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
- 感知威胁分析 (CTA) 适配器
- Qualys

注释 TC-NAC 流目前仅支持 Qualys 企业版。

- Rapid7 Nexpose
- Tenable 安全中心

当检测到终端威胁事件时，可以在**受到危害的终端 (Compromised Endpoints)** 窗口选择该终端的 MAC 地址并应用一个 ANC 策略，例如隔离。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：

- CTA-Course_Of_Action（值可以是内部屏蔽 [Internal Blocking]、清除 [Eradication] 或监控 [Monitoring]）
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

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

当收到某个终端的漏洞事件时，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。
- 可以停止并重新启动适配器，而不会丢失其配置。配置适配器之后，您可以随时停止适配器。即使重新启动 ISE 服务，适配器也将保持此状态。选择适配器并点击**重新启动 (Restart)** 以重新启动适配器。

注释 当适配器处于停止 (Stopped) 状态时，您只能编辑适配器实例的名称；无法编辑适配器配置或高级设置。

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。
- **威胁事件 (Threat Events)**：威胁事件报告提供思科 ISE 从已配置的各种适配器接收的所有威胁事件的列表。此报告不包括漏洞评估事件。
- **漏洞评估 (Vulnerability Assessment)**：漏洞评估报告提供您的终端正在进行的评估的信息。您可以查看此报告以确认评估是否以配置策略为基础正在进行。

可以在**操作 (Operations) > 报告 (Reports) > 诊断 (Diagnostics) > ISE 计数器 (ISE Counters) > 阈值计数器趋势 (Threshold Counter Trends)** 位置查看以下信息：

- 收到事件的总数
- 威胁事件的总数
- 漏洞事件的总数
- 发出（到 PSN）的 CoA 的总数

系统每 5 分钟收集一次这些属性的值，因此，这些值表示最近 5 分钟的计数。

威胁 (Threat) 控制面板包含以下 Dashlet：

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

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

“受到危害的终端” (Compromised Endpoint) 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。

“操作过程”(Course Of Action) 图表显示根据从 CTA 适配器收到的 CTA-Course_Of_Action 属性，对威胁事件执行的操作（内部屏蔽、根除或监控）。

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

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

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

支持捆绑包中包含以威胁防护为中心的 NAC 服务日志。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**。

相关主题

添加 Sourcefire FireAMP 适配器， 第 5 页
配置感知威胁分析适配器， 第 6 页
为 CTA 适配器配置授权配置文件， 第 6 页
使用操作过程属性配置授权策略， 第 6 页
以威胁防护为中心的 NAC 服务， 第 1 页

添加 Sourcefire FireAMP 适配器

开始之前

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

步骤 1

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 选择要订阅的事件源。可提供以下选项：

- **仅 AMP 事件**
- **仅 CTA 事件**
- **CTA 和 AMP 事件**

步骤 11 点击 FireAMP 链路并以管理员的身份登录 FireAMP。点击**应用 (Applications)** 窗格中的**允许 (Allow)**，以授权流事件导出请求。
您将被重定向回到思科 ISE。

步骤 12 选择您要监控的事件（例如，可疑下载、连接到可疑域、已执行恶意软件、Java 威胁）。

当更改高级设置或重新配置适配器时，如果向 AMP 云中添加了任何新事件，则这些事件也会列在**事件列表 (Events Listing)** 窗口中。

可以为适配器选择一种日志级别。可用选项为：**错误 (Error)** 、**信息 (Info)** 和**调试 (Debug)**。

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

配置感知威胁分析适配器

开始之前

- 您需要在部署节点上启用以威胁防护为中心的 NAC 服务（请参阅启用威胁中心 NAC 服务，第 4 页）。
- 通过 http://cognitive.cisco.com/login 登录到思科感知威胁分析 (CTA) 门户并请求 CTA STIX/TAXII 服务。有关详细信息，请参阅 Cisco ScanCenter 管理员指南。
- 感知威胁分析 (CTA) 适配器使用含 SSL 的 TAXII 协议轮询 CTA 云是否有检测到的威胁。它还支持使用代理。
- 将适配器证书导入到受信任证书库。依次选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任证书 (Trusted Certificates) > 导入 (Import)** 导入证书。

注释 CTA 使用 Web 代理日志中作为 IP 地址或用户名列出的用户身份。具体而言，在使用 IP 地址的情况下，通过代理日志可用的设备的 IP 地址可能与内部网络上另一台设备的 IP 地址冲突。例如，通过 AnyConnect 和分割隧道直接连接到互联网的漫游用户可以获取本地 IP 范围地址（例如，10.0.0.X 地址），该地址可能与内部网络中使用的重叠私用 IP 范围中的地址冲突。我们建议您在定义策略时考虑逻辑网络架构，以避免对不匹配的设备应用隔离操作。

为 CTA 适配器配置授权配置文件

对于每个威胁事件，CTA 适配器会返回行动方案属性的以下值之一：内部阻止、监控或根除。您可以根据这些值创建授权配置文件。

步骤 1 依次选择在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**策略 (Policy) > 策略元素 (Policy Elements) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)** 。

步骤 2 点击**添加 (Add)**。

步骤 3 输入授权配置文件的名称和描述。

步骤 4 选择访问类型。

步骤 5 输入所需的详细信息，并点击**提交 (Submit)**。

使用操作过程属性配置授权策略

您可以使用 CTA-Course_Of_Action 属性为报告威胁事件的终端配置授权策略。此属性在“威胁”(Threat) 目录下可用。

您还可以根据 CTA-Course_Of_Action 属性创建例外规则。

步骤 1 选择**策略 (Policy) > 策略集 (Policy Sets)**
您可以为有威胁事件的终端编辑现有策略规则或创建新例外规则。

步骤 2 创造一个条件检查 CTA-Course_Of_Action 属性值并分配合适的授权配置文件。例如：

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

注释 “Internal Blocking”是建议用于隔离终端的操作过程属性。

步骤 3 单击**保存**。

当收到终端的威胁事件时，思科 ISE 会检查该终端是否有任何匹配的授权策略，并仅在终端处于活动状态时触发 CoA。如果终端处于离线状态，威胁事件详细信息会添加到“威胁事件”(Threat Events) 报告（“操作”(Operations)>“报告”(Reports)>“以威胁防护为中心的 NAC”(Threat Centralic NAC)>“威胁事件”(Threat Events)）。

注释 有时，CTA 会在一个事件中发送多个风险及其关联的操作过程属性。例如，它可以在一个事件中发送“内部阻断”(Internal Blocking) 和“监控”(Monitoring)（操作过程属性）。在这种情况下，如果您已使用“equals”运算符配置隔离终端的授权策略，则不会隔离终端。例如：

