实施ISE无重定向终端安全评估

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- Connectiondata.xml
- Call Home列表

设计

配置

- 网络设备组（可选）
- 网络设备
- 客户端调配
  - 手动调配（预部署）
  - 客户端调配门户（Web部署）
  - 客户端调配策略
- 授权
  - 授权配置文件
  - 授权策略

故障排除

- 思科安全客户端上合规且安全评估在ISE上不适用（挂起）
  - 陈旧/幻像会话
  - 识别
  - 解决方案
- 性能
  - 识别
  - 解决方案
- 记账

相关信息

简介

本文档介绍无重定向状态流程的使用和配置以及故障排除提示。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE上的终端安全评估流程

- 在ISE上配置终端安全评估组件
- 重定向至ISE门户

为了更好地了解下文介绍的概念，建议完成以下步骤：

比较ISE终端安全评估重定向流与ISE终端安全评估无重定向流
排除ISE会话管理和状态故障

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.3
- 思科安全客户端5.0.01242

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

ISE终端安全评估流程包括以下步骤：

0.身份验证/授权。通常在终端安全评估流程启动之前执行，但某些使用案例（例如终端安全评估重新评估[PRA]）可以绕过此流程。

由于身份验证本身不会触发状态发现，这并非每个状态流所必需的。

1. 发现。由安全客户端ISE终端安全评估模块执行的进程，查找当前活动会话的PSN所有者。
2. 客户端调配。由ISE执行的为客户端调配相应思科安全客户端（以前称为AnyConnect）ISE终端安全评估模块和合规性模块版本的流程。在此步骤中，特定PSN中包含和签名的终端安全评估配置文件的本地副本也会被推送到客户端。
3. 系统扫描。在ISE上配置的状况策略由合规性模块评估。
4. 补救（可选）。 在任何状况策略不合规的情况下执行。
5. 答：需要重新授权才能授予最终（符合或不符合）网络访问权限。

本文档重点介绍ISE终端安全评估流程的发现流程。

思科建议使用重定向执行发现过程，但在某些情况下，无法实施重定向，例如使用不支持重定向的第三方网络设备。本文档旨在提供一般指南和最佳实践，以便在这些环境中实施无重定向状态并进行故障排除。

无重定向流的完整说明在将ISE终端安全评估重定向流与ISE终端安全评估无重定向流进行比较

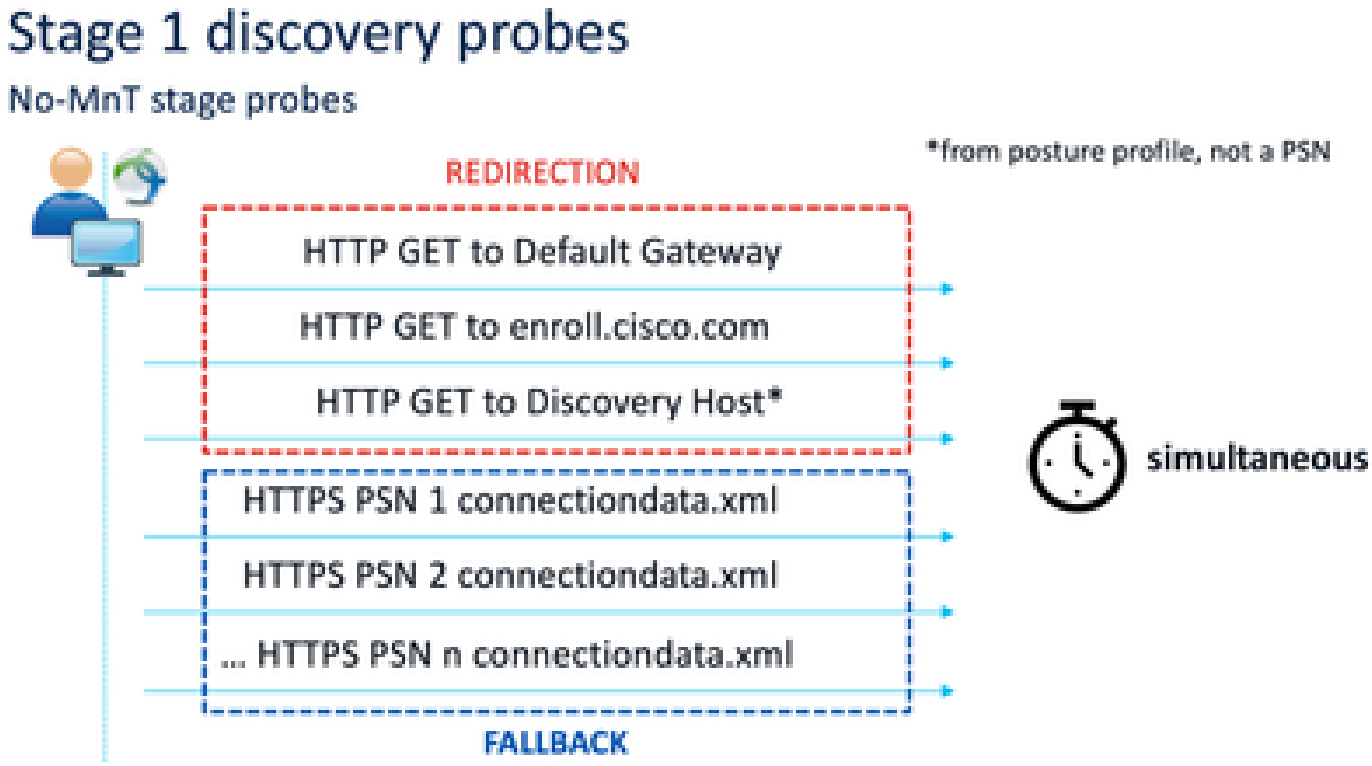
有两种类型的状况发现探针不使用重定向：

1. Connectiondata.xml
2. Call Home列表

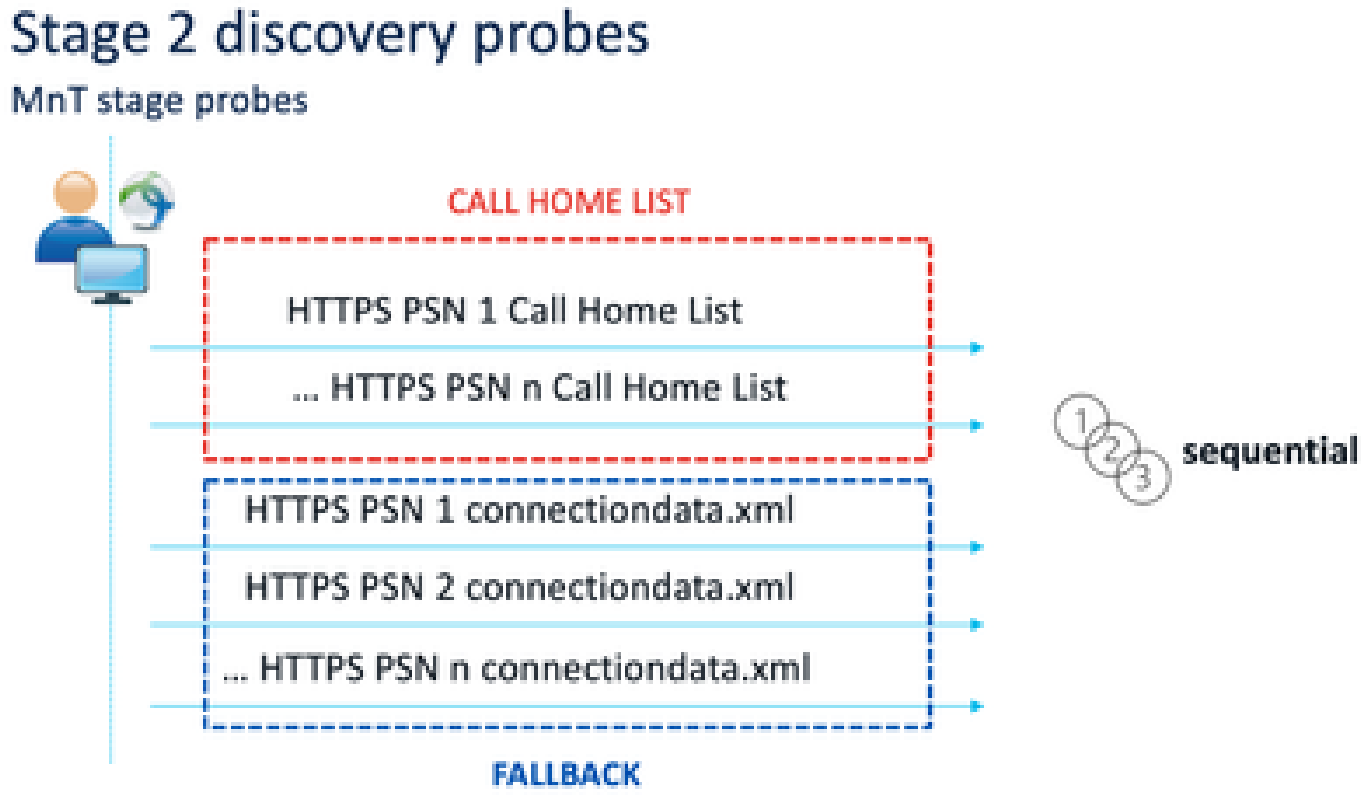
Connectiondata.xml

Connectiondata.xml是由Cisco安全客户端自动创建和维护的文件。它包含客户端以前成功连接到的PSN列表以进行安全评估，因此，这只是一个本地文件，其内容不会在所有终端上持续存在。

connectiondata.xml的主要用途是用作第1阶段和第2阶段发现探测功能的备份机制。如果重定向或Call Home List探测功能无法找到具有活动会话的PSN，Cisco安全客户端会向connectiondata.xml中列出的每个服务器发送直接请求。



第1阶段发现探测



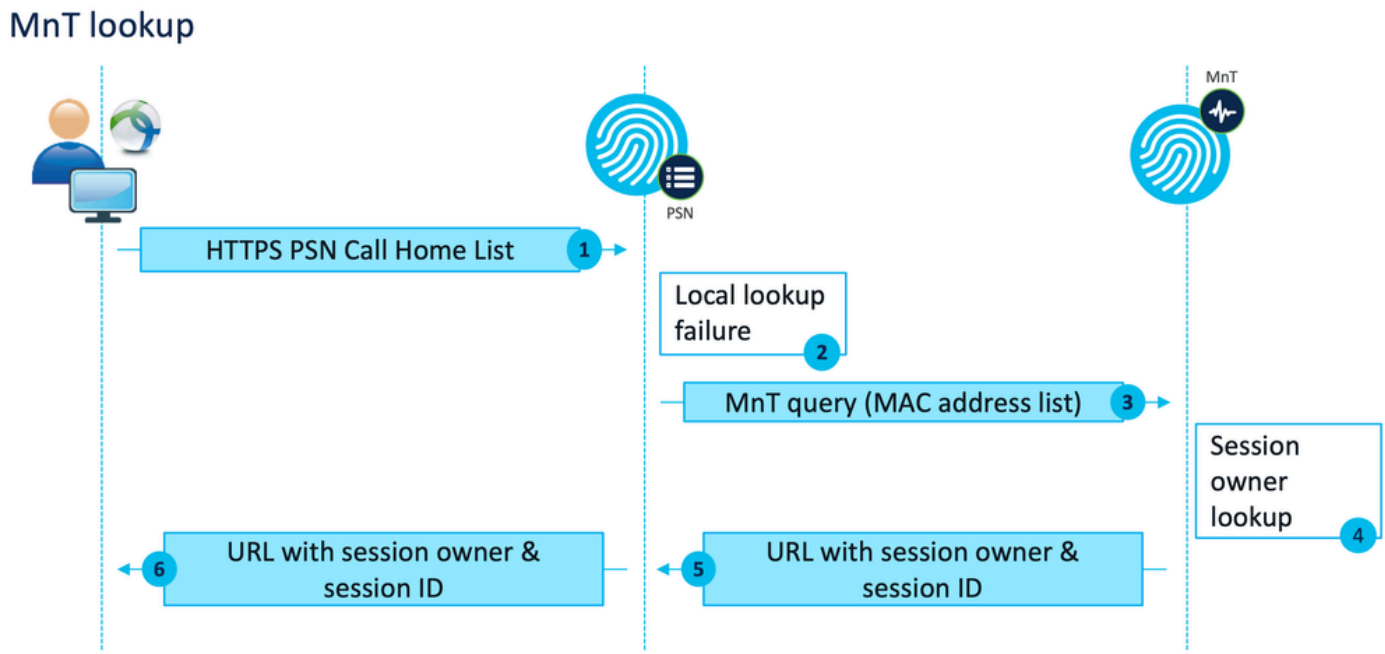
第2阶段发现探测

使用connectiondata.xml探测功能导致的常见问题是由于终端发送大量HTTPS请求而导致的ISE部署过载。需要考虑的是，虽然connectiondata.xml可有效作为备份机制来避免重定向和无重定向状态机制的完全中断，但它不是状态环境的可持续解决方案，因此，必须诊断和解决导致主要发现探测功能失败并导致发现问题的设计和配置问题。

