配置终端安全评估

Cisco Secure Client 提供 Cisco Secure Firewall 终端安全评估模块（以前称为 HostScan）和 ISE 终端安全评估模块。这两个模块都为 Cisco Secure Client 提供了评估终端在以下方面是否合规的功能，例如主机上所安装的防病毒、反间谍软件以及防火墙软件。您可以限制网络访问权限直至终端合规，或者提高本地用户的权限，使其可以制定补救措施。

Cisco Secure Firewall 终端安全评估 与 secure-firewall-posture-<*version*>-k9.pkg 捆绑在一起，后者是一款收集主机上安装了哪些操作系统、防病毒软件、反间谍软件和其他软件的应用。ISE 终端安全评估可在访问 ISE 控制的网络时部署一个客户端，而不必部署 Cisco Secure Client 和 NAC 代理。ISE 终端安全评估是一个模块，可选作额外的安全组件安装到 Cisco Secure Client 产品中。

ISE 终端安全评估可执行客户端评估。客户端从头端获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回头端。尽管 ISE 实际确定终端是否合规，但它依赖终端自己的策略评估结果。

相反，Cisco Secure Firewall 终端安全评估 将执行服务器端评估，其中 Cisco Secure Firewall ASA 仅请求终端属性（例如操作系统、IP 地址、注册表项、本地证书和文件名）的列表，而且这些属性由 Cisco Secure Firewall 终端安全评估 返回。根据策略评估的结果，您可以控制哪些主机可获准与安全设备建立远程访问连接。

注释 不支持组合使用 Cisco Secure Firewall 终端安全评估 和 ISE 终端安全评估代理。运行两个不同的终端安全评估代理时会出现意外结果。

Cisco Secure Firewall 终端安全评估 中支持以下终端安全评估检查，但不支持 ISE 终端安全评估：主机名、IP 地址、MAC 地址、端口号、OPSWAT 版本、BIOS 序列号和证书字段属性。

ISE 终端安全评估模块提供的功能

终端安全评估检查

ISE 终端安全评估模块使用 OPSWAT 版本 3 或版本 4 的库来执行终端安全评估检查。对于初始终端安全评估检查，任何未能满足所有强制性要求的终端都被视为不合规。其他终端授权状态为终端安全评估未知或合规（满足强制性要求）。

注释 对于 macOS 64 位迁移，Cisco Secure Client ISE 终端安全评估模块与旧的 OPSWAT v3 合规性模块不兼容。

如果在终端安全评估检查阶段出错并且 Cisco Secure Client 能够继续，用户将收到通知，但如果可能，终端安全评估检查将继续。如果在强制终端安全评估检查期间出错，检查将标记为失败。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。

任何必要的补救措施

补救窗口在后台运行，以保证网络活动更新不会弹出，引起干扰或中断。您可以在 Cisco Secure Client UI 的 ISE 终端安全评估磁贴部分点击**详细信息 (Details)**，查看检测到的内容和您加入网络前所需的更新。如果必须进行手动补救，补救窗口会打开，显示需要操作的项目。此 ISE 终端安全评估窗口显示更新的进度、所分配更新时间的剩余时间、任何要求的状态以及系统合规性状态。

注释 需要提升权限的应用仅使用非管理员用户帐户进行自动补救。管理员帐户必须手动执行补救。

注释 仅在服务器受信任时才会执行需要更高权限的终端安全评估检查和补救。

当仅剩下可选更新时，才可选择**跳过 (Skip)** 跳到下一步操作，或选择**全部跳过 (Skip All)** 以忽略所有剩余补救项。您可以出于时间考虑跳过可选补救项或仍然保持网络访问。

在补救后（或在无需补救时执行要求检查后），您可能收到可接受使用策略的通知。它要求您接受该策略才能进行网络访问，若拒绝则限制访问。在此部分补救过程中，Cisco Secure Client UI 的终端

安全评估磁贴部分会显示“ISE 终端安全评估：网络可接受的使用策略”(ISE 终端安全评估: Network Acceptable Use Policy)。

当补救完成后，作为所需更新列出的所有检查都显示 Done 状态和绿色复选框。补救后，代理会向 ISE 发送终端安全评估结果。

补丁管理检查和补救

Cisco Secure Client 4.x 和 Microsoft 系统中心配置管理器 (SCCM) 集成提供了补丁管理检查和补丁管理补救。它将检查终端上缺失的重要补丁的状态，以查看是否应该触发软件补丁。如果 Windows 终端上没有缺失重要补丁，则补丁管理检查将通过。补丁管理补救只会为管理员级用户触发，并且仅当 Windows 终端上缺失一个或多个重要补丁时才会触发。

如果 SCCM 客户端安装的某个补丁是在重新启动之前安装的，则 SCCM 客户端将在计算机重新启动后尽快报告该补丁的安装状态（已安装或未安装）。但是，如果 SCCM 客户端安装的某个补丁是在重新启动之后开始安装的，则 SCCM 客户端不会立即报告该补丁的状态。

Cisco Secure Client 合规性模块无法强制 SCCM 客户端在此时提供任何状态。终端安全评估模块客户端完成本机 API 请求所花费的时间是不同动态 OS 参数（例如 CPU 负载、挂起修补程序数量、修补程序安装后无重启等）以及网络因素（如终端安全评估模块客户端和服务器之间的连接和延迟）的函数。您可能必须等待 SCCM 客户端响应，但对已知修补程序进行实验后，有些结果约为 10 分钟。

通过 Windows Server 更新服务 (WSUS) 搜索 API 也可观察到类似行为，它需要更多时间才会响应，有时长达 20 - 30 分钟。Windows 更新会检查所有 Microsoft 产品（例如 Microsoft Office）未安装的补丁，而不仅限于 Windows 操作系统。用于 WSUS 条件和补救的 API 不可靠，您可能会看到意外行为。建议您使用补丁管理条件和补救来验证 Windows 平台上的补丁。

请参阅策略条件了解如何在 ISE 上设置策略条件，或请参阅补丁管理补救了解有关补丁管理补救的更多信息。

重新评估终端合规性

当终端被视为合规并授予网络访问权限后，可选择基于管理员配置的控制对终端定期进行重新评估。被动重新评估终端安全评估检查与初始终端安全评估检查不同。如果管理员配置了相应的设置，那么当发生任何不符合要求的情形时，用户都可选择修复选项。配置设置用于控制用户是否维持受信任的网络访问（即使用户未达到一项或多项强制要求）。在初始终端安全评估过程中，如果终端未满足所有强制要求，将被视为不合规。默认情况下，此功能被禁用。如果为某一用户角色启用该功能，则每 1 到 24 小时执行一次终端安全重新评估。

管理员可将结果设置为“继续”(Continue)、“注销”(Logoff) 或“补救”(Remediate)，并可配置诸如强制执行和正常时间等其他选项。

您可以使用 ISE UI 创建在 Cisco Secure Firewall 终端安全评估配置文件中显示的更多信息性消息。按钮文本和链接也可以自定义。

不兼容设备的宽限期

您可以在 Cisco ISE UI 中设置宽限期。通过此配置，可以向不符合要求、但在先前终端安全评估状态下符合要求的终端授予网络的访问权限。思科 ISE 在其缓存中查找先前已知的良好状态，并为设

