

# 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

为了更好地理解下文介绍的概念，建议进行以下介绍：

[比较早期的ISE版本与ISE 2.2中的ISE终端安全评估流程](#)  
[ISE会话管理和状态](#)

## 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3.1
- 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含以下步骤：

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。

无重定向流量的完整说明在[Compare Earlier ISE Versions to ISE Posture Flow in ISE 2.2](#)中介绍。

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

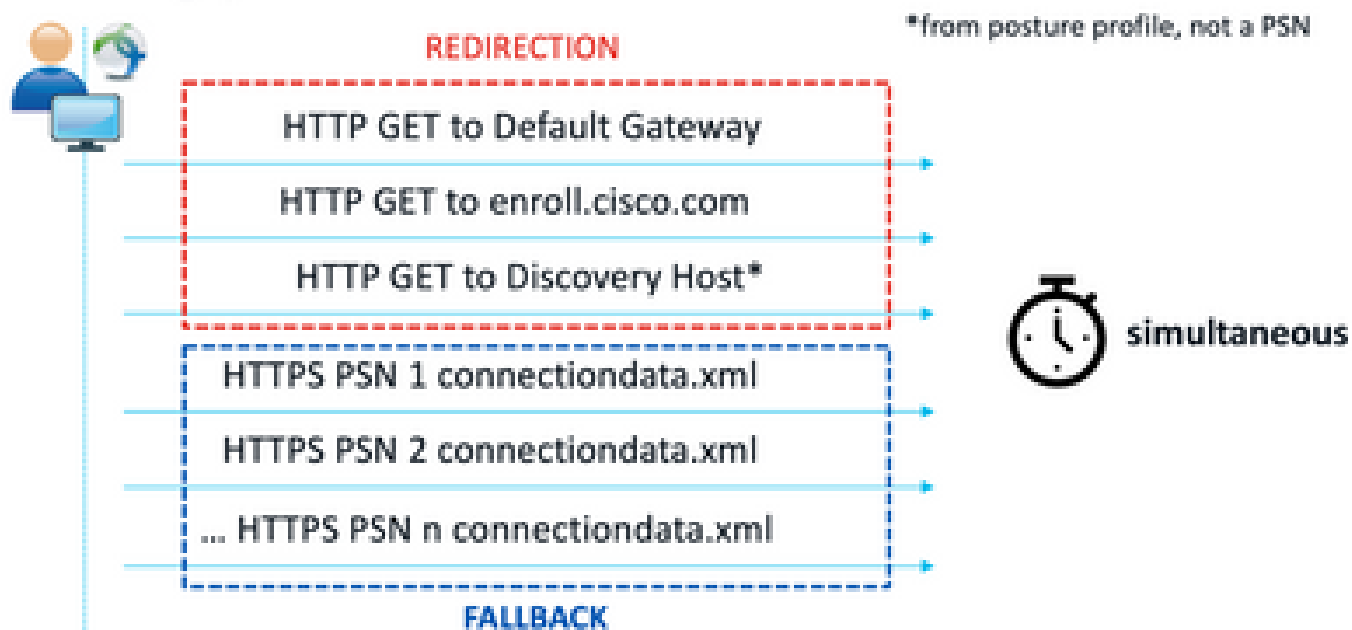
## Connectiondata.xml

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。

