAC，请使用令牌“-ANY-”代替。
- CLI/DNIS - 您可以添加主叫方 ID (CLI) 和被叫方 ID (DNIS) 的列表，用逗号分隔。如果不需要主叫方 ID (CLI) 或被叫方 ID (DNIS)，请使用令牌“-ANY-”代替。

步骤 5 点击**提交 (Submit)**。

创建时间和日期条件

使用 Policy Elements Conditions 页面显示、创建、修改、删除、复制以及搜索时间和日期策略元素条件。策略元素是共享的对象，定义一个基于您所配置的特定时间和日期属性设置的条件。

使用时间和日期条件，使您可以按照您做出属性设置所指定的特定时间和日期来设置或限制访问Cisco ISE 系统资源的权限。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **通用 (Common)** > **时间和日期 (Time and Date)** > **添加 (Add)**

步骤 2 在字段中输入适当的值。

- 在 Standard Settings 区域中，指定提供访问的时间和日期。
- 在 Exceptions 区域中，指定限制访问的时间和日期。

步骤 3 点击**提交 (Submit)**。

在授权策略中使用 IPv6 条件属性

Cisco ISE 可以检测、管理和保护来自终端的 IPv6 流量。

当一个支持 IPv6 的终端连接至Cisco ISE 网络时，它通过 IPv6 网络与 NAD 通信。NAD 通过 IPv4 网络将来自终端的计费和分析信息（包括 IPv6 值）发送至Cisco ISE。您可以使用规则条件中的 IPv6 属性在Cisco ISE 中配置授权配置文件和策略，以处理来自支持 IPv6 终端的这些请求，并且确保终端合规。

您可以在 IPv6 前缀和 IPv6 接口值中使用通配符。例如：2001:db8:1234::/48。

支持的 IPv6 地址格式包括：

- 完整表示法：冒号分隔的八组四个十六进制数字。例如，2001:0db8:85a3:0000:0000:8a2e:0370:7334
- 缩短表示法：去除组中的前导零；使用两个连续的冒号替换零值组。例如：2001:db8:85a3::8a2e:370:7334
- 点分四组表示法（IPv4 映射和兼容 IPv4 的 Ipv6 地址）：例如，::ffff:192.0.2.128

支持的 IPv6 属性包括：

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address

- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

下表列出了受支持的Cisco属性-值对及其等效 IETF 属性：

Cisco属性值对	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

RADIUS 实时日志页面、RADIUS 身份验证报告、RADIUS 记账报告、当前活动会话报告、RADIUS 错误报告、错误配置的 NAS 报告、、自适应网络控制审核和错误配置的请求方客户端报告均支持 IPv6 地址。您可以从 RADIUS 实时日志页面或通过任何这些报告查看有关这些会话的详细信息。您可以根据 IPv4、IPv6 或 MAC 地址来过滤记录。

注释 如果将一个 Android 设备连接至支持 IPv6 的 DHCPv6 网络，它从 DHCP 服务器仅接收本地链路 IPv6 地址。因此，全局 IPv6 地址不在实时日志和终端页面（**工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**）中显示。

以下步骤描述了如何在授权策略中配置 IPv6 属性。

开始之前

确保在您的部署中网络接入设备 (NAD) 支持具备 IPv6 的 AAA。有关如何在 NAD 上启用 AAA IPv6 支持的信息，请参阅 **AAA IPv6 支持**。

步骤 1 对于网络访问策略，请选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。对于设备管理策略，请选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

步骤 2 创建授权规则。

步骤 3 创建授权规则时，请从 Conditon Studio 创建条件。在 Condition Studio 中，从 RADIUS 字典中选择 RADIUS IPv6 属性、运算符和值。

步骤 4 点击**保存 (Save)** 以将授权规则保存在策略集中。

策略集用于身份验证的

必须先在Cisco ISE 中定义全局协议设置，然后才能使用这些协议创建、保存和实施策略集。您可以使用 Protocol Settings 页面为 Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 和 Protected Extensible Authentication Protocol (PEAP) 协议定义全局选项，这些协议可以与网络中的其他设备进行通信。

支持的网络访问策略集协议

以下是您在定义网络访问策略集策略时可以选择的协议的列表：

- 密码身份验证协议 (PAP)
- 受保护的可扩展身份验证协议 (PEAP)
- Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)
- 可扩展身份验证协议消息摘要 5 (EAP-MD5)
- 可扩展身份验证协议-传输层安全 (EAP-TLS)
- 可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST)
- 可扩展的身份验证协议-基于隧道的传输层安全 (EAP-TTLS)
- 受保护的可扩展身份验证协议-传输层安全 (PEAP-TLS)

将 EAP-FAST 用作协议的指南

将 EAP-FAST 用作身份验证协议时，请遵循以下规定：

- 在经过身份验证的调配中启用 EAP-FAST 接受客户端证书时，强烈建议启用 EAP-TLS 内部方法。经过身份验证的调配中的 EAP-FAST 接受客户端证书不是一个单独的身份验证方法，而是一种更简短的客户端证书身份验证形式，它使用相同的证书凭证类型来对用户进行身份验证，但是不需要运行内部方法。
- 经过身份验证的调配中的接受客户端证书适用于无PAC完全握手和经过身份验证的PAC调配。它不适用于无 PAC 会话恢复、匿名 PAC 调配和基于 PAC 的身份验证。
- EAP属性按身份显示（所以在EAP链中会显示两次），即使身份验证按照不同的顺序进行，在监控工具的身份验证详细信息中仍然会按照先用户后设备的顺序显示。
- 当使用 EAP-FAST 授权 PAC 时，实时日志中显示的 EAP 身份验证方法等于用于完全身份验证（如在 PEAP 中）而非用于查找的身份验证方法。
- 在 EAP 链接模式中，当隧道 PAC 到期，然后 ISE 退回调配且 AC 请求用户和设备授权 PAC 时 - 无法调配设备授权 PAC。当 AC 请求时，它将在后续基于 PAC 的身份验证对话中进行调配。

- 当为链接配置Cisco ISE 并且为单一模式配置 AC 时，则 AC 使用身份类型 TLV 向 ISE 做出响应。但是，第二个身份的身份验证会失败。您可以通过此对话看到客户端适合执行链接，但当前未为单一模式执行配置。
- Cisco ISE 支持在仅适用于 AD 的 EAP-FAST 链中检索设备和用户的属性与组。对于 LDAP 和内部数据库，ISE 仅使用最后的身份属性。

注释 如果 EAP-FAST 身份验证协议用于 High Sierra、Mojave 或 Catalina MAC OSX 设备，可能会看到“EAP-FAST 加密绑定验证失败”(EAP-FAST cryptobinding verification failed) 消息。我们建议您配置“允许的协议”(Allowed Protocols) 页面中的“首选 EAP 协议”(Preferred EAP Protocol) 字段，以使这些 MAC OSX 设备使用 PEAP 或 EAP-TLS 而非 EAP-FAST。

配置 EAP-FAST 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP Fast 设置 (EAP Fast Settings)**。

步骤 2 按需输入详细信息，定义 EAP-FAST 协议。

步骤 3 如果要调用以前生成的所有主密钥和 PAC，请点击**撤销 (Revoke)**。

步骤 4 点击**保存 (Save)**，保存 EAP-FAST 设置。

为 EAP-FAST 生成 PAC

您可以使用Cisco ISE 中的 Generate PAC 选项为 EAP-FAST 协议生成隧道或计算机 PAC。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

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

步骤 2 从左侧的 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **EAP-FAST** > **生成 PAC (Generate PAC)**。

步骤 4 根据需要输入用于为 EAP-FAST 协议生成计算机 PAC 的详细信息。

步骤 5 点击**生成 PAC (Generate PAC)**。

EAP-FAST 设置

下表介绍“协议设置”(Protocol Settings) 窗口中的字段，您可以使用此窗口配置 EAP-FAST、EAP-TLS 和 PEAP 协议。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP-FAST 设置 (EAP-FAST Settings)**。

表 *5:* 配置 *EAP-FAST* 设置

字段名称	使用指南
Authority Identity Info Description	输入用于说明向客户端发送凭证的Cisco ISE 节点的用户友好字符串。客户端可以在类型、长度和值 (TLV) 的受保护访问凭证 (PAC) 信息中发现此字符串。默认值为 Identity Services Engine。
Master Key Generation Period	指定主键生成期（以秒、分钟、小时、天或周为单位）。值必须是范围在 1 至 2147040000 秒内的正整数。默认值为 604800 秒，相当于一周。
Revoke all master keys and PACs	点击“撤销”(Revoke) 可撤销所有主键和 PAC。
Enable PAC-less Session Resume	如果您要在没有 PAC 文件的情况下使用 EAP-FAST，请选中此复选框。
PAC-less Session Timeout	指定无 PAC 会话恢复超时的时间（以秒为单位）。默认值为 7200 秒。

相关主题

策略集用于身份验证的，第 48 页
将 EAP-FAST 用作协议的指南，第 48 页
EAP-FAST 的优势，第 91 页
配置 EAP-FAST 设置，第 49 页

PAC 设置

下表介绍“生成 PAC”(Generate PAC) 窗口上的字段，您可以使用此窗口为 EAP-FAST 身份验证配置受保护的访问凭证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **生成 PAC (Generate PAC)**。

表 *6:* 为 *EAP-FAST* 设置生成 *PAC*

字段名称	使用指南
Tunnel PAC	点击此单选按钮生成隧道 PAC。
Machine PAC	点击此单选按钮生成设备 PAC。

字段名称	使用指南
Trustsec PAC	点击此单选按钮生成 Trustsec PAC。
Identity	（针对 Tunnel 和 Machine PAC 身份字段）指定 EAP-FAST 协议显示为“内部用户名”的用户名或设备名称。如果身份字符串与该用户名不匹配，则身份验证失败。 这是主机定义在自适应安全设备 (ASA) 上定义的主机名。身份字符串必须与 ASA 主机名匹配，否则 ASA 无法导入生成的 PAC 文件。 如果生成的是 Trustsec PAC，则 Identity 字段指定 Trustsec 网络设备的设备 ID 并且由 EAP-FAST 协议提供发起方 ID。如果在此处输入的 Identity 字符串与该设备 ID 不匹配，则身份验证失败。
PAC Time to Live	（对于隧道和设备 PAC）请以秒为单位输入 PAC 的到期时间。默认值为 604800 秒，相当于一周。该值必须是介于 1 和 157680000 秒之间的正整数。对于 Trustsec PAC，请以天、周、月或年为单位输入一个值。默认情况下，该值为一年。最小值为一天，最大值为 10 年。
Encryption Key	输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。
Expiration Data	（仅对于 Trustsec PAC）到期日期根据 PAC Time to Live 计算。

相关主题

策略集用于身份验证的，第 48 页
将 EAP-FAST 用作协议的指南，第 48 页
为 EAP-FAST 生成 PAC，第 49 页

将 EAP-TTLS 用作身份验证协议

EAP-TTLS 是对 EAP-TLS 协议功能进行了扩展的两阶段协议。第 1 阶段建立安全隧道，并获取用于在第 2 阶段安全地在服务器与客户端之间隧道化属性的会话密钥。您可以使用在第 2 阶段隧道化的属性通过多种不同机制执行其他身份验证。

Cisco ISE 能够处理各种 TTLS 请求方的身份验证包括：

- Windows 系统上的 AnyConnect 网络访问管理器 (NAM)
- Windows 8.1 本地请求方

- Secure W2（在 MultiOS 上也称为 JoinNow）
- MAC OS X 本地请求方
- IOS 本地请求方
- 基于 Android 的本地请求方
- Linux WPA 请求方

注释 如果需要加密绑定，则必须使用 EAP-FAST 作为内部方法。

配置 EAP-TTLS 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-TTLS**。

步骤 2 在“EAP-TTLS 设置”(EAP-TTLS Settings) 页面输入所需的详细信息。

步骤 3 点击**保存 (Save)**。

EAP-TTLS 设置

下表介绍“EAP-TTLS 设置”(EAP-TTLS Settings) 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-TTLS**。

表 7: EAP-TTLS 设置

字段名称	使用指南
Enable EAP-TTLS Session Resume	如果您选中此复选框，Cisco ISE 将缓存在 EAP-TTLS 身份验证第一阶段创建的 TLS 会话，前提是用户在 EAP-TTLS 第二阶段成功通过身份验证。如果用户需要重新连接而且原来的 EAP-TTLS 会话尚未超时，Cisco ISE 使用缓存的 TLS 会话，从而加快 EAP-TTLS 性能、降低 AAA 服务器负载。 注释 当 EAP-TTLS 会话恢复时，跳过内部验证方法。

字段名称	使用指南
EAP-TTLS Session Timeout	指定 EAP-TTLS 会话在多少秒的时间后超时。默认值为 7200 秒。

相关主题

策略集用于身份验证的，第 48 页
将 EAP-TTLS 用作身份验证协议，第 51 页
配置 EAP-TTLS 设置，第 52 页

配置 EAP-TLS 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-TLS**。

步骤 2 根据需要输入详细信息可定义 EAP-TLS 协议。

步骤 3 点击**保存 (Save)** 保存 EAP-TLS 设置。

EAP-TLS 设置

下表介绍了“EAP-TLS 设置”(EAP-TLS Settings) 窗口上的字段，可以使用此窗口配置 EAP-TLS 协议设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-TLS**。

表 *8: EAP-TLS* 设置

字段	使用指南
Enable EAP-TLS Session Resume	选中此复选框可通过完全 EAP - TLS 认证用户的行为。此功能仅使用安全套接字层(SSL)握手（而不使用证书）对用户提供重新身份验证。只有在 EAP-TLS 会话未超时的情况下，EAP-TLS 会话才会重新运行。
EAP-TLS Session Timeout	指定 EAP-TLS 会话在多少秒的时间后超时。默认值为 7200 秒。
无状态会话恢复	
Master Key Generation Period	输入主键重新生成前经过的时间。此值确定主键保持活动的持续时间。您可以输入以秒、分钟、小时、天或周为单位的值。

字段	使用指南
Revoke	点击**撤销 (Revoke)** 以取消以前生成的所有主键和票证。此选项在辅助节点上禁用。

相关主题

策略集用于身份验证的，第 48 页
配置 EAP-TLS 设置，第 53 页

配置 PEAP 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

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

步骤 2 从左侧的 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **PEAP**。

步骤 4 根据需要，输入详细信息以定义 PEAP 协议。

步骤 5 点击**保存 (Save)** 以保存 PEAP 设置。

PEAP 设置

下表列出“PEAP 设置”(PEAP Settings) 窗口上的字段，您可以使用此窗口配置 PEAP 协议设置。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **PEAP**。

表 *9: PEAP* 设置

字段名称	使用指南
Enable PEAP Session Resume	选中此复选框，使Cisco ISE 缓存在 PEAP 身份验证的第一阶段创建的 TLS 会话，前提是用户在 PEAP 的第二阶段成功通过身份验证。如果用户需要重新连接，原始PEAP会话尚未超时，Cisco ISE使用缓存的TLS会话，从而加快PEAP性能、降低的 AAA 服务器的负载。您必须指定 PEAP 会话恢复功能的 PEAP 会话超时值可以工作。
PEAP Session Timeout	指定 PEAP 会话超时的时间（单位：秒）。默认值为 7200 秒。

字段名称	使用指南
Enable Fast Reconnect	选中此复选框，允许在Cisco ISE 中恢复 PEAP 会话，而无需在启用会话恢复功能时检查用户凭证。

相关主题

策略集用于身份验证的，第 48 页
配置 PEAP 设置，第 54 页
使用 PEAP 的优势，第 90 页
PEAP 协议支持的请求方，第 90 页
PEAP 协议流程，第 90 页

配置 RADIUS 设置

您可以配置 RADIUS 设置，以检测未能通过身份验证的客户端，并禁止重复报告成功的身份验证。

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

步骤 2 在 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **RADIUS**。

步骤 4 输入定义 RADIUS 设置所需的详细信息。

步骤 5 点击**保存 (Save)**，保存设置。

RADIUS 设置

下表介绍“RADIUS 设置”(RADIUS Settings) 窗口中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **RADIUS**。

如果启用**抑制重复失败的客户端 (Suppress Repeated Failed Clients)** 选项，系统会从审核日志中抑制身份验证重复失败的客户端，并在指定的时间段内自动拒绝来自这些客户端的请求。您还可以指定身份验证失败的次数，在此之后应拒绝来自这些客户端的请求。例如，如果此值配置为 5，当客户端身份验证失败五次时，将在配置的时间段内拒绝从该客户端收到的所有请求。

注释 如果身份验证失败的原因是输入了错误的密码，则不会抑制客户端。

注释 如果配置RADIUS失败抑制，则在配置RADIUS日志抑制后，仍可能会收到错误“5440终端已放弃会话并启动了新会话”(5440 Endpoint Abandoned EAP Session and started a new one)。有关详细信息，请参阅以下 ISE 社区帖子：

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

。

表 *10: RADIUS* 设置

字段名称	使用指南
抑制重复失败的客户端 (Suppress Repeated Failed Clients)	
抑制重复失败的客户端 (Suppress Repeated Failed Clients)	选中此复选框可抑制因相同原因导致身份验证重复失败的客户端。系统会从审核日志中抑制这些客户端，如果已启用**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 选项，还会在指定时间段内拒绝来自这些客户端的请求。
检测两次失败的时间范围 (Detect Two Failures Within)	输入以分钟为单位的时间间隔。如果客户端在该时间段内因相同原因导致两次身份验证失败，则系统会从审核日志中将其抑制，并且，如果已启用**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 选项，还会拒绝来自此客户端的请求。
每几分钟报告一次故障 (Report Failures Once Every)	以分钟为单位输入报告失败身份验证的时间间隔。例如，如果此值设置为 15 分钟，则每 15 分钟在审核日志中仅报告一次重复身份验证失败的客户端，从而防止过度报告。
拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)	选中此复选框可自动拒绝来自身份验证重复失败的客户端的RADIUS请求。您可以启用此选项，以避免Cisco ISE进行不必要的处理，并防范潜在的拒绝服务攻击。
自动拒绝前的失败次数 (Failures Prior to Automatic Rejection)	输入身份验证失败次数，超过此次数后，会自动拒绝来自重复失败客户端的请求。在配置的时间段内（在**持续拒绝请求的时长 (Continue Rejecting Requests for)** 字段中指定），系统会自动拒绝从这些客户端收到的所有请求。在该间隔到期后，系统会处理来自这些客户端的身份验证请求。
持续拒绝请求的时长 (Continue Rejecting Requests for)	输入一个时间间隔（分钟），在此间隔内会拒绝来自重复失败客户端的请求。

字段名称	使用指南
忽略重复记账更新的时间范围 **(Ignore Repeated Accounting Updates Within)**	在此期间内发生的重复记账更新将被忽略。
抑制成功报告 **(Suppress Successful Reports)**	
Suppress Repeated Successful Authentications	选中此复选框以防重复报告前 24 小时内在身份情景、网络设备和授权方面没有变更的成功身份验证。
身份验证详细信息 **(Authentications Details)**	
突出显示长于该值的步骤 **(Highlight Steps Longer Than)**	以毫秒为单位输入时间间隔。如果单个步骤的执行超出指定阈值，则在身份验证详细信息页面中使用时钟图标来标记此步骤。
检测 **RADIUS** 请求的高速率 **(Detect High Rate of RADIUS Requests)**	
检测 **RADIUS** 请求的稳定高速率 **(Detect Steady High Rate of Radius Requests)**	选中此复选框可在超过 **RADIUS 请求持续时间 (Duration of RADIUS requests)** 字段和 **RADIUS 请求总数 (Total number of RADIUS requests)** 字段中指定的限制时，发出高 RADIUS 请求负载警报。
RADIUS 请求持续时间 **(Duration of RADIUS Requests)**	输入将用于计算 RADIUS 速率的时间段（以秒为单位）。默认值为 60 秒。有效范围为 20 至 86400 秒。
RADIUS 请求总数 **(Total Number of RADIUS Requests)**	输入将用于计算 RADIUS 速率的请求限制。默认为 72000 个请求。有效范围为 24000 到 103680000 个请求。
RADIUS UDP 端口 **(RADIUS UDP Ports)**	
身份验证端口 **(Authentication Ports)**	指定将用于 RADIUS UDP 身份验证流程的端口。您可以指定最多 4 个端口号（用逗号分隔）。默认情况下，使用端口 1812 和端口 1645。有效范围为 1024 到 65535。
记帐端口 **(Accounting Ports)**	指定将用于 RADIUS UDP 记帐流程的端口。您可以指定最多 4 个端口号（用逗号分隔）。默认情况下，使用端口 1813 和端口 1646。有效范围为 1024 到 65535。 注释　确保其他服务未使用这些端口。
RADIUS DTLS	

字段名称	使用指南
身份验证和记账端口 (Authentication and Accounting Port)	指定将用于 RADIUS DTLS 身份验证和记帐流程的端口。默认情况下，使用端口 2083。有效范围为 1024 到 65535。 **注释** 确保其他服务未使用此端口。
空闲超时 （Idle Timeout）	如果没有从网络设备收到数据包，请输入希望 Cisco ISE 在关闭 TLS 会话之前等待的时间（以秒为单位）。默认值为 120 秒。有效范围为 60 至 600 秒。
启用 RADIUS/DTLS 客户端身份验证 (Enable RADIUS/DTLS Client Identity Verification)	如果希望Cisco ISE 在 DTLS 握手期间验证 RADIUS/DTLS 客户端的身份，请选中此复选框。如果客户端身份无效，则Cisco ISE 握手失败。默认网络设备会跳过身份检查（如果已配置）。身份检查按以下顺序执行： **1.** 如果客户端证书包含使用者备用名称 (SAN) 属性： • 如果 SAN 包含 DNS 名称，则证书中指定的 DNS 名称会与为Cisco ISE 中的网络设备配置的 DNS 名称进行比较。 • 如果 SAN 包含 IP 地址（且不包含 DNS 名称），则证书中指定的 IP 地址会与 Cisco ISE 中配置的所有设备 IP 地址进行比较。 **2.** 如果证书不包含 SAN，则使用者 CN 会与为 Cisco ISE 中的网络设备配置的 DNS 名称进行比较。如果不匹配，则Cisco ISE 握手失败。

相关主题

策略集用于身份验证的 ， 第 48 页
思科 ISE 中的 RADIUS 协议支持 ， 第 64 页
配置 RADIUS 设置 ， 第 55 页

配置安全设置

要配置安全设置：

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全设置 (Security Settings)**。

步骤 2 在“安全设置”(Security Settings) 页面上，选择所需的选项：

- **Allow TLS 1.0 (允许 TLS 1.0)**：在以下工作流程中允许 TLS 1.0 用于与以下传统对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端
- **Allow TLS 1.1 (允许 TLS 1.1)**：在以下工作流程中允许 TLS 1.1 用于与以下传统对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端
- **允许 SHA1 密码 (Allow SHA1 Ciphers)**：在以下工作流程中允许 SHA-1 密码用于与对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 配置为 RADIUS DTLS 服务器
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

  您可以选择以下其中一个选项：
  - **允许所有 SHA-1 密码**
  - **仅允许 TLS_RSA_with_AES_128_CBC_SHA**

  注释 我们建议使用 SHA-256 或 SHA-384 密码以增强安全性。
- **允许 ECDHE-RSA 密码 (Allow ECDHE-RSA Ciphers)**：在以下工作流程中允许 ECDHE-RSA 密码用于与对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 配置为 RADIUS DTLS 服务器
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端

- Cisco ISE 配置为安全 LDAP 客户端

- **允许 3DES 密码 (Allow 3DES Ciphers)**：在以下工作流程中允许 3DES 密码用于与对等体通信：
  - Cisco ISE 配置为 EAP 服务器
  - Cisco ISE 配置为 RADIUS DTLS 服务器
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

- **接受证书而不验证用途 (Accept Certificates without Validating Purpose)**：当 ISE 充当 EAP 或 RADIUS DTLS 服务器时，系统会接受客户端证书，而不检查密钥使用扩展是否包含用于 ECDHE-ECDSA 密码的 keyAgreement 位或用于其他密码的 keyEncipherment 位。

- **允许 DSS 密码用于作为客户端的 ISE (Allow DSS ciphers for ISE as a client)**：当Cisco ISE 充当客户端时，在以下工作流程中允许使用 DSS 密码与服务器通信：
  - Cisco ISE 配置为 RADIUS DTLS 客户端
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

- **允许传统的不安全 TLS 重新协商用于作为客户端的 ISE (Allow Legacy Unsafe TLS Renegotiation for ISE as a Client)**：在以下工作流程中允许与不支持安全 TLS 重新协商的传统 TLS 服务器通信：
  - Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - Cisco ISE 配置为安全系统日志客户端
  - Cisco ISE 配置为安全 LDAP 客户端

步骤 3 **披露无效用户名 (Disclose invalid usernames)**：默认情况下，对于因用户名不正确而导致的身份验证失败，ISE 会显示无效。为了帮助进行调试，此选项会强制 ISE 在报告中披露（显示）用户名，而不是无效。无论是否选中此选项，对于因用户名不正确而导致的身份验证失败，始终会显示用户名。

当启用**披露无效用户名 (Disclose invalid usernames)** 时，必须选择**始终显示无效用户名 (Always show invalid usernames)**或**在特定时间内显示无效用户名 (Show invalid usernames for a specific time)**。当选择时间选项时，请以分钟为单位选择时间，最多一个月（43,200 分钟）。

此功能适用于 Active Directory、内部用户、LDAP 和 ODBC 身份源。其他身份存储库（如 RADIUS 令牌、RSA 或 SAML）不支持此功能。对于这些身份库，错误输入的用户名始终报告为“无效”。

步骤 **4** 点击**保存 (Save)**。

支持的密码套件

Cisco ISE 支持 TLS 版本 1.0、1.1 和 1.2。

Cisco ISE 支持 RSA 和 ECDSA 服务器证书。支持以下椭圆曲线：

- secp256r1
- secp384r1
- secp521r1

下表列出了支持的密码套件：

密码套件	当思科 **ISE** 配置为 **EAP** 服务器时 当思科 **ISE** 配置为 **RADIUS DTLS** 服务器时	当思科 **ISE** 从 **HTTPS** 或安全 **LDAP** 服务器下载 **CRL** 时 当思科 **ISE** 配置为安全系统日志客户端或安全 **LDAP** 客户端时 当思科 **ISE** 配置为 **CoA** 的 **RADIUS DTLS** 客户端时
TLS 1.0 支持	当允许 TLS 1.0 时 （DTLS 服务器仅支持 DTLS 1.2） 默认情况下，在Cisco ISE 2.3 及更高版本中，“允许 TLS 1.0”选项 (Allow TLS 1.0) 选项处于禁用状态。当禁用此选项时，基于 TLS 的 EAP 身份验证方法（EAP-TLS、EAP-FAST/TLS）和 802.1X 请求方不支持 TLS 1.0。如果要在 TLS 1.0 中使用基于 TLS 的 EAP 身份验证方法，请选中**安全设置 (Security Settings)**窗口中的“允许 TLS 1.0”(Allow TLS 1.0) 复选框。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **安全设置 (Security Settings)**。	当允许 TLS 1.0 时 （DTLS 客户端仅支持 DTLS 1.2）
TLS 1.1 支持	当允许 TLS 1.1 时	当允许 TLS 1.1 时

