合规性

终端安全评估类型

以下终端安全评估代理可监控和实施思科 ISE 终端安全评估策略：

- **AnyConnect**：部署 AnyConnect 代理以监控和实施需要客户端交互的思科 ISE 策略。 AnyConnect 代理留在客户端上。有关在思科 ISE 中使用 AnyConnect 的详细信息，请参阅 思科 AnyConnect 安全移动， 第 105 页。

- **AnyConnect Stealth**：作为服务运行终端安全评估，没有用户界面。代理留在客户端上。

  当在终端安全评估要求中选择 AnyConnect Stealth 终端安全评估类型时，某些条件、补救或条件中的属性会被禁用（显示为灰色）。例如，当启用 AnyConnect 要求时，手动补救类型会被禁用（显示为灰色），因为此操作需要客户端交互。

  当您将姿势配置文件映射到 AnyConnect 配置，然后将 AnyConnect 配置映射到用于 AnyConnect Stealth 模式部署的客户端配置窗口时：

  - AnyConnect 可以读取终端安全评估配置文件并将其设置为目标模式。
  - AnyConnect 可以在初始终端安全评估请求期间将与所选模式的相关信息发送到思科 ISE。
  - 思科 ISE 可以根据模式和其他因素匹配正确的策略，如身份组、操作系统和合规性模块。

注释 AnyConnect Stealth 模式需要 AnyConnect 4.4 及更高版本。

有关在思科 ISE 中配置 AnyConnect Stealth 的详细信息，请参阅 配置 AnyConnect 隐身模式工作流程，第 74 页。

- **临时代理**：当客户端尝试访问受信任网络时，思科 ISE 会打开“客户端调配”(Client Provisioning) 门户。门户会指示用户下载并安装代理，然后运行代理。临时代理会检查合规性状态，并将状态发送到思科 ISE。思科 ISE 会根据结果采取行动。在合规性处理完成后，临时代理会将自身从客户端中删除。临时代理不支持自定义补救。默认补救仅支持消息文本。

  临时代理不支持以下条件：

  - 服务条件 macOS - 系统后台守护程序检查
  - 服务条件 macOS - 后台守护程序或用户代理检查
  - PM - 最新检查
  - PM - 已启用检查
  - DE - 加密检查
  - 使用**终端安全评估类型 (Posture Types)** **临时代理 (Temporal Agent)** 和**合规性模块 (Compliance Module) 4.x 或更高版本 (4.x or later)** 配置终端安全评估策略。请勿将合规性模块配置为 **3.x 或更低版本**或**任何版本**。
  - 对于临时代理，只能在**要求 (Requirements)** 窗口中查看包含**安装 (Installation)** 检查类型的补丁管理条件。
  - 思科 ISE 不支持使用 macOS 临时代理的 VLAN 控制终端安全评估。当您将网络访问从现有 VLAN 更改为新 VLAN 时，用户的 IP 地址会在 VLAN 更改之前释放。当用户连接到新 VLAN 时，客户端通过 DHCP 获取新 IP 地址。识别新 IP 地址需要根权限，但临时代理作为用户进程运行。
  - 思科 ISE 支持 ACL 控制的终端安全评估环境，后者不需要刷新终端 IP 地址。
  - 有关在思科 ISE 中配置临时代理的详细信息，请参阅配置思科临时代理工作流程，第 78 页。

- **AMP 启用程序**：AMP 启用程序从托管在企业本地的服务器将面向终端软件的 AMP 推送到一部分终端，并将 AMP 服务安装到现有用户群中。此处介绍 AMP 分析器AMP 启用程序配置文件设置，第 90 页。

- **无代理终端安全评估**：无代理终端安全评估提供来自客户的终端安全评估信息，并在完成后完全删除自身。最终用户无需执行任何操作。与临时代理不同，无代理终端安全评估以管理用户身份连接到客户端。有关在思科 ISE 中使用无代理终端安全评估的详细信息，请参阅 无代理终端安全评估，第 4 页。

您可以在“**客户端调配**”窗口中选择终端安全评估类型 (**Policy > Policy Elements > Results > Client Provisioning > Resources**) and the **Posture Requirements** window (**Policy > Policy Elements > Results > Posture > Requirements**)。最佳实践是在“客户端调配”(Client Provisioning) 窗口中调配终端安全评估配置文件。

相关主题

配置 AnyConnect 隐身模式工作流程，第 74 页
配置思科临时代理工作流程，第 78 页

无代理终端安全评估

无代理终端安全评估从客户端提供终端安全评估信息，并在完成后完全删除自身。最终用户无需执行任何操作。

要求

- 客户端必须可通过其 IP 地址访问，并且此 IP 地址必须在 RADIUS 记帐中可用。不支持 IPv6。
- 目前支持 Windows 和 Mac 客户端。
  - 对于 Windows 客户端，必须打开访问客户端上 Powershell 的端口 5985。Powershell 必须为版本 5.1 或更高版本。客户端必须具有 cURL 版本 7.34 或更高版本。
  - 对于 macOS 客户端，必须打开访问 SSH 的端口 22 才能访问客户端。客户端必须具有 cURL 版本 7.34 或更高版本。
- 用于外壳登录的客户端凭证必须具有本地管理员权限。
- 运行终端安全评估源更新以获取最新客户端，如配置步骤中所述。
- 确保在 sudoers 文件中更新以下条目，以避免在终端安装证书时失败：

  ```
  <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
  ```

- 对于 macOS，配置的用户账户必须是管理员账户。要查看此处窗口，请单击**菜单**图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端脚本 (Endpoint Scripts)** > **登录配置 (Login Configuration)** > **MAC 本地用户 (MAC Local User)**。MacOS 的无代理终端安全评估不适用于任何其他账户类型，即使您授予更多权限也是如此。
- 如果 Windows 客户端中的端口相关活动因 Microsoft 的更新而发生变化，则可能需要为 Windows 客户端重新配置无代理安全评估配置工作流程。

支持的终端安全评估条件

- 文件条件，使用 USER_DESKTOP 和 USER_PROFILE 文件路径的条件除外
- 服务条件，MacOS 上的系统后台守护程序和后台守护程序或用户代理检查除外
- 应用条件
- 外部数据源条件

- 复合条件
- 防恶意软件条件
- 补丁管理条件，但“已启用”和“最新”条件检查除外
- 防火墙条件
- 磁盘加密条件，但基于位置的加密条件检查除外
- 注册表条件，使用 HCSK 作为根密钥的条件除外

不支持的终端安全评估条件

- 补救
- 宽限期
- 定期重新评估
- 可接受使用策略

支持的客户端操作系统

- Microsoft Windows 版本：10
- MacOS 版本：10.13、10.14、10.15

无代理终端安全评估流程

1. 客户端连接到网络。
2. 思科 ISE 检测是否已在客户端使用的授权配置文件中启用了无代理终端安全评估。
3. 如果是，思科 ISE 会向思科 ISE 消息队列发送无代理终端安全评估作业请求。
4. 思科 ISE 从消息队列获取作业，并启动无代理终端安全评估流程。
5. 思科 ISE 通过 Power Shell 或 SSH 连接到客户端。
6. 如果证书不在客户端的信任证书颁发机构存储区中，思科 ISE 将推送证书。
7. 思科 ISE 运行客户端调配策略。
8. 思科 ISE 将无代理插件推送到客户端并启动该插件。
9. 终端安全评估在客户端上运行，并将状态发送到思科 ISE。
10. 思科 ISE 从客户端删除无代理插件。终端安全评估流程的日志在客户端上保留 24 小时，或保留到客户端将其删除。

无代理终端安全评估配置

1. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)**，创建一个或多个使用无代理终端安全评估来标识要求的终端安全评估要求。
2. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers) > 终端安全评估 (Posture) > 终端安全评估策略 (Posture Policy)**，创建一个或多个使用无代理终端安全评估来标识终端安全评估要求的受支持终端安全评估策略规则。可以复制计划使用的规则，并将终端安全评估类型更改为“Agentless”(无代理)。
3. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authoriation) > 授权配置文件 (Authorization Profiles)**，创建从无代理终端安全评估来评估结果的授权配置文件。
   - 在授权配置文件中启用无代理终端安全评估。
   - 仅将此配置文件用于无代理终端安全评估。请勿将其用于其他终端安全评估类型。
   - CWA 和重定向 ACL 不是无代理终端安全评估所必需的。可以将 VLAN、DACL 或 ACL 用作分段规则的一部分。
4. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy) > 客户端调配 (Client Provisioning)**，添加客户端调配策略。对于思科代理配置，选择适于您配置的操作系统的无代理插件。对于 Windows，此插件为 CiscoAgentlessWindows 4.9.01095。对于 MacOS，此插件为 CiscoAgentlessOSX 4.9.01095。选择此规则检查的终端安全评估条件。请注意，如果您使用的是 Active Directory，可以在策略中使用 Active Directory 组。

注释 只有在更新终端安全状态源之后，适于 MACOSX 10.14 和 10.15 版本的无代理终端安全评估配置才可用。请先更新终端安全评估 URL，然后才能运行终端安全评估源。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **设置 (Settings)** > **软件更新 (Software Updates)** > **终端安全评估更新 (Posture Updates)**。在**终端安全评估更新 (Posture Updates)** 窗口中，在**更新源 URL (Update Feed URL)** 字段中输入 URL (https://www.cisco.com/web/secure/spa/posture-update.xml)，然后单击**立即更新 (Update Now)**。

5. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy) > 策略集 (Policy Sets)**，展开“授权策略”(Authorization Policy)。启用并配置以下三个授权策略：
   - **Unknown_Compliance_Redirect**：使用结果“无代理终端安全评估”(Agentless Posture) 配置条件 Network_Access_Authentication_Passed 和 Compliance_Unknown_Devices。
   - **NonCompliant_Devices_Redirect**：使用结果“DenyAccess”配置条件 Network_Access_Authentication_Passed 和 Non_Compliant_Devices。
   - **Compliant_Devices_Access**：使用结果“PermitAccess”配置条件 Network_Access_Authentication_Passed 和 Compliant_Devices。

6. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 > 设置 > 终端脚本 > 终端登录配置**，然后配置客户端凭证以登录客户端。这些相同凭证由终端脚本使用。
7. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration) > 设置 (Settings) > 终端脚本 (Endpoint Scripts) > 设置 (Settings)**，并配置**操作系统标识的最大重试次数 (Max retry attempts for OS identification)** 和**操作系统标识重试之间的延迟 (Delay between retries for OS identification)**。这些设置决定了确认连接问题的速度。例如，表明 PowerShell 端口未打开的错误仅在所有重试未用尽后才会显示在日志中。
8. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings)**，配置“无代理终端安全评估”(Agentless Posture) 设置。
9. 当客户端与无代理终端安全评估连接时，可以在实时日志中进行查看。

调试和故障排除

为以下项启用调试日志级别：

- 基础设施
- 客户端调配
- 终端安全评估

调试日志位于 *ise-psc.log*中

无代理终端安全评估故障排除在以下位置提供：

- 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 > 实时日志** -“终端安全评估状态”列下的三个点将打开无代理终端安全评估故障排除。
- 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断 (Diagnostic) > 常规工具 (General Tools)**

无代理终端安全状态故障排除

“无代理终端安全评估”(Agentless Posture) 报告是当无代理终端安全评估未按预期工作时使用的主要故障排除工具。此报告显示无代理流的各个阶段，包括脚本上传完成、脚本上传失败、脚本执行完成等事件，以及任何已知的失败原因（如有）。

您可以从两个位置访问无代理终端安全评估故障排除：

- 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 (Operations) > 实时日志 (Live Logs)**，然后在要进行故障排除的客户端旁边的**终端安全评估状态 (Posture Status)** 列上单击三个竖点。
- 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断 (Diagnostic) > 常规工具 (General Tools) > 无代理终端安全评估故障排除 (Agentless Posture Troubleshooting)**。

无代理终端安全评估故障排除工具会收集指定客户端的无代理终端安全评估活动。**无代理终端安全评估流 (Agentless Posture Flow)** 会启动终端安全评估并显示当前活动客户端与思科 ISE 之间的所有交互。**仅下载客户端日志 (Only Download Client Logs)** 会创建一些日志，其中包含最长 24 小时的客户端终端安全评估流。客户端可以随时删除日志。收集完成后，可以导出日志的 ZIP 文件。

报告

在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 终端和用户 (Endpoints and Users) > 无代理终端安全评估 (Agentless Posture)**，查看运行无代理终端安全评估的所有终端。

安全评估管理设置

您可以从全局为 Admin 门户配置安全评估服务。您可以从思科通过 Web 将更新自动下载至思科 ISE 服务器。之后您还可以离线手动更新思科 ISE。此外，如果已在客户端上安装 AnyConnect或 Web 代理之类的代理，则可以为客户端提供终端安全评估和补救服务。客户端代理定期向思科 ISE 更新客户端的合规性状态。登录并成功完成安全状态要求评估之后，客户端代理显示带有一个链接的对话框，要求最终用户遵守网络使用的条款和条件。您可以使用此链接为您的企业网络定义最终用户在可以访问您的网络之前必须接受的网络使用信息。

客户端安全评估要求

要创建终端安全评估要求，请执行以下操作：

1. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)**。
2. 从任何要求行末尾处的**编辑 (Edit)** 下拉列表中，选择**插入新要求 (Insert New Requirement)**。
3. 输入所需的详细信息，并点击**完成 (Done)**。

下表介绍**客户端终端安全评估要求 (Client Posture Requirements)** 窗口中的字段。

表 1: Posture Requirement

字段名称	使用指南
Name	输入要求名称。
Operating Systems	选择操作系统。 点击加号 [+]，将多个操作系统关联到策略。 点击减号 [-]，从策略删除操作系统。

字段名称	使用指南
合规性模块	从**合规性模块 (Compliance Module)** 下拉列表中，选择所需的合规性模块： • 4.x 或更高版本：支持反恶意软件、磁盘加密、补丁管理和 USB 条件。 • 3.x 或更低版本：支持防病毒、反间谍软件、磁盘加密和补丁管理条件。 • 任意版本：支持文件、服务、注册、应用和复合条件。 有关合规性模块的详细信息，请参阅合规性模块，第 24 页。
终端安全评估类型	从**终端安全评估类型 (Posture Type)** 下拉列表中，选择所需的终端安全评估类型。 • AnyConnect：部署 AnyConnect 代理以监控和实施需要客户端交互的思科 ISE 策略。 • AnyConnect 隐身：部署 AnyConnect 代理以监控和实施思科 ISE 安全评估策略，无需任何客户端交互。 • 临时代理：在客户端运行的临时可执行文件，用于检查合规性状态。
Conditions	从列表中选择一个条件。 您也可以点击 Action 图标，将其与要求关联起来，创建任何用户定义的条件。创建用户定义的条件时，不能编辑已关联的母操作系统。 pr_WSUSRule 是虚拟的复合条件，在终端安全评估要求中与已关联的 Windows Server Update Services (WSUS) 补救一起使用。您必须使用严重性级别选项，将已关联的 WSUS 补救操作配置为验证 Windows 更新。当此要求无法满足时，Windows 客户端上的代理会根据您在 WSUS 补救中定义的严重性级别执行 WSUS 补救操作。 pr_WSUSRule 在复合条件列表页面看不到。您只能从条件构件选择 pr_WSUSRule。

字段名称	使用指南
Remediation Actions	从列表中选择一个补救操作。 您也可以创建补救操作，并将其与要求相关联。 您可以在文本框中写下所有补救类型，传达给代理用户。除了补救操作，还可以向代理用户传达关于客户端不合规的消息。 **仅消息文本**选项可以向代理用户传达不合规的信息。它还提供可选说明，让用户联系服务中心获得详细信息，或者手动修复客户端。在这种情况下，代理不会触发任何补救操作。

相关主题

配置安全评估的可接受使用政策，第 20 页
创建客户端安全评估要求，第 69 页

客户端的计时器设置

您可以为用户设置计时器，用于进行补救、从一个状态过渡到另一个状态，以及控制登录成功屏幕。

我们建议配置具有补救计时器和网络过渡延迟计时器的代理配置文件，以及用于控制客户端计算机登录成功屏幕的计时器，以便这些设置以策略为基础。您可以在 **AnyConnect 安全评估配置文件**窗口 (**Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **AnyConnect Posture Profile**)。

但是，当没有任何配置为与客户端调配策略相匹配的代理配置文件时，您可以使用**常规设置 (General Settings)** 配置窗口中的设置（**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**）。

设定补救计时器，使客户端在指定时间内补救

您可以配置计时器，使客户端在指定时间内补救。在初始评估期间，客户端不符合配置的终端安全评估策略，代理将等待客户端在补救计时器中配置的时间内补救。如果客户端无法在指定时间内补救，则客户端代理将向终端安全评估运行服务发送报告，然后，客户端过渡到不合规状态。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**管理** > **系统** > **设置** > **终端安全评估** > **常规设置** 。

步骤 2 在**补救计时器 (Remediation Timer)** 字段中，以分钟为单位输入时间值。

默认值为 4 分钟。有效范围为 1 至 300 分钟。

步骤 3 点击**保存**。

设置网络转换延迟计时器，使客户端实现转换

可以为客户端配置计时器，使客户端在指定的时间内，使用网络过渡延迟计时器从一种状态过渡到另一种状态，这是完成授权更改 (CoA) 所必需的操作。当客户端在终端安全评估成功和失败期间需要获得新的 VLAN IP 地址时，可能需要更长的延迟时间。终端安全评估成功时，思科 ISE 允许客户端在使用网络过渡延迟计时器指定的时间内从未知模式过渡为合规模式。终端安全评估失败时，思科 ISE 允许客户端在计时器指定的时间内从未知模式过渡为非合规模式。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**管理** > **系统** > **设置** > **终端安全评估** > **常规设置** 。

步骤 2 以秒为单位，在 **Network Transition Delay** 字段中输入时间值。

默认值为 3 秒。有效范围为 2 至 30 秒。

步骤 3 点击**保存**。

将登录成功窗口设置为自动关闭

成功完成安全状态评估之后，客户端代理会显示一个临时网络访问屏幕。用户需要点击登录窗口中的**确定 (OK)** 按钮将其关闭。您可以设置计时器以在指定时间之后自动关闭此登录屏幕。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**管理** > **系统** > **设置** > **终端安全评估** > **常规设置** 。

步骤 2 选中 **Automatically Close Login Success Screen After** 复选框。

步骤 3 在 **Automatically Close Login Success Screen After** 复选框旁边的字段中以秒为单位输入时间值。

有效范围为 0 至 300 秒。如果时间设置为零，则 AnyConnect 不显示登录成功界面。

步骤 4 点击**保存**。

设置非代理设备的终端安全评估状态

您可以配置在非代理设备上运行的终端的安全评估状态。当 Android 设备和 Apple 设备（如 iPod、iPhone 或 iPad）连接到支持思科 ISE 的网络时，这些设备采用默认安全评估状态设置。

安全评估运行期间找不到匹配的客户端调配策略时，还可以将这些设置应用到在 Windows 和 Macintosh 操作系统中运行的终端，同时将终端重定向到客户端调配门户。

开始之前

要在一个终端上强制实施策略，必须配置相应的客户端调配策略（代理安装包）。否则，该终端的安全评估状态会自动反映默认设置。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**管理** > **系统** > **设置** > **终端安全评估** > **常规设置** 。

步骤 2 从**默认终端安全评估 (Default Posture Status)** 下拉列表中， 选择**合规 (Compliant)** 或**不合规 (Noncompliant)** 选项。

步骤 3 点击**保存**。

安全评估租约

您可以将思科 ISE 配置为在每次用户登录您的网络时执行安全评估或按指定的间隔执行安全评估。有效范围为 1 至 365 天。

此配置仅适用于使用 AnyConnect 代理进行安全评估的用户。

当终端安全评估租约处于活动状态时，思科 ISE 将使用上次已知的终端安全评估状态，并且不会连接到终端以检查合规性。但是，当终端安全评估租约到期时，思科 ISE 不会自动触发终端的重新身份验证或终端安全评估。因为正在使用相同的会话，所以终端将保持相同的合规性状态。当终端重新进行身份验证时，将运行终端安全评估，并重置终端安全评估租用时间。

使用案例场景示例：

- 用户登录终端，使其终端安全评估符合设置为一天的终端安全评估租约。
- 四小时后，用户从终端注销（终端安全评估租约现在还剩 20 小时）。
- 一小时后，用户再次登录。现在，终端安全评估租约还剩19小时。最后已知的终端安全评估状态为合规。因此为用户提供访问权限，无需在终端上运行终端安全评估。
- 四小时后，用户注销（终端安全评估租约现在还剩 15 小时）。
- 14 小时后，用户登录。终端安全评估租约还剩一个小时。最后已知的终端安全评估状态为合规。系统会为用户提供访问权限，无需在终端上运行终端安全评估。
- 一小时后，终端安全评估租约到期。用户仍连接到网络，因为正在使用同一用户会话。
- 一小时后，用户注销（会话与用户绑定，但不与计算机绑定，因此计算机可以留在网络上）。
- 一小时后，用户登录。由于终端安全评估租约已到期且已启动新的用户会话，因此计算机会执行终端安全评估，结果会发送到思科 ISE，在此使用案例中，终端安全评估租约计时器会重置为一天。

定期重新评估

只有成功完成合规性安全评估的客户端才可以执行定期重新评估 (PRA)。如果您网络上的客户端不合规，则不会执行 PRA。

只有在终端处于合规状态下，PRA 才有效和适用。策略服务节点检查相关策略，根据配置中定义的客户端角色编制实施 PRA 的要求。如果找到 PRA 配置匹配项，策略服务节点在发出 CoA 请求之前会用 PRA 配置中为客户端定义的 PRA 属性对客户端代理做出响应。客户端代理根据配置中指定的间隔定期发送 PRA 请求。如果 PRA 成功或继续执行 RPA 配置中配置的操作，客户端会保持合规状态。如果客户端未能满足 PRA 要求，则客户端会从合规状态变为不合规状态。

即使是安全评估状态重新评估请求，PostureStatus 属性也会在 PRA 请求中将当前安全状态显示为合规状态而不是未知状态。监控报告中也会更新 PostureStatus。

当终端安全评估租约未到期时，终端根据访问控制列表 (ACL) 变为合规，并启动 PRA。如果 PRA 失败，终端视为不合规，并重置终端安全评估租约。

注释 在 PSN 故障切换期间，不支持 PRA。PSN 故障切换后，您必须在客户端上启用重新扫描或启用终端安全评估。

配置定期重新评估

您可以配置仅定期重新评估已成功通过合规性安全状态评估的客户端。您可以为系统中定义的用户身份组配置各项 PRA。

开始之前

- 确保每个定期重新评估 (PRA) 配置都有分配给该配置的唯一组或用户身份组的唯一组合。
- 您可以分配 role_test_1 和 role_test_2，这是 PRA 配置独有的两个角色。您可以使用逻辑运算符组合这两个角色并将 PRA 配置分配为两个角色的唯一组合。例如，role_test_1 OR role_test_2。
- 确保两个 PRA 配置没有相同的用户身份组。
- 如果已有用户身份组为任何 *(Any)* 的 PRA 配置，您就无法创建其他 PRA 配置，除非您执行以下操作之一：
  - 用 Any 用户组更新现有 PRA 配置以反映 *Any* 之外的用户身份组。
  - 删除“*Any*”用户身份组的现有 PRA 配置。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **重新评估 (Reassessments)**。

步骤 2 点击**添加 (Add)**。

步骤 3 修改**新重新评估配置 (New Reassessment Configuration)** 窗口中的值以创建新 PRA。

步骤 4 点击 **Submit** 以创建 PRA 配置。

安全评估故障排除设置

下表介绍“终端安全评估故障排除”(Posture troubleshooting) 窗口上的字段，您可以使用该窗口查找并解决网络中的终端安全评估问题。 在思科 ISE GUI 中，单击**菜单** 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)** > **终端安全状态故障排除 (Posture Troubleshooting)**。

表 *2:* 终端安全评估故障排除设置

字段名称	使用指南
搜索并选择一个需要进行故障排除的安全评估事件	
用户名	输入要过滤的用户名。
MAC 地址	输入要过滤的 MAC 地址，请使用格式：xx-xx-xx-xx-xx-xx
Posture Status	选择要过滤的身份验证状态：
Failure Reason	输入故障原因，或者点击 **Select** 以从列表中选择故障原因。点击 **Clear** 以清除故障原因。
Time Range	选择时间范围。使用在此时间范围内创建的 RADIUS 身份验证记录。
Start Date-Time:	（仅当您选择自定义时间范围时可用）输入开始日期和时间，或点击日历图标选择开始日期和时间。日期应为 *mm/dd/yyyy* 格式，而时间应为 *hh:mm* 格式。
End Date-Time:	（仅当您选择自定义时间范围时可用）输入结束日期和时间，或点击日历图标选择结束日期和时间。日期应为 *mm/dd/yyyy* 格式，而时间应为 *hh:mm* 格式。
Fetch Number of Records	选择要显示的记录数：10、20、50、100、200、500
搜索结果	
时间	事件时间
状态	终端安全评估状态
用户名	与事件关联的用户名
MAC 地址	系统的 MAC 地址
Failure Reason	事件的失败原因

相关主题

安全评估故障排除工具，第 80 页

安全评估常规设置

下表介绍“终端安全评估常规设置”(Posture General Settings) 窗口中的字段，可以使用此窗口配置补救时间和终端安全评估状态等常规终端安全评估设置。要查看此处窗口，请单击**菜单**图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