Call Home列表

Call Home List是安全评估配置文件的一个部分，其中指定了PSN列表以用于安全评估。与connectiondata.xml不同，它由ISE管理员创建和维护，可能需要设计阶段才能实现最佳配置。Call Home列表中的PSN列表与网络设备或RADIUS负载均衡器中配置的身份验证和记帐服务器列表匹配。

如果PSN中的本地查找失败，Call Home List探测功能可在活动会话搜索期间使用MnT查找。只有在第2阶段发现期间使用相同功能时，它们才会扩展到connectiondata.xml探测器。因此，所有第2阶段探测也称为新一代探测。



MnT查找流程

设计

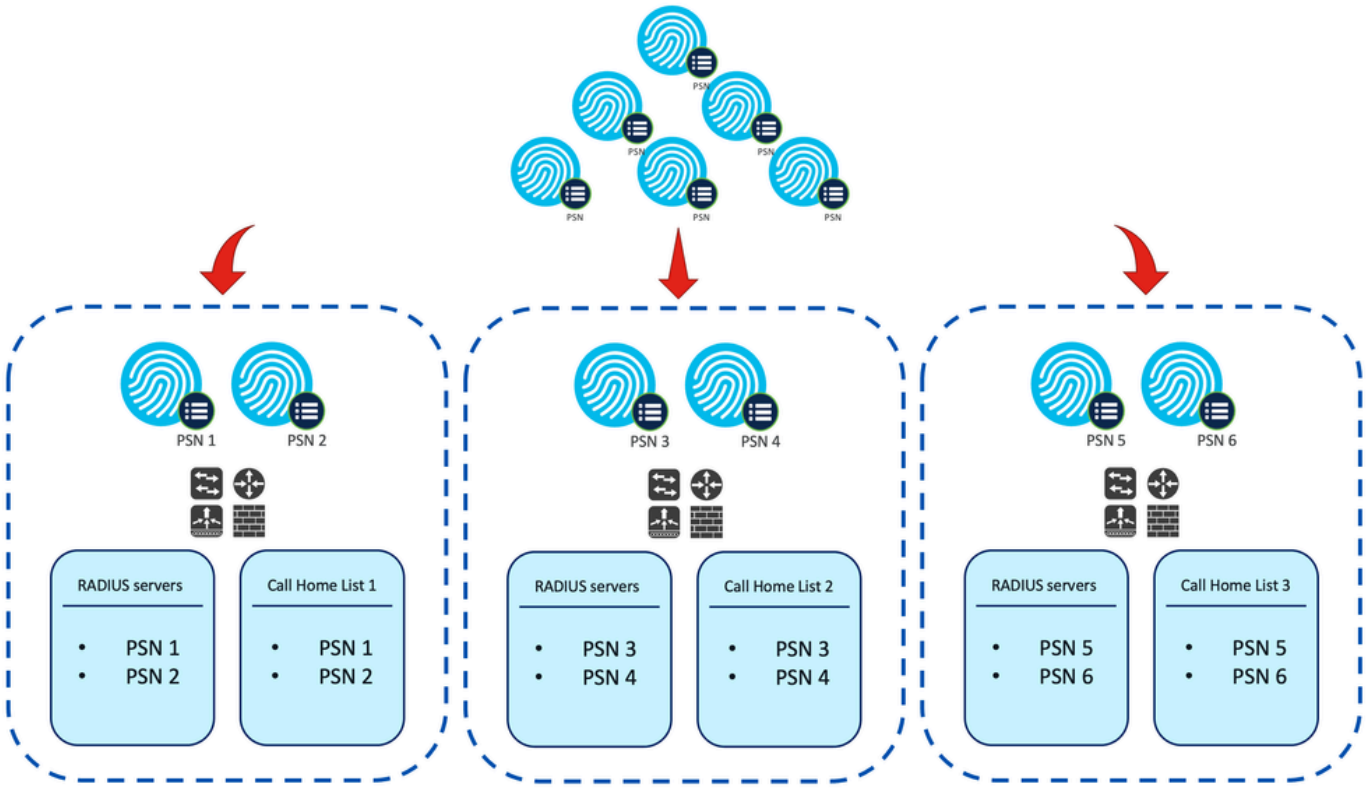
与重定向流程相比，无重定向发现流程通常需要更复杂的流程以及对PSN和MnT的更大处理量，因此在实施过程中可能会出现两个常见挑战：

1. 有效发现
2. ISE部署性能

为了应对这些挑战，建议设计Call Home列表以限制给定终端可用于终端安全评估的PSN数量。对于中型和大型部署，必须分发部署以便创建多个Call Home列表，减少PSN的数量，因此，用于给定网络设备的RADIUS身份验证的PSN列表可以同样限制为与相应的Call Home列表匹配。

制定PSN分配策略以确定每个Call Home列表中的PSN最大数量时，可以考虑以下方面：

- 部署中的PSN数量
- PSN和MnT节点的硬件规格
- 部署中并发状态会话的最大数量
- 网络设备数量
- 混合环境（同步重定向和无重定向状态实施）
- 终端使用的适配器数量
- 网络设备和PSN的位置
- 用于安全评估的网络连接类型（有线、无线、VPN）



示例：无重定向状态的PSN分配

提示：使用网络设备组根据设计对网络设备进行分类。

配置

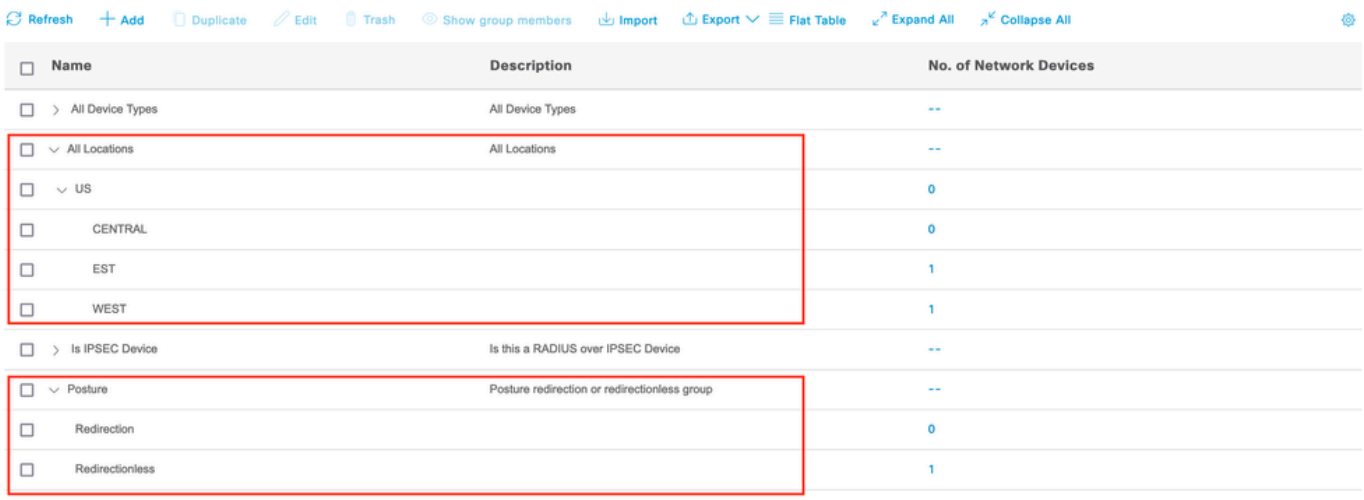
网络设备组（可选）

网络设备组可用于标识网络设备并与其对应的RADIUS服务器列表和Call Home列表相匹配。在混合环境中，它们还可用于识别支持从不支持重定向的设备重定向的设备。

如果在设计阶段制定的分配策略依赖于网络设备组，请按照以下步骤在ISE上配置它们：

1. 导航到Administration > Network Resources Network Resource Groups。
2. 单击Add添加新组，提供名称，然后选择父组（如果适用）。
3. 重复第2步创建所有必要的组。

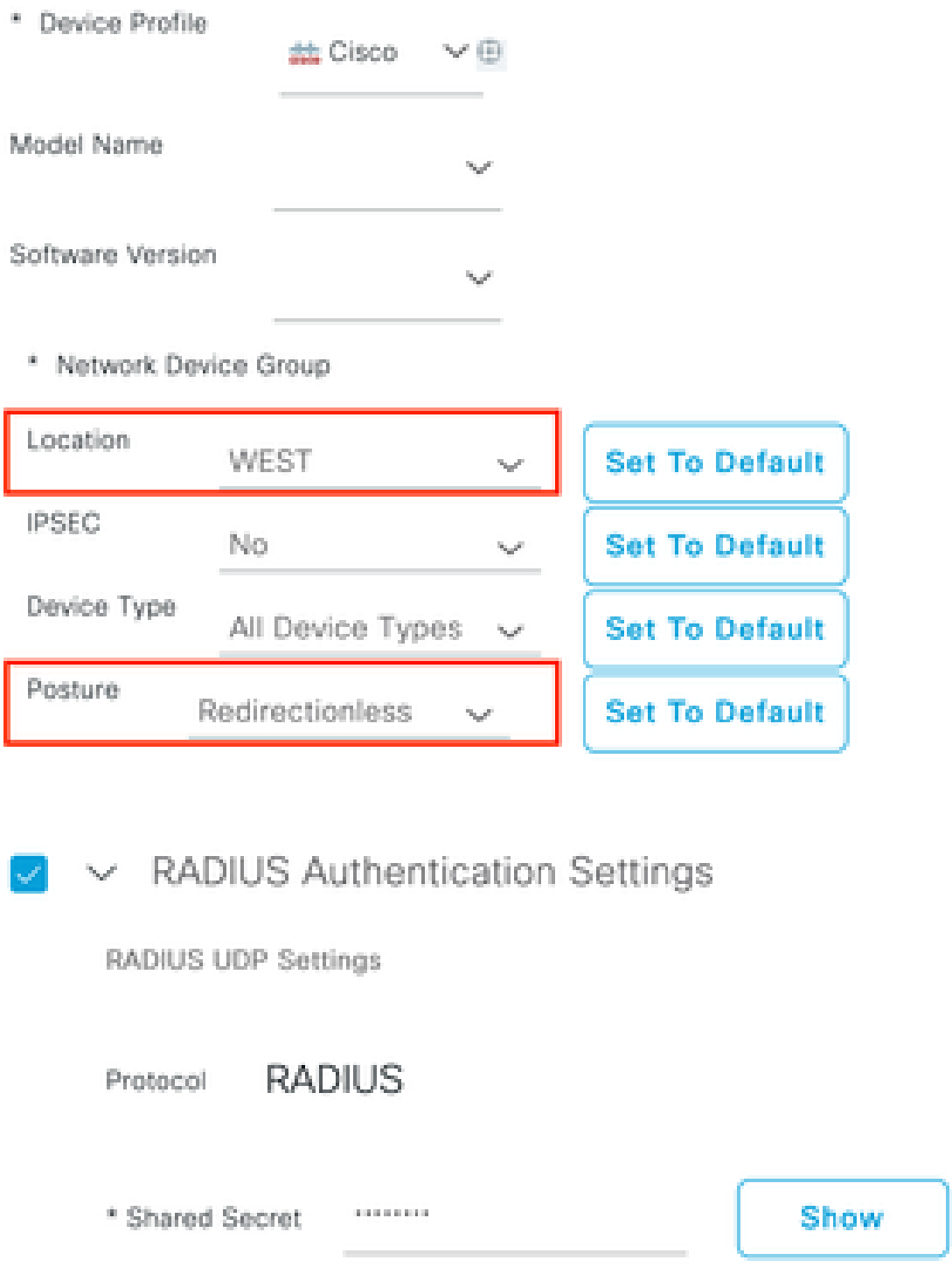
在本指南使用的示例中，位置设备组用于标识RADIUS服务器列表和Call Home列表，自定义终端安全评估设备组用于标识来自无重定向终端安全评估设备的重定向。



网络设备组

网络设备

1. 可以配置网络设备进行RADIUS身份验证、授权和记帐。有关配置步骤，请参阅每个供应商文档。根据对应的Call Home列表配置RADIUS服务器列表。
2. 在ISE上，导航到Administration > Network Resources > Network Devices，然后点击Add。根据设计配置网络设备组，并启用RADIUS身份验证设置以配置共享密钥。



