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 45 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 无客户端模式工作流程。

- **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。

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 无客户端模式工作流程
配置思科临时代理工作流程

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、NAC 代理或 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. 依次选择**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

相关主题

配置安全评估的可接受使用政策，第 12 页
创建客户端安全评估要求，第 35 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。

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 选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

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 (Save)**。

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 选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

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 (Save)**。

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 选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

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 (Save)**。

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 MacOS 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 选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **终端安全评估 (Posture)** > **常规设置 (General Settings)**。

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 (Save)**。

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 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。此窗口的导航路径为：**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：

字段名称	使用指南
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 39 页

安全评估常规设置

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

常规终端安全评估设置

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

安全评估租约

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

相关主题

安全评估服务
安全评估管理设置，第 3 页
安全评估租约，第 5 页
在思科 ISE 中启用安全评估会话服务
设定补救计时器，使客户端在指定时间内补救，第 4 页
设置网络转换延迟计时器，使客户端实现转换，第 4 页
将登录成功窗口设置为自动关闭，第 5 页
设置非代理设备的终端安全评估状态，第 5 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 MacOS 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 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：。

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 启动思科 ISE 管理员用户界面，并选择 **Administration > System > Settings > 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 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 (Save)**。

安全评估可接受使用政策配置设置

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。

字段名称	使用指南
“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

安全评估服务

配置安全评估的可接受使用政策，第 12 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 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 (Submit)**。

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。
-

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 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 (Submit)**。

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
-

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 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 (Submit)**。

字典复合条件设置

下表介绍**字典复合条件 (Dictionary Compound Conditions)** 窗口中的字段。此窗口的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **词典复合条件 (Dictionary Compound Condition)**。

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 思科 ISE 将按顺序处理复合条件中的每个 OR 条件。例如，如果复合条件检查 A OR B，思科 ISE 会首先检查 A，然后检查 B。如果条件 A 或 B 均通过，则整体结果标记为通过。 如果条件 A 失败，条件 B 成功，则整体结果标记为通过。在这种情况下，在安全评估报告中，条件 A 标记为失败，条件 B 为通过。 如果条件 A 成功，思科 ISE 将跳过条件 B 并将整体结果标记为通过。在安全评估报告中，条件 A 标记为通过，条件 B 标记为已跳过，总体结果为通过。
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 14 页
创建复合安全评估条件，第 14 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 MacOS 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。

Inline Posture 节点

Inline Posture 节点是守门节点，放在网络访问设备后面，例如网络上的无线 LAN 控制器 (WLC) 和 VPN 集线器。Inline Posture 节点在用户通过身份验证并被授予访问权限后实施访问策略，并且处理 WLC 或 VPN 无法满足的授权更改 (CoA) 请求。思科 ISE 允许您有两个 Inline Posture 节点，承担主要或辅助角色，提供高可用性。

Inline Posture 节点必须为专用节点。它必须仅用于内联状态服务，不能与其他思科 ISE 服务同时运行。同样，由于其服务的专业化性质，Inline Posture 节点无法承担任何角色。例如，它不能用作管理节点提供管理服务，不能用作策略服务节点提供网络访问、安全评估、配置文件和访客服务，也不能用作监控节点为思科 ISE 网络提供监控和故障排除服务。

思科 ISE 3495 平台不支持 Inline Posture 角色。确保在以下任何受支持的平台上安装 Inline Posture 角色：思科 ISE 3315、思科 ISE 3355、思科 ISE 3395 或思科 ISE 3415。

您不能访问 Inline Posture 节点的基于 Web 的用户界面，只能从 PAN 配置这些节点。

Inline Posture 节点的安装

您必须从 Cisco.com 下载 Inline Posture ISO (IPN ISO) 映像，然后将其安装到任何支持的平台上。然后，您必须通过命令行界面 (CLI) 配置证书。接下来，您可以从管理员门户注册此节点。

注释 不提供 版本的 Inline Posture ISO 映像。使用 1.2 IPN ISO 映像安装并设置 Inline Posture 节点。

安装和设置 Inline Posture 应用后，您必须先配置证书，然后才能注册 Inline Posture 节点。有关详细信息，请参阅《思科身份服务引擎硬件安装指南》。

注册 Inline Posture 节点

我们建议您在注册时确定节点的类型（思科 ISE 或 Inline Posture）。如果希望稍后更改节点类型，您必须将该节点从部署中注销，重启独立节点上的思科 ISE 并重新注册该节点。

开始之前

- 确保主节点的证书信任列表 (CTL) 具有适当的证书颁发机关 (CA) 证书，以验证要注册的辅助节点的 HTTPS 证书。
- 向主要节点注册辅助节点之后，如果您更改辅助节点上的 HTTPS 证书，您必须将相应的 CA 证书导入主要节点的 CTL。

步骤 1 登录到 PAN。

步骤 2 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击左侧导航窗格中的 **Deployment**。

步骤 4 选择注册 **(Register)** > 注册 **Inline Posture** 节点 **(Register an Inline Posture Node)** 以注册 Inline Posture 节点。

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
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

终端安全评估条件	合规性模块版本
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。

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
- 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 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 (Submit)**。

相关主题

补丁管理条件设置
添加补丁管理补救

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 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 (Submit)**。

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。此窗口的导航路径为： **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)**。

相关主题

简单安全评估条件，第 13 页
复合安全评估条件，第 14 页
创建终端安全评估条件

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。此窗口的导航路径为： **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 *6:* 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 13 页
复合安全评估条件，第 14 页

应用条件设置

下表说明“应用条件”窗口中的字段。此窗口的导航路径为： **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **应用条件 (Application Condition)**。

相关主题

简单安全评估条件，第 13 页
复合安全评估条件，第 14 页

服务条件设置

下表介绍**服务条件 (File Conditions)** 窗口中的字段。此窗口的导航路径为： **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)**。

相关主题

简单安全评估条件，第 13 页
复合安全评估条件，第 14 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。此窗口的导航路径为： **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 *7:* 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 13 页
创建复合安全评估条件，第 14 页

防病毒条件设置

下表介绍了**防病毒条件 (Anti-Virus Condition)** 窗口中的字段。此窗口的导航路径为：**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)**。

表 *8:* 防病毒条件设置

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。
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。
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。

字段名称	使用指南
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。
选定供应商的产品	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。

