Configure Client Posture Policies

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.

- Posture Service, on page 1
- Posture Administration Settings, on page 5
- Download Posture Updates to Cisco ISE, on page 9
- Configure Acceptable Use Policies for Posture Assessment, on page 10
- Posture Conditions, on page 10
- Simple Posture Conditions, on page 11
- Create Simple Posture Conditions, on page 11
- Compound Posture Conditions, on page 12
- Predefined Condition for Enabling Automatic Updates in Windows Clients, on page 12
- Preconfigured Antivirus and Antispyware Conditions, on page 13
- Antivirus and Antispyware Support Chart, on page 13
- Compliance Module, on page 13
- Create Compound Posture Conditions, on page 14
- Create Patch Management Conditions, on page 15
- Create Disk Encryption Conditions, on page 16
- Configure Posture Policies, on page 16
- Posture Assessment Options, on page 17
- Posture Remediation Options, on page 18
- Custom Conditions for Posture, on page 19
- Custom Posture Remediation Actions, on page 19
- Posture Assessment Requirements, on page 23
- Custom Permissions for Posture, on page 25
- Configure Standard Authorization Policies, on page 26

Posture Service

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the compliance, also known as posture, of endpoints, before allowing them to connect to your network. A posture agent, such as the AnyConnect ISE Posture Agent or Network Admission Control (NAC) Agent, runs on the endpoint. Client Provisioning ensures that the endpoints receive the appropriate Posture Agent.
The ISE Posture Agent for Cisco ISE does not support Windows Fast User Switching when using the native supplicant, because there is no clear disconnect of the previous user. When a new user is sent, the Agent is hung on the old user process and session ID, so a new posture session cannot start. As per the Microsoft Security policies, it is recommended to disable Fast User Switching.

Related Topics
- Components of Posture Services, on page 2
- Posture and Client-Provisioning Policies Workflow, on page 3
- Posture Service Licenses, on page 3

Components of Posture Services

Cisco ISE posture service primarily includes the posture administration services and the posture run-time services.

Posture Administration Services

If you have not installed the Apex license in Cisco ISE, then the posture administration services option is not available from the Admin portal.

Administration services provide the back-end support for posture-specific custom conditions and remediation actions that are associated with the requirements and authorization policies that are configured for posture service.

Posture Run-Time Services

The posture run-time services encapsulate all the interactions that happen between the client agent and the Cisco ISE server for posture assessment and remediation of clients.

Posture run-time services begin with the Discovery Phase. An endpoint session is created after the endpoint passes 802.1x authentication. The client agent then attempts to connect to a Cisco ISE node by sending discovery packets through different methods in the following order:

1. via HTTP to Port 80 on a Cisco ISE server (if configured)
2. via HTTPS to Port 8905 on a Cisco ISE server (if configured)
3. via HTTP to Port 80 on the default gateway
4. via HTTPS to Port 8905 to each previously contact server
5. via HTTP to Port 80 on enroll.cisco.com

The Posture Phase begins when the Acceptable User Policy (if any) is accepted. The Cisco ISE node issues a posture token for the Posture Domain to the client agent. The posture token allows the endpoint to reconnect to the network without going through the posture process again. It contains information such as the Agent GUID, the Acceptable User Policy status, and endpoint operating system information.

The messages used in the Posture Phase are in the NEA PB/PA format (RFC5792).
Posture and Client-Provisioning Policies Workflow

Figure 1: Posture and Client Provisioning Policies Workflow in Cisco ISE

In Stage 1 of posture discovery, all discovery probes execute at the same time by the Posture agent. The timeout value is 5 seconds. Stage two contains two discovery probes, which allows the posture module to establish a connection to the PSN. This connection to the PSN supports authentication in environments where redirection is not supported. During stage two, all probes are sequential. If stage 2 fails, the posture agent tries stage 1 again. This cycle continues for 30 seconds, after which you see "No policy server detected". This state continues until a discovery probe triggers.

Related Topics
Configure Client Provisioning Resource Policies

Posture Service Licenses

Cisco ISE provides you with three types of licenses, the Base license, the Plus license, and the Apex license. If you have not installed the Apex license on the Primary PAN, then the posture requests will not be served in Cisco ISE. The posture service of Cisco ISE can run on a single node or on multiple nodes.

Posture Service Deployment

You can deploy Cisco ISE in a standalone environment (on a single node) or in a distributed environment (on multiple nodes).
In a standalone Cisco ISE deployment, you can configure a single node for all the administration services, the monitoring and troubleshooting services, and the policy run-time services.

In a distributed Cisco ISE deployment, you can configure each node as a Cisco ISE node for administration services, monitoring and troubleshooting services, and policy run-time services. A node that runs the administration services is the primary node in that Cisco ISE deployment. The other nodes that run other services are the secondary nodes which can be configured for backup services for one another.

