CHAPTER 20

Configuring Client Posture Policies

This chapter describes the posture service in the Cisco Identity Services Engine (Cisco ISE) appliance that allows you to check the state (posture) for all the endpoints that are connecting to your Cisco ISE enabled network with your corporate security policies for compliance before clients access protected areas of your network.

This chapter guides you through the features of the Cisco ISE posture service in detail.

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. At the same time, the NAC Agents enforce security policies on noncompliant endpoints by blocking network access to your protected network. They assist you in evaluating clients against posture policies, and as well as enforce clients to meet requirements that are required for compliance with your organization's security policies.

The posture service checks the state (posture) of the clients for compliance with your corporate security policies before the client gains the privileged network access. The Client Provisioning service ensures that the clients are setup with appropriate Agents that provide posture assessment and remediation for the clients.

The NAC Agent for 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.

For information on the posture service in detail, see the "Understanding the Posture Service" section on page 20-3.

For information on the Posture Compliance dashlet, see the "Posture Compliance Dashlet" section on page 20-8.

For information on posture reports, see the "Viewing Posture Reports" section on page 20-8.

SWISS Protocol

The SWISS protocol is a stateless request response protocol that allows NAC Agents which are 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 URL or URLs that are required to perform posture assessment and remediation on the client machine.

For descriptions of the various types of agents available in Cisco ISE, see Cisco ISE Agents, page 19-2.

Understanding the Posture Service

Cisco ISE posture service primarily includes the posture administration services and the posture run-time services. If you do not have the advanced license package installed on your Cisco ISE deployment, then the posture administration services user interface will not be available for you to use in Cisco ISE.

Posture Administration Services

The administration services provide the back-end support for posture specific custom conditions, and remediation actions that are associated to the requirements and authorization policies that are configured for posture service on your Cisco ISE deployment.

Posture Run-time Services

The posture run-time services encapsulates 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.

Validating a Posture Requirement Request

Once the client (an endpoint) is authenticated on the network, the client can be granted limited access on the network. For example, the client can access remediation-only resources on the network. The NAC Agent that is installed on the client validates the requirements for an endpoint and the endpoint is moved to a compliant state upon successful validation of the requirements. If the endpoint satisfies the requirement, a compliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a Change of Authorization (CoA) for the posture compliant status. If the endpoint fails to satisfy the requirement, a noncompliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a CoA for the posture noncompliant status.

Now, the agent gets its session ID from the redirect URL and sends it along with its MAC address and IP address in a SWISS request. The posture run-time services looks up in the session cache using the session ID first, MAC address, and then the IP address, if required. If the posture run-time services finds the same session using the session ID in the session cache, then it queries the posture policies in Cisco ISE and tries to match the posture policies. Once matched, it generates the specified XML format that contains the matched requirements and sends to the NAC Agents. The NAC Agents send the posture report to the posture run-time services.

Generating a Posture Requirement

The run-time services requests for the posture requirement for the endpoint by looking up at the role to which the user belongs to and the operating system on the client. If you do not have a policy associated with the role, then the run-time services communicate to the NAC Agent with an empty requirement. If you have a policy associated with the role, then the run-time services run through the posture policies through one or more requirements associated with the policies and for each requirement through one or more conditions. Once the posture policy is retrieved for the endpoint, the posture run-time services communicate the requirement to the NAC Agent in a specified XML format.

Processing the Posture Report from the Cisco NAC Agent

The NAC Agent validates the endpoint for compliance based on the requirements that are sent from the Cisco ISE server and determines the posture of the endpoint. If the endpoint is not compliant with the requirement, then the NAC Agent prompts to remediate the endpoint for compliance. Any failures during posture evaluation results in the noncompliance of the endpoint. The NAC Agent sends the appropriate compliance report to the Cisco ISE server once postured compliant or noncompliant.

Issuing a CoA Based on the Posture Report Evaluation

Upon evaluating the posture report received from the NAC Agent, an endpoint may be identified as compliant or noncompliant. If the endpoint is compliant or noncompliant, then the posture run-time services triggers a CoA for that endpoint session. Based on the profile configured for compliant or noncompliant, the end user gets the appropriate level of access privileges to the network.

Logging

Upon processing the posture request and report, the run-time services sends audit log messages to the Cisco ISE node that assumes the Monitoring persona.

For information on how posture and client provisioning session services work in Cisco ISE, see the "Posture and Client Provisioning Services" section on page 20-4.

For information on licenses for the posture service, see the "Licenses for the Posture Service" section on page 20-5.

For information on how to deploy the posture service in detail, see the "Deploying the Posture Service" section on page 20-6.

Posture and Client Provisioning Services

Prerequisites:

Before you begin, you should have an understanding of the available client provisioning resources in Cisco ISE that you can configure for the clients.

For information on how to configure client provisioning resource policies, see the "Configuring Client Provisioning Resource Policies" section on page 19-31.

Before you begin, you should have an understanding of the Client Provisioning session service in Cisco ISE. Cisco ISE manage client provisioning resources for your clients and uses the client provisioning resource policies to ensure that the client systems are set up with an appropriate Agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles.

For information on the Client Provisioning session service, see Chapter 19, "Configuring Client Provisioning Policies."

For information on the NAC Agent that is installed on the client and the client operating system compatibility, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x*.

Posture and Client Provisioning Policies Flow

Figure 20-1 shows the flow of posture and client provisioning policies in the Cisco ISE posture service.

Figure 20-1 Posture and Client Provisioning Policies Workflow in CIsco ISE

Licenses for the Posture Service

Prerequisites:

Before you begin, you should have an understanding on how licenses restrict the usage of Cisco ISE posture service with both the base and advanced license packages.

For more information on Cisco ISE license packages, refer to the Performing Post Installation Tasks chapter in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

Cisco ISE allows you to configure the posture service to run on multiple Cisco ISE nodes in a distributed deployment. You can also configure the posture service on a single node in a standalone Cisco ISE deployment.

Cisco ISE deployment provides you with two main types of licenses, namely the base license and advanced license. You also have an evaluation license which, if further use is desired, needs to be upgraded to the appropriate base or advanced license once the evaluation license period is over.

In addition, if you do not have the advanced license installed on your 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. If the advanced license is not installed in Cisco ISE, then the posture service menus on the Cisco ISE administration user interface will be removed except the default posture status configuration for unsupported operating system in the Administration > System > Settings > Posture > General Settings page. The posture run-time services takes appropriate action when you add or remove any advanced license file to your 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.

Deploying the Posture Service

Prerequisites:

Before you begin, you should have an understanding of the centralized configuration and management of Cisco ISE nodes in the distributed deployment.

For information on Cisco ISE distributed deployment, Chapter 9, "Setting Up Cisco ISE in a Distributed Environment"

You can deploy Cisco ISE either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes). Depending on the type of your deployment and the license you have installed, the posture service of Cisco ISE can run on a single node or on multiple nodes. You need to install either the base license to take advantage of the basic services or the advanced license to take advantage of all the services of Cisco ISE.

In a standalone Cisco ISE deployment, you can configure a single node for all the administration services, the monitoring and trouble shooting services, and the policy run-time services. You cannot configure a node as a node in a standalone deployment.

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.

Configuring the Posture Service in Cisco ISE

From the Administration menu, you can choose Deployment to manage the ISE deployment on a single node or multiple nodes. You can use the Deployment Nodes page to configure the posture service for your Cisco ISE deployment.

To manage the Cisco ISE deployment, complete the following steps:

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

The Deployment navigation pane appears. Use the format selector icons to view the nodes in rows or in a tabbed display.

Step 2 Click the row view button.

Step 3 Click the quick picker (right arrow) icon to view the nodes that are registered in your deployment.

The row view displays all the nodes that are registered in a row format in the Deployment Nodes page.

Note To view the nodes in your deployment in a tree, click the tabbed view button. An arrow appears in front of Deployment in the Deployment navigation pane. Click the arrow in front of the Deployment navigation pane to view the nodes that are registered in your deployment in a tabbed view.

From the Deployment Nodes page, you can configure the posture service on any Cisco ISE node that assumes the Policy Service persona in a distributed deployment.

To deploy the posture session service, complete the following steps:

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

The Deployment navigation menu appears. Use the Table view or the List view button to display the nodes in your deployment.

Step 2 Click the Table view.

Step 3 Click the quick picker (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format in the Deployment Nodes page. The Deployment Nodes page displays the Cisco ISE nodes that you have registered along with their names, personas, roles, and the replication status for the secondary nodes in your deployment.

Step 4 Choose a Cisco ISE node from the Deployment Nodes page.

Note 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 have the option to configure each node as a Cisco ISE node (Administration, Policy Service, and Monitoring personas) or an Inline Posture node.

Step 5 Click **Edit**.

The Edit Node page appears. This page contains the General settings tab that is used to configure the Cisco ISE deployment. This page also features the Profiling Configuration tab, which is used to configure the probes on each node.

Note If you have the Policy Service persona disabled, or if enabled but the Enable Profiler services option is not selected, then the Cisco ISE administrator user interface does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any Cisco ISE node, Cisco ISE displays only the General settings tab. It does not display the Profiling Configuration tab that prevents you from configuring the probes on the node.

Step 6 On the General settings tab, check the **Policy Service** check box, if it is already active.

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

Step 7 For the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services, check the **Enable Session Services** check box, if it is not already active. To stop the session services, uncheck the **Enable Session Services** check box.

Note 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 8 Click **Save** to save the node configuration.

Posture Compliance Dashlet

The Posture Compliance dashlet summarizes the posture compliance in percentage, and Mean Time To Remediate (MTTR) data for the last 24 hour period, as well as 60 minutes from the current system time. It refreshes data every minute and displays it in the dashlet. You can invoke the Posture Detail Assessment report from the tool tips that are displayed on the 24 hour and 60 minutes spark lines for a specific period. The stack bars display the posture noncompliance distribution of endpoints by operating systems and the reason for failures of the requirements.

The MAC address is used as a key to calculate MTTR.

The dashlet provides you the following distribution details for the last 24 hour period, as well as 60 minutes from the current system time.

Table 20-1 describes the details, which are shown in the Posture Compliance dashlet on Cisco ISE.

Table 20-1 Posture Compliance Dashlet

Name	Description
Passed in percentage	Displays the percentage (passed percentage) of posture compliance of endpoints by using posture compliance and noncompliance of endpoints.
Mean Time to Remediate (MTTR)	Displays the mean time difference between endpoints moving from the noncompliant state to the complaint state based on the unique MAC address.
Operating System	Displays the noncompliance distribution by operating system that is running on the client.
Reason	Displays the noncompliance distribution by failures of posture conditions.

Viewing Posture Reports

Cisco ISE provides you with various reports on posture, and troubleshooting tools that you can use to efficiently manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to look into more details. For large reports, you can also schedule reports and download them in various formats.

For more information on how to generate reports and work with the interactive viewer, see Chapter 25, "Reporting."

For more information on posture reports see the "Standard Reports" section on page 20-9.

Standard Reports

For your convenience, the standard reports present a common set of predefined report definitions. You can click on the Report Name link to run the report for today. You can query the output by using various system predefined parameters. You can enter specific values for these parameters.

You can use the Run button to run the report for a specific period, as well as use the Query and Run option. The Query and Run option allows you to query the output by using various parameters. The Add to Favorite button allows you to add your reports that you use frequently to the Operations > Reports > Favorites location. The Reset Reports button allows you to reset your reports in this catalog to factory defaults.

You can run the reports on posture from the following location:

Operations > Reports > Catalog > Posture.

The following are the standard reports for posture:

- Posture Detail Assessment—A report to view the posture authentication summary information for a particular user for a selected time period
- Posture Trend—A report to view the count of passed/failed and status information for a particular policy along with the graphical representation for a selected time period

Posture Administration Settings in Cisco ISE

After you deploy Cisco ISE on your network, you can globally configure Cisco ISE to download updates automatically through web to the Cisco ISE server, or updates that can be done offline later.

For information on posture updates, see the "Posture Updates" section on page 20-22.

In addition, the NAC Agents and Web Agents, which are 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.

For information on posture periodic assessment of clients for compliance that NAC Agents and Web Agents do, see the "Posture Reassessments" section on page 20-13.

For information on accepting network usage policies for your network, see the "Posture Acceptable Use Policy" section on page 20-25.

This section describes the configuration settings that you define for clients to remediate on Cisco ISE, periodic reassessments of clients for compliance that NAC and Web Agents check periodically and report to Cisco ISE. It describes the configuration settings that you define for Cisco ISE updates with Cisco rules, checks, antivirus and antispyware charts, and operating system support. It also provides information on the configuration settings that end users must comply with network usage policies for using your network resources.

This section provides procedures that describe the following topics:

- Posture General Settings, page 20-10
- Posture Reassessments, page 20-13
- Posture Updates, page 20-22
- Posture Acceptable Use Policy, page 20-25

Posture General Settings

The posture general settings for agents on Windows clients and Macintosh clients can be configured in client provisioning resources. Here, you can configure agent profiles in client provisioning by setting the timers used for remediation and transition of clients posture state on your network, and also setting the timer to close the login success screens automatically on agents without user intervention.

You can configure all these timers for agents on Windows clients and Macintosh clients in client provisioning resources in Policy > Policy Elements > Results > Client Provisioning > Resources > Add > New Profile.

For more information on creating agent profiles and setting agent profile parameters, see the "Agent Profile Parameters and Applicable Values" section on page 19-16.

We recommend configuring agent profiles with remediation timers, network transition delay timers and the timer used to control the login success screen on client machines so that these settings are policy based. 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 to accomplish the same goal.

Remediation Timer

You can configure the timer for clients to remediate themselves within the time specified in the timer after failing to meet all the requirements defined in the posture policies for compliance. 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 and Web Agents send a report to the posture run-time services after which the clients are moved to the noncompliance state. The remediation timer default value is four minutes.

Network Transition Delay Timer

You can configure the timer for clients to transition from one state to the other state within a specified time as specified in the network transition delay timer, which is required for Change of Authorization (CoA) to complete for clients to move from one state to the other state. This timer is used for clients in both successful and failure of posture. 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.

Default Posture Status

You can configure the posture status of endpoints to compliant or noncompliant for endpoints that run on Linux and iDevices like iPad and iPod (non-agent devices). The same settings also apply to endpoints that run on Windows and Macintosh operating systems when there is no client provisioning policy matching found during posture runtime.

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 19-31.

iDevices and Android Smart Phones

When an Android device and Apple iDevices such as iPod, iPhone, and iPad connect to your Cisco ISE enabled network via WLC (that supports CoA), CoA Session Termination is issued.

If these devices connect to your Cisco ISE enabled network via VPN/iPEP, then CoA Re-Auth is issued and the posture status of those devices will take the Default Posture Status settings in Cisco ISE.

Successful Login Screen

After login and successful posture assessment, the NAC Agents and Web Agents display a temporary network access screen. Here, the agents display a network usage term and conditions link for end users to accept the network usage policies that you define for your network. If end users reject network usage policies from the temporary network access screen, then they are denied to access your network. If they accept the network usage policies, then the agents display the login success screen and permit network access.

This section describes the following posture general settings that you configure for clients in posture:

- Remediation Timer—Specifies the time, in minutes, required for any type of remediation within which the clients need to remediate from the noncompliance state to the compliance state
- Network Transition Delay—Specifies the time, in seconds, for network transition for both success and failure of client posture on your network
- Default Posture Status—Specifies the posture status for clients that do not run supported operating systems in Cisco ISE
- Successful Login Screen—Specifies the time out, in seconds, that closes the login success screen without user intervention.

You can use the posture General Settings page to configure the timers for remediation, network transition, and closing the login success screen on Windows clients.

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

The Settings navigation pane appears.

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand Posture.

Step 4 Click **General Settings**.

The Posture General Settings page appears.

Tip The information icon next to the Posture General Settings page title provides the following message: “These settings will be used if there is no profile under client provisioning policy.”

Step 5 Enter a time value, in minutes, in the Remediation Timer text box.

The default value is 4 minutes. You can configure the remediation timer. The information icon displays Valid range between 1 to 300 minutes.

Step 6 Enter a time value, in seconds, in the Network Transition Delay text box.

The minimum default value is 3 seconds. You can configure the network transition delay timer. The information icon displays Valid range between 2 to 30 seconds.

Step 7 From the Default Posture Status, choose the option from the drop-down list.

You can configure the posture status of endpoints as **Compliant** or **Noncompliant**. The information icon displays: “Provides posture status for non-agent devices (i.e. Linux based operating systems), and endpoints for which no agent installation policy applies.”

Step 8 Check the **Automatically Close Login Success Screen After** check box.

Step 9 Enter a time value, in seconds, in the Automatically Close Login Success Screen After check box.

When you check the check box, and configure the time in seconds, the NAC Agents and Web Agents display the login success screen till the time out occurs. This setting allows clients to login into your network failing which the login success screen is closed automatically. You can configure the timer to close the login screen automatically between 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.

Tip The information icon next to the Automatically Close Login Success Screen After text field displays the following message: “Setting the time to zero seconds will not display the login success screen. Valid range: 0-300 seconds.

Step 10 Click **Save** to save the current input data.

To reset the posture general settings, complete the following steps:

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

The Settings navigation pane appears.

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand Posture.

Step 4 Click **General Settings**.

The Posture General Settings page appears.

