Implement ISE Redirectionless Posture

Contents

Introduction

This document describes the use and configuration of redirectionless posture flow and troubleshooting tips.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Posture flow on ISE
- Configuration of posture components on ISE

- Redirection to ISE portals

For a better understanding of the concepts described later, it is recommended to go through:

Compare ISE Posture Redirection Flow to ISE Posture Redirectionless Flow
Troubleshoot ISE Session Management and Posture

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE version 3.3
- Cisco Secure Client 5.0.01242

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

ISE Posture flow consists of these steps:

0. Authentication/Authorization. Generally performed right before posture flow is initiated but it can be bypassed for certain use cases such as Posture Reassessment (PRA).

As authentication itself does not trigger posture discovery this is not considered essential for every posture flow.

1. Discovery. Process performed by the Secure Client ISE Posture module to find the PSN owner of the current active session.
2. Client Provisioning. Process performed by ISE to provision the client with the corresponding Cisco Secure Client (formerly AnyConnect) ISE Posture module and Compliance Module versions. In this step, the local copy of the posture profile contained in and signed by the particular PSN is also pushed to the client.
3. System Scan. Posture policies configured on ISE are evaluated by the Compliance Module.
4. Remediation (Optional). Performed in the case of any posture policies being not compliant.
5. CoA. Reauthorization is necessary to grant final (Compliant or Not Compliant) network access.

This document focuses on the Discovery process of ISE Posture flow.

Cisco recommends to use redirection for the discovery process, however, there are certain cases where redirection is not possible to implement such as the use of third party Network Devices where redirection is not supported. This document aims to provide a general guidance and best practices to implement and troubleshoot redirectionless posture in such environments.

Full description of redirectionless flow is described in Compare ISE Posture Redirection Flow to ISE Posture Redirectionless Flow

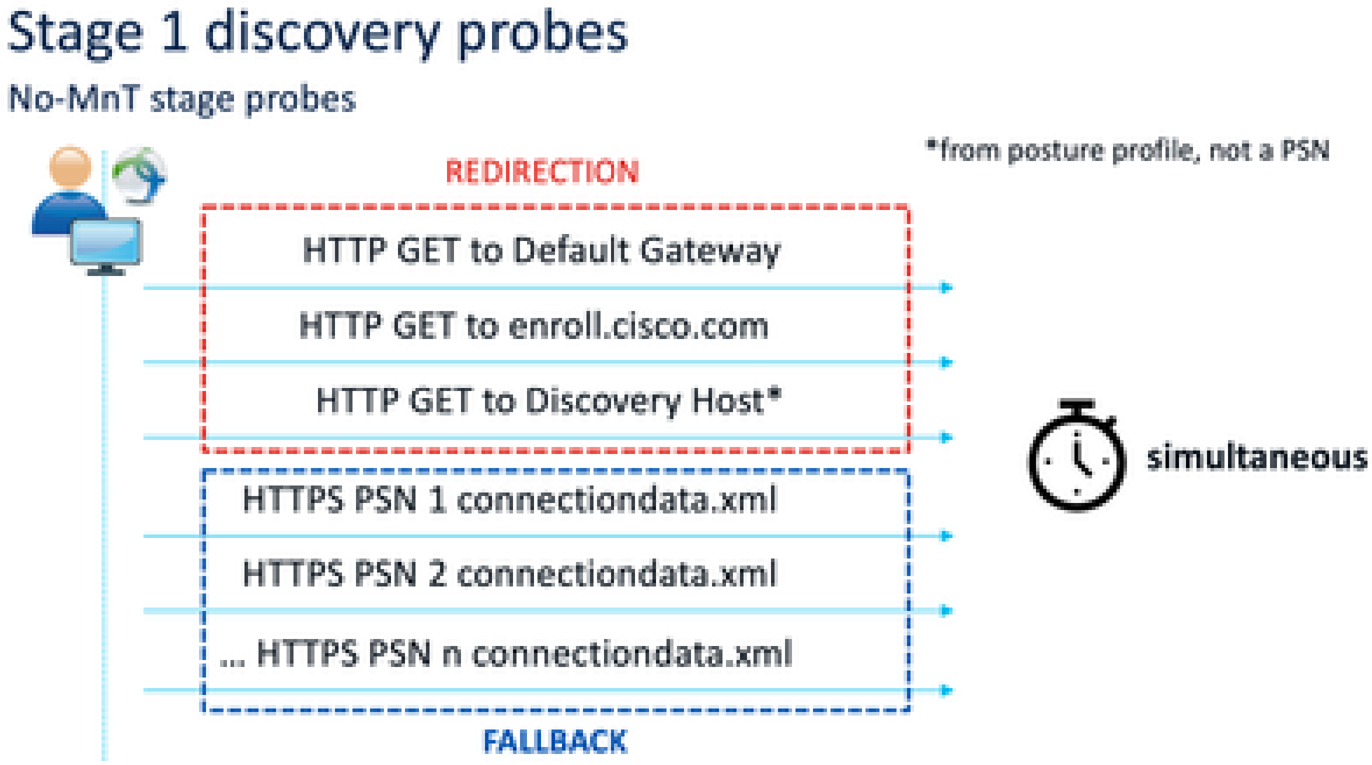
There are two types of posture discovery probes that do not use redirection:

1. Connectiondata.xml
2. Call Home List

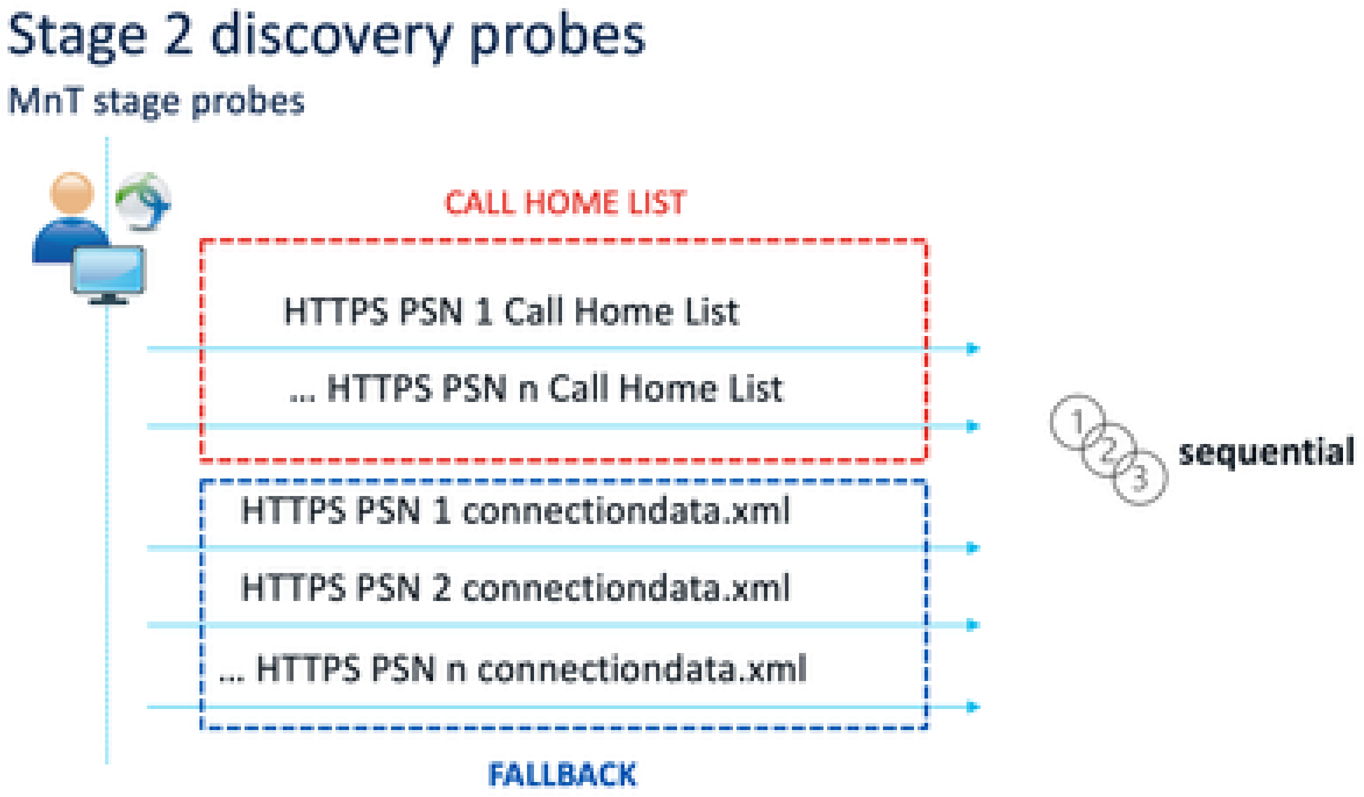
Connectiondata.xml

Connectiondata.xml is a file created and maintained automatically by Cisco Secure Client. It consists of a list of PSNs that the client has previously successfully connected to for posture, hence, this is only a local file and its content is not persistent across all endpoints.

The main purpose of connectiondata.xml is to work as a backup mechanism for both Stage 1 and Stage 2 discovery probes. In case that redirection or Call Home List probes are unable to find a PSN with an active session, Cisco Secure Client sends a direct request to each of the servers listed in connectiondata.xml.


Stage 1 discovery probes
No-MnT stage probes
*from posture profile, not a PSN
REDIRECTION
HTTP GET to Default Gateway
HTTP GET to enroll.cisco.com
HTTP GET to Discovery Host*
simultaneous
HTTPS PSN 1 connectiondata.xml
HTTPS PSN 2 connectiondata.xml
... HTTPS PSN n connectiondata.xml
FALLBACK

Stage 1 Discovery Probes


Stage 2 discovery probes
MnT stage probes
CALL HOME LIST
HTTPS PSN 1 Call Home List
... HTTPS PSN n Call Home List
HTTPS PSN 1 connectiondata.xml
HTTPS PSN 2 connectiondata.xml
... HTTPS PSN n connectiondata.xml
FALLBACK
1
2
3
sequential

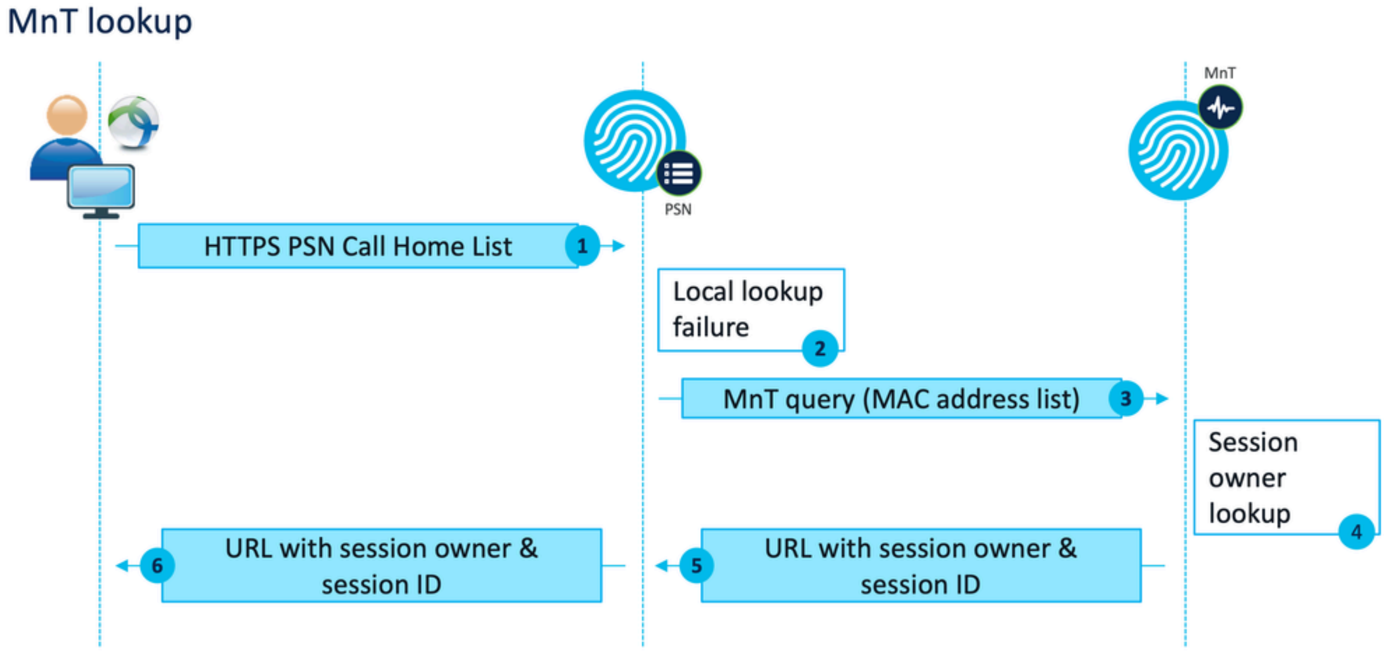
Stage 2 Discovery Probes

A common problem caused by the use of connectiondata.xml probes is an overload of the ISE deployment due to a large number of HTTPS requests sent by the endpoints. It is important to consider that while connectiondata.xml is effective as a backup mechanism to avoid full outages for both redirection and redirectionless posture mechanisms, it is not a sustainable solution for a posture environment, therefore, it is necessary to diagnose and resolve the design and configuration problems that cause the failure of the main discovery probes and that result in discovery issues.

Call Home List

Call Home List is a section of the posture profile where a list of PSNs is specified to be used for posture. Unlike connectiondata.xml, this is created and maintained by an ISE administrator and can require a design phase for optimal configuration. The list of PSNs in Call Home List matches the list of authentication and accounting servers that is configured in the network device or load balancer for RADIUS.

Call Home List probes enable the use of an MnT lookup during active session search in case of a local lookup failure in a PSN. The same functionality extends to connectiondata.xml probes only when they are used during Stage 2 discovery. For this reason, all Stage 2 probes are also referred to as New Generation probes.