网络设备配置

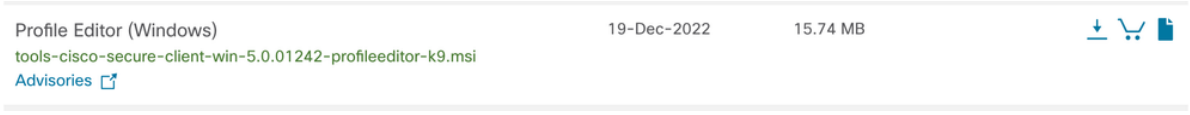
客户端调配

可通过两种方式为客户端调配正确的软件和配置文件，以便在无重定向环境中执行安全评估：

1. 手动调配（预部署）
2. 客户端调配门户（Web部署）

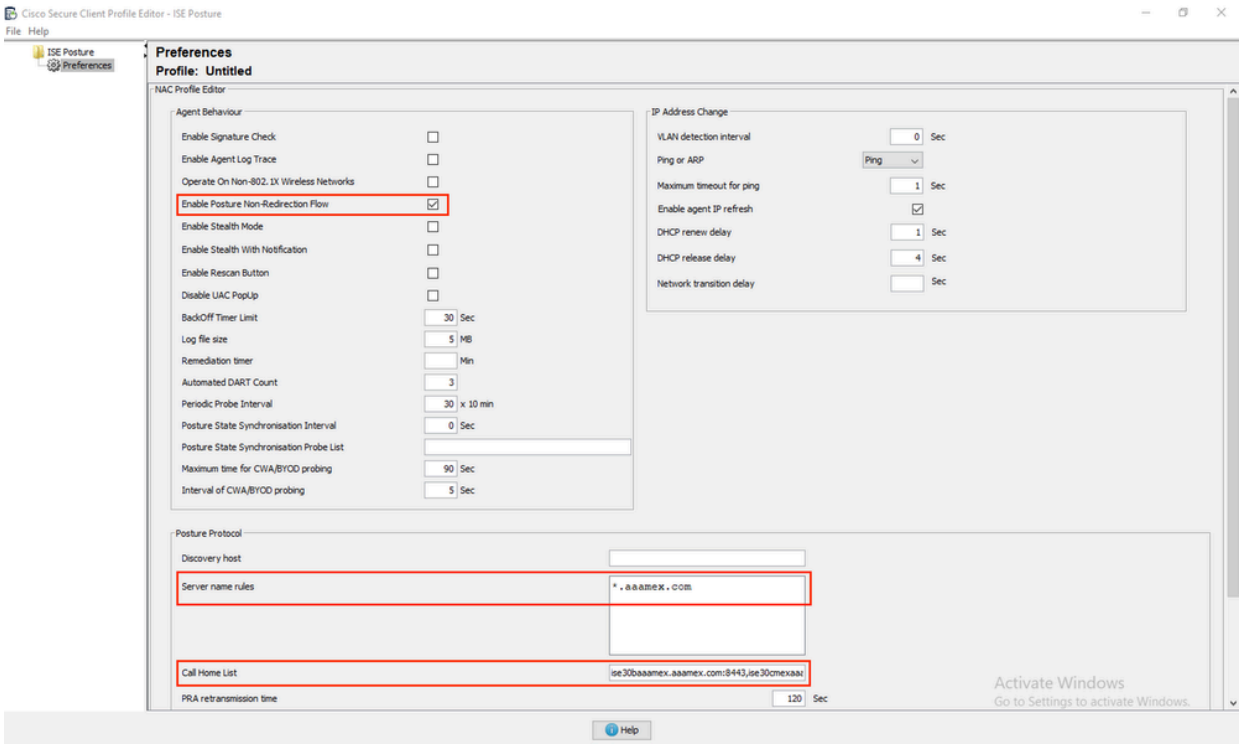
手动调配（预部署）

1. 从Cisco Software Download（思科软件下载）下载并安装Cisco Secure Client Profile Editor。



配置文件编辑器包

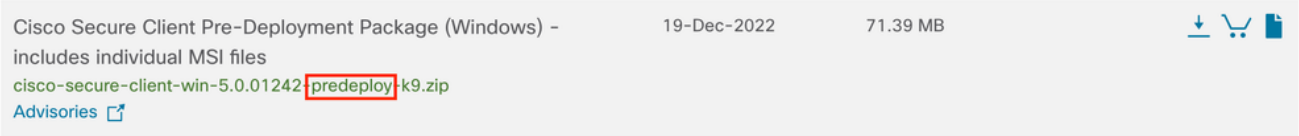
2. 打开ISE终端安全评估配置文件编辑器：
   - 确保已启用启用状态非重定向流。
   - 配置以逗号分隔的服务器名称规则。选择以下配置之一：
     - 一个星号*，用于连接任何PSN。
     - 通配符值(例如，*.aaamex.com)允许连接到特定域中的任何PSN。
     - PSN FQDN列表（以逗号分隔），用于限制与特定PSN的连接。如果使用，此列表必须与Call Home列表匹配。
   - 配置Call Home List以指定PSN的逗号分隔列表。确保使用FQDN:port或IP:port格式添加客户端调配门户端口。



使用配置文件编辑器的状态配置文件配置

> 注意：请参阅“客户端调配策略”一节的第4步，了解在必要时如何验证客户端调配门户端口的说明。

3. 将配置文件另存为ISEPostureCFG.xml。
4. 重复第2步和第3步，为正在使用的每个Call Home列表创建新的posture配置文件。
5. 从Cisco Software Download下载Cisco Secure Client Pre-Deployment Package。

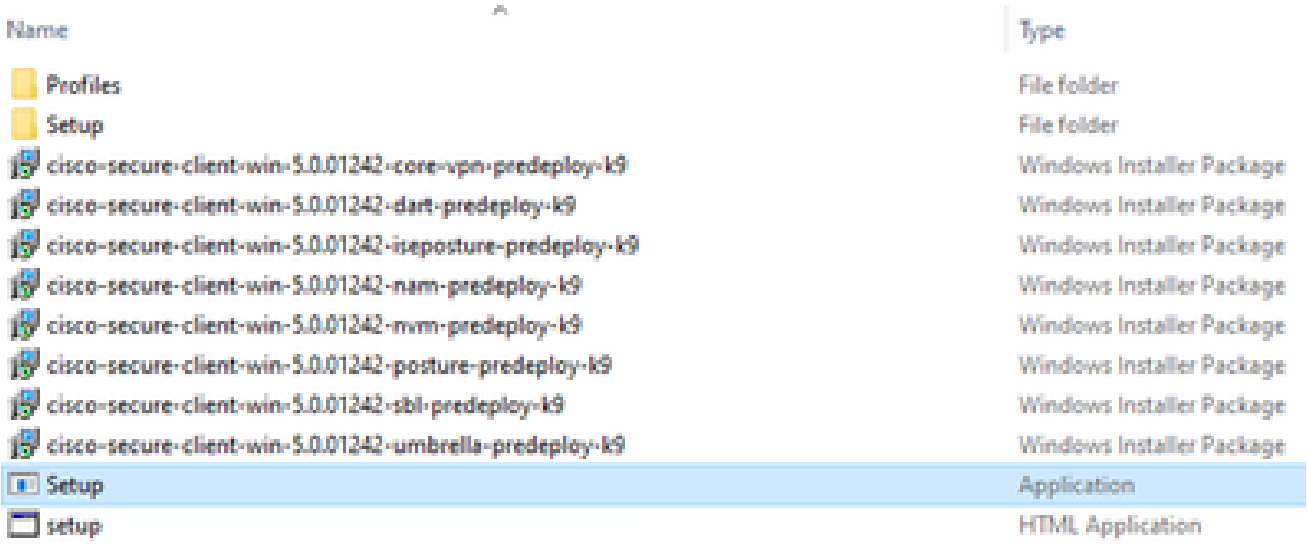


思科安全客户端预部署软件包

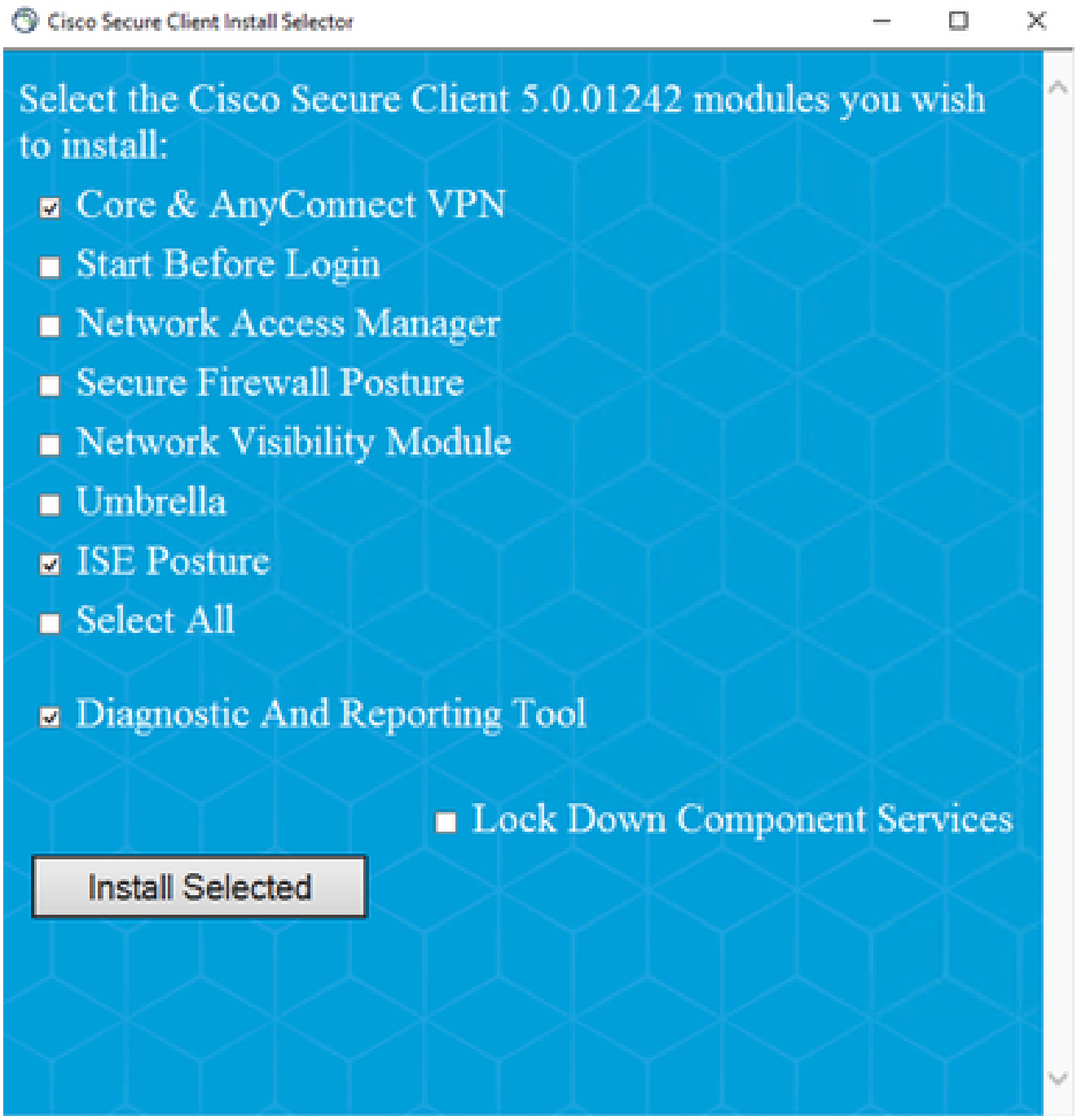
6. 在存档文件中分发配置文件和安装文件，或将文件复制到客户端。

> ⚠ 警告：确保计划连接的头端上也包含相同的Cisco安全客户端文件：安全防火墙ASA、ISE等。即使使用手动调配，也必须配置ISE以使用相应软件版本的客户端调配。有关详细说明，请参阅客户端调配策略配置部分。

7. 在客户端上，打开zip文件并运行Setup以安装核心和ISE终端安全评估模块。或者，单个msi文件可用于安装每个模块，在这种情况下，您必须确保先安装core-vpn模块。



