威胁控制

以威胁防护为中心的 NAC 服务

凭借以威胁防护为中心的网络访问控制 (TC-NAC) 功能，您可依据接收自威胁和漏洞适配器的威胁和漏洞属性创建授权策略。

威胁严重级别和漏洞评估结果可用于动态控制终端或用户的访问级别。

您可以配置漏洞和威胁适配器来向思科 ISE 发送高保真危害表现 (IoC)、检测到威胁事件和 CVSS 分数，以便创建以威胁防护为中心的访问策略来相应地更改终端的授权和情景。

思科 ISE 支持以下适配器：

- SourceFire FireAMP
- Qualys

注释 TC-NAC 流目前仅支持 Qualys 企业版。

当检测到终端威胁事件时，可以在**受到危害的终端 (Compromised Endpoints)** 窗口选择该终端的 MAC 地址并应用一个 ANC 策略，例如隔离。思科 ISE 对该终端触发 CoA 并应用相应的 ANC 策略。如果 ANC 策略不可用，则思科 ISE 对该终端触发 CoA 并应用原始的授权策略。可以使用**受到危害的终端 (Compromised Endpoints)** 窗口上的**清除威胁和漏洞 (Clear Threat and Vulnerabilities)** 选项来（从思科 ISE 系统数据库）清除与某终端关联的威胁和漏洞。

以下属性列在威胁 (Threat) 字典下：

- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score

基础评分 (Base Score) 和临时分数 (Temporal Score) 属性的有效范围均为 0 至 10。

当收到某个终端的漏洞事件时，思科 ISE 对该终端触发 CoA。但是，在收到威胁事件时不会触发 CoA。

您可以通过使用漏洞属性来创建授权策略，从而基于属性值自动隔离易受攻击的终端。例如：

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

要查看在 CoA 事件期间自动隔离的终端的日志，请选择**操作 (Operations)** > **以威胁防护为中心的 NAC 实时日志 (Threat-Centric NAC Live Logs)**。要查看手动隔离的终端的日志，请选择**操作 (Operations)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。

启用以威胁防护为中心的 NAC 服务时，请注意以下几点：

- 以威胁防护为中心的 NAC 服务需要思科 ISE Apex 许可证。
- 在一个部署中，只能在一个节点上启用以威胁防护为中心的 NAC 服务。
- 对于漏洞评估服务，每个供应商只能添加一个适配器实例。但是，您可以添加多个 FireAMP 适配器实例。

您可以在以下页面上查看终端的威胁信息：

- **主页 (Home page)** > **威胁控制面板 (Threat dashboard)**
- **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **受到危害的终端 (Compromised Endpoints)**

以下警报由以威胁防护为中心的 NAC 服务触发：

- 无法访问适配器（系统日志 ID：91002）：表示适配器无法访问。
- 适配器连接失败（系统日志 ID：91018）：表示适配器可访问，但是适配器和源服务器之间的连接已中断。
- 适配器因出错而停止工作（系统日志 ID：91006）：如果适配器未处于所需状态，则触发此警报。如果显示此警报，请检查适配器配置和服务器连接。有关详细信息，请参阅适配器日志。
- 适配器错误（系统日志 ID：91009）：表示 Qualys 适配器无法与 Qualys 站点建立连接或通过其下载信息。

以下报告可用于以威胁防护为中心的 NAC 服务：

- **适配器状态 (Adapter Status)**：适配器状态报告显示威胁和漏洞适配器的状态。
- **COA 事件 (COA Events)**：当收到某个终端的漏洞事件时，思科 ISE 对该终端触发 CoA。CoA 事件报告显示这些 CoA 事件的状态。同时显示这些终端的新旧授权规则和配置文件详细信息。
- **漏洞评估 (Vulnerability Assessment)**：漏洞评估报告提供您的终端正在进行的评估的信息。您可以查看此报告以确认评估是否以配置策略为基础正在进行。
- 收到事件的总数
- 威胁事件的总数
- 漏洞事件的总数
- 发出（到 PSN）的 CoA 的总数

威胁 (Threat) 控制面板包含以下 Dashlet：

- **受到危害的终端总数 (Total Compromised Endpoints)** Dashlet 显示当前网络中受影响的终端总数（包括连接和断开连接的终端）。
- **特定时段受危害的终端 (Compromised Endpoints Over Time)** Dashlet 显示特定时间段内对终端影响的历史视图。
- **首要威胁 (Top Threats)** Dashlet 显示基于受影响的终端数量和威胁的严重程度的首要威胁。
- 可以使用**威胁关注列表 (Threats Watchlist)** Dashlet 分析所选事件的趋势。

首要威胁 (Top Threats) Dashlet 中的气泡大小表示受影响终端的数量，而浅色面积表示断开连接终端的数量。颜色和垂直刻度表示威胁的严重程度。威胁分为两类 - 指标和事故。指标的严重程度属性是“Likely_Impact”，而事故的严重程度属性是“Impact_Qualification”。

“受到危害的终端” (Compromised Endpoint) 窗口会显示受影响终端的矩阵视图以及各个威胁类别的影响严重性。您可以点击设备链接以查看某终端的详细威胁信息。

在主页 (Home) 上的漏洞 (Vulnerability) 控制面板包含以下 Dashlet：

- **易受攻击的终端总数 (Total Vulnerable Endpoints)** Dashlet 显示 CVSS 分数大于指定值的终端总数。此外，还显示 CVSS 分数大于指定值的连接和断开连接的终端总数。
- **首要漏洞 (Top Vulnerability)** Dashlet 显示基于受影响的终端数量或漏洞的严重程度的首要漏洞。首要漏洞 (Top Vulnerability) Dashlet 中的气泡大小表示受影响终端的数量，而浅色面积表示断开连接终端的数量。颜色和垂直刻度表示漏洞的严重程度。
- 可以使用**漏洞关注列表 (Vulnerability Watchlist)** Dashlet 分析一段时间内所选漏洞的趋势。点击 Dashlet 中的搜索图标并输入供应商特定 ID（Qualys ID 号码为“qid”）以选择和查看该特定 ID 号码的趋势。
- **特定时段易受攻击终端 (Vulnerable Endpoints Over Time)** Dashlet 显示一段时间内对终端的影响的历史视图。

易受攻击的终端 (Vulnerable Endpoints) 窗口上的“按 CVSS 排序的终端数”(Endpoint Count By CVSS) 图表显示受影响终端的数量及其 CVSS 分数。在**易受攻击的终端 (Vulnerable Endpoints)** 窗口，还可以查看受影响的终端列表。可以点击设备链接以查看各个终端的详细漏洞信息。

支持捆绑包中包含以威胁防护为中心的 NAC 服务日志。以威胁防护为中心的 NAC 服务日志位于 support/logs/TC-NAC/

启用威胁中心 NAC 服务

要配置漏洞和威胁适配器，您必须首先启用威胁中心NAC服务。此服务只可在您部署中的一个策略服务节点上启用。

步骤 1

步骤 2 选中要启用威胁中心 NAC 服务的 PSN 旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 选中**启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)** 复选框。

步骤 4 点击**保存 (Save)**。

相关主题

添加 Sourcefire FireAMP 适配器， 第 4 页
配置感知威胁分析适配器
为 CTA 适配器配置授权配置文件
使用操作过程属性配置授权策略
以威胁防护为中心的 NAC 服务， 第 1 页

添加 Sourcefire FireAMP 适配器

开始之前

- 您必须有一个配有 SourceFire FireAMP 的账户。
- 您需要在所有终端部署 FireAMP 客户端。
- 您需要在部署节点上启用以威胁防护为中心的 NAC 服务（请参阅启用威胁中心 NAC 服务，第 4 页）。
- FireAMP 适配器使用 SSL 进行 REST API 调用（对于 AMP 云），并使用 AMQP 接收事件。它还支持使用代理。FireAMP 适配器使用端口 443 进行通信。

步骤 1

步骤 2 点击**添加 (Add)**。

步骤 3 从**提供商 (Vendor)**下拉列表中选择 **AMP：威胁防护 (AMP : Threat)**。

步骤 4 输入适配器实例的名称。

步骤 5 点击**保存 (Save)**。

步骤 6 刷新“供应商实例列表”(Vendor Instances listing) 窗口。在“供应商实例列表”(Vendor Instances listing) 窗口中，仅在适配器状态变为**配置就绪 (Ready to Configure)** 之后，您才可配置适配器。

步骤 7 点击**准备配置 (Ready to Configure)** 链接。

步骤 8 （可选）如果您配置了 SOCKS 代理服务器用于路由所有流量，请输入主机名和该代理服务器的端口号。

步骤 9 选择您想要连接的云。您可以选择 US 云或 EU 云。

步骤 10 点击 FireAMP 链路并以管理员的身份登录 FireAMP。点击**应用 (Applications)** 窗格中的**允许 (Allow)**，以授权流事件导出请求。
您将被重定向回到思科 ISE。

步骤 11 选择您要监控的事件（例如，可疑下载、连接到可疑域、已执行恶意软件、Java 威胁）。

适配器实例配置摘要将在**配置摘要 (Configuration Summary)** 页面中显示。

思科 ISE 中的漏洞评估支持

来自生态系统合作伙伴的结果被转换为结构化威胁信息表达式 (STIX)表示，然后基于该值根据需要触发授权更改 (CoA)，并授予终端相应的访问权限级别。

评估终端漏洞所需的时间取决于多种因素，因此无法实时执行 VA。影响评估终端漏洞所需时间的因素包括：

- 漏洞评估生态系统
- 扫描的漏洞类型
- 启用的扫描类型
- 生态系统为扫描设备分配的网络和系统资源

在此版本的思科 ISE 中，仅对采用 IPv4 地址的终端进行漏洞评估。

支持的漏洞评估生态系统合作伙伴

思科 ISE 支持 Qualys，Qualys 是一种基于云的评估系统，其在网络中部署有扫描设备。

思科 ISE 允许您配置与 Qualys 通信并获取 VA 结果的适配器。您可以从管理门户配置适配器。您需要具有超级管理员权限的思科 ISE 管理员帐户来配置适配器。

Qualys 适配器使用 REST API 与 Qualys 云服务进行通信。您需要 Qualys 中具有管理器权限的用户帐户来访问 REST API。思科 ISE 使用以下 Qualys REST API：

- 托管检测列表 API - 检查终端的最后一次扫描结果
- 扫描 API - 触发终端的按需扫描

Qualys 对已订阅用户可进行的 API 调用数量实施限制。默认速率限制数为每 24 小时 300 次。

思科 ISE 使用 Qualys API 版本 2.0 连接到 Qualys。请参阅 Qualys API V2 用户指南，以了解这些 API 功能的详细信息。

Qualys 漏洞评估流程

1. 终端发送请求到 NAD
2. NAD 向思科 ISE 发送身份验证请求。
3. 终端会得到身份验证，并获得网络访问权限。
4. 在思科 ISE 上运行的 VA 服务发送请求到 Qualys，以扫描终端。基于思科 ISE 中的 Qualys 适配器实例配置，Qualys 执行以下操作之一：
   - 扫描终端。
   - 根据终端 IP 地址从数据库获取最后一次扫描的结果。或者，您可以在使用最后一次扫描结果时，使用终端的 MAC 地址。
5. Qualys 将 CVSS 得分返回到思科 ISE。
6. 根据 Qualys 返回的 CVSS 得分和您在思科 ISE 中配置的策略，TC-NAC 核心引擎容器（在思科 ISE 上运行的进程）可以发出授权变更 (CoA) 以授予对终端的完全、有限或或无访问权限。

启用并配置漏洞评估服务

要启用和配置思科 ISE 的漏洞评估服务，请执行以下任务：

开始之前

请在启用以威胁防护为中心的 NAC 服务时注意以下问题：

- 在一个部署中，只能在一个节点上启用以威胁防护为中心的 NAC 服务
- 您只能每供应商添加一个适配器实例

步骤 1 启用威胁中心 NAC 服务，第 4 页。
步骤 2 配置 Qualys 适配器，第 7 页。
步骤 3 配置授权配置文件，第 10 页。
步骤 4 配置隔离易受攻击的终端的例外规则，第 10 页。

启用威胁中心 NAC 服务

要配置漏洞和威胁适配器，您必须首先启用威胁中心NAC服务。此服务只可在您部署中的一个策略服务节点上启用。

步骤 1

步骤 2 选中要启用威胁中心 NAC 服务的 PSN 旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 选中**启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)** 复选框。

步骤 4 点击**保存 (Save)**。

相关主题

添加 Sourcefire FireAMP 适配器，第 4 页
配置感知威胁分析适配器
为 CTA 适配器配置授权配置文件
使用操作过程属性配置授权策略
以威胁防护为中心的 NAC 服务，第 1 页

配置 Qualys 适配器

思科 ISE 支持 Qualys 漏洞评估生态系统。您必须创建一个 Qualys 适配器供思科 ISE 与 Qualys 通信和获取 VA 结果。此思科 ISE 版本仅支持每个供应商一个适配器。

开始之前

- 您必须拥有以下用户帐户：
  - 带可配置供应商适配器的超级管理员权限的思科 ISE 的管理员用户帐户。
  - 带管理器权限的 Qualys 用户帐户
- 确保您拥有适当的 Qualys 许可证订用。您需要 Qualys 报告中心、知识库 (KBX) 和 API 的访问权限。有关详细信息，请联系您的 Qualys 客户经理。
- 将 Qualys 服务器证书导入思科 ISE 的受信任证书库（**管理 (Administration) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates) > 导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）思科 ISE 受信任证书库中。
- 请参阅《Qualys API 指南》以了解以下配置：
  - 确保已启用 Qualys CVSS 评分（**报告 (Reports) > 设置 (Setup) > CVSS 评分 (CVSS Scoring) > 启用 CVSS 评分 (Enable CVSS Scoring)**）。
  - 确保添加了 IP 地址和 Qualys 终端子网掩码（**资产 (Assets) > 主机资产 (Host Assets)**）。
  - 确保拥有 Qualys 选项配置文件的名称。选项配置文件是 Qualys 用于扫描的扫描器模板。我们建议您使用包括身份验证扫描的选项配置文件（此选项也检查终端的 MAC 地址）。
- 思科 ISE 通过 HTTPS/SSL （端口443）与 Qualys 通信。

步骤 1

步骤 2 点击**添加 (Add)**。

步骤 3 从**供应商 (Vendor)** 下拉列表中选择**Qualys:VA**。

步骤 4 输入适配器实例的名称。例如，Qualys_Instance。

系统会显示一个列表窗口，其中包含配置的适配器实例列表。

步骤 5 刷新“供应商实例列表”(Vendor Instances listing) 窗口。新添加的 Qualys_Instance 适配器的状态应更改为**准备配置 (Ready to Configure)**。