相关主题

复合安全评估条件，第 14 页
预配置的防病毒和反间谍软件条件，第 16 页
防病毒和反间谍软件支持图表，第 16 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。此窗口的导航路径为： **策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **AS 复合条件 (AS Compound Condition)**。

表 *9:* 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。

字段名称	使用指南
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)。
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 14 页
预配置的防病毒和反间谍软件条件，第 16 页
防病毒和反间谍软件支持图表，第 16 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。此窗口的导航路径为： **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 *10:* 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。

字段名称	使用指南
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 13 页
创建简单安全评估条件，第 14 页

字典复合条件设置

下表介绍**字典复合条件 (Dictionary Compound Conditions)** 窗口中的字段。此窗口的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **词典复合条件 (Dictionary Compound Condition)**。

表 *11:* 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 思科 ISE 将按顺序处理复合条件中的每个 OR 条件。例如，如果复合条件检查 A OR B，思科 ISE 会首先检查 A，然后检查 B。如果条件 A 或 B 均通过，则整体结果标记为通过。 如果条件 A 失败，条件 B 成功，则整体结果标记为通过。在这种情况下，在安全评估报告中，条件 A 标记为失败，条件 B 为通过。 如果条件 A 成功，思科 ISE 将跳过条件 B 并将整体结果标记为通过。在安全评估报告中，条件 A 标记为通过，条件 B 标记为已跳过，总体结果为通过。

字段名称	使用指南
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 14 页
创建复合安全评估条件，第 14 页

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。

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。

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)。

步骤 1 选择**策略 (Policy)** > **终端安全评估 (Posture)** 。

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 （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 6 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 7 从**身份组 (Identity Groups)** 列中，选择所需的身份组。

步骤 8 从**操作系统 (Operating Systems)** 列中，选择操作系统。

步骤 9 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 10 在**要求 (Requirements)** 字段中指定要求。

步骤 11 点击**保存 (Save)**。

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：

开始之前

在以下思科 ISE 版本中，漏洞 CSCvs39880 会导致垃圾收集进程，从而影响从主 PSN 到辅助 PSN 的内存空间和文件复制。由于此漏洞，在以下思科 ISE 版本中，在大型思科 ISE 部署中上传代理包可能需要约 7 个小时，而在小型部署中则需要约 40 分钟。

以下是受影响的思科 ISE 版本：

在更高的思科 ISE 版本中，此漏洞已得到修复，使得代理软件包上传时间约为 5 分钟。

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。

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：

- 思科 NAC Web 代理：用户在登录时安装在系统中的临时代理，一旦登录会话终止，临时代理在客户端计算机上就不再可见。
- 思科 NAC 代理：持久代理，安装后，依然在 Windows 或 Mac OS X 客户端计算机上执行所有安全合规性功能。
- 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。

终端安全状态评估选项

安全评估补救选项

安全评估的自定义条件

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”。

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 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 (Submit)**。

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 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 (Submit)**。

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 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 (Submit)**。

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 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 (Submit)**。

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 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 (Submit)**。

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 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 (Submit)**。

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 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。

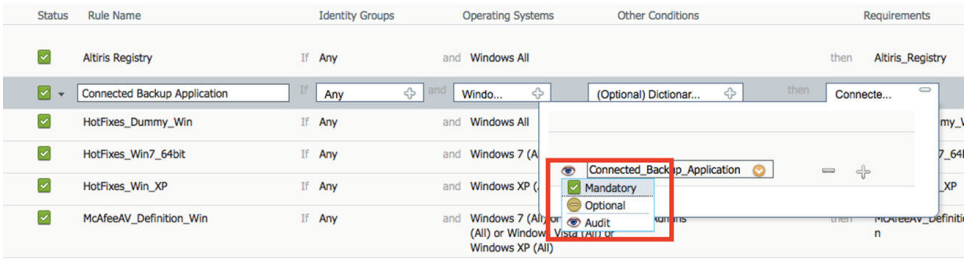
步骤 6 点击提交 **(Submit)**。

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 *1:* 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。

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：

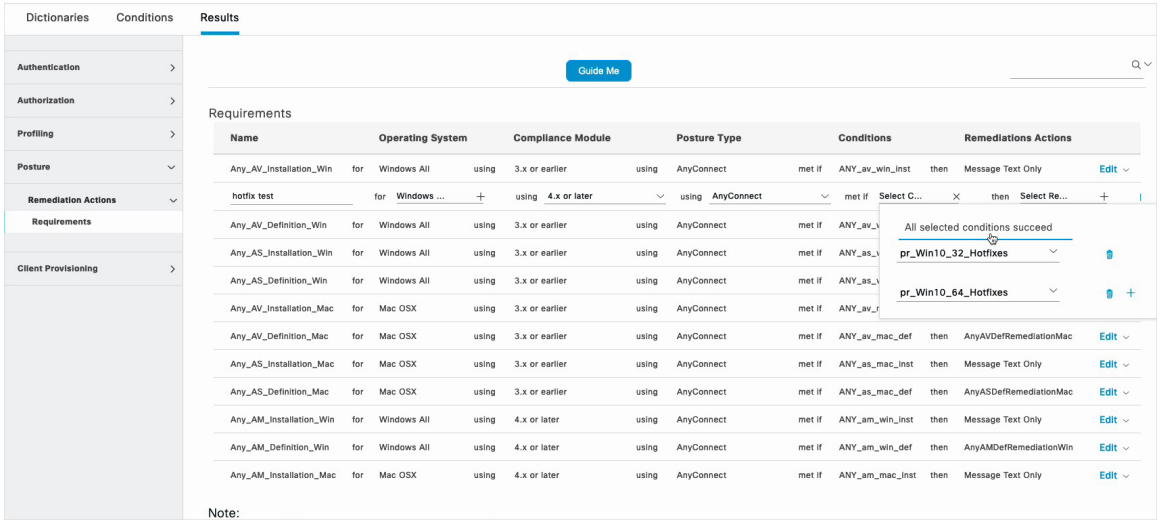
- 在 802.1X 的有线和无线授权更改 (CoA) 环境下：
  - 当您在新授权策略窗口中新建授权配置文件时，您可以配置特定授权策略的重新验证计时器。此方法不支持内联安全评估部署。
  - 一旦断开并重新连接到网络时，有线用户即可离开隔离状态。在无线环境中，用户必须断开与无线局域网控制器 (WLC) 的连接并等待用户空闲超时过期后才能尝试重新连接到网络。
- 在 VPN 环境中 - 断开并重新连接 VPN 隧道。