## Stage 1 discovery probes

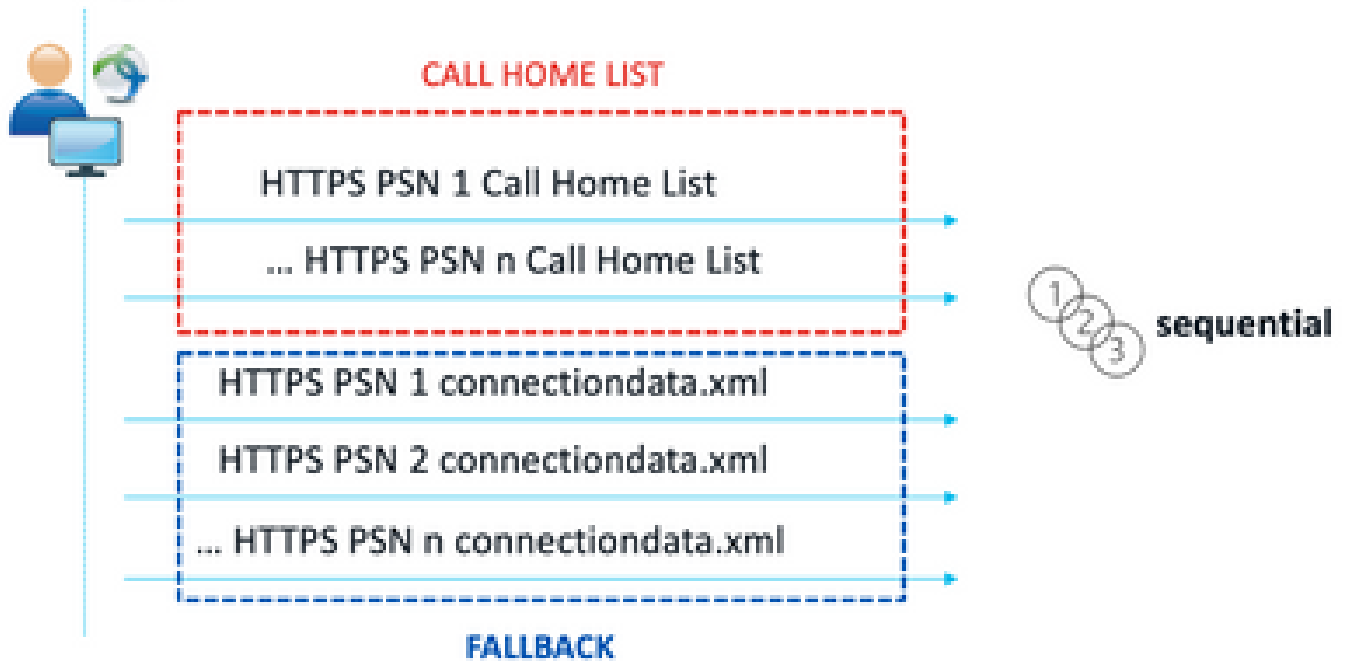
### No-MnT stage probes



第1阶段发现探测

# Stage 2 discovery probes

## MnT stage probes



### 第2阶段发现探测

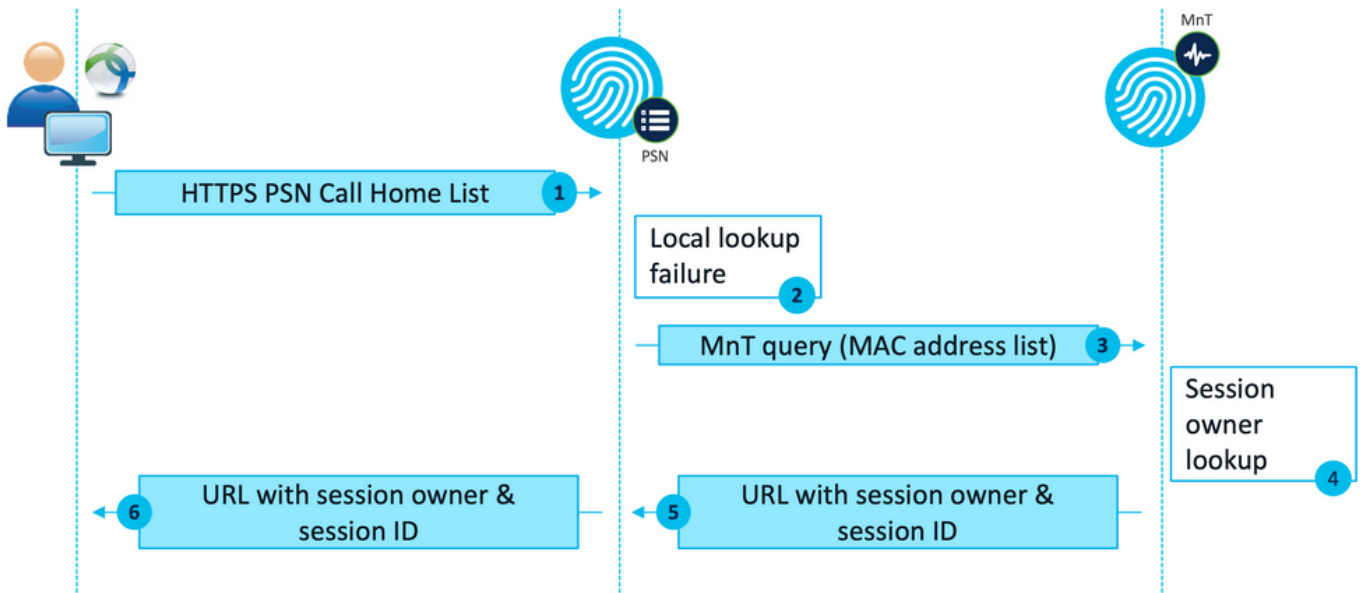
使用connectiondata.xml探测功能导致的常见问题是由于终端发送大量HTTPS请求而导致的ISE部署过载。需要考虑的是，虽然connectiondata.xml可有效作为备份机制来避免重定向和无重定向状态机制的完全中断，但它不是状态环境的可持续解决方案，因此，必须诊断和解决导致主要发现探测功能失败并导致发现问题的设计和配置问题。

### 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不同的是，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列表应与网络设备或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 lookup



