# 安全有线接入



# 在思科 ISE 中定义网络设备

网络设备（如交换机或路由器）是一种向Cisco ISE 发送身份验证、授权和记账 (AAA) 服务请求所借助的 AAA 客户端。在Cisco ISE 中定义网络设备，以启用Cisco ISE 与网络设备之间的交互。

可以配置用于 RADIUS 或 TACACS AAA 的网络设备，以及用于分析服务的简单网络管理协议 (SNMP)，以收集Cisco发现协议和链路层发现协议 (LLDP) 属性进行终端分析，以及用于Cisco Trustsec 设备的 Trustsec 属性。未在Cisco ISE 中定义的网络设备无法收到Cisco ISE 的 AAA 服务。

在网络设备定义中：

- 选择适合网络设备的供应商配置文件。配置文件包括设备的预定义配置，如URL 重定向设置和授权变更。
- 配置用于 RADIUS 身份验证的 RADIUS 协议。当Cisco ISE 收到网络设备的 RADIUS 请求时，它会查找相应的设备定义以检索所配置的共享密钥。如果Cisco ISE 找到设备定义，它会获取在设备上配置的共享密钥并将其与请求中的共享密钥进行匹配，对访问权限进行身份验证。如果共享密钥匹配，RADIUS 服务器将进一步根据策略和配置处理该请求。如果共享密钥不匹配，系统会向网络设备发送拒绝响应。并生成一份未通过身份验证的报告，提供失败原因。
- 配置用于进行 TACACS+ 身份验证的 TACACS+ 协议。当Cisco ISE 收到网络设备的 TACACS+ 请求时，它会查找相应的设备定义以检索配置的共享密钥。如果Cisco ISE 找到设备定义，它会获取在设备上配置的共享密钥并将其与请求中的共享密钥进行匹配，对访问权限进行身份验证。如果共享密钥匹配，TACACS+ 服务器将进一步根据策略和配置处理该请求。如果共享密钥不匹配，系统会将拒绝响应发送到网络设备，并生成一份未通过身份验证的报告，提供失败原因。

- 可以在网络设备定义中配置用于分析服务的简单网络管理协议(SNMP)，以便与网络设备进行通信并对连接到网络设备的终端进行分析。
- 必须在Cisco ISE 中定义支持Cisco Trustsec 的设备才能处理来自这类设备的请求，支持 Trustsec 的设备可以是Cisco Trustsec 解决方案的一部分。任何支持Cisco Trustsec 解决方案的交换机都是支持Cisco TrustSec 的设备。

  Cisco Trustsec 设备不使用 IP 地址。相反，必须定义其他设置，以便Cisco Trustsec 设备可与Cisco ISE 通信。

  支持Cisco TrustSec 的设备使用 Trustsec 属性与Cisco ISE 通信。支持Cisco Trustsec 的设备（例如 Nexus 7000 系列交换机、Catalyst 6000 系列交换机、Catalyst 4000 系列交换机和 Catalyst 3000 系列交换机）使用您在添加Cisco Trustsec 设备时定义的 Trustsec 属性进行身份验证。

**注释** 在Cisco ISE 上配置网络设备时，我们建议不要在共享密钥中包含反斜线 (\)。这是因为，在升级Cisco ISE 时，反斜线不会出现在共享密钥中。但请注意，如果重新映像Cisco ISE 而不是对其进行升级，则共享密钥中会显示反斜线。

# 在思科 ISE 中定义默认网络设备

Cisco ISE 支持用于 RADIUS 和 TACACS 身份验证的默认设备定义。您可以定义Cisco ISE 在找不到特定 IP 地址的设备定义时可以使用的默认网络设备。此功能允许您为新调配的设备定义一个默认的 RADIUS 或 TACACS 共享密钥和访问权限级别。

**注释** 我们建议仅为基本 RADIUS 和 TACACS 身份验证添加默认设备定义。对于高级流程，您必须为每个网络设备添加单独的设备定义。

当Cisco ISE 从网络设备接收到 RADIUS 或 TACACS 请求时，Cisco ISE 会查找对应的设备定义，以检索网络设备定义中配置的共享密钥。

当Cisco ISE 收到 RADIUS 或 TACACS 请求时，它执行以下程序：

1. 查找与请求中的地址匹配的具体 IP 地址。
2. 查找范围以了解请求中的 IP 地址是否属于指定的范围。
3. 如果步骤 1 和 2 都失败了，它会使用默认设备定义（如已定义）处理请求。

Cisco ISE 会获取设备定义中为该设备配置的共享密钥并将其与 RADIUS 或 TACACS 请求中的共享密钥进行匹配以执行访问身份验证。如果找不到设备定义，Cisco ISE 会从默认网络设备定义中获取共享密钥并处理 RADIUS 或 TACACS 请求。

# 网络设备

您可以使用这些窗口在Cisco ISE 中添加和管理网络设备。

## 网络设备定义设置

下表介绍**网络设备 (Network Devices)** 窗口上的字段，您可以使用该窗口配置Cisco ISE 中的网络访问设备。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**，然后点击**添加 (Add)**。

### 网络设备设置

下表介绍**新网络设备 (New Network Devices)** 窗口中的字段。

**表 *1:* 网络设备设置**

| 字段名称 | 说明 |
|---|---|
| 名称 | 输入网络设备的名称。<br>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。<br>**注释** 配置设备名称后无法进行编辑。 |
| 说明 | 输入设备的说明。 |

| 字段名称 | 说明 |
| --- | --- |
| **IP** 地址或 **IP** 范围 | 从下拉列表中选择以下选项之一，并在显示的字段中输入所需的值：<br>• **IP** 地址：输入单个 IP 地址（IPv4 或 IPv6 地址）和子网掩码。<br>• **IP** 范围：输入所需的 IPv4 地址范围。要在身份验证期间排除 IP 地址，请在**排除 (Exclude)** 字段中输入 IP 地址或 IP 地址范围。<br>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：<br>• 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。<br>• 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。<br>• 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。<br>• 您不能使用相同的特定 IP 地址定义两台设备。<br>• 您不能使用同一 IP 地址范围定义两台设备。IP 地址范围不得部分或全部重叠。 |
| 设备配置文件 | 从下拉列表中选择网络设备的供应商。<br>使用下拉列表旁的工具提示可查看选定供应商的网络设备所支持的流和服务。工具提示还显示设备使用的 RADIUS CoA 端口和 URL 重定向类型。这些属性在设备类型的网络设备配置文件中进行定义。 |
| 型号名称 | 从下拉列表中选择设备型号。<br>在基于规则的策略中查找条件时，可以将型号名称用作其中一个参数。此属性存在于设备字典中。 |

| 字段名称 | 说明 |
| --- | --- |
| 软件版本 | 从下拉列表中选择在网络设备上运行的软件版本。<br>在基于规则的策略中查找条件时，您可以将软件版本用作其中一个参数。此属性存在于设备字典中。 |
| 网络设备组 | 在**网络设备组 (Network Device Group)** 区域中，从**位置 (Location)**、**IPSEC** 和**设备类型 (Device Type)** 下拉列表中选择所需的值。<br>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 *2:* “*RADIUS* 身份验证设置”*(RADIUS Authentication Settings)* 区域中的字段

| 字段名称 | 使用指南 |
| --- | --- |
| **RADIUS UDP 设置** | |
| 协议 | 显示 **RADIUS** 作为所选协议。 |
| 共享密钥 | 输入网络设备的共享密钥。<br>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。<br>注释 共享密钥长度必须等于或大于在**设备安全设置 (Device Security Settings)** 窗口（**管理 [Administration] > 网络资源 [Network Resources] > 网络设备 (Network Devices) > 设备安全设置 [Device Security Settings]**）的 **RADIUS 共享密钥最小长度 (Minimum RADIUS Shared Secret Length)** 字段中配置的值。<br>对于 RADIUS 服务器，长度最好为 22 个字符。对于新安装和升级的部署，默认情况下，共享密钥长度为四个字符。您可以在**设备安全设置 (Device Security Settings)** 窗口中更改此值。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 使用第二个共享密钥 | 指定网络设备和Cisco ISE 要使用的第二个共享密钥。<br>注释 虽然Cisco TrustSec 设备可以利用双重共享密钥（密钥），但Cisco ISE 发送的Cisco TrustSec CoA 数据包将始终使用第一个共享密钥（密钥）。要启用第二个共享密钥，请选择必须从哪一个 Cisco ISE 节点向 TrustSec 设备发送 Cisco TrustSec CoA 数据包。在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **高级 TrustSec 设置 (Advanced TrustSec Settings)** 窗口的**发送自 (Send From)** 下拉列表中，配置要用于此任务的Cisco ISE 节点。您可以选择主管理节点 (PAN) 或策略服务节点 (PSN)。如果所选 PSN 节点关闭，PAN 将向Cisco TrustSec 设备发送Cisco TrustSec CoA 数据包。<br>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。<br>设备的默认CoA端口在为网络设备配置的网络设备配置文件中进行定义（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Device Profiles)**）。点击**设置为默认 (Set To Default)** 按钮以使用默认 CoA 端口。<br>注释 如果修改在 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 下的**网络设备 (Network Devices)** 窗口（**管理 [Administration]** > **网络资源 [Network Resources]** > **网络设备 [Network Devices]**）中指定的 CoA 端口，请确保在**网络设备配置文件 (Network Device Profile)** 窗口（**管理 [Administration]** > **网络资源 [Network Resources]** > **网络设备配置文件 [Network Device Profiles]**）中为相应配置文件指定相同的 CoA 端口。 |
| **RADIUS DTLS 设置** | |
| **需要 DTLS** | 如果选中**需要 DTLS (DTLS Required)** 复选框，则Cisco ISE 仅处理来自此设备的 DTLS 请求。如果禁用此选项，则Cisco ISE 会同时处理来自此设备的 UDP 和 DTLS 请求。<br>RADIUS DTLS 为安全套接字层 (SSL) 隧道建立和 RADIUS 通信提供了更高的安全性。 |
| **共享密钥** | 显示用于 RADIUS DTLS 的共享密钥。此值为固定值，用于计算消息摘要 5 (MD5) 完整性检查。 |
| **CoA 端口** | 指定用于 RADIUS DTLS CoA 的端口。 |
| **CoA ISE 证书 CA 颁发者** | 从下拉列表中选择要用于 RADIUS DTLS CoA 的证书颁发机构。 |

| 字段名称 | 使用指南 |
| --- | --- |
| **DNS 名称** | 输入网络设备的 DNS 名称。如果在 **RADIUS 设置 (RADIUS Settings)** 窗口下启用**启用 RADIUS/DTLS客户端身份验证选项**（**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **RADIUS**，Cisco ISE会将此DNS名称与客户端证书中指定的DNS名称进行比较，以验证网络设备的身份。 |
| 常规设置 | |
| 启用 **KeyWrap** | 仅当网络设备支持 KeyWrap 算法时，选中**启用 KeyWrap (Enable KeyWrap)** 复选框。此选项用于通过 AES KeyWrap 算法提高 RADIUS 安全性。<br>注释　当在 FIPS 模式下运行思科 ISE 时，必须在网络设备上启用 KeyWrap。 |
| 密钥加密密钥 | 输入用于会话加密（保密）的加密密钥。 |
| 消息身份验证器代码密钥 | 输入用于 RADIUS 消息键控散列消息验证码 (HMAC) 计算的密钥。 |
| 密钥输入格式 | 点击以下格式之一对应的单选按钮：<br>• **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）。<br>• **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）。<br>指定想要用于输入Cisco ISE FIPS 加密密钥的密钥输入格式，从而使其与无线 LAN 控制器上的配置一致。您指定的值必须是密钥的正确（完整）长度，不允许使用短于此长度的值。 |

### TACACS 身份验证设置

表 *3: TACACS* 身份验证设置区域中的字段

| 字段名称 | 使用指南 |
| --- | --- |
| 共享密钥 | 当启用 TACACS+ 协议时，会向网络设备分配文本字符串。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。 |
| 停用的共享密钥处于启用状态 | 当停用期处于启用状态时显示。 |
| 淘汰 | 停用现有的共享密钥而不是结束它。点击**停用 (Retire)** 时，系统会显示一个消息框。您可以点击**是 (Yes)** 或**否 (No)**。 |
| 剩余停用期 | （仅当在**停用 (Retire)** 消息框中选择**是 (Yes)** 时可用）显示在以下导航路径中指定的默认值：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。您可以更改默认值。<br>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：<br>• **传统思科设备 (Legacy Cisco Devices)**<br>• **TACACS 草案合规性单连接支持**<br>如果禁用**单连接模式 (Single Connect Mode)**，Cisco ISE 会对每个 TACACS 请求使用新的 TCP 连接。 |

### SNMP 设置

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

表 *4: SNMP* 设置区域中的字段

| 字段名称 | 使用指南 |
| --- | --- |
| **SNMP 版本** | 从 **SNMP (SNMP 版本)** 下拉列表中，选择以下选项之一：<br>• **1**：SNMPv1 不支持通知。<br>• **2c**<br>• **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。<br>注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的**网络设备会话状态 (Network Device Session Status)** 摘要报告（**操作 [Operations]** > **报告 [Reports]** > **诊断 [Diagnostics]** > **网络设备会话状态 [Network Device Session Status]**）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。 |
| **SNMP 只读社区** | （仅适用于 SNMP 版本 1 和 2c）输入只读社区字符串，为Cisco ISE 提供特殊类型的设备访问权限。<br>注释 不允许使用插入符号 (circumflex ^)。 |
| **SNMP 用户名** | （仅适用于 SNMP 版本 3）输入 SNMP 用户名。 |
| **安全级别** | （仅适用于 SNMP 版本 3）从**安全级别 (Security Level)** 下拉列表中选择以下选项之一：<br>• **身份验证 (Auth)**：启用 MD5 或安全散列算法 (SHA) 数据包身份验证。<br>• **无身份验证 (No Auth)**：无身份验证，无隐私安全级别。<br>• **隐私 (Priv)**：启用数据加密标准 (DES) 数据包加密。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 身份验证协议 | （选择安全级别**身份验证 [Auth]** 和**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）从**身份验证协议 (Auth Protocol)** 下拉列表中，选择希望网络设备使用的身份验证协议。<br>• **MD5**<br>• **SHA** |
| 身份验证密码 | （选择安全级别**身份验证 [Auth]** 和**隐私 [Priv]** 时，仅适用于SNMP版本3）输入身份验证密钥。密码的长度应至少为 8 个字符。<br>点击**显示 (Show)**，显示已为设备配置的身份验证密码。<br>**注释** 不能使用插入符号 (circumflex ^)。 |
| 隐私协议 | （选择安全级别**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）从**隐私协议 (Privacy Protocol)** 下拉列表中，选择以下选项之一：<br>• **DES**<br>• **AES128**<br>• **AES192**<br>• **AES256**<br>• **3DES** |
| 隐私密码 | （选择安全级别**隐私 [Priv]** 时，仅适用于 SNMP 版本 3）输入隐私密钥。<br>点击**显示 (Show)**，显示已为设备配置的隐私密码。<br>**注释** 不能使用插入符号 (circumflex ^)。 |
| 轮询间隔 | 输入轮询间隔（秒）。默认值为 3600 秒。 |
| 链路陷阱查询 | 选中**链路陷阱查询 (Link Trap Query)** 复选框，可接收和解析通过SNMP陷阱接收的链路接通和链路断开通知。 |
| **MAC** 陷阱查询 | 选中**链路陷阱查询 (Link Trap Query)** 复选框，可接收和解析通过 SNMP 陷阱接收的 MAC 通知。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 原始策略服务节点 | 从**原始策略服务节点 (Originating Policy Services Node)** 下拉列表中，选择要用于轮询 SNMP 数据的Cisco ISE 服务器。此字段的默认值为**自动 (Auto)**。从下拉列表中选择特定值以覆盖设置。 |

### 高级 Trustsec 设置

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

表 *5:* 高级 *TrustSec* 设置区域中的字段

| 字段名称 | 使用指南 |
| --- | --- |
| **设备身份验证设置** | |
| **将设备 ID 用于 Trustsec 标识** | 如果希望在**设备 ID (Device ID)** 字段中将设备名称作为设备标识符列出，请选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框。 |
| **设备 ID** | 仅当未选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框时，才能在此字段中输入设备 ID。 |
| **密码** | 输入在Cisco TrustSec 设备 CLI 中配置的密码，用于对Cisco TrustSec 设备进行身份验证。<br>点击**显示 (Show)** 可显示密码。 |
| **HTTP REST API 设置** | |
| **启用 HTTP REST API (Enable HTTP REST API)** | 选中**启用 HTTP REST API (Enable HTTP REST API)** 复选框以使用 HTTP REST API 向网络设备提供所需的Cisco TrustSec 信息。与 RADIUS 协议相比，这提高了在短时间内下载大型配置的效率和能力。它还通过使用 TCP over UDP 提高了可靠性。 |
| **用户名** | 输入在Cisco TrustSec 设备 CLI 中配置的用户名，用于对Cisco TrustSec 设备进行身份验证。用户名不能包含特殊字符，如空格 ! % ^ : ; , [ { \| } ] ` " = < > ? |
| **密码** | 输入在Cisco TrustSec 设备 CLI 中配置的密码，用于对Cisco TrustSec 设备进行身份验证。 |
| **Trustsec 设备通知和更新** | |