常规终端安全评估设置

- **补救计时器 (Remediation Timer)**：输入开始补救前等待的时间。默认值为 4 分钟。有效范围为 1 至 300 分钟。
- **网络过渡延迟 (Network Transition Delay)**：以秒为单位输入时间值。默认值为 3 秒。有效范围为 2 至 30 秒。
- **默认终端安全评估状态 (Default Posture Status)**：选择**合规 (Compliant)** 或**不合规 (Noncompliant)**。在连接到网络时，非代理设备会处于此状态。
- **自动关闭登录成功屏幕前等待 (Automatically Close Login Success Screen After)**：选中此复选框可在指定的时间过后自动关闭成功登录屏幕。可以配置计时器以自动关闭登录屏幕。有效范围为 0 至 300 秒。如果将时间设置为零，则客户端上的代理不会显示成功登录屏幕。
- **连续监控间隔**：指定 AnyConnect 开始发送监控数据之前的时间间隔。 对于应用和硬件条件，默认值为 5 分钟。
- **无代理终端安全评估客户端超时**：指定在终端安全评估检查被视为失败之前等待的时间。
- **每次运行后删除无代理插件 (Remove Agentless Plugin)**：启用此设置可在运行无代理终端安全评估后从客户端删除代理。我们强烈禁用此功能，以便下载的插件可以重复使用，直到有新版本可用。禁用此选项有助于减少网络流量。
- **隐身模式下的可接受使用策略 (Acceptable Use Policy)**：如果不符合贵公司的网络使用条款和条件，请在隐身模式下选择**阻止 (Block)** 以将客户端转移到不合规的终端安全评估状态。

安全评估租约

- **每当用户连接到网络时执行终端安全评估 (Perform posture assessment every time a user connects to the network)**：选择此选项可在用户每次连接网络时启动终端安全评估
- **每 n 天执行一次终端安全评估 (Perform posture assessment every n days)**：选择此选项可在指定天数过后启动终端安全评估，即使客户端的状态已评估为“合规”也是如此。
- **缓存最后已知终端安全评估合规状态 (Cache Last Known Posture Compliant Status)**：选中此复选框可使思科 ISE 缓存终端安全评估的结果。默认情况下，此字段处于禁用状态。
- **最后已知终端安全评估合规状态 (Last Known Posture Compliant Status)**：仅当已选中**缓存最后已知终端安全评估合规状态 (Cache Last Known Posture Compliant Status)** 时，此设置才适用。

思科 ISE 会在此字段中指定的时间量内缓存终端安全评估结果。有效值为 1 到 30 天，或 1 到 720 小时，或 1 到 43200 分钟。

相关主题

安全评估管理设置，第 8 页
安全评估租约，第 12 页
设定补救计时器，使客户端在指定时间内补救，第 10 页
设置网络转换延迟计时器，使客户端实现转换，第 11 页
将登录成功窗口设置为自动关闭，第 11 页
设置非代理设备的终端安全评估状态，第 11 页

将安全评估更新下载至思科 ISE

安全评估更新包括针对适用于 Windows 和 Macintosh 操作系统的防病毒和反间谍软件的一系列预定义的检查、规则和支持图表，以及思科支持的操作系统信息。您还可以从您包含最新更新档案的本地系统上的文件离线更新思科 ISE。

当您首次在您的网络上部署思科 ISE 时，您可以从 Web 下载安全评估更新。此过程通常大约需要 20 分钟。初次下载后，您可以将思科 ISE 配置为自动验证和下载增量更新。

在初始安全评估更新期间，思科 ISE 仅创建一次默认安全评估策略、要求和补救。如果您删除所创建的这些内容，在后续手动或计划更新期间思科 ISE 不会再进行创建。

开始之前

要确保能够访问合适的远程位置以便将安全评估资源下载至思科ISE，您可能需要验证您已按照“在思科 ISE 中指定代理设置”的说明为您的网络配置了正确的代理设置。

您可以使用“安全评估更新”(Posture Update) 窗口从 Web 动态下载更新。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全评估 (Posture)** > **更新 (Updates)**。

步骤 2 选择 **Web** 选项以动态地下载更新。

步骤 3 点击**设置为默认值 (Set to Default)** 为**更新源 URL (Update Feed URL)** 字段设置思科默认值。

如果您的网络限制 URL 重定向功能（例如通过代理服务器）而且您在访问上述 URL 时遇到了问题，请尝试将您的思科 ISE 也指向相关主题中的备选 URL。

步骤 4 在**安全评估更新 (Posture Updates)** 窗口更改相应值。

步骤 5 点击**现在更新 (Update Now)** 以从思科下载更新。

更新后，“安全评估更新”(Posture Updates) 窗口显示当前思科更新版本信息，作为对“安全评估更新”(Posture Updates) 窗口“更新信息”(Update Information) 部分下的更新的验证。

步骤 6 点击 **Yes** 以继续操作。

思科 ISE 离线更新

当从思科 ISE 设备通过互联网直接访问 Cisco.com 不可用或者安全策略不允许时，您可以使用离线更新选项来下载客户端调配和安全状态安全评估更新。

要下载离线客户端调配资源：

步骤 1 前往：https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0。

步骤 2 提供登录凭证。

步骤 3 导航至 Cisco 身份识别服务引擎下载窗口，然后选择版本。

以下离线安装程序包可供下载：

- **win_spw-**<*version*>**-isebundle.zip** — 适用于 Windows 的离线 SPW 安装程序包
- **mac-spw-**<*version*>**.zip** — 适用于 Mac OS X 的离线 SPW 安装程序包
- **compliancemodule-**<*version*>**-isebundle.zip** — 离线合规性模块安装程序包
- **macagent-**<*version*>**-isebundle.zip** — 离线 Mac 代理安装程序包
- **webagent-**<*version*>**-isebundle.zip** — 离线 Web 代理安装程序包

步骤 4 单击**下载 (Download)** 或**加入购物车 (Add to Cart)**。

有关将下载的安装程序包添加至思科 ISE 的详细信息，请参阅 《思科身份服务引擎管理员指南》中的“从本地计算机添加客户端调配资源”一节。

您可以使用安全状态安全评估更新，以离线方式通过本地系统上的存档为 Windows 和 Mac 操作系统更新检查、操作系统信息以及防病毒和反间谍软件支持图表。

要进行离线更新，请确保存档文件版本与配置文件中的版本一致。您可以在配置思科 ISE 后并且想要为状态策略服务启用动态更新时使用离线状态更新。

要下载离线安全状态安全评估更新：

步骤 1 转至https://www.cisco.com/web/secure/spa/posture-offline.html。

步骤 2 将 **posture-offline.zip** 文件保存到本地系统。此文件用于为 Windows 和 Mac 操作系统更新操作系统信息、检查、规则以及防病毒和反间谍软件支持图表。

步骤 3 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture)**。

步骤 4 点击箭头查看安全状态安全评估的设置。

步骤 5 单击**更新 (Update)**。
将显示**终端安全评估更新 (Posture Updates)** 窗口。

步骤 6 单击**离线 (Offline)** 选项。

步骤 7 单击**浏览 (Browse)** 可从您系统中的本地文件夹查找存档文件 (posture-offline.zip)。

注释 **待更新文件 (File to Update)** 字段为必填。您可以选择包含适当文件的单个存档文件 (.zip)。不支持 .zip 之外的其他存档文件，例如 .tar 和 .gz。

步骤 8 点击**立即更新 (Update Now)**。

自动下载安全评估更新

在初始更新后，您可以将思科 ISE 配置为检查更新并自动下载这些更新。

开始之前

- 您起初应已下载安全评估更新来将思科 ISE 配置为检查更新并自动下载这些更新。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全评估 (Posture)** > **更新 (Updates)**。

步骤 2 在**终端安全评估更新 (Posture Updates)** 窗口中，选中**从初始延迟开始自动检查更新 (Automatically check for updates starting from initial delay)** 复选框。

步骤 3 以 hh:mm:ss 格式输入初始延迟时间。

思科 ISE 在初始延迟时间结束后开始检查更新。

步骤 4 输入时间间隔（以小时为单位）。

思科 ISE 从初始延迟时间起按指定间隔将更新下载到部署。

步骤 5 点击**保存**。

安全评估可接受使用政策配置设置

下表介绍了“终端安全评估可接受使用策略配置”(Posture Acceptable Use Policy Configurations) 窗口中的字段，可以使用此窗口为终端安全评估配置可接受使用策略。要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **可接受使用政策 (Acceptable Use Policy)**。

表 *3:* 安全评估 ***AUP*** 配置设置

字段名称	使用指南
Configuration Name	输入要创建的 AUP 配置的名称。
Configuration Description	输入要创建的 AUP 配置的说明。
“向代理用户显示 AUP”(Show AUP to Agent users)（仅适用于 **Windows**）	选中后，系统会在身份验证和终端安全评估成功后，向用户显示您的网络的网络使用条款和条件的链接。
为 AUP 消息使用 URL (Use URL for AUP message)	选中后，必须在“AUP URL”字段中输入 AUP 消息的 URL。
为 AUP 消息使用文件 (Use file for AUP message)	选中后，必须浏览至文件位置并以压缩格式上传文件。此文件必须在顶层包含 index.html。 除 index.html 文件以外，该 .zip 文件还可包含其他文件和子目录。这些文件可以使用 HTML 标签相互引用。
AUP URL	输入 AUP 的 URL，用户必须在身份验证和安全评估成功后访问该 URL。
AUP File	浏览至文件并将其上传到思科 ISE 服务器。它应是压缩文件，并且应在顶层包含 index.html 文件。
Select User Identity Groups	针对 AUP 配置选择唯一用户身份组或用户身份组的唯一组合。 创建 AUP 配置时，请注意以下事项： • 安全评估 AUP 不适用于访客流程 • 两个配置不会共同具有任何用户身份组 • 如果您要使用用户身份组“Any”创建 AUP 配置，则要先删除所有其他 AUP 配置 • 如果使用用户身份组“Any”创建 AUP 配置，则无法使用唯一用户身份组或用户身份组的唯一组合创建其他 AUP 配置。要使用除 Any 以外的用户身份组创建 AUP 配置，请先删除具有用户身份组“Any”的现有 AUP 配置，或者使用唯一用户身份组或用户身份组的唯一组合更新具有用户身份组“Any”的现有 AUP 配置。
Acceptable use policy configurations - Configurations list	列出现有 AUP 配置以及与 AUP 配置关联的最终用户身份组。

相关主题

配置安全评估的可接受使用政策，第 20 页

配置安全评估的可接受使用政策

登录并对客户端成功完成安全状态评估之后，客户端代理会显示一个临时网络访问屏幕。此屏幕包含可接受使用政策 (AUP) 的链接。当用户点击此链接时，系统会将用户重定向至显示网络使用条款和条件的页面，用户必须阅读并理解这些条款和条件。

每个可接受使用政策配置都必须具有唯一的用户身份组或唯一的用户身份组组合。思科 ISE 找到第一个匹配的用户身份组，然后与显示 AUP 的客户端代理通信。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **可接受使用政策 (Acceptable Use Policy)**。

步骤 2 点击**添加 (Add)**。

步骤 3 修改**新可接受使用政策配置 (New Acceptable Use Policy Configuration)** 窗口中的值。

步骤 4 点击**提交**。

安全评估条件

安全评估条件可以是以下任何一个简单条件：文件、注册表、应用、服务或字典条件。这些简单条件中的一个或多个条件构成可与安全评估要求相关联的复合条件。

当您首次在您的网络上部署思科 ISE 时，您可以从 Web 下载安全评估更新。此过程称为初始安全评估更新。

在初始安全评估更新后，思科 ISE 还会创建思科定义的简单条件与复合条件。思科定义的简单条件以 pc_ 作为前缀，复合条件以 pr_ 作为前缀。

您也可以将思科 ISE 配置为由于通过 Web 进行动态安全评估更新而定期下载思科定义的条件。您不能删除或编辑思科定义的安全评估条件。

用户定义的条件或思科定义的条件同时包含简单条件与复合条件。

简单安全评估条件

您可以使用**安全评估导航 (Posture Navigation)** 窗格管理以下简单条件：

- 文件条件：在客户端上检查文件的存在性、文件的日期以及文件的版本的条件。
- 注册条件：在客户端上检查注册表项的存在性或注册表项的值的条件。
- 应用条件：在客户端上检查应用（进程）是否在运行的条件。

注释 如果进程已安装并正在运行，则用户合规。但是，应用条件的逻辑正好相反；如果应用未安装且未运行，则最终用户合规。如果应用已安装并正在运行，则最终用户不合规。

- 服务条件：检查服务是否在客户端上运行的条件。
- 词典条件：检查带某个值的词典属性的条件。
- USB 条件：检查 USB 大量存储设备是否存在的条件。

创建简单安全评估条件

可以创建文件、注册表、应用、服务和字典简单条件，在终端安全评估策略或其他复合条件中可以使用这些条件。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)**。

步骤 2 选择以下任意一项：**文件 (File)**、**注册表 (Registry)**、**应用 (Application)**、**服务 (Service)** 或**字典简单条件 (Dictionary Simple Condition)**。

步骤 3 点击**添加 (Add)**。

步骤 4 在字段中输入适当的值。

步骤 5 点击**提交**。

复合安全评估条件

复合条件由一个或多个简单条件或复合条件组成。您可以利用以下复合条件定义安全评估策略。

- 复合条件：包含一个或多个简单条件或文件、注册表、应用或服务条件类型的复合条件
- 防病毒复合条件：包含一个或多个 AV 条件或 AV 复合条件
- 反间谍软件复合条件：包含一个或多个 AS 条件或 AS 复合条件
- 字典复合条件：包含一个或多个字典简单条件或字典复合条件
- 防恶意软件条件：包含一个或多个 AM 条件。

创建复合安全评估条件

您可以创建复合条件用于安全评估和验证的状态策略。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policyp)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **复合条件 (Compound Conditions)** > **添加 (Add)**。

步骤 2 输入适当的字段值。

步骤 3 点击 **Validate Expression** 验证条件。

步骤 4 点击**提交**。

字典复合条件设置

表 *4:* 字典复合条件设置

字段名称	使用指南
Name	输入要创建的字典复合条件的名称。
Description	输入要创建的字典复合条件的说明。
Select Existing Condition from Library	通过从策略要素库选择预定义的条件来定义表达式，或在后续步骤中将临时属性/值对添加到表达式中。
Condition Name	选择已从策略要素库中创建的字典简单条件。
Expression	Expression 会根据从 Condition Name 下拉列表选择的选项进行更新。
AND 或 OR 运算符	选择 AND 或 OR 运算符可逻辑组合可从策略要素库添加的字典简单条件。 点击 **Action** 图标可执行以下操作： • Add Attribute/Value • Add Condition from Library • Delete
Create New Condition (Advance Option)	从各种系统或用户定义的字典中选择属性。 还可以在后续步骤中从策略要素库中添加预定义条件。

字段名称	使用指南
Condition Name	选择已创建的字典简单条件。
Expression	从 Expression 下拉列表可以创建字典简单条件。
Operator	选择要将值关联到属性的运算符。
值	输入要关联到字典属性的值，或者从下拉列表中选择一个值。

相关主题

复合安全评估条件，第 21 页
创建复合安全评估条件，第 22 页

用于在 Windows 客户端中启用自动更新的预定义条件

pr_AutoUpdateCheck_Rule 是思科预定义条件，会下载至“复合条件”(Compound Conditions) 窗口。您可以通过此条件检查在 Windows 客户端上是否启用了自动更新功能。如果 Windows 客户端未满足此要求，则网络访问控制 (NAC) 代理会强制 Windows 客户端启用（补救）自动更新功能。这种补救完成后，Windows 客户端就符合安全评估。如果在 Windows 客户端上未启用自动更新功能，您在安全评估策略中关联的 Windows 更新会覆盖 Windows 管理员设置。

预配置的防病毒和反间谍软件条件

思科 ISE 在“AV 复合条件”(AV Compound Condition) 和“AS 复合条件”(AS Compound Condition) 窗口加载预配置的防病毒和反间谍软件复合条件（在适用于 Windows 和 Macintosh 操作系统的防病毒和反间谍软件支持图表中定义）。如果指定的防病毒和反间谍软件产品存在于全部客户端，则这些复合条件则可以选中。此外，您还可以在思科 ISE 中创建新的防病毒和反间谍软件复合条件。

防病毒和反间谍软件支持图表

思科 ISE 使用防病毒和反间谍软件支持图表，此图表在各供应商产品的定义文件中提供最新版本和日期。用户必须定期访问防病毒和反间谍软件支持图表来查看更新。防病毒和反间谍软件供应商会经常更新防病毒和反间谍软件定义文件，请在各供应商产品的定义文件中查找最新版本和日期。

每次系统更新防病毒和反间谍软件支持图表来反映对新防病毒和反间谍软件供应商、产品及其发行版本的支持时，代理都会收到新的防病毒和反间谍软件库。这可以帮助代理支持新增的防病毒和反间谍软件。代理检索到此支持信息后，会从定期更新的 se-checks.xml 文件（此文件随 se-templates.tar.gz 档案中的 se-rules.xml 文件一起发布）检查最新定义信息，然后确定客户端是否符合安全评估策略。根据防病毒和反间谍软件库对于特定防病毒或反间谍软件产品的支持情况，系统会向代理发送相应的要求，在安全评估验证过程中来验证客户端上具体的防病毒和反间谍软件产品是否存在。

有关 ISE 终端安全评估代理支持的防病毒和防恶意软件产品的详细信息，请参阅思科 AnyConnect ISE 终端安全评估支持图表：思科 ISE 兼容性指南。

您可以在创建防恶意软件终端安全评估条件时验证最低合规性模块版本。更新终端安全评估源后，请选择**工作中心 (Work Centers) > 终端安全评估 (Posture) > 策略元素 (Policy Elements) > 防恶意软件条件 (Anti-Malware Condition)**，然后选择**操作系统 (Operating System)** 和**供应商 (Vendor)** 以查看支持图表。

注释 某些防恶意软件终端安全解决方案（如FireEye、Cisco AMP、Sophos等）需要通过网络访问各自的集中服务才能正常运行。对于此类产品，AnyConnect ISE 终端安全评估模块（或 OESIS 库）要求终端能够连接互联网。建议在这些在线代理的终端安全评估预评估期间允许此类终端访问互联网（如果未启用离线检测）。签名定义条件可能不适用于此类情况。

合规性模块

合规性模块包含一个字段列表，例如由支持思科 ISE 安全评估条件的 OPSWAT 提供的供应商名称、产品版本、产品名和属性。

供应商会经常更新定义文件中的产品版本和日期，因此，您必须频繁轮询合规性模块的新情况，以找到每个供应商产品的定义文件中的最新版本和日期。每次更新合规性模块以反映对新供应商、产品和版本的支持时， AnyConnect代理都会收到一个新库。从而使AnyConnect代理可支持新增产品。AnyConnect代理检索到此支持信息后，会从定期更新的se-checks.xml文件（此文件随se-templates.tar.gz档案中的se-rules.xml文件一起发布）检查最新定义信息，然后确定客户端是否符合安全评估策略。根据库文件对于特定防病毒、反间谍软件、防恶意软件、磁盘加密或补丁管理产品的支持情况，系统会向AnyConnect代理发送相应的要求，在安全评估验证过程中验证客户端上是否存在这些产品以及它们的状态。

合规性模块可从 Cisco.com 获取。

下表列出了支持和不支持 ISE 终端安全评估策略的 OPSWAT API 版本。对于支持版本 3 和 4 的代理，存在不同的策略规则。

表 *5: OPSWAT API* 版本

终端安全评估条件	合规性模块版本
OPSWAT	
防病毒软件	3.x 或更低版本
反间谍软件	3.x 或更低版本
反恶意软件	4.x 或更高版本
磁盘加密	3.x 或更低版本以及 4.x 或更高版本
补丁管理	3.x 或更低版本以及 4.x 或更高版本
USB	4.x 或更高版本

终端安全评估条件	合规性模块版本
非 OPSWAT	
文件	任何版本
应用	任何版本
复合	任何版本
注册表	任何版本
服务	任何版本

注释

- 请务必为版本 3.x 或更低版本以及版本 4.x 或更高版本创建单独的终端安全评估策略，因为预计客户端可能已安装以上任何一个版本。
- 为合规性模块 4.x 和 Cisco AnyConnect 4.3 及更高版本提供了 OESIS 版本 4 支持。但是，AnyConnect 4.3 同时支持 OESIS 版本 3 和版本 4 策略。
- ISE 2.1 和更高版本支持第 4 版合规性模块。

检查安全评估合规性

步骤 1 登录思科 ISE 并访问控制板。

步骤 2 在**安全评估合规性 (Posture Compliance)** Dashlet 中，将光标悬停于堆积条形图或迷你图上。

工具提示提供详细的信息。

步骤 3 展开数据类别，了解更多信息。

步骤 4 展开 **Posture Compliance** dashlet。

系统将显示详细的实时报告。

注释 您可以在**情景可视性 (Context Visibility)** 窗口中查看终端安全评估合规报告。导航到**情景可视性 (Context Visibility) > 终端 (Endpoints) > 合规 (Compliance)**。此窗口根据**合规状态 (Compliance Status)**、**位置 (Location)**、**终端 (Endpoints)** 和**应用（按类别）(Applications by Categories)** 显示不同的图表。

您可能会看到没有任何活动会话的终端的安全评估状态。例如，如果终端的上一已知安全评估状态为**合规 (Compliant)**，即使终端会话已终止，在收到终端的下一次更新之前，**情景可视性 (Context Visibility)** 窗口中的状态仍然保持为**合规 (Compliant)**。在终端被删除或清除之前，安全评估状态始终保留在**情景可视性 (Context Visibility)** 窗口中。

创建补丁管理条件

可以创建用于检查选定供应商的补丁管理产品状态的策略。

例如，可以创建一个条件，用以检查微软系统中心配置管理器 (SCCM) 客户端版本 4.x 软件产品是否安装在终端上。

注释 思科 ISE 和 AnyConnect 支持的版本：

- 思科 ISE 版本 1.4 及更高版本
- AnyConnect 版本 4.1 及更高版本

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **补丁管理条件 (Patch Management Condition)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**名称 (Name)** 和**说明 (Description)** 字段中输入条件名称和说明。

步骤 4 从**操作系统 (Operating System)** 下拉字段中选择适当的操作系统。

步骤 5 从下拉列表中选择**合规性模块 (Compliance Module)**。

步骤 6 从下拉列表中选择**供应商名称 (Vendor Name)**。

步骤 7 选择**检查类型 (Check Type)**。

步骤 8 从**检查已安装的补丁 (Check patches installed)** 下拉列表中选择适当的补丁。

步骤 9 点击**提交**。

相关主题

补丁管理条件设置，第 47 页
添加补丁管理补救，第 67 页

创建磁盘加密条件

您可以创建一个策略以检查终端是否与指定的数据加密软件兼容。

例如，您可以创造条件检查 C 盘是否在终端加密。如果 C 盘没有加密，终端会收到一个非合规性通知，同时 ISE 会记录一条消息。

开始之前

要执行以下任务，您必须是超级管理员或策略管理员。只有当您使用 AnyConnect ISE 终端安全评估代理时，您才可以将磁盘加密条件与终端安全评估需求进行关联。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **磁盘加密条件 (Disk Encryption Condition)**。

步骤 2 单击**添加**。

步骤 3 在**磁盘加密条件 (Disk Encryption Condition)** 窗口中，在字段中输入适当的值。

步骤 4 点击**提交**。

安全评估条件设置

本节介绍用于安全评估的简单条件和复合条件。

文件条件设置

下表介绍**文件条件 (File Conditions)** 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **文件条件 (File Condition)**。

表 *6:* 文件条件设置

字段名称	**Windows** 操作系统使用指南	**MacOS** 使用指南	**Linux** 操作系统使用指南
Name	输入文件条件的名称。	输入文件条件的名称。	输入文件条件的名称。
Description	输入文件条件的说明。	输入文件条件的说明。	输入文件条件的说明。

字段名称	**Windows** 操作系统使用指南	**MacOS** 使用指南	**Linux** 操作系统使用指南

Operating System	选择应向其应用文件条件的任何 Windows 操作系统。	选择应向其应用文件条件的任何 macOS。	选择应向其应用文件条件的任何 Linux 操作系统。可提供以下选项：
			• **Ubuntu**
			  • **18.04**
			  • **20.04**
			• **Red Hat**
			  • **7.5**
			  • **7.9**
			  • **8.1**
			  • **8.2**
			  • **8.3**
			• **SUSE**
			  • **12.3**
			  • **12.4**
			  • **12.5**
			  • **15.0**
			  • **15.1**
			  • **15.2**

字段名称	**Windows** 操作系统使用指南	**MacOS** 使用指南	**Linux** 操作系统使用指南
文件类型	选择以下选项之一： • **FileDate**：检查系统中是否存在带有特定文件创建或文件修改日期的文件。 • **FileExistence**：检查系统中是否存在文件。 • **FileVersion**：检查系统中是否存在特定版本的文件。 • **CRC32**：使用校验和函数检查文件的数据完整性。 • **SHA-256**：使用哈希函数检查文件的数据完整性。	选择以下选项之一： • **FileDate**：检查系统中是否存在带有特定文件创建或文件修改日期的文件。 • **FileExistence**：检查系统中是否存在文件。 • **CRC32**：使用校验和函数检查文件的数据完整性。 • **SHA-256**：使用哈希函数检查文件的数据完整性。 • **PropertyList**：检查 plist 文件（例如，loginwindow.plist）中的属性值。	选择以下选项之一： • **FileDate**：检查系统中是否存在带有特定文件创建或文件修改日期的文件。 • **FileExistence**：检查系统中是否存在文件。 • **CRC32**：使用校验和函数检查文件的数据完整性。 • **SHA-256**：使用哈希函数检查文件的数据完整性。