MnT查找流程

## 设计

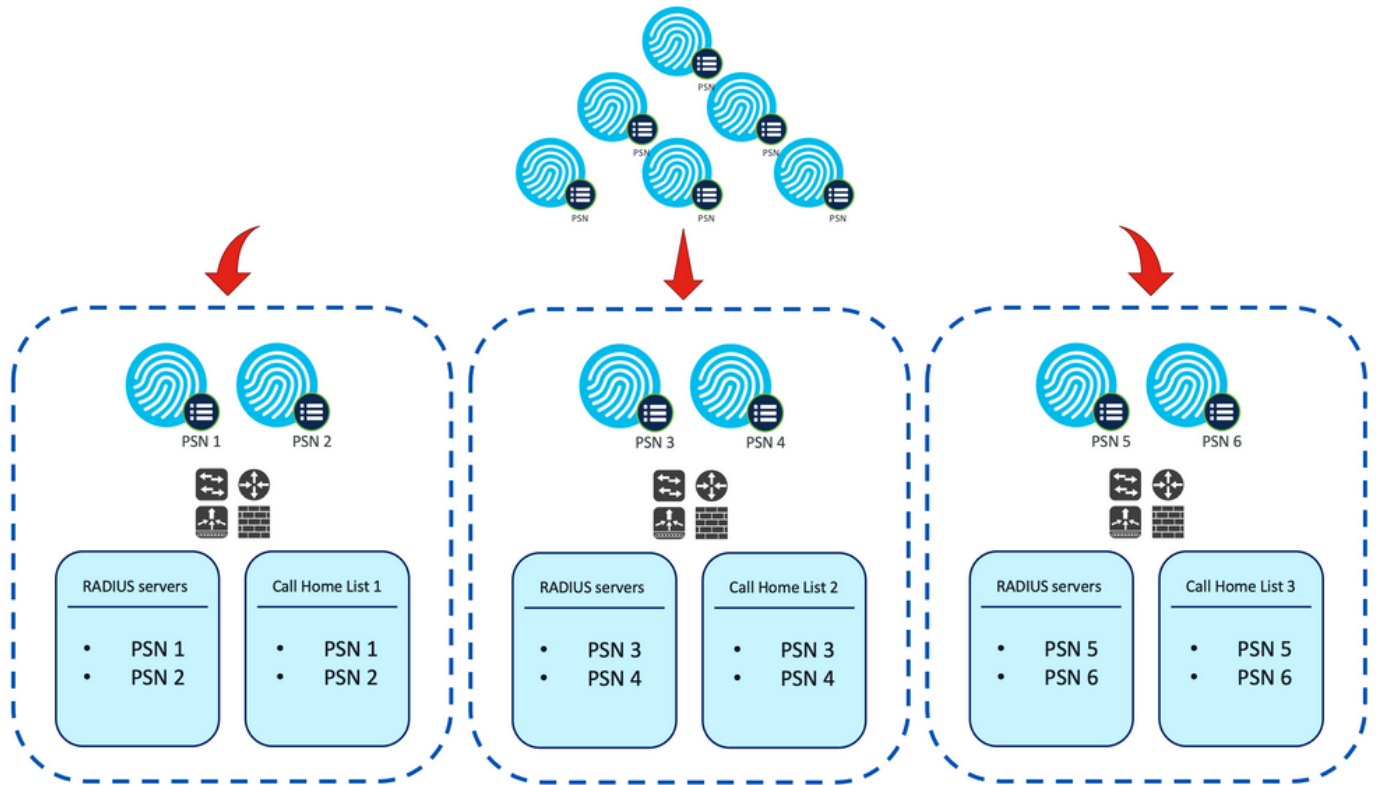
与重定向流程相比，无重定向发现流程通常需要更复杂的流程以及对PSN和MnT的更大处理量，因此在实施过程中可能会出现两个常见挑战：

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列表应以相同的方式加以限制，以匹配相应的呼叫总部列表。

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，提供名称并选择父组（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。

| <input type="checkbox"/> Name               | Description                                  | No. of Network Devices |
|---|--|------------------------|
| <input type="checkbox"/> > All Device Types | All Device Types                             | --                     |
| <input type="checkbox"/> ∨ All Locations    | All Locations                                | --                     |
| <input type="checkbox"/> ∨ US               |  | 0                      |
| <input type="checkbox"/> CENTRAL            |  | 0                      |
| <input type="checkbox"/> EST                |  | 1                      |
| <input type="checkbox"/> WEST               |  | 1                      |
| <input type="checkbox"/> > Is IPSEC Device  | Is this a RADIUS over IPSEC Device           | --                     |
| <input type="checkbox"/> ∨ Posture          | Posture redirection or redirectionless group | --                     |
| <input type="checkbox"/> Redirection        |  | 0                      |
| <input type="checkbox"/> Redirectionless    |  | 1                      |

网络设备组

## 网络设备

1. 网络设备应配置为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，然后单击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。

▪ Device Profile  Cisco  

Model Name

Software Version

▪ Network Device Group

|             |   |   |
|-------------|---|---|
| Location    | WEST <input type="checkbox"/>             | <input type="button" value="Set To Default"/> |
| IPSEC       | No <input type="checkbox"/>               | <input type="button" value="Set To Default"/> |
| Device Type | All Device Types <input type="checkbox"/> | <input type="button" value="Set To Default"/> |
| Posture     | Redirectionless <input type="checkbox"/>  | <input type="button" value="Set To Default"/> |

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

▪ Shared Secret

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）



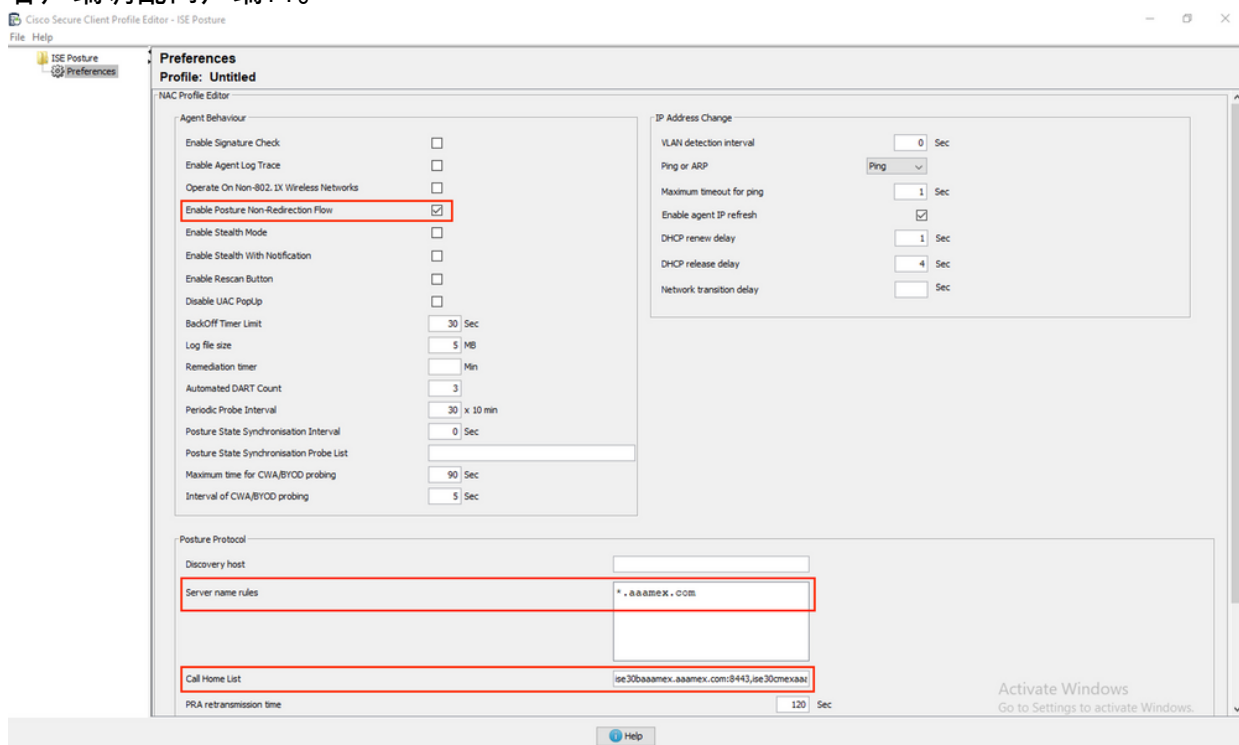
## 手动调配 ( 预部署 )