MnT lookup
PSN
MnT
HTTPS PSN Call Home List
1
Local lookup failure
2
MnT query (MAC address list)
3
Session owner lookup
4
URL with session owner & session ID
5
URL with session owner & session ID
6

MnT Lookup Flow

Design

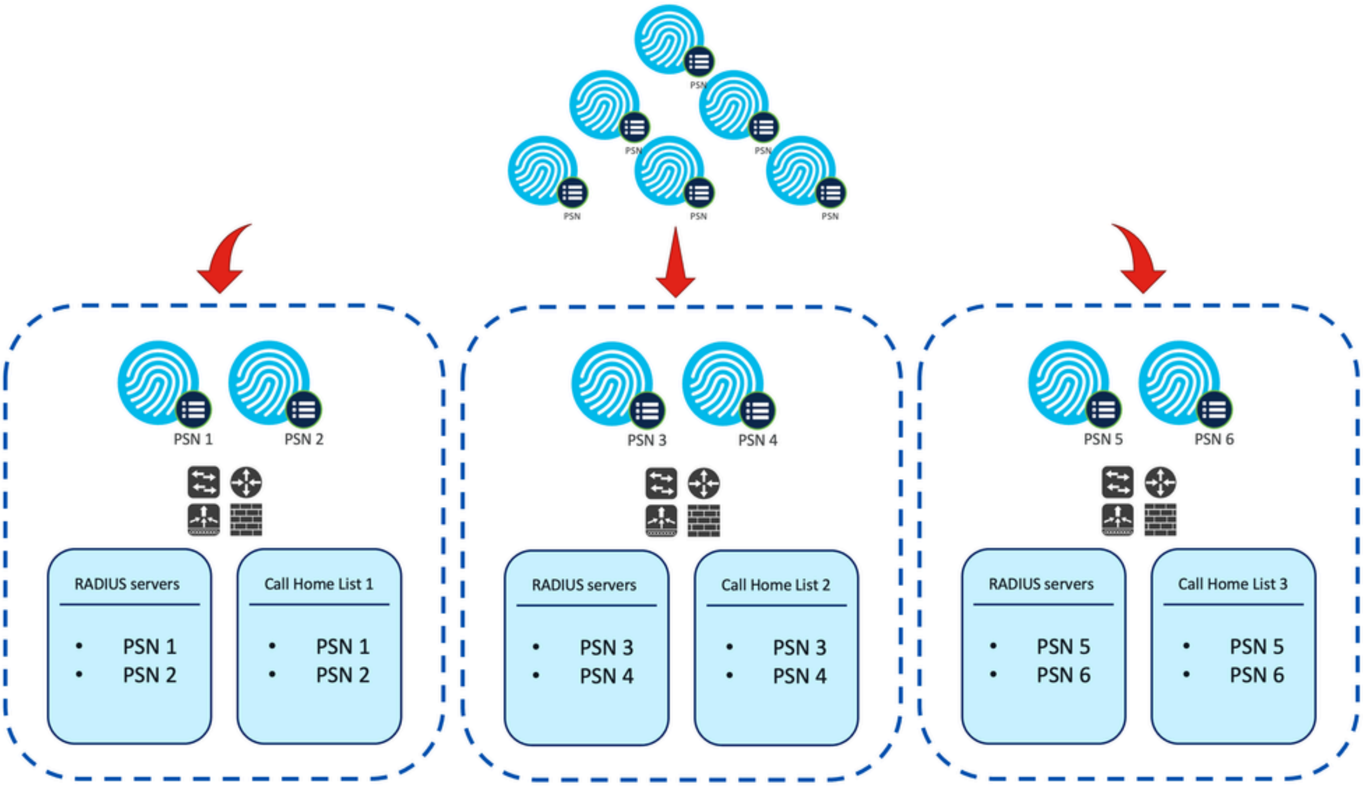
As a redirectionless discovery process often entails a more complex flow and a larger amount of processing on PSNs and MnT compared to a redirection flow, there are two common challenges that can arise during implementation:

1. Effective discovery
2. Performance of ISE deployment

In order to cope with these challenges, it is recommended to design the Call Home List to limit the number of PSNs that a given endpoint can use for posture. For medium and large deployments, it is necessary to distribute the deployment in order to create multiple Call Home Lists with reduced number of PSNs, in consequence the list of PSNs that are used for RADIUS authentication for a given Network Device can be limited in the same way to match the corresponding Call Home List.

These aspects can be taken into consideration while developing the PSN distribution strategy to determine the maximum number of PSNs in each Call Home List:

- Number of PSNs in the deployment
- Hardware specs of PSNs and MnT nodes
- Maximum number of concurrent posture sessions in the deployment
- Number of network devices
- Hybrid environments (simultaneous redirection and redirectionless posture implementation)
- Number of adapters used by the endpoints
- Location of network devices and PSNs
- Network connection types used for posture (wired, wireless, VPN)



Example: PSN Distribution for Redirectionless Posture

Tip: Use Network Device Groups to classify the network devices according to the design.

Configure

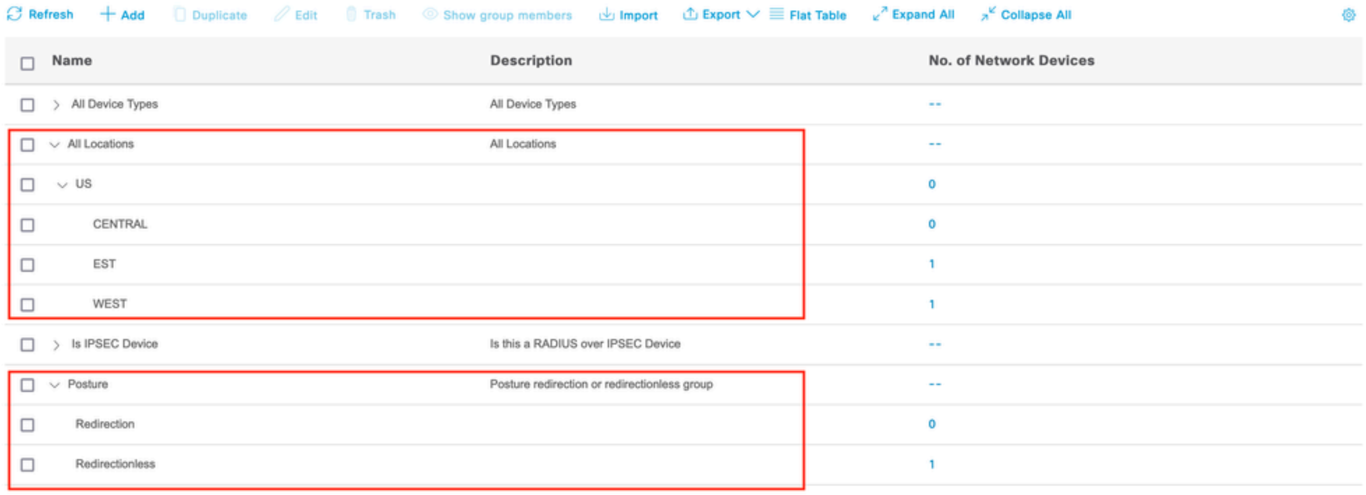
Network Device Groups (Optional)

Network Device Groups can be used to identify and match network devices with their corresponding RADIUS server list and Call Home List. In the case of hybrid environments, they can also be used to identify devices that support redirection from devices that do not.

If the distribution strategy developed during design phase relies on Network Device Groups, follow the next steps to configure them on ISE:

1. Navigate to **Administration** > **Network Resources Network Resource Groups.**
2. Click **Add** to add a new group, provide a **name** and select the **parent group**, if applicable.
3. Repeat step 2 to create all the necessary groups.

In the examples used throughout this guide, Location Device Group is used to identify the RADIUS servers list and Call Home List, and a custom Posture Device Group is used to identify Redirection from Redirectionless posture devices.

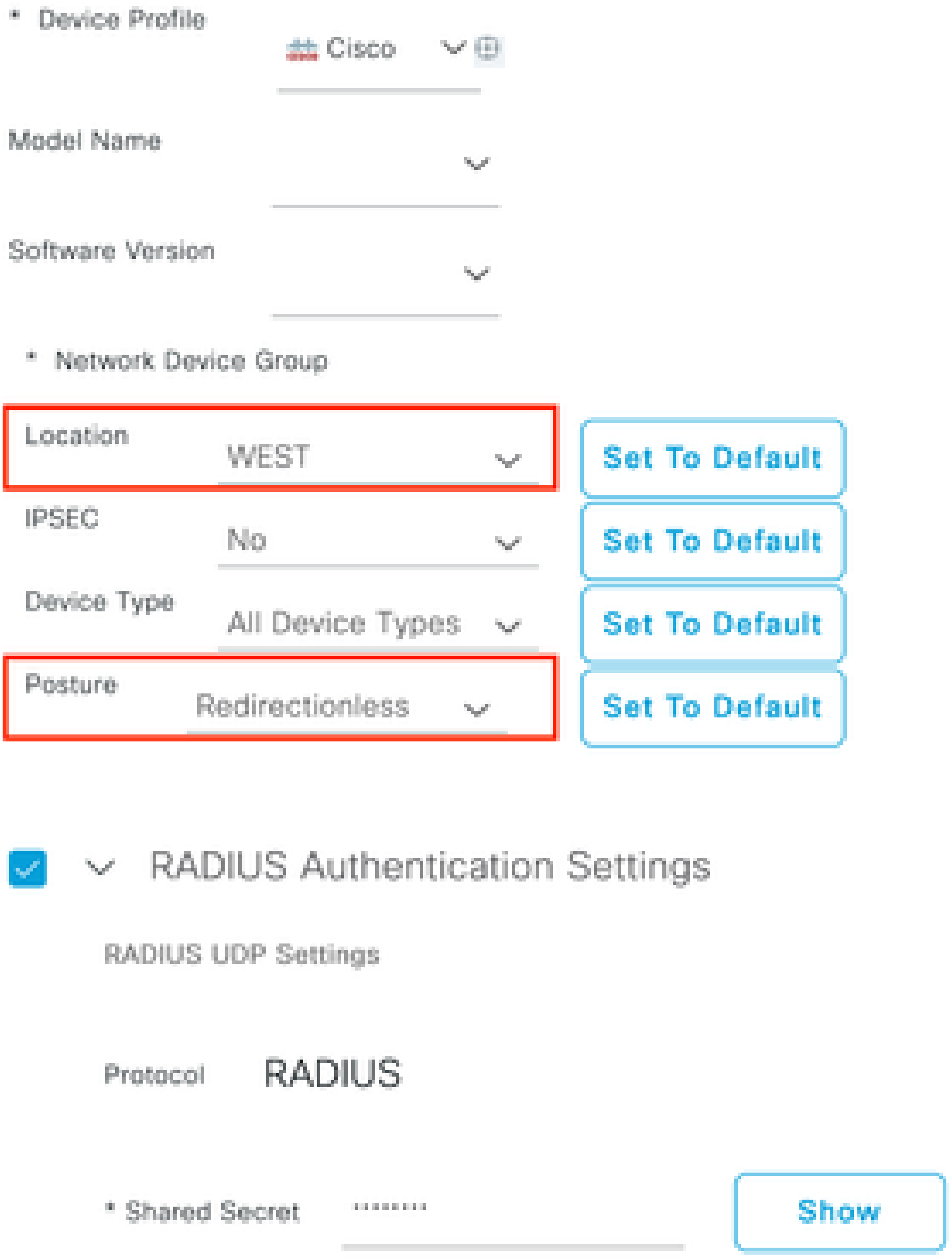


□	Name	Description	No. of Network Devices
□	> All Device Types	All Device Types	--
□	∨ All Locations	All Locations	--
□	∨ US		0
□	CENTRAL		0
□	EST		1
□	WEST		1
□	> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--
□	∨ Posture	Posture redirection or redirectionless group	--
□	Redirection		0
□	Redirectionless		1

Network Device Groups

Network Device

1. The network device can be configured for RADIUS authentication, authorization and accounting. Refer to each vendor documentation for configuration steps. Configure the RADIUS servers list according to the corresponding Call Home List.
2. On ISE, navigate to **Administration > Network Resources > Network Devices** and click **Add**. Configure the Network Device Groups according to the design and enable **RADIUS Authentication Settings** to configure the **Shared Secret**.



* Device Profile: Cisco

Model Name

Software Version

* Network Device Group

Location: WEST

IPSEC: No

Device Type: All Device Types

Posture: Redirectionless

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: ·········

Network Device Configuration

Client Provisioning

There are two ways to provision the client with the right software and profile to perform posture in a redirectionless environment:

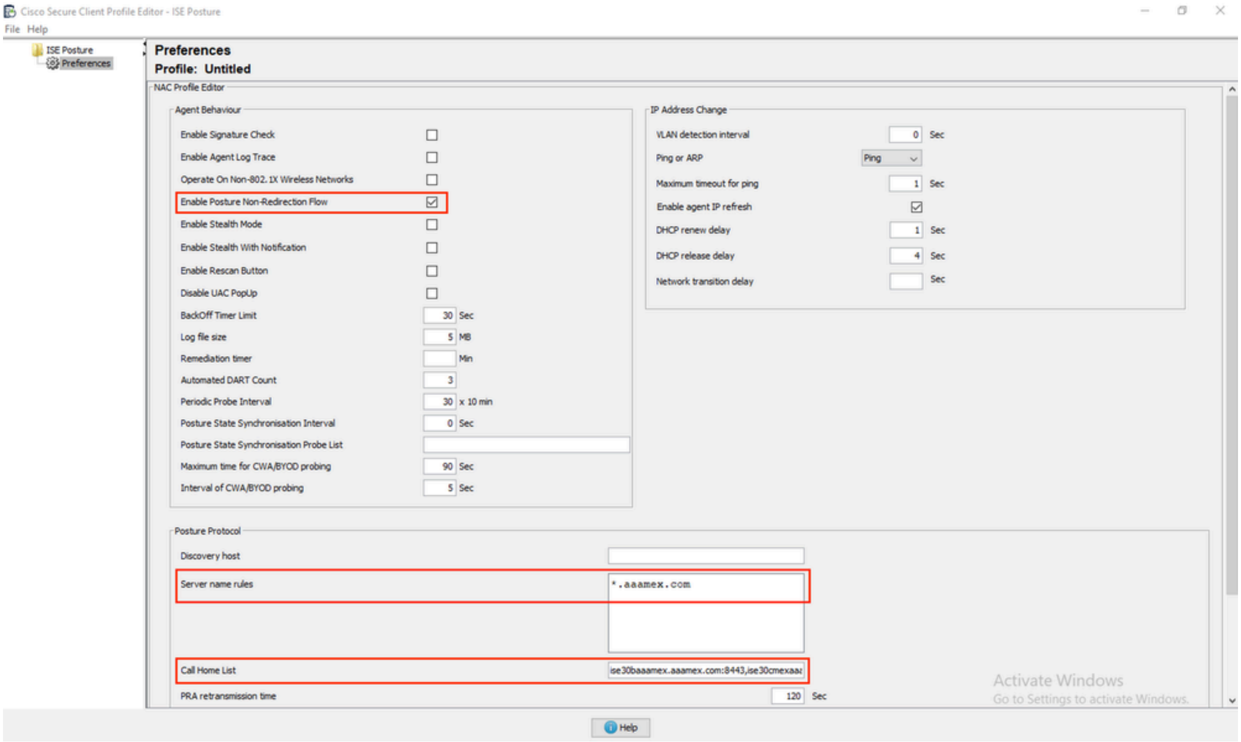
1. Manual provisioning (pre-deploy)
2. Client Provisioning Portal (web deploy)

Manual Provisioning (Pre-deploy)

1. Download and install Cisco Secure Client **Profile Editor** from Cisco Software Download.

   Profile Editor package

2. Open ISE Posture profile editor:
   - Make sure that **Enable Posture Non-Redirection Flow** is enabled.
   - Configure the **Server name rules** separated by commas. Choose one of the these configurations:
     - A single asterisk * to allow connection to any PSN.
     - Wildcard values (for example, *.aaamex.com) to allow connection to any PSN in specific domains.
     - List of PSN FQDNs, comma-separated, to restrict the connection to specific PSNs. If used, this list must match the Call Home List.
   - Configure **Call Home List** to specify the comma-separated list of PSNs. Make sure to add the Client Provisioning Portal port with the format FQDN:port or IP:port.