字段名称	**Windows** 操作系统使用指南	**MacOS** 使用指南	**Linux** 操作系统使用指南
数据类型和运算符	NA	（仅当您选择的文件类型为 **PropertyList** 时可用）选择要在 plist 文件中搜索的数据类型或密钥值。每种数据类型包含一组运算符。 • **未指定**：检查是否存在指定的密钥。输入一个运算符 (Exists, DoesNotExist)。 • **数字**：检查数字数据类型的指定密钥。输入运算符（等于、不等于、大于、小于、大于或等于和小于或等于）和值。 • **字符串**：检查字符串数据类型的指定密钥。输入运算符（等于、不等于、等于（忽略大小写）、以其开始、不以其开始、包含、不包含、以其结尾和不以其结尾）和值。 • **版本**：检查作为版本字符串的指定密钥的值。输入运算符（低于、高于、等与）和值。	不适用
属性名称	NA	（仅当您选择的文件类型为 **PropertyList** 时可用）输入密钥名称，例如，BuildVersionStampAsNumber	不适用

字段名称	Windows 操作系统使用指南	MacOS 使用指南	Linux 操作系统使用指南
File Path	选择以下选项之一： • **ABSOLUTE_PATH**：检查文件的完全限定路径中的文件。例如，C:\<directory>\file name。对于其他设置，请仅输入文件名。 • **SYSTEM_32**：检查 C:\WINDOWS\system32 目录中的文件。输入文件名。 • **SYSTEM_DRIVE**：检查 C:\ 驱动器中的文件。输入文件名。 • **SYSTEM_PROGRAMS**：检查 C:\Program Files 中的文件。输入文件名。 • **SYSTEM_ROOT**：检查 Windows 系统的根路径中的文件。输入文件名。 • **USER_DESKTOP**：检查指定的文件是否显示在 Windows 用户的桌面上。输入文件名。 • **USER_PROFILE**：检查文件是否显示在 Windows 用户的本地配置文件目录中。输入文件路径。	选择以下选项之一： • **Root**：检查根 (/) 目录中的文件。输入文件路径。 • **Home**：检查主 (~) 目录中的文件。输入文件路径。	选择以下选项之一： • **Root**：检查根 (/) 目录中的文件。输入文件路径。 • **Home**：检查主 (~) 目录中的文件。输入文件路径。

字段名称	**Windows** 操作系统使用指南	**MacOS** 使用指南	**Linux** 操作系统使用指南
File Date Type	（仅当您选择的文件类型为 **FileDate** 时可用）选择 **Creation Date** 或 **Modification Date**。	（仅当您选择的文件类型为 **FileDate** 时可用）选择 **Creation Date** 或 **Modification Date**。	（仅当您选择的文件类型为 **FileDate** 时可用）选择 **Creation Date** 或 **Modification Date**。
文件操作符	文件操作符 **(File Operator)** 选项会根据在 **文件类型 (File Type)** 中选择的设置而更改。选择适当的设置： **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • 范围 **(Within)**：最近 *n* 天。有效范围为 1 到 300。 **FileExistence** • **Exists** • **DoesNotExist** **FileVersion** • **EarlierThan** • **LaterThan** • **EqualTo**	文件操作符 **(File Operator)** 选项会根据在 **文件类型 (File Type)** 中选择的设置而更改。选择适当的设置： **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • 范围 **(Within)**：最近 *n* 天。有效范围为 1 到 300。 **FileExistence** • **Exists** • **DoesNotExist**	文件操作符 **(File Operator)** 选项会根据在 **文件类型 (File Type)** 中选择的设置而更改。选择适当的设置： **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • 范围 **(Within)**：最近 *n* 天。有效范围为 1 到 300。 **FileExistence** • **Exists** • **DoesNotExist**
文件 **CRC** 数据	（仅当您选择的**文件类型 (File Type)** 为 **CRC32** 时可用）您可以输入校验和值（例如，0x3c37fec3）来检查文件完整性。校验和值应以 0x（一个十六进制整数）开头。	（仅当您选择的**文件类型 (File Type)** 为 **CRC32** 时可用）您可以输入校验和值（例如，0x3c37fec3）来检查文件完整性。校验和值应以 0x（一个十六进制整数）开头。	（仅当您选择的**文件类型 (File Type)** 为 **CRC32** 时可用）您可以输入校验和值（例如，0x3c37fec3）来检查文件完整性。校验和值应以 0x（一个十六进制整数）开头。

字段名称	**Windows** 操作系统使用指南	**MacOS** 使用指南	**Linux** 操作系统使用指南
文件 **SHA-256** 数据	（仅当您选择的**文件类型 (File Type)** 为 **SHA-256** 时可用）您可以可以输入 64 字节十六进制哈希值来检查文件完整性。	（仅当您选择的**文件类型 (File Type)** 为 **SHA-256** 时可用）您可以可以输入 64 字节十六进制哈希值来检查文件完整性。	（仅当您选择的**文件类型 (File Type)** 为 **SHA-256** 时可用）您可以可以输入 64 字节十六进制哈希值来检查文件完整性。
日期和时间	（仅当您选择的**文件类型 (File Type)** 为 **FileDate** 时可用）以 mm/dd/yyyy 和 hh:mm:ss 格式输入客户端系统的日期和时间。	（仅当您选择的**文件类型 (File Type)** 为 **FileDate** 时可用）以 mm/dd/yyyy 和 hh:mm:ss 格式输入客户端系统的日期和时间。	（仅当您选择的**文件类型 (File Type)** 为 **FileDate** 时可用）以 mm/dd/yyyy 和 hh:mm:ss 格式输入客户端系统的日期和时间。

相关主题

简单安全评估条件，第 20 页
复合安全评估条件，第 21 页
创建终端安全评估条件，第 76 页

防火墙条件设置

防火墙条件检查终端上是否运行有特定防火墙产品。支持的防火墙产品列表基于 OPSWAT 支持图表。在初始安全评估和定期重新评估 (PRA) 期间，您可以实施策略。

思科 ISE 为 Windows 和 macOS 提供默认防火墙条件。默认情况下会禁用这些条件。

字段名称	使用指南
Name	输入防火墙条件的名称。
说明	输入对防火墙条件的说明。
合规性模块	选择所需的合规性模块。 • 4.x 或更高版本 • 3.x 或更高版本 • 任何版本
操作系统	检查终端上是否安装有必需的防火墙产品。您可以选择 Windows OS 或 macOS。

字段名称	使用指南
Vendor	从下拉列表中选择一个供应商名称。供应商的防火墙产品，及其检查类型显示于**所选供应商的产品 (Products for Selected Vendor)** 表中，可从该表检索。表中所列内容根据所选操作系统而变化。
Check Type	已启用 (Enabled)：检查终端上是否运行了特定防火墙。通过参考 **Products for Selected Vendor** 列表，验证供应商产品是否支持所选检查类型。

注册表条件设置

下表介绍了“注册表条件”(Registry Conditions) 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **注册表条件 (Registry Condition)**。

表 *7:* 注册表条件设置

字段名称	使用指南
Name	输入注册表条件的名称。
Description	输入对注册表条件的说明。
Registry Type	选择一个预定义设置作为注册表类型。
Registry Root Key	选择一个预定义设置作为注册表根项。
Sub Key	输入不带反斜杠的子项（“\”）以检查在 Registry Root Key 中指定的路径中的注册表项。 例如，SOFTWARE\Symantec\Norton AntiVirus\version 将检查以下路径中的注册表项： HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
Value Name	（仅在选择 **RegistryValue** 或 **RegistryValueDefault** 作为 Registry Type 的情况下可用）为 **RegistryValue** 输入要检查的注册表项名称值。 这是 **RegistryValueDefault** 的默认字段。

字段名称	使用指南
Value Data Type	（仅在选择 **RegistryValue** 或 **RegistryValueDefault** 作为 Registry Type 的情况下可用）选择一个以下设置： • **未指定 (Unspecified)**：检查注册表项值是否存在。此选项仅可用于 **RegistryValue**。 • **数值 (Number)**：检查注册表项值中指定的数值 • **字符串 (String)**：检查注册表项值中的字符串 • **版本 (Version)**：检查注册表项值中的版本
Value Operator	选择相应的设置。
Value Data	（仅在选择**RegistryValue** 或 **RegistryValueDefault** 作为 Registry Type 的情况下可用）根据您在 **Value Data Type** 中选择的数据类型输入注册表项的值。
操作系统	选择应该应用此注册表条件的操作系统。

相关主题

简单安全评估条件，第 20 页
复合安全评估条件，第 21 页

连续的终端属性监控

可以使用 AnyConnect 代理连续监控不同终端属性，以确保在安全评估期间观察动态变化。这会提高终端的整体可视性，并帮助您根据其行为创建安全评估策略。AnyConnect 代理监控安装并运行在终端上的应用。您可以打开和关闭此功能，并配置应监控数据的频率。默认情况下，每 5 分钟收集一次数据，并存储在数据库中。在初始安全评估过程中，AnyConnect 报告正在运行和已安装的应用的完整列表。在初始安全评估后， AnyConnect 代理每 X 分钟扫描一次应用，并将其与最后一次扫描的差异发送到服务器。服务器显示正在运行和已安装的应用的完整列表。

应用条件设置

安装在终端上的应用的应用条件查询。这有助于您了解终端上分布的软件的汇聚可视性。

下表介绍了**应用条件 (Application Conditions)** 窗口中的字段。要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **策略元素 (Policy Elements)** > **应用条件 (Application Condition)** > **添加 (Add)**。

字段名称	使用指南
Name	输入应用条件的名称。
Description	输入应用条件的说明。
操作系统	选择应用条件适用的操作系统。可提供以下选项： • **Windows 的 ISE 安全评估代理** • **Mac OSX** • **Linux**
合规性模块	选择以下选项之一： • **4.x 或更高版本** • **3.x 或更低版本** • **任何版本**
检查方式	选择以下选项之一： • **进程 (Process)**：选择此选项可检查进程是否正在终端上运行。 • **应用 (Application)**：选择此选项可检查应用是否正在终端上运行。 注释 对于 Linux 操作系统，仅显示**进程 (Process)** 选项。
进程名称	（仅当选择**进程 (Process)** 作为**检查方式 (Check By)** 选项时可用）输入所需的进程名称。
Application Operator	（仅当选择**进程 (Process)** 作为**检查方式 (Check By)** 选项时可用）选择以下选项之一： • **正在运行 (Running)**：选择此选项可检查应用是否正在终端上运行。 • **未在运行 (Not Running)**：选择此选项可检查某应用是否未在终端上运行。

字段名称	使用指南
应用状态 **(Application State)**	（仅当选择**应用 (Application)** 作为**检查方式 (Check By)** 选项时可用）选择以下选项之一： • **已安装 (installed)**：选择此选项可检查客户端中是否安装了恶意应用。如果找到恶意应用，则触发补救操作。 • **正在运行 (Running)**：选择此选项可检查应用是否正在终端上运行。
调配分类依据 **(Provision By)**	（仅当选择**应用 (Application)** 作为**检查方式 (Check By)** 选项时可用）选择以下选项之一： • **一切 (Everything)**：您可以选择所有列出的类别，如浏览器、补丁管理等。 • **名称 (Name)**：您应至少选择一个类别。例如，如果选择**浏览器 (Browser)** 类别，则会在**供应商 (Vendor)** 下拉列表中显示相应的供应商。 • **类别 (Category)**：您可以选中一个或多个类别，如防恶意软件、备份、浏览器或数据存储。 **注释** 类别会通过 OPSWAT 库动态更新。

您可以在**情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **合规性 (Compliance)** 窗口查看各个终端已安装和正在运行的应用数量。

主页 (Home) > **摘要 (Summary)** > **合规性 (Compliance)** 窗口显示接受终端安全状态评估并且合规的终端的百分比。

服务条件设置

下表介绍**服务条件 (File Conditions)** 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **服务条件 (Service Condition)**。

表 *8:* 服务条件设置

字段名称	使用指南
Name	输入服务条件的名称。
Description	输入对服务条件的说明。

字段名称	使用指南
操作系统	选择应该应用此服务条件的操作系统。您可以选择不同版本的 Windows OS 或 macOS 操作系统。
服务名称	输入以 root 身份运行的后台守护程序或用户代理服务的名称，例如，com.apple.geod。 AnyConnect 代理使用 **sudo launchctl list** 命令验证服务条件。
服务类型	选择 AnyConnect 应检查的服务类型以确保客户端合规性： • **后台守护程序 (Daemon)**：检查客户端中后台守护程序的指定列表中是否存在特定服务，例如扫描客户端设备中的恶意软件。 • **用户代理 (User Agent)**：检查客户端中用户服务的指定列表中是否存在特定服务，例如当检测到恶意软件时运行的服务。 • **后台守护程序或用户代理 (Daemon or User Agent)**：检查后台守护程序或用户代理服务列表中是否存在特定服务。
Service Operator	选择您希望在客户端中检查的服务状态： • **Windows OS**：检查服务**正在运行 (Running)**还是**未运行 (Not Running)**。 • **Mac OSX**：检查服务**已加载 (Loaded)**、**未加载 (Not Loaded)**、**已加载并运行 (Loaded and Running)**、**已加载并含有退出代码 (Loaded with Exit Code)** 还是**已加载并运行或含有退出代码 (Loaded & running or with Exit code)**。

相关主题

简单安全评估条件，第 20 页
复合安全评估条件，第 21 页

安全评估复合条件设置

下表介绍**复合条件 (Compound Conditions)** 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **复合条件 (Compound Condition)**。

表 *9:* 安全评估复合条件设置

字段名称	使用指南
Name	输入您要创建的复合条件的名称。
说明 **(Description)**	输入对您要创建的复合条件的说明。
操作系统	选择一个或多个 Windows 操作系统。这允许关联应用该条件的 Windows 操作系统。
括号 **( )**	点击此括号以将以下简单条件类型的两个简单条件组合起来：文件、注册表、应用和服务条件。
(&)：AND 运算符（用“&”表示 AND 运算符，不需要加引号）	您可以在复合条件中使用 AND 运算符（与号 [&]）。例如，输入 **Condition1 & Condition2**。
(|)：OR 运算符（用“|”表示 OR 运算符，不需要加引号）	您可以在复合条件中使用 OR 运算符（小竖线 [|]）。例如，输入 **Condition1 & Condition2**。
(!)：NOT 运算符（用“!”表示 NOT 运算符，不需要加引号）	您可以在复合条件中使用 NOT 运算符（感叹号 [!]）。例如，输入 **Condition1 & Condition2**。
简单条件	从以下类型的简单条件列表中选择：文件、注册表、应用和服务条件。 您还可以从对象选择器创建文件、注册表、应用和服务条件的简单条件。 在**操作 (Action)** 按钮上点击快速选择器（向下箭头）以创建文件、注册表、应用和服务条件的简单条件。

相关主题

安全评估条件，第 20 页
创建复合安全评估条件，第 22 页

防病毒条件设置

在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **防病毒条件 (Anti-Virus Condition)**。

字段名称	使用指南
Name	输入要创建的防病毒条件的名称。
Description	输入要创建的防病毒条件的说明。

字段名称	使用指南
操作系统	选择用于检查客户端的防病毒程序安装情况，或检查条件所适用的最新防病毒定义文件更新的操作系统。
供应商 (Vendor)	从下拉列表中选择供应商。通过选择供应商，系统会检索供应商的防病毒产品和版本，这些信息显示在 Products for Selected Vendor 表中。
Check Type	选择是检查客户端的防恶意软件程序安装情况，还是检查最新定义文件更新。
Installation	选择此选项，只检查客户端的防病毒程序安装情况。
Definition	选择此选项，只检查客户端的防病毒产品的最新定义文件更新。

Products for Selected Vendor

从表中选择防病毒产品。根据在“新防病毒条件”(New Anti-virus Condition) 页面中选择的供应商，此表会检索有关供应商的防病毒产品和版本、其提供的补救支持、最新定义文件日期及其版本的信息。

通过从表中选择产品，可以检查防病毒程序的安装情况，或检查最新防病毒定义文件日期，及其最新版本。

注释 从**基准条件 (Baseline Condition)** 或**高级条件 (Advanced Condition)** 中，只能为每个防病毒产品配置一个条件。

基准条件 (Baseline Condition)

字段名称	指南
最低版本	（仅当您更新操作系统和供应商时可用）从下拉列表中选择防病毒程序的最小版本。 该检查会在网络上的所有终端上实施网络策略，以符合防病毒程序的最小版本条件。
最高版本 (Maximum Version)	当您更新终端安全评估源时，系统会自动修订防病毒软件的最高版本。
最低合规性模块版本 (Minimum Compliance Module Version)	最低合规性模块版本会从 AnyConnect更新。

高级条件 (Advance Condition)

字段名称	指南
请针对最新防病毒定义文件版本进行检查（如适用）	（仅当选择 Definition 检查类型时可用）如果最新防病毒定义文件版本由于思科 ISE 中的终端安全评估更新变为可用，则选择此选项以针对最新防病毒定义文件版本检查客户端的防病毒定义文件版本。否则，此选项使您可以针对思科 ISE 中的最新定义文件日期检查客户端的定义文件日期。
Allow virus definition file to be（已启用）	（仅当选择 Definition 检查类型时可用）选择此选项，检查客户端的防病毒定义文件版本和最新防病毒定义文件日期。最新定义文件日期不能早于在下一个字段（days older than 字段）定义的产品的最新防病毒定义文件日期或当前系统日期。 如果未选中，则思科 ISE 使您可以使用 Check against latest AV definition file version, if available 选项，只检查防病毒定义文件的版本。
早于的天数 **(Days Older Than)**	定义客户端的最新防病毒定义文件日期可以早于产品的最新防病毒定义文件日期或当前系统日期的天数。默认值为零 (0)。
最新文件日期 **(Latest File Date)**	选择此选项，检查客户端的防病毒定义文件日期，该日期可以早于在 days older than 字段中定义的天数。 如果将天数设置为默认值 (0)，则客户端的防病毒定义文件日期不应早于产品的最新防病毒定义文件日期。
当前系统日期 **(Current System Date)**	选择此选项，检查客户端的防病毒定义文件日期，该日期可以早于在 days older than 字段中定义的天数。 如果将天数设置为默认值 (0)，则客户端的防病毒定义文件日期不应早于当前系统日期。

相关主题

复合安全评估条件，第 21 页
预配置的防病毒和反间谍软件条件，第 23 页
防病毒和反间谍软件支持图表，第 23 页

反间谍软件复合条件设置

下表介绍**作为复合条件 (AS Compound Conditions)** 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **AS 复合条件 (AS Compound Condition)**。

表 *10:* 反间谍软件复合条件设置

字段名称	使用指南
Name	输入您要创建的反间谍软件复合条件的名称。
Description	输入对您要创建的反间谍软件复合条件的说明。
Operating System	选择一个操作系统，该操作系统应允许检查客户端上的反间谍软件程序的安装，或检查应用该条件的最新反间谍软件定义文件更新。
供应商	从下拉列表中选择供应商。选择供应商会检索其反间谍软件产品和版本，这些信息显示于 Products for Selected Vendor 表中。
Check Type	选择您是想要在客户端上检查安装，还是检查最新定义文件更新。
Installation	选择您是否只想检查客户端上的反间谍软件程序的安装。
Definition	选择您是否只想检查客户端上的反间谍软件软件的最新定义文件更新。
允许病毒定义文件 (Allow virus definition file to be)（已启用）	当您创建的是反间谍软件定义检查类型时，请选中此复选框；当您创建的是反间谍软件安装检查时，请禁用此复选框。 如果选中此复选框，系统将允许您在客户端上检查反间谍软件定义文件版本和最新反间谍软件定义文件日期。最新的定义文件日期不能早于您在 days older than 字段中定义的距离当前系统日期的天数。 如果未选中此复选框，您就只能选择反间谍软件定义文件的版本，因为未选中 Allow virus definition file to be 复选框。
早于的天数 (Days Older Than)	定义在客户端上最新的反间谍软件定义文件日期可以早于当前系统日期的天数。默认值为零 (0)。

字段名称	使用指南
当前系统日期 (Current System Date)	选择在客户端上检查反间谍软件定义文件日期，此日期可以早您在 days older than 字段中定义的天数。 如果您将此天数设置为默认值 (0)，则客户端上的反间谍软件定义文件日期不得早于当前系统日期。
选定供应商的产品	从表中选择反间谍软件产品。根据您在 New Anti-spyware Compound Condition 页面选择的供应商，此表检索关于其反间谍软件产品及版本的信息、其所提供的补救支持、最新定义文件日期及其版本。 您可以通过从表中选择产品，检查反间谍软件程序的安装，或检查最新反间谍软件定义文件日期，及其最新版本。

相关主题

复合安全评估条件，第 21 页
预配置的防病毒和反间谍软件条件，第 23 页
防病毒和反间谍软件支持图表，第 23 页

防恶意软件条件设置

防恶意软件条件是反间谍软件和防病毒条件的组合，由 OESIS 版本 4.x 或更高版本合规性模块支持。

要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **终端安全评估元素 (Posture Elements)** > **条件 (Conditions)** > **防恶意软件 (Antimalware)**。

注释 建议您手动更新已安装的防恶意软件产品，使其至少有一次最新的定义。否则，使用 AnyConnect 对防恶意软件定义的安全评估检查可能会失败。

字段名称	使用指南
Name	输入防恶意软件条件的名称。
Description	输入防恶意软件条件的说明。
Operating System	选择一操作系统，以检查客户端的防恶意软件程序安装情况，或检查条件所适用的最新防恶意软件定义文件更新。 它支持 Windows、macOS 和 Linux 操作系统。

字段名称	使用指南
供应商	从下拉列表中选择供应商。**所选供应商的产品 (Products for Selected Vendor)** 表会显示该供应商提供的防恶意软件产品、版本、最新定义日期、最新定义版本和最低合规性模块版本。
Check Type	选择以下选项之一： • **安装 (Installation)**：选择此选项只会检查客户端的防恶意软件程序安装情况。 • **定义 (Definition)**：选择此选项以便只检查客户端防恶意软件产品的最新定义文件更新。
请针对最新 **AV** 定义文件版本进行检查（如适用）	（仅当选择**定义 (Definition)** 检查类型时可用）如果最新防恶意软件定义文件版本由于思科 ISE 中的终端安全评估更新变为可用，则选择此选项以便针对最新防恶意软件定义文件版本，来检查客户端的防恶意软件定义文件版本。否则，此选项使您可以针对思科 ISE 中的最新定义文件日期检查客户端的定义文件日期。 只有在思科 ISE 中所选产品的**最新定义日期 (Latest Definition Date)** 或**最新定义版本 (Latest Definition Version)** 字段内列有数值，该检查才有效。否则，必须使用**当前系统日期 (Current System Date)** 字段。
允许病毒定义文件 **(Allow Virus Definition File to be)**	（仅当选择**定义 (Definition)** 检查类型时可用）选择此选项以便检查客户端的防恶意软件定义文件版本和最新防恶意软件定义文件日期。最新的定义文件日期不能早于您在**早于的天数 (Days Older Than)** 字段中定义的天数。 如果未选中，则思科 ISE 允许您使用**请针对最新 AV 定义文件版本进行检查”(Check against latest AV definition file version)** 选项，只检查防恶意软件定义文件的版本。
早于的天数 **(Days Older Than)**	定义客户端的最新防恶意软件定义文件日期可以早于产品的最新防恶意软件定义文件日期或当前系统日期的天数。默认值为零。

字段名称	使用指南
最新文件日期 (Latest File Date)	选择此选项，以便定义客户端的最新防恶意软件定义文件日期可以早于产品的最新防恶意软件定义文件日期或当前系统日期的天数。 如果将该天数设置为默认值，则客户端的防恶意软件定义文件日期不应早于产品的最新防恶意软件定义文件日期。 只有在思科 ISE 中所选产品的**最新定义日期 (Latest Definition Date)** 字段列有数值，该检查才有效。否则，必须使用**当前系统日期 (Current System Date)** 字段。
当前系统日期 (Current System Date)	选择此选项，以便定义在客户端上最新的反间谍软件定义文件日期可以早于当前系统日期的天数。 如果将天数设置为默认值，则客户端的防恶意软件定义文件日期不应早于当前系统日期。

相关主题

复合安全评估条件，第 21 页

字典简单条件设置

下表介绍了**字典简单条件 (Dictionary Simple Conditions)** 窗口上的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **字典简单条件 (Dictionary Simple Condition)**。

表 *11:* 字典简单条件设置

字段名称	使用指南
Name	输入您要创建的字典简单条件的名称。
Description	输入对您要创建的字典简单条件的说明。
Attribute	从字典选择属性。
Operator	选择将值与您所选择的属性关联的运算符。
Value	输入您想要与字典属性关联的值，或从下拉列表选择预定义值。

相关主题

简单安全评估条件，第 20 页
创建简单安全评估条件，第 21 页

字典复合条件设置

表 *12:* 字典复合条件设置

字段名称	使用指南
Name	输入要创建的字典复合条件的名称。
Description	输入要创建的字典复合条件的说明。
Select Existing Condition from Library	通过从策略要素库选择预定义的条件来定义表达式，或在后续步骤中将临时属性/值对添加到表达式中。
Condition Name	选择已从策略要素库中创建的字典简单条件。
Expression	Expression 会根据从 Condition Name 下拉列表选择的选项进行更新。
AND 或 OR 运算符	选择 AND 或 OR 运算符可逻辑组合可从策略要素库添加的字典简单条件。 点击 **Action** 图标可执行以下操作： • Add Attribute/Value • Add Condition from Library • Delete
Create New Condition (Advance Option)	从各种系统或用户定义的字典中选择属性。 还可以在后续步骤中从策略要素库中添加预定义条件。
Condition Name	选择已创建的字典简单条件。
Expression	从 Expression 下拉列表可以创建字典简单条件。
Operator	选择要将值关联到属性的运算符。
值	输入要关联到字典属性的值，或者从下拉列表中选择一个值。