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems（授权配置文件）
```

在这种情况下，必须在授权策略中使用“contains”运算符来隔离终端。例如：

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

思科 ISE 中的漏洞评估支持

思科 ISE 与以下漏洞评估 (VA) 生态系统合作伙伴集成，以获取连接到思科 ISE 网络的终端漏洞结果：

- Qualys：Qualys 是一种基于云的评估系统，在网络中部署有扫描设备。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：用于检查终端的最后扫描结果
  - 扫描 API：用于触发终端的按需扫描

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

- Rapid7 Nexpose：思科 ISE 与漏洞管理解决方案 Rapid7 Nexpose 集成，以帮助检测漏洞，使您能够快速响应此类威胁。思科 ISE 从 Nexpose 接收漏洞数据，并根据在 ISE 中配置的策略隔离受影响的终端。从思科 ISE 控制板，可以查看受影响的终端并采取适当的操作。

  思科 ISE 已经过 Nexpose 版本 6.4.1 测试。

- Tenable SecurityCenter（Nessus 扫描程序）：思科 ISE 与 Tenable SecurityCenter 集成并从 Tenable Nessus 扫描程序（由 Tenable SecurityCenter 管理）接收漏洞数据，然后，系统根据您在 ISE 中配置的策略来隔离受影响的终端。从思科 ISE 控制板，可以查看受影响的终端并采取适当的操作。

  思科 ISE 已经过 Tenable SecurityCenter 5.3.2 测试。

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

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

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

在此版本的思科 ISE 中，仅对采用 IPv4 地址的终端进行漏洞评估。

启用并配置漏洞评估服务

要启用和配置思科 ISE 的漏洞评估服务，请执行以下任务：

步骤 1 启用威胁中心 NAC 服务，第 4 页。

步骤 2 若要配置以下项：

- Qualys 适配器，请参阅配置 Qualys 适配器，第 9 页。
- Nexpose 适配器，请参阅配置 Nexpose 适配器，第 11 页。
- 租户适配器，请参阅。配置 Tenable 适配器，第 14 页

步骤 3 配置授权配置文件，第 17 页。

步骤 4 配置隔离易受攻击的终端的例外规则，第 17 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**。

相关主题

添加 Sourcefire FireAMP 适配器，第 5 页
配置感知威胁分析适配器，第 6 页
为 CTA 适配器配置授权配置文件，第 6 页
使用操作过程属性配置授权策略，第 6 页
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。

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**。

配置 Nexpose 适配器

必须创建一个 Nexpose 适配器，供思科 ISE 与 Nexpose 通信和获取 VA 结果。

开始之前

- 确保已在思科 ISE 中启用以威胁防护为中心的 NAC 服务。
- 登录 Nexpose 安全控制台并创建具有以下权限的用户帐户：
  - 管理站点

- 创建报告

- 将 Nexpose 服务器证书导入思科 ISE 中的受信任证书存储区（**管理 (Administration) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates) > 导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）思科 ISE 受信任证书库中。
- 思科 ISE 通过 HTTPS/SSL（端口 3780）与 Nexpose 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 **Rapid7 Nexpose:VA**。

步骤 4 输入适配器实例的名称。例如，Nexpose。

系统会显示一个列表窗口，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 Nexpose 适配器的状态应该会更改为**准备配置 (Ready to Configure)**。

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

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

字段名称	说明
Nexpose 主机 (Nexpose Host)	Nexpose 服务器的主机名。
Nexpose 端口 (Nexpose Port)	3780。
用户名 (Username)	Nexpose 管理员用户帐户。
密码 (Password)	Nexpose 管理员用户帐户的密码。
HTTP 代理主机 (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。

步骤 8 点击**下一步 (Next)** 以配置高级设置。

步骤 9 在**高级设置 (Advanced Settings)** 窗口中输入以下值。此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
用于检查最新扫描结果的设置	
检查最新扫描结果之间的间隔（分钟）**(Interval between checking the latest scan results in minutes)**	必须再次检查最后扫描结果之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
可以触发检查最新扫描结果的待处理请求数 **(Number of pending requests that can trigger checking the latest scan results)**	如果队列中的扫描请求数超过此处指定的最大数量，则系统会在检查最新扫描结果之间的间隔（分钟）(Interval between checking the latest scan results in minutes) 字段中指定的时间间隔之前检查最后扫描结果。有效范围为 1 到 1000。
验证 MAC 地址	正确还是错误？当设置为 true 时，Nexpose 的最后扫描结果只会在其包括终端 MAC 地址时使用。
扫描设置	
每个站点的扫描触发间隔（分钟）**(Scan trigger interval for each site in minutes)**	触发扫描之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
各站点触发扫描之前待处理请求的数量 **(Number of pending requests before a scan is triggered for each site)**	如果队列扫描请求数超过此处指定的最大数量，则会在**扫描超时（分钟）(Scan timeout in minutes)** 字段中的指定时间间隔之前触发扫描。有效范围为 1 到 1000。
扫描超时（按分钟计）	时间（按分钟计），该时间后扫描请求将超时。如果扫描请求超时，将生成警报。有效范围为 20 到 1440。
可以并行触发扫描的站点数量 **(Number of sites for which scans could be triggered concurrently)**	可同时对其运行扫描的站点数。有效范围为 1 到 200。
时区	根据 Nexpose 服务器中配置的时区选择时区。

字段名称	说明
用于检查最新扫描结果的设置	
Http 超时（秒）(Http timeout in seconds)	思科 ISE 等待来自 Nexpose 的响应的时间间隔（秒）。有效范围为 5 到 1200。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG)和“跟踪”(TRACE)。

步骤 10 点击**下一步 (Next)** 以审核配置设置。

步骤 11 点击**完成**。

配置 Tenable 适配器

必须创建一个 Tenable 适配器，供思科 ISE 与 Tenable SecurityCenter（Nessus 扫描器）通信和获取 VA 结果。

开始之前

注释 必须在 Tenable SecurityCenter 中配置以下内容，然后才能在思科 ISE 中配置 Tenable 适配器。请参阅 Tenable SecurityCenter 文档以了解这些配置。

- 您必须安装 Tenable Security Center 和 Tenable Nessus 漏洞扫描器。在注册 Tenable Nessus 扫描器时，请确保在**注册 (Registration)** 字段中选择**由 SecurityCenter 管理 (Managed by SecurityCenter)**。
- 在 Tenable SecurityCenter 中创建具有安全管理器权限的用户帐户。
- 在 SecurityCenter 中创建存储库（使用管理员凭证登录到 Tenable SecurityCenter 并选择**存储库 (Repository) > 添加 (Add)**）。
- 在存储库中添加要扫描的终端 IP 范围。
- 添加 Nessus 扫描器。
- 创建扫描区域，并向扫描区域和映射到这些扫描区域的扫描器分配 IP 地址。
- 为 ISE 创建扫描策略。
- 添加活动扫描并将其与 ISE 扫描策略关联。配置设置和目标（IP/DNS 名称）。
- 从 Tenable SecurityCenter 导出系统和根证书，并将其导入思科 ISE 中的受信任证书存储区（**管理 (Administration) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates) > 导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）思科 ISE 受信任证书库中。

• 思科 ISE 通过 HTTPS/SSL （端口 443）与 Tenable SecurityCenter 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，选择 **Tenable Security Center:VA**。