思科安全客户端预部署软件包内容



思科安全客户端安装程序

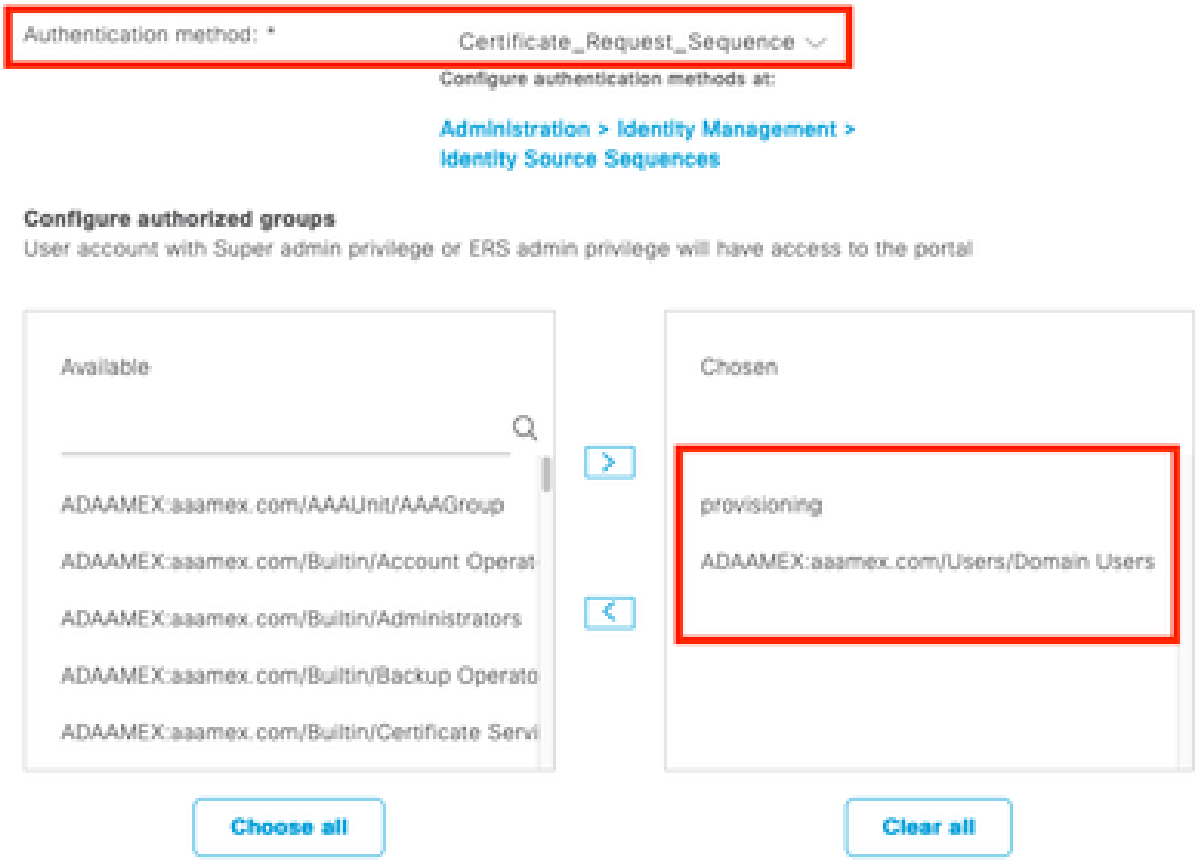
提示：安装用于故障排除的诊断和报告工具。

8. 安装完成后，将posture profile xml复制到以下位置：
   - Windows 窗口版本:%ProgramData%\Cisco\Cisco Secure Client\ISE终端安全评估
   - MacOS:/opt/cisco/secureclient/iseposture/

客户端调配门户（Web部署）

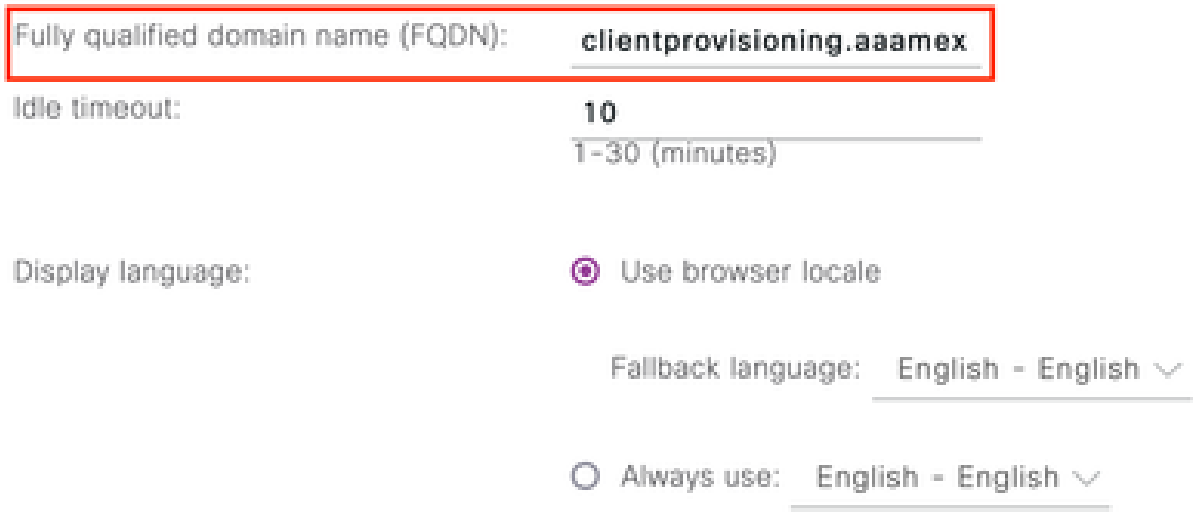
ISE客户端调配门户可用于从ISE安装思科安全客户端ISE终端安全评估模块和终端安全评估配置文件，如果客户端上已安装ISE终端安全评估模块，也可以单独推送终端安全评估配置文件。

1. 导航至工作中心>状态>客户端调配>客户端调配门户，以打开门户配置。展开Portal Settings部分并找到Authentication method字段，选择要用于门户中的身份验证的身份源序列。
2. 配置授权使用客户端调配门户的内部和外部身份组。