Enable Posture Session Service in Cisco ISE

Before you begin

• You must enable session services in Cisco ISE and install the advanced license package to serve all the posture requests received from the clients.
• If you have more than one node that is registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, apart from the primary node. You can configure each node as a Cisco ISE node (Administration, Policy Service, and Monitoring personas).
• The posture service only runs on Cisco ISE nodes that assume the Policy Service persona and does not run on Cisco ISE nodes that assume the administration and monitoring personas in a distributed deployment.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Administration &gt; System &gt; Deployment &gt; Deployment</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose a Cisco ISE node from the Deployment Nodes window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Under the <strong>General Settings</strong> tab, check the <strong>Policy Service</strong> check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Check the <strong>Enable Session Services</strong> check box, for the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services. To stop the session services, uncheck the check box.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Run the Posture Assessment Report

You can run the Posture Detail Assessment report to generate a detailed status of compliance of the clients against the posture policies that are used during posture assessment.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Operations &gt; Reports &gt; ISE Reports &gt; Endpoints and Users &gt; Posture Detail Assessment</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the <strong>Time Range</strong> drop-down list, choose the specific time period.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Run</strong> to view the summary of all the end points that were active during the selected time period.</td>
</tr>
</tbody>
</table>

Related Topics

- Reports
Posture Administration Settings

You can globally configure the Admin portal for posture services. You can download updates automatically to the Cisco ISE server through the web from Cisco. You can also update Cisco ISE manually offline later. In addition, having an agent like AnyConnect, the NAC Agent, or the Web Agent installed on the clients provides posture assessment and remediation services to clients. The client agent periodically updates the compliance status of clients to Cisco ISE. After login and successful requirement assessment for posture, the client agent displays a dialog with a link that requires end users to comply with terms and conditions of network usage. You can use this link to define network usage information for your enterprise network that end users accept before they can gain access to your network.

Related Topics
- Timer Settings for Clients, on page 5
- Set Posture Status for Nonagent Devices, on page 6
- Posture Lease, on page 7
- Configure Acceptable Use Policies for Posture Assessment, on page 10

Timer Settings for Clients

You can set up timers for users to remediate, to transition from one state to another, and to control the login success screen.

We recommend configuring agent profiles with remediation timers and network transition delay timers as well as the timer used to control the login success screen on client machines so that these settings are policy based. You can configure all these timers for agents in client provisioning resources in the NAC or AnyConnect Posture Profile window (Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC or AnyConnect Posture Profile).

However, when there are no agent profiles configured to match the client provisioning policies, you can use the settings in the General Settings configuration window (Administration > System > Settings > Posture > General Settings).

Related Topics
- Agent Profile Parameters and Applicable Values
- Set Remediation Timer for Clients to Remediate Within Specified Time, on page 5
- Set Network Transition Delay Timer for Clients to Transition, on page 6
- Set Login Success Window to Close Automatically, on page 6

Set Remediation Timer for Clients to Remediate Within Specified Time

You can configure the timer for client remediation within a specified time. When clients fail to satisfy configured posture policies during an initial assessment, the agent waits for the clients to remediate within the time configured in the remediation timer. If the client fails to remediate within this specified time, then the client agent sends a report to the posture run-time services after which the clients are moved to the noncompliance state.

Step 1  Choose Administration > System > Settings > Posture > General Settings.
Step 2  In the Remediation Timer field, enter a time value in minutes.
The default value is 4 minutes. The valid range is 1 to 300 minutes.

**Step 1** Choose Administration > System > Settings > Posture > General Settings.

**Step 2** Enter a time value in seconds, in the Network Transition Delay field.

The default value is 3 seconds. The valid range is 2 to 30 seconds.

**Step 3** Click Save.

**Related Topics**

Posture General Settings

---

### Set Network Transition Delay Timer for Clients to Transition

You can configure the timer for clients to transition from one state to the other state within a specified time using the network transition delay timer, which is required for Change of Authorization (CoA) to complete. It may require a longer delay time when clients need time to get a new VLAN IP address during success and failure of posture. When successfully postured, Cisco ISE allows clients to transition from unknown to compliant mode within the time specified in the network transition delay timer. Upon failure of posture, Cisco ISE allows clients to transition from unknown to noncompliant mode within the time specified in the timer.

**Step 1** Choose Administration > System > Settings > Posture > General Settings.

**Step 2** Enter a time value in seconds, in the Network Transition Delay field.

The default value is 3 seconds. The valid range is 2 to 30 seconds.

**Step 3** Click Save.

**Related Topics**

Posture General Settings

---

### Set Login Success Window to Close Automatically

After successful posture assessment, the client agent displays a temporary network access screen. The user needs to click the OK button in the login window to close it. You can set up a timer to close this login screen automatically after specified time.

**Step 1** Choose Administration > System > Settings > Posture > General Settings.

**Step 2** Check the Automatically Close Login Success Screen After check box.

**Step 3** Enter a time value in seconds, in the field next to Automatically Close Login Success Screen After check box.

The valid range is 0 to 300 seconds. If the time is set to zero, then AnyConnect does not display the login success screen.