步骤 6 点击**准备配置 (Ready to Configure)** 链接。

步骤 7 在 Qualys 配置屏幕输入以下值并点击**下一步 (Next)**。

字段名称	说明
REST API 主机	托管 Qualys 云的服务器的主机名。请联系 Qualys 代表以获得此信息。
REST API 端口	443
用户名	具有管理器权限的 Qualys 用户帐户。
密码	Qualys 帐户的密码。
HTTP 代理主机 (HTTP Proxy Host)	如果您拥有配置为路由所有 Internet 流量的代理服务器，输入该代理服务器的主机名。
HTTP 代理端口 (HTTP Proxy Port)	输入代理服务器使用的端口号。

如果与 Qualys 服务器建立了连接，将显示“扫描仪映射”(Scanner Mappings) 窗口，其中包含 Qualys 扫描仪列表。您网络中的 Qualys 扫描仪将显示在此窗口中。

步骤 8 选择思科 ISE 用于按需扫描的默认扫描仪。

步骤 9 在 **PSN 到扫描仪映射 (PSN to Scanner Mapping)** 区域中，选择一个或多个到 PSN 节点的 Qualys 扫描仪设备，然后点击**下一步 (Next)**。

系统将显示**高级设置 (Advanced Settings)** 窗口。

步骤 10 在**高级设置 (Advanced Settings)** 窗口中输入以下值。此窗口中的设置确定按需扫描是否会触发或最后扫描结果将用于 VA。

字段名称	说明
选项配置文件	选择要 Qualys 用于端口的选项配置文件。您可以选择默认选项配置文件初始选项。
最后扫描结果 - 检查设置	
最后扫描结果检查间隔（按分钟计）	（影响主机检测列表 API 的接入速率）时间间隔（按分钟计），该时间后会再次检查最后扫描结果。有效范围为 1 到 2880。

字段名称	说明
检查最后扫描结果之前的最大结果数	（影响主机检测列表 API 的接入速率）如果队列扫描请求数超过此处指定的最大数量，最后扫描结果会在**最后扫描结果检查间隔（按分钟计）(Last scan results check interval in minutes)** 之前接受检查。有效范围为 1 到 1000。
验证 MAC 地址	正确还是错误？当设置为 true 时，Qualys 的最后扫描结果只会在春包括终端的 MAC 地址时使用。
扫描设置	
扫描触发间隔（按分钟计）	（影响扫描 API 接入速率）时间间隔（按分钟计），该时间后按需扫描会触发。有效范围为 1 到 2880。
在扫描触发之前的最大请求数	（影响扫描 API 的接入速率）如果队列扫描请求数超过此处指定的最大数量，按需扫描会在**扫描触发间隔（按分钟计）(Scan trigger interval in minutes)** 字段中的指定时间间隔之前被触发。有效范围为 1 到 1000。
扫描状态检查间隔（按分钟计）	思科 ISE 与 Qualys 通信以检查扫描状态的时间间隔（按分钟计）。有效范围为 1 到 60。
可同时触发的扫描数量	（此选项取决于您映射到在扫描仪映射屏幕的每个节点的扫描仪数量）每个扫描仪每次只能处理一个请求。如果映射了一个以上扫描仪到 PSN，则可以根据选定的扫描仪数量增加此值。有效范围为 1 到 200。
扫描超时（按分钟计）	时间（按分钟计），该时间后扫描请求将超时。如果扫描请求超时，将生成警报。有效范围为 20 到 1440。
每个扫描仪将提交的 IP 地址最大数量	指示可排列为一个请求以发送到 Qualys 进行处理的请求数。有效范围为 1 到 1000。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG) 和“跟踪”(TRACE)。

步骤 11 点击**下一步 (Next)** 以审核配置设置。

步骤 12 点击**完成**。

Qualys 适配器实例的状态更改为“活动”。有关如何在授权配置文件中启用 VA 服务的信息，请参阅配置授权配置文件，第 10 页。

配置授权配置文件

思科 ISE 中的授权配置文件现在包括扫描漏洞终端的选项。您可以选择定期运行扫描，并指定这些扫描的时间间隔。定义授权配置文件后，可以将其应用于现有授权策略规则，或创建新的授权策略规则。

开始之前

您必须已启用以威胁防护为中心的 NAC 服务，并且已配置供应商适配器。

步骤 1

步骤 2 创建新授权配置文件或编辑现有配置文件。

步骤 3 从**常见任务 (Common Tasks)** 区域中，选中**评估漏洞 (Assess Vulnerabilities)** 复选框。

步骤 4 从**适配器实例 (Adapter Instance)** 下拉列表中，选择已配置的供应商适配器。例如，Qualys_Instance。

步骤 5 如果上一次扫描的时间大于文本框中的时间，请在触发扫描字段中输入以小时为单位的扫描间隔。有效范围为 1 到 9999。

步骤 6 勾选**按上述间隔定期评估 (Assess periodically using above internval)** 复选框。

步骤 7 点击**提交 (Submit)**。

配置隔离易受攻击的终端的例外规则

您可以使用以下漏洞评估 (Vulnerability Assessment) 属性来配置一个例外规则，并提供对以下易受攻击终端的有限访问权限：

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score

这些属性在威胁目录下可用。有效值范围为 0 到 10。

您可以选择隔离终端，提供有限访问权限（重定向至不同的门户）或拒绝请求。

步骤 1 系统会显示授权策略页面。您可以编辑现有策略规则或创建新例外规则，以检查 VA 属性。

步骤 2 创造条件检查 Qualys 评分并分配正确的授权配置文件。例如：

任何身份组和 Threat:Qualys-CVSS_Base_Score (Any Identity Group & Threat:Qualys-CVSS_Base_Score) > 5 -> 隔离（授权配置文件）(Quarantine (authorization profile))

步骤 3 点击**保存 (Save)**。

漏洞评估日志

思科 ISE 为故障排除 VA 服务提供以下日志。

- vaservice.log - 包含 VA 核心信息，在运行 TC-NAC 服务的节点上可用。
- varuntime.log - 包含终端和 VA 流程的信息；在监控节点和运行 TC-NAC 服务的节点上可用。
- vaaggregation.log - 包含终端漏洞的每小时汇聚详细信息，在主管理节点上可用。

部署和节点设置

您可以通过**部署节点 (Deployment Nodes)** 窗口配置思科 ISE（PAN、PSN 和 MnT）节点和内联终端安全评估节点并设置部署。

部署节点列表窗口

表 *1:* 部署节点列表

字段名称	使用指南
主机名	显示节点的主机名。
Node Type	显示节点类型。 它可以是下列类型之一： • 思科 ISE（PAN、PSN、Mnt）节点 • Inline Posture 节点
相关角色	（只有在节点类型为思科 ISE 时才显示）列出思科 ISE 节点承担的角色，例如管理 (Administration)、策略服务 (Policy Service)、监控 (Monitoring) 或 pxGrid。 例如，**管理 (Administration)**、**策略服务 (Policy Service)**、**监控 (Monitoring)** 或 **pxGrid**。
角色	如果在此节点上启用了管理和监控角色，则指示管理和监控角色承担的职责（主要、辅助或独立职责）。职责可以是以下一项或多项： • **PRI(A)**：指主 PAN。 • **SEC(A)**：指辅助 PAN。 • **PRI(M)**：指主 MnT。 • **SEC(M)**：指辅助 MnT。

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

相关主题

思科 ISE 分布式部署
思科 ISE 部署术语
配置思科 ISE 节点
注册辅助思科 ISE 节点

常规节点设置

下表说明思科 ISE 节点的**常规设置 (General Settings)** 窗口中的字段。在此窗口中，可以将角色分配给节点并配置要在其上运行的服务。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **部署节点 (Deployment Node)** > **编辑 (Edit)** > **常规设置 (General Settings)** 。

表 *2:* 常规节点设置

字段名称	使用指南
主机名	显示思科 ISE 节点的主机名。
FQDN	显示思科 ISE 节点的完全限定域名，例如 ise1.cisco.com。
IP 地址	显示思科 ISE 节点的 IP 地址。
Node Type	显示节点类型。可以为以下任一项：身份服务引擎 (ISE)、Inline Posture 节点
相关角色	

字段名称	使用指南
管理	如果思科 ISE 节点承担管理角色，请选中此复选框。只有在受许可提供管理服务的节点上才可以启用 Administration 角色。 **角色 (Role)** - 显示管理角色在部署中承担的职责。个人可以选择其中一种值 - **独立 (Standalone)**、**主要 (Primary)** 或**辅助 (Secondary)**。 **设为主要 (Make Primary)** - 选择它可使该节点成为主思科 ISE 节点。在部署中您只能有一个主要思科 ISE 节点。当您将此节点设置为主要节点之后，此窗口中的其他选项将进入活动状态。在部署中您只能有两个 Administration 节点。如果节点具有**独立 (Standalone)** 角色，则旁边会显示**设为主要 (Make Primary)** 按钮。如果节点具有**辅助 (Secondary)** 角色，则旁边会显示**升级为主要 (Promote to Primary)** 按钮。如果节点具有**主要 (Primary)** 角色，并且没有其他节点注册到该节点，则旁边会显示**设为独立 (Make Standalone)** 按钮。点击**设为独立 (Make Standalone)** 按钮以使您的主要节点成为独立节点。
Monitoring	如果要思科 ISE 节点承担监控角色并充当日志收集器，请选中此复选框。分布式部署中必须至少有一个监控节点。配置主 PAN 时，必须启用监控角色。在部署中注册辅助监控节点之后，如有必要，可以编辑主 PAN 和禁用监控角色。 要在 VMware 平台上将思科 ISE 节点配置为您的日志收集器，请使用以下规定确定您所需要的最低磁盘空间：您的网络中每天每个终端 180 KB，您的网络中每天每个思科 ISE 节点 2.5 MB。 您可以根据您想要将多少个月的数据至于监控模式下，计算您所需的最大磁盘空间。如果您的部署中只有一个监控节点，则该节点会承担独立职责。如果在部署中有两个监控节点，思科 ISE 还会显示另一个监控节点的名称以供您配置主要/辅助角色。要配置这些职责，请选择以下选项之一： • **主 (Primary)**：使当前节点成为主监控节点。 • **辅助 (Secondary)**：使当前节点成为辅助监控节点。 • **无 (None)** - 如果要使监控节点不承担主要-辅助角色。 如果您将您的一个监控节点配置为主要或辅助节点，另一个监控节点相应地自动成为辅助或主要节点。主要监控节点和辅助监控节点都接收管理和策略服务日志。如果将一个监控节点的角色改为**无 (None)**，则另一个监控节点的角色也会成为**无 (None)**，从而会在您将某个节点指定为监控节点之后取消高可用性对。您会在**远程日志记录目标 (Remote Logging Targets)** 窗口中发现此节点被列为系统日志目标：**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

字段名称	使用指南
策略服务	选中此复选框可启用以下任一或所有服务： • **启用会话服务 (Enable Session Services)**：选中此复选框可启用网络访问、终端安全评估、访客和客户端调配服务。从**在节点组中包含节点 (Include Node in Node Group)** 下拉列表中选择此策略服务节点所属的组。请注意，证书颁发机构 (CA) 和安全传输注册 (EST) 服务只能在已启用会话服务的策略服务节点上运行。 对于**在节点组中包含节点 (Include Node in Node Group)**，如果不希望此策略服务节点加入某个组，请选择**无 (None)**。 同一个节点组中的所有节点都应在网络接入设备上配置为 RADIUS 客户端，并获CoA授权，因为这些节点中的任何一个节点均可为通过节点组中的任何节点建立的会话发出CoA请求。如果您未使用负载均衡器，则节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或作为 RADIUS 服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。 虽然单个 NAD 可以配置多个思科 ISE 节点以作为 RADIUS 服务器和动态授权客户端，但节点不必全部位于同一个节点组。 一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。有关详细信息，请参阅创建策略服务节点组。 • **启用分析服务 (Enable Profiling Service)**：选中此复选框可启用分析服务。如果启用分析服务，必须点击**分析配置 (Profiling Configuration)** 选项卡并根据要求输入详细信息。当您启用或禁用策略服务节点上运行的任意服务或对此节点做任何更改时，您将重新启动运行这些服务的应用服务器进程。这些服务重新启动时，预计会有延迟。您可以从 CLI 使用 **show application status ise** 命令，确定何时在节点上重新启动了应用服务器。
pxGrid	选中此复选框可启用 pxGrid 角色。思科 pxGrid 用于将来自思科 ISE 会话目录区分上下文的信息共享给其他策略网络系统，如思科自适应安全设备 (ASA)。此pxGrid框架还可用于在节点之间交换策略和配置数据，例如在思科ISE和第三方供应商之间共享标签和策略对象，以及交换威胁信息等非思科 ISE 相关信息。

相关主题

- 分布式思科 ISE 部署中的角色
- 管理节点
- 策略服务节点
- 监控节点
- 思科 pxGrid 节点
- 同步主要和辅助思科 ISE 节点
- 创建策略服务节点组

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

分析节点的设置

下表介绍**分析配置 (Profiling Configuration)** 窗口上的字段，您可以使用此窗口为分析器服务配置探测功能。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **ISE 节点 (ISE Node)** > **编辑 (Edit)** > **分析配置 (Profiling Configuration)**。

表 *3:* 分析节点的设置

字段名称	使用指南
NetFlow	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 NetFlow，以便接收从路由器发送的 NetFlow 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择思科 ISE 节点上的接口。 • **端口 (Port)**：输入从路由器接收 NetFlow 导出数据的 NetFlow 侦听器端口号。默认端口为 9996。
DHCP	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项提供值： • **接口 (Interface)**：选择思科 ISE 节点上的接口。 • **端口 (Port)**：输入 DHCP 服务器 UDP 端口号。默认端口为 67。
DHCP SPAN	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便收集 DHCP 数据包。 • **接口 (Interface)**：选择思科 ISE 节点上的接口。
HTTP	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 • **接口 (Interface)**：选择思科 ISE 节点上的接口。
RADIUS	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 RADIUS 服务器，以便收集 RADIUS 会话属性，以及来自已启用思科 IOS 传感器的设备的思科设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
Network Scan (NMAP)	选中此复选框可启用 NMAP 探测。

字段名称	使用指南
DNS	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DNS，以便对 FQDN 执行 DNS 查找。以秒为单位输入**超时 (Timeout)** 期间。 注释 要使 DNS 探测功能在分布式部署中特定思科 ISE 节点上运行，您必须启用这些探测功能 - DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用这些探测功能之一。
SNMP Query	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。在**重试 (Retries)**、**超时 (Timeout)**、**事件超时 (Event Timeout)**（必填）和**说明 (Description)**（可选）字段中输入值。 注释 除配置 SNMP 查询探测功能之外，还必须在**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** 中配置其他 SNMP 设置。当在网络设备上配置 SNMP 设置时，请确保在网络设备上全局启用 CDP 和 LLDP。
SNMP 陷阱	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 陷阱探测，以便从网络设备接收链路接通、链路断开和 MAC 通知陷阱。提供或启用以下信息： • **链接陷阱查询 (Link Trap Query)**：选中此复选框可接收和解释通过 SNMP 陷阱接收的通知。 • **MAC 陷阱查询 (MAC Trap Query)**：选中此复选框可接收和解释通过 SNMP 陷阱接收的 MAC 通知。 • **接口 (Interface)**：选择思科 ISE 节点上的接口。 • **端口 (Port)**：输入要使用的主机 UDP 端口。默认端口为 162。
Active Directory	选中此复选框可扫描所定义的 Active Directory 服务器，以获取有关 Windows 用户的信息。 • **重新扫描前的天数 (Days before rescan)**：选择您希望经过多少天后再次运行扫描。