相关主题

复合安全评估条件，第 21 页
创建复合安全评估条件，第 22 页

补丁管理条件设置

下表介绍了**补丁管理条件** (Patch Management Conditions) 窗口上的字段。要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **补丁管理条件 (Patch Management Condition)** 。

表 *13:* 补丁管理条件

字段名称	使用指南
Name	输入补丁管理条件的名称。
Description	输入对补丁管理条件的说明。
操作系统	选择操作系统以检查终端上补丁管理软件的安装，或检查应用该条件的最新补丁管理定义文件更新。您可以选择 Windows，macOS 或 Linux OS。您还可以选择不止一个版本的操作系统以创建补丁管理条件。
Vendor Name	从**供应商名称 (Vendor Name)** 下拉列表中选择一个供应商。根据您的选择，补丁管理产品及其支持的版本、检查类型和最低合规模块支持详细信息会显示在**选定供应商产品 (Products for Selected Vendor)** 表中。表中所列内容根据所选操作系统而变化。

字段名称	使用指南
Check Type	选择以下选项之一： • **安装 (Installation)**：检查是否在终端上安装了所选产品。所有供应商均支持此检查类型。 注释 对于思科临时代理，只能在**要求 (Requirements)** 窗口中查看包含**安装 (Installation)** 检查类型的补丁管理条件。 • **已启用 (Enabled)**：检查是否在终端上启用了所选产品。通过参考 **Products for Selected Vendor** 列表，验证供应商产品是否支持所选检查类型。 • **最新 (Up to Date)**：检查所选产品是否缺失补丁。通过参考 **Products for Selected Vendor** 列表，验证供应商产品是否支持所选检查类型。 单击**所选供应商的产品 (Products for Selected Vendor)** 下拉列表，以查看您在**供应商名称 (Vendor Name)** 字段中指定的供应商支持的产品列表。例如，如果您选择了供应商 A，该供应商有两个产品，分别是为产品 1 和产品 2。产品 1 可能会支持**启用 (Enabled)** 选项，而产品 2 可能不支持此选项。或者，如果产品 1 不支持任何一个检查类型，它将灰显。 注释 （适用于思科 ISE 2.3 及更高版本以及 AnyConnect 4.5 及更高版本）如果在 SCCM 的补丁管理条件中选择**最新 (Up to Date)** 检查类型，则思科 ISE： 1. 使用 Microsoft API 检查指定严重性级别的当前安全补丁。 2. 触发对于此缺失安全补丁的补丁管理补救。

字段名称	使用指南
检查已安装的补丁	（仅当您选择**最新 (Up To Date)** 检查类型时可用。）可以为缺失的补丁配置严重性级别，然后根据严重性进行部署。选择以下选项之一： • **仅严重级别 (Critical Only)**：检查部署中的终端上是否安装了严重级别软件补丁。 • **重要和严重级别 (Important and Critical)**：检查部署中的终端上是否安装了重要和严重级别软件补丁。 • **中级、重要和严重级别 (Moderate, Important, and Critical)**：检查部署中的终端上是否安装了中级、重要和严重级别软件补丁。 • **低级到严重级别 (Low To Critical)**：检查部署中的终端上是否安装了低级、中级、重要和严重级别软件补丁。 • **全部 (All)**：安装所有严重性级别的缺失补丁。

相关主题

创建补丁管理条件，第 26 页

磁盘加密条件设置

下表介绍了**磁盘加密条件 (Disk Encryption Condition)** 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **磁盘加密条件 (Disk Encryption Condition)**。

表 ***14:*** 磁盘加密条件设置

字段名称	使用指南
Name	输入要创建的磁盘加密条件的名称。
Description	输入对磁盘加密条件的说明。
操作系统	选择要进行磁盘加密检查的终端的一个操作系统。您可以选择 Windows OS 或 macOS。您还可以选择一个操作系统的多个版本，以创建磁盘加密条件。

字段名称	使用指南
供应商名称	从下拉列表中选择一个供应商名称。**所选供应商的产品 (Products for Selected Vendor)** 表中检索并显示供应商的数据加密产品、其支持的版本、加密状态检查和最低的兼容性模块支持。表中所列内容根据所选操作系统而变化。

位置	仅当**所选供应商的产品 (Products for Selected Vendor)**部分有项目被勾选时才启用。请选择以下任意一个选项：
	• **特定位置**：检查指定的磁盘驱动器是否已在终端加密（例如，Windows 操作系统的 C:），或指定的卷标是否已加密（例如，macOS 的 Mackintosh HD）。
	• **系统位置**：检查默认的 Windows 操作系统驱动器或 macOS 硬盘驱动器是否已在终端加密。
	• **所有内部驱动器 (All Internal Drives)**：检查内部驱动器。包括已挂载和加密的所有硬盘以及所有内部分区。不包括只读驱动器、系统恢复磁盘/分区、引导分区、网络分区和终端外部的不同物理磁盘驱动器（包括但不限于通过 USB 和 Thunderbolt 连接的磁盘驱动器）。经过验证的加密软件产品包括：
	  • Bit-locker-6.*x*/10.*x*
	  • Windows 7 上的 Checkpoint 80.*x*

加密状态	当所选的产品不支持加密状态检查时，“加密状态”(Encryption State) 复选框为禁用状态。仅该复选框被选中时，才会显示中继器。您可以选择“完全加密”(Fully Encrypted) 选项来检查客户端的磁盘驱动器是否为完全加密。 如果您创建一个条件（例如，TrendMicro），并选择两个供应商，其中一个的加密状态为“是”，另一个的加密状态为“否”，则“加密状态”(Encryption State) 将被禁用，因为其中有一个供应商的加密状态为“否”。 **注释** 您可以点击中继器以添加更多位置，并且每个位置之间的关系为逻辑 && 运算符。

相关主题

创建磁盘加密条件，第 26 页

USB 条件设置

下表介绍了 **USB 条件 (USB Condition)** 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **策略元素 (Policy Elements)** > **USB**。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **USB 条件 (USB Condition)**

USB 检查是一个预定义条件且仅支持 Windows 操作系统。

表 *15: USB* 条件设置

字段名称	使用指南
Name	USB_Check
Description	思科预定义检查
操作系统	Windows 的 ISE 安全评估代理
合规性模块	用于版本 4.x（及更高版本）的支持 ISE 终端安全评估状态合规性模块的只显示字段。

相关主题

简单安全评估条件，第 20 页

硬件属性条件设置

在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **硬件属性条件 (Hardware Attributes Condition)**，以便访问**硬件属性条件 (Hardware Attributes Condition)** 窗口。下表介绍了**硬件属性条件 (Hardware Attributes Condition)** 窗口中的字段。

字段名称	使用指南
Name	Hardware_Attributes_Check：分配给条件的默认名称。
Description	从客户端收集硬件属性的思科预定义检查。
操作系统	Windows 或 Mac OS
合规性模块	4.x 或更高版本

终端安全评估外部数据源条件

您可以配置条件，将终端 UDID 与外部数据源进行匹配。目前，仅支持 Active Directory。ISE 不包括终端安全评估代理将 UDID 发送到 Active Directory 所需的脚本。

配置安全评估策略

安全评估策略是与一个或多个身份组和操作系统关联的状态要求的集合。词典属性是可与身份组和操作系统一起使用以便为设备定义不同策略的可选条件。

思科 ISE 提供一个为不合规的设备配置宽限时间的选项。如果发现设备不合规，思科 ISE 会在安全评估结果缓存中查找之前已知的良好状态，并为设备提供相应的宽限时间。在宽限期内，设备将获得网络访问权限。您可以按分钟、小时或天（最多 30 天）配置宽限时段。

有关详细信息，请参阅《ISE 安全评估规范性部署指南》中的“安全评估策略”一节。

注释 如果在**策略 (Policy)** > **终端安全评估 (Posture)**的“其他条件”(Other Conditions) 下配置了“终端策略”(Endpoint policies) 和“逻辑配置文件”(Logical Profiles)，则分析器策略评估将不起作用。

注释

- 当宽限期延长或缩短时，如果设备再次经历安全评估流程（例如，如果启用了**延迟通知 (Delayed Notification)** 选项，选择了**重新扫描 (Re-Scan)** 选项，则设备将断网或重新连网），新宽限期和延迟通知将应用。
- 宽限期不适用于临时代理。
- Linux 代理不支持宽限期。
- 当设备匹配多个终端安全评估策略（每个策略有不同的宽限期）时，设备将获取在不同策略中配置的最大宽限期。
- 设备处于宽限期时，不会显示“可接受使用政策”(AUP)。

开始之前

- 您必须了解可接受使用政策 (AUP)。
- 您必须了解定期重新评估 (PRA)。
- 您必须使用 AnyConnect 代理 4.7 或更高版本才能查看与合规性相关的通知。有关配置 AnyConnect 代理的详细信息，请参阅创建 AnyConnect 配置，第 106 页。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **终端安全评估 (Posture)** 或 **工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **终端安全评估策略 (Posture Policy)**。

步骤 2 使用下拉箭头添加新策略。

步骤 3 要编辑配置文件，请双击策略或点击行末的“编辑”(Edit)。

步骤 4 从**规则状态 (Rule Status)** 下拉列表中，选择**已启用 (Enabled)**或**已禁用 (Disabled)**。

步骤 5 选择**策略选项 (Policy Options)** 下的下拉列表，并以分钟，小时或天为单位指定**宽限期设置 (Grace Period Settings)**。

有效值为：

- 1 到 90 天
- 1 到 2,160 小时
- 1 到 129,600 分钟

默认情况下，此设置处于禁用状态。

注释 即使终端安全评估结果不合规，如果发现设备之前已合规且缓存尚未过期，则系统会在**宽限期设置 (Grace Period Settings)** 中指定的时间段内授予设备访问权限。

步骤 6 （可选）拖动名为**延迟通知 (Delayed Notification)** 的滑块延迟宽限期提示，直到宽限期消耗特定百分比后再显示给用户。例如，通知延迟期设置为 50% 且配置的宽限期为 10 分钟，则思科 ISE 将在 5 分钟后检查安全评估状态，如果发现终端不合规，则显示宽限期通知。如果终端状态为合规，则不会显示宽限期通知。如果通知延迟时间设置为 0%，系统会在宽限期开始时立即提示用户以解决问题。但在宽限期过期之前，终端会被授予访问权限。此字段的默认值为 0%。有效范围为 0 到 95%。

步骤 7 在**规则名称 (Rule Name)** 字段中，输入策略的名称。

注释 最好将每项要求作为单独的规则来配置安全评估策略，以避免意外结果。

步骤 8 从**身份组 (Identity Groups)** 列中，选择所需的身份组。

您可以根据用户或终端身份组来创建安全评估策略。

步骤 9 从**操作系统 (Operating Systems)** 列中，选择操作系统。

步骤 10 从**合规性模块 (Compliance Module)** 列中，选择所需的合规性模块：

- **4.x 或更高版本 (4.x or Later)**：支持反恶意软件、磁盘加密、补丁管理和 USB 条件。
- **3.x 或更低版本 (3.x or Earlier)**：支持防病毒、反间谍软件、磁盘加密和补丁管理条件
- **任何版本 (Any Version)**：支持文件、服务、注册表、应用和复合条件。

步骤 11 从**终端安全评估类型 (Posture Type)** 列中，选择终端安全评估类型 (Posture Type)。

- **AnyConnect** - 部署 AnyConnect 代理以监视和实施需要客户端干预的思科 ISE 策略。
- **AnyConnect Stealth** - 部署 AnyConnect 代理以监控和实施思科 ISE 安全评估策略，而无需任何客户端干预。
- **临时代理 (Temporal Agent)** - 在客户端上运行以检查合规性状态的临时可执行文件。

步骤 12 在 **Other Conditions** 中，您可以添加一个或多个词典属性，然后以简单或复合条件的方式将它们保存到词典中。

注释 您在**终端安全评估策略 (Posture Policy)** 窗口中创建的词典简单条件和复合条件在配置授权策略时不显示。

步骤 13 在**要求 (Requirements)** 字段中指定要求。

步骤 14 点击**保存**。

配置 AnyConnect 工作流程

要配置 AnyConnect 代理，请在思科 ISE 中执行以下步骤：

步骤 1 创建 AnyConnect 代理配置文件。

步骤 2 为 AnyConnect 软件包创建 an AnyConnect 配置。

步骤 3 创建客户端调配策略。

步骤 4 （可选）创建自定义终端安全评估条件。

步骤 5 （可选）创建自定义补救操作。

步骤 6 （可选）创建自定义终端安全评估要求。

步骤 7 创建终端安全评估策略。

步骤 8 配置客户端调配策略。

步骤 9 创建授权配置文件。

步骤 10 配置授权策略。

步骤 11 下载并启动 AnyConnect。

a) 连接到 SSID。
b) 启动浏览器，您将重定向至客户端调配门户。
c) 点击**开始**。这样将检查 AnyConnect 代理是否已安装并正在运行。
d) 点击**这是我第一次访问 (This Is My First Time Here)**。
e) 选择 **点击此处下载并启动 AnyConnect**。
f) 分别保存适用于 Windows 或 macOS 的思科 Anyconnect .exe 或 .dmg 文件。对于 Windows，请运行 .exe 文件；对于 macOS，请双击 .dmg 文件并运行应用。

注释 思科 ISE 不支持 ARM64 版本的 AnyConnect 用于 AnyConnect 终端安全评估流程。确保不要在客户端调配策略中使用 ARM64版本的 AnyConnect ，否则可能会导致客户端故障。如果 AnyConnect 由于此问题无法正常工作，请重新启动客户端。

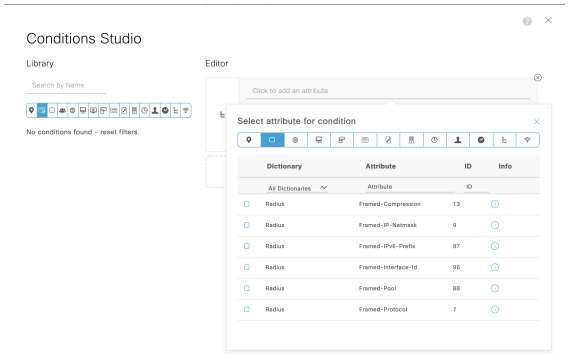
基于证书的条件的先决条件

客户端调配和终端安全评估策略规则可能包括基于证书属性的条件。客户端调配或终端安全评估策略中基于证书的条件的先决条件是为了确保存在基于同一证书属性的匹配授权策略规则。

例如，您应使用图中所示的相同属性，Issuer - Common Name 属性同时用于客户端调配或终端安全评估和授权策略。

图 *1:* 思科调配策略

图 *2: Conditions Studio*



注释 ISE 服务器证书必须在 AnyConnect 4.6 MR2 及更高版本的系统证书库中受信任。如果服务器不受信任，则需要提升权限的终端安全评估检查和补救都不会起作用。

- Windows 操作系统：必须将服务器证书添加到系统证书存储区。
- MAC 操作系统：必须将服务器证书添加到系统密钥链。建议使用命令行实用程序信任证书。如果登录密钥链中已存在证书，则可能无法使用密钥链访问应用将证书添加到系统密钥链。

默认终端安全评估策略

思科 ISE 软件附带了许多有助于您轻松创建授权策略和配置文件的预配置终端安全评估策略。默认情况下，这些策略处于禁用状态。您可以根据要求启用这些策略。以下是一些默认的安全评估策略。

规则名称	说明	要求
Default_Antimalware_Policy_Mac	检查终端是否已在设备中安装并运行任何支持的供应商的防恶意软件（ AnyConnect能识别）。	Any_AM_Installation
Default_Antimalware_Policy_Win	检查终端是否已在设备中安装并运行任何支持的供应商的防恶意软件（ AnyConnect能识别）。	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	收集信息并报告给定终端上安装的所有应用。	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	收集信息并报告给定终端上安装的所有应用。	Default_AppVis_Requirement_Win

规则名称	说明	要求
Default_Firewall_Policy_Mac	检查终端是否安装了任何支持的供应商的防火墙程序（AnyConnect能识别）。	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	检查终端是否安装了任何支持的供应商的防火墙程序（AnyConnect能识别）。	Default_Firewall_Requirement_Win
Default_USB_Block_Win	确保终端设备未连接任何 USB 存储设备。	USB_Block

客户端安全评估

为确保已应用的网络安全措施保持相关和有效，思科 ISE 使您能够在任何可访问受保护网络的客户端计算机上验证和维护安全功能。通过应用旨在确保最新安全设置或应用在客户端计算机上可用的终端安全评估策略，思科 ISE 管理员可以确保任何访问网络的客户端都符合并且继续符合为企业网络访问定义的安全标准。终端安全评估合规性报告在用户登录时以及在周期性再评估发生时，为思科 ISE 提供客户端计算机合规性级别快照。

使用思科 ISE 中提供的下列代理类型之一，终端安全评估和合规性会发生：

- AnyConnect ISE 代理：持久代理，可以安装在 Windows 或 Mac OS X 客户端计算机上执行终端安全评估合规性功能。
- 思科临时代理：在客户端运行的临时可执行文件，用于检查合规性状态。登录会话终止后，将从客户端计算机中删除代理。默认情况下，代理位于思科 ISE ISO 映像中，并在安装期间上传到思科 ISE。

终端安全状态评估选项

下表提供适用于 Windows 和 Macintosh 的思科 ISE 终端安全评估代理以及适用于 Windows 的 Web 代理支持的终端安全状态评估（终端安全评估条件）选项的列表。

表 *16:* 终端安全状态评估选项

适用于 **Windows** 的 **ISE** 终端安全评估代理	适用于 **Windows** 的思科临时代理	适用于 **Macintosh OS X** 的 **ISE** 终端安全评估代理	适用于 **Macintosh OS X** 的思科临时代理
操作系统/服务包/修补程序	-	-	-

适用于 **Windows** 的 **ISE** 终端安全评估代理	适用于 **Windows** 的思科临时代理	适用于 **Macintosh OS X** 的 **ISE** 终端安全评估代理	适用于 **Macintosh OS X** 的思科临时代理
服务检查	服务检查（临时代理4.5和 ISE 2.3）	服务检查（AC 4.1 和 ISE 1.4）	不支持后台守护程序检查
注册表检查	注册表检查（临时代理4.5 和 ISE 2.3）	-	-
文件检查	文件检查（临时代理4.5和 ISE 2.3）	文件检查（AC 4.1 和 ISE 1.4）	文件检查（临时代理4.5和 ISE 2.3）
应用检查	应用检查（临时代理4.5和 ISE 2.3）	应用检查（AC 4.1 和 ISE 1.4）	应用检查（临时代理4.5和 ISE 2.3）
防病毒软件安装	防恶意软件安装	防病毒软件安装	防恶意软件安装
防病毒软件版本/防病毒软件定义日期	正使用 OPSWAT 版本4，因此不支持防病毒/反间谍软件；仅支持防恶意软件	防病毒软件版本/防病毒软件定义日期	正使用 OPSWAT 版本4，因此不支持防病毒/反间谍软件；仅支持防恶意软件
反间谍软件安装	正使用 OPSWAT 版本4，因此不支持防病毒/反间谍软件；仅支持防恶意软件	反间谍软件安装	正使用 OPSWAT 版本4，因此不支持防病毒/反间谍软件；仅支持防恶意软件
反间谍软件版本/反间谍软件定义日期	正使用 OPSWAT 版本4，因此不支持防病毒/反间谍软件；仅支持防恶意软件	反间谍软件版本/反间谍软件定义日期	正使用 OPSWAT 版本4，因此不支持防病毒/反间谍软件；仅支持防恶意软件
补丁管理检查（AC 4.1 和 ISE 1.4）	仅补丁管理安装检查	补丁管理检查（AC 4.1 和 ISE 1.4）	-
Windows 更新运行	-	-	-
Windows 更新配置	-	-	-
WSUS 合规性设置	-	-	—

安全评估补救选项

下表列出了思科 ISE 终端安全评估代理（适用于 Windows 和 Macintosh）和 Web 代理（适用于 Windows）支持的终端安全评估补救选项列表。

表 *17:* 终端安全评估补救选项

ISE 终端安全评估代理（适用于 Windows 的 ISE 终端安全评估代理	**适用于 Macintosh OS X**）
消息文本（本地检查）	消息文本（本地检查）
URL 链路（链路分布）	URL 链路（链路分布）
文件分发	-
启动计划	-
防病毒定义更新	防病毒实时更新
反间谍程序定义更新	反间谍程序实时更新
补丁修复检查（AC 4.1 - 和 ISE 1.4）	-
Windows 更新	-
WSUS	-

ISE 社区资源

思科 ISE 与 SCCM 集成参考指南

安全评估的自定义条件

安全评估条件可以是以下任何一个简单条件：文件、注册表、应用、服务或字典条件。这些简单条件中的一个或多个条件构成可与安全评估要求相关联的复合条件。

在初始安全评估更新后，思科 ISE 还会创建思科定义的简单条件与复合条件。思科定义的简单条件使用 pc_ 作为前缀，复合条件使用 pr_ 作为前缀。

用户定义的条件或思科定义的条件同时包含简单条件与复合条件。

安全评估服务基于防病毒和反间谍软件 (AV/AS) 复合条件利用内部检查。因此，安全评估报告不会反映您已创建的精确 AV/AS 复合条件名称。报告仅显示 AV/AS 复合条件的内部检查名称。

例如，如果您已创建名为“MyCondition_AV_Check”的 AV 复合条件来检查任何供应商与任何产品，则安全评估报告会将内部检查（即“av_def_ANY”）显示为条件名称，而不是显示“MyCondition_AV_Check”。

终端安全评估终端自定义特性

您可以使用终端安全评估终端自定义属性创建客户端调配和终端安全评估策略。最多可以创建 100 个终端自定义属性。支持以下终端自定义属性类型：Int、String、Long、Boolean 和 Float。

终端自定义属性可用于根据某些属性允许或阻止设备，或根据安全评估或客户端调配策略分配特定权限。

使用终端自定义属性创建终端安全评估策略

要使用终端自定义属性创建终端安全评估策略，请执行以下操作：

步骤 1 创建终端自定义属性。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端自定义属性 (Endpoint Custom Attributes)**。

b) 在**终端自定义属性 (Endpoint Custom Attributes)** 区域，输入**属性名称 (Attribute Name)**（例如，deviceType）和“数据类型”（例如，字符串）。

c) 单击**保存**。

步骤 2 为自定义属性分配值。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **情景可视性 (Context Visibility)** > **终端 (Endpoints)**。

b) 分配自定义属性值。

- 选中所需的 MAC 地址复选框，然后点击**编辑 (Edit)**。
- 或者，点击所需的 MAC 地址，然后点击**终端 (Endpoints)** 页面中的**编辑 (Edit)** 。

c) 确保您创建的自定义属性显示在**编辑终端 (Edit Endpoint)** 对话框的**自定义属性 (Custom Attributes)** 区域中。

d) 点击**编辑 (Edit)**并输入所需的属性值（例如，deviceType = Apple-iPhone）。

e) 单击**保存**。

步骤 3 使用自定义属性和值创建授权策略。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **安全评估 (Posture)** > **终端安全评估策略 (Posture Policy)**。

b) 创建所需的策略。通过点击**其他条件 (Other Conditions)** 选择自定义属性，然后选择所需的字典，例如，选择“终端”(Endpoints) >“设备类型”(deviceType)，即您在第 1 步中创建的自定义属性。有关详细信息，请参阅配置思科临时代理工作流程，第 78 页。

c) 单击**保存**。

要使用终端自定义属性创建客户端调配策略，请执行以下操作：

1. 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **客户端调配 (Client Provisioning)** > **客户端调配策略 (Client Provisioning Policy)**。

2. 创建所需的策略。
   - 创建所需的规则（例如，Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。
   - 点击**其他条件 (Other Conditions)** 并选择所需的字典，选择自定义属性。

自定义安全评估补救措施

自定义安全评估补救措施是文件、链接、防病毒或反间谍软件定义更新、启动程序、Windows 更新或 Windows Server Update Services (WSUS) 补救类型。

添加反间谍程序补救

可以创建反间谍程序补救，从而在补救之后使用最新文件定义更新客户端以确保合规。

“AS 补救”(AS Remediations) 窗口显示所有防病毒软件补救以及补救的名称、说明和模式。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **AS Remediation**。

步骤 4 点击 **Add**。

步骤 5 修改新 **AS 补救 (New AS Remediations)** 窗口中的值。

步骤 6 点击**提交**。

添加防病毒软件补救

您可以创建防病毒软件补救，在补救完成后，用最新的合规性文件定义更新客户端。

“AV 补救”(AV Remediations) 窗口显示所有防病毒软件补救以及补救的名称、说明和模式。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **AV Remediation**。

步骤 4 点击 **Add**。

步骤 5 修改新 **AV 补救 (New AV Remediation)** 窗口中的值。

步骤 6 点击**提交**。

添加文件补救

客户端可以通过文件补救下载实现合规性所需的文件版本。客户端代理可以利用客户端或合规性要求的文件对终端进行补救。

您可以在“文件补救”(File Remediations) 窗口过滤、查看、添加或删除文件补救，但无法编辑文件补救。“文件补救”(File Remediations) 窗口显示所有文件补救及其名称与说明，还有补救所需的文件。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **File Remediation**。

