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

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.

Clients interact with the posture service through the AnyConnect ISE Posture Agent or Network Admission Control (NAC) Agent on the endpoint to enforce security policies, meet compliance, and allow the endpoint to gain access to your protected network. Client Provisioning ensures 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. 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 session cannot take place. As per the Microsoft Security policies, it is recommended to disable Fast User Switching.

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:

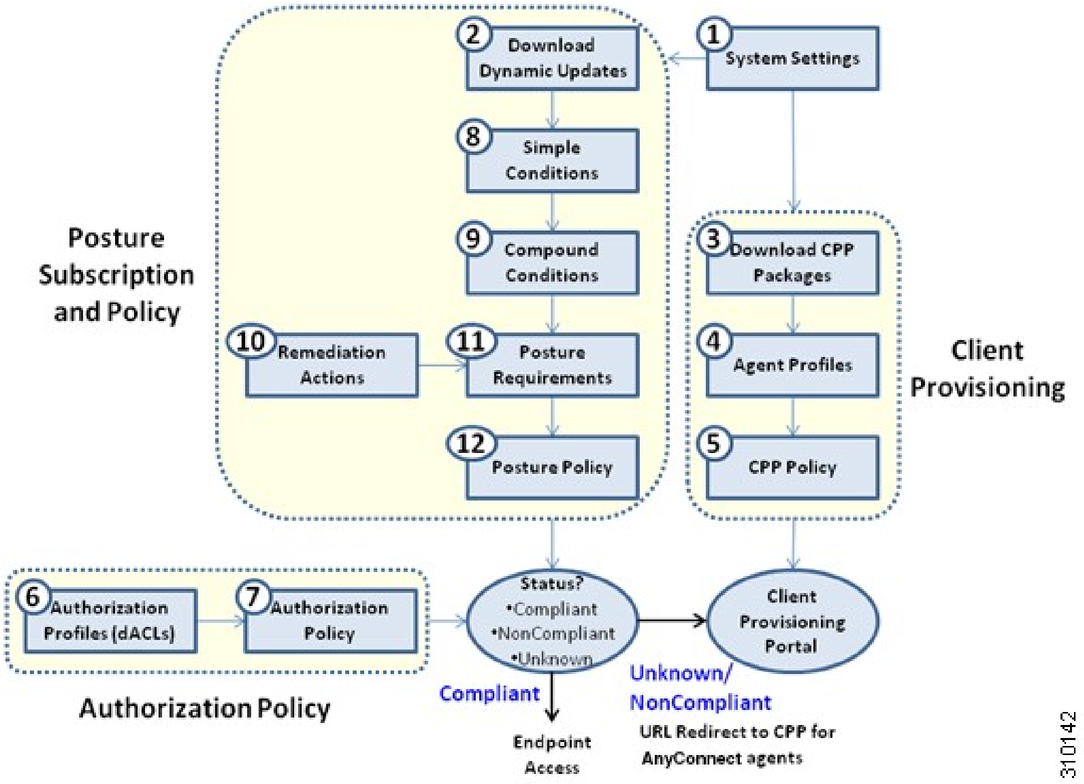
1. via HTTP to Port 80 on a Cisco ISE server (if configured)
2. via HTTPS to Port 8905 on a Cisco ISE server (if configured)
3. via HTTP to Port 80 on the default gateway
4. via HTTPS to Port 8905 to each previously contact server
5. via HTTP to Port 80 on enroll.cisco.com

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



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 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, 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.

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) 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**.

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.

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.

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.

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** > **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 **Administration** > **System** > **Settings** > **Posture** > **General Settings** configuration page.

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 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**.

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**.

Set Login Success Screen 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 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 AnyConnect does not display the login success screen.

Step 4 Click **Save**.

Set 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, 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**, choose the option as **Compliant** or **Noncompliant**.

Step 3 Click **Save**.

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.

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.

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 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.

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 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.

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.

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**.

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.

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**.

Configure 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).
- You must have an understanding of periodic reassessments (PRA).

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**.