| 字段名称 | 使用指南 |
| --- | --- |
| **设备 ID** | 仅当未选中**将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)** 复选框时，才能在此字段中输入设备 ID。 |
| 密码 | 输入在Cisco TrustSec 设备 CLI 中配置的密码，用于对Cisco TrustSec 设备进行身份验证。<br>点击**显示 (Show)** 可显示密码。 |
| **每<...> 下载一次环境数据 (Download Environment Data Every <...>)** | 通过从此区域的下拉列表中选择所需的值，指定设备从Cisco ISE 下载其环境数据时必须遵守的时间间隔。您可以选择秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。 |
| **每 <...>下载一次对等授权策略 (Download Peer Authorization Policy Every <...>)** | 通过从此区域的下拉列表中选择所需的值，指定设备从Cisco ISE 下载对等授权策略时必须遵守的时间间隔。您可以指定单位为秒、分钟、小时、天或周的时间间隔。默认值为一天。 |
| **每 <...>重新进行身份验证 (Reauthentication Every <...>)** | 通过从此区域的下拉列表中选择所需的值，指定在初始身份验证后设备对照Cisco ISE 重新进行身份验证的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。例如，如果输入 1000 秒，则设备会每 1000 秒对照Cisco ISE 对自身重新进行身份验证。默认值为一天。 |
| **每 <...>下载 SGACL 列表 (Download SGACL Lists Every <...>)** | 通过从此区域的下拉列表中选择所需的值，指定设备从Cisco ISE 下载 SGACL 列表时遵守的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。 |
| 其他 **TrustSec** 设备信任该设备（**Trustsec** 信任） | 选中**其他 TrustSec 设备信任该设备 (Other TrustSec Devices to Trust This Device)** 复选框，可允许所有对等设备信任此Cisco TrustSec 设备。如果取消选中此复选框，则对等设备不信任此设备，所有从此设备到达的数据包都会相应地标注颜色或进行标记。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 将配置更改发送到设备 | 如果希望Cisco ISE 使用 CoA 或 CLI (SSH) 将Cisco TrustSec 配置更改发送到Cisco TrustSec 设备，请选中**将配置更改发送到设备 (Send Configuration Changes to Device)** 复选框。根据需要，点击 **CoA** 或 **CLI (SSH)** 的单选按钮。<br>如果希望Cisco ISE 使用 CoA 将配置更改发送到 Cisco TrustSec 设备，请选择 **CoA** 选项。<br>如果希望Cisco ISE 使用 CLI（使用 SSH 连接）将配置更改发送到Cisco TrustSec 设备，请选择 **CLI (SSH)** 选项。有关详细信息，请参阅向不支持 CoA 的设备推送配置更改。 |
| 发送自 | 从下拉列表中选择必须从哪一个Cisco ISE 节点将配置更改发送到Cisco TrustSec 设备。您可以选择 PAN 或 PSN 节点。如果所选择的 PSN 节点关闭，则使用 PAN 将配置更改发送到Cisco TrustSec 设备。 |
| 测试连接 | 您可以使用此选项测试Cisco TrustSec 设备与所选 Cisco ISE 节点（PAN 或 PSN）之间的连接。 |
| **SSH 密钥** | 要使用此功能，请打开从Cisco ISE 到网络设备的 SSHv2 隧道，然后使用设备的 CLI 检索 SSH 密钥。您必须复制此密钥并将其粘贴到 **SSH 密钥 (SSH Key)** 字段中以进行验证。有关详细信息，请参阅《》中的“ SSH 密钥验证”部分请参阅 SSH 密钥验证。 |
| 设备配置部署设置 | |
| 当部署安全组标签映射更新时纳入该设备 | 如果希望Cisco TrustSec 设备使用设备接口凭据获取 IP-SGT 映射，请选中**当部署安全组标记映射更新时包含此设备 (Include this device when deploying Security Group Tag Mapping Updates)** 复选框。 |
| **EXEC 模式用户名** | 输入用于登录Cisco TrustSec 设备的用户名。 |
| **EXEC 模式密码** | 输入设备密码。<br>点击**显示 (Show)** 可查看密码。 |
| 启用模式密码 | （可选）输入用于在特权模式下编辑Cisco TrustSec 设备配置的启用密码。<br>点击**显示 (Show)** 可查看密码。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 带外 **Trustsec PAC** | |
| 颁发日期 | 显示Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发日期。 |
| 到期日期 | 显示Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的到期日期。 |
| 颁发者 | 显示Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发者（Cisco TrustSec 管理员）名称。 |
| 生成 **PAC** | 点击**生成 PAC (Generate PAC)** 按钮，为Cisco TrustSec 设备生成带外Cisco TrustSec PAC。 |

相关主题

在思科 ISE 中定义网络设备，第 1 页
思科 ISE 中的第三方网络设备支持，第 22 页
网络设备组，第 30 页
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，第 26 页

## 默认网络设备定义设置

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

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

表 *6:* “默认网络设备”*(Default Network Device)* 窗口中的字段

| 字段名称 | 使用指南 |
| --- | --- |
| 默认网络设备状态 | 从**默认网络设备状态 (Default Network Device Status)** 下拉列表中选择**启用 (Enable)**，以启用默认网络设备定义。<br>注释 如果默认设备已启用，则必须通过选中窗口中的复选框启用 RADIUS 或 TACACS+ 身份验证设置。 |
| 设备配置文件 | 显示**思科 (Cisco)** 为默认的设备供应商。 |

| 字段名称 | 使用指南 |
| --- | --- |
| **RADIUS 身份验证设置** | |
| 启用 **RADIUS** | 选中**启用 RADIUS (Enable RADIUS)** 复选框，启用设备的 RADIUS 身份验证。 |
| **RADIUS UDP 设置** | |
| 共享密钥 | 输入共享密钥。共享密钥最大长度为 127 个字符。<br>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。<br>注释 共享密钥长度必须等于或大于在**设备安全设置 (Device Security Settings)** 窗口的 **RADIUS 共享密钥最小长度 (Minimum RADIUS Shared Secret Length)** 字段中配置的值（**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **设备安全设置 (Device Security Settings)**）。默认情况下，对于新安装和升级的部署，此值为 4 个字符。对于 RADIUS 服务器，长度最好为 22 个字符。 |
| **RADIUS DTLS 设置** | |
| 需要 **DTLS** | 如果选中**需要 DTLS (DTLS Required)** 复选框，则Cisco ISE 仅处理来自此设备的 DTLS 请求。如果禁用此选项，则Cisco ISE 会同时处理来自此设备的 UDP 和 DTLS 请求。<br>RADIUS DTLS 为 SSL 隧道建立和 RADIUS 通信提供了更高的安全性。 |
| 共享密钥 | 显示用于 RADIUS DTLS 的共享密钥。此值为固定值，用于计算 MD5 完整性检查。 |
| **CoA ISE 证书 CA 颁发者** | 从 **CoA ISE 证书 CA 颁发者 (Issuer CA of ISE Certificates for CoA)** 下拉列表中，选择要用于 RADIUS DTLS CoA 的证书颁发机构。 |
| 常规设置 | |

| 字段名称 | 使用指南 |
| --- | --- |
| 启用 **KeyWrap** | 仅在网络设备支持 KeyWrap 算法时选中**启用 KeyWrap (Enable KeyWrap)** 复选框，这可以通过 AES KeyWrap 算法提高 RADIUS 安全性。 |
| 密钥加密密钥 | 启用 KeyWrap 时，输入用于会话加密（保密）的加密密钥。 |
| 消息身份验证器代码密钥 | 启用 KeyWrap 时，输入对 RADIUS 消息进行键控散列消息身份认证代码 (HMAC) 计算的密钥。 |
| 密钥输入格式 | 通过点击相应的单选按钮选择以下格式之一，并在**密钥加密密钥 (Key Encryption Key)** 和**消息身份验证器代码密钥 (Message Authenticator Code Key)** 字段中输入值：<br>• **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）。<br>• **十六进制 (Hexadecimal)**：**密钥加密密钥 (Key Encryption Key)** 长度必须为 32 个字节，而**消息身份验证器代码密钥 (Message Authenticator Code Key)** 长度必须为 40 个字节。 |
| **TACACS 身份验证设置** | |
| 共享密钥 | 当 TACACS+ 协议启用时，将文本字符串分配给网络设备。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。 |
| 停用的共享密钥处于启用状态 | 当停用期处于启用状态时显示。 |
| 淘汰 | 停用现有的共享密钥而不是结束它。点击**停用 (Retire)** 时，系统会显示一个消息框。点击**是 (Yes)** 或**否 (No)**。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 剩余停用期 | （仅当在上述消息框中选择**是 (Yes)** 时可用）显示在以下导航路径中指定的默认值： **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。 您可以更改默认值。<br>这允许您输入新的共享密钥，而且旧共享密钥将在指定天数中保持启用状态。 |
| 结束 | （只有当您在上述消息框中选择**是**时才可用）结束停用期并终止旧共享密钥。 |
| 启用单连接模式 | 选中**启用单连接模式 (Enable Single Connect Mode)** 复选框，将单一 TCP 连接用于与网络设备之间的所有 TACACS+ 通信。点击以下选项之一的单选按钮：<br>• **传统思科设备 (Legacy Cisco Devices)**<br>• **TACACS 草案合规性单连接支持 (TACACS Draft Compliance Single Connect Support)**。<br>如果禁用此选项，Cisco ISE 会为每个 TACACS+ 请求使用新的 TCP 连接。 |

## 网络设备导入设置

下表介绍 Network Device Import 页面上的字段，您可以使用此页面将网络设备详细信息导入Cisco ISE。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。

**表 *7:* 网络设备导入设置**

| 字段名称 | 使用指南 |
| --- | --- |
| 生成模板 | 点击**创建模板 (Generate a Template)** 可创建逗号分隔值 (CSV) 模板文件。<br>使用相同格式的网络设备信息更新模板，并将其保存在本地。然后，使用编辑的模板将网络设备导入任何Cisco ISE 部署。 |

| 字段名称 | 使用指南 |
| --- | --- |
| 文件 | 点击**选择文件 (Choose File)**，选择您可能最近创建的或以前从任何Cisco ISE 部署导出的 CSV 文件。<br>您可以使用**导入 (Import)** 选项将包含新的和更新后的网络设备信息的网络设备导入其他Cisco ISE 部署中。 |
| 用新数据覆盖现有数据 | 选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框可用您的导入文件中的设备取代现有网络设备。<br>如不选中此复选框，则导入文件中可用的新网络设备定义将添加到网络设备存储库。系统会忽略重复条目。 |
| 遇到第一个错误时停止导入 | 如果您希望Cisco ISE 在导入过程中遇到错误时停止导入，请选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。Cisco ISE 会导入网络设备，直至出现错误。<br>如未选中此复选框并且遇到错误，系统会报错并且Cisco ISE 会继续导入剩余设备。 |

相关主题

在思科 ISE 中定义网络设备，第 1 页
思科 ISE 中的第三方网络设备支持，第 22 页
将网络设备导入思科 ISE，第 20 页

# 在思科 ISE 中添加网络设备

您可以在Cisco ISE 中添加网络设备或使用默认网络设备。

您还可以在**网络设备 (Network Devices)** 窗口（**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）中添加网络设备。

### 开始之前

必须在要添加的网络设备上启用 AAA 功能。请参阅启用 AAA 功能的命令。

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

**步骤 2** 点击**添加 (Add)**。

**步骤 3** 在**名称 (Name)**、**说明** 和 **IP 地址 (IP Address)** 字段中输入相应的值。

**步骤 4** 从**设备配置文件 (Device Profile)**、**型号名称 (Model Name)**、**软件版本 (Software Version)** 和**网络设备组 (Network Device Group)** 字段的下拉列表中选择所需的值。

**步骤 5** （可选）选中 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 复选框以配置用于身份验证的 RADIUS 协议。

**步骤 6** （可选）选中 **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框以配置用于身份验证的 TACACS 协议。

**步骤 7** （可选）选中 **SNMP 设置 (SNMP Settings)** 复选框以为Cisco ISE 分析服务配置 SNMP，以便从设备收集信息。

**步骤 8** （可选）选中**高级 Trustsec 设置 (Advanced Trustsec Settings)** 复选框以配置启用Cisco Trustsec 的设备。

**步骤 9** 点击**提交 (Submit)**。

# 将网络设备导入思科 ISE

要使Cisco ISE 能够与网络设备通信，您必须在Cisco ISE 中添加网络设备的设备定义。通过**网络设备 (Network Devices)** 窗口将网络设备的设备定义导入Cisco ISE（从主菜单中，选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**）。

使用逗号分隔值 (CSV) 文件，将设备定义列表导入到Cisco ISE 节点中。当您在**网络设备 (Network Devices)** 窗口中点击**导入 (Import)** 时，CSV 模板文件可用。下载此文件，输入所需的设备定义，然后通过**导入 (Import)** 窗口上传编辑的文件。

您不能同时运行同一资源类型的多项导入。例如，不能同时从两个不同的导入文件导入网络设备。

导入设备定义的 CSV 文件时，您可以通过点击**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 选项创建新记录或更新现有记录。

每个Cisco ISE 中的模板导入可能有所不同。请勿导入从其他Cisco ISE 版本导出的网络设备的 CSV 文件。在您的版本的 CSV 模板文件中输入网络设备的详细信息，然后将此文件导入Cisco ISE。

**注释** 您可以导入 IP 地址在所有八位组的范围内的网络设备。

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

**步骤 2** 点击**导入**。

**步骤 3** 在显示的**导入网络设备 (Import Network Devices)** 窗口中，点击**生成模板 (Generate A Template)** 下载一个 CSV 文件，您可以编辑它，填好所需的详细信息后导入Cisco ISE。

**步骤 4** 点击**选择文件 (Choose File)**，从正在运行客户端浏览器的系统中选择该 CSV 文件。

**步骤 5** （可选）根据需要，选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 和**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。

**步骤 6** 点击**导入**。

文件导入完成后，Cisco ISE 会显示摘要消息。摘要消息包括导入状态（成功或不成功）、遇到的错误数（如果有）以及文件导入过程所需的总处理时间。

# 从思科 ISE 导出网络设备

您可以用 CSV 文件的形式导出Cisco ISE 节点中可用的网络设备的设备定义。然后，您可以将此 CSV 文件导入另一个Cisco ISE 节点，以便设备定义可用于所需的Cisco ISE 节点。

注释 您可以导出 IP 地址在所有八位组中的网络设备。

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

**步骤 2** 点击**导出**。

**步骤 3** 通过执行以下操作之一，导出添加到Cisco ISE 节点的网络设备的设备定义。

- 选中要导出的设备旁边的复选框，点击**导出 (Export)**，然后从下拉列表中选择**导出所选 (Export Selected)**。
- 点击**导出 (Export)** 并从下拉列表中选择**全部导出 (Export All)**，以便导出添加到Cisco ISE 节点的所有网络设备。

**步骤 4** 在这两种情况下，设备定义 CSV 文件都会下载到您的系统。

# 解决网络设备配置问题

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **评估配置验证器 (Evaluate Configuration Validator)**。

**步骤 2** 在**网络设备 IP (Network Device IP)** 字段中输入您想要评估其配置的网络设备的 IP 地址。

**步骤 3** 选中相应复选框，然后点击要与建议模板进行比较的配置选项旁边的单选按钮。

**步骤 4** 点击**运行 (Run)**。

**步骤 5** 在显示的**进度详细信息... (Progress Details...)** 区域中，点击**点击此处输入凭证 (Click Here to Enter Credentials)**。在显示的**凭证窗口 (Credentials Window)** 对话框中，输入与网络设备建立连接所需的连接参数和凭证，然后点击**提交 (Submit)**。

要取消工作流程，请在**进度详细信息... (Progress Details...)** 窗口中点击**点击此处取消正在运行的工作流程 (Click Here to Cancel the Running Workflow)**。

**步骤 6** 选中想要分析的接口旁边的复选框，然后点击**提交 (Submit)**。

**步骤 7** 点击**显示结果摘要 (Show Results Summary)** 以查看配置评估的详细信息。

# 执行网络设备命令诊断工具

执行网络设备命令诊断工具允许您在任何网络设备上运行 **show** 命令。

显示的结果与您应在控制台上看到的结果相同。通过此工具，您可以发现设备配置中的任何问题。

使用此工具可验证任何网络设备的配置，也可以使用此工具了解网络设备的配置方式。

要访问执行网络设备命令诊断工具，请选择以下导航路径之一：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **执行网络设备命令 (Execute Network Device Command)**。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **解析器 (Profiler)** > **故障排除 (Troubleshoot)** > **执行网络设备命令 (Execute Network Device Command)**。

在显示的**执行网络设备命令 (Execute Network Device Command)** 窗口中，在相应字段中输入网络设备的 IP 地址和您想要运行的 show 命令。点击**运行 (Run)**。

# 思科 ISE 中的第三方网络设备支持

Cisco ISE 通过使用网络设备配置文件，支持第三方网络访问设备 (NAD)。不管供应商端实施如何，NAD 配置文件都使用简化的策略配置定义第三方设备的功能。网络设备配置文件包含以下内容：

- 该网络设备支持的协议，例如 RADIUS、TACACS+ 和Cisco TrustSec。可以将任何有关该网络设备的供应商特定的 RADIUS 字典导入到Cisco ISE 中。
- 该设备用于各种身份验证流程的属性和值，例如有线 MAB 和 802.1x。通过这些属性和值，Cisco ISE 可以根据网络设备使用的属性为您的设备检测正确的身份验证流程。
- 网络设备具有的授权更改 (CoA) 功能。虽然 RADIUS 协议 RFC 5176 定义了 CoA 请求，但 CoA 请求中使用的属性因网络设备而异。大多数支持 RFC 5176 的非Cisco设备都会支持“推送”和“断开连接”功能。对于不支持 RADIUS CoA 类型的设备，Cisco ISE 还支持 SNMP CoA。
- 网络设备针对 MAB 流程使用的属性和协议。不同供应商的网络设备采用不同方式执行 MAB 身份验证。
- 设备使用的 VLAN 和 ACL 权限。保存配置文件后，Cisco ISE 为每个配置的权限自动生成授权配置文件。
- URL 重定向技术信息。对于高级流程（如自带设备 (BYOD)、访客访问和终端安全评估服务），URL 重定向是必需的。在网络设备上有两种类型的 URL 重定向：静态和动态。对于静态 URL 重定向，可以复制Cisco ISE 门户 URL 并将其粘贴到配置中。对于动态 URL 重定向，Cisco ISE 会通过 RADIUS 属性告诉网络设备应重定向至哪个地址。

如果网络设备既不支持动态 URL 重定向，也不支持静态 URL 重定向，则Cisco ISE 提供身份验证 VLAN 配置，用于模拟 URL 重定向。身份验证 VLAN 配置基于Cisco ISE 中运行的 DHCP 和 DNS 服务。要创建身份验证 VLAN 配置，请定义 DHCP 和 DNS 服务设置。有关详细信息，请参阅 DHCP 和 DNS 服务。

在Cisco ISE 中定义网络设备后，配置这些设备配置文件或使用Cisco ISE 提供的预配置设备配置文件，以定义Cisco ISE用于启用基本身份验证流程以及高级流程（如分析器、访客、BYOD、MAB 和终端安全评估）的功能。

### URL 重定向机制和身份验证 VLAN

在网络中使用第三方设备且该设备不支持动态或静态URL重定向时，ISE将模拟URL重定向流程。通过在Cisco ISE 上运行 DHCP 或 DNS 服务来运行此类设备的 URL 重定向模拟流程。

