Configuring 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.

This chapter describes the posture service in Cisco ISE in the following topics:

Posture Service

The Network Admission Control (NAC) Agents that are installed on the clients interact with the posture service to enforce security policies on all the endpoints that attempt to gain access to your protected network. The NAC Agents assist you in evaluating the clients against the posture policies and enforcing the security policies on clients to meet the compliance.

The NAC Agent for Cisco ISE does not support Windows Fast User Switching when using the native supplicant. This is because there is no clear disconnect of the older user. When a new user is sent, the Agent is hung on the old user process and session ID, and hence a new posture cannot take place. As per the Microsoft Security policies, it is recommended to disable Fast User Switching.

Client Provisioning is a service to ensure that the clients are setup with appropriate Agents that provide posture assessment and remediation for the clients.

Related Topics

- Components of Posture Services, page 24-2
- Running Posture Reports, page 24-5

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 advanced 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 the SWISS protocol services and all the interactions that happen between the NAC Agents and the Cisco ISE server for posture assessment and remediation of clients.

The SWISS protocol is a stateless request response protocol that allows NAC Agents running on managed clients to discover the Cisco ISE server and retrieve configuration and operational information. The NAC Agent connects to the Cisco ISE server by sending SWISS unicast discovery packets out on User Datagram Protocol (UDP) port 8905 until a Cisco ISE node that assumes the Policy Service persona sends a response to the client. The SWISS protocol uses TCP transport for all the messages and UDP transport for periodical requests. The NAC Agent tunnels all the SWISS requests over HTTPS and pings the Cisco ISE SWISS UDP server for changes to its authentication and posture state.

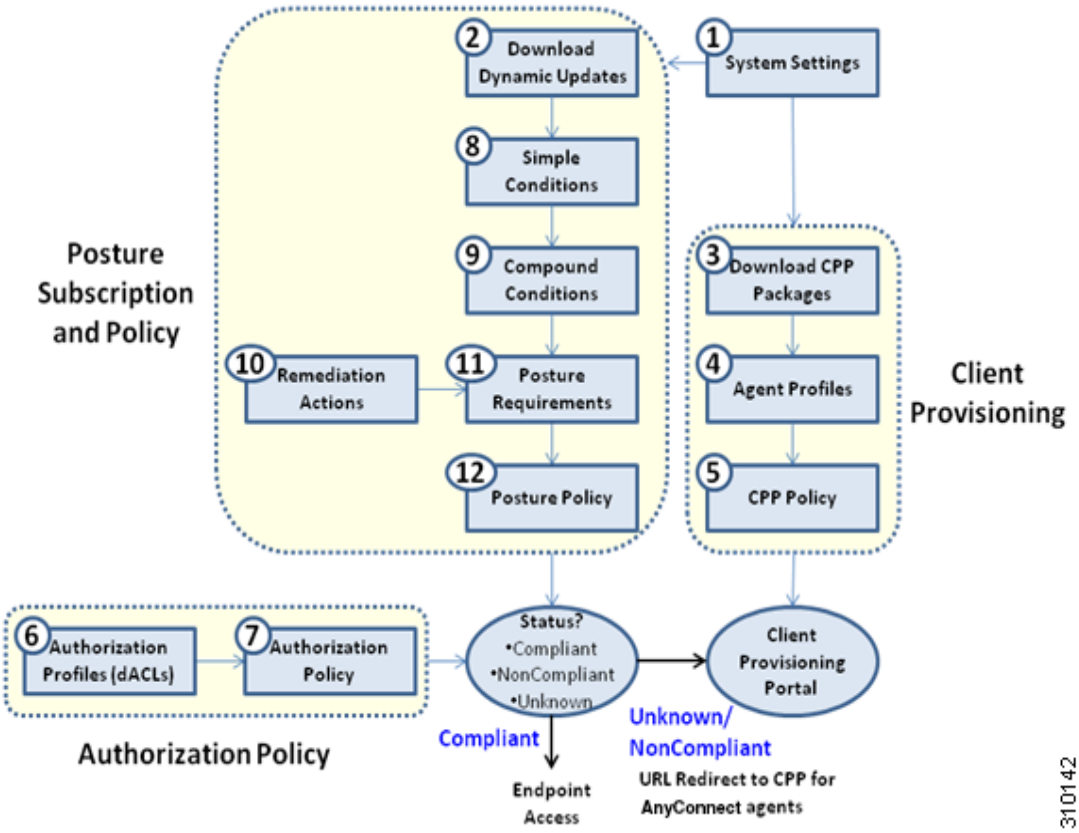
The SWISS request message that comes from the client machine includes information pertaining to resource types for the following items:

- Agent profiles
- Agent compliance modules
- Agent customization package

In addition to answering these request items, the SWISS response from the Cisco ISE server can also contain prompts to update the current Agent and URLs that are required to perform posture assessment and remediation on the client machine.

Posture and Client-Provisioning Policies Workflow

Figure 24-1 Posture and Client Provisioning Policies Workflow in Cisco ISE



Related Topics

- Configuring Client Provisioning Resource Policies, page 23-45
- Chapter 23, "Configuring Client Provisioning."
- *Cisco Identity Services Engine Network Component Compatibility, Release 1.2*

Posture Service Licenses

Cisco ISE provides you with two types of licenses, the base license and advanced license. You must install the base license for the basic services or the advanced license for all the services of Cisco ISE. Depending on the type of deployment and the license you have installed, the posture service of Cisco ISE can run on a single node or on multiple nodes. You also have an evaluation license which can be upgraded to the appropriate base or advanced license once the evaluation license period is over.

If you have not installed the advanced license on the primary Administration node, then the SWISS server does not get initialized during run time. If the SWISS server does not initialize, then the posture requests will not be served in Cisco ISE. The posture run-time services takes appropriate action when

you add or remove any advanced license file to the Cisco ISE deployment. During run time, the SWISS server initializes when you add the advanced license, and it stops when you remove the advanced license, or when the advanced license expires.

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, or as an inline posture node as needed. 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.

Deploying Posture Session Service

You must enable session services in Cisco ISE and install the advanced licence package to initialize the SWISS server and serve all the posture requests received from the clients.

Before You Begin

- 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) or an Inline Posture node.
- 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.

Step 1 Choose **Administration > System > Deployment > Deployment**.

Step 2 Choose a Cisco ISE node from the Deployment Nodes page.

Step 3 Click **Edit**.

Step 4 On the General settings tab, check the **Policy Service** check box,

If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

Step 5 Check the **Enable Session Services** 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.

Step 6 Click **Save**.

Running Posture Reports

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.

Step 1 Choose **Operations > Reports > ISE Reports > Endpoints and Users > Posture Detail Assessment**.

Step 2 Click the **Time Range** drop-down arrow and select the specific time period.

Step 3 Click **Run** to view the summary of all the endpoints that logged on for a selected period of time.

Related Topics

- Chapter 27, "Reporting."

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, the NAC Agents and Web Agents installed on the clients provide posture assessment and remediation services to clients. The NAC Agents and Web Agents periodically update the compliance status of clients to Cisco ISE. After login and successful requirement assessment for posture, the NAC Agents and Web Agents on Windows display 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, page 24-5
- Setting Posture Status for Non-Agent Devices, page 24-7
- Periodic Reassessments, page 24-7
- Downloading Posture Updates, page 24-9
- Downloading Posture Updates Automatically, page 24-9
- Configuring Acceptable Use Policies for Posture Assessment, page 24-10

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 **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > New Profile**.

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

Related Topics

- Agent Profile Parameters and Applicable Values, page 23-21
- Setting Timer for Users to Remediate, page 24-6
- Setting Timer for Users to Transition, page 24-6
- Setting Timer to Automatically Close the Login Window, page 24-7

Setting Timer for Users to Remediate

You can configure the timer for clients to remediate themselves within specified time. When clients fail to satisfy configured posture policies during an initial assessment, the NAC Agents wait 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 NAC Agents send 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 Enter a time value in minutes, in the **Remediation Timer** field.

The default value is 4 minutes. The valid range is 1 to 300 minutes.

Step 3 Click **Save**.