1. 从[Cisco Software Download](#)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。使用单个星号\*可允许连接到任何PSN，使用通配符值可允许连接到特定域中的任何PSN，或使用PSN FQDN限制连接到特定PSN。
- 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配置安全评估配置文件

注意：有关如何验证客户端调配门户端口 ( 如有必要 ) 的说明，请参阅客户端调配策略部分的第4步。

3. 对正在使用的每个Call Home列表重复步骤2。
4. 从[Cisco Software Download](#) ( 思科软件下载 ) 下载Cisco Secure Client预部署软件包。

Cisco Secure Client Pre-Deployment Package (Windows) -  
includes individual MSI files  
cisco-secure-client-win-5.0.01242-predeploy-k9.zip  
[Advisories](#)

19-Dec-2022

71.39 MB



思科安全客户端预部署软件包

5. 将配置文件另存为ISEPostureCFG.xml。

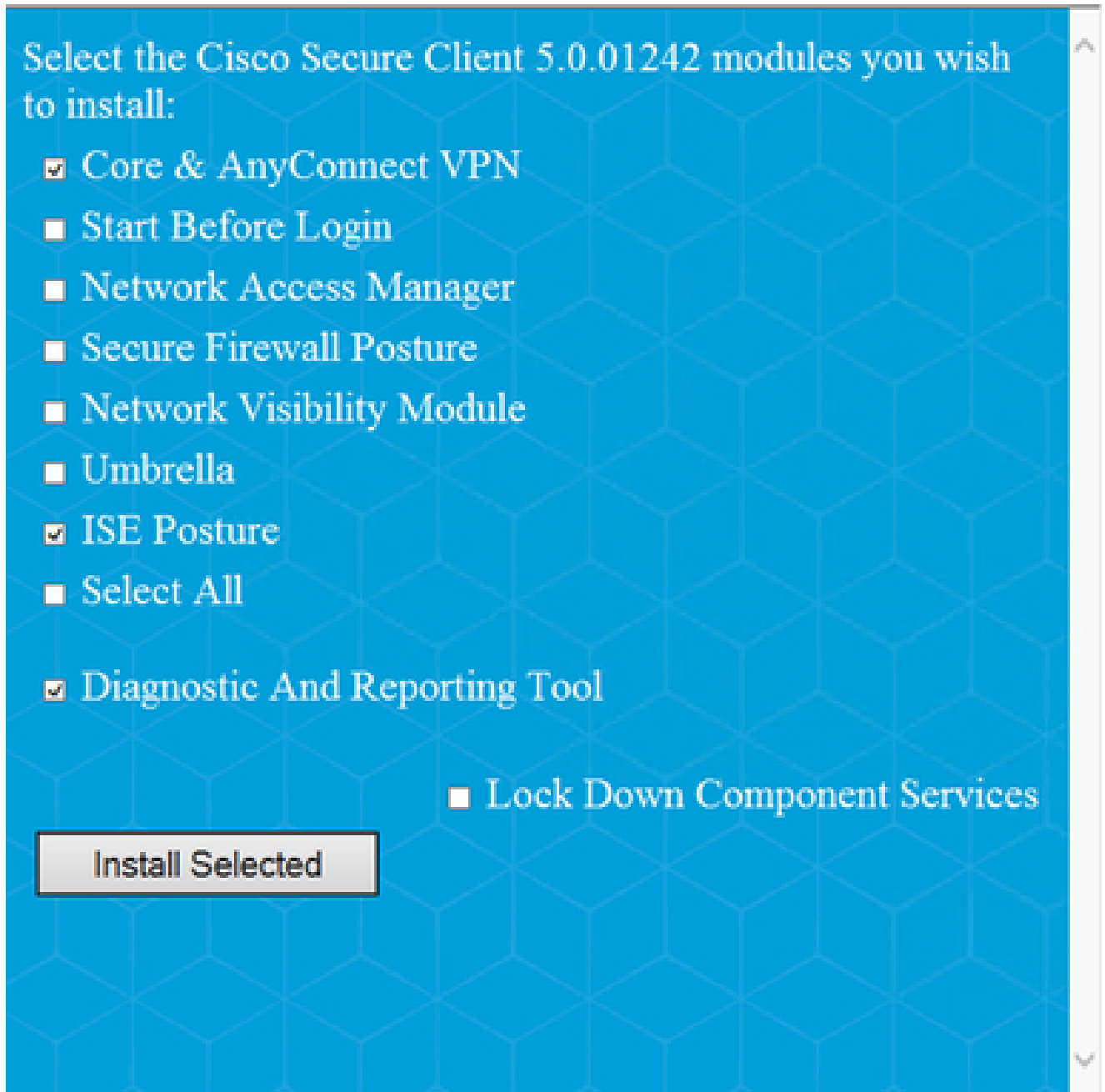
6. 将配置文件和安装文件分发到存档文件中，或将文件复制到客户端。

**警告：**确保计划连接到的头端上也包含相同的思科安全客户端文件：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，打开中的zip文件并运行安装程序以安装核心和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。