步骤 4 输入适配器实例的名称。例如，Tenable。

系统会显示一个列表窗口，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 Tenable 适配器的状态应更改为**准备配置 (Ready to Configure)**。

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

步骤 7 在 Tenable SecurityCenter 配置窗口中输入以下值并点击**下一步 (Next)**。

字段名称	说明
Tenable SecurityCenter 主机	Tenable SecurityCenter 的主机名。
Tenable SecurityCenter 端口	443
用户名	在 Tenable SecurityCenter 中具有安全管理器权限的用户帐户的用户名。
密码	在 Tenable SecurityCenter 中具有安全管理器权限的用户帐户的密码。
HTTP 代理主机 (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	输入代理服务器使用的端口号。

步骤 8 单击**下一步**。

步骤 9 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
存储库	选择您在 Tenable SecurityCenter 中创建的存储库。
扫描策略	选择您在 Tenable SecurityCenter 中为 ISE 创建的扫描策略。
用于检查最新扫描结果的设置	

字段名称	说明
检查最新扫描结果之间的间隔（分钟）**(Interval between checking the latest scan results in minutes)**	必须再次检查最后扫描结果之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
可以触发检查最新扫描结果的待处理请求数 **(Number of pending requests that can trigger checking the latest scan results)**	如果队列中的扫描请求数超过此处指定的最大数量，则系统会在**检查最新扫描结果之间的间隔（分钟）(Interval between checking the latest scan results in minutes)** 字段中指定的时间间隔之前检查最后扫描结果。有效范围为 1 到 1000。默认值为 10。
验证 **MAC** 地址	正确还是错误？当设置为 true 时，Tenable SecurityCenter 的最后扫描结果只会在其包括终端 MAC 地址时使用。
扫描设置	
每个站点的扫描触发间隔（分钟）**(Scan trigger interval for each site in minutes)**	触发按需扫描之前所经历的时间间隔（分钟）。有效范围为 1 到 2880。
触发扫描之前待处理请求的数量 **(Number of pending requests before a scan is triggered)**	如果队列扫描请求数超过此处指定的最大数量，则会在**每个站点的扫描触发间隔（分钟）(Scan trigger interval for each site in minutes)** 字段中的指定时间间隔之前触发按需扫描。有效范围为 1 到 1000。
扫描超时（按分钟计）	扫描请求超时之前所经历的时间（分钟）。如果扫描请求超时，将生成警报。有效范围为 20 到 1440。
可以并行运行的扫描数 **(Number of scans that could run in parallel)**	可同时运行的扫描数量。有效范围为 1 到 200。
Http 超时（秒）**(Http timeout in seconds)**	思科 ISE 等待来自 Tenable SecurityCenter 的响应的时间间隔（秒）。有效范围为 5 到 1200。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG)和“跟踪”(TRACE)。

步骤 10 点击**下一步 (Next)** 以审核配置设置。

步骤 11 点击**完成**。

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**。

配置隔离易受攻击的终端的例外规则

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

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

这些属性在威胁目录下可用。有效值范围为 0 到 10。

您可以选择隔离终端，提供有限访问权限（重定向至不同的门户）或拒绝请求。

步骤 1 选择**策略 (Policy)** > **策略集 (Policy Sets)**。
您可以编辑现有策略规则或创建新例外规则，以检查 VA 属性。

步骤 2 创造条件检查 Qualys 评分并分配正确的授权配置文件。例如：

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

步骤 3 点击**保存**。

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。

受信任证书设置

下表介绍了受信任证书的**编辑 (Edit)** 窗口中的字段。在此窗口中编辑 CA 证书属性。此页面的导航路径为： **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。选中要编辑的受信任证书的复选框，然后单击**编辑 (Edit)**。

表 *1:* 受信任证书编辑设置

字段名称	使用指南
Certificate Issuer	
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	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。
说明	（可选）输入说明。
Usage	
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。

字段名称	使用指南
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。
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。
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。
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。
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。
OCSP 响应器无法访问时拒绝请求 (Reject the request if OCSP Responder is unreachable)	选中此复选框供思科 ISE 在 OCSP 响应器无法访问时拒绝请求。
Download CRL	选中此复选框以使思科 ISE 下载 CRL。
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。
Retrieve CRL	可以自动或定期下载 CRL。请配置下载时间间隔。
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。

字段名称	使用指南
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。
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

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 *2:* 存储库设置

字段	使用指南
存储库	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。
协议	从可用协议中选择一个您想要使用的协议。
Server Name	（对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段）输入您想要在其上创存储库的服务器的主机名或 IP 地址（IPv4 或 IPv6）。 注释　如果要添加具有 IPv6 地址的存储库，请确保 ISE eth0 接口已配置有 IPv6 地址。

字段	使用指南
路径	输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。 此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于FTP协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。
启用 PKI 身份验证	（可选；仅适用于SFTP存储库）如果要在SFTP存储库中启用RSA公钥身份验证，请选中此复选框。
用户名	（对于 FTP、SFTP 为必填字段）输入对指定服务器拥有写入权限的用户名。用户名可以包含字母数字和 _-。/@\$ 字符。
Password	（对于 FTP、SFTP 为必填字段）输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、|、@、#、$、^、&、*、(、)、+、和 =。

相关主题

备份和恢复存储库

创建存储库

按需备份设置

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

表 *3:* 按需备份设置

字段名称	使用指南
类型	选择以下其中一个选项： • **配置数据备份 (Configuration Data Backup)**：包含应用特定配置数据和思科 ADE 操作系统配置数据 • **运行数据备份 (Operational Data Backup)**：包含监控和故障排除数据
Backup Name	输入备份文件的名称。

字段名称	使用指南
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 *4:* 计划备份设置

字段名称	使用指南
类型	选择以下其中一个选项： • **配置数据备份 (Configuration Data Backup)**：包含应用特定配置数据和思科 ADE 操作系统配置数据 • **运行数据备份 (Operational Data Backup)**：包含监控和故障排除数据
名称	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。
说明	输入对备份的说明。

字段名称	使用指南
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