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 *2:* 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 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 (Save)**。

重新进行安全评估配置设置

表 *12:* 重新进行安全评估配置设置

字段名称	使用指南
Configuration Name	输入 PRA 配置的名称。
Configuration Description	输入 PRA 配置的说明。
Use Reassessment Enforcement?	选中此复选框，将 PRA 配置应用到用户身份组。
Enforcement Type	选择要执行的操作： • **继续 (Continue)**：用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。 • **注销 (Logoff)**：如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。 • **补救 (Remediate)**：如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送PRA报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。 如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的RADIUS会话，才能再次布置客户端。 如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续”(Continue)选项。用户可以继续停留在当前的网络中，不受任何限制。
Interval	输入第一次成功登录后在客户端上启动 PRA 的时间间隔分钟数。 默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。
Grace time	输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于 PRA 间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。 最小值为 5 分钟，最大值为 60 分钟。 **注释** 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。
Select User Identity Groups	为 PRA 配置选择唯一组或唯一组组合。
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 5 页
定期重新评估，第 6 页
终端安全状态评估选项，第 30 页
安全评估补救选项，第 30 页
安全评估的自定义条件，第 30 页
自定义安全评估补救措施，第 31 页
配置定期重新评估，第 7 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 Authorization Policy 页面中定义两种类型的授权策略：标准和例外授权策略。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 选择**策略 (Policy)** > **授权 (Authorization)**。

步骤 2 从 Authorization Policy 页面顶部显示的下拉列表中选择其中一个要应用的匹配规则类型。

- **应用第一个匹配的规则 (First Matched Rule Applies)** - 此选项使用标准授权策略列表中在评估过程中第一个匹配的单个授权策略设置访问权限。找到第一个匹配授权策略后，便不会评估其余标准授权策略。
- **Multiple Matched Rule Applies** - 此选项使用所有标准授权策略列表中在评估过程中匹配的多个授权策略设置访问权限。

步骤 3 点击默认标准授权策略行中**编辑 (Edit)** 旁的向下箭头。

步骤 4 点击 **Insert New Rule Above**。

步骤 5 输入规则名称，选择身份组和其他条件，然后关联显示在默认标准授权策略行上方的新授权策略行中的授权配置文件。

步骤 6 点击**完成 (Done)** 以在只读模式下创建新的标准授权策略。

步骤 7 点击**保存 (Save)**。

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。

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 客户端、Mac OS X 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 选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **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/pmbu/provisioning-update.xml。

如果您的网络限制 URL 重定向功能（例如，通过代理服务器），并且您在访问默认 URL 时遇到困难，则另请尝试将您的思科 ISE 指向以下 URL：https://www.perfigo.com/ise/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**。

注释 如果 ISE 证书缓存在终端的 HTTP 严格传输安全 (HSTS) 存储中，则客户端调配门户重定向可能会失败，您可能会看到以下错误消息：

您现在无法访问 `hostname.domain.com`，因为该网站使用 `HSTS`。网络错误和攻击是暂时的，因此此页面稍后可能会恢复正常。

要解决这个问题，请删除终端上的浏览器缓存，或者导航到 chrome://net-internals/#hsts 并删除自签名 ISE 证书。

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。

客户端调配资源在 **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 NAC、 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 39 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 42 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者配置文件。
- **NAC 代理或 AnyConnect ISE 终端安全评估配置文件 (NAC Agent or AnyConnect ISE Posture Profile)**：当您不希望创建和分配代理 XML 配置文件时，请在此配置 NAC 代理和 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。有关 NAC 代理配置文件的详细信息，请参阅为思科 NAC 代理创建代理自定义文件 ， 第 53 页。
- **AMP 启用程序配置文件**：创建从外部 Web 服务器下载安装程序（用于在终端上安装 AnyConnect AMP 启用程序客户端）的客户端调配配置文件。您可以通过添加另一个调配资源并选择**本地磁盘中的代理资源 (Agent resources from local disk)** 将该配置文件上传到 ISE。有关 AMP 启用程序 XML 配置文件的详细信息，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 66 页。

相关主题

在思科 ISE 中配置客户端调配 ， 第 39 页
从思科添加客户端调配资源 ， 第 41 页
从本地计算机添加思科提供的客户端调配资源 ， 第 42 页
从本地计算机添加 AnyConnect 的客户创建资源 ， 第 42 页

从思科添加客户端调配资源

可以从 Cisco.com 添加适用于 AnyConnect 和思科 NAC 代理（Windows 和 MAC OSX 客户端）以及思科 Web 代理的客户端调配资源。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 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**。

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 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 、思科 NAC 代理、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 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

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。

创建本地请求者配置文件

您可以创建本地请求者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者调配向导。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

- 如果您要对远程设备注册使用 TLS 设备协议，请至少设置一个简单证书注册协议 (SCEP) 配置文件。
- 打开 TCP 端口 8909 和 UDP 端口 8909 以启用Cisco NAC 代理、Cisco NAC Web 代理和**请求者调配 (Supplicant Provisioning)** 向导安装。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 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)** > **本地请求者配置文件 (Native Supplicant Profile)**。

步骤 3 使用本地请求者配置文件设置，第 44 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。

本地请求者配置文件设置

当您选择 **策略** > **策略元素** > **结果** > **客户端调配** > **资源** > **添加** > **本地请求者配置文件**时，将显示以下设置。

- **名称 (Name)**：输入您创建的本地请求者配置文件的名称。
- **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者的网络连接的设置。

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。
- **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

- **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。

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。

- **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。

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。思科 AnyConnect 是与思科ISE NAC代理共存于同一终端上的终端安全评估代理。一次只有一个代理处于活动状态。

注释 AnyConnect 不支持 CWA 流 。您无法通过访客门户使用 **访客访问** > **配置** > **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

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 42 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 42 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 47 页）。

步骤 1 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** 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，AnyConnect DesktopWindows 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，AnyConnect ComplianceModulewindows 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、、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 (Submit)**。

创建终端安全评估代理配置文件

按照此程序创建 AnyConnect 或 NAC 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 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 **NAC AnyConnect 代理终端安全评估配置文件 (NAC AnyConnect Agent Posture Profile)**。