Step 5 Edit one of the following settings:

Enter a time value (current input data), in minutes, in the Remediation Timer text box.

or

Enter a time value (current input data), in seconds, in the Network Transition Delay text box.

or

From the Default Posture Status field, choose the option from the drop-down list.

The following options appear: Compliant (default), NonCompliant

or

Check to enable, or uncheck to disable the **Automatically Close Login Success Screen After** check box.

Step 6 Click **Save** to save the current input data or **Reset** to restore previous data.

Posture Reassessments

This section describes the periodic reassessment (PRA) configurations for clients that are successfully postured already for compliance on your network. PRA cannot occur if clients are not compliant on your network.

For more information on initiating and requesting a PRA, see the Initiating and Requesting a PRA, page 20-13.

For more information on PRA failure action configuration, see the PRA Failure Actions, page 20-13.

For more information on PRA and a user identity group (role) assignment, see the User Identity Group (Role) Assignment, page 20-14.

For more information on PRA report tracking and enforcement, see the PRA Report Tracking and Enforcement, page 20-15

For more information on PRA enforcements when Cisco ISE distributed deployment failures, see the PRA Enforcement During Distributed System Failure, page 20-15

Initiating and Requesting a PRA

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.

Note 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 PostureStatus attribute of any client before reassessment of new requirements and posture policies retrieved from the server in a PRA request should represent the posture status as unknown in a PRA request assuming that the client is being postured after successful authentication.

PRA Failure Actions

If the client is not compliant, the policy service node activates a PRA failure action. The PRA failure action that will be taken is either to continue so that the client continues to access your network or log off from your network or remediate itself.

If you associate a user to different roles and each associated role is configured with different PRA failure actions (logoff, remediate, and continue) then the *logoff* action is applied on the endpoint.

The following enforcement types apply to PRA failure actions:

- Continue
- Logoff
- Remediate

PRA Failure Action to Continue

In this scenario, the client is not compliant, and the configured PRA failure action is to continue. This failure action to continue does not allow the user to remediate the client and the NAC Agent does not show the user the need to remediate the client for compliance. Instead, the user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement, which is set to mandatory or optional.

PRA Failure Action to Logoff

In this scenario, the client is not compliant, and the configured PRA failure action is to force the client to log off from your network. The agent sends a logoff request to the policy service node, and the client logs off. The client logs in again, and its compliance status is unknown for the current session.

PRA Failure Action to Remediate

In this scenario, the client is not compliant, and the configured PRA failure action is to remediate. The agent waits for a specified time for the remediation to occur. After the client has remediated, the agent sends the PRA report to the policy service node. If the remediation is ignored on the client, then the agent sends a logoff request to the policy service node to force the client to log off from your network and log in again to remediate for compliance.

If the posture requirement is set to mandatory, then the RADIUS session will be cleared as a result of the PRA failure action and a new RADIUS session has to start for the client to be postured again.

If the posture requirement is set to optional, then the NAC Agent allows the user to click the continue option from the agent. The user can continue to stay in the current network without any restriction.

User Identity Group (Role) Assignment

You can configure each PRA to a user identity group (a role) that is defined in the system. If you configure a PRA with a role *Any* then only the configuration with the role *Any* exists, and no other configurations can exist in the system.

The following section summarizes the PRA configuration to a user identity group:

1. Ensure that each PRA configuration has a unique group or a unique combination of user identity groups assigned to the configuration.

   Note You can assign a role_test_1 and a role_test_2, 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.

2. Ensure that two PRA configurations cannot have a user identity group in common.
3. If a PRA configuration already exists with a user identity group "*Any*", you cannot create other PRA configurations unless you perform the following:
   a. You update the existing PRA configuration with a user identity group "*Any*" to reflect a user identity group (or user identity groups) other than *Any*.

      or

   b. You delete the existing PRA configuration with a user identity group "*Any*".

Note If you *must* create a PRA configuration with a user identity group *“Any”,* ensure that you delete all other PRA configurations from the Reassessment configurations.

PRA Report Tracking and Enforcement

You can keep track of the PRA reports from the NAC Agent and enforce PRA on the clients that are already successfully postured on your network.

Upon successful compliance for posture, the NAC Agent validates the client for compliance and sends the compliance reports to the policy service node. The NAC Agent periodically sends the PRA requests for reassessment based on the interval that is specified in the configuration.

If the policy service node does not receive the PRA report within the maximum wait interval period, then the policy service node assigns the client to the unknown status and the client needs to be checked again for posture compliance. The maximum wait interval is an interval between two consecutive compliance (PRA) reports from the NAC Agent sent to the policy service node before the execution of a PRA failure action for noncompliance and the end of the client session.

Note The maximum wait interval is the sum of the PRA interval and twice the grace time that is configured in the PRA configuration as maximum wait interval = PRA interval + (grace time * 2).

PRA Enforcement During Distributed System Failure

The PRA is not supported in cases where policy service nodes fail in the distributed environment.

You cannot enforce a PRA on your clients, and the clients stay connected on your network regardless of their compliance in the event of a failure in the distributed environment. The agents stop sending the PRA requests to the policy service nodes.

Configuring Client Posture Periodic Reassessments

Upon successful compliance for posture, the NAC Agents validate the compliance of clients, and periodically send the compliance reports to the Cisco ISE policy service node. The Cisco ISE policy service nodes check the relevant policies and compiles requirements depending on the client roles that are defined in the configuration to enforce a periodic reassessment. The Cisco ISE policy service nodes then respond to the NAC Agents with PRA attributes defined in the PRA configurations. As you associate a user to more than one user identity group (user identity groups), the PRA configurations are applied according to the most restricted attributes on the relevant role’s related configurations.

The following are the most restricted configuration definitions for the PRA attributes:

- Use reassessment enforcement—Requires at least one configuration and has its reassessment required flag on the PRA configuration
- Interval—The least interval of all the relevant PRA configurations
- Grace time—The least interval of all the relevant PRA configurations
- Enforce type—The most restricted enforcement type is logoff; after log off, the client must remediate and then continue.

You can use the Reassessment configurations page to display and manage the periodic reassessments for a posture.

This section describes the procedures you use to configure the periodic reassessment configurations:

- Creating, Duplicating, Editing, and Deleting a Client Posture Periodic Reassessment, page 20-16
- Filtering Client Posture Periodic Reassessments, page 20-19

Creating, Duplicating, Editing, and Deleting a Client Posture Periodic Reassessment

This section describes the periodic reassessment configuration that you can create in Cisco ISE for your clients after they are successfully postured.

The Reassessment configurations page displays existing configurations that are configured to groups along with their names, description, and the action enforced on the clients when the clients fail posture assessment. You can create, duplicate, edit, delete, or filter a PRA from the Reassessment configurations page. Once created and saved a PRA, you can see existing PRA configurations, and the groups to which the PRA configurations apply on the Reassessment configurations page.

To create a periodic reassessment, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you create.

Step 5 Click **Add**.

Step 6 Modify the values in the New Reassessment Configuration page to create a new PRA, as shown in Table 20-2 on page 20-18.

Step 7 Click **Submit** to create a PRA configuration.

Click **Cancel** to return to the Reassessment configurations page if you do not want to add a new PRA.

To duplicate a periodic reassessment, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you create. PRA configurations display the user identity groups to which existing PRAs are configured in the configurations list.

Step 5 Click a PRA that you want to duplicate, and click **Duplicate** to create a copy of a PRA.

Step 6 Click **Submit**.

Click **Cancel** to return to the Reassessment configurations page if you do not want to create a copy of a PRA.

To edit a periodic reassessment, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 5 Click the PRA that you want to edit, and click **Edit** to edit a PRA.

Step 6 Click **Save** to save the changes made to the PRA.

The PRA will be available in the Reassessment configurations page after you edit the PRA, as well as appear in the PRA configurations group box that displays the groups to which existing PRAs are configured in the configurations list.

Step 7 Click the **Reassessment Configurations List** link from the edit page to return to the Reassessment configurations page.

To delete a periodic reassessment, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 5 Click the PRA that you want to delete, and click **Delete**.

A confirmation dialog appears with the following message: “Are you sure you want to delete?”.

Step 6 Click **OK** to delete a PRA.

Click **Cancel** to return to the Reassessment configurations page without deleting a PRA.

Table 20-2 describes the fields in the New Reassessment Configuration page that allow you to create, duplicate, and edit a PRA.

Table 20-2 PRA Configurations

Field Name	Field Description
Configuration Name	In the Configuration Name text box, enter the name of the PRA configuration that you want to create.
Configuration Description	In the Configuration Description text box, enter the description of the PRA configuration.
Use Reassessment Enforcement?	When the Use Reassessment Enforcement check box is checked, the PRA configurations configured for the user identity groups are applied. If unchecked, the PRA configurations configured for the user identity groups are not applied.
Enforcement Type	If clients fail to meet the posture requirement, then one of the following actions is enforced on the client. View the predefined settings in the drop-down list: • Continue • Logoff • Remediate Choose one from the list.
Interval	In the Interval text box, enter a time interval specified in minutes to initiate PRA on the clients thereafter first successful log in. The information icon next to the Interval field provides you with the minimum and maximum interval that you can set for PRAs. The minimum interval can be 60 minutes (one hour), and the maximum interval can be 1440 minutes (24 hours) for PRAs. The default interval time is specified as 240 minutes (4 hours).
Grace time	In the Grace Time text box, enter a time interval specified in minutes to allow the client to complete remediation. The grace time cannot be zero, and greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval. The information icon next to the Grace time field provides you the minimum and maximum interval that you can set for PRAs. The minimum grace time can be 5 minutes and the maximum grace time can be 60 minutes. **Note** The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.

Table 20-2 PRA Configurations (continued)

Field Name	Field Description
Select User Identity Groups	In the Select User Identity Groups text box, choose a unique group, or a unique combination of groups for your PRA configuration. Note the following while creating a PRA configuration: • Each configuration must have a unique user identity group, or a unique combination of user identity groups. • No two configurations can have any user identity group in common. • If you want to create a PRA configuration with a user identity group "Any", delete all other PRA configurations first. • If you create a PRA configuration with a user identity group "Any", then you cannot create other PRA configurations with a unique user identity group, or user identity groups. To create a PRA configuration with a user identity group other than "Any", either delete an existing PRA configuration with an user identity group "Any" first, or update an existing PRA configuration with a user identity group "Any" with a unique user identity group, or user identity groups.
PRA configurations—configurations list	An area that lists existing PRA configurations and user identity groups associated to PRA configurations.

Filtering Client Posture Periodic Reassessments

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Reassessment configurations page. A quick filter is a simple filter that can be used to filter periodic reassessments in the Reassessment configurations page. The quick filter filters periodic reassessments based on field description, such as the name of the periodic reassessments, description, action enforced on the clients when clients fail posture assessment, user identity groups to which periodic reassessments are configured, and periodic reassessments that are enabled or disabled in the Reassessment configurations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Reassessment configurations page. The advanced filter filters periodic reassessments based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Reassessment configurations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the filtered results on the Reassessment configurations page. You can also edit preset filters and remove them from the preset filters list.

To filter periodic reassessments, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 5 From the Reassessment configurations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-3.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-20 and To filter by using the Advanced Filter option, complete the following steps:, page 20-20.

Note To return to the Reassessment configurations page, choose **All** from the Show drop-down list to display all the periodic reassessments without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters periodic reassessments based on each field description in the Reassessment configurations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Reassessment configurations page. If you clear the field, it displays the list of all the periodic reassessments in the Reassessment configurations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Reassessment configurations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter periodic reassessments by using variables that are more complex. It contains one or more filters, which filter periodic reassessments based on the values that match the field description. A filter on a single row filters periodic reassessments based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter periodic reassessments by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add a filter, or click **Remove Row** (minus [-] sign) to remove the filters.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**, or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click Cancel to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-3 describes the fields that allow you to filter the PRAs:

Table 20-3 Filtering Reassessment Configurations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter periodic reassessments by the name of the periodic reassessment.
	Description	This field enables you to filter periodic reassessments by the description of the periodic reassessment.
	Type	This field enables you to filter periodic reassessments by actions enforced on the client.
	User Identity Groups	This field enables you to filter periodic reassessments by user identity groups configured for periodic reassessments.
	Enable	This field enables you to filter periodic reassessments by those reassessments that are enabled.
Advanced Filter	Choose the field description from the following: • Name • Description • Type • User Identity Groups • Enable	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter periodic assessments from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter periodic assessments from the Value drop-down list.

Posture Updates

Prerequisite

If the default Update Feed URL is not reachable, you must configure the proxy settings in Administration > System > Settings > Proxy.

For more information on proxy settings, see Specifying Proxy Settings in Cisco ISE, page 8-17.

Updates for posture include a set of predefined checks, rules, antivirus and antispyware support charts for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco. You can download posture updates from Cisco to your Cisco ISE deployment through the web dynamically, as well as configure updates to occur automatically after allowing a time delay within a maximum of 24 hours in hh:mm:ss format. Thereafter, Cisco ISE checks and downloads updates at specified intervals from the initial updates automatically. 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 initially posture updates from the web. This process usually takes approximately 20 minutes. Thereafter, you can configure to check, and download incremental updates to occur automatically on Cisco ISE without user intervention. Once updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information.

Note 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 updates that you perform either manually or using scheduled posture updates.

This section provides procedures that describe dynamic and offline update configurations for posture updates.

- Dynamic Posture Updates, page 20-22
- Offline Posture Updates, page 20-25

Related Topics

Custom Conditions for Posture, page 20-42

Dynamic Posture Updates

You can use the Posture Update page to download updates dynamically from the web, and configure updates to occur automatically after allowing a time delay from the initial updates. Thereafter, you can check for and download updates at regular intervals without user intervention.

To download updates dynamically from the web, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Updates**.

The Posture Updates page appears.

Step 5 In the Posture Updates page, choose the **Web** option to download updates dynamically.

Step 6 Click **Set to Default** to set the Cisco default value for the Update Feed URL field.

For example, the default Update Feed URL is https://www.cisco.com/web/secure/pmbu/posture-update.xml.

Note If this default Update Feed URL is not reachable, then you can configure the proxy settings alternatively on the Posture Updates page. For more information on proxy settings, see Specifying Proxy Settings in Cisco ISE, page 8-17.

Step 7 Modify the values on the Posture Updates page, as shown in Table 20-4.

Step 8 Click **Update Now** to download updates from Cisco.

Cisco ISE displays an information dialog with the following message:

"The update might take up to 20 minutes to finish. Navigating to other pages will not stop the updating and you can check the result on this page later."

Step 9 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.

Note Downloading updates dynamically from the web may take a few minutes for the first time to update the Cisco ISE server. When an update is in progress, you can leave the updates page to continue with other tasks on Cisco ISE. If an update is in progress, then you will see a waning dialog displayed on the updates page when you return to the Posture Updates page. When an update is in progress, Cisco ISE displays a warning dialog with the following warning message: "There is already an update running. Please try later."

After an initial update, you can configure to check for updates and download updates to your Cisco ISE deployment automatically on the Posture Updates page. Cisco ISE downloads updates at specified intervals from the web automatically after an allowed initial delay from the first time updates.

To continue to check for updates automatically and download at a specified interval from the initial updates, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Updates**.

The Posture Updates page appears.

Step 5 Check the **Automatically check for updates starting from initial delay** check box.

Step 6 Enter the initial delay time in hh:mm:ss format.

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

Step 7 Enter the time interval in hours.

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

Step 8 Click **Yes** to continue.

Step 9 Click **Save** to download updates at regular intervals from the initial time delay.

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.

Table 20-4 describes the fields that allow you to download updates dynamically from the web, or offline.

Table 20-4 Update Configurations

Field	Field Description
Posture Updates options	The following options are available for Posture updates on Cisco ISE: Web and Offline.
Update Feed URL	A valid URL to update from the web. For example: https://www.cisco.com/web/secure/pmbu/posture-update.xml
Set to Default	Click to set the Cisco default URL for Update Feed URL.
Proxy Address	The IP address of the configured proxy server.
Proxy Port	The port of the configured proxy server.
Automatically check for updates starting from initial delay check box	This allows automatically to check Cisco ISE for updates after the delay time is over, and thereafter download updates at regular intervals. Click this check box.
An initial delay time specified in hh:mm:ss format, after which Cisco ISE checks for updates	Cisco ISE starts checking for updates after an initial delay time has passed. From the drop-down list, choose the initial delay time in hh:mm:ss format after which Cisco ISE should start to check for updates.
An interval specified in hours, at which Cisco ISE downloads updates automatically from the initial delay time.	Enter the interval hours of time at which Cisco ISE should download updates automatically from the initial delay time.

Offline Posture Updates

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 1.1.x*.

Posture Acceptable Use Policy

After login and successful posture assessment of clients, the NAC Agents and Web Agents display a temporary network access screen. The agents display a link on the temporary network access screen for users to click the link that redirects users to a page, where you can define your network usage terms and conditions that users must read, and accept the network usage policies.

Each Acceptable Use Policy (AUP) configuration must have a unique user identity group, or a unique combination of user identity groups. Even though a user can be associated to multiple user identity groups in Cisco ISE, and there are different AUP configurations for a unique user identity group, or a unique combination of user identity groups, Cisco ISE looks for the user identity groups and the associated AUP configuration for the 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 to display the AUP of the first matched user identity group. The user can click the link to accept the network usage policies after which the user gets access privileges to your network.

Authorization Profile Configuration Guidance for Posture Clients Quarantine State

This section describes you through the configuration when clients are moved into quarantine state due to end users deny to comply with your network usage policies, or when clients fail to meet the mandatory requirements.