Cisco Secure Client Profile Editor - ISE Posture

Preferences

Profile: Untitled

NAC Profile Editor

Agent Behaviour

Enable Signature Check □
Enable Agent Log Trace □
Operate On Non-802. 1X Wireless Networks □
Enable Posture Non-Redirection Flow ☑
Enable Stealth Mode □
Enable Stealth With Notification □
Enable Rescan Button □
Disable UAC PopUp □
BackOff Timer Limit 30 Sec
Log file size 5 MB
Remediation timer Min
Automated DART Count 3
Periodic Probe Interval 30 x 10 min
Posture State Synchronisation Interval 0 Sec
Posture State Synchronisation Probe List
Maximum time for CWA/BYOD probing 90 Sec
Interval of CWA/BYOD probing 5 Sec

IP Address Change

VLAN detection interval 0 Sec
Ping or ARP Ping
Maximum timeout for ping 1 Sec
Enable agent IP refresh ☑
DHCP renew delay 1 Sec
DHCP release delay 4 Sec
Network transition delay Sec

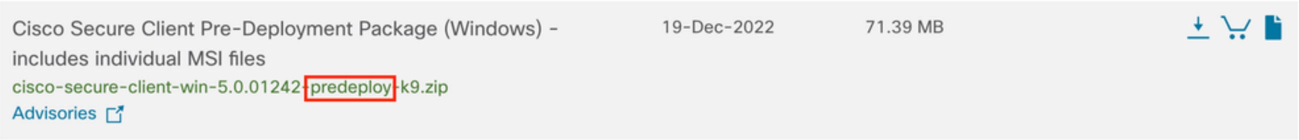
Posture Protocol

Discovery host
Server name rules *.aaamex.com
Call Home List ise30baaamex.aaamex.com:8443,ise30cmexaa
PRA retransmission time 120 Sec

Posture Profile Configuration with Profile Editor

Note: Refer to step 4 of the Client provisioning policy section for instructions on how to verify the Client Provisioning Portal port if necessary.

3. Save the **profile** as **ISEPostureCFG.xml**.
4. Repeat steps 2 and 3 to Create a new **posture profile** for each Call Home List in Use.
5. Download the **Cisco Secure Client Pre-Deployment Package** from Cisco Software Download.



Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files 19-Dec-2022 71.39 MB

cisco-secure-client-win-5.0.01242-predeploy-k9.zip

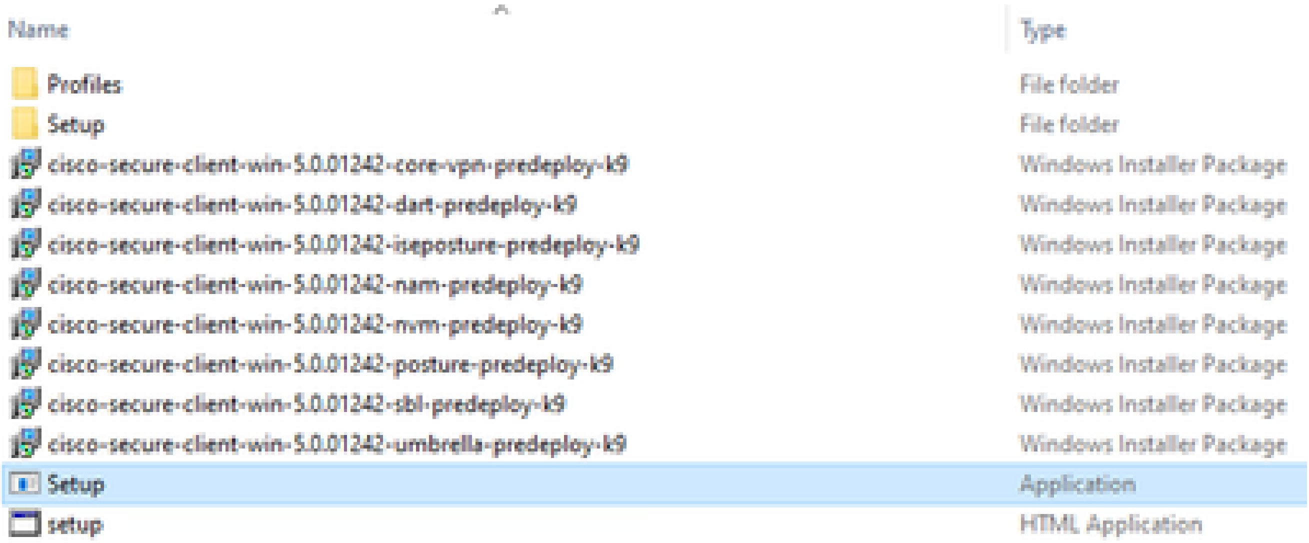
Advisories

Cisco Secure Client pre-deploy package

6. Distribute the **profile** and **installation files** in an archive file, or copy the **files** to the clients.

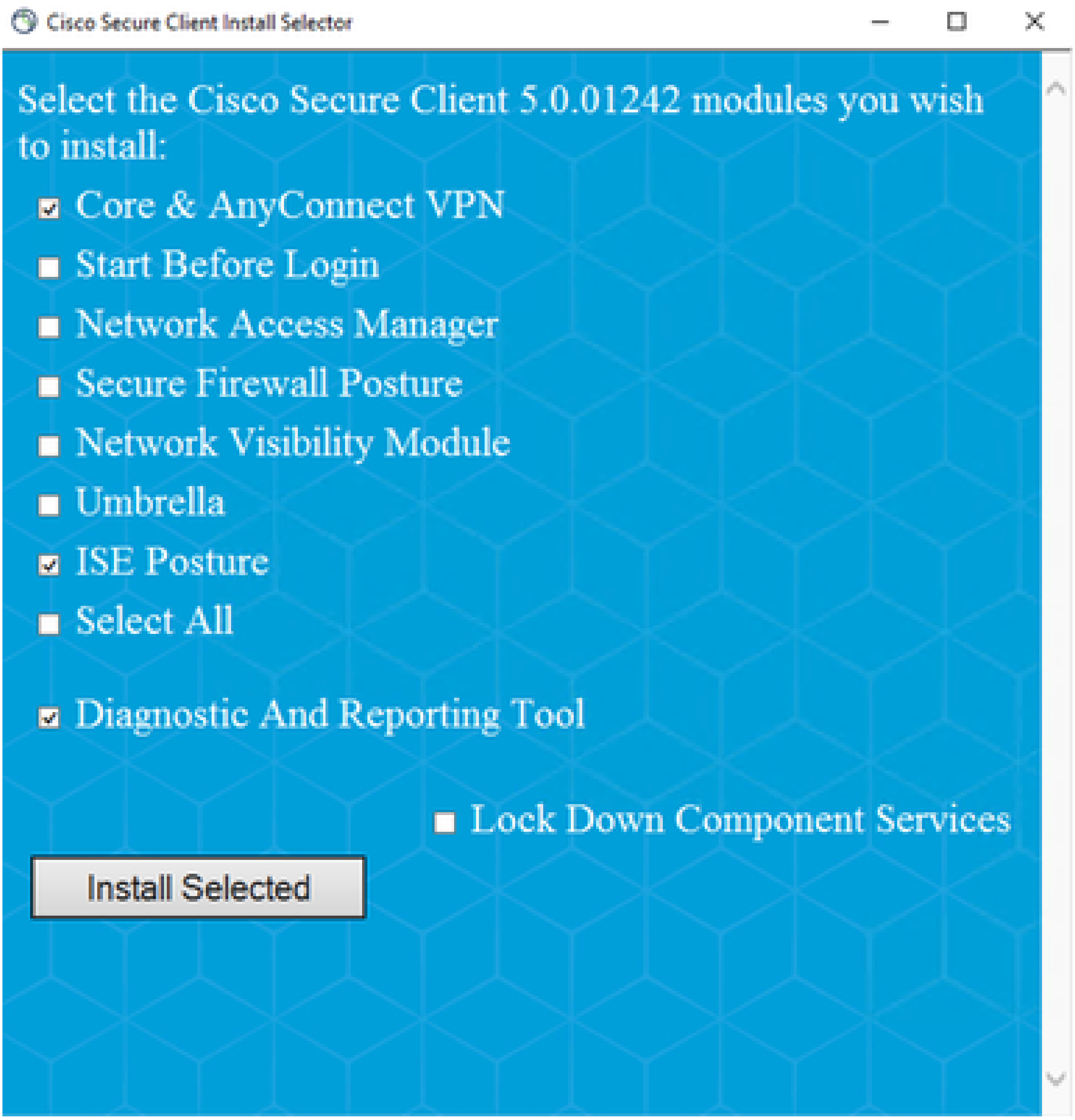
> **Warning**: Make sure that the same Cisco Secure Client files are also on the headends you plan to connect to: Secure Firewall ASA, ISE, and so on. Even when manual provisioning is used, ISE must be configured for client provisioning with the corresponding software version. Refer to the Client provisioning policy configuration section for detailed instructions.

7. On the client, open the **zip file** and run the **Setup** to install the Core and ISE Posture modules. Alternatively the individual msi files can be used to install each module, in this case, you must make sure that core-vpn module is installed first.



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-nvm-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

Cisco Secure Client Pre-deploy Package Contents



Cisco Secure Client Install Selector

Select the Cisco Secure Client 5.0.01242 modules you wish to install:

☑ Core & AnyConnect VPN
□ Start Before Login
□ Network Access Manager
□ Secure Firewall Posture
□ Network Visibility Module
□ Umbrella
☑ ISE Posture
□ Select All

☑ Diagnostic And Reporting Tool

□ Lock Down Component Services

Cisco Secure Client Installer

Tip: Install the Diagnostic and Reporting Tool to be used for troubleshooting purposes.

8. Once installation is complete copy the **posture profile xml** to the these locations:
   - Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
   - MacOS: /opt/cisco/secureclient/iseposture/

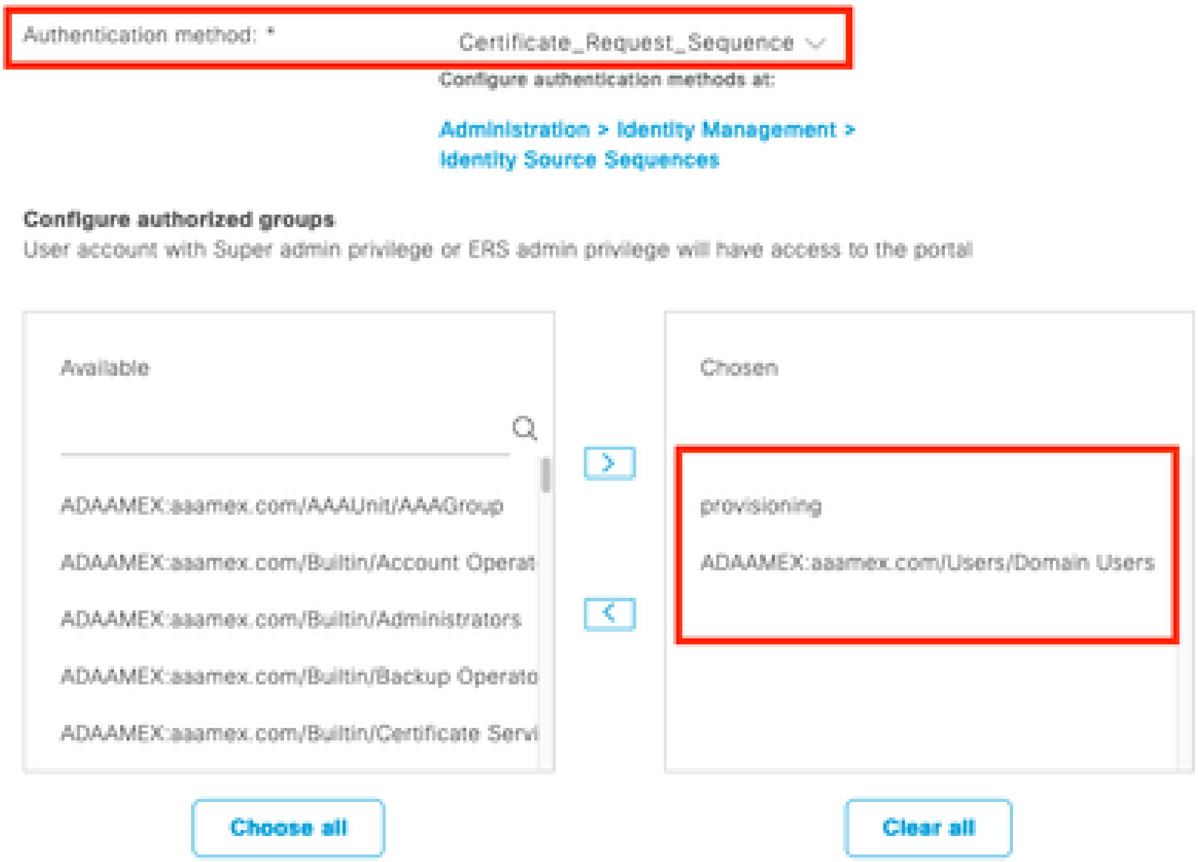
Client Provisioning Portal (Web Deploy)

ISE Client Provisioning Portal can be used to install Cisco Secure Client ISE Posture module and the posture profile from ISE, it can also be used to push the posture profile alone if ISE Posture module is already installed on the client.