| Name  | Type                      |
|---|---------------------------|
| Profiles  | File folder               |
| Setup   | File folder               |
| cisco-secure-client-win-5.0.01242-core-vpn-predeploy-k9   | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-dart-predeploy-k9       | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-iseposture-predeploy-k9 | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-nam-predeploy-k9        | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-mvm-predeploy-k9        | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-posture-predeploy-k9    | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-sbl-predeploy-k9        | Windows Installer Package |
| cisco-secure-client-win-5.0.01242-umbrella-predeploy-k9   | Windows Installer Package |
| Setup   | Application               |
| setup   | HTML Application          |

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，将状态配置文件xml复制到以下位置：

- Windows: %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. 导航到工作中心 > Posture > Client Provisioning > Client Provisioning 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。

Authentication method: \* Certificate\_Request\_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

**Configure authorized groups**  
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available

- ADAAMEX:aaamex.com/AAAUnit/AAAGroup
- ADAAMEX:aaamex.com/Builtin/Account Operat
- ADAAMEX:aaamex.com/Builtin/Administrators
- ADAAMEX:aaamex.com/Builtin/Backup Operato
- ADAAMEX:aaamex.com/Builtin/Certificate Servi

Chosen

- provisioning
- ADAAMEX:aaamex.com/Users/Domain Users

Choose all Clear all

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。

Fully qualified domain name (FQDN): clientprovisioning.aaamex

Idle timeout: 10  
1-30 (minutes)

Display language:  Use browser locale

Fallback language: English - English

Always use: English - English

4. 配置DNS服务器，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：要使用门户FQDN，客户端必须在受信任存储中安装PSN管理员证书链和门户证书链，并且管理员证书必须在SAN字段中包含门户FQDN。

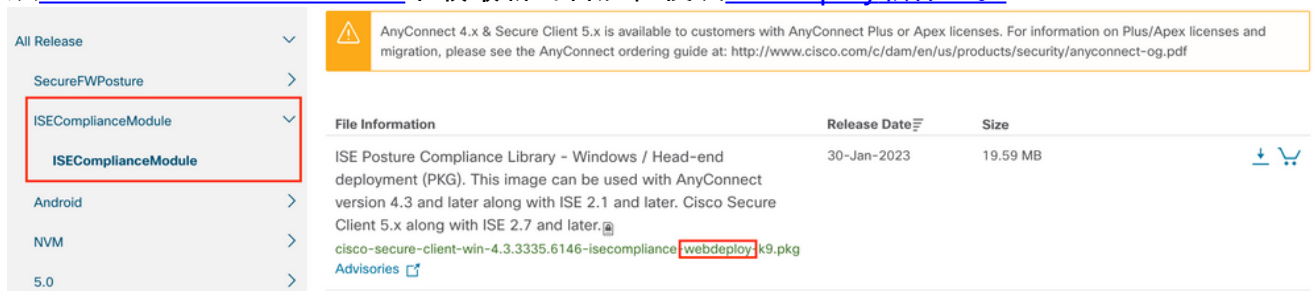
## 客户端调配策略

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[Cisco Software Download](#)（思科软件下载）下载Cisco Secure Client [webdeploy](#)软件包。

Cisco安全客户端Web部署包

2. 从[Cisco Software Download](#)下载最新的合规性模块[webdeploy](#)软件包。

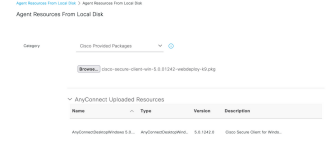


The screenshot shows the Cisco Software Download interface. On the left, a navigation menu is expanded to 'ISEComplianceModule'. The main content area displays a table of file information for the 'ISE Posture Compliance Library - Windows / Head-end deployment (PKG)'. The table has columns for 'File Information', 'Release Date', and 'Size'. The release date is '30-Jan-2023' and the size is '19.59 MB'. The file name is 'cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy.k9.pkg'. A warning banner at the top indicates that AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or Apex licenses.

| File Information   | Release Date | Size     |
|--|--------------|----------|
| ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later. <a href="#">@</a><br>cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy.k9.pkg<br><a href="#">Advisories</a> | 30-Jan-2023  | 19.59 MB |

ISE合规性模块Web部署包

3. 在ISE上，导航到工作中心(Work Centers)>状态(Posture)>客户端调配(Client Provisioning)>资源(Resources)，然后点击本地磁盘上的添加(Add)>代理资源(Agent resources from local disk)。从Category下拉菜单中选择Cisco Provided Packages，并上传以前下载的Cisco



Secure Client webdeploy软件包。重复相同的过程以上传合规性模块。

将思科提供的软件包上传到ISE

4. 返回Resources选项卡，单击Add > AnyConnect Posture Profile。在配置文件上：
  - 配置名称，该名称可用于标识ISE中的配置文件。
  - 配置以逗号分隔的服务器名称规则。使用单个星号\*可允许连接到任何PSN，使用通配符值可允许连接到特定域中的任何PSN，或使用PSN FQDN限制连接到特定PSN。
  - 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。