有关详细信息，请参阅 DHCP 和 DNS 服务。

以下是身份验证 VLAN 流程的示例：

1. 访客终端连接到 NAD。
2. 网络设备将 RADIUS 或 MAB 请求发送至Cisco ISE。
3. Cisco ISE 运行已配置的身份验证和授权策略，并存储用户帐户信息。
4. Cisco ISE 发送 RADIUS 访问-接受消息，其中包含身份验证 VLAN ID。
5. 访客终端接收网络访问。
6. 终端广播 DHCP 请求，并从Cisco ISE DHCP 服务获取客户端 IP 地址和Cisco ISE DNS sinkhole IP 地址。
7. 访客终端打开浏览器，从中发送 DNS 查询并接收Cisco ISE IP 地址。
8. 终端 HTTP 和 HTTPS 请求定向到Cisco ISE。
9. Cisco ISE 使用“HTTP 301 已移动”(HTTP 301 Moved) 消息进行响应并提供访客门户 URL。终端浏览器重定向到访客门户窗口。
10. 访客终端用户登录以进行身份验证。
11. Cisco ISE 验证终端合规性，然后响应 NAD。Cisco ISE 发送 CoA，授权终端并绕过 sinkhole。
12. 访客用户基于 CoA 获得适当访问权限，终端从企业 DHCP 接收 IP 地址。访客用户现在即可使用网络。

可以使身份验证 VLAN 独立于企业网络，以防止访客终端在通过身份验证之前进行未经授权的网络访问。将身份验证 VLAN IP 助手配置为指向Cisco ISE 计算机，或将一个Cisco ISE 网络接口连接到身份验证 VLAN。

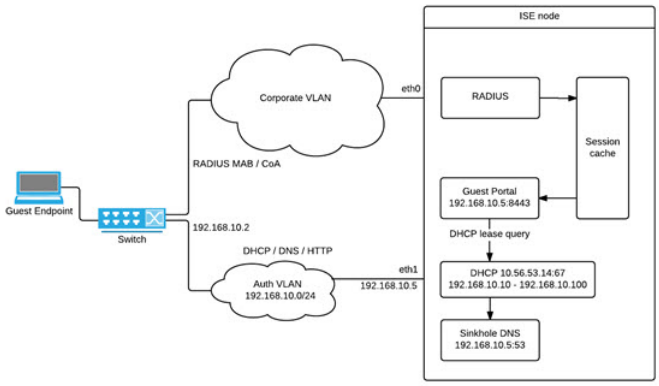
有关VLAN（DHCP和要创建身份验证VLAN配置）设置的详细信息，请参阅DHCP和DNS服务。

通过从 NAD 配置中配置 VLAN IP 助手可以将多个 VLAN 连接到一个网络接口卡。有关配置 IP 助手的详细信息，请参阅网络设备的管理指南说明。对于包含具有IP助手的VLAN的访客访问流程，

请定义访客门户，并在绑定到MAB授权的授权配置文件中选择此门户。有关访客门户的详细信息，请参阅思科 ISE 访客服务。

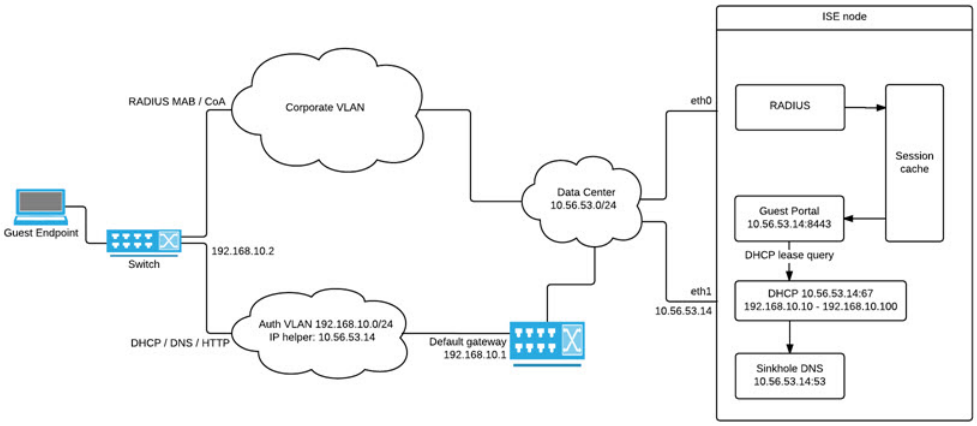
下图显示了定义身份验证VLAN时的基本网络设置（身份验证VLAN直接连接到Cisco ISE节点）。

**图 *1:* 连接到思科 *ISE* 节点的身份验证 *VLAN***




下图显示了带有身份验证 VLAN 和 IP 助手的网络：

**图 *2:* 配置有 *IP* 助手的身份验证 *VLAN***




## CoA 类型

Cisco ISE 同时支持 RADIUS 和 SNMP CoA 类型。必须支持 RADIUS 或 SNMP CoA 类型，NAD 才能在复杂流程中工作，而这对于基本流程不是强制性的。

在从Cisco ISE 中配置 NAD 时定义网络设备支持的 RADIUS 和 SNMP 设置，并在配置 NAD 配置文件时指出要用于特定流程的CoA类型。有关为NAD定义协议的详细信息，请参阅网络设备。在Cisco ISE 中创建设备和 NAD 配置文件之前，请与您的第三方供应商联系，以确认您的 NAD 所支持的 CoA 类型。

# 网络设备配置文件

Cisco ISE 通过使用网络设备配置文件，支持某些第三方网络访问设备 (NAD)。这些配置文件定义用于启用基本流量和高级流量（如访客、自带设备、MAB 和终端安全评估）的Cisco ISE 功能。

Cisco ISE 包含多个供应商网络设备的预定义配置文件。思科 ISE 2.1 及更高版本已在下表所列的网络设备上测试：

表 *8:* 已经过思科 ***ISE 2.1*** 及更高版本测试的供应商设备

| 设备类型 | 供应商 | CoA 类型 | URL 重定向类型 | 支持或验证的使用案例 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 802.1X 和 MAB 流 | 无 CoA 的分析器 | 带 CoA 的分析器 | 终端安全评估 | 访客和 BYOD 流 |
| 无线 | Aruba 7000，InstantAP | RADIUS | 静态 URL | 支持 | 支持 | 支持 | 支持 | 支持 |
| | Motorola RFS 4000 | RADIUS | 动态 URL | 支持 | 支持 | 支持 | 支持 | 支持 |
| | HP 830 | RADIUS | 静态 URL | 支持 | 支持 | 支持 | 支持 | 支持 |
| | Ruckus ZD 1200 | RADIUS | - | 支持 | 支持 | 支持 | 支持 | 支持 |
| 有线 | HP A5500 | RADIUS | ISE 提供的 Auth VLAN | 支持 | 支持 | 支持 | 支持 | 支持 |
| | HP 3800 和 2920 (ProCurve) | RADIUS | ISE 提供的 Auth VLAN | 支持 | 支持 | 支持 | 支持 | 支持 |
| | Alcatel 6850 | SNMP | 动态 URL | 支持 | 支持 | 支持 | 支持 | 支持 |
| | Brocade ICX 6610 | RADIUS | ISE 提供的 Auth VLAN | 支持 | 支持 | 支持 | 支持 | 支持 |
| | Juniper EX3300-24p | RADIUS | ISE 提供的 Auth VLAN | 支持 | 支持 | 支持 | 支持 | 支持 |

| | | | | |
|---|---|---|---|---|
| 对于其他第三方 NAD，您必须在Cisco ISE 中确定设备属性和功能并创建自定义 NAD 配置文件。 | 支持 | 支持 | 需要 CoA 支持 | 需要 CoA 支持。<br>如果有线设备不支持 URL 重定向，Cisco ISE 将使用 Auth VLAN。尚未使用 Auth VLAN 测试无线设备。 |

您必须为没有预定义配置文件的其他第三方网络设备创建自定义NAD配置文件。对于高级流量（例如访客、自带设备和终端安全评估），网络设备必须支持有关 CoA是否支持这些流量取决于 NAD 的功能。请参阅设备的管理指南，了解在Cisco ISE 中创建网络设备配置文件所需的属性的相关信息。

如果从Cisco ISE 版本 2.0 或更低版本升级到Cisco ISE 版本 2.1 或更高版本，则升级后，早期版本中创建的用于与非Cisco NAD 通信的身份验证策略规则和 RADIUS 词典将继续在Cisco ISE 中运行。

> ISE 社区资源
>
> 有关第三方 NAD 配置文件的信息，请参阅 ISE 第三方 NAD 配置文件和配置。

# 在思科 ISE 中配置第三方网络设备

Cisco ISE 通过使用网络设备配置文件支持第三方 NAD。这些配置文件对Cisco ISE 用于启用流（例如，访客、BYOD、MAB 和安全状态）的功能进行定义。

### 开始之前

请参阅网络设备配置文件，第 25 页。

**步骤 1** 在Cisco ISE 中配置第三方网络设备（参阅将网络设备导入思科 ISE，第 20 页。如果要配置访客、BYOD 或终端安全评估工作流程，请确保已定义授权更改(CoA)，并且已将NAD的URL 重定向机制配置为指向相关的Cisco ISE 门户。要配置 URL 重定向，请从门户的登录页面复制Cisco ISE 门户 URL。有关在 ISE 中为 NAD 配置 CoA 类型和 URL 重定向的详细信息，请参阅网络设备，第 3 页。此外，请参阅第三方的设备管理指南以了解有关说明。

**步骤 2** 确保在 ISE 中可使用设备的适当 NAD 配置文件。要查看现有配置文件，请选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。如果Cisco ISE 中不存在适当的配置文件，请创建自定义配置文件。有关如何创建自定义配置文件的信息，请参阅创建网络设备配置文件，第 27 页。

**步骤 3** 将 NAD 配置文件分配至您想要配置的 NAD。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。打开您希望为其分配配置文件的设备，从**设备配置文件 (Device Profile)** 下拉列表中，选择正确的配置文件。

**步骤 4** 当您在配置策略规则时，在第 1 步中应明确地将授权配置文件设置为 NAD 配置文件；或者如果您使用 VLAN 或者 ACL，或者在您的网络中存在不同供应商的不同设备，则设置为“Any”。要设置授权配置文件的NAD配置文件，请选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。打开相关的授权配置文件，从**网络设备配置文件 (Network Device Profile)** 下拉列表中，选择相关的 NAD 配置文件。在对访客流量使用 Auth VLAN 时，象常规的访客流量一样，您还应定义访客门户，

并在绑定至MAB授权的授权配置文件中选择该访客门户。有关访客门户的详细信息，请参阅《》 中的“思科ISE访客服务”部分请参阅思科 ISE 访客服务。

# 创建网络设备配置文件

开始之前

- 大多数 NAD 都具有供应商特定的 RADIUS 字典，除了提供标准的 IETF RADIUS 属性之外，该字典还提供多个供应商特定属性。如果网络设备有供应商特定的 RADIUS 字典，请将其导入到 Cisco ISE。有关需要哪一个 RADIUS 字典的说明，请参阅第三方设备的管理指南。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)** > **系统 (System)** > **Radius** > **RADIUS 供应商 (RADIUS Vendors)**。要导入 RADIUS 字典，请参阅创建 RADIUS 供应商字典。
- 对于访客和终端安全评估等复杂流，网络设备必须支持 RFC 5176中定义的 CoA 类型。
- 有关创建网络设备配置文件的字段和可能值的信息，请参阅网络设备配置文件设置。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。

**步骤 2** 点击**添加 (Add)**。

**步骤 3** 在显示的**新网络设备配置文件 (New Network Device Profile)** 窗口中，在网络设备的**名称 (Name)** 和**说明 (Description)** 字段中输入相应的值。

**步骤 4** 从**供应商 (Vendor)** 下拉列表中，选择网络设备的供应商。

**步骤 5** 在**图标 (Icon)** 区域中，点击**更改图标... (Change Icon...)** 按钮，从您的系统上传网络设备的图标。

点击**图标 (Icon)** 区域中的**设置为默认 (Set To Default)** 按钮，使用Cisco ISE 提供的默认图标。

**步骤 6** 在**支持的协议 (Supported Protocols)** 区域中，选中设备支持的协议所对应的复选框。仅选中要实际使用的协议对应的复选框。如果网络设备支持 RADIUS 协议，请从 **RADIUS 字典 (RADIUS Dictionaries)** 下拉列表中选择要用于设备的 RADIUS 字典。

**步骤 7** 在**模板 (Templates)** 区域，输入如下相关详细信息：

a) 点击**身份验证/授权 (Authentication/Authorization)** 折叠部分，配置网络设备的默认流类型、属性别名和主机查找设置。在显示的新**流类型条件 (Flow Type Conditions)** 区域中，输入设备用于各种身份验证和授权流（如有线 MAB 和 802.1x）的属性和值。这使Cisco ISE 能够根据它使用的属性为设备检测到正确的流类型。对于MAB没有 IETF 标准，不同的供应商对于 Service-Type 使用不同的值。请参阅设备的用户指南或使用 MAB 身份验证嗅探器跟踪以确定正确的设置。在**属性别名 (Attribute Aliasing)** 区域中，将设备特定的属性名称映射到通用名称以简化策略规则。目前，仅定义服务集标识符 (SSID)。如果网络设备具有无线 SSID 的概念，则将此设置为其使用的属性。在标准化 RADIUS 字典中，Cisco ISE 将它映射至称为 SSID 的属性。您可以在一个规则中引用SSID，并且即使底层属性不同，它也适用于多个设备，因此可简化策略规则配置。在**主机查找 (Host Lookup)** 区域中，选中**处理主机查找 (Process Host Lookup)** 复选框，并根据第三方提供的说明为设备选择相关 MAB 协议和属性。

b) 点击**权限 (Permissions)** 折叠部分，配置网络设备的默认 VLAN 和 ACL 设置。这些设置会根据您在Cisco ISE 中创建的授权配置文件自动映射。
c) 点击**授权更改 (CoA)** 折叠部分以配置网络设备的 CoA 功能。
d) 点击**重定向 (Redirect)** 折叠部分以配置网络设备的 URL 重定向功能。URL 重定向对于访客、BYOD 和终端安全评估服务来说是必需的。

**步骤 8** 点击**提交 (Submit)**。

相关主题

如何创建 ISE 网络访问设备配置文件

# 从思科 ISE 导出网络设备配置文件

以 XML 文件的形式导出在Cisco ISE 中配置的单个或多个网络设备配置文件。然后，可以编辑 XML 文件并将其作为新的网络配置文件导入到Cisco ISE 文件中。

开始之前

请参阅如何创建 ISE 网络访问设备配置文件。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。
**步骤 2** 选中您要导出的设备旁边的复选框，然后点击**导出选定对象 (Export Selected)**。
**步骤 3** 将名为 **DeviceProfiles.xml** 的文件下载到您的本地硬盘。

# 将网络设备配置文件导入到思科 ISE

可以使用具有Cisco ISE XML 结构的单个 XML 文件将单个或多个网络设备配置文件导入到Cisco ISE。您无法同时导入来自多个导入文件的网络设备配置文件。

通常，您将首先从Cisco ISE 管理员门户导出现有配置文件以用作模板。必要时在文件中输入设备配置文件详细信息，并将其另存为 XML 文件。然后，将编辑后的文件重新导入到Cisco ISE。为了使用多个网络设备配置文件，可将多个构造在一起的配置文件导出为单个 XML 文件，编辑该文件，然后将配置文件一并导入，以便在Cisco ISE 中创建多个配置文件。

在导入网络设备配置文件时，只能创建新记录。您无法覆盖现有的配置文件。要更新现有网络设备配置文件，请从Cisco ISE 导出现有配置文件，从Cisco ISE 删除配置文件，然后在相应编辑后导入配置文件。

开始之前

请参阅如何创建 ISE 网络访问设备配置文件。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备配置文件 (Network Devices Profiles)**。

**步骤 2** 点击**导入**。

**步骤 3** 点击 **选择文件 (Choose File)**，从正在运行客户端浏览器的系统中选择 XML 文件。

**步骤 4** 点击**导入**。

# 管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

## 网络设备组设置

下表介绍**网络设备组 (Network Device Groups)** 窗口上的字段，您可以使用此窗口创建网络设备组。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **组 (Groups)**。

您还可以在以下位置创建网络设备组：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **所有组 (All Groups)** 窗口。

表 *9:*“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。<br>网络设备组层次结构中最多可以有六个节点，包括根节点。每个网络设备组的名称最多可以包含 32 个字符。 |
| 说明 | 为根网络设备组或子网络设备组输入一段说明。 |
| 网络设备数 | 此列中显示网络组中的网络设备数量。 |

相关主题

网络设备组，第 30 页
思科 ISE 在策略评估中使用的网络设备属性，第 32 页
在思科 ISE 中添加网络设备

# 网络设备组导入设置

下表列出了**网络设备组 (Network Device Group)** 窗口上**导入 (Import)** 对话框中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** 。

**表 *10:*** 网络设备组导入窗口中的字段

| 字段名称 | 使用指南 |
|---|---|
| 生成模板 | 点击此链接下载 CSV 模板文件。<br>以相同格式的网络设备组信息更新模板，并将其保存于本地位置，以将网络设备组导入任何Cisco ISE 部署中。 |
| 文件 | 点击 **选择文件 (Choose File)**，找到您要上传的 CSV 文件的位置。这可能是新创建的文件，也可能是之前从其他Cisco ISE 部署导出的文件。<br>可以将包含新的和更新后的网络设备组信息的网络设备组从一个Cisco ISE 部署导入另一部署。 |
| 用新数据覆盖现有数据 | 如果想要用您的导入文件中的设备组替换现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。<br>如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。 |
| 遇到第一个错误时停止导入 | 选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，可在导入期间遇到错误的第一个实例时停止导入。<br>如果未选中此复选框并且遇到错误，Cisco ISE 将报告错误，并继续导入剩余设备组。 |

相关主题

网络设备组 ， 第 30 页
思科 ISE 在策略评估中使用的网络设备属性 ， 第 32 页
将网络设备组导入思科 ISE ， 第 32 页

# 网络设备组

Cisco ISE 支持创建分层网路设备组。使用网络设备组根据不同的条件（例如地理位置、设备类型或其在网络中的相对位置 [例如，“接入层”或“数据中心”等]）对网络设备进行逻辑分组。

要查看网络设备组窗口，请点击**菜单 (Menu)** 图标 (☰) 并选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

例如，要按地理位置组织网络设备，可以按大洲、区域和国家/地区将设备进行分组：

- 非洲 > 南部 > 纳米比亚
- 非洲 > 南部 > 南非
- 非洲 > 南部 > 博茨瓦纳

根据设备类型对网络设备进行分组：

- 非洲 > 南部 > 博茨瓦纳 > 防火墙
- 非洲 > 南部 > 博茨瓦纳 > 路由器
- 非洲 > 南部 > 博茨瓦纳 > 交换机

将网络设备分配给一个或多个分层网络设备组。当Cisco ISE 通过已配置的网络设备组的有序列表确定要分配给特定设备的适当组时，它可能会发现同一设备配置文件适用于多个设备组。在这种情况下，Cisco ISE 将应用匹配的第一个设备组。