Without accepting the network usage terms and conditions, even though clients meet all the mandatory requirements that are defined in the posture assessment policies the clients are denied network access to your network, and moved into a quarantine state. If clients are moved into the quarantine state, they will not be able to reauthenticate again in order to be postured successfully for compliance again. If clients need to come out of the quarantine state and become compliant, then the network access devices must be configured to restart a new RADIUS session after the session times out so that clients can reauthenticate again depending on your configuration, and then agree to the network usage policies of your network.

You can choose an authorization profile and configure it using the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page.

For more information on authorization policies and profiles, see Chapter 17, “Managing Authorization Policies and Profiles.”

You can choose the Access-Accept option from the Access Type drop-down list, and configure information for reauthentication under Common Tasks, or under Advanced Attributes Settings for an authorization profile.

For example, you can configure the value of RADIUS: Termination-Action attribute to Default, and the RADIUS: Session-Timeout attribute to a time value under Common Tasks > Re-authentication, or under Advanced Attributes Settings. If the value of RADIUS: Termination-Action attribute is set to RADIUS-Request, the NAS sends a new Access-Request to the RADIUS server, including the state attribute, if any upon termination of the specified service. This configuration allows you to set a timeout value for a quarantine state. After the time out, a new RADIUS session can be started and the client can reauthenticate again and check for posture.

- RADIUS: Termination-Action—An action, which should be taken by the NAS when the specified service is completed. It is only used in Access-Accept message.
- RADIUS: Session-Timeout—A timeout value specified in maximum number of seconds of service to be provided to the user before termination of the RADIUS session, where the client remains connected by the NAS. It is an attribute to be sent by the RADIUS server to the client in an Access-Accept, or Access-Challenge messages.

In addition to the above, you have to enter the following additional commands for your network device:

- authentication periodic—use this interface configuration command to enable, or disable re-authentication on a port. Enter the no form of this command to disable re-authentication.

  This CLI command shows how to enable periodic re-authentication on a port.

  ```
  Switch(config-if)# authentication periodic
  ```
- authentication timer reauthenticate server—use this interface configuration command to configure the time out and re-authentication parameters for an 802.1x-enabled port.

  This CLI command shows how to set the re-authentication timer where reauthenticate specifies time in seconds after which an automatic re-authentication attempt should start, and server specifies an interval in seconds after which an attempt can be made to authenticate an unauthorized port.

  authentication timer—interface configuration command

  reauthenticate—specifies time in seconds after which an automatic re-authentication attempt starts. It is set to one hour.

  server—specifies interval in seconds after which an attempt is made to authenticate an unauthorized port

  ```
  Switch(config-if)# authentication timer reauthenticate server
  ```

Configuring Acceptable Use Policies

You can view, create, delete, or filter acceptable use policies (AUPs) on the Acceptable Use Policy Configurations page. It displays all the AUPs with their names, description, type, the name of the zipped file, or the URL that contains the network usage policies depending on the type of the AUPs, and the user identity groups to which they are configured.

This section covers the following procedures:

- Viewing, Adding, and Deleting an Acceptable Use Policy, page 20-26
- Filtering Acceptable Use Policies, page 20-29

Viewing, Adding, and Deleting an Acceptable Use Policy

You can use the Acceptable Use Policy Configurations page to view, create, or delete acceptable use policies, which allow network access to clients after acceptance of the network usage policies.

To view an acceptable use policy, complete the following steps:

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

Step 2 From the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 Click an acceptable use policy from the list.

Step 6 Click **View** to view the acceptable use policy.

Step 7 Click the **Acceptable Use Policy Configuration list** link to return to the Acceptable Use Policy Configuration page.

Click **Cancel** to return to the Acceptable use policy configuration page. A confirmation dialog appears with the following message: "Are you sure you want to cancel? You will lose all the changes you have made." Click **Yes** to return to the Acceptable use policy configuration page. If you click **No**, you are on the same page.

To create an acceptable use policy, complete the following steps:

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

Step 2 From the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 Click **Add**.

Step 6 Modify the values on the New Acceptable Use Policy Configuration page, as shown in Table 20-5.

You can configure a new AUP for a user identity group on the Acceptable Use Policy Configurations page.

Step 7 Click **Submit** to create an AUP configuration.

Step 8 Click **Cancel** to return to the Acceptable Use Policy Configurations page if you do not want to add a new AUP from this page.

To delete an acceptable use policy, complete the following steps:

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

Step 2 From the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 Choose an acceptable use policy that you want to delete.

Step 6 In the Acceptable Use Policy Configurations page, choose **Delete**.

A confirmation dialog appears with the following message: "Are you sure you want to delete?".

Step 7 Click **OK** to delete an AUP.

Step 8 Click **Cancel** to return to the Acceptable Use Policy Configurations page without deleting the AUP that you selected.

Table 20-5 describes the fields that allow you to create an AUP configuration on the Acceptable use policy configurations page.

Table 20-5 AUP Configurations

Field	Field Description
Configuration Name	In the Configuration Name text box, enter the name of the AUP configuration that you want to create.
Configuration Description	In the Configuration Description text box, enter the description of the AUP configuration that you want to create.
Show AUP to Agent users (for NAC Agent and Web Agent on Windows only)	If checked, the Show AUP to Agent users check box displays users (for NAC Agents, and Web Agents on Windows only) the link to network usage terms and conditions for your network and click it to view the AUP upon successful authentication and posture assessment.
Use URL for AUP message radio button	When selected, you must enter the URL to the AUP message in the AUP URL, which clients must access upon successful authentication and posture assessment.
Use file for AUP message radio button	When selected, you must browse to the location and upload a file in a zipped format in the AUP File, which contains the index.html at the top level. The .zip file can include other files and subdirectories in addition to the index.html file. These files can reference each other using HTML tags.
AUP URL	In the AUP URL, enter the URL to the AUP, which clients must access upon successful authentication and posture assessment.
AUP File	In the AUP File, browse to the file and upload it to the Cisco ISE server. It should be a zipped file and the zipped file should contain the index.html file at the top level.

Table 20-5 AUP Configurations (continued)

Field	Field Description
Select User Identity Groups	In the Select User Identity Groups drop-down list, choose a unique user identity group, or a unique combination of user identity groups, for your AUP configuration. Note the following while creating an AUP configuration: • Posture AUP is not applicable for a guest flow • Each configuration must have a unique user identity group, or a unique combination of user identity groups • No two configurations have any user identity group in common • If you want to create a AUP configuration with a user identity group "Any", then delete all other AUP configurations first • If you create a AUP configuration with a user identity group "Any", then you cannot create other AUP configurations with a unique user identity group, or user identity groups. To create an AUP configuration with a user identity group other than Any, either delete an existing AUP configuration with a user identity group "Any" first, or update an existing AUP configuration with a user identity group "Any" with a unique user identity group, or user identity groups.
Acceptable use policy configurations—Configurations list	Lists existing AUP configurations and end user identity groups associated to AUP configurations.

Filtering Acceptable Use Policies

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Acceptable Use Policy Configurations page. A quick filter is a simple filter that can be used to filter acceptable use policies in the Acceptable Use Policy Configurations page. The quick filter filters acceptable use policies based on the field description such as the name of the acceptable use policies, description, URL of the acceptable use policy, user identity groups to which acceptable use policies are configured, acceptable use policies that are enabled, or disabled in the Acceptable Use Policy Configurations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Acceptable Use Policy Configurations page. The advanced filter filters acceptable use policies based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Acceptable Use Policy Configurations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the filtered results in the Acceptable Use Policy Configurations page. You can also edit preset filters and remove them from the preset filters list.

To filter acceptable use policies, complete the following steps:

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

Step 2 In the Settings navigation pane, choose **Posture**.

Step 3 Click the right arrow to expand posture.

Step 4 Click **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 In the Acceptable Use Policy Configurations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-6.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-30 and To filter by using the Advanced Filter option, complete the following steps:, page 20-30.

Note To return to the Acceptable Use Policy Configurations page, choose **All** from the Show drop-down list to display all the acceptable use policies without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters acceptable use policies based on each field description in the Acceptable Use Policy Configurations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Acceptable Use Policy Configurations page. If you clear the field, it displays the list of all the acceptable use policies in the Acceptable Use Policy Configurations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Acceptable Use Policy Configurations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter acceptable use policies by using variables that are more complex. It contains one or more filters, which filter acceptable use policies based on the values that match the field description. A filter on a single row filters acceptable use policies based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter acceptable use policies by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-6 describes the fields that allow you to filter the AVPs:

Table 20-6 Filtering Acceptable Use Policy Configurations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter acceptable use policies by the name of the acceptable use policy.
	Description	This field enables you to filter acceptable use policies by the description of the acceptable use policy.
	Type	This field enables you to filter acceptable use policies by the type that a file is used, or the remote location of the acceptable use policy.
	File Name/URL	This field enables you to filter acceptable use policies by the file name that is used or the remote location of the acceptable use policy.
	User Identity Groups	This field enables you to filter acceptable use policies by the user identity groups configured for acceptable use policies.
	Enabled	This field enables you to filter acceptable use policies by AUPs that are configured to display, or not to agent users (for NAC Agent and Web Agent on Windows only). • True—Displays AUP to agent users • False—Does not display AUP to agent users

Table 20-6 Filtering Acceptable Use Policy Configurations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type • File Name/ URL • User Identity Groups • Enabled	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter acceptable use policies from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter acceptable use policies from the Value drop-down list.

Client Posture Assessments in Cisco ISE

The posture service assists in determining the compliance of endpoints that are accessing your Cisco ISE-enabled network by using posture policies based on posture requirements, which are associated to posture policies. It evaluates the configured posture policies for all the endpoints that are connecting to your network, which are associated to one or more identity groups to which the users belong, and the operating systems that are installed on the clients. The NAC Agents that are installed on your clients interact with the Cisco ISE posture service, and evaluate the posture policies which are configured for your clients.

In addition, you should have an understanding of how Cisco ISE provides support for operating systems that are installed on the clients for posture.

Support for Hierarchical Operating Systems

Cisco ISE provides support to all the Windows and Macintosh operating systems, which are structured in a hierarchical group. You can also select an individual operating system from the hierarchy. A parent group includes the operating system versions for the group, and each version of the group includes the underlying operating system versions. When you select a parent group of an operating system from the hierarchy, you implicitly select all the underlying operating systems of the parent group. The posture conditions apply to all the underlying versions of the operating systems when you select the parent group or the group.

For example, when you choose Windows All from the Operating Systems drop-down list while creating a posture policy for posture in Cisco ISE, a condition that you define in the posture policy applies to all Microsoft Windows operating systems and their underlying operating systems, which includes Microsoft Windows 7 (All), Microsoft Windows Vista (All), Microsoft Windows XP (All), and their underlying operating systems for Windows All.

Filtering by Operating System

The selection of an operating system within the hierarchy implements the filtering of conditions, compound conditions and requirements that overrides a parent operating system Group associated to a simple condition. This implementation filters conditions, compound conditions and requirements by using the operating system that is associated with the compound condition. If you have a simple condition that is associated with a parent operating system group and a compound condition that is associated with the underlying version from the parent operating system group, then the filtering is based only on the underlying version of the operating system that is associated in the compound condition.

For example, you might have a simple condition that is associated with the Windows Vista parent operating system group. And you might also have a compound condition that is associated with the underlying version of Windows Vista from the operating system group. However, the filtering is done using only the underlying version of the operating system that is associated in the compound condition.

Dynamic Support for Operating System Version

You can configure the posture policies for an endpoint that is associated with the role to which you belong, as well as the operating system on the client. The posture configurations that you save apply only at the group level of an operating system that is not at the operating system level. This level of application allows you to map multiple versions of an operating system that is structured in the hierarchical groups.

For example, when you choose the Windows All option from the operating system group, you are choosing the hierarchical structure of all of the Windows 7, Windows Vista, and Windows XP groups that contain each of their underlying versions.

Cisco ISE dynamically supports new versions of client operating systems and agents, including both the Windows and Macintosh NAC agents and NAC Web agent. Located on the ISE server, the osgroups.xml file is automatically updated by Cisco to reflect the latest version support information. If an agent sends the Cisco ISE server an operating system version that is not listed in the osgroups.xml file, then you cannot continue to work with the posture service through the agents.

Related Topics

- Client Posture Assessment Policies, page 20-33
- Client Posture Assessment Requirements, page 20-151

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Client Posture Assessment 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.

Here, posture requirements are associated to the posture policies and also optional dictionary attributes where you can use dictionary simple and compound conditions from the library or create new dictionary simple and compound conditions.

Prerequisite:

You must have an understanding of acceptable use policy (AUP) and posture reassessments (PRA) as you create posture policies with respect to posture compliance.

For more information on AUP, see Posture Acceptable Use Policy, page 20-25 and on PRA, see Posture Reassessments, page 20-13.

In addition, see the following:

- Dictionary Simple Conditions, page 20-100
- Dictionary Compound Conditions, page 20-105
- Configuring Time and Date Conditions, page 17-24

You can use the Posture Policies page to insert (create) a new policy, or duplicate an existing policy, or delete an existing policy.

Table 20-7 describes the fields in the Posture Policies page that allow you to insert a new posture policy, or duplicate an existing policy. or delete an existing posture policy.

Table 20-7 Posture Policy

Field	Field Description
Status	Choose an option from the drop-down list. It can be used to enforce, or not to enforce a posture assessment policy for evaluation.
Rule Name	In the Rule Name text box, enter the name of the posture policy that you want to create. Once created and saved, the name of the posture policy in not editable.
Identity Groups	Choose an identity group from the drop-down list. The selection of an identity group applies to the role of the user to which the user belongs in conjunction with the operating system that is installed on the client.
Operating Systems	Choose an operating system from the drop-down list. It allows you to select specific Windows, or Macintosh operating systems to which the posture requirement is applied.
Other Conditions	Choose a dictionary simple condition, or a dictionary compound condition to which the posture requirement should apply. If more than one condition is selected, then all the conditions must be met to form a compound condition. The system uses "&" (a logical AND) as the AND operator.
Requirements	Choose a posture requirement from the drop-down list. The selection of a posture requirement that is associated to the matching posture policy determines the compliance of an endpoint during a posture policy evaluation.
Actions	Allows you to insert a new posture policy, duplicate an existing policy, or delete an existing policy.

For information on how to manage posture policies, see the “Creating, Duplicating, and Deleting Client Posture Policies” section on page 20-35.

For more information on simplified posture policy configuration, see the “Simplified Posture Policy Configuration” section on page 20-34.

Simplified Posture Policy Configuration

This section describes the process to configure a posture policy in three steps in the Posture Policy page itself without navigating away to other configuration pages.

Once a posture policy is created in the Posture Policy page, posture conditions and remediation actions that you create in the Add Requirement widget are associated to the posture requirement, and posture requirements that you create in the Add Requirement widget are associated to the posture policy.

This section describes the process to configure a posture policy in three steps.

Simplified Posture Policy involves the following three steps:

Choose **Policy > Posture**. The Posture Policy page appears.

Step 1 Click the plus [+] sign to expand the Requirements anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can invoke the Requirements object selector, and create a new posture requirement from the Add Requirement dialog. For more information, see the "Creating a New Posture Policy" section on page 20-36.

Step 2 Click the plus [+] sign to expand the Conditions anchored overlay in the Add Requirement dialog. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can invoke the Conditions object selector that lists user defined conditions and Cisco defined conditions separately.

You can create new conditions such as simple file, registry, application, service conditions, regular compound conditions, antivirus compound conditions, and antispyware compound conditions, and associate them to the requirement. You can also associate existing user defined simple and compound conditions that appear in the Conditions object selector.

You can also choose Cisco defined conditions of file, registry, application, service conditions, regular compound conditions, antivirus compound conditions, and antispyware compound conditions, and associate them to the requirement.

For more information, see the "Creating a New Posture Requirement" section on page 20-153.

Step 3 Click the plus [+] sign to expand the Remediation Actions anchored overlay in the Add Requirement dialog. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can invoke the Remediations object selector that lists all the remediations that you have already created.

You can create new remediations such as file remediations, link remediations, launch program remediations, antivirus remediations, antispyware remediations, Windows Server Update Services remediations, and Windows Update remediations, and associate them to the requirement.

You can also choose existing remediations that appear in the Remediations object selector.

For more information, see the "Creating a New Posture Requirement" section on page 20-153.

Once the posture conditions and posture remediations configuration is complete in the Add Requirement dialog, the requirement is associated to the posture policy.

Creating, Duplicating, and Deleting Client Posture Policies

This section describes the following procedures on how to insert (create) a new policy, duplicate an existing policy, or delete an existing policy in the Posture Policies page.

- Creating a New Posture Policy, page 20-36
- Duplicating a Posture Policy, page 20-40

- Deleting a Posture Policy, page 20-40

Creating a New Posture Policy

You can create a new posture policy in the Posture Policies page.

To create a new posture policy, complete the following steps:

Step 1 Choose **Policy > Posture**.

The Posture Policy page appears.

Step 2 Choose the **Status** type.

You can enforce a posture policy to be one of the following types:

- **Enabled**—Allows you to enforce a posture policy for evaluation
- **Disabled**—Allows you not to enforce a posture policy for evaluation

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

Step 4 From the Identity Groups, choose **Select Role**.

The identity group anchored overlay appears.