1. Navigate to **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Portal** to

open the portal configuration. Expand **Portal Settings** section and locate the **Authentication method** field, select the **Identity Source Sequence** to be used for authentication in the portal.

2. Configure **internal** and **external identity groups** that are authorized to use the Client Provisioning Portal.



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

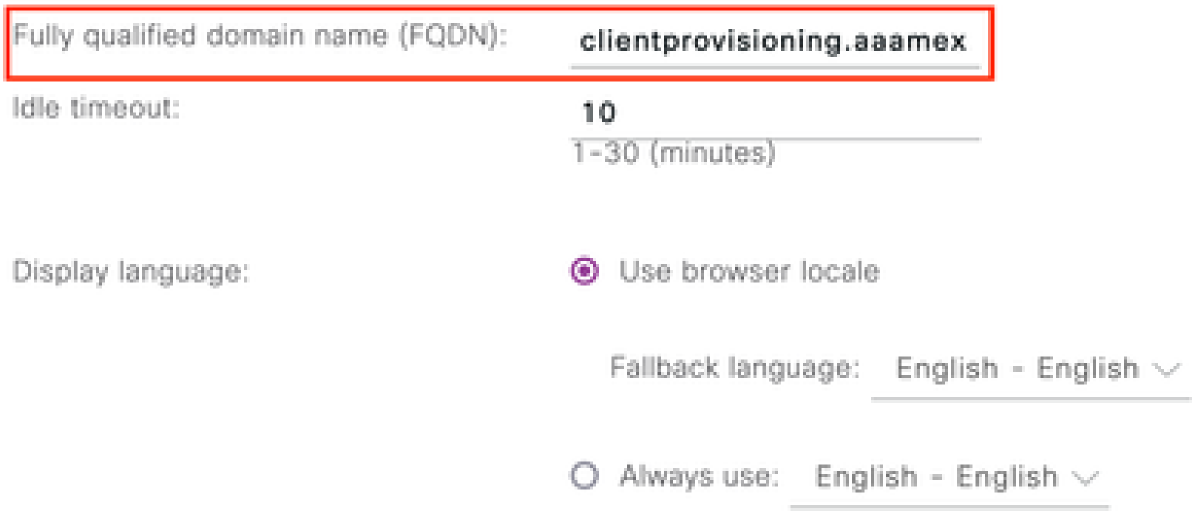
Chosen

provisioning

ADAAMEX:aaamex.com/Users/Domain Users

Authentication Method and Authorized Groups in Portal Settings

3. In the **Fully qualified domain name (FQDN)** field, configure the **URL** that is used by the clients to access the portal. To configure multiple FQDNs, enter the values separated by commas.



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. Configure the **DNS server(s)** to resolve the portal URL to the PSNs of the corresponding Call Home List.
5. Provide the FQDN to the end users to access the portal in order to install the ISE Posture software.

Note: To make use of the portal FQDN, clients must have the PSN Admin certificate chain as well as the Portal certificate chain installed in the trusted store, and the Admin certificate must contain the portal FQDN in the SAN field.

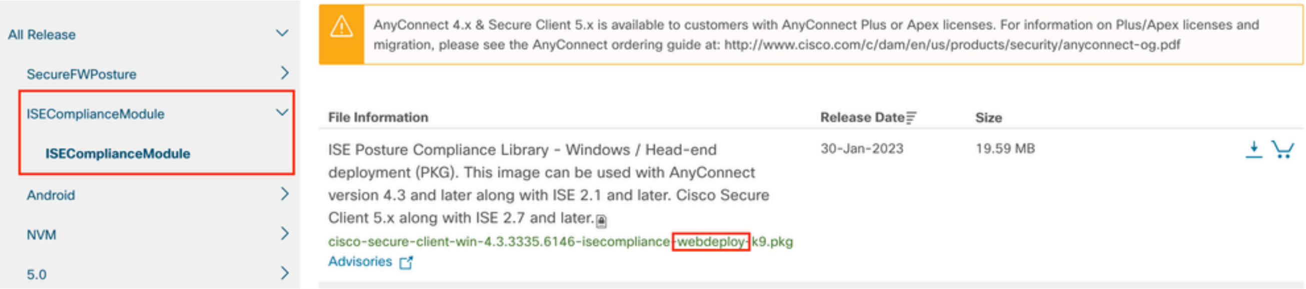
Client Provisioning Policy

Client provisioning must be configured on ISE regardless of the type of provisioning (pre-deploy or web deploy) that is used to install Cisco Secure Client on the endpoints.

1. Download the **Cisco Secure Client Headend Deployment Package** from Cisco Software Download.

   Cisco Secure Client Webdeploy Package

2. Download the latest **ISE Compliance Module** webdeploy package from Cisco Software Download.

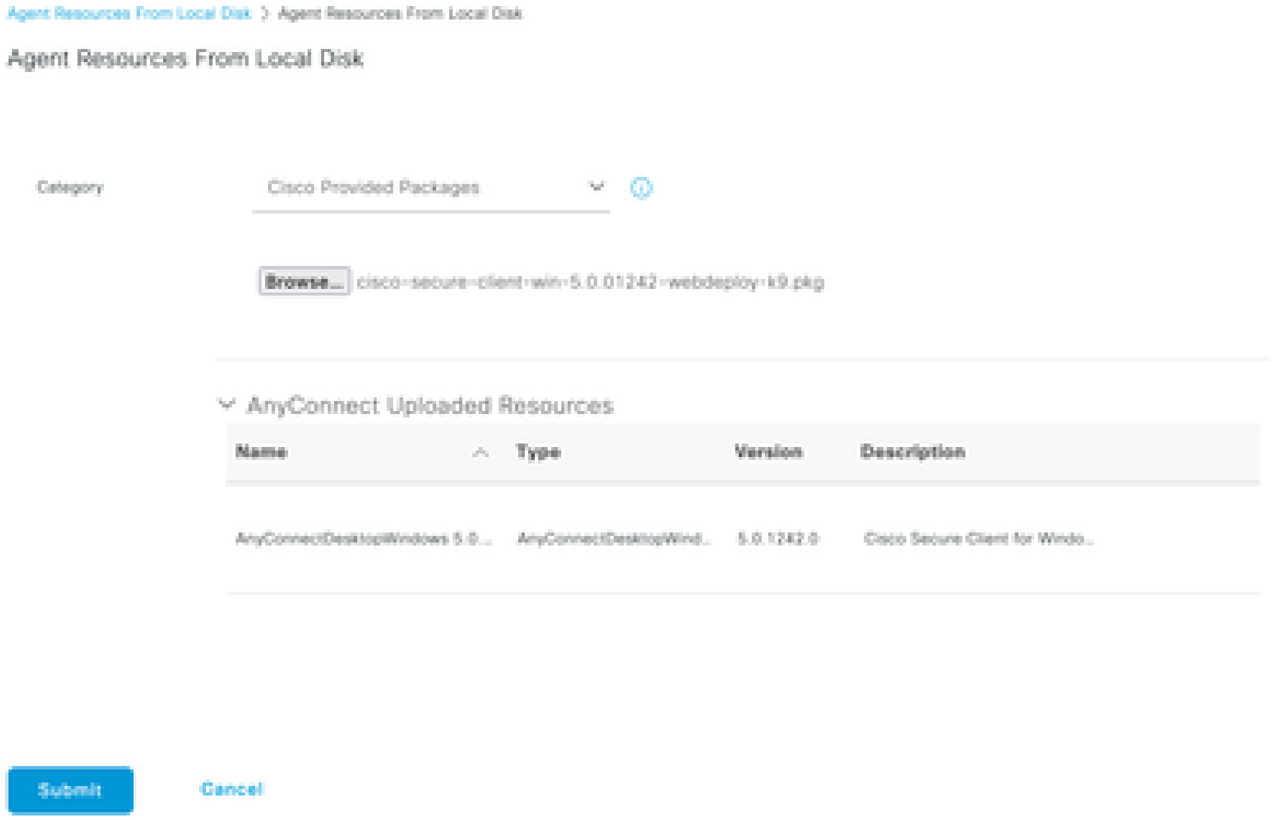


AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

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. cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg Advisories	30-Jan-2023	19.59 MB

ISE Compliance Module Webdeploy Package

3. On ISE, navigate to **Work Centers** > **Posture** > **Client Provisioning** > **Resources** and click **Add** > **Agent resources from local disk**. Select **Cisco Provided Packages** from the Category drop down menu and upload the **Cisco Secure Client Headend Deployment Package** previously downloaded. Repeat the same process to upload the Compliance Module.


Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

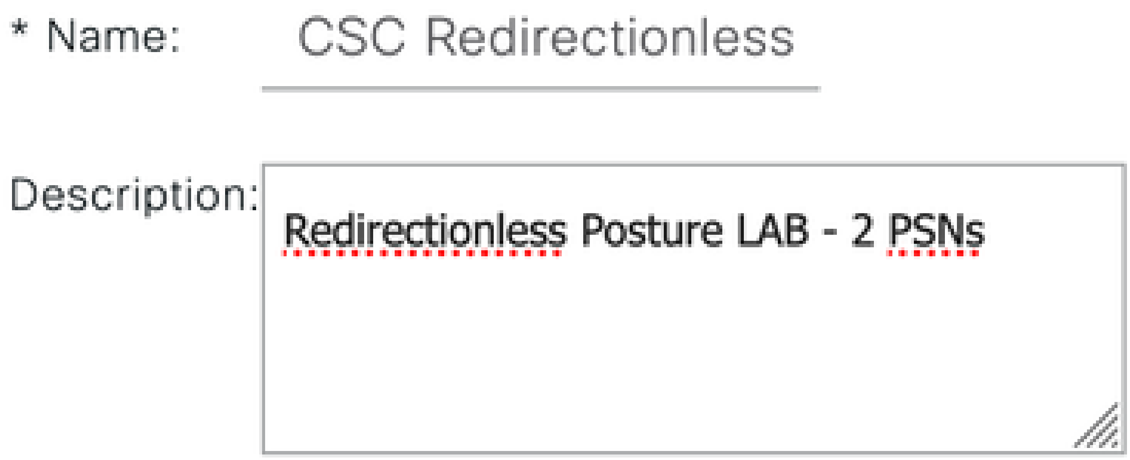
cisco-secure-client-win-5.0.01242-webdeploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 5.0...	AnyConnectDesktopWind...	5.0.1242.0	Cisco Secure Client for Windo...

Upload Cisco Provided Packages to ISE

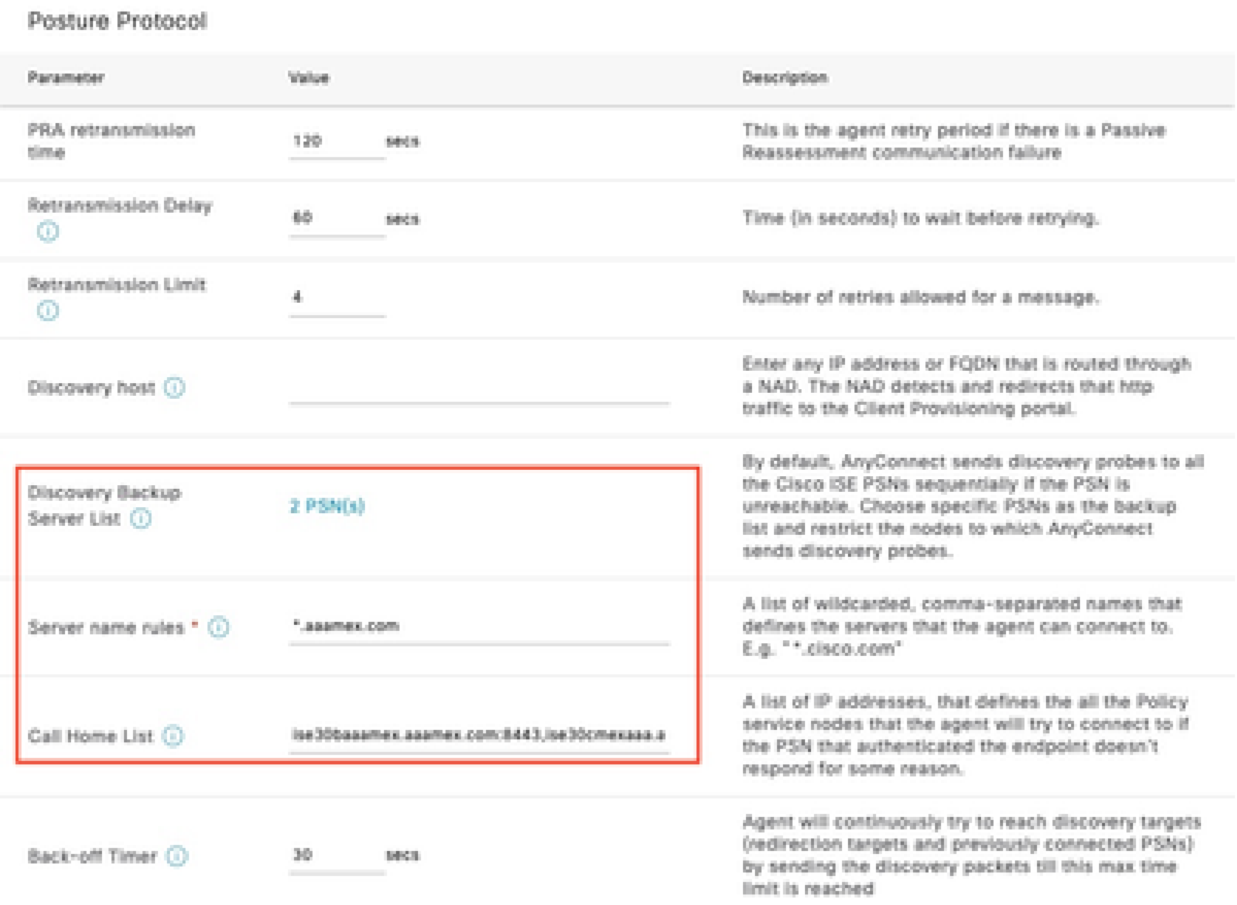
4. Back in the **Resources** tab, click **Add** > **Agent Posture Profile**. On the profile:
    - Configure a **name** that can be used to identify the profile and the Call Home List within ISE.
    - Make sure that **Enable extra probes so non-redirection flow can work** is set to **Yes**.
    - Configure **Discovery Backup Server List**. Select the **PSNs** that match the Call Home List that is being configured.
      This is the list of PSNs that are saved in ConnectionData.xml after the first connection.
    - Configure the **Server name rules** separated by commas**.** Choose one of the these configurations:
        - A single asterisk * to allow connection to any PSN.
        - Wildcard values (for example, *.aaamex.com) to allow connection to any PSN in specific domains.
        - List of PSN FQDNs, comma-separated, to restrict the connection to specific PSNs. If used, this list must match the Call Home List.
    - Configure **Call Home List** to specify the comma-separated list of PSNs. Make sure to add the Client Provisioning Portal port using the format FQDN:port or IP:port.
      To find or modify the CPP port, navigate to **Work Centers > Posture > Client Provisioning > Client Provisioning Portal**, select the **portal** in use, expand **Portal Settings** and look for **HTTPs port**.