步骤 4 在 **终端代理配置文件设置**下，选择 **AnyConnect** 或 **NAC 代理**。

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 (Submit)**。

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。选择 **Policy** > **Policy Elements** > **Resilts** > **Client Provisioning** > **Resources** > **Add** > **NAC or AnyConnect Posture Profile**。

字段名称	默认值	模式（仅适用于思科 NAC 代理）	使用指南
“VLAN 检测时间间隔”(VLAN detection interval)	0, 5	合并	此设置是代理检查 VLAN 更改的时间间隔。 对于 Windows NAC 代理，默认值为 0。默认情况下，对 Windows 禁用访问身份验证 VLAN 更改功能。有效范围为 0 至 5 秒。 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	合并	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。

字段名称	默认值	模式（仅适用于思科 NAC 代理）	使用指南
“重试检测计数”**(Retry detection count)**	3	合并	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。	合并	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。	合并	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）	覆盖	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。
“**DHCP** 更新延迟”**(DHCP renew delay)**	0 有效范围为 0 至 60 秒。	覆盖	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。	覆盖	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

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。

思科 NAC 代理 XML 文件安装目录

在一个将思科 NAC 代理安装在默认位置的系统中，您可以在以下目录中找到下列 .xml 文件：

- nac_login.xml 文件位于“C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login”目录中。
- nacStrings_xx.xml 文件中的“xx”表示区域设置。您可以在“C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility”目录中找到完整的文件列表。

如果代理安装在其他位置，则文件应位于“<代理安装路径>\Cisco\Cisco NAC Agent\UI\nac_divs\login”和“<代理安装路径>\Cisco\Cisco NAC Agent\cues_utility”。

适用于 Windows 客户端的思科 NAC 代理

思科 NAC 代理为客户端设备提供安全状态评估和补救。

用户可以下载并安装思科NAC代理（只读客户端软件），它可以检查主机历史记录、进程、应用和服务。思科 NAC 代理可用于执行 Windows 更新或防病毒和反间谍软件定义更新，启动合格补救程序，将上传的文件分发给思科 ISE 服务器，分发网站链接以供用户下载文件来修复他们的系统，或单纯用于分发信息和说明。

思科强烈建议您确保在 Windows XP 客户端上安装最新的 Windows 修补程序和补丁，从而使思科 NAC 代理可以与思科 ISE 建立安全的加密通信（通过 SSL over TCP）。

从 Windows 7 及早期版本客户端中卸载思科 NAC 代理

思科 NAC 代理安装在 Windows 客户端上的 **C:\Program Files\Cisco\Cisco NAC Agent**。

您可以用以下方式卸载代理：

- 双击 **Uninstall Cisco NAC Agent** 桌面图标。
- 前往**开始菜单** > **程序 (Programs)** > **思科系统 (Cisco Systems)** > **思科 Clean Access (Cisco Clean Access)** > **卸载思科 NAC 代理 (Uninstall Cisco NAC Agent)**
- 依次选择 **Start Menu** > **Control Panel** > **Add or Remove Programs** > **Cisco NAC Agent** 并卸载思科 NAC 代理。

在 Windows 8 客户端中卸载思科 NAC 代理

可以在 Metro 模式下在 Windows 8 客户端中卸载思科 NAC 代理。

步骤 1 切换到 Metro 模式。

步骤 2 右键点击 **Cisco NAC Agent** 缩略图。

步骤 3 从屏幕底部的选项中选择 **Un-Install**。

步骤 4 系统自动切换到桌面模式，打开 **Add/Remove** 控制面板。

步骤 5 在 **Add/Remove** 控制面板中，执行以下操作之一：

a) 双击 **Cisco NAC Agent**，点击 **Uninstall**。

b) 选择 **Cisco NAC Agent**，点击 **Uninstall**。

c) 右键点击 **Cisco NAC Agent**，选择 **Uninstall**。

Windows 8 Metro 和 Metro 应用支持 - Toast 通知

思科 NAC 代理托盘图标上显示 Enable Toast Notification 选项，使用该选项可以将相关通知发送至 Windows 8 客户端上的用户。

在思科NAC代理场景中，如果用户没有获得网络访问权限，例如“补救失败”或“网络访问权限已到期”，代理会显示以下 Toast 通知：Network not available, Click "OK" to continue。

为了获取更多详细信息，您可以选择 Toast，系统会将您重定向至桌面模式，并显示思科 NAC 代理对话框。

对于用户需要执行才能获得网络访问权限的所有积极的建议操作，系统都会显示 Toast 通知。以下列出某些示例：

- 对于网络接受策略，Toast 通知将显示为：“Click Accept to gain network access”
- 对于代理/兼容模块升级，Toast 通知将显示为：“Click OK to Upgrade/Update”

- 在“用户已注销”事件中，当 Clean Access Manager (CAM) 中未启用用于注销的“Auto Close”选项时，系统会显示 Toast 通知。通过该 Toast 通知，用户知道他们已注销并且需要再次登录才能获得网络访问权限。

适用于 Macintosh 客户端的思科 NAC 代理

思科 NAC OS X 代理为 Macintosh 客户端计算机提供安全评估和补救。

用户可以下载并安装思科 NAC OS X 代理（只读客户端软件），该代理可检查防病毒和反间谍软件定义更新。

在用户登录到思科 NAC OS X 代理后，代理会从思科 ISE 服务器获取针对用户角色和操作系统配置的要求，检查所需软件包并向思科 ISE 服务器发回报告。如果在客户端上满足要求，则允许用户进行网络访问。如果未满足要求，则代理会针对未满足的每项要求向用户显示一个对话框。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，如果未满足指定要求，则用户可以在尝试补救客户端系统时接受受限网络访问。

从 Macintosh 客户端卸载思科 NAC 代理

您可以通过运行如下所示的卸载脚本，为 Mac OS X 客户端卸载思科 NAC 代理：

步骤 1 打开导航器窗格，并导航至 <本地驱动器 *ID*> > **应用 (Applications)**。

步骤 2 突出显示并右键点击 **CCAAgent** 图标，以显示选择菜单。

步骤 3 选择**显示软件包内容 (Show Package Contents)** 并双击 **NacUninstall**，可在 Mac OS X 上卸载思科 NAC 代理。