ECC DSA 密码		
ECDHE-ECDSA-AES256-GCM-SHA384	支持	支持
ECDHE-ECDSA-AES128-GCM-SHA256	支持	支持
ECDHE-ECDSA-AES256-SHA384	支持	支持
ECDHE-ECDSA-AES128-SHA256	支持	支持
ECDHE-ECDSA-AES256-SHA	当允许 SHA-1 时	当允许 SHA-1 时
ECDHE-ECDSA-AES128-SHA	当允许 SHA-1 时	当允许 SHA-1 时
ECC RSA 密码		
ECDHE-RSA-AES256-GCM-SHA384	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES128-GCM-SHA256	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES256-SHA384	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES128-SHA256	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES256-SHA	当允许 ECDHE-RSA/SHA-1 时	当允许 ECDHE-RSA/SHA-1 时
ECDHE-RSA-AES128-SHA	当允许 ECDHE-RSA/SHA-1 时	当允许 ECDHE-RSA/SHA-1 时
DHE RSA 密码		
DHE-RSA-AES256-SHA256	不支持	支持
DHE-RSA-AES128-SHA256	不支持	支持
DHE-RSA-AES256-SHA	否	当允许 SHA-1 时
DHE-RSA-AES128-SHA	否	当允许 SHA-1 时
RSA 密码		
AES256-SHA256	支持	支持
AES128-SHA256	支持	支持
AES256-SHA	当允许 SHA-1 时	当允许 SHA-1 时
AES128-SHA	当允许 SHA-1 时	当允许 SHA-1 时
3DES 密码		

DES-CBC3-SHA	当允许 3DES / SHA-1 时	当启用 3DES/DSS 和 SHA-1 时
DSS 密码		
DHE-DSS-AES256-SHA	否	当启用 3DES/DSS 和 SHA-1 时
DHE-DSS-AES128-SHA	否	当启用 3DES/DSS 和 SHA-1 时
EDH-DSS-DES-CBC3-SHA	否	当启用 3DES/DSS 和 SHA-1 时
弱 RC4 密码		
RC4-SHA	当“允许的协议”（Allowed Protocols）页面中启用“允许弱密码”（Allow weak ciphers）选项且允许 SHA-1 时	否
RC4-MD5	当“允许的协议”（Allowed Protocols）页面中启用“允许弱密码”（Allow weak ciphers）选项时	否
仅 EAP-FAST 匿名调配： ADH-AES-128-SHA	支持	不支持
对等证书限制		
验证 KeyUsage	对于以下密码，客户端证书应具有 KeyUsage=密钥协议和 ExtendedKeyUsage=客户端身份验证： • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

验证 ExtendedKeyUsage	对于以下密码，客户端证书应具有 KeyUsage=密钥加密和 ExtendedKeyUsage=客户端加密： • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	服务器证书应具有 ExtendedKeyUsage=服务器身份验证

思科 ISE 中的 RADIUS 协议支持

RADIUS 是一个客户端/服务器协议，通过该协议，远程访问服务器与中央服务器发生通信，对拨入用户进行身份验证，并对拨入用户所请求的系统或服务的访问进行授权。您可以在所有远程服务器可共享的中央数据库中使用 RADIUS 维护用户配置文件。此协议提供更高的安全性，并且您可以使用它来设置策略以应用于单个管理的网络点。

RADIUS 还可以在Cisco ISE 中用作 RADIUS 客户端以代理远程 RADIUS 服务器的请求，并且它还可在活动会话期间提供授权更改 (CoA)。

Cisco ISE 依据 RFC 2865 对 RADIUS 协议流程提供支持，并广泛支持所有 RADIUS 常规属性（如 RFC 2865 及其扩展中所描述）。Cisco ISE 支持仅解析在Cisco ISE 字典中定义的供应商特定属性。

RADIUS 接口支持下述在 RFC 2865 中定义的属性数据类型：

- 文本（Unicode 转换格式 [UTF]）
- 字符串（二进制）
- 地址 (IP)
- 整数
- 时间

ISE 社区资源

有关Cisco ISE 支持的网络访问属性的信息，请参阅 ISE 网络访问属性。

允许的协议

下表介绍**允许的协议 (Allowed Protocols)** 窗口中的字段，您可以使用此窗口配置身份验证过程中要使用的协议。 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)**。

表 *11:* 允许的协议

字段名称	使用指南
允许的协议 > 身份验证旁路	
流程主机查找	如果希望Cisco ISE 处理主机查询请求，请选中此复选框。当 RADIUS 服务类型等于 10 (呼叫-检查）且用户名等于呼叫 - 站 - ID 时，对于 PAP/CHAP 协议，会对主机查询请求进行处理。当服务类型等于 1（框到的）且用户名等于呼叫 - 站 - ID 时，对于 EAP-MD5 协议，会对主机查询请求进行处理。如果您希望Cisco ISE 忽略主机查找请求并使用系统用户名属性的原始值进行身份验证，请取消选中此复选框。当取消选中时，系统会根据协议（例如 PAP）进行消息处理。 注释 禁用此选项可能会导致现有 MAB 身份验证失败。
允许的协议 > 身份验证协议	
Allow PAP/ASCII	此选项可启用 PAP/ASCII。PAP 使用明文密码（即，未加密的密码），并且是最不安全的身份验证协议。
允许 CHAP (Allow CHAP)	此选项可启用 CHAP 身份验证。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。
允许 MS-CHAPv1 (Allow MS-CHAPv1)	选中此复选框可启用 MS-CHAPv1。
允许 MS-CHAPv2 (Allow MS-CHAPv2)	选中此复选框可启用 MS-CHAPv2。
允许 EAP-MD5 (Allow EAP-MD5)	选中此复选框可启用基于 EAP 的 MD5 密码散列身份验证。

字段名称	使用指南
允许 EAP-TLS (Allow EAP-TLS)	选中此复选框可启用EAP-TLS身份验证协议并配置 EAP-TLS 设置。您可以指定Cisco ISE 将如何按照来自最终用户客户端的EAP身份响应中的说明对用户身份进行验证。用户身份根据最终用户客户端提供的证书中的信息进行验证。在Cisco ISE 与最终用户客户端之间建立 EAP-TLS 隧道后，会发生此比较。 **注释** EAP-TLS是基于证书的身份验证协议。仅在您已完成配置证书的所需步骤后，才能发生 EAP-TLS 身份验证。 • **在授权策略中允许过期证书的身份验证以允许证书续订 (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy)** 复选框：如果要允许用户续订证书，请选中此复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。 • **启用无状态会话恢复 (Enable Stateless Session Resume)**：选中此复选框可允许恢复EAP-TLS会话，而无需将会话状态存储在服务器上。Cisco ISE 支持 RFC 5077 中所述的会话票证扩展。Cisco ISE创建一个票证并将其发送到EAP-TLS客户端。客户端向ISE提供票证以恢复会话。 • **主动会话票证更新 (Proactive Session Ticket update)**：输入一个百分比值，以表示会话票证更新之前必须经过的有效时间 (TTL)。例如，如果您输入的值为 60，则在经过 TTL 的 60% 后更新会话票证。 • **会话票证有效时间 (Session ticket Time to Live)**：输入会话票证过期前所经过的时间。此值可确定会话票证保持活动状态的持续时间。您可以输入以秒、分钟、小时、天或周为单位输入值。
允许 LEAP (Allow LEAP)	选中此复选框可启用轻量级可扩展身份验证协议 (LEAP) 身份验证。

字段名称	使用指南
允许 **PEAP (Allow PEAP)**	

字段名称	使用指南

	选中此复选框可启用PEAP身份验证协议和PEAP设置。默认内部方法为 MS-CHAPv2。
	
	当选中“允许 PEAP”(Allow PEAP) 复选框时，您可以配置以下 PEAP 内部方法：
	
	• **允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE支持密码更改。
	  • **重试尝试数 (Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。
	
	• **允许 EAP-GTC (Allow EAP-GTC)**：选中此复选框可使用 EAP-GTC 作为内部方法。
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE支持密码更改。
	  • **重试尝试数 (Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效范围为 0 到 3。
	
	• **允许 EAP-TLS (Allow EAP-TLS)**：选中此复选框可使用 EAP-TLS 作为内部方法。
	
	如果要允许用户更新证书，请选中**允许过期证书的身份验证以允许身份验证策略中的证书更新 (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy)** 复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。
	
	• **需要加密的 TLV (Require Cryptobinding TLV)**：如果希望 EAP 对等体和 EAP 服务器都参与 PEAP 身份验证的内部和外部 EAP 身份验证，则选中此复选框。
	
	• **仅对传统客户端允许 PEAPv0 (Allow PEAPv0 Only for Legacy Clients)**：选中此复选框可

字段名称	使用指南
	允许 PEAP 请求方使用 PEAPv0 进行协商。某些传统客户端不符合 PEAPv1 协议标准。要确保不丢弃此类 PEAP 对话，请选中此复选框。

字段名称	使用指南
允许 **EAP-FAST (Allow EAP-FAST)**	

字段名称	使用指南

	选中此复选框可启用 EAP-FAST 身份验证协议和 EAP-FAST 设置。EAP-FAST 协议可以在同一服务器上支持多个内部协议。默认内部方法为 MS-CHAPv2。
	
	当选中“允许 EAP-FAST”(Allow EAP-FAST) 复选框时，您可以将 EAP-FAST 配置为内部方法：
	
	• **允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE 支持密码更改。
	  • **重试尝试数 (Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。
	
	• **Allow EAP-GTC**
	
	允许密码更改 (Allow Password Change)：选中此复选框可使Cisco ISE 支持密码更改。
	
	重试尝试数 (Retry Attempts)：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。
	
	• **使用 PAC (Use PACs)**：选中此选项可配置 Cisco ISE 以便为 EAP-FAST 客户端调配授权受保护访问凭证 (PAC)。系统显示其他 PAC 选项。
	
	• **不使用 PAC (Don't Use PACs)**：选择此选项可配置Cisco ISE 以使用 EAP-FAST，而不发出或接受任何隧道或计算机 PAC。系统会忽略对 PAC 的所有请求，并且Cisco ISE 会在没有 PAC 的情况下使用 Success-TLV 进行响应。
	
	当选择此选项时，您可以将Cisco ISE 配置为执行计算机身份验证。
	
	• **允许 EAP-TLS (Allow EAP-TLS)**：选中此复选框可使用 EAP-TLS 作为内部方法。
	
	如果要允许用户更新证书，请选中**允许过期证书的身份验证以允许身份验证策略中的证书更新 (Allow authentication of expired**

字段名称	使用指南
	certificates to allow certificate renewal in Authorization Policy) 复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。 • **启用 EAP 链接 (Enable EAP Chaining)**：选中此复选框可启用 EAP 链接。 EAP 链接允许Cisco ISE 将用户和计算机身份验证的结果相关联，并且使用 EAPChainingResult 属性应用相应的授权策略。 EAP 链接要求请求方在客户端设备上支持 EAP 链接。选择请求方中的“用户和计算机身份验证”(User and Machine Authentication) 选项。 当选择 EAP-FAST 协议（二者均处于基于 PAC 的模式和无 PAC 模式下）时，EAP 链接可用。 对于基于 PAC 的身份验证，您可以使用用户授权 PAC 和/或计算机授权 PAC 跳过内部方法。 对于基于证书的身份验证，如果您为 EAP-FAST 协议启用“接受客户端调配证书”(Accept Client Certificate for Provisioning) 选项（在允许的协议服务中），并且如果终端 (AnyConnect) 配置为在隧道内发送用户证书，则在隧道建立过程中，ISE 会使用证书对用户进行身份验证（跳过内部方法），而计算机身份验证会通过内部方法来完成。如果未配置这些选项，则 EAP-TLS 会用作用于进行用户身份验证的内部方法。 在您启用 EAP 链接后，使用 NetworkAccess:EapChainingResult 属性更新授权策略并添加条件，然后分配相应的权限。

字段名称	使用指南

允许 **EAP-TTLS (Allow EAP-TTLS)**	选中此复选框可启用 EAP-TTLS 协议。
	您可以配置以下内部方法：
	• 允许 **PAP/ASCII (Allow PAP/ASCII)**：选中此复选框可使用 PAP/ASCII 作为内部方法。可以使用 EAP-TTLS PAP 进行基于令牌和基于 OTP 的身份验证。
	• 允许 **CHAP (Allow CHAP)**：选中此复选框可使用 CHAP 作为内部方法。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。
	• 允许 **MS-CHAPv1 (Allow MS-CHAPv1)**：选中此复选框可使用 MS-CHAPv1 作为内部方法。
	• 允许 **MS-CHAPv2 (Allow MS-CHAPv2)**：选中此复选框可使用 MS-CHAPv2 作为内部方法。
	• 允许 **EAP-MD5 (Allow EAP-MD5)**：选中此复选框可使用 EAP-MD5 作为内部方法。
	• 允许 **EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。
	  • 允许密码更改 **(Allow Password Change)**：选中此复选框可使Cisco ISE 支持密码更改。
	  • 重试尝试数 **(Retry Attempts)**：指定Cisco ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。

字段名称	使用指南
允许 **TEAP (Allow TEAP)**	

字段名称	使用指南

	选中此复选框可启用隧道可扩展身份验证协议 (TEAP) 并配置 TEAP 设置。TEAP 是一种基于隧道的 EAP 方法，可通过使用传输层安全 (TLS) 协议建立隧道，实现对等体和服务器之间的安全通信。类型长度值 (TLV) 对象在 TEAP 隧道内用于在 EAP 对等体和 EAP 服务器之间传输与身份验证相关的数据。
	
	您可以为 TEAP 配置以下内部方法：
	
	• **允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)**：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。
	
	  • **允许密码更改 (Allow Password Change)**：选中此复选框可使Cisco ISE 支持密码更改。
	
	  • **重试次数 (Retries)**：输入Cisco ISE 在显示登录失败消息之前允许用户输入凭证的次数。有效范围为 0 到 3。
	
	• **允许 EAP-TLS (Allow EAP-TLS)**：选中此复选框可使用 EAP-TLS 作为内部方法。
	
	  • **在授权策略中允许过期证书的身份验证以允许证书续订 (Allow Authentication of Expired Certificates to Allow Certificate Renewal in Authorization Policy)**：如果要允许用户续订证书，请选中此复选框。如果启用此选项，请确保配置相应的授权策略规则，确认在进一步处理请求之前是否已续订证书。
	
	• **允许降级到 MSK (Allow Downgrade to MSK)**：如果内部方法支持扩展主会话密钥 (EMSK)，但客户端设备仅提供主会话密钥 (MSK)，请选中此复选框。请注意，虽然 EMSK 比 MSK 更安全，但某些客户端设备可能不支持 EMSK。
	
	• **在隧道建立期间接受客户端证书 (Accept Client Certificate during Tunnel Establishment)**：如果希望Cisco ISE 在 TEAP 隧道建立期间请求客户端证书，请选中此复选框。如果未提供证书，则Cisco ISE 使用所配置的内部方法进行身份验证。

字段名称	使用指南
	• **启用 EAP 链接 (Enable EAP Chaining)**：选中此复选框可启用 EAP 链接。EAP 链接允许Cisco ISE 在同一 TEAP 隧道内同时运行用户和计算机身份验证的内部方法。这可以让 Cisco ISE 使用 EAPChainingResult 属性关联身份验证结果，并应用相应的授权策略。 在启用 EAP 链接后，应使用 NetworkAccess:EapChainingResult 属性更新授权策略并添加条件，然后分配相应的权限。 **注释** 启用 EAP 链接时，如果要同时执行用户和计算机身份验证，请确保在请求方中复制用户和计算机证书。 **注释** • 如果在思科 ISE 中启用了 EAP 链接，则必须为 Microsoft 请求方同时配置主身份验证方法和辅助身份验证方法。 • 如果在思科 ISE 中禁用了 EAP 链接，则必须仅为 Microsoft 请求方配置主身份验证方法。 • 如果主身份验证方法和辅助身份验证方法均配置为“无”，则 EAP 协商可能会失败，并显示以下消息： `请求方已停止响应ISE (Supplicant stopped responding to ISE)`
Preferred EAP Protocol	选中此复选框可从以下任一选项中选择首选EAP协议：EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS 和 EAP-MD5。如果没有指定首选协议，则默认情况下使用 EAP - TLS。
“EAP-TLS L-位”(EAP-TLS L-bit)	选中此复选框可支持传统EAP请求方，后者默认情况下期望来自 ISE 的 TLS 更改密码规格报文和加密握手报文中具有长度包含标志（L位标志）。

字段名称	使用指南
允许 EAP 的弱密码 (Allow Weak Ciphers for EAP)	如果启用了此选项，会允许传统客户端使用弱密码协商（例如：RSA_RC4_128_SHA, RSA_RC4_128_MD5）。我们建议仅在您的传统客户端只支持弱密码时启用此选项。 默认情况下该选项处于禁用状态。 注释 思科 ISE 不支持 EDH_RSA_DES_64_CBC_SHA 和 EDH_DSS_DES_64_CBC_SHA。
所有 RADIUS 请求均需要消息身份验证器 (Require Message Authenticator for all RADIUS Requests)	如果启用此选项，Cisco ISE 验证 RADIUS 消息中是否存在 RADIUS 消息身份验证器 (RADIUS Message Authenticator) 属性。如果消息身份验证器属性不存在，则 RADIUS 消息将被丢弃。 启用此选项可提供保护,免受欺骗性访问请求消息和篡改 RADIUS 消息的威胁。 RADIUS 消息身份验证器 (RADIUS Message Authenticator) 属性是整个 RADIUS 消息的消息摘要 5 (MD5) 散列。 注释 EAP 默认使用消息身份验证器属性，不要求您将其启用。

相关主题

FIPS 和非 FIPS 模式支持的 TACACS+ 设备管理协议
为网络访问定义允许的协议，第 85 页

PAC 选项

下表介绍了在**允许协议服务列表 (Allowed Protocols Services List)** 窗口中选择了“使用 PAC”(Use PACs) 后显示的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)**。

表 *12: PAC* 选项

字段名称	使用指南
使用 **PAC (Use PAC)**	

字段名称	使用指南
	• “隧道 PAC 存活时间”(Tunnel PAC Time To Live)：存活时间 (TTL) 值限制 PAC 的生存期。指定生存期值和单位。默认值为 90 天。时间范围为 1 至 1825 天。 • “当剩下 <n%> 的 PAC TTL 时主动进行 PAC 更新”(Proactive PAC Update When: <n%> of PAC TTL is Left)：更新值确保客户端拥有有效的 PAC。首次成功通过身份验证后，但在 TTL 设置的到期时间前，Cisco ISE 启动更新。更新值是指 TTL 中的剩余时间百分比。默认为 90%。 • “允许匿名带内 PAC 调配”(Allow Anonymous In-band PAC Provisioning)：选中此复选框，使Cisco ISE 与客户端建立安全的匿名 TLS 握手，并使用 EAP-FAST 的零阶段和 EAP-MSCHAPv2，通过 PAC 调配客户端。要启用匿名 PAC 调配，必须选择这两种内部方法：EAP-MSCHAPv2 和 EAP-GTC。 • “允许经验证的带内 PAC 调配 ”(Allow Authenticated In-band PAC Provisioning)：Cisco ISE 使用 SSL 服务器侧身份验证，在 EAP-FAST 的零阶段期间通过 PAC 调配客户端。此选项比匿名调配的安全性更高，但要求在Cisco ISE 上安装服务器证书和受信任的根 CA。 如果您选中此选项，可将Cisco ISE 配置为在成功对 PAC 调配进行身份验证后将 Access-Accept 消息传送至客户端。 • “服务器在对调配进行身份验证后返回 Access-Accept 消息”(Server Returns Access Accept After Authenticated Provisioning)：如果希望Cisco ISE 在成功对 PAC 调配进行身份验证后传送 Access-Accept 消息，请选中此复选框。 • “允许机器身份验证”(Allow Machine Authentication)：选中此复选框，使Cisco ISE 使用计算机 PAC 调配最终用户客户端，并执行计算机身份验证（适用于没有计算机凭证的最终用户客户端）。可以通过请求（频内）或管理员（频外）将计算机 PAC 调配至

字段名称	使用指南
	客户端。当Cisco ISE 收到最终用户客户端发送的有效计算机 PAC 时，会从 PAC 提取计算机身份详细信息，并在Cisco ISE 外部身份源中进行验证。Cisco ISE 只支持 Active Directory 作为计算机身份验证的外部身份源。正确验证这些详细信息后，不会再执行进一步的身份验证。 如果您选中此选项，可以输入接受使用计算机 PAC 的时间值。当Cisco ISE 收到过期的计算机 PAC 时，会自动使用新的计算机 PAC 重新调配最终用户客户端（无需等待最终用户客户端发送新的计算机 PAC 请求）。 • “启用无状态会话恢复”(Enable Stateless Session Resume)：选中此复选框后，Cisco ISE 会为 EAP-FAST 客户端调配授权 PAC，并跳过 EAP-FAST 的第二阶段（默认为启用）。 在下列情况下取消选中此复选框： • 如果您不希望Cisco ISE 为 EAP-FAST 客户端调配授权 PAC • 要始终执行 EAP-FAST 的第二阶段 如果您选中此选项，可以输入用户授权 PAC 的授权时间段。在此时间段后，PAC 过期。当Cisco ISE 收到过期的授权 PAC 时，会执行执行 EAP-FAST 身份验证的第二阶段。

相关主题

OOB TrustSec PAC，第 108 页
为 EAP-FAST 生成 PAC，第 49 页

将思科 ISE 用作 RADIUS 代理服务器

Cisco ISE 可用作 RADIUS 服务器和 RADIUS 代理服务器。用作代理服务器时，Cisco ISE 从网络接入服务器 (NAS) 接受身份验证和记帐请求并将这些请求转发至外部 RADIUS 服务器。Cisco ISE 接受请求的结果并将结果返回至 NAS。

Cisco ISE 可以同时用作多个外部 RADIUS 服务器的代理服务器。您可以在 RADIUS 服务器序列中使用此处配置的外部 RADIUS 服务器。External RADIUS Server 页面会列出您已在Cisco ISE 中定义的所有外部 RADIUS 服务器。您可以使用过滤器选项，根据名称或说明或同时根据名称和说明搜索

具体 RADIUS 服务器。在简单身份验证策略和基于规则的身份验证策略中，您都可以使用 RADIUS 服务器序列来代理对 RADIUS 服务器的请求。

RADIUS 服务器序列从 RADIUS-Username 属性删除域名以进行 RADIUS 身份验证。这种域名删除操作不适用于使用 EAP-Identity 属性的 EAP 身份验证。RADIUS 代理服务器从 RADIUS-Username 属性获取用户名并从您配置 RADIUS 服务器序列时指定的字符删除用户名。对于 EAP 身份验证，RADIUS 代理服务器从 EAP-Identity 属性获取用户名。只有在 EAP-Identity 和 RADIUS-Username 值相同时，使用 RADIUS 服务器序列的 EAP 身份验证才会成功。

配置外部 RADIUS 服务器

您必须在Cisco ISE 中配置外部 RADIUS 服务器，使其向外部 RADIUS 服务器转发请求。您可以定义超时时间和连接尝试的次数。

开始之前

- 您无法单独使用您在本节中创建的外部 RADIUS 服务器，而必须创建 RADIUS 服务器序列并将其配置为使用您在本节创建的RADIUS服务器。然后，您就可以在身份验证策略中使用RADIUS服务器序列。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 RADIUS 服务器 (External RADIUS Servers)**。

系统将显示 RADIUS Servers 页面，其中包含已在Cisco ISE 中定义的外部 RADIUS 服务器的列表。

步骤 2 点击**添加 (Add)** 以添加外部 RADIUS 服务器。

步骤 3 根据要求输入相应值。

步骤 4 点击**提交 (Submit)** 以保存外部 RADIUS 服务器配置。

定义 RADIUS 服务器序列

Cisco ISE 中的 RADIUS 服务器序列允许您将 NAD 发送的请求代理到外部 RADIUS 服务器，此外部 RADIUS 服务器会处理该请求并将结果返回至Cisco ISE，随后Cisco ISE 会将响应转发至 NAD。

RADIUS Server Sequences 页面列出您在Cisco ISE 中定义的所有 RADIUS 服务器序列。在此页面上，您可以创建、编辑或复制 RADIUS 服务器序列。

开始之前

- 在开始此程序之前，您应该基本了解代理服务，并且必须成功完成相关链接的第一个条目中的任务。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 管理 **(Administration)** > 网络资源 **(Network Resources)** > **RADIUS** 服务器序列 **(RADIUS Server Sequences)**。

步骤 2 点击添加 **(Add)**。

步骤 3 根据要求输入相应值。

步骤 4 点击提交 **(Submit)** 以保存要用于策略的 RADIUS 服务器序列。

思科 ISE 充当 TACACS+ 代理客户端

Cisco ISE 可以充当外部 TACACS+ 服务器的代理客户端。当用作代理客户端时，Cisco ISE 接收来自网络接入服务器 (NAS) 的身份验证、授权和计费请求并将这些请求转发至外部 TACACS+ 服务器。Cisco ISE 接受请求的结果并将结果返回至 NAS。

“外部 TACACS+ 服务器”(TACACS+ External Servers) 页面列出了您已在Cisco ISE 中定义的所有外部 TACACS+ 服务器。您可以使用过滤器选项来根据名称和/或说明搜索具体的 TACACS+ 服务器。

Cisco ISE 可以同时充当多台外部 TACACS+ 服务器的代理客户端。要配置多台外部服务器，您可以使用 TACACS+ 服务器序列页面。有关更多详细信息，请参阅TACACS+ 服务器序列设置页面。

配置外部 TACACS+ 服务器

您必须在Cisco ISE 中配置外部 TACACS 服务器，使其向外部 TACACS 服务器转发请求。您可以定义超时时间和连接尝试的次数。

开始之前

- 您不能在策略中直接使用在本节中创建的外部 TACACS 服务器。而必须创建 TACACS 服务器序列并将其配置为使用您在本节创建的 TACACS 服务器。然后，您就可以在策略集中使用 TACACS 服务器序列。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 工作中心 **(Work Centers)** > 设备管理 **(Device Administration)** > 网络资源 **(Network Resources)** > **TACACS** 外部服务器 **(TACACS External Servers)**。
系统将显示**TACACS** 外部服务器 **(TACACS External Servers)** 页面，其中包含已在Cisco ISE 中定义的外部 TACACS 服务器的列表。

步骤 2 点击添加 **(Add)** 以添加外部 TACACS 服务器。

步骤 3 根据要求输入相应值。

步骤 4 点击提交 **(Submit)** 以保存外部 TACACS 服务器配置。

TACACS+ 外部服务器设置

下表列出“TACACS 外部服务器”(TACACS External Servers) 页面中的字段。导航路径为 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **TACACS 外部服务器 (TACACS External Servers)** 页面。

表 *13: TACACS+* 外部服务器设置

字段	使用指南
名称 (Name)	输入 TACACS+ 外部服务器的名称。
说明	输入 TACACS+ 外部服务器设置的说明。
Host IP	输入远程 TACACS+ 外部服务器的 IP 地址（IPv4 或 IPv6 地址）。
连接端口	输入远程 TACACS+ 外部服务器的端口号。端口号为 49。
Timeout	指定Cisco ISE 等待外部 TACACS+ 服务器响应的秒数。默认值为 5 秒。有效值范围为 1 至 120。
共享密钥	文本字符串用于获得与 TACACS+ 外部服务器的连接。如果配置不正确，则连接将被 TACACS+ 外部服务器拒绝。
使用单连接	TACACS 协议支持两种将会话与连接关联的模式：单连接和非单连接。单连接模式重复使用用于客户端可能发起的多个 TACACS+ 会话的单 TCP 连接。非单连接打开一个用于客户端发起的每个 TACACS+ 会话的新 TCP 连接。TCP 连接在每个会话之后关闭。 对于高流量环境，您可以选中使用单连接 (Use Single Connect) 复选框，对于低流量环境可取消选中。