* Name: CSC Redirectionless

Description: Redirectionless Posture LAB - 2 PSNs

Agent Posture Profile Configuration



Posture Protocol

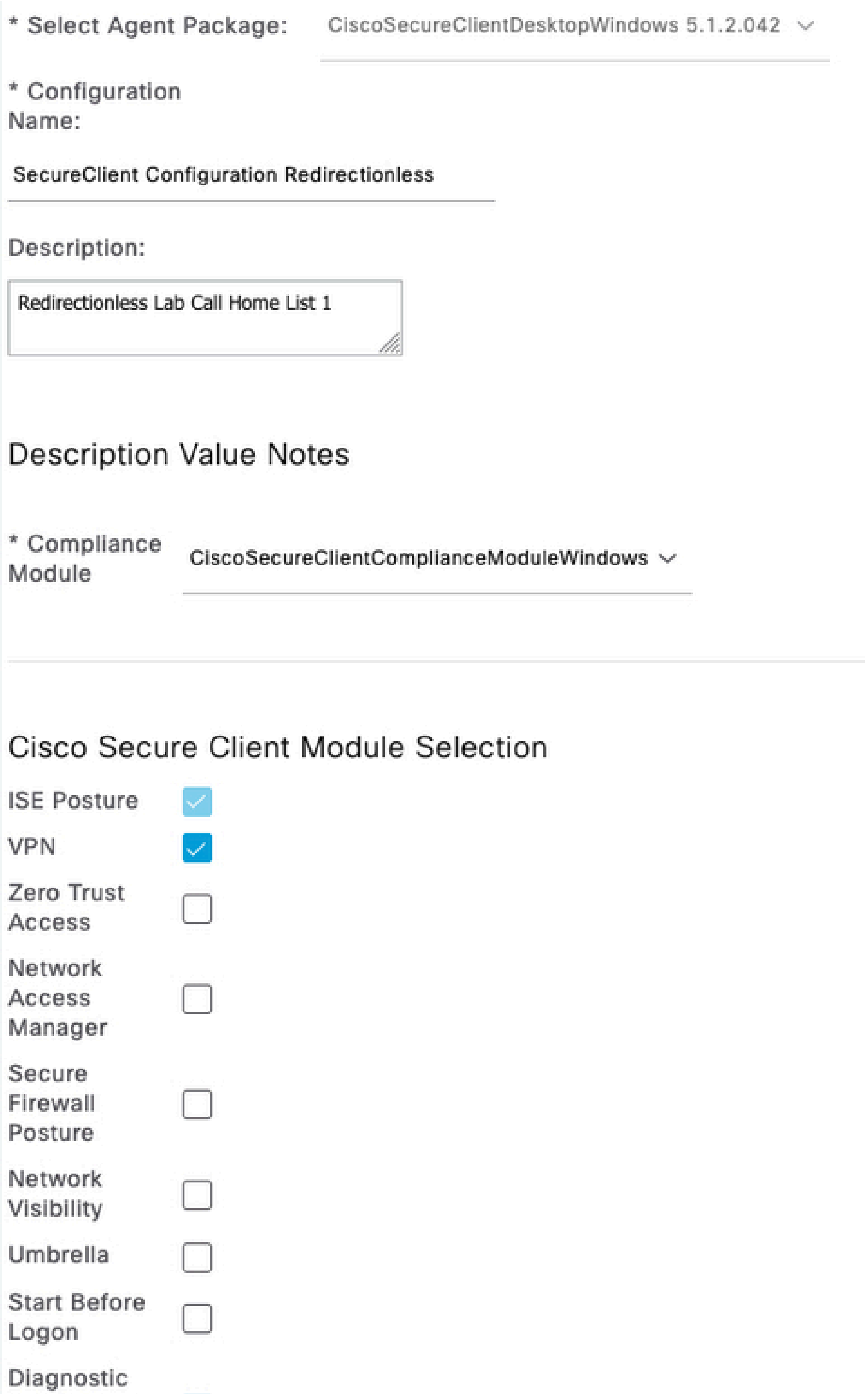
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		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.
Discovery Backup Server List ⓘ	2 PSN(s)	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*.aaamex.com	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List ⓘ	ise30baaamex.aaamex.com:8443,ise30cmexaaa.a	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 secs	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

Posture Protocol Configuration in Agent Posture Profile

5. Back in the **Resources** tab, click **Add > Agent Configuration**. Select the **Cisco Secure Client package** and **Compliance Module** to be used.

> **Warning**: If Cisco Secure Client has been pre deployed to the clients, make sure that the version on ISE matches the version on the endpoints. If ASA or FTD is used for web deploy, the version on this device can match as well.

6. Scroll down to the **Posture Selection** section and select the **profile** that was created on step 1. Click **Submit** at the bottom of the page to save the configuration.



* 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 □

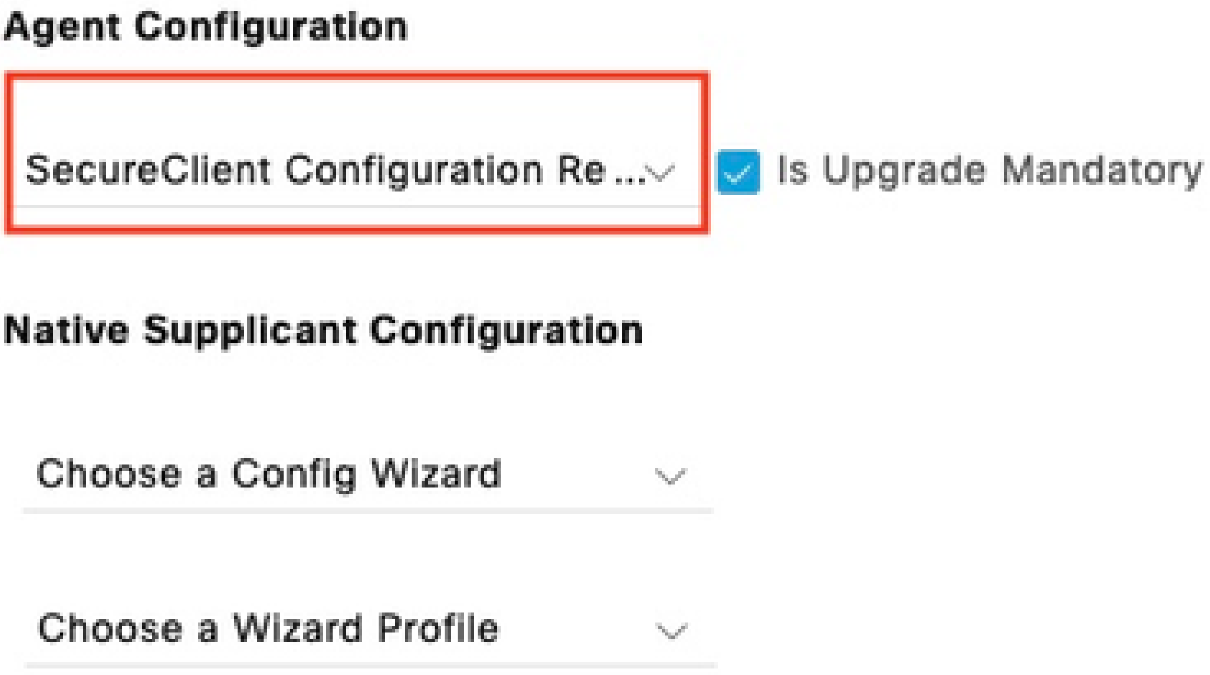
Start Before Logon □

Diagnostic

7. Navigate to **Work Centers > Posture > Client Provisioning > Client provisioning policy**. Locate the policy that is used for the required Operating System and click **Edit**. Click the +sign on the **Results** column and select the **agent configuration** from step 5 under the **Agent Configuration** section. Click **Save** at the bottom of the page**.**

Note: In the case of multiple Call Home Lists, use the **Other Conditions** field to push the right profile to the corresponding clients. In this example, Device Location Group is used to identify the posture profile that is pushed in the policy.

Tip: If multiple client provisioning policies are configured for the same OS, it is recommended to make them mutually exclusive, that is, a given client can only be able to hit one policy at a time. RADIUS attributes can be used under **Other Conditions** column to differentiate one policy from another.



Agent Configuration

SecureClient Configuration Re ...

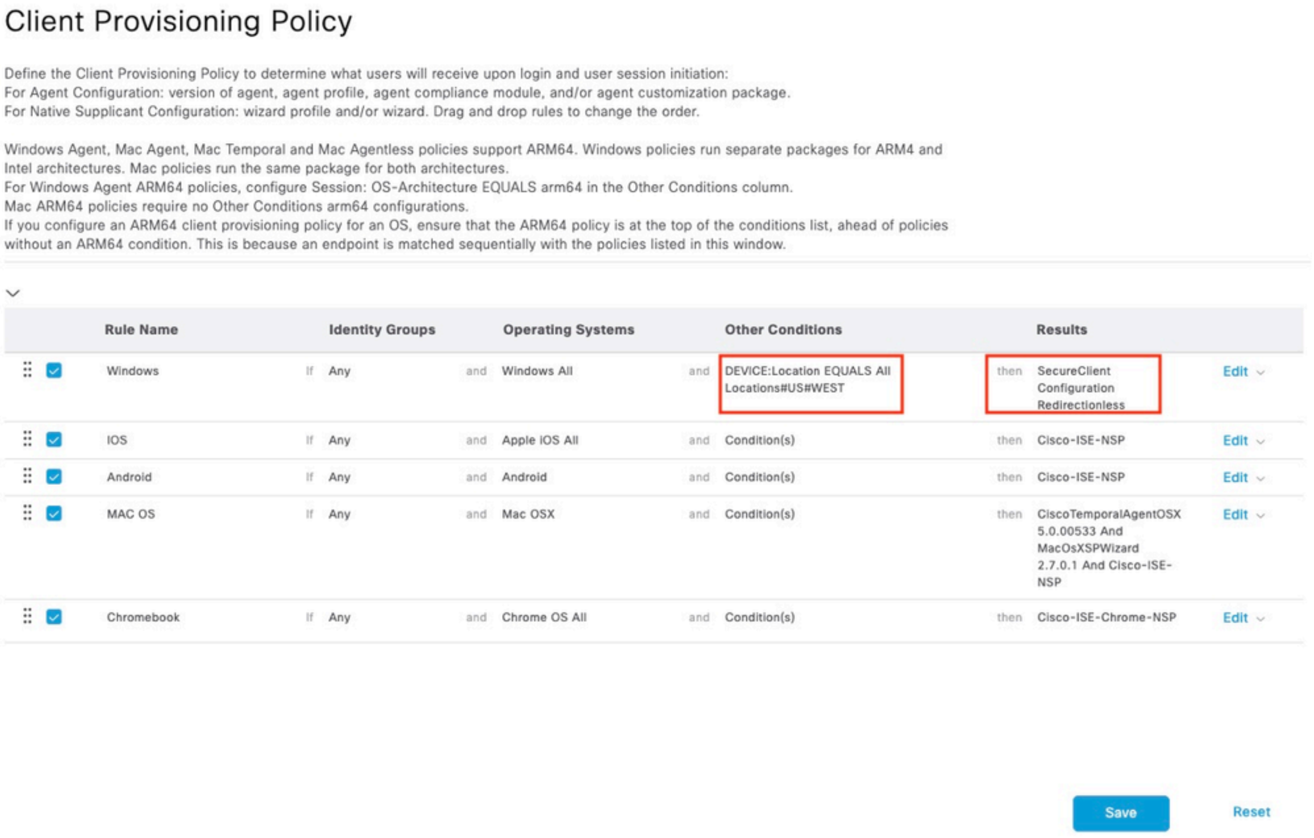
☑ Is Upgrade Mandatory

Native Supplicant Configuration

Choose a Config Wizard

Choose a Wizard Profile

Agent Configuration in Client Provisioning Policy



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.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

		Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
⠿	☑	Windows	If	Any	and	Windows All	and	DEVICE:Location EQUALS All Locations#US#WEST	then	SecureClient Configuration Redirectionless	Edit ⌄
⠿	☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit ⌄
⠿	☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit ⌄
⠿	☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	CiscoTemporalAgentOSX 5.0.00533 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP	Edit ⌄
⠿	☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	Cisco-ISE-Chrome-NSP	Edit ⌄