门户设置中的身份验证方法和授权组

3. 在完全限定域名(FQDN)字段中，配置客户端用于访问门户的URL。要配置多个FQDN，请输入以逗号分隔的值。



4. 配置DNS服务器以将门户URL解析为对应的Call Home列表的PSN。
5. 为最终用户提供FQDN以访问门户，以便安装ISE终端安全评估软件。

注意：要使用门户FQDN，客户端必须在受信任存储中安装PSN管理员证书链以及门户证书链，并且管理员证书必须在SAN字段中包含门户FQDN。

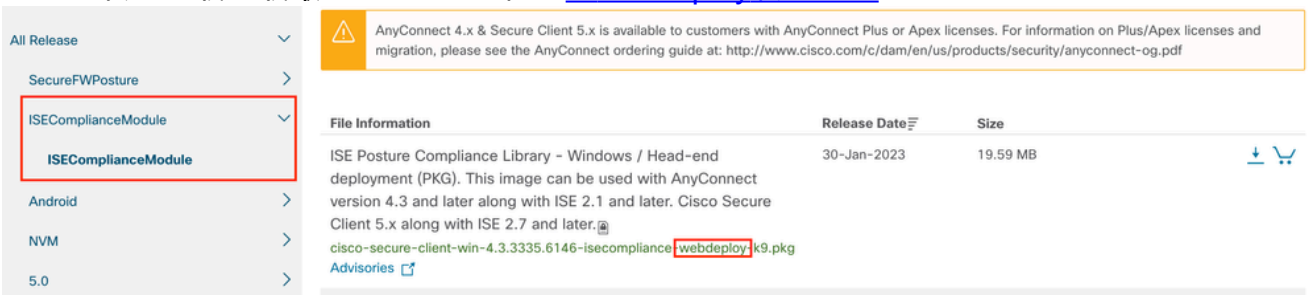
客户端调配策略

无论用于在终端上安装Cisco Secure Client的调配类型（预部署或Web部署），都必须在ISE上配置客户端调配。

1. 从下载Cisco Secure Client Headend Deployment Package 思科软件下载。

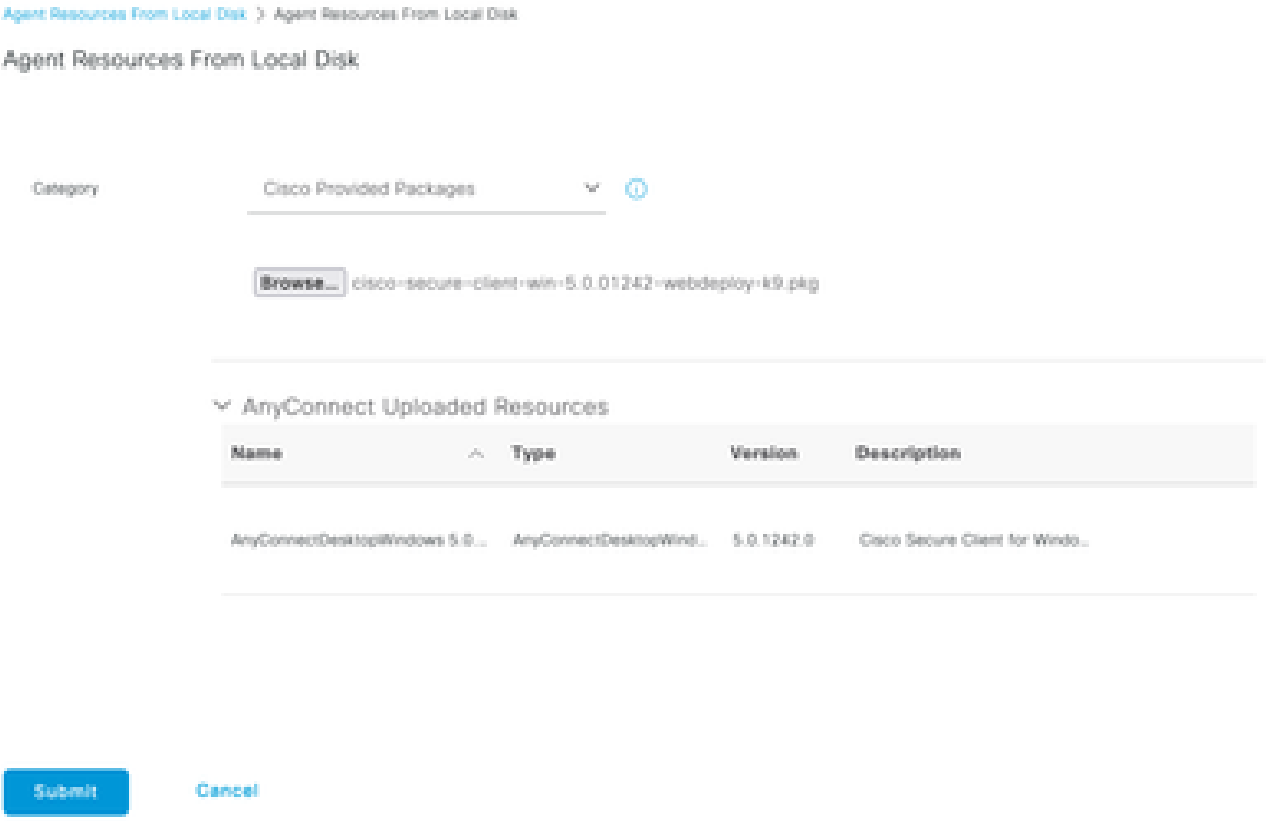
思科安全客户端Web部署包

2. 从思科软件下载下载最新的ISE合规性模块webdeploy软件包。

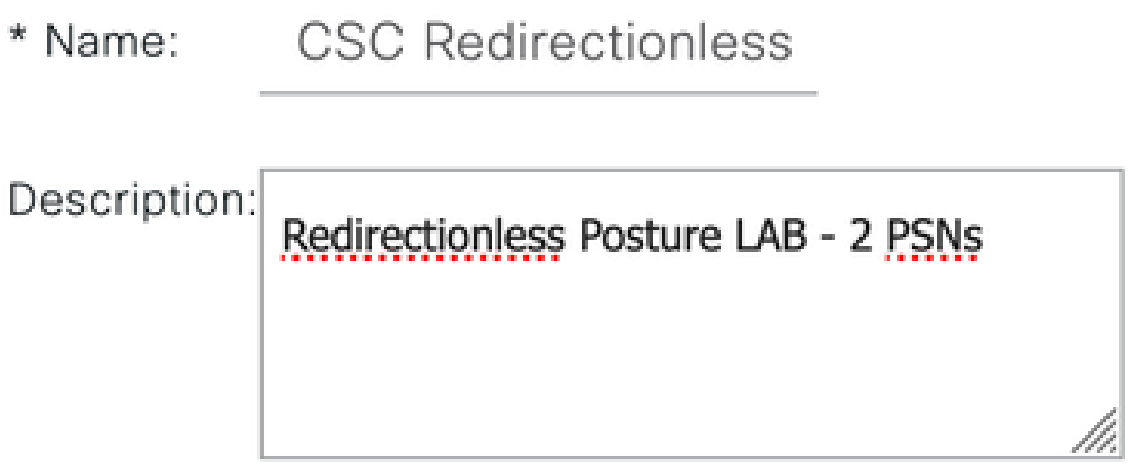


ISE合规性模块Webdeploy包

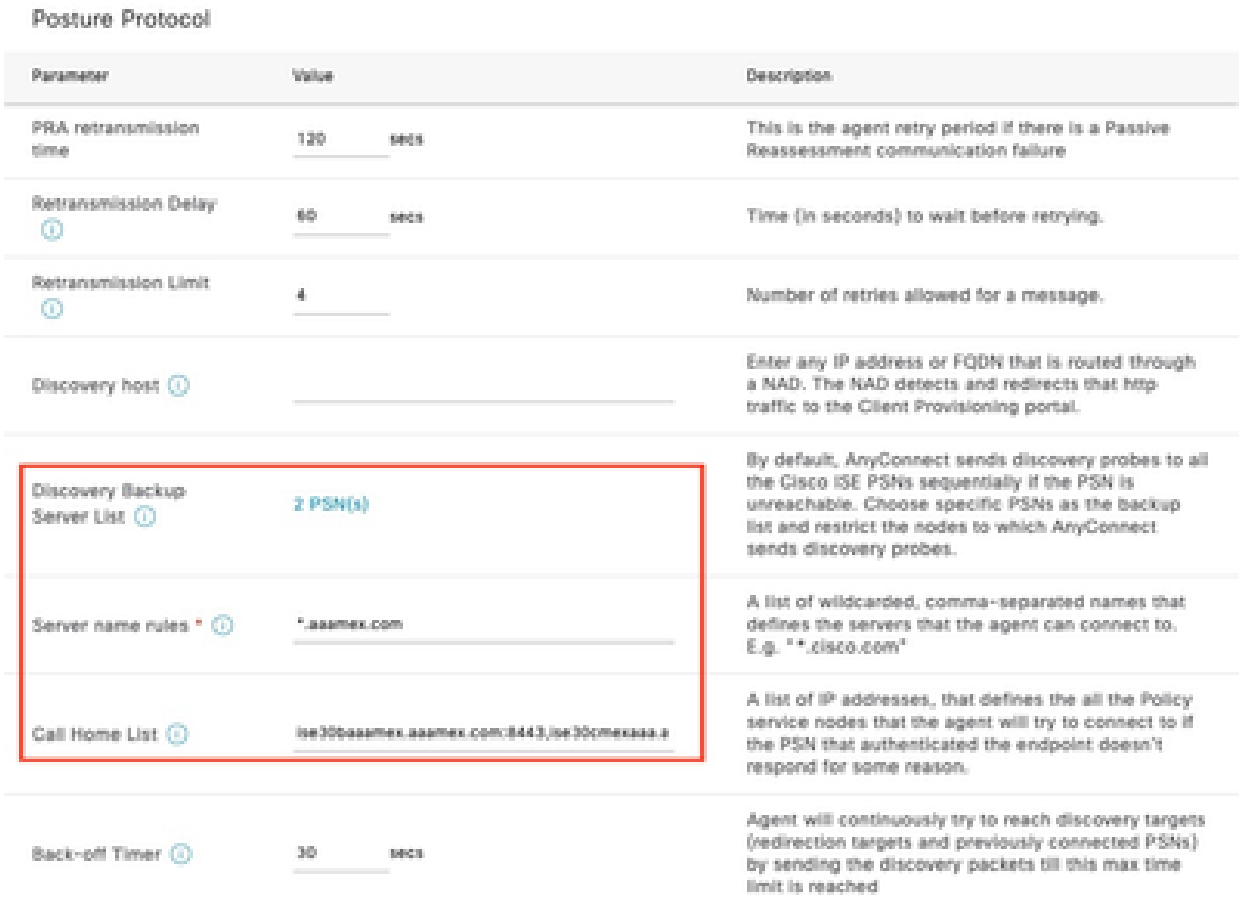
3. 在ISE上，导航到工作中心> Posture > Client Provisioning > Resources，然后单击Add > Agent resources from local disk。从Category下拉菜单中选择Cisco Provided Packages，并上传之前下载的Cisco Secure Client Headend Deployment Package。重复相同的过程以上传合规性模块。



4. 返回Resources选项卡，单击Add > Agent Posture Profile。在配置文件上：
   - 配置名称，该名称可用于在ISE中标识配置文件和Call Home列表。
   - 确保将Enable extra probes so non-redirection flow can work设置为Yes。
   - 配置Discovery Backup Server List。选择与正在配置的Call Home列表匹配的PSN。这是首次连接后保存在ConnectionData.xml中的PSN列表。
   - 配置以逗号分隔的服务器名称规则。 选择以下配置之一：
     - 一个星号*，用于连接任何PSN。
     - 通配符值(例如，*.aaamex.com)允许连接到特定域中的任何PSN。
     - 以逗号分隔的PSN FQDN列表，用于限制与特定PSN的连接。如果使用，此列表必须与Call Home列表匹配。
   - 配置Call Home List以指定PSN的逗号分隔列表。确保使用FQDN:port或IP:port格式添加客户端调配门户端口。
     要查找或修改CPP端口，请导航至Work Centers > Posture > Client Provisioning > Client Provisioning Portal，选择Portal，展开Portal设置，然后查找HTTPs端口。



代理状态配置文件配置



座席状态配置文件中的状态协议配置

5. 返回Resources选项卡，单击Add > Agent Configuration。选择要使用的Cisco Secure Client软件包和Compliance Module。

> ⚠ 警告：如果Cisco Secure Client已预先部署到客户端，请确保ISE上的版本与终端上的版本匹配。如果使用ASA或FTD进行Web部署，则此设备上的版本也可以匹配。

6. 向下滚动到状况选择部分并选择在第1步中创建的配置文件。点击页面底部的提交以保存配置。

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1.2.042

* Configuration Name:

SecureClient Configuration Redirectionless

Description:

Redirectionless Lab Call Home List 1

Description Value Notes

* Compliance Module: CiscoSecureClientComplianceModuleWindows

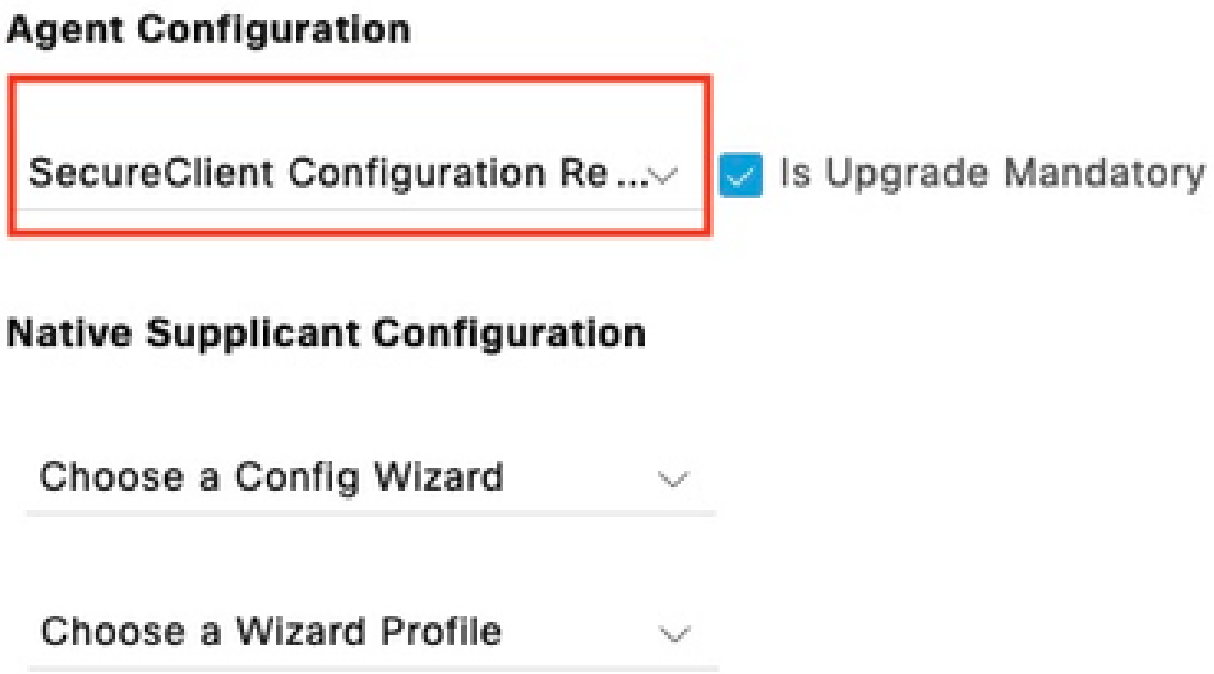
Cisco Secure Client Module Selection

ISE Posture	☑
VPN	☑
Zero Trust Access	☐
Network Access Manager	☐
Secure Firewall Posture	☐
Network Visibility	☐
Umbrella	☐
Start Before Logon	☐
Diagnostic	

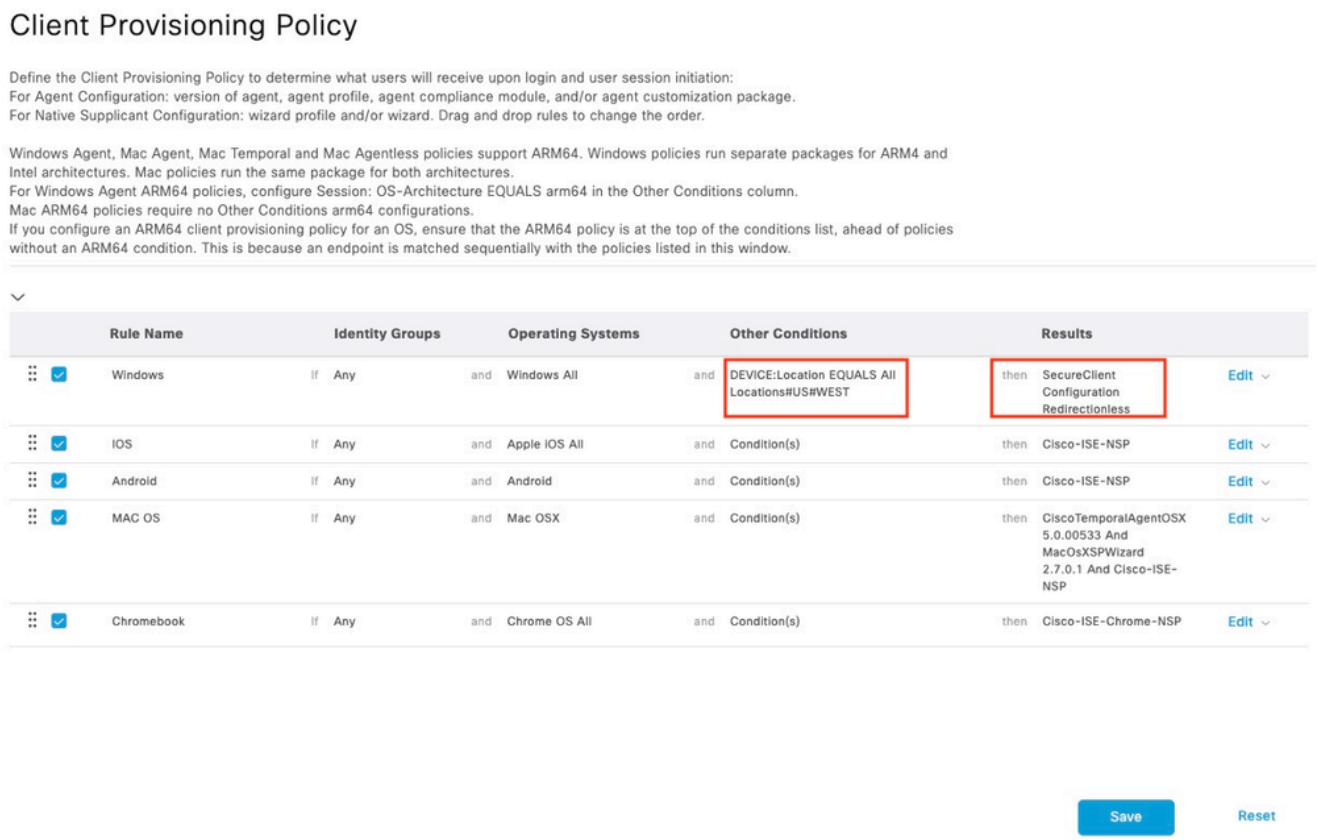
7. 导航至工作中心>状态>客户端调配>客户端调配策略。找到用于所需操作系统的策略，然后单击Edit。单击Results列上的+，然后选择Agent Configuration部分下的步骤5中的agent配置。点击页面底部的Save。

