

# Assess Endpoint Compliance Using Cisco Secure Client ISE Posture Module and Cisco Secure Firewall Management Center

---

**First Published:** 2023-07-27

**Last Modified:** 2023-08-01

## Assess Endpoint Compliance Using Cisco Secure Client ISE Posture Module and Cisco Secure Firewall Management Center

### Introduction

Cisco Secure Client's ISE Posture module helps you to assess endpoint compliance before allowing them to connect to your network. The assessment can be for a specific version of an antivirus, an antispysware, a file, a registry key, and so on. During posture evaluation, all clients connecting to your network must meet the mandatory requirements to be compliant.

The ISE Posture module performs a client-side evaluation. The client receives the posture requirement policy from ISE, performs the posture data collection, compares the results against the policy, and sends the assessment results back to the ISE. The posture service classifies the posture states as unknown, compliant, and noncompliant.

#### Benefits

Using a threat defense to configure ISE Posture modules offers significant benefits such as:

- Easily distribute and manage the ISE posture modules and profiles on each endpoint.
- Easily assess endpoint compliance before they connect to the corporate network.

### Is this Guide for You?

This use case is primarily intended for network administrators who use the management center to configure the ISE Posture module for endpoint compliance assessment.

### System Requirements

The following table shows the supported platforms for this feature.

Product	Version	Version used in this document
Cisco Secure Firewall Threat Defense (formerly Firepower Threat Defense/FTD)	6.3 and later	7.3
Cisco Secure Firewall Management Center (formerly Firepower Management Center/FMC)	6.7 and later	7.3
Cisco Secure Client (formerly AnyConnect)	4.0 and later	5.0
Cisco ISE	2.0 and later	3.1

## Prerequisites

Ensure that you have:

- Access to a Cisco ISE server with admin privileges.
- Downloaded the Secure Client package and the Secure Client profile editor from [Cisco Software Download Center](#) to your local host.
- Installed the Secure Client profile editor to your local host.
- Downloaded the ISE Compliance Module from [Cisco Software Download Center](#) to your local host.
- Configured ISE server details in the managed threat defense. See [Configure ISE in the Management Center](#).
- Configured a remote access VPN in the management center.

### Licenses

- ISE Premier license.
- One of the following Secure Client licenses:  
Secure Client Premier, Secure Client Advantage, or Secure Client VPN Only.
- Management center Essentials (formerly Base) license must allow export-controlled functionality.  
Choose **System** > **Licenses** > **Smart Licenses** to verify this functionality in the management center.

## Configure ISE in the Management Center

You must configure the ISE server in the management center to:

- Allow AAA requests from the threat defense for remote access VPN.
- Receive the posture requirement policy from ISE.
- Send the assessment results to ISE.

You must create a RADIUS Server object and configure it with the ISE server details.

## Procedure

**Step 1** Choose **Objects > Object Management > AAA Server > RADIUS Server Group**.

**Step 2** Click **Add RADIUS Server Group**.

**Step 3** Enter a name and a retry interval.

Name:\*  
ISE

Description:

Group Accounting Mode:  
Single

Retry Interval:\* (1-10) Seconds  
10

Realms:

Enable authorize only

Enable interim account update

Interval:\* (1-120) hours  
24

Enable dynamic authorization

Port:\* (1024-65535)  
1700

RADIUS Servers (Maximum 16 servers) +

IP Address/Hostname	

**Step 4** Configure the port as 1700.

**Step 5** Click + to add the ISE server.

**Step 6** Enter the IP address of the ISE server.

**Step 7** Leave the **Authentication Port** as 1812.

**Step 8** Configure the key.

Enter the shared secret to encrypt data between the managed device (client) and the ISE server.

**Step 9** Enter the key again in the **Confirm Key** field.

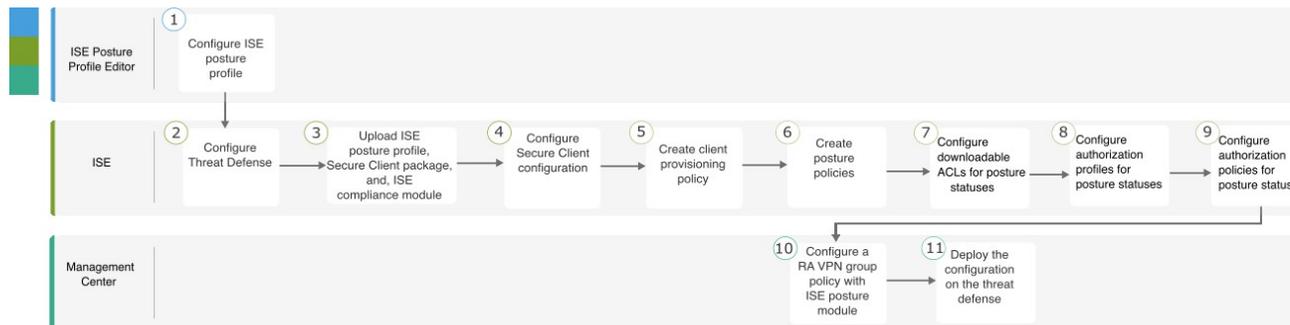
You need this key when you add the threat defense in ISE.