Related Topics

Posture General Settings, page A-19

Setting Timer for Users 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, page A-19

Setting Timer to Automatically Close the Login Window

After successful posture assessment, the NAC Agents and Web Agents display a temporary network access screen. The user needs to click the OK button in the login screen 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 the NAC Agents and Web Agents do not display the login success screen.

Step 4 Click **Save**.

Related Topics

- Posture General Settings, page A-19

Setting Posture Status for Non-Agent 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 with a matching Posture policy, you must configure a corresponding Client Provisioning policy (Agent installation package). Otherwise, the posture status of the endpoint automatically reflects the default setting. For details, see Configuring Client Provisioning Resource Policies, page 23-45.

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

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

Step 3 Click **Save**.

Related Topics

- Posture General Settings, page A-19

Periodic Reassessments

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

The NAC Agent sends a compliance report to the policy service node once the client is postured successfully and is 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 NAC Agent with the PRA attributes that are defined in the PRA configuration for the client before issuing a CoA request. The NAC 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. The posture status is unknown when the PostureStatus attribute of any client before reassessment of new requirements and posture policies retrieved from the server in a PRA request assuming that the client is being postured after successful authentication.

Related Topics

- Configuring Periodic Reassessments, page 24-8

Configuring 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. If you configure a PRA with the *Any* role then only the configuration with this role exists, and no other configurations can exist 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 the following:
  - Update the existing PRA configuration with the Any user identity group to reflect a user identity group other than *Any*.

    or
  - Delete the existing PRA configuration with a user identity group "*Any*".

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

Step 2 Click **Add**.

Step 3 Modify the values in the **New Reassessment Configuration** page to create a new PRA.

Step 4 Click **Submit** to create a PRA configuration.

Related Topics

- Posture Reassessment Configuration Settings, page A-19

Downloading Posture Updates

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 6-3.

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. The default Update Feed URL is https://www.cisco.com/web/secure/pmbu/posture-update.xml.

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 https://www.perfigo.com/ise/posture-update.xml.

Step 4 Modify the values on 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.

Once 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.

Downloading 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. See "Downloading Posture Updates" section on page 24-9.

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

Step 2 In the **Posture Updates** page, check the **Automatically check for updates starting from initial delay** check box.

Step 3 Enter the initial delay time in hh:mm:ss format.

Cisco ISE starts checking for updates after the initial delay time is over.

Step 4 Enter the time interval in hours.

Cisco ISE downloads the updates to your deployment at specified intervals from the initial delay time.

Step 5 Click **Yes** to continue.

Step 6 Click **Save**.

Note When you configure Cisco ISE to check for the updates automatically, the latest AV/AS Support charts get populated accordingly. Anyway, you need to download the latest Compliance Module and add it to the Client Provisioning policy manually. If the latest Support charts do not synchronize with the existing Compliance Module, ensure that you are downloading the latest Compliance Module and adding it to the Client Provisioning policy.

Related Topics

- For details on performing offline posture package updates in Cisco ISE, refer to the "Cisco ISE Offline Updates" section of the *Release Notes for the Cisco Identity Services Engine, Release 1.2*.
- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Configuring Client Provisioning Resource Policies, page 23-45
- Custom Conditions for Posture, page 24-13

Configuring Acceptable Use Policies for Posture Assessment

After login and successful posture assessment of clients, the NAC Agents and Web Agents display 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 NAC Agent and Web Agent that displays the AUP.

Step 1 Choose **Administration > System > Settings > Posture > Acceptable Use Policy**.

Step 2 Click **Add**.

Step 3 Modify the values in the **New Acceptable Use Policy Configuration** page.

Step 4 Click **Submit**.

Related Topics

- Posture Acceptable Use Policy Configuration Settings, page A-20

Configuring Posture Policies

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. The Dictionary Attributes are optional conditions in conjunction with the identity groups and the operating systems that allow you to define different policies for the clients.

Before You Begin

- You must have an understanding of acceptable use policy (AUP). See "Configuring Acceptable Use Policies for Posture Assessment" section on page 24-10
- You must have an understanding of periodic reassessments (PRA). See "Configuring Periodic Reassessments" section on page 24-8.