计划策略导入设置

下表对**计划策略导出 (Schedule Policy Export)** 窗口中的字段进行了说明。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **备份和恢复(Backup and Restore)** > **策略导出 (Policy Export)**。

表 *5:* 计划策略导入设置

通用 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

- **系统将分配 SGT 编号 (System will Assign SGT Numbers)**：如果希望思科 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。思科 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，思科 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，思科 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

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

您可以使用这些窗口在思科 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**新网络设备 (New Network Devices)** 窗口中的字段。

表 *6:* 网络设备设置

字段名称	说明
名称	输入网络设备的名称。 您可以为网络设备提供一个不同于设备主机名的描述性名称。设备名称是一个逻辑标识符。 **注释** 配置设备名称后无法进行编辑。
说明	输入设备的说明。
IP 地址或 **IP** 范围	从下拉列表中选择以下选项之一，并在显示的字段中输入所需的值： • **IP 地址**：输入单个 IP 地址（IPv4 或 IPv6 地址）和子网掩码。 • **IP 范围**：输入所需的 IPv4 地址范围。要在身份验证期间排除 IP 地址，请在**排除 (Exclude)** 文本框中输入 IP 地址或 IP 地址范围。 以下是定义 IP 地址和子网掩码或 IP 地址范围时必须遵守的准则： • 您可以定义一个特定 IP 地址或具有子网掩码的 IP 地址范围。如果设备 A 定义了 IP 地址范围，则可以使用在设备 A 中定义的 IP 地址范围的某个地址配置另一设备 B。 • 您可以在所有八位组中定义 IP 地址范围。您可以使用连字符 (-) 或使用星号 (*) 作为通配符来指定 IP 地址范围。例如，*.*.*.*、1-10.1-10.1-10.1-10 或 10-11.*.5.10-15。 • 在已添加 IP 地址范围子集的场景中，可以从配置的范围中排除该子集。例如，10.197.65.*/10.197.65.1 或 10.197.65.* 会排除 10.197.65.1。 • 您不能使用相同的特定 IP 地址定义两台设备。 • 您不能使用同一 IP 地址范围定义两台设备。IP 地址范围不得部分或全部重叠。

字段名称	说明
设备配置文件	从下拉列表中选择网络设备的供应商。 使用下拉列表旁的工具提示可查看选定供应商的网络设备所支持的流和服务。工具提示还显示设备使用的RADIUS CoA端口和URL重定向类型。这些属性在设备类型的网络设备配置文件中进行定义。
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)**、**IPSEC** 和**设备类型 (Device Type)** 下拉列表中选择所需的值。 如果未将设备专门分配到组，则设备将加入默认设备组（根网络设备组），位置为**所有位置 (All Locations)**，设备类型为**所有设备类型 (All Device Types)**。

RADIUS 身份验证设置

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

表 *7:*“*RADIUS* 身份验证设置”*(RADIUS Authentication Settings)* 区域中的字段

字段名称	使用指南
RADIUS UDP 设置	
协议	显示 **RADIUS** 作为所选协议。

字段名称	使用指南
共享密钥 **(Shared Secret)**	输入网络设备的共享密钥。 共享密钥是使用 **radius-host** 命令和 **pac** 选项在网络设备上配置的密钥。 注释 共享密钥长度必须等于或大于在**设备安全设置 (Device Security Settings)** 窗口的 **RADIUS 共享密钥最小长度 (Minimum RADIUS Shared Secret Length)** 字段中配置的值（ **管理 (Administration) 网络资源 (Network Resources) 网络设备 (Network Devices) 设备安全设置 (Device Security Settings)** ）。 对于 RADIUS 服务器，长度最好为 22 个字符。对于新安装和升级的部署，默认情况下，共享密钥长度为四个字符。您可以在**设备安全设置 (Device Security Settings)** 窗口中更改此值。

字段名称	使用指南
使用第二个共享密钥	指定网络设备和思科 ISE 要使用的第二个共享密钥。 注释 虽然思科 TrustSec 设备可以利用双重共享密钥（密钥），但思科 ISE 发送的思科 TrustSec CoA 数据包将始终使用第一个共享密钥（密钥）。要启用第二个共享密钥，请选择必须从哪一个思科 ISE 节点向 TrustSec 设备发送思科 TrustSec CoA 数据包。在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **高级 TrustSec 设置 (Advanced TrustSec Settings)** 窗口的**发送自 (Send From)** 下拉列表中，配置要用于此任务的思科 ISE 节点。您可以选择主管理节点 (PAN) 或策略服务节点 (PSN)。如果所选 PSN 节点关闭，PAN 将向思科 TrustSec 设备发送思科 TrustSec CoA 数据包。 注释 RADIUS 访问请求的“第二共享密钥”功能仅适用于包含**消息-身份验证器 (Message-Authenticator)** 字段的数据包。

字段名称	使用指南
CoA 端口	指定要用于 RADIUS DTLS CoA 的端口。 设备的默认CoA端口在为网络设备配置的网络设备配置文件中进行定义（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**）。点击**设置为默认 (Set To Default)** 按钮以使用默认 CoA 端口。 注释 如果修改在 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 下的**网络设备 (Network Devices)** 窗口（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）中指定的 CoA 端口，请确保在**网络设备配置文件 (Network Device Profile)** 窗口（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Device Profiles)**）中为相应配置文件指定相同的 CoA 端口。
RADIUS DTLS 设置	
需要 DTLS	如果选中**需要 DTLS (DTLS Required)** 复选框，则思科 ISE 仅处理来自此设备的 DTLS 请求。如果禁用此选项，则思科 ISE 会同时处理来自此设备的 UDP 和 DTLS 请求。 RADIUS DTLS 为安全套接字层 (SSL) 隧道建立和 RADIUS 通信提供了更高的安全性。
共享密钥	显示用于 RADIUS DTLS 的共享密钥。此值为固定值，用于计算消息摘要 5 (MD5) 完整性检查。
CoA 端口	指定用于 RADIUS DTLS CoA 的端口。
CoA ISE 证书 CA 颁发者	从下拉列表中选择要用于 RADIUS DTLS CoA 的证书颁发机构。

字段名称	使用指南
DNS 名称	输入网络设备的 DNS 名称。如果在 **RADIUS 设置 (RADIUS Settings)** 窗口下启用了**启用 RADIUS/DTLS 客户端身份验证 (Enable RADIUS/DTLS Client Identity Verification)**（**管理 (Adminstration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **RADIUS**，思科 ISE 会将此 DNS 名称与客户端证书中指定的 DNS 名称进行比较，以验证网络设备的身份。
常规设置	
启用 **KeyWrap (Enable KeyWrap)**	仅当网络设备支持 KeyWrap 算法时，选中**启用 KeyWrap (Enable KeyWrap)** 复选框。此选项用于通过 AES KeyWrap 算法提高 RADIUS 安全性。 注释　当您在 FIPS 模式下运行思科 ISE 时，您必须在网络设备上启用 KeyWrap。
密钥加密密钥 **(ey Encryption Key)**	输入用于会话加密（保密）的加密密钥。
消息身份验证器代码密钥 **(Message Authenticator Code Key)**	输入用于 RADIUS 消息键控散列消息验证码 (HMAC) 计算的密钥。
密钥输入格式 **(Key Input Format)**	点击以下格式之一对应的单选按钮： • **ASCII**：在**密钥加密密钥 (Key Encryption Key)** 字段中输入的值的长度必须为 16 个字符（字节），在**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入的值长度必须为 20 个字符（字节）。 • **十六进制 (Hexadecimal)**：在**密钥加密密钥 (Key Encryption Key)** 字段中输入的值的长度必须为 32 个字符（字节），在**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入的值长度必须为 40 个字符（字节）。 指定想要用于输入思科 ISE FIPS 加密密钥的密钥输入格式，从而使其与无线 LAN 控制器上的配置一致。您指定的值必须是密钥的正确（完整）长度，不允许使用短于此长度的值。

TACACS 身份验证设置

表 *8: TACACS* 身份验证设置区域中的字段

字段名称	使用指南
Shared Secret	当启用 TACACS+ 协议时，会向网络设备分配文本字符串。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。