**Step 4** Click Save.

**Related Topics**

Posture General Settings

---

### Set Posture Status for Nonagent Devices

You can configure the posture status of endpoints that run on non-agent devices like Linux or iDevices. When Android devices and Apple iDevices such as an iPod, iPhone, or iPad connect to a Cisco ISE enabled network, these devices assume the Default Posture Status settings.
These settings can also be applied to endpoints that run on Windows and Macintosh operating systems when a matching policy is not found during posture runtime.

**Before you begin**

In order to enforce policy on an endpoint, you must configure a corresponding Client Provisioning policy (Agent installation package). Otherwise, the posture status of the endpoint automatically reflects the default setting.

**Step 1**  
Choose **Administration > System > Settings > Posture > General Settings**.

**Step 2**  
From the **Default Posture Status** drop-down list, choose the option as **Compliant** or **Noncompliant**.

**Step 3**  
Click **Save**.

**Related Topics**

- Configure Client Provisioning Resource Policies
- Posture General Settings

**Posture Lease**

You can configure Cisco ISE to perform posture assessment every time a user logs into your network or perform posture assessment in specified intervals. The valid range is 1 to 365 days.

This configuration applies only for those who use AnyConnect agent for posture assessment.

When the posture lease is active, Cisco ISE will use the last known posture state and will not reach out to the endpoint to check for compliance. But when the posture lease expires, Cisco ISE does not automatically trigger a re-authentication or a posture reassessment for the endpoint. The endpoint will stay in the same compliance state since the same session is being used. When the endpoint re-authenticates, posture will be run and the posture lease time will be reset.

Example Use Case Scenario:

- The user logs on to the endpoint and gets it posture compliant with the posture lease set to one day.
- Four hours later the user logs off from the endpoint (the posture lease now has 20 hours left).
- One hour later the user logs on again. Now the posture lease has 19 hours left. The last known posture state was compliant. Hence the user is provided access without posture being run on the endpoint.
- Four hours later the user logs off (the posture lease now has 15 hours left).
- 14 hours later, the user logs on. The posture lease has one hour left. The last known posture state was compliant. The user is provided access without posture being run on the endpoint.
- One hour later, the posture lease expires. The user is still connected to the network as the same user session is being used.
- One hour later, user logs off (the session is tied to the user but not to the machine, so the machine can stay on the network).
- One hour later the user logs on. Since the posture lease has expired and a new user session is launched, the machine performs a posture assessment, the results are sent to the Cisco ISE and the posture lease timer is reset to one day in case of this use case.
Periodic Reassessments

Periodic reassessment (PRA) can be done only for clients that are already successfully postured for compliance. PRA cannot occur if clients are not compliant on your network.

A PRA is valid and applicable only if the endpoints are in a compliant state. The policy service node checks the relevant policies, and compiles the requirements depending on the client role that is defined in the configuration to enforce a PRA. If a PRA configuration match is found, the policy service node responds to the client agent with the PRA attributes that are defined in the PRA configuration for the client before issuing a CoA request. The client agent periodically sends the PRA requests based on the interval specified in the configuration. The client remains in the compliant state if the PRA succeeds, or the action configured in the PRA configuration is to continue. If the client fails to meet PRA, then the client is moved from the compliant state to the noncompliant state.

The PostureStatus attribute shows the current posture status as compliant in a PRA request instead of unknown even though it is a posture reassessment request. The PostureStatus is updated in the Monitoring reports as well.

When the posture lease has not expired, an endpoint becomes compliant based on the Access Control List (ACL), and PRA is initiated. If PRA fails, the endpoint is deemed noncompliant and the posture lease is reset.

Configure Periodic Reassessments

You can configure periodic reassessments only for clients that are already successfully postured for compliance. You can configure each PRA to a user identity group that is defined in the system.

Before you begin

- Ensure that each PRA configuration has a unique group or a unique combination of user identity groups assigned to the configuration.
- You can assign a role_test_1 and a role_test_2, which are the two unique roles to a PRA configuration. You can combine these two roles with a logical operator and assign the PRA configuration as a unique combination of two roles. For example, role_test_1 OR role_test_2.
- Ensure that two PRA configurations do not have a user identity group in common.
- If a PRA configuration already exists with a user identity group “Any”, you cannot create other PRA configurations unless you perform one of the following:
  - Update the existing PRA configuration with the Any user identity group to reflect a user identity group other than Any.
  - Delete the existing PRA configuration with a user identity group “Any”.

---

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Settings &gt; Posture &gt; Reassessments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Modify the values in the New Reassessment Configuration page to create a new PRA.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Submit to create a PRA configuration.</td>
</tr>
</tbody>
</table>

Related Topics

Posture Reassessment Configuration Settings
Download Posture Updates to Cisco ISE

Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco. You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web. This process usually takes approximately 20 minutes. After the initial download, you can configure Cisco ISE to verify and download incremental updates to occur automatically.

Cisco ISE creates default posture policies, requirements, and remediations only once during an initial posture updates. If you delete them, Cisco ISE does not create them again during subsequent manual or scheduled updates.