Step 1 Choose **Policy > Posture**.

Step 2 Choose the **Status** type.

Step 3 In the **Rule Name** text box, enter the policy name.

It is a best practice to configure posture policy with each requirement as a separate rule, to avoid unexpected results.

Step 4 From **identity Groups**, choose the role.

Step 5 From **Operating Systems**, choose the operating system.

Step 6 In **Other Conditions**, you can add one or more dictionary attributes and save them as simple or compound conditions to a dictionary.

Note Dictionary simple conditions and dictionary compound conditions that you create in the Posture Policy page are not visible while configuring an authorization policy.

Step 7 From **Requirements**, choose a requirement. You can also create a new Requirement.

Step 8 Click **Done.**

Step 9 Click **Save**.

Related Topics

- Posture Assessment Options, page 24-12
- Creating Client Posture Requirements, page 24-19
- Creating Simple Posture Conditions, page 19-6
- Creating Compound Posture Conditions, page 19-7
- Time and Date Conditions, page 21-10

- Agent Fails to Initiate Posture Assessment, page G-33
- *Posture Services on the Cisco ISE Configuration Guide*

Posture Assessment Options

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

Table 24-1 Posture Assessment Options

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Operating System/Service Packs/Hotfixes	Operating System/Service Packs/Hotfixes	—
Process Check	Process Check	—
Registry Check	Registry Check	—
File Check	File Check	—
Application Check	Application Check	—
Antivirus Installation	Antivirus Installation	Antivirus Installation
Antivirus Version/ Antivirus Definition Date	Antivirus Version/ Antivirus Definition Date	Antivirus Version/ Antivirus Definition Date
Antispyware Installation	Antispyware Installation	Antispyware Installation
Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date
Windows Update Running	Windows Update Running	—
Windows Update Configuration	Windows Update Configuration	—
WSUS Compliance Settings	WSUS Compliance Settings	—

Posture Remediation Options

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

Table 24-2 Posture Remediation Options

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)	URL Link (Link Distribution)

Table 24-2 Posture Remediation Options (continued)

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
File Distribution	File Distribution	—
Launch Program	—	—
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update
Windows Update	—	—
WSUS	—	—

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, page 19-1
- Posture Conditions, page 19-5
- Simple Posture Conditions, page 19-5
- Creating Simple Posture Conditions, page 19-6
- Compound Posture Conditions, page 19-6
- Creating Compound Posture Conditions, page 19-7

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.

Table 24-3 shows remediation types that are supported by NAC Web Agent and NAC Agents for Windows and Macintosh clients.

Table 24-3 Remediation Types Supported by Agents

Remediation Types	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh
File Remediation	Supported	Supported	—
Link remediation (manual)	Supported	Supported	Supported
Link remediation (automatic)	Supported	Not supported	Not supported
Antivirus remediation (manual)	Supported	Not supported	Supported
Antivirus remediation (automatic)	Supported	Not supported	Not supported
Antispyware remediation (manual)	Supported	Not supported	Not supported
Antispyware remediation (automatic)	Supported	Not supported	Not supported
Launch Program remediation (manual)	Supported	Not supported	—
Launch Program remediation (automatic)	Supported	Not supported	—
Windows Update remediation (manual)	Supported	Not supported	—
Windows Update remediation (automatic)	Supported	Not supported	—
Windows Server Update Services remediation (manual)	Supported	Not supported	—
Windows Server Update Services remediation (automatic)	Supported	Not supported	—

Related Topics

- Adding a File Remediation, page 24-15
- Adding a Link Remediation, page 24-15
- Adding an Antivirus Remediation, page 24-15
- Adding an Antispyware Remediation, page 24-16
- Adding a Launch Program Remediation, page 24-16
- Adding a Windows Update Remediation, page 24-17
- Adding a Windows Server Update Services Remediation, page 24-18
- Agent Fails to Initiate Posture Assessment, page G-33

Adding a File Remediation

A file remediation allows clients to download the required file version for compliance. The NAC Agents and Web Agents remediate 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.