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。

思科 NAC 代理日志

在适用于 Windows 的思科 NAC 代理中，右键点击代理托盘图标，然后点击 **Log Packager** 以运行支持包并收集代理日志。

在适用于 NAC OS X 的思科 NAC 代理中，点击 Tools 菜单，右键点击 Agent 图标，然后点击 **Collect Support Logs** 选项，以收集代理日志和支持信息。所收集的信息以 zip 文件形式提供。用户可以选择文件位置和文件名以保存文件。默认情况下，此文件以 *CiscoSupportReport.zip* 作为文件名，保存于桌面上。

如果代理崩溃或挂起，您可以运行 **CCAAgentLogPackager.app** 以收集日志。可于 /Applications/CCAAgent.app 处获得此文件。您可以右键点击 **CCAAgent.app**，选择 **Show Package Contents**，然后双击 **CCAAgentLogPackager**，以收集支持信息。

为思科 NAC 代理创建代理自定义文件

使用代理自定义文件，可以自定义思科NAC代理屏幕对话框中包含的徽标、字段和消息文本，适应特定的 Windows 客户端网络访问要求。

您可以将自定义软件包创建成一个包含XML描述符文件的.zip文件和另一个包含构成自定义选项的内容的 .zip 文件。

步骤 1 安装构成代理屏幕自定义软件包所需的文件：

- 自定义的 nac_login.xml 文件
- 创建为 .gif 文件的自定义公司/企业徽标
- 一个或多个自定义的 nacStrings_xx.xml 文件
- 自定义的 updateFeed.xml descriptor 文件

步骤 2 创建一个名为“brand-win.zip”的 zip 文件，其中包含已安装的文件。例如，在 Linux 或 UNIX 环境中，请执行以下操作：**zip -r brand-win.zip nac_login.xml nac_logo.gif nacStrings_en.xml nacStrings_cy.xml nacStrings_el.xml**

步骤 3 创建一个“custom.zip”文件，其中包含适当的updateFeed.xml描述符文件和上面创建的.zip文件。例如，在Linux或 UNIX 环境中，请执行以下操作：**zip -r custom.zip updateFeed.xml brand-win.zip**

步骤 4 将得到的“custom.zip”文件保存到本地计算机上的某个位置，方便在将文件上传到思科 ISE 时访问。

自定义 nac_login.xml 文件模板

nac_login.xml 文件是您的代理屏幕自定义软件包中需要的文件之一，您可通过此文件自定义思科NAC代理对话框（例如Properties窗口）中包含的徽标、字段和消息文本，以满足您的特定Windows客户端网络接入要求。

使用以下模板构建适当的“nac_login.xml”文件，自定义思科NAC代理屏幕中包含的徽标、字段和消息文本。

以下是一个自定义文件示例。

```
<tr class="nacLoginMiddleSectionContainerInput">
<td colspan="2">
<fieldset width="100%" id="nacLoginCustomAlert"  style="display:block"
class="nacLoginAlertBox">
<table width="100%">
<tr>
<td id="nacLoginCustomAlert.img" valign="top" width="32px">
<img src="./cues_icons/Status_warning_icon.png" align="absmiddle"
onload="cuesFixPNG(null,this)"></img>
</td>
<td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
<cues:localize key="login.customalert"/>
</td>
</tr>
</table>
</fieldset>
</td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
<td>
<cues:localize key="cd.nbsp"/>
</td>
<td class="cuesLoginField">
<nobr>
<input type="checkbox" alt="" title="" name="rememberme"  id="rememberme" checked="true"/>

<cues:localize key="login.remember_me"/>
</nobr>
</td>
</tr>
```

自定义 nacStrings_*xx*.xml 文件模板

这是在代理屏幕自定义软件包中需要的其中一个文件，使您能够对思科NAC代理对话框（如Properties屏幕）中包含的徽标、字段和消息文本进行自定义，以满足特定 Windows 客户端网络访问要求。