Before you begin

To ensure that you are able to access the appropriate remote location from which you can download posture resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE, page 5-2.

You can use the Posture Update page to download updates dynamically from the web.

---

**Step 1**  
Choose Administration > System > Settings > Posture > Updates.

**Step 2**  
Choose the Web option to download updates dynamically.

**Step 3**  
Click Set to Default to set the Cisco default value for the Update Feed URL field.

If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the above URL, try also pointing your Cisco ISE to the alternative URL in the related topics.

**Step 4**  
Modify the values in the Posture Updates page.

**Step 5**  
Click Update Now to download updates from Cisco.

**Step 6**  
Click OK to continue with other tasks on Cisco ISE.

After being updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information section in the Posture Updates page.

---

**Related Topics**

Download Posture Updates Automatically, on page 9

---

Download Posture Updates Automatically

After an initial update, you can configure Cisco ISE to check for the updates and download them automatically.
Before you begin

- You should have initially downloaded the posture updates to configure Cisco ISE to check for the updates and download them automatically.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Settings &gt; Posture &gt; Updates.</td>
</tr>
<tr>
<td>2</td>
<td>In the Posture Updates page, check the Automatically check for updates starting from initial delay check box.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the initial delay time in hh:mm:ss format. Cisco ISE starts checking for updates after the initial delay time is over.</td>
</tr>
<tr>
<td>4</td>
<td>Enter the time interval in hours. Cisco ISE downloads the updates to your deployment at specified intervals from the initial delay time.</td>
</tr>
<tr>
<td>5</td>
<td>Click Yes to continue.</td>
</tr>
<tr>
<td>6</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

Configure Acceptable Use Policies for Posture Assessment

After login and successful posture assessment of clients, the client agent displays a temporary network access screen. This screen contains a link to an acceptable use policy (AUP). When users click the link, they are redirected to a page that displays the network-usage terms and conditions, which they must read and accept. Each Acceptable Use Policy configuration must have a unique user identity group, or a unique combination of user identity groups. Cisco ISE finds the AUP for the first matched user identity group, and then it communicates to the client agent that displays the AUP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Settings &gt; Posture &gt; Acceptable Use Policy.</td>
</tr>
<tr>
<td>2</td>
<td>Click Add.</td>
</tr>
<tr>
<td>3</td>
<td>Modify the values in the New Acceptable Use Policy Configuration page.</td>
</tr>
<tr>
<td>4</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

Related Topics
- Posture Acceptable Use Policy Configuration Settings

Posture Conditions

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web for the first time. This process is called the initial posture update.
After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple conditions have `pc_` as their prefixes and compound conditions have `pr_` as their prefixes.

You can also configure Cisco ISE to download the Cisco-defined conditions periodically as a result of dynamic posture updates through the web. You cannot delete or edit Cisco defined posture conditions.

A user defined condition or a Cisco defined condition includes both simple conditions and compound conditions.

**Related Topics**

- Download Posture Updates to Cisco ISE, on page 9

---

## Simple Posture Conditions

You can use the **Posture Navigation** pane to manage the following simple conditions:

- **File Conditions**—A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.

- **Registry Conditions**—A condition that checks for the existence of a registry key or the value of the registry key on the client.

- **Application Conditions**—A condition that checks if an application or process is running or not running on the client.

  **Note** If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is compliant. If an application is installed and running, the end user is non-compliant.

- **Service Conditions**—A condition that checks if a service is running or not running on the client.

- **Dictionary Conditions**—A condition that checks a dictionary attribute with a value.

- **USB Conditions**—A condition that checks for the presence of USB mass storage device.

**Related Topics**

- Posture Condition Settings
- File Condition Settings
- Registry Condition Settings
- Application Condition Settings
- Service Condition Settings
- Dictionary Simple Condition Settings
- USB Condition Settings

---

## Create Simple Posture Conditions

You can create file, registry, application, service, and dictionary simple conditions that can be used in posture policies or in other compound conditions.
Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Policy &gt; Policy Elements &gt; Conditions &gt; Posture.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose any one of the following: File, Registry, Application, Service, or Dictionary Simple Condition.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the appropriate values in the fields.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

Compound Posture Conditions

Compound conditions are made up of one or more simple conditions, or compound conditions. You can make use of the following compound conditions while defining a Posture policy.

- Compound Conditions—Contains one or more simple conditions, or compound conditions of the type File, Registry, Application, or Service condition
- Antivirus Compound Conditions—Contains one or more AV conditions, or AV compound conditions
- Antispyware Compound Conditions—Contains one or more AS conditions, or AS compound conditions
- Dictionary Compound Conditions—Contains one or more dictionary simple conditions or dictionary compound conditions
- Antimalware Conditions—Contains one or more AM conditions.

Related Topics
- Posture Compound Condition Settings
- AntiVirus Condition Settings
- Antispyware Compound Condition Settings
- Dictionary Compound Condition Settings

Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions page. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.
Preconfigured Antivirus and Antispyware Conditions

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition pages, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These compound conditions can check if the specified antivirus and antispyware products exist on all the clients. You can also create new antivirus and antispyware compound conditions in Cisco ISE.