停用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。点击**停用 (Retire)** 时，系统会显示一个消息框。您可以点击**是 (Yes)** 或**否 (No)**。
剩余停用期 **(Remaining Retired Period)**	（只有当您在**淘汰 (Retire)** 消息框中选择**是 (Yes)** 时才可用）在以下导航路径中显示指定的默认值：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。您可以更改默认值。 这允许输入新的共享密钥。旧共享密钥会在指定天数内保持有效。
结束	（仅当在**停用 (Retire)** 消息框中选择**是 (Yes)** 时可用）结束停用期并终止旧共享密钥。
启用单连接模式	选中**启用单连接模式 (Enable Single Connect Mode)** 复选框，将单一 TCP 连接用于与网络设备之间的所有 TACACS 通信。点击以下选项之一的单选按钮： • **传统思科设备 (Legacy Cisco Devices)** • **TACACS 草案合规性单连接支持** 如果禁用**单连接模式 (Single Connect Mode)**，思科 ISE 会对每个 TACACS 请求使用新的 TCP 连接。

SNMP 设置

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

表 *9: 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，因为当在后续步骤中选择 **Priv** 安全级别时，它允许加密数据包。 注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的**网络设备会话状态 (Network Device Session Status)** 摘要报告（**操作 (Operations)** > **报告 (Reports)** > **诊断 (Diagnostics)** > **网络设备会话状态 (Network Device Session Status)**）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。
SNMP 只读社区 (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。 注释 不允许使用插入符号 (circumflex ^)。
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。

字段名称	使用指南
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。 **注释** 不能使用插入符号 (circumflex ^)。
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。 **注释** 不能使用插入符号 (circumflex ^)。
轮询间隔 (Polling Interval)	输入轮询间隔（秒）。默认值为 3600 秒。
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。

字段名称	使用指南
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 *10:* 高级 *TrustSec* 设置区域中的字段

字段名称	使用指南
设备身份验证设置	
将设备 ID 用于 Trustsec 标识 (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 (Use Device ID for TrustSec Identification)** 复选框时，才能在此字段中输入设备 ID。
密码	输入在思科 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	
设备 ID	仅当未选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框时，才能在此字段中输入设备 ID。
密码	输入在思科 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。

字段名称	使用指南
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。
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。
将配置更改发送到设备 (Send Configuration Changes to Device)	如果希望思科 ISE 使用 CoA 或 CLI (SSH) 将思科 TrustSec 配置更改发送到思科 TrustSec 设备，请选中**将配置更改发送到设备 (Send Configuration Changes to Device)** 复选框。根据需要，点击 **CoA** 或 **CLI (SSH)** 的单选按钮。 如果希望思科 ISE 使用 CoA 将配置更改发送到思科 TrustSec 设备，请选择 **CoA** 选项。 如果希望思科 ISE 使用 CLI（使用 SSH 连接）将配置更改发送到思科 TrustSec 设备，请选择 **CLI (SSH)** 选项。有关详细信息，请参阅向不支持 CoA 的设备推送配置更改。
发送自 (Send From)	从下拉列表中选择必须从哪一个思科 ISE 节点将配置更改发送到思科 TrustSec 设备。您可以选择 PAN 或 PSN 节点。如果所选择的 PSN 节点关闭，则使用 PAN 将配置更改发送到思科 TrustSec 设备。
测试连接	您可以使用此选项测试思科 TrustSec 设备与所选思科 ISE 节点（PAN 或 PSN）之间的连接。

字段名称	使用指南
SSH 密钥	要使用此功能，请打开从思科 ISE 到网络设备的 SSHv2 隧道，然后使用设备的 CLI 检索 SSH 密钥。您必须复制此密钥并将其粘贴到 **SSH 密钥 (SSH Key)** 字段中以进行验证。有关详细信息，请参阅《》中的“ SSH 密钥验证”部分请参阅 SSH 密钥验证。
设备配置部署设置	
当部署安全组标签映射更新时纳入该设备 **(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 (Include this device when deploying Security Group Tag Mapping Updates)** 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 **Trustsec PAC**	
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。
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。

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 *11:*“默认网络设备”*(Default Network Device)* 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。
RADIUS UDP 设置	
共享密钥	输入共享密钥。共享密钥最大长度为 127 个字符。 共享密钥是您使用 **radius-host** 命令和 **pac** 选项在网络设备上配置的密钥。 注释 共享密钥长度必须等于或大于在**设备安全设置 (Device Security Settings)** 窗口的 **RADIUS 共享密钥最小长度 (Minimum RADIUS Shared Secret Length)** 字段中配置的值（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **设备安全设置 (Device Security Settings)**）。默认情况下，对于新安装和升级的部署，此值为 4 个字符。对于 RADIUS 服务器，长度最好为 22 个字符。

字段名称	使用指南
RADIUS DTLS 设置	
需要 **DTLS**	如果选中**需要 DTLS (DTLS Required)** 复选框，则思科 ISE 仅处理来自此设备的 DTLS 请求。如果禁用此选项，则思科 ISE 会同时处理来自此设备的 UDP 和 DTLS 请求。 RADIUS DTLS 为 SSL 隧道建立和 RADIUS 通信提供了更高的安全性。
共享密钥	显示用于 RADIUS DTLS 的共享密钥。此值为固定值，用于计算 MD5 完整性检查。
CoA ISE 证书 CA 颁发者	从 **CoA ISE 证书 CA 颁发者 (Issuer CA of ISE Certificates for CoA)** 下拉列表中，选择要用于 RADIUS DTLS CoA 的证书颁发机构。
常规设置	
启用 **KeyWrap (Enable KeyWrap)**	仅在网络设备支持 KeyWrap 算法时选中**启用 KeyWrap (Enable KeyWrap)** 复选框，这可以通过 AES KeyWrap 算法提高 RADIUS 安全性。 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。
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认证代码 (HMAC) 计算的密钥。

字段名称	使用指南
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。 指定输入思科 ISE 加密密钥时必须使用的格式，以便匹配无线 LAN 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。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，将文本字符串分配给网络设备。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。
停用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。点击**停用 (Retire)** 时，系统会显示一个消息框。点击**是 (Yes)** 或**否 (No)**。
剩余停用期 (Remaining Retired Period)	（只有当您在上述消息框选择**是**时才可用）在以下导航路径中显示指定的默认值：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。您可以更改默认值。 这允许您输入新的共享密钥，而且旧共享密钥将在指定天数中保持启用状态。

字段名称	使用指南
结束 (End)	（只有当您在上述消息框中选择**是**时才可用）结束停用期并终止旧共享密钥。