注意：如果有多个Call Home列表，请使用Other Conditions字段将正确的配置文件推送到相应的客户端。在本示例中，设备位置组用于标识在策略中推送的安全评估配置文件。

提示：如果为同一操作系统配置了多个客户端调配策略，则建议使它们相互排斥，也就是说，给定客户端一次只能命中一个策略。RADIUS属性可以在Other Conditions列下使用，以区分不同的策略。



客户端调配策略中的代理配置



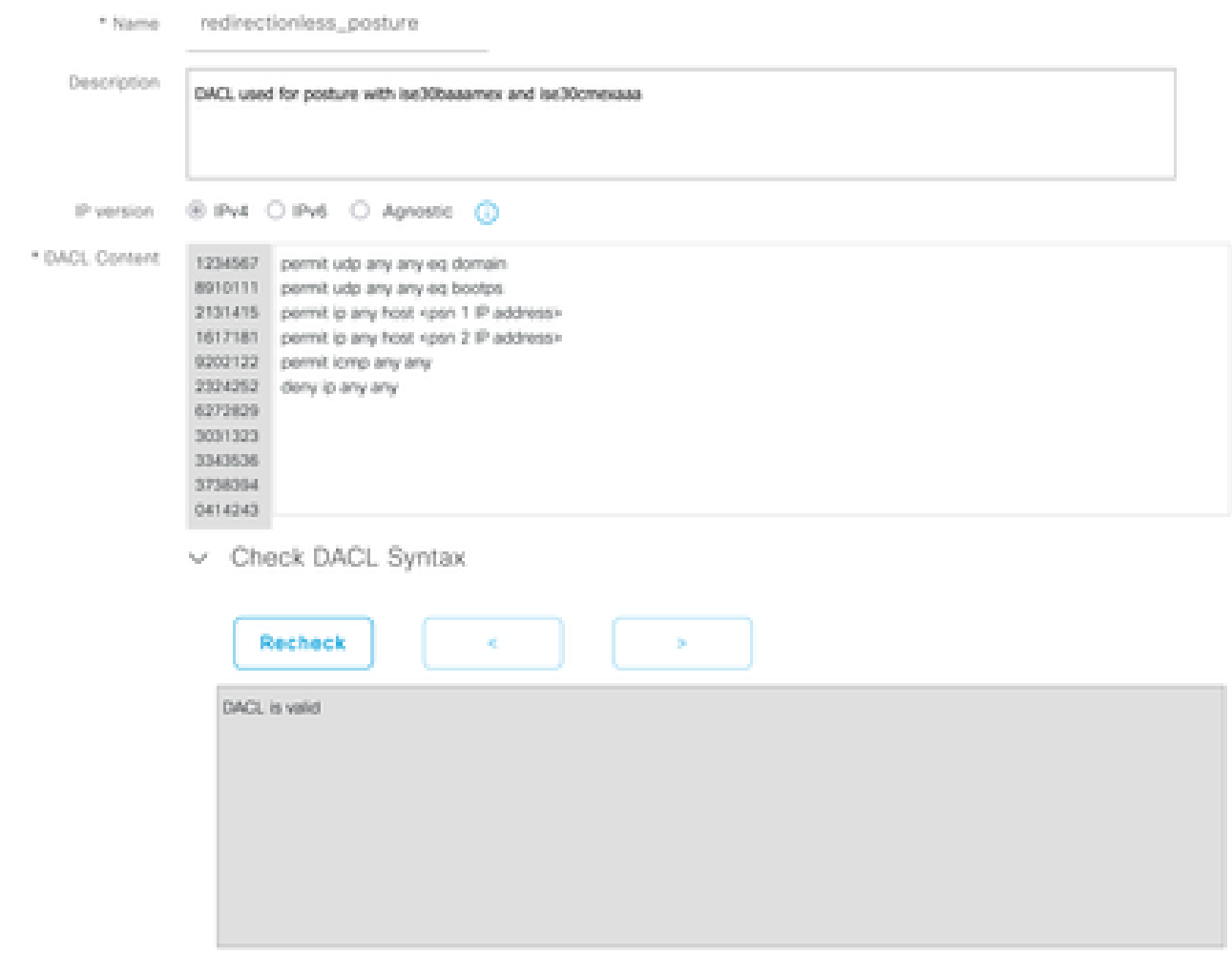
客户端调配策略

8. 对每个使用中的Call Home列表和相应的状态配置文件重复步骤4至7。对于混合环境，相同的配置文件可用于重定向客户端。

授权

授权配置文件

1. 导航到Policy > Policy Elements > Results > Authorization > Downloadable ACLs，然后单击Add。
2. 创建DACL以允许流量发送到DNS、DHCP（如果使用）、ISE PSN并阻止其他流量。在最终合规访问之前，请确保允许访问所需的任何其他流量。



DACL配置

permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

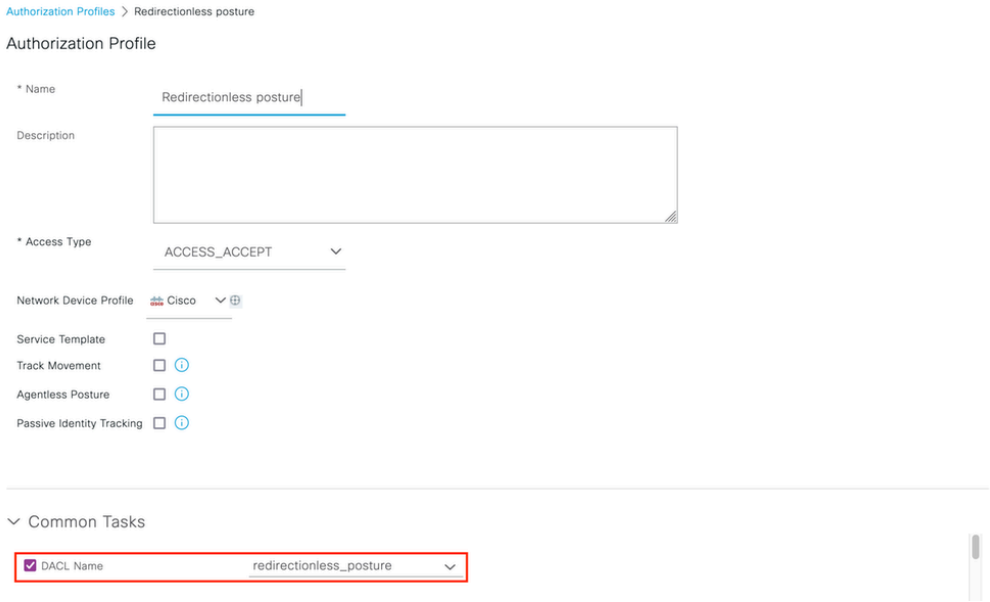
permit ip any host

deny ip any any

⚠ 警告：某些第三方设备不支持DACL，在这种情况下，需要使用过滤器ID或其他供应商特定属性。有关详细信息，请参阅供应商文档。如果未使用DACL，请确保在网络设备

⚠ 上配置相应的ACL。

3. 导航到Policy > Policy Elements > Results > Authorization > Authorization profiles，然后单击Add。为授权配置文件指定名称，然后从常见任务中选择DACL名称。从下拉菜单中，选择第2步中创建的DACL。



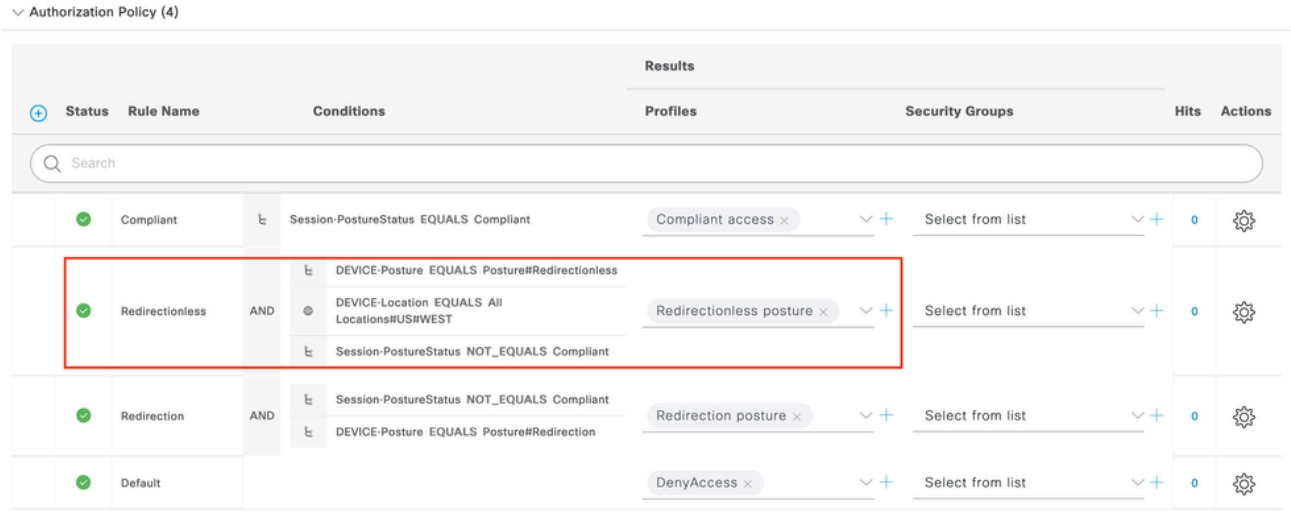
授权配置文件

✎ 注意：如果未使用DACL，请使用常见任务或高级属性设置中的Filter-ID推送相应的ACL名称。

4. 对正在使用的每个Call Home列表重复步骤1到步骤3。对于混合环境，只需一个用于重定向的授权配置文件。重定向授权配置文件的配置不在本文档的讨论范围之内。

授权策略

1. 导航到Policy > Policy Sets，然后打开正在使用的策略集或创建新策略集。
2. 向下滚动到Authorization Policy部分。使用Session PostureStatus NOT_EQUALS Compliant创建授权策略，然后选择在上一部分中创建的授权配置文件。