备提供宽限期。当宽限期到期时，Cisco Secure Client 将再次执行终端安全评估检查（这一次不进行修复），并根据检查结果确定终端状态是否合规。

注释 当设备处于宽限期但在终端安全评估策略中更新时，会出现以下情况：

- （如果宽限期延长），在以前的宽限期过期或设备从 ISE 中删除时，系统将应用新的宽限期。
- （如果宽限期缩短），仅当设备再次经过终端安全评估流过程时，新的宽限期才会应用到设备。

宽限期不适用于临时代理、硬件库存和应用监控。

当用户处于宽限期时，定期重新评估 (PRA) 不适用。

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。

将设备移至宽限期时，不会显示“可接受使用策略”(AUP)。

宽限期在 ISE UI 的**策略 (Policy) > 终端安全评估或工作中心 (Posture or Work Centers) > 终端安全评估 (Posture) > 终端安全评估策略 (Posture Policy)** 中的 Cisco Secure Firewall 终端安全评估下进行设置。有效值以天、小时或分钟为单位指定。默认情况下，此设置处于禁用状态。

灵活的通知

您可以使用“延迟通知”(Delay Notification) 选项来延迟自定义通知窗口的显示，直到经过特定百分比的宽限期。例如，如果 ISE UI 上的“延迟通知”字段设置为 50% 且配置的宽限期为 10 分钟，则 ISE 终端安全评估将在 5 分钟后重新扫描终端，并在发现终端不合规时显示通知窗口。如果终端状态为合规，则不会显示通知窗口。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。在宽限期过期之前，终端会被授予访问权限。

如果终端不合规，只有在 ISE UI 上配置自定义通知时，Cisco Secure Client UI 才会弹出警告。通知还指示宽限期的开始以及宽限期开始后不合规的任何终端。Cisco Secure ClientISE 终端安全评估磁贴会突出显示所有终端安全评估失败，您可以点击**再次扫描 (Scan Again)** 按钮，以通过强制重新运行终端安全评估策略来维持完整的网络访问。

注释 若要显示“再次扫描”(Scan Again) 选项，必须将“启用重新扫描按钮”(Enable Rescan Button) 选项设置为“启用”(Enabled)。

在补救流程中，解决问题之前您基本上无法访问。没有可用的临时访问权限。在宽限期流程中，您可以获得延迟的访问权限，为您提供解决问题的宽限期。如果点击灵活通知流中的**启动浏览器 (Launch Browser)** 选项，则可以启动浏览器（如果服务器受信任）。您可以通过浏览器选项获取有关遵守终端安全评估策略的其他详细信息。

用于多个连接和自动化目的的终端安全评估 CLI

仅当选择 ISE 终端安全评估模块作为思科安全客户端的一部分进行预部署或 Web 部署时，才会在 Windows 上安装并使用 ISE 终端安全评估 CLI。有关 ISE 终端安全评估的其他安装程序部署详细信息，请参阅用于预部署和网络部署的 Cisco Secure Client 模块可执行文件。使用终端安全评估 CLI，您可以将多个客户端连接到终端安全评估子系统，并且可以将数据发送到这些连接的客户端进程，而不是仅一个客户端和一个服务器进行通信，这是所有 UI 进程均可以支持的。

要运行终端安全评估 CLI，请导航至思科安全客户端的安装位置并运行 **threatcli.exe**。默认情况下，路径为 C:\Program Files(x86)\Cisco\Cisco Secure Client\。下面提供了可用的命令及其结果。执行命令时，安全客户端 GUI 的 ISE 终端安全评估磁贴也会发生变化，以指示各种状态。有关其他 ISE 终端安全评估磁贴的更新，请参阅ISE 终端安全评估的状态，第 11 页。

启动终端安全评估扫描

在 ISEPosture> 提示符后，输入 **rescan**。终端安全评估扫描将开始。

验证策略服务器的状态

在 ISEPosture> 提示符后，输入 **state**。提供策略服务器的状态。

检索 ISE 终端安全评估模块统计信息

在 ISEPosture> 提示符后，输入 **stats**。将返回以下统计信息：

- 当前状态 (Current Status) - 根据终端是否符合 ISE 前端策略，将客户端设备定义为合规或不合规。
- 策略服务器 (Policy Server) - 提供策略服务器的 IP 地址或名称。
- 扫描开始时间 (Scan Start Time) - 提供最新的扫描开始时间。
- 合规性模块版本 (Compliance Module Version) - 提供合规性模块版本。

查看有哪些安全产品

在 ISEPosture> 提示符后，输入 **showproducts**。此命令将显示客户端的安全产品。

获取扫描摘要结果

在 ISEPosture> 提示符后，输入 **showreport**。此命令可提供终端安全评估扫描结果。

获取合规性模块版本

在 ISEPosture> 提示符后，输入 **showcmversion**。此命令提供合规性模块版本。

断开 CLI 接口

在 ISEPosture> 提示符后，输入 **exit**。此命令用于断开 CLI 接口。任何现有终端安全评估会话保持活动状态。

获取有关 ISE 终端安全评估 CLI 命令的帮助

在 ISEPosture> 提示符后，输入 **help** 以获取有关 CLI 命令的帮助。有关特定命令的帮助，请输入 **help<command**。

思科临时代理

思科临时代理专为 Windows 或 macOS 环境而设计，用于在用户接入受信任网络时共享合规性状态。思科临时代理在 ISE UI 中进行配置。每当思科临时代理尝试访问互联网时，系统便会将其可提取文件 .exe（适用于 Windows）或 dmg（适用于 macOS）下载到终端。用户必须运行下载的可执行文件或 dmg 以执行合规性检查：无需管理员权限。

然后，UI 会自动启动并开始检查，以确定终端是否合规。在完成合规性检查后，根据策略在 ISE UI 上的配置方式，ISE 可以采取任何必要的操作。

在 Windows 中，可执行文件为自提取文件，所有必要的 dll 和用于合规性检测的其他文件会被置于此提取文件的临时文件夹中。完成合规性检查后，系统会删除所有提取的文件和可执行文件。为了完全删除这些文件和可执行文件，用户必须退出 UI。

有关在 ISE UI 上执行配置的详细步骤，请参阅《思科身份服务引擎管理员指南》中的思科临时代理工作流程。

思科临时代理的限制

- macOS 不支持临时代理的 VLAN 控制终端安全评估环境，因为在没有根权限的情况下无法执行刷新适配器（DHCP 续订）进程。临时代理可以仅作为用户进程运行。支持 ACL 控制的终端安全评估环境，因为它不需要刷新终端的 IP。
- 如果网络接口在补救期间发生，则用户必须离开当前 UI 并重新执行整个程序。
- 在 macOS 中，不会删除 dmg 文件。
- 在启动临时代理安装程序后，该安装程序在终端上运行时可能会隐藏在浏览器后面。要继续收集临时代理应用的运行状况，最终用户应将浏览器最小化。大部分 Windows 10 用户都会遇到该问题，因为在这些客户端上 UAC 模式设置为高，以接受以高安全条件运行的第三方应用。
- 在终端上启用隐藏模式时，无法使用临时代理。
- 思科临时代理不支持下列条件：
  - Service Condition-macOS - 系统后台守护程序检查
  - Service Condition-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 - 基于加密位置的检查

用于可选模式的终端安全评估策略增强功能

无论强制检查通过还是失败，均可在可选模式下对失败的要求检查执行补救。将在Cisco Secure Client ISE 终端安全评估 UI 上显示一条关于补救的消息，您可以查看哪些要求失败，哪些要求需要补救操作。