To choose a role, complete the following steps:

a. Click the plus [+] sign to expand the identity group anchored overlay.

The identity group anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the quick picker (down arrow).

The Roles object selector appears. The Table view shows the roles that lists Any and the User Identity Groups in a row format in the right pane of the widget. The Tree view shows Any and the User Identity Groups in a tree format.

c. From the Roles object selector, choose the role.

d. Click **Add** (plus [+] sign) to associate more than one role to the policy.

e. Click **Remove** (minus [-] sign) to remove the role from the policy.

Step 5 From the Operating Systems, choose **Select Operating Systems**.

The operating system anchored overlay appears.

To choose an operating system, complete the following steps:

a. Click the plus [+] sign to expand the operating system anchored overlay.

The operating system anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the quick picker (down arrow).

The Operating System Groups object selector appears. The Table view shows MAC OSX and Windows All operating system groups and their underlying versions in a row format in the right pane of the widget. The Tree view shows MAC OSX and Windows All operating system groups and their underlying versions in a tree format.

You cannot choose both the operating system types.

c. From the Operating System Groups object selector, choose either **MAC OSX** or **Windows All**.

Click the quick picker (right arrow) icon to view the operating system groups.

Mac OS X (Macintosh) has three underlying versions.

- From the Mac OS X (Macintosh) group, choose the underlying Macintosh operating system.

Or

Windows has Windows 7 (All), Windows Vista (All), and Windows XP (All) groups and each group contains underlying versions.

- From the Windows All group, choose the underlying Windows group and the Windows version. Each Windows group contains its own underlying versions.

d. Click **Add** (plus [+] sign) to associate more than one operating system to the policy.

e. Click **Remove** (minus [-] sign) to remove the operating system from the policy.

Step 6 From the Other Conditions, choose **(Optional) Dictionary Attributes**.

The conditions anchored overlay appears, which allows you an option to add new one or more dictionary attributes, and save them as simple, and compound conditions to a dictionary (a library). You can use an AND, or OR operator to form a dictionary compound condition, and then save them to the dictionaries. From the Other Conditions field, you can choose dictionary simple, and compound conditions from the library for validation during posture policies evaluation.

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

To choose a condition, complete the following steps:

a. Optional. Click the plus [+] sign to expand the conditions anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

A dialog displays Select Existing Condition from Library and Create New Condition (Advance Option).

Select Existing Condition from Library—You can define an expression by selecting predefined conditions from the policy elements library. You can add ad-hoc attribute/value pairs to your expression in the subsequent steps.

Create New Condition (Advance Option)—You can define an expression by selecting attributes from various system or user-defined dictionaries. You can add pre-defined conditions from the policy elements library in the subsequent steps.

b. Click **Select Existing Condition from Library**.

c. Click the quick picker (down arrow).

The Dictionaries object selector appears, which lists the dictionary simple conditions and dictionary compound conditions.

d. Choose the condition.

e. Choose an **AND** operator or an **OR** operator from the drop-down list.

f. Click **Action** to add a new dictionary attribute and its value, add a condition from the library, or delete the existing conditions or dictionary attributes.

You can do the following:

– Add Attribute/Value

- Add Condition from Library
- Delete

g. Click the **Save** icon to add all the conditions below to the policy elements library from the conditions overlay.

To choose a dictionary attribute, complete the following steps:

a. Optional. Click the plus [+] sign to expand the conditions anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

A dialog displays Select Existing Condition from Library and Create New Condition (Advance Option)

b. Click **Create New Condition (Advance Option)**.

The conditions anchored overlay appears. It allows you to create a new dictionary simple condition or dictionary compound condition (an expression).

c. In the Expression field, click the quick picker (down arrow) icon.

The Dictionaries object selector appears that lists the following dictionaries:

- AD1
- DEVICE
- Network Access
- Radius
- Session

d. In the Dictionaries object selector, choose an existing dictionary.

e. Click the navigation arrow (right arrow) to view the dictionary attributes.

The dictionary attributes appear for the dictionary.

f. Choose a dictionary attribute.

g. Choose an operator, and a value to create a dictionary simple condition.

h. Click **Action** to add a dictionary simple condition to a library.

Enter a name for that dictionary simple condition to be saved to the library.

i. Click **Action** to add a new dictionary attribute and its value, add a condition from the library, duplicate a condition, add a condition to the library, or delete the existing conditions or dictionary attributes.

You can do the following:

- Add Attribute/Value
- Add Condition from Library
- Duplicate
- Add Condition to Library
- Delete

j. Choose an **AND** operator or an **OR** operator from the drop-down list to create a dictionary compound condition.

k. Click the **Save** icon to add all the conditions from the conditions anchored overlay to the library.

Here, you can define an expression by selecting attributes from various system, or user-defined dictionaries. You can create a new dictionary simple condition (an expression) by adding a new dictionary attribute and associating a value, which can be saved to the policy elements library. You can also add pre-defined conditions from the policy elements library in the subsequent steps.

Session Agent-Request-Type

The Session dictionary that you choose from the Dictionaries widget has the following attributes and values.

- Agent-Request-Type—Initial and Periodic Reassessment are the values.
- OS-Architecture—32-bit and 64-bit are the values.
- URL-Redirected—Specify the value.

By default, all the matching posture requirements are validated upon initial posture assessment and then periodically according to the periodic reassessments that are defined for posture assessment of clients. The Session attribute Agent-Request-Type can be used in the posture policy to selectively apply posture requirements either during initial posture assessment or during periodic reassessments of clients.

- To apply a matching posture requirement during initial posture assessment only, set the Session Agent-Request-Type attribute EQUAL to Initial.
- To apply a matching posture requirement during periodic reassessment only, set the Session Agent-Request-Type attribute EQUAL to Periodic Reassessment.
- To apply a matching posture requirement to both the initial posture assessment and periodic reassessments, then do not set the Session Agent-Request-Type attribute in the posture policy.

Step 7 From the Requirements, choose **Select Requirement**.

To choose a requirement, complete the following steps:

a. Click the plus [+] sign to expand the requirements anchored overlay.

The requirements anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can enforce a posture requirement to be one of the following items types:

Mandatory—This option enforces the client to meet the posture requirement. The user cannot proceed or have access to the network unless the client meets the posture requirement.

Optional—This option does not enforce the client to meet the posture requirement. The client can bypass the requirement, if required. The client does not require to meet the requirement for the user to proceed or have network access.

Audit—This option checks the client for the posture requirement without notifying the user. It does not affect user network access.

b. Click the quick picker (down arrow).

The Requirements object selector appears.

c. Choose a requirement.

d. Click **Add** (plus [+] sign) to associate more than one requirement to the posture policy.

e. Click **Remove** (minus [-] sign) to remove the requirement from the posture policy.

To create a requirement, complete the following steps:

a. From the Requirements, choose **Select Requirement**.

b. Click the plus [+] sign to expand the requirements anchored overlay.

The requirements anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can enforce a posture requirement to be one of the following items types:

Mandatory—This option forces the client to meet the posture requirement. The user cannot proceed or have access to the network unless the client meets the posture requirement.

Optional—This option does not force the client to meet the posture requirement. The client can bypass the requirement, if required. The client does not require to meet the requirement for the user to proceed or have network access.

Audit—This option checks the client for the posture requirement without notifying the user. It does not affect user network access.

c. Click quick picker (down arrow).

The Requirements object selector appears.

d. Click the quick picker (down arrow) on the **Action** button.

e. Click **Create Requirement**.

The Add Requirement dialog appears. You can configure the posture requirement from the Posture Policy page where you can associate posture conditions and posture remediation actions for that requirement.

Step 8 Click **Done** to save the posture policy, and switch the posture policy row to read-only mode. Click **Edit** to switch the posture policy row to editing mode.

Step 9 Click **Save**.

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Duplicating a Posture Policy

You can create a copy of the posture policy that you want to duplicate in the Posture Policies page.

To duplicate a policy, complete the following steps:

Step 1 Choose **Policy > Posture**.

Step 2 Click the down arrow in the policy row.

The action items appear in a list box.

Step 3 Click **Duplicate** to create a copy of the policy that you want to duplicate in the Posture Policies page.

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Deleting a Posture Policy

You can also delete a posture policy from the Posture Policies page.

To delete a policy, complete the following steps:

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

Step 2 Click the down arrow in the policy row.

The action items appear in a list box.

Step 3 Choose **Delete**.

A confirmation dialog appears with the following message: "Are you sure you want to delete the policy".

Step 4 Click **Yes** to delete a posture policy from the Posture Policies page.

Step 5 Click **No** to return to the Posture Policies page without deleting the posture policy.

Posture Assessment and Remediation Options in Cisco ISE

The NAC Agent and the Web Agent for Windows provide the posture assessment and remediation for Windows clients, and the NAC Agent for Macintosh provide the posture assessment and remediation for Macintosh clients. Before you begin to configure custom conditions and remediation actions in Cisco ISE, you must understand the posture assessment and remediation types that are supported by the NAC Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 20-8 provides the list of posture assessment (checks) and remediation options that are supported by the NAC Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 20-8 Posture Assessment and Remediation Options

	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Posture Assessments	Operating System/Service Packs/Hotfixes	Operating System/Service Packs/Hotfixes	Not Applicable
	Process Check	Process Check	Not Applicable
	Registry Check	Registry Check	Not Applicable
	File Check	File Check	Not Applicable
	Application Check	Application Check	Not Applicable
	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	Not Applicable
	Windows Update Configuration	Windows Update Configuration	Not Applicable
	WSUS Compliance Settings	WSUS Compliance Settings	Not Applicable

Table 20-8 Posture Assessment and Remediation Options (continued)

	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Posture Remediations	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	Not Applicable
	Launch Program	Not Applicable	Not Applicable
	Antivirus Definition Update	Not Applicable	Antivirus Live Update
	Antispyware Definition Update	Not Applicable	Antispyware Live Update
	Windows Update	Not Applicable	Not Applicable
	WSUS	Not Applicable	Not Applicable

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 to a posture requirement.

User Defined Conditions and Cisco Defined Conditions

Cisco ISE redefines posture conditions into either user defined conditions that you create on their respective conditions list pages or Cisco defined conditions.

After an initial posture update, Cisco ISE creates the following user defined AV compound conditions and AS compound conditions:

- ANY_av_mac_def—Any AV definition check on MAC
- ANY_av_mac_inst—Any AV installation check on MAC
- ANY_av_win_def—Any AV definition check on Windows
- ANY_av_mac_inst—Any AV installation check on Windows
- ANY_as_mac_def—Any AS definition check on MAC
- ANY_as_mac_inst—Any AS installation check on MAC
- ANY_as_win_def—Any AS definition check on Windows
- ANY_as_mac_inst—Any AS installation check on Windows

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple file, registry, application, and service conditions have pc_ as their prefixes, and compound conditions have pr_ as their prefixes.

Note The conditions that appear in the Policy > Policy Elements > Conditions > Posture > AV Compound Conditions or AS Compound Conditions page may vary as follows:

- If you have performed a new installation of Cisco ISE, Release 1.1.x and have not performed a compliance module update, this display will be empty.
- If you have performed a new installation of Cisco ISE, Release 1.1.x and perform a compliance module update, Cisco ISE displays the appropriate antivirus or antispyware subset of the list above.
- If you have updated from an earlier release of Cisco ISE to release 1.1.x and perform a compliance module update, Cisco ISE displays the appropriate antivirus or antispyware subset of the list above in addition to many other vendor specific conditions carried over from the earlier release database.

A user defined condition or a Cisco defined condition includes both simple conditions such as a file condition, a registry condition, an application condition, and a service condition, as well as compound conditions such as a regular compound condition, an antivirus compound condition, and an antispyware compound condition.

You can use the Posture navigation pane to manage the following posture simple conditions:

- File Conditions—A simple 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 simple condition that checks for the existence of a registry key or the value of the registry key on the client
- Application Conditions—A simple condition that checks if an application (process) is running or not running on the client
- Service Conditions—A simple condition that checks if a service is running or not running on the client
- Dictionary Simple Conditions—A simple condition that checks an attribute associated to an operator and the operator to a value

Note A simple condition cannot be deleted due to Referential Integrity errors in Cisco ISE when it is associated to one or more compound conditions. As simple conditions can be associated to a compound condition, you cannot delete the following simple conditions: a file, a registry, an application, a service, and a dictionary simple condition. If you attempt to delete a simple condition, Cisco ISE throws an error message stating that the compound conditions need to be updated, or deleted first to which simple conditions are associated.

Note You cannot delete or edit Cisco defined posture simple conditions.

You can use the Posture navigation pane to manage the following posture compound conditions:

- 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

Note A compound condition cannot be deleted due to Referential Integrity errors in Cisco ISE. As compound conditions can be associated to a posture requirement, you cannot delete the following compound conditions: a compound condition, an antivirus, an antispyware, and a dictionary compound condition. If you attempt to delete a compound condition, Cisco ISE throws an error message stating that the posture requirements need to be updated, or deleted first to which compound conditions are associated.

Note You cannot delete or edit Cisco defined posture compound conditions.

File Conditions

A file condition is a simple (single) condition that checks for a file by its existence on the client, or its date when created or modified on the client, or its version that exists on the client. You can create FileExistence, FileDate, and FileVersion types of file conditions to check the compliance of the file on the client. The FileExistence type checks the existence of a file on the client. The FileDate type checks the file based on its file-created date, or file-modified date on the client. The FileVersion type checks for the specific version of the file that you define in the file condition. When you create a file condition in the File Conditions page, you can see the fields change to provide details according to your input.

The File Conditions page displays file conditions along with their names and description. It also displays the names of the files to be checked for each of the file condition type.

Note Cisco defined file conditions that are listed in the File Conditions page are not editable.

Configuring File Conditions

You can create any one of the following types of a file condition in the File Conditions page: FileExistence, FileDate, and FileVersion. You can also duplicate, edit, delete, or filter file conditions from the File Conditions page.

This section covers the following procedures:

- Viewing File Conditions, page 20-44
- Creating, Duplicating, Editing, and Deleting a File Condition of FileExistence Type, page 20-45
- Creating, Duplicating, Editing, and Deleting a File Condition of FileDate Type, page 20-48
- Creating, Duplicating, Editing, and Deleting a File Condition of FileVersion Type, page 20-51
- Filtering File Conditions, page 20-53

Viewing File Conditions

You can use the File Conditions page to view file conditions.

To view file conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click a file condition from the file conditions list, and click **View** to view the details.

Step 6 Click the **File Conditions List** link to return to the File Conditions page.

Creating, Duplicating, Editing, and Deleting a File Condition of FileExistence Type

You can use the File Conditions page to create, duplicate, edit or delete a file condition of FileExistence type, which allows you to check that a file exists on the client, or does not exist on the client.

To create a file condition of FileExistence type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click **Add**.

⚠ **Caution** Once created and saved, the name of the file condition is not editable.

Step 6 Modify the values in the File Conditions List > New File Condition page, as shown in Table 20-9 to add a file condition of FileExistence type, which appears in the File Conditions page.

Step 7 Click **Submit** to create a file condition of FileExistence type.

To duplicate a file condition of FileExistence type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, choose **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click the file condition that you want to duplicate, and click **Duplicate** to create a copy of the file condition of FileExistence type.

Step 6 Click **Submit** to create a copy of the file condition of FileExistence type.

To edit a file condition of FileExistence type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 5 Click the file condition that you want to edit, and click **Edit** to edit a file condition of FileExistence type.

Step 6 Click **Save** to save the changes to the file condition of FileExistence type.

The file condition of FileExistence type will be available in the File Conditions page after you edit the file condition of FileExistense type.

Step 7 Click the **File Conditions List** link to return to the File Conditions page.

To delete a file condition of FileExistence type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 5 Click the file condition that you want to delete, and click **Delete** to delete a file condition of FileExistence type.

⚠ **Caution** Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-9 describes the fields in the New File Condition page that allow you to create, duplicate, or edit a file condition of FileExistence type condition.

Table 20-9 File Condition of FileExistence Type

Field Name	Field Description
Name	Enter the name of a file condition that you want to create.
Description	Enter a description of the file condition that you want to create.
File Path	From the File Path drop-down list, this option allows you to check the existence of a file in the location you specify. Choose from the following predefined settings: • **ABSOLUTE_PATH**—Checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • **SYSTEM_32**—Checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • **SYSTEM_DRIVE**—Checks the file in the C:\ drive. Enter the file name. • **SYSTEM_PROGRAMS**—Checks the file in the C:\Program Files. Enter the file name. • **SYSTEM_ROOT**—Checks the file in the root path for Windows system. Enter the file name.
File Type	From the File Type drop-down list, selecting a File Type allows you to check a file for the existence of a file on the client, file-created or file-modified date of the file, and its version. Choose from the following predefined settings: • **FileExistence**—Checks whether a file exists on the system. • **FileDat**e—Checks whether a file with a particular file-created or file-modified date exists on the system. • **FileVersion**—Checks whether a particular version of a file exists on the system.
File Operator	From the File Operator drop-down list, selecting an operator allows you to check the existence of a file in the specified location. Choose from the following predefined settings: • **Exists** • **DoesNotExist**
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a File Condition of FileDate Type

You can use the File Conditions page to create, duplicate, edit, or delete a file condition of FileDate type by using the file-created, or file-modified date.

To create a File Condition of FileDate type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click **Add**.

Caution Once created and saved, the name of the file condition is not editable.