相关主题

思科 ISE 分析服务

分析服务使用的网络探测功能

在思科 ISE 节点中配置分析服务

Inline Posture 节点设置

受信任证书设置

表 *4:* 受信任证书编辑设置

字段名称	使用指南
证书颁发者 (Certificate Issuer)	
友好名称 (Friendly Name)	输入证书的友好名称。此字段是可选字段。如果不输入友好名称，则系统会以以下格式生成默认名称： *common-name#issuer#nnnnn*
状态 (Status)	从下拉列表中选择**启用 (Enabled)** 或**禁用 (Disabled)**。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。
Description	（可选）输入说明。
使用情况 (Usage)	
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您想要使用此证书验证服务器证书（从其他思科 ISE 节点或 LADP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅在选中了**信任 ISE 中的身份验证” (Trust for authentication within ISE)** 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至思科 ISE 的终端进行身份验证。 • 信任系统日志服务器。
信任基于证书的管理员身份验证	仅当选择**信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)** 时，才能选中此复选框。 选中此复选框可启用基于证书的身份验证用于管理员访问。将所需的证书链导入受信任证书存储区。
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部思科服务，请选中此复选框。

字段名称	使用指南
证书状态验证 (Certificate Status Validation)	思科 ISE 支持使用两种方法检查特定 CA 颁发的客户端或服务器证书的吊销状态。第一种方法是使用在线证书状态协议 (OCSP) 验证证书，其将向 CA 维护的 OCSP 服务发送请求。第二种方法是按照从 CA 下载至思科 ISE 的 CRL 验证证书。可以同时启用这两种方法，在这种情况下首先使用 OCSP 方法，只有在无法确定证书状态时，才会使用 CRL 方法。
验证 OCSP 服务 (Validate Against OCSP Service)	选中此复选框以按照 OCSP 服务验证证书。您必须先创建 OCSP 服务才能选中此复选框。
如果 OCSP 返回未知状态则拒绝请求 (Reject the request if OCSP returns UNKNOWN status)	如果 OCSP 服务无法确定证书状态，则选中此复选框以拒绝请求。在选中此复选框的情况下，如果 OCSP 服务返回未知状态值，此服务将导致思科 ISE 拒绝当前评估的客户端或服务器证书。
下载 CRL (Download CRL)	选中此复选框以使思科 ISE 下载 CRL。
CRL 分类的 URL (CRL Distribution URL)	输入用于从 CA 下载 CRL 的 URL。如果在证书颁发机构证书中指定了 URL，则系统会自动填写此字段。URL 必须以“http”、“https”或“ldap”开头。
检索 (Retrieve CRL)	可以自动或定期下载 CRL。请配置下载时间间隔。
如果下载失败，请稍候 (If download failed, wait)	配置在思科 ISE 再次尝试下载 CRL 之前等待的时间间隔。
如果 CRL 没有收到，绕过此 CRL 验证 (Bypass CRL Verification if CRL is not Received)	选中此复选框，以使系统在收到CRL之前接受客户端请求。如果取消选中此复选框，思科 ISE 会拒绝使用选定 CA 签名的证书的所有客户端请求，直到收到 CRL 文件为止。
忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)	如果您希望思科 ISE 忽略开始日期和到期日期并继续使用非活动或已过期 CRL 以及根据 CRL 内容允许或拒绝 EAP-TLS 身份验证，请选中此复选框。 如果您希望思科 ISE 在 Effective Date 字段指定的开始日期和 Next Update 字段指定的到期日期检查 CRL 文件，请取消选中此复选框。如果 CRL 尚未激活或已到期，思科 ISE 会拒绝使用此 CA 签名的证书的所有身份验证。

相关主题

受信任证书库

编辑受信任证书

证书存储设置

通过“证书存储区”(Certificate Store) 窗口，您可以在思科 ISE 中配置可用于身份验证的证书。

自签证书设置

表 *5:* 自签证书设置

字段名称	使用指南
Select Node	（必填）从下拉列表中选择您要为其生成系统证书的节点。
Common Name (CN)	（如果您不指定 SAN，则此字段必填）默认情况下，Common Name 为您要生成自签证书的思科 ISE 节点的 FQDN。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
Organization (O)	组织名称。例如，Cisco。
City (L)	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。输入两个字母 ISO 国家/地区代码。例如，US。
主体可选名称 (SAN) (Subject Alternative Name [SAN])	与该证书关联的 。

字段名称	使用指南
密钥长度	公共密钥的位大小。从 RSA 的下拉列表中选择以下选项之一： • 512 • 1024 • 2048 • 4096 从 ECDSA 的下拉列表中选择以下选项之一： • 256 • 384 如果您计划获得公共 CA 签名的证书，请选择 2048。
Digest to Sign With	从下拉列表中选择以下散列算法之一： • SHA-1 • SHA-256
Expiration TTL	指定证书到期之前的天数。从下拉列表中选择值。
友好名称 **(Friendly Name)**	输入证书的友好名称。如果未指定名称，思科 ISE 会自动创建以下格式的名称：<common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
使用情况	选择必须使用此系统证书的服务： • **管理员 (Admin)**：用于确保与部署中的管理门户和思科 ISE 节点之间安全通信的服务器证书。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL 或 TLS 隧道的身份验证的服务器证书。 • **pxGrid**：用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务器证书。 • **门户 (Portal)**：用于确保与所有思科 ISE Web 门户的安全通信的服务器证书。

相关主题

系统证书

查看系统证书

生成自签证书

证书签名请求设置

通过思科 ISE，只需一个请求即可从管理门户为部署中的所有节点生成证书签名请求。此外，还可以选择为部署中的单个节点或多个两个节点生成证书签名请求。如果选择为单个节点生成证书签名请求，则 ISE 会自动在证书使用者的 CN 字段中替换特定节点的完全限定域名 (FQDN)。如果在 CN 字段中输入的域名不是节点的 FQDN，思科 ISE 将拒绝使用该证书进行身份验证。如果选择在证书的“主体可选名称 (SAN)”(Subject Alternative Name (SAN)) 字段中包含某个条目，则除了其他 SAN 属性之外，还必须输入 ISE 节点的 FQDN。如有必要，您还可以在 SAN 字段中添加其他 FQDN。如果选择为部署中的所有节点生成证书签名请求，请选中“允许通配符证书”(Allow Wildcard Certificates) 复选框，然后在 SAN 字段（“DNS 名称”(DNS name)）中输入通配符 FQDN 符号，例如，*.amer.example.com。如果计划对 EAP 身份验证使用证书，请不要在 CN= 字段中输入通配符值。

通过使用通配符证书，不再需要为每个思科 ISE 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (*)，可以在部署中的多个两个节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个思科 ISE 节点分配唯一服务器证书的安全性低。

表 *6:* 证书签名请求设置

字段	使用指南
证书将用于 **(Certificate(s) will be used for)**	

字段	使用指南
	选择即将对其使用证书的服务： **思科 ISE 身份证书** • **管理 (Admin)** - 用于服务器身份验证（以确保与管理员门户之间的安全通信，以及部署中 ISE 节点之间的安全通信）。签名 CA 的证书模板通常称为 Web 服务器证书模板。此模板具有以下属性： • **密钥用法 (Key Usage)**：数字签名（签名） • **扩展密钥用法 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **EAP 身份验证 (EAP Authentication)**：用于服务器身份验证。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **密钥用法 (Key Usage)**：数字签名（签名） • **扩展密钥用法 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) **注释** EAP-TLS 客户端证书需要使用数字签名密钥。 • **门户 (Portal)**：用于服务器身份验证（以确保与所有 ISE Web 门户之间的安全通信）。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **密钥用法 (Key Usage)**：数字签名（签名） • **扩展密钥用法 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) • **pxGrid** - 同时用于客户端和服务器身份验证（以确保 pxGrid 客户端与服务器之间的安全通信）。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： • **密钥用法 (Key Usage)**：数字签名（签名） • **扩展密钥用法 (Extended Key Usage)**：TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2) **注释** 建议您不要将包含值 2.5.29.37.0 的证书用于“扩展密钥用法”(Extended Key Usage) 属性中的任意用途对象标识符。如果将包含值 2.5.29.37.0 的证书用于“扩展密钥用法”(Extended Key Usage) 属性中的任意用途对象标识符，系统会将此证书视为无效，并显示以下错误消息： `source=local type=fatal message="unsupported certificate"` **思科 ISE 证书颁发机构颁发的证书** • **ISE 根 CA (ISE Root CA)** -（仅适用于内部 CA 服务）用于重新生成整个内部 CA 证书链，包括主 PAN 上的根 CA 和 PSN 上的辅助 CA。 • **ISE 中间 CA (ISE Intermediate CA)**：（仅适用于当 ISE 用作外部 PKI 的中间 CA 时的内部 CA 服务）用于在主 PAN 上生成中间 CA 证书，在 PSN 上生成从属 CA 证书。签名 CA 的

字段	使用指南
	证书模板通常称为辅助证书颁发机构。此模板具有以下属性： • **基本约束 (Basic Constraints)**：关键、是证书颁发机构 • **密钥用法 (Key Usage)**：证书签名、数字签名 • **扩展密钥用法 (Extended Key Usage)**：OCSP 签名 (1.3.6.1.5.5.7.3.9) • **更新 ISE OCSP 响应方证书 (Renew ISE OCSP Responder Certificates)**：（仅适用于内部 CA 服务）用于更新整个部署的 ISE OCSP 响应方证书（不是证书签名请求）。出于安全原因，建议您每六个月更新一次 ISE OCSP 响应方证书。
允许通配符证书 (Allow Wildcard Certificates)	选中此复选框以在 CN 中和/或证书的 SAN 字段的 DNS 名称中使用通配符 (*)。如果选中此复选框，系统会自动选择部署中的所有节点。必须在最左侧的标签位置使用星号 (*) 通配符。如果使用通配符证书，我们建议您对域名空间进行分区以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，可能会导致安全问题。
为这些节点生成 CSR (Generate CSRs for these Nodes)	选中要为其生成证书的节点旁边的复选框。要为部署中的选定节点生成 CSR，必须取消 Allow Wildcard Certificates 选项。
公共名称 (CN) (Common Name [CN])	默认情况下，公用名是您正为其生成证书签名请求的 ISE 节点的 FQDN。$FQDN$ 表示 ISE 节点的 FQDN。当为部署中的多个节点生成证书签名请求时，证书签名请求中的 Common Name 字段会替换为各个 ISE 节点的 FQDN。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
主体可选名称 (SAN) (Subject Alternative Name [SAN])	• **DNS 名称 (DNS name)**：如果选择“DNS 名称”(DNS name)，请输入 ISE 节点的完全限定域名。如果已启用 Allow Wildcard Certificates 选项，请指定通配符符号（域名前的星号和句号）。例如：*.amer.example.com。 • **IP 地址 (IP address)**：将与证书关联的 ISE 节点的 IP 地址。
密钥长度 (Key Length)	如果计划获取公共的 CA 签名证书或将思科 ISE 部署为符合 FIPS 标准的策略管理系统，请选择 2048 或更大长度。

字段	使用指南
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。

相关主题

- 证书签名请求
- 创建证书签名请求并将其提交给证书颁发机构
- 将 CA 签名的证书绑定到证书签名请求

终端证书概述窗口 (Endpoint Certificate Overview Window)

表 *7:* 证书管理概述 *(Certificate Management Overview)*

字段名称	使用指南
Node name	发出证书的策略服务节点 (PSN) 的名称。
Endpoint Certificates Issued	PSN 节点发出的终端证书的数量。
Endpoint Certificates Revoked	已吊销的证书的数量（已由 PSN 节点发出的证书）。
Endpoint Certificates Requests	PSN 节点处理的基于证书的身份验证请求数量。
Endpoint Certificates Failed	PSN 节点处理的失败身份验证请求数量。

注释 已过期或已撤销的证书将在 30 天后自动删除。

相关主题

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

系统证书导入设置

表 *8:* 系统证书导入设置

字段名称	说明
Select Node	（必填）从下拉列表中选择您要导入系统证书的思科 ISE 节点。
Certificate File	（必填）单击**浏览 (Browse)**，从本地系统中选择证书文件。
Private Key File	（必需）单击**浏览 (Browse)**，从本地系统中选择私钥文件。
密码	（必填）输入密码以解密私钥文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，思科 ISE 会自动创建以下格式的名称： <common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是一个唯一的五位数。
Allow Wildcard Certificates	如果要导入通配符证书，请选中此复选框。通配符证书使用通配符号（在域名前带一个星号和一个句点）。通配符证书会在组织中的多个主机之间共享。 如果选中此复选框，思科 ISE 会将此证书导入到部署中的所有其他节点。
	如果希望思科 ISE 验证证书扩展，请选中此复选框。如果选中此复选框，并且要导入的证书包含 CA 标志设为 true 的基本限制扩展，请确保密钥用法扩展存在。还必须设置 keyEncipherment 位和/或 keyAgreement 位。
使用情况	选择必须使用此系统证书的服务： • **管理员 (Admin)**：用于确保与部署中的管理门户和思科 ISE 节点之间安全通信的服务器证书。 **注释** 在主 PAN 上更改管理员角色证书的证书将在所有其他思科 ISE 节点上重新启动服务。 • **EAP 身份验证 (EAP Authentication)**：用于使用 EAP 协议建立 SSL 或 TLS 隧道的身份验证的服务器证书。 • **pxGrid**：用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务器证书。 • ：用于**经思科 ISE 消息传递的系统日志 (Syslog Over Cisco ISE Messaging)** 功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 • **门户 (Portal)**：用于确保与所有思科 ISE Web 门户的安全通信的服务器证书。

注释 如果证书是由其他第三方工具而不是思科 ISE 生成的，则无法将证书或其私钥导入思科 ISE。

相关主题

- 系统证书
- 查看系统证书
- 导入系统证书

受信任证书列表

表 *9:* 受信任证书窗口列

字段名称	使用指南
Friendly Name	显示证书的名称。
状态	此列会显示**已启用 (Enabled)** 或**已禁用 (Disabled)**。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。
Trusted for	显示以下一项或多项使用此证书的服务。 • 基础设施 • 思科服务 • 终端
Issued To	显示证书持有者的通用名称。
颁发者	显示证书颁发机构的通用名称。
Valid From	显示证书的颁发日期和时间。该值也称为“不早于”(Not Before) 证书属性。
到期日期	显示证书到期的日期和时间。该值也称为“不迟于”(Not After) 证书属性。
Expiration Status	提供有关证书到期状态的信息。此列会显示五个图标和提示消息类别： • 绿色：距到期还有 90 天以上 • 蓝色：距到期还有 90 天或更短 • 黄色：距到期还有 60 天或更短 • 橙色：距到期还有 30 天或更短 • 红色：已到期