\* Name: CSC Redirectionless

Description:

Redirectionless Posture LAB - 2 PSNs

ISE终端安全评估配置文件配置I

Posture Protocol

| Parameter               | Value               | Notes   | Description   |
|-------------------------|---------------------|---|---|
| PSM retransmission time | 120<br>secs         |   | This is the agent retry period if there is a Passive Reassessment communication failure.  |
| Retransmission Delay    | 60<br>secs          | Default value: 60. Acceptable Range: between 5 to 300. Accept only integer values.  | Time (in seconds) to wait before retrying.  |
| Retransmission Limit    | 4                   | Default value: 4. Acceptable Range: between 0 to 10. Accept only integer values.  | Number of retries allowed for a message.  |
| Discovery Host          |                     | [IPv4 or IPv6] addresses or FQDNs. [IPv6] address should be without square brackets]  | Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.   |
| * Server name rules     | *.asames.com        | need to be blank by default to force admin to enter a value. "*" means agent will connect to all  | A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"  |
| Call Home List          | ipx.asames.com:8443 | List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port [Port number should be the same, specified in the Client Provisioning portal] | A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.     |
| Back-off Timer          | 30<br>secs          | Enter value of back-off timer in seconds, the supported range is between 10s - 600s.  | Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached. |

ISE终端安全评估配置文件配置II

要查找应在Call Home列表中使用的端口，请导航到Work Centers > Posture > Client Provisioning > Client Provisioning Portal，选择正在使用的门户，然后展开Portal Settings。

# Portals Settings and Customization

Portal Name:

Client Provisioning Portal (default)

Description:

Default portal and user experience user

Language File



Portal test URL

Portal Behavior and Flow Settings

Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:\*

8443

(8000 - 8999)

客户端调配门户端口

5. 返回Resources选项卡，单击Add > AnyConnect Configuration。选择要使用的Cisco安全客户端软件包和合规性模块。

**警告：**如果Cisco安全客户端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应匹配。

6. 向下滚动到Posture Selection部分并选择在第1步中创建的配置文件。点击页面底部的Submit以保存配置。

\* Select AnyConnect Package: CiscoSecureClientDesktopWindows 5.0 

---

\* Configuration Name: AnyConnect Configuration Redirectionless

---

Description:

ISE Redirectionless Posture LAB

## Description Value Notes

\* Compliance Module complianceModuleWindows 4.3.3335.6146 

---

## Cisco Secure Client Module Selection

- |                               |                                     |
|-------------------------------|-------------------------------------|
| ISE Posture                   | <input checked="" type="checkbox"/> |
| VPN                           | <input checked="" type="checkbox"/> |
| Network Access Manager        | <input type="checkbox"/>            |
| Secure Firewall Posture       | <input type="checkbox"/>            |
| Network Visibility            | <input type="checkbox"/>            |
| Umbrella                      | <input type="checkbox"/>            |
| Start Before Logon            | <input type="checkbox"/>            |
| Diagnostic and Reporting Tool | <input checked="" type="checkbox"/> |

AnyConnect配置



## Profile Selection

|               |                     |   |
|---------------|---------------------|---|
| * ISE Posture | CSC Redirectionless | ▼ |
| VPN           |                     | ▼ |

配置文件选择

7. 导航到工作中心 > 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+，并从Agent Configuration部分下的步骤5中选择AnyConnect配置。

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。在示例中，设备位置组用于标识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。

## Agent Configuration

|                                    |  |
|------------------------------------|--|
| ect Configuration Redirectionless▼ | <input checked="" type="checkbox"/> Is Upgrade Mandatory |
|------------------------------------|--|

## Native Supplicant Configuration

|                         |   |
|-------------------------|---|
| Choose a Config Wizard  | ▼ |
| Choose a Wizard Profile | ▼ |

客户端调配策略代理配置

## Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

|                                       | Rule Name  | Identity Groups | Operating Systems | Other Conditions                                 | Results   |        |
|---------------------------------------|------------|-----------------|-------------------|--|---|--------|
| ☰ <input checked="" type="checkbox"/> | IOS        | If Any          | and Apple iOS All | and Condition(s)                                 | then Cisco-ISE-NSP  | Edit ▾ |
| ☰ <input checked="" type="checkbox"/> | Android    | If Any          | and Android       | and Condition(s)                                 | then Cisco-ISE-NSP  | Edit ▾ |
| ☰ <input checked="" type="checkbox"/> | Windows    | If Any          | and Windows All   | and DEVICE:Location EQUALS All Locations#USHWEST | then AnyConnect Configuration Redirectionless                         | Edit ▾ |
| ☰ <input checked="" type="checkbox"/> | MAC OS     | If Any          | and Mac OSX       | and Condition(s)                                 | then MacOS Configuration And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP | Edit ▾ |
| ☰ <input checked="" type="checkbox"/> | Chromebook | If Any          | and Chrome OS All | and Condition(s)                                 | then Cisco-ISE-Chrome-NSP   | Edit ▾ |

[Save](#) [Reset](#)

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DAACL以允许流量到达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。

\* Name

Description

IP version  IPv4  IPv6  Agnostic

\* DACL Content

|         |                                       |
|---------|---------------------------------------|
| 1234567 | permit udp any any eq domain          |
| 8910111 | permit udp any any eq bootps          |
| 2131415 | permit ip any host <ipn 1 IP address> |
| 1617181 | permit ip any host <ipn 2 IP address> |
| 9200122 | permit icmp any any                   |
| 2324252 | deny ip any any                       |
| 6372629 |                                       |
| 3001323 |                                       |
| 3340536 |                                       |
| 3738094 |                                       |
| 0414243 |                                       |