- 可选模式手动补救 (Manual Remediation of Optional Mode) - “系统扫描摘要”(ISE 终端安全评估 Summary) 屏幕显示如果某种情况失败，可能需要补救的任何可选模式状态。您可以手动点击“开始”(Start) 进行补救，或者点击“跳过”(Skip)。即使补救失败，终端仍会符合要求，因为这些只是可选要求。“系统摘要”(ISE 终端安全评估 Summary) 将显示它们是被跳过、已失败，还是已成功。
- Automatic Remediation of Optional Mode - 您可以监控 ISE 终端安全评估 磁贴，因为它会在应用可选更新时显示提示。不会要求您启动补救，因为补救是自动进行的。如果任何自动补救失败，您将收到一条消息，指出未能尝试补救。此外，如果需要，您还可以选择跳过补救操作。

查看硬件清单

ISE UI 的“上下文可见性”(Context Visibility) 下已添加了“终端”(Endpoints) > “硬件”(Hardware) 选项卡。它可以帮助您收集、分析和报告短时间内的终端硬件信息。您可以收集信息，例如查找内存容量低的终端或查找终端的 BIOS 型号/版本。根据查找结果，您可以增加内存容量，升级 BIOS 版本或在计划购买资产之前评估需求。制造商使用情况 Dashlet 显示运行 Windows 或 macOS 的终端的硬件清单详细信息，终端使用情况 Dashlet 显示终端的 CPU、内存和磁盘利用率。有关详细信息，请参阅《思科身份服务引擎管理员指南》的“硬件”(Hardware) 选项卡。

隐身模式

管理员可在从终端用户客户端隐藏 Cisco Secure Client UI 磁贴时配置 ISE 终端安全评估。不会显示任何弹出消息，并且任何需要用户干预的情形都将采取默认操作。此功能可在 Windows 和 macOS 操作系统上使用。

请参阅思科身份服务引擎管理员指南中的配置终端安全评估策略部分，您可以在此处将无客户端状态下的隐身型号指定为禁用或启用。

在 ISE 用户界面上，您可以将隐身型号设置为启用通知，以便最终用户仍然看到错误通知。

在映射 ISE 终端安全评估配置文件编辑器，第 14 页中的配置文件，然后将 Cisco Secure Client 配置映射到 ISE 中的 Client Provisioning 页面后，Cisco Secure Client 即可读取终端安全评估配置文件，将其设置为预期型号，以及在初始终端安全评估请求期间将与选定型号相关的信息发送到 ISE。根据型号和其他因素（如身份组、OS 及合规性模块），思科 ISE 将与适当政策进行匹配。

请参阅思科身份服务引擎管理员指南中的隐身型号部署及其影响。

ISE 终端安全评估不允许您在隐身型号下设置以下功能：

- 任何手动补救
- 链接补救
- 文件补救
- WSUS 显示 UI 补救
- 激活 GUI 补救
- AUP 策略

终端安全评估策略实施

要提高您的终端上安装的软件的整体可见性，我们提供了以下终端安全评估增强功能：

- 您可以检查终端防火墙产品的状态，以查看其是否正在运行。如果需要，可以启用防火墙，并在首次终端安全评估和定期重新评估 (PRA) 过程中实施策略。要设置，请参阅思科身份服务引擎配置指南中的防火墙条件设置部分。
- 同样，您可以对终端上安装的应用运行查询。如果运行或安装了不需要的应用，则可停止该应用，或者卸载不需要的应用。要设置，请参阅思科身份服务引擎配置指南中的应用补救部分。

UDID 集成

在设备上安装 Cisco Secure Client 时，它会在 Cisco Secure Client 中的所有模块中共享自己的唯一标识符 (UDID)。此 UDID 是终端的标识符，并将另存为终端属性，这可确保对特定终端而非 MAC 地址的终端安全评估控制。随后您可基于该 UDID 查询终端，它是一个常量，无论该终端如何连接，甚至是在更新或卸载后也不会改变。随后，ISE UI **(Context Visibility > Endpoints > Compliance)** 上的 Context Visibility 页面可为装有多个 NIC 的中断显示一个条目（而非多个条目）。

应用监控

终端安全评估客户端可以持续监控不同终端属性，以便观察动态变化，并向策略服务器汇报。根据终端安全评估的配置，您可以监控不同属性，如安装和运行了哪些应用用于反间谍软件、防病毒、防恶意软件、防火墙等。有关应用条件设置的详细信息，请参阅思科身份服务引擎管理员指南中的持续终端属性监控部分。

USB 存储设备检测

在将 USB 大容量存储设备连接到 Windows 终端时，终端安全评估客户端可以检测到该设备，并将根据终端安全评估策略块阻止或允许该设备。通过 USB 检测，只要终端仍然位于同一个受 ISE 控制的网络中，代理即可持续监控该终端。如果在此时段内连接了符合该条件的 USB 设备，将执行指定的补救操作。还会向策略服务器报告该事件。

USB 存储检测需要依靠 OPSWAT v4 合规性模块。必须在 ISE UI 上的定期重新评估策略 (PRA) 中配置 USB 检查，位于 **Work Centers > Posture > Policy Elements > USB**。

注释 将按顺序执行检查和补救，因此将其他检查的 PRA 宽限期设定为最小值可以防止处理 USB 检查时的延迟。宽限期在 ISE UI 上的 **Work Centers > Posture > Settings > Reassessment Config** 中进行设置。

有关在 ISE UI 上配置 USB 存储设备检测的步骤，请参阅 USB 大容量存储设备检查工作流程。

自动合规性

凭借终端安全评估租约，ISE 服务器可以完全跳过终端安全评估检查，直接将系统置于合规状态。通过此功能，如果最近检查过系统终端安全评估，用户不必再经历网络间切换的延迟。ISE 终端安全评估代理仅需在发现 ISE 服务器后立即向 UI 发送状态消息，指示系统是否合规。在 ISE UI（“设置”(Settings)>“终端安全评估”(Posture)>“常规设置”(General Settings)）中，您可以指定在初始合规性检查后多长时间内，将终端视为满足安全评估要求。即使用户从一个通信接口切换到另一个，也应保持合规状态。

注释 使用终端安全评估租约时，如果 ISE 上的会话有效，终端会从未知状态变为合规状态。

VLAN 监控和转换

某些站点使用不同的 VLAN 或子网划分其集团公司和访问级别的网络。来自 ISE 的授权更改 (CoA) 指定 VLAN 更改。管理员操作（例如会话终止）也可能导致发生更改。为支持有线连接期间的 VLAN 更改，请在 ISE 终端安全评估配置文件中配置以下设置：

- VLAN Detection Interval - 确定代理检测 VLAN 转换的频率以及监控是否禁用。当此时间间隔设置为非 0 值时，会启用 VLAN 监控。对于 macOS，将此值至少设置为 5。

  VLAN 监控在 Windows 和 macOS 上都可实施，但在 macOS 上仅当检测意外 VLAN 更改时才需要实施。如果 VPN 已连接或者 acise（主要 Cisco Secure Client ISE 进程）未运行，它会自动禁用。有效范围为 0 到 900 秒。

- 启用代理 IP 地址刷新 (Enable agent IP refresh) - 未选中时，ISE 会向代理发送“网络过渡延迟”(Network Transition Delay) 值。选中后，ISE 将向代理发送 DHCP 释放和续订值，然后代理更新 IP 以检索最新的 IP 地址。