授权策略

3. 对每个授权配置文件重复第2步，并使用其对应的Call Home列表。对于混合环境，只需一个重定向授权策略。

故障排除

思科安全客户端上合规且安全评估在ISE上不适用（挂起）

陈旧/幻像会话

部署中存在过时的或幻像会话可能会生成间歇性且明显随机的无重定向状态发现故障，导致用户在ISE上停滞状态未知/不适用的访问，而思科安全客户端UI显示合规访问。

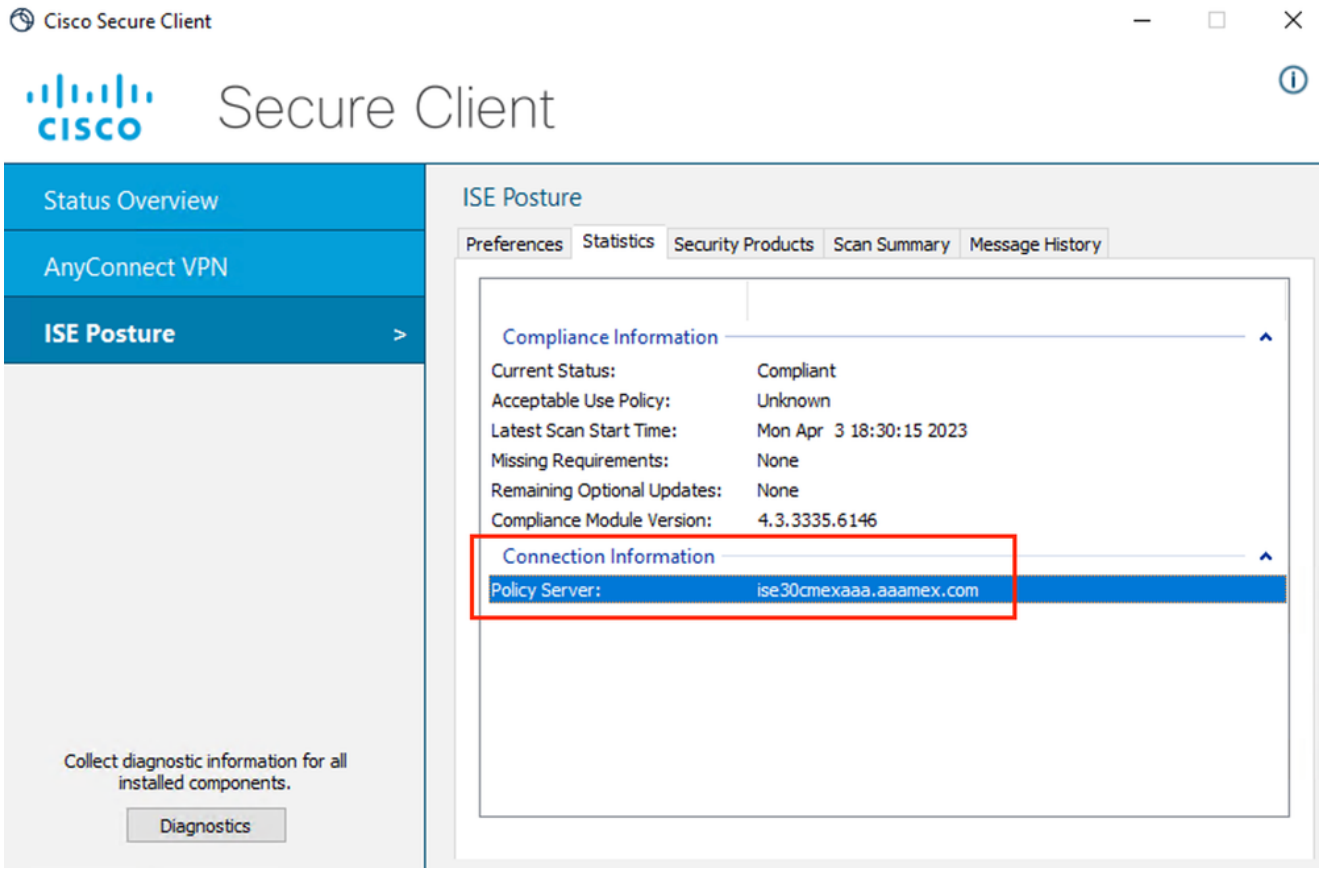
过时的会话是不再活动的旧会话。它们由身份验证请求和记帐启动创建，但PSN上未收到清除会话的记帐停止。

幻像会话是从未在特定PSN中实际处于活动状态的会话。它们通过记帐临时更新创建，但PSN上未收到清除会话的记帐停止。

识别

要识别陈旧/幻像会话问题，请验证客户端上系统扫描中使用的PSN，并与执行身份验证的PSN进行比较：

1. 在Cisco Secure Client UI中，点击左下角的gear图标。从左菜单中，打开ISE Posture部分，导航到Statistics选项卡。注意Policy Server in Connection Information。



思科安全客户端中的ISE终端安全评估策略服务器

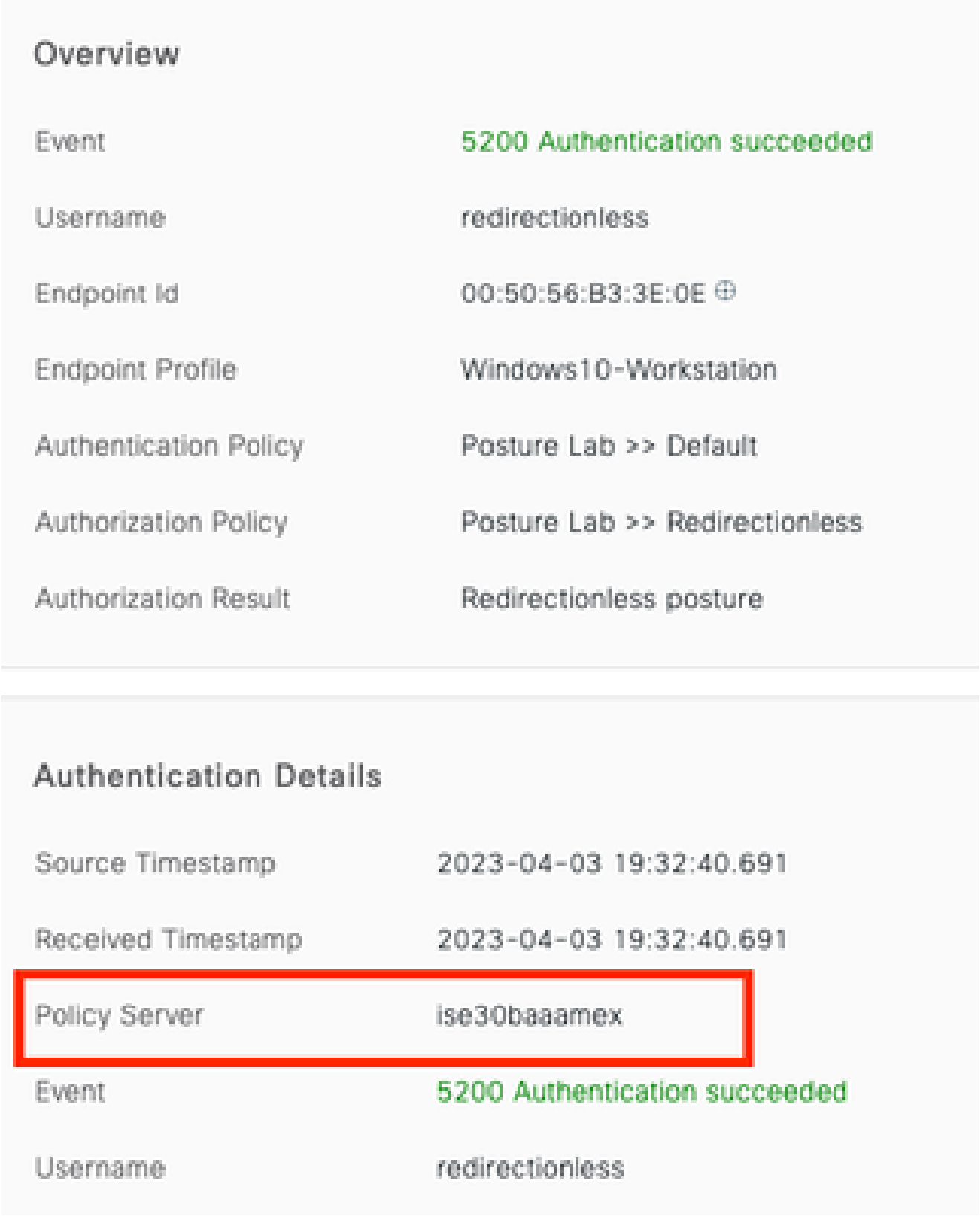
2. 在ISE RADIUS实时日志中，请注意以下几点：
   - 状态更改
   - 服务器更改
   - 授权策略和授权配置文件无更改
   - 无CoA实时日志



Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa	Compliant	Redirectionless posture
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baaamex		
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex	NotApplicable	Redirectionless posture

过期/幻像会话的实时日志

3. 打开实时会话或上次身份验证实时日志详细信息。请注意，如果策略服务器与步骤1中观察到的服务器不同，则表明存在过期/幻像会话的问题。

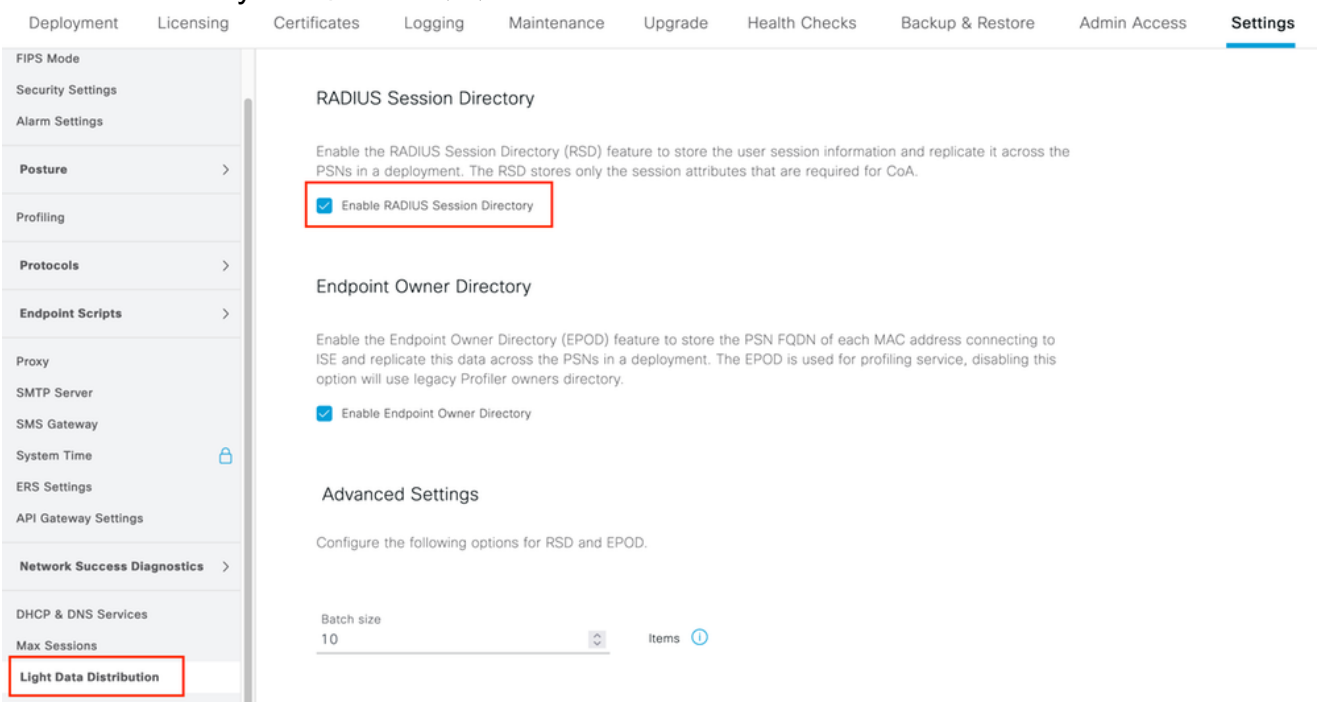


实时日志详细信息中的策略服务器

解决方案

在ISE 2.6补丁6和2.7补丁3之后的ISE版本将RADIUS会话目录作为无重定向安全评估流程中陈旧/幻像会话方案的解决方案。

1. 导航到Administration > System > Settings > Light Data Distribution，并验证Enable RADIUS Session Directory复选框是否已启用。