相关主题

- 受信任证书库

查看受信任的证书
更改受信任证书库中的证书状态
在受信任的证书库中添加证书

受信任证书导入设置

表 *10:* 受信任证书导入设置

字段名称	说明
	点击**浏览 (Browse)** 从运行浏览器的计算机选择证书文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果您不指定名称，思科 ISE 会自动按照 <通用名称>#<颁发者>#<nnnnn> 的格式创建名称，其中 <nnnnn> 为唯一的五位数编号。
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您希望将此证书用于验证服务器证书（从其他 ISE 节点或 LDAP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅在选中了“信任 ISE 中的身份验证”(Trust for authentication within ISE) 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框： • 对使用 EAP 协议连接至 ISE 的终端进行身份验证 • 信任系统日志服务器
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部思科服务，请选中此复选框。
	（仅适用于同时选中“信任客户端身份验证和系统日志”(Trust for client authentication and Syslog) 选项和“证书扩展上启用验证”(Enable Validation of Certificate Extensions) 选项的情况下）确保有“keyUsage”扩展并且设置了“keyCertSign”位，而且有将 CA 标志设置为 true 的基本限制扩展。
说明 (Description)	输入可选的说明。

相关主题

受信任证书库
证书链导入
将根证书导入受信任证书库

OCSP 客户端配置文件设置

表 *11: OCSP* 客户端配置文件设置

字段名称	使用指南
Name	OCSP 客户端配置文件的名称。
说明	输入可选的说明。
启用辅助服务器	选中此复选框来以启用高可用性辅助 OCSP 服务器。
总是先访问主服务器	使用此选项以在尝试移至辅助服务器之前先检查主要服务器。即使之前已检查主要服务器并且发现主服务器无响应，思科 ISE 在移至辅助服务器之前仍会尝试向主要服务器发送请求。
在 ***n*** 分钟后回退至主服务器	当您希望思科 ISE 移至辅助服务器，然后再回退到主服务器时，请使用此选项。在这种情况下，系统将跳过所有其他请求，并按照该文本框中配置的时间使用辅助服务器。允许的时间范围是 1 至 999 分钟。
URL	输入主要和/或辅助 OCSP 服务器的 URL。
启用 **Nonce** 扩展支持	您可以配置一个作为 OCSP 请求的一部分发送的 Nonce。Nonce 会在 OCSP 请求中包含一个伪随机数。系统会验证在响应中接收的数值是否与请求中包含的此数相同。此选项可确保重放攻击无法利用旧通信数据。
验证响应签名	OCSP 响应器用以下一个证书为响应签名： • CA 证书 • 与 CA 证书不同的证书 为了使思科 ISE 验证响应签名，OCSP 响应器需要连同该证书一起发送响应，否则响应验证会失败，而且证书状态不可靠。根据 RFC，OCSP 可以使用不同的证书给响应签名。只要 OCSP 发送给响应签名的证书以供思科 ISE 进行验证，就会如此。如果 OCSP 使用思科 ISE 中未配置的其他证书给响应签名，响应验证将失败。

字段名称	使用指南
缓存条目生存时间 *n* 分钟 (Cache Entry Time To Live n Minutes)	以分钟为单位输入缓存项目在多长时间之后过期。来自 OCSP 服务器的每个响应都有一个 nextUpdate 值。此值显示服务器上接下来将于何时更新证书的状态。缓存 OCSP 响应时，系统会比较两个值（一个是来自配置的值，另一个是来自响应的值），系统会按照这两个值中最低的值将响应缓存相应的时间。如果 nextUpdate 值为 0，则根本不缓存响应。思科 ISE 将 OCSP 响应缓存所配置的时间。缓存不复制，也不是持久性的，所以当思科 ISE 重新启动时，系统会清除缓存。使用 OCSP 缓存是为了保持 OCSP 响应以及出于以下原因： • 减少网络流量和降低 OCSP 服务器对已知证书带来的负载 • 通过缓存已知证书状态提高思科 ISE 性能
清除缓存	点击 **清除缓存** 以清除连接至 OCSP 服务的所有证书颁发机构的条目。 在部署中，**清楚缓存**与所有节点交互并执行此操作。此机制可更新部署中的每个节点。

相关主题

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

内部 CA 设置

表 *12:* 内部 *CA* 设置

字段名称	使用指南
Disable Certificate Authority	点击此按钮以禁用内部 CA 服务。
主机名	运行 CA 服务的思科 ISE 节点的主机名。
相关角色	在运行 CA 服务的节点上启用的思科 ISE 节点角色。例如管理角色、策略服务角色等。

字段名称	使用指南
Role(s)	运行CA服务的思科ISE节点承担的职责。例如，独立、主要或辅助职责。
CA & OCSP Responder Status	启用或禁用
OCSP Responder URL	思科 ISE 节点用于访问 OCSP 服务器的 URL。

相关主题

思科 ISE CA 服务

配置思科 ISE 以使用证书对个人设备进行身份验证

证书模板设置

注释 在证书模板字段（“组织单位”[Organizational Unit]、“企业”[Organization]、“城市”[City]、“省”[State] 和“国家/地区”[Country]）中不支持 UTF-8 字符。如果在证书模板中使用 UTF-8 字符，则证书调配将会失败。

字段名称	使用指南
Name	（必填）输入证书模板的名称。例如，Internal_CA_Template。
Description	（可选）输入说明。
Common Name (CN)	（仅显示）公用名自动填充为用户名。
Organizational Unit (OU)	组织单位名称。例如，Engineering。
Organization (O)	组织名称。例如，Cisco。
城市 (L) (City [L])	（请勿缩写）城市名称。例如，圣何塞。
省/自治区/直辖市 (ST) (State [ST])	（请勿缩写）省/自治区/直辖市名称。例如，加州。
Country (C)	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
Subject Alternative Name (SAN)	（仅显示）终端的 MAC 地址。
Key Size	指定密钥大小为 1024 或更大数字。
SCEP RA Profile	选择 ISE Internal CA 或您已创建的外部 SCEP RA 配置文件。

字段名称	使用指南
Valid Period	输入证书的到期天数。

相关主题

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

日志记录设置

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

远程日志记录目标设置

下表介绍**远程日志记录目标 (Remote Logging Targets)** 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。此页面的导航路径为**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。单击**添加 (Add)**。

表 *13:* 远程日志记录目标设置

字段名称	使用指南
Name	为新的系统日志目标输入名称。
Target Type	从下拉列表中选择目标类型。默认值为 **UDP 系统日志 (UDP Syslog)**。
Description	输入新目标的简短说明。
IP 地址	输入将存储日志的目标计算机的 IP 地址或主机名。
端口	输入目标计算机的端口号。
Facility Code	从下拉列表中选择必须用于记录的系统日志设备代码。有效选项为 Local0 至 Local7。
Maximum Length	输入远程日志目标消息的最大长度。有效值为 200 至 1024 字节。
包括此目标的警报 (Include Alarms For This Target)	选中此复选框时，警报消息也会发送到远程服务器。

字段名称	使用指南
符合 RFC 3164 (Comply to RFC 3164)	选中此复选框时，即使使用了反斜线 (\)，发送到远程服务器的系统日志消息中的分隔符 (, ; { } \ \) 也不会转义。
Buffer Message When Server Down	当您从**目标类型 (Target Type)** 下拉列表中选择 **TCP 系统日志 (TCP Syslog)** 或**安全系统日志 (Secure Syslog)** 时，系统会显示此复选框。如果希望思科 ISE 在 TCP 系统日志目标或安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。思科 ISE 会在与目标的连接恢复时重新尝试将消息发送到目标。连接恢复后，将按从最旧到最新的顺序发送消息。缓冲消息会始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
Buffer Size (MB)	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。
Reconnect Timeout (Sec)	输入时间（以秒为单位），以便配置在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
Select CA Certificate	当您从**目标类型 (Target Type)** 下拉列表中选择 **安全系统日志 (Secure Syslog)** 时，系统会显示此下拉列表。从下拉列表中选择一个客户端证书。
Ignore Server Certificate Validation	当您从**目标类型 (Target Type)** 下拉列表中选择 **安全系统日志 (Secure Syslog)** 时，系统会显示此复选框。选中此复选框，以便让思科 ISE 忽略服务器证书身份验证并接受任何系统日志服务器。默认情况下，除非在禁用此复选框时系统处于 FIPS 模式，否则此选项设置为关闭。

相关主题

- 思科 日志记录机制
- 思科 ISE 系统日志
- 思科 ISE 消息目录
- 集合过滤器
- 事件抑制绕行过滤器
- 配置远程系统日志收集位置
- 配置集合过滤器

配置日志记录类别

下表介绍了可用于配置日志记录类别的字段。设置日志严重性级别，然后为日志记录类别的日志选择日志记录目标。此窗口的导航路径为**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

单击想要查看的日志记录类别旁边的单选按钮，单击**编辑 (Edit)**。下表对日志记录类别的编辑窗口中显示的字段进行了说明。

表 *14:* 日志记录类别设置

字段名称	使用指南
Name	显示日志记录类别的名称。
Log Severity Level	对于某些日志记录类别，默认情况下会设置此值，并且您无法对其进行编辑。对于某些日志记录类别，您可以从下拉列表中选择以下严重性级别之一： • **严重 (FATAL)**：紧急级别。此级别意味着您无法使用思科 ISE，并且必须立即采取必要的操作。 • **错误 (ERROR)**：此级别表示严重错误情况。 • **警告 (WARN)**：此级别表示正常但值得注意的情况。这是会为很多日志记录类别设置的默认级别。 • **信息 (Info)**：此级别表示供参考的消息。 • **调试 (DEBUG)**：此级别表示诊断错误消息。
Local Logging	选中此复选框可为本地节点上的类别启用日志记录事件。
目标	该区域允许您使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 区域之间转移目标，从而更改类别的目标。 **可用 (Available)** 区域包含本地（预定义）和外部（用户定义）的现有日志记录目标。 **选定 (Selected)** 区域最初为空，然后会显示为该类别选择的目标。

相关主题

思科 ISE 消息代码
配置远程系统日志收集位置
设置消息代码的严重性级别

维护设置

使用备份、恢复和数据清除功能，这些窗口可帮助您管理数据。

存储库设置

表 *15:* 存储库设置

字段	使用指南
Repository	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。

字段	使用指南
协议 (Protocol)	从可用协议中选择一个您想要使用的协议。
服务器名称 (Server Name)	（对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段）输入您想要在其上创存储库的服务器的主机名或 IPv4 地址。 注释　如果要添加具有 IPv6 地址的存储库，请确保 ISE eth0 接口已配置有 IPv6 地址。
路径 (Path)	输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。 此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。
用户名	（对于 FTP、SFTP 和 NFS 为必填字段）输入对指定服务器拥有写入权限的用户名。用户名可以包含字母数字和 _-。/@\$ 字符。
密码 (Password)	（对于 FTP、SFTP 和 NFS 为必填字段）输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、|、@、#、$、^、&、*、(、)、+、和 =。

相关主题

备份和恢复存储库
创建存储库

按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **备份和恢复(Backup & Restore)**。

表 *16:* 按需备份设置

字段名称	使用指南
Backup Name	输入备份文件的名称。
Repository Name	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
Encryption Key	此密钥用于加密和解密备份文件。

相关主题

备份数据类型
按需备份和计划备份
备份历史记录
备份失败
思科 ISE 恢复操作

导出身份验证和授权策略配置
在分布式环境中同步主节点和辅助节点
执行按需备份

计划备份设置

下表介绍“定期备份”(Scheduled Backup) 窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **备份和恢复(Backup and Restore)**。

表 *17:* 计划备份设置

字段名称	使用指南
Name	输入备份文件的名称。您可以输入您所选的描述性名称。思科 ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup) 列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 **kron** 作业。
Description	输入对备份的说明。
Repository Name	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
Encryption Key	输入用于加密和解密备份文件的密钥。
Schedule Options	选择计划备份的频率并相应地填写其他选项。

相关主题

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

管理员访问设置

您可以通过这些部分来为管理员配置访问设置。

管理员密码策略设置

下表介绍了**密码策略 (Password Policy)** 选项卡中的字段，可以使用此选项卡来定义管理员密码应满足的条件。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。。

表 *18:* 管理员密码策略设置

字段名称	使用指南
最小长度 (Minimum Length)	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。
密码不可包含管理员姓名或其反向顺序的字符	选中此复选框可限制使用管理员用户名或其反向顺序的字符。
密码不可包含“cisco”或其反向顺序的字符	选中此复选框可限制使用字词“cisco”或其反向顺序的字符。
密码不可包含 _____ 或其反向顺序的字符	选中此复选框可限制使用您定义的任何字词或其反向顺序的字符。
密码不可包含连续重复四次或以上的字符	选中此复选框可限制使用连续重复四次或以上的字符。
必用字符	指定管理员密码必须包含从以下选项中选择的类型的至少一个字符： • 小写字母字符 • 大写字母字符 • 数字字符 • 非字母数字字符
密码历史记录 (Password History)	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。

字段名称	使用指南
“密码有效期”(Password Lifetime)	指定以下选项来强制用户在经过指定时间段后更改密码： • “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。”(Time (in days) before the administrator account is disabled if the password is not changed.)（允许的范围是 0 至 2147483647 天。） • “禁用管理员帐户之前的提醒时间（按天计）。”(Reminder (in days) before the administrator account is disabled.)
“不正确的登录尝试之后锁定或暂停帐户”(Lock or Suspend Account with Incorrect Login Attempts)	指定思科 ISE 在将管理员锁定以及暂停或禁用帐户凭证之前记录错误管理员密码的次数。 系统会向其帐户已锁定的管理员发送邮件。您可以输入自定义邮件补救消息。

相关主题

思科 ISE 管理员

创建新管理员

会话超时和会话信息设置

下表介绍**会话 (Session)** 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *19:* 会话超时和会话信息设置

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

相关主题

管理员访问设置

配置管理员会话超时

终止活动管理会话

TrustSec 设置

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。如果在思科 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，或当思科 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。

- **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)：如果希望思科 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)：指定您希望思科 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，思科 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

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。点击**权限 (Permissions)** 字段中显示的**加号 (+)** 标志可编辑 SGT 名称和值。

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。

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，则思科 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)**