定义 TACACS+ 服务器序列

Cisco ISE 中的 TACACS+ 服务器序列允许您将 NAD 发送的请求代理到外部 TACACS+ 服务器，此外部 TACACS+ 服务器会处理该请求并将结果返回至Cisco ISE，随后Cisco ISE 会将响应转发至 NAD。TACACS+ 服务器序列页面列出您在Cisco ISE 中定义的所有 TACACS+ 服务器序列。在此页面上，您可以创建、编辑或复制 TACACS+ 服务器序列。

开始之前

- 您应该对代理服务、Cisco ISE 管理员组、访问级别、权限和限制有一个基本了解。

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 确保您希望在 TACACS+ 服务器序列中使用的外部 TACACS+ 服务器已定义。

步骤 1 选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **TACACS 外部服务器 (TACACS External Servers)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入所需的值。

步骤 4 点击**提交 (Submit)** 以保存用于策略的 TACACS+ 服务器序列。

TACACS+ 服务器序列设置

下表介绍“TACACS 服务器序列”页面中的字段。导航路径为 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **TACACS 服务器序列 (TACACS Server Sequence)** 页面。

表 *14: TACACS+* 服务器序列设置

字段	使用指南
名称 (Name)	输入 TACACS 代理服务器序列的名称。
说明	输入 TACACS 代理服务器序列的说明。
服务器列表	从可用列表中选择所需的TACACS代理服务器。可用列表包含在“外部 TACACS+ 服务”(TACACS External Services) 页面配置的 TACACS 代理服务器列表中。
日志记录控制 (Logging Control)	选中此复选框以启用日志记录控制： • “本地计费”(Local Accounting)：计费消息由处理设备请求的服务器记录。 • “远程计费”(Remote Accounting)：计费消息由处理设备请求的代理服务器记录。

字段	使用指南
“用户名剥离”(Username Stripping)	用户名前缀/后缀剥离： • “前缀剥离”(Prefix Strip)：选中此复选框以删除用户名的前缀。例如，如果主题名称是 acme\smith，分隔符为 \，则用户名变成 smith。默认分隔符为 \。 • “后缀剥离”(Suffix Strip)：选中此复选框以删除用户名的后缀。例如，如果主题名称是 smith@acme.com，分隔符为 @，则用户名变成 smith。默认分隔符为 @。

网络访问服务

网络访问服务包含请求的身份验证策略条件。可以为不同的使用案例创建单独的网络访问服务，例如，有线 802.1X、有线 MAB 等。要创建网络访问服务，请配置允许的协议或服务器序列。然后，从“策略集”(Policy Sets) 页面配置网络访问策略的网络访问服务。

为网络访问定义允许的协议

允许的协议定义了Cisco ISE 可以用于与请求访问网络资源的设备通信的协议集。允许的协议访问服务是一个您应在配置身份验证策略前创建的独立实体。允许的协议访问服务是一个包含特定使用案例的选定协议的对象。

Allowed Protocols Services 页面列出了您创建的所有允许的协议服务。Cisco ISE 中预定义了默认网络访问服务。

开始之前

在开始此程序之前，您应该具备用于身份验证的协议服务的基本知识。

- 请查看本章节中的“Cisco ISE 身份验证策略”部分，以了解身份验证类型和各种数据库支持的协议。
- 查看“PAC 选项”，了解每种协议服务的功能和选项，以便您可以做出适合您的网络的选择。
- 确保您已定义全局协议设置。

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许的协议 (Allowed Protocols)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入所需信息。

步骤 4 为您的网络选择适当的身份验证协议和选项。

步骤 5 如果您选择使用 PAC，请进行适当的选择。

要启用 Anonymous PAC Provisioning，您必须同时选择以下两个内部方法：EAP-MSCHAPv2 和可扩展身份验证协议-通用令牌卡 (EAP-GTC)。另请注意，Cisco ISE 只支持 Active Directory 作为计算机身份验证的外部身份源。

步骤 6 点击**提交 (Submit)** 保存允许的协议服务。

允许的协议服务在简单和基于规则的身份验证策略页面中显示为独立对象。您可以将此对象用于不同的规则。

您现在可以创建简单或基于规则的身份验证策略。

如果禁用 EAP-MSCHAP 作为内部方法并为 PEAP 或 EAP-FAST 启用 EAP-GTC 和 EAP-TLS 内部方法，则 ISE 会在内部方法协商过程中启动 EAP-GTC 内部方法。在第一个 EAP-GTC 消息发送到客户端之前，ISE 会执行身份选择策略以从身份库获取 GTC 密码。在执行此策略的过程中，EAP 身份验证等于 EAP-GTC。如果 EAP-GTC 内部方法被客户端拒绝且 EAP-TLS 已经过协商，则系统不会再次执行身份库策略。如果身份库策略基于 EAP 身份验证属性，则它可能会出现意外结果，因为实时 EAP 身份验证基于 EAP-TLS，但设置于身份策略评估之后。

用户的网络接入

对网络接入，主机会连接至网络设备并且请求使用网络资源。网络设备识别新连接的主机，并且将 RADIUS 协议用作传输机制，向Cisco ISE 请求对用户进行身份验证和授权。

Cisco ISE 根据基于 RADIUS 协议传输的协议支持网络接入流程。

不使用 EAP 的基于 RADIUS 的协议

不包含 EAP 的基于 RADIUS 的协议包含以下协议：

- 密码身份验证协议 (PAP)
- CHAP
- Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)
- MS-CHAP 版本 2 (MS-CHAPv2)

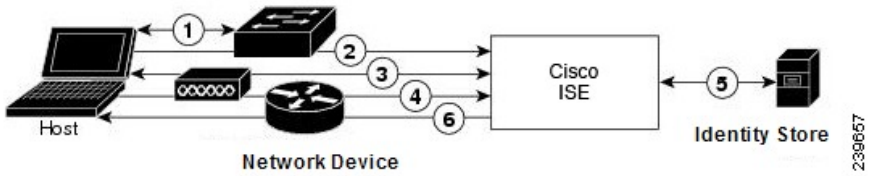
基于 RADIUS 的非 EAP 身份验证流程

本节介绍不使用 EAP 的基于 RADIUS 的身份验证。使用 PAP 身份验证的基于 RADIUS 的流程按以下程序进行：

1. 主机连接至网络设备。
2. 网络设备向Cisco ISE 发送包含适用于所用具体协议（PAP、CHAP、MS-CHAPv1 或 MS-CHAPv2）的 RADIUS 属性的 RADIUS 请求。
3. Cisco ISE 使用身份存储区验证用户凭证。
4. Cisco ISE 向网络设备发送 RADIUS 响应（Access-Accept 或 Access-Reject），然后网络设备将应用此响应决策。

下图显示不使用 EAP 的基于 RADIUS 的身份验证。

图 *5:* 不使用 *EAP* 的基于 *RADIUS* 的身份验证



Cisco ISE 支持的非 EAP 协议如下：

密码身份验证协议

PAP 使用双向握手为用户提供建立其身份的简单方法。PAP 密码使用共享密钥加密，是最简单的身份验证协议。PAP 不是强大的身份验证方法，因为其几乎无法抵御反复试错攻击。

思科 *ISE* 中基于 *RADIUS* 的 *PAP* 身份验证

Cisco ISE 根据身份存储区检查用户名和密码对，直到其最终确认身份验证或终止连接。

您可以同时将不同安全级别应用于Cisco ISE 以满足不同要求。PAP 使用二次握手过程。如果身份验证成功，Cisco ISE 返回确认信息；否则，Cisco ISE 将停止连接或向发起方提供第二次机会。

发起方完全控制尝试的频率和计时。因此，可以使用更强的身份验证方法的任意服务器都可以在PAP之前主动协商该方法。RFC 1334 定义 PAP。

Cisco ISE 支持基于 RADIUS UserPassword 属性的标准 RADIUS PAP 身份验证。RADIUS PAP 身份验证与所有身份存储区都兼容。

RADIUS PAP 身份验证流程包括记录成功和失败的尝试。

质询握手身份验证协议

CHAP 使用质询响应机制，其中会对响应进行单向加密。CHAP 使Cisco ISE 可以从最安全的加密机制向下协商到最不安全的加密机制，并且会保护流程中传输的密码。CHAP 密码可重复使用。如果使用Cisco ISE 内部数据库进行身份验证，您可以使用 PAP 或 CHAP。CHAP 不适用于 Microsoft 用户数据库。与 RADIUS PAP 相比，CHAP 可在从最终用户客户端到 AAA 客户端的通信期间为密码加密实现更高的安全性。

Cisco ISE 支持基于 RADIUS ChapPassword 属性的标准 RADIUS PAP 身份验证。Cisco ISE 仅支持使用内部身份库进行 RADIUS CHAP 身份验证。

Microsoft 质询握手身份验证协议版本 *1*

Cisco ISE 支持 RADIUS MS-CHAPv1 身份验证和更改密码功能。RADIUS MS-CHAPv1 包含两个版本的更改密码功能：Change-Password-V1 和 Change-Password-V2。Cisco ISE 不支持基于 RADIUS MS-CHAP-CPW-1 属性的 Change-Password-V1，仅支持基于 MS-CHAP-CPW-2 属性的 Change-Password-V2。以下身份源支持 RADIUS MS-CHAPv1 身份验证和更改密码功能：

- 内部身份库

- Microsoft Active Directory 身份库

Microsoft 质询握手身份验证协议版本 *2*

RADIUS MS - CHAPv2 身份验证和更改密码功能受以下身份来源支持：

- 内部身份库
- Microsoft Active Directory 身份库

基于 RADIUS 的 EAP 协议

EAP 提供了可扩展的框架，支持各种身份验证类型。本节介绍Cisco ISE 支持的 EAP 方法，包含下列主题：

简单的 EAP 方法

- EAP 消息摘要 5
- 轻型 EAP

使用思科 ISE 服务器证书进行身份验证的 EAP 方法

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

除了上面列出的方法，还有使用证书进行服务器和客户端身份验证的 EAP 方法。

基于 RADIUS 的 EAP 身份验证流程

只要身份验证流程中涉及 EAP，则开始此流程之前都要执行 EAP 协商以确定应该使用哪个具体的 EAP 方法（以及在适当的情况下使用内部方法）。基于 EAP 的身份验证按照以下程序进行：

1. 主机连接至网络设备。
2. 网络设备向主机发送 EAP 请求。
3. 主机向网络设备回复 EAP 响应。
4. 网络设备将其从主机接收的 EAP 响应封装入 RADIUS 访问请求（使用 EAP-Message RADIUS 属性）并将此 RADIUS 访问请求发送至Cisco ISE。
5. Cisco ISE 从此 RADIUS 数据包提取 EAP 响应，并且创建新 EAP 请求，将其封装入 RADIUS 访问质询（也是使用 EAP-Message RADIUS 属性），然年后将其发送至网络设备。
6. 网络设备提取 EAP 请求并将其发送至主机。

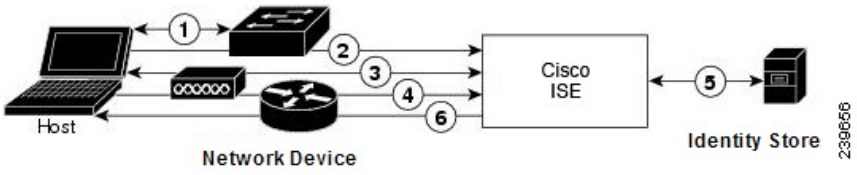
这样，主机和Cisco ISE 就间接地交换 EAP 消息（通过 RADIUS 传输并穿过网络设备）。以此方式交换的首批 EAP 消息会协商以后用于执行身份验证的具体 EAP 方法。

之后交换的 EAP 消息就用于传输执行实际身份验证所需的数据。如果所协商的具体 EAP 身份验证方法需要，Cisco ISE 会使用身份库来验证用户凭证。

Cisco ISE 确定身份验证成功还是失败之后，会向网络设备（而且最终也向主机）发送封装入 RADIUS Access-Accept 或 Access-Reject 消息的 EAP-Success 或 EAP-Failure 消息。

下图显示使用 EAP 的基于 RADIUS 的身份验证。

图 *6:* 使用 *EAP* 的基于 *RADIUS* 的身份验证



可扩展身份验证协议-消息摘要 *5*

可扩展身份验证协议-消息摘要 5 (EAP - MD5) 提供单向客户端身份验证。服务器向客户端发送随机质询。客户端在响应中通过使用 MD5 加密质询及密码证明其身份。由于人为截取可看到质询和响应，所以在开放式媒体上使用时，EAP-MD5 容易遭受字典攻击。由于不发生服务器验证，所以也很容易遭受欺骗。Cisco ISE 支持Cisco ISE 内部身份库的 EAP-MD5 身份验证。在使用 EAP-MD5 协议时，还支持主机查找。

轻型可扩展身份验证协议

目前，Cisco ISE 仅将轻型可扩展身份验证协议 (LEAP) 用于Cisco Aironet 无线网络。如果不启用此选项，配置为执行 LEAP 身份验证的Cisco Aironet 最终用户客户端就无法访问网络。如果所有Cisco Aironet 最终用户客户端都使用不同的身份验证协议（例如，可扩展身份验证协议-传输层安全 [EAP-TLS]），我们建议您禁用此选项。

注释 如果用户使用网络设备 *(Network Devices)* 部分中定义的 AAA 客户端作为 RADIUS（思科 Aironet）设备访问您的网络，您必须启用 LEAP、EAP-TLS 或同时启用这两项；否则思科 Aironet 用户将无法进行身份验证。

受保护的可扩展身份验证协议

受保护的可扩展身份验证协议 (PEAP) 提供相互身份验证，确保易受攻击的用户凭证的机密性和完整性，保护其自身抵御被动（窃听）和主动（中间人）攻击，以及安全地生成加密密钥材料。PEAP 与 IEEE 802.1X 标准和 RADIUS 协议兼容。Cisco ISE 使用可扩展身份验证协议-Microsoft 质询握手身份验证协议 (EAP-MS-CHAP)、可扩展身份验证协议-通用令牌卡 (EAP-GTC) 和 EAP-TLS 内部方法支持 PEAP 版本 0 (PEAPv0) 和 PEAP 版本 1 (PEAPv1)。Cisco安全服务客户端 (SSC) 请求方支持Cisco ISE 支持的所有 PEAPv1 内部方法。

使用 *PEAP* 的优势

使用 PEAP 有这些优势：PEAP 以 TLS 为基础，而 TLS 实施广泛，经过了大量安全审查；它为不派生密钥的方法建立密钥；它在隧道内发送身份；它保护内部方法交换和结果消息；它支持分段。

PEAP 协议支持的请求方

PEAP 支持这些请求方：

- Microsoft 内置客户端 802.1X XP
- Microsoft 内置客户端 802.1X Vista
- Cisco安全服务客户端 (SSC)，4.0 版
- Cisco SSC，5.1 版
- Funk Odyssey 访问客户端，4.72 版
- Intel，12.4.0.0 版

PEAP 协议流程

PEAP 会话可以分为三部分：

1. Cisco ISE 和对等体建立 TLS 隧道。Cisco ISE 提供其证书，但对等体不提供。对等体和Cisco ISE 创建密钥以加密隧道内的数据。
2. 内部方法确定隧道内的数据流：
   - EAP-MS-CHAPv2 内部方法 - EAP-MS-CHAPv2 数据包在不带报头的情况下在隧道内传输。报头的第一个字节包含类型字段。EAP-MS-CHAPv2 内部方法支持更改密码功能。可以配置用户可以尝试通过管理门户更改密码的次数。用户身份验证尝试次数受此数值限制。
   - EAP-GTC 内部方法 - PEAPv0 和 PEAPv1 均支持 EAP-GTC 内部方法。支持的请求方不支持使用 EAP-GTC 内部方法的 PEAPv0。EAP-GTC 支持更改密码功能。可以配置用户可以尝试通过管理门户更改密码的次数。用户身份验证尝试次数受此数值限制。
   - EAP-TLS 内部方法 - Windows 内置请求方不支持在建立隧道后对消息分段，这会影响 EAP-TLS 内部方法。在建立隧道后，Cisco ISE 不支持外部 PEAP 消息分段。在建立隧道时，分段会按照 PEAP 文档中的规定进行工作。在 PEAPv0 中，系统将删除 EAP-TLS 数据包信头，而在 PEAPv1 中， EAP-TLS 数据包在传输时保持不变。
   - 可扩展身份验证协议类型、长度、值 (EAP-TLV) 扩展 - EAP TLV 数据包在传输时保持不变。EAP-TLV 数据包在带标头的情况下在隧道内传输。
3. 如果会话已达到内部方法，会以一种受保护的方式确认成功和失败。

   客户端 EAP 消息始终载于 RADIUS Access-Request 消息中，而服务器 EAP 消息始终载于 RADIUS Access-Challenge 消息中。EAP-Success 消息始终载于 RADIUS Access-Accept 消息中。EAP-Failure 消息始终载于 RADIUS Access-Reject 消息中。丢弃客户端 PEAP 消息会导致丢弃 RADIUS 客户端消息。

注释 Cisco ISE 要求在 PEAPv1 通信期间确认 EAP-成功或 EAP-失败消息。对等体必须发送回带有空 TLS 数据字段的 PEAP 数据包，以确认收到成功或失败消息。

可扩展身份验证协议-通过安全隧道的灵活身份验证 *(EAP-FAST)*

可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST) 是提供相互身份验证和使用共享密钥建立隧道的一种身份验证协议。隧道用于保护基于密码的弱身份验证方法。共享密钥称为受保护的访问凭证 (PAC) 密钥，用于为客户端和服务器进行相互身份验证，同时保护隧道安全。

EAP-FAST 的优势

EAP-FAST 相比其他身份验证协议提供以下优势：

- 相互身份验证 - EAP 服务器必须能够验证对等体的身份和真实性，而且对等体必须能够验证 EAP 服务器的真实性。
- 抵抗被动字典式攻击 - 许多身份验证协议要求对等体向 EAP 服务器明确地提供纯文本或散列形式密码。
- 抵抗中间人攻击 - 建立相互验证保护隧道时，协议必须阻止敌对者在对等体和 EAP 服务器之间的对话中成功插入信息。
- 确保支持许多不同的密码身份验证接口的灵活性，例如 MS-CHAPv2、通用令牌卡 (GTC) 及其他 - EAP-FAST 是一个扩展框架，允许同一服务器支持多个内部协议。
- 提高效率 - 使用无线介质时，对等体的计算资源和电力资源有限。EAP-FAST 使网络访问通信能够减少计算资源占用。
- 最大限度减少身份验证服务器的每用户身份验证状态要求 - 对于大型部署，通常有许多服务器充当多个对等体的身份验证服务器。此外，非常理想的情况是，对等体使用同一共享秘钥保护隧道的方式，与它使用用户名和密码获得网络访问权限的方式基本相同。EAP-FAST 促进对等体使用一个强大的共享秘钥，同时使服务器最大限度减少它必须缓存和管理的每用户和设备状态。

EAP-FAST 流程

EAP-FAST 协议流程始终由以下阶段组成：

1. 调配阶段 - 此阶段是 EAP-FAST 的初始阶段。在此阶段，系统使用Cisco ISE 和对等体之间共享的叫作 PAC 的唯一强密钥调配对等体。
2. 建立隧道阶段 - 客户端和服务器通过使用 PAC 建立全新隧道密钥相互进行身份验证。系统然后使用隧道密钥保护其余对话并实现消息机密性和可靠性。
3. 身份验证阶段 - 身份验证在隧道内部处理，其包含生成会话密码和受保护的终止。Cisco ISE 支持 EAP-FAST 版本 1 和 1a。

从非思科设备启用 MAB

按顺序配置以下设置，可从非Cisco设备配置 MAB。

步骤 1 确保终端数据库中具有要进行身份验证的终端的 MAC 地址。可以添加这些终端或由分析器服务自动分析这些终端。

步骤 2 根据非Cisco设备（PAP、CHAP 或 EAP-MD5）使用的 MAC 身份验证类型创建网络设备配置文件。

a) 选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备配置文件 (Network Device Profiles)**。

b) 点击**添加 (Add)**。

c) 输入网络设备配置文件的名称和描述。

d) 从**供应商 (Vendor)** 下拉列表中选择供应商名称。

e) 选中设备支持的协议所对应的复选框。如果设备支持 RADIUS，请选择 RADIUS 字典与网络设备配合使用。

f) 扩展**身份验证/授权 (Authentication/Authorization)** 部分，对设备的数据流类型、属性别名和主机查找进行默认设置。

g) 在**主机查找 (MAB)** （**Host Lookup (MAB))**部分，请执行以下操作：

- 处理主机查找 - 选中此复选框以定义网络设备配置文件在主机查找时使用的协议。

  不同供应商的网络设备采用不同方式执行 MAB 身份验证。根据设备类型，为您使用的协议选中**检查密码 (Check Password)** 复选框和/或**检查呼叫站 ID 等于 MAC 地址 (Check Calling-Station-Id equals MAC Address)** 复选框。

- 通过 PAP/ASCII (Via PAP/ASCII) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的 PAP 请求作为一个主机查找请求进行检测

- 通过 CHAP (Via CHAP) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的此类请求作为一个主机查找请求进行检测

- 通过 EAP MD5 (Via EAP-MD5) - 选中启用网络设备配置文件基于 EAP 的 MD5 散列身份验证。

h) 在“权限”(Permissions)、“授权更改 (CoA)”(Change of Authorization (CoA)) 和“重定向”(Redirect) 部分输入所需的详细信息，然后点击**提交 (Submit)**。

有关如何创建自定义 NAD 配置文件的信息，请参阅支持思科身份服务引擎的网络接入设备配置文件。

步骤 3 选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**。

步骤 4 选择要启用 MAB 的设备，然后点击**编辑 (Edit)**。

步骤 5 在“网络设备”(Network Device) 页面，在**设备配置文件 (Device Profile)** 下拉列表中选择在步骤 2 中创建的网络设备配置文件。

步骤 6 点击**保存 (Save)**。

注释 对于Cisco NAD，MAB 和网络/用户身份验证使用的服务类型值不同。这样在使用Cisco NAD 时，ISE 可将 MAB 身份验证与网络身份验证区分开来。在某些非Cisco NAD 中，MAB 身份验证与网络/用户身份验证使用相同的服务类型属性值；这可能会导致您的访问策略出现安全问题。如果您在非Cisco 设备上使用 MAB，我们建议您配置其他的授权策略规则，以确保您的网络安全不受影响。例如，如果一台打印机使用了 MAB，您可以配置授权策略规则，以便于在 ACL 中将 MAB 限制在打印机协议端口。

从思科设备启用 MAB

按顺序配置以下设置从Cisco设备配置 MAB。

步骤 1 确保终端数据库中具有要进行身份验证的终端的 MAC 地址。可以添加这些终端或由分析器服务自动分析这些终端。

步骤 2 根据Cisco设备（PAP、CHAP 或 EAP-MD5）使用的 MAC 身份认证类型创建网络设备配置文件。

a) 依次选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备配置文件 (Network Device Profiles)**。

b) 点击**添加 (Add)**。

c) 输入网络设备配置文件的名称和描述。

d) 选中设备支持的协议的复选框。如果设备支持 RADIUS，请选择 RADIUS 字典与网络设备配合使用。

e) 扩展**身份验证/授权 (Authentication/Authorization)** 部分，对设备的数据流类型、属性别名和主机查找进行默认设置。

f) 在**主机查找 (MAB)** （**Host Lookup (MAB))**部分，请执行以下操作：

- 处理主机查找 - 选中此复选框以定义网络设备配置文件在主机查找时使用的协议。

  根据设备类型，为您使用的协议选中**检查密码 (Check Password)** 复选框和/或**检查呼叫站 ID 等于 MAC 地址 (Check Calling-Station-Id equals MAC Address)** 复选框。

- 通过 PAP/ASCII (Via PAP/ASCII) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的 PAP 请求作为一个主机查找请求进行检测

- 通过 CHAP (Via CHAP) - 选中该复选框可配置Cisco ISE 将网络设备配置文件中的此类请求作为一个主机查找请求进行检测

- 通过 EAP MD5 (Via EAP-MD5) - 选中启用网络设备配置文件基于 EAP 的 MD5 散列身份验证。

g) 在“权限”(Permissions)、“授权更改 (CoA)”(Change of Authorization (CoA)) 和“重定向”(Redirect) 部分输入所需的详细信息，然后点击**提交 (Submit)**。

有关如何创建自定义 NAD 配置文件的信息，请参阅支持思科身份服务引擎的网络接入设备配置文件。

步骤 3 选择**管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**。

步骤 4 选择要启用 MAB 的设备，然后点击**编辑 (Edit)**。

步骤 5 在“网络设备”(Network Device) 页面，在**设备配置文件 (Device Profile)** 下拉列表中选择在步骤 2 中创建的网络设备配置文件。

步骤 6 点击**保存 (Save)**。

ISE 社区资源

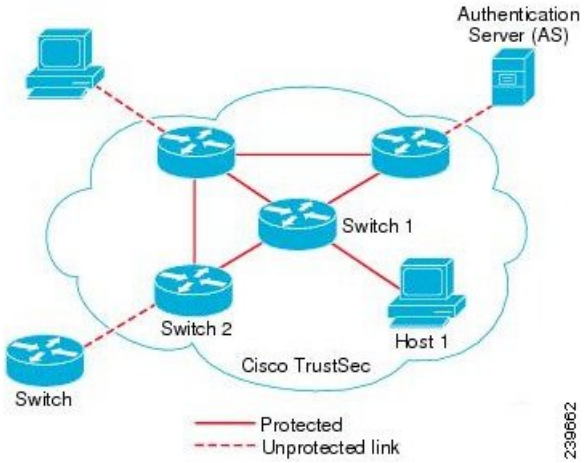
有关 IP 电话身份验证功能的信息，请参阅电话身份验证功能。

TrustSec 架构

Cisco TrustSec 解决方案可建立受信任的网络设备云以构建安全网络。Cisco TrustSec 云中的每个设备都由其相邻设备（对等体）进行身份验证。TrustSec 云中设备之间的通信由加密、消息完整性检查和数据路径重放保护机制进行保护。TrustSec 解决方案使用在身份验证期间获取的设备和用户身份信息来在数据包进入网络时给数据包进行分类或确定颜色。此数据包分类在数据包进入 TrustSec 网络时由标记数据包进行维护，从而可以正确识别数据包，以沿着数据路径应用安全性和其他策略条件。此标签也称为安全组标签 (SGT)，Cisco ISE 可通过此标签使终端设备在 SGT 上执行操作以过滤流量，从而实施访问控制策略。

下图显示 TrustSec 网络云的一个示例。

图 *7: TrustSec* 架构



ISE 社区资源

有关如何使用Cisco TrustSec 简化网络分段并提高安全性的信息，请参阅使用思科 TrustSec 简化网络分段和基于策略的软件定义分段和思科 TrustSec 提高安全性白皮书。

有关CiscoTrustSec平台支持矩阵的完整列表，请参阅CiscoTrustSec平台支持表。http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