**Step 10** Use the default values for the remaining parameters.

**Step 11** Click **Save**.

## End-to-End Process for Configuring ISE Posture Module Using Management Center

The following flowchart illustrates the workflow for configuring Secure Client ISE posture module using management center.



Step	Application	Description
1	ISE Posture Profile Editor	Configure the Posture Profile using the ISE Posture Profile Editor, on page 5
2	ISE	Configure Threat Defense in ISE, on page 6
3	ISE	Upload ISE Posture Profile, Secure Client Package, and ISE Compliance Module to ISE, on page 6
4	ISE	Configure a Secure Client Configuration in ISE, on page 8
5	ISE	Create a Client Provisioning Policy in ISE, on page 9
6	ISE	Configure Posture Policy in ISE, on page 10
7	ISE	Configure Downloadable ACLs for the Posture Statuses in ISE, on page 12
8	ISE	Configure Authorization Profiles for the Posture Statuses in ISE, on page 13
9	ISE	Configure Authorization Policies for the Posture Statuses in ISE, on page 15

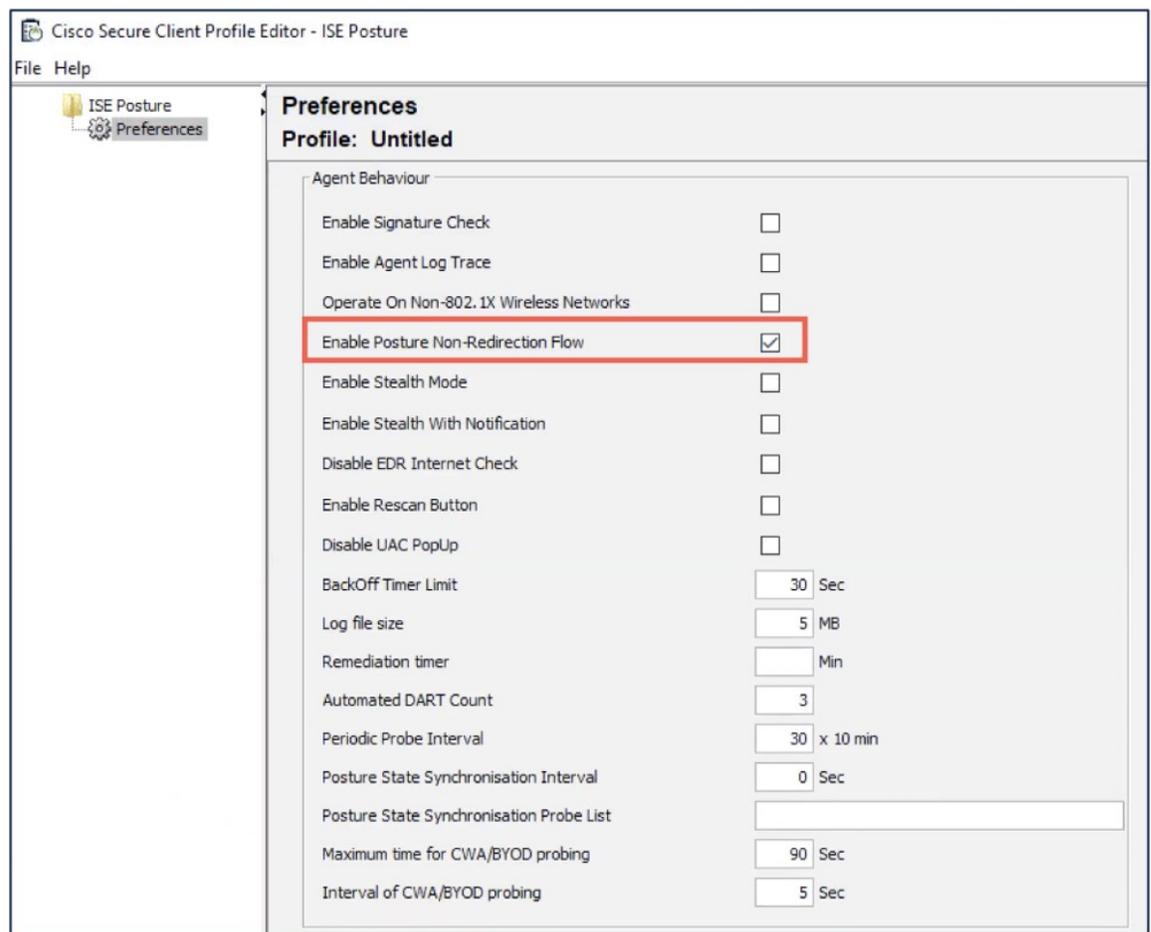
Step	Application	Description
10	Management Center	Configure a Remote Access VPN Group Policy with ISE Posture Module in the Management Center, on page 16
11	Management Center	On the management center menu bar, click <b>Deploy</b> and then select <b>Deployment</b> .