✓ Check DACL Syntax

DACL is valid

### 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

```

注意：某些第三方设备可能不支持DACL，在这种情况下，必须使用过滤器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

Authorization Profiles > Redirectionless posture

Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

DACL Name

2步中创建的DACL。

授权配置文件

注：如果未使用DACL，请使用Common Tasks中的Filter-ID或Advanced Attribute Settings来推送相应的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并打开正在使用的策略集，或创建一个新的策略集。
2. 向下滚动到Authorization Policy部分。使用Session PostureStatus NOT\_EQUALS Compliant创建授权策略，并选择在上一部分中创建的授权配置文件。

|                 |           |   | Results                   |                  |      |         |
|-----------------|-----------|---|---------------------------|------------------|------|---------|
| Status          | Rule Name | Conditions  | Profiles                  | Security Groups  | Hits | Actions |
| Compliant       |           | Session-PostureStatus EQUALS Compliant  | Compliant access x        | Select from list | 0    |         |
| Redirectionless | AND       | DEVICE-Posture EQUALS Posture#Redirectionless<br>DEVICE-Location EQUALS All Locations#US#WEST<br>Session-PostureStatus NOT_EQUALS Compliant | Redirectionless posture x | Select from list | 0    |         |
| Redirection     | AND       | Session-PostureStatus NOT_EQUALS Compliant<br>DEVICE-Posture EQUALS Posture#Redirection   | Redirection posture x     | Select from list | 0    |         |
| Default         |           |   | DenyAccess x              | Select from list | 0    |         |

### 授权策略

- 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账开始创建，但PSN上未收到用于清除会话的记账停止。

**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：

- 在Cisco Secure Client UI中，点击左下角的齿轮图标。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。



The screenshot shows the Cisco Secure Client interface. On the left, there is a navigation menu with 'Status Overview', 'AnyConnect VPN', and 'ISE Posture' (selected). The main area is titled 'ISE Posture' and has tabs for 'Preferences', 'Statistics', 'Security Products', 'Scan Summary', and 'Message History'. Under 'Compliance Information', the current status is 'Compliant'. Under 'Connection Information', the 'Policy Server' is set to 'ise30cmexaaa.aaamex.com', which is highlighted with a red box.

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，请注意以下事项：

- 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... | <span style="color: blue;">●</span>  |         | 0        | redirectionless | 00:50:5...  | Posture Lab >> Redirectionless | ise30cmexaaa | Compliant      | Redirectionless posture |
| Apr 03, 2023 07:32:40.7... | <span style="color: green;">✓</span> |         |          | #ACSACL#-IP...  |             |                                | ise30baaamex |                |                         |
| Apr 03, 2023 07:32:40.6... | <span style="color: green;">✓</span> |         |          | 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。

## Overview

|                       |                                |
|-----------------------|--------------------------------|
| Event                 | 5200 Authentication succeeded  |
| Username              | redirectionless                |
| Endpoint Id           | 00:50:56:B3:3E:0E ⓘ            |
| Endpoint Profile      | Windows10-Workstation          |
| Authentication Policy | Posture Lab >> Default         |
| Authorization Policy  | Posture Lab >> Redirectionless |
| Authorization Result  | Redirectionless posture        |

## Authentication Details

|                    |                         |
|--------------------|-------------------------|
| Source Timestamp   | 2023-04-03 19:32:40.691 |
| Received Timestamp | 2023-04-03 19:32:40.691 |

|               |              |
|---------------|--------------|
| Policy Server | ise30baaamex |
|---------------|--------------|

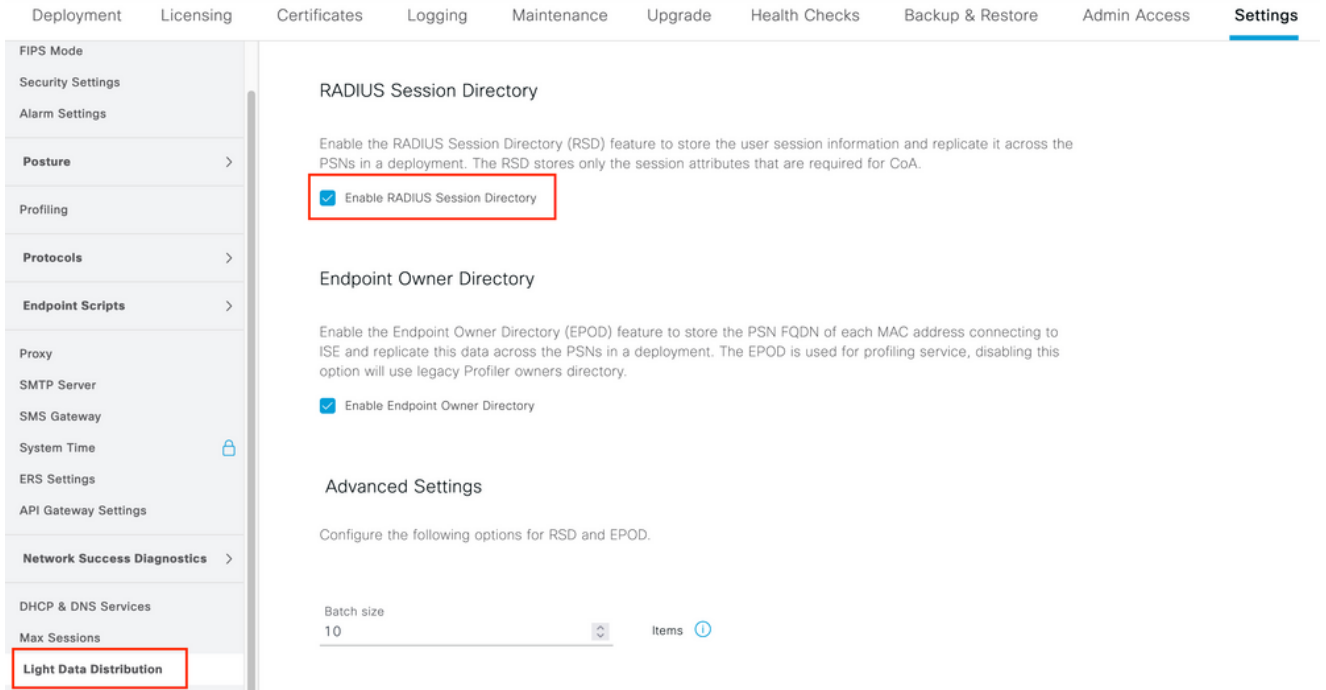
|          |                               |
|----------|-------------------------------|
| Event    | 5200 Authentication succeeded |
| Username | redirectionless               |

实时日志详细信息中的策略服务器

### 解决方案

ISE 2.6补丁6和2.7补丁3以上的ISE版本将[RADIUS会话目录](#)作为无重定向状态流中陈旧/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. 从ISE CLI，通过运行命令验证ISE消息服务在所有PSN上运行 显示应用状态ise。