有关适用于 TrustSec 的支持文档的完整列表，请参阅思科 TrustSec。

有关 TrustSec 社区资源的完整列表，请参阅 TrustSec 社区。

TrustSec 组件

TrustSec 的重要组件包括：

- 网络设备准入控制 (NDAC) - 在受信任网络中，在身份验证期间，TrustSec 云上的每个网络设备（例如以太网交换机）都由其对等体设备对其凭证和可信度进行验证。NDAC 使用基于 IEEE 802.1X 端口的身份验证并且将可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST) 用作其可扩展身份验证协议 (EAP) 方法。如果在 NDAC 流程中身份验证和授权成功，则系统将为 IEEE 802.1AE 加密执行安全关联协议协商。
- 终端准入控制 (EAC) - 对连接 TrustSec 云的终端用户或设备执行的身份验证流程。EAC 通常发生于访问级别交换机上。如果在 EAP 流程中身份验证和授权成功，系统将向用户或设备分配 SGT。用于身份验证和授权的 EAC 访问方法包括：
  - 基于 802.1X 端口的身份验证
  - MAC 身份验证绕行 (MAB)
  - Web 身份验证 (WebAuth)
- 安全组 (SG) - 共用访问控制策略的一组用户、终端设备和资源。SG 由Cisco ISE 中的管理员定义。当向 SGA 域添加新用户和设备时，Cisco ISE 将这些新的实体分配到相应的安全组。
- 安全组标签 (SGT) - TrustSec 服务向每个安全组分配一个唯一 16 位安全组编号，其范围为 TrustSec 域内的全局范围。交换机内安全组的数量限制为已通过身份验证的网络实体的数量。您无需手动配置安全组数量。它们是自动生成的，但是您可以选择将一系列 SGT 保留用于 IP 到 SGT 的映射。
- 安全组访问控制列表 (SGACL) - SGACL 允许您根据所分配的 SG 控制访问和权限。将权限归入角色可以简化安全策略的管理。当您添加设备时，只需分配一个或多个安全组，这些安全组就会立即获得相应权限。您可以修改安全组以引入新的权限或限制当前权限。
- 安全交换协议 (SXP) - SGT 交换协议 (SXP) 是为 TrustSec 服务开发的一种协议，将整个不具有支持 SGT 的硬件的网络设备上的 IP 到 SGT 绑定表传送至支持 SGT/SGACL 的硬件。
- 环境数据下载 - TrustSec 设备在首次联接受信任网络时从Cisco ISE 获取其环境数据。您也可以在设备上手动配置某些数据。设备必须在到期之前刷新环境数据。TrustSec 设备从Cisco ISE 获取以下环境数据：
  - 服务器列表 - 列出客户端可以用于以后的 RADIUS 请求的服务器列表（适用于身份验证和授权）
  - 设备 SG - 设备自身所属的设备组
  - 过期超时 - 控制 TrustSec 设备应该多久下载或更新一次其环境变量的时间间隔
- 身份到端口的映射 - 交换机在终端所连接的端口上定义身份以及将身份用于在Cisco ISE 服务器中查找特定 SGT 值所使用的方法。

TrustSec 术语

下表列出某些用于 TrustSec 解决方案的常用术语及其在 TrustSec 环境中的含义。

表 *15: TrustSec* 术语

术语	含义
请求方	尝试加入受信任网络的设备。
身份验证	在允许每台设备加入受信任网络之前验证设备身份的过程。
授权	根据已经过身份验证的设备身份决定请求访问受信任网络上的资源的设备的访问级别的过程。
访问控制	根据分配给每个数据包的SGT对每个数据包应用访问控制的过程。
安全通信	为保护流经受信任网络中的每条链路的数据包进行加密、完整性和数据路径重放保护的过程。
TrustSec 设备	支持 TrustSec 解决方案的任何Cisco Catalyst 6000 系列或 Cisco Nexus 7000 系列交换机。
支持 TrustSec 的设备	支持 TrustSec 的设备将具有支持 TrustSec 的硬件和软件。例如，带 Nexus 操作系统的 Nexus 7000 系列交换机。
TrustSec 种子设备	直接对Cisco ISE 服务器进行身份验证的 TrustSec 设备。此设备同时用作验证器和请求方。
入口	当数据包首次遇到支持 TrustSec 的设备时，这些数据包会被标上SGT标记。该设备已加入启用了Cisco TrustSec 解决方案的网络。进入受信任网络的这个点称为入口。
出口	当数据包通过最后一台支持 TrustSec 的设备时，这些数据包会被取消标记。该设备已加入启用了Cisco TrustSec 解决方案的网络。退出受信任网络的这个点称为出口。

TrustSec 支持的交换机和需要的组件

要设置启用Cisco TrustSec 解决方案的Cisco ISE 网络，您需要支持 TrustSec 解决方案的交换机和其他组件。除交换机外，您还需要其他组件用于基于身份的用户访问控制（使用 IEEE 802.1X 协议）。有关支持 Trustsec 的Cisco交换机平台和必要组件的完整的最新列表，请参阅启用 TrustSec 的思科基础设施。

与思科 DNA 中心的集成

Cisco ISE 是Cisco全数字化网络架构 (DNA) 的主要部分。Cisco DNA 中心可使您实现网络自动化以提供业务灵活性。集成Cisco ISE 和Cisco DNA 中心时，Cisco ISE 为Cisco DNA 中心提供终端身份验证。

将思科 DNA 中心连接到思科 ISE

请参阅《DNAC 用户指南》https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html 中有关配置Cisco DNA 中心和Cisco ISE 的要求与说明。

本部分提供有关适于Cisco DNA 中心的Cisco ISE 配置的其他信息。

- 密码：Cisco DNA 中心在连接到Cisco ISE 时使用Cisco ISE 管理员用户名和密码来验证对Cisco ISE 的访问权限。有关系统密码的详细信息，请参阅对思科 ISE 的管理访问。

  注释 在早于 2.2.1.0 的Cisco DNA 中心版本中，Cisco ISE CLI 用于执行初始集成步骤，因此Cisco ISE CLI 以及管理员用户名和密码必须相同。从Cisco DNA 中心版本 2.2.1.0 开始，不再使用Cisco ISE CLI，因此Cisco ISE CLI 以及管理员用户名和密码无需相同。

- API：Cisco DNA 中心通过调用 ISE API 配置 ISE 的某些部分。在Cisco ISE 中启用 API 访问，但不启用 CSRF。有关详细信息，请参阅启用外部 RESTful 服务 API

- pxGrid：Cisco ISE 是 pxGrid 控制器，Cisco DNA 中心是用户。Cisco ISE 和Cisco DNA 中心均监控 Trustsec (SD-Access) 内容，其中包含 SGT 和 SGACL 信息。同步Cisco ISE 与Cisco DNA 中心之间的系统时钟。Cisco ISE 使用证书连接到 pxGrid，Cisco DNA 中心将其配置为用于连接。有关Cisco ISE 中 pxGrid 的详细信息，请参阅 中的“pxGrid 节点”部分请参阅思科 pxGrid 节点。

  注释 Cisco ISE 2.4 及更高版本支持 pxGrid 2.0 和 pxGrid 1.0。虽然 pxGrid 2.0 允许Cisco ISE 部署中有最多 4 个 pxGrid 节点，但是Cisco DNA 中心目前不支持两个以上 pxGrid 节点。

- Cisco ISE IP 地址：Cisco ISE PAN 与Cisco DNA 中心之间的连接必须是直接连接。不能通过代理、负载均衡器或虚拟 IP 地址进行连接。Cisco ISE 和Cisco DNA 中心会互相配置静态地址。

  验证Cisco ISE 是否未使用代理。如果使用代理，请从代理中排除Cisco DNA 中心 IP。

  以下功能支持 IPv4 和 IPv6 IP 地址：

  - 外部 RESTful 服务 (ERS) API
  - 管理 REST API

- Secure Shell (SSH) 协议

- SXP：DNA 中心不需要 SXP。您可能希望在将Cisco ISE 连接到 DNA 托管网络时启用 SXP，以便Cisco ISE 与没有 Trustsec (SD-Access) 硬件支持的网络设备进行通信。

  注释 将 ISE 部署配置为支持 Trustsec 时，或者当 ISE 与Cisco DNA 中心集成时，请勿将 ISE 策略服务节点配置为仅 SXP。SXP 是 Trustsec 与非 Trustsec 设备之间的接口。它不与启用了 Trustsec 的网络设备通信。

- Cisco ISE 连接的证书：
  - Cisco ISE 管理员证书必须在使用者名称或 SAN 中包含Cisco ISE IP 或 FQDN。
  - SSH 密钥、ISE SSH 访问或Cisco DNA 中心与Cisco ISE 连接证书不支持 ECDSA。
  - Cisco DNA 中心上的自签名证书必须具有 cA:TRUE 的基本约束扩展（RFC5280 部分 4.2.19）。

注释 在早于 2.2.1.0 的Cisco DNA 中心版本中，需要启用 SSH。从Cisco DNA 中心版本 2.2.1.0 开始，不再使用 SSH，因此无需启用 SSH。

TrustSec 控制面板

TrustSec 控制面板是 TrustSec 网络中的一个集中式监控工具。

TrustSec 控制面板包含以下面板：

- **指标 (Metrics)**：“指标”(Metrics) Dashlet 显示与 TrustSec 网络行为有关的统计信息。
- **活动 SGT 会话 (Active SGT Sessions)**：“活动 SGT 会话”(Active SGT Sessions) Dashlet 显示网络中当前活动的 SGT 会话。“警报”(Alarms) Dashlet 显示与 TrustSec 会话相关的警报。
- **警报**
- **NAD/SGT/ACI 快速查看 (NAD / SGT/ACI Quick View)**：“快速查看” (Quick View) Dashlet 显示 NAD 和 SGT 的 TrustSec 相关信息。
- **TrustSec 会话/ NAD 活动/ACI 终端活动实时日志 (TrustSec Sessions / NAD Activity/ACI endpoint Activity Live Log)**：在“实时日志”(Live Log) Dashlet 中，点击“TrustSec 会话”(TrustSec Sessions) 链接可查看活动的 TrustSec 会话。您还可以查看有关 TrustSec 协议数据请求的信息，以及 NAD 发给Cisco ISE 的响应的信息。

指标

本节显示有关TrustSec网络行为的统计信息。您可以选择时间段（例如，过去2小时、过去2天等）和图表类型（例如，条形图、折线图、样条曲线图）。

图中显示了最新的数据条值。它还显示了相对于之前数据条的变化百分比。如果数据条值增加，则它将显示为绿色并带一个加号。如果值有所下降，则它将显示为红色并带一个减号。

将光标置于图形的数据条上，可查看该值的计算时间及其确切值，格式如下：<Value:xxxx Date/Time: xxx>

您可以查看以下指标：

SGT 会话	显示在所选时间段内创建的 SGT 会话总数。 **注释** SGT 会话是在授权流中接收 SGT 的用户会话。
正在使用的 SGT	显示在所选时间段内使用的唯一 SGT 总数。例如，如果在一个小时内有 200 个 TrustSec 会话，但在授权响应中 ISE 仅以 6 种类型的 SGT 进行响应，则图形将针对该小时显示值 6。
警报	显示在所选时间段内发生的警报和错误总数。错误以红色显示，而警报以黄色显示。
正在使用的 NAD	显示在所选时间段内参与 TrustSec 身份验证的唯一 NAD 数。

当前网络状态

控制面板的中间部分显示有关TrustSec网络当前状态的信息。在加载页面时，图中显示的值会更新，且可使用“刷新控制面板”(Refresh Dashboard) 选项刷新这些值。

活动 SGT 会话

此dashlet显示当前在网络中处于活动状态的SGT会话。您可以查看使用最多或最少的前10个SGT。X 轴显示 SGT 使用情况，Y 轴显示 SGT 的名称。

要查看 SGT 的 TrustSec 会话详细信息，请点击与该 SGT 对应的条形。与该 SGT 相关的 TrustSec 会话的详细信息显示在“实时日志”(Live Log) dashlet 中。

警报

此 dashlet 显示与 TrustSec 会话相关的警报。您可以查看以下详细信息：

- 警报严重性 - 显示一个表示警报严重性级别的图标。
  - 高 - 包括指示 TrustSec 网络中出现故障的警报（例如，设备无法刷新其 PAC）。用红色图标标记。
  - 中 - 包括指示网络设备配置错误的警告（例如，设备无法接受 CoA 消息）。用黄色标记。
  - 低 - 包括有关网络行为的一般信息和更新（例如，TrustSec 中的配置更改）。用蓝色标记。

- 警报说明
- 自上次重置此警报计数器以来发生的警报次数。
- 最后一次发生警报的时间

快速查看

“快速查看”(Quick View) 面板显示网络接入设备 (NAD) 的 TrustSec 相关信息。还可以查看 SGT 的 TrustSec 相关信息。

NAD 快速查看

在搜索框中输入您想要查看其详细信息的 TrustSec 网络设备的名称并按 **Enter**。搜索框提供自动填写功能，当用户在文本框中输入时，它可过滤设备名称并在下拉框中显示匹配的设备名称。

此 Dashlet 会显示以下信息：

- **NDG**：列出此网络设备所属的网络设备组 (NDG)。
- **IP 地址 (IP Address)**：显示网络设备的 IP 地址点击此链接可在“实时日志”(Live Logs) Dashlet 中查看 NAD 活动详细信息。
- **活动会话 (Active sessions)**：连接到此设备的活动 TrustSec 会话数。
- **PAC 有效期 (PAC expiry)**：显示 PAC 的到期日期。
- **上次策略更新时间 (Last Policy Refresh)**：显示策略的上次下载日期。
- **上次身份验证时间 (Last Authentication)**：显示此设备上次身份验证报告的时间戳。
- **活动 SGT (Active SGTs)**：列出在与此网络设备相关的活动会话中使用的 SGT。方括号中显示的数字表示当前正在使用该 SGT 的会话的数量。点击 SGT 链接，在“实时日志”(Live Log) Dashlet 中查看 TrustSec 会话的详细信息。

您可以使用“显示最新日志”(Show Latest Logs) 选项查看该设备的 NAD 活动实时日志。

SGT 快速查看

在搜索框中输入您想要查看详细信息的 SGT 的名称并按 **Enter**。

此 Dashlet 会显示以下信息：

- **值 (Value)**：显示 SGT 值（十进制和十六进制）。
- **图标 (Icon)**：显示分配给该 SGT 的图标。
- **活动会话 (Active sessions)**：列出当前正在使用该 SGT 的活动会话的数量。
- **唯一用户 (Unique users)**：列出在活动会话中持有该 SGT 的唯一用户的数量。
- **已更新的 NAD (Updated NADs)**：列出已下载用于该 SGT 的策略的 NAD 数量。

ACI 快速查看

此 Dashlet 会显示以下信息：

- **SDA SGTs**：列出Cisco ISE 发送到Cisco SD-Access 的 SGT 数量。
- **ACI EPGs**：列出Cisco ISE 从Cisco ACI 获取的 EPG 数量。
- **SDA 绑定 (SDA Bindings)**：列出Cisco ISE 发送到Cisco SD-Access 的绑定数量。
- **ACI 绑定 (ACI Bindings)**：列出Cisco ISE 从Cisco ACI 获知的绑定数量。
- **SDA VNs**：列出Cisco ISE 从Cisco SD-Access 获知的虚拟网络数量。
- **ACI VNs**：列出Cisco ISE 从Cisco ACI 获知的虚拟网络数量。
- **SDA 扩展 VN (SDA Extended VNs)**：列出从Cisco SD-Access 域发送到Cisco ACI 域的扩展虚拟网络数量。
- **SDA 租户 (SDA Tenant)**：显示Cisco SD-Access 与Cisco ISE 共享的租户的名称。
- **ACI 租户 (ACI Tenants)**：列出Cisco ACI 与Cisco SD-Access 共享的租户的数量。
- **SDA 域 ID (SDA Domain ID)**：显示Cisco SD-Access 的域 ID 编号。
- **ACI 域 ID (ACI Domain ID)**：显示Cisco ACI 的域 ID 编号。
- **对等状态 (Peering State)**：显示Cisco SD-Access 域与Cisco ACI 域之间对等关系的当前状态。

要了解有关Cisco软件定义接入（Cisco SD-Access）和Cisco以应用为中心的基础设施（Cisco ACI）的详细信息，请参阅TrustSec-思科 ACI 集成，第 144 页和思科 ACI 和思科 SD-Access 与虚拟网络感知的集成，第 147 页。

实时日志

点击 **TrustSec 会话 (TrustSec Sessions)** 链接查看活跃的 TrustSec 会话（响应中包含 SGT 的会话）。

点击 **NAD 活动 (NAD Activity)** 链接查看有关 TrustSec 协议数据请求和 NAD 对Cisco ISE 的响应的信息。

点击 **ACI 终端活动 (ACI endpoint Activity)** 链接，查看Cisco ISE 向Cisco ACI 学习的 IP-SGT 信息。

配置 TrustSec 全局设置

为了让Cisco ISE 充当 TrustSec 服务器并提供 TrustSec 服务，必须定义某些全局 TrustSec 设置。

开始之前

- 配置全局 TrustSec 设置之前，确保已定义全局 EAP-FAST 设置（依次选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **EAP-FAST 设置 (EAP-FAST Settings)**）。

可以将 Authority Identity Info Description 更改为Cisco ISE 服务器名称。此说明是用户友好字符串，描述向终端客户端发送凭证的Cisco ISE 服务器。Cisco TrustSec 架构中的客户端可以是运行 EAP-FAST 作为其 EAP 方法进行 IEEE 802.1X 身份验证的终端，也可以是执行网络设备访问控制 (NDAC) 的请求方网络设备。客户端可以在受保护的访问凭证 (PAC) 类型长度值 (TLV) 信息中发现此字符串。默认值为 Identity Services Engine。应该更改此值，以便可以在 NDAC 身份验证时在网络设备上唯一识别Cisco ISE PAC 信息。

- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 通用 TrustSec 设置 (General TrustSec Settings)**

步骤 2 在字段中输入值。有关这些字段的信息，请参阅 常规 TrustSec 设置，第 102 页

步骤 3 点击**保存 (Save)**。

下一步做什么

- 配置 TrustSec 设备，第 107 页

常规 TrustSec 设置

定义全局 TrustSec 设置，以便Cisco ISE 作为 TrustSec 服务器运行。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 常规 TrustSec 设置 (General TrustSec Settings)**。

验证 Trustsec 部署 (Verify Trustsec Deployment)

此选项可帮助验证所有网络设备上是否部署了最新的 TrustSec 策略。如果在Cisco ISE 和网络设备上配置的策略之间存在任何差异，“警报”(Alarms) Dashlet 中会显示警报，该 Dashlet 位于**工作中心 (Work Centers) > TrustSec > 控制板和主页 (Dashboard and Home) > 摘要 (Summary)** 下。TrustSec 控制板中会显示以下警报：

- 每当验证过程开始或完成时，系统都会显示带有**信息 (Info)** 图标的警报。
- 如果由于新的部署请求而取消验证过程，则会显示带有**信息 (Info)** 图标的警报。
- 如果验证过程因错误而失败，则会显示带有**警告 (Warning)** 图标的警报。例如，无法打开与网络设备的 SSH 连接，或当网络设备不可用，或当Cisco ISE 和网络设备上配置的策略之间存在任何差异。

验证部署 (Verify Deployment) 选项也可从以下窗口选择。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择：

- **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)**
- **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**

- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 源树 (Source Tree)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 目标树 (Destination Tree)

每次部署后自动验证 (Automatic Verification After Every Deploy)：如果希望Cisco ISE 在每次部署后验证所有网络设备上的更新，请选中此复选框。部署过程完成后，经过您在**部署过程后的时间 (Time after Deploy Process)** 字段中指定的时间后，验证过程开始。

部署过程后的时间 (Time After Deploy Process)：指定您希望Cisco ISE 在部署过程完成后等待多长时间，然后再开始验证过程。有效范围为 10 – 60 分钟。

如果在等待期间收到新的部署请求或正在进行其他验证，则会取消当前验证过程。

立即验证 (Verify Now)：点击此选项可立即开始验证过程。

受保护的访问凭证 (PAC)

- **隧道 PAC 生存时间 (Tunnel PAC Time to Live)**：

  指定 PAC 的到期时间。隧道 PAC 为 EAP-FAST 协议生成隧道。您可以秒、分钟、小时、天或周为单位指定时间。默认值为 90 天。以下是有效范围：

  - 1 – 157680000 秒
  - 1 – 2628000 分钟
  - 1 – 43800 小时
  - 1 – 1825 天
  - 1 – 260 周

- **进行主动 PAC 更新前所经历的时间 (Proactive PAC Update Will Occur After)**：当剩余的隧道 PAC TTL 百分比达到设定值时，Cisco ISE 会在成功身份验证后主动向客户端提供新 PAC。如果第一次成功身份验证发生在 PAC 到期之前，则服务器会启动隧道 PAC 更新。此机制会为客户端更新有效的 PAC。默认值为 10%。

安全组标签编号

- **系统将分配 SGT 编号 (System will Assign SGT Numbers)**：如果希望Cisco ISE 自动生成 SGT 编号，请选择此选项。
- **除范围内的编号外 (Except Numbers in Range)**：选择此选项可保留一系列 SGT 编号以进行手动配置。Cisco ISE 在生成 SGT 时不会使用此范围的值。
- **用户必须手动输入 SGT 编号 (User Must Enter SGT Numbers Manually)**：选择此选项可手动定义 SGT 编号。

APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)

APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)：选中此复选框，指定编号范围以用于根据从 APIC 获取的 EPG 创建的 SGT。

自动创建安全组

创建授权规则时自动创建安全组 (Auto Create Security Groups When Creating Authorization Rules)：选中此复选框可在创建授权策略规则时自动创建 SGT。

如果选中此选项，**授权策略 (Authorization Policy)** 窗口顶部会显示以下消息：`开启自动安全组创建 (Auto Security Group Creation is On)`。

系统会根据规则属性命名自动创建的 SGT。

注释 当删除相应的授权策略规则时，不会删除自动创建的 SGT。

默认情况下，此选项在全新安装或升级后会被禁用。

- **自动命名选项 (Automatic Naming Options)**：使用此选项可定义自动创建的 SGT 的命名约定。

  （必填）**名称将包括 (Name Will Include)**：选择以下选项之一：

  - **规则名称**
  - **SGT 号**
  - **规则名称 (Rule name) 和 SGT 编号 (SGT number)**

  默认选中**规则名称 (Rule name)** 选项。

  或者，可以将以下信息添加到 SGT 名称：

  - **策略集名称 (Policy Set Name)**（此选项仅在已启用**策略集 (Policy Sets)** 时可用）
  - **前缀 (Prefix)**（最多 8 个字符)
  - **后缀 (Suffix)**（最多 8 个字符)

  根据您的选择，Cisco ISE 会在**示例名称 (Example Name)** 字段中显示一个 SGT 名称示例。

  如果存在名称相同的 SGT，ISE 会在 SGT 名称上附加 *_x*，其中 *x* 是从1（如果当前名称中未使用 1）开始的第一个值。如果新名称大于 32 个字符，Cisco ISE 会截取前 32 个字符。

IP SGT 主机名静态映射

IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames)：如果使用 FQDN 和主机名，则Cisco ISE 会在部署映射和检查部署状态的同时在 PAN 和 PSN 节点中查找对应的 IP 地址。您可以使用此选项指定为 DNS 查询返回的 IP 地址创建的映射数。您可以选择以下其中一个选项：

- **为 DNS 查询返回的所有 IP 地址创建映射 (Create mappings for all IP addresses returned by a DNS query)**

- **仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射 (Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query)**

用于网络设备的 TrustSec HTTP 服务

- **启用 HTTP 服务 (Enable HTTP Service)**：使用 HTTP 通过端口 9063 将 Trustsec 数据传输到网络设备。
- **在审核中包括整个响应负载正文 (Include entire response payload body in Audit)**：启用此选项可在审核日志中显示整个 TrustSec HTTP 响应负载正文。此选项可能会显着降低性能。当禁用此选项时，仅会记录 HTTP 信头、状态和身份验证信息。

相关主题

TrustSec 架构，第 94 页
TrustSec 组件，第 95 页
配置 TrustSec 全局设置，第 101 页

配置 TrustSec 矩阵

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 依次选择**工作站 (Work Centers) > TrustSec >设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

步骤 3 在“TrustSec 矩阵设置”(TrustSec Matrix Settings) 页面输入所需的详细信息。

步骤 4 点击**保存 (Save)**。

TrustSec 表格设置

下表介绍“TrustSec 矩阵设置”(TrustSec Matrix Settings) 窗口上的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

表 *16:* 配置 *TrustSec* 表格设置

字段名称	使用指南
允许多个 SGACL (Allow Multiple SGACLs)	如果要在一个单元格中允许多个 SGACL 请选中此复选框。如果未选择此选项，Cisco ISE 只允许每个单元格一个 SGACL。 默认情况下，此选项在全新安装时禁用。 升级后，Cisco ISE 将扫描出口单元格，因此，如果识别到至少一个被分配多个 SGACL 的单元格，将允许管理员在单元格中添加多个 SGACL。否则，它仅允许每个单元格一个 SGACL。 **注释** 在禁用的多个 SGACL 之前，您必须编辑包含多个 SGACL 的单元格仅包含一个 SGACL。
允许监控 (Allow Monitoring)	选中此复选框可启用对表格中所有单元格的监控。如果禁用监控，“监控全部”(Monitor All) 图标会灰显，“编辑单元格”(Edit Cell) 对话中的“监控”(Monitor) 选项被禁用。 默认情况下，监控在全新安装禁用。 **注释** 在禁用表格级别的监控之前，必须禁用对当前接受监控的单元格的监控。
显示 SGT 数量 (Show SGT Numbers)	使用此选项可显示或隐藏表格单元格中 SGT 值（十进制和十六进制）。 默认情况下，SGT 值在单元格中显示。
外观设置 (Appearance Settings)	可提供以下选项： • **自定义设置 (Custom settings)**：最初显示默认主题（有颜色无图案）。您可以自主设置颜色和图案。 • **默认设置 (Default settings)**：预定义的有颜色无图案列表（不可编辑）。 • **辅助功能设置 (Accessibility settings)**：预定义的有颜色有图案列表（不可编辑）。

字段名称	使用指南
颜色/图案 (Color/Pattern)	要使表格更易读，可根据单元格颜色将颜色和图案应用于表格单元格。 提供以下显示类型： • 允许 IP/允许 IP 日志 (Permit IP/Permit IP Log)：单元格内已配置 • 拒绝 IP/拒绝 IP 日志 (Deny IP/Deny IP Log)：单元格内已配置 • SGACL：用于单元格内已配置的 SGACL • 允许 IP/允许 IP日志（沿用）(Permit IP/Permit IP Log (Inherited))：从（非已配置单元格）默认策略中获取 • 拒绝 IP/拒绝 IP 日志（沿用）(Deny IP/Deny IP Log (Inherited))：从（非已配置单元格）默认策略中获取 • SGACL（沿用）(SGACLs (Inherited))：从（非已配置单元格）默认策略中获取

相关主题

出口策略，第 118 页
矩阵视图，第 119 页
配置 TrustSec 矩阵，第 105 页

配置 TrustSec 设备

为了让Cisco ISE 处理来自启用 TrustSec 的设备的请求，您必须在Cisco ISE 中定义这些启用 TrustSec 的设备。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 网络设备 (Network Devices)**

步骤 2 点击**添加 (Add)**。

步骤 3 在 **Network Devices** 部分中输入所需信息。

步骤 4 选中 **Advanced Trustsec Settings** 复选框以配置支持 Trustsec 的设备。

步骤 5 点击**提交 (Submit)**。

OOB TrustSec PAC

所有 TrustSec 网络设备都将 TrustSec PAC 视为 EAP-FAST 协议的一部分。安全 RADIUS 协议也使用此 TrustSec PAC，其中 RADIUS 共享密钥是根据 PAC 携带的参数推导而来。这些参数中的 Initiator-ID 参数包含 TrustSec 网络设备身份，即设备 ID。