步骤 4 点击 **Add**。

步骤 5 在**名称 (Name)** 和**说明 (Description)** 字段中输入文件补救的名称和说明。

步骤 6 在**新建文件补救 (New File Remediation)** 窗口中修改值。

步骤 7 点击**提交**。

添加脚本补救

您可以创建安全评估补救脚本并将其上传到思科 ISE，以便消除终端中的不合规问题。

开始之前

- 建立信任以获取安全评估策略。有关详细信息，请参阅建立信任以执行脚本条件，第 64 页
- 下载脚本。有关详细信息，请参阅脚本下载，第 65 页

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 单击**脚本补救 (Script Remediations)**。

步骤 4 单击**添加**。

步骤 5 输入脚本的**名称**和**说明**。

步骤 6 从相应的下拉列表中选择**操作系统 (Operating System)** 和**补救类型 (Remediation Type)**。

如果选择 **Windows** 操作系统，系统将显示**脚本类型 (Script Type)** 和 **Windows PowerShell 执行策略 (Windows PowerShell Execution policy)** 字段。单击相应的单选按钮，选择所需的脚本类型和执行策略。

步骤 7 从**补救类型 (Remediation Type)** 下拉列表中选择**自动 (Automatic)** 或**手动 (Manual)**。

注释
- 只有 Linux 代理仅支持自动补救。不支持手动补救。
- Linux 代理仅支持 shell 脚本。

步骤 8 输入**间隔 (Interval)** 和**重试计数 (Retry Count)**。有效范围为 0 至 999。

步骤 9 单击**要上传的文件 (File To Upload)** 旁边的**选择文件 (Choose File)**，然后选择要从本地系统上传的脚本。

步骤 10 要以管理员身份运行脚本，请单击**管理员/根 (Administrator/ Root)** 单选按钮。要以登录用户身份运行脚本，请单击**已登录的用户 (Logged-in User)** 单选按钮。

步骤 11 点击**提交**。

步骤 12 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端安全评估脚本补救 (Posture Script Remediation)**以检查补救脚本执行的状态。

系统将显示以下状态之一：

- 补救脚本执行成功。
- 已尝试补救，并且脚本退出失败。
- 未尝试补救（默认）。
- 补救尝试失败。该脚本未通过完整性检查，因为包含的策略可能已被篡改。
- 补救尝试失败。客户端无法下载脚本。
- 补救尝试失败。脚本未通过完整性测试，因为脚本可能已损坏或已被篡改。
- 补救尝试失败。脚本已执行，但未及时退出（超时）。
- 补救尝试失败。发生通用内部系统故障。
- 补救尝试失败。脚本类型不受支持。
- 补救尝试失败。启动脚本失败。
- 证书验证失败。客户端无法验证思科 ISE 提供的服务器证书。

建立信任以执行脚本条件

您必须建立信任关系才能在终端上执行脚本，并确保思科 ISE 服务器不受影响。思科 ISE 环境可以配置一个或多个 PSN。每个 PSN 都有一个有效的证书链。证书链以任何证书开头，后跟中间证书或根 CA 证书。您可以使用证书链中的任何证书进行指纹验证。

您可以在 AnyConnectLocalPolicy 的配置文件编辑器中配置证书链中任何证书的 SHA-256 指纹。例如，以下命令会生成名称为 input.cer 的证书的 SHA-256 指纹：

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

以下是输出的示例：

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

以下示例显示了 AnyConnectLocalPolicy.xml 中的新标记：

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

注释 可以添加带或不带冒号的 SHA-256 指纹。您可以采用以下任一格式添加指纹：`B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` 或 `B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`。指纹不区分大小写。

在获取脚本时，代理会将思科 ISE 证书指纹与受信任证书指纹（存在于 AnyConnectLocalPolicy.xml 中）进行匹配。如果终端缺少有效的证书指纹，则不会在终端上执行脚本。

注释 如果在 AnyConnectLocalPolicy.xml 中配置了指纹，那么这些指纹将用于验证所有流的思科 ISE 信任。如果证书不受信任，或者指纹不匹配，则不会显示错误消息。但是，**终端安全评估脚本条件** 报告（**操作 > 报告 > 终端和用户**）中包含以下错误消息：

`条件脚本证书验证失败。客户端无法验证思科 ISE 提供的服务器证书。`

脚本下载

当终端安全评估检查失败并触发相关补救操作时，AnyConnect将从终端安全评估策略中配置的HTTPS URL 下载脚本。要下载脚本，必须满足以下条件：

- 受信任的指纹应存在于 AnyConnectLocalPolicy.xml 中。
- HTTPS URL 提供的指纹应与 AnyConnectLocalPolicy.xml 中存在的受信任证书指纹匹配。

添加启动程序补救

您可以创建启动程序补救，其中客户端代理将通过启动一个或多个合规性应用来补救客户端。

Launch Program Remediations 页面显示所有启动程序补救，以及它们的名称和说明及补救模式。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Launch Program Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 在**新启动程序补救 (New Launch Program Remediation)** 页面中修改值。

步骤 6 点击**提交**。

排除启动程序补救故障

问题

当应用作为使用启动计划修复的补救措施启动时，应用成功启动（可在 Windows 任务管理器观察到），但是应用 UI 不可见。

解决方案

启动计划 UI 应用在系统权限运行，并会显示在交互式服务检测 (ISD) 窗口中。要查看启动计划 UI 应用，以下操作系统应启用 ISD：

- Windows Vista：默认情况下 ISD 处于停止状态。通过启动 services.msc 中的 ISD 服务启用 ISD。
- Windows 7：默认情况下启用 ISD 服务。
- Windows 8/8.1：通过在注册表中将 " NoInteractiveServices " 从 1 更改为 0 启用 ISD：\HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Windows。

添加链接补救

客户端可以通过链接补救点击URL以访问补救窗口或资源。客户端代理用此链接打开浏览器，并且允许客户端执行进行合规性补救。

“链接补救”(Link Remediation) 窗口显示所有链接补救及其名称与说明和补救模式。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Link Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 在**新建链接补救 (New Link Remediation)** 窗口修改相应值。

步骤 6 点击**提交**。

添加补丁管理补救

您可以创建补丁管理补救，在补救完成后，用最新的合规性文件定义更新客户端。

“补丁管理补救”(Patch Management Remediation) 窗口显示补救类型、补丁管理供应商名称和各种补救选项。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Patch Mangement Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 修改**补丁管理补救 (Patch Management Remediation)** 窗口中的值。

步骤 6 点击**提交 (Submit)**，将补救操作添加到**补丁管理补救 (Patch Management Remediation)** 页面。

添加 Windows 服务器更新服务补救

您可以将 Windows 客户端配置为从本地管理或 Microsoft 管理的 WSUS 服务器接收最新的 WSUS 更新，以实现合规性。Windows 服务器更新服务 (WSUS) 补救安装来自本地管理的 WSUS 服务器或 Microsoft 管理的 WSUS 服务器的 Windows 服务包、热补救和补丁。

在客户端代理与本地 WSUS 代理相集成的情况下，您可以创建 WSUS 补救，以检查终端是否安装最新的 WSUS 更新。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)**。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Windows Server Update Services Remediation**。

步骤 4 点击 **Add**。

步骤 5 修改**新 Windows 服务器更新服务补救 (New Windows Server Update Services Remediation)** 窗口中的值。

步骤 6 点击**提交**。

添加 Windows 更新补救

Windows Update Remediations 页面显示所有 Windows 更新补救及其名称和说明与补救模式。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > > **终端安全评估 (Posture)**。。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Windows Update Remediation**。

步骤 4 点击**添加 (Add)**。

步骤 5 修改**新建 Windows 更新补救 (New Windows Update Remediation)** 窗口中的值。

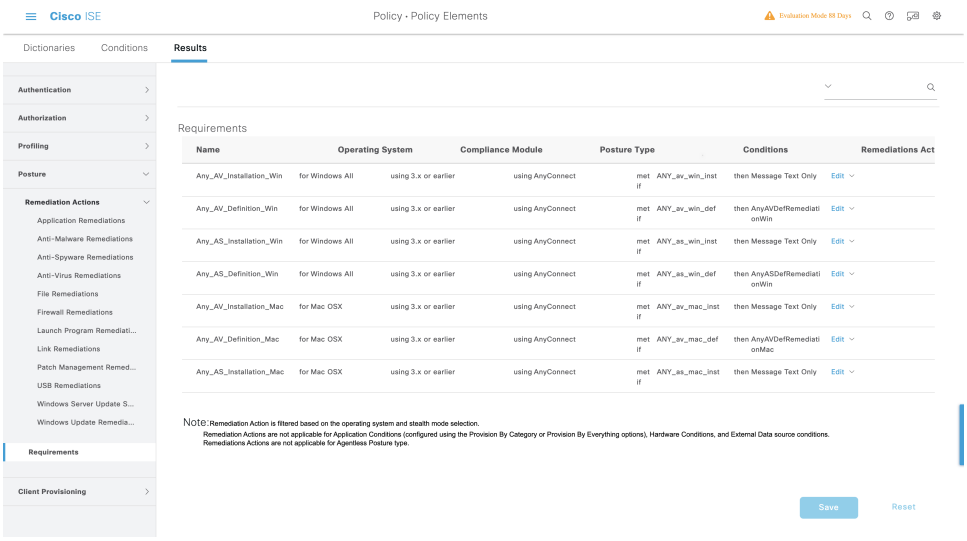
步骤 6 点击**提交**。

终端安全评估要求

安全评估要求是一组具有关联补救操作的复合条件，可与角色和操作系统相关联。连接到网络的所有客户端必须在安全评估过程中满足强制性要求才能在网络上达到合规状态。

安全评估策略要求可在安全评估策略中设置为强制性、可选或审核类型。如果要求为可选类型且客户端未能满足这些要求，则客户端可选择继续对终端进行安全评估。

图 *3:* 终端安全评估策略要求类型



强制性要求

在策略评估期间，代理对未能满足终端安全评估策略中定义的强制性要求的客户端提供补救选项。最终用户必须在补救计时器设置中指定的时间内进行补救以满足要求。

例如，您已通过一个用户定义条件指定强制性要求以检查绝对路径中 C:\temp\text.file 的存在。如果该文件不存在，则强制性要求未通过，用户将会被移至非合规状态。

可选要求

在策略评估期间，当无法满足终端安全评估策略中指定的可选要求时，代理会为客户端提供一个选项继续。允许最终用户跳过指定可选要求。

例如，您通过一个用户定义条件指定一个可选要求以检查在客户端机器上运行的应用，例如Calc.exe。虽然客户端未能满足该条件，但代理会提示一个继续后续操作的选项，以便跳过可选要求并将最终用户移至合规状态。

审核要求

审核要求指定用于内部目的，代理不提示任何消息或来自最终用户的四输入，无论策略评估期间状态是失败还是通过。

例如，您在创建一个强制性策略条件以检查最终用户是否拥有防病毒程序的最新版本的过程中。如果要在将其作为策略条件实际实施前找出非合规的最终用户，您可以将其指定为审核要求。

可视性要求

在策略评估期间时，代理每五到十分钟报告一次可视性要求的合规性数据。

客户端系统处于不合规状态

如果客户机无法通过修复符合强制性要求，则安全评估状态会更改为“不合规”，且代理会话会被隔离。若要使客户机通过此“不合规”状态，则需要重启安全评估会话从而使代理再次启动客户机上的安全评估。您可以按以下方法重启安全评估会话：

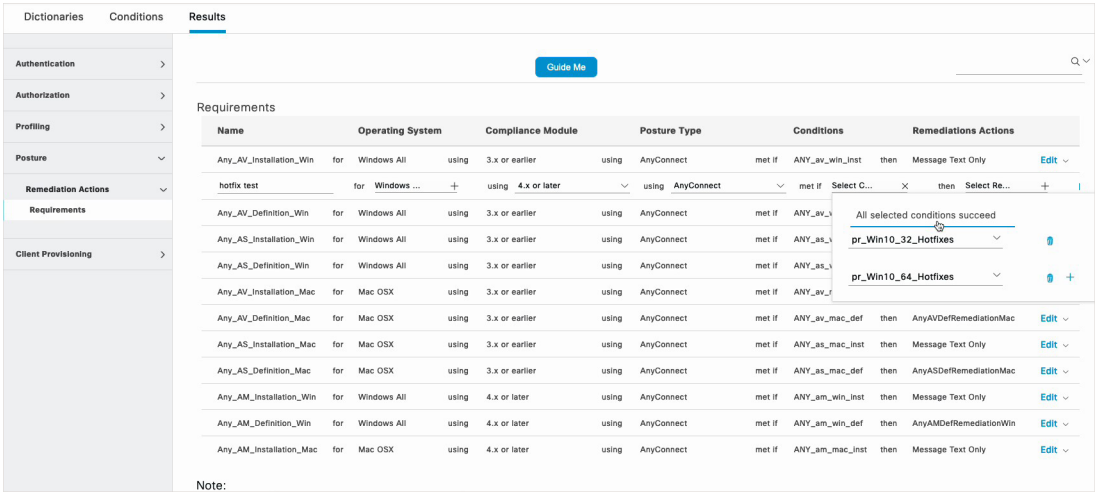
- 在 802.1X 的有线和无线授权更改 (CoA) 环境下：
  - 当您在新授权策略窗口中新建授权配置文件时，您可以配置特定授权策略的重新验证计时器。
  - 一旦断开并重新连接到网络时，有线用户即可离开隔离状态。在无线环境中，用户必须断开与无线局域网控制器 (WLC) 的连接并等待用户空闲超时过期后才能尝试重新连接到网络。
- 在 VPN 环境中 - 断开并重新连接 VPN 隧道。

创建客户端安全评估要求

可以在“要求”(Requirements) 窗口创建要求，可以通过此窗口将用户定义的条件和思科定义的条件与补救操作关联起来。在“要求”(Requirements) 窗口创建并保存用户定义的条件和补救操作后，可以从各自的列表窗口查看这些条件和操作。

注释 要创建安全评估要求以验证环境中的所有 Windows 10 补丁，您必须将“要求”的“条件”区域配置为包含 pr_Win10_32_Hotfixes 和 pr_Win10_64_Hotfixes。在条件的顶部，确保选中 **所有选定的条件成功** 。如果配置成功，系统将显示 **pr_Win10_32_Hotfixes & pr_Win10_64_Hotfixes** 。要查看终端的已验证条件的详细信息，请从主菜单选择**操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **按终端进行终端安全评估 (Posture Assessment by Endpoints)**。单击终端可查看相应的终端安全评估详细信息。

图 *4:* 验证 ***Windows 10*** 中的安全评估要求



开始之前

- 必须了解适用于安全评估的可接受使用政策 (AUP)。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)** > **要求 (Requirements)**。

步骤 2 在**要求 (Requirements)** 窗口中输入值。

步骤 3 点击**完成 (Done)**，在只读模式下保存终端安全评估要求。

步骤 4 点击**保存**。

重新进行安全评估配置设置

下表列出“终端安全再评估配置”(Posture Reassessment Configurations) 窗口中的字段，您可以使用此窗口配置终端安全再评估。要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **重新评估 (Reassessments)**。

表 *18:* 重新进行安全评估配置设置

字段名称	使用指南
Configuration Name	输入 PRA 配置的名称。
Configuration Description	输入 PRA 配置的说明。
Use Reassessment Enforcement?	选中此复选框，将PRA配置应用到用户身份组。
Enforcement Type	选择要执行的操作： • **继续 (Continue)**：用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。 • **注销 (Logoff)**：如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。 • **补救 (Remediate)**：如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送 PRA 报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。 如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的RADIUS会话，才能再次布置客户端。 如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续”(Continue) 选项。用户可以继续停留在当前的网络中，不受任何限制。
Interval	输入第一次成功登录后在客户端上启动PRA的时间间隔分钟数。 默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。

字段名称	使用指南
Grace time	输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于PRA间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。 最小值为 5 分钟，最大值为 60 分钟。 注释 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。
Select User Identity Groups	为 PRA 配置选择唯一组或唯一组组合。
PRA configurations	显示现有的 PRA 配置以及关联到 PRA 配置的用户身份组。

相关主题

安全评估租约，第 12 页
定期重新评估，第 12 页
终端安全状态评估选项，第 58 页
安全评估补救选项，第 59 页
安全评估的自定义条件，第 60 页
自定义安全评估补救措施，第 62 页
配置定期重新评估，第 13 页

自定义安全评估权限

自定义权限是一个在思科 ISE 中定义的标准授权配置文件。标准授权配置文件根据终端的匹配合规性状态设置访问权限。终端安全评估服务将终端安全评估广泛地划分为未知、合规和不合规的配置文件。终端安全评估策略和终端安全评估要求确定终端的合规性状态。

您必须为终端的未知、合规和不合规安全评估状态创建三种不同的授权配置文件，这些终端可以具有不同的 VLAN、DACL 和其他属性值对集合。这些配置文件可与三种不同的授权策略相关联。为了区分这些授权策略，可以使用 Session:PostureStatus 属性以及其他条件。

未知的配置文件

如果没有为终端定义匹配的终端安全评估策略，则终端的终端安全评估合规性状态可能设置为未知。未知的终端安全评估合规性状态也可适用于匹配的终端安全评估策略已启用但其终端安全评估评估尚未进行的终端，因此，客户端代理尚未提供合规性报告。

注释 我们建议您对所有思科网络接入设备使用终端安全评估和重定向。

合规的配置文件

如果已为终端定义匹配的终端安全评估策略，则终端的终端安全评估合规性状态会设置为合规。当进行终端安全评估时，终端会满足匹配的终端安全评估策略中定义的所有强制性要求。对于终端安全评估合规的终端，可以向其授予对网络的网络访问权限。

不合规的配置文件

当为某个终端定义匹配的终端安全评估策略，但该策略在终端安全评估过程中未能满足所有强制性要求时，该终端的终端安全评估合规性状态会设置为不合规。终端安全评估不合规的终端会将终端安全评估要求与补救操作匹配，并且应对该终端授予对补救资源的有限网络访问权限以便自行补救。

配置标准授权策略

您可以在“授权策略”(Authorization Policy) 窗口中定义两种类型的授权策略：标准策略和例外授权策略。特定于安全评估的标准授权策略用于根据终端的合规性状态制定策略决策。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

步骤 2 在**视图 (View)** 列中，点击相应默认策略旁边的箭头图标。

步骤 3 在**操作 (Actions)** 列中，点击齿轮图标，然后从下拉列表中选择新的授权策略。
新行将显示在**策略集 (Policy Sets)** 表中。

步骤 4 输入规则名称。

步骤 5 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 6 在 **Conditions Studio** 页面上创建所需的条件。在**编辑器 (Editor)** 部分中，点击**点击以添加属性 (Click To Add an Attribute)** 文本框，然后选择所需的字典和属性。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 7 点击**使用 (Use)** 以在只读模式下创建新的标准授权策略。

步骤 8 点击**保存**。

使用终端安全评估进行网络驱动器映射的最佳实践

在 Windows 终端安全评估期间，终端用户可能会在访问桌面时遇到延迟。这可能是由于 Windows 向用户提供桌面访问权限之前尝试恢复文件服务器的驱动盘号映射。避免在安全评估期间出现延迟的最佳做法是：

- 终端应能够访问 Active Directory 服务器，因为文件服务器驱动盘号无法在不访问 AD 的情况下进行映射。当触发终端安全评估（使用 AnyConnect ISE 终端安全评估代理）时，它会阻止对 AD 的访问，导致登录延迟。在终端安全评估完成之前，使用安全评估补救 ACL 来访问 AD 服务器。

- 您应为登录脚本设置一个延迟，直到终端安全评估完成为止，然后您必须将“持久性”(Persistence) 属性设置为“否”(NO)。Windows 会在登录期间尝试重新连接所有网络驱动器，只有在 AnyConnect ISE 终端安全评估代理获得完全网络访问权限后才能执行此操作。

配置 AnyConnect 隐身模式工作流程

在隐身模式下配置 AnyConnect 的过程涉及一系列步骤。您可以在思科 ISE 中执行以下步骤。

步骤 1 创建 AnyConnect 代理配置文件，请参阅创建 AnyConnect 代理配置文件。

步骤 2 为 AnyConnect 软件包创建 AnyConnect 配置，请参阅 为 AnyConnect 软件包创建 an AnyConnect 配置。 。

步骤 3 在思科 ISE 中上传开放式 DNS 配置文件，请参阅 在思科 ISE 中上传开放式 DNS 配置文件。

步骤 4 创建客户端调配策略，请参阅 创建客户端调配策略。

步骤 5 创建终端安全评估条件，请参阅 创建终端安全评估条件。

步骤 6 创建终端安全评估补救，请参阅创建终端安全评估补救。

步骤 7 在无客户端模式下创建终端安全评估要求，请参阅 在隐身模式下创建终端安全评估要求。

步骤 8 创建终端安全评估策略，请参阅创建终端安全评估策略。

步骤 9 配置授权配置文件

a) 在思科 ISE GUI 中，单击**菜单** 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)**。

b) 点击**添加 (Add)** 并输入配置文件的**名称 (Name)**。

c) 在“常见任务”(Common Tasks) 中，启用 **Web 重定向（CWA、MDM、NSP、CPP）(Web Redirection (CWA, MDM, NSP, CPP))** 并从下拉列表中选择**客户端调配（终端安全评估）(Client provisioning (Posture))**，然后输入重定向 **ACL** 名称并选择客户端调配门户**值 (Value)**。您可以在**工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **客户端调配 (Client Provisioning)** > **客户端调配门户 (Client Provisioning Portal)** 中编辑或创建新的客户端调配门户。

步骤 10 配置授权策略。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**

b) 点击 >，然后选择**授权策略 (Authorization Policy)**，然后点击 + 图标以创建新的授权规则，该规则采用 **Session:Posture Status EQUALS Unknown** 条件和之前配置的授权文件。

c) 在上一个规则之上，创建新的授权规则，该规则采用 **Session:Posture Status EQUALS NonCompliant** 条件，另一个采用 **Session:Posture Status EQUALS Compliant** 条件。

创建 AnyConnect 代理配置文件

开始之前

必须上传 MAC 和 Windows 操作系统的 AnyConnect 软件包以及 AnyConnect 合规性模块。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 从 **添加** 下拉列表中，选择 **AnyConnect 终端安全评估配置文件**。

步骤 3 从 **安全评估代理配置文件设置** 下拉列表中，选择 **AnyConnect**。

步骤 4 在**名称 (Name)** 字段中，键入所需的名称（例如，AC_Agent_Profile）。

步骤 5 在**代理行为 (Agent Behavior)** 部分，选择**隐藏模式 (Stealth Mode)** 参数为**已启用 (Enabled)** 。

步骤 6 点击**保存 (Save)**。

下一步做什么

应当为 AnyConnect软件包创建 AnyConnect 配置。

为 AnyConnect 软件包创建 an AnyConnect 配置。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 从**添加 (Add)** 下拉列表中，选择 **AnyConnect 配置 (AnyConnect Configuration)**。

步骤 3 从**选择 AnyConnect 软件包**下拉列表中，选择所需的 AnyConnect 软件包。

步骤 4 在**配置名称 (Configuration Name)** 文本框中，键入所需的名称。

步骤 5 从**合规性模块 (Compliance Module)** 下拉列表中，选择所需的合规性模块。

步骤 6 在**AnyConnect 模块选择 (AnyConnect Module Selection)** 部分，选中 **ISE 终端安全评估 (ISE Posture)** 和**网络访问管理器 (Network Access Manager)** 复选框。

步骤 7 在**配置文件选择 (Profile Selection)**部分，从**ISE 终端安全评估 (ISE Posture)**下拉列表中选择 AnyConnect代理配置文件。

步骤 8 从**网络访问管理器 (Network Access Manager)**下拉列表中，选择所需的 AnyConnect代理配置文件。

下一步做什么

应上传将推送到客户端的开放式 DNS 配置文件。

在思科 ISE 中上传开放式 DNS 配置文件

开放式 DNS 配置文件会被推送到客户端。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 从**添加 (Add)** 下拉列表中，选择**来自本地磁盘的代理资源 (Agent Resources From Local Disk)**。

步骤 3 从**类别 (Category)** 下拉列表中选择**客户创建的数据包 (Customer Created Packages)**。

步骤 4 从 **类型** 下拉列表中，选择 **AnyConnect 配置文件** 。

步骤 5 在**名称 (Name)** 文本框中，键入所需的名称（例如，OpenDNS）。

步骤 6 点击**浏览 (Browse)** 并从本地磁盘上找到 JSON 文件。

步骤 7 点击 **Submit**。

下一步做什么

您应创建客户端调配策略。

创建客户端调配策略

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 创建所需的规则（例如，Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。

下一步做什么

您应创建终端安全评估条件。

创建终端安全评估条件

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **文件条件 (File Condition)**。

步骤 2 输入所需的名称（例如，filechk）。

步骤 3 从**操作系统 (Operating Systems)** 下拉列表中，选择 Windows 7 (All)。

步骤 4 从**文件类型 (File Type)** 下拉列表中，选择 FileExistence。

步骤 5 从**文件路径 (File Path)** 下拉列表中，选择 ABSOLUTE_PATH C:\test.txt。

步骤 6 从**文件运算符 (File Operator)** 下拉列表中，选择 DoesNotExist。

下一步做什么

您应创建终端安全评估补救。

创建终端安全评估补救

文件条件检查终端上是否存在 test.txt 文件。如果不存在，则补救方法是屏蔽 USB 端口并阻止使用 USB 设备安装该文件。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **补救措施 (Remediation Actions)** > **USB 补救 (USB Remediations)** 页面。