- DHCP Release Delay and DHCP Renew Delay - 用于关联 IP 刷新和 Enable Agent IP Refresh 设置。选中“启用代理 IP 地址刷新” (Enable agent IP refresh) 复选框且此值不是 0 时，代理会等待一定秒数的释放延迟，更新 IP 地址，然后等待一定秒数的续订延迟。如果 VPN 已连接，将自动禁用 IP 刷新。如果 4 次连续探测被丢弃，将会触发 DHCP 刷新。
- 网络过渡延迟 (Network Transition Delay) - 当 VLAN 监控被代理禁用或启用（在 Enable Agent IP Refresh 复选框中）时使用。此延迟在未使用 VLAN 时会增加缓冲，给代理适当的时间等待来自服务器的准确状态。ISE 将此值发送给代理。如果您还在 ISE 用户界面的全局设置中设置了 Network Transition Delay 值，ISE 终端安全评估配置文件编辑器中的值将覆盖它。

注释 Cisco Secure Firewall ASA 不支持 VLAN 更改，因此这些设置在客户端通过 Cisco Secure Firewall ASA 连接到 ISE 时不适用。

故障排除

如果终端设备在终端安全评估完成后无法访问网络，请检查以下内容：

- 在 ISE 用户界面上是否配置了 VLAN 更改？
  - 如已配置，是否在配置文件中设置了 DHCP 释放延迟和续订延迟？
  - 如果这两项设置都为 0，是否在配置文件中设置了 Network Transition Delay？

用于中断 Cisco Secure Client ISE 流的操作

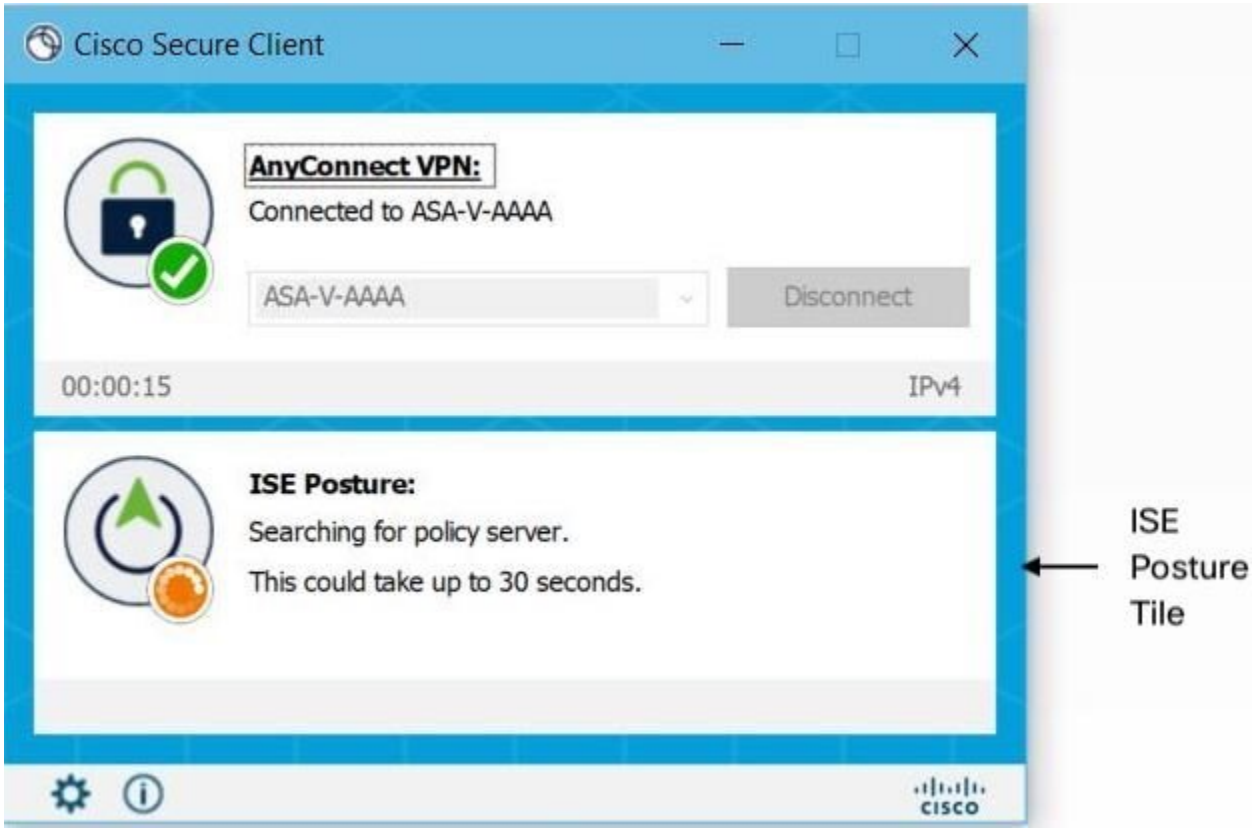
由于各种原因，在初始终端安全评估重新评估或被动重新评估过程中，Cisco Secure Client ISE 终端安全评估流可能中断。

- 用户取消 Cisco Secure Client ISE - 在终端安全评估检查和补救期间，用户可以取消 Cisco Secure Client ISE。UI 会立即通知用户正在进行取消，但只在避免将终端置于出问题状态的时期才会出现这种情况。如果使用了第三方软件，一些取消操作可能需要重新启动。取消后，Cisco Secure Client UI 的 ISE 终端安全评估磁贴部分显示合规状态。
- 修复计时器超时 - 满足终端安全评估要求的管理员控制时间已到期。一份评估报告被发送到前端。在被动重新评估期间，用户保留网络访问权限。而对于终端安全评估，满足所有强制性要求后将授予网络访问权限。
- 终端安全评估检查过程中出错 - 如果在终端安全评估检查阶段出错并且 Cisco Secure Client 能够继续，用户将收到通知，但如果可能，终端安全评估检查将继续。如果在强制终端安全评估检查期间出错，检查将标记为失败。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。
- 补救过程中出错 - 如果在补救阶段出错并且 Cisco Secure Client ISE 终端安全评估可以继续，用户会收到通知。如果失败的补救步骤与某个强制性终端安全评估要求相关，Cisco Secure Client ISE 终端安全评估将停止补救进程。如果失败的补救步骤与某个可选终端安全评估要求相关，则会尝试继续下一步并完成 ISE 终端安全评估操作。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。
- 默认网关更改 - 用户可能由于默认网关更改而失去受信任网络访问，导致 ISE 终端安全评估尝试重新发现 ISE。当 ISE 终端安全评估进入重新发现模式时，Cisco Secure Client UI 的 ISE 终端安全评估磁贴部分会显示 ISE 终端安全评估的状态。
- Cisco Secure Client 和 ISE 之间的连接丢失 - 终端被认为合规并被授予网络访问权限后，可能发生各种网络状况：终端可能遇到网络连接完全丢失的情况，ISE 可能性能下降，ISE 终端安全评估可能出现故障（由于会话超时、手动重启等）或 Cisco Secure Firewall ASA 后面的 ISE 可能丢失 VPN 隧道。
- 使用 ISE 终端安全评估时，不能在 macOS 终端上登录多个控制台用户。