Antivirus and Antispyware Support Chart

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date in the definition files for each vendor product. Users must frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, look for the latest version and date in the definition files for each vendor product.

Each time the antivirus and antispyware support chart is updated to reflect support for new antivirus and antispyware vendors, products, and their releases, the NAC Agents receive a new antivirus and antispyware library. It helps NAC Agents to support newer additions. Once the NAC Agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the antivirus and antispyware library for a particular antivirus, or antispyware product, the appropriate requirements will be sent to the NAC Agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

The antivirus and antispyware support chart is available on Cisco.com.

Compliance Module

The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.

Vendors frequently update the product version and date in the definition files, therefore, you must look for the latest version and date in the definition files for each vendor product by frequently polling the compliance module for updates. Each time the compliance module is updated to reflect the support for new vendors, products, and their releases, the AnyConnect agents receives a new library. It helps AnyConnect agent to support newer additions. Once the AnyConnect agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the library for a particular antivirus, antispyware, antimalware, disk encryption, or patch management product, the appropriate requirements will be sent to the AnyConnect agents for validating their existence, and the status of the particular products on the clients during posture validation.

The compliance module is available on Cisco.com.

Table given below lists the OPSWAT API versions that support and do not support the ISE posture policy. There are different policy rules for agents that support versions 3 and 4.
Table 1: OPSWAT API Versions

<table>
<thead>
<tr>
<th>Posture Condition</th>
<th>Compliance Module Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSWAT</td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td>3.0.x or earlier</td>
</tr>
<tr>
<td>Antispyware</td>
<td>3.0.x or earlier</td>
</tr>
<tr>
<td>Antimalware</td>
<td>4.0.x or later</td>
</tr>
<tr>
<td>Disk Encryption</td>
<td>3.0.x or earlier and 4.0.x or later</td>
</tr>
<tr>
<td>Patch Management</td>
<td>3.0.x or earlier and 4.0.x or later</td>
</tr>
<tr>
<td>USB</td>
<td>4.0.x or later</td>
</tr>
<tr>
<td>Non-OPSWAT</td>
<td></td>
</tr>
<tr>
<td>File</td>
<td>Any version</td>
</tr>
<tr>
<td>Application</td>
<td>Any version</td>
</tr>
<tr>
<td>Compound</td>
<td>Any version</td>
</tr>
<tr>
<td>Registry</td>
<td>Any version</td>
</tr>
<tr>
<td>Service</td>
<td>Any version</td>
</tr>
</tbody>
</table>

• Be sure to create separate posture policies for version 3.0.x or earlier and version 4.0.x or later, in anticipation of clients that may have installed any one of the above versions.

• OESIS version 4 support is provided for compliance module 4.0.x and Cisco AnyConnect 4.3 and higher. However, AnyConnect 4.3 supports both OESIS version 3 and version 4 policies.

• Version 4 compliance module is supported by ISE 2.1 and higher.

Create Compound Posture Conditions

You can create compound conditions that can be used in posture policies for posture assessment and validation.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1  Choose Policy > Policy Elements > Conditions > Posture > Compound Conditions > Add.
Step 2  Enter appropriate values for the fields.
Step 3  Click Validate Expression to validate the condition.
Step 4  Click Submit.

**Related Topics**
- Posture Conditions
- Simple Posture Conditions
- Compound Posture Conditions
- Predefined Condition for Enabling Automatic Updates in Windows Clients
- Preconfigured Antivirus and Antispyware Conditions

## Create Patch Management Conditions

You can create a policy to check the status of a selected vendor's patch management product.

For example, you can create a condition to check if Microsoft System Center Configuration Manager (SCCM), Client Version 4.x software product is installed at an endpoint.

**Note**

Supported versions of Cisco ISE and AnyConnect:
- Cisco ISE version 1.4 and later
- AnyConnect version 4.1 and later

**Before you begin**

To perform the following task, you must be a Super Admin or Policy Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Policy</strong> &gt; <strong>Policy Elements</strong> &gt; <strong>Conditions</strong> &gt; <strong>Posture</strong> &gt; <strong>Patch Management Condition</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter the condition name and description in the <strong>Name</strong> and <strong>Description</strong> fields.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Choose the appropriate operating system from the <strong>Operating System</strong> drop-down field.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Choose the <strong>Compliance Module</strong> from the drop-down list.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Choose the <strong>Vendor Name</strong> from the drop-down list.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Choose the <strong>Check Type</strong>.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Choose the appropriate patch from the <strong>Check patches installed</strong> drop-down list.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Click <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Patch Management Condition Settings
- Add a Patch Management Remediation, on page 20
Create Disk Encryption Conditions

You can create a policy to check if an end point is compliant with the specified data encryption software. For example, you can create a condition to check if the C: drive is encrypted in an end point. If the C: drive is not encrypted then the end point receives a non-compliance notification and ISE logs a message.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin. You can associate a Disk Encryption condition with a posture requirement only when you use the AnyConnect ISE posture agent.