启用单连接模式 (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。点击以下选项之一的单选按钮： • **传统思科设备 (Legacy Cisco Devices)** • **TACACS 草案合规性单连接支持 (TACACS Draft Compliance Single Connect Support)**。 如果禁用此选项，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

网络设备导入设置

表 *12:* 网络设备导入设置

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。 使用相同格式的网络设备信息更新模板，并将其保存在本地。然后，使用编辑的模板将网络设备导入任何思科 ISE 部署。

字段名称	使用指南
文件	点击**选择文件 (Choose File)**，选择您可能最近创建的或以前从任何思科 ISE 部署导出的 CSV 文件。 您可以使用**导入 (Import)** 选项将包含新的和更新后的网络设备信息的网络设备导入其他思科 ISE 部署中。
Overwrite Existing Data with New Data	选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框可用您的导入文件中的设备取代现有网络设备。 如不选中此复选框，则导入文件中可用的新网络设备定义将添加到网络设备存储库。系统会忽略重复条目。
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。

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

您还可在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **全部组 (All Groups)** 窗口。

表 *13*:“网络设备组”*(Network Device Group)*窗口中的字段

字段名称	使用指南
名称	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。 网络设备组层次结构中最多可以有六个节点，包括根节点。每个网络设备组的名称最多可以包含 32 个字符。
说明	为根网络设备组或子网络设备组输入一段说明。

字段名称	使用指南
网络设备数	此列中显示网络组中的网络设备数量。

网络设备组导入设置

表 *14:* 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。 以相同格式的网络设备组信息更新模板，并将其保存于本地位置，以将网络设备组导入任何思科 ISE 部署中。
文件 (File)	点击 **选择文件 (Choose File)**，找到您要上传的 CSV 文件的位置。这可能是新创建的文件，也可能是之前从其他思科 ISE 部署导出的文件。 可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 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)	如果想要用您的导入文件中的设备组替换现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。 如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。
Stop Import on First Error	选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，可在导入期间遇到错误的第一个实例时停止导入。 如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。

网络设备配置文件设置

下表介绍了“网络设备配置文件”(Network Device Profiles) 窗口上的字段，您可以用其为特定供应商的一种网络设备配置默认设置，例如设备的协议支持、重定向 URL 和 CoA 设置。然后使用配置文件定义特定网络设备。

网络设备配置文件设置

下表列出“网络设备配置文件”(Network Device Profile) 部分的字段。

表 *15:* 网络设备配置文件设置

字段名称	说明
名称	输入网络设备配置文件的名称。
说明	输入网络设备配置文件的说明。
图标	选择要用于网络设备配置文件的图标。此图标将默认为您选择的供应商的图标。 您选择的图标必须是 16 x 16 PNG 文件。
供应商	选择网络设备配置文件的供应商。
支持的协议	
RADIUS	如果此网络设备配置文件支持 RADIUS，请选中此复选框。
TACACS+	如果此网络设备配置文件支持 TACACS+，请选中此复选框。
TrustSec	如果此网络设备配置文件支持 TrustSec，请选中此复选框。
RADIUS 字典	选择此配置文件支持的一个或多个 RADIUS 字典。在创建配置文件之前，请导入所有供应商特定 RADIUS 字典。

身份验证/授权模版设置

下表列出“身份验证/授权”(Authentication/Authorization) 部分的字段。

表 *16:* 身份验证/授权设置

字段名称	说明
流量类型条件 **(Flow Type Conditions)**	思科 ISE 支持 802.1X、MAC 身份验证绕行 (MAB) 和基于浏览器的 Web 身份验证登录，通过有线和无线网络为用户提供基本身份验证和访问。 对于此类型网络设备支持的身份验证登录选中此复选框。可以是下面的一项或多项： • 有线 MAC 身份验证绕行 (MAB) • 无线 MAB • 有线 802.1X • 无线 802.1X • 有线 Web 身份验证 • 无线 Web 身份验证 在查看网络设备配置文件支持的身份验证登录后，指定用于登录的条件。
属性别名 **(Attribute Aliasing)**	选中 SSID 复选框可将设备的服务集标识符 (SSID) 用作策略规则中的友好名称。这样您可创建一个在策略规则中使用的一致名称。
主机查找 **(MAB)**	
Process Host Lookup	选中此复选框可定义网络设备配置文件使用的主机查找的协议。 来自不同供应商的网络设备以不同的方式执行 MAB 身份验证。根据设备类型，为您使用的协议选中**检查密码 (Check Password)** 或检查**呼叫站 ID 等于 MAC 地址 (Checking Calling-Station-Id equals MAC Address)** 复选框。
通过 **PAP/ASCII (Via PAP/ASCII)**	选中此复选框可配置思科 ISE 检测作为主机查找请求的来自网络设备配置文件的 PAP 请求。
通过 **CHAP**	选中此复选框可配置思科 ISE 检测作为主机查找请求的来自网络设备配置文件这种请求类型。 此选项可启用 CHAP 身份验证。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。

字段名称	说明
通过 EAP-MD5 (Via EAP-MD5)	选中此复选框可启用用于网络设备配置文件的基于 EAP 的 MD5 散列身份验证。

权限

您可以定义用于此网络设备配置文件的 VLAN 和 ACL 权限。保存配置文件后，思科 ISE 为每个配置权限的授权配置文件自动生成授权配置文件。

表 *17:* 权限

字段名称	说明
设置 VLAN	选中此复选框可为此网络设备配置文件设置VLAN权限。选择以下其中一个选项： • IETF 802.1X 属性。这是一组由 Internet 工程工作小组定义的 RADIUS 默认属性。 • 唯一属性您可以指定多个 RADIUS 属性值对。
设置 ACL	选中此复选框可选择为网络设备配置文件上的 ACL 设置的 RADIUS 属性。

授权更改 (CoA) 模板设置

此模板定义如何将 CoA 发送至此类网络设备。下表列出“授权更改”(CoA) 部分的字段。

表 *18:* 授权更改 *(CoA)* 设置

字段名称	**Definition**
CoA 发送协议	选择以下选项之一： • RADIUS • SNMP • 不支持
通过 RADIUS 发送 CoA	
默认 CoA 端口	发送 RADIUS CoA 的端口。默认情况下，端口 1700 用于思科设备，端口 3799 用于非思科供应商的设备。 您可以在“网络设备”(Network Device) 窗口对此进行覆盖。

字段名称	Definition
超时间隔 (**Timeout Interval**)	思科 ISE 在发送 WLAN 后等待响应的秒数。
Retry Count	思科 ISE 在首次超时后尝试发送 CoA 的次数。
Disconnect	选择如何将断开请求发送至这些设备。 • **RFC 5176**：为标准会话终止选中此复选框并使端口准备好新会话，如 RFC 5176 中所定义。 • **端口退回 (Port Bounce)**：选中此复选框可终止会话并重新启动端口。 • **端口关闭 (Port Shutdown)**：选中此复选框可终止会话并关闭端口。
重新进行身份验证	选择如何发送重新进行身份验证请求至网络设备。当前仅思科设备支持此功能。 • **基本 (Basic)**：为标准会话重新进行身份验证选中此复选框。 • **重新运行 (Rerun)**：选中此复选框可从一开始运行身份验证方法。 • **上次 (Last)**：为会话使用上次成功的身份验证方式。
CoA 推送	如果网络设备不支持思科的 TrustSec CoA 功能，请选择此选项允许思科ISE推送配置更改至设备。
通过 SNMP 发送 CoA	
超时间隔	思科 ISE 在发送 WLAN 后等待响应的秒数。
Retry Count	思科 ISE 尝试发送 CoA 的次数。
NAD 端口检测	相关 RADIUS 属性是当前唯一选项。
相关 RADIUS 属性	选择如何检测 NAD 端口： • Nas-Port • NAS-Port-Id

字段名称	Definition
Disconnect	选择如何将断开请求发送至这些设备： • **重新验证 (Reauthenticate)**：选中此复选框可终止会话并重新启动端口。 • **端口退回 (Port Bounce)**：选中此复选框可终止会话并重新启动端口。 • **端口关闭 (Port Shutdown)**：选中此复选框可终止会话并关闭端口。

重定向模版设置

如果 HTTP 请求配置为授权配置文件的一部分，网络设备可重定向客户端的 HTTP 请求。此模板指定此网络设备配置文件是否支持 URL 重定向。您将使用指定给设备类型的 URL 参数名称。

下表列出“重定向”(Redirect) 部分的字段。

表 *19:* 重定向设置

字段名称	Definition