对可创建的网络设备组的最大数量没有限制。您可以为网络设备组创建最多六个层级（包括父级组）。

设备组层级以两种视图显示：**树表 (Tree Table)** 和**平面表 (Flat Table)**。点击网络设备组列表上方的**树表 (Tree Table)** 或**平面表 (Flat Table)**，按所需视图组织列表。

在**树表 (Tree Table)** 视图中，根节点显示在树顶部，下面是按层级顺序排列的子组。点击**全部展开 (Expand All)** 以查看每个根组中的所有设备组。点击**全部折叠 (Collapse All)** 以查看仅含根组的列表。

在**平面表 (Flat Table)** 视图中，**组层次结构 (Group Hierarchy)** 列中显示每个设备组的层次结构。

在两个视图中，分配给每个子组的网络设备的数量显示在相应的**网络设备数量 (No. of Network Devices)** 列中。点击数字可启动一个对话框，其中列出了分配给该设备组的所有网络设备。显示的对话框还包含两个按钮，可将网络设备从一个组移动到另一个组。点击**将设备移动到另一个组 (Move Devices to Another Group)** 按钮，可将网络设备从当前组移动到另一个组。点击**将设备添加到组 (Add Devices to Group)** 按钮，可将网络设备移至所选网络设备组。

要在**网络设备组 (Network Device Groups)** 窗口中添加网络设备组，请点击**添加 (Add)**。在**父级组 (Parent Group)** 下拉列表中，选择网络设备组必须添加到的父级组，或选择**添加为根组 (Add As Root Group)** 选项将新网络设备组添加为父级组。

**注释** 如果已向设备组分配了任何设备，则无法删除该设备组。在删除设备组之前，您必须将所有现有设备移动到另一个设备组。

### 根网络设备组

Cisco ISE 包含两个预定义的根网路设备组：**所有设备类型 (All Device Types)** 和**所有位置 (All Locations)**。无法编辑、复制或删除这些预定义的网路设备组，但可以在这些组中添加新设备组。

您可以创建根网络设备组（网络设备组），然后在**网络设备组 (Network Device Groups)** 窗口中的根组下创建子网络设备组，如上一节所述。

# 思科 ISE 在策略评估中使用的网络设备属性

创建新网络设备组时，新网络设备属性将添加至**系统字典 (System Dictionaries)** 中的**设备 (Device)** 字典（**策略 (Policy)** > **策略元素 (Policy Elements)** > **字典 (Dictionaries)**）。添加的设备属性随后将在策略定义中使用。

Cisco ISE 允许您使用**设备 (Device)** 字典属性（例如设备类型、位置、型号名称或网络设备上运行的软件版本）配置身份验证和授权策略。

# 将网络设备组导入思科 ISE

您可以使用逗号分隔值 (CSV) 文件将网络设备组导入到Cisco ISE 节点。您不能同时从两个不同的导入文件导入网络设备组。

从Cisco ISE 管理员门户下载 CSV 模板，在模板中输入网络设备组详细信息，并将模板另存为 CSV 文件，然后将编辑的文件导入到Cisco ISE。

导入设备组时，您可以创建新记录或更新现有记录。导入设备组时，您还可以定义在Cisco ISE 遇到第一个错误时希望Cisco ISE 使用新组覆盖现有设备组还是停止导入过程。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

**步骤 2** 点击**导入**。

**步骤 3** 在显示的对话框中，点击**选择文件 (Choose File)**，从正在运行客户端浏览器的系统中选择 CSV 文件。

要下载用于添加网络设备组的 CSV 模板文件，请点击**生成模板 (Generate a Template)**。

**步骤 4** 要覆盖现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。

**步骤 5** 选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框。

**步骤 6** 点击**导入**。

# 从思科 ISE 导出网络设备组

您可以用 CSV 文件的形式导出在Cisco ISE 中配置的网络设备组。然后，您可以将这些网络设备组导入另一个Cisco ISE 节点。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **组 (Groups)**。

**步骤 2** 要导出网络设备组，可以执行以下操作之一：

- 选中要导出的组旁的复选框，然后选择 **导出 (Export)** > **导出所选 (Export Selected)**。
- 选择 **导出 (Export)** > **全部导出 (Export All)**，导出已定义的所有网络设备组。

**步骤 3** 一个 CSV 文件会下载到您的本地硬盘。

# 管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

## 网络设备组设置

下表介绍**网络设备组 (Network Device Groups)** 窗口上的字段，您可以使用此窗口创建网络设备组。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **组 (Groups)**。

您还可以在以下位置创建网络设备组：**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **所有组 (All Groups)** 窗口。

表 *11:*“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。<br>网络设备组层次结构中最多可以有六个节点，包括根节点。每个网络设备组的名称最多可以包含 32 个字符。 |
| 说明 | 为根网络设备组或子网络设备组输入一段说明。 |
| 网络设备数 | 此列中显示网络组中的网络设备数量。 |

**相关主题**

网络设备组，第 30 页
思科 ISE 在策略评估中使用的网络设备属性，第 32 页
在思科 ISE 中添加网络设备

## 网络设备组导入设置

下表列出了**网络设备组 (Network Device Group)** 窗口上**导入 (Import)** 对话框中的字段。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

表 *12:* 网络设备组导入窗口中的字段

| 字段名称 | 使用指南 |
| --- | --- |
| 生成模板 | 点击此链接下载 CSV 模板文件。<br>以相同格式的网络设备组信息更新模板，并将其保存于本地位置，以将网络设备组导入任何Cisco ISE 部署中。 |
| 文件 | 点击 **选择文件 (Choose File)**，找到您要上传的 CSV 文件的位置。这可能是新创建的文件，也可能是之前从其他Cisco ISE 部署导出的文件。<br>可以将包含新的和更新后的网络设备组信息的网络设备组从一个Cisco ISE 部署导入另一部署。 |
| 用新数据覆盖现有数据 | 如果想要用您的导入文件中的设备组替换现有网络设备组，请选中**用新数据覆盖现有数据 (Overwrite Existing Data with New Data)** 复选框。<br>如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。 |
| 遇到第一个错误时停止导入 | 选中**遇到第一个错误时停止导入 (Stop Import on First Error)** 复选框，可在导入期间遇到错误的第一个实例时停止导入。<br>如果未选中此复选框并且遇到错误，Cisco ISE 将报告错误，并继续导入剩余设备组。 |

相关主题

网络设备组，第 30 页
思科 ISE 在策略评估中使用的网络设备属性，第 32 页
将网络设备组导入思科 ISE，第 32 页

# 在思科 ISE 中导入模板

Cisco ISE 可以让您使用 CSV 文件导入大量网络设备和网络设备组。模板包含用于定义字段格式的标题行。不得编辑此信头行。

在网络设备和网络设备组的相关导入流中，可以使用**生成模板 (Generate a Template)** 链接将 CSV 文件下载到本地系统。

# 网络设备导入模板格式

下表列出了重要网络设备 CSV 模板文件标题中的字段，并进行了说明。

表 *13:* 网络设备的 *CSV* 模板字段和说明

| 字段 | 说明 |
|---|---|
| **Name:String(32)** | （必填）此字段是网络设备名称。这是一个最大长度为 32 个字符的字母数字字符串。 |
| **说明:String(256)** | 此字段是网络设备的说明。这是一个最大长度为 256 个字符的字符串。 |
| **IP Address:Subnets(a.b.c.d/m\|...)** | （必填）此字段是网络设备的 IP 地址和子网掩码。它可以包含多个使用竖线“\|”符号分隔的值。<br>网络设备（TACACS 和 RADIUS）配置以及外部 RADIUS 服务器配置支持 IPv4 和 IPv6。<br>输入 IPv4 地址时，可以使用地址范围和子网掩码。 |
| **Model Name:String(32)** | （必填）此字段是网络设备的型号名称。这是一个最大长度为 32 个字符的字符串。 |
| **Software Version:String(32)** | （必填）此字段是网络设备的软件版本。这是一个最大长度为 32 个字符的字符串。 |
| **Network Device Groups:String(100)** | （必填）此字段是现有的网络设备组。如果是子组，必须同时包含由空格分隔的父组和子组。这是一个最大长度为 100 个字符的字符串。例如，位置 *(Location)* > 所有位置 *(All Location)* > 美国 *(US)* |
| **Authentication:Protocol:String(6)** | 此字段是要使用的身份验证协议。唯一有效的值为“ RADIUS”（不区分大小写）。 |
| **Authentication:Shared Secret:String(128)** | （如果在身份验证协议字段中输入一个值，则此字段为必填字段）此字段是一个最大长度为 128 个字符的字符串。 |
| **EnableKeyWrap:Boolean(true\|false)** | 它仅在网络设备上支持此字段时才启用。有效值为“true”和“false”。 |

| 字段 | 说明 |
| --- | --- |
| **EncryptionKey:String(ascii:16\|hexa:32)** | （如果启用 KeyWrap，则此字段为必填字段）此字段是用于会话加密的加密密钥。<br>ASCII 值 - 长度为 16 个字符（字节）<br>十六进制值 - 长度为 32 个字符（字节）。 |
| **AuthenticationKey:String(ascii:20\|hexa:40)** | （如果启用 KeyWrap，则此字段为必填字段）。此字段表示基于 RADIUS 消息的键控散列消息验证码 (HMAC) 计算。<br>ASCII 值 - 长度为 20 个字符（字节）<br>十六进制值 - 长度为 40 个字符（字节）。 |
| **InputFormat:String(32)** | 此字段是加密和身份验证密钥输入格式。接受 ASCII 和十六进制值。 |
| **SNMP:Version:Enumeration (\|2c\|3)** | 此字段由分析器服务使用。它是 SNMP 协议的版本 1、2c 或 3。 |
| **SNMP:RO Community:String(32)** | （如果为 SNMP 版本字段输入一个值，则此字段为必填字段）SNMP 只读社区。此字段是一个最大长度为 32 个字符的字符串。 |
| **SNMP:RW Community:String(32)** | （如果为 SNMP 版本字段输入一个值，则此字段为必填字段）SNMP 读写社区。此字段是一个最大长度为 32 个字符的字符串。 |
| **SNMP:Username:String(32)** | 此字段是一个最大长度为 32 个字符的字符串。 |
| **SNMP:Security Level:Enumeration(Auth\|No Auth\|Priv)** | （如果选择 SNMP 版本 3，则此字段为必填字段）此字段接受的值为“Auth”、“No Auth”或“Priv”。 |
| **SNMP:Authentication Protocol:Enumeration(MD5\|SHA)** | （如果已输入“Auth”或“Priv”作为 SNMP 安全级别，则此字段为必填字段）此字段接受的值为“MD5”或“SHA”。 |
| **SNMP:Authentication Password:String(32)** | （如果已输入 Auth 作为 SNMP 安全级别，则此字段为必填字段）此字段是一个最大长度为 32 个字符的字符串。 |
| **SNMP:Privacy Protocol:Enumeration(DES\|AES128\|AES192\|AES256\|3DES)** | （如果已输入“Priv”作为 SNMP 安全级别，则此字段为必填字段）此字段接受的值为“DES”、“AES128”、“AES192”、“AES256”或“3DES”。 |

| 字段 | 说明 |
| --- | --- |
| **SNMP:Privacy Password:String(32)** | （如果已输入 Auth 作为 SNMP 安全级别，则此字段为必填字段）此字段是一个最大长度为 32 个字符的字符串。 |
| **SNMP:Polling Interval:Integer:600-86400 seconds** | 此字段用于设置 SNMP 轮询间隔。有效值为介于 600 和 86400 之间的整数。 |
| **SNMP:Is Link Trap Query:Boolean(true\|false)** | 此字段用于启用或禁用 SNMP 链路陷阱。有效值为“true”或“false”。 |
| **SNMP:Is MAC Trap Query:Boolean(true\|false)** | 此字段用于启用或禁用 SNMP MAC 陷阱。有效值为“true”或“false”。 |
| **SNMP:Originating Policy Services Node:String(32)** | 此字段用于指示必须用于轮询 SNMP 数据的Cisco ISE 服务器。它默认情况下是自动的，但可以通过在此字段中分配不同的值来覆盖该设置。 |
| **Trustsec:Device Id:String(32)** | 此字段为Cisco Trustsec 设备 ID，是最大长度为 32 个字符的字符串。 |
| **Trustsec:Device Password:String(256)** | （如果已输入Cisco Trustsec 设备 ID，则此字段为必填字段）此字段为Cisco Trustsec 设备密码，是最大长度为 256 个字符的字符串。 |
| **Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds** | 此字段是Cisco Trustsec 环境数据下载间隔。有效值为介于 1 和 24850 之间的整数。 |
| **Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds** | 此字段用于设置Cisco Trustsec 对等体授权策略下载间隔。有效值为介于 1 和 24850 之间的整数。 |
| **Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds** | 此字段用于设置Cisco Trustsec 重新身份验证间隔。有效值为介于 1 和 24850 之间的整数。 |
| **Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds** | 此字段用于设置Cisco TrustSec 安全组 ACL 列表下载间隔。有效值为介于 1 和 24850 之间的整数。 |
| **Trustsec:Is Other Trustsec Devices Trusted:Boolean(true\|false)** | 此字段用于指示Cisco TrustSec 设备是否受信任。有效值为“true”或“false”。 |
| **Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL\|DISABLE_ALL)** | 此字段用于向Cisco Trustsec 设备通知Cisco Trustsec 配置更改。有效值为 **ENABLE_ALL** 或 **DISABLE_ALL**。 |
| **Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true\|false)** | 此字段指示Cisco TrustSec 设备是否包含在安全组标签中。有效值为“true”或“false”。 |

| 字段 | 说明 |
| --- | --- |
| **Deployment:Execution Mode Username:String(32)** | 此字段是有权编辑设备配置的用户名。这是一个最大长度为 32 个字符的字符串。 |
| **Deployment:Execution Mode Password:String(32)** | 此字段为设备密码，是最大长度为 32 个字符的字符串。 |
| **Deployment:Enable Mode Password:String(32)** | 此字段是设备的密码，可以让您编辑设备的配置。这是一个最大长度为 32 个字符的字符串。 |
| **Trustsec:PAC issue date:Date** | 此字段是Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发日期。 |
| **Trustsec:PAC expiration date:Date** | 此字段是Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的到期日期。 |
| **Trustsec:PAC issued by:String** | 此字段是Cisco ISE 为Cisco Trustsec 设备生成的最后一个Cisco Trustsec PAC 的颁发者（Cisco TrustSec 管理员）名称。它是一个字符串值。 |

# 网络设备组导入模板格式

下表列出模板标题中的字段并提供网络设备组 CSV 文件中的字段描述。

表 *14:* 网络设备组的 *CSV* 模板字段和描述

| 字段 | 说明 |
| --- | --- |
| Name:String(100): | （必填）此字段为网络设备组的名称。它是长度最大为 100 个字符的字符串。NDG 全名的长度最大为 100 个字符。例如，如果您要在父组 Global > Asia 下创建子组 India，则您创建的 NDG 的全名为 Global#Asia#India，并且该全名的长度不得超过 100 个字符。如果 NDG 的全名超过 100 个字符，则 NDG 将无法创建。 |
| 说明:String(1024) | 这是可选的网络设备组说明。它是长度不超过 1024 个字符的字符串。 |
| Type:String(64): | （必填）此字段为网络设备组的类型。它是长度最大为 64 个字符的字符串。 |
| Is Root:Boolean(true\|false): | （必填）此字段用于确定特定的网络设备组是否为根组。有效值为 true 或 false。 |

# IPsec 安全保护思科 ISE 与 NAD 间的通信

IPsec 是为 IP 提供安全保护的一组协议。AAA、RADIUS 和 TACACS + 协议使用 MD5 散列算法。为了提高安全性，Cisco ISE 提供 IPsec 功能。IPsec 通过对发送方进行身份验证，发现数据在传输过程中的任何变化以及对发送的数据进行加密来保证安全通信。

Cisco ISE 在隧道及传输模式下支持 IPSec。当在Cisco ISE 接口上启用 IPsec 并配置对等体时，会在 Cisco ISE 和 NAD 之间创建 IPsec 隧道以保护通信。

可以定义预共享密钥或使用 X.509 证书进行 IPsec 身份验证。可以在千兆以太网 1 到千兆以太网 5 接口上启用 IPsec。每个 PSN 仅可以在一个Cisco ISE 接口上配置 IPSec。

由于智能许可证默认处于启用状态 (e0/2—> eth2)，因此无法在千兆以太网2上启用IPsec。但是，如果需要启用 IP 安全，需要为智能许可选择其他接口。

**注释** 千兆以太网 0 和绑定 0（当千兆以太网 0 和千兆以太网 1 接口绑定时）是Cisco ISE CLI 中的管理接口。千兆以太网 0 和绑定 0 不支持 IPsec。

所需组件包括：

- Cisco ISE 2.2 和更高版本。
- Cisco IOS 软件、C5921 ESR 软件 (C5921_I86-UNIVERSALK9-M)：默认情况下，ESR 5921 配置在隧道及传输模式下支持 IPsec。支持 Diffie-Hellman 组 15 和组 16。

**注释** C5921 ESR 软件与 Cisco ISE 2.2 及更高版本捆绑在一起。您需要 ESR 许可证才能将其启用。请参阅《Cisco 5921 嵌入式服务路由器集成指南》，了解 ESR 许可信息。

## 在思科 ISE 上配置 RADIUS IPSec

要在Cisco ISE 上配置 RADIUS IPsec，您必须：

**步骤 1** 从Cisco ISE CLI 配置接口上的 IP 地址。

千兆以太网 1 至千兆以太网 5 接口（绑定 1 和绑定 2）支持 IPsec。但是，只能在Cisco ISE 节点的一个接口上配置 IPSec。

**步骤 2** 将直连网络设备添加到 IPsec 网络设备组。

**注释** RADIUS IPsec 需要通过设备的接口直接连接静态路由网关。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。
b) 在**网络设备 (Network Devices)** 窗口中，点击**添加 (Add)**。
c) 在相应字段中输入要添加的网络设备的名称、IP 地址和子网。
d) 从 IPSEC 下拉列表中，选择**是 (Yes)**。
e) 选中 **RADIUS Authentication Settings** 复选框。
f) 在**共享密钥 (Shared Secret)** 字段中，输入您在网络设备上配置的共享密钥。
g) 点击**保存 (Save)**。