Step 1 Choose Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition.
Step 2 Click Add.
Step 3 In the Disk Encryption Condition page, enter the appropriate values in the fields.
Step 4 Click Submit.

Configure Posture Policies

A posture policy is a collection of posture requirements that are associated with one or more identity groups and operating systems. The Dictionary Attributes are optional conditions that can be used along with the identity groups and the operating systems to define different policies for the devices.

See Posture Services on the Cisco ISE Configuration Guide for more information.

Before you begin

• You must understand the AUP.
• You must understand periodic reassessments (PRA).

Step 1 Choose Policy > Posture.
Step 2 Use the drop-down arrow to add a new policy.
Step 3 From the Rule Status drop-down list, choose Enabled or Disabled.
Step 4 (Optional) Drag the slider named Delayed Notification to delay the grace period prompt from being displayed to the user until a specific percentage of grace period has elapsed. For example, if the notification delay period is set to 50% and the configured grace period is 10 minutes, Cisco ISE checks the posture status after 5 minutes and displays the grace period notification if the endpoint is found to be noncompliant. Grace period notification is not displayed if the endpoint status is compliant. If the notification delay period is set to 0%, the user is prompted immediately at the beginning of the grace period to remediate the problem. However, the endpoint is granted access until the grace period expires. The default value for this field is 0%. The valid range is from 0 to 95%.
Step 5 In the Rule Name field, enter the name of the policy.

Note It is a best practice to configure a posture policy with each requirement as a separate rule in order to avoid unexpected results.
Step 6 From the **Identity Groups** column, select the desired identity group.

Step 7 From the **Operating Systems** column, select the operating system.

Step 8 From the **Compliance Module** column, select the required compliance module:

- **4.x or Later**—Supports antimalware, disk encryption, patch management, and USB conditions.
- **3.x or Earlier**—Supports antivirus, antispyware, disk encryption, and patch management conditions
- **Any Version**—Supports file, service, registry, application, and compound conditions.

Step 9 In **Other Conditions**, you can add one or more dictionary attributes and save them as simple or compound conditions to a dictionary.

**Note** The dictionary simple conditions and compound conditions that you create in the **Posture Policy** window are not displayed while configuring an authorization policy.

Step 10 Specify the requirements in the **Requirements** field.

Step 11 Click **Save**.

---

**Related Topics**

- Create Simple Posture Conditions
- Create Compound Posture Conditions
- Time and Date Conditions
- Agent Fails to Initiate Posture Assessment
- Create Client Posture Requirements, on page 25
- Configure Periodic Reassessments, on page 8

---

**Posture Assessment Options**

The following table provides a list of posture assessment (posture conditions) options that are supported by the ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

**Table 2: Posture Assessment Options**

<table>
<thead>
<tr>
<th>ISE Posture Agent for Windows</th>
<th>Web Agent for Windows</th>
<th>ISE Posture Agent for Macintosh OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System/Service Packs/Hotfixes</td>
<td>Operating System/Service Packs/Hotfixes</td>
<td>—</td>
</tr>
<tr>
<td>Service Check</td>
<td>Service Check</td>
<td>Service Check (AC 4.1 and ISE 1.4)</td>
</tr>
<tr>
<td>Registry Check</td>
<td>Registry Check</td>
<td>—</td>
</tr>
<tr>
<td>File Check</td>
<td>File Check</td>
<td>File Check (AC 4.1 and ISE 1.4)</td>
</tr>
<tr>
<td>Application Check</td>
<td>Application Check</td>
<td>Application Check (AC 4.1 and ISE 1.4)</td>
</tr>
</tbody>
</table>
## Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

### Table 3: Posture Remediation Options

<table>
<thead>
<tr>
<th>ISE Posture Agent for Windows</th>
<th>Web Agent for Windows</th>
<th>ISE Posture Agent for Macintosh OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Text (Local Check)</td>
<td>Message Text (Local Check)</td>
<td>Message Text (Local Check)</td>
</tr>
<tr>
<td>URL Link (Link Distribution)</td>
<td>URL Link (Link Distribution)</td>
<td>URL Link (Link Distribution)</td>
</tr>
<tr>
<td>File Distribution</td>
<td>File Distribution</td>
<td>—</td>
</tr>
<tr>
<td>Launch Program</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Antivirus Definition Update</td>
<td>—</td>
<td>Antivirus Live Update</td>
</tr>
<tr>
<td>Antispyware Definition Update</td>
<td>—</td>
<td>Antispyware Live Update</td>
</tr>
<tr>
<td>Patch Management Remediation (AC 4.1 - and ISE 1.4)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Windows Update</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>WSUS</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
Custom Conditions for Posture

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated with a posture requirement.

After an initial posture update, Cisco ISE also creates Cisco-defined simple and compound conditions. Cisco-defined simple conditions use the pc_ as and compound conditions use pr_ as.