类型	选择网络设备配置文件是否支持静态或动态URL重定向。 如果设备两者都不支持，请选择**不支持 (Not Supported)** 并从**设置 (Settings)** > **DHCP & DNS 服务 (DHCP & DNS Services)** 设置 VLAN。
重定向 URL 参数名称 (Redirect URL Parameter Names)	
客户端 IP 地址	输入网络设备用于客户端的IP地址的参数名称。
客户端 MAC 地址 (Client MAC Address)	输入网络设备用于客户端MAC地址的参数名称。
Originating URL	输入网络设备用于原始 URL 的参数名称。
Session ID	输入网络设备用于会话 ID 的参数名称。
SSID	输入网络设备用于服务集标识符 (SSID) 的参数名称。
动态 URL 参数 (Dynamic URL Parameters)	
参数	当您选择使用动态URL用于重定向时，您需要指定这些网络设备如何创建重定向URL。您还可以指定重定向URL是否使用会话ID或客户端MAC地址。

高级设置

您可以使用网络设备配置文件生成大量策略要素以方便在策略规则中使用网络设备。这些元素包括复合条件、授权配置文件和允许协议。

点击**生成策略元素 (Generate Policy Elements)** 创建这些元素。

外部 RADIUS 服务器设置

表 *20:* 外部 *RADIUS* 服务器设置

字段名称	使用指南
名称	输入外部 RADIUS 服务器的名称。
说明	输入外部 RADIUS 服务器的说明。
Host IP	输入外部 RADIUS 服务器的 IP 地址。输入 IPv4 地址时，可以使用地址范围和子网掩码。IPv6 不支持地址范围。
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。
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 140-2 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。

字段名称	使用指南
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。
Accounting Port	输入 RADIUS 记账端口号。有效范围为 1 至 65535。默认值为 1813。
Server Timeout	输入思科 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。
RADIUS 代理故障转移到期	输入连接失败后到再次尝试连接此服务器之前经过的时间。有效范围为 1 到 600。 配置此参数可跳过服务器超时，直接进行故障转移。

RADIUS 服务器序列

表 *21: 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。
Description	输入可选的说明。
Host IP	输入外部 RADIUS 服务器的 IP 地址。

字段名称	使用指南
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，而且您使用的是思科 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思科 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。

字段名称	使用指南
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。

NAC 管理器设置

表 *22: 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。

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。

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。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale)**：使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 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。

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。
- 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
- 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。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。

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。

字段名称	使用指南
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。
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。

证书调配门户的门户设置

- **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。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定

NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

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

  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 IdP，请依次选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **SAML 身份提供程序 (SAML Id Providers)**。

  要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。
- **配置授权组 (Configure authorized groups)**：选择要为其授予权限以生成证书并将证书移至“已选”(Chosen) 框的用户身份组。
- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**：为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com,sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。

  如果更改默认 FQDN，还需执行以下操作：

  - 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在思科 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。如果为发起人门户启用了**允许 Kerberos SSO (Allow Kerberos SSO)** 选项，则必须在门户使用的本地服务器证书的 SAN 属性中包含思科 ISE PSN 的 FQDN 或通配符。
- **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。

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。
- **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。

可接受使用政策 (AUP) 页面设置

- **包含 AUP (Include an AUP)**：在单独的页面上向用户显示公司的网络使用条款和条件。
- **对员工使用不同的 AUP (Use Different AUP for Employees)**：仅为员工显示不同的 AUP 及网络使用条款和条件。如果您选择此选项，则不能同时选择**跳过面向员工的 AUP (Skip AUP for employees)**。
- **对员工跳过 AUP (Skip AUP for Employees)**：员工在访问网络之前无需接受 AUP。如果您选择此选项，则不能同时选择**使用面向员工的不同 AUP (Use different AUP for employees)**。
- **要求接受 (Require Acceptance)**：在完全启用用户的帐户之前要求用户接受 AUP。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
- **要求滚动至 AUP 末尾 (Require Scrolling to End of AUP)**：此选项仅在已启用**在页面上包含 AUP (Include an AUP on page)** 时显示。

  确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。配置何时向用户显示 AUP。

  - **仅首次登录时 (On First Login only)**：仅在用户首次登录网络或门户时显示 AUP。
  - **每次登录时 (On Every Login)**：每次用户登录网络或门户时都显示 AUP。
  - **每 __ 天（从首次登录算起）(Every __ Days [starting at first login])**：在用户首次登录网络或门户后定期显示 AUP。

客户端调配门户的门户设置

门户设置

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（**黑名单**门户除外，其端口值为 8444）。如果您已使用此范围外的端口值进行升级，则在对此页面进行任何更改之前会遵循这些设置。如果您对此页面进行任何更改，则必须更新端口设置以遵守此限制。
- **允许接口 (Allowed interfaces)**：选择可以运行门户的 PSN 接口。仅配备了允许接口的 PSN 可以创建门户。您可以配置物理接口和绑定接口的任意组合。这是整个 PSN 的配置；所有门户只能在这些接口上运行，这些接口配置被推送到所有节点。
  - 您必须使用不同子网上的 IP 地址配置以太网接口。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书主题名称/备用主题名称必须解析到接口 IP。
  - 在 ISE CLI 中配置 ip host x.x.x、x yyy.domain.com 以将辅助接口 IP 映射到 FQDN，FQDN 将用于匹配证书主题名称/备用主题名称。

- 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。它不会尝试在物理接口上启动门户。