**步骤 3** 添加单独的管理界面，以与Cisco Smart Software Manager (CSSM) 交互。有关嵌入式服务路由器 (ESR) 的信息，请参阅 Smart Software Manager satellite。要执行此操作，请从Cisco ISE CLI 运行以下命令以选择相应的管理接口（千兆以太网 1 至 5 或绑定 1 或 2）：

ise/admin# **license esr smart** {*interface*}

此接口必须能够连通 Cisco.com 才能访问Cisco在线许可服务器。

**步骤 4** 从Cisco ISE CLI 将网络设备添加到直连网关。

**ip route** [*destination network*] [*network mask*] **gateway** [*next-hop address*]

**步骤 5** 在Cisco ISE 节点上激活 IPsec。

a) 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **IPSec**。

此窗口中列出了部署中的所有Cisco ISE 节点。

b) 选中要激活 IPsec 的Cisco ISE 节点旁边的复选框，然后点击**启用 (Enable)** 单选按钮。
c) 从**所选节点的 IPSec 接口：(IPSec Interface for selected nodes:)** 下拉列表中选择要用于 IPsec 通信的接口。
d) 点击所选Cisco ISE 节点的以下身份验证类型之一的单选按钮：

- **预共享密钥 (Pre-shared Key)**：如果选择此选项，必须输入预共享密钥并在网络设备上配置相同的密钥。预共享密钥需使用字母数字字符。不支持特殊字符。有关如何在网络设备上配置预共享密钥的说明，请参阅网络设备文档。有关预共享密钥配置输出的示例，请参阅示例：思科 Catalyst 3850 系列交换机上预共享密钥配置的输出 ， 第 44 页。
- **X.509 证书 (X.509 Certificates)**：如果您选择此选项，请从Cisco ISE CLI 转到 ESR shell 并为 ESR 5921 配置和安装 X.509 证书。然后，为 IPsec 配置网络设备。有关说明，请参阅在 ESR-5921 上配置和安装 X.509 证书 ， 第 42 页。

e) 点击**保存 (Save)**。

**注释** 不能直接修改 IPsec 配置。要在启用 IPsec 时修改 IPsec 隧道或身份验证，请禁用当前 IPsec 隧道，修改 IPsec 配置，然后重新启用不同配置的 IPsec 隧道。

**注释** 启用后，IPsec 将从Cisco ISE 接口删除 IP 地址并关闭该接口。当用户从Cisco ISE CLI 登录时，接口显示为无 IP 地址且处于关闭状态。此 IP 地址将在 ESR-5921 接口上配置。

**步骤 6** 键入 **esr** 进入 ESR shell。

```
ise/admin# esr % Entering ESR 5921 shell % Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M),
 Version 15.5(2)T2, RELEASE SOFTWARE (fc3) % Technical Support: http://www.cisco.com/techsupport %
Copyright (c) 1986-2015 Cisco Systems, Inc. Press RETURN to get started, CTRL-C to exit ise-esr5921>
ise-esr5921>
```

注释 对于 FIPS 合规性，必须配置长度至少为八个字符的加密密码。输入 **Enable secret level 1** 命令以指定密码：

```
ise-esr5921(config)#enable secret level 1 ? 0 Specifies an UNENCRYPTED password will follow 5
Specifies a MD5 HASHED secret will follow 8 Specifies a PBKDF2 HASHED secret will follow 9
Specifies a SCRYPT HASHED secret will follow LINE The UNENCRYPTED (cleartext) 'enable' secret
```

注释 如果从 GUI 配置自定义 RADIUS 端口（除 1645、1646、1812 和 1813 之外），您必须在 ESR shell 中输入以下 CLI 命令以接受配置的 RADIUS 端口：

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

**步骤 7** 验证 IPsec 隧道和经由 IPsec 隧道的 RADIUS 身份验证。

a) 在Cisco ISE 中添加用户并将用户分配到用户组（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰) 并选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**）。

b) 执行以下步骤，验证是否已在Cisco ISE 和 NAD 之间建立 IPsec 隧道：

1. 使用 **ping** 命令测试Cisco ISE 和 NAD 之间的连接是否已建立。
2. 从 ESR shell 或 NAD CLI 运行以下命令，验证连接是否处于活动状态：

   **show crypto isakmp sa**

   ```
   ise-esr5921#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id status 192.168.30.1
    192.168.30.3 QM_IDLE 1001 ACTIVE
   ```

3. 从 ESR shell 或 NAD CLI 运行以下命令，验证隧道是否已建立：

   **show crypto ipsec sa**

   ```
   ise-esr5921#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: radius, local addr
   192.168.30.1 protected vrf: (none) local ident (addr/mask/prot/port):
   (192.168.30.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port):
   (192.168.30.2/255.255.255.255/0/0) current_peer 192.168.30.2 port 500 PERMIT, flags={} #pkts
   encaps: 52, #pkts encrypt: 52, #pkts digest: 52 #pkts decaps: 57, #pkts decrypt: 57, #pkts verify:
    57 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto
    endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2 plaintext mtu 1438, path mtu 1500, ip
   mtu 1500, ip mtu idb Ethernet0/0 current outbound spi: 0x393783B6(959939510) PFS (Y/N): N, DH
   group: none inbound esp sas: spi: 0x8EA0F6EE(2392913646) transform: esp-aes esp-sha256-hmac , in
    use settings ={Tunnel, } conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
    sa timing: remaining key lifetime (k/sec): (4237963/2229) IV size: 16 bytes replay detection
   support: Y Status: ACTIVE(ACTIVE) inbound ah sas: inbound pcp sas: outbound esp sas: spi:
   0x393783B6(959939510) transform: esp-aes esp-sha256-hmac , in use settings ={Tunnel, } conn id:
   100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius sa timing: remaining key lifetime
    (k/sec): (4237970/2229) IV size: 16 bytes replay detection support: Y Status: ACTIVE(ACTIVE)
   outbound ah sas: outbound pcp sas:
   ```

c) 使用以下方法之一验证 RADIUS 身份验证：

- 使用您在步骤 8 (a) 中创建的用户的凭证登录网络设备。RADIUS 身份验证请求将发送到Cisco ISE 节点。在**实时身份验证 (Live Authentications)** 窗口中查看详细信息。

- 将终端主机连接到网络设备并配置 802.1X 身份验证。使用您在步骤 8 (a) 中创建的用户的凭证登录终端主机。RADIUS 身份验证请求将发送到Cisco ISE 节点。在**实时身份验证 (Live Authentications)** 窗口中查看详细信息。

# 在 ESR-5921 上配置和安装 X.509 证书

**步骤 1** 键入 **esr** 进入 ESR shell。

```
ise/admin# esr % Entering ESR 5921 shell % Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M),
 Version 15.5(2)T2, RELEASE SOFTWARE (fc3) % Technical Support: http://www.cisco.com/techsupport %
Copyright (c) 1986-2015 Cisco Systems, Inc. Press RETURN to get started, CTRL-C to exit ise-esr5921>
ise-esr5921>
```

**注释** 对于 FIPS 合规性，必须配置长度至少为八个字符的加密密码。输入 **Enable secret level 1** 命令以指定密码：

```
ise-esr5921(config)#enable secret level 1 ? 0 Specifies an UNENCRYPTED password will follow 5
Specifies a MD5 HASHED secret will follow 8 Specifies a PBKDF2 HASHED secret will follow 9
Specifies a SCRYPT HASHED secret will follow LINE The UNENCRYPTED (cleartext) 'enable' secret
```

**注释** 如果从 GUI 配置自定义 RADIUS 端口（除 1645、1646、1812 和 1813 之外），必须在 ESR shell 中输入以下 CLI 命令以接受配置的 RADIUS 端口：

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

**步骤 2** 使用以下命令生成 RSA 密钥对：

**示例：**

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

**步骤 3** 使用以下命令创建信任点：

**示例：**

```
crypto pki trustpoint trustpoint-name enrollment terminal serial-number none fqdn none ip-address none
subject-name cn=networkdevicename.cisco.com revocation-check none rsakeypair rsa2048
```

**步骤 4** 使用以下命令生成证书签名请求：

**示例：**

```
crypto pki enroll rsaca-mytrustpoint Display Certificate Request to terminal? [yes/no]: yes
```

**步骤 5** 将证书签名请求的输出复制到文本文件，将其提交到外部 CA 进行签名，然后获取签名证书和 CA 证书。

**步骤 6** 使用以下命令导入证书颁发机构 (CA) 证书：

**示例：**

```
crypto pki authenticate rsaca-mytrustpoint
```

复制并粘贴 CA 证书的内容，包括“—**BEGIN**—”和“—**-End**—”行。

**步骤 7** 使用以下命令导入签名证书：

**示例：**

```
crypto pki import rsaca-mytrustpoint
```

复制并粘贴签名证书的内容，包括“—**BEGIN**—”和“—**-End**—”行。

以下是在Cisco 5921 ESR 上配置和安装 X.509 证书时显示的输出示例：

```
ise-esr5921#show running-config ! hostname ise-esr5921 ! boot-start-marker boot host unix:default-config
 boot-end-marker ! no aaa new-model bsd-client server url https://cloudsso.cisco.com/as/token.oauth2 mmi
 polling-interval 60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180 call-home ! 如果 call-home 中
的联系电子邮件地址配置为 sch-smart-licensing@cisco.com ! 将使用Cisco智能许可证门户中配置的电子邮件地址作为发送 SCH
通知的联系电子邮件地址。contact-email-addr sch-smart-licensing@cisco.com profile "CiscoTAC-1" active
destination transport-method http no destination transport-method email ! ip cef no ipv6 cef ! multilink
 bundle-name authenticated ! crypto pki trustpoint SLA-TrustPoint enrollment pkcs12 revocation-check crl
 ! crypto pki trustpoint rsaca-mytrustpoint enrollment terminal serial-number none fqdn none ip-address
 none subject-name cn=ise-5921.cisco.com revocation-check none rsakeypair rsa2048 ! crypto pki certificate
 chain SLA-TrustPoint certificate ca 01 30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101
0B050030 32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73
696E6720 526F6F74 20434130 1E170D31 33303533 30313934 3834375A 170D3338 30353330 31393438 34375A30
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A6BCBD96
131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A
9CAE6388 8A38E520 1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE 4AA4E80D
DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC 7390A3EB 2B5436AD C847A2C5 DAB553EB
69A9A535 58E9F3E3 C0BD23CF 58BD7188 68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B
42C68BB7 C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191 C55F0D76 61F9A4CD
3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44 DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06
03551D0F 0101FF04 04030201 06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500 03820101 00507F24 D3932A66
86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905 604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB
9093D3B1 6C9E3D8B D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8 467A3DF4
4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C 7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB
E973DE7F 5BDDEB86 C71E3B49 1765308B 5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69
39F08678 80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB 418616A9 4093E049
4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0 D697DF7F 28 quit crypto pki certificate chain
rsaca-mytrustpoint certificate 39 30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
 61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06 03550407 0C035254 50310E30
0C060355 040A0C05 43495343 4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
65726368 616F2E63 6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734 335A301D
311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F 6D308201 22300D06 092A8648 86F70D01
01010500 0382010F 00308201 0A028201 0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536
BF1EBBD3 73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617 194AF1B0 7F04B4EA
B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F 8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A
C2BB3174 361B13FA 2CB7BDFE 22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0 F9A21FFB 3C3C507A 20B924F7
E0125D60 6552321C 35736079 42449401 15E68DA6 B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69
A46173B6 96CC84FB 5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801 86F84201
0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469 66696361 7465301D 0603551D 0E041604
146DD31C 03690B98 330B67FA 6EDC7B20 F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690
423599CC EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D 01010B05 00038201
0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965 1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36
236F528E E30C921C 81DA29E1 EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1 2CFDDBE3 EA9D407C 8D1B0F49
BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27 69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC
7BDCC1BB 61F69B31 BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D CD2E1A95
7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585 89AE82F6 A37E51D6 EECD quit certificate
ca 008DD3A81106B14664 308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886 F70D0101
05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06 03550407 0C035254
50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273
6163612E 65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531 30313832 31313534
335A3061 310B3009 06035504 06130255 53310B30 09060355 04080C02 4E43310C 300A0603 5504070C 03525450
310E300C 06035504 0A0C0543 4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
```

```
0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190 16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085
6FAC5425 14AFE225 0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11 B4C32D38
AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B D985703D F3BB9ED1 7DE99614 422D765C
86AB25CD E80008C5 22049BE8 66D1CA27 E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929
D22E2C42 B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B DFBE6EA7 56EBE30B
D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A A196DA5A 1B525175 C26B3581 EA4B0203 010001A3
5D305B30 1D060355 1D0E0416 0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405 30030101 FF300B06 03551D0F
04040302 02A4300D 06092A86 4886F70D 01010505 00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3
05B7D05F 926CC863 220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354 86C6D9DF
D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D 43B80E44 AE69C164 2C9F41A2 8284F577
21FFAB8E A6771A5E DD34EBE4 A0DC2EAD 95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1
DEE50B07 12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3 60E2ED42 7F10D1A6
F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5 3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B
437D82DD D74A4A9F 3557B3D9 D0BD055F 65A8 quit license udi pid CISCO5921-K9 sn 9XG4481W768 username lab
password 0 lab ! redundancy ! crypto keyring MVPN-spokes rsa-pubkey address 0.0.0.0 address 0.0.0.0
key-string quit ! crypto isakmp policy 10 encr aes hash sha256 group 16 ! crypto isakmp policy 20 encr
aes hash sha256 group 14 crypto isakmp profile MVPN-profile description LAN-to-LAN for spoke router(s)
connection keyring MVPN-spokes match identity address 0.0.0.0 ! crypto ipsec transform-set radius esp-aes
 esp-sha256-hmac mode tunnel crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac mode transport
 ! crypto dynamic-map MVPN-dynmap 10 set transform-set radius radius-2 ! crypto map radius 10 ipsec-isakmp
 dynamic MVPN-dynmap ! interface Ethernet0/0 description e0/0->connection to external NAD ip address
192.168.20.1 255.255.255.0 ip nat outside ip virtual-reassembly in no ip route-cache crypto map radius
! interface Ethernet0/1 description e0/1->tap0 internal connection to ISE ip address 10.1.1.1
255.255.255.252 ip nat inside ip virtual-reassembly in no ip route-cache ! interface Ethernet0/2 no ip
address shutdown ! interface Ethernet0/3 no ip address shutdown ! ip forward-protocol nd ! no ip http
server no ip http secure-server ip nat inside source list 1 interface Ethernet0/0 overload ip nat inside
 source static udp 10.1.1.2 1645 interface Ethernet0/0 1645 ip nat inside source static udp 10.1.1.2
1646 interface Ethernet0/0 1646 ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
 ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813 ! access-list 1 permit 10.1.1.0
 0.0.0.3 ! control-plane ! line con 0 logging synchronous line aux 0 line vty 0 4 login transport input
 none ! end
```

以下是在Cisco Catalyst 3850 系列交换机上配置和安装 X.509 证书时显示的输出示例：

```
cat3850#show running-config enable password lab ! username lab password 0 lab aaa new-model ! aaa group
 server radius ise server name ise-vm deadtime 60 ! aaa authentication login default group radius local
 aaa authentication enable default group radius enable ! crypto isakmp policy 10 encr aes hash sha256
authentication rsa-sig group 16 ! crypto ipsec security-association lifetime seconds 86400 ! crypto ipsec
 transform-set radius esp-aes esp-sha256-hmac mode tunnel ! crypto ipsec profile radius-profile ! crypto
 map radius 10 ipsec-isakmp set peer 192.168.20.1 set transform-set radius match address 100 ! interface
 GigabitEthernet1/0/1 no switchport ip address 192.168.20.2 255.255.255.0 crypto map radius ! access-list
 100 permit ip host 192.168.20.2 host 192.168.20.1 ! snmp-server community public RO snmp-server community
 private RW ! radius server rad-ise address ipv4 192.168.20.1 auth-port 1645 acct-port 1646 key secret
```

# 示例：思科 Catalyst 3850 系列交换机上预共享密钥配置的输出

以下是在Cisco Catalyst 3850 系列交换机上配置预共享密钥时显示的输出示例：

```
cat3850#show running-config enable password lab ! username lab password 0 lab aaa new-model
 ! aaa group server radius ise server name ise-vm deadtime 60 ! aaa authentication login
default group radius local aaa authentication enable default group radius enable ! crypto
isakmp policy 10 encr aes hash sha256 authentication pre-share group 16 crypto isakmp key
123456789 address 0.0.0.0 ! crypto ipsec security-association lifetime seconds 86400 !
crypto ipsec transform-set radius esp-aes esp-sha256-hmac mode tunnel ! crypto ipsec profile
 radius-profile ! crypto map radius 10 ipsec-isakmp set peer 192.168.20.1 set transform-set
 radius match address 100 ! interface GigabitEthernet1/0/1 no switchport ip address
192.168.20.2 255.255.255.0 crypto map radius ! access-list 100 permit ip host 192.168.20.2
```

```
 host 192.168.20.1 ! snmp-server community public RO snmp-server community private RW !
radius server rad-ise address ipv4 192.168.20.1 auth-port 1645 acct-port 1646 key secret
```

# 移动设备管理器与思科 ISE 的互操作性

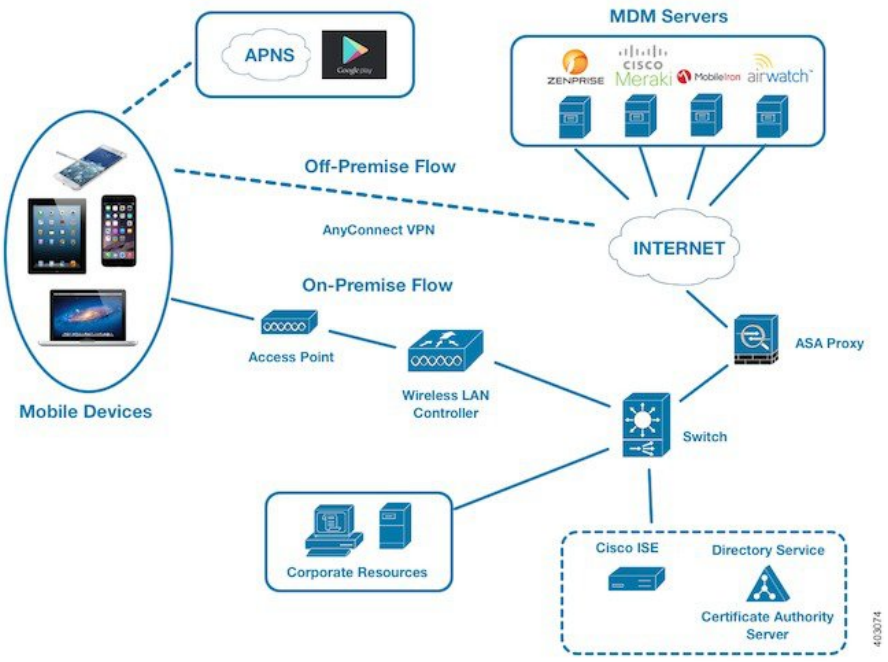
移动设备管理(MDM)服务器保护、监控、管理和支持跨移动运营商、服务提供商和企业部署的移动设备。MDM服务器作为策略服务器运行，用于控制移动设备上的某些应用（例如，电子邮件应用）在部署环境中的使用。但是，网络是基于访问控制列表(ACL)提供精细终端访问的唯一实体。Cisco ISE 会在 MDM 服务器上查询所需的设备属性，以创建为这些设备提供网络访问控制的 ACL。