相关主题

TrustSec 架构
TrustSec 组件
配置 TrustSec 全局设置

设置

通过这些窗口，您可以配置各种服务的常规设置。

安全评估常规设置

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

常规终端安全评估设置

- **补救计时器 (Remediation Timer)**：输入开始补救前等待的时间。默认值为 4 分钟。有效范围为 1 至 300 分钟。
- **网络过渡延迟 (Network Transition Delay)**：以秒为单位输入时间值。默认值为 3 秒。有效范围为 2 至 30 秒。
- **默认终端安全评估状态 (Default Posture Status)**：选择**合规 (Compliant)** 或**不合规 (Noncompliant)**。在连接到网络时，非代理设备会处于此状态。
- **自动关闭登录成功屏幕前等待 (Automatically Close Login Success Screen After)**：选中此复选框可在指定的时间过后自动关闭成功登录屏幕。可以配置计时器以自动关闭登录屏幕。有效范围为 0 至 300 秒。如果将时间设置为零，则客户端上的代理不会显示成功登录屏幕。

安全评估租约

- **每当用户连接到网络时执行终端安全评估 (Perform posture assessment every time a user connects to the network)**：选择此选项可在用户每次连接网络时启动终端安全评估
- **每 n 天执行一次终端安全评估 (Perform posture assessment every n days)**：选择此选项可在指定天数过后启动终端安全评估，即使客户端的状态已评估为“合规”也是如此。

相关主题

安全评估服务
安全评估管理设置
安全评估租约
在思科 ISE 中启用安全评估会话服务
设定补救计时器，使客户端在指定时间内补救
设置网络转换延迟计时器，使客户端实现转换
将登录成功窗口设置为自动关闭

设置非代理设备的终端安全评估状态

重新进行安全评估配置设置

表 *20:* 重新进行安全评估配置设置

字段名称	使用指南
Configuration Name	输入 PRA 配置的名称。
Configuration Description	输入 PRA 配置的说明。
Use Reassessment Enforcement?	选中此复选框，将 PRA 配置应用到用户身份组。
Enforcement Type	选择要执行的操作： • **继续 (Continue)**：用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。 • **注销 (Logoff)**：如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。 • **补救 (Remediate)**：如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送 PRA 报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。 如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的 RADIUS 会话，才能再次布置客户端。 如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续”(Continue) 选项。用户可以继续停留在当前的网络中，不受任何限制。
Interval	输入第一次成功登录后在客户端上启动 PRA 的时间间隔分钟数。 默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。
Grace time	输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于 PRA 间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。 最小值为 5 分钟，最大值为 60 分钟。 **注释** 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。
Select User Identity Groups	为 PRA 配置选择唯一组或唯一组组合。

字段名称	使用指南
PRA configurations	显示现有的 PRA 配置以及关联到 PRA 配置的用户身份组。

相关主题

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

安全评估可接受使用政策配置设置

表 *21:* 安全评估 *AUP* 配置设置

字段名称	使用指南
Configuration Name	输入要创建的 AUP 配置的名称。
Configuration Description	输入要创建的 AUP 配置的说明。
“向代理用户显示 AUP”(Show AUP to Agent users)（仅适用于 **Windows**）	选中后，系统会在身份验证和终端安全评估成功后，向用户显示您的网络的网络使用条款和条件的链接。
为 AUP 消息使用 URL (Use URL for AUP message)	选中后，必须在“AUP URL”字段中输入 AUP 消息的 URL。
为 AUP 消息使用文件 (Use file for AUP message)	选中后，必须浏览至文件位置并以压缩格式上传文件。此文件必须在顶层包含 index.html。 除 index.html 文件以外，该 .zip 文件还可包含其他文件和子目录。这些文件可以使用 HTML 标签相互引用。
AUP URL	输入 AUP 的 URL，用户必须在身份验证和安全评估成功后访问该 URL。
AUP File	浏览至文件并将其上传到思科 ISE 服务器。它应是压缩文件，并且应在顶层包含 index.html 文件。

字段名称	使用指南
Select User Identity Groups	针对 AUP 配置选择唯一用户身份组或用户身份组的唯一组合。 创建 AUP 配置时，请注意以下事项： • 安全评估 AUP 不适用于访客流程 • 两个配置不会共同具有任何用户身份组 • 如果您要使用用户身份组“Any”创建 AUP 配置，则要先删除所有其他 AUP 配置 • 如果使用用户身份组“Any”创建 AUP 配置，则无法使用唯一用户身份组或用户身份组的唯一组合创建其他 AUP 配置。要使用除 Any 以外的用户身份组创建 AUP 配置，请先删除具有用户身份组“Any”的现有 AUP 配置，或者使用唯一用户身份组或用户身份组的唯一组合更新具有用户身份组“Any”的现有 AUP 配置。
Acceptable use policy configurations - Configurations list	列出现有 AUP 配置以及与 AUP 配置关联的最终用户身份组。

相关主题

安全评估服务

配置安全评估的可接受使用政策

EAP-FAST 设置

表 *22:* 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思科 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

- 用于身份验证的协议设置
- 将 EAP-FAST 用作身份验证协议的指南
- EAP-FAST 的优势
- 配置 EAP-FAST 设置

PAC 设置

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

表 *23*: 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。
Trustsec PAC	点击此单选按钮生成 Trustsec PAC。
Identity	（针对 Tunnel 和 Machine PAC）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。

字段名称	使用指南
Expiration Data	（仅对于 Trustsec PAC）到期日期根据 PAC Time to Live 计算。

相关主题

用于身份验证的协议设置

将 EAP-FAST 用作身份验证协议的指南

为 EAP-FAST 生成 PAC

EAP-TLS 设置

相关主题

用于身份验证的协议设置

配置 EAP-TLS 设置

PEAP 设置

相关主题

用于身份验证的协议设置

配置 PEAP 设置

使用 PEAP 的优势

PEAP 协议支持的请求方

PEAP 协议流程

RADIUS 设置

当您启用异常客户端抑制并且在配置的检测间隔内终端身份验证失败两次时，思科 ISE 会将请求方标识为配置错误并抑制由于相同失败原因导致的失败身份验证。您可以通过在 Live Authentications 页面点击 Misconfigured Supplicant Counter 链接，找到关于此抑制功能的更多详细信息。如果从受抑制的终端成功完成身份验证，则会清除此抑制，而且会降低 Live Authentications 页面上 Misconfigured Supplicant Counter 的值。此外，如果在六小时的时间内受抑制终端没有任何身份验证活动，系统会自动清除抑制。

思科 ISE 允许通过启用 Reject Requests After Detection 选项，实施强抑制。如果您选中 Reject Requests After Detection 复选框，并且终端身份验证因同一失败原因失败五次，思科 ISE 就会激活强抑制。所有后续的身份验证，无论成功与否，都会被抑制，所以不会进行身份验证。经过所配置的 Request Rejection Interval 间隔或终端无身份验证活动达六小时后，系统会清除“强”抑制。

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，请参阅以下思科 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 *24: RADIUS* 设置

字段名称	使用指南
记住	• 如果选中**抑制重复失败的客户端 (Suppress Repeated Failed Clients)** 复选框，并且在**检测两次失败的时间范围 (Detect Two Failures Within)** 指定的时间内发生两次故障，则终端被视为配置错误。配置错误的终端需要管理员的干预才能确保身份验证成功。当终端首次身份验证失败时，管理员的控制面板中会显示相关信息。具有相同原因的后续身份验证失败不包含任何添加的管理员信息。因此，在**报告失败次数 (Report Failures Once Every)** 字段中指定的持续时间内，由于特定原因，终端的身份验证重复失败不会在审核日志中报告。 在**报告失败次数间隔 (Report Failures Once Every)** 字段中指定的持续时间过后，有关错误配置的终端的 **TotalFailedAttempts** 和 **TotalFailedTime** 信息将报告给监控节点。 • 如果选中**抑制重复失败的客户端 (Suppress Repeated Failed Clients)** 复选框，并且在**检测两次失败的时间范围 (Detect Two Failures Within)** 中指定的时间内发生两次故障，则在审核日志中将失败的终端身份验证尝试报告为单独的实例，即使身份验证的原因是故障保持不变。 • 思科 ISE 允许终端执行多个具有不同故障原因的连续故障，因为终端可以具有各种请求方配置文件。因此，如果终端由于不同的失败原因多次进行身份验证，则思科 ISE 会单独计算每个失败原因。
Suppress Anomalous Clients	选中此复选框以检查身份验证重复失败的客户端。每经过一个 Reporting Interval 间隔，系统会报告失败身份验证摘要。
Detection Interval	以分钟为单位输入检测客户端的时间间隔。
Reporting Interval	以分钟为单位输入报告失败身份验证的时间间隔。
Reject Requests After Detection	选中此复选框以拒绝来自被识别为异常或配置错误的客户端的请求。在请求拒绝间隔期间，系统会拒绝来自异常客户端的请求。

字段名称	使用指南
记住	• 如果选中**拒绝重复失败客户端的 RADIUS 请求 (Reject RADIUS Requests from Clients with Repeated Failures)** 复选框，并且终端遇到的身份验证失败次数等于**自动拒绝前的失败次数 (Failures Prior to Automatic Rejection)** 字段中提到的次数，则终端将被视为配置错误并被拒绝。思科 ISE 将立即拒绝包含来自此终端的身份验证请求的第一个 RADIUS 消息，因此不允许终端完成身份验证。不会为终端生成审核日志。终端在**持续拒绝请求的时长 (Continue Rejecting Requests for)** 字段中指定的持续时间内保持拒绝状态。终端可以在**继续拒绝请求 (Continue Rejecting Requests for)** 中指定的持续时间后发送身份验证请求，并且如果身份验证成功，则会配置终端。 • 您可以在**情景可视性 (Context Visibility)**（**情景可视性 (Context Visibility)** > **终端 (Endpoints)**）页面中查看和放行被拒绝的终端。选择被拒绝的终端，然后点击**释放已拒绝 (Release Rejected)** 以释放被拒绝的终端。被释放终端的审计日志将被发送到监控节点。 • 如果被错误配置的端点在六小时内没有任何活动，它将不再被视为被错误配置。
Request Rejection Interval	以分钟为单位输入拒绝请求的时间间隔。此选项仅在已选择**在检测后拒绝请求 (Reject Requests After Detection)** 复选框时可用。
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。
Accounting Suppression Interval	以秒为单位输入抑制记帐请求报告的时间间隔。
Long Processing Step Threshold Interval	以毫秒为单位输入时间间隔。身份验证详细信息报告中会显示这些步骤。如果单个步骤的执行超出指定阈值，则在身份验证详细报告中会突出显示此步骤。
RADIUS UDP 端口	

相关主题

用于身份验证的协议设置

思科 ISE 中的 RADIUS 协议支持

配置 RADIUS 设置

SMS 网关设置

这些设置的导航路径为 **Guest Access** > **Settings** > **SMS Gateway**。

这些设置的导航路径为**管理 (Administration)** > **设置 (Settings)** > **SMS 网关 (SMS Gateway)**。

使用以下设置配置通过邮件服务器向访客和发起人发送 SMS 消息。

表 *25: SMS* 邮件网关的 *SMS* 网关设置

字段	使用指南
SMS Gateway Provider Domain	输入作为用于向提供商 SMS/MMS 网关发送消息的邮件地址主机部分的提供商域和作为此地址用户部分的访客帐户移动号码。
Provider account address	（可选） 输入作为电子邮件发件人地址（通常是帐户地址）的帐户地址，并在**访客访问 (Guest Access)** > **设置 (Settings)**中覆盖**默认电子邮件地址 (Default Email Address)**全局设置。
SMTP API destination address	（可选） 如果您使用的是需要具体帐户收件人地址的SMTP SMS API（例如 Clickatell SMTP API），请输入 SMTP API 目标地址。 此地址用作邮件的 TO 地址并且系统会将访客帐户的移动号码代入消息的正文模板中。
SMTP API body template	（可选） 如果您使用的是需要使用特定邮件正文模板来发送 SMS 的 SMTP SMS API（例如 SMTP API），请输入 SMTP API 正文模板。 支持的动态替换为 $mobilenumber$、和 $message$。

这些设置的导航路径为 **Guest Access** > **Settings** > **SMS Gateway**。

使用以下设置配置通过 HTTP API（GET 或 POST 方法）向访客和发起人发送 SMS 消息。

表 *26: SMS HTTP API* 的 *SMS* 网关设置

字段	使用指南
URL	输入 API 的 URL。 此字段不是URL 编码的。系统将访客帐户的移动号码代入 URL 中。支持的动态替换为 $mobilenumber$ and $message$。 如果您将 HTTPS 用于 HTTP API，请在 URL 字符串中包含 HTTPS 并将您的提供商的受信任证书上传至思科 ISE。依次选择 **Administration** > **System** > **Certificates** > **Trusted Certificates**。

字段	使用指南
Data (Url encoded portion)	输入 GET 或 POST 请求的数据（Url 编码部分）。 此字段是 URL 编码的。如果使用默认 GET 方法，此数据附加于上述指定 URL 后面。
Use HTTP POST method for data portion	如果使用 POST 方法，请选中此选项。 上述指定数据用作 POST 请求的内容。
HTTP POST data content type	如果使用 POST 方法，请指定内容类型，例如“plain/text”或“application/xml”。
HTTPS Username HTTPS Password HTTPS Host name HTTPS Port number	输入此信息。

相关主题

SMS 运营商和服务
配置 SMS 网关以向访客发送 SMS 通知

身份管理

您可以使用这些窗口在思科 ISE 中配置和管理身份。

终端

通过这些窗口，您可以配置和管理连接到您的网络的终端。

终端设置

表 *27:* 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的 MAC 地址以静态创建终端。 MAC 地址是连接到启用思科 ISE 的网络的接口设备标识符。
Static Assignment	如果您想要在“终端”(Endpoints) 窗口静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。 您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。

字段名称	使用指南
Policy Assignment	（除非选中**静态分配 (Static Assignment)** 复选框，否则会默认禁用此字段）从**策略分配 (Policy Assignment)** 下拉列表选择匹配的终端策略。 您可以执行以下操作之一： • 如果您不选择匹配的终端策略，而是使用默认终端策略 Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。 • 如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中**静态分配 (Static Assignment)** 复选框。
Static Group Assignment	当您想要向身份组静态分配终端时，请选中此复选框。 如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。 如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。

Identity Group Assignment	选择您要将终端分配至哪个终端身份组。
	当您静态创建终端，或在为某个终端评估终端策略期间不想使用**创建匹配身份组 (Create Matching Identity Group)** 选项时，可将终端分配至身份组。
	思科 ISE 包括以下系统创建的终端身份组：
	• 黑名单
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

相关主题

已识别的终端

使用策略和身份的静态分配创建终端

从 LDAP 设置导入终端

表 *28:* 从 *LDAP* 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。 注释 思科 ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。
Enable Secure Connection	选中**启用安全连接 (Enable Secure Connection)** 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	点击下拉箭头，查看受信任的 CA 证书。 根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在思科 ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
Anonymous Bind	您必须选中**匿名绑定 (Anonymous Bind)** 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
Admin DN	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
密码 (Password)	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
Base DN	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
查询设置	
MAC Address objectClass	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
MAC Address Attribute Name	输入导入操作返回的属性名称，例如，macAddress。