Step 6 Modify the values in the File Conditions List > New File Condition page**,** as shown in Table 20-10 to add a file condition of FileDate type with file-created date or file-modified date.

Step 7 Click **Submit** to create a file condition of FileDate type.

To duplicate a file condition of FileDate type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click the file condition that you want to duplicate, and click **Duplicate** to create a copy of the file condition of FileDate type.

Step 6 Click **Submit** to create a copy of the file condition of FileDate type.

To edit a file condition of FileDate type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click the file condition that you want to edit, and click **Edit** to edit a file condition of FileDate type.

Step 6 Click **Save** to save the changes to the file condition of FileDate type.

The file condition of FileDate type will be available in the File Conditions page after you edit the file condition of FileDate type.

Step 7 Click the **File Conditions List** link to return to the File Conditions page.

To delete a file condition of FileDate type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click the file condition that you want to delete, and click **Delete** to delete a file condition of FileDate type.

⚠ **Caution** Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-10 describes the fields in the New File Condition page that allow you to create, duplicate, or edit a file condition of FileDate type condition.

Table 20-10 File Condition of FileDate Type

Field Name	Field Description
Name	Enter the name of a file condition that you want to create.
Description	Enter the description of a file condition that you want to create

Table 20-10 File Condition of FileDate Type (continued)

Field Name	Field Description
File Path	From the File Path drop-down list, this option allows you to check the existence of a file in the location you specify. Choose from the following predefined settings: • **ABSOLUTE_PATH**—Checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • **SYSTEM_32**—Checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • **SYSTEM_DRIVE**—Checks the file in the C:\ drive. Enter the file name. • **SYSTEM_PROGRAMS**—Checks the file in the C:\Program Files. Enter the file name. • **SYSTEM_ROOT**—Checks the file in the root path for Windows system. Enter the file name.
File Type	From the File Type drop-down list, selecting a File Type allows you to check a file for the existence of the file on the client, file-created or file-modified date of the file, and its version. Choose from the following predefined settings: • **FileExistence**—Checks whether a file exists on the system. • **FileDate**—Checks whether a file with a particular file-created or file-modified date exists on the system. • **FileVersion**—Checks whether a particular version of a file exists on the system.
File Date Type	From the File Date Type, selecting the date type allows you to check the existence of a file with a particular file-created or file-modified date. Choose from the following predefined settings: • **Creation Date** • **Modification Date**
Operator	From the Operator drop-down list, selecting an operator allows you to check the existence of a file with a particular date or version. Choose from the following predefined settings: • **EarlierThan** • **LaterThan** • **EqualTo**
Date and Time	From the Date and Time fields, entering date and time of the client system, which is expressed in mm/dd/yyyy and hh:mm:ss format allows you to check the existence of a file with date and time of the client system.
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a File Condition of FileVersion Type

You can use the File Conditions page to create, duplicate, edit, or delete a file condition of FileVersion type that has more than one version.

To create a file condition of FileVersion type, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click **Add**.

Caution Once created and saved, the name of the file condition is not editable.

Step 6 Modify the values in the File Conditions List > New File Condition page**,** as shown in Table 20-11 to add a file condition of FileVersion type, where the file has more than one version.

Step 7 Click **Submit** to create a file condition of FileVersion type.

To duplicate a file condition of FileVersion type, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 5 Click the file condition that you want to duplicate, and click **Duplicate** to create a copy of the file condition of FileVersion type.

Step 6 Click **Submit** to create a copy of the file condition of FileVersion type.

To edit a file condition of FileVersion type, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 5 Click the file condition that you want to edit, and click **Edit** to edit a file condition of FileVersion type.

Step 6 Click **Save** to save the changes to the file condition of FileVersion type.

The file condition of FileVersion type will be available in the File Conditions page after you edit the file condition of FileVersion type.

Step 7 Click the **File Conditions List** link from the edit page to return to the File Conditions page.

To delete a file condition of FileVersion type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 5 Click the file condition that you want to delete, and click **Delete** to delete a file condition of FileVersion type.

⚠ **Caution** Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-11 describes the fields in the New File Condition page that allow you to create, duplicate, or edit a file condition of FileVersion type condition.

Table 20-11 File Condition of FileVersion Type

Field Name	Field Description
Name	Enter the name of a file condition that you want to create.
Description	Enter the description of a file condition that you want to create

Table 20-11 File Condition of FileVersion Type (continued)

Field Name	Field Description
File Path	From the File Path drop-down list, this option allows you to check the existence of a file in the location you specify. Choose from the following predefined settings: • **ABSOLUTE_PATH**—Checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • **SYSTEM_32**—Checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • **SYSTEM_DRIVE**—Checks the file in the C:\ drive. Enter the file name. • **SYSTEM_PROGRAMS**—Checks the file in the C:\Program Files. Enter the file name. • **SYSTEM_ROOT**—Checks the file in the root path for Windows system. Enter the file name.
File Type	From the File Type drop-down list, selecting a File Type allows you to check a file for the existence of the file on the client, file-created or file-modified date of the file, and its version. Choose from the following predefined settings: • **FileExistence**—Checks whether a file exists on the system. • **FileDate**—Checks whether a file with a particular file-created or file-modified date exists on the system. • **FileVersion**—Checks whether a particular version of a file exists on the system.
Operator	From the Operator drop-down list, selecting an operator allows you to check the existence of a file with a particular date or version. Choose from the following predefined settings: • **EarlierThan** • **LaterThan** • **EqualTo**
File Version	From the File Version drop-down list, enter the version of the file that allows you to check the existence of a file with a particular version of the file.
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering File Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the File Conditions page. A quick filter is a simple filter that can be used to filter file conditions in the File Conditions page. The quick filter filters file conditions based on the field description such as the name of the file conditions, description, and the file to be checked in the File Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the File Conditions page. The advanced filter filters file conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the File Conditions page. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the File Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter file conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation, click **File Condition**.

The File Conditions page appears, which lists all the file conditions that you have already created.

Step 5 In the File Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-12.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-54 and To filter by using the Advanced Filter option, complete the following steps:, page 20-55.

Note To return to the File Conditions page, choose **All** from the Show drop-down list to display all the file conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters file conditions based on each field description in the File Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the File Conditions page. If you clear the field, it displays the list of all the file conditions in the File Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the File Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter file conditions by using variables that are more complex. It contains one or more filters, which filter file conditions based on the values that match the field description. A filter on a single row filters file conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter file conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-12 describes the fields that allow you to filter file conditions in the File Conditions page.

Table 20-12 Filtering File Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter file conditions by the condition name.
	Description	This field enables you to filter file conditions by the condition description.
	Field Name	This field enables you to filter file conditions by the filename.
	Condition Type	This field enables you to filter file conditions by Cisco predefined and not Cisco predefined conditions.

Table 20-12 Filtering File Conditions (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • File Name • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter file conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against which to filter file conditions from the Value drop-down list.

Registry Conditions

A registry condition is a simple (single) condition that checks a registry key or the value of the registry on the client. You can create RegistryKey, RegistryKeyValue, and RegistryValueDefault types of registry conditions to check the compliance of the client on a registry. The RegistryKey type checks the existence of a registry on the client, and the RegistryKeyValue type checks the data of the registry key on the client. The RegistryValueDefault is the same as the RegistryKeyValue except that the former checks for the default value. When you create a registry condition in the Registry Conditions page, you can see the fields change to provide details according to your input.

The Registry Conditions page displays registry conditions along with their names, description, and the type of registry conditions.

Note Cisco predefined registry conditions that are listed in the Registry Conditions page are not editable.

Configuring Registry Conditions

You can create any one of the following types of a registry condition in the Registry Conditions page: RegistryKey, RegistryKeyValue, and RegistryValueDefault types. You can also duplicate, edit, delete, or filter the registry conditions from the Registry Conditions page.

This section covers the following procedures:

- Viewing Registry Conditions, page 20-57
- Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryKey Type, page 20-57
- Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValue Type, page 20-60
- Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValueDefault Type, page 20-63
- Filtering Registry Conditions, page 20-66

Viewing Registry Conditions

You can use the Registry Conditions page to view registry conditions.

To view registry conditions, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click a registry condition from the registry conditions list, and click **View** to view the details.

Step 6 Click the **Registry Conditions List** link to return to the Registry Conditions page.

Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryKey Type

You can use the Registry Conditions page to create, duplicate, edit, or delete a registry condition of RegistryKey type, which allows you to check the existence of a registry on the client.

To create a registry condition of RegistryKey type, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click **Add**.

Caution Once created and saved, the name of the registry condition is not editable.

Step 6 Modify the values in the Registry Conditions List link > New Registry Condition page, as shown in Table 20-13 to add a registry condition of RegistryKey type, which appears in the Registry Conditions page.

Step 7 Click **Submit** to create a registry condition of RegistryKey type.

To duplicate a registry condition of RegistryKey type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to duplicate, and click **Duplicate** to create a copy of the registry condition of RegistryKey type.

Step 6 Click **Submit** to create a copy of the registry condition of RegistryKey type.

To edit a registry condition of RegistryKey type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to edit, and click **Edit** to edit a registry condition of RegistryKey type.

Step 6 Click **Save** to save the changes to the registry condition of RegistryKey type.

The registry condition of RegistryKey type will be available in the Registry Conditions page after you edit the registry condition of RegistryKey type.

Step 7 Click the **Registry Conditions List** link to return to the Registry Conditions page.

To delete a registry condition of RegistryKey type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to delete, and click **Delete** to delete a registry condition of RegistryKey type.

Caution Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-13 describes the fields in the New Registry Condition page that allow you to create, duplicate, or edit a registry condition of RegistryKey type condition.

Table 20-13 Registry Condition for RegistryKey

Field Name	Field Description
Name	Enter the name of the registry condition that you want to create.
Description	Enter the description of the registry condition that you want to create.
Registry Type	From the Registry Type drop-down list, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Choose from the following predefined settings: • **RegistryKey**—Checks whether a specific registry key exists in the registry. • **RegistryValue**—Checks whether a named registry key exists or has a particular value, version, or modification date. • **RegistryValueDefault**—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key drop-down list, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Choose from the following Registry Root Key locations: • **HKEY_LOCAL_MACHINE (HKLM)** • **HKEY_CURRENT_CONFIG (HKCC)** • **HKEY_CURRENT_USER (HKCU)** • **HKEY_USERS (HKU)** • **HKEY_CLASSES_ROOT (HKCR)**
Sub Key	Selecting a sub key without the leading backslash (“\”) allows you to check the registry key and the registry key value in the path specified in the sub key in the Sub Key text box. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version

Table 20-13 Registry Condition for RegistryKey (continued)

Field Name	Field Description
Value Operator	From the Value Operator drop-down list, selecting an operator allows you to check the existence or nonexistence of the registry key and the registry key value. Choose from the following predefined settings: • **Exists** • **DoesNotExist**
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValue Type

You can use the Registry Conditions page to create, duplicate, edit, or delete a registry condition of RegistryValue type.

To create a registry condition of RegistryValue type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click **Add**.

⚠ **Caution** Once created and saved, the name of the registry condition is not editable.

Step 6 Modify the values in the Registry Conditions List > New Registry Condition page, as shown in Table 20-14 to add a Registry Condition of RegistryValue type, which appears in the Registry Conditions page.

Step 7 Click **Submit** to create a registry condition of RegistryValue type.

To duplicate a registry condition of RegistryValue type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to duplicate, and click **Duplicate** to create a copy of the registry condition of RegistryValue type.

Step 6 Click **Submit** to create a copy of the registry condition of RegistryValue type.

To edit a registry condition of RegistryValue type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to edit, and click **Edit** to edit a registry condition of RegistryValue type.

Step 6 Click **Save** to save the changes to the registry condition of RegistryValue type.

The registry condition of RegistryValue type will be available in the Registry Conditions page after you edit the registry condition of RegistryValue type.

Step 7 Click the **Registry Conditions List** link to return to the Registry Conditions page.

To delete a registry condition of RegistryValue type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to delete, and **Delete** to delete a registry condition of RegistryValue type.

Caution Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-14 describes the fields in the New Registry Condition page that allow you to create, duplicate, or edit a registry condition of RegistryValue type condition.

Table 20-14 Registry Condition for RegistryValue

Field Name	Field Description
Name	Enter the name of the registry condition that you want to create.
Description	Enter the description of the registry condition that you want to create.
Registry Type	From the Registry Type drop-down list, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Choose from the following predefined settings: • **RegistryKey**—Checks whether a specific registry key exists in the registry. • **RegistryValue**—Checks whether a named registry key exists or has a particular value, version, or modification date. • **RegistryValueDefault**—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key drop-down list, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Choose from the following Registry Root Key locations: • **HKEY_LOCAL_MACHINE (HKLM)** • **HKEY_CURRENT_CONFIG (HKCC)** • **HKEY_CURRENT_USER (HKCU)** • **HKEY_USERS (HKU)** • **HKEY_CLASSES_ROOT (HKCR)**
Sub Key	Selecting a sub key without the leading backslash ("\") allows you to check the registry key and the registry key value in the path specified in the sub key in the Sub Key text box. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version
Value Name	Enter the name of the registry key value against which you want to check in the client registry.
Value Data Type	From the Value Data drop-down list, selecting the data type allows you to check the registry key value data type, and its value using an operator. Choose from the following predefined settings: • **Unspecified**—choose one of the operators in the drop-down list to check the existence of the registry key value • **Number**—choose one of the operators in the drop-down list to check the registry key value using a number in the registry key value • **String**—choose one of the operators in the drop-down list to check the registry key value using a string in the registry key value • **Version**—choose one of the operators in the drop-down list to check the registry key value using its version

Table 20-14 Registry Condition for RegistryValue (continued)

Field Name	Field Description
Value Operator	From the Value Operator drop-down list, selecting an operator allows you to check the existence or nonexistence of data type of the registry key value using an operator. Choose from the following predefined settings: • **Exists** • **DoesNotExist**
Value Data	Enter the value of the registry key for the data type of the registry that you select in the Value Data text box.
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValueDefault Type

You can use the Registry Conditions page to create, duplicate, edit, or delete a registry condition of RegistryValueDefault type.

To create a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click **Add**.

⚠ **Caution** Once created and saved, the name of the registry condition is not editable.

Step 6 Modify the values in the Registry Conditions List > New Registry Condition page, as shown in Table 20-15 to add a Registry Condition of RegistryValueDefault type, which appears in the Registry Conditions page.

Step 7 Click **Submit** to create a registry condition of RegistryValueDefault type.

To duplicate a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to duplicate, and click **Duplicate** to create a copy of the registry condition of RegistryValueDefault type.

Step 6 Click **Submit** to create a copy of the registry condition of RegistryValueDefault type.

To edit a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to edit, and click **Edit** to edit a registry condition of RegistryValueDefault type.

Step 6 Click **Save** to save the changes to the registry condition of RegistryValueDefault type.

The registry condition of RegistryValueDefault type will be available in the Registry Conditions page after you edit the registry condition of RegistryValueDefault type.

Step 7 Click the **Registry Conditions List** link to return to the Registry Conditions page.

To delete a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click the registry condition that you want to delete, and click **Delete** to delete a registry condition of RegistryValueDefault type.

Caution Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-15 describes the fields in the New Registry Condition page that allow you to create, or edit a registry condition of RegistryValueDefault type condition.

Table 20-15 Registry Condition for RegistryValueDefault

Field Name	Field Description
Name	Enter the name of the registry condition that you want to create.
Description	Enter the description of the registry condition that you want to create.
Registry Type	From the Registry Type drop-down list, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Choose from the following predefined settings: • **RegistryKey**—Checks whether a specific registry key exists in the registry. • **RegistryValue**—Checks whether a named registry key exists or has a particular value, version, or modification date. • **RegistryValueDefault**—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key drop-down list, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Choose from the following Registry Root Key locations: • **HKEY_LOCAL_MACHINE (HKLM)** • **HKEY_CURRENT_CONFIG (HKCC)** • **HKEY_CURRENT_USER (HKCU)** • **HKEY_USERS (HKU)** • **HKEY_CLASSES_ROOT (HKCR)**
Sub Key	Selecting a sub key without the leading backslash ("\") allows you to check the registry key and the registry key value in the path specified in the sub key in the Sub Key test box. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version
Value Name	(Default)

Table 20-15 Registry Condition for RegistryValueDefault (continued)

Field Name	Field Description
Value Data Type	From the Value Data Type drop-down list, selecting the data type allows you to check the registry key value data type, and its value using an operator. Choose from the following predefined settings: • **Number**—choose one of the operators in the drop-down list to check the registry key value using a number in the registry key value • **String**—choose one of the operators in the drop-down list to check the registry key value using a string in the registry key value • **Version**—choose one of the operators in the drop-down list to check the registry key value using its version
Value Operator	From the Value Operator field, selecting an operator allows you to check the existence or nonexistence of data type of the registry key value using an operator. Choose from the following predefined settings: • **Exists** • **DoesNotExist**
Value Data	Enter the value of the registry key for the data type of the registry that you select in the Value Data text box.
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering Registry Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Registry Conditions page. A quick filter is a simple filter that can be used to filter registry conditions in the Registry Conditions page. The quick filter filters registry conditions based on the field description such as the name of the registry conditions, description, and the type of registry conditions in the Registry Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Registry Conditions page. The advanced filter filters registry conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Registry Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Registry Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter registry conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Registry Condition**.

Step 5 The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 6 In the Registry Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-16.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-67 and To filter by using the Advanced Filter option, complete the following steps:, page 20-67.