您可以在网络上运行多个活动 MDM 服务器，包括来自不同供应商的 MDM 服务器。这样，您就可以根据位置或设备类型等设备因素，将不同的终端路由到不同的 MDM 服务器。

Cisco ISE 还使用Cisco MDM 服务器信息 API 版本 2 与 MDM 服务器集成，以便允许设备通过Cisco AnyConnect 4.1 和Cisco自适应安全设备 9.3.2 或更高版本，利用 VPN 访问网络。

在此示例图中，Cisco ISE 是执行点，而 MDM 策略服务器是策略信息点。Cisco ISE 从 MDM 服务器获取数据，以提供完整的解决方案。

图 *3: MDM* 与思科 *ISE* 的互通性




您可以配置Cisco ISE，使其与一个或多个外部移动设备管理器(MDM)服务器进行互操作。通过设置此类第三方连接，您可以使用 MDM 数据库中的详细信息。Cisco ISE 使用 REST API 调用，从外部 MDM 服务器检索信息。Cisco ISE 将相应的访问控制策略应用到交换机、接入路由器、无线接入点和其他网络接入点。策略可以让您能够更好地控制访问支持Cisco ISE 的网络的远程设备。

有关Cisco ISE 支持的 MDM 供应商的列表，请参阅支持的移动设备管理服务器，第 47 页。

# 支持的移动设备管理使用情形

Cisco ISE 与外部 MDM 服务器联合执行以下功能：

- 管理设备注册：访问网络的未注册终端会重定向到 MDM 服务器上托管的注册页面。设备注册包括用户角色、设备类型等。
- 处理设备补救 ：在补救期间向终端授予有限访问权限。
- 增强终端数据：使用来自 MDM 服务器的信息更新终端数据库，这些信息是无法使用Cisco ISE 分析服务收集的。Cisco ISE 使用可在**终端 (Endpoints)** 窗口中查看的六个设备属性。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

  以下是可用设备属性的示例。

  - MDMImei: 99 000100 160803 3
  - MDMManufacturer: Apple
  - MDMModel: iPhone
  - MDMOSVersion: iOS 6.0.0
  - MDMPhoneNumber: 9783148806
  - MDMSerialNumber: DNPGQZGUDTF9

- 每 4 小时轮询一次 MDM 服务器，获取设备合规性数据。在**外部 MDM 服务器 (External MDM Servers)** 窗口中配置轮询间隔。（要查看此窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **网络资源 (Network Resources)** > **外部 MDM 服务器 (External MDM Servers)**。
- 通过 MDM 服务器发出设备指示：Cisco ISE 通过 MDM 服务器发出针对用户设备的远程操作。通过**终端 (Endpionts)** 窗口从Cisco ISE 管理门户发起远程操作。要查看此窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**。选中 MDM 服务器旁的复选框，然后点击**MDM 操作 (MDM Actions)**。从显示的下拉列表中选择所需的操作。

### 供应商 MDM 属性

在Cisco ISE 中配置 MDM 服务器时，供应商的属性会添加到Cisco ISE 系统字典中名为 **mdm** 的新条目。以下属性用于注册状态，通常受 MDM 供应商支持。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus

- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- 无法
- MDMServerName
- MDMServerReachable
- MEID
- Model
- UDID

如果不支持供应商的唯一属性，可以使用 ERS API 来交换供应商特定属性。请查阅供应商的文档，了解有关支持的 ERS API 的信息。

新 MDM 字典属性可以在授权策略中使用。

# 支持的移动设备管理服务器

支持的 MDM 服务器包括来自以下供应商的产品：

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco Meraki 系统管理器
- Citrix Endpoint Management（之前称为 Xenmobile）
- Globo
- IBM MaaS360
- JAMF Casper Suite
- Microsoft Intune（用于移动设备）
- Microsoft SCCM（用于桌面设备）
- MobileIron UEM

注释 某些版本的 MobileIron 不适用于Cisco ISE。MobileIron 已了解此问题，并已修复。请联系 MobileIron 了解更多信息。

- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE（之前称为 AirWatch）
- 42 Gears

**ISE 社区资源**

何操作方法：Meraki EMM/MDM 与 ISE 集成

# 移动设备管理服务器使用的端口

下表列出Cisco ISE 和 MDM 服务器之间要相互通信必须打开的端口。有关必须在 MDM 代理和服务器上打开的端口的列表，请参阅 MDM 供应商的文档。

表 *15: MDM* 服务器使用的端口

| **MDM** 服务器 | 端口 |
|---|---|
| MobileIron | 443 |
| Zenprise | 443 |
| Good | 19005 |
| Airwatch | 443 |
| Afaria | 443 |
| Fiberlink MaaS | 443 |
| Meraki | 443 |
| Microsoft Intune | 80 和 443 |
| Microsoft SCCM | 80 和 443 |

# 移动设备管理集成流程

1. 用户将设备与 SSID 关联。
2. ISE 向 MDM 服务器发出 API 调用。
3. 此 API 调用会返回用户的设备列表和这些设备的终端安全评估状态。

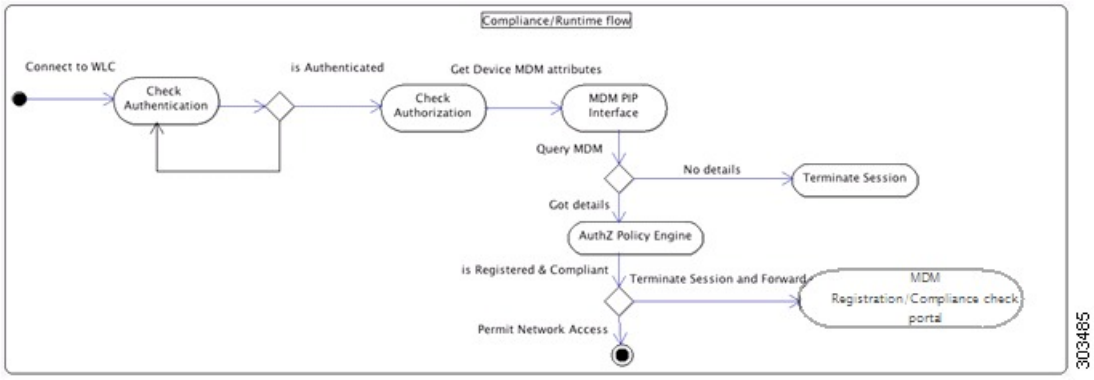
   注释 输入参数是终端设备的 MAC 地址。对于异地 Apple iOS 设备（通过 VPN 连接到思科 ISE 的任何设备），输入参数为 UDID。

4. 如果用户的设备不在此列表中，意味着该设备未注册。Cisco ISE 向 NAD 发送授权请求以重定向至Cisco ISE。系统会向用户显示 MDM 服务器页面。

   注释 对于在Cisco ISE 网络之外注册到 MDM 服务器上的设备，必须通过 MDM 门户对其进行注册。这适用于Cisco ISE 1.4 及更高版本。在之前的Cisco ISE 版本中，如果在启用Cisco ISE 的网络外部注册的设备符合终端安全评估策略，将自动对其进行注册。

5. Cisco ISE 使用 MDM 调配设备并向用户显示相应的页面供其注册设备。
6. 用户在 MDM 服务器中注册设备，然后 MDM 服务器通过自动重定向或手动刷新浏览器将此请求重定向至Cisco ISE。
7. Cisco ISE 重新查询 MDM 服务器获取安全评估状态。
8. 如果用户的设备不符合 MDM 服务器上配置的终端安全评估（合规性）策略，系统会向用户告知设备不合规。用户必须采取必要的措施来确保设备合规。
9. 用户设备合规后，MDM 服务器会在其内部表中更新设备状态。
10. 如果用户现在刷新浏览器，Cisco ISE 将恢复控制。
11. Cisco ISE 每四小时轮询 MDM 服务器一次，以获取合规性信息并发出适当的授权更改 (CoA)。您可以配置轮询间隔。Cisco ISE 还会每五分钟检查一次 MDM 服务器以确保其可用。

下图说明 MDM 流程。




**注释** 一个设备一次只能向一台 MDM 服务器注册。如果您要向其他供应商的 MDM 设备注册同一设备，用户必须删除设备上的前供应商的配置文件。MDM 服务通常提供“公司擦除”功能，仅删除设备的供应商配置（而不是整个设备）。用户还可以删除文件。例如，在iOS设备上，用户可以转到“设置”(Settings) > “常规”(General) > “设备管理”(Device management) 窗口，然后点击**移除管理 (Remove Management)**。或者，用户可以转到Cisco ISE 中的我的设备门户，然后点击**公司擦除 (Corporate Wipe)**。

# 使用思科 ISE 设置移动设备管理服务器

要使用Cisco ISE 设置 MDM 服务器，您必须执行以下高级任务：

**步骤 1** 将 MDM 服务器证书导入Cisco ISE，但 Intune 除外，后者需将策略管理节点 (PAN) 的证书导入 Azure。

**步骤 2** 创建移动设备管理器定义。

**步骤 3** 在无线 LAN 控制器上配置 ACL。

**步骤 4** 配置将非注册设备重定向到 MDM 服务器的授权配置文件。

**步骤 5** 如果网络上有多个 MDM 服务器，请为每个供应商配置单独的授权配置文件。

**步骤 6** 为 MDM 使用案例配置授权策略规则。

# 将移动设备管理服务器证书导入思科 ISE

要使Cisco ISE 连接 MDM 服务器，您必须将 MDM 服务器证书导入Cisco ISE 受信任证书库。如果您的 MDM 服务器有一个 CA 签名的证书，您必须将根证书导入Cisco ISE 受信任证书库。

**注释** 对于 Microsoft Azure，请将Cisco ISE 证书导入 Azure。请参阅将 Microsoft Intune 配置为移动设备管理服务器，第 54 页。

**步骤 1** 从您的 MDM 服务器导出 MDM 服务器证书并将其保存至您的本地计算机上。

**步骤 2** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificate)** > **导入 (Import)**。

**步骤 3** 在**将新证书导入证书库 (Import a new Certificate into the Certificate Store)** 窗口中，点击**选择文件 (Choose File)**，选择从 MDM 服务器获取的 MDM 服务器证书。

**步骤 4** 在**友好名称 (Friendly Name)** 字段中，输入证书名称。

**步骤 5** 选中**信任 ISE 中的身份验证 (Trust for authentication within ISE)** 复选框。

**步骤 6** 点击**提交 (Submit)**。

**步骤 7** 确认**信任证书 (Trust Certificates)** 窗口列出新添加的 MDM 服务器证书。

### 下一步做什么

在 ISE 中定义移动设备管理服务器，第 51 页

。

# 在 ISE 中定义移动设备管理服务器

您可以为外部 MDM 服务器创建一个或多个 MDM 和桌面设备管理器 (SCCM) 定义。

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)**。
2. 点击**添加 (Add)**。
3. 在相应的字段中输入要添加的 MDM 服务器的名称和说明。
4. 从**服务器类型 (Server Type)** 下拉列表中，选择**移动设备管理器 (Mobile Device Manager)** 或**桌面设备管理器 (Desktop Device Manager)**。您在此做出的选择决定了您在下一步能够看到的字段。要配置桌面设备管理器服务器，请参阅桌面设备管理 (Desktop Device Management)，第 53 页。要配置移动设备管理器服务器，请继续执行此步骤列表。
5. 从**身份验证类型 (Authentication Type)** 下拉列表中，选择**基础 (Basic)** 或 **OAuth-客户端凭证 (OAuth - Client Credentials)**。要为 Microsoft Intune 服务器配置 **OAuth-客户端凭证 (OAuth - Client Credentials)**，请参阅移动设备管理（采用 OAuth-客户端凭证身份验证类型），第 52 页。要配置**基础 (Basic)** 身份验证类型，请继续执行此步骤列表。
6. 所有界面都要求名称并描述此MDM服务器定义。下节基于服务器和身份验证类型介绍其他字段和步骤。

### 移动设备管理（采用基本身份验证类型）

- **主机名/IP 地址 (Host Name/IP Address)**：输入 MDM 服务器主机名或 IP 地址。
- **端口 (Port)**：输入连接至 MDM 服务器时要使用的端口，通常为 443。

- **实例名称 (Instance Name)**：如果此 MDM 服务器有多个实例，应输入要连接到的实例。
- **轮询间隔 (Polling Interval)**：输入Cisco ISE 轮询 MDM 服务器以获取合规性检查信息的轮询间隔（以分钟为单位）。此值应与MDM服务器上的轮询间隔相同。有效范围为15至1440分钟。默认值为 240 分钟。我们建议仅在网络上测试若干活动客户端时将轮询间隔设置为小于 60 分钟。如果为具有许多活动客户端的生产环境将此值设置为小于60分钟，则系统的负载会显著增加并可能对性能造成不利影响。

  如果将轮询间隔设置为 0，则Cisco ISE 会禁用与 MDM 服务器的通信。
- **合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)**：当终端通过身份验证或重新进行身份验证时，Cisco ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)** 值，则Cisco ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则Cisco ISE 会触发相应的 CoA。

  有效范围为 1 至 1440 分钟。默认值为 1 分钟。

### 移动设备管理（采用 OAuth-客户端凭证身份验证类型 ）

要使用 OAuth 身份验证类型，请按照将 Microsoft Intune 配置为移动设备管理服务器 ， 第 54 页中所述配置 OAuth 服务器。

- **自动发现 URL (Auto Discovery URL)**：输入 Microsoft Azure 管理门户中的 *Microsoft Azure AD* 图形 *API* 终端 *(Microsoft Azure AD Graph API Endpoint)* 值。此 URL 是应用可使用图形 API 访问 Microsoft Azure AD 中的目录数据的终端。URL 格式为：`https://<hostname>/<tenant id>`

  例如，`https://graph.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329`。

  此 URL 的扩展版本也在属性文件中，格式为：
  `https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>`。
- **客户端 ID (Client ID)**：应用的唯一标识符。如果应用访问其他应用中的数据，如 Microsoft Azure AD Graph API、Microsoft Intune API 等，则需要使用此属性。
- **颁发令牌的 URL (Token Issuing URL)**：输入上一步中的 *Oauth2.0* 授权终端 *(Oauth2.0 Authorization Endpoint)* 值。在该终端上，应用可以使用 OAuth2.0 获得访问令牌。在对应用进行身份验证后，Microsoft Azure AD 会为应用（Cisco ISE）颁发一个访问令牌，允许应用调用图形 API/Intune API。
- **令牌受众 (Token Audience)**：令牌面向的接收资源，通常为指向 Microsoft Intune API 的公共知名 **APP ID URL**。
- **轮询间隔 (Polling Interval)**：输入Cisco ISE 轮询 MDM 服务器以获取合规性检查信息的轮询间隔（以分钟为单位）。此值应与MDM服务器上的轮询间隔相同。有效范围为15至1440分钟。默认值为 240 分钟。我们建议仅在网络上测试若干活动客户端时将轮询间隔设置为小于 60 分钟。如果为具有许多活动客户端的生产环境将此值设置为小于60分钟，则系统的负载会显著增加并可能对性能造成不利影响。

  如果将轮询间隔设置为 0，则Cisco ISE 会禁用与 MDM 服务器的通信。

- **合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)**：当终端通过身份验证或重新进行身份验证时，Cisco ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)** 值，则Cisco ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则Cisco ISE 会触发相应的 CoA。

  有效范围为 1 至 1440 分钟。默认值为 1 分钟。

### 桌面设备管理 (Desktop Device Management)

以下设置要求您在 SCCM 服务器上配置 WMI，以便它能够与Cisco ISE 通信。请参阅为思科 ISE 配置 Microsoft System Center Configuration Manager Server，第 58 页。

- **主机名/IP 地址 (Host Name/IP Address)**：输入 MDM 服务器主机名或 IP 地址。
- **站点或实例名称 (Site or Instance Name)**：输入站点名称，或者在 MDM 服务器有多个实例的情况下输入实例名称。

# 针对 Microsoft Intune 和 Microsoft System Center Configuration Manager 的思科 ISE 移动设备管理支持

- **Microsoft Intune**：Cisco ISE 支持 Microsoft Intune 设备管理，将其作为伙伴 MDM 服务器来管理移动设备。

  在管理移动设备的 Microsoft Intune 服务器上配置Cisco ISE 作为 OAuth 2.0 客户端应用。Cisco ISE 从 Azure 获取令牌，以便与Cisco ISE Intune 应用建立会话。

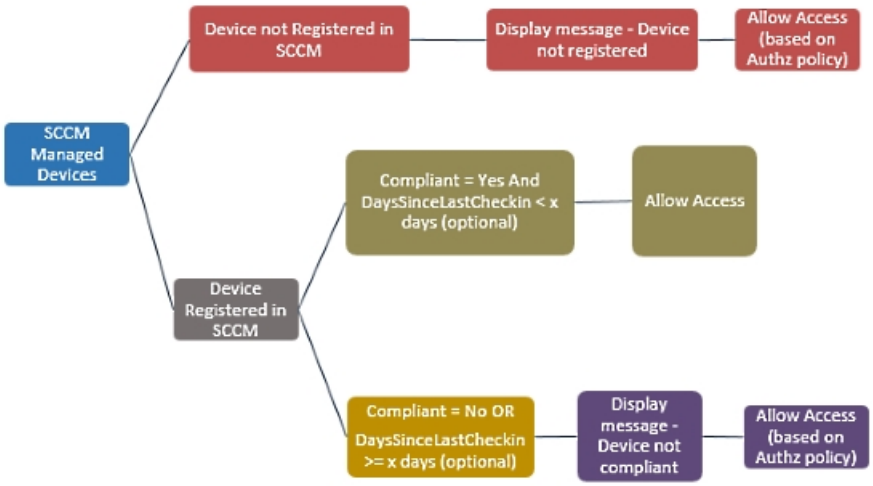
  有关 Microsoft Intune 如何与客户端应用通信的信息，请参阅 https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx。

- **桌面设备管理器 (Microsoft SCCM)**：Cisco ISE 支持 Microsoft System Center Configuration Manager (SCCM)，将其作为伙伴 MDM 服务器来管理 Windows 计算机。Cisco ISE 使用 WMI 从 Microsoft SCCM 服务器检索合规性信息，并使用该信息向用户 Windows 设备授予或拒绝网络访问权限。