```
lise30cmexaaa/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：此服务是指用于PSN之间的RSD的通信方法，无论可以从ISE UI设置的系统日志的ISE消息服务设置的状态如何，该通信方法都应运行。

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。单击警报的名称可查看更多详细信息。

| Severity | Name             | Occu... | Last Occurred |
|----------|------------------|---------|---------------|
| ▼        | queue            | x       |               |
|          | Queue Link Error | 2143    | 37 mins ago   |

Last refreshed: 2023-04-03 14:45:19

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。

Alarms: Queue Link Error

##### Description

The queue link between two nodes in the ISE deployment is down.

##### Suggested Actions

Please check and restore connectivity between the nodes. Ensure that the nodes and the ISE Messaging Service are up and running. Ensure that ISE Messaging Service ports are not blocked by firewall. Please note that these alarms could occur between nodes, when the nodes are being registered to deployment or manually-synced from PSPAN or when the nodes are in out-of-sync state or when the nodes are getting restarted.

Rows/Page 100 / 22 > > | Go 2143 Total Rows

Refresh Acknowledge

| <input type="checkbox"/> Time Stamp                  | Description   | Cause={ts_alert;" unknown Ca"} | Details |
|--|---|--------------------------------|---------|
| <input type="checkbox"/> Apr 03 2023 21:07:00.977 PM | Queue Link Error: Message=From ise30cmexaaa.aaamex.com To ise30baaamex.aaamex.com; Cause={ts_alert;" unkno... |                                |         |
| <input type="checkbox"/> Apr 03 2023 21:07:00.959 PM | Queue Link Error: Message=From ise30baaamex.aaamex.com To ise30cmexaaa.aaamex.com; Cause={ts_alert;" unkno... |                                |         |

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。
- Unknown CA：表示对ISE消息证书进行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. 导航到Administration > 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：重新生成证书时，应观察由于未知CA或Econnrefused导致的Queue Link Error警报，并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：

- Cisco安全客户端中的随机或间断No policy server detected errors
- 门户服务线程池达到阈值事件的已达到最大资源限制的报告。导航到Operations > Reports > Reports > Audit > Operations Audit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. 从终端清除connectiondata.xml，方法是从Cisco Secure Client文件夹删除文件并重新启动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，也应执行此操作。
2. 使用DAACL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。

### Authorization Profile

\* Name: Redirectionless PSN1

Description: Authorization profile for redirectionless posture with DACL allowing traffic only to PSN1, DNS and DHCP

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  ⓘ

Agentless Posture:  ⓘ

Passive Identity Tracking:  ⓘ

Common Tasks

DACL Name: redirectionless\_posture\_psn1

具有单个PSN的DACL的授权配置文件

|                      |   |                      |
|----------------------|---|----------------------|
| Compliant            | Session-PostureStatus EQUALS Compliant                      | Compliant access     |
| Redirectionless PSN1 | DEVICE-Posture EQUALS Posture#Redirectionless               | Redirectionless PSN1 |
|                      | DEVICE-Location EQUALS All Locations#US#WEST                |                      |
|                      | Session-PostureStatus NOT_EQUALS Compliant                  |                      |
|                      | Network Access-ISE Host Name EQUALS ise30baamex.aaamex.com  |                      |
| Redirectionless PSN2 | DEVICE-Posture EQUALS Posture#Redirectionless               | Redirectionless PSN2 |
|                      | DEVICE-Location EQUALS All Locations#US#WEST                |                      |
|                      | Session-PostureStatus NOT_EQUALS Compliant                  |                      |
|                      | Network Access-ISE Host Name EQUALS ise30cmexaaa.aaamex.com |                      |
| Redirection          | Session-PostureStatus NOT_EQUALS Compliant                  | Redirection posture  |
|                      | DEVICE-Posture EQUALS Posture#Redirection                   |                      |

每个PSN的授权策略

## 记账

RADIUS记账对于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。验证在网络设备上是否正确配置了记账以对每个会话向单个PSN发送身份验证请求、记账开始、记账停止和记账更新非常重要。

要验证ISE上接收的记账数据包，请导航到操作 > 报告 > 报告 > 终端和用户 > RADIUS记账。

## 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）。