- 初始化和终端安全评估流程延迟（仅 macOS）- Apple 建议您允许其子网处于终端安全评估前阶段，以避免合规性模块库签名验证失败。

ISE 终端安全评估的状态

当 Cisco Secure Client ISE 终端安全评估按预期正常运行和阻止网络访问时，Cisco Secure Client 用户界面的 ISE 终端安全评估磁贴中显示“ISE 终端安全评估: Searching for policy server”。在 Windows 任务管理器或 macOS 系统日志中，您可以看到该进程正在运行。如果该服务未运行，ISE 终端安全评估 用户界面的 ISE 终端安全评估磁贴中显示“ISE 终端安全评估: Service is unavailable”。



网络变化启动发现阶段。使用 Cisco Secure Client ISE 终端安全评估时，如果主要接口的默认路由发生更改，会使代理回到发现过程。例如，当 Wi-Fi 和主要 LAN 连接时，代理会重新启动发现。同样，如果 Wi-Fi 和主要 LAN 建立连接，然后 Wi-Fi 断开连接，则代理不会重新启动发现。

在 Cisco Secure Client 用户界面的 ISE 终端安全评估磁贴中的“ISE 终端安全评估”之后，还可能出现以下状态消息：

- 未能加载合规性模块 (Failed to load compliance module) - 在 *ISEPosture* > CLI 提示符后返回，但未加载合规性模块。
- Limited or no connectivity - 未进行发现，因为您没有连接。Cisco Secure Client ISE 终端安全评估代理可能正在网络中的错误终端上执行发现。

- 当前 Wi-Fi 不需要系统扫描 (System scan not required on current WiFi) - 未进行发现，因为检测到不安全的 WiFi。Cisco Secure Client ISE 终端安全评估代理仅在 LAN、无线网络（如果使用 802.1X 身份验证）以及 VPN 上启动发现。Wi-Fi 可能不安全，或者您通过在代理配置文件中将 *OperateOnNonDot1XWireless* 设置为 1 禁用了该功能。
- Unauthorized policy server - 主机与 ISE 网络的服务器名称规则不匹配，因此网络访问受限或不允许访问。
- Cisco Secure Client 下载程序正在执行更新... (AnyConnect Downloader is performing update...) - 下载程序已调用，将比较软件包版本、下载 Cisco Secure Client 配置，并执行必要的升级。
- Scanning System... - 扫描防病毒和反间谍软件安全产品是否已启动。如果在此过程中网络发生更改，代理将循环生成日志文件的过程，并且状态返回到“No policy server detected”。
- 绕过 AnyConnect 扫描 (Bypassing Cisco Secure Client scan) - 网络配置为使用思科 NAC 代理。
- “被用户取消的不受信任的策略服务器”(Untrusted Policy Server Cancelled by the user) - 在 Cisco Secure Client 用户界面中使用“系统扫描首选项”(ISE 终端安全评估 Preferences) 选项卡取消阻止连接到不受信任的服务器时，弹出窗口中会出现 Cisco Secure Client 下载程序的安全警告。在此警告页面上点击**取消连接 (Cancel Connection)** 时，ISE 终端安全评估磁贴会更改为此状态。

  在 ISEPosture> CLI 提示符后进入 *state* 并确定策略服务器不受信任时，也会出现此消息。
- Network Acceptable Use Policy - 访问网络时，您必须查看并接受“可接受的使用策略”。拒绝该政策可能会导致网络访问受限。
- Updating Network Settings - 在 ISE 用户界面的 Settings > Posture > General Settings 中，您可以指定网络转换之间应发生的延迟秒数。
- Not Compliant. Update time expired - 为补救设置的时间已过期。
- Compliant. Network access allowed. - 补救完成。“系统扫描”(Cisco Secure Client) >“扫描摘要”(Scan Summary) 也显示状态为完成。

  在 ISEPosture> CLI 提示符后进入 *state* 并确定策略服务器受信任时，也会出现此消息。
- No policy server detected - 找不到 ISE 网络。30 秒钟后，代理会减慢探测。默认网络访问权限生效。

脚本补救消息传送

您可能会在脚本补救过程中看到补救或用户通知弹出窗口，除非您是在用户界面有限的 Linux 中运行。要使脚本补救成功，指纹必须存在于 AnyConnectLocalPolicy.xml 中。如果添加了指纹，即使在正常终端安全评估流程中，无论 ISE 上是否配置了脚本条件或补救措施，都会对指纹进行验证。您可能会遇到有关脚本补救的以下消息：

- **由于脚本包含无效散列，因此无法尝试补救 (Remediation cannot be attempted because the script has an invalid hash)** - 当下载的脚本存在散列不匹配或者策略签名验证失败时，会在ISE 终端安全评估详细信息中显示此消息。

- **您尝试运行的脚本退出并出现错误 (The script you are trying to run exits with an error)** - 当脚本存在非零退出代码时，会在ISE 终端安全评估详细信息中显示此消息。 在 Windows 中，配置的执行策略也可能不允许执行脚本。
- **补救由于脚本超时而不成功 (Remediation was unsuccessful because the script timed out)** - 当脚本花费的时间超出补救计时器的退出时间时，会在ISE 终端安全评估详细信息中显示此消息。如果脚本未在剩余补救计时器的时间内退出，则 Cisco Secure Client 会停止脚本并将补救标记为失败。
- **由于您连接到了不受信任的服务器，因此无法执行补救 (Remediation cannot be done because you are connected to an untrusted server)** - 当终端连接到不受信任的 ISE 服务器时，会在Cisco Secure Client详细信息中显示此消息。服务器证书在证书存储库中未被标记为受信任，或者您没有在 AnyConnectLocalPolicy.xml 中配置指纹。ISE 提供的证书中的指纹必须与 AnyConnectLocalPolicy.xml 中配置的指纹匹配。

终端安全评估条件脚本

您可以创建并上传终端安全评估条件脚本，以便对终端进行安全评估检查。支持以下平台和脚本类型。有关添加脚本条件的配置详细信息，请参阅《思科身份服务引擎管理员指南》。

- Windows：PowerShell 脚本 (.ps1)
- macOS：外壳脚本 (.sh)
- Linux：外壳脚本 (.sh)

终端安全评估和多宿主

Cisco Secure Client ISE 终端安全评估模块不支持多宿主，因为此类场景的行为未定义。例如，当介质模式从有线更改为无线然后返回到有线时，即使终端实际上在有线连接上进行重定向，用户也可能会看到 ISE 终端安全评估模块的评估状态是合规的。

终端上的并发用户

当多名用户同时登录到终端而共享网络连接时，Cisco Secure Client ISE 终端安全评估不支持单独的终端安全评估。当运行 Cisco Secure Client ISE 终端安全评估的第一位用户的状态被成功捕获时，终端将被授予受信任的网络访问权限，该终端上的所有其他用户都将继承网络访问权限。为防止发生此情况，管理员可在终端上禁用允许并发用户的功能。

终端安全评估模块的日志记录

对于 ISE 终端安全评估，事件将写入本地操作系统的事件日志（Windows 事件日志查看器或 macOS 系统日志）。

对于 Cisco Secure Firewall 终端安全评估，任何错误和警告都将写入系统日志（非 Windows）和事件查看器 (Windows)。所有可用的消息都将写入日志文件。

Cisco Secure Firewall 终端安全评估 模块组件会根据操作系统、权限级别和启动机制来提供日志输出：

- libcsd.log - 由使用 Cisco Secure Firewall 终端安全评估 API 的 Cisco Secure Client 线程创建。调试条目根据日志记录级别配置写入此日志。
- cscan.log - 通过扫描可执行文件 (cscan.exe) 而创建，是 Cisco Secure Firewall 终端安全评估的主要日志。调试条目根据日志记录级别配置写入此日志。