## Configure the Posture Profile using the ISE Posture Profile Editor

The standalone Secure Client profile editor package contains the ISE posture profile editor. Use this editor to create the ISE posture profile and then upload it to ISE and the management center.

Configure the following parameters:

1. Check the **Enable posture non-redirect flow** check box.



2. Enter the **Server name rules** as \*.
3. Configure **Call Homes List** with the FQDN or the IP address of the ISE.

The screenshot shows the 'Posture Protocol' configuration page. It contains the following fields and values:

- Discovery host: [Empty text box]
- Server name rules: [Empty text box]
- Call Home List: [Empty text box]
- PRA retransmission time: 120 Sec
- Retransmission delay: 60 Sec
- Retransmission limit: 4

## Configure Threat Defense in ISE

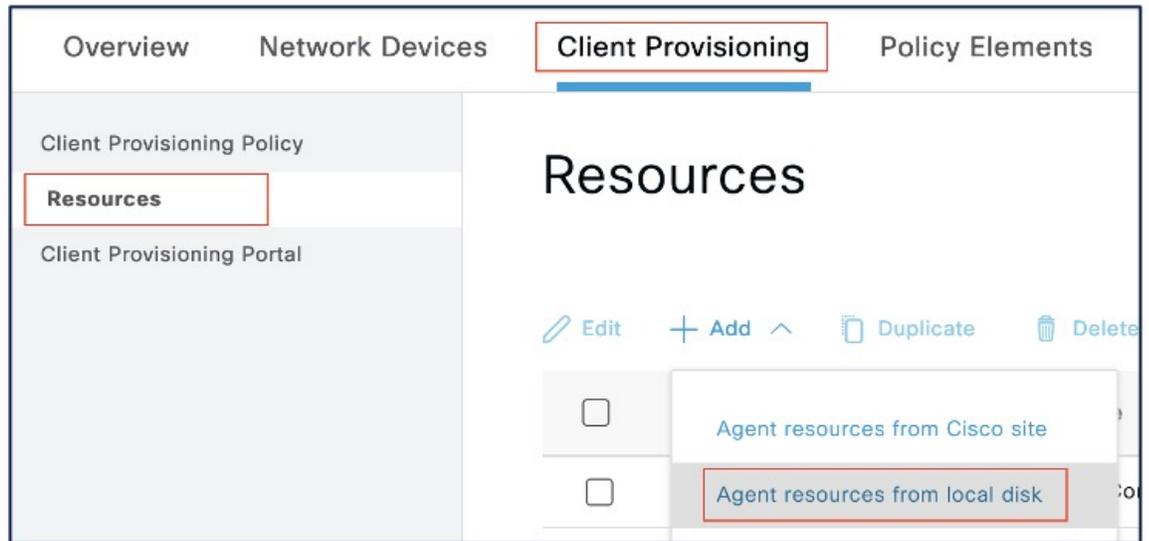
### Procedure

- 
- Step 1** Log in to ISE.
  - Step 2** Choose **Administration > Network Resources > Network Devices**.
  - Step 3** Click **Add**.
  - Step 4** Enter the name, description, and IP address of the threat defense.
  - Step 5** Choose **Cisco** from the **Device Profile** drop-down list.
  - Step 6** Expand **RADIUS Authentication Settings**.
  - Step 7** Configure the **Shared Secret** and the **CoA Port**.  
You need this secret and the port when you configure ISE in the threat defense. For more information, see [Configure ISE in the Management Center](#).
  - Step 8** Click **Save**.
- 

## Upload ISE Posture Profile, Secure Client Package, and ISE Compliance Module to ISE

### Procedure

- 
- Step 1** Choose **Work Centers > Posture > Client Provisioning > Resources**.
  - Step 2** Click **Add** and choose **Agent resources from local disk**.