如果使用 TrustSec PAC 识别设备，并且在Cisco ISE 上为该设备配置的设备 ID 和 PAC 上的 Initiator-ID 之间不匹配，则身份验证失败。

有些 TrustSec 设备（例如Cisco防火墙 ASA）不支持 EAP-FAST 协议。因此，Cisco ISE 无法通过 EAP-FAST 使用 TrustSec PAC 调配这些设备。系统会在Cisco ISE 上生成 TrustSec PAC 并且需要手动将其复制到设备上，所以这又称为带外 (OOB) TrustSec PAC 生成。

当从Cisco ISE 生成 PAC 时，系统会生成使用加密密钥加密的 PAC 文件。

本节介绍以下主题：

从设置屏幕生成 TrustSec PAC

可以从设置屏幕生成 TrustSec PAC。

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

步骤 2 从左侧的 Settings 导航窗格中，点击 **Protocols**。

步骤 3 选择 **EAP-FAST** > **生成 PAC (Generate PAC)**。

步骤 4 生成 TrustSec PAC。

从网络设备屏幕生成 TrustSec PAC

您可以从网络设备 屏幕生成 TrustSec PAC。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **TrustSec** > **组件 (Components)** > **网络设备 (Network Devices)**

步骤 2 点击**添加 (Add)**。您还可以从网络设备 导航窗格的操作图标上点击 **添加新设备 (Add new device)**。

步骤 3 如果要添加新设备，请提供设备名称。

步骤 4 选中**TrustSec 高级设置 (Advanced TrustSec Settings)** 复选框以配置 TrustSec 设备。

步骤 5 在**带外 (OOB) TrustSec PAC (Out of Band (OOB) TrustSec PAC)** 子部分下，点击**生成 PAC (Generate PAC)**。

步骤 6 提供以下详细信息：

- PAC Time to Live - 输入值（单位：天、周、月或年）。默认情况下，该值为一年。最小值为一天，最大值为十年。
- Encryption Key - 输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。

加密密钥用于对生成的文件中的 PAC 进行加密。此密钥也用于解密该设备上的 PAC 文件。因此，建议管理员保存加密密钥以供日后使用。

“身份”(Identity) 字段指定 TrustSec 网络设备的设备 ID，并且 EAP-FAST 协议会提供发起方 ID。如果此处输入的身份字符串与“网络设备创建”(Network Device creation) 页面中 TrustSec 部分下定义的设备 ID 不匹配，那么身份验证将会失败。

根据 PAC 存活时间 (PAC Time to Live) 计算到期日期。

步骤 7 点击**生成 PAC (Generate PAC)**。

从网络设备 列表屏幕生成 TrustSec PAC

您可以从网络设备 列表屏幕生成 TrustSec PAC。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 网络设备 (Network Devices)**

步骤 2 点击**网络设备 (Network Devices)**。

步骤 3 选中要为其生成 TrustSec PAC 的设备旁边的复选框，然后点击**生成 PAC (Generate PAC)**。

步骤 4 在字段中提供详细信息。

步骤 5 点击**生成 PAC (Generate PAC)**。

按钮

出口策略中的 Push 选项可以启动 CoA 通知，告知 Trustsec 设备立即从Cisco ISE 请求关于出口策略中的配置更改的更新。

配置 TrustSec AAA 服务器

可以在 AAA 服务器列表中配置启用了 Trustsec 的Cisco ISE 服务器列表。TrustSec 设备向其中任意服务器进行身份验证。点击“推送”(Push)时，此列表中的新服务器将下载到TrustSec 设备。当TrustSec 设备尝试进行身份验证时，它会从此列表中选择任意Cisco ISE 服务器。如果第一台服务器关闭或繁忙，TrustSec 设备可以向此列表中的任何其他服务器自行进行身份验证。默认情况下，主要Cisco ISE 服务器是 TrustSec AAA 服务器。建议您配置更多Cisco ISE 服务器，以获得更可靠的 Trustsec 环境。

此页面列出了部署中您已配置为 TrustSec AAA 服务器的Cisco ISE 服务器。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > TrustSec AAA 服务器 (TrustSec AAA Servers)**

步骤 2 点击**添加 (Add)**。

步骤 3 按如下所述输入值：

- “名称”(Name) - 要分配至此 AAA 服务器列表中的Cisco ISE 服务器的名称。此名称可与Cisco ISE 服务器的主机名不同。
- 说明 - 可选说明。
- IP - 您正添加到 AAA 服务器列表的Cisco ISE 服务器的 IP 地址。
- “端口”(Port) - TrustSec 设备与服务器之间进行通信所在的端口。默认值为 1812。

步骤 4 点击**推送**。

下一步做什么

配置安全组。

TrustSec HTTPS 服务器

默认情况下，Cisco ISE 使用 RADIUS 在Cisco ISE 和 Trustsec NAD 之间交换 Trustsec 环境数据。您可以将Cisco ISE 配置为使用 HTTPS，它比 RADIUS 更快、更可靠。Cisco ISE 使用 REST API 实施 HTTP 传输。

HTTPS 传输要求：

- 端口 9603 必须在 HTTPS 服务器和 Trustsec 网络设备之间开放。
- 连接到 PSN 的每个网络设备上的 HTTPS 服务器凭证必须是唯一的。
- Cisco交换机运行 16.12.2、17.1.1 或更高版本。

要配置 HTTPS 传输，请执行以下操作：

1. 在每个网络设备上，启用 HTTP 文件传输，并要求凭证。
2. 在Cisco ISE 中，在**常规 Trustsec 设置 (General Trustsec Settings)** 中启用**网络设备的 Trustsec REST API 服务 (Trustsec REST API Service for Network Devices)**。
3. 在Cisco ISE 中，编辑每个 PSN 的网络设备定义，选中**启用 HTTP REST API (Enable HTTP REST API)** 并输入网络设备的 HTTP 服务器的凭证。
4. 在Cisco ISE 中，将该网络设备作为 Trustsec HTTPs 服务器添加到 **Trustsec > 组件 (Components)** 下。

注释 如果仅为 HTTPS 配置一个节点，则未为 HTTPS 配置的 Trustsec 服务器不会显示在 Trustsec 服务器列表中。您必须在 HTTPS 部署中配置所有其他启用 Trustsec 的节点。如果未为 HTTPS 配置 PSN，则使用 RADIUS，并且所有Cisco ISE 都会列出此 Trustsec 部署中的所有 PSN 节点。

配置完成后，Cisco ISE 会在 **Trustsec > 网络设备 (Network Devices)** 下的 TrustSec 环境数据中返回已配置服务器的列表。

调试

在调试中启用 ERS。此设置记录所有 ERS 流量。请勿将此设置保持启用状态超过 30 分钟，以避免日志文件过载。

您可以通过选中 **Trustsec > 设置 (Settings) > 常规 TrustSec 设置 (General Trustsec Settings)** 上**网络设备的 Trustsec REST API 服务 (Trustsec REST API Service for Network Devices)** 下的**包括请求负载正文 (Include request payload body)**，启用其他审核信息。常规 TrustSec 设置

安全组配置

安全组 (SG) 或安全组标签 (SGT) 是在 TrustSec 策略配置中用到的元素。在可信任的网络中移动时，SGT连接到数据包。这些数据包在进入可信任的网络（入口）时被标记，离开可信任的网络（出口）时被取消标记。

SGT 按顺序生成，但您可以选择为 IP 到 SGT 映射保留一些 SGT。生成 SGT 时，Cisco ISE 跳过保留的编号。

TrustSec 服务使用这些 SGT 在出口实施 TrustSec 策略。

您可以在 Admin 门户从以下页面配置安全组：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)**
- 直接从出口策略页面： **配置 (Configure)** > **创建新安全组 (Create New Security Group)**。

更新多个 SGT 后，点击 **Push** 按钮，发起环境 CoA 通知。此环境 CoA 通知转至全部 TrustSec 网络设备，强迫它们开始策略/数据刷新请求。

在思科 ISE 中管理安全组

必备条件

要创建、编辑或删除安全组，您必须是超级管理员或系统管理员。

添加安全组

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components)> 安全组 (Security Groups)**。
2. 点击**添加 (Add)** 以添加新安全组。
3. 为新安全组输入名称和说明（可选）。
4. 如果要将此 SGT 传播至 Cisco ACI，请选中**传播至 ACI (Propagate to ACI)** 复选框。只有当与此 SGT 相关的 SXP 映射属于在 Cisco ACI“设置”(Settings) 页面中选择的同一 VPN 时，它们才会传播至 Cisco ACI。

   默认情况下该选项处于禁用状态。
5. 输入 Tag Value。标签值可以设置为手动输入或自动生成。您还可以为 SGT 保留范围。您可以从以下位置对其进行配置：“通用 TrustSec 设置”(General TrustSec Settings) 页面（**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 通用 TrustSec 设置 (General TrustSec Settings)**）。
6. 点击**保存 (Save)**。

删除安全组

您无法删除源或目标仍在使用的安全组。这包括映射到Cisco ISE 中的功能的默认组：

- 自带设备
- 访客
- TrustSec 设备
- 未知

将安全组导入思科 ISE

您可以使用逗号分隔值 (CSV) 文件将安全组导入Cisco ISE 节点。您必须在更新模板之后才能将安全组导入Cisco ISE。您不能同时运行同一资源类型的导入。例如，您无法同时导入来自两个不同导入文件的安全组。

您可以从管理员门户下载 CSV 模板，在模板中输入您的安全组详细信息，并将该目标保存为 CSV 文件，接着您就可以将此文件导入回Cisco ISE。

在导入安全组的过程中，您可以在Cisco ISE 遇到第一个错误时停止导入过程。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components)> 安全组 (Security Groups)**。

步骤 2 点击**导入 (Import)**。

步骤 3 点击**浏览 (Browse)** 从正在运行客户端浏览器的系统选择 CSV 文件。

步骤 4 选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。

步骤 5 点击**导入 (Import)**。

从思科 ISE 导出安全组

您可以将Cisco ISE 中配置的安全组导出为 CSV 文件，您可以使用此文件将这些安全组导入到其他 Cisco ISE 节点中。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**。

步骤 2 点击**导出 (Export)**。

步骤 3 要导出安全组，您可以执行下述操作中的一项：

- 选中要导出的组旁的复选框，然后选择 **导出 (Export) > 导出所选 (Export Selected)**。
- 选择 **导出 (Export) > 全部导出 (Export All)**以导出所有定义的安全组。

步骤 4 将 export.csv 文件保存到您的本地硬盘中。

添加 IP SGT 静态映射

您可以使用 IP-SGT 静态映射在 TrustSec 设备和 SXP 域上以统一的方式部署映射。当创建新的 IP-SGT 静态映射时，您可以指定要部署此映射的 SXP 域和设备。也可以将 IP - SGT 映射关联到一个映射组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在显示的**新 (New)** 区域中，从下拉列表中选择 **IP 地址 (IP Address)** 或**主机名 (Hostname)**，并在其旁边的字段中输入相应的值。

在后续步骤的**单独映射到 SGT (Map to SGT individually)** 选项中，可以指定要映射到的 SXP 域。但是，如果在此步骤中选择**主机名 (Hostname)**，则无法访问**发送到 SXP 域 (Send to SXP Domain)** 字段。要在下一步中添加 SXP 域，必须在此处选择 **IP 地址 (IP Address)**。

步骤 4 如果要使用现有映射组，点击**添加至映射组 (Add to a Mapping Group)**，并从**映射组 (Mapping Group)** 选择所需的组。

如果要将此 IP 地址/主机名单独映射到 SGT，请点击**单独映射到 SGT (Map to SGT Individually)** 并执行以下操作：

- 从 SGT 下拉列表中选择一个 SGT。
- 从下拉列表中选择用于映射的虚拟网络。
- 选择须部署映射的 SXP VPN 组。

- 指定要部署此映射的设备。您可以在所有 Trustsec 设备、选定的网络设备组或选定的网络设备上部署该映射。

步骤 5 点击**保存 (Save)**。

部署 IP SGT 静态映射

添加映射后，使用**部署 (Deploy)** 选项在目标网络设备上部署映射。即使您之前保存了这些映射，也必须明确地执行此操作。点击**检查状态 (Check Status)** 检查设备的配置状态。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**

步骤 2 选中要部署的映射旁边的复选框。如果要部署所有映射，请选中顶部的复选框。

步骤 3 点击 **Deploy**（部署）。

所有 TrustSec 设备都列在**部署 IP SGT 静态映射 (Deploy IP SGT Static Mapping)** 窗口中。

步骤 4 选中所选映射必须部署到的设备或设备组旁边的复选框。

- 如果要选择所有设备，请选中顶部的复选框。
- 使用过滤选项搜索特定的设备。
- 如果不选择任何设备，则所选映射将部署在所有 TrustSec 设备上。
- 选择要部署新映射的设备时，ISE 会选择将受新映射影响的**所有**设备。

步骤 5 点击 **Deploy**（部署）。部署按钮会更新受新映射影响的所有设备上的映射。

部署状态 (Deployment Status) 窗口显示设备更新顺序以及由于错误或设备无法访问而未更新的设备。部署完成后，窗口会显示已成功更新的设备总数和未更新的设备数量。

使用 **IP SGT 静态映射 (IP SGT Static Mapping)** 页面中的**检查状态 (Check Status)** 选项检查是否为特定设备的同一 IP 地址分配了不同的 SGT。您可以使用此选项查找映射冲突的设备、映射到多个 SGT 的 IP 地址以及分配到同一 IP 地址的 SGT。即使在部署中使用了设备组、FQDN、主机名或 IPv6 地址，也可以使用**检查状态 (Check Status)** 选项。在部署这些映射之前，必须删除冲突的映射或修改部署范围。

IPv6 地址可用于 IP SGT 静态映射。这些映射可以使用 SSH 或 SXP 传播到特定网络设备或网络设备组。

如果使用 FQDN 和主机名，Cisco ISE 会在部署映射和检查部署状态时查找 PAN 和 PSN 节点中对应的 IP 地址。

使用**常规 TrustSec 设置 (General TrustSec Settings)** 窗口中的 **IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames)** 选项可指定为 DNS 查询返回的 IP 地址创建的映射数。选择以下选项之一：

- 为 DNS 查询返回的所有 IP 地址创建映射。
- 仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射

将 IP SGT 静态映射导入到思科 ISE

您可以使用 CSV 文件导入 IP SGT 映射。

您还可以从管理门户下载 CSV 模板，输入您的映射详细信息，将该模板另存为 CSV 文件，然后将其导回Cisco ISE。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**

步骤 2 点击**导入 (Import)**。

步骤 3 点击**浏览 (Browse)** 从正在运行客户端浏览器的系统选择 CSV 文件。

步骤 4 点击**上传**。

从思科 ISE 导出 IP SGT 静态映射

您可以 CSV 文件的形式导出 IP SGT 映射。您可以使用此文件将这些映射导入到另一个Cisco ISE 节点。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**。

步骤 2 执行以下操作之一：

- 选中要导出的映射旁的复选框，然后选择**导出 (Export) > 已选择 (Selected)**。
- 选择**导出 (Export) > 所有 (All)** 导出所有映射。

步骤 3 将 mappings.csv 文件保存到您的本地硬盘中。

添加 SGT 映射组

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping) > 管理组 (Manage Groups)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入映射组的名称和说明。

步骤 4 执行以下操作：

- 从 **SGT** 下拉列表中选择一个 SGT。
- 从下拉列表中选择映射的虚拟网络。
- 选择映射必须在其之上部署的 SXP VPN 组。
- 指定要部署映射的设备。您可以在所有 Trustsec 设备、选定的网络设备组或选定的网络设备上部署该映射。

步骤 5 点击**保存 (Save)**。

您可以将 IP SGT 映射从一个映射组移至到另一个映射组。

您还可以更新或删除映射和映射组。要更新一个映射或映射组，请选中要更新的映射或映射组旁边的复选框，然后点击**编辑 (Edit)**。要删除映射或映射组，请选中要删除的映射或映射组旁边的复选框，然后点击**垃圾 (Trash) > 选定 (Selected)**。当删除映射组时，该组内的 IP SGT 映射也会删除。

添加安全组访问控制列表

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)**。

步骤 2 添加**添加 (Add)** 创建新安全组 ACL。

步骤 3 输入以下信息：

- Name - SGACL 的名称
- 说明 - SGACL 的可选说明
- IP Version - 此 SGACL 支持的 IP 版本：
  - IPv4 - 支持 IP 版本 4 (IPv4)
  - IPv6 - 支持 IP 版本 6 (IPv6)
  - Agnostic - 同时支持 IPv4 和 IPv6
- Security Group ACL Content - 访问控制列表 (ACL) 命令。例如：

  permit icmp

  deny ip

在ISE中未检查SGACL输入的语法。确保使用正确的语法，以便交换机、路由器和接入点可以正确无误地应用它们。默认策略可以配置为 **permit IP**、**permit ip log**、**deny ip** 或 **deny ip log**。TrustSec 网络设备将默认策略附加到特定信元策略的末尾。

以下是两个指导性的 SGACL 示例。两者都包含一个 final catch all 规则。第一个拒绝为 final catch all 规则，第二个则允许。

Permit_Web_SGACL

```
permit tcp dst eq 80 permit tcp dst eq 443 deny ip
```

Deny_JumpHost_Protocols

```
deny tcp dst eq 23 deny tcp dst eq 23 deny tcp dst eq 3389 permit ip
```

下表列出适用于 IOS、IOS XE 和 NS-OS 操作系统的 SGACL 语法。

SGACL CLI 和 **ACE**	**IOS**、**IOS XE** 和 **NX-OS** 通用的语法
config acl	deny, exit, no, permit
deny permit	ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp
deny tcp deny tcp src deny tcp dst	dst, log, src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst, log, src
deny tcp dst eq www deny tcp src eq www	range 0 65535

注释 某些Cisco交换机不允许使用连字符。所以 `permit dst eq 32767-65535` 无效。请使用 `permit dst eq range 32767 65535`。

步骤 4 点击**推送**。

“推送”(Push) 选项可启动 CoA 通知，告知 Trustsec 设备立即向Cisco ISE 请求关于配置更改的更新。

注释 Cisco ISE 具有以下预定义的 SGACL：Permit IP、Permit IP Log、Deny IP 和 Deny IP Log。您可以使用这些 SGACL 通过 GUI 或 ERS API 配置 TrustSec 矩阵。虽然这些 SGACL 未在 GUI 的“安全组 ACL”(Security Group ACLs) 列表页面中列出，但当您使用 ERS API 列出可用的 SGACL（ERS getAll 调用）时，这些 SGACL 将列出。

出口策略

出口表列出已保留和未保留的源和目标 SGT。此页还允许您过滤出口表以查看特定策略并保存这些预设过滤器。当源 SGT 尝试到达目标 SGT时，基于出口策略中定义的 TrustSec 策略，支持 TrustSec 的设备会执行 SGACL。Cisco ISE 创建并调配策略。

SGT 和 SGACL 是创建 TrustSec 策略的基础，在您创建 SGT 和 SGACL 后，通过将 SGACL 分配至源和目标 SGT，您就可以在二者之间建立起关系。

每个源 SGT 到目标 SGT 的组合即为出口策略中的一个信元。

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**

有三种方式查看出口策略：

- 源树视图
- 目标树视图
- 矩阵视图

源树视图

源树视图以折叠状态列出源 SGT 紧凑而且组织有序的视图。您可以展开任意源 SGT 以查看列出与所选源 SGT 相关的所有信息的内部表。该视图仅显示映射至目标 SGT 的源 SGT。如果您展开具体源 SGT，其将在表中列出映射至此源 SGT 的所有目标 SGT 和相应的策略 (SGACL)。

您会在某些字段旁边看到三个点 (...)。这表示此单元格包含更多信息。您可以将光标放在这三个点上以在快速视图弹出窗口中查看其余信息。当您将光标放在 SGT 名称或 SGACL 名称上时，系统会打开一个快速查看弹出窗口，显示该具体 SGT 或 SGACL 的内容。

目标树视图

目标树视图以折叠状态列出目标 SGT 的精简和组织视图。可以展开任意目标 SGT，以查看列出所有与该选定目标 SGT 相关的信息的内部表。此视图仅显示映射到源 SGT 的目标 SGT。如果展开特定目标 SGT，该 SGT 会在表中列出映射到此目标 SGT 的所有源 SGT，以及对应的策略 (SGACL)。

您会在某些字段旁边看到三个点(...)。这表示此单元格包含更多信息。您可以将光标放在这三个点上以在快速视图弹出窗口中查看其余信息。当您将光标放在 SGT 名称或 SGACL 名称上时，系统会打开一个快速查看弹出窗口，显示该具体 SGT 或 SGACL 的内容。

矩阵视图

出口策略的矩阵视图与电子表格类似。它包含两个轴：

- 源轴 - 此垂直轴列出所有源 SGT。
- 目标轴 - 此水平轴列出所有目标 SGT。

源 SGT 到目标 SGT 的映射以单元格表示。如果某个单元格包含数据，则表示对应的源 SGT 和目标 SGT 之间有一个映射。此矩阵视图中有两类单元格：

- 有映射的单元格 - 源和目标 SGT 对与一组有序的 SGACL 关联并且具有指定的状态。
- 无映射的单元格 - 源和目标 SGT 对不与任何 SGACL 关联并且不具有指定的状态。

出口策略单元格显示源 SGT、目标 SGT 和在 SGACL 下作为单独列表的 Final Catch All Rule，以逗号隔开。如果 Final Catch All Rule 设置为 None，则不显示。矩阵中空单元格表示无映射的单元格。

在出口策略矩阵视图中，您可以滚动浏览矩阵以查看所需单元格集。浏览器不会一次性加载全部矩阵数据。浏览器会请求服务器加载属于您所滚动浏览区域的数据。这样可以防止内存溢出和性能问题。

您可使用**视图 (View)** 下拉列表中的以下选项更改表格视图。

- 带 SGACL 名称压缩 - 如果选择此选项，空单元格会被隐藏，且单元格中显示 SGACL 名称。
- 不带 SGACL 名称压缩 - 空单元格会被隐藏，且单元格中不显示 SGACL 名称。当您要查看更多表格单元格和使用颜色、图案和图标（单元格状态）区分单元格时，此视图非常有用。
- 带 SGACL 名称全屏 - 如果选择此选项，左侧与上面的菜单会被隐藏，且单元格中显示 SGACL 名称。
- 不带 SGACL 名称全屏 - 选中此选项时，表格以全屏模式显示，且单元格中不显示 SGACL 名称。

ISE 允许您创建、命名并保存自定义视图。要创建自定义视图，请选择**显示 (Show) > 创建自定义视图 (Create Custom View)**。您还可以更新视图标准或删除未使用的视图。

此表格视图的 GUI 元素与源视图及目标视图的相同。但是，它还包括以下其他元素：

矩阵维度

通过 Matrix 视图中的 **Dimension** 下拉列表，可以设置矩阵的维度。

导入/导出矩阵

使用**导入 (Import)** 和**导出 (Export)** 按钮，您可以导入或导出矩阵。

创建自定义视图

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在矩阵视图 (Matrix View) 页面，从**显示 (Show)** 下拉列表中选择**创建自定义视图 (Create Custom View)** 选项。

步骤 2 在**编辑视图 (Edit View)** 对话框中，输入以下详细信息：

- “视图名称”(View Name) - 输入自定义视图的名称。
- “源安全组”(Source Security Groups) - 将要纳入自定义视图的 SGT 移至“显示”(Show) 转发框。
- “显示与目标相关”(Show Relevant for Destination) - 如果要覆盖您在“源安全组显示”(Source Security Group Show) 转发框中的选择，并复制“目标安全组隐藏”(Destination Security Group Hide) 转发框中的所有条目，选中此复选框。如果条目超过 200 个，将不能对数据进行复制，并且会显示警告消息。
- “目标安全组”(Destination Security Groups) - 将要纳入自定义视图的 SGT 移至“显示”(Show) 转发框。
- “显示与源相关”(Show Relevant for Source) - 如果要覆盖您在“目标安全组显示”(Destination Security Group Show) 转发框中的选择，并复制“源安全组隐藏”(Source Security Group Hide) 转发框中的所有条目，选中此复选框。
- “通过…排序矩阵”(Sort Matrix By) - 您可以选择以下其中一个选项：
  - “手动顺序”(Manual Order)
  - “标签号”(Tag Number)
  - “SGT 名称”(SGT Name)

步骤 3 点击**保存 (Save)**。

矩阵操作

通过矩阵进行导航

您可以通过矩阵进行导航，方法是使用光标拖曳矩阵内容区域，或者使用水平和垂直滚动条。您可以点击并按住某个单元格，沿任何方向拖曳该单元格以及整个矩阵内容。源栏和目标栏随单元格一起移动。选中某个单元格时，矩阵视图突出显示该单元格以及相应的行（源 SGT）和列（目标 SGT）。选定单元格的坐标（源 SGT 和目标 SGT）显示在矩阵内容区域的下方。

选中矩阵中的单元格

要选中矩阵视图中的某个单元格，请点击该单元格。选定的单元格会显示不同的颜色，并且源 SGT 和目标 SGT 会突出显示。要取消选中某个单元格，只需再次点击该单元格或者选中另一个单元格即可。不允许在矩阵视图中选中多个单元格。双击单元格以编辑单元格的配置。

从出口策略配置 SGACL

您可以直接从“出口策略”(Egress Policy) 页面创建安全组 ACL。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**。

步骤 2 从“源或目标树视图”(Source or Destination Tree View) 页面，选择**配置 (Configure) > 创建新的安全组 ACL (Create New Security Group ACL)**。

步骤 3 输入所需的详细信息，并点击**提交 (Submit)**。

配置工作进程设置

开始之前

要执行以下任务，您必须是超级管理员。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 工作流程设置 (Work Process Settings)**。

步骤 2 选择以下选项之一：

- 单个矩阵 (Single Matrix) - 如果要仅为 TrustSec 网络中的所有设备创建一个策略矩阵，请选择此选项。
- 多个矩阵 (Multiple Matrices) - 允许您为不同场景创建多个策略矩阵。您可以使用这些矩阵将不同的策略部署到不同的网络设备。

  注释 矩阵是独立的，并且每个网络设备只能分配给一个矩阵。

- 具有批准进程的生产和暂存矩阵 (Production and Staging Matrices with Approval Process) - 如果要启用工作流模式，请选择此选项。选择分配给编辑和审批人角色的用户。您可以仅从策略管理员和超级管理员组中选择用户。用户不能同时分配给编辑和审批人角色。

  对于已分配给编辑和审批人角色的用户，确保其电子邮件地址已配置，否则有关工作流程进程的电子邮件通知不会发送给这些用户。

  启用工作流模式后，分配到编辑器角色的用户可以创建暂存矩阵，选择要在其上部署暂存策略的设备，并将暂存策略提交给批准人以供批准。指定为审批人角色的用户可以审核暂存策略，并批准或拒绝请求。暂存策略只有经审批人审核并批准后，才可以在选择的网络设备上进行部署。

步骤 3 如果要创建 DEFCON 矩阵，请选中**使用 DEFCONS (Use DEFCONS)** 复选框。

DEFCON 矩阵是备用策略矩阵，可以在出现网络安全漏洞时轻松部署。

您可以创建以下严重性级别的 DEFCON 矩阵：Critical、Severe、Substantial 和 Moderate。

当激活 DEFCON 矩阵时，相应的 DEFCON 策略将立即部署在所有 TrustSec 网络设备上。您可以使用禁用 (Deactivate) 选项从网络设备中删除 DEFCON 策略。