步骤 2 输入所需的名称（例如，clientless_mode_block）。

步骤 3 点击 **Submit**。

下一步做什么

您应创建终端安全评估要求。

在隐身模式下创建终端安全评估要求

在“要求”(Requirements) 页面中创建补救操作时，仅显示适用于隐身模式的补救：防恶意软件、启动程序、补丁管理、USB、Windows 服务器更新服务和 Windows Update。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 创建所需的终端安全评估要求（例如，Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block）。

下一步做什么

您应创建终端安全评估策略。

创建终端安全评估策略

开始之前

确保终端安全评估策略要求和策略是在无客户端模式下创建的。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **终端安全评估 (Posture)**。

步骤 2 创建所需的规则。例如，if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=AnyConnect Stealth then Requirements=win7Req。

注释　对于没有URL重定向的客户端调配，使用网络访问或Radius的特定属性配置条件将不起作用，并且，由于思科ISE服务器中特定用户的会话信息不可用，因此客户端调配策略的匹配可能会失败。但是，思科ISE允许为外部添加的身份组配置条件。

启用 AnyConnect 隐身模式通知

思科ISE为AnyConnect隐身模式部署提供多个新的故障通知。在隐身模式下启用故障通知可帮助您识别有线、无线或VPN连接问题。要在隐身模式下启用通知，请执行以下操作：

注释　AnyConnect 版本 4.5.0.3040 及更高版本支持隐身模式通知。

开始之前

在隐身模式下配置 AnyConnect 。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择依次选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 依次选择 **添加** > **AnyConnect ISE 终端安全评估配置文件**。

步骤 3 从 **选择一个类别** 下拉列表中，选择 **AnyConnect**。

步骤 4 从**代理行为 (Agent Behavior)** 部分，对**在隐身模式下启用通知 (Enable notifications in stealth mode)** 选项选择**已启用 (Enabled)**。

配置思科临时代理工作流程

配置思科临时代理的过程涉及一系列步骤。您可以在思科 ISE 中执行以下步骤。

步骤 1 创建终端安全评估条件

步骤 2 创建终端安全评估要求

步骤 3 创建终端安全评估策略

步骤 4 配置客户端调配策略

步骤 5 配置授权配置文件

a) 在思科ISE GUI中，单击**菜单** 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)**。

b) 点击**添加 (Add)** 并输入配置文件的**名称 (Name)**。

c) 在“常见任务”(Common Tasks) 中，启用 **Web 重定向（CWA、MDM、NSP、CPP）(Web Redirection (CWA, MDM, NSP, CPP))** 并从下拉列表中选择**客户端调配（终端安全评估）(Client provisioning (Posture))**，然后输入重定向 **ACL** 名称并选择客户端调配门户**值 (Value)**。您可以在**工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **客户端调配 (Client Provisioning)** > **客户端调配门户 (Client Provisioning Portal)** 中编辑或创建新的客户端调配门户。

步骤 6 配置授权策略。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)**。

b) 点击 **>**，然后选择**授权策略 (Authorization Policy)**，然后点击 **+** 图标以创建新的授权规则，该规则采用 **Session:Posture Status EQUALS Unknown** 条件和之前配置的授权文件。

c) 在上一个规则之上，创建新的授权规则，该规则采用 **Session:Posture Status EQUALS NonCompliant** 条件，另一个采用 **Session:Posture Status EQUALS Compliant** 条件。

步骤 7 下载并启动思科临时代理

创建终端安全评估条件

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端安全评估 (Posture)** > **文件条件 (File Condition)**。

步骤 2 输入所需的名称（例如 filecondwin）。

步骤 3 从**操作系统 (Operating Systems)** 下拉列表中，选择 Windows 7 (All)。

步骤 4 从**文件类型 (File Type)** 下拉列表中，选择 FileExistence。

步骤 5 从**文件路径 (File Path)** 下拉列表中，选择 ABSOLUTE_PATH C:\test.txt。

步骤 6 从**文件运算符 (File Operator)** 下拉列表中，选择 DoesNotExist。

创建终端安全评估要求

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **终端安全评估 (Posture)** > **要求 (Requirements)**。

步骤 2 从**编辑 (Edit)** 下拉列表中，选择**插入新要求 (Insert New Requirement)**。

步骤 3 输入**名称**、**操作系统**和**合规性模块**（例如，名称为 filereqwin，操作系统为 Windows All，合规性模块为 4.x 或更高版本）。

步骤 4 在**终端安全评估类型 (Posture Type)** 下拉列表中，选择**临时代理 (Temporal Agent)**。

步骤 5 选择所需条件（例如 filecondwin）。

注释 对于思科临时代理，只能在**要求 (Requirements)** 页面中查看包含**安装 (Installation)** 检查类型的补丁管理条件。

步骤 6 选择**仅消息文本 (Message Text Only)** 补救操作。

注释 AnyConnect 4.x 或更高版本支持临时代理。

创建终端安全评估策略

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **终端安全评估 (Posture)**。

步骤 2 创建所需的规则（例如，Name=filepolicywin, Identity Groups=Any, Operating Systems=Windows All, Compliance Module=4.x or later, Posture Type=Temporal Agent, and Requirements=filereqwin）。

配置客户端调配策略

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 创建所需规则（例如 Rule Name=Win、Identity Groups=Any、Operating Systems=Windows All、Other Conditions=Conditions、Results=CiscoTemporalAgentWindows4.5）。

下载并启动思科临时代理

步骤 1 连接到 SSID。

步骤 2 启动浏览器，您将重定向至客户端调配门户。

步骤 3 点击**开始**。这将检查思科临时代理是否已安装并正在运行。

步骤 4 点击**这是我第一次访问 (This Is My First Time Here)**。

步骤 5 选择**点击此处下载并启动思科临时代理 (Click Here to Download and Launch Cisco Temporal Agent)**。

步骤 6 分别保存适用于 Windows 或 macOS 的思科临时代理 .exe 或 .dmg 文件。对于 Windows，请运行 .exe 文件；对于 macOS，请双击 .dmg 文件并运行 acisetempagent 应用。
思科临时代理会扫描客户端并显示结果，例如不合规检查的红色叉号标记。

安全评估故障排除工具

安全评估故障排除工具可帮助您查找安全状态检查失败的原因，以确定以下事项：

- 在安全评估检查中哪些终端成功，哪些终端失败。

- 如果终端在安全评估检查中失败，则确定安全评估流程中哪些步骤失败。
- 哪些强制检查和可选检查成功，哪些强制检查和可选检查失败。

您可以根据用户名、MAC 地址和安全评估状态等参数过滤请求，确定这些信息。

配置终端登录凭证

终端登录配置 (Endpoint Login Configuration) 窗口用于配置登录凭证，以便思科 ISE 可以登录客户端。以下思科 ISE 功能使用在此窗口中配置的登录凭证：

在思科 ISE GUI 中，单击**菜单**图标 (☰) 并选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端脚本 (Endpoint Scripts)** > **设置 (Settings)**。

显示以下选项卡：

- **Windows 域用户 (Windows Domain User)**：配置思科 ISE 必须用于通过 SSH 登录客户端的域凭证。单击**加号**图标并输入任意数量的 Windows 登录。对于每个域，请在**域 (Domain)**、**用户名 (Username)** 和**密码 (Password)** 字段中输入所需的值。如果配置域凭证，则在 **Windows 本地用户 (Windows Local User)** 选项卡中配置的本地用户凭证将被忽略。
- **Windows 本地用户 (Windows Local User)**：配置思科 ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。
- **MAC 本地用户 (MAC Local User)**：配置思科 ISE 用来通过 SSH 访问客户端的本地帐户。本地帐户必须能够运行 Powershell 和 Powershell 远程。在**用户名 (Username)** 字段中，输入本地帐户的帐户名称。要查看 Mac OS 帐户名称，请在终端中运行以下命令：

  ```
  whoami
  ```

终端脚本设置

此页面配置终端脚本和无代理终端安全评估的选项。

- **将终端脚本执行日志上传到 ISE (Upload endpoint script execution logs to ISE)**：默认情况下已启用，可以将终端脚本上传到思科 ISE。禁用此选项将禁用终端脚本，无法上传或运行终端脚本。
- **终端脚本执行详细日志记录 (Endpoint script execution verbose logging)**：启用详细日志记录以进行调试。
- **终端处理器批处理大小 (Endpoints processor batch size)**：可以根据网络负载和系统性能进行调整。
- **适用于 MAC 的终端处理并发 (Endpoints processing concurrency for MAC)**
- **适用于 Windows 的终端处理并发 (Endpoints processing concurrency for Windows)**
- **操作系统标识的最大重试次数 (Maximum retry attempts for OS identification)**

- 操作系统标识重试之间的延迟（毫秒）**(Delay between retries for OS identification (msec))**
- 终端分页批处理大小 **(Endpoint pagination batch size)**
- 终端上的日志保留期（天）**(Log retention period on Endpoints (Days))**
- 连接超时（秒）**(Connection Time out (sec))**
- 连接的最大重试次数 **(Max-retry attempts for Connection)**
- **Powershell 的端口号 (Port Number for Powershell)**：将它更改为使用非标准端口号。
- **SSH 的端口号 (Port Number for SSH)**：将它更改为使用非标准端口号。

在思科 ISE 中配置客户端调配

启用客户端调配以允许用户下载客户端调配资源并配置代理配置文件。您可以配置 Windows、Mac OS X 和 Linux 客户端的代理配置文件，并可配置个人设备的本地请求方文件。如果禁用客户端调配，则尝试访问网络的用户会收到警告消息，表明他们无法下载客户端调配资源。

开始之前

如果使用代理并在远程系统上托管客户端调配资源，请验证代理是否允许客户端访问该远程位置。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **客户端调配 (Client Provisioning)** 或**工作中心 (Work Centers)** > **终端安全评估 (Posture)** > **设置 (Settings)** > **软件更新 (Software Updates)** > **客户端调配 (Client Provisioning)** 。

步骤 2 从**启用调配 (Enable Provisioning)** 下拉列表中，选择**启用 (Enable)** 或**禁用 (Disable)**。

步骤 3 从 **Enable Automatic Download** 下拉列表中选择 **Enable**。

源下载包括所有可用的客户端调配资源。其中一些资源可能与您的部署并不相关。思科建议尽可能手动下载资源，而不是设置此选项。

步骤 4 在**更新源 URL (Update Feed URL)** 文本框中指定思科 ISE 搜索系统更新所在的 URL。例如，用于下载客户端调配资源的默认 URL 是 https://www.cisco.com/web/secure/spa/provisioning-update.xml。

步骤 5 当设备没有客户端调配资源时，请选择以下选项之一：

- **允许网络访问 (Allow Network Access)**：用户可以在网络上注册其设备，而不必安装和启动本地请求方向导。
- **应用定义的授权策略 (Apply Defined Authorization Policy)**：用户必须尝试通过标准身份验证和授权策略应用访问思科 ISE 网络（在本地请求方配置过程之外）。如果您启用了此选项，则用户设备会根据应用于用户 ID 的任何客户端调配策略进行标准注册。如果用户的设备需要证书才能访问思科 ISE 网络，则还必须向用户提供详细说明，介绍如何使用面向用户的可自定义文本字段获取和应用有效证书。

步骤 6 点击**保存**。

下一步做什么

配置客户端调配资源策略

客户端调配资源

在终端连接到网络后，客户端调配资源将会下载到终端。客户端调配资源包括适用于台式电脑的合规性和终端安全评估代理，以及适用于手机和平板电脑的本地请求方配置文件。客户端调配策略将这些调配资源分配给终端，以开始网络会话。

在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**中列出。可以通过点击**添加 (Add)** 按钮将以下资源类型添加到列表中：

- **思科站点中的代理资源**：选择要使其可用于客户端调配策略的 AnyConnect 和请求方调配向导。思科会定期更新该资源列表，以便添加新资源和更新现有资源。还可以将 ISE 设置为自动下载所有思科资源和资源更新，请参阅在思科 ISE 中配置客户端调配，第 82 页了解详细信息。
- **本地磁盘中的代理资源 (Agent resources from local disk)**：在 PC 中选择要上传到 ISE 的资源，请参阅从本地计算机添加思科提供的客户端调配资源，第 85 页。
-
- **本地请求方配置文件 (Native Supplicant Profile)**：为手机和平板电脑配置一个包含网络设置的请求方配置文件。有关详细信息，请参阅创建本地请求方配置文件。
- **AnyConnect ISE 终端安全评估配置文件**：当您不希望创建和分配代理 XML 配置文件时，请在此配置 AnyConnect ISE 终端安全评估。有关 AnyConnect ISE 终端安全评估代理和 ISE 终端安全评估配置文件编辑器的详细信息，请参阅适用于您的 AnyConnect 版本的《AnyConnect 管理员指南》 https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html。

在创建客户端调配资源后，请创建客户端调配策略，以便将客户端调配资源应用于终端。请参阅配置客户端调配资源策略，第 113 页。

相关主题

在思科 ISE 中配置客户端调配，第 82 页
从思科添加客户端调配资源，第 83 页
从本地计算机添加思科提供的客户端调配资源，第 85 页
从本地计算机添加 AnyConnect 的客户创建资源，第 85 页

从思科添加客户端调配资源

您可以从 Cisco.com 添加适用于思科 Web 代理、 AnyConnect Windows、MacOS 和 Linux 客户端的客户端调配资源。根据您选择的资源和可用网络带宽，思科 ISE 会用几分钟时间，将客户端调配资源下载到思科 ISE。

开始之前

- 确保已在思科 ISE 中配置正确的代理设置。
- 在思科 ISE 中启用客户端调配。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 依次选择 **Add** > **Agent resources from Cisco site**。

步骤 3 从**下载远程资源 (Download Remote Resources)** 对话框中的可用列表选择一个或多个所需的客户端调配资源。

步骤 4 单击 **Save**。

在安装 Linux 代理时，请注意以下事项：

- 如果使用自签名证书：
  - 您必须启用 SSH 代理才能将 ISE 证书复制到 Linux 代理。
    - 对于 RHEL：
      1. 从思科 ISE GUI 导出证书。
      2. 复制 <certificate>.pem to /etc/pki/ca-trust/source/anchors/ 并将文件重命名为 <certificate>.crt。
      3. 运行以下命令：**sudo update-ca-trust extract**
      4. 转到 /etc/pki/tls/certs/
      5. 运行以下命令：**openssl x509 -in ca-bundle.crt -text -noout**
    - 对于 Ubuntu：
      1. 从思科 ISE GUI 导出证书。
      2. 复制 <certificate>.pem to /usr/local/share/ca-certificates/ 并将其重命名为 <certificate>.crt。
      3. 运行以下命令：**sudo update-ca-certificates**

         要验证 CA 证书是否正确安装，请转至 /etc/ssl/certs/ca-certificates.crt 并检查此文件中存在的证书。

注释 如果 ISE 证书由受信任的 CA 颁发，则无需导入证书。

- 启动 dot1x 重定向或非重定向流。

- 如果您使用的是 RHEL，请确保使用订用管理器来更新 yum。如果您使用的 Ubuntu，请更新 apt-get。

  有关 Linux 代理的系统要求的详细信息，请参阅 思科 AnyConnect 安全移动客户端版本 4.9 发行说明。

下一步做什么

在成功将客户端调配资源添加到思科 ISE 之后，您可以开始配置客户端调配资源策略。

从本地计算机添加思科提供的客户端调配资源

您可以从本地磁盘添加之前从思科下载的客户端调配资源。

开始之前

请确保仅向思科 ISE 上传支持的最新资源。较旧且不受支持的资源可能会导致客户端访问出现严重问题。

如果要从 Cisco.com 手动下载资源文件，请参阅思科 ISE 发行说明中的“思科 ISE 离线更新”部分。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**

步骤 2 依次选择 **Add** > **Agent resources from local disk**。

步骤 3 从**类别 (Category)** 下拉列表中，选择**思科提供的软件包 (Cisco Provided Packages)**。

步骤 4 点击 **Browse** 以浏览要下载到思科 ISE 的资源文件所在的本地计算机上的目录。

您可以添加之前从思科下载到本地计算机的 AnyConnect 或思科 Web 代理资源。

步骤 5 点击 **Submit**。

下一步做什么

在成功将客户端调配资源添加到思科 ISE 之后，即可开始配置客户端调配资源策略。

从本地计算机添加 AnyConnect 的客户创建资源

从本地计算机将 AnyConnect 自定义和本地化包及 AnyConnect 配置文件等客户创建资源添加到思科 ISE。

开始之前

确保 AnyConnect 的客户创建资源是压缩的文件且在您的本地磁盘中可用。A

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 依次选择**添加 (Add)** > **来自本地磁盘的代理资源 (Agent Resources from local disk)**。

步骤 3 从**类别 (Category)** 下拉列表中，选择**客户创建的包 (Customer Created Packages)**。

步骤 4 输入 AnyConnect 资源的名称和说明。

步骤 5 点击 **Browse** 以浏览要下载到思科 ISE 的资源文件所在的本地计算机上的目录。

步骤 6 选择以下要上传到思科 ISE 的 AnyConnect 资源：

- AnyConnect 自定义捆绑包
- AnyConnect 本地化捆绑包
- AnyConnect 配置文件
- 高级恶意软件防护 (AMP) 启用程序配置文件

步骤 7 点击 **Submit**。
上传的 AnyConnect 表会显示您添加到思科 ISE 的 AnyConnect 资源。

下一步做什么

创建 AnyConnect 代理配置文件

创建本地请求方配置文件

您可以创建本地请求方配置文件来允许用户将其自己的设备带入思科 ISE 网络。当用户登录时，思科 ISE 使用与该用户的权限要求相关的配置文件选择必要的请求方调配向导。向导运行并设置用户的个人设备以访问网络。

注释 调配向导仅配置活动接口。因此，除非两个接口都是活动状态，具有有线和无线连接的用户不会为两个接口进行调配。

开始之前

- 打开 TCP 端口 8905 以支持安装思科 AnyConnect Agent、思科 Web 代理和请求方调配向导。有关端口用法的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“思科 ISE 设备端口参考”附录。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 依次选择**添加 (Add)** > **本地请求方配置文件 (Native Supplicant Profile)**。

步骤 3 使用 本地请求方配置文件设置，第 87 页中所述的步骤来创建配置文件。

下一步做什么

启用自助调配功能，允许员工直接将其个人设备连接到网络，在“对多个访客门户的支持”一节中进行了介绍。

本地请求方配置文件设置

在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略** > **策略元素** > **结果** > **客户端调配** > **资源** > **添加** > **本地请求方配置文件**时，将显示以下设置。

- **名称 (Name)**：输入您创建的本地请求方配置文件的名称。
- **操作系统 (Operating System)**：从下拉列表中选择此配置文件要应用于的操作系统。

每个配置文件定义思科 ISE 将应用于客户端本地请求方的网络连接的设置。

无线配置文件

配置一个无线配置文件，用于客户端可用的每个 SSID：

- **SSID 名称 (SSID Name)**：输入客户端将连接到的 SSID 的名称。
- **代理自动配置文件 URL (Proxy Auto-Config File URL)**：如果客户端将连接到代理以获取用于其请求方的网络配置，请输入该代理服务器的 URL。
- **代理主机/IP (Proxy Host/IP)**：如果客户端将连接到代理以获取用于其请求方的网络配置，请输入该代理服务器的 主机/IP。
- **代理端口 (Proxy Port)**：如果客户端将连接到代理以获取用于其请求方的网络配置，请输入该代理服务器的 代理。
- **安全 (Security)**：选择 **WPA** 或 **WPA2**。
- **允许的协议 (Allowed Procotol)**：选择 **PEAP** 或 **EAP-TLS**。
- **证书模板 (Certificate Template)**：对于 TLS，选择一个证书模板证书模板在**管理 (Administration)** > **系统证书 (System Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)**中定义。

可选设置

如果展开**可选 (Optional)**，则会显示以下字段。

Windows 设置

- **身份验证模式 (Authentication Mode)**选择**用户 (User)**、**计算机 (Machine)** 或**两者 (both)**作为进行授权的凭证。

- **不提示用户授权新服务器或受信任的证书颁发机构 (Do not prompt user to authorize new servers or trusted certification authorities)**：如果启用此选项，则不会提示用户授权。用户证书会被自动接受。
- **对连接使用不同的用户名 (Use a different user name for the connection)**：这仅适用于无线配置文件。会对连接使用不同的用户名。
- **网络不广播其名称 (SSID) 时也连接 (Connect even if the network is not broadcasting its name (SSID))**：这仅适用无线配置文件。即使未广播其 SSID，也要连接到网络。

iOS 设置

- **目标网络隐藏时启用 (Enable if Target Network is Hidden)**： 仅在隐藏目标网络时选中此复选框。

Android 设置

- **认证登记协议 (Certificate Enrollment Protocol:)**：单击以下任一单选按钮以选择认证登记协议：**安全传输注册 (EST) (Enrollment over Secure Transport [EST])** 或**简单证书注册协议 (SCEP) (Simple Certificate Enrollment Protocol [SCEP])**。如果您选择 EST 协议，思科 ISE 将在颁发证书时要求 Android 用户额外输入密码。

有线配置文件

- **允许的协议 (Allowed Protocol)**：选择 **PEAP** 或 **EAP-TLS**。
- **证书模板 (Certificate Template)**：对于 TLS，选择一个证书模板证书模板在**管理 (Administration)** > **系统证书 (System Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)**中定义。

可选设置

如果展开**可选 (Optional)**，以下字段对 Windows 客户端可用。

- **身份验证模式 (Authentication Mode)**选择**用户 (User)**、**计算机 (Machine)** 或**两者 (both)**作为进行授权的凭证。
- **自动使用登录名和密码（和域，如果有）(Automatically use logon name and password (and domain if any))**：如果选择了用于**身份验证模式**的**用户**，若信息可用，请使用登录名和密码，而无需提示用户。
- **启用快速重连接 (Enable Fast Reconnect)**：当 PEAP 协议选项中的会话恢复功能启用时，允许 PEAP 会话恢复，而不检查用户凭据，该功能在**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **PEAP** 上配置。
- **启用隔离检查 (Enable Quarantine Checks)**：检查客户端是否已隔离。
- **服务器不存在加密绑定 TLV 时断开 (Disconnect if server does not present cryptobinding TLV)**：网络连接不支持加密绑定 TLV 时断开。

- **不提示用户授权新服务器或受信任的证书颁发机构 (Do not prompt user to authorize new servers or trusted certification authorities)**：自动接收用户证书；不提示用户。

无面向不同网络的 URL 重定向的客户端调配

当第三方 NAC 不支持 CoA 时，需要无 URL 重定向的客户端调配。您可以在有无 URL 重定向的情况下执行客户端调配。

注释 对于有 URL 重定向的客户端调配，如果客户端计算机配置了代理设置，请确保将思科 ISE 添加到浏览器设置中的例外列表。此设置适用于所有使用 URL 重定向的流、BYOD、MDM、访客和终端安全评估。例如，在 Windows 计算机上执行以下操作：

1. 在控制面板中，单击 **Internet 属性 (Internet Properties)**。
2. 选择**连接**选项卡。
3. 单击**局域网设置 (LAN settings)**。
4. 单击“代理服务器”(Proxy server) 区域的**高级 (Advanced)**。
5. 在**例外**框中输入思科 ISE 节点的 IP 地址。
6. 点击**确定**。

以下是您在不重定向不同网络的情况下调配终端的步骤。

Dot1X EAP-TLS

1. 将思科 ISE 网络与已调配证书连接起来。
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户。

   AnyConnect 执行终端安全评估。终端会根据安终端全评估合规性转移至正确的网络。

Dot1X PEAP

1. 通过 NSP 将思科 ISE 网络与用户名和密码连接起来
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户

   AnyConnect 执行终端安全评估。终端会根据安终端全评估合规性转移至正确的网络。

MAB (有线网络)

1. 连接思科 ISE 网络。
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。

3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户。

   AnyConnect 执行终端安全评估。终端会根据安终端全评估合规性转移至正确的网络。

MAB (无线网络)

1. 连接思科 ISE 网络
2. 打开浏览器窗口，输入调配 URL：provisioning.cisco.com。
3. 通过内部用户、AD、LDAP 或 SAML 登录到 CP 门户。

   AnyConnect 执行终端安全评估。系统仅为无线 802.1X 启动终端安全评估。

AMP 启用程序配置文件设置

下表介绍了“高级恶意软件防护 (AMP) 启用程序配置文件”(Advanced Malware Protection (AMP) Enabler Profile) 窗口中的字段。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

点击 **Add** 下拉箭头，选择 **AMP Enabler Profile**。

表 *19: AMP Enabler Profile* 页面

字段名称	使用指南
Name	输入想要创建的AMP启用程序配置文件的名称。
Description	输入 AMP 启用程序配置文件的说明。
Install AMP Enabler	• **Windows 安装程序 (Windows Installer)**：指定托管 AMP for Windows OS 软件的本地服务器的 URL。 AnyConnect 模块使用此 URL 将 .exe 文件下载到终端。文件大小大约为 25 MB。 • **Mac 安装程序**：指定托管 AMP for macOS 软件的本地服务器的 URL。 AnyConnect 模块使用此 URL 将 .pkg 文件下载到终端。文件大小大约为 6 MB。 **Check** 按钮与服务器进行通信，验证 URL 是否有效。如果 URL 有效，则显示“File found”消息，否则显示错误消息。
Uninstall AMP Enabler	从终端卸载终端软件的 AMP。
Add to Start Menu	在终端上安装终端软件的 AMP 后，将终端软件 AMP 的快捷方式添加到终端的 Start 菜单中。

字段名称	使用指南
Add to Desktop	在终端上安装终端软件的 AMP 后，将终端软件的 AMP 图标添加到终端桌面上。
Add to Context Menu	在终端上安装终端软件的 AMP 后，将 Scan Now 选项添加到终端右键点击情景菜单中。

使用嵌入式配置文件编辑器创建 AMP 启用程序配置文件

使用思科 ISE 嵌入式配置文件编辑器或独立编辑器创建 AMP 启用程序配置文件。

要使用思科 ISE 嵌入式配置文件编辑器创建 AMP 启用程序配置文件，请执行以下操作：

开始之前

- 从 SOURCEfire 门户下载终端软件的 AMP，在本地服务器上托管 AMP。
- 将托管终端软件 AMP 的服务器的证书导入 ISE 证书存储区。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**。
- 确保在 **AnyConnect Configuration** 窗口 (**Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources** > **Add** > **AnyConnect Configuration** > **Select AnyConnect Package**) 的 **AnyConnect Module Selection** 和 **Profile Selection** 部分中选择了**思科高级恶意软件保护启用程序**选项。
- 必须登录 SOURCEfire 门户，为终端组创建策略，为终端软件下载 AMP。该软件使用您选择的策略进行了预配置。您必须下载两个映像，即，为 Windows OS 的终端软件下载 AMP 的可再分发版本，为 macOS 的终端软件下载 AMP。已下载的软件托管在一台可从企业网络访问的服务器上。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provision)** > **资源 (Resources)**。

步骤 2 点击 **Add** 下拉列表。

步骤 3 选择 **AMP Enabler Profile**，创建新的 AMP 启用程序配置文件。

步骤 4 在字段中输入适当的值。

使用独立编辑器创建 AMP 启用程序配置文件

要使用 AnyConnect 独立编辑器创建 AMP 启用程序配置文件，请执行以下步骤。

开始之前

您可以使用 AnyConnect 4.1 独立编辑器通过上传 XML 格式的配置文件来创建 AMP 启用程序配置文件。

- 从 Cisco.com 下载适用于 Windows 和 Mac OS 的 AnyConnect 独立配置文件编辑器。
- 启动独立配置文件编辑器，并输入 AMP 启用程序配置文件设置 中指定的字段。
- 在您的本地磁盘上将配置文件保存为 XML 文件。
- 确保在 **AnyConnect Configuration** 窗口 (**Policy** > **Policy Elements** > **Results** > **Client provisioning** > **Resources** > **Add** > **AnyConnect Configuration** > **Select AnyConnect Package**) 的 **AnyConnect Module Selection** 和 **Profile Selection** 部分中选择了**思科高级恶意软件保护启用程序**选项。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2 点击**添加 (Add)**。

步骤 3 选择 **Agent resources from local disk**。

步骤 4 从 **Category** 下拉列表中选择 **Customer Created Packages**。

步骤 5 从 **Type** 下拉列表中选择 **AMP Enabler Profile**。

步骤 6 输入 **Name** 和 **Description**。

步骤 7 点击 **Browse** 并从本地磁盘选择已保存的配置文件（XML 文件）。以下示例显示一个自定义安装文件。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

以下示例显示一个自定义卸载文件。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

步骤 8 点击 **Submit**。

新创建的 AMP 启用程序配置文件显示在**资源 (Resources)** 页面中。

常见 AMP 启用程序安装错误故障排除

当您在 Windows or MAC Installer 文本框中输入 SOURCEfire URL 并点击 **Check** 时，您可能会遇到下述错误中的一种：

- 错误消息：The certificate for the server containing the Mac/Windows installer file is not trusted by ISE。Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.