### Microsoft SCCM 工作流程

Cisco ISE 会从 Microsoft SCCM 服务器检索有关设备是否注册的信息，如果设备已注册，则检索其是否合规的信息。下图显示了 Microsoft SCCM 管理的设备的工作流程。

图 *4: SCCM* 工作流程




当设备连接网络并且与 Microsoft SCCM 策略匹配时，Cisco ISE 会查询在授权策略中指定的 SCCM 服务器，以检索合规性和最后登录（签入）时间。借助这些信息，Cisco ISE 可在**终端 (Endpoint)** 列表中更新设备合规状态和 lastCheckinTimeStamp。

如果设备不合规或未在 Microsoft SCCM 上注册，且授权策略中使用了重定向配置文件，则系统会向用户显示一则消息，说明该设备不合规或未在 Microsoft SCCM 上注册。在用户确认该消息后，Cisco ISE 会向 Microsoft SCCM 注册站点发出 CoA。可根据授权策略和配置文件授予用户访问权限。

### Microsoft SCCM 服务器连接监控

您无法为 Microsoft SCCM 配置轮询间隔。

Cisco ISE 运行 MDM 心跳作业以验证与 Microsoft SCCM 服务器的连接，如果Cisco ISE 断开了与 Microsoft SCCM 服务器的连接，则会发出警报。无法配置心跳作业间隔。

# 将 Microsoft Intune 配置为移动设备管理服务器

配置 Microsoft Intune 作为Cisco ISE 的 MDM 服务器的过程与配置其他 MDM 服务器的过程略有不同。以下步骤可帮助您配置Cisco ISE 和 Microsoft Azure 之间的连接。

1. 从 Microsoft Intune 或 Azure Active Directory 租户获取公共证书，并将其导入Cisco ISE 中以支持 SSL 握手。
    1. 登录到 Microsoft Intune 或 Microsoft Azure 的管理员控制台（如适用）。
    2. 使用浏览器获取证书详细信息。例如，使用 Internet Explorer：
        1. 点击浏览器工具栏中的锁定符号，然后点击**查看证书 (View Certficates)**。
        2. 在**证书 (Certificate)** 窗口中，点击**证书路径 (Certification Path)**。
        3. 找到 **Baltimore Cyber Trust Root**，然后导出此根证书。

3. 登录Cisco ISE。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。点击**添加 (Add)** 并导入您保存的根证书。为证书指定一个有意义的名称，例如“Azure MDM”。

2. 从Cisco ISE 导出自签证书，并准备用于 Microsoft InTune 或 Azure。

   1. 在 PAN 的管理员门户中，在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。在显示的证书列表中，选择**默认自签名服务器证书 (Default Self-Signed Server Certificate)** 复选框，然后点击**导出 (Export)**。

   2. 在显示的新对话框中，点击**仅导出证书 (Export Certificate Only)** 单选按钮，然后点击**导出 (Export)**

      。

   在导出的证书文件上运行以下 PowerShell 脚本：

   ```
   $cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
   $cer.Import(“mycer.cer”) $bin = $cer.GetRawCertData() $base64Value =
   [System.Convert]::ToBase64String($bin) $bin = $cer.GetCertHash() $base64Thumbprint =
   [System.Convert]::ToBase64String($bin) $keyid = [System.Guid]::NewGuid().ToString()
   ```

   记下 **$base64Thumbprint**、**$base64Value** 和 **$keyid** 的值。这些值将在以后使用。

3. 在 Microsoft Intune 中创建一个Cisco ISE 应用。

   1. 在 Microsoft Azure 管理门户 (https://manage.windowsazure.com) 中登录到您的客户域。选择 **目录 (Directory)** > **应用 (Applications)** > **添加应用 (Add an Application)**，然后选择**添加我的组织正在开发的应用 (Add an application my organization is developing)**。

   2. 在 Microsoft Azure 中使用以下参数配置Cisco ISE 应用：

      - **应用名称 (Application Name)**：输入 **`CiscoISE`**。
      - 选择 **WEB 应用和/或 WEB APP (WEB APPLICATION AND/OR WEB APP)**。
      - **登录 URL 和应用 ID URL (SIGN-ON URL and APP ID URL)**：添加任何有效的 URL，Cisco ISE 不使用这些值。

4. 从 Microsoft Azure 获取该清单文件，添加Cisco ISE 证书信息，然后将更新后的清单上传至 Microsoft Azure。

   1. 在Microsoft Azure管理门户中，打开AAD管理单元，然后导航至创建的“CiscoISE”应用。

   从**管理清单 (Manage Manifest)** 菜单下载应用清单文件。

5. 更新清单 JSON 文件中的 **keyCredentials** 字段，如以下示例所示。将 *Base64 Encoded String of ISE PAN cert* 替换为从Cisco ISE 导出且经过编辑的证书文件，即 PowerShell 脚本中的 $base64Value：

   ```
   "keyCredentials": [ { “customKeyIdentifier“: “$base64Thumbprint_from_above”, “keyId“:
    “$keyid_from_above“, "type": "AsymmetricX509Cert", "usage": "Verify", "value": "Base64
    Encoded String of ISE PAN cert" } ]
   ```

注释 请勿更改清单文件的名称。

KeyCredentials 复合类型在以下位置记录：
http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx。

6. 将更新后的清单文件上传至 Microsoft Azure。
7. 在 Microsoft Azure 管理门户，导航至**应用终端 (App Endpoints)** 列表。您将使用以下终端属性的值在Cisco ISE 中配置 MDM：
   - **MICROSOFT AZURE AD GRAPH API ENDPOINT**
   - **OAUTH 2.0 TOKEN ENDPOINT**
8. 在Cisco ISE 中，配置 Microsoft Intune 服务器。有关配置外部 MDM 服务器的详细信息，请参阅在 ISE 中定义移动设备管理服务器，第 51 页。以下字段对于配置 Microsoft Intune 很重要：
   - **自动发现 URL (Auto Discovery URL)**：输入 Microsoft Azure 管理门户中的 *Microsoft Azure AD* 图形 *API* 终端 *(Microsoft Azure AD Graph API Endpoint)* 值。此 URL 是应用可使用图形 API 访问 Microsoft Azure AD 中的目录数据的终端。URL 格式为：`https://<hostname>/<tenant id>`

     例如，`https://graph.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329`。

     此 URL 的扩展版本也在属性文件中，格式为：`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>`。
   - **客户端 ID (Client ID)**：应用的唯一标识符。如果应用访问其他应用中的数据，如 Microsoft Azure AD Graph API、Microsoft Intune API 等，则需要使用此属性。
   - **颁发令牌的 URL (Token Issuing URL)**：输入上一步中的 *Oauth2.0* 授权终端 *(Oauth2.0 Authorization Endpoint)* 值。在该终端上，应用可以使用 OAuth2.0 获得访问令牌。在对应用进行身份验证后，Microsoft Azure AD 会为应用（Cisco ISE）颁发一个访问令牌，允许应用调用图形 API/Intune API。
   - **令牌受众 (Token Audience)**：令牌面向的接收资源，通常为指向 Microsoft Intune API 的公共知名 **APP ID URL**。

有关 Microsoft Intune 应用的详细信息，请参阅：

- https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest

# Microsoft System Center Configuration Manager 策略集示例

以下新字典条目在策略中用于支持 Microsoft SCCM。

- **MDM.DaysSinceLastCheckin**：自用户最后使用 Microsoft SCCM 签入或同步设备以来的天数。此值可以介于 1 至 365 天之间。
- **MDM.UserNotified**：有效值为 **Y** 或 **N**。该值指示是否通知用户其设备未注册。然后，您可以允许用户有限地访问网络，然后将他们重定向到注册门户，或者拒绝他们访问网络。
- **MDM.ServerType**：有效值为 **MDM**，表示 MDM 服务器，以及 **DM**，表示桌面设备管理。

以下是支持 Microsoft SCCM 的策略集示例。

| 策略名称 | 如果 | 过去 |
|---|---|---|
| SCCM_Comp | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceRegisterStatus EQUALS Registered | PermitAccess |
| SCCM_NonComp_Notify | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceCompliantStatus EQUALS NonCompliant AND<br>MDM:UserNotified EQUALS 28 | PermitAccess |
| SCCM_NonComp_Days | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:MDMDeviceCompliantStatus EQUALS Registered AND<br>MDM:DaysSinceLastCheckin EQUALS 28 | SCCM_Redirect |
| SCCM_NonComp | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceCompliantStatus EQUALS NonCompliant AND<br>MDM:DeviceRegisterStatus EQUALS Registered | SCCM_Redirect |

| 策略名称 | 如果 | 过去 |
| --- | --- | --- |
| SCCM_UnReg_Notify | Wireless_802.1X AND<br>MDM:DeviceRegisterStatus EQUALS Registered AND<br>MDM:UserNotified EQUALS Yes | PermitAccess |

# 为思科 ISE 配置 Microsoft System Center Configuration Manager Server

Cisco ISE 使用 Windows 管理规范 (WMI) 与 Microsoft SCCM 服务器通信。在运行 Microsoft SCCM 的 Windows 服务器上配置 WMI。

注释 用于思科 ISE 集成的用户帐户必须符合以下条件之一：

- 成为 SMS 管理员用户组的成员。
- 具有与 WMI 命名空间下的 SMS 对象相同的权限：

  `root\sms\site_<sitecode>`

  ，其中 *sitecode* 是 Microsoft SCCM 站点。

## 为域管理员组中的 Microsoft Active Directory 用户设置权限

默认情况下，对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，域管理员组对 Windows 操作系统中的某些注册表项没有完全控制权限。Microsoft Active Directory 管理员必须给予 Microsoft Active Directory 用户对以下注册表项的完全控制权限：

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

以下 Microsoft Active Directory 版本不需要对注册表进行更改：

- Windows 2003
- Windows 2003R2
- Windows 2008

要授予完全控制权限，Microsoft Active Directory 管理员必须首先获得注册表项的所有权：

**步骤 1** 右键点击注册表项图标，然后选择**所有者 (Owner)** 选项卡。

**步骤 2** 点击 **Permissions**（权限）。

**步骤 3** 点击 **Advanced**。

## 不在域管理员组中的 Microsoft Active Directory 用户的权限

对于 Windows Server 2012 R2，授予 Microsoft AD 用户对以下注册表项的完全控制权限：

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

在 Windows PowerShell 中使用以下命令来检查是否提供了对注册表项的完整权限：

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

当 Microsoft AD 用户不在域管理员组，但在域用户组中时，还需要以下权限：

- 添加注册表项以允许思科 ISE 连接到域控制器。
- 在域控制器上使用 DCOM 的权限
- 设置访问 WMI Root/CIMv2 名称空间的权限

只有以下 Active Directory 版本要求具有这些权限：

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

### 添加注册表项以允许思科 ISE 连接到域控制器

必须手动将一些注册表项添加到域控制器，以允许思科 ISE 以域用户身份进行连接，并检索登录身份验证事件。域控制器或该域中的任何其他机器都不需要代理。

以下注册脚本显示了要添加的密钥。您可以将其复制并粘贴到一个文本文件，并另存为扩展名为 .reg 的文件，然后双击该文件进行注册更改。要添加注册密钥，用户必须是根秘钥的所有者。

```
Windows 注册表编辑器版本 5.00 [HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
 "AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"="
 "
```

确保DllSurrogate注册表项的值包含两个空格。如果手动更新注册表，必须仅包含两个空格，不包含引号。手动更新注册表时，请确保 AppID、DllSurrogate 及其值中不包含引号。

如前一脚本所示，保留所有空行，包括文件末尾的空行。

在 Windows 命令提示符下使用以下命令，以确认注册表项是否已创建并包含正确值：

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

## 在域控制器上使用 DCOM 的权限

用于思科 ISE 被动身份服务的 Microsoft Active Directory 用户必须具有在域控制器服务器上使用 DCOM 的权限。通过 **dcomcnfg** 命令行工具配置权限。

**步骤 1** 从命令行运行 **dcomcnfg** 工具。

**步骤 2** 扩展**组件服务 (Component Services)**。

**步骤 3** 扩展 **计算机 (Computers)** > **我的计算机 (My Computer)**。

**步骤 4** 从菜单栏中选择**操作 (Action)**，点击**属性 (Properties)**，然后点击 **COM 安全性 (COM Security)**。

**步骤 5** Cisco ISE 用于访问和启动的帐户必须具有允许权限。将 Microsoft Active Directory 用户添加至所有四个选项（**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)** 的**编辑限制设置 (Edit Limits)** 和**编辑默认设置 (Edit Default)**）。

**步骤 6** 对于**访问权限 (Access Permissions)** 和**启动并激活权限 (Launch and Activation Permissions)**，允许所有本地和远程访问。

图 ***5:*** 访问权限的本地和远程访问

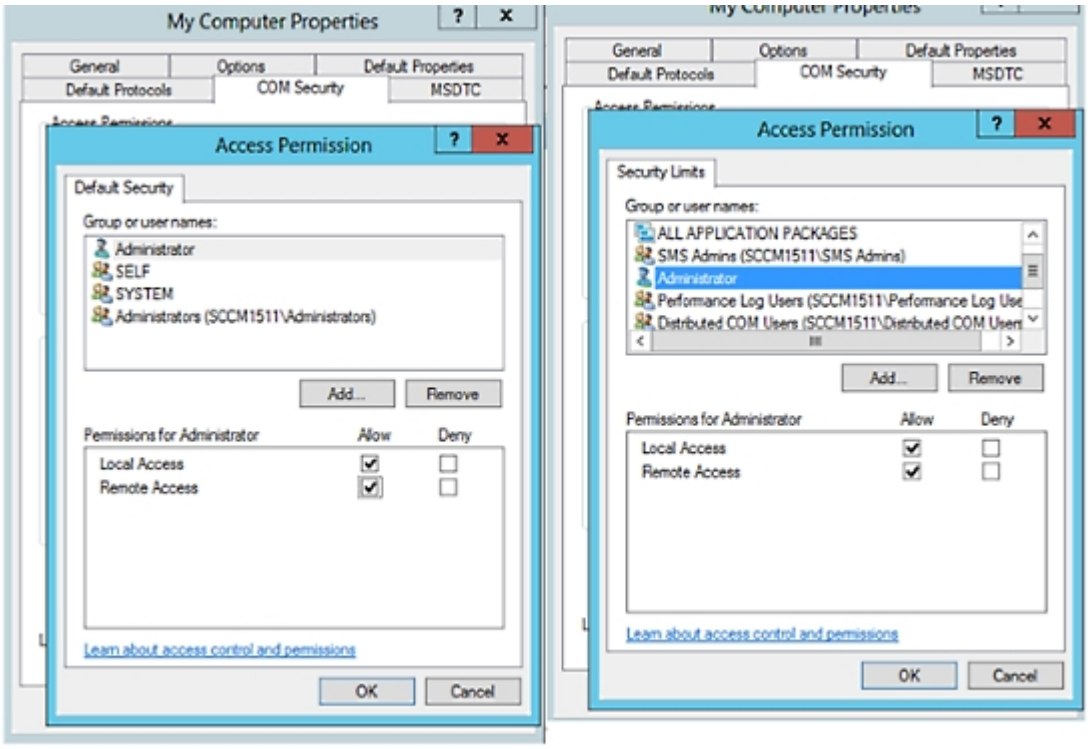
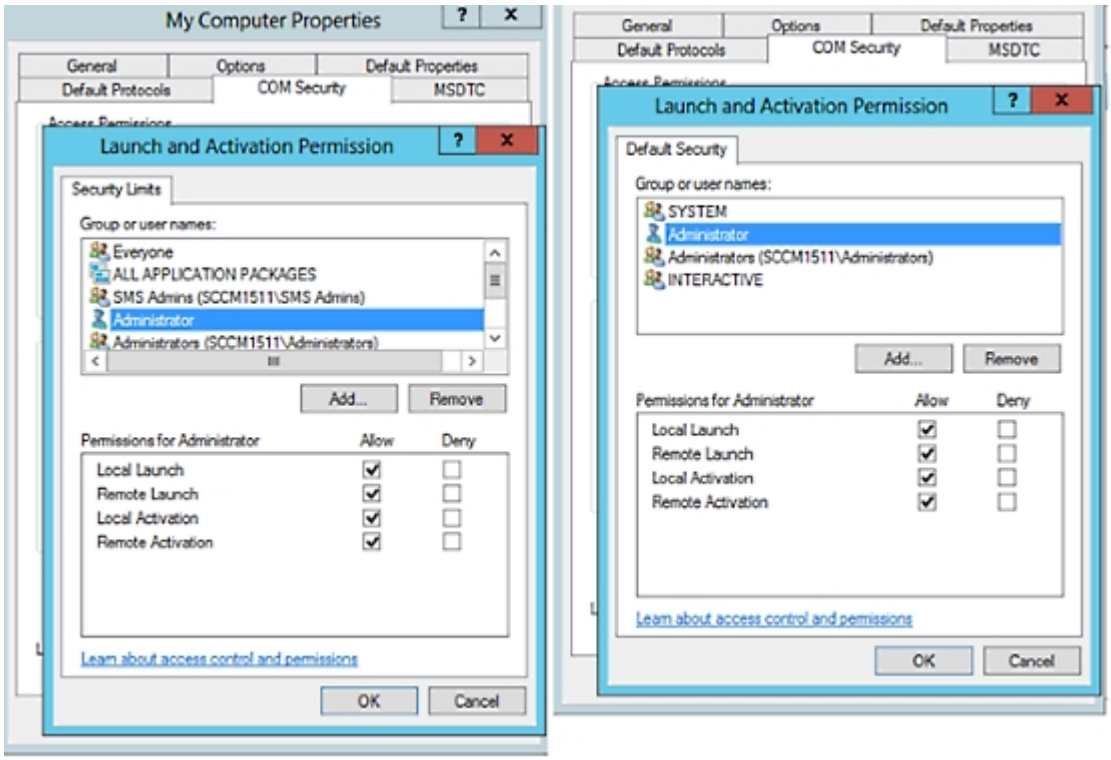


图 *6:* 启动以及激活权限的本地和远程访问




## 设置访问 WMI Root/CIMv2 名称空间的权限

默认情况下，Microsoft Active Directory 用户没有对“执行方法”(Execute Methods) 和“远程启用”(Remote Enable) 的权限。您可以使用 wmimgmt.msc MMC 控制台授予访问权限。