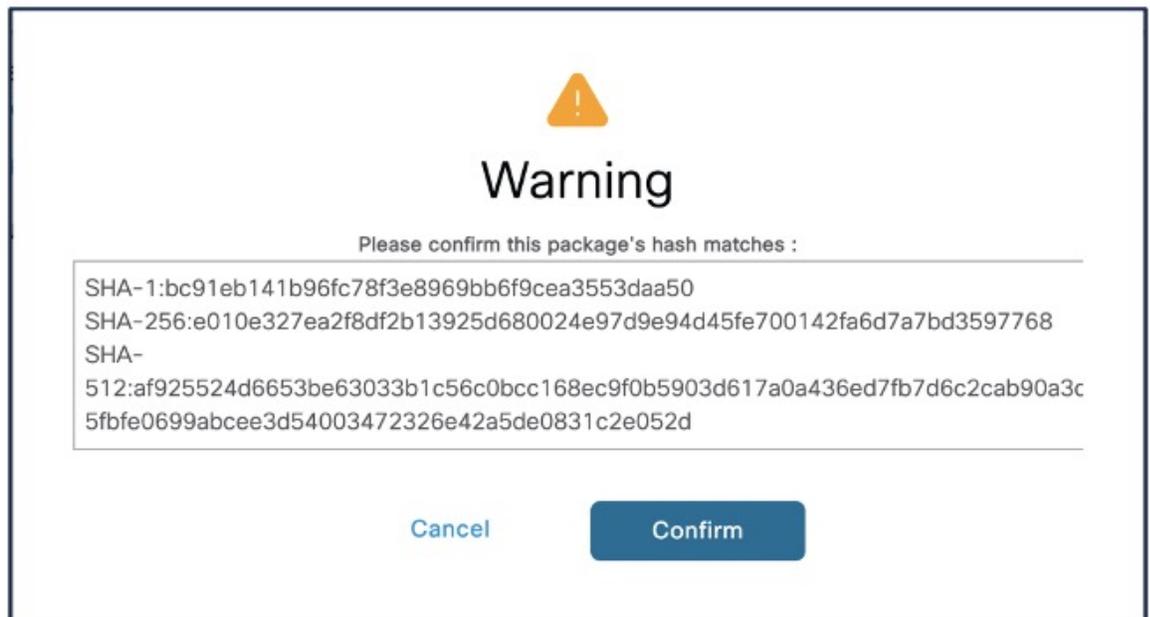
**Step 3** Choose **Cisco Provided Packages** from the **Category** drop-down list.

**Step 4** Click **Choose File** and select one of the following from the local host:

- a. ISE Posture Profile (ISEPostureCFG.xml)
- b. Secure Client package
- c. ISE Compliance Module

**Step 5** Click **Submit**.

**Step 6** Click **Confirm** to validate the checksum.



**Step 7** Repeat steps 2 to 6 to upload the remaining two files.

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	AnyConnectComplianceModuleWi...	AnyConnectComplianceM...	4.3.3534.81...	2023/06/24 08:26:48	Cisco Secure Client Windows...
<input type="checkbox"/>	CiscoTemporalAgentOSX 4.10.02...	CiscoTemporalAgentOSX	4.10.2051.0	2021/08/09 19:12:31	With CM: 4.3.1858.4353
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Suppli...
<input type="checkbox"/>	CiscoAgentlessOSX 4.10.02051	CiscoAgentlessOSX	4.10.2051.0	2021/08/09 19:12:36	With CM: 4.3.1858.4353
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2021/08/09 19:12:27	Supplicant Provisioning Wizar...
<input type="checkbox"/>	CiscoAgentlessWindows 4.10.02...	CiscoAgentlessWindows	4.10.2051.0	2021/08/09 19:12:33	With CM: 4.3.2227.6145
<input type="checkbox"/>	AnyConnect Configuration	AnyConnectConfig	Not Applicable	2023/06/24 16:05:27	
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Suppli...
<input type="checkbox"/>	WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/09 19:12:27	Supplicant Provisioning Wizar...
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.1...	CiscoTemporalAgentWind...	4.10.2051.0	2021/08/09 19:12:28	With CM: 4.3.2227.6145
<input type="checkbox"/>	AnyConnectDesktopWindows 5.0...	AnyConnectDesktopWind...	5.0.3072.0	2023/06/26 18:45:44	Cisco Secure Client for Wind...
<input type="checkbox"/>	AC-Posture-Profile	AnyConnectProfile	Not Applicable	2023/06/26 17:57:02	

## Configure a Secure Client Configuration in ISE

Secure Client Configuration (AnyConnect Configuration in ISE) is the Secure Client software and its different configuration files like the Secure Client binary packages for clients, ISE compliance module, ISE module profiles, customization, and language packages for AnyConnect.

### Procedure

- Step 1** Choose **Work Centers > Posture > Client Provisioning > Resources**.
- Step 2** Click **Add** and choose **AnyConnect Configuration**.
- Step 3** Choose the Secure Client package from the **Select AnyConnect Package** drop-down list.
- Step 4** Choose the ISE Compliance Module from the **Compliance Module** drop-down list.

AnyConnect Configuration > AnyConnect Configuration

\* Select AnyConnect Package: CiscoSecureClientDesktopWindows 5.0 ✓

\* Configuration Name: AnyConnect Configuration

Description:

Description Value Notes

\* Compliance Module: CiscoSecureClientComplianceModuleW ✓

- Step 5** Under **Cisco Secure Client Module Selection**, by default, ISE Posture is enabled.
- Step 6** Under **Profile Selection**, choose the ISE Posture file from the **ISE Posture** drop-down list.
- Step 7** Click **Submit**.

## Create a Client Provisioning Policy in ISE

A user receives specific versions of resources such as agents, agent compliance modules, or agent customization profiles from ISE based on the client provisioning policy.