终端安全评估模块的日志文件和位置

对于 ISE 终端安全评估，事件包含在安装的 Cisco Secure Client 版本的事件子文件夹中，因此易于与其余 Cisco Secure Client 事件隔开。每个查看器均可搜索关键字和过滤。Web 代理事件写入标准应用日志。

为便于故障排除，会将 ISE 终端安全评估要求策略和评估报告记录到终端上经过模糊处理的单独文件中，而不会是事件日志中。某些日志文件的大小（例如 aciseposture），可由管理员在配置文件中配置。但 UI 日志大小是预定义的。

每当进程异常终止时，都会生成一个小型转储文件，就像其他 Cisco Secure Client 模块提供的一样。

对于 Cisco Secure Firewall 终端安全评估，文件位于用户主文件夹中的以下目录中：

- （非 Windows）- .cisco/posture/log
- (Windows)— C:\Users\<user_name>\AppData\Local\Cisco Cisco Secure Firewall 终端安全评估 \log\cscan.log

ISE 终端安全评估配置文件编辑器

管理员可以选择使用独立编辑器创建终端安全评估配置文件，然后将其上载至 ISE。否则，嵌入式终端安全评估配置文件编辑器配置在 ISE 用户界面中的 Policy Elements 下。Cisco Secure Client 配置编辑器在 ISE 中启动后，它会创建 Cisco Secure Client 配置以及 Cisco Secure Client 软件及其关联的模块、配置文件、OPSWAT 和任何自定义。 ISE 终端安全评估的独立配置文件编辑器包含以下参数：

- 代理的行为

- **启用签名检查 (Enable signature check)** - 如果选中，则在代理运行可执行文件之前，会启用这些文件的签名检查。
- **日志文件大小 (Log file size)** - 合规模块日志文件的最大大小。有效值为 5 Mb 到 200 Mb。
- **修复计时器 (Remediation timer)** - 用户必须在此时间内完成修复，否则将被标记为不合规。有效值为 1 - 300 分钟。
- **自动 DART 计数 (Automated DART Count)** - 确定在故障情况下要收集的自动 DART 捆绑包的数量。
- **启用代理日志跟踪 (Enable agent log trace)** - 在代理上启用调试日志。
- **在非 802.1X 无线网络上运行 (Operate on non-802.1X wireless networks)** - 如果选中，会启用代理在非 802.1X 无线网络上工作。
- **启用终端安全评估状态非重定向流 (Enable posture non-redirection flow)**- 如未选中，则会禁用终端安全评估状态非重定向流。在禁用之前，请确保所有 NAD 均支持重定向。
- **启用隐身模式 (Enable Stealth Mode)** - 选择是否启用隐身模式，这将允许终端安全评估作为服务运行，而无需用户干预。
- **通过通知启用隐身 (Enable Stealth With Notification)** - 如果隐身型号通知设置为启用，则当 Cisco Secure Client 隐身型号出现处于不合规状态、网络访问受限、有无法访问的服务器等情况时，最终用户仍然会收到通知消息。
- **禁用 EDR Internet 检查 (Disable EDR Internet Check)** - 当终端具有已配置的代理时，观察到定义检查失败。当终端配置了代理时，它会导致任何 EDR 产品（例如 Cortex XDR）无法访问互联网。要绕过互联网检查并跳过实时传输协议检查以及终端和检测响应产品 (EDR) 的定义检查，请点击此复选框将其设置为“是”(Yes)。
- **启用重新扫描按钮 (Enable Rescan Button)** - 如果要在发生故障后、手动修复后或终端安全评估陷入停滞状态等情况后重启终端安全评估（或发现），请启用此按钮，以便在ISE 终端安全评估磁贴中显示 **再次扫描 (Scan Again)** 选项。您可以在 ISE 终端安全评估配置文件中显示或隐藏该选项。点击**再次扫描 (Scan Again)** 时，系统将启动发现，并启动整个终端安全评估流。

注释 仅当终端安全评估配置文件中的 EnableRescan 标记设置为 1 时，磁贴中才会显示“再次扫描”。如果设置为 0，则“再次扫描”(Scan Again) 按钮仅在其以前通常显示的条件下显示（在此选项之前）。

注释 如果在 ISE 端发生配置文件更改，则 Cisco Secure Client 磁贴将在系统下一次启动发现时反映相关更改。

- **禁用 UAC 弹出窗口 (Disable UAC Popup)** - 确定在策略验证期间是否显示“Windows 用户帐户控制 (UAC)”弹出窗口。如果使用默认值（未选中），在进行连接时系统会继续提示

最终用户获得管理员权限。如果启用，在策略验证期间，最终用户将看不到 Windows 用户帐户控制 (UAC) 提示。通过禁用 UAC 提示，Cisco Secure Firewall 终端安全评估使用系统进程进行权限升级，而不是“以管理员身份运行”。在禁用UAC提示之前，在用户具有本地管理员权限的设备上验证您的终端安全评估策略。

- **补偿计时器限制 (Backoff Timer Limit)** - 输入 Cisco Secure Client 发送 ISE 发现探测所需的最长时间。Backoff Timer Limit 由于探测会增加更多流量，因此您应选择不会造成您的网络中断的值。
- **定期探测间隔 (Periodic Probe Interval)** - 指定超过回退计时器限制后的发现探测间隔。 Cisco Secure Client 会持续发送具有给定间隔的定期探测，直到找到有效的 ISE 服务器。默认值为 30 分钟，在初始几轮探测后，会持续以 30 分钟的间隔发送探测。将该值设置为 0 会禁用定期探测。
- **终端安全评估状态同步间隔 (Posture State Synchronization Interval)** - 输入 0 以禁用定期探测。有效范围为 0 至 300 秒。
- **终端安全评估状态同步探测列表 (Posture State Synchronization Probe List)** - 在发现阶段，代理将探测发送到备份列表以查找 ISE 服务器。默认值为无值。它使用所有数据包交换网络作为备份服务器。
- **CWA/BYOD 探测的最长时间 (Maximum time for CWA/BYOD probing)** - 如果配置了集中式 Web 身份验证 (CWA) 或自带设备 (BYOD) 流，则代理将在此秒数内探测数据包交换机网络，以确定是否结束用户已完成流程。如果完成，代理将启动终端安全评估流程。
- **CWA/BYOD 探测时间间隔 (Interval of CWA/BYOD probing)** - 如果配置了集中式 Web 身份验证 (CWA) 或自带设备 (BYOD) 流，则代理将在此秒间隔内探测数据包交换机网络，直到 CWA/BYOD 流完成或已达到最长时间。

- **IP 地址更改**

为了获得最佳用户体验，请将以下值设置为我们推荐的值。

- **VLAN 检测时间间隔 (VLAN detection interval)** - 代理在刷新客户端 IP 地址前检查 VLAN 变化的时间间隔。有效范围为 0 到 900 秒，推荐值为 5 秒。如果设为 0，则禁用 VLAN 检测功能。设为 1 至 900 时，代理将每隔 x 秒发送一次 Internet 控制消息协议 (ICMP) 或地址解析协议 (ARP) 查询。
- **Ping 或 ARP (Ping or ARP)** - 检测 IP 地址更改的方法。选项包括：Ping (0) 使用 ICMP 轮询，Arp (1) 使用 ARP 轮询，Ping then Arp (2) 先使用 ICMP 轮询，如果 ICMP 失败，再使用 ARP 轮询。建议使用 ARP 轮询，因为默认网关可能被配置为阻止 ICMP 数据包。
- **ping 最长超时 (Maximum timeout for ping)** - 从 1 到 10 秒的 ping 超时时间。
- **启用代理 IP 地址刷新 (Enable agent IP refresh)** - 选中可启用 VLAN 更改检测。
- **DHCP 续约延迟 (DHCP renew delay)** - 代理在 IP 刷新之后等待的秒数。如果启用了“启用代理 IP 刷新”(Enable Agent IP Refresh)，请配置此值。如果该值不是 0，则代理将在此预期的过渡期间进行一次 IP 刷新。如果在刷新时检测到 VPN，则刷新将被禁用。有效值为 0 到 60 秒，推荐值为 5 秒。将此参数设置为 0 可禁用此功能。