**步骤 1** 选择 **开始 (Start)** > **运行 (Run)** 并键入 `wmimgmt.msc`。

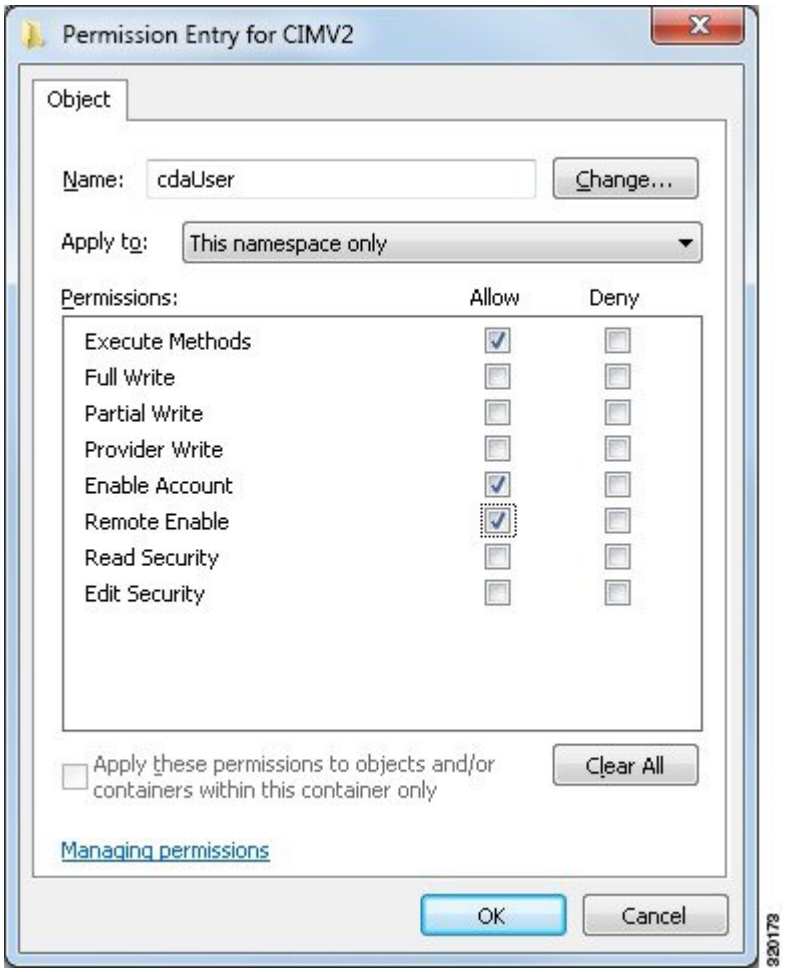
**步骤 2** 右键点击 **WMI 控制 (WMI Control)** 并点击**属性 (Properties)**。

**步骤 3** 在**安全 (Security)** 选项卡下，展开**根 (Root)** 并选择 **CIMV2**。

**步骤 4** 点击 **Security**。

**步骤 5** 添加 Active Directory 用户，并按如下所示配置所需的权限。

图 *7: WMI Root\CIMv2* 名称空间所需的权限




# 为 WMI 访问开放防火墙端口

Microsoft Active Directory 域控制器上的防火墙软件可能会阻止对 WMI 的访问。您可以关闭防火墙，或者允许在特定 IP 地址（Cisco ISE IP 地址）访问以下端口：

- TCP 135：通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端处理此请求的组件使用哪个端口。
- UDP 138：NetBIOS 数据报服务
- TCP 139：NetBIOS 会话服务
- TCP 445：SMB

注释 思科 ISE 支持 SMB 2.0。

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 *%SystemRoot%\System32\dllhost.exe* 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP 地址（Cisco ISE IP）。

# 在思科 ISE 中配置移动设备管理服务器

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)**。

**步骤 2** 点击。

**步骤 3** 为以下字段输入所需的值：**名称 (Name)**、**主机名/IP 地址 (Host Name/IP Address)**、**端口 (Port)**、**实例名称 (Instance Name)**、**用户名 (Username)**、**密码 (Password)**、**说明 (Description)**、**轮询间隔 (Polling Interval)** 和**合规设备重新身份验证查询的时间间隔 (Time Interval for Compliance Device ReAuth Query)**。

**步骤 4** 从**服务器类型 (Server Type)** 下拉列表选择**移动设备管理器 (Mobile Device Manager)** 或**桌面设备管理器 (Desktop Device Manager)**。

**步骤 5** 从**身份验证类型 (Authentication type)** 下拉列表中选择身份验证。

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

**步骤 7** 要验证 MDM 服务器是否已连接到Cisco ISE，请点击**测试连接 (Test Connection)**。**测试连接 (Test Connection)** 并非旨在检查所有使用案例的权限（获取基准、获取设备信息等）。这些在服务器添加到Cisco ISE 时进行验证。

**步骤 8** 在配置**桌面设备管理器**服务器时，点击**保存并继续 (Save & Continue)**；在配置**移动设备管理器**服务器时，点击**保存 (Save)**。

# 从桌面设备管理器服务器选择用于终端合规性的配置基准策略

您可以查看添加到Cisco ISE 的桌面设备管理器服务器（例如，Microsoft SCCM 服务器）中可用的基准策略，并选择特定基准策略以检查网络访问的终端合规性。可以在Cisco ISE 管理门户中查看在桌面设备管理器服务器中启用和部署的配置基准策略。

注释 检查您的桌面设备管理服务器中的用户权限，确保您拥有所需的安全权限，允许将基准策略和合规性信息发送到Cisco ISE。必须在桌面设备管理器的“**安全**”**(Security)** > “**管理员用户**”**(Administrator Users)** 文件夹中添加管理员。

要在Cisco ISE GUI 中查看桌面设备管理器服务器中的基准策略，请点击**菜单 (Menu)** 图标（☰），然后选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)** > **MDM 服务器 (MDM Servers)**。

### 向思科 ISE 添加新的桌面设备管理器服务器，然后选择配置基准策略

在 **MDM 服务器 (MDM Servers)** 窗口中，点击**添加 (Add)** 以添加新的桌面设备管理器服务器。

要验证服务器是否已连接到Cisco ISE，请点击**测试连接 (Test Connection)** 按钮。要查看此服务器中可用的配置基准策略，请点击**保存并继续 (Save & Continue)**。系统将显示一个新窗口，其中包含基准策略的名称和 ID 列表。

### 从现有桌面设备管理器服务器中选择配置基准策略

在 **MDM 服务器 (MDM Servers)** 窗口中，选中所需服务器的复选框，然后点击**编辑 (Edit)**。点击**配置基准 (Configuration Baselines)** 选项卡，获取此服务器中可用的基准策略列表。

默认情况下，系统会选择所有基准策略。取消选中**名称 (Name)** 旁的复选框，以取消选择所有基准策略。通过选中基准策略名称旁的复选框，选择所需的基准策略。点击**保存 (Save)**。

根据所选配置基准策略检查终端合规性。

如果桌面设备管理器服务器中的配置基准策略有任何更改，请点击**配置基准 (Configuration Baselines)** 选项卡中的**立即更新 (Update Now)** 按钮，以在Cisco ISE 中更新更改。

### 配置 Windows 终端的设备标识符

桌面设备管理器服务器使用某些属性作为标识符来验证连接到网络的终端。终端 MAC 地址是最常用的标识符。但是，当使用加密狗、扩展坞或 MAC 地址随机化技术时，MAC 地址不是最可靠的标识符。

您现在可以选择使用主机名作为标识符。主机名派生自证书中可用的通用名称 (CN) 或 SAN-DNS 属性。对于使用主机名检查基准策略合规性来说，基于证书的终端身份验证是强制的。

要配置桌面设备管理器服务器的设备标识符，请转至其**服务器配置 (Server Configuration)** 选项卡。从主菜单中选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)** > **MDM 服务器 (MDM Servers)** > **编辑 (Edit)**。

在**设备标识符配置 (Device Identifier Configurations)** 部分中，默认情况下按如下顺序启用以下标识符：

1. **旧版 MAC 地址**
2. **证书 - CN、主机名**
3. **证书 - SAN-DNS、主机名**

要取消选择标识符，请取消选中该标识符对应的复选框。可以拖动属性以重新排列服务器用于验证的顺序。

### 验证设备标识符的配置

当使用主机名进行验证时，Cisco ISE 会为终端分配一个 GUID。请参阅**实时日志 (Live Logs)** 窗口（在Cisco ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)**），并检 GUID 条目以了解详细信息。

# 配置用于重定向未注册设备的授权配置文件

您必须在Cisco ISE 中配置授权配置文件来重定向每个外部 MDM 服务器的非注册设备。

### 开始之前

- 确保您已在Cisco ISE 中创建 MDM 服务器定义。只有在成功将Cisco ISE 与 MDM 服务器集成之后，才会填充 MDM 字典，您才可以使用 MDM 字典属性创建授权策略。
- 在无线 LAN 控制器上配置用于重定向未注册设备的 ACL。
- 如果使用代理进行互联网连接，并且 MDM 服务器是内部网络的一部分，则必须将 MDM 服务器名称或其 IP 地址置于代理绕行列表中。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **代理 (Proxy)** 以执行此操作。

---

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

**步骤 2** 创建用于重定向不合规或未注册的非注册设备的授权配置文件。

**步骤 3** 在**名称 (Name)** 字段中，为授权配置文件输入与 MDM 服务器名称匹配的名称。

**步骤 4** 从**访问类型 (Access Type)** 下拉列表中，选择 **ACCESS_ACCEPT**。

**步骤 5** 在**常见任务 (Common Tasks)** 部分中，选中 **Web 重定向 (Web Redirection)** 复选框，然后从下拉列表中选择 **MDM 重定向 (MDM Redirect)**。

**步骤 6** 从 **ACL** 下拉列表中，选择输入您在无线 LAN 控制器上配置的 ACL 的名称。

**步骤 7** 从**值 (Value)** 下拉列表中，选择 MDM 门户。

**步骤 8** 从 **MDM 服务器 (MDM Server)** 下拉列表中，选择要使用的 MDM 服务器。

**步骤 9** 点击**提交 (Submit)**。

---

### 下一步做什么

为移动设备管理用例配置授权策略规则。

# 为移动设备管理用例配置授权策略规则

您必须在Cisco ISE 中配置授权策略规则才能完成 MDM 配置。

### 开始之前

- 将 MDM 服务器证书添加到Cisco ISE 证书库。
- 确保您已在Cisco ISE 中创建了 MDM 服务器定义。只有在成功将Cisco ISE 与 MDM 服务器集成之后，才会填充 MDM 字典，您才可以使用 MDM 字典属性创建授权策略。
- 在无线 LAN 控制器上配置 ACL 以重定向未注册或不合规设备。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开策略集以查看授权策略规则。

**步骤 2** 添加以下规则：

- **MDM_Un_Registered_Non_Compliant**：适用于尚未向 MDM 服务器注册或不符合 MDM 策略的设备。请求与此规则匹配之后，系统会显示Cisco ISE MDM 窗口，其中包含有关向 MDM 注册设备的信息。

  注释　请勿在此策略中使用 **MDM.MDMServerName** 条件。使用此条件时，仅当终端注册到 MDM 服务器注册后，才与策略匹配。

- **PERMIT**：如果设备已注册到Cisco ISE、MDM，并符合Cisco ISE 和 MDM 策略，则系统将根据Cisco ISE 中配置的访问控制策略向它授予网络访问权限。

**步骤 3** 点击**保存 (Save)**。

# 在无线 LAN 控制器上配置 ACL 以实现移动设备管理互操作

必须在无线 LAN 控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备和证书调配。ACL 必须采用以下顺序。

**步骤 1** 允许所有从服务器到客户端的出站流量。

**步骤 2** （可选）允许从客户端到服务器的 ICMP 入站流量以进行故障排除。

**步骤 3** 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。

**步骤 4** 允许从客户端到服务器再到 ISE 的所有入站流量以执行 Web 门户和请求方以及证书调配流程。

**步骤 5** 允许从客户端到服务器的入站 DNS 流量以进行名称解析。

**步骤 6** 允许从客户端到服务器的入站 DHCP 流量以获取 IP 地址。

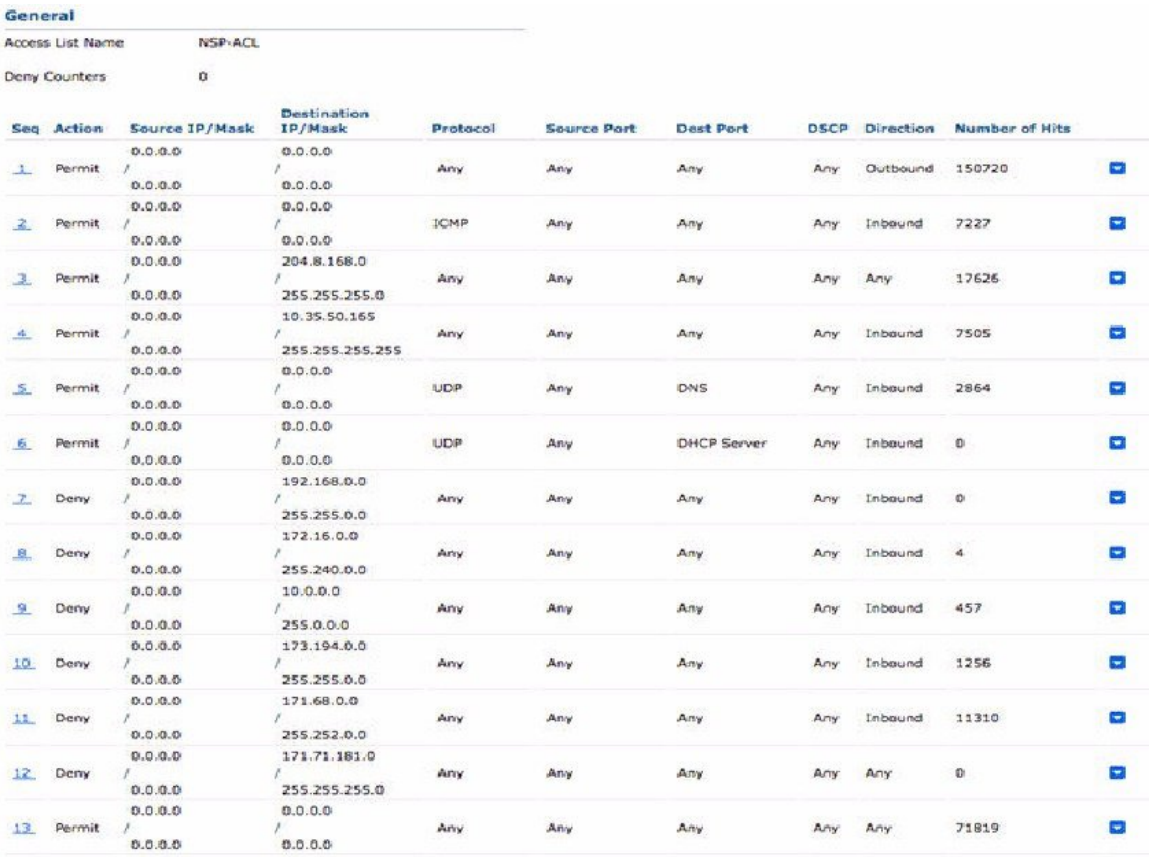
**步骤 7** 拒绝所有从客户端到服务器再到企业资源的入站流量，以重定向至Cisco ISE（根据公司策略）。

**步骤 8** （可选）允许其余流量。

### 示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，Cisco ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 *8:* 用于重定向未注册设备的 ***ACL***



General

Access List Name: NSP-ACL

Deny Counters: 0

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Outbound | 150720 |
| 2 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | ICMP | Any | Any | Any | Inbound | 7227 |
| 3 | Permit | 0.0.0.0 / 0.0.0.0 | 204.8.168.0 / 255.255.255.0 | Any | Any | Any | Any | Any | 17626 |
| 4 | Permit | 0.0.0.0 / 0.0.0.0 | 10.35.50.165 / 255.255.255.255 | Any | Any | Any | Any | Inbound | 7505 |
| 5 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | Any | DNS | Any | Inbound | 2864 |
| 6 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | Any | DHCP Server | Any | Inbound | 0 |
| 7 | Deny | 0.0.0.0 / 0.0.0.0 | 192.168.0.0 / 255.255.0.0 | Any | Any | Any | Any | Inbound | 0 |
| 8 | Deny | 0.0.0.0 / 0.0.0.0 | 172.16.0.0 / 255.240.0.0 | Any | Any | Any | Any | Inbound | 4 |
| 9 | Deny | 0.0.0.0 / 0.0.0.0 | 10.0.0.0 / 255.0.0.0 | Any | Any | Any | Any | Inbound | 457 |
| 10 | Deny | 0.0.0.0 / 0.0.0.0 | 173.194.0.0 / 255.255.0.0 | Any | Any | Any | Any | Inbound | 1256 |
| 11 | Deny | 0.0.0.0 / 0.0.0.0 | 171.68.0.0 / 255.252.0.0 | Any | Any | Any | Any | Inbound | 11310 |
| 12 | Deny | 0.0.0.0 / 0.0.0.0 | 171.71.181.0 / 255.255.255.0 | Any | Any | Any | Any | Any | 0 |
| 13 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 71819 |

# 擦除或锁定设备

Cisco ISE 可以让您擦除已丢失的设备或打开其 pin 锁。您可以从**终端 (Endpoints)** 窗口配置此特性。

**步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)**。

**步骤 2** 选中您想要擦除或锁定的设备旁边的复选框。

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

- **完全擦除 (Full Wipe)**：此选项会删除公司应用或将设备重置为出厂设置，具体取决于 MDM 供应商。
- **企业擦除 (Corporate Wipe)**：此选项会删除您在 MDM 服务器策略中配置的应用。
- **PIN 锁定**：此选项会锁定设备。

**步骤 4** 点击**是 (Yes)** 擦除或锁定设备。

# 查看移动设备管理报告

Cisco ISE 记录 MDM 服务器定义的所有添加、更新和删除操作。可以在**更改配置审核 (Change Configuration Audit)** 报告中查看这些事件，该报告显示选定时段内任何系统管理员的全部配置更改。

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。检查您要查看的 MDM 服务器的**对象类型 (Object Type)** 和**对象名称 (Object Name)** 列中的条目，然后点击相应的**事件 (Event)** 值以查看配置事件的详细信息。

# 查看移动设备管理日志

您可以使用**调试向导 (Debug Wizard)** 窗口查看移动设备管理日志消息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)**。点击Cisco ISE 节点旁的单选按钮，然后点击**编辑 (Edit)**。在显示的新窗口中，点击组件名称 **external-mdm** 旁的单选按钮，然后点击**编辑 (Edit)**。此组件的默认日志级别为**信息 (INFO)**。从相应的**日志级别 (Log Level)** 下拉列表中，选择**调试 (DEBUG)** 或**跟踪 (TRACE)**，然后点击**保存 (Save)**。