### Procedure

- Step 1** Choose **Policy > Client Provisioning**.
- Step 2** Click **Edit**, and choose **Insert new policy above**.
- Step 3** Enter the policy name, and choose an operating system.
- Step 4** Click + under **Results**, and choose the AnyConnect Configuration from the **Agent** drop-down list.

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
AC_Windows	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-

Save Reset

**Step 5** Click **Save**.

## Configure Posture Policy in ISE

The posture policies, posture requirements, and the posture conditions determine the compliance status of the endpoint.

### Procedure

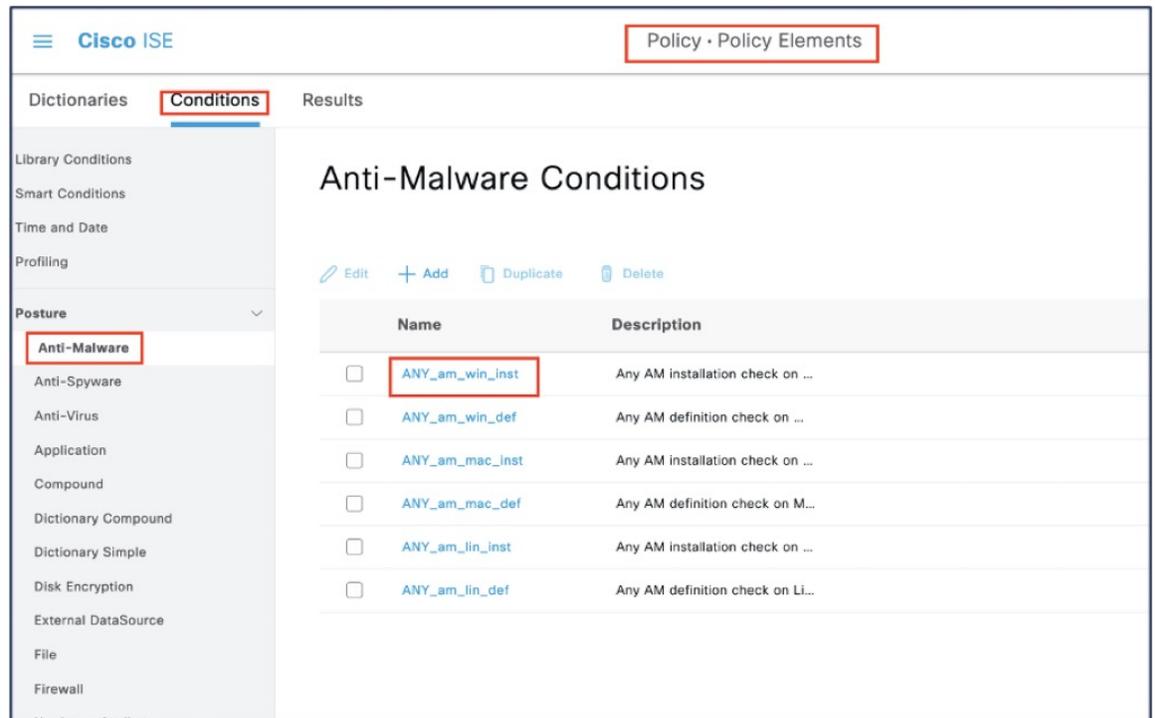
**Step 1** Configure posture conditions.

a. Choose **Policy > Policy Elements > Conditions > Posture**.

You can choose one or more posture conditions.

b. Click **Anti-Malware** to choose an anti-malware condition.

You can choose a predefined anti-malware condition or create a new one. For Windows, you can select the 'ANY\_am\_win\_inst' anti-malware posture condition.