启用RADIUS会话目录

2. 在ISE CLI中，通过运行show applications status ise命令，验证ISE消息服务是否正在所有PSN上运行。

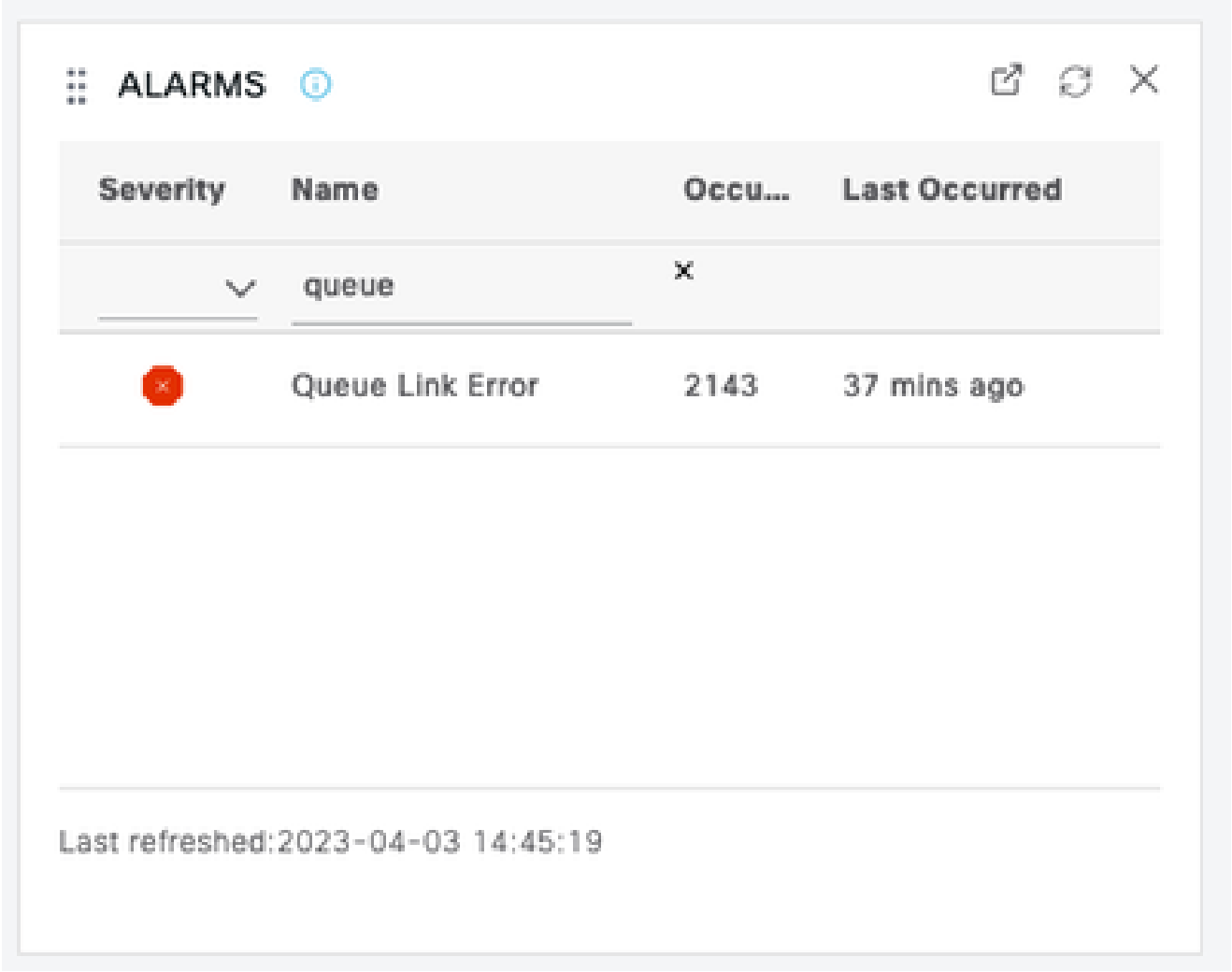
```
ise30cmexaaa/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          12434
Database Server                        running          112 PROCESSES
Application Server                     running          33093
Profiler Database                      running          19622
ISE Indexing Engine                    running          42923
AD Connector                           running          60317
M&T Session Database                   running          19361
M&T Log Processor                      running          33283
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          14791
TC-NAC MongoDB Container               running          18594
TC-NAC Core Engine Container           running          18981
VA Database                            running          53465
VA Service                             running          53906
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  running          55480
PassiveID Syslog Service               running          56312
PassiveID API Service                  running          57153
PassiveID Agent Service                running          58079
PassiveID Endpoint Service             running          59138
PassiveID SPAN Service                 running          60059
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          16526
ISE API Gateway Database Service       running          18463
ISE API Gateway Service                running          23052
```

ISE消息服务正在运行

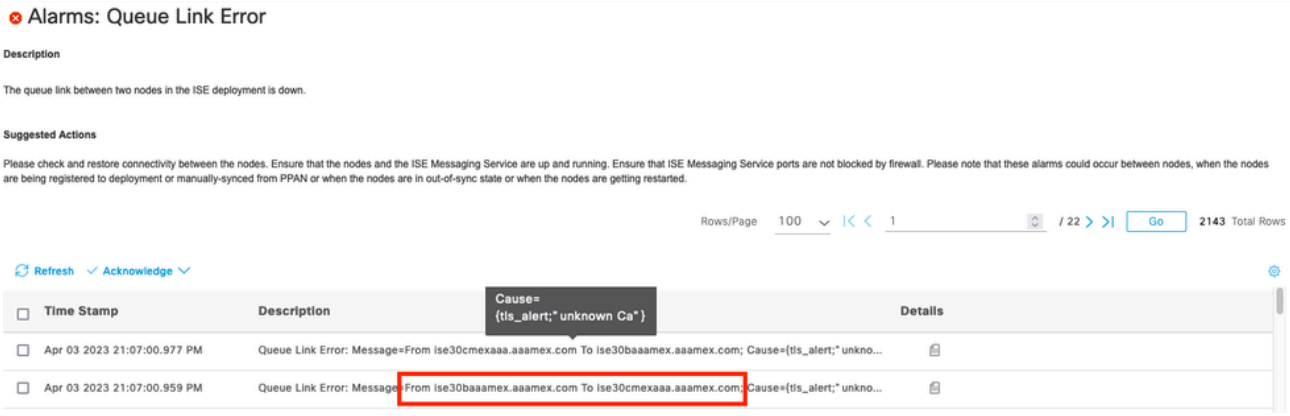
注意：此服务是指用于PSN之间的RSD的通信方法，无论可从ISE UI设置的系统日志的ISE消息服务设置的状态如何，都可以运行。

3. 导航到ISE控制面板并找到警报 dashlet。验证是否有任何Queue Link Error警报。单击alarm的名称可查看更多详细信息。



队列链路错误警报

4. 验证是否在用于状态的PSN之间生成警报。



队列链路错误警报详细信息

5. 将鼠标悬停在警报描述上可查看完整的详细信息，并注意Cause（原因）字段。队列链路错误最常见的两种原因如下：
   - 超时:表示节点向端口8671上的其他节点发送的请求在阈值内未响应。要修复，请验证节点之间是否允许TCP端口8671。
   - 未知CA:指示ISE消息证书签名的证书链无效或不完整。要修正此错误，请执行以下操作：

a. 导航至管理> System > Certificates > Certificate signing requests。
b. 单击Generate Certificate Signing Requests(CSR)。
c. 从下拉菜单中选择ISE Root CA，然后单击Replace ISE Root CA Certificate chain。
如果ISE根CA不可用，请导航到证书颁发机构> 内部CA设置，然后单击启用证书颁发机构，然后返回到CSR并重新生成根CA。
d. 生成新的CSR并从下拉菜单中选择ISE消息服务。
e. 从部署中选择所有节点并重新生成证书。

注意：在重新生成证书时，应该观察队列链路错误警报，原因为Unknown CA或Econnrefused。在证书生成后监控警报以确认问题已解决。

性能

识别

性能问题（例如与无重定向状态相关的高CPU使用率和高负载平均数）可能会影响PSN和MnT节点，并且通常伴随或先于以下事件：

- 在Cisco安全客户端中，随机或间歇性策略服务器未检测到错误。
- 门户服务线程池已达到阈值事件的最大资源限制报告达到阈值事件。导航到操作>报告>报告>审计>操作审计以查看报告。
- MNT查找的状态查询是高警报。这些警报仅在ISE 3.1及更高版本上生成。

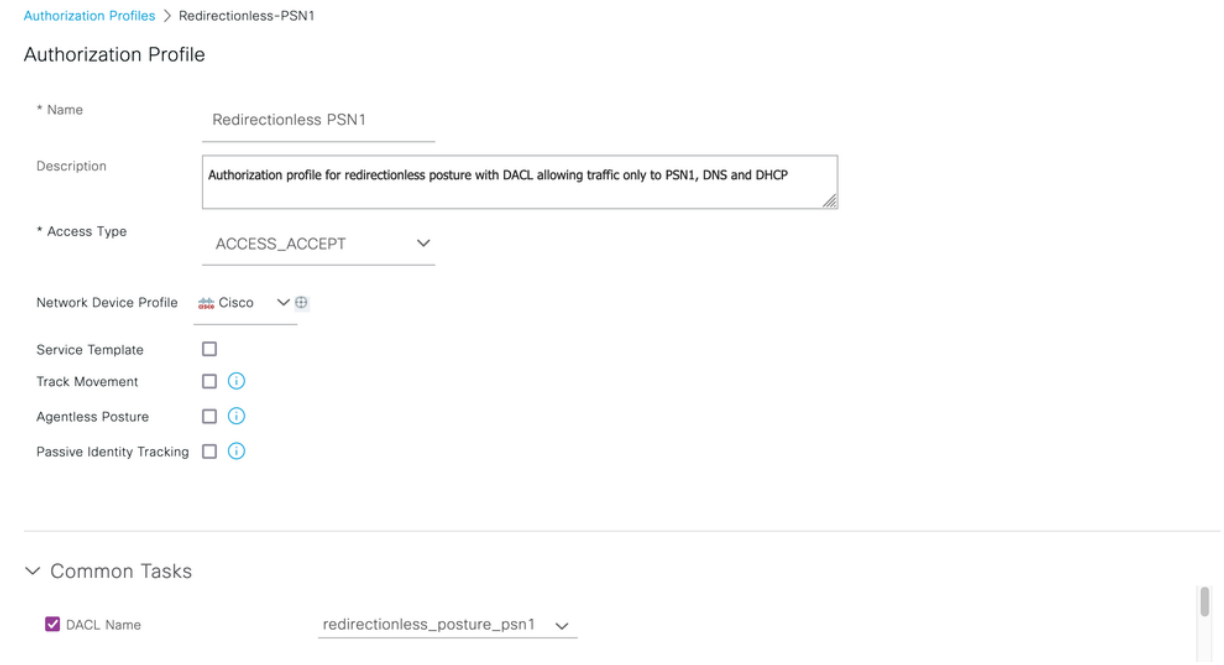
解决方案

如果部署性能受到无重定向状态的影响，这通常表示实施效果不佳。建议修改以下方面：

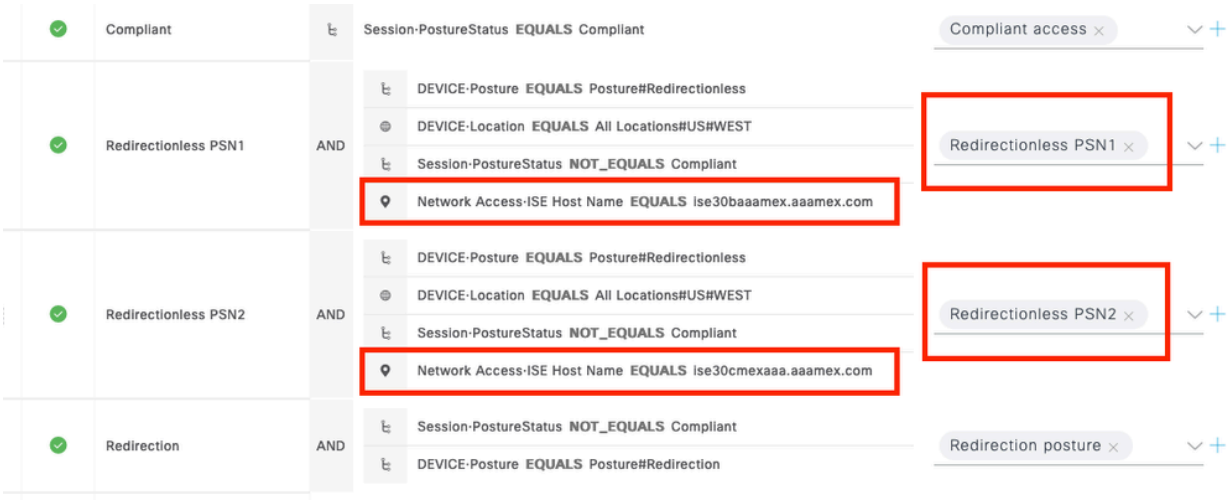
- 每个呼叫总部列表使用的PSN数量。根据设计，考虑减少每个终端或网络设备可用于终端安全评估的PSN数量。
- Call Home列表中的客户端调配门户端口。确保门户端口号包含在每个节点的IP或FQDN之后。

要减轻影响，请执行以下操作：

1. 通过从思科安全客户端文件夹删除文件并从终端清除connectiondata.xml，然后重新启动ISE终端安全评估服务或思科安全客户端。如果服务未重新启动，旧文件将重新生成，更改不会生效。修改和修改Call Home列表后，也可以执行此操作。
2. 使用DACL或其他ACL阻止流量发送到ISE PSN用于不相关的网络连接：
    - 对于授权策略中未实施终端安全评估，但适用于已安装思科安全客户端ISE终端安全评估模块的终端的连接，阻止从客户端到所有ISE PSN的流量用于TCP端口8905和客户端调配门户端口。建议将此操作用于实施重定向的终端安全评估。
    - 对于在授权策略中实施安全状态的连接，允许从客户端到身份验证PSN的流量并阻止到部署中其他PSN的流量。修改设计时可以临时执行此操作。



具有单个PSN的DACL的授权配置文件



每个PSN的授权策略

记账

RADIUS记帐对于ISE上的会话管理至关重要。由于终端安全评估依赖于要执行的活动会话，因此不正确或缺少记账配置也会影响终端安全评估发现和ISE性能。必须验证在网络设备上是否正确配置了记帐，以便为每个会话向单个PSN发送身份验证请求、记账开始、记账停止和记账更新。

要验证ISE上接收的记帐数据包，请导航到操作> Reports > Reports > Endpoints and Users > RADIUS Accounting。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。