字段名称	使用指南
Profile Attribute Name	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置**分析属性名称 (Profile Attribute Name)** 字段时，请考虑以下事项： • 如果未在**分析属性名称 (Profile Attribute Name)** 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知”(Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。 • 如果您在**分析属性名称 (Profile Attribute Name)** 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与思科 ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。
超时	输入时间值（以秒为单位）。有效范围是从 1 到 60 秒。

相关主题

已识别的终端
从 LDAP 服务器导入终端

终端身份组设置

表 *29:* 终端身份组设置

字段名称	使用指南
Name	输入您要创建的终端身份组的名称。
Description	输入对您要创建的终端身份组的说明。
Parent Group	从**父级组 (Parent Group)** 下拉列表选择您要关联新创建的终端身份组的终端身份组。 思科 ISE 包括以下终端身份组： • Blacklist • GuestEndpoints • Profiled • RegisteredDevices • Unknown 此外，它还会再创建两个身份组：Cisco-IP-Phone 和 Workstation，这两个身份组与 Profiled（父）身份组关联。

相关主题

已识别终端划分为终端身份组
创建终端身份组

外部身份源

您可以通过这些窗口配置和管理包含思科 ISE 用于身份验证和授权的用户数据的外部身份源。

LDAP 身份源设置

LDAP 常规设置

下表介绍**常规 (General)** 选项卡上的字段。

表 *30: LDAP* 常规设置

字段名称	使用指南
Name	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
Description	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。
架构 (Schema)	您可以选择以下任一内置架构类型或创建自定义架构： • Active Directory • Sun 目录服务器 (Sun Directory Server) • Novell eDirectory 您可以点击 Schema 旁边的箭头以查看架构详细信息。 如果您编辑该预定义架构的属性，思科 ISE 会自动创建自定义架构。
注释　仅在您选择定制架构时，可以编辑以下字段。	
Subject Objectclass	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
主题名称属性 (Subject Name Attribute)	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。
证书属性 (Certificate Attribute)	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
Group Objectclass	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。

字段名称	使用指南
组映射属性 (Group Map Attribute)	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 (Subject Objects Contain Reference To Groups)	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 (Group Objects Contain Reference To Subjects)	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 (Subjects in Groups Are Stored in Member Attribute As)	（仅适用于启用**组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects)** 选项时）指定在组成员属性中如何搜索成员，其默认值为 DN。

注释 配置的主题名称属性应在外部 ID 存储区中编入索引。

LDAP 连接设置

下表介绍**连接设置 (Connection Settings)** 选项卡中的字段。

表 *31: LDAP* 连接设置

字段名称	使用指南
启用辅助服务器	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效 IP 地址。对于主机名，仅字母数字字符（a 至 z；A 至 Z；0 至 9）、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。

字段名称	使用指南
访问	**匿名访问 (Anonymous Access)**：点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。 **身份验证访问 (Authenticated Access)**：点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员 DN”(Admin DN) 字段和“密码”(Password) 字段输入信息。
管理员 DN (Admin DN)	输入管理员的 DN。管理员 DN 是有权限搜索“用户目录子树”(User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。
安全身份验证 (Secure Authentication)	点击此字段以对思科 ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口”(Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA”(LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 (Server Timeout)	以秒为单位输入思科 ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 (Max. Admin Connections)	输入利用 LADP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于 0）。这些连接用于在“用户目录子树”(User Directory Subtree) 和 “组目录子树”(Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
测试与服务器的绑定 (Test Bind to Server)	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
Failover	
Always Access Primary Server First	如果您希望思科 ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
...后故障恢复到主服务器 (Failback to Primary Server after)	如果思科 ISE 尝试连接的主 LDAP 服务器无法访问，思科 ISE 会尝试连接辅助 LDAP 服务器。如果您希望思科 ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

LDAP 目录组织设置

下表介绍**目录组织 (Directory Organization)** 选项卡上的字段。

表 *32: LDAP* 目录组织设置

字段名称	使用指南
主题搜索库 (Subject Search Base)	输入包含所有主题的子树的 DN。例如： o=corporation.com 如果包含主题的树是基本 DN，请输入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
组搜索库 (Group Search Base)	输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com 如果包含组的树是基本 DN，请键入： o=corporation.com 或 dc=corporation,dc=com 根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	输入一个 MAC 地址格式供思科 ISE 用于在 LDAP 数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当思科 ISE 收到主机查找请求时，思科 ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。 使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <*format*> 可以是以下任何一种格式： • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。

字段名称	使用指南
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	输入适当的文本以删除用户名的域前缀。 如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <start_string> 框中指定的多个字符，思科 ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则思科 ISE 会向 LDAP 服务器提交 user1。 注释 <start_string> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。思科 ISE 不允许在用户名中使用这些字符。
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	输入适当的文本以删除用户名的域后缀。 如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，思科 ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 *user1@domain*，则思科 ISE 会向 LDAP 服务器提交 *user1*。 注释 <*end_string*> 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (>) 和左尖括号 (<)。思科 ISE 不允许在用户名中使用这些字符。

LDAP 组设置

表 *33: LDAP* 组设置

字段名称	使用指南
添加	选择 **Add> 添加组**添加新组或从目录**中选择** Add> 选择 Group 选择组从 LDAP 目录。 如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击**检索组 (Retrieve Groups)**。点击要选择的组旁边的复选框，然后点击**确定 (OK)**。选中的组将显示在**组 (Groups)** 窗口中。

LDAP 属性设置

表 *34: LDAP* 属性设置

字段名称	使用指南
添加	选择 **Add> 添加属性**添加新属性或从目录**中选择** Add> 选择属性从 LDAP 服务器的属性。 如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击**检索属性 (Retrieve Attributes)** 以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。

相关主题

- LDAP 目录服务
- LDAP 用户身份验证
- LDAP 用户查找
- 添加 LDAP 身份源

RADIUS 令牌身份源设置

相关主题

- RADIUS 令牌身份源
- 添加 RADIUS 令牌服务器

RSA SecurID 身份源设置

RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 *35: RSA* 提示设置

字段名称	使用指南
Enter Passcode Prompt	输入文本字符串以获取密码。
Enter Next Token Code	输入文本字符串以请求下一个令牌。
Choose PIN Type	输入文本字符串以请求 PIN 类型。
Accept System PIN	输入文本字符串以接受系统生成的 PIN。
Enter Alphanumeric PIN	输入文本字符串以请求字母数字 PIN。
Enter Numeric PIN	输入文本字符串以请求数字 PIN。

字段名称	使用指南
Re-enter PIN	输入文本字符串以请求用户重新输入 PIN。

RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 *36: RSA* 消息设置

字段名称	使用指南
Display System PIN Message	输入文本字符串以编辑系统 PIN 消息。
Display System PIN Reminder	输入文本字符串以通知用户记住新 PIN。
Must Enter Numeric Error	输入一条消息，指导用户仅输入数字作为 PIN。
Must Enter Alpha Error	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
PIN Rejected Message	输入在系统拒绝用户的 PIN 时用户所看到的消息。
User Pins Differ Error	输入在用户输入错误 PIN 时所看到的消息。
System PIN Accepted Message	输入在系统接受用户的 PIN 时用户所看到的消息。
Bad Password Length Error	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

相关主题

RSA 身份源

思科 ISE 和 RSA SecurID 服务器集成

添加 RSA 身份源

网络资源

对会话感知网络 (SAnet) 的支持

思科 ISE 为会话感知网络 (SAnet) 提供有限支持。SAnet 是在许多思科交换机上运行的会话管理框架。SAnet 管理访问会话，包括可视性、身份验证和授权。SAnet 使用服务模板，其中包含 RADIUS 授权属性。思科 ISE 在授权配置文件中包含服务模板。思科 ISE 在授权配置文件中使用标志来标识服务模板，该标志会将配置文件标识为兼容“服务模板”。

思科 ISE 授权配置文件包含转换为属性列表的 RADIUS 授权属性。SAnet 服务模板还包含 RADIUS 授权属性，但这些属性不会转换为列表。

对于 SAnet 设备，思科 ISE 会发送服务模板的名称。设备会下载服务模板的内容，除非该内容已存在于缓存或静态定义的配置中。当服务模板更改 RADIUS 属性时，思科 ISE 会向设备发送 CoA 通知。

网络设备

下列会话所描述的窗口可使您在思科 ISE 中添加和管理网络设备。

网络设备定义设置

下表介绍**网络设备 (Network Devices)** 窗口上的字段，您可以使用该窗口配置思科 ISE 中的网络访问设备。此页面的导航路径为： **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**，然后单击**添加 (Add)**。

网络设备设置

下表介绍**网络设备设置 (Network Device Settings)** 窗口中的字段。

表 *37:* 网络设备设置

字段名称	说明
名称	输入网络设备的名称。 您可以为网络设备提供一个不同于设备主机名的描述性名称。设备名称是一个逻辑标识符。 **注释** 如果需要，可以在配置后更改设备的名称。
说明	输入设备的说明。

字段名称	说明
IP 地址或 IP 掩码	输入单一 IP 地址和子网掩码。 以下是定义 IP 地址和子网掩码时必须遵守的准则： • 您可以使用子网掩码定义一个特定 IP 地址或 IP 地址范围。如果设备 A 定义了 IP 地址范围，则可以使用在设备 A 中定义的 IP 地址范围的某个地址配置另一设备 B。 • 您不能使用相同的特定 IP 地址定义两台设备。 • 您不能使用同一 IP 地址范围定义两台设备。IP 地址范围不得部分或全部重叠。
Model Name	从下拉列表中选择设备型号。 在基于规则的策略中查找条件时，可以将型号名称用作其中一个参数。此属性存在于设备字典中。
软件版本	从下拉列表中选择在网络设备上运行的软件版本。 在基于规则的策略中查找条件时，您可以将软件版本用作其中一个参数。此属性存在于设备字典中。
网络设备组 **(Network Device Group)**	在**网络设备组 (Network Device Group)** 区域中，从**位置 (Location)**、 和**设备类型 (Device Type)** 下拉列表中选择所需的值。 如果未将设备专门分配到组，则设备将加入默认设备组（根网络设备组），位置为**所有位置 (All Locations)**，设备类型为**所有设备类型 (All Device Types)**。

注释 使用过滤器从思科 ISE 部署中选择和删除网络访问设备 (NAD) 时，请清除浏览器缓存，以确保仅删除选定的 NAD。

RADIUS 身份验证设置

下表介绍 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 区域中的字段。

表 ***38: RADIUS*** 身份验证设置

字段名称	使用指南
协议	显示 **RADIUS** 作为所选协议。
共享密钥	输入最大长度为 127 个字符的共享密钥。 共享密钥是您使用 **radius-host** 命令和 **pac** 关键词在网络设备上配置的密钥。

字段名称	使用指南
启用 KeyWrap (Enable KeyWrap)	仅当网络设备支持 KeyWrap 算法时，选中**启用 KeyWrap (Enable KeyWrap)** 复选框。网络设备必须与 AES KeyWrap RFC (RFC 3394) 兼容。 此选项用于通过 AES KeyWrap 算法提高 RADIUS 安全性。
密钥加密密钥 (ey Encryption Key)	（仅在启用 KeyWrap 时显示）输入用于会话加密（保密）的加密密钥。 **注释** 当您在 FIPS 模式下运行思科 ISE 时，您必须在网络设备上启用 KeyWrap。
消息身份验证器代码密钥 (Message Authenticator Code Key)	（仅在启用 KeyWrap 时显示）输入用于通过 RADIUS 消息传输的加密散列消息验证码 (HMAC) 计算的密钥。
密钥输入格式 (Key Input Format)	点击以下格式之一对应的单选按钮： • **ASCII**：“密钥加密密钥”(Key Encryption Key) 长度必须为 16 个字符（字节），“消息身份验证器代码密钥”(Message Authenticator Code Key) 长度必须为 20 个字符（字节）。 • **十六进制 (Hexadecimal)**：“密钥加密密钥”(Key Encryption Key) 长度必须为 32 个字节，“消息身份验证器代码密钥”(Message Authenticator Code Key) 长度必须为 40 个字节。 您可以指定要用于输入密钥加密密钥和消息身份验证器代码密钥的密钥输入格式，以便与网络设备上的配置相匹配。您指定的值必须是密钥的正确（完整）长度。不允许使用较短的值。

SNMP 设置

下表介绍 **SNMP 设置 (SNMP Settings)** 部分中的字段。

表 *39: SNMP* 设置区域中的字段

字段名称	使用指南
SNMP 版本 (SNMP Version)	从 **SNMP (SNMP 版本)** 下拉列表中，选择以下选项之一： • **1**：SNMPv1 不支持通知。 • **2c** • **3**：SNMPv3 是最安全的型号，因为它允许您在选择 **安全级别** 字段中 **Priv** 时加密数据包。 注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的**网络设备会话状态 (Network Device Session Status)** 摘要报告（**操作 (Operations) > 报告 (Reports) > 目录 (Catalog) > 网络设备 (Network Device) > 会话状态摘要 (Session Status Summary)**）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。
SNMP 只读社区 (SNMP RO Community)	（仅适用于 SNMP 版本 1 和 2c）输入只读社区字符串，为思科 ISE 提供特殊类型的设备访问权限。
SNMP 用户名 (SNMP Username)	（仅适用于 SNMP 版本 3）输入 SNMP 用户名。
安全级别 (Security Level)	（仅适用于 SNMP 版本 3）从**安全级别 (Security Level)** 下拉列表中选择以下选项之一： • **身份验证 (Auth)**：启用 MD5 或安全散列算法 (SHA) 数据包身份验证。 • **无身份验证 (No Auth)**：无身份验证，无隐私安全级别。 • **隐私 (Priv)**：启用数据加密标准 (DES) 数据包加密。
身份验证协议 (Auth Protocol)	（选择安全级别**身份验证 [Auth]** 和**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）从**身份验证协议 (Auth Protocol)** 下拉列表中，选择希望网络设备使用的身份验证协议。 • **MD5** • **SHA**
身份验证密码 (Auth Password)	（选择安全级别**身份验证 [Auth]** 和**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）输入身份验证密钥。密码的长度应至少为 8 个字符。 点击**显示 (Show)**，显示已为设备配置的身份验证密码。