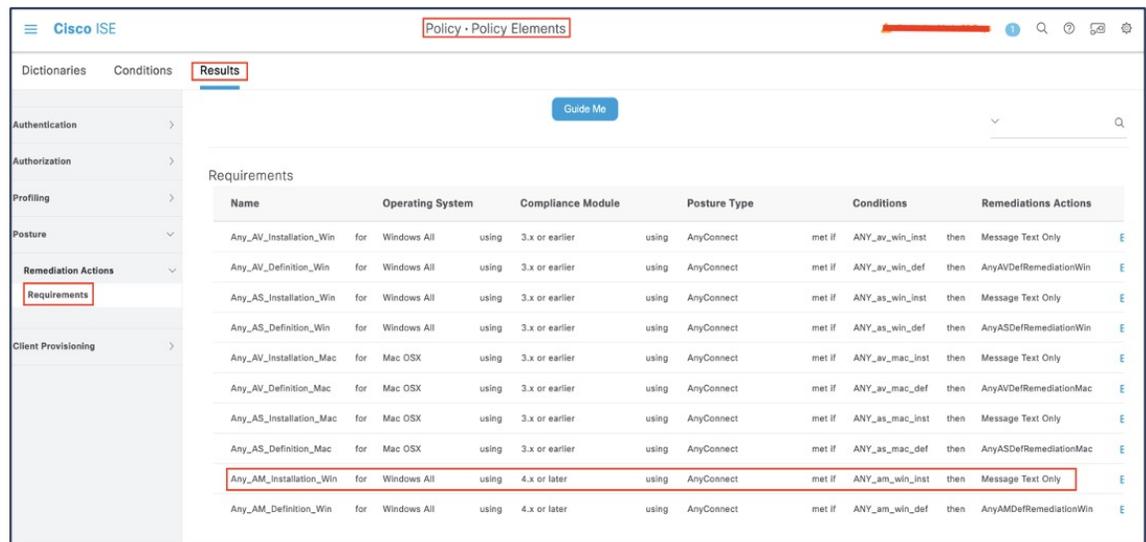


**Step 2** Configure posture requirements.

Choose **Policy > Policy Elements > Results > Posture > Requirements**.

A posture requirement is a set of posture conditions associated with a remediation action. You can choose one of the multiple default or predefined posture requirements, or create a new one.

For Windows, you can select the 'Any\_AM\_Installation\_Win' anti-malware posture requirement.



**Step 3** Configure posture policy.

a. Choose **Policy > Posture**.

You must define a posture policy by configuring a rule based on an operating system and one or more posture requirements.

For Windows, you can select the 'Default\_AntiMalware\_Policy\_Win' anti-malware posture policy.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements	
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Any_AM_Installation_Mac	Edit
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Mac_temporal	Edit
<input checked="" type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Any_AM_Installation_Win	Edit
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Win_temporal	Edit
<input type="checkbox"/>	Policy Options	Default_AppVis_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Mac	Edit
<input type="checkbox"/>	Policy Options	Default_AppVis_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Mac_temporal	Edit
<input type="checkbox"/>	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Win	Edit
<input type="checkbox"/>	Policy Options	Default_AppVis_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Win_temporal	Edit
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Mac	Edit
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal	Edit

b. Check the **Status** check box to enable the posture policy.

c. Click **Save**.

## Configure Downloadable ACLs for the Posture Statuses in ISE

You must configure downloadable ACLs (DACL) for the Unknown, Noncompliant, and Compliant posture statuses. Default authorization DACLs are also available.

### Procedure

**Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

**Step 2** Click **Add**.

**Step 3** Enter a name and description.

**Step 4** Click the radio button for the required IP version.

**Step 5** Enter the values for the DACL.

Downloadable ACL List > Posture\_Unknown

Downloadable ACL

\* Name Posture\_Unknown

Description

IP version  IPv4  IPv6  Agnostic ⓘ

\* DACL Content

1234567	permit udp any any eq domain
8910111	permit ip any host x.x.x.x
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
0414243	

**Step 6** Click **Submit**.

**Step 7** Repeat steps 2 to 6 to create DACLs for the remaining posture statuses.

Examples of DACLs for Unknown, Noncompliant, and Compliant posture statuses:

Type of DACL	Description	DACL
Posture Unknown DACL	Allows traffic to DNS and Policy Service (PSN).	permit udp any any eq domain permit ip any host x.x.x.x
Posture Noncompliant DACL	Denies access to private subnets and allow only internet traffic.	deny ip any x.x.x.x 255.255.255.0 permit ip any any
Posture Compliant DACL	Allows all traffic.	permit ip any any

### What to do next

Configure authorization profiles using these DACLs. For more information, see [Configure Authorization Profiles for the Posture Statuses in ISE](#).

## Configure Authorization Profiles for the Posture Statuses in ISE

You must create three authorization profiles for the Unknown, Noncompliant, and Compliant posture statuses.

### Procedure

**Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

- Step 2** Create an authorization profile for each posture status.
- Step 3** Click **Add**.
- Step 4** Enter a name.
- Step 5** From the **Access Type** drop-down list, choose **ACCESS\_ACCEPT**.
- Step 6** From the **Network Device Profile** drop-down list, choose **Cisco**.
- Step 7** Under **Common Tasks**, check the **DACL Name** check box and choose the DACL for the posture state from the drop-down list.

You can view the configured attributes under **Attributes Details**.

The example below shows the authorization profile for the Unknown status.

The screenshot shows the configuration page for an Authorization Profile named 'FTD\_VPN\_Unknown'. The page is titled 'Authorization Profiles > FTD\_VPN\_Unknown' and 'Authorization Profile'. The configuration includes:

- Name:** FTD\_VPN\_Unknown
- Description:** (Empty text area)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**  ⓘ
- Agentless Posture:**  ⓘ
- Passive Identity Tracking:**  ⓘ

Under the **Common Tasks** section:

- DACL Name:** Posture\_Unknown
- IPv6 DACL Name
- ACL

Under the **Attributes Details** section:

- Access Type = ACCESS\_ACCEPT
- DACL = Posture\_Unknown

- Step 8** Click **Submit**.
- Step 9** Repeat steps 3 to 8 to create authorization profiles for the remaining posture statuses.