步骤 4 点击**保存 (Save)**。

矩阵列表页面

TrustSec 策略矩阵和 DEFCON 矩阵列于矩阵列表 (Matrices Listing) 页面中。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵列表 (Matrices List)**。您还可以查看分配给每个矩阵的设备数量。

注释 当启用单个矩阵模式并禁用 DEFCON 矩阵选项时，不会显示“矩阵列表”(Matrices Listing) 页面。

您可以在矩阵列表 (Matrices Listing) 页面执行以下操作：

- 添加新矩阵
- 编辑现有矩阵
- 删除矩阵
- 复制现有矩阵
- 将 NAD 分配到矩阵

通过使用分配 NAD (Assign NAD) 选项，可以将 NAD 分配到矩阵。为此：

1. 在“分配网络设备”(Assign Network Devices) 窗口中，选择要分配到矩阵的网络设备。还可以使用过滤器选项选择网络设备。
2. 从矩阵下拉列表中选择矩阵。所有现有矩阵和默认矩阵均列于此下拉列表中。

在向矩阵分配设备后，点击“推送”(Push) 向相关网络设备通知 TrustSec 配置更改。

在对矩阵列表 (Matrices Listing) 页面进行操作时，请注意以下问题：

- 您无法编辑、删除或重命名默认矩阵。
- 在创建新的矩阵时，您可以从空白矩阵开始，也可以从复制现有矩阵的策略开始。
- 如果删除矩阵，分配给该矩阵的 NAD 会自动移动到默认矩阵。
- 当您复制现有矩阵时，系统将创建矩阵副本，但不会自动将设备分配给此副本矩阵。
- 在多矩阵模式下，所有设备将在初始阶段分配到默认矩阵。
- 在多矩阵模式下，某些 SGACL 可能在矩阵之间共享。在这种情况下，更改 SGACL 内容将影响一个单元格中包含此 SGACL 的所有矩阵。
- 如果正在进行暂存，则无法启用多矩阵。
- 当您从多矩阵模式迁移到单个矩阵模式时，所有 NAD 将自动分配到默认矩阵。

- 如果当前已激活某个 DEFCON 矩阵活动，则无法删除该矩阵。

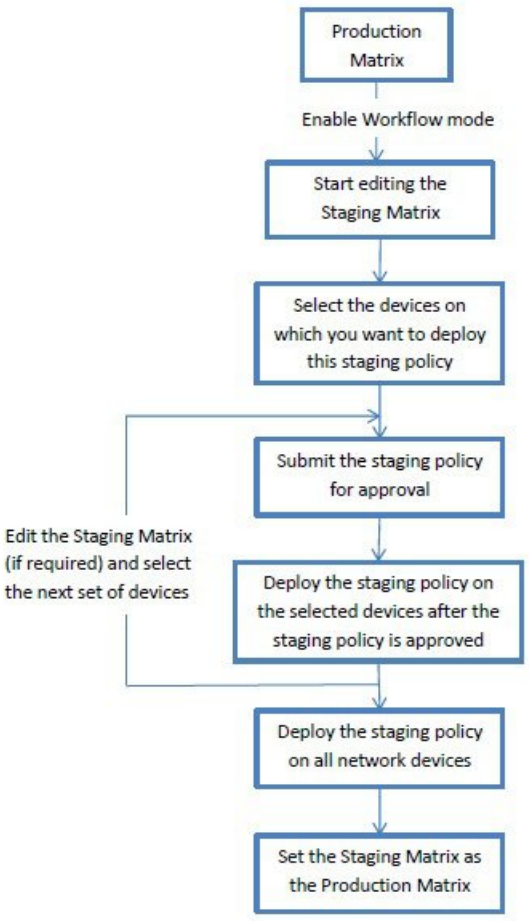
TrustSec 表格工作流过程

通过“表格工作流”(Matrix Workflow) 功能，您可以在所有网络设备上部署策略之前，使用该表格的草稿版（称为暂存表格）在一组有限的设备上测试该新策略。您可以提交暂存策略以供批准，并在获得批准后在选择的网络设备上部署该暂存策略。此功能可帮助您在有限数量的设备上部署新策略，检查是否工作正常，并在需要的时候做出更改。您可以继续在下一组设备或所有设备上部署该策略。当在所有的网络设备上部署暂存策略时，暂存表格可设置为新的生产表格。

启用工作流模式时，指定为编辑人角色的用户可以创建暂存表格，以及编辑表格中的单元格。该暂存表格是目前在 TrustSec 网络中部署的生产表格的副本。编辑人可以选择其希望部署暂存策略的设备，并提交暂存策略给审批人进行批准。指定为审批人角色的用户可以审核暂存策略，并批准或拒绝请求。暂存策略只有经审批人审核并批准后，才可以在选择的网络设备上进行部署。

下图中描述了工作流过程。

图 *8:* 表格工作流过程



超级管理员用户可以在**工作流过程设置 (Workflow Process Settings)** 页面中选择分配到编辑器和批准者角色的用户。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 设置 (Settings) > 工作流程 (Workflow Process)**。

在所选设备上部署暂存策略后，您将无法编辑 SGT 和 SGACL，但可以编辑表格中的单元格。您可以使用“配置 Delta”(Configuration Delta) 报告来跟踪生产表格和暂存表格之间的区别。您也可以点击单元格上 Delta 图标，查看暂存过程期间对单元格所做的更改。

下表介绍了工作流的不同阶段：

阶段	说明
编辑状态 (Staging in Edit)	当编辑人开始编辑暂存表格时，该表格将移至编辑状态。编辑完暂存表格后，编辑人可以选择其希望部署新的暂存策略的设备。
等待审批状态 (Staging Awaiting Approval)	编辑完表格后，编辑人提交暂存表格给审批人进行审核和批准。 提交有待审批的暂存表格时，编辑人可以添加评论，这些评论会通过邮件一起发送给审批人。 审批人可以审核暂存策略，并批准或拒绝请求。审批人还可以查看所选网络设备和配置 Delta 报告。在批准或拒绝请求时，审批人可以添加评论，这些评论会通过邮件一起发送给编辑人。 只要暂存策略没有在任何网络设备上部署，编辑人就可以取消审批请求。
部署已批准 (Deploy Approved)	当审批人批准请求时，暂存表格将移至部署已批准状态。当审批人拒绝请求时，表格则移回编辑状态。 只有在审批人批准了暂存策略后，编辑人才能将其部署在所选的网络设备上。
部分已部署 (Partially Deployed)	当在所选设备上部署暂存表格后，表格将移至部分已部署状态。直到暂存策略部署于所有的网络设备之前，该表格将维持在部分已部署状态。 在该阶段，您无法编辑 SGT 和 SFACL，但可以编辑表格中的单元格。 在网络设备部署 (Network Device Deployment) 窗口中，未部署最新策略的设备（不同步设备）显示为橙色（斜体）。配置进程状态栏中也会显示为该状态。编辑人可以选择这些设备，并请求批准对不同部署周期中更新的设备进行同步。

阶段	说明
已完全部署 (Fully Deployed)	直到暂存策略部署于所有的网络设备之前，系统将重复上述流程。当暂存策略部署于所有的网络设备后，审批人可以将暂存表格设置为生产表格。 由于在暂存表格替代生产表格后，您将无法回滚至先前的生产表格版本，因此我们建议您在设置暂存表格为生产表格之前，保留一个生产表格副本。

“工作流”(Workflow) 下拉列表中显示的选项会根据工作流状态和用户角色（编辑人或审批人）出现变化。下表中列出了编辑人和审批人界面显示的菜单选项：

工作流状态	编辑人视图显示的菜单	审批人视图显示的菜单
编辑状态	• 选择网络设备 网络设备配置窗口中提供以下选项： • 请求批准所选设备 • 请求批准所有/过滤的暂存列表 • 请求批准所有/过滤的生产列表 • 请求批准所有/过滤的设备 • 请求批准所有设备 • 丢弃暂存 • 查看 deltas	• 查看网络设备 • 查看 deltas
等待审批阶段 (Staging Awaiting Approval)	• 取消审批请求 • 查看网络设备 网络设备配置窗口中提供以下选项： • 取消审批请求 • 查看 deltas	• 批准部署 • 拒绝部署 • 查看网络设备 网络设备配置窗口中提供以下选项： • 批准部署 • 拒绝部署 • 查看 deltas

工作流状态	编辑人视图显示的菜单	审批人视图显示的菜单
已批准 - 部署就绪	• 部署 • 取消审批请求 • 查看网络设备 网络设备配置窗口中提供以下选项： • 部署 • 取消审批请求 • 查看 deltas	• 拒绝部署 • 查看网络设备 网络设备配置窗口中提供以下选项： • 拒绝部署 • 查看 deltas
部分已部署 (Partially deployed)	• 选择网络设备 网络设备配置窗口中提供以下选项： • 请求批准所选设备 • 请求批准所有/过滤的暂存列表 • 请求批准所有/过滤的生产列表 • 请求批准所有/过滤的设备 • 请求批准所有设备 • 查看 deltas	• 查看网络设备 • 查看 deltas

工作流状态	编辑人视图显示的菜单	审批人视图显示的菜单
已完全部署 (Fully deployed)	• 选择网络设备 网络设备配置窗口中提供以下选项： • 请求批准所选设备 • 请求批准所有/过滤的暂存列表 • 请求批准所有/过滤的生产列表 • 请求批准所有/过滤的设备 • 请求批准所有设备 • 查看 deltas	• 设置为生产 • 查看网络设备 • 查看 deltas

源和目的树视图中也提供这些工作流选项。

您可以使用 TrustSec 策略下载报告（“工作中心”[Work Centers] > TrustSec > “报告”[Reports]）查看下载了暂存/生产策略的设备。TrustSec 策略下载报告列出了网络设备发送的策略 (SGT/SGACL) 下载请求，以及 ISE 发送的详细信息。如果启用工作流模式，对于生产或暂存表，可对请求进行过滤。

出口策略表单元格配置

通过Cisco ISE，可以使用工具栏中可用的各种选项配置单元格。如果所选源和目标 SGT 与映射的单元格相同，则Cisco ISE 不允许进行单元格配置。

添加出口策略单元格映射

您可以从 Policy 页面添加出口策略的映射单元格。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**。

步骤 2 要选择矩阵单元格，请执行以下操作：

- 在矩阵视图中，点击某个单元格将其选定。
- 在 Source 和 Destination 树状视图中，选中内部表中某一行的对应复选框以选定该行。

步骤 3 点击**添加 (Add)** 以添加新映射单元格。

步骤 4 选择下列各项的相应值：

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

步骤 5 点击**保存 (Save)**。

导出出口策略

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix) > 导出 (Export)**。

步骤 2 如果要在导出文件中包括空信元（没有任何已配置 SGACL），请选中**包括空信元 (Include Empty Cells)** 复选框。

启用此选项后，整个矩阵会导出，空信元会在 SGACL 列中标有“空”关键字。

注释 确保导出文件不超过 500000 行，否则导出可能会失败。

步骤 3 选择以下选项之一：

- “本地磁盘”(Local Disk) - 如果要导出文件至本地驱动器，请选择此选项。
- “存储库”(Repository) - 如果要导出文件至远程存储库，请选择此选项。

  您必须在导出文件之前配置存储库。要配置存储库，请依次选择**管理 (Administration) > 维护 (Maintenance) > 存储库 (Repository)**。确保已授予选定存储库读取和写入权限。

  通过使用加密密钥，您可以加密导出文件。

  您可以更改文件名称。文件名不应超过 50 个字符。默认情况下，文件名包括当前时间，但是，如果远程存储库存在相同的文件名，则文件会被覆盖。

步骤 4 点击**导出 (Export)**。

导入出口策略

您可以离线创建出口策略，然后将该策略导入Cisco ISE。如果具有大量的安全组标记，那么逐个创建安全组 ACL 映射可能需要一些时间。相反，离线创建出口策略并将该策略导入Cisco ISE 可节省时间。在导入过程中，Cisco ISE 会将 CSV 文件中的条目附加到出口策略矩阵，并且不会覆盖数据。

如果出现以下情况，出口策略导入会失败：

- 源或目标 SGT 不存在
- SGACL 不存在
- 监控状态与当前在Cisco ISE 中为该信元配置的状态不同

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **TrustSec 策略 (TrustSec Policy)** > **出口策略 (Egress Policy)** > **矩阵 (Matrix)** > **导入 (Import)**。

步骤 2 点击**生成模版 (Generate a Template)**。

步骤 3 从“出口策略”(Egress Policy) 页面下载模板（CSV 文件），然后在 CSV 文件中输入以下信息：

- 源 SGT
- 目标 SGT
- SGACL
- 监控状态（启用、禁用或监控）

步骤 4 如果您要以正在导入的策略覆盖现有策略，请选中**用新数据覆盖现有数据 (Overwrite existing data with new data)** 复选框。如果导入文件中包括空信元（SGACL 列中标有“空”关键字的信元），相应矩阵信元中现有策略将被删除。

导出出口策略时，如果要包括空信元，请选中**包括空信元 (Include Empty Cells)** 复选框。有关详细信息，请参阅导出出口策略，第 128 页。

步骤 5 点击**验证文件 (Validate File)** 验证已导入的文件。Cisco ISE 会在导入文件之前验证 CSV 结构、SGT 名称、SGACL 和文件大小。

步骤 6 请选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，使Cisco ISE 在遇到任何错误时取消导入。

步骤 7 点击**导入**。

从出口策略配置 SGT

您可以直接从“出口策略”(Egress Policy) 页面创建安全组。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **TrustSec 策略 (TrustSec Policy)** > **出口策略 (Egress Policy)**。

步骤 2 从“源或目标树视图”(Source or Destination Tree View) 页面，选择**配置 (Configure)** > **创建新的安全组 (Create New Security Group)**。

步骤 3 输入所需的详细信息，并点击**提交 (Submit)**。

监控模式

只需点击一下，您就可以通过出口策略中的 Monitor All 选项将整个出口策略配置状态改为监控模式。在出口策略页面，选中**Monitor All** 复选框，将所有单元的出口策略配置状态改为监控模式。选中 Monitor All 复选框后，配置状态中会发生以下更改：

- 状态为 Enabled 的单元将显示受监控行为，但看起来仍然像处于启用状态一样。
- 状态为 Disable 的单元不受影响。

- 状态为 Monitored 的单元仍保持 Monitored 状态。

取消选中**Monitor All**复选框即可恢复原始配置状态。这不会更改数据库中单元的实际状态。如果您取消选择 **Monitor All**，出口策略中的每个单元将恢复原配置状态。

监控模式功能

监控模式的监控功能可帮助您：

- 知悉已筛选但受监控模式监控的流量
- 知悉 SGT-DGT 对是处于监控模式还是执行模式，并且观察网络中是否在发生任何异常丢包
- 了解 SGACL 丢弃实际是由执行模式执行还是由监控模式允许
- 根据监控类型（监控和/或执行）创建自定义报告
- 标识在 NAD 上已应用的 SGACL 并显示差异（如有）

未知安全组

未知安全组是一个无法修改、使用标签值 0 表示 Trustsec 的预配置安全组。

当Cisco安全组网络设备没有来源或目标的 SGT 时，这些设备会请求引用未知 SGT 的信元。如果仅来源未知，则请求适用于<unknown, Destination SGT>信元。如果仅目标未知，则请求适用于<source SGT, unknown>信元。如果来源和目标均未知，则请求适用于 <Unknown, Unknown>信元。

默认策略

默认策略是指 <ANY,ANY> 信元。所有源 SGT 均映射到所有目标 SGT。此处，ANY SGT 不可修改，且未在任何源或目标 SGT 中列出。ANY SGT 仅可与 ANY SGT 配对。ANY SGT 无法与其他任何 SGT 配对。TrustSec 网络设备将默认策略附加到特定信元策略的末尾。

- 如果信元为空，则意味着该信元仅包含默认策略。
- 如果信元包含某种策略，则生成的策略为信元特定策略与默认策略的组合。

根据Cisco ISE，信元策略和默认策略为两套独立的SGACL，由设备分别获取以响应两个独立的策略查询。

默认策略的配置与其他信元不同：

- 状态仅可为两个值，启用或监控。
- 安全组 ACL 是默认策略的可选字段，因此可留空。
- 最终抓取所有规则可为以下任意项：允许 IP、拒绝 IP、允许 IP 日志或拒绝 IP 日志。显然此处 None 选项不可用，因为默认策略之外无安全网。

SGT 分配

如果您知道设备主机名或 IP 地址，Cisco ISE 允许向 TrustSec 设备分配 SGT。当具有特定主机名或 IP 地址的设备加入网络时，Cisco ISE 会在对其进行身份验证之前分配 SGT。

默认情况下将创建以下 SGT:

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

有时需要手动将设备配置为将安全组标签映射至终端。您可以从 Security Group Mappings 页面创建此映射。在执行此操作前，请确保您保留了一系列 SGT。

ISE 允许创建最多 10000 个 IP 到 SGT 映射。您可以创建 IP 到 SGT 映射组，从逻辑上将这些大规模的映射进行分组。每组 IP 到 SGT 映射都包含一个 IP 地址列表，其要映射的单个安全组，以及作为这些映射的部署目标的网络设备或网络设备组。

NDAC 授权

您可以通过向设备分配 SGT 配置 TrustSec 策略。您可以根据 TrustSec 设备 ID 属性向设备分配安全组。

配置 NDAC 授权

开始之前

- 确保创建用于策略中的安全组。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 网络设备授权 (Network Device Authorization)**。

步骤 2 点击 Default Rule 行右侧的 **Action** 图标，然后点击 **Insert New Row Above**。

步骤 3 为此规则输入名称。

步骤 4 点击 **Conditions** 旁边的加号 (+) 以添加策略条件。

步骤 5 您可以点击 **创建新条件（高级选项）**，然后创建新条件。

步骤 6 从**安全组 (Security Group)** 下拉列表中，选择在此条件评估为 true 的情况下要分配的 SGT。

步骤 7 在此行中点击 **Action** 图标，根据设备属性在当前规则上方或下方添加更多的规则。您可以重复此过程，为 TrustSec 策略创建所需的所有规则。您可以通过点击  图标，拖放规则以为其重新排序。您还可以复制现有条件，但请确保更改策略名称。

评估为 true 的第一条规则决定评估的结果。如果没有匹配的规则，则将应用默认规则；您可以编辑默认规则以指定在没有匹配的规则的情况下必须应用的 SGT。

步骤 8 点击**保存 (Save)** 以保存您的 TrustSec 策略。

如果在您配置了网络设备策略后 SGA 设备尝试进行身份验证，设备将获取其 SGT 及其对等设备的 SGT 并且将可以下载所有相关的详细信息。

注释 默认情况下，默认**网络设备授权 (Network Device Authorization)** 策略的结果设置为 **TrustSec_Devices**。

配置最终用户授权

Cisco ISE 允许您分配安全组作为授权策略评估的结果。使用此选项，您可以将安全组分配到用户和终端。

开始之前

- 请参阅授权策略的信息。
- 要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **授权策略 (Authorization Policy)**。

步骤 2 创建新的授权策略。

步骤 3 选择安全组的权限。

如果在此授权策略中指定的条件对用户或终端为真，则此安全组会被分配到该用户或终端，且该用户或终端所发送的所有数据包会标记为此特定的 SGT。

TrustSec 配置和策略推送

Cisco ISE 支持授权更改 (CoA)，通过 CoA Cisco ISE 可以通知 TrustSec 设备 TrustSec 配置和策略更改，这样设备就可以用获取相关数据的请求作为回复。

CoA 通知可以触发 TrustSec 网络设备发送环境 CoA 或策略 CoA。

您可以向本身不支持 TrustSec CoA 功能的设备推送对设备的配置更改。

支持 CoA 的网络设备

Cisco ISE 可向以下网络设备发送 CoA 通知：

- 具有单个 IP 地址的网络设备（不支持子网）
- 配置为 TrustSec 设备的网络设备
- 设置为支持 CoA 的网络设备

在有多个辅助设备与很多不同的设备互操作的分布式环境中部署Cisco ISE 时，CoA 请求从Cisco ISE 主节点发送至所有网络设备。因此，TrustSec 网络设备需要配置为将Cisco ISE 主节点作为 CoA 客户端。

设备向Cisco ISE 主节点返回 CoA NAK 或 ACK。但是，来自网络设备的以下 TrustSec 会话会发送至接收网络设备发送的所有其他 AAA 请求的Cisco ISE 节点，而不一定会发送至主节点。

向不支持 CoA 的设备推送配置更改

某些平台不支持Cisco ISE 的更改授权 (CoA)“推送”功能，例如：Nexus 网络设备的某些版本。对于这种情况，ISE 将连接到网络设备，使该设备触发对 ISE 的更新配置请求。为此，ISE 对网络设备开放 SSHv2 隧道，Cisco ISE 发送触发刷新 TrustSec 策略矩阵的命令。此方法也可以在支持 CoA 推送的网络平台上实施。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 选中所需网络设备旁边的复选框，然后点击**编辑 (Edit)**。

验证网络设备的名称、IP 地址、RADIUS 和 TrustSec 设置是否已正确配置。

步骤 3 向下滚动至 **TrustSec 高级设置 (Advanced TrustSec Settings)**，在 **TrustSec 通知和更新 (TrustSec Notifications and Updates)** 部分，选中**发送配置更改至设备 (Send configuration changes to device)** 复选框，点击 **CLI (SSH)** 单选按钮。

步骤 4 （可选） 提供 SSH 密钥。

步骤 5 选中**当部署安全组标记影射更新时包含此设备 (Include this device when deploying Security Group Tag Mapping Updates)** 复选框，使此 SGA 设备使用设备接口凭据获取 IP-SGT 映射。

步骤 6 输入拥有在执行模式下编辑设备配置的权限的用户的用户名和密码。

步骤 7 （可选） 输入密码，对设备启用执行模式密码，将允许编辑设备配置。可以点击**显示 (Show)**，显示已为此设备配置的执行模式密码。

步骤 8 点击页面底部的**提交 (Submit)**。

现在，网络设备已配置为推送 Trustsec 更改。更改Cisco ISE 策略后，点击**推送 (Push)**，让新配置在网络设备上体现出来。

SSH 密钥验证

可能想要使用 SSH 密钥增强安全性。Cisco ISE 利用其 SSH 密钥验证功能支持此操作。

要使用此功能，请打开从Cisco ISE 到网络设备的 SSHv2 隧道，然后使用网络设备的 CLI 检索 SSH 密钥。然后，复制此密钥，并将其粘贴到Cisco ISE 中进行验证。如果 SSH 密钥错误，Cisco ISE 将终止连接。

限制：目前，Cisco ISE 只能验证一个 IP（而不是 IP 范围，或者 IP 内的子网）

开始之前

您将需要：

- 登录凭证
- 检索 SSH 密钥的 CLI 命令

希望Cisco ISE 与其安全通信的网络设备。

步骤 1 在网络设备上：

a) 登录想要Cisco ISE 使用 SSH 密钥验证与其通信的网络设备。

b) 使用设备的 CLI 显示 SSH 密钥。

示例：

对于 Catalyst 设备，命令是：`sho ip ssh`。

c) 复制显示的 SSH 密钥。

步骤 2 从Cisco ISE 用户界面：

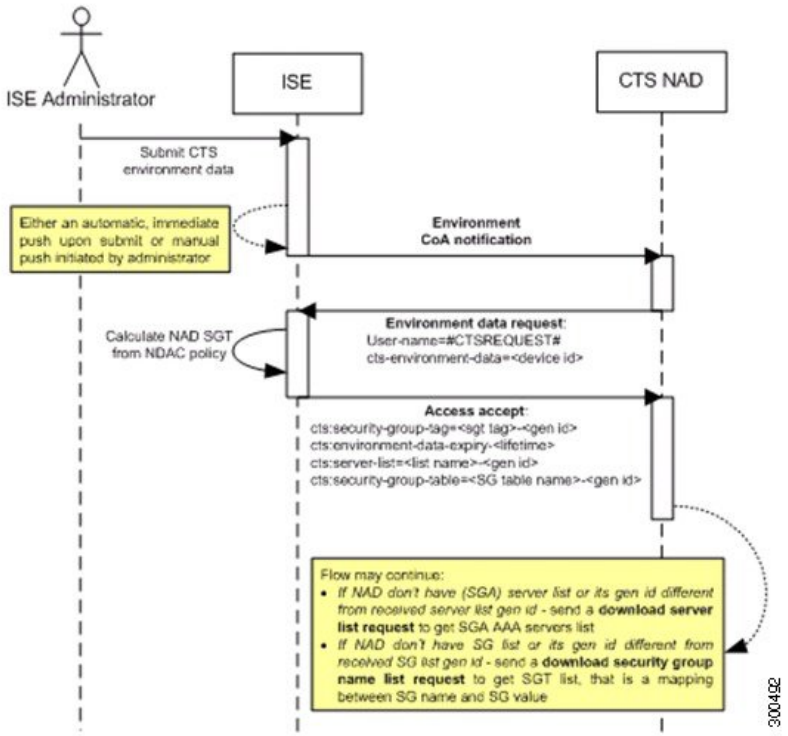
a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**，然后验证所需的网络设备名称、IP 地址、RADIUS 和 TrustSec 设置是否已正确配置。
b) 向下滚动至 **TrustSec 高级设置 (Advanced TrustSec Settings)**，在 **TrustSec 通知和更新 (TrustSec Notifications and Updates)** 部分，选中**发送配置更改到设备 (Send configuration changes to device)** 复选框，点击 **CLI (SSH)** 单选按钮。
c) 在 **SSH 密钥 (SSH Key)** 字段中，粘贴之前从网络设备检索的 SSH 密钥。
d) 点击页面底部的**提交 (Submit)**。

现在，网络设备可以使用 SSH 密钥验证与Cisco ISE 的通信。

环境 CoA 通知流程

下图显示环境 CoA 通知流程。

图 *9:* 环境 *CoA* 通知流程



1. Cisco ISE 向 TrustSec 网络设备发送环境 CoA 通知。
2. 设备返回环境数据请求。
3. Cisco ISE 返回以下数据以响应环境数据请求：

发送请求的设备的环境数据 - 这包括 TrustSec 设备的 SGT（根据 NDAC 策略推断）和下载环境 TTL。

TrustSec AAA 服务器列表的名称和生成 ID。

SGT 表（可能有多个）的名称和生成 ID - 这些表列出 SGT 名称和 SGT 值，并且这些表共同提供 SGT 的完整列表。

4. 如果设备不包含 TrustSec AAA 服务器列表，或者生成 ID 与所接收的生成 ID 不同，设备会再发送另一个请求以获取 AAA 服务器列表内容。
5. 如果设备不包含响应中列出的 SGT 表，或生成 ID 不同于所接收的生成 ID，则设备会发送另一个请求以获取该 SGT 表的内容。

环境 CoA 触发器

系统可以为以下因素触发环境 CoA：

- 网络设备
- 安全组
- AAA 服务器

为网络设备触发环境 CoA

要为网络设备触发环境 CoA，请完成以下步骤：

步骤 1 依次选择在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

步骤 2 添加或编辑网络设备。

步骤 3 更新 Advanced TrustSec Settings 部分下的 TrustSec Notifications 和 Updates 参数。

只有发生更改的特定 TrustSec 网络设备会收到更改环境属性的通知。

由于只有一个设备受到影响，环境 CoA 通知会在提交后立即发送。所产生的结果是对设备的环境属性进行更新。

为安全组触发环境 CoA

要为安全组触发环境 CoA，请完成以下步骤。

步骤 1 **工作中心 (Work Centers) > TrustSec > 组件 (Components)> 安全组 (Security Groups)**。