  如果您未将 SOURCEfire 受信任证书导入思科 ISE 证书库，系统会显示此错误消息。获取一个 SOURCEfire 受信任证书并将其导入思科 ISE 受信任证书库 (Administration > Certificates > Trusted Certificates)。

- 错误消息：The installer file is not found at this location, this may be due to a connection issue. Enter a valid path in the Installer text box or check your connection.

  当承载 AMP 或终端软件的服务器宕机或 Windows Installer or MAC Installer 文本框中有排字错误时，系统会显示此错误消息。

- 错误消息：The Windows/Mac installer text box does not contain a valid URL.

  当您输入语法上不正确的 URL 格式时，系统会显示此错误消息。

思科 ISE 支持登录 Chromebook 设备

不同于其他设备 (Apple、Windows、Android)，Chromebook 设备是受管设备（由 Google 域托管），且只提供有限的登录支持。思科 ISE 可支持网络上的 Chromebook 设备的登录。登录是指将所需的设置和文件传输至一个终端，由该终端在通过思科 ISE 身份验证后连接到一个安全网络的过程。该过程包括证书调配和/或本地请求方调配。但在 Chromebook 设备中，您只能执行证书调配。本机请求方调配通过 Google 管理员控制台完成。

非托管 Chromebook 设备无法登录到安全网络中。

Chromebook 登录过程中涉及的实体如下：

- Google 管理员
- ISE 管理员
- Chromebook 用户/设备
- Google 管理控制台（由 Google 管理员管理）

Google 管理员：

- 获得以下许可证：

1. Google 管理控制台配置所需的 Google Apps 管理员许可证 - URL: https://admin.google.com。管理员可使用 Google 管理控制台管理为某组织中的人员提供的 Google 服务。
2. Chromebook 设备管理许可证 - URL: https://support.google.com/chrome/a/answer/2717664?hl=en。Chromebook 设备管理许可证可用于配置设置，以及在特定 Chromebook 设备上执行策略。它可以让Google管理员访问设备设置，进而控制用户访问、自定义功能和配置网络访问等。

- 使用 Google 设备许可证实现 Chromebook 设备的调配和注册。
- 通过 Google 管理控制台管理 Chromebook 设备。
- 为每个 Chromebook 用户设置和管理 Wi-Fi 网络配置。
- 通过配置要安装在 Chromebook 设备上的应用和强制扩展程序，实现对 Chromebook 设备的管理。要登录 Chromebook 设备，需在 Chromebook 设备上安装 Cisco Network Setup Assistant 扩展程序。这样 Chromebook 设备可连接到思科 ISE，并安装 ISE 证书。由于只有受管设备才能执行安装证书操作，因此需强制安装扩展程序。
- 确保 Google 管理控制台上安装了思科 ISE 证书，以提供服务器验证和安全连接。Google 管理员可以决定是否应为某设备或用户生成证书。思科 ISE 提供以下选项：
  - 为不共享 Chromebook 设备的单个用户生成证书。
  - 为多名用户共享的 Chromebook 设备生成证书。要查看所需的其他配置，请参阅 在 Google 管理控制台中配置网络与强制扩展 章节中的步骤 5。

  Google 管理员安装 ISE 服务器证书后，ISE 便可以受信任地在 Chromebook 设备上执行证书调配，并支持基于证书的 EAP-TLS 身份验证。Google Chrome 37 及以上版本的支持 Chromebook 设备使用基于证书的身份验证。Google 管理员需在 Google 管理控制台中加载 ISE 调配，并使其适用于 Chromebook 设备，以便从 ISE 获取证书。
- 确保建议的 Google 主机名能够列在为实现 SSL 安全连接而在 WLC 中配置的 ACL 定义列表中。请参阅 Google 支持页面中建议和允许的主机名。

ISE 管理员：

- 定义包括了证书模板结构的 Chromebook 操作系统的本地请求者配置文件。
- 在思科 ISE 中为 Chromebook 用户创建必要的授权规则和客户端调配策略。

Chromebook 用户：

- 消除 Chromebook 设备，并将其登记至 Google 域，以便确保 Google 管理员定义的实施策略的安全。
- 接收 Chromebook 设备策略以及由 Google 管理控制台安装的 Cisco Network Setup Assistant 扩展程序。
- 连接到调配的 SSID（根据 Google 管理员的定义），打开浏览器，打开自带设备页面，并开始登录流程。
- Cisco Network Setup Assistant 在 Chromebook 设备上安装客户端证书，利用该证书，设备可以执行基于证书的 EAP-TLS 身份验证。

Google 管理控制台:

Google 管理控制台支持 Chromebook 设备管理，同时也支持配置安全网络并推送 Cisco Network Setup Assistant 证书管理扩展程序到 Chromebook。该扩展程序发送 SCEP 请求至思科 ISE，并安装客户端证书，用于支持安全连接和网络访问。

在共享环境中使用 Chromebook 设备的最佳实践

在共享的环境（如学校和图书馆）中使用 Chromebook 设备时，该 Chromebook 设备在不同的用户之间共享。思科建议的一些最佳实践包括：

- 当登录具有特定用户（学生或教授）名称的 Chromebook 设备时，用户名会填充在证书的主题 (Subject) 字段的通用名称 (CN) 中。此外，共享的 Chromebook 列于特定用户下的我的设备 (My Devices) 门户中。因此，建议共享设备在登录时使用共享凭证，以便设备仅在特定用户的我的设备 (My Devices) 门户列表下显示。该共享帐户可由管理员或教授作为单独帐户管理，以控制共享设备。
- 思科 ISE 管理员可以为共享的 Chromebook 设备创建自定义证书模板，并在策略中使用。例如，不使用与主题通用名称 (CN) 值匹配的标准证书模板，而可以在凭证中指定一个名称（例如，chrome-shared-grp1），同一名称也可以分配给 Chromebook 设备。策略可设计为与该名称匹配，以允许或拒绝对 Chromebook 设备的访问。
- 思科 ISE 管理员可以创建一个终端组，其中包含完成 Chromebook 登录所需的所有 Chromebook 设备的 MAC 地址（需要为其限制访问的设备）。授权规则应将其与设备类型 Chromebook 一起调用，这将允许访问重定向到 NSP。

Chromebook 登录过程

Chromebook 登录过程包括一系列步骤：

步骤 1 在 Google 管理控制台中配置网络与强制扩展 。
步骤 2 配置思科 ISE 以支持 Chromebook 登录。
步骤 3 擦除 Chromebook 设备。
步骤 4 注册 Chromebook 到 Google 管理控制台。
步骤 5 将 Chromebook 连接到思科 ISE 网络以实现 BYOD 登录。

在 Google 管理控制台中配置网络与强制扩展

Google 管理员执行以下步骤。

步骤 1 登录到 Google 管理员控制台。

a) 在浏览器输入以下 URL：https://admin.google.com。

b) 输入所需的用户名和密码。
c) 在**欢迎使用管理控制台 (Welcome to Admin Console)** 窗口中，请点击**设备管理 (Device Management)**。
d) 在**设备管理 (Device Management)** 窗口中，请点击**网络 (Network)**。

步骤 2 为受管设备创建 Wi-Fi 网络。

a) 在**网络 (Networks)** 窗口中，点击 **Wi-Fi**。
b) 点击**添加 Wi - Fi (Add Wi - Fi)** 以添加所需的 SSID。有关详细信息，请参阅 Google 管理控制台 - Wi-Fi 网络设置。

对于MAB流，请创建两个SSID，一个用于开放网络，另一个用于证书身份验证。当连接至开放网络时，思科 ISE ACL 将您重定向至信任的访客门户，进行身份验证。成功进行身份验证后，ACL 会将您重定向到 BYOD 门户。

如果 ISE 证书由中间 CA 颁发，则必须将中间证书映射到“服务器证书颁发机构”，而不是根 CA。

c) 点击**添加 (Add)**。

步骤 3 创建强制扩展程序。

a) 在**设备管理 (Device Management)** 窗口的**设备设置 (Device Settings)** 区域中，点击 **Chrome 管理 (Chrome Management)**。
b) 点击**用户设置 (User Settings)**。
c) 向下滚动，在**应用和扩展程序 (Apps and Extensions)** 部分的**强制安装的应用和扩展程序 (Force-Installed Apps and Extensions)** 选项中，点击**管理强制安装的应用 (Manage Force-Installed Apps)**。

步骤 4 安装强制的扩展程序。

a) 在**强制安装的应用和扩展程序 (Force-Installed Apps and Extensions)** 窗口中，点击 **Chrome Web Store**。
b) 在**搜索 (Search)** 文本框，输入“思科网络设置助手”(Cisco Network Setup Assistant) 以定位扩展程序。

Chromebook 设备的强制思科网络设置助手扩展程序向思科 ISE 请求证书，并且在 Chromebook 设备上安装 ISE 证书。因为证书安装仅允许在受管设备上进行，所以扩展程序必须配置为强制安装。如果在注册过程中扩展程序未安装，则无法安装思科 ISE 证书。

请参阅中的“思科 ISE 国际化和本地化”部分 中有关扩展程序支持的语言的详细信息。

c) 点击**添加 (Add)** 以强制安装应用。
d) 点击**保存 (Save)**。

步骤 5 （可选）定义配置文件，以在由多个用户共享的 Chromebook 设备中安装证书。

a) 将以下代码复制并粘贴在记事本文件，然后将其保存到您的本地磁盘。

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) 依次选择**设备管理 (Device Management)** > **Chromebook 管理 (Chromebook Management)** > **应用管理 (App Management)**。
c) 点击**思科网络设置助手 (Cisco Network Setup Assistant)** 扩展程序。
d) 点击**用户设置 (User Settings)** 并选择您的域。
e) 点击**上传配置文件 (Upload Configuration File)** 并选择您在本地磁盘保存的 .txt 文件。

注释　要使用思科网络设置助手为多个用户共享的设备创建证书，您必须在 Google 管理控制台中添加记事本文件。否则，思科 NSA 为单个用户创建证书。

f) 点击**保存 (Save)**。

步骤 6 （可选）为不共享 Chromebook 的单个用户安装证书。

a) 依次选择**设备管理 (Device Management)** > **网络 (Network)** > **证书 (Certificates)**。

b) 在**证书 (Certificates)** 窗口中，点击**添加证书 (Add Certificate)** 并上传思科 ISE 证书文件。

下一步做什么

配置思科 ISE 以支持 Chromebook 登录。

配置思科 ISE 以支持 Chromebook 登录

开始之前

思科 ISE 管理员必须创建所需的策略。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略集 (Policy Sets)** 窗口。

以下是授权策略的示例：

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess 是一种配置的授权结果。在思科 ISE GUI 中，单击**菜单** 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)** 窗口。

步骤 1 在思科 ISE 上配置的本地请求方配置文件 (NSP)。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

Chromebook 设备会显示在客户端调配 (Client Provisioning) 页面中，以便进行全新的思科 ISE 安装。但是，对于升级，您应下载终端安全评估更新。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **更新 (Updates)** 窗口。

b) 点击**添加 (Add)** > **本地请求方配置文件 (Native Supplicant Profile)**。

c) 输入**名称 (Name)** 和**说明 (Description)**。

d) 在**操作系统 (Operating System)** 字段，选择**Chrome OS 全部 (Chrome OS All)**。

e) 在**证书模版 (Certificate Template)** 字段，选择所需的证书模板。

f) 点击 **Submit**。请注意 SSID 是通过 Google 管理控制台而不是本地请求方调配流程进行调配。

步骤 2 映射“客户端调配”(Client Provisioning) 页面的 NSP。

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择**策略 (Policy)** > **客户端调配 (Client Provisioning)**。
b) 定义结果。
   - 在客户端调配策略的**结果 (Results)** 中选择内置本地请求方配置（思科 ISE Chrome NSP）。
   - 或者可以创建一个新规则，并确保选择为 Chromebook 设备创建的**结果 (Result)**。

擦除 Chromebook 设备

Google 管理控制台由 Google 管理员进行配置后，必须擦除 Chromebook 设备。Chromebook 用户必须擦除该设备（这是一个一次性过程）以强制分机和配置网络设置。有关详细信息，您可以参阅以下 URL：https://support.google.com/chrome/a/answer/1360642。

Chromebook 用户执行以下步骤：

步骤 1 按 **Esc-刷新-电源**按键组合。屏幕显示黄色感叹号 (!)。
步骤 2 按 **Ctrl -D** 按键组合启动设备模式，然后按 **Enter** 键。屏幕显示红色感叹号。
步骤 3 按 **Ctrl -D** 按键组合。Chromebook 删除其本地数据，返回初始状态。删除大约需要 15 分钟。
步骤 4 在过渡完成时，按**空格 (Spacebar)** 键，然后按 **Enter** 键返回已验证模式。
步骤 5 在登录前请注册 Chromebook。

下一步做什么

向 Google 管理控制台注册 Chromebook。

注册 Chromebook 到 Google 管理控制台

为调配 Chromebook 设备，Chromebook 用户必须首先在 Google 管理控制台页面注册，并接收设备策略和强制的扩展程序。

步骤 1 请启动 Chromebook 设备并按照屏幕上的说明进行操作，直到您在屏幕上看到登录窗口。现在先不要登录。
步骤 2 在登录到 Chromebook 设备之前，请按 **Ctrl-Alt-E** 组合键。系统将显示**企业注册 (Enterprise Enrolment)** 屏幕。
步骤 3 输入您的电子邮件地址，然后点击**下一步 (Next)**。
您将会收到以下消息：您的设备已成功登记企业管理。
步骤 4 点击 **Done**。
步骤 5 输入您 Google 管理员欢迎函中的用户名和密码，或您的有注册资格的账号上现有 Google 应用用户的用户名和密码。
步骤 6 点击**注册设备 (Enroll Device)**。您将收到一条设备已成功注册的确认消息。

注意：Chromebook 设备注册是一次性的。

将 Chromebook 连接到思科 ISE 网络以实现 BYOD 登录

该程序适用于双 SSID - 要使用 EAP-TLS 协议连接到 802.x 网络，Chromebook 用户需要执行以下步骤：

注释 如果使用双 SSID - 当从 802.x PEAP 连接 EAP-TLS 网络时，应在网络请求方（不是 Web 浏览器）中输入凭证以连接到网络。

步骤 1 在 Chromebook 中，点击**设置 (Settings)**。

步骤 2 在**互联网连接 (Internet Connection)** 部分，点击**调配 Wi-Fi 网络 (Provisioning Wi-Fi Network)**，然后点击您的网络。

步骤 3 此时会打开需要提供凭证的访客门户。

1. 在“登录”(Sign On) 页面，输入**用户名 (Username)** 和**密码 (Password)**。
2. 点击**登录 (Sign On)**。

步骤 4 在 BYOD 欢迎页面，请点击**开始 (Start)**。

步骤 5 在**设备信息 (Device Information)** 字段中，为设备输入名称和说明。例如，“个人设备：Jane 的学校用 Chromebook 或共享设备：图书馆 Chromebook 1 或教室 1 Chromebook 1”。

步骤 6 点击**继续 (Continue)**。

步骤 7 在**思科网络设置助手 (Cisco Network Setup Assistant)** 对话框中，点击**是 (Yes)** 以安装证书访问安全网络。

如果 Google 管理员配置了安全 Wi-Fi，则应该会自动建立网络连接。如果没有，请从可用网络列表中选择安全 SSID。

已在域中登记并且装有思科网络设置助手扩展程序的 Chromebook 用户可以更新该扩展程序，无需等待自动更新。通过执行以下步骤手动更新扩展程序。

1. 在 Chromebook 上，打开浏览器并输入以下 **URL：chrome://Extensions**。
2. 选中开发人员模式 (**Developer Mode**) 复选框。
3. 点击**立即更新扩展程序 (Update Extensions Now)**。
4. 检查并验证思科网络设置助手扩展程序版本为 2.1.0.35 和更高版本。

Google 管理控制台 - Wi-Fi 网络设置

Wi-Fi 网络配置用于配置客户网络中的 SSID 或使用证书属性与证书匹配（用于 EAP-TLS）。当证书安装于 Chromebook 时，它与 Google 管理设置同步。仅在其中一个已定义的证书属性与 SSID 配置匹配时方可建立连接。

下列为必填字段，专用于 EAP-TLS、PEAP 和开放网络流，由 Google 管理员配置，以在 Google 管理控制台 (Google Admin Console) 页面中为每位 Chromebook 用户建立 Wi-Fi 网络（**设备管理 [Device Management] > 网络 [Network] > Wi-Fi > 添加 Wi-Fi [Add Wi-Fi]**）。

字段	EAP-TLS	PEAP	开放
Name	输入网络连接的名称。	输入网络连接的名称。	输入网络连接的名称。
服务集标识符 (SSID)	输入 SSID（例如，tls_ssid）。	输入 SSID（例如，tls_ssid）。	输入 SSID（例如，tls_ssid）。
不广播该 SSID (This SSID Is Not Broadcast)	选择相应选项。	选择相应选项。	选择相应选项。
自动连接 (Automatically Connect)	选择相应选项。	选择相应选项。	选择相应选项。
安全类型 (Security Type)	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	开放
可扩展身份验证协议	EAP-TLS	PEAP	—
内部协议 (Inner Protocol)	—	• Automatic • MSCHAP v2（选择相应选项） • MD5 • PAP • MSCHAP • GTC	—
外部身份 (Outer Identity)	-	-	-
用户名	在用户登录时设置固定值或使用变量（可选）：${LOGIN_ID} 或 ${LOGIN_EMAIL}。	输入 PEAP 凭证以对 ISE（内部 ISE 用户/AD/其他 ISE 身份）和“密码”(Password) 字段进行身份验证。	—

字段	EAP-TLS	PEAP	开放
服务器证书颁发机构 (Server Certificate Authority)	选择 ISE 证书（自“设备管理”[Device Management] > “网络”[Network] > “证书”[Certificates] 导入）。	选择 ISE 证书（自“设备管理”[Device Management] > “网络”[Network] > “证书”[Certificates] 导入）。	—
限制通过平台接入此 Wi-Fi 网络 (Restrict Access to this Wi-Fi Network by Platform)	• 选择移动设备。 • 选择 Chromebook。	• 选择移动设备。 • 选择 Chromebook。	—
客户端注册 URL (Client Enrollment URL)	输入一个 URL，当用户未注册时，Chromebook 设备浏览器为该用户重定向至此 URL。在无线局域网控制器上配置用于为未注册用户重定向的 ACL。	-	-

字段	EAP-TLS	PEAP	开放
颁发者模式 (Issuer Pattern)	证书中的一个属性。至少选择一个来自颁发者模式或主题模式的属性，而且这两个模式需与安装的证书属性匹配。指定要与 Chromebook 设备匹配的证书属性，用于接收证书。 • 通用名称 (Common Name)：指证书的“主题”(Subject) 字段或指证书的“主题”(Subject) 字段中的通配符域，它必须与节点的 FQDN 匹配。 • 位置 (Locality)：指与证书主题相关的测试位置（城市）。 • 组织 (Organization)：指与证书主题相关的组织名称。 • 组织单位 (Organizational Unit)：指与证书主题相关的组织单位名称。	-	-

字段	EAP-TLS	PEAP	开放
主题模式 (Subject Pattern)	证书中的一个属性。至少选择一个来自颁发者模式或主题模式的属性，而且这两个模式需与安装的证书属性匹配。指定要与 Chromebook 设备匹配的证书属性，用于接收证书。 • 通用名称 (Common Name)：指证书的“主题”(Subject) 字段或指证书的“主题”(Subject) 字段中的通配符域，它必须与节点的 FQDN 匹配。 • 位置 (Locality)：指与证书主题相关的测试位置（城市）。 • 组织 (Organization)：指与证书主题相关的组织名称。 • 组织单位 (Organizational Unit)：指与证书主题相关的组织单位名称。	-	-

字段	EAP-TLS	PEAP	开放
代理设置	• 直接互联网接入 (Direct Internet Connection)（已选） • 手动代理配置 (Manual Proxy Configuration) • 自动代理配置 (Automatic Proxy Configuration)	• 直接互联网接入 (Direct Internet Connection)（已选） • 手动代理配置 (Manual Proxy Configuration) • 自动代理配置 (Automatic Proxy Configuration)	—
应用网络 (Apply Network)	按用户 (By User)	按用户 (By User)	—

监控思科 ISE 中的 Chromebook 设备活动

思科 ISE 提供多种报告和日志以查看 Chromebook 设备身份验证和授权的相关信息。您可以按需或定期运行这些报告。可以查看身份验证方法（例如 802.1x）和身份验证协议（例如 EAP-TLS）。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live Logs)** 窗口。还可以确定归类为 Chromebook 设备的终端数量。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **网络访问 (Network Access)** > **身份 (Identities)** > **终端 (Endpoints)** 窗口

排除 Chromebook 设备登录故障

本节介绍在登录 Chromebook 设备时您可能会遇到的问题。

- 错误：无法从应用商店安装扩展名 - 您无法安装从 Webstore 安装扩展名。将由网络管理员自动安装在您的 Chromebook 设备上。
- 错误：证书安装完成，但是无法连接到安全网络 - 在管理控制台上验证已安装证书与定义的颁发者/主题属性模式匹配。您可以从此处获取有关安装证书的信息：chrome://settings/certificates
- 错误：当尝试手动连接到 Chromebook 的安全网络时，显示错误消息“获取网络证书”- 点击“获取新证书”(Get New Certificate)，浏览器打开并将您重定向到 ISE 自带设备流程安装证书。但是，如果您无法连接到安全网络，请在管理控制台上验证已安装证书与定义的颁发者/主题属性模式匹配。
- 错误：点击“获取新证书”(Get New Certificate)，但会转至 www.cisco.com 网站 - 为了被重定向到 ISE 并开始证书安装过程，用户需要连接到调配 SSID。请确保已为此网络定义正确的访问列表。
- 错误：显示错误消息“仅受管设备可使用此扩展名。请联系服务中心或网络管理员”-Chromebook 是一个受管设备，扩展名必须配置为强制安装以获得 Chrome 操作系统 API 访问权限在设备上