Note To return to the Registry Conditions page, choose **All** from the Show drop-down list to display all the registry conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters registry conditions based on each field description in the Registry Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Registry Conditions page. If you clear the field, it displays the list of all the registry conditions in the Registry Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Registry Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter registry conditions by using variables that are more complex. It contains one or more filters, which filter registry conditions based on the values that match the field description. A filter on a single row filters registry conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter registry conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-16 describes the fields that allow you to filter registry conditions in the Registry Conditions page.

Table 20-16 Filtering Registry Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter registry conditions by the condition name.
	Description	This field enables you to filter registry conditions by the condition description.
	Registry Type	This field enables you to filter registry conditions by the registry type.
	Condition Type	This field enables you to filter registry conditions by Cisco predefined and not Cisco predefined conditions
Advanced Filter	Choose the field description from the following: • Name • Description • Registry Type • Condition type	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter registry conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against which to filter registry conditions from the Value drop-down list.

Application Conditions

An application condition is a simple (single) condition, which checks applications that are running, and are not running on the client. The application condition can check for various application processes that are typically viewable under Windows Task Manager.

The Application Conditions page displays application conditions along with their names, description, as well as applications that are running and are not running on the client. It also shows the status of applications whether they are running, or are not running on the client.

Note Cisco predefined application conditions that are listed in the Application Conditions page are not editable.

Configuring Application Conditions

You can create an application condition to check that an application is running, or not running on the client. You can also duplicate, edit, delete, or filter application conditions from the Application Conditions page.

This section covers the following procedures:

- Viewing Application Conditions, page 20-69
- Creating, Duplicating, Editing, and Deleting an Application Condition, page 20-69
- Filtering Application Conditions, page 20-71

Viewing Application Conditions

You can use the Application Conditions page to view application conditions.

To view application conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Click an application condition from the application conditions list, and click **View** to view the details.

Step 6 Click the **Application Conditions List** link to return to the Application Conditions page.

Creating, Duplicating, Editing, and Deleting an Application Condition

You can use the Application Conditions page to create, duplicate, edit, or delete an application condition, which allows you to check various application processes that are running, or are not running on the client.

To create an application condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Click **Add**.

Caution Once created and saved, the name of the application condition is not editable.

Step 6 Modify the values in the Applications Conditions List > New Application Condition page, as shown in Table 20-17 to add an application condition, which appears in the Application Conditions page.

Step 7 Click **Submit** to create an application condition.

To duplicate an application condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Click the application condition that you want to duplicate, and click **Duplicate** to create a copy of the application condition.

Step 6 Click **Submit** to create a copy of the application condition.

To edit an application condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Click the application condition that you want to edit, and click **Edit** to edit an application condition.

Step 6 Click **Save** to save the changes to the application condition.

The application condition will be available in the Application Conditions page after you edit the application condition.

Step 7 Click the **Application Conditions List** link to return to the Application Conditions page.

To delete an application condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Click the application condition that you want to delete, and click **Delete** to delete an application condition.

Caution Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-17 describes the fields in the New Application Condition list page that allow you to create, duplicate, or edit an application condition.

Table 20-17 Application Condition

Field Name	Field Description
Name	Enter the name of the application condition that you want to create.
Description	Enter the description of the application condition that you want to create.
Process Name	Enter the name of the application that you want to check whether it is running, or not running on the client.
Application Operator	From the Application Operator drop-down list, selecting the status of an application allows you to check whether that application is running, or not running on the client. Choose from the following predefined settings: • **Running** • **NotRunning**
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering Application Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Applications Conditions page. A quick filter is a simple and quick filter that can be used to filter application conditions in the Application Conditions page. The quick filter filters application conditions based on the field description such as the name of the application conditions, description, and that shows the status whether applications are running, or not running on the client in the Application Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Application Conditions page. The advanced filter filters application conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Application Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Application Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter application conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 In the Application Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-18.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-72 and To filter by using the Advanced Filter option, complete the following steps:, page 20-73.

Note To return to the Application Conditions page, choose **All** from the Show drop-down list to display all the application conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters application conditions based on each field description in the Application Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Application Conditions page. If you clear the field, it displays the list of all the application conditions in the Application Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Application Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter application conditions by using variables that are more complex. It contains one or more filters, which filter application conditions based on the values that match the field description. A filter on a single row filters application conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter application conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-18 describes the fields that allow you to filter application conditions in the Application Conditions page.

Table 20-18 Filtering Application Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter application conditions by the condition name.
	Description	This field enables you to filter application conditions by the condition description.
	Status	This field enables you to filter application conditions by checking the status of applications whether they are running or not running.
	Condition Type	This field enables you to filter application conditions by Cisco defined and user defined conditions.

Table 20-18 Filtering Application Conditions (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Status • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter application conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against which to filter application conditions from the Value drop-down list.

Service Conditions

A service condition is a simple (single) condition, which checks services that are running, and are not running on the client. The service condition can check for various services such as security, or application agents that are typically viewable from the Windows Services console.

The Service Conditions page displays service conditions along with their names and description of the service conditions. It also shows the status whether the services are, or are not running on the client.

Cisco Predefined Checks

The Service Conditions page displays predefined Cisco checks as well as service conditions that you create in the Service Conditions page. The predefined Cisco checks are downloaded on your Cisco ISE deployment as a result of dynamic posture updates. The pc_AutoUpdateCheck is one of the predefined Cisco checks, which is downloaded to the service conditions list (simple conditions).

For information on downloading Posture updates through the web, see the "Dynamic Posture Updates" section on page 20-22.

pc_AutoUpdateCheck

The pc_AutoUpdateCheck is a single (simple) condition, which can be used in a compound condition. The pr_AutoUpdateCheck_Rule is a compound condition that uses the pc_AutoUpdateCheck simple condition.

For information on how the pr_AutoUpdateCheck_Rule is used in a Windows update remediation, see the "pr_AutoUpdateCheck_Rule" section on page 20-80.

Note Cisco predefined service conditions that are listed in the Service Conditions page are not editable.

Configuring Service Conditions

You can create a service condition to check that a service is running, or not running on the client. You can also duplicate, edit, delete, or filter service conditions from the Services conditions list page.

This section covers the following procedures:

- Viewing Service Conditions, page 20-75
- Creating, Duplicating, Editing, and Deleting a Service Condition, page 20-75
- Filtering Service Conditions, page 20-77

Viewing Service Conditions

You can use the Service Conditions page to view service conditions.

To view service conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you create.

Step 5 Click the service condition from the service conditions list, and click **View** to view the details.

Step 6 Click the **Service Conditions List** link to return to the Service Conditions page.

Creating, Duplicating, Editing, and Deleting a Service Condition

You can use the Service Conditions page to create, duplicate, edit, or delete a service condition, which allows you to check various services that are running or not running on the client.

To create a service condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you create.

Step 5 Click **Add**.

⚠ **Caution** Once created and saved, the name of the service condition is not editable.

Step 6 Modify the values in the Service Conditions List > New Service Condition page, as shown in Table 20-19 to add a service condition, which appears in the Service Conditions page.

Step 7 Click **Submit** to create a service condition.

To duplicate a service condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Service Condition**.

Step 5 Click the service condition that you want to duplicate, and click **Duplicate** to create a copy of the service condition.

Step 6 Click **Submit** to create a copy of the service condition.

To edit a service condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Service Condition**.

Step 5 Click the service condition that you want to edit, and click **Edit** to edit the service condition.

Step 6 Click **Save** to save the changes to the service condition.

The service condition will be available in the Service Conditions page after you edit the service condition.

Step 7 Click the **Service Conditions List** link from the edit page to return to the Service Conditions page.

To delete a service condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you create.

Step 5 Click the service condition that you want to delete, and click **Delete** to delete a service condition.

⚠ **Caution** Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-19 describes the fields in the New Service Condition page that allow you to create, duplicate, or edit a service condition.

Table 20-19 Service Condition

Field Name	Field Description
Name	Enter the name of the service condition that you want to create.
Description	Enter the description of the service condition that you want to create.
Service Name	Enter the name of the service that you want to check whether it is running, or not running on the client.
Service Operator	From the Service Operator drop-down list, selecting the status of a service allows you to check whether that service is running, or not running on the client. Choose from the following predefined settings. • **Running** • **NotRunning**
Operating System	From the Operating System drop-down list, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering Service Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Service Conditions page. A quick filter is a simple and quick filter that can be used to filter service conditions in the Service Conditions page. The quick filter filters service conditions based on the field description such as the name of the service condition, description, and that checks for services that are running, or not running on the client in the Service Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Service Conditions page. The advanced filter filters service conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Service Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Service Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter service conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Service Condition**.

The Service Conditions page appears, which lists all the service conditions that you have create.

Step 5 In the Service Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-20.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-78 and To filter by using the Advanced Filter option, complete the following steps:, page 20-78.

Note To return to the Service Conditions page, choose **All** from the Show drop-down list to display all the service conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters service conditions based on each field description in the Service Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Service Conditions page. If you clear the field, it displays the list of all the service conditions in the Service Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Service Conditions Page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter service conditions by using variables that are more complex. It contains one or more filters, which filter service conditions based on the values that match the field description. A filter on a single row filters service conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter service conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-20 describes the fields that allow you to filter service conditions in the Service Conditions page.

Table 20-20 Filtering Service Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter service conditions by the condition name.
	Description	This field enables you to filter service conditions by the condition description.
	Check for	This field enables you to filter service conditions by checking the status of applications whether it is running or not.
	Condition Type	This field enables you to filter service conditions by Cisco predefined and user defined conditions.
Advanced Filter	Choose the field description from the following: • Name • Description • Check for • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter service conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against which to filter service conditions from the Value drop-down list.

Compound Conditions

A compound condition includes one or more simple conditions, or compound conditions of the type file, registry, application, service, or dictionary conditions. You can combine one or more conditions using an AND (ampersand [&]), an OR (horizontal bar [|]), or a NOT (exclamation point [!]) operator to create a compound condition.

Cisco Predefined Rules

The Compound Conditions page displays predefined Cisco rules, as well as compound conditions that you create in the Compound Conditions page. The predefined Cisco rules are downloaded on your Cisco ISE deployment as a result of dynamic posture updates through the web.

For information on downloading Posture updates through the web, see the "Dynamic Posture Updates" section on page 20-22.

pr_AutoUpdateCheck_Rule

The pr_AutoUpdateCheck_Rule is a predefined Cisco Rule, which is downloaded to the Compound Conditions page. It contains only the pc_AutoUpdateCheck, a single (simple) condition.

When used in a posture requirement, the pr_AutoUpdateCheck_Rule compound condition allows you to check whether Windows clients are enabled with the automatic updates feature. If the Windows clients fail to meet the requirement, then the NAC Agents enforce Windows clients to be enabled (remediate) with the automatic updates feature, and upon which the clients are postured compliant. The Windows update remediation that you associate in the posture requirement overrides the Windows administrator setting, if the automatic updates feature is not enabled on Windows clients.

The Compound Conditions page displays compound conditions along with their names and description according to their operating systems. The Compound Conditions page allows you to filter the conditions based on the operating systems, as every condition is associated with one or more operating systems. The filtering options allow you to quickly pick the right set of conditions for a specific operating system.

Note Cisco predefined compound conditions that are listed in the Compound Conditions page are not editable.

Configuring Compound Conditions

You can create, duplicate, edit, delete, or filter compound conditions from the Compound Conditions page.

This section covers the following procedures:

- Viewing Compound Conditions, page 20-80
- Creating, Duplicating, Editing, and Deleting a Compound Condition, page 20-81
- Filtering Compound Conditions, page 20-84

Viewing Compound Conditions

You can use the Compound Conditions page to view compound conditions.

To view compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 Click a compound condition from the compound conditions list, and **View** to view the details.

Step 6 Click the **Compound Conditions List** link to return to the Compound Conditions page.

Creating, Duplicating, Editing, and Deleting a Compound Condition

You can use the Compound Conditions page to create, duplicate, edit, or delete a compound condition.

To add a compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 Click **Add**.

Caution Once created and saved, the name of the compound condition is not editable. The operating system is also not editable in the compound condition after you have associated the newly created compound condition to a requirement. To edit the operating system in the compound condition, you need to remove the compound condition association from the posture requirement.

Step 6 Modify the values in the Compound Conditions List > New Compound Condition page, as shown in Table 20-21.

You can create an expression by using logical operators to form a compound condition by combining simple conditions. You can use the Simple Conditions object selector to choose one or more simple conditions.

a. Click the Select a condition to insert below drop-down list.

The Simple Conditions object selector appears that displays simple file, registry, application and service conditions.

b. Choose a simple condition from any one of the file, registry, application, and service condition types from the conditions.

or

c. click the quick picker (down arrow) on the **Action** button to create a simple condition that allows you to save it to the existing list of respective simple conditions.

Choose one of the following simple conditions:

- Create File Condition

  Add File Condition dialog appears. Here, you can create a file (simple) condition.

- Create Registry Condition

  Add Registry Condition dialog appears. Here, you can create a registry (simple) condition.

- Create Application Condition

  Add Application Condition dialog appears. Here, you can create an application (simple) condition.

- Create Service Condition

  Add Service Condition dialog appears. Here, you can create a service (simple) condition.

d. Choose an AND (ampersand [&]), an OR (horizontal bar [|]), or a NOT (exclamation point [!]) operator to combine simple conditions. Use the parentheses [( )], and the logical operators to create a compound condition.

e. Choose a simple condition from any one of the file, registry, application, and service condition types from the conditions to the previously chosen simple conditions to create a compound condition.

Step 7 Click **Validate Expression** to validate the compound condition.

Step 8 Click **Submit** to create a compound condition.

To duplicate a compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 Click the compound condition that you want to duplicate, and click **Duplicate** to create a copy of the compound condition.

Step 6 Click **Submit** to create a copy of the compound condition

To edit a compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 Click the compound condition that you want to edit, and click **Edit** to edit a compound condition, which you have already created, and saved in the Compound Conditions page. The predefined Cisco rules are not editable.

Step 6 Click **Save** to save the changes to the compound condition.

The compound condition will be available in the Compound Conditions page after you edit the compound condition.

Step 7 Click the **Compound Conditions List** link to return to the Compound Conditions page.

To delete a compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 Click the compound condition that you want to delete, and **Delete** to delete a compound condition.

⚠ **Caution** Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-21 describes the fields in the New Compound Condition page that allow you to create, duplicate, or edit a compound condition.

Table 20-21 Compound Condition

Field Name	Field Description
Name	Enter the name of the compound condition that you want to create.
Description	Enter the description of the compound condition that you want to create.

Table 20-21 Compound Condition

Field Name	Field Description
Operating System	From the Operating System drop-down list, selecting one or more Windows operating systems allow you to associate Windows operating systems to which the condition is applied.
Select a condition to insert below	Click the Select a condition to insert below drop-down list to display the Simple Conditions object selector.
Expression	A field in the New Compound Condition page where you can create compound conditions using logical operators.
Parentheses ( )	Click the parentheses to combine two simple conditions from the following simple condition types: file, registry, application, and service conditions.
(&)—AND operator (use “&” for an AND operator, without the quotes)	You can use the AND operator (ampersand [&]) in a compound condition. For example, enter **Condition1 & Condition2**.
(|)—OR operator (use “|” for an OR operator, without the quotes)	You can use the OR operator (horizontal bar [|]) in a compound condition. For example, enter **Condition1 | Condition2**.
(!)—NOT operator (use “!” for a NOT operator, without the quotes)	You can use the NOT operator (exclamation point [!]) in a compound conditions. For example, enter **Condition1 & (!Condition2)**.
Simple Conditions	The Simple Conditions object selector provides you with the list of simple conditions of the following types: file, registry, application, and service conditions. You can also create simple conditions of file, registry, application and service conditions from the object selector. Click the quick picker (down arrow) on the **Action** button to create simple conditions of file, registry, application, and service conditions.

Filtering Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter compound conditions in the Compound Conditions page. The quick filter filters compound conditions based on the field description such as the name and description of the compound condition in the Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Compound Conditions page. The advanced filter filters compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Compound Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Compound Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation menu appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 In the Compound Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-22.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-85 and To filter by using the Advanced Filter option, complete the following steps:, page 20-85.

Note To return to the Compound Conditions page, choose **All** from the Show drop-down list to display all the compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters compound conditions based on each field description in the Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Compound Conditions page. If you clear the field, it displays the list of all the compound conditions in the Compound Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Compound Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter compound conditions by using variables that are more complex. It contains one or more filters, which filter compound conditions based on the values that match the field description. A filter on a single row filters compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-22 describes the fields that allow you to filter compound conditions in the Compound Conditions page.

Table 20-22 Filtering Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter compound conditions by the condition name.
	Description	This field enables you to filter compound conditions by the condition description.
	Condition Type	This filed enables you to filter compound conditions by Cisco defined and user defined conditions.
Advanced Filter	Choose the field description from the following: • Name • Description • Condition Type	Click drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter compound conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against which to filter compound conditions from Value the drop-down list.

Antivirus and Antispyware Compound Conditions

Prerequisites:

Before you begin, you should read and understand the following antivirus and antispyware topics:

- Antivirus and Antispyware Support Charts, which explain antivirus and antispyware support.
- Antivirus and Antispyware Definition Updates, which explain updating antivirus and antispyware definition files.