**What to do next**

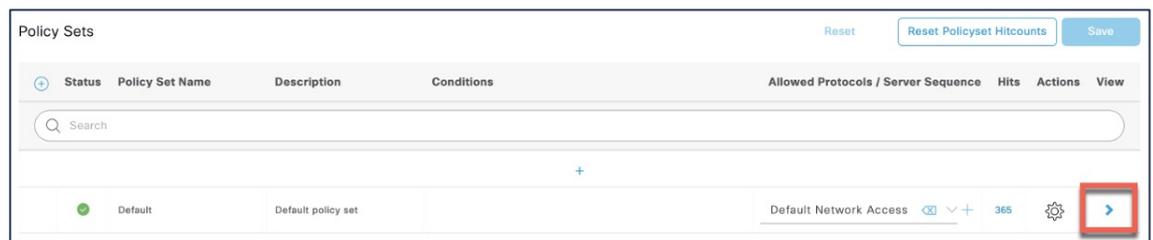
Configure authorization policies using these authorization profiles. For more information, see [Configure Authorization Policies for the Posture Statuses in ISE](#).

**Configure Authorization Policies for the Posture Statuses in ISE**

You must create an authorization policy for each posture status.

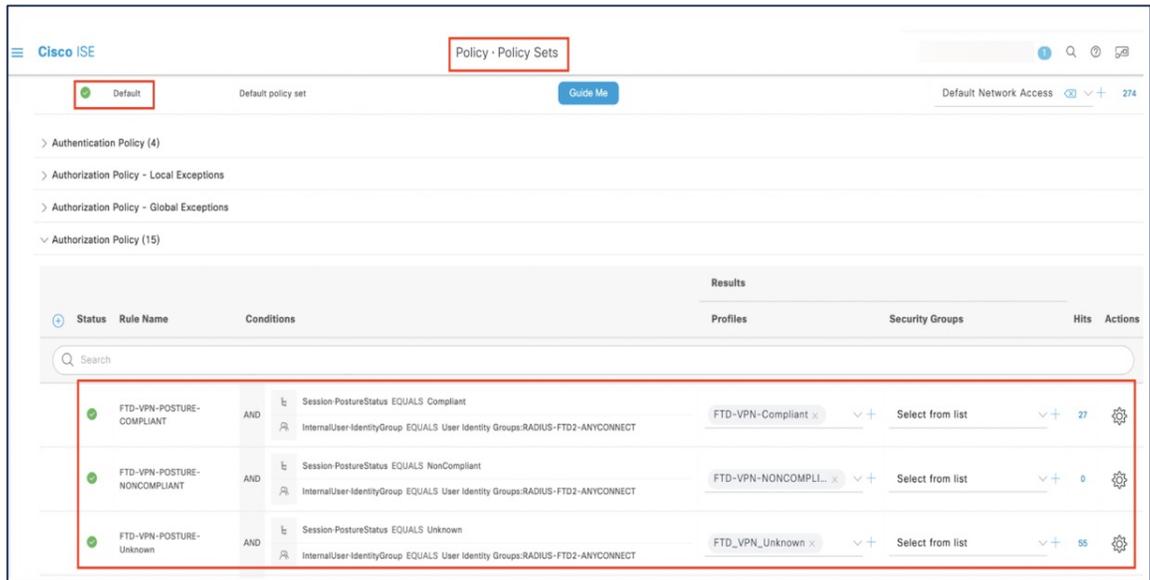
**Procedure**

- Step 1** Choose **Policy > Policy Sets**.
- Step 2** In the **View** column, click the arrow icon adjacent to the Default policy.



- Step 3** Expand **Authorization Policy**.
- Step 4** Click + adjacent to the **Status** column.
- Step 5** Use **Posture Status** and **Identity Group** as conditions of the policy.
- Step 6** Choose the appropriate authorization profile from the drop-down list for the posture status.
- Step 7** Click **Save**.
- Step 8** Repeat steps 4 to 7 for the remaining authorization policies.

The image below shows the authorization policies for the posture statuses.



## Configure a Remote Access VPN Group Policy with ISE Posture Module in the Management Center

### Before you begin

Configure a remote access VPN policy in the management center.

### Procedure

- Step 1** Log in to your management center web interface.
- Step 2** Choose **Devices > Remote Access**.
- Step 3** Select a remote access VPN policy, and click **Edit**.
- Step 4** Select a connection profile, and click **Edit**.
- Step 5** Click **Edit Group Policy**.
- Step 6** Click the **Secure Client** tab.
- Step 7** Click **Client Modules**, and click +.
- Step 8** Choose the ISE Posture module from the **Client Module** drop-down list.
- Step 9** Choose the ISE profile from the **Profile to download** drop-down list.
- Step 10** Check the **Enable module download** check box.
- Step 11** Click **Add**.