- **NIC 结合 (NIC Teaming)** 或绑定是一个 O/S 配置选项，通过该选项可以配置两个独立的 NIC 以实现高可用性（容错能力）。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据门户设置配置为门户选定一个 NIC：
  - 如果物理 NIC 和相应的绑定 NIC 均已配置 - 当 PSN 尝试配置门户时会首先尝试连接到绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group Tag)**：选择要用于门户 HTTPS 流量的证书组的组标签。
- **身份验证方法 (Authentication Method)**：选择用于用户身份验证的身份源序列 (ISS) 或身份提供程序 (IdP)。ISS 是按顺序搜索验证用户凭证的身份库的列表。一些示例包括：内部访客用户、内部用户、Active Directory 和 LDAP 目录。

  思科 ISE 包含客户端调配门户的默认客户端调配身份源序列，Sponsor_Portal_Sequence。

- **完全限定域名 (Fully Qualified Domain Name [FQDN])**：为客户端调配门户输入至少一个唯一 FQDN 和/或主机名。例如，您可以输入 provisionportal.yourcompany.com，以便在用户将其中任一名称输入到浏览器中时，可以访问客户端调配门户。
  - 更新 DNS，以确保新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在思科 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。

  注释 对于没有 URL 重定向的客户端调配，必须在 DNS 配置中配置完全限定域名 (FQDN) 字段中输入的门户名称。此 URL 必须传达给用户，以在没有 URL 重定向的情况下启用客户端调配。

- **空闲超时 (Idle Timeout)**：输入思科 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。

注释 在客户端调配门户中，可以定义端口号和证书，以便主机允许您为客户端调配和终端安全评估下载相同的证书。如果门户证书由官方证书颁发机构签名，您将不会收到任何安全警告。如果证书是自签证书，您将收到门户和思科 AnyConnect 终端安全评估组件二者的同一安全警告。

登录页面设置

- 启用登录 (Enable Login)：选择此复选框可在客户端调配门户中启用登录步骤

- 速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)：指定在思科 ISE 开始人为减缓可进行登录尝试的速率（从而防止更多登录尝试）之前，单个浏览器会话的失败登录尝试次数。在 **Time between login attempts when rate limiting** 中指定了达到此失败登录次数后，前后两次尝试之间的间隔时间。
- 限制速率时登录尝试之间的间隔时间 (Time between login attempts when rate limiting)：设置用户在达到**速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting)** 中定义的登录失败次数后，尝试再次登录之前必须等待的时间长度（以分钟为单位）。
- 包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])：显示公司的网络使用条款和条件，可以是当前为用户显示的页面上的文本，或是一个链接，能够打开包含 AUP 文本的新选项卡或窗口。
- 要求接受 (Require acceptance)：要求用户必须接受 AUP，然后才能访问门户。除非用户接受 AUP，否则不会启用**登录 (Login)** 按钮。如果用户不接受 AUP，便无法访问该门户。
- 要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)：此选项仅在启用**在页面上包含一个 AUP (Include an AUP on page)** 时显示。确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。

可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)

- 包含一个 AUP (Include an AUP)：在单独的页面上向用户显示公司的网络使用条款和条件。
- 要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)：确保用户已完全阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活“接受”(Accept) 按钮。
- 仅在首次登录时 (On first login only)：仅在用户首次登录到网络或门户时显示 AUP。
- 在每次登录时 (On every login)：每次用户登录到网络或门户时都显示 AUP。
- 每 __ 天（从首次登录算起）(Every __ days [starting at first login])：在用户首次登录到网络或门户后定期显示 AUP。

登录后横幅页面设置

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

更改密码设置 (Change Password Settings)

允许内部用户更改其密码 (Allow internal users to change their own passwords)：允许内部用户在登录到客户端调配门户后更改其密码。这仅适用于帐户存储于思科 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。

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。

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。
  - 如果仅选择绑定 NIC，则当 PSN 尝试配置门户时，首先会尝试配置绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 记录错误并退出。PSN 不会尝试在物理接口上启动门户。
  - 若要配置两个单独的 NIC 以提供高可用性（容错），NIC 组合 (NIC Teaming) 或绑定是一种配置选择。如果其中一个 NIC 失败，属于绑定连接中一部分的另一个 NIC 会继续连接。根据**门户设置 (Portal Settings)** 配置，为门户选择一个 NIC。如果物理 NIC 和相应的绑定 NIC 均已配置，则当 PSN 尝试配置门户时，首先会尝试连接绑定接口。如果不成功，可能是因为 PSN 上没有绑定设置，然后 PSN 尝试在物理接口上启动门户。

- **证书组标签 (Certificate Group tag)**：选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。

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

  如果更改默认 FQDN，还需执行以下操作：

  - 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在思科 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。如果为发起人门户启用了**允许 Kerberos SSO (Allow Kerberos SSO)** 选项，则必须在门户使用的本地服务器证书的 SAN 属性中包含思科 ISE PSN 的 FQDN 或通配符。

- **身份验证方法 (Authentication Method)**：选择将哪个身份源序列或身份提供程序 (IdP) 用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

  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 IdP，请依次选择**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **SAML 身份提供程序 (SAML Id Providers)**。

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

- **终端身份组 (Endpoint Identity Group)**：选择用于跟踪访客设备的终端身份组。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。

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。

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。
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。

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。

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。

管理我的设备门户的设备设置

表 *23:* 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。
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**工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。
Stolen	使员工可以指示其设备已被盗。此操作会将“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。

字段名称	使用指南
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。

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。

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。

字段名称	使用指南
显示含默认值的标签 (Display Label with Default Value)	如果标签将会包含的信息不存在，请在**支持信息 (Support Information)** 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用”(Not Available)，并且故障代码未知，则**故障代码 (Failure Code)** 将显示**不可用 (Not Available)**。