A user-defined condition or a Cisco-defined condition includes both simple and compound conditions.

Posture service makes use of internal checks based on antivirus and antispyware (AV/AS) compound conditions. Hence, posture reports do not reflect the exact AV/AS compound-condition names that you have created. The reports display only the internal check names of AV/AS compound conditions.

For example, if you have created an AV compound condition named "MyCondition_AV_Check" to check any Vendor and any Product, the posture reports will display the internal check, that is "av_def_ANY", as the condition name, instead of "MyCondition_AV_Check".

Related Topics
- Simple and Compound Conditions
- Posture Conditions
- Simple Posture Conditions
- Create Simple Posture Conditions
- Compound Posture Conditions
- Create Compound Posture Conditions

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

Related Topics
- Agent Fails to Initiate Posture Assessment
- Add a File Remediation, on page 19
- Add a Link Remediation, on page 20
- Add an Antivirus Remediation, on page 21
- Add an Antispyware Remediation, on page 21
- Add a Launch Program Remediation, on page 22
- Add a Windows Update Remediation, on page 22
- Add a Windows Server Update Services Remediation, on page 23
- Add a Patch Management Remediation, on page 20

Add a File Remediation

A file remediation allows clients to download the required file version for compliance. The client agent remediates an endpoint with a file that is required by the client for compliance.
You can filter, view, add, or delete file remediations in the File Remediations page, but you cannot edit file remediations. The File Remediations page displays all the file remediations along with their name and description and the files that are required for remediation.

---

**Add a Link Remediation**

A link remediation allows clients to click a URL to access a remediation page or resource. The client agent opens a browser with the link and allow the clients to remediate themselves for compliance.

The Link Remediaion page displays all the link remediations along with their name and description and their modes of remediation.

---

**Add a Patch Management Remediation**

You can create a patch management remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The Patch Management Remediation page displays the remediation type, patch management vendor names, and various remediation options.
Step 3 Click **Patch Management Remediation**.
Step 4 Click **Add**.
Step 5 Modify the values in the **Patch Management Remediation** page.
Step 6 Click **Submit** to add the remediation action to the **Patch Management Remediations** page.

**Related Topics**

- **Patch Management Remediation**

---

### Add an Antivirus Remediation

You can create an antivirus remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AV Remediations page displays all the antivirus remediations along with their name and description and their modes of remediation.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Posture**.
Step 2 Click **Remediation Actions**.
Step 3 Click **AV Remediation**.
Step 4 Click **Add**.
Step 5 Modify the values in the **New AV Remediation** page.
Step 6 Click **Submit**.

**Related Topics**

- **Antivirus Remediation**

---

### Add an Antispyware Remediation

You can create an antispyware remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AS Remediations page displays all the antivirus remediations along with their name and description and their modes of remediation.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Posture**.
Step 2 Click **Remediation Actions**.
Step 3 Click **AS Remediation**.
Step 4 Click **Add**.
Step 5 Modify the values in the **New AS Remediations** page.
Step 6 Click **Submit**.

**Related Topics**

- **Antispyware Remediation**
Add a Launch Program Remediation

You can create a launch program remediation, where the client agent remediates clients by launching one or more applications for compliance.

The Launch Program Remediations page displays all the launch program remediations along with their name and description and their modes of remediation.

Step 1 Choose Policy > Policy Elements > Results > Posture.
Step 2 Click Remediation Actions.
Step 3 Click Launch Program Remediation.
Step 4 Click Add.
Step 5 Modify the values in the New Launch Program Remediation page.
Step 6 Click Submit.

Related Topics
Launch Program Remediation

Troubleshoot Launch Program Remediation

Problem
When an application is launched as a remediation using Launch Program Remediation, the application is successfully launched (observed in the Windows Task Manager), however, the application UI is not visible.

Solution
The Launch program UI application runs with system privileges, and is visible in the Interactive Service Detection (ISD) window. To view the Launch program UI application, ISD should be enabled for the following OS:

- Windows Vista: ISD is in stop state by default. Enable ISD by starting ISD service in services.msc.
- Windows 7: ISD service is enabled by default.
- Windows 8/8.1: Enable ISD by changing "NoInteractiveServices" from 1 to 0 in the registry: \HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Windows.

Add a Windows Update Remediation

The Windows Update Remediations page displays all the Windows update remediations along with their name and description and their modes of remediation.

Step 1 Choose Policy > Policy Elements > Results > Posture.
Step 2 Click Remediation Actions.
Step 3 Click Windows Update Remediation.
Step 4 Click Add.
Add a Windows Server Update Services Remediation

You can configure Windows clients to receive the latest WSUS updates from a locally administered or a Microsoft-managed WSUS server for compliance. A Windows Server Update Services (WSUS) remediation installs latest Windows service packs, hotfixes, and patches from a locally managed WSUS server or a Microsoft-managed WSUS server.