使用以下模板构建一个或多个 nnacStrings_xx.xml 文件，其中 xx 是具体语言的双字符标识符。

以下是自定义 nacStrings_xx.xm 文件示例。

```
<cueslookup:appstrings xmlns:cueslookup="http://www.cisco.com/cues/lookup">
<cueslookup:name key="nac.brand.legal_name">Cisco Systems, Inc.</cueslookup:name>
<cueslookup:name key="nac.brand.full_name">Cisco Systems</cueslookup:name>
<cueslookup:name key="nac.brand.short_name">Cisco</cueslookup:name>
<cueslookup:name key="nac.brand.abbreviation">Cisco</cueslookup:name>
<cueslookup:name key="nac.copyright">Copyright </cueslookup:name>
<cueslookup:name key="nac.copyright.period">2009-2013</cueslookup:name>
<cueslookup:name key="nac.copyright.arr">All Rights Reserved</cueslookup:name>
<cueslookup:name key="updateagent.rqst">NAC Agent %1 is available.%br% Do you want to install
 this update now?</cueslookup:name>
<cueslookup:name key="updateagent.rqst.retry">Unable to update NAC Agent. Please try
again.</cueslookup:name>
<cueslookup:name key="downloadagent.report">Downloading the update of NAC
Agent.</cueslookup:name>
<cueslookup:name key="downloadagent.packagename.label">Package Name</cueslookup:name>
<cueslookup:name key="downloadagent.completed.label">Completed</cueslookup:name>
<cueslookup:name key="downloadagent.completed.value">%1 of %2 bytes</cueslookup:name>
<cueslookup:name key="downloadagent.speed.label">Speed</cueslookup:name>
<cueslookup:name key="downloadagent.speed.value">%1 bytes/sec</cueslookup:name>
<cueslookup:name key="updateopswat.rqst">NAC Agent Posture component version %1 is
```

```
available.%br% Do you want to install this update now?</cueslookup:name>
<cueslookup:name key="updateopswat.rqst.retry">Unable to update NAC Agent Posture component.
 Please try again.</cueslookup:name>
<cueslookup:name key="downloadopswat.report">Downloading the update of NAC Agnet Posture
component.</cueslookup:name>
<cueslookup:name key="login.productname">Education First Compliance Check</cueslookup:name>

<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.opswatversion">Posture Component Version</cueslookup:name>
<cueslookup:name key="login.username">Enter your username</cueslookup:name>
<cueslookup:name key="login.password">Enter your PIN</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Custom EF package version 2.1.1.1 with EF
Logo</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
<cueslookup:name key="menu_devtools">Dev Tools</cueslookup:name>
<cueslookup:name key="c.sso.ad">Performing Windows Domain automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.generic">Unknown authentication type</cueslookup:name>
<cueslookup:name key="c.sso.macauth">Performing device filter automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.vpn">Performing automatic login into NAC environment for remote
 user</cueslookup:name>
<cueslookup:name key="c.title.status.authenticating">Authenticating User</cueslookup:name>

<cueslookup:name key="c.title.status.answeringchallenge">Sending Response</cueslookup:name>

<cueslookup:name key="c.title.status.checking">Checking Requirements</cueslookup:name>
<cueslookup:name key="c.title.status.checkcomplete">System Check Complete</cueslookup:name>

<cueslookup:name key="c.title.status.loggedin">NAC Process Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netaccess.none">NAC Process Completed</cueslookup:name>

<cueslookup:name key="c.title.status.netpolicy">Network Usage Policy</cueslookup:name>
<cueslookup:name key="c.title.status.properties">Agent Properties &
Information</cueslookup:name>
<cueslookup:name key="c.title.status.remediating">Remediating System</cueslookup:name>
<cueslookup:name key="c.title.status.session.expired">Session has Expired</cueslookup:name>

<cueslookup:name key="c.title.status.update.available">Update Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.downloading">Downloading Agent</cueslookup:name>

<cueslookup:name key="c.title.status.update.opswat.available">Update Posture
Component</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.downloading">Downloading Posture
Component</cueslookup:name>
<cueslookup:name key="scanning">Checking</cueslookup:name>
<!-- <cueslookup:name key="scanningitemcomplete">Finished Checking</cueslookup:name> -->
<cueslookup:name key="ph.about">About</cueslookup:name>
<cueslookup:name key="ph.cancel">Cancel</cueslookup:name>
<!-- <cueslookup:name key="ph.details">Details</cueslookup:name> -->
<cueslookup:name key="ph.logout">Logout</cueslookup:name>
<cueslookup:name key="title_remediating">Remediating System</cueslookup:name>
<cueslookup:name key="title_check_conplete">System Check Complete</cueslookup:name>
<cueslookup:name key="title_full_access_granted">Logged In</cueslookup:name>
<cueslookup:name key="title_access_denied">Network Access Denied</cueslookup:name>
<cueslookup:name key="tempNetAccess">Temporary Network Access</cueslookup:name>
<cueslookup:name key="announcePleaseBePatient">Please be patient while your system is checked
 against the network security policy
</cueslookup:name>
```

```
<cueslookup:name key="bttn.accept">Accept</cueslookup:name>
<cueslookup:name key="bttn.apply">Apply</cueslookup:name>
<cueslookup:name key="bttn.cancel">Cancel</cueslookup:name>
<cueslookup:name key="bttn.continue">Update Later</cueslookup:name>
<cueslookup:name key="bttn.close">Close</cueslookup:name>
<cueslookup:name key="bttn.detailshide">Hide Compliance</cueslookup:name>
<cueslookup:name key="bttn.detailsshow">Show Compliance</cueslookup:name>
<cueslookup:name key="bttn.download">Download</cueslookup:name>
<cueslookup:name key="bttn.guestAccess">Guest Access</cueslookup:name>
<cueslookup:name key="bttn.go2link">Go To Link</cueslookup:name>
<cueslookup:name key="bttn.launch">Launch</cueslookup:name>
<cueslookup:name key="bttn.login">Log In</cueslookup:name>
<cueslookup:name key="bttn.next">Re-Scan</cueslookup:name>
<cueslookup:name key="bttn.ok">OK</cueslookup:name>
<cueslookup:name key="bttn.propertieshide">Hide Properties</cueslookup:name>
<cueslookup:name key="bttn.reject">Reject</cueslookup:name>
<cueslookup:name key="bttn.remediate">Repair</cueslookup:name>
<cueslookup:name key="bttn.rescan">Rescan</cueslookup:name>
<cueslookup:name key="bttn.reset">Reset</cueslookup:name>
<cueslookup:name key="bttn.restrictedNet">Get Restricted NET access This one comes down
from the network</cueslookup:name>
<cueslookup:name key="bttn.savereport">Save Report</cueslookup:name>
<cueslookup:name key="bttn.skip">Skip</cueslookup:name>
<cueslookup:name key="bttn.skipao">Skip All Optional</cueslookup:name>
<cueslookup:name key="bttn.submit">Submit</cueslookup:name>
<cueslookup:name key="bttn.update">Update</cueslookup:name>
<cueslookup:name key="cd.days">
days
</cueslookup:name>
<cueslookup:name key="cd.nbsp">

</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.counting">
There is approximately %1 left until your temporary network access expires
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.expired">
Your Temporary Network Access has Expired!
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.counting">
%1 left
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.expired">
Expired!
</cueslookup:name>
<cueslookup:name key="cd.window.counting">
This window will close in %1 secs
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess">
Full Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">
Your device conforms with all the security policies for this protected
network
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">
Refreshing IP address. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">
Refreshing IP address succeeded.
```

```
</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">
Connecting to protected Network. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">
Guest Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">
Network Access Denied
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">
There is at least one mandatory requirement failing.
You are required to update your system before
you can access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">
Network Usage Terms and Conditions are rejected. You will not be
allowed to access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">
Restricted Network Access granted.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">
You have been granted restricted network access because your device
did not conform with all the security policies for this protected
network and you have opted to defer updating your system. It is recommended
that you update your system at your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">
Temporary Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">
Please be patient while your system is checked against the network security policy.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">
There is at least one mandatory requirement failing.
You are required to update your system otherwise
your network access will be restricted.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">
Temporary Access to the network has expired.
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose">

</cueslookup:name>
<cueslookup:name key="ia.status.checkcomplete">
Finished Checking Requirements
```

```
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress">
Please be patient while we determine if your system is compliant with the security policy
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress.01">
Checking %1 out of %2
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicy">
Access to the network requires that you view and accept the following
Network Usage Policy
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicylinktxt">
Network Usage Policy Terms and Conditions
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.inprogress">
Remediating
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.start">
Please Remediate
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.checkinprogress">
Checking for compliance with Requirement
</cueslookup:name>
<cueslookup:name key="ia.table.name">
Name
</cueslookup:name>
<cueslookup:name key="ia.table.location">
Location
</cueslookup:name>
<cueslookup:name key="ia.table.software">
Software
</cueslookup:name>
<cueslookup:name key="ia.table.software.programs">
program(s)
</cueslookup:name>
<cueslookup:name key="ia.table.update">
Update
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.nochange">
Do not change current setting
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforedownload">
Notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforeinstall">
Notify before install
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.scheduledinstallation">
Download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforedownload">