字段名称	使用指南
隐私协议 **(Privacy Protocol)**	（选择安全级别**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）从**隐私协议 (Privacy Protocol)** 下拉列表中，选择以下选项之一： • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
隐私密码 **(Privacy Password)**	（选择安全级别**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）输入隐私密钥。 点击**显示 (Show)**，显示已为设备配置的隐私密码。
轮询间隔 **(Polling Interval)**	输入轮询间隔（秒）。默认值为 3600。
链路陷阱查询 **(Link Trap Query)**	选中**链路陷阱查询 (Link Trap Query)** 复选框，可接收和解析通过 SNMP 陷阱接收的链路接通和链路断开通知。
MAC 陷阱查询 **(Mac Trap Query)**	选中**链路陷阱查询 (Link Trap Query)** 复选框，可接收和解析通过 SNMP 陷阱接收的 MAC 通知。
Originating Policy Services Node (原始策略服务节点**)**	从**原始策略服务节点 (Originating Policy Services Node)** 下拉列表中，选择要用于轮询 SNMP 数据的思科 ISE 服务器。此字段的默认值为**自动 (Auto)**。从下拉列表中选择特定值以覆盖设置。

高级 Trustsec 设置 (Advanced TrustSec Settings)

下表介绍**高级 Trustsec 设置 (Advanced Trustsec Settings)** 部分中的字段。

表 *40:* 高级 *TrustSec* 设置区域中的字段

字段名称	使用指南
将设备 ID 用于 Trustsec 标识 **(Use Device ID for TrustSec Identification)**	如果希望在**设备 ID (Device ID)** 字段中将设备名称作为设备标识符列出，请选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框。
设备 ID	仅当未选中 **将设备 ID 用于 Trustsec 标识** 复选框时，才能使用此字段。

字段名称	使用指南
密码	输入在思科 TrustSec 设备 CLI 中配置的密码，用于对思科 TrustSec 设备进行身份验证。 点击**显示 (Show)** 可显示密码。
HTTP REST API 设置	
Trustsec 设备通知和更新设置	
将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)	如果希望在**设备 ID (Device ID)** 字段中将设备名称作为设备标识符列出，请选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框。
设备 ID	仅当未选中 **将设备 ID 用于 Trustsec 标识** 复选框时，才能使用此字段。
密码	输入在思科 TrustSec 设备 CLI 中配置的密码，用于对思科 TrustSec 设备进行身份验证。 点击**显示 (Show)** 可显示密码。
每<...>下载一次环境数据 (Download Environment Data Every <...>)	通过从此区域的下拉列表中选择所需的值，指定设备从思科 ISE 下载其环境数据时必须遵守的时间间隔。您可以选择秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。
每 <...>下载一次对等授权策略 (Download Peer Authorization Policy Every <...>)	通过从此区域的下拉列表中选择所需的值，指定设备从思科 ISE 下载对等授权策略时必须遵守的时间间隔。您可以指定单位为秒、分钟、小时、天或周的时间间隔。默认值为一天。
每 <...>重新进行身份验证 (Reauthentication Every <...>)	通过从此区域的下拉列表中选择所需的值，指定在初始身份验证后设备对照思科 ISE 重新进行身份验证的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。例如，如果输入 1000 秒，则设备会每 1000 秒对照思科 ISE 对自身重新进行身份验证。默认值为一天。
每 <...>下载 SGACL 列表 (Download SGACL Lists Every <...>)	通过从此区域的下拉列表中选择所需的值，指定设备从思科 ISE 下载 SGACL 列表时遵守的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。

字段名称	使用指南
其他 **TrustSec** 设备信任该设备（**Trustsec** 信任）**(Other TrustSec Devices to Trust This Device [TrustSec Trusted])**	选中**其他 TrustSec 设备信任该设备 (Other TrustSec Devices to Trust This Device)** 复选框，可允许所有对等设备信任此思科 TrustSec 设备。如果取消选中此复选框，则对等设备不信任此设备，所有从此设备到达的数据包都会相应地标注颜色或进行标记。
向此设备通知 **Trustsec** 配置更改 **(Notify this device about TrustSec configuration changes)**	如果希望思科 ISE 向此 TrustSec 设备发送 TrustSec CoA 通知，请选中此复选框。
设备配置部署设置设置	
当部署安全组标签映射更新时纳入该设备 **(Include this device when deploying Security Group Tag Mapping Updates)**	如果希望思科 TrustSec 设备使用设备接口凭据获取 IP-SGT 映射，请选中 **当部署安全组标记映射更新时包含此设备** 复选框。
EXEC 模式用户名 **(EXEC Mode Username)**	输入用于登录思科 TrustSec 设备的用户名。
EXEC 模式密码 **(EXEC Mode Password)**	输入设备密码。 点击**显示 (Show)** 可查看密码。 注释　我们建议您避免在密码（包括 EXEC 模式和启用模式密码）中使用 % 字符，以避免安全漏洞。
启用模式密码 **(Enable Mode Password)**	（可选）输入用于在特权 EXEC 模式下编辑思科 TrustSec 设备配置的启用密码。 点击**显示 (Show)** 可查看密码。
带外 **(OOB) Trustsec PAC** 显示	
颁发日期 **(Issue Date)**	显示思科 ISE 为思科 Trustsec 设备生成的最后一个思科 Trustsec PAC 的颁发日期。
到期日期	显示思科 ISE 为思科 Trustsec 设备生成的最后一个思科 Trustsec PAC 的到期日期。

字段名称	使用指南
颁发者	显示思科 ISE 为思科 Trustsec 设备生成的最后一个思科 Trustsec PAC 的颁发者（思科 TrustSec 管理员）名称。
生成 PAC (Generate PAC)	点击**生成 PAC (Generate PAC)** 按钮，为思科 TrustSec 设备生成带外思科 TrustSec PAC。

相关主题

在思科 ISE 中定义网络设备
思科 ISE 中的第三方网络设备支持
网络设备组
在思科 ISE 中添加网络设备
在思科 ISE 中配置第三方网络设备

默认网络设备定义设置

下表介绍**默认网络设备 (Default Network Device)** 窗口中的字段，该窗口用于配置思科 ISE 可用于 RADIUS 和 TACACS+ 身份验证的默认网络设备。选择以下导航路径之一：

- **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **默认设备 (Default Device)**
- **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **默认设备 (Default Devices)**

表 *41:*“默认网络设备”窗口中的字段

字段名称	使用指南
Default Network Device Status	从**默认网络设备状态 (Default Network Device Status)** 下拉列表中选择**启用 (Enable)**，以启用默认网络设备定义。 注释　如果默认设备已启用，则必须通过选中窗口中的复选框启用 RADIUS 或 TACACS+ 身份验证设置。
设备配置文件	显示**思科 (Cisco)** 为默认的设备供应商。
RADIUS 身份验证设置	
启用 **RADIUS**	选中**启用 RADIUS (Enable RADIUS)** 复选框，启用设备的 RADIUS 身份验证。
共享密钥	输入共享密钥。共享密钥最大长度为 127 个字符。 共享密钥是您使用 **radius-host** 命令和 **pac** 关键词在网络设备上配置的密钥。
启用 **KeyWrap (Enable KeyWrap)**	（可选）仅在网络设备支持 KeyWrap 算法时选中**启用 KeyWrap (Enable KeyWrap)** 复选框，这可以通过 AES KeyWrap 算法提高 RADIUS 安全性。

字段名称	使用指南
密钥加密密钥 (ey Encryption Key)	启用 KeyWrap 时，输入用于会话加密（保密）的加密密钥。
Message Authenticator Code Key	启用KeyWrap时，输入对RADIUS消息进行键控散列消息身份验证代码(HMAC)计算的密钥。
Key Input Format	通过点击相应的单选按钮选择以下格式之一，并在**密钥加密密钥 (Key Encryption Key)** 和**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入值： • **ASCII**：**密钥加密密钥 (Key Encryption Key)** 长度必须为 16 个字符（字节），而**消息身份验证器代码密钥 (Message Authenticator Code Key)** 长度必须为 20 个字符（字节）。 • **十六进制 (Hexadecimal)**：**密钥加密密钥 (Key Encryption Key)** 长度必须为 32 个字节，而**消息身份验证器代码密钥 (Message Authenticator Code Key)** 长度必须为 40 个字节。 指定要用于输入密钥加密密钥和消息身份验证器代码密钥的密钥输入格式，以便与网络设备上的配置相匹配。您指定的值必须是密钥的正确（完整）长度。不允许使用较短的值。
TACACS 身份验证设置	
共享密钥	当 TACACS+ 协议启用时，输入文本字符串以分配给网络设备。请注意，在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。
停用共享密钥处于启用状态 (Retired Shared Secret is Active)	当停用期处于启用状态时显示。
淘汰	停用现有的共享密钥而不是结束它。当您点击 **停用** 时，系统会显示一个对话框。点击**是 (Yes)** 或**否 (No)**。
剩余停用期 (Remaining Retired Period)	（可选）仅当您在 **停用** 对话框中点击 **是** 时可用。显示在**工作中心** > **设备管理** > **设置** > **连接设置** > **默认共享密钥失效期**窗口中指定的默认值。您可以更改默认值。 这允许输入新的共享密钥。旧共享密钥将在指定天数内保持有效。
结束	（可选）仅当您在 **剩余停用期间** 对话框中选择 **是** 时可用。结束停用期并终止旧的共享密钥。

字段名称	使用指南
启用单连接模式 (Enable Single Connect Mode)	选中**启用单连接模式 (Enable Single Connect Mode)** 复选框，将单一 TCP 连接用于与网络设备之间的所有 TACACS+ 通信。点击以下单选按钮之一： • **传统思科设备 (Legacy Cisco Devices)** • **TACACS 草案合规性单连接支持 (TACACS Draft Compliance Single Connect Support)**。 注释 如果禁用此字段，思科 ISE 会为每个 TACACS+ 请求使用新的 TCP 连接。

设备安全设置

指定 RADIUS 共享密钥的最小长度。默认情况下，对于新安装和升级的部署，此值为 4 个字符。对于 RADIUS 服务器而言，长度最好为 22 个字符。

注释 在“网络设备”(Network Devices) 页面输入的共享密钥长度必须等于或大于在“设备安全设置”(Device Security Settings) 页面的“RADIUS 共享密钥最小长度”(Minimum RADIUS Shared Secret Length) 字段中配置的值。

相关主题

网络设备定义设置，第 61 页

网络设备导入设置

表 *42:* 导入网络设备设置

字段名称	使用指南
生成模板 (Generate a Template)	点击**创建模板 (Generate a Template)** 可创建逗号分隔值 (CSV) 模板文件。 使用 CSV 格式的网络设备信息更新模板，并将其保存在本地。然后，使用编辑的模板将网络设备导入任何思科 ISE 部署。
文件	点击 **浏览**，选择您可能最近创建的或以前从思科 ISE 部署导出的 CSV 文件。 您可以使用 **导入** 选项将包含新的和更新后的网络设备信息的网络设备导入其他思科 ISE 部署中。
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	选中 **用新数据覆盖现有数据** 复选框可用您的导入文件中的设备取代现有网络设备。 如不选中此复选框，则导入文件中可用的新网络设备定义将添加到网络设备存储库。系统会忽略重复条目。

字段名称	使用指南
Stop Import on First Error	如果您希望思科 ISE 在导入过程中遇到错误时停止导入，请选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。思科 ISE 会导入网络设备，直至出现错误。 如未选中此复选框并且遇到错误，系统会报错并且思科 ISE 会继续导入剩余设备。

相关主题

- 在思科 ISE 中定义网络设备
- 思科 ISE 中的第三方网络设备支持
- 将网络设备导入思科 ISE

管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

网络设备组设置

表 *43:*“网络设备组”*(Network Device Group)* 窗口中的字段

字段名称	使用指南
Name	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。 网络设备组的全称最多可以包含 100 个字符。例如，如果在父组**全球 (Global) > 亚洲 (Asia)** 下创建一个名为**印度 (India)** 的子组，则您创建的网络设备组的全称将为**全球 (Global) > 亚洲 (Asia) > 印度 (India)**。全称不能超过 100 个字符。如果网络设备组的全称超过 100 个字符，则网络设备组创建失败。
Description	为根网络设备组或子网络设备组输入一段说明。
Parent Group	要将所创建的组添加到现有父组，请从下拉列表中选择一个父组。要将此新组添加为根组，请从下拉列表中选择**添加为根组 (Add as root group)**。
Type	输入根网络设备组 (NDG) 的类型。 所有添加到根网络设备组的子网络设备组都将继承组类型。 如果此网络设备组是根网络设备组，则其类型可作为设备字典中的属性使用。您可以基于此属性定义条件。网络设备组的名称是此属性可以采用的值之一。

相关主题

- 网络设备组
- 思科 ISE 在策略评估中使用的网络设备属性
- 在思科 ISE 中添加网络设备

网络设备组导入设置

表 *44:* 网络设备组导入窗口中的字段

字段名称	使用指南
生成模板 (Generate a Template)	点击此链接下载 CSV 模板文件。 使用相同格式的网络设备组信息更新模板。将模板保存在本地，以便将网络设备组导入任何思科 ISE 部署中。
文件	点击 **浏览**，导航至您要上传的 CSV 文件的位置。该文件可能是新文件，也可能是从另一个思科 ISE 部署中导出的文件。 可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 ISE 部署导入另一部署。
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	如果您希望思科 ISE 用您的导入文件中的设备组替换现有网络设备组，请选中此复选框。 如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。
Stop Import on First Error	选中此复选框，可在导入期间遇到错误的第一个实例时停止导入。 如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。

相关主题

网络设备组
思科 ISE 在策略评估中使用的网络设备属性
将网络设备组导入到思科 ISE

外部 RADIUS 服务器设置

表 *45:* 外部 *RADIUS* 服务器设置

字段名称	使用指南
Name	输入外部 RADIUS 服务器的名称。
Description	输入外部 RADIUS 服务器的说明。
Host IP	输入外部 RADIUS 服务器的 IP 地址。
Shared Secret	输入思科 ISE 和外部 RADIUS 服务器之间用于对外部 RADIUS 服务器进行身份验证的共享密钥。共享密钥是用户必须提供的预期文本字符串，使网络设备能够验证用户名和密码。在用户提供共享密钥之前，连接始终被拒绝。共享密钥最大长度为 128 个字符。

字段名称	使用指南
Enable KeyWrap	启用此选项，通过 AES KeyWrap 算法增加 RADIUS 协议安全性，帮助在思科 ISE 中实现 FIPS 140 合规性。
Key Encryption Key	（仅当选中**启用密钥封装 (Enable Key Wrap)** 复选框时）输入要用于会话加密（保密）的密钥。
Message Authenticator Code Key	（仅当选中**启用密钥封装 (Enable Key Wrap)** 复选框时）输入用于基于 RADIUS 消息的键控 HMAC 计算的密钥。
Key Input Format	指定要在输入思科 ISE 加密密钥时使用的格式，使其匹配 WLAN 控制器上可用的配置。您指定的值必须是密钥的正确（完整）长度，符合下方的定义（不允许使用短于此长度的值）。 • ASCII：“密钥加密密钥”(Key Encryption Key) 长度必须为 16 个字符（字节），“消息身份验证器代码密钥”(Message Authenticator Code Key) 长度必须为 20 个字符（字节）。 • 十六进制 (Hexadecimal)：“密钥加密密钥”(Key Encryption Key) 长度必须为 32 个字节，“消息身份验证器代码密钥”(Message Authenticator Code Key) 长度必须为 40 个字节。
身份验证端口	输入 RADIUS 身份验证端口号。有效范围为 1 至 65535。默认值为 1812。
计费端口	输入 RADIUS 记账端口号。有效范围为 1 至 65535。默认值为 1813。
Server Timeout	输入思科 ISE 等待外部 RADIUS 服务器响应的秒数。默认值为 5 秒。有效值为 5 至 120。
Connection Attempts	输入思科 ISE 尝试连接到外部 RADIUS 服务器的次数。默认值为 3 次。有效值为 1 至 9。