An Antivirus Compound Condition

Cisco ISE loads preconfigured antivirus compound conditions in the AV Compound Conditions page, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These antivirus compound conditions can check for antivirus products for their existence on all the clients. You can also create new antivirus compound conditions in the New Antivirus Compound Condition page.

The New Antivirus Compound Condition page displays the Products for Selected Vendor table, which provides information on antivirus products for a selected vendor.

An Antispyware Compound Condition

Cisco ISE loads preconfigured antispyware compound conditions in the AS Compound Conditions page, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These antispyware compound conditions can check for antispyware products for their existence on all the clients. You can also create new antispyware compound conditions in the New Antispyware Compound Condition page.

The New Antispyware Compound Condition page displays the Products for Selected Vendor table, which provides information on antivirus products for a selected vendor.

Antivirus and Antispyware Support Charts

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, and the antivirus and antispyware chart provides them 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.

Antivirus and Antispyware Definition Updates

The New Antivirus Compound Condition and New Antispyware Compound Condition configuration pages allow you to use the information from the av-chart archive files, which display the list of vendors, supported products, and their releases to configure client remediations in the AV Remediations and AS Remediations page.

in the New Anti-virus Compound Condition and New Anti-spyware Compound Condition configuration pages, you have an option to check for antivirus and antispyware definition file date, or version on all the clients for the following: a particular vendor product, or any product from a vendor, or for any vendor any product. In addition, you also have an option to specify that the definition files can be older than a specified certain number of days. It gives users a certain amount of time to enforce security policies with respect to how old the definition files can be on their system.

Antivirus and antispyware compound conditions allow you to verify that the virus definition files for a specified vendor are up-to-date on your clients. You can optionally configure antivirus and antispyware definition files of antivirus and antispyware compound conditions to be older by a number of days than the definition files, which are updated in the Cisco ISE servers. Even if the definition files have not been updated by the vendor, this option allows you to configure antivirus and antispyware compound conditions so that clients are validated for compliance with older versions by a few days.

For antivirus definition file updates, you can specify the number of days either from the latest antivirus definition file updates for a specified vendor, or from the current system date on Cisco ISE. For antispyware definition file updates, you must specify the number of days from the current system date. You do not have the option to specify the number of days from the latest antispyware definition file updates. The default number of days is zero (0), indicating that the antivirus and antispyware file definition date cannot predate the latest file or current system date.

You can also associate antivirus and antispyware compound conditions to the AV remediations and AS remediation actions. If your clients fail to meet antivirus and antispyware compound conditions, then the NAC Agents that are installed on your clients communicate directly with the installed antivirus and antispyware software on the clients. The NAC Agents display a dialog with an update, or remediate button on it for end users to use them to remediate clients automatically with the latest antivirus and antispyware definition files.

Related Topics

Antivirus Compound Conditions, page 20-88

Antispyware Compound Conditions, page 20-94

Antivirus Compound Conditions

An antivirus compound condition contains one or more antivirus conditions (simple conditions), or antivirus compound conditions. An antivirus compound condition checks an antivirus installation, or checks for an antivirus signature definition version/date on a client. You can create an antivirus compound condition to check for an antivirus installation, or definition updates on the client for any vendor.

Configuring Antivirus Compound Conditions

The AV Compound Conditions page displays antivirus compound conditions along with their names and description.

You can create an antivirus compound condition to check that an antivirus installation exists on your clients, or check that the latest antivirus signature definition version/date on the client for a selected vendor. You can duplicate, edit, delete, or filter antivirus compound conditions from the AV Compound Conditions page.

This section covers the following procedures:

- Creating, Duplicating, Editing, and Deleting an Antivirus Compound Condition, page 20-89
- Filtering Antivirus Compound Conditions, page 20-92

Creating, Duplicating, Editing, and Deleting an Antivirus Compound Condition

You can use the AV Compound Conditions page to create, duplicate, edit, or delete an antivirus compound condition.

To create an antivirus compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also antivirus compound conditions that you create in the New Anti-virus Compound Condition page.

Step 5 Click **Add**.

Caution Once created and saved, the name of the antivirus compound condition is not editable.

Step 6 Modify the values in the Anti-virus Compound Condition List > New Anti-virus Compound Conditions page, as shown in Table 20-23 to add an antivirus compound condition to check the installation of an antivirus program, or check that an antivirus definition file is up-to-date.

Note Choose a product from the Products for Selected Vendor table.

Step 7 Click **Submit** to create an antivirus compound condition.

To duplicate an antivirus compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also antivirus compound conditions that you create in the New Anti-virus Compound Condition page.

Step 5 Click the antivirus compound condition that you want to duplicate, and click **Duplicate** to create a copy of the antivirus compound condition.

Step 6 Click **Submit** to create a copy of the antivirus compound condition.

To edit an antivirus compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also antivirus compound conditions that you have already created.

Step 5 Click an antivirus compound condition that you want to edit, and click **Edit** to edit an antivirus compound condition, which you have already created and saved in the AV Compound Conditions page. The predefined Cisco rules are not editable.

Step 6 Click **Save** to save the changes to the antivirus compound condition.

The antivirus compound condition will be available in the AV Compound Conditions page after you edit the antivirus compound condition.

Step 7 Click the **Anti-virus Compound Conditions List** link to return to the AV Compound Conditions page.

To delete an antivirus compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also AV compound conditions that you have already created.

Step 5 Click an antivirus compound condition that you want to delete, and **Delete** to delete an antivirus compound condition.

⚠ **Caution** Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-23 describes the fields in the AV Compound Conditions page that allow you to create, duplicate, or edit an antivirus compound condition.

Table 20-23 AV Compound Condition

Field Name	Field Description
Name	Enter the name of the antivirus compound condition that you want to create.

Table 20-23 AV Compound Condition (continued)

Field Name	Field Description
Description	Enter the description of the antivirus compound condition that you want to create.
Operating System	Selecting an operating system allows you to check the installation of an antivirus programs on your client, or check the latest antivirus definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antivirus products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	The Check Type radio button allows you to choose whether to check an installation or check the latest definition file update on the client.
Installation	The Installation radio button allows you to check only the installation of an antivirus program on the client.
Definition	The Definition radio button allows you to check only the latest definition file update of an antivirus product on the client. When enabled, Cisco ISE provides you the following two options to check clients against latest antivirus definition file version or latest antivirus definition file date: • Check against latest AV definition file version if available. Otherwise check against latest definition file date • Allow virus definition file to be a specific number of days days older than latest file date or current system date
Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).	The field selection allows you to check the antivirus definition file version on the client against the latest antivirus definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, it allows you to check the definition file date on the client against the latest definition file date in Cisco ISE.
Allow virus definition file to be (Enabled)	The Allow virus definition file to be check box is enabled only when you choose creating antivirus definition check types, and disabled when creating antivirus installation check types. If checked, the selection allows you to check the antivirus definition file version and the latest antivirus definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the latest antivirus definition file date of the product or the current system date. If unchecked, Cisco ISE allows you to check only the version of the antivirus definition file using the Check against latest AV definition file version, if available option.
days older than	The days older than radio button defines the number of days that the latest antivirus definition file date on the client can be older from the latest antivirus definition file date of the product or the current system date. The default value is zero (0).

Table 20-23 AV Compound Condition (continued)

Field Name	Field Description
latest file date	The latest file date radio button checks that the antivirus definition file date on the client, which can be older by the number of days that you define in the next field (days older than field). If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the latest antivirus definition file date of the product.
current system date	The current system date radio button checks that the antivirus definition file date on the client, which can be older by the number of days that you define in the next field (days older than field). If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the current system date.
Products for Selected Vendor	Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus Compound Condition page, the table retrieves information on their antivirus products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antivirus program, or check for the latest antivirus definition file date, and its latest version.

Filtering Antivirus Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the AV Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter antivirus compound conditions in the AV Compound Conditions page. The quick filter filters antivirus compound conditions based on the field description such as the name and description of the antivirus compound condition in the AV Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the AV Compound Conditions page. The advanced filters antivirus compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the AV Compound Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the AV Compound Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter antivirus compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the antivirus compound conditions.

Step 5 In the AV Compound Conditions page, click the Show drop-down arrow list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-24.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-93 and To filter by using the Advanced Filter option, complete the following steps:, page 20-93.

Note To return to the AV Compound Conditions page, choose **All** from the Show drop-down list to display all the antivirus compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antivirus compound conditions based on each field description in the AV Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the AV Compound Conditions page. If you clear the field, it displays the list of all the antivirus compound conditions in the AV Compound Conditions page.

Step 1 To filter, click **Go** within each field within each field to refresh the page with the results that are displayed in the AV Compound Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antivirus compound conditions by using variables that are more complex. It contains one or more filters, which filter antivirus compound conditions based on the values that match the field description. A filter on a single row filters antivirus compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antivirus compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-24 describes the fields that allow you to filter antivirus compound conditions in the AV Compound Conditions page.

Table 20-24 Filtering Antivirus Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter antivirus compound conditions by the condition name.
	Description	This field enables you to filter antivirus compound conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Description	Click the drop-down arrow to choose the field description.
	Operator	Choose an operator that can be used to filter antivirus compound conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against to filter the antivirus compound conditions from the Value drop-down list.

Antispyware Compound Conditions

An antispyware compound condition contains one or more antispyware conditions (simple conditions), or antispyware compound conditions. An antispyware compound condition checks an antispyware installation, or checks for an antispyware signature definition version/date on a client against the current system date. You can create an antispyware compound condition to check for an antivirus installation, or definition updates on the client for any vendor.

When you create an antispyware definition file update condition, the antispyware definition file date can be older than the current system date by the number of days that you specify for checking the definition file date on the client. The default value is zero (0) days.

Here, you must enable (check) the Allow virus definition file to be check box to check that the latest antispyware definition file date on the client. It can be older than the current system date by the number of days, which you define in the days older than field.

Configuring Antispyware Compound Conditions

The AS Compound Conditions page displays antispyware compound conditions along with their names and description.

You can create an antispyware compound condition to check that an antispyware installation exists on your clients, or check that the latest antispyware signature definition version/date on the client for a selected vendor. You can duplicate, edit, delete, or filter antispyware compound conditions from the AS Compound Conditions page.

This section covers the following procedures:

- Creating, Duplicating, Editing, and Deleting an Antispyware Compound Condition, page 20-95
- Filtering Antispyware Compound Conditions, page 20-98

Creating, Duplicating, Editing, and Deleting an Antispyware Compound Condition

You can use the AS Compound Conditions page to create, duplicate, edit, or delete an antispyware compound condition.

To create an antispyware compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also antispyware compound conditions that you create in the New Anti-spyware Compound Condition page.

Step 5 Click **Add**.

Caution Once created and saved, the name of the antispyware compound condition is not editable.

Step 6 Modify the values in the AS Compound Conditions List > New Anti-spyware Compound Condition page, as shown in Table 20-25 to add an antispyware compound condition to check the installation of an antispyware program, or check that an antispyware definition file is up-to-date.

Note Choose a product from the Products for Selected Vendor table.

Step 7 Click **Submit** to create an antispyware compound condition.

To duplicate an antispyware compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also antispyware compound conditions that you have already created.

Step 5 Click the antispyware compound condition that you want to duplicate, and click **Duplicate** to create a copy of the antispyware compound condition.

Step 6 Click **Submit** to create a copy of the antispyware compound condition.

To edit an antispyware compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also antispyware compound conditions that you have already created.

Step 5 Click an antispyware compound condition that you want to edit, and click **Edit** to edit an antispyware compound condition, which you have already created and saved in the AS Compound Conditions page. The predefined Cisco rules are not editable.

Step 6 Click **Save** to save the changes to the antispyware compound condition.

The antispyware compound condition will be available in the AS Compound Conditions page after you edit the antispyware compound condition.

Step 7 Click the **AS Compound Conditions List** link to return to the AS Compound Conditions page.

To delete an antispyware compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also AS compound conditions that you have already created.

Step 5 Click an antispyware compound condition that you want to delete, click **Delete** to delete an antispyware compound condition.

⚠

Caution Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.

Table 20-25 describes the fields in the AS Compound Conditions page that allow you to create, duplicate, or edit an antispyware compound condition.

Table 20-25 Antispyware Compound Condition

Field Name	Field Description
Name	Enter the name of the antispyware compound condition that you want to create.
Description	Enter the description of the antispyware compound condition that you want to create.
Operating System	Selecting an operating system allows you to check the installation of an antispyware programs on your client, or check the latest antispyware definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antispyware products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	The Check Type radio button allows you to choose a type whether to check an installation, or check the latest definition file update on the client.
Installation	The Installation radio button allows you to check only the installation of an antispyware program on the client.
Definition	The Definition radio button allows you to check only the latest definition file update of an antispyware product on the client.
Allow virus definition file to be (Enabled)	The Allow virus definition file to be check box is enabled only when creating antispyware definition check types, and disabled when creating antispyware installation check types. If checked, the selection allows you to check antispyware definition file version and the latest antispyware definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the current system date. If unchecked, the selection allows you to check only the version of the antispyware definition file as the Allow virus definition file to be check box is not checked.
days older than	The days older than radio button defines the number of days that the latest antispyware definition file date on the client can be older from the current system date. The default value is zero (0).

Table 20-25 Antispyware Compound Condition (continued)

Field Name	Field Description
The current system date	The current system date radio button checks that the antispyware definition file date on the client, which can be older by the number of days that you define in the next field (days older than field). If you set the number of days to the default value (0), then the antispyware definition file date on the client should not be older than the current system date.
Products for Selected Vendor	Choose an antispyware product from the table. Based on the vendor that you select in the New Anti-spyware Compound Condition page, the table retrieves information on their antispyware products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antispyware program, or check for the latest antispyware definition file date, and its latest version.

Filtering Antispyware Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the AS Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter antispyware compound conditions in the AS Compound Conditions page. The quick filter filters antispyware compound conditions based on the field description such as the name and description of the antispyware compound condition in the AS Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the AS Compound Conditions page. The advanced filter filters antispyware compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the AS Compound Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the AS Compound Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter antispyware compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation menu, click **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the antispyware compound conditions.

Step 5 In the AS Compound Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-26.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-99 and To filter by using the Advanced Filter option, complete the following steps:, page 20-99.

Note To return to the AS Compound Conditions page, choose **All** from the Show drop-down list to display all the antispyware compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antispyware compound conditions based on each field description in the AS Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Compound conditions list page. If you clear the field, it displays the list of all the antispyware compound conditions in the AS Compound Conditions page.

Step 1 To filter, click **Go** within each field within each field to refresh the page with the results that are displayed in the AS Compound Conditions page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antispyware compound conditions by using variables that are more complex. It contains one or more filters, which filter antispyware compound conditions based on the values that match the field description. A filter on a single row filters antispyware compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antispyware compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-26 describes the fields that allow you to filter antispyware compound conditions in the AS Compound Conditions page.

Table 20-26 Filtering Antispyware Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter conditions by the condition name.
	Description	This field enables you to filter conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Description	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter antispyware compound conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against to filter antispyware compound conditions from the Value drop-down list.

Dictionary Simple Conditions

A dictionary simple condition is a simple (single) condition, where you can associate a value to a dictionary attribute. Once created and saved, the dictionary simple conditions are added to a library. You can use these dictionary simple conditions to form a dictionary compound condition in the Dictionary Compound Conditions page.

This section provides the procedure that you can use to configure dictionary simple conditions.

Configuring Dictionary Simple Conditions, page 20-100

Configuring Dictionary Simple Conditions

You can create a dictionary simple condition to check the value of an attribute that you associate to the dictionary attribute in the dictionary simple condition. You can also duplicate, edit, delete, or filter dictionary simple conditions from the Dictionary Simple Conditions page.

The Dictionary Simple Conditions page displays dictionary simple conditions along with their names and description, as well as the conditions in detail that you define in the dictionary simple conditions.

Creating, Duplicating, Editing, and Deleting a Dictionary Simple Condition

You can use the Dictionary Simple Conditions page to create, duplicate, edit, or delete a dictionary simple condition.

To create a dictionary simple condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

Step 4 The Posture navigation pane appears, which lists all the posture condition types.

Step 5 In the Posture navigation pane, click **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you create.

Step 6 Click **Add**.

Caution Once created and saved, the name of the dictionary simple condition is not editable.

Step 7 Modify the values in the Dictionary Conditions List > New Dictionary Condition page, as shown in Table 20-27 to add a dictionary simple condition where you can associate a value to a dictionary attribute.

Step 8 Click **Submit** to create a dictionary simple condition.

To duplicate a dictionary simple condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you create.

Step 5 Click a dictionary simple condition that you want to duplicate, and click **Duplicate** to create a copy of a dictionary simple condition.

Step 6 Click **Submit** to create a copy of a dictionary simple condition.

To edit a dictionary simple condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you create.

Step 5 Click a dictionary simple condition that you want to edit, and click **Edit** to edit a dictionary simple condition.

Step 6 Click **Save** to save the changes to a dictionary simple condition.

The dictionary simple condition will be available in the Dictionary Simple Conditions page after you edit the dictionary simple condition.

Step 7 Click the **Dictionary Conditions List** link to return to the Dictionary Simple Conditions page.

You cannot delete a dictionary simple condition, which is associated to a dictionary compound condition. To delete, you must first remove the association from the dictionary compound condition, and then delete it.

To delete a dictionary simple condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you create.

Step 5 Click a dictionary simple condition that you want to delete, and click **Delete** to delete a dictionary simple condition.