安装证书。虽然扩展名可通过从 Google Webstore 下载手动安装，但是未注册的 Chromebook 用户无法安装该证书。

如果用户属于域用户组，未注册 Chromebook 设备可以获得证书。扩展名跟踪所有设备的域用户。但是域用户可以为未注册设备的生成基于用户的身份验证密钥。

- 错误：Google 管理控制台中 SSID 连接的顺序不明 -
  - 如果 Google 管理控制台配置了多个 SSID （PEAP 和 EAP-TLS）在，在安装证书且匹配属性后，Chrome 操作系统会通过基于证书的身份验证自动连接到 SSID，无论 SSID 以什么顺序配置。
  - 如果两个 EAP-TLS SSID 匹配相同的属性，则连接取决于无法通过用户或管理员控制的其他因素（例如信号强度和其他网络级别信号）。
  - 如果 Chromebook 设备上安装多个 EAP-TLS 证书，并且它们全部与管理控制台上已配置的证书模式匹配，则最新的证书将用于连接。

思科 AnyConnect 安全移动

思科 ISE 使用 思科 AnyConnect 中的集成模块来满足思科 ISE 终端安全评估要求。

注释 AnyConnect 不支持 CWA 流 。您无法通过访客门户使用 **工作中心访客访问** > **门户和组件** > **访客门户** > **创建、编辑或复制** > **门户行为和流设置** > **访客设备合规性设置** 窗口中的 **要求访客设备合规** 字段来调配 AnyConnect。相反，应在客户端调配门户上调配AnyConnect。此方法会导致按照授权权限中的配置进行重定向。

当将思科 ISE 与 思科 AnyConnect 代理集成时，思科 ISE 会：

- 充当暂存服务器以部署 思科 AnyConnect 4.0 版本及其未来版本
- 与 AnyConnect 终端安全评估组件进行交互以满足思科 ISE 终端安全评估要求
- 支持部署 思科 AnyConnect 配置文件、自定义及语言包，以及 Windows 和 Mac OS x 操作系统的 OPSWAT 库更新
- 同时支持 思科 AnyConnect 和传统代理

注释 在切换网络介质时，必须更改默认网关，以便终端安全评估模块能够检测网络更改并重新评估客户端。

创建 AnyConnect 配置

AnyConnect 配置包括 AnyConnect 软件及其相关的配置文件。可在允许用户下载 AnyConnect 资源并将其安装到客户端上的客户端调配策略中使用此配置。如果您使用 ISE 和 ASA 部署 AnyConnect，则两个前端上的配置必须匹配。

要在连接到 VPN 时推送 ISE 终端安全评估模块，Cisco 建议您通过使用思科自适应安全设备管理器 (ASDM) GUI 工具的思科自适应安全设备 (ASA) 安装 AnyConnect 代理。ASA 使用 VPN 下载程序执行安装。在下载后，将通过 ASA 推送 ISE 终端安全评估配置文件，并在 ISE 终端安全评估模块联系 ISE 之前提供随后调配该配置文件所需的发现主机。而对于 ISE，ISE 终端安全评估模块只会在发现 ISE 后获取该配置文件，这有可能导致错误。因此，在连接到 VPN 时，建议使用 ASA 推送 ISE 终端安全评估模块。

注释 当思科 ISE 与 ASA 集成时，请确保在 ASA 中将记帐模式设置为**单一 (Single)**。记帐数据在“单一”(Single) 模式下仅发送到一个记帐服务器。

开始之前

在配置 AnyConnect 配置对象之前，必须：

1. 从 Cisco 软件下载页面下载 AnyConnect 前端部署数据包和合规性模块。
2. 将这些资源上传到思科 ISE（请参阅从本地计算机添加思科提供的客户端调配资源，第 85 页）。
3. （可选）添加自定义和本地化捆绑包（请参阅从本地计算机添加 AnyConnect 的客户创建资源，第 85 页）。
4. 配置 AnyConnect 终端安全评估代理配置文件（请参阅 创建终端安全评估代理配置文件，第 107 页）。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provision)** > **资源 (Resources)**。

步骤 2 点击 **添加** 创建 AnyConnect 配置。

步骤 3 选择 **AnyConnect 配置**。

步骤 4 选择您之前上传的 AnyConnect 软件包。例如， AnyConnectWindows xxx.x.xxxxx.x。

步骤 5 输入当前 AnyConnect 配置的名称。例如，AC Config xxx.x.xxxxx.x。

步骤 6 选择您之前上传的合规性模块。例如，AnyConnectComplianceModulewindows x.x.xxxx.x

步骤 7 选中一个或多个 AnyConnect 模块复选框。例如，从下列软件中选择一个或多个模块：ISE Posture、VPN、网络访问管理器、网络安全、AMP 启用程序、ASA Posture、Start Before Log on（仅适用于 Windows OS）以及诊断和报告工具。

注释　取消选中 AnyConnect 模块选择下的 VPN 模块，不会在调配的客户端禁用 VPN 磁贴。您必须配置 VPNDisable_ServiceProfile.xml，才能在 AnyConnect GUI 上禁用 VPN 磁贴。在将 AnyConnect 安装到默认位置的系统中，可以在 C:\Program Files\Cisco 下找到此文件。如果 AnyConnect 安装到不同位置，则此文件将位于 <AnyConnect 安装的路径>\Cisco 下。

步骤 8　为选定的 AnyConnect 模块选择 AnyConnect 配置文件。例如，ISE Posture、VPN、NAM 和网络安全模块。

步骤 9　选择 AnyConnect 自定义和本地化捆绑包。

步骤 10　点击**提交**。

创建终端安全评估代理配置文件

按照此程序创建 AnyConnect 终端安全评估代理配置文件，您可以在其中指定参数以定义终端安全评估协议的代理行为。

步骤 1　在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **客户端调配 (Client Provisioning)** > **资源 (Resources)**。

步骤 2　点击**添加 (Add)**。

步骤 3　选择 **AnyConnect 终端安全评估配置文件**。

步骤 4　输入配置文件的**名称**。

步骤 5　配置以下各项的参数：

- 思科 ISE 终端安全评估代理行为
- 客户端 IP 地址更改
- 思科 ISE 安全评估协议

步骤 6　点击**提交**。

客户端 IP 地址刷新配置

下表描述 NAC AnyConnect 终端安全评估配置文件窗口中的字段，您可以通过此窗口为客户端配置在 VLAN 更改之后要更新或刷新其 IP 地址的参数。在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **Policy** > **Policy Elements** > **Resilts** > **Client Provisioning** > **Resources** > **Add** > **AnyConnect Posture Profile**。

字段名称	默认值	使用指南
“VLAN 检测时间间隔”(VLAN detection interval)	0, 5	此设置是代理检查 VLAN 更改的时间间隔。 对于 Mac OS X 代理，默认值为 5。默认情况下，已启用访问身份验证 VLAN 更改功能，对于 Mac OS X，VlanDetectInteval 为 5 秒。有效范围为 5 至 900 秒。 0 - 禁用访问身份验证 VLAN 更改功能。 1 至 5 - 代理每隔 5 秒发送一个互联网控制消息协议 (ICMP) 或地址解析协议 (ARP) 查询。 6 至 900 - 每隔 x 秒发送一个 ICMP 或 ARP 查询。
Enable VLAN detection without UI（不适用于 Mac OS X 客户端）	否	即使用户未登录，此设置仍可启用或禁用 VLAN 检测。 “否” - 禁用 VLAN 检测功能。 “是” - 启用 VLAN 检测功能。
“重试检测计数”(Retry detection count)	3	如果互联网控制消息协议(ICMP)或地址解析协议 (ARP) 轮询失败，此设置将代理配置为重试 x 次再刷新客户端 IP 地址。
“Ping 命令或 ARP”(Ping 命令或 ARP)	0 有效范围为 0 至 2。	此设置指定用于检测客户端 IP 地址更改的方法。 0 - 使用 ICMP 轮询 1 - 使用 ARP 轮询 2 - 首先使用 ICMP 轮询，然后（如果 ICMP 失败）使用 ARP 轮询
“ping 命令最长超时时间”(Maximum timeout for ping)	1 有效范围为 1 至 10 秒。	使用 ICMP 轮询，并且如果在指定时间内没有响应，则宣布 ICMP 轮询失败。
“启用代理 IP 地址刷新”(Enable agent IP refresh)	“是”（默认值）	指定在交换机（或 WLC）更改相应交换机端口上客户端登录会话的 VLAN 之后客户端设备是否更新或刷新其 IP 地址。

字段名称	默认值	使用指南
“DHCP 更新延迟”(DHCP renew delay)	0 有效范围为 0 至 60 秒。	此设置指定客户端设备在尝试向网络 DHCP 服务器请求新 IP 地址之前等待的时间。
“DHCP 释放延迟”(DHCP release delay)	0 有效范围为 0 至 60 秒。	此设置指定客户端设备在释放当前 IP 地址之前等待的秒数。

注释 将参数值与现有代理配置文件设置合并或覆盖这些设置，从而相应地配置 Windows 客户端和 Mac OS X 客户端以刷新 IP 地址。

安全评估协议设置

下表介绍 “AnyConnect 终端安全评估配置文件”(AnyConnect Posture Profile) 窗口中的字段，您可以通过此页面配置 AnyConnect 安全评估协议设置。有关详细信息，请参阅 AnyConnect 版本对应的《思科 AnyConnect 安全移动客户端管理员指南》。

字段名称	默认值	使用指南
PRA 重新传输时间 (PRA Retransmission Time)	120 秒	如果存在被动重新评估通信失败，这是代理重试期。
重新传输延迟 (Retransmission Delay)	60 秒	在重试之前等待的时间（秒）
重新传输限制 (Retransmission Limit)	4	邮件允许的重试次数。
发现主机 (Discovery Host)	—	输入通过 NAD 路由的任何 IP 地址或 FQDN。NAD 会检测该 HTTP 流量并将其重定向到客户端调配门户。
发现备份服务器列表 (Discovery Backup Server List)	—	从下拉列表中选择 PSN。AnyConnect会探测此服务器列表，以查找必须在其上执行安全评估的 PSN 节点。如果不选择任何 PSN，节点组或集群中的所有 PSN 都将作为备份服务器列表发送到 AnyConnect。
Server Name Rules	—	由带有通配符且以逗号分隔的名称组成的列表，用于定义代理可以连接到的服务器。

字段名称	默认值	使用指南
Call Home 列表	—	输入逗号分隔的 IP 地址和端口列表，在 IP 地址和端口之间输入冒号。
回退计时器	30 秒	使用此设置，AnyConnect 代理能够通过发送发现数据包持续到达发现目标（重定向目标和之前连接的PSN），直到达到此最大时间限制为止。有效范围为 10 至 600 秒。

连续的终端属性监控

可以使用 AnyConnect 代理连续监控不同终端属性，以确保在安全评估期间观察动态变化。这会提高终端的整体可视性，并帮助您根据其行为创建安全评估策略。 AnyConnect 代理监控安装并运行在终端上的应用。您可以打开和关闭此功能，并配置应监控数据的频率。默认情况下，每 5 分钟收集一次数据，并存储在数据库中。在初始安全评估过程中，AnyConnect 报告正在运行和已安装的应用的完整列表。在初始安全评估后， AnyConnect 代理每 X 分钟扫描一次应用，并将其与最后一次扫描的差异发送到服务器。服务器显示正在运行和已安装的应用的完整列表。

双向安全评估流程

有时，由于网络配置发生更改，思科ISE可能会将客户端或终端更改为待处理状态。但是，AnyConnect 无法检测到更改，并让客户端或终端保持在合规状态。因此，安全评估状态不匹配，理想情况下，必须在此场景中探测思科 ISE 才能获得正确的安全评估状态。您可以通过将 AnyConnect 配置为以指定的时间间隔探测思科 ISE，以便在客户端或终端的安全评估状态为待处理时，此探测将防止客户端或终端在思科 ISE 中停留在“待处理”状态。

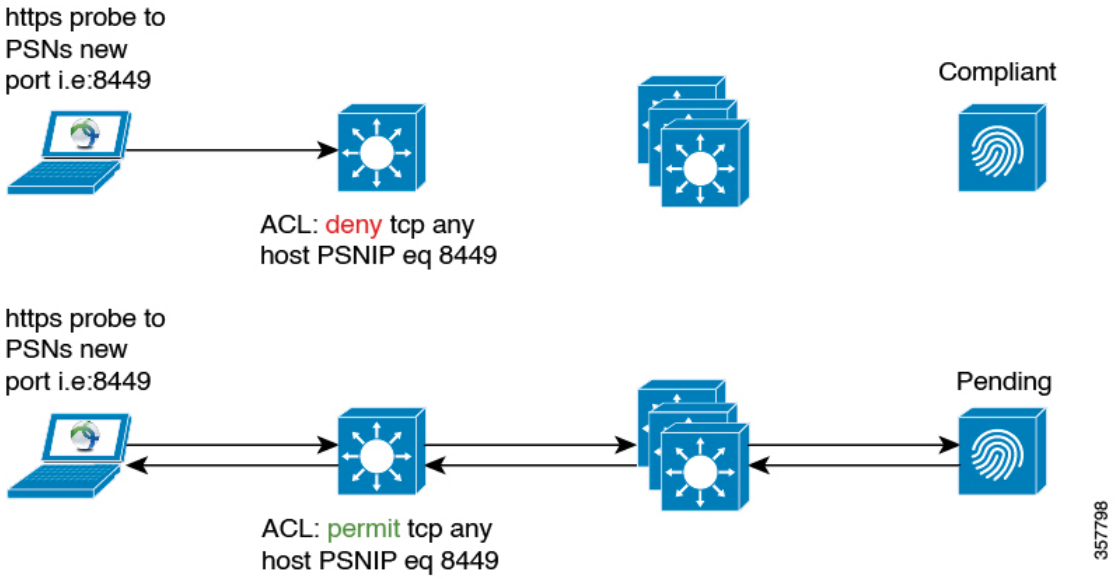
Windows、Linux 和 MacOS 客户端支持双向安全评估流程。

双向安全评估流程包括以下步骤：

1. 客户端尝试连接到网络。
2. PSN 执行终端安全评估流程。如果客户端符合终端安全评估策略，则终端会被移至合规状态。
3. AnyConnect 代理从思科 ISE 接收安全评估探测备份列表和安全评估状态同步间隔的配置详细信息。
4. AnyConnect 代理以指定的间隔开始探测思科 ISE。

   例如，思科 ISE 将安全评估状态显示为待处理， AnyConnect 将安全评估状态显示为合规。当 AnyConnect 探测思科 ISE 并获知新状态时，可能会触发重新评估。

图 5: 双向安全评估流程



注释 如果客户端的状态因任何原因变为 **待处理**，则 AnyConnect 代理将收到来自客户端的探测请求。它将探测并从思科 ISE 接收正确的客户端状态，然后将客户端移至正确的状态。

配置双向安全评估流程

步骤 1 在 **AnyConnect 终端安全评估配置文件**中配置**终端安全评估备份列表** 和**终端安全评估状态同步间隔**。为此：

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)**。

b) 从 **添加** 下拉列表中，选择 **AnyConnect 安全评估配置文件**。

c) 在**代理行为 (Agent Behavior)** 区域中配置以下设置：

- **终端安全评估备份列表**：从此下拉列表中，选择 AnyConnect 必须为终端安全评估合规性状态检测的 PSN。您最多可以选择六个 PSN。

  AnyConnect 向这些 PSN 发送探测，以检查终端的终端安全评估合规性状态是否仍然有效。如果不选择任何 PSN，则连接的 PSN 和任何两个备份服务器将用作状态安全状态同步的备份。

- **终端安全评估状态同步间隔**：定义 AnyConnect 与思科 ISE 同步终端安全评估状态的频率。有效范围为 0 到 300。如果输入 0，则会禁用终端安全评估状态同步探测。如果此值大于 0，则必须为合规授权配置文件阻止终端安全评估状态同步端口。

步骤 2 配置端口 8449 以进行双向通信。为此：

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 客户端调配门户 (Client Provisioning Portals) > 门户行为和流程设置**。

b) 单击**门户设置 (Portal Settings)**。

c) 在**双向端口 (Bidirectional Port)** 字段中，确保将端口 8449 设置为双向通信。

默认情况下，端口 8449 会被用于双向通信。

步骤 3 配置 ACL 以便在客户端安全评估状态合规时阻止安全评估状态同步探测到达思科 ISE。为此：

a) 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 可下载的 ACL (Downloadable ACLs)**。

b) 配置 ACL。

确保仅允许处于待处理状态的客户端通过双向端口访问配置的PSN。这样将避免来自处于合规状态的客户端的不需要的流量。以下是 ACL 的示例：

```
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
permit ip any any
```

如果没有配置 ACL，就会在思科 ISE 控制面板上触发姿态配置检测警报。仅应在符合要求的策略集上配置 ACL。此警报的主要目的是防止流向思科 ISE 的大量流量。

注释 确保当客户端处于待处理状态时，防火墙不会阻止相应端口上的通信。

思科 Web 代理

思科 Web 代理为客户端设备提供临时安全评估。

用户可以启动思科 Web 代理可执行文件，此文件会通过 ActiveX 控件或 Java 小应用程序在客户端设备上的临时目录中安装 Web 代理文件。

用户登录思科 Web 代理后，Web 代理会从思科 ISE 服务器获取为用户角色和操作系统配置的要求，检查主机注册表、进程、应用和服务以获取所需的数据包，并向思科 ISE 服务器发回报告。如果客户端设备满足这些要求，用户就可以访问网络。如果不满足这些要求，Web 代理会向用户显示对话框，指出没有满足的各项要求。此对话框会为用户提供让客户端设备满足要求的说明和应执行的操作。或者，如未满足指定的要求，用户可以选择接受有限网络访问，同时尝试对客户端系统进行补救以满足对用户登录角色的要求。

注释 仅 32 位版本的 Internet Explorer 支持 ActiveX。无法安装在 Firefox Web 浏览器或 64 位版本的 Internet Explorer 上安装 ActiveX。

配置客户端调配资源策略

对于客户端，客户端调配资源策略确定在登录和用户会话启动时哪些用户会从思科 ISE 收到哪个版本的资源（代理、代理合规性模块和代理自定义包或配置文件）。

对于 AnyConnect，可以从 **客户端调配资源** 窗口选择资源，创建可在**客户端调配策略** 窗口中使用的 AnyConnect 配置。AnyConnect 配置指定了 AnyConnect 软件及其与不同配置文件的关联，其中包括 Windows 和 Mac OSX 和 Linux 客户端的 AnyConnect 二进制包、合规性模块、模块配置文件以及 AnyConnect 的自定义包和语言包。

开始之前

- 请确保您已将资源添加到思科 ISE，然后才能创建有效的客户端调配资源策略。当您下载代理合规性模块时，它始终会覆盖系统中可用的现有模块（如果有）。
- 检查客户端配置中使用的原生 Supplicant 客户端配置文件，并确保无线 SSID 是正确的。对于 iOS 设备，如果您尝试连接到的网络已隐藏，请从 **iOS 设置 (iOS Settings)** 区域中，选中 **目标网络隐藏时启用 (Enable if target network is hidden)** 复选框。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 **策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 从**行为 (Behavior)** 下拉列表中，选择以下选项之一：

- **启用 (Enable)**：确保思科 ISE 使用此策略，以在用户登录到网络时帮助实现客户端调配功能，并帮助遵守客户端调配策略规定。
- **禁用 (Disable)**：思科 ISE 不使用指定的资源策略来实现客户端调配功能。
- **监控 (Monitor)**：禁用策略并“观察”客户端调配会话请求，以查看思科 ISE 尝试根据“受监控”策略进行调用的次数。

步骤 3 在**规则名称 (Rule Name)** 文本框中输入新资源策略的名称。

步骤 4 指定登录到思科 ISE 的用户可能所属的一个或多个身份组。

您可以选择指定**任何 (Any)** 身份组类型，或者从已配置的现有身份组列表中选择一个或多个组。

步骤 5 使用**操作系统 (Operating Systems)** 字段指定可能在用户登录到思科 ISE 所通过的客户端计算机或设备上运行的一个或多个操作系统。

注释　虽然在思科 ISE GUI 的 **客户端调配** 窗口中提供了选择 macOS 10.6、10.7 和 10.8 的选项，但 AnyConnect 不支持这些版本。

步骤 6 在**其他条件 (Other Conditions)** 字段中，指定要为此特定资源策略创建的新表达式。

步骤 7 对于客户端计算机，使用**代理配置 (Agent Configuration)** 选项指定将在客户端计算机上供使用和进行调配的代理类型、合规性模块、代理自定义包和配置文件。

必须在授权策略中包含客户端调配 URL，以使代理能够在客户端计算机中弹出。这会阻止来自任何随机客户端的请求，并且确保只有具有正确重定向 URL 的客户端可以请求安全状态评估。

步骤 8 点击保存。

下一步做什么

在您已成功配置一个或多个客户端调配资源策略后，即可开始配置思科 ISE，以在登录过程中在客户端计算机上执行安全评估。

在客户端调配策略中配置思科 ISE 安全评估代理

对于客户端计算机，请配置代理类型、合规性模块、代理自定义包和/或配置文件，使之可供使用和调配，以便用户下载和安装到客户端计算机。

开始之前

您必须在思科 ISE 中为 AnyConnect 添加客户端调配资源。

步骤 1 从 **Agent** 下拉列表中选择可用代理，并根据需要启用或禁用 **Is Upgrade Mandatory** 选项来指定此处定义的代理升级（下载）对于客户端设备而言是否为强制性的。

Is Upgrade Mandatory 设置仅适用于代理下载。代理配置文件、合规性模块和代理自定义包更新始终为强制性的。

步骤 2 从 **Profile** 下拉列表中选择现有的代理配置文件。

步骤 3 使用 **Compliance Module** 下拉列表选择要下载到客户端设备的可用合规性模块。

步骤 4 从 **Agent Customization Package** 下拉列表中选择用于客户端设备的可用代理自定义包。

为个人设备配置本地请求方

员工可以直接使用本地请求方将个人设备连接至网络，本地请求方可用于 Windows、Mac OS、iOS 和 Android 设备。对于个人设备，请指定在所注册的个人设备上提供和调配哪个本地请求方配置。

开始之前

创建本地请求方配置文件，使思科 ISE 在用户登录时根据您为用户授权要求关联的配置文件提供必要的请求方调配向导，以将用户个人设备设置为接入网络。

步骤 1 在思科 ISE GUI 中，单击**菜单** 图标 (☰)，然后选择 选择**策略 (Policy)** > **客户端调配 (Client Provisioning)**。

步骤 2 从行为下拉列表中选择**Enable**、**Disable** 或 **Monitor**。

步骤 3 在 Rule Name 文本框中输入新资源策略的名称。

步骤 4 指定以下项：

- 使用 **Identity Groups** 字段指定登录思科 ISE 的用户可能隶属的一个或多个身份组。
- 使用 **Operating System** 字段指定用户个人设备上可能运行的、用户借以登录思科 ISE 的一个或多个操作系统。

- 使用 **Other Conditions**字段指定想要为此特定资源策略创建的新表达式。

步骤 5 对于个人设备，请使用**本地请求方配置 (Native Supplicant Configuration)** 以选择向这些个人设备分发的具体 **Configuration Wizard**。

步骤 6 为特定个人设备类型指定适用的 **Wizard Profile**。

步骤 7 点击**保存**。

客户端调配报告

可以访问思科 ISE 监控和故障排除功能，以检查成功或失败的用户登录会话的整体趋势，收集有关在指定时间段登录网络的客户端计算机的数量和类型的统计信息，或检查客户端调配资源中的所有最新配置更改。

客户端调配请求

操作 (Operations) > **报告 (Reports)** > **ISE 报告 (ISE Reports)** > **终端和用户 (Endpoints and Users)** > **客户端调配 (Client Provisioning)** 报告显示有关成功和失败的客户端调配请求的统计信息。当选择 **Run** 并指定其中一个预设时间段时，思科 ISE 会梳理数据库并显示产生的客户端调配数据。

请求方调配请求

Operations > **Reports** > **ISE Reports** > **Endpoints and Users** > **Supplicant Provisioning** 窗口显示有关最新成功和失败的用户设备注册和请求方调配请求的信息。当选择 **Run** 并指定其中一个预设时间段时，思科 ISE 会梳理数据库并显示产生的请求方调配数据。

Supplicant Provisioning 报告提供有关特定时间段内通过设备注册门户注册的终端列表的信息，包括登录日期和时间、身份（用户 ID）、IP 地址、MAC 地址（终端 ID）、服务器、配置文件、终端操作系统、SPW 版本、故障原因（如有）和注册状态等数据。

客户端调配事件日志

您可以搜索事件日志条目，帮助诊断客户端登录行为可能存在的问题。例如，您网络上的客户端设备在登录后无法获取客户端调配资源更新，您可能需要确定问题的原因。您可以将日志条目用于安全评估和客户端调配审核以及安全评估和客户端调配诊断。

客户端调配门户的门户设置

要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **创建、编辑、复制或删除 (Create, Edit, Duplicate, or Delete)** > **门户行为和流量设置 (Portal Behavior and Flow Settings)**。

门户设置

- **HTTPS 端口 (HTTPS Port)**：输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（**阻止列表**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：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：设置用户在达到**速率限制之前最大失败登录尝试次数**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。

客户端调配门户语言文件的 HTML 支持

要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

注释 以下是文件中字典键的不完整列表。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1

- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

当地语言翻译版本说明

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