Change to notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforeinstall">
Change to notify before installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcescheduledinstall">
Change to download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.description">
Description
</cueslookup:name>
<cueslookup:name key="scs.table.title">
Security Compliance Summary
```

```
</cueslookup:name>
<cueslookup:name key="scs.table.header1.scan_rslt">
Scan Result
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_name">
Requirement Name
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_details">
Requirement Description - Remediation Suggestion
</cueslookup:name>
<cueslookup:name key="scs.table.data.mandatory">
Mandatory
</cueslookup:name>
<cueslookup:name key="scs.table.data.optional">
Optional
</cueslookup:name>
<cueslookup:name key="scs.table.data.pass">
Passed
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_download">
Please download and install the optional software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_download">
Please download and install the required software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_launch">
Please launch the optional remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_launch">
Please launch the required remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
 the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
 the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_win_update">
Please download and install the optional windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_win_update">
Please download and install the required windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_prog">
Launching Remediation Program(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_url">
Launching Remediation URL...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_av">
Updating Virus Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_as">
Updating Spyware Definition...
```

```
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_win_update">
Launching Windows auto Update(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_launch_downloaded_file">
Downloaded at %1. %br% Please open this folder & double-click executable file to install
the required software.
</cueslookup:name>
<cueslookup:name key="discoveryhost.label">
Discovery Host
</cueslookup:name>
<cueslookup:name key="properties.table.title">
List of Antivirus & Anti-Spyware Products Detected by the Agent
</cueslookup:name>
<cueslookup:name key="properties.table.header1.index">
No.
</cueslookup:name>
<cueslookup:name key="properties.table.header1.description">
Description
</cueslookup:name>
<cueslookup:name key="properties.table.header1.value">
Value
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_type">
Product Type
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_name">
Product Name
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_version">
Product Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_version">
Definition Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_date">
Definition Date
</cueslookup:name>
<cueslookup:name key="reboot.mandatory.001">
Mandatory System Reboot Required
</cueslookup:name>
<cueslookup:name key="reboot.optional.001">
You need to reboot your system in order for the changes to take effect.
</cueslookup:name>
<cueslookup:name key="rem.error.001">
Unable to remediate particular requirement
</cueslookup:name>
<cueslookup:name key="rem.error.av_access_denied">
The remediation you are attempting is reporting an access denied error. This is usually due
 to a privilege issue. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_buffer_too_small">
The remediation you are attempting has failed with an internal error. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_elevation_required">
The remediation you are attempting requires elevation. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_failed">
The remediation you are attempting had a failure. If the problem persists contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_internal_error">
```

```
The remediation you are attempting has reported an internal error. If this problem persists
 please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_implemented">
The remediation you are attempting is not implemented for this product. Please contact your
 system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_supported">
The remediation you are attempting is not supported for this product. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_faile">
The AV/AS update has failed. Please try again and if this message continues to display
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_failed_due_to_network">
The AV/AS update failed due to a networking issue. Please try again and if this message
continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_timeout">
The remediation you are attempting has timed out waiting for the operation to finish. If
this continues please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_dist_size_error">
The size of the downloaded file does not match the package! Please discard downloaded file
 and check with your administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_is_not_signed">
The file that has been requested was not digitally signed. Please try again and if this
message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_save_location_error">
The location for the file to be saved to can not be written. Please choose a different
location.
</cueslookup:name>
<cueslookup:name key="rem.error.http_file_not_found">
The requested file is not found. Please try again and if this problem persists, contact
your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.launch_file_not_found">
The file that has been requested could not be launched either because it could not be found
 or there was a problem launching it. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.malformed_URL">
The file that is trying to be downloaded has an incorrect URL. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.network_error">
There has been a network error, please try the remediation again. If this message continues
 to be seen contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.update_fail_for_non_admin">
The remediation you are trying to do can not be accomplished at your user level. Please
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.wsus_search_failure">
The WSUS search failed. This is probably due to a network issue. Please try again and if
this message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="server.error.generic">
Agent encountered problems logging user
</cueslookup:name>
<cueslookup:name key="server.error.255">
Network Error: NAC Server could not establish a secure connection to NAC Manager.
```

```
This could be due to one or more of the following reasons:
1) NAC Manager certificate has expired or
2) NAC Manager certificate cannot be trusted or
3) NAC Manager cannot be reached or
4) NAC Manager is not responding
Please report this to your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5000">
Invalid provider name
</cueslookup:name>
<cueslookup:name key="server.error.5001">
Failed to add user to online list
</cueslookup:name>
<cueslookup:name key="server.error.5002">
Server communication error
</cueslookup:name>
<cueslookup:name key="server.error.5003">
Invalid username or password
</cueslookup:name>
<cueslookup:name key="server.error.5004">
Unknown user
</cueslookup:name>
<cueslookup:name key="server.error.5005">
Account expired
</cueslookup:name>
<cueslookup:name key="server.error.5006">
Account currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5007">
Exceed quota limit
</cueslookup:name>
<cueslookup:name key="server.error.5008">
Insufficient Clean Access packages installed
</cueslookup:name>
<cueslookup:name key="server.error.5009">
Access to network is blocked by the administrator
</cueslookup:name>
<cueslookup:name key="server.error.5010">
Vulnerabilities not fixed
</cueslookup:name>
<cueslookup:name key="server.error.5011">
This client version is old and not compatible. Please login from web browser to see the
download link for the new version.
</cueslookup:name>
<cueslookup:name key="server.error.5012">
Network policy is not accepted
</cueslookup:name>
<cueslookup:name key="server.error.5013">
Invalid switch configuration
</cueslookup:name>
<cueslookup:name key="server.error.5014">
Too many users using this account
</cueslookup:name>
<cueslookup:name key="server.error.5015">
Invalid session
</cueslookup:name>
<cueslookup:name key="server.error.5016">
Null session
</cueslookup:name>
<cueslookup:name key="server.error.5017">
Invalid user role
</cueslookup:name>
<cueslookup:name key="server.error.5018">
Invalid login page
```

```
</cueslookup:name>
<cueslookup:name key="server.error.5019">
Encoding failure
</cueslookup:name>
<cueslookup:name key="server.error.5020">
A security enhancement is required for your Agent. Please upgrade your Agent or contact
your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5021">
Can not find server reference
</cueslookup:name>
<cueslookup:name key="server.error.5022">
User role currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5023">
Authentication server is not reachable
</cueslookup:name>
<cueslookup:name key="server.error.5024">
Agent user operating system is not supported
</cueslookup:name>
<cueslookup:name key="server.error.generic_emergency">
The Agent has encountered an unexpected error and is restarting.
</cueslookup:name>
<cueslookup:name key="server.error.http_error">
Clean Access Server is not available on the network.
</cueslookup:name>
<cueslookup:name key="server.error.nw_interface_chg">
Authentication interrupted due to network status change. Press OK to retry.
</cueslookup:name>
<cueslookup:name key="server.error.svr_misconfigured">
Clean Access Server is not properly configured.
</cueslookup:name>
<cueslookup:name key="server.clarification.generic_emergency">
Please contact your administrator if the problem persists.
</cueslookup:name>
<cueslookup:name key="announce.savingreport">
Saving Report
</cueslookup:name>
<cueslookup:name key="announce.savingreport.failed">
Unable to save report
</cueslookup:name>
<cueslookup:name key="announce.cancelremediationack">
Clicking Cancel may change your network connectivity and interrupt download or required
updates.<p> Do you want to continue?</p>
</cueslookup:name>
<cueslookup:name key="announce.dismiss.default">
Dismiss to continue
</cueslookup:name>
<cueslookup:name key="announce.logoutconfirm">
Successfully logged out from the network!
</cueslookup:name>
</cueslookup:appstrings>
```