Table 20-27 describes the fields in the Dictionary Simple Conditions page that allow you to create, duplicate a dictionary simple condition, or edit a dictionary simple condition.

Table 20-27 Dictionary Simple Condition

Field Name	Field Description
Name	Enter the name of the dictionary simple condition that you want to create.
Description	Enter the description of the dictionary simple condition that you want to create.
Attribute	From the Attribute drop-down list, you can choose an attribute from a dictionary in the dictionaries object selector.
Operator	From the Operator drop-down list, you can choose an operator to associate a value to an attribute that you have selected. Choose an operator from the predefined settings for each of the dictionary attribute that you have selected.
Value	In the Value text box, enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.

Filtering Dictionary Simple Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Dictionary Simple Conditions page. A quick filter is a simple and quick filter that can be used to filter dictionary simple conditions in the Dictionary Simple Conditions page. The quick filter filters dictionary simple conditions based on the field description such as the name of the dictionary simple condition, condition that you define in the dictionary simple condition, and description in the Dictionary Simple Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Dictionary Simple Conditions page. The advanced filter filters dictionary simple conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Dictionary Simple Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Dictionary Simple Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter dictionary simple conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you create.

Step 5 In the Dictionary Simple Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-28.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-103 and To filter by using the Advanced Filter option, complete the following steps:, page 20-104.

Note To return to the Dictionary Simple Conditions page, choose **All** from the Show drop-down list to display all the dictionary simple conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters dictionary simple conditions based on each field description in the Dictionary Simple Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Dictionary Simple Conditions page. If you clear the field, it displays the list of all the dictionary simple conditions in the Dictionary Simple Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Dictionary Simple Condition page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter dictionary simple conditions by using variables that are more complex. It contains one or more filters, which filter dictionary simple conditions based on the values that match the field description. A filter on a single row filters dictionary simple conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-28 describes the fields in the Dictionary Simple Conditions page that allow you to filter dictionary simple conditions.

Table 20-28 Filtering Dictionary Simple Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter dictionary simple conditions by the condition name.
	Condition	This field enables you to filter dictionary simple conditions by the condition that you define in the dictionary simple condition.
	Description	This field enables you to filter dictionary simple conditions by the condition description.

Table 20-28 Filtering Dictionary Simple Conditions (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Name • Condition • Description	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter dictionary simple conditions from the Operator drop-down list.
	Value	Enter the value for the field description that you selected against which to filter dictionary simple conditions from the Value drop-down list.

Dictionary Compound Conditions

A dictionary compound condition is a logical combination of more than one dictionary simple condition (a dictionary attribute that is associated with a value). It is a set of dictionary simple conditions (dictionary attributes that are associated with values) that are logically combined with an AND, or an OR operator. You can save a dictionary compound condition, only when you define more than one dictionary simple condition, and then combine them in the Dictionary Compound Conditions page. One or more dictionary simple conditions that you create in the Dictionary Compound Conditions page must be saved to a library first, which can be added later from the library to form a dictionary compound condition.

Configuring Dictionary Compound Conditions

The Dictionary Compound Conditions page displays the list of dictionary compound conditions along with their names and description, as well as dictionary simple conditions that are logically combined.

This section covers the following procedure:

- Creating, Duplicating, Editing, and Deleting a Dictionary Compound Condition, page 20-105
- Filtering Dictionary Compound Conditions, page 20-109

Creating, Duplicating, Editing, and Deleting a Dictionary Compound Condition

You can create, duplicate, edit, or delete a dictionary compound condition from the Dictionary Compound Conditions page.

To create a dictionary compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you create.

Step 5 Click **Add**.

⚠ **Caution** Once created and saved, the name of the dictionary compound condition is not editable.

Step 6 Modify the values in the New Dictionary Compound Condition page, as shown in Table 20-29 to add a dictionary compound condition where you can logically combine more than one dictionary simple conditions.

Step 7 Click **Submit** to create a dictionary compound condition.

To duplicate a dictionary compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you create.

Step 5 Click a dictionary compound condition that you want to duplicate, and **Duplicate** to create a copy of a dictionary compound condition.

Step 6 Click **Submit** to create a copy of a dictionary compound condition.

To edit a dictionary compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you create.

Step 5 Click the dictionary compound condition that you want to edit, and **Edit** to edit a dictionary compound condition.

Step 6 Click **Save** to save the changes to a dictionary compound condition.

The dictionary compound condition will be available in the Dictionary Compound Conditions page after you edit the dictionary compound condition.

Step 7 Click the **Dictionary Compound Conditions List** link to return to the Dictionary Compound Conditions page.

To delete a dictionary compound condition, complete the following steps:

Step 1 Choose **Policy** > **Policy Elements** > **Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you create.

Step 5 Click the dictionary compound condition that you want to delete, and click **Delete** to delete a dictionary compound condition.

Table 20-29 describes the fields in the Dictionary Compound Conditions page that allow you to create, duplicate a dictionary compound condition, or edit a dictionary compound condition.

Table 20-29 Dictionary Compound Condition

Field Name	Field Description
Name	Enter the name of the dictionary compound condition that you want to create.
Description	Enter the description of the dictionary compound condition that you want to create.

Table 20-29 Dictionary Compound Condition (continued)

Field Name	Field Description
Select Existing Condition from Library	You can define an expression by selecting pre-defined conditions from the policy elements library. Click the **Action** icon to do the following: • Add Attribute/Value • Add Condition from Library • Delete You can add ad-hoc attribute/value pairs to your expression in the subsequent steps. Click the **Action** icon to do the following: • Add Attribute/Value—Allows you to create a dictionary simple condition • Add Condition from Library—Allows you to choose a dictionary simple, or dictionary compound condition from the library that are already created and saved • Duplicate—Allows you to duplicate a condition that you create or choose on this page. • Add Condition to Library—Allows you to save new dictionary simple, and dictionary compound conditions that you create for use later • Delete—Allows you to remove the association of a dictionary simple or dictionary compound condition from the dictionary compound condition.
Condition Name	From the Condition Name drop-down list, you can choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression is updated based on your selection from the Condition Name drop-down list.
AND or OR operator	Either an AND operator, or an OR operator allows you to logically combine dictionary simple conditions, which can be added from the library. Click the **Action** icon to do the following: • Add Attribute/Value • Add Condition from Library • Delete

Table 20-29 Dictionary Compound Condition (continued)

Field Name	Field Description
Create New Condition (Advance Option)	You can define an expression by selecting attributes from various system or user-defined dictionaries. Click the **Action** Icon to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete You can add predefined conditions from the policy elements library in the subsequent steps.
Condition Name	In the Condition Name text box, you can create a new dictionary simple condition and then save it to the library, or choose dictionary simple conditions that you have already created from the library.
Expression	From the Expression drop-down list, you can create a dictionary simple condition by choosing an attribute from a dictionary in the dictionaries object selector to which you can associate a value.
Operator	From the Operator drop-down list, you can choose an operator to associate a value to an attribute. Click the drop-down arrow to choose an operator from the predefined settings for each of the dictionary attribute that you select.
Value	From the Value field, enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.
AND or OR operator	Either an AND operator, or an OR operator allows you to logically combine dictionary simple conditions, which can be added from the library.

Filtering Dictionary Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Dictionary Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter dictionary compound conditions in the Dictionary Compound Conditions page. The quick filter filters dictionary compound conditions based on the field description such as the name of the dictionary compound condition, conditions that you define in the dictionary compound condition, and description in the Dictionary Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Dictionary Compound Conditions page.The advanced filter filters dictionary compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Dictionary Compound Conditions page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Dictionary Compound Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 In the Conditions navigation pane, expand **Posture**.

Step 3 Click the quick picker (right arrow) icon to navigate to the list of all posture conditions.

The Posture navigation pane appears, which lists all the posture condition types.

Step 4 In the Posture navigation pane, click **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you create.

Step 5 In the Dictionary Compound Conditions page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-30.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-110 and To filter by using the Advanced Filter option, complete the following steps:, page 20-110.

Note To return to the Dictionary Compound Conditions page, choose **All** from the Show drop-down list to display all the dictionary compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters dictionary compound conditions based on each field description in the Dictionary Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Dictionary Compound Conditions page. If you clear the field, it displays the list of all the compound conditions in the Dictionary Compound Conditions page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Dictionary Compound Condition page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter dictionary compound conditions by using variables that are more complex. It contains one or more filters, which filter dictionary compound conditions based on the values that match the field description. A filter on a single row filters dictionary compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-30 describes the fields in the Dictionary Compound Conditions page that allow you to filter dictionary compound conditions.

Table 20-30 Filtering Dictionary Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter compound conditions by the condition name.
	Condition	This field enables you to filter dictionary compound conditions by the condition that you define in the dictionary compound condition.
	Description	This field enables you to filter compound conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Condition • Description	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter dictionary compound conditions from the Operator drop-down list.
	Value	enter the value for the field description that you selected against which to filter dictionary compound conditions from the Value drop-down list.

Posture Results

Posture results are associated mandatory requirements to posture policies that all clients must meet their requirements during posture evaluation, and associated remediation actions to requirements that are required by clients to remediate themselves to meet failed requirements to become compliant on your network.

Posture results in posture requirements which all clients must meet for compliance with your organization security policies during policy evaluation of endpoints The posture requirements can be set to mandatory, optional, or audit types in posture policies during posture evaluation of endpoints.

Mandatory Requirements

If clients fail to meet mandatory requirements as defined in posture policies, then they are provided with remediation options in order for clients to meet them during policy evaluation. When clients fail to meet mandatory requirements during policy evaluation, it results in remediation actions that are associated to requirements, and end users are given remediation time within minutes specified in the remediation timer settings to remediate failed requirements.

If a client machine is unable to remediate a mandatory requirement, the session posture status changes to “non-compliant” and the agent session is quarantined. The only way to get the client machine past this “non-compliant” state is by initiating a new RADIUS or posture session where the agent starts posture assessment on the client machine again.

You can restart posture assessment on the client machine by doing one of the following:

- For wired and wireless CoA in an 802.1X environment—You can configure the Reauthentication Timer for the specific authorization policy in the Policy > Policy Elements > Results > Authorization > Authorization Profiles page. When you have the authorization policy page open, enable the Reauthentication function under Common Tasks and set the Maintain Connectivity During Reauthentication option to “Default.” The result is that the timer expires and a brand new session launches, thus restarting posture assessment. For more details, see Modifying an Existing Authorization Profile, page 17-32. (This method is not supported in Inline Posture deployments.)

  Alternatively, 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 WLC and wait until the user idle timeout period has expired before attempting to reconnect to the network.
- In a VPN environment—The only option is to disconnect and reconnect the VPN tunnel.

Optional Requirements

If client machines fail to meet optional requirements during policy evaluation, then the agents prompt end users with an option to continue further so that end users can skip optional requirements even though they fail during policy evaluation.

Audit Requirements

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

Related Topics

- Custom Posture Remediation Actions, page 20-113
- Configuring Custom Posture Remediation Actions, page 20-114
- Client Posture Assessment Requirements, page 20-151

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Custom Posture Remediation Actions

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

Here, you also have a text box for all the remediation types that can be used to communicate to the Agent users. In addition to remediation actions, you can also communicate to Agent users of non compliance of clients only with messages. Here, the NAC Agent does not trigger any remediation action.

Message Text Only

The Message Text Only option informs Agent users about noncompliance of clients. It also provides optional instructions to the user to contact the Help desk for more information, or to remediate the client manually.

When you create a posture requirement in the Requirements page, you can associate any one of a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) types to the requirement.

You can use the Posture Remediation Actions menu to manage the following remediations for a posture in Cisco ISE:

- A file remediation—Downloads the required file version on your client for compliance
- A link remediation—Provides a URL link for the client to click for access to a remediation page or resource
- An antivirus remediation—Updates antivirus signature definitions on the client for compliance
- An antispyware remediation—Updates antispyware signature definitions on the client for compliance
- Launch programs remediation—Launches one or more programs on the client for compliance
- Windows update remediation—Changes the Windows Automatic Update configuration (System Properties) on the client per customer security policy, and helps to ensure Windows Update remediates the client for compliance
- Windows Server Update Services (WSUS) remediation—Remediates the Windows client from a locally managed WSUS server, or Microsoft-managed WSUS server with the latest WSUS updates for compliance

To manage the posture remediation actions, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

The following results appear:

- Remediation Actions—Associated to requirements, which are required by clients to remediate themselves to meet failed requirements during policy evaluation
- Requirements—Associated to posture policies that all clients must meet during policy evaluation

Step 3 Click the quick picker (right arrow) icon to list all remediation actions.

The following remediation types appear:

- Antispyware Remediation

- Antivirus Remediation
- File Remediation
- Launch Program Remediation
- Link Remediation
- Windows Server Update Services Remediation
- Windows Update Remediation

Step 4 Click a remediation type to view the remediations list.

Configuring Custom Posture Remediation Actions

This section describes the custom remediation types that you can define in Cisco ISE.

Table 20-31 shows remediation types that are supported by NAC web agent, NAC agents for Windows and Macintosh clients.

Table 20-31 Remediation Types Supported by Agents

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

This section covers the following procedures for managing remediation actions for a posture:

- Viewing, Adding, and Deleting a File Remediation, page 20-115
- Adding, Duplicating, Editing, and Deleting a Link Remediation, page 20-119
- Adding, Duplicating, Editing, and Deleting an Antivirus Remediation, page 20-124
- Adding, Duplicating, Editing, and Deleting an Antispyware Remediation, page 20-128
- Adding, Duplicating, Editing, and Deleting a Launch Program Remediation, page 20-133
- Adding, Duplicating, Editing, and Deleting a Windows Update Remediation, page 20-139
- Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation, page 20-145

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

File Remediation

A file remediation allows clients to download the required file version for compliance. You are only allowed to create a file remediation, where the NAC Agent and Web Agent can 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 as you are allowed to edit other remediation types. The File Remediations page displays all the file remediations along with their names, description, and the files that are required for remediation.

This section describes the following procedures to configure and filter file remediations.

- Viewing, Adding, and Deleting a File Remediation, page 20-115
- Filtering File Remediations, page 20-117

Viewing, Adding, and Deleting a File Remediation

This section describes the procedures to view, add, or delete file remediations from the File Remediations page.

To view a file remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions**. or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **File Remediation**.

The File Remediations page appears, which lists all the file remediations.

Step 5 Check the check box to choose a file remediation, and click **View** to view a file remediation.

Step 6 Click the **File Remediations List** link to return back to the File Remediations page.

To add a file remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **File Remediation**.

The File Remediations page appears, which lists all the file remediations.

Step 5 Click **Add**.

The New File Remediation page appears.

⚠ **Caution** Once created and saved, the name of the file remediation is not editable.

Step 6 Modify the values in the New File Remediation page to add a new file remediation, as shown in Table 20-32.

Step 7 Click **Submit**.

The new file remediation appears in the File Remediations page.

To delete a file remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **File Remediation**.

The File Remediations page appears, which lists all the file remediations.

Step 5 Check the check box to choose a file remediation, and click **Delete** to delete a file remediation from the File Remediations page.

Table 20-32 describes the fields that allow you to create a file remediation in the New File Remediation page.

Table 20-32 File Remediation

Field Name	**Field Description**
File Remediation Name	Enter the name of the file remediation that you want to create.
File Remediation Description	Enter the description of the file remediation.

Table 20-32 File Remediation (continued)

Field Name	Field Description
Version	Enter the version of the file in the Version text box.
File to upload	Click Browse to locate the name of the file to be uploaded to the Cisco ISE server. This is in turn the file that is downloaded to the client, if file remediation action is triggered.

Filtering File Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the File Remediations page. A quick filter is a simple filter that can be used to filter file remediations in the File Remediations page. The quick filter filters file remediations based on the field description such as the name of the file remediations, description, and the file to be uploaded that is required for remediation in the File Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the File Remediations page. The advanced filter filters file remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the File Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the File Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter file remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **File Remediation**.

The File Remediations page appears, which lists all the file remediations.

Step 5 In the File Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-32.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-118 and To filter by using the Advanced Filter option, complete the following steps:, page 20-118.

Note To return to the File Remediations page, choose **All** from the Show drop-down list to display all the file remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters file remediations based on each field description in the File Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the File Remediations page. If you clear the field, it displays the list of all the file remediations in the File Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the File Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter file remediations by using variables that are more complex. It contains one or more filters, which filter file remediations based on the values that match the field description. A filter on a single row filters file remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter file remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-33 describes the fields that allow you to filter file remediations.

Table 20-33 Filtering File Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter file remediations by the name of the file remediation.
	Description	This field enables you to filter file remediations by the description of the file remediation.
	File Name	This field enables you to filter file remediations by the file name.

Table 20-33 Filtering File Remediations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • File Name	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter file remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter file remediations from the Value drop-down list.

Link Remediation

A link remediation allows clients to click a URL link for access to a remediation page, or resource. You can create a link remediation, where the NAC Agents and Web Agents open a browser with a link for clients to access a remediation page or resource, and remediate themselves for compliance.

You can filter, add, duplicate, edit, or delete link remediations in the Link Remediations page. The Link Remediations page displays all the link remediations along with their names, description, and their modes of remediation.

This section describes the procedures to configure and filter link remediations.

- Adding, Duplicating, Editing, and Deleting a Link Remediation
- Filtering Link Remediations

Adding, Duplicating, Editing, and