- **DHCP 释放延迟 (DHCP release delay)** - 代理延迟进行 IP 刷新的秒数。如果启用了“启用代理 IP 刷新”(Enable Agent IP Refresh)，请配置此值。如果该值不是 0，则代理将在此预期的过渡期间进行一次 IP 刷新。如果在刷新时检测到 VPN，则刷新将被禁用。有效值为 0 到 60 秒，推荐值为 5 秒。将此参数设置为 0 可禁用此功能。
- **网络转换延迟 (Network transition delay)** - 代理暂停网络监控以便等待计划好的 IP 更改的时间范围（以秒为单位）。推荐值为 5 秒。

- 终端安全评估协议
  - **发现主机 (Discovery host)** - 用于基于重定向的网络中的策略服务节点发现。使用 IP 或 FQDN 确定网络访问设备可执行重定向的服务器。对于独立配置文件编辑器，仅输入单个主机。
  - **服务器名称规则 (Server name rules)** - 由通配符、逗号分隔名称组成的列表，用于定义代理可以连接到的服务器（如 example1.cisco.com 或 *.cisco.com）。
  - **Call Home 列表 (Call Home List)** - 输入您想用于负载均衡、监控和故障排除查找的 IP 或 FQDN，或者您想用于映射到该节点中默认策略服务节点 (PSN) 的 DNS 的 FQDN（如果处于多重情形下）。在配置此选项后，将发送用于监控和故障排除查找的第一次探测，以拨打住宅电话。在从重定向网络迁移到非重定向网络时，必须配置此选项。
  - **PRA 重新传输时间 (PRA retransmission time)** - 当发生被动重新评估通信失败时，就会指定此代理重试时间范围。有效范围为 60 到 3600 秒。
  - **重新传输延迟 (Retransmission Delay)** - 指定在执行 HTTP 任务（GET 或 POST）失败后重试之前要等待的时间（以秒为单位）。有效范围为 5 到 300 秒，默认值为 60，仅接受整数值。
  - **重新传输限制 (Retransmission Limit)** - 指定在执行 HTTP 任务（GET 或 POST）失败后允许消息重试的次数。有效范围为 0 到 10，默认值为 4，仅接受整数值。

高级面板

Cisco Secure Client UI 的高级面板是每个组件显示统计信息、用户首选项和特定于组件的任何其他信息的区域。如果点击 Cisco Secure Client 系统托盘上的**所有组件的高级窗口 (Advanced Window for all components)** 图标，则新的“系统扫描”(System Scan) 部分将包含以下选项卡：

注释 这些统计信息、用户首选项、消息历史记录等等均显示在 macOS 的“统计信息”(Statistics) 窗口下面。首选项在“首选项”(Preferences) 窗口中，而不像在 Windows 中那样在选项卡中。

- **首选项 (Preferences)** — 允许您阻止与不受信任的服务器的连接，以便在下载程序过程中，对于任何具有不受信任的认证且未经验证的 ISE 服务器，您都会收到“已阻止不受信任的服务器”(Untrusted Server Blocked) 消息。如果禁用阻止，Cisco Secure Client 不会阻止与潜在恶意网络设备的连接。

- **统计 (Statistics)** — 提供当前 ISE 终端安全评估状态（合规或不合规）、OPSWAT 版本信息、可接受使用策略的状态、终端安全评估的最新运行时间戳、所有缺少的要求以及对故障排除来说足够重要而要显示的任何其他统计信息。
- **安全产品 (Security Products)** — 访问系统中安装的防恶意软件产品的列表。
- **扫描摘要 (Scan Summary)** — 允许用户查看管理员为其配置以供查看的任何终端安全评估项。例如，配置时，他们可以查看查看显示终端安全评估的所有项或者只查看终端安全评估检查和要求的补救失败的项。
- **消息历史记录 (Message History)** — 为组件提供向系统托盘发送的每条状态消息的历史记录。该历史记录对于故障排除非常有用。

Cisco Secure Firewall 终端安全评估 模块提供的功能

Cisco Secure Firewall 终端安全评估

Cisco Secure Firewall 终端安全评估（之前的 HostScan）是在用户连接到 Cisco Secure Firewall ASA 后但在登录前安装到远程设备上的软件包。Cisco Secure Firewall 终端安全评估由基本模块、终端评估模块和高级终端评估模块任意组合而成。Cisco Secure Firewall 终端安全评估不支持移动设备（Android、iOS、Chrome 或 UWP）。

基本功能

Cisco Secure Firewall 终端安全评估 自动在建立思科无客户端 Cisco Secure Client 客户端会话的任何远程设备上识别操作系统和服务包。

您还可以配置 Cisco Secure Firewall 终端安全评估 以检查终端的特定流程、文件和数字密钥。它在全隧道建立之前执行上述所有检查项，然后向 Cisco Secure Firewall ASA 发送此信息以区分公司拥有的计算机、个人计算机和公共计算机。该信息也可用于评估。

注释 评估信息和返回的证书信息不可用。Cisco Secure Firewall 终端安全评估 不是身份验证方法。它只是检验尝试连接的设备上存在什么。

Cisco Secure Firewall 终端安全评估 也会自动返回以下其他值，用于根据已配置的 DAP 终端条件进行评估：

- Microsoft Windows、macOS 和 Linux 操作系统
- Microsoft 知识库编号 (KB)
- 设备终端属性类型（如：主机名、MAC 地址、BIOS 序列号、端口号（传统属性）、TCP/UDP 端口号、隐私保护和终端评估（OPSWAT）的版本

注释 Cisco Secure Firewall 终端安全评估 会收集有关 Windows 客户端系统上 Microsoft 软件更新的服务版本 (GDR) 信息。服务版本包含多个修补程序。服务版本终端属性用在 DAP 规则（而非修补程序）中。

终端评估

终端评估是一项 Cisco Secure Firewall 终端安全评估 扩展功能，用于检查远程计算机上是否存在大量防病毒和反间谍软件应用、相关定义更新以及防火墙。在 Cisco Secure Firewall ASA 向会话分配特定 Dynamic Access Policy (DAP) 之前，可以使用此功能组合终端条件来满足您的要求。

有关详细信息，请参阅相应版本的《思科 ASA 系列 VPN CLI 或 ASDM 配置指南》中的动态访问策略部分。

高级终端评估：防恶意软件和防火墙补救

在 Windows、macOS 和 Linux 桌面中，如果软件允许单独的应用启动补救，高级终端评估可以尝试发起防恶意软件和个人防火墙保护等各方面的补救。

防恶意软件 - 高级终端评估可以尝试补救防恶意软件的以下组件：

- 强制文件系统保护 - 如果防恶意软件已被禁用，则高级终端评估将启用它。
- 强制病毒定义更新 - 如果在高级终端评估配置定义的天数内未更新防恶意软件定义，则高级终端评估将尝试发起病毒定义更新。