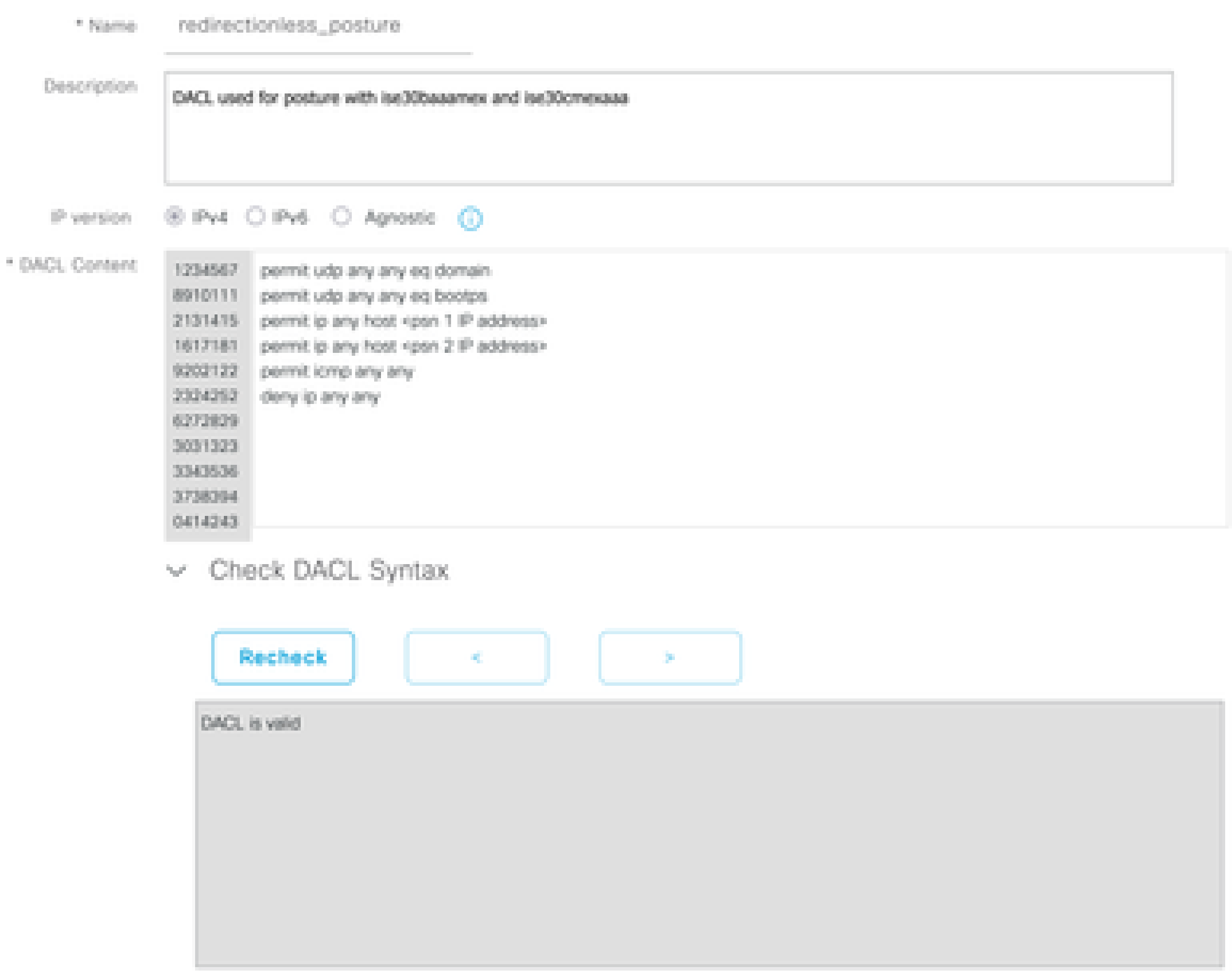
Client Provisioning Policy

8. Repeat steps 4 to 7 for each Call Home List and corresponding posture profile in use. For hybrid environments, the same profiles can be used for redirection clients.

Authorization

Authorization Profile

1. Navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** and click **Add**.
2. Create a **DACL** to allow traffic to DNS, DHCP (if used), ISE PSNs and block other traffic. Make sure to allow any other traffic that is necessary to access before final compliant access.



* Name: redirectionless_posture

Description: DACL used for posture with ise30baaamex and ise30cmexaaa

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit udp any any eq domain
permit udp any any eq bootps
permit ip any host <psn 1 IP address>
permit ip any host <psn 2 IP address>
permit icmp any any
deny ip any any
```

Check DACL Syntax

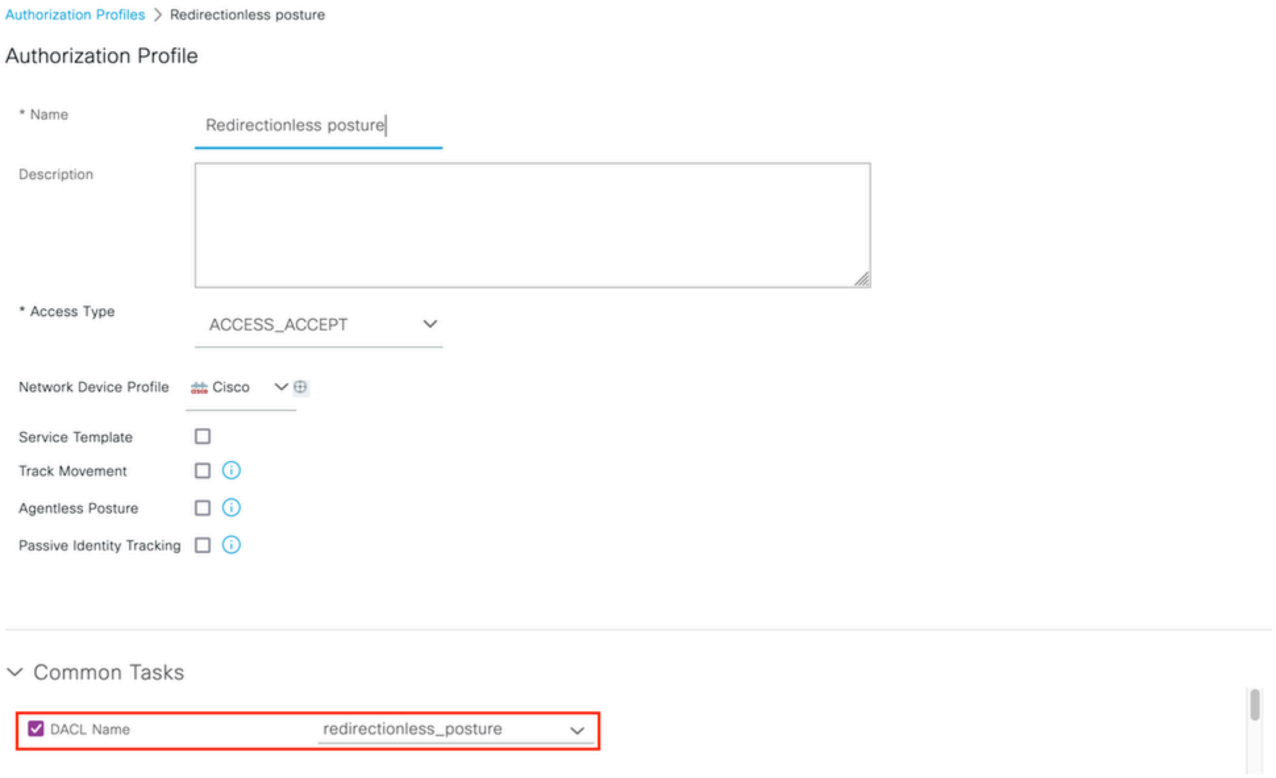
DACL is valid

DACL Configuration