You can create a WSUS remediation where the client agent integrates with the local WSUS Agent to check whether the endpoint is up-to-date for WSUS updates.

Step 1 Choose Policy > Policy Elements > Results > Posture.
Step 2 Click Remediation Actions.
Step 3 Click Windows Server Update Services Remediation.
Step 4 Click Add.
Step 5 Modify the values in the New Windows Server Update Services Remediation page.
Step 6 Click Submit.

Related Topics
Windows Server Update Services Remediation

Posture Assessment Requirements

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints.

Figure 2: Posture Policy Requirement Types
Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.

Optional Requirements

During policy evaluation, the agent provides an option to clients to continue, when they fail to meet the optional requirements specified in the posture policy. End users are allowed to skip the specified optional requirements.

For example, you have specified an optional requirement with a user-defined condition to check for an application running on the client machine, such as Calc.exe. Although, the client fails to meet the condition, the agent prompts an option to continue further so that the optional requirement is skipped and the end user is moved to Compliant state.

Audit Requirements

Audit requirements are specified for internal purposes and the agent does not prompt any message or input from end users, regardless of the pass or fail status during policy evaluation.

For example, you are in the process of creating a mandatory policy condition to check if end users have the latest version of the antivirus program. If you want to find out the non-compliant end users before actually enforcing it as a policy condition, you can specify it as an audit requirement.

Related Topics

Agent Fails to Initiate Posture Assessment

Client System Stuck in Noncompliant State

If a client machine is unable to remediate a mandatory requirement, the posture status changes to “noncompliant” and the agent session is quarantined. To get the client machine past this “noncompliant” state, you need to restart the posture session so that the agent starts posture assessment on the client machine again. You can restart the posture session as follows:

- In wired and wireless Change of Authorization (CoA) in an 802.1X environment:
  - You can configure the Reauthentication timer for a specific authorization policy when you create a new authorization profile in the New Authorization Profiles page. “Configuring Permissions for Downloadable ACLs” section on page 20-11 for more information.
  - Wired users can get out of the quarantine state once they disconnect and reconnect to the network. In a wireless environment, the user must disconnect from the wireless lan controller (WLC) and wait until the user idle timeout period has expired before attempting to reconnect to the network.
  - In a VPN environment—Disconnect and reconnect the VPN tunnel.
Create Client Posture Requirements

You can create a requirement in the Requirements page where you can associate user-defined conditions and Cisco defined conditions, and remediation actions. Once created and saved in the Requirements page, user-defined conditions and remediation actions can be viewed from their respective list pages.

Before you begin

• You must have an understanding of acceptable use policies (AUPs) for a posture.

Step 1 Choose Policy > Policy Elements > Results > Posture > Requirements.
Step 2 Enter the values in the Requirements page.
Step 3 Click Done to save the posture requirement in read-only mode.
Step 4 Click Save.

Related Topics
Client Posture Requirements
Client System Stuck in Noncompliant State, on page 24
Posture Assessment Requirements, on page 23

Custom Permissions for Posture

A custom permission is a standard authorization profile that you define in Cisco ISE. Standard authorization profiles set access privileges based on the matching compliance status of the endpoints. The posture service broadly classifies the posture into unknown, compliant, and noncompliant profiles. The posture policies and the posture requirements determine the compliance status of the endpoint.

You must create three different authorization profiles for an unknown, compliant, and noncompliant posture status of endpoints that can have different set of VLANs, DACLs and other attribute value pairs. These profiles can be associated with three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

Unknown Profile
If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint and, therefore no compliance report has been provided by the client agent.

Compliant Profile
If a matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint is set to compliant. When the posture assessment occurs, the endpoint meets all the mandatory requirements that are defined in the matching posture policy. For an endpoint that is postured compliant, it can be granted privileged network access on your network.
Noncompliant Profile

The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself.

Related Topics
Configure Standard Authorization Policies, on page 26

Configure Standard Authorization Policies

You can define two types of authorization policies in the Authorization Policy page, standard exceptions authorization policies. The standard authorization policies that are specific to posture are used to make policy decisions based on the compliance status of endpoints.

Step 1
Choose Policy > Authorization.

Step 2
Choose one of the matching rule type to apply from the drop-down list shown at the top of the Authorization Policy page.

- **First Matched Rule Applies** — This option sets access privileges with a single authorization policy that is first matched during evaluation from the list of standard authorization policies. Once the first matching authorization policy is found, the rest of the standard authorization policies are not evaluated.
- **Multiple Matched Rule Applies** — This option sets access privileges with multiple authorization policies that are matched during evaluation from the list of all the standard authorization policies.

Step 3
Click the down arrow next to Edit in the default standard authorization policy row.

Step 4
Click Insert New Rule Above.

Step 5
Enter a rule name, choose identity groups and other conditions, and associate an authorization profile in the new authorization policy row that appears above the default standard authorization policy row.

Step 6
Click Done to create a new standard authorization policy in read-only mode.

Step 7
Click Save.

Related Topics
Authorization Policy Settings
Manage Authorization Policies and Profiles