Step 1 Choose **Policy > Policy Elements > Results > Posture**.

Step 2 Click **Remediation Actions**.

Step 3 Click **File Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New File Remediation** page.

Step 6 Click **Submit**.

Related Topics

- File Remediation, page C-26

Adding a Link Remediation

A link remediation allows clients to click a URL to access a remediation page or resource. The NAC Agents and Web Agents open a browser with the link and allow the clients to remediate themselves for compliance.

The Link Remediation page displays all the link 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 **Link Remediation**.

Step 4 Click **Add**.

Step 5 Modify the values in the **New Link Remediation** page.

Step 6 Click **Submit**.

Related Topics

- Link Remediation, page C-26

Adding 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, page C-26

Adding 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, page C-27

Adding a Launch Program Remediation

You can create a launch program remediation, where the NAC Agents and Web Agents remediate 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, page C-27

Windows Update Remediation

Windows update remediation ensures that Automatic Updates configuration is turned on Windows clients per your security policy. Windows administrators have an option to turn on or turn off Automatic Updates on Windows clients. Microsoft Windows uses this feature to check for updates regularly. If the Automatic Updates feature is turned on, then Windows automatically updates Windows-recommended updates before any other updates.

The Windows Automatic Updates setting will differ for different Windows operating systems.

For example, Windows XP provides the following settings for configuring Automatic Updates:

- Automatic (recommended)—Windows allows clients to download recommended Windows updates and install them automatically
- Download updates for me, but let me choose when to install them—Windows downloads updates for clients and allows clients to choose when to install updates
- Notify me but don't automatically download or install them—Windows only notifies clients, but does not automatically download, or install updates
- Turn off Automatic Updates—Windows allows clients to turn off the Windows Automatic Updates feature. Here, clients are vulnerable unless clients install updates regularly, which can be done from the Windows Update Web site link.

You can check whether or not the Windows updates service (wuaserv) is started or stopped in any Windows client by using the **pr_AutoUpdateCheck_Rule**. This is a predefined Cisco rule, which can be used to create a posture requirement. If the posture requirement fails, the Windows update remediation that you associate to the requirement enforces the Windows client to remediate by using one of the options in Automatic Updates.

Related Topics

- Adding a Windows Update Remediation

Adding 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**.

Step 5 Modify the values in the **New Windows Update Remediation** page.

Step 6 Click **Submit**.

Related Topics

- Windows Update Remediation, page C-28

Adding 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 a NAC 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, page C-29

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 further during posture evaluation of endpoints.

Mandatory Requirements

If clients fail to meet mandatory requirements as defined in the posture policies, then they are provided with remediation options during policy evaluation. End users should remediate to meet the requirements within the time specified in the remediation timer settings.

If a client is unable to remediate a mandatory requirement, the posture status changes to "non-compliant" and the agent session is quarantined. To get the client out of a non-compliant state, refer to "Client System Stuck in Noncompliant State" section on page 24-19.

Optional Requirements

If clients fail to meet optional requirements during policy evaluation, then the agent prompts end users with an option to continue further so that they can skip optional requirements.

Audit Requirements

Audit requirements are not shown to end users even though they pass or fail during policy evaluation.

Related Topics

- Client System Stuck in Noncompliant State, page 24-19
- Custom Posture Remediation Actions, page 24-13
- Agent Fails to Initiate Posture Assessment, page G-33

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. See the "Configuring Permissions for Downloadable ACLs" section on page 21-13 for more information. This method is not supported in Inline Posture deployments.
  - 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.

Related Topics

- Configuring Posture Policies, page 24-11
- Custom Posture Remediation Actions, page 24-13
- Creating Client Posture Requirements, page 24-19

Creating 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. See the "Configuring Acceptable Use Policies for Posture Assessment" section on page 24-10.

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

- Configuring Standard Authorization Policies, page 24-21
- Client Posture Requirements, page C-31

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 NAC 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

- Configuring Standard Authorization Policies, page 24-21

Configuring 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

- Custom Permissions for Posture, page 24-20
- Authorization Policy Settings, page C-5
- Chapter 21, “Managing Authorization Policies and Profiles.”