```
permit udp any any eq domain
permit udp any any eq bootps
permit ip any host <PSN 1>
permit ip any host <PSN 2>
deny ip any any
```

⚠ **Caution**: Some third party devices cannot support DACLs, in such cases it is necessary to use a Filter-ID or other vendor specific attributes. Refer to the vendor documentation for more information. If DACLs are not used, make sure to configure the corresponding ACL in the network device.

3. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization profiles** and click **Add**. Give a name to the authorization profile and select **DACL name** from **Common Tasks**. From the drop down menu, select the **DACL** created in step 2.



Authorization Profiles > Redirectionless posture

Authorization Profile

* Name: Redirectionless posture

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Common Tasks

☑ DACL Name: redirectionless_posture

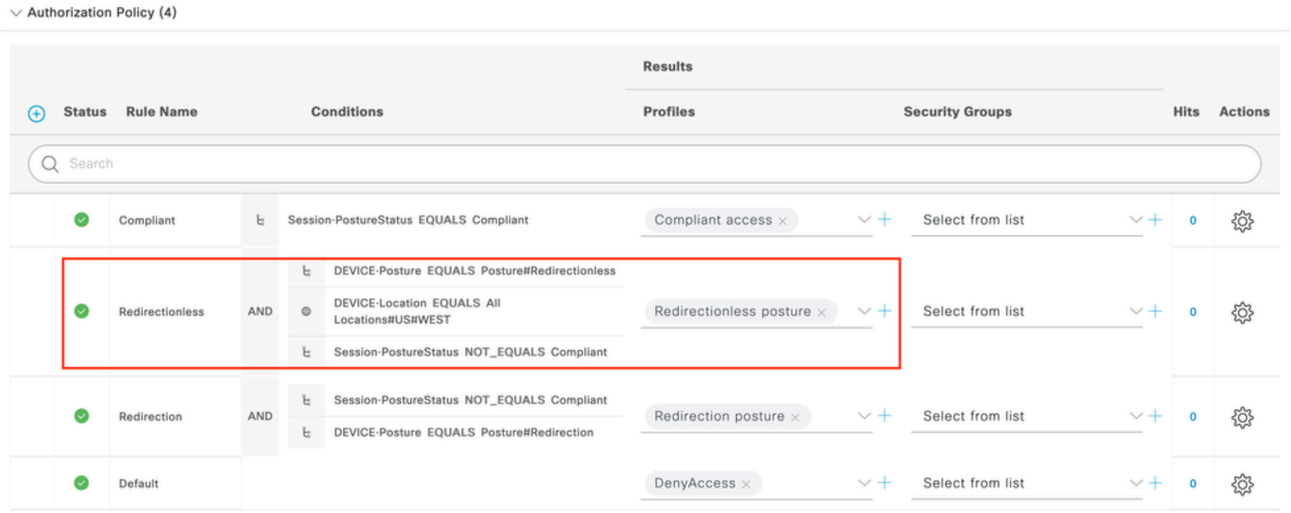
Authorization Profile

Note: If DACLs are not used, use **Filter-ID** from **Common Tasks** or the **Advanced Attribute Settings** to push the corresponding ACL name.

4. Repeat steps 1 to 3 for each Call Home List in use. For hybrid environments, only a single authorization profile for redirection is necessary. The configuration of the authorization profile for redirection is out of the scope of this document.

Authorization Policy

1. Navigate to **Policy > Policy Sets** and open the **policy set** in use or **create** a new one.
2. Scroll down to **Authorization Policy** section. Create an authorization policy using **Session PostureStatus NOT_EQUALS Compliant** and select the **authorization profile** created in the previous section.



Authorization Policy (4)

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

Authorization policies

3. Repeat step 2 for each Authorization Profile with their corresponding Call Home List in use. For hybrid environments, only a single authorization policy for redirection is necessary.

Troubleshoot

Compliant on Cisco Secure Client and Posture Not Applicable (Pending) on ISE

Stale/Phantom Sessions

The presence of stale or phantom sessions in the deployment can generate intermittent and apparently random failures with redirectionless posture discovery which result in users being stuck in a posture unknown/not applicable access on ISE while Cisco Secure Client UI shows Compliant access.

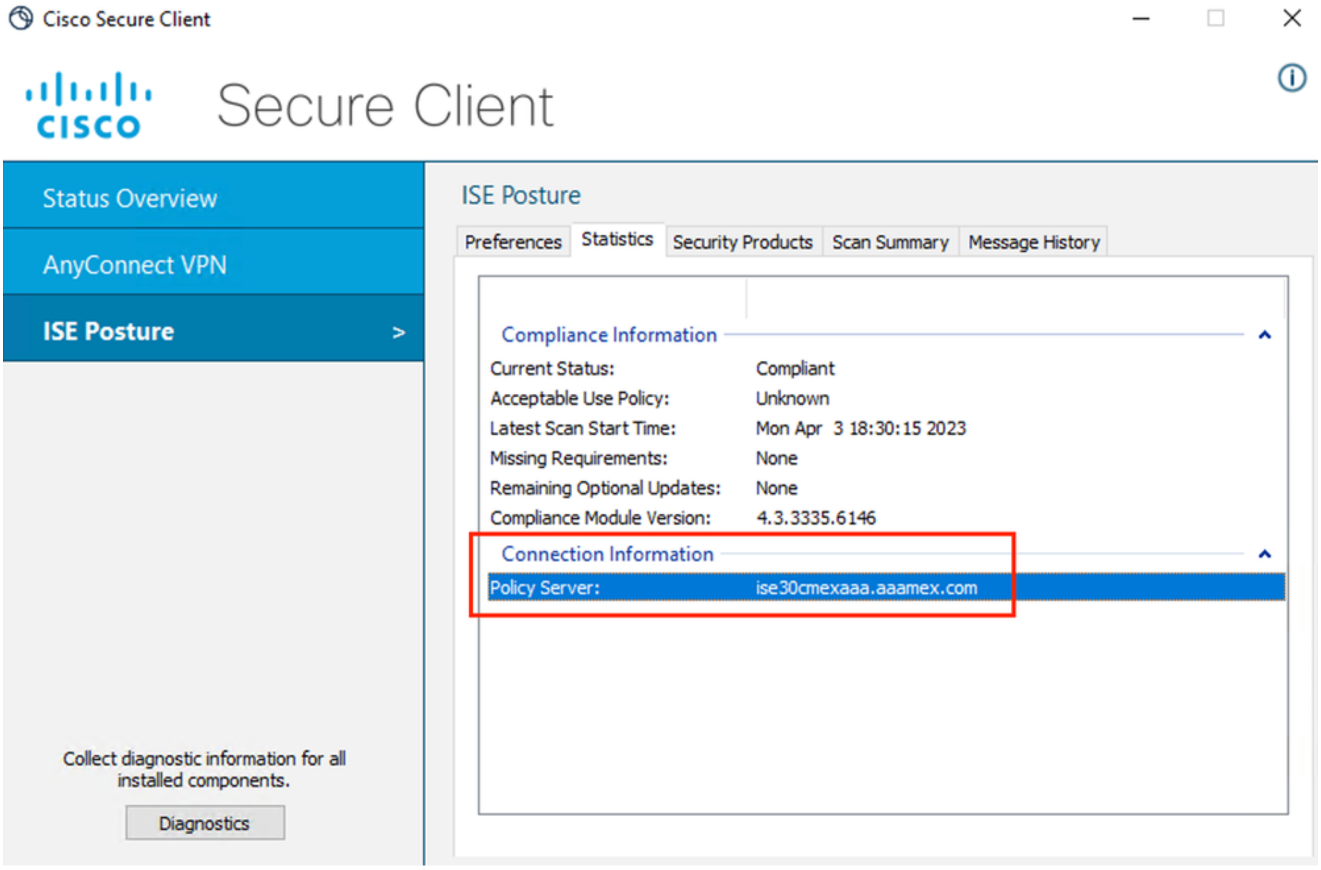
Stale sessions are old sessions that are no longer active. They are created by an authentication request and accounting start, but no accounting stop is received on the PSN to clear the session.

Phantom sessions are sessions that were never actually active in a particular PSN. They are created by an accounting interim update, but no accounting stop is received on the PSN to clear the session.

Identify

To identify a stale/phantom session issue, verify the PSN used in system scan on the client and compare with the PSN performing the authentication:

1. In Cisco Secure Client UI, click the **gear icon** at the bottom left corner. From the left menu, open **ISE Posture** section and navigate to **Statistics** tab. Take note of the Policy Server in Connection Information.



Cisco Secure Client

Secure Client

- Status Overview
- AnyConnect VPN
- ISE Posture >

Collect diagnostic information for all installed components.

Diagnostics

ISE Posture

Preferences | Statistics | Security Products | Scan Summary | Message History

Compliance Information

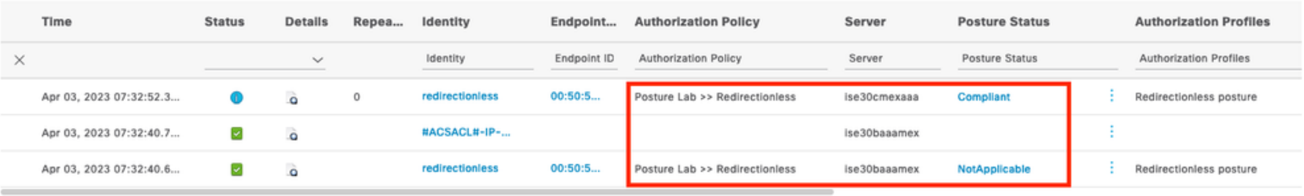
Current Status:	Compliant
Acceptable Use Policy:	Unknown
Latest Scan Start Time:	Mon Apr 3 18:30:15 2023
Missing Requirements:	None
Remaining Optional Updates:	None
Compliance Module Version:	4.3.3335.6146

Connection Information

Policy Server:	ise30cmexaaa.aaamex.com

Policy Server for ISE Posture in Cisco Secure Client

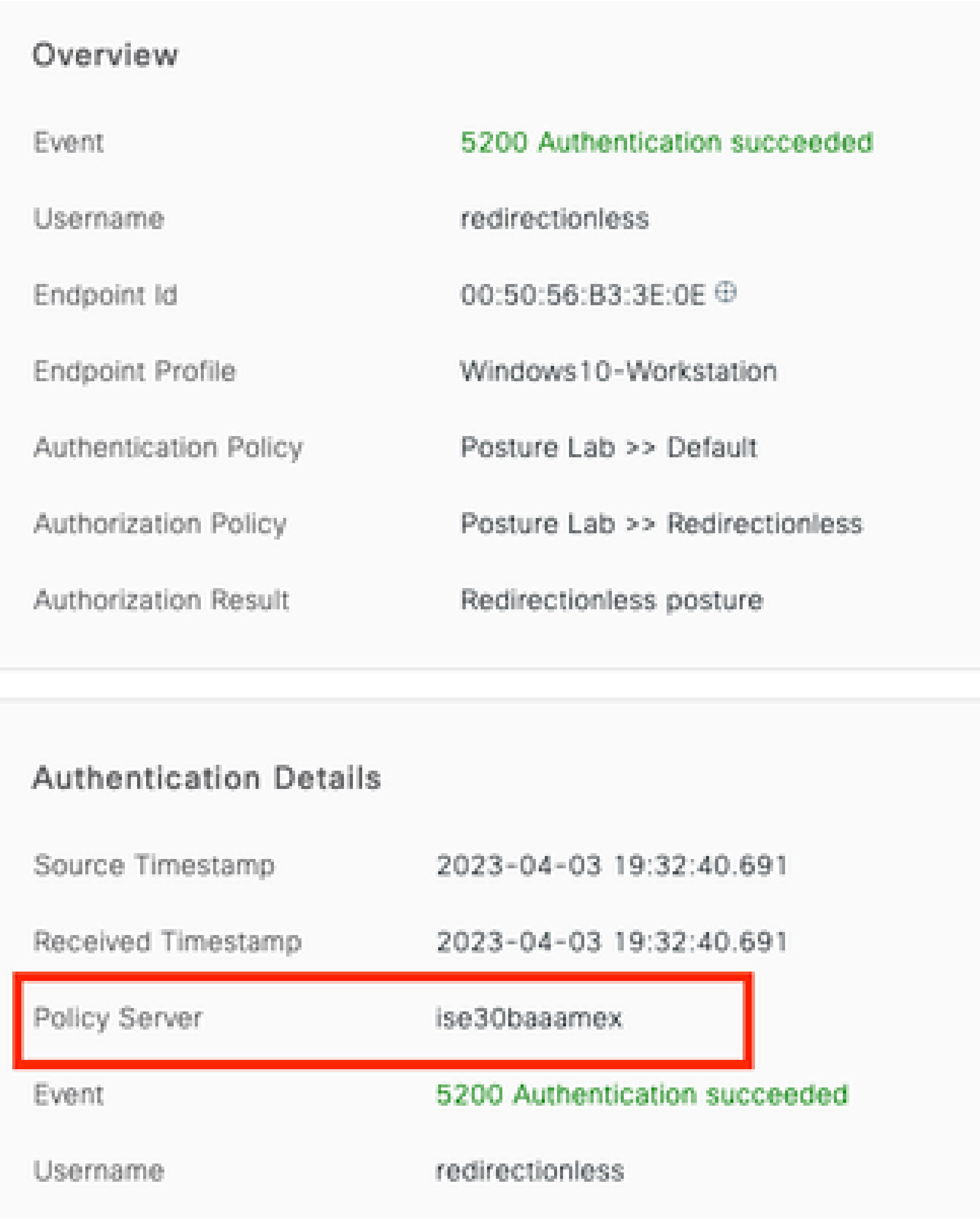
2. In ISE RADIUS live logs take note of these:
   - Change in Posture Status
   - Change in Server
   - No change in Authorization Policy and Authorization Profile
   - No CoA live log



Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
×				Identity	Endpoint ID	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

Live logs for stale/phantom session

3. Open the **live session** or the **last authentication live log details**. Take note of the Policy Server, if it differs from the server observed on step 1, this indicates an issue with stale/phantom sessions.



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

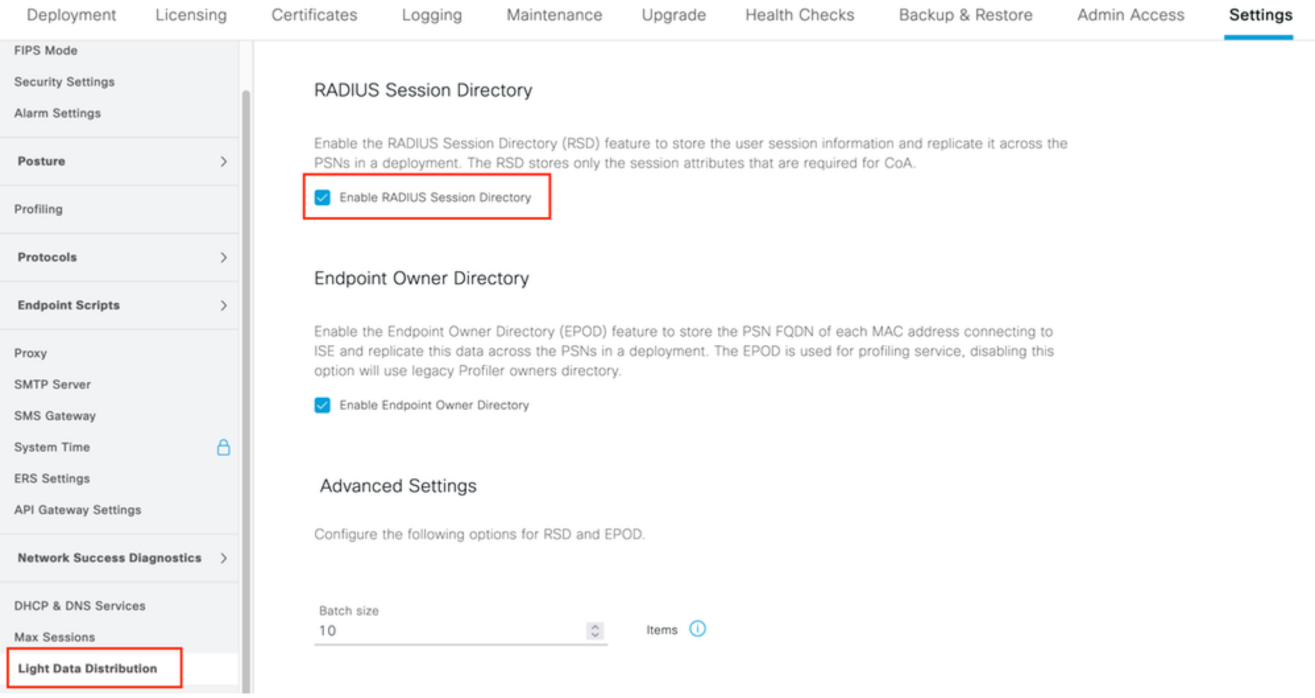
Policy server in live log details

Solution

ISE versions after ISE 2.6 patch 6 and 2.7 patch 3 implement RADIUS Session Directory as a solution for stale/phantom session scenario in re-directionless posture flow.

1. Navigate to **Administration** > **System** > **Settings** > **Light Data Distribution** and verify that **Enable**

RADIUS Session Directory checkbox is enabled.



RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

☑ Enable RADIUS Session Directory

Endpoint Owner Directory

Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address connecting to ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling service, disabling this option will use legacy Profiler owners directory.

☑ Enable Endpoint Owner Directory

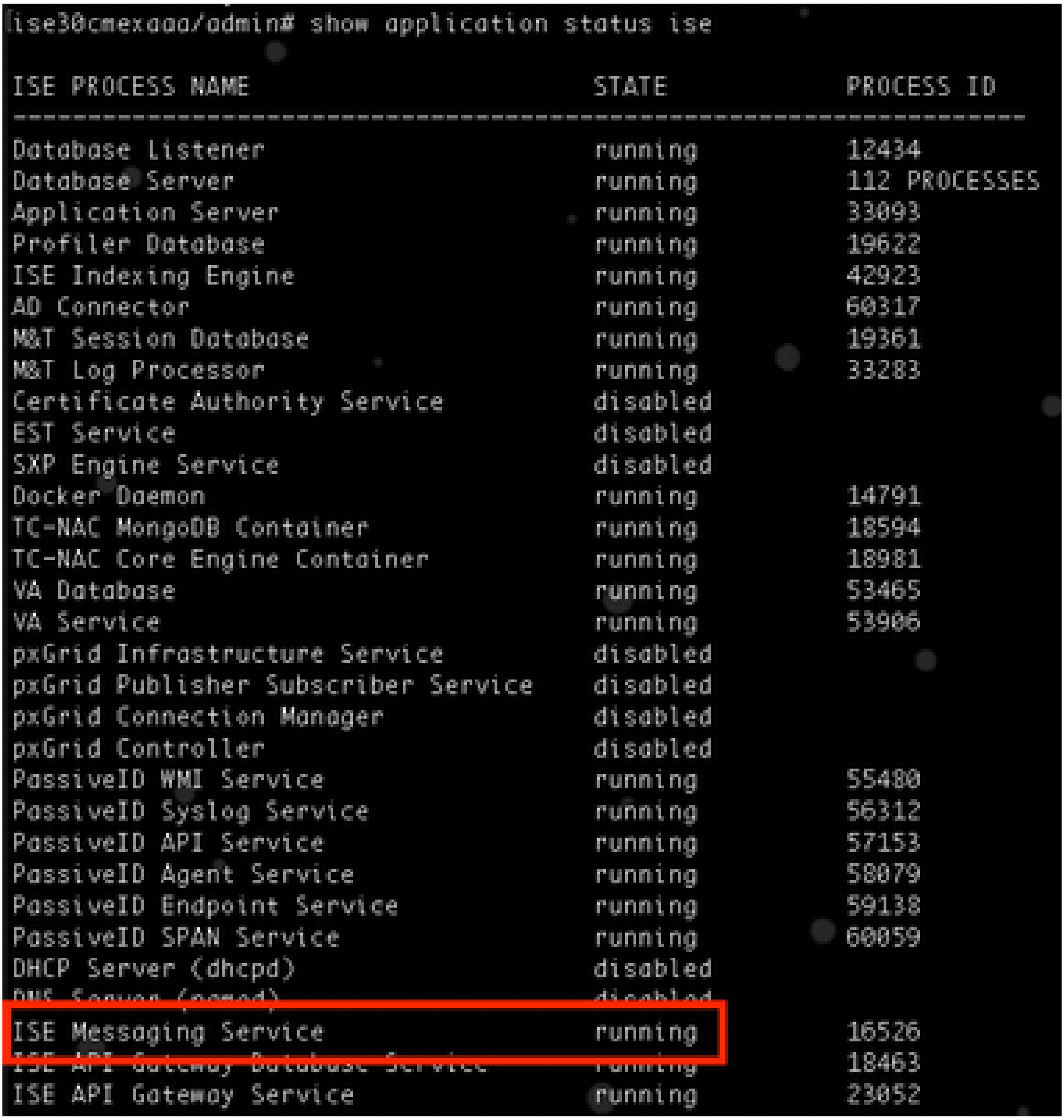
Advanced Settings

Configure the following options for RSD and EPOD.

Batch size 10 Items

Enable RADIUS Session Directory

2. From ISE CLI, verify that **ISE Messaging Service** is running on **all PSNs** by running the command **show applications status ise**.



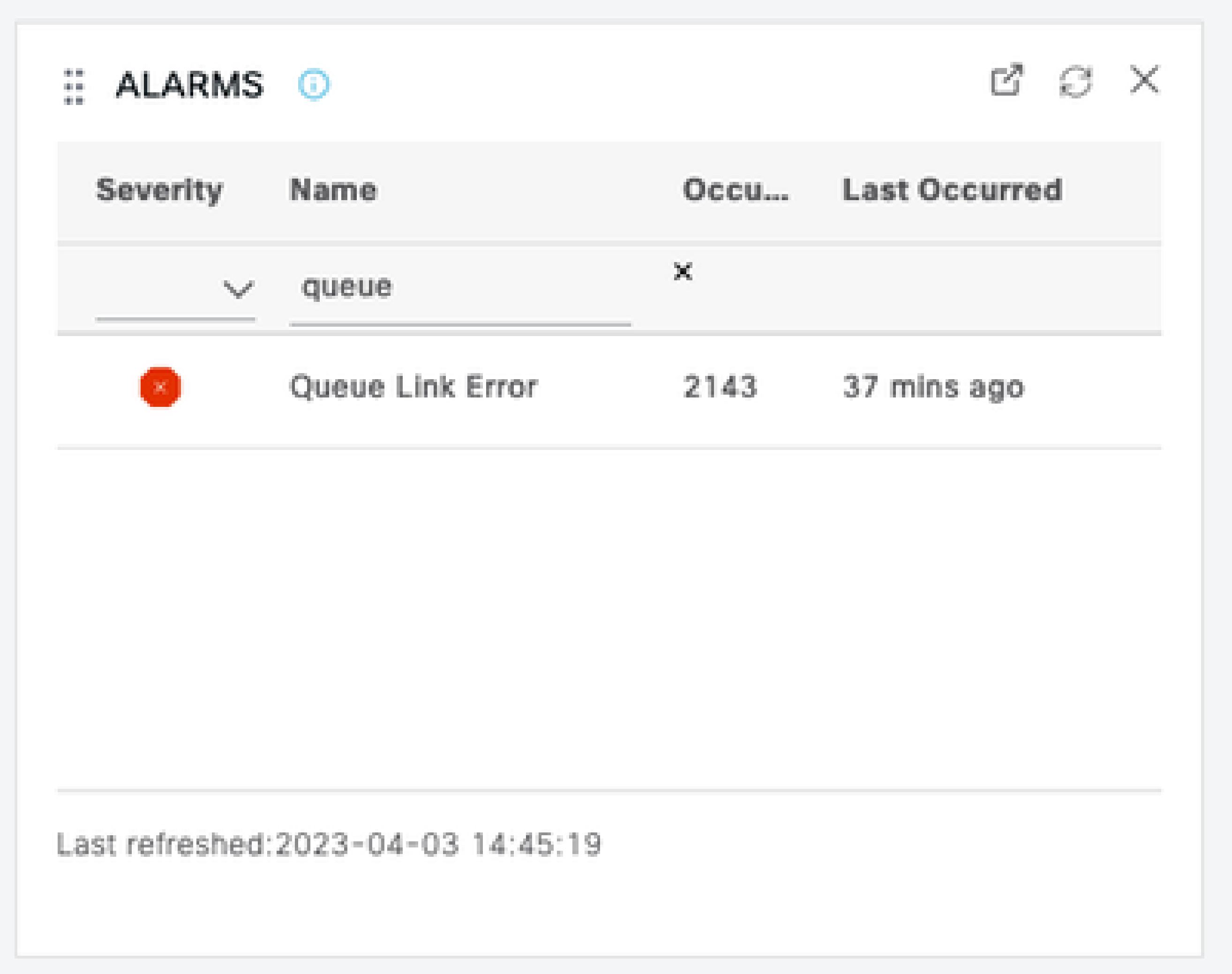
```
ise30cmexaaa/admin# show application status ise