相关主题

将思科 ISE 用作 RADIUS 代理服务器

配置外部 RADIUS 服务器

RADIUS 服务器序列

表 *46: RADIUS* 服务器序列

字段名称	使用指南
Name	输入 RADIUS 服务器序列的名称。
说明 (Description)	输入可选的说明。

字段名称	使用指南
Host IP	输入外部 RADIUS 服务器的 IP 地址。
User Selected Service Type	从 Available 列表框选择您要用作策略服务器的外部 RADIUS 服务器，并将其移入 Selected 列表框。
Remote Accounting	选中此复选框以在远程策略服务器上启用记账功能。
Local Accounting	选中此复选框以在思科 ISE 上启用记帐功能。
高级属性设置	
Strip Start of Subject Name up to the First Occurrence of the Separator	选中此复选框以删除用户名的前缀。例如，如果主题名称是 acme\userA，分隔符为 \，则用户名成为 userA。
Strip End of Subject Name from the Last Occurrence of the Separator	选中此复选框以删除用户名的后缀。例如，如果主题名称是 userA@abc.com，分隔符为 @，则用户名成为 userA。 • 您必须启用这些删除选项以从 NetBIOS 或用户主体名称 (UPN) 格式用户名（user@domain.com 或 /domain/user）提取用户名，因为系统向 RADIUS 服务器仅传递用户名以对用户进行身份验证。 • 如果您同时激活 \ 和 @ 删除功能，而且您使用的是 AnyConnect ，则思科 ISE 会从字符串中准确地删除第一个 \。但是，每个单独使用的剥离功能都按照设计与 AnyConnect 配合运行。
Modify Attributes in the Request to the External RADIUS Server	选中此复选框以允许思科 ISE 修改往来于经过身份验证的 RADIUS 服务器的属性。 属性修改操作包括以下选项： • **添加 (Add)** - 向整体 RADIUS 请求/响应添加其他属性。 • **更新 (Update)** - 更改属性值（固定或静态）或将一个属性值替代为另一个属性值（动态）。 • **删除 (Remove)** - 删除属性或属性-值对。 • **删除所有 (RemoveAny)** - 删除所有出现的属性。
Continue to Authorization Policy	选中此复选框以将代理流程转为运行授权策略，从而根据身份库组和属性检索结果执行进一步决策。如果启用此选项，来自外部 RADIUS 服务器的响应的属性将适用于身份验证策略选择。上下文中已有的属性将根据 AAA 服务器 accept response 属性的相应值进行更新。
Modify Attributes before send an Access-Accept	选中此复选框以在快要向设备发回响应之前修改属性。

相关主题

将思科 ISE 用作 RADIUS 代理服务器
定义 RADIUS 服务器序列

NAC 管理器设置

表 *47: NAC* 管理器设置

字段	使用指南
名称	输入思科接入管理器 (CAM) 的名称。
Status	点击 Status 复选框，启用从验证连接的思科 ISE 分析器到 CAM 的 REST API 通信。
Description	输入 CAM 的说明。
IP Address	输入 CAM 的 IP 地址。在思科 ISE 中创建和保存 CAM 后，无法编辑 CAM 的 IP 地址。 您不能使用 0.0.0.0 和 255.255.255.255，因为在思科 ISE 中验证 CAM 的 IP 地址时，这些 IP 地址被排除在外。因此，它们不是您可以在 CAM 的 IP Address 字段中使用的有效 IP 地址。 注释 您可以使用一对 CAM 在高可用性配置中共享的虚拟服务 IP 地址。这允许在高可用性配置中支持 CAM 故障切换。
Username	输入允许您登录 CAM 用户界面的 CAM 管理员的用户名。
Password	输入允许您登录 CAM 用户界面的 CAM 管理员的密码。

设备门户管理

配置设备门户设置

设备门户的全局设置

选择 工作中心 **(Work Centers)** > **BYOD** > 设置 **(Settings)** > 员工注册的设备 **(Employee Registered Devices)** 或管理 **(Administration)** > 设备门户管理 **(Device Portal Management)** > 设置 **(Settings)**。

您可以为 BYOD 门户和 My Devices 门户配置以下常规设置：

- 员工注册的设备 **(Employee Registered Devices)**：在将员工限制为 **(Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

- **重试 URL (Retry URL)**：在**重试激活 URL (Retry URL for onboarding)** 中输入可用于将设备重定向至思科 ISE 的 URL。

当您配置这些常规设置后，它们适用于为您的公司设置的所有 BYOD 门户和 My Devices 门户。

相关主题

限制员工注册的个人设备的数量
提供用于重新连接 BYOD 注册流程的 URL
分布式环境中的最终用户设备门户

设备门户的门户标识设置

这些设置的导航路径为： **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portal)**、**客户端调配门户 (Client Provisioning Portals)**、**BYOD 门户 (BYOD Portals)**、**MDM 门户 (MDM Portals)** 或**我的设备门户 (My Devices Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户设置和自定义 (Portals Settings and Customization)**。

- **门户名称 (Portal Name)**：输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

  此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述 (Description)**：可选。

- **门户测试 URL (Portal test URL)**：点击**保存 (Save)** 后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

  点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。

注释 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。

- **语言文件 (Language File)**：默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

  语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

  如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

在**门户页面自定义 (Portal Page Customizations)** 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

相关主题

创建授权策略规则
创建授权配置文件
个人设备门户

黑名单门户的门户设置

此窗口的导航路径为：**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portal)** > **编辑 (Edit)** > **门户行和流设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

使用这些设置指定值，或者定义适用于整体门户而不仅是向用户（适用情况下的访客、发起人或员工）显示的特定门户页面的行为。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：
    - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
  - 无效组合包括：
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在思科 ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

相关主题

编辑黑名单门户
黑名单门户
黑名单门户语言文件的 HTML 支持

BYOD 和 MDM 门户的门户设置

配置这些设置以定义门户页面操作。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：
    - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
  - 无效组合包括：
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。

- 在思科 ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。思科 ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

  选择用于跟踪员工设备的终端身份组。思科 ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

相关主题

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

BYOD 门户的 BYOD 设置

字段名称	使用指南
包含一个 AUP（在页面上/作为链接） (Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的窗口上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。

字段名称	使用指南
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。
在注册期间显示设备 ID 字段 (Display Device ID Field During Registration)	在注册过程中向用户显示设备 ID，即使设备 ID 已预配置并在使用 BYOD 门户时无法更改也如此。
原始 URL (Originating URL)	成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示“身份验证成功”(Authentication Success) 窗口。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的思科 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。 对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。
注册成功页面	显示设备注册成功的页面。
URL	成功对网络进行身份验证后，将用户的浏览器重定向到指定的URL，例如贵公司的网站。

注释 如果您在身份验证后将一个访客重定向到外部 URL，可能会在解析 URL 地址和重定向会话时有延迟。

相关主题

自带设备门户
创建 BYOD 门户
自带设备门户语言文件的 HTML 支持

客户端调配门户的门户设置

这些设置的导航路径为**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **创建、编辑或复制 (Create, Edit or Duplicate)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)** > **门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在思科 ISE CLI 中配置 **ip host x.x.x、x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **身份源序列 (Identity Source Sequence)**：选择将哪个身份源序列用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  思科 ISE 包含适用于发起人门户的默认身份源序列：Sponsor_Portal_Sequence。

  要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

相关主题

客户端调配门户

创建客户端调配门户

客户端调配门户语言文件的 HTML 支持

MDM 门户的员工移动设备管理设置

字段名称	使用指南
包含一个 AUP（在页面上/作为链接） (Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的窗口上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。

相关主题

移动设备管理门户

创建 MDM 门户

移动设备管理器与思科 ISE 的互操作性

我的设备门户的门户设置

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

  如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

  仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

  分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

  - 有效的组合包括（以发起人门户为例）：
    - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
  - 无效组合包括：
    - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
    - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。

注释 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**：选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

  这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

  - 以太网接口必须使用不同子网上的 IP 地址。

- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- 在思科 ISE CLI 中配置 **ip host x.x.x**、**x yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**：为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com,sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。

  如果更改默认 FQDN，还需执行以下操作：

  - 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在思科 ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。

- **身份源序列 (Identity Source Sequence)**：选择将哪个身份源序列用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  思科 ISE 包含适用于发起人门户的默认身份源序列：Sponsor_Portal_Sequence。

  要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。

- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。思科 ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

  选择用于跟踪员工设备的终端身份组。思科 ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

- **当此身份组中的终端达到 __ 天时将其清除 (Purge Endpoints in this Identity Group when they Reach __ Days)**：指定从思科 ISE 数据库中清除设备之前应经历的天数。每天都会进行清除，并且清除活动与整体清除时间同步。更改全局应用于此终端身份组。

  如果根据其他策略条件对终端清除策略进行更改，则此设置不可再使用。

- **空闲超时 (Idle Timeout)**：输入思科 ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。
- 显示语言
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。

- **回退语言 (Fallback Language)**：选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
- **始终使用 (Always Use)**：选择要用于门户的显示语言。此设置会覆盖**用户浏览器区域 (User Browser Locale)** 选项。

相关主题

我的设备门户
创建我的设备门户

我的设备门户的登录页面设置

- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定思科 ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting)**：指定思科 ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **包含 AUP (Include an AUP)**：将可接受使用政策窗口添加到流。可以将 AUP 添加到窗口，或链接到另一个窗口。

相关主题

我的设备门户
创建我的设备门户
监控我的设备门户和终端活动

我的设备门户的可接受使用策略页面设置

字段	使用指南
包含 AUP 页面 (Include AUP page)	在单独的页面上向用户显示公司的网络使用条款和条件。
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用**接受 (Accept)** 按钮。
仅首次登录时 (On First Login only)	仅在用户首次登录到网络或门户时显示 AUP。
每次登录时 (On Every Login)	每次用户登录到网络或门户时显示 AUP。

字段	使用指南
每 __ 天（从首次登录算起）(Every __ Days [starting at first login])	在用户首次登录到网络或门户时定期显示 AUP。

相关主题

我的设备门户

创建我的设备门户

我的设备门户的登录后横幅页面设置

字段名称	使用指南
包含登录后横幅页面 (Include a Post-Login Banner page)	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

相关主题

我的设备门户

创建我的设备门户

我的设备门户的员工更改密码设置

要设置员工密码策略，请依次选择 **Administration** > **Identity Management** > **Settings** > **Username Password Policy**。

字段名称	使用指南
Allow internal users to change password	在员工登录 My Devices 门户后，允许员工更改其密码。 这仅适用于帐户存储于思科 ISE 数据库中的员工，不适用于帐户存储于外部数据库（例如 Active Directory 或 LDAP）的员工。

相关主题

创建我的设备门户

门户中的 UTF-8 字符支持

管理我的设备门户的设备设置

表 *48:* 管理我的设备门户的设备设置

字段名称	使用指南
Lost	使员工可以指示其设备已丢失。此操作会将“我的设备”(My Devices) 门户中的设备状态更新为“丢失”(Lost) 并将该设备添加至黑名单终端身份组。

字段名称	使用指南
Reinstate	此操作可恢复列入黑名单、已丢失或被盗的设备并将其状态重置为上一次的已知值。此操作会将被盗设备的状态重置为 Not Registered，因为它要经过额外调配才能连接网络。 如果您要阻止员工恢复您已列入黑名单的设备，请勿在“我的设备”(My Devices) 门户中启用此选项。
删除	使员工在已注册设备达到最大数量时，可以从“我的设备”(My Devices) 门户删除已注册设备或删除未使用的设备和添加新设备。此操作会将设备从 My Devices 门户中显示的设备列表上删除，但是设备仍保留在思科 ISE 数据库中并继续列于 Endpoints 列表上。 要定义员工可以使用 BYOD 门户或“我的设备”(My Devices) 门户注册的个人设备最大数量，请选择**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。 要从思科 ISE 永久删除设备，选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)**。
Stolen	使员工可以指示其设备已被盗。此操作会将“我的设备”(My Devices) 门户中的设备状态更新为 Stolen 并将该设备添加至黑名单终端身份组，然后删除其证书。
Device lock	仅适用于已向 MDM 注册的设备。 在员工设备丢失或被盗的情况下，使员工可以立即从 My Devices 门户远程锁定其设备。此操作可防止他人未经授权而使用设备。 但是，在 My Devices 门户中无法设置 PIN 而且员工应已提前在其移动设备上配置 PIN。
Unenroll	仅适用于已向 MDM 注册的设备。 如果员工在工作中不再需要使用其设备，则可以选择此选项。此操作仅删除您公司安装的那些应用和设置，其他应用和数据仍会保留在员工的移动设备上。
Full wipe	仅适用于已向 MDM 注册的设备。 使员工丢失其设备或换成使用新设备的情况下可以选择此选项。此操作会将员工的移动设备重置为其默认出厂设置，删除所安装的应用和数据。

相关主题

管理员工添加的个人设备

我的设备门户

为我的设备门户自定义添加、编辑和定位设备

在 **Page Customizations** 下，您可以自定义显示在我的设备门户的添加、编辑和定位选项卡中的消息、标题、内容、说明以及字段和按钮标签。

相关主题

我的设备门户
创建我的设备门户

设备门户的支持信息页面设置

字段名称	使用指南
包含支持信息页面 (Include a Support Information Page)	在门户的所有已启用窗口上显示指向信息窗口（例如**联系我们 [Contact Us]**）的链接。
MAC 地址	在**支持信息 (Support Information)** 窗口上包含设备的 MAC 地址。
IP 地址	在**支持信息 (Support Information)** 窗口上包含设备的 IP 地址。
浏览器用户代理	在**支持信息 (Support Information)** 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 (Policy Server)	在**支持信息 (Support Information)** 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。
隐藏字段 (Hide Field)	如果字段标签将会包含的信息不存在，请勿在**支持信息 (Support Information)** 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示**故障代码 (Failure code)**，即使已选择故障代码也如此。
显示不含任何值的标签 (Display Label with no Value)	在**支持信息 (Support Information)** 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示**故障代码 (Failure code)**，即使其为空白也如此。
显示含默认值的标签 (Display Label with Default Value)	如果标签将会包含的信息不存在，请在**支持信息 (Support Information)** 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用”(Not Available)，并且故障代码未知，则**故障代码 (Failure Code)** 将显示**不可用 (Not Available)**。

相关主题

监控我的设备门户和终端活动
访问设备门户

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。