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 1: Posture Assessment Options

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Operating System/Service Packs/Hotfixes	Operating System/Service Packs/Hotfixes	—
Service Check	Service Check	Service Check (AC 4.1 and ISE 1.4)
Registry Check	Registry Check	—

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
File Check	File Check	File Check (AC 4.1 and ISE 1.4)
Application Check	Application Check	Application Check (AC 4.1 and ISE 1.4)
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
Patch Management Check (AC 4.1 and ISE 1.4)	—	Patch Management Check (AC 4.1 and ISE 1.4)
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 ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 2: Posture Remediation Options

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture 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)
File Distribution	File Distribution	—
Launch Program	—	—
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Windows Update	—	—
WSUS	—	—

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

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture 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)
File Distribution	File Distribution	—
Launch Program	—	—
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—	—
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".

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.

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.

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**.

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 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**.

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

Step 2 Click **Remediation Actions**.

Step 3 Click **Patch Mangement 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.

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**.

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**.

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**.

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.

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.

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**.

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

Step 6 Click **Submit**.

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.

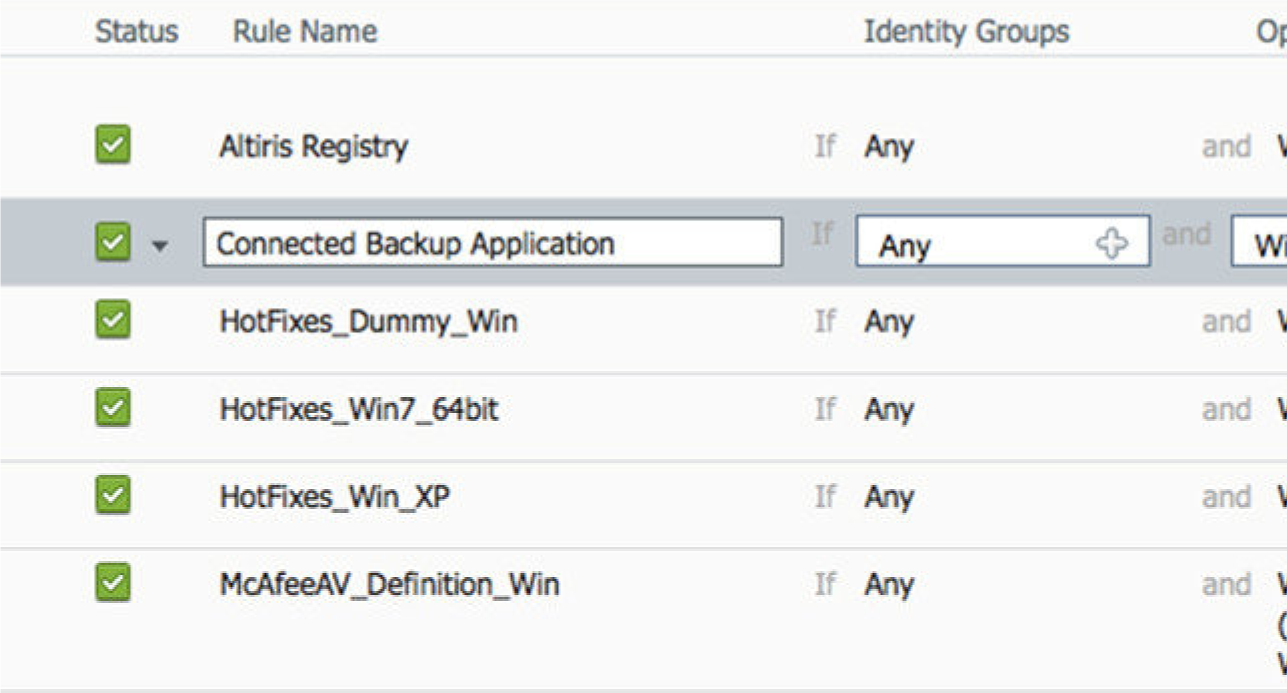
Step 6 Click **Submit**.

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



Status	Rule Name		Identity Groups		Op
☑	Altiris Registry	If	Any	and	V
☑ ▾	Connected Backup Application	If	Any	and	Wi
☑	HotFixes_Dummy_Win	If	Any	and	V
☑	HotFixes_Win7_64bit	If	Any	and	V
☑	HotFixes_Win_XP	If	Any	and	V
☑	McAfeeAV_Definition_Win	If	Any	and	V (V

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.

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. 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.

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**.

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.

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**.