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 Messaging Service running

Note: This service refers to the communication method that is used for RSD between PSNs and can be running regardless of the status of the ISE Messaging Service setting for syslog that can be set from ISE UI.

3. Navigate to ISE **Dashboard** and locate the **Alarms** dashlet. Verify if there are any **Queue Link Error** alarms. Click the **name** of the alarm to see more details.



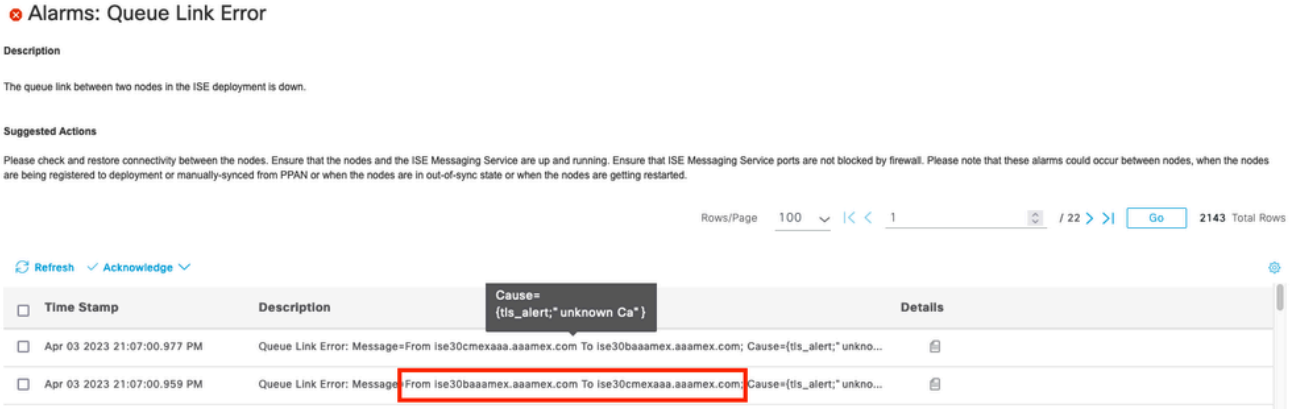
ALARMS

Severity	Name	Occu...	Last Occurred
	queue		
✖	Queue Link Error	2143	37 mins ago

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

Queue Link Error alarms

4. Verify if the alarms are generated between the PSNs used for posture.



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 PPAN or when the nodes are in out-of-sync state or when the nodes are getting restarted.

Cause=
{tls_alert;" unknown Ca" }

☐ Time Stamp	Description	Details
☐ Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From ise30cmexaaa.aaamex.com To ise30baaamex.aaamex.com; Cause={tls_alert;" unkno...	
☐ Apr 03 2023 21:07:00.959 PM	Queue Link Error: Message=From ise30baaamex.aaamex.com To ise30cmexaaa.aaamex.com; Cause={tls_alert;" unkno...	

Queue Link Error alarm details

5. Hover over the alarm description to see the full details and take note of the Cause field. The two most common causes for queue link error are:
   - Time out: indicates that the requests sent by a node to another node on port 8671 are not responded to within the threshold. To remediate, verify that TCP port 8671 is allowed between the nodes.
   - Unknown CA: indicates the certificate chain signing the ISE Messaging certificate is not valid or incomplete. To remediate this error:
     a. Navigate to **Administration** > **System** > **Certificates** > **Certificate signing requests**.

b. Click **Generate Certificate Signing Requests (CSR)**.
c. From the drop down menu select **ISE Root CA** and click **Replace ISE Root CA Certificate chain**.
If ISE Root CA is not available, navigate to **Certificate Authority > Internal CA settings** and click **Enable Certificate Authority**, then go back to the CSR and regenerate the Root CA.
d. Generate a new CSR and select **ISE Messaging Service** from the drop down menu.
e. Select all the nodes from the deployment and regenerate the certificate.

Note: It is expected to observe Queue Link Error alarms with cause Unknown CA or Econnrefused while the certificates are regenerated. Monitor the alarms after certificate generation to confirm that the issue is resolved.

Performance

Identify

Performance issues such as high CPU utilization and high load average related to redirectionless posture can impact PSN as well as MnT nodes and are often accompanied or preceded by these events:

- Random or intermittent, No policy server detected errors, in Cisco Secure Client.
- Maximum resource limit reached reports for Portal service thread pool reached threshold value events. Navigate to **Operations > Reports > Reports > Audit > Operations Audit** to see the reports.
- Posture Query to MNT lookup is high alarms. These alarms are only generated on ISE 3.1 and later versions.

Solution

If performance of the deployment is impacted by redirectionless posture, this is often indicative of an ineffective implementation. It is recommended to revise these aspects:

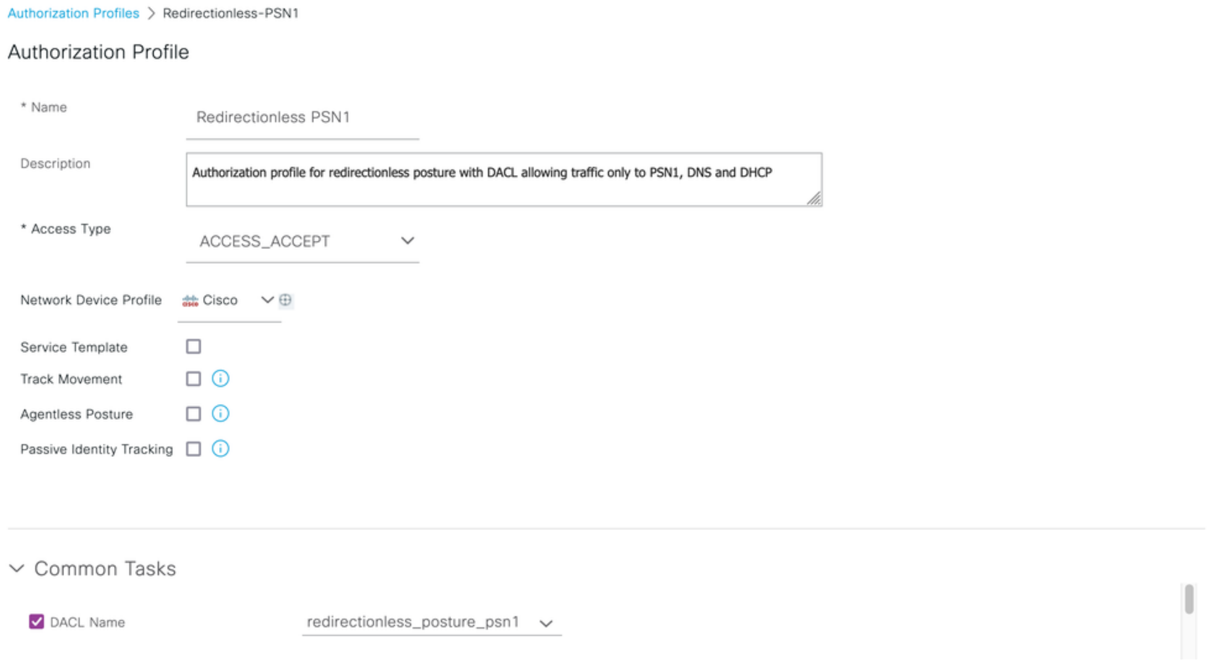
- Number of PSNs used per Call Home List. Consider reducing the number of PSNs that can be used for posture per endpoint or network device according to the design.
- Client provisioning portal port in Call Home List. Make sure that the portal port number is included after the IP or FQDN of each node.

To mitigate the impact:

1. Clear connectiondata.xml from the endpoints by removing the **file** from the **Cisco Secure Client folder** and restart the **ISE Posture service** or **Cisco Secure Client**. If the services are not restarted, the old file is regenerated and the changes do not take effect. This action can also be performed after revising and modifying the Call Home lists.
2. Use DACLs or other ACLs to block traffic to ISE PSNs for network connections where it is not relevant:

    - For connections where posture is not enforced in the authorization policies, but that apply to endpoints with Cisco Secure Client ISE Posture module installed, block traffic from the clients to all ISE PSNs for TCP ports 8905 and Client Provisioning Portal port. This action is recommended for posture with redirection implementation as well.
    - For connections where posture is enforced in the authorization policies, allow traffic from the clients to the authenticating PSN and block traffic to other PSNs in the deployment. This action

can be implemented temporarily while the design is revised.



Authorization Profiles > Redirectionless-PSN1

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 □

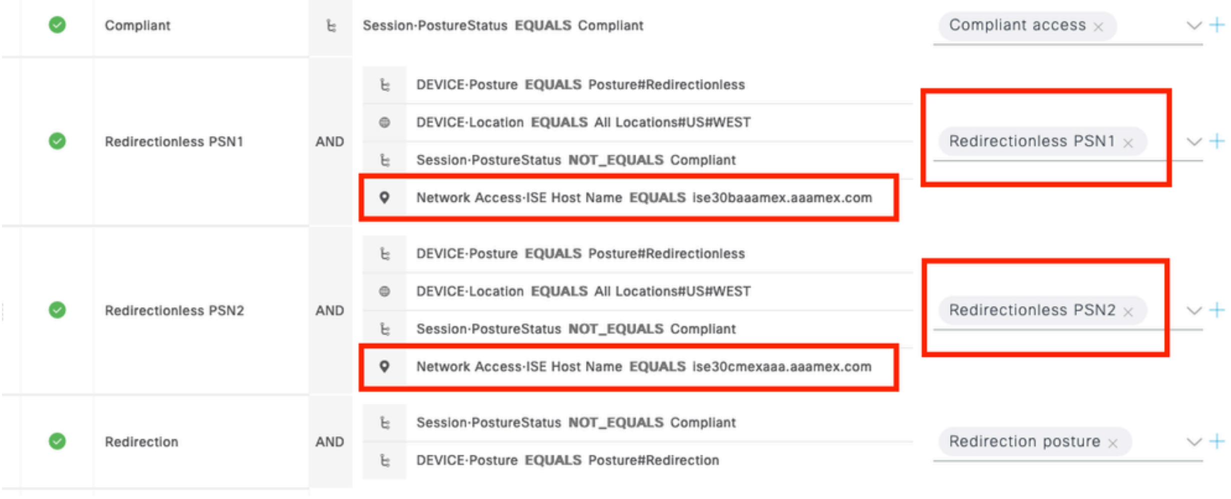
Agentless Posture □

Passive Identity Tracking □

Common Tasks

☑ DACL Name: redirectionless_posture_psn1

Authorization profile with DACL for single PSN



✓	Compliant		Session·PostureStatus EQUALS Compliant	Compliant access
✓	Redirectionless PSN1	AND	DEVICE·Posture EQUALS Posture#Redirectionless DEVICE·Location EQUALS All Locations#US#WEST Session·PostureStatus NOT_EQUALS Compliant Network Access·ISE Host Name EQUALS ise30baaamex.aaamex.com	Redirectionless PSN1
✓	Redirectionless PSN2	AND	DEVICE·Posture EQUALS Posture#Redirectionless DEVICE·Location EQUALS All Locations#US#WEST Session·PostureStatus NOT_EQUALS Compliant Network Access·ISE Host Name EQUALS ise30cmexaaa.aaamex.com	Redirectionless PSN2
✓	Redirection	AND	Session·PostureStatus NOT_EQUALS Compliant DEVICE·Posture EQUALS Posture#Redirection	Redirection posture

Authorization policies per PSN

Accounting

RADIUS accounting is essential for session management on ISE. Since posture relies on an active session to be performed, incorrect or lack of accounting configuration can also impact posture discovery and ISE performance. It is important to verify that accounting is correctly configured on the network device to send authentications requests, accounting start, accounting stop and accounting updates to a single PSN for each session.

To verify accounting packets received on ISE, navigate to **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **RADIUS Accounting.**

Related Information

- [Cisco Technical Support & Downloads]()