步骤 2 在 Security Group 页面中，更改 SGT 的名称，此操作将更改该 SGT 的映射值的名称。这会触发环境更改。

步骤 3 点击 **Push** 按钮，以在更改多个 SGT 的名称后发起环境 CoA 通知。此环境 CoA 通知会转至所有 TrustSec 网络设备并提供已更改的所有 SGT 的更新。

为 TrustSec AAA 服务器触发环境 CoA

要为 TrustSec AAA 服务触发环境 CoA，请完成以下步骤。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 组件 (Components) > TrustSec AAA 服务器 (TrustSec AAA Servers)**。

步骤 2 在 TrustSec AAA Servers 页面可以创建、删除或更新 TrustSec AAA 服务器的配置。这会触发环境更改。

步骤 3 在配置多个 TrustSec AAA 服务器之后，点击 **推送 (Push)** 按钮发起环境 CoA 通知。此环境 CoA 通知将发送到所有 TrustSec 网络设备并提供已更改的所有 TrustSec AAA 服务器的更新。

为 NDAC 策略触发环境 CoA

要为 NDAC 策略触发环境 CoA，请完成以下步骤。

步骤 1 依次选择**工作中心 (Work Centers) > TrustSec > 策略 (Policy) > 网络设备授权 (Network Device Authorization)**。

在“NDAC 策略”(NDAC policy) 页面，您可以创建、删除或更新 NDAC 策略的规则。系统会向所有网络设备通知这些环境更改。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 网络设备授权 (Network Device Authorization)**。

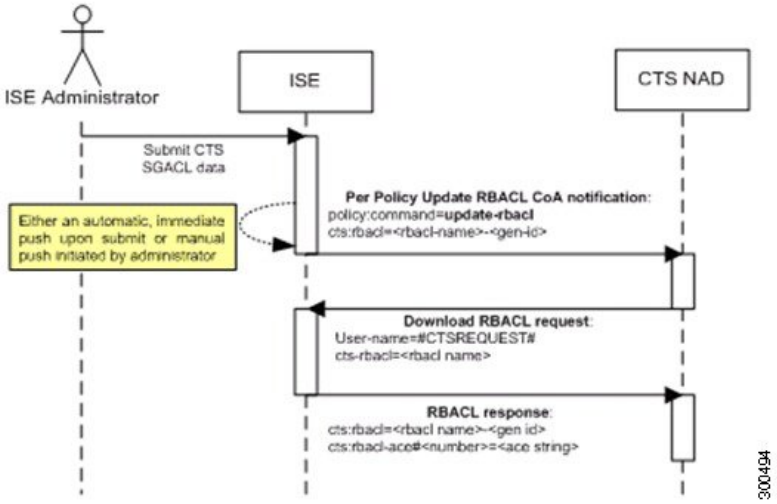
在“NDAC 策略”(NDAC policy) 页面，您可以创建、删除或更新 NDAC 策略的规则。系统会向所有网络设备通知这些环境更改。

步骤 3 您可以点击“NDAC 策略”(NDAC policy) 页面中的 **推送 (Push)** 按钮，发起环境 CoA 通知。此环境 CoA 通知将发送至所有 TrustSec 网络设备并更新网络设备自身 SGT。

更新 SGACL 内容流程

下图显示更新 SGACL 内容流程。

图 *10:* 更新 *SGACL* 内容流程



1. Cisco ISE 将更新 RBACL 命名列表 CoA 通知发送到 TrustSec 网络设备。通知包含 SGACL 名称和生成 ID。
2. 如果满足以下两个条件，设备可能会根据 SGT 数据请求进行重放：

   如果 SGACL 是设备所载出口信元的一部分。设备载有一个出口策略数据子集，这些数据是与相邻设备和终端的 SGT 相关的信元（选定目标 SGT 的出口策略列）。

   CoA 通知中的生成 ID 与设备为此 SGACL 保留的生成 ID 不同。
3. 为了响应 SGACL 数据请求，Cisco ISE 会返回 SGACL 的内容 (ACE)。

启动更新 SGACL 命名的列表 CoA

要触发更新 SGACL 命名的列表 CoA，请完成以下步骤：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **TrustSec** > **组件 (Components)** > **安全组 ACL (Security Group ACLs)**。

步骤 2 更改 SGACL 的内容。在您提交 SGACL 后，它会提高 SGACL 的生成 ID。

步骤 3 点击**推送 (Push)** 按钮以在您更改多个 SGACL 的内容之后发起更新 SGACL 命名的列表 CoA 通知。此通知将发送至所有 TrustSec 网络设备，并且在相关设备上提供该 SGACL 内容的更新。

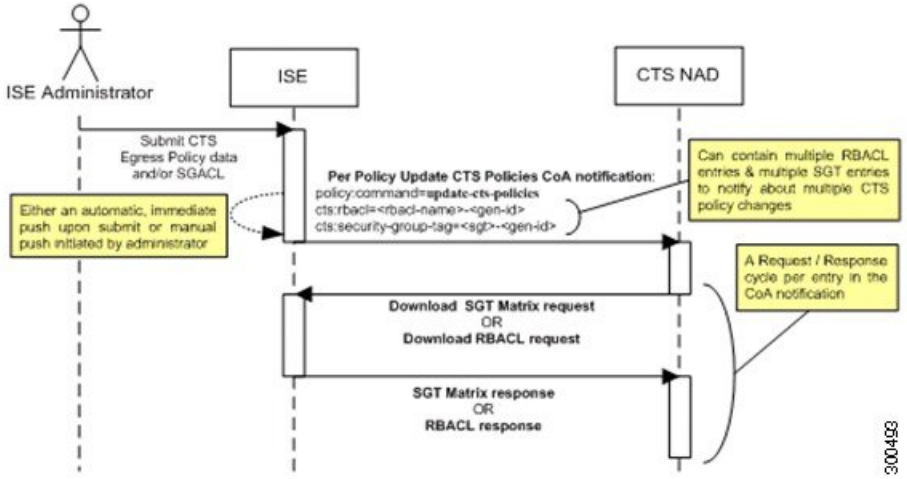
更改 SGACL 的名称或 IP 版本不会更改其生成 ID；因此不需要发送更新 RBACL 命名的列表 CoA 通知。

但是，如果更改出口策略中当前使用的 SGACL 的名称或 IP 版本，则会相应地更改包含该 SGACL 的单元格，并且这会更改该单元格目标 SGT 的生成 ID。

策略更新 CoA 通知流程

下图显示了策略 CoA 通知流程。

图 *11:* 策略 *CoA* 通知流程

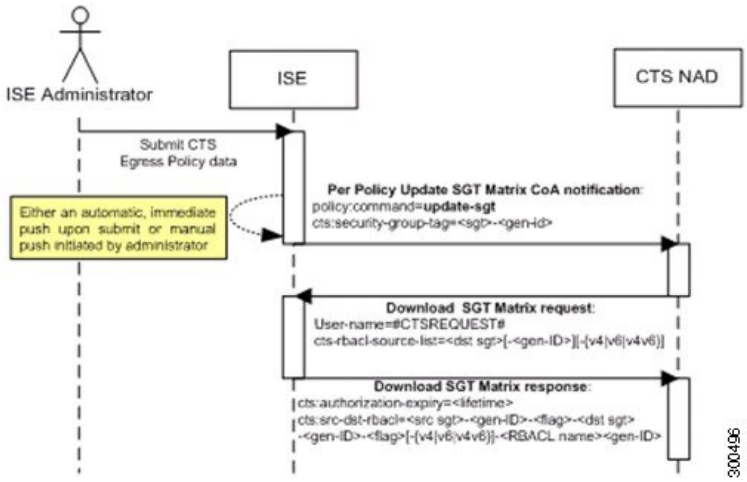


1. Cisco ISE 向 TrustSec 网络设备发送更新策略 CoA 通知。通知可以包含多个 SGACL 名称及其生成 ID，以及多个 SGT 值及其生成 ID。
2. 设备可能重放多个 SGACL 数据请求和/或多个 SGT 数据。
3. 作为对 SGACL 数据请求或 SGT 数据请求的响应，Cisco ISE 返回相关数据。

更新 SGT 矩阵 CoA 流程

下图显示了更新 SGT 矩阵 CoA 的流程。

图 *12:* 更新 *SGT* 矩阵 *CoA* 流程



1. Cisco ISE 将更新的 SGT 矩阵 CoA 通知发送到 TrustSec 网络设备。通知包含 SGT 值和生成 ID。
2. 如果满足以下两个条件，设备可以重放 SGT 数据请求：

   如果 SGT 是毗邻设备或终端的 SGT，设备将下载并保留与毗邻设备和终端的 SGT（目标 SGT）相关的信元。

   CoA 通知中的生成 ID 不同于设备为 SGT 保留的生成 ID。
3. 作为对 SGT 数据请求的响应，Cisco ISE 返回所有出口信元的数据，例如源 SGT 和目标 SGT、信元状态以及在此信元中配置的 SGACL 名称的顺序列表。

发起从出口策略更新 SGT 矩阵 CoA

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy)**。

步骤 2 在“出口策略”(Egress Policy) 页面，更改单元格的内容（状态、SGACL）。

步骤 3 在提交更改后，系统会提高该单元格目标 SGT 的生成 ID。

步骤 4 点击**推送 (Push)** 按钮以在您更改多个出口单元格的内容之后发起更新 SGACL 命名的列表 CoA 通知。此通知将发送至所有 TrustSec 网络设备，并且在相关设备上提供该单元格内容的更新。

TrustSec CoA 摘要

下表汇总了可能要求发起 TrustSec CoA 的各种场景、每个场景中使用的 CoA 的类型以及相关 UI 页面。

表 *17: TrustSec CoA* 摘要

UI 页面	触发 CoA 的操作	触发方式	CoA 类型	发送到
Network Device	更改页面的 TrustSec 部分中的环境 TTL	在成功提交 TrustSec 网络设备后	环境	特定网络设备
TrustSec AAA Server	TrustSec AAA 服务器中的任何更改（创建、更新、删除、重新排序）	可以通过点击 TrustSec AAA 服务器列表页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
Security Group	SGT 中的任何更改（创建、重命名、删除）	可以通过点击 SGT 列表页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备

UI 页面	触发 CoA 的操作	触发方式	CoA 类型	发送到
NDAC Policy	NDAC 策略中的任何更改（创建、更新、删除）	可以通过点击 NDAC 策略页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
SGACL	更改 SGACL ACE	可以通过点击 SGACL 列表页面中的 Push 按钮推送累积更改。	更新 RBACL 命名列表	所有 TrustSec 网络设备
	更改 SGACL 名称或 IP 版本	可以通过点击 SGACL 列表页面中的 Push 按钮或 Egress 表中的 Policy Push 按钮推送累积更改。	更新 SGT 矩阵	所有 TrustSec 网络设备
Egress Policy	用于更改 SGT 的生成 ID 的操作。	可以通过点击 Egress Policy 页面中的 Push 按钮推送累积更改。	更新 SGT 矩阵	所有 TrustSec 网络设备

安全组标记交换协议

安全组标记 (SGT) 交换协议 (SXP) 用于在所有不具备 TrustSec 硬件支持的网络设备中传播 SGT。SXP 可用于将终端的 SGT 和 IP 地址从一个可感知 SGT 的网络传输设备到另一个此类设备。SXP 传输的数据称为 IP-SGT 映射。属于终端的 SGT 可通过静态或动态的方式进行分配，并且 SGT 可在网络策略中用作分类器。

要在节点上启用 SXP 服务，请在“通用节点设置”(General Node Settings) 页面选中“启用 SXP 服务”(Enable SXP Service) 复选框。您还必须指定 SXP 服务使用的接口。

SXP 使用 TCP 作为传输协议，用于在两个单独的网络设备间建立 SXP 连接。每对 SXP 连接中，一个对等设备被指定为 SXP 发言者，另一个对等设备被指定为 SXP 倾听者。这两个对等设备也可在双向模式中进行配置，此类配置中两个对等设备都可作为发言者和倾听者。任一对等设备都可发起连接，但映射信息总是从发言者传播给倾听者。

注释 始终在默认 SXP 域中传播会话绑定。

下表列出了在 SXP 环境中的一些常用术语：

IP-SGT 映射	通过 SXP 连接交换的 IP 地址到 SGT 的映射。 要查看 SXP 设备学习到的所有映射（包括静态映射和会话映射），请选择**工作中心 (Work Centers) > TrustSec > SXP > 所有 SXP 映射 (All SXP Mappings)**。
SXP 发言者	通过 SXP 连接发送 IP-SGT 映射的对等设备。
SXP 倾听者	通过 SXP 连接接受 IP-SGT 映射的对等设备。

要查看添加到Cisco ISE 的 SXP 对等设备，请选择**工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices)**。

注释 我们建议您在独立节点上运行 SXP 服务。

使用 SXP 服务时,请注意以下几点：

- Cisco ISE 不支持具有相同 IP 地址的多个 SXP 会话绑定。
- 如果 RADIUS 计费更新太过频繁（例如，几秒钟内有大约 6 至 8 次计费更新），计费更新数据包可能会丢失，并且 SXP 可能未收到 IP-SGT 绑定。
- 从先前版本的 ISE 升级后，SXP 不会自动启动。在升级后，必须更改 SXP 密码并重新启动 SXP 过程。

添加 SXP 设备

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择**工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices)**。

步骤 2 点击**添加 (Add)**。

步骤 3 输入设备详细信息：

- 点击**从 CSV 文件上传 (Upload from a CSV file)** 使用 CSV 文件添加 SXP 设备。浏览并选择 CSV 文件，然后点击**上传 (Upload)**。

  您也可以下载 CSV 模板文件，填写要添加设备的详细信息，并上传 CSV 文件。

- 点击**添加单个设备 (Add Single Device)** 为每个 SXP 设备手动添加设备的详细信息。

  输入名称、IP 地址、SXP 角色（侦听程序、扬声器或两者）、密码类型、SXP 版本和用于对等设备的连接 PSN。您还必须指定对等设备连接的 SXP 域。

步骤 4 (可选)点击**高级设置 (Advanced Settings)**，然后输入以下详细信息：

- “最短可接受保持时间”(Minimum Acceptable Hold Timer) - 指定时间（以秒为单位），扬声器将发送保持连接存活的保持存活消息。有效范围为 1 到 65534。
- “保持存活计时器”(Keep Alive Timer) - 在没有其他信息通过更新消息导出的间隔，扬声器用其触发保持连接消息的调度。有效范围为 0 到 64000。

步骤 5 点击**保存 (Save)**。

添加 SXP 域过滤器

可以查看 SXP 设备学习的所有映射（包括静态映射和会话映射）。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > SXP > 所有 SXP 映射 (All SXP Mappings)**

默认情况下，从网络设备学习的会话映射仅会发送到默认 VPN 组。您可以创建 SXP 域过滤器，以便将映射发送到不同的 SXP 域 (VPN)。

您将在此窗口中找到根据 IP-SGT 映射中配置的虚拟网络自动创建的映射。

注释 从思科 ISE 3.0 开始，网络设备可以属于多个 SXP 域。

要添加 SXP 域过滤器，请执行以下操作：

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > SXP > 所有 SXP 映射 (All SXP Mappings)**。

步骤 2 点击**添加 SXP 域过滤器 (Add SXP Domain Filter)**。

步骤 3 执行以下操作：

- 输入子网详细信息。具有来自此子网的 IP 地址的网络设备的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域 (VPN)。
- 从 SGT 下拉列表中选择一个 SGT。与此 SGT 相关的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域。

  如果已同时指定子网和 SGT，则与此过滤器匹配的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域。
- 从下拉列表中选择虚拟网络。与此虚拟网络相关的会话映射会发送到在 **SXP 域 (SXP Domain)** 字段中选择的 SXP 域。

- 选择必须将映射发送到的 SXP 域。

步骤 4 点击**保存 (Save)**。

您还可以更新或删除 SXP 域过滤器。要更新过滤器，请点击**管理 SXP 域过滤器 (Manage SXP Domain Filter)**，选中要更新的过滤器旁的复选框，然后点击**编辑 (Edit)**。要删除过滤器，请选中要删除的过滤器旁的复选框，然后点击**回收站 (Trash) > 所选项 (Selected)**。

配置 SXP 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > SXP 设置**。

步骤 2 在“SXP 设置”(SXP Settings) 页面输入所需的详细信息。

如果您取消选中**发布 PxGrid 上 SXP 绑定**复选框，IP - SGT 映射不会在网络设备间传播。

步骤 3 点击**保存 (Save)**。

注释 当 SXP 设置更改时，SXP 服务重新启动。

TrustSec-思科 ACI 集成

Cisco ISE 可以将 SGT 和 SXP 映射与内部终端组 (IEPG)、外部终端组 (EEPG) 和Cisco以应用为中心的基础设施（Cisco ACI）的终端 (EP) 配置同步。

Cisco ISE 可通过同步 IEPG，并在 ISE 中创建关联的只读 SGT，支持将数据包从Cisco ACI 域发送到 TrustSec 域。这些 SGT 对Cisco ACI 中配置的终端进行映射，并在 ISE 中创建关联的 SXP 映射。这些 SGT 会显示在“安全组”(Security Group) 页面（“获知源”(Learned From) 字段的值为“Cisco ACI”(Cisco ACI)）。您可以在“所有 SXP 映射” (All SXP Mappings) 页面查看 SXP 映射。只有在已选择“策略平面”(Policy Plane) 选项（在“思科 ACI 设置”(Cisco ACI Settings) 页面中）且 SXP 设备属于您在“Cisco ACI 设置”(Cisco ACI Settings) 页面上设置的 SXP 域时，才会将这些映射发送到Cisco ACI。

注释 在 IP-SGT 映射、映射组和 SXP 本地映射中无法使用只读 SGT。

添加安全组时，可以通过启用**传播到 ACI (Propagate to ACI)** 选项指定是否将 SGT 发送到Cisco ACI。启用此选项后，与此 SGT 相关的 SXP 映射将发送到Cisco ACI。但是，只有在已选择“策略平面”(Policy Plane) 选项（在“思科 ACI 设置”(Cisco ACI Settings) 页面中）且 SXP 设备属于您在“Cisco ACI 设置”(Cisco ACI Settings) 页面上设置的 SXP 域时，才会发送这些映射。

Cisco ACI 可通过同步 SGT，并创建关联的 EEPG，支持将数据包从 TrustSec 域发送到Cisco ACI 域。Cisco ACI 根据来自Cisco ISE 的 SXP 映射在 EEPG 下创建子网。当在Cisco ISE 中删除了相应的 SXP 映射时，这些子网不会从Cisco ACI 中删除。

在Cisco ACI 中更新 IEPG 后，Cisco ISE 中的相应 SGT 配置也会更新。在Cisco ISE 中添加 SGT 后，Cisco ACI 中会创建新的 EEPG。删除 SGT 后，相应的 EEPG 也会在Cisco ACI 中删除。在Cisco ACI 中对终端进行更新后，Cisco ISE 中相应的 SXP 映射也会更新。

如果与Cisco ACI 服务器的连接丢失，则Cisco ISE 会在重新建立连接后重新同步数据。

注释 必须启用 SXP 服务，才能使用思科 ACI 集成功能。

可以在**所有 ACI 映射 (All ACI Mappings)** 窗口中查看Cisco ISE 与Cisco ACI 之间收发的所有绑定。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **TrustSec** > **ACI**。从Cisco ACI 获知绑定时，**获知者 (Learned By)** 列显示 **ACI**，并且**涉及的 PSN (PSNs involved)** 列为空。而当绑定从Cisco ISE 发送到Cisco ACI 时，**获知者 (Learned By)** 列将显示绑定类型（例如静态、SXP 或会话），**涉及的 PSN (PSNs involved)** 列显示所涉及的 PSN 的 FQDN。使用窗口中的过滤器选项可以监控完整列表中的特定映射。

注释 要成功集成Cisco ISE 和Cisco ACI，签名证书应具有适当的 SAN 字段。Cisco ISE 将使用 APIC 服务器提供的证书的 SAN 扩展属性中指定的值。

配置 ACI 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)** > **导入 (Import)**。

步骤 2 导入Cisco ACI 证书。有关详细信息，请参阅将根证书导入受信任证书库。

步骤 3 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **TrustSec** > **设置 (Settings)** > **ACI 设置 (ACI Settings)**。

步骤 4 选中**启用 ACI 集成 (Enable ACI Integration)** 复选框，向Cisco ACI 学习终端并使用 SXP 传播它们。

步骤 5 选择以下选项之一：

- 数据平面/硬件集成
- 策略平面/API 集成

注释　如果选择**数据平面/硬件集成 (Data Plane / Hardware Integration)**，则Cisco ISE 必须与Cisco DNA 中心集成。如果选择**策略平面/API 集成 (Policy Plane / API Integration)**，则在没有活动 SXP 服务的情况下无法进行 SXP 传播。在选择此选项之前，在**部署 (Deployment)** 窗口中激活 SXP 服务。

步骤 6 如果选择**数据平面/硬件集成 (Data Plane / Hardware Integration)**，请输入以下详细信息

- **IP 地址 (IP address)**：输入Cisco ACI 服务器的 IP 地址或主机名。可以输入三个 IP 地址或主机名，用逗号分隔。
- **用户名 (Username)**：输入Cisco ACI 管理员用户的用户名。
- **密码 (Password)**：输入Cisco ACI 管理员用户的密码。
- **租户名称 (Tenant name)**：输入在Cisco ACI 上配置的租户名称。
- **测试与 ACI 的连接 (Test Connection to ACI)**：点击此按钮可检查与Cisco ACI 服务器的连接。
- **续订证书 (Renew Certificate)**：点击此按钮可执行域管理器刷新。证书的有效期通常为 10 年。在续订证书之前，系统中应能成功进行对等互连。续订证书后，需要从部署中所有节点的 CLI 重新启动Cisco ISE 应用。续订证书的大概时间为 5 分钟。
- **新 SGT 后缀 (New SGT Suffix)**：此后缀将添加至根据从Cisco ACI 学习的 EPG 新创建的 SGT。

  注释　如果超过 32 个字符，EPG 名称会被截断。但是，您可以在“安全组”(Security Groups) 列表页面的“说明”(Description) 字段 查看 EPG 的全称，应用配置文件名称和 SGT 后缀详细信息。

- **新 EPG 后缀 (New EPG Suffix)**：此后缀将添加至Cisco ACI 中根据从Cisco ISE 学习的 SGT 新创建的 EPG。
- **启用数据平面 (Enable Data Plane)**：选中此复选框可下载边界路由器的转换表。如果启用此复选框，则必须为无法与任何其他现有 SGT 匹配的数据包选择默认 SGT 名称。
  - **默认 SGT 名称 (Default SGT name)**：从下拉列表中选择 SGT 的默认名称。
- **启用元素限制 (Enable Elements Limit)**：仅当启用数据平面时，此选项才可用。
  - **IEPG 的最大数量 (Max number of IEPGs)**：指定要转换为 SGT 的 IEPG 的最大数量。系统将按字母顺序转换 IEPG。默认值为 1000。
  - **SGT 的最大数量 (Max number of SGTs)**：指定将转换为 IEPG 的 SGT 的最大数量。系统将按字母顺序转换 SGT。默认值为 500。

步骤 7 如果选择了**策略平面 (Policy Plane)** 选项，则输入以下详细信息：

- **IP 地址/主机名 (IP address / Hostname)**：输入Cisco ACI 服务器的 IP 地址或主机名。可以输入三个 IP 地址或主机名，用逗号分隔。
- **管理员名称 (Admin name)**：输入Cisco ACI 管理员用户的用户名。
- **管理员密码 (Admin password)**：输入Cisco ACI 管理员用户的密码。

- **租户名称 (Tenant name)**：输入在Cisco ACI 上配置的租户名称。
- **L3 路由网络名称 (L3 Route network name)**：输入在Cisco ACI 上为同步策略元素而配置的第 3 层路由网络的名称。
- **测试设置 (Test Settings)**：点击此按钮检查与Cisco ACI 服务器的连接。
- **新 SGT 后缀 (New SGT Suffix)**：此后缀将添加至根据从Cisco ACI 学习的 EPG 新创建的 SGT。
- **新 EPG 后缀 (New EPG Suffix)**：此后缀将添加至Cisco ACI 中根据从Cisco ISE 学习的 SGT 新创建的 EPG。
- 在 **SXP 传播 (SXP Propagation)** 区域，可以选择所有 SXP 域或指定与Cisco ACI 共享映射的 SXP 域。
- **启用数据平面 (Enable Data Plane)**：选中此复选框可下载边界路由器的转换表。如果启用此复选框，则必须为无法与任何其他现有 SGT 匹配的数据包选择默认 SGT 名称。
  - **未标记数据包的 EEPG 名称 (EEPG name for untagged packets)**：未转换为 EEPG 的Cisco TrustSec 数据包在Cisco ACI 中使用此名称进行标记。
  - **默认 SGT 名称 (Default SGT name)**：从下拉列表中选择 SGT 的默认名称。
- **启用元素限制 (Enable Elements Limit)**：仅当启用数据平面时，此选项才可用。
  - **IEPG 的最大数量 (Max number of IEPGs)**：指定要转换为 SGT 的 IEPG 的最大数量。系统将按字母顺序转换 IEPG。默认值为 1000。
  - **SGT 的最大数量 (Max number of SGTs)**：指定将转换为 IEPG 的 SGT 的最大数量。系统将按字母顺序转换 SGT。默认值为 500。

步骤 8 点击**保存 (Save)**。

思科 ACI 和思科 SD-Access 与虚拟网络感知的集成

Cisco ISE 版本 2.7 中有一种基本的实施机制，可以将 SGT 和 SXP 映射同步到内部终端组 (IEPG)、外部终端组 (EEPG) 和Cisco ACI 的终端配置。

Cisco ISE 版本 3.0 支持一种额外的实施机制，为具有Cisco ACI 基础设施的Cisco软件定义接入 (SD-Access) 交换矩阵提供信息交换和跨域自动化的增强型转化。此实施机制在以下方面提供支持：

- 交换和转换 EPG 和 SGT 信息
- 将Cisco SD-Access 虚拟网络扩展到Cisco ACI 交换矩阵
- Cisco SD-Access 和Cisco ACI 交换矩阵数据平面自动化
- IP-SGT 绑定交换
- 将绑定发送到 pxGrid 和 SXP 域

Cisco ISE 从 RADIUS 绑定或Cisco ACI 绑定获知虚拟网络信息，并为特定虚拟网络提供本地静态映射。虚拟网络可用于增强 SXP 过滤器逻辑，利用该逻辑可协调与Cisco ACI 的 IP-SGT 绑定共享。请注意，因为扩展到Cisco ACI 的虚拟网络是与Cisco ACI 共享 IP-SGT 绑定的唯一结构，所以在这个意义上 SXP 域和虚拟网络是紧密关联的。因此，特定 SXP 域（以 SD-Access- 前缀表示）映射到Cisco ISE 中的等效虚拟网络（SXP 域减去 SD-Access- 前缀）。

为了让Cisco SD-Access 边界节点能了解Cisco ACI 绑定，Cisco ACI 绑定在复制之后再通过 SXP 过滤器逻辑发送出去，仿佛它们源自所有扩展的虚拟网络。例如，Cisco SD-Access 虚拟网络 1、虚拟网络 2 和虚拟网络 3 扩展到Cisco ACI，则Cisco ACI 与原始Cisco ACI 虚拟网络的绑定会通过 SXP 过滤器发送四次。这个完全相同的绑定将通过所有四个虚拟网络的过滤器。可以根据特定部署要求修改和自定义过滤器。但是，面向所有扩展虚拟网络的复制始终会发生。