注释 可用于自定义文本的字符没有数量限制。但是，思科建议限制字符长度，确保在所产生的自定义登录屏幕显示于客户端上时，这些字段不会占用太多空间。

扩展的 nacStrings_*xx*.xml 文件示例

```
<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address
succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected Network.
 Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.
</cueslookup:name><cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage
Terms and Conditions are rejected. You will not be allowed to access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted restricted
 network access because your device did not conform with all the security policies for this
 protected network and you have opted to defer updating your system. It is recommended that
 you update your system at your earliest convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network Access</cueslookup:name>

<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one mandatory
 requirement failing. You are required to update your system otherwise your network access
 will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements are
 failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network has
 expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>
```

UpdateFeed.xml 描述符文件模板

这是在代理屏幕自定义软件包中需要的其中一个文件，使您能够对思科NAC代理对话框（如Properties屏幕）中包含的徽标、字段和消息文本进行自定义，以满足特定 Windows 客户端网络访问要求。

必须先构建合适的 updateFeed.xml 描述符文件，才能完成代理屏幕自定义软件包。使用以下示例作为模板，以设置自定义软件包所需的 updateFeed.xml 描述符文件。

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:update="http://www.cisco.com/cpm/update/1.0">

<title>Provisioning Update</title>
<updated>2011-12-21T12:00:00Z</updated>
<id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
```

```
<author>
<name>Cisco Support</name>
<email>support@cisco.com</email>
</author>
<!-- Custom Branding -->
<entry>
<id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/7</id>
<title>Agent Customization Package</title>
<updated>2010-06-07T12:00:00Z</updated>
<summary>This is EF Agent Customization Package 1.1.1.7</summary>
<link rel="enclosure" type="application/zip" href="brand-win.zip" length="18884" />
<update:type>AgentCustomizationPackage</update:type>
<update:version>1.1.1.7</update:version>
<update:os>WINDOWS_ALL</update:os>
</entry>
</feed>
```

在创建 updateFeed.xml 描述符文件时，请注意以下几点：

- <update:os> - 必须始终将此属性设置为“WINDOWS_ALL”，才能包含思科 NAC 代理支持的所有 Windows 操作系统版本。有关思科 NAC 代理支持的 Windows 操作系统版本列表，请参阅 Cisco NAC 设备代理的支持信息。
- <update:version> - 这是指要升级到的代理自定义软件包版本。此值应为四位数 <n.n.n.n>，且应大于当前安装的自定义软件包版本。
- <id> - 此 ID 可以是任何内容，但对于每个代理自定义软件包都应唯一。

使用创建配置文件功能生成的 XML 文件示例

```
<?xml version="1.0" ?>
<cfg>
   <VlanDetectInterval>0</VlanDetectInterval>
   <RetryDetection>3</RetryDetection>
   <PingArp>0</PingArp>
   <PingMaxTimeout>1</PingMaxTimeout>
   <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
   <SignatureCheck>0</SignatureCheck>
   <DisableExit>0</DisableExit>
   <PostureReportFilter>displayFailed</PostureReportFilter>
   <BypassSummaryScreen>1</BypassSummaryScreen>
   <LogFileSize>5</LogFileSize>
   <DiscoveryHost></DiscoveryHost>
   <DiscoveryHostEditable>1</DiscoveryHostEditable>
   <Locale>default</Locale>
   <AccessibilityMode>0</AccessibilityMode>
   <SwissTimeout>1</SwissTimeout>
   <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
   <HttpTimeout>120</HttpTimeout>
   <ExceptionMACList></ExceptionMACList>
   <GeneratedMAC></GeneratedMAC>
   <AllowCRLChecks>1</AllowCRLChecks>
   <DisableL3SwissDelay>0</DisableL3SwissDelay>
   <ServerNameRules></ServerNameRules>
</cfg>
```

注释 此文件还包含两个静态（即，不可由用户或思科 ISE 管理员编辑）参数“AgentCfgVersion”和“AgentBrandVersion”，分别用于标识客户端上的当前版本的代理配置文件和代理自定义文件。

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 OS X 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。

对于思科 ISE NAC 代理，可以从**客户端调配 (Client Provisioning)** 窗口选择资源。

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 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。

您可以选择指定单个操作系统，例如 Android、Mac iOS 和 macOS，或者指定用于处理多个客户端计算机操作系统的伞操作系统，例如“Windows XP (All)”或“Windows 7 (All)”。

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 和思科 ISE NAC 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 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 (Save)**。

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。

客户端调配门户语言文件的 HTML 支持

此门户的**说明 (Instructional Text)**、**内容 (Content)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 文本框的导航路径为 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **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。