个人防火墙 - 高级终端评估模块可以启用或禁用防火墙。

Cisco Secure Firewall 终端安全评估 不支持阻止或允许使用个人防火墙的应用和端口。

注释 并非所有个人防火墙都支持此 Force Enable/Force Disable 功能。

为 Cisco Secure Firewall 终端安全评估 配置防恶意软件应用

在安装 Cisco Secure Firewall 终端安全评估 模块之前，请配置您的防恶意软件，将以下这些应用归为安全例外。防恶意软件应用可能会将这些应用的行为误判为恶意行为：

- cscan.exe
- ciscod.exe
- cstub.exe

与动态访问策略集成

Cisco Secure Firewall ASA 将 Cisco Secure Firewall 终端安全评估 功能集成到动态访问策略 (DAP) 中。根据配置，Cisco Secure Firewall ASA 将一个或多个终端属性值与可选 AAA 属性值组合作为分配 DAP 的条件。DAP 的终端属性支持的 Cisco Secure Firewall 终端安全评估 功能包括操作系统检测、策略、基本结果和终端评估。

可以指定单个属性或组合多个属性来构成将 DAP 分配到会话所需的条件。DAP 提供适用于终端 AAA 属性值级别的网络访问。当满足所有已配置的终端条件后，ASA 应用 DAP。

请参阅思科 ASA 系列 VPN CLI 或 ASDM 配置指南中的配置动态访问策略部分。

DAP 中的 BIOS 序列号

Cisco Secure Firewall 终端安全评估可以检索主机的 BIOS 序列号。您可以使用动态访问策略 (DAP) 允许或阻止基于该 BIOS 序列号建立到 Cisco Secure Firewall ASA 的 VPN 连接。

将 BIOS 指定为 DAP 终端属性

步骤 1 登录到 ASDM。

步骤 2 选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** 或**无客户端 SSL VPN 访问 (Clientless SSL VPN Access)** > **动态接入策略 (Dynamic Access Policies)**。

步骤 3 在“配置动态访问策略”(Configure Dynamic Access Policies) 面板中，点击**添加 (Add)** 或**编辑 (Edit)** 将 BIOS 配置为 DAP 终端属性。

步骤 4 在“终端 ID”(Endpoint ID) 表的右侧，点击**添加 (Add)**。

步骤 5 在“终端属性类型”(Endpoint Attribute Type) 字段中，选择**设备 (Device)**。

步骤 6 选中 **BIOS 序列号 (BIOS Serial Number)** 复选框，选择 **=**（等于）或 **!=**（不等于），然后在“BIOS 序列号”(BIOS Serial Number) 字段中输入 BIOS 编号。点击**确定 (OK)** 保存在“终端属性”(Endpoint Attribute) 对话框中的更改。

步骤 7 点击**确定 (OK)** 保存对“编辑动态访问策略”(Edit Dynamic Access Policy) 的更改。

步骤 8 点击**应用 (Apply)** 保存对动态访问策略的更改。

步骤 9 点击**保存 (Save)**。

如何获取 BIOS 序列号

- Windows - http://support.microsoft.com/kb/558124
- macOS—http://support.apple.com/kb/ht1529
- Linux - 使用此命令：

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

确定在 Cisco Secure Firewall ASA 上启用的 Cisco Secure Firewall 终端安全评估 映像

打开 ASDM 并选择**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 终端安全评估**（对于 **Cisco Secure Firewall**）**(Posture [for Secure Firewall]) > 终端安全评估映像 (Posture Image)**。

磁盘加密

您可以启用报告终端上安装的磁盘加密产品。然后，在csc_cscan日志中，您可以找到磁盘的版本详细信息和加密状态。

在 ASDM 上的“高级终端评估”(Advanced Endpoint Assessment) 屏幕中， 识别终端上的加密磁盘 *(Identify Encrypted Disks on Endpoint)* 复选框可激活磁盘加密。ASDM 中此屏幕的导航是“配置”(Configuration) > 远程接入 VPN (Remote Access VPN) > 终端安全评估（适用于 Cisco Secure Firewall）(Posture [for Secure Firewall]) > 终端安全评估设置 (Posture Settings) > 配置 (Configure)。

升级 Cisco Secure Firewall 终端安全评估

如果您要手动升级 Cisco Secure Client 和 Cisco Secure Firewall 终端安全评估（使用 msiexec），请确保先升级 Cisco Secure Client，然后再升级 Cisco Secure Firewall 终端安全评估。

OPSWAT 支持

Cisco Secure Firewall 终端安全评估（之前的 Hostscan）终端安全评估和 ISE 终端安全评估模块均使用 OPSWAT 框架来保护终端。

此框架涉及客户端和头端，可协助评估终端上的第三方应用。根据所使用的OPSWAT版本，为每种终端安全评估方法提供支持图表。它们包含应用列表的产品和版本信息。

当头端（Cisco Secure Firewall ASA 或 ISE）和终端（Cisco Secure Firewall 终端安全评估或 ISE 终端安全评估）之间存在版本号不匹配的情况时，OPSWAT 合规性模块将会进行升级或降级，以便与头端上的版本匹配。这些升级/降级是强制性的，并会自动进行，无需最终用户干预，只要建立了到头端的连接即可。

Cisco Secure Firewall 终端安全评估 OPSWAT 支持

Cisco Secure Firewall 终端安全评估 支持图表对应于 Cisco Secure Firewall 终端安全评估 软件包版本，并提供适用于 Cisco Secure Firewall ASA 头端的内容。

Cisco Secure Firewall 终端安全评估 的版本将与 Cisco Secure Client 的主版本和维护版本保持协调。在 ASDM 的**配置 (Configuration) > 远程接入 VPN (Remote Access VPN) > 安全桌面管理器 (Secure Desktop Manager) > HostScan 映像 (HostScan Image)** 中配置 Cisco Secure Firewall 终端安全评估 软件包时指定版本。

注释 在即将发布的 ASDM 版本中，此菜单路径将为**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 终端安全评估 (Posture)**（对于 **Cisco Secure Firewall**）**> 终端安全评估映像 (Posture Image)**，因为 HostScan 已重命名。

Cisco Secure Firewall 终端安全评估 准则：

- 在客户端和头端中使用的 OPSWAT 版本必须匹配。
- 所有 4.3.x 以下（包括 4.3.x）版本的 HostScan 都使用 OPSWAT v2。HostScan 4.6 x 和更高版本使用 OPSWAT v4。所有版本的 HostScan 都不支持 OPSWAT v3。

ISE 终端安全评估 OPSWAT 支持

Cisco Secure Client 代理合规性模块适用于 ISE 终端安全评估模块。

ISE 代理合规性模块版本反映了基础 OPSWAT 版本。在 ISE 终端安全评估中，OPSWAT 二进制文件封装在一个单独的安装程序中。您可以手动将 OPSWAT 库从本地文件系统载入 ISE 头端，或配置 ISE 使用 ISE 更新源 URL 直接获取该库。

将 Cisco Secure Client与 ISE 2.1（或更高版本）配合使用时，可以选择将 OPSWAT v3 或 v4 用于 ISE 合规性模块。防恶意软件的配置位于 ISE UI 的 **Work Centers > Posture > Posture Elements > Conditions > Antimalware**。

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。