Cisco ISE 尽可能从Cisco ACI 获知 IP-SGT、EPG 绑定。但是，Cisco ISE 无法强制Cisco ACI 获知任何绑定。Cisco ACI 必须明确向Cisco ISE 请求绑定信息。

下表列出了Cisco ISE 中 IP-SGT 或 IP-EPG 绑定可能存在的源和目标组合。

源域	目标域名	源分组	目标分组	注
Cisco ACI	SXP	Cisco ACI 虚拟网络	SXP 域	Cisco ACI 虚拟网络可用作 SXP 过滤器中的密钥，以与一个或多个 SXP 域共享绑定。
Cisco ACI	pxGrid	Cisco ACI 虚拟网络	PxGrid 上的 VPN for SXP 主题	Cisco ACI 虚拟网络可用作 SXP 过滤器中的密钥，以与 pxGrid 上的一个或多个 SXP VPN 共享绑定。
Cisco ACI	Cisco SD-Access 边界节点	Cisco SD-Access 扩展虚拟网络	SXP 域	Cisco ACI 绑定分享给为边界节点虚拟网络信息交换而自动创建的所有 SXP 域（有“SD-Access-”前缀的域）。
Cisco ISE 静态映射	SXP	Cisco SD-Access 虚拟网络或现有 SXP 域	SXP 域	静态绑定可以直接发送到 SXP 域（在静态映射中指定 SXP 域）或通过 SXP 过滤器发送（连同虚拟网络信息）。如果未指定虚拟网络，则 SXP 过滤器使用虚拟网络 DEFAULT_VN。
Cisco ISE 静态映射	pxGrid	Cisco SD-Access 虚拟网络	SXP 域	静态绑定可以直接发送到 SXP 域（在静态映射中指定 SXP 域）或通过 SXP 过滤器发送（连同虚拟网络信息）。如果未指定虚拟网络，则 SXP 过滤器使用虚拟网络 DEFAULT_VN。
Cisco ISE 静态映射	Cisco ACI	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络必须扩展到Cisco ACI (mdpExtendvirtual networkReq)，并且绑定使用 SXP 过滤器中的虚拟网络发送到 Cisco ACI，同时 SXP 域映射到虚拟网络。
SXP	pxGrid	SXP 域	SXP 域	SXP 域在 pxGrid 上的 SXP 主题中显示为 VPN。

SXP	Cisco ACI	SXP 域	Cisco SD-Access 虚拟网络	在Cisco ACI 设置下选择 SXP 域共享。 仅共享由Cisco SD-Access 虚拟网络自动创建的 SXP 域（虚拟网络等效 SXP 域）。 Cisco SD-Access 虚拟网络应扩展到Cisco ACI，以使虚拟网络有机会共享绑定。 绑定必须包含在让Cisco ACI 请求终端数据的消费者服务中。
SXP	SXP	SXP 域	SXP 域	通过优先级排序实现的 SXP 绑定是共享的。
RADIUS 绑定	Cisco ACI	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络	RADIUS 绑定通过 SXP 过滤器（连同虚拟网络信息）发送。如果未为绑定指定虚拟网络，则 SXP 过滤器使用虚拟网络 DEFAULT_VN。
RADIUS 绑定	pxGrid	Cisco SD-Access 虚拟网络	Cisco SD-Access 虚拟网络	RADIUS 绑定进入 pxGrid 上的会话目录主题，虚拟网络字段也添加到该主题。
RADIUS 绑定	SXP	Cisco SD-Access 虚拟网络	SXP 域	Cisco SD-Access 虚拟网络可用作 SXP 过滤器中的密钥，以选择要与之共享绑定的 SXP 域。

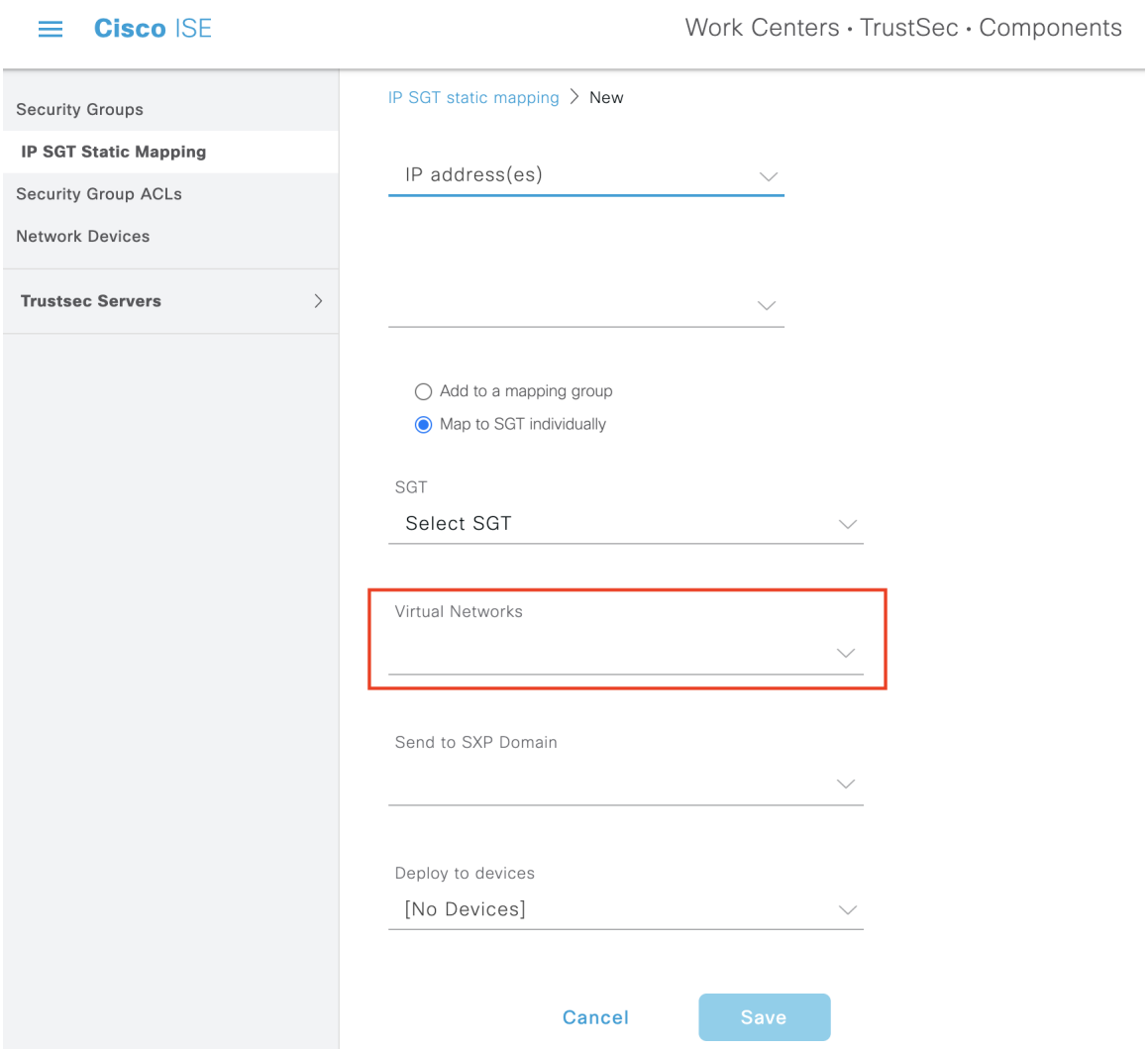
要促进跨域支持，您必须能够在两个策略域（或一个策略域内的转发域）之间交换和过滤各种网络转发域，例如 IP 地址、子网掩码、安全组标记、EPG、虚拟网络、虚拟路由和转发 (VRF)。当策略域（例如Cisco SD-Access、Cisco ACI、SD-WAN、CPC 和 Meraki）有多个转发域时，这一点尤其重要。

您可以识别、捕获和存储策略域的网络特定转发域以及从其他策略域获取的所有会话和绑定的域特定属性。策略管理员将使用这些属性将会话和绑定过滤到特定 SXP 域。此外，管理员还能创建策略，仅将特定绑定从一个转发域映射或过滤到另一个转发域。

从Cisco ISE 3.0 开始，在Cisco ISE 从 Cisco DNA Center 获知的每个虚拟网络中，您将在“SXP 设备”(SXP Devices) 窗口中找到自动创建的 SXP 过滤器和 SXP 域。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices)**。这些 SXP 域将用于在与Cisco ACI 共享的绑定中设置虚拟网络。

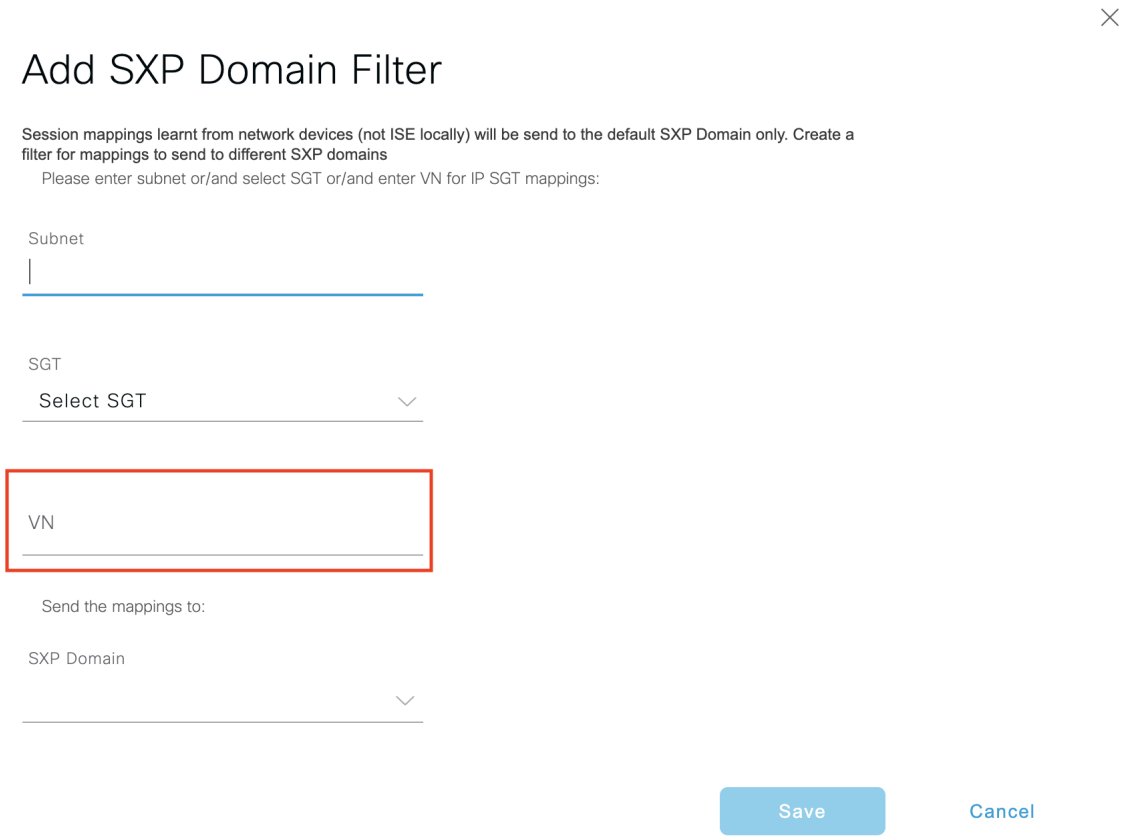
您可以在“IP-SGT 静态映射”(IP-SGT Static mapping) 窗口中向 IP-SGT 静态映射添加虚拟网络并编辑虚拟网络。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > 组件 (Components) > IP SGT 静态映射 (IP SGT Static Mapping)**。点击**添加 (Add)** 添加新映射，或点击**编辑 (Edit)** 修改现有映射。

图 *13:* 在 ***IP SGT*** 静态映射中添加虚拟网络



您还可以在 SXP 域过滤器中包含虚拟网络，以指定当Cisco ISE 收到的映射被映射到特定虚拟网络时将映射发送到哪个 SXP 域。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers) > TrustSec > SXP > SXP 设备 (SXP Devices) > 所有 SXP 映射 (All SXP Mappings)** 并点击**添加 SXP 域过滤器 (Add SXP Domain Filter)**。Cisco ACI 获知的绑定有原始Cisco ACI 虚拟网络，这些绑定发送到过滤器中配置的 SXP 域。此过滤器还会影响绑定发送到Cisco ACI 的方式。

图 *14:* 在 ***SXP*** 设备过滤器中添加虚拟网络信息



配置思科 ISE 以支持思科 ACI 和思科 SD-Access 集成

此任务可帮助您配置Cisco ISE 以支持Cisco ACI 和Cisco SD-Access 集成。

开始之前

确保Cisco ISE 与 Cisco DNA Center 的最新版本集成，并且使用的 APIC 版本为 5.1 或更高版本。

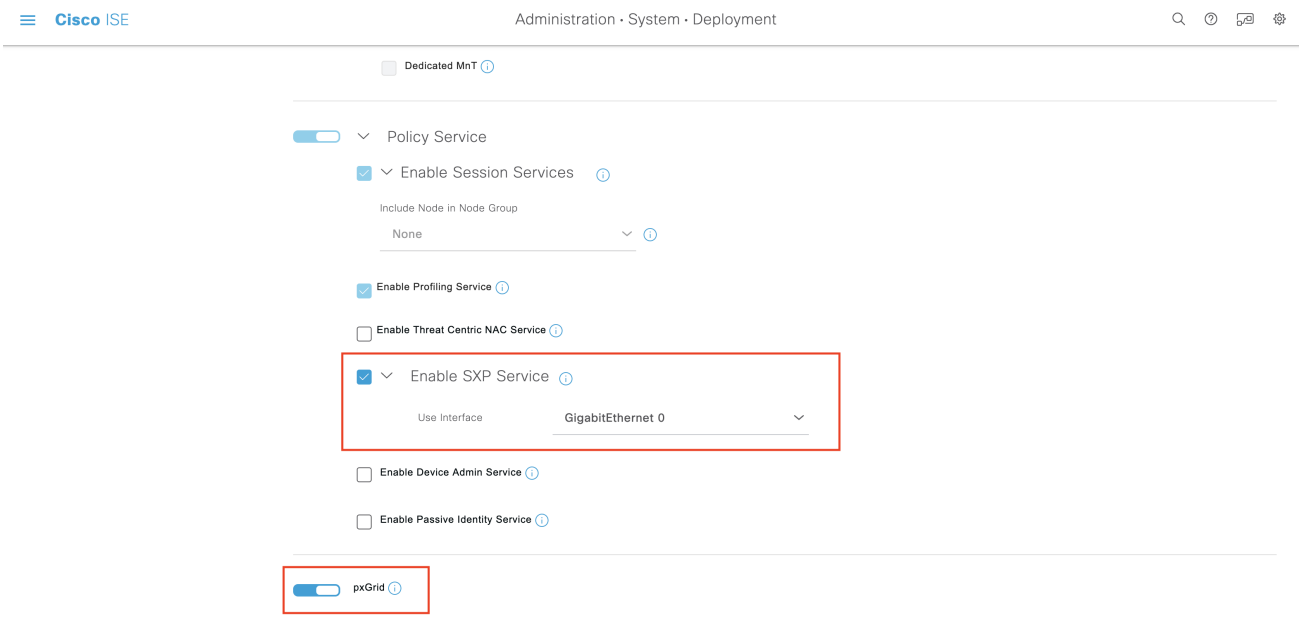
步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 从节点列表中，选中您想要启用 SXP 和 pxGrid 服务的节点旁边的复选框。

步骤 3 向下滚动到**策略服务 (Policy Service)** 部分并启用 pxGrid 和 SXP 服务，如下图所示。

如果您在Cisco ISE 上启用了多个接口，请在**启用 SXP 服务 (Enable SXP Service)** 区域中指定哪个接口将保持 SXP 连接。

图 *15:* 启用 ***SXP*** 和 ***pxGrid*** 服务



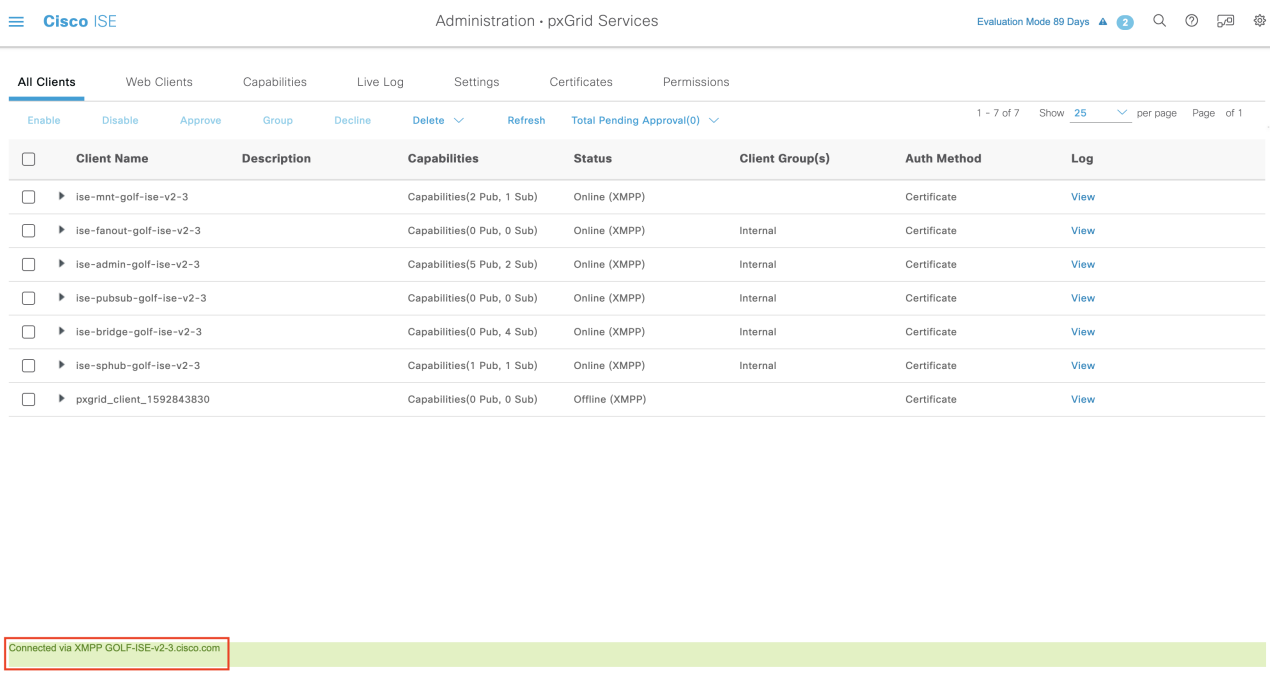
步骤 4 点击**保存 (Save)**。

步骤 5 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **所有客户端 (All Clients)**。

步骤 6 验证 pxGrid 服务是否已启动并正常运行。

连接成功的通知显示在窗口的左下角，如下图所示：

图 *16:* 验证与 *pxGrid* 服务的连接



步骤 7 从 APIC 控制器浏览器下载 APIC 证书。点击浏览器地址栏中的锁定图标，查看证书并将其下载为 PEM 文件。

步骤 8 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。

步骤 9 在**受信任证书 (Trusted Certificates)** 窗口中导入下载的 APIC 证书文件。

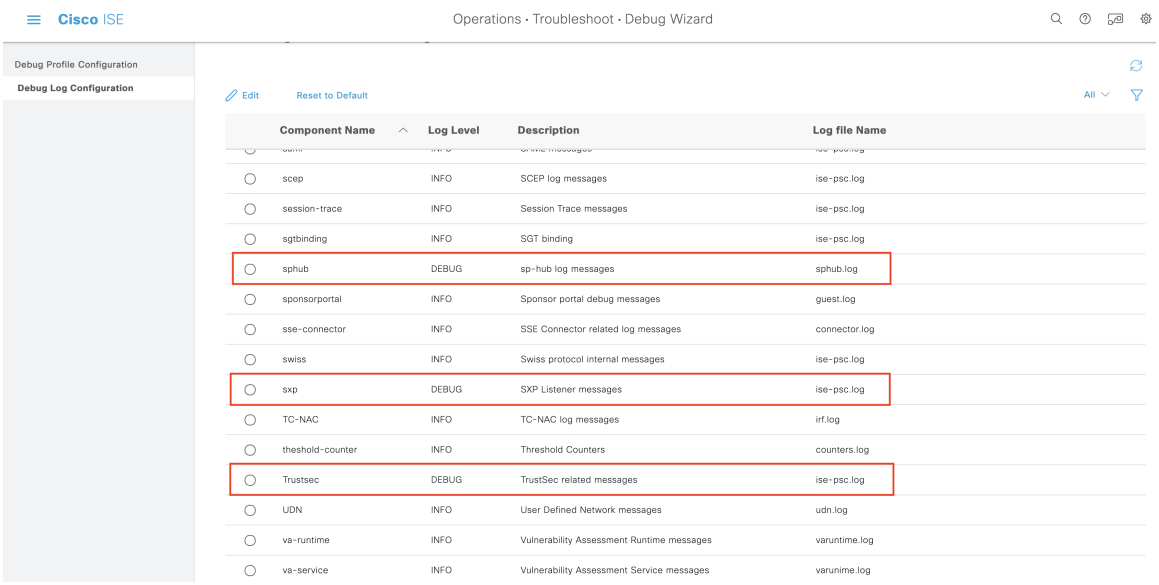
步骤 10 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centres)** > **TrustSec** > **设置 (Settings)** > **ACI 设置 (ACI Settings)**。

步骤 11 根据需要配置 ACI 设置。有关详细信息，请参阅配置 ACI 设置，第 145 页

验证思科 ACI 与思科 SD-Access 的集成

要获取Cisco ACI 和Cisco SD-Access 连接之间的详细信息，请选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)**。选择启用了 SXP 和 pxGrid 服务的Cisco ISE 节点，然后点击“编辑”(Edit)。如下图所示，将 **spbhub**、**sxp** 和 **TrustSec** 组件的日志级别设置为“调试”(DEBUG)。

图 *17:* 启用调试记录



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

此外，还可以使用从Cisco ACI 集成中吸取的信息增强TrustSec 控制面板，第 98 页，这对于排除 Cisco ACI 相关问题非常有用。

在Cisco DNA 中心发出域通告后，应同时在Cisco ISE 的**受信任证书 (Trusted Certificates)** 窗口和**系统证书 (System Certificates)** 窗口中确认 APIC 证书是否是从 APIC 域管理器获取的。

图 *18:* 在“系统证书”*(System Certificates)* 窗口中验证证书

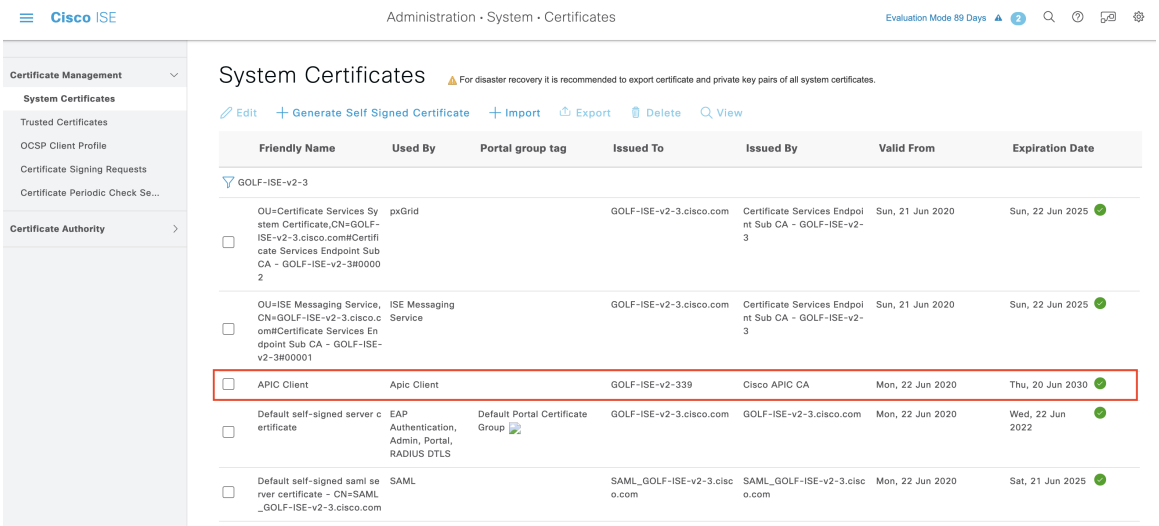
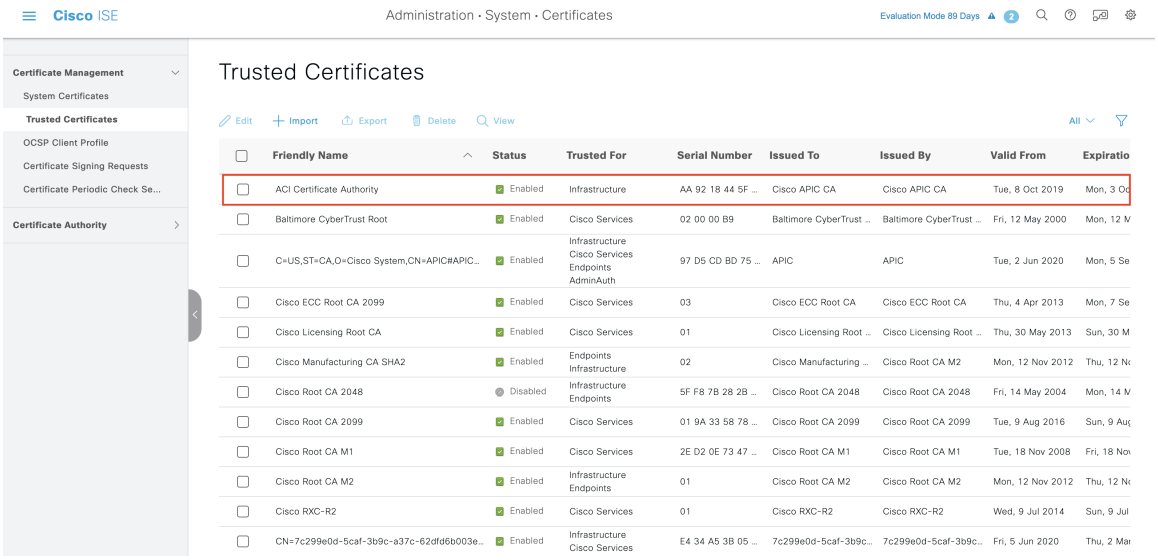


图 *19:* 在“受信任证书”*(Trusted Certificates)* 窗口中验证证书



按用户报告运行前 N 个 RBACL 丢包

可以按用户报告运行前 N 个 RBACL 丢包，以便按特定用户查看策略违规（基于丢包）。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**操作 (Operations)** > **报告 (Reports)** > **TrustSec**。

步骤 2 点击 **Top N RBACL Drops by User**。

步骤 3 从 **Filters** 下拉菜单中添加所需的监控模式。

步骤 4 相应地输入选定参数的值。可以从 Enforcement mode 下拉列表中将模式指定为 Enforce、Monitor 或 Both。

步骤 5 从 **Time Range** 下拉菜单中选择将收集报告数据的时间段。

步骤 6 点击**运行 (Run)** 在特定时间段内运行报告，以及选定的参数。