### Edit Group Policy

Name:\*  
DfltGrpPolicy

Description:

General **Secure Client** Advanced

Profile  
Management Profile  
**Client Modules**  
SSL Settings  
Connection Settings  
Custom Attributes

Download optional client modules to the endpoint. Secure Client requests download from the Firewall Threat Defense of only the modules that are configured here.

Client Module	Profile	Download	
ISE Posture	ISEPostureCFG.xml		

**Step 12** Click **Save**.

#### What to do next

1. Deploy the configuration on the threat defense. On the management center menu bar, click **Deploy** and then select **Deployment**.
2. Establish a VPN connection to the threat defense using the Secure Client.
3. Verify ISE posture module configuration.

## Verify ISE Posture Module Configuration

### On the Threat Defense

Use the following commands on the threat defense CLI to verify the ISE posture module configuration:

**show run webvpn:** View details of the Secure Client configurations.

```
> show run webvpn
webvpn
  enable Outside
  http-headers
  hsts-server
    enable
    max-age 31536000
    include-sub-domains
    no preload
  hsts-client
    enable
  x-content-type-options
  x-xss-protection
  content-security-policy
  anyconnect image disk0:/csm/cisco-secure-client-win-5.0.03072-
webdeploy-k9.pkg 1 regex "Windows"
  anyconnect profiles ISEPostureCFG.xml disk0:/csm/ISEPostureCFG.xml
  anyconnect profiles raftd1.xml disk0:/csm/raftd1.xml
  anyconnect enable
  tunnel-group-list enable
  cache
    disable
  error-recovery disable
```

**show run group-policy <rapn\_group\_policy\_name>:** View details of the RA VPN group policy for Secure Client.

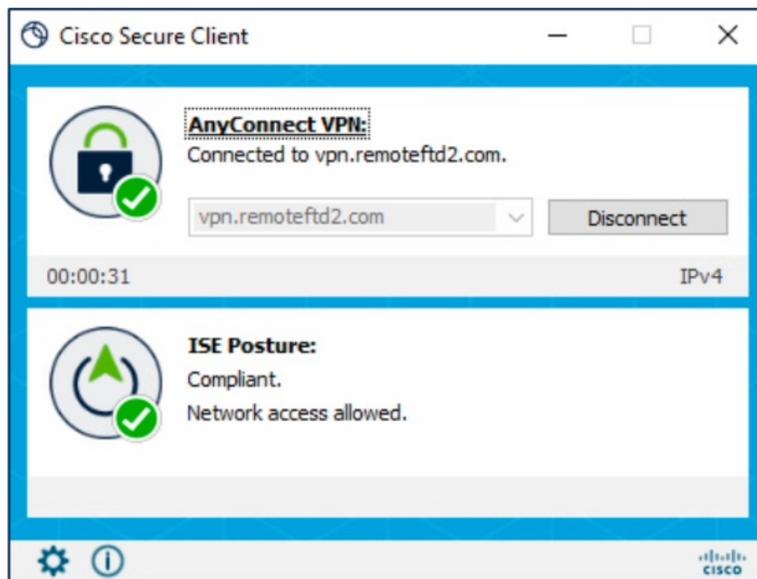
```
> show run group-policy AC-Posture
group-policy AC-Posture internal
group-policy AC-Posture attributes
  banner none
  wins-server none
  dns-server none
  dhcp-network-scope none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelall
  ipv6-split-tunnel-policy tunnelall
  split-tunnel-network-list none
  default-domain none
  split-dns none
  split-tunnel-all-dns disable
  client-bypass-protocol disable
  vlan none
  address-pools none
  webvpn
    anyconnect ssl dtls enable
    anyconnect mtu 1406
    anyconnect firewall-rule client-interface public none
    anyconnect firewall-rule client-interface private none
    anyconnect ssl keepalive 20
    anyconnect ssl rekey time none
    anyconnect ssl rekey method none
    anyconnect dpd-interval client 30
    anyconnect dpd-interval gateway 30
    anyconnect ssl compression none
    anyconnect dtls compression none
    anyconnect modules value iseposture
    anyconnect profiles value ISEPostureCFG.xml type iseposture
    anyconnect ask none default anyconnect
    anyconnect ssl df-bit-ignore disable
```

**show run aaa-server:** View details of the ISE server.

```
> show run aaa-server
aaa-server ISE protocol radius
  authorize-only
  interim-accounting-update periodic 24
  dynamic-authorization
aaa-server ISE (Inside) host [redacted]
  key *****
  authentication-port 1812
  accounting-port 1813
```

### On the Endpoint

Establish a VPN connection to the threat defense using the Secure Client and verify the ISE posture module installation.



### Related Documentation:

- [Cisco Identity Services Engine Administrator Guides](#)
- [Secure Firewall Management Center Administration and Device Configuration Guides](#)
- [Cisco Secure Client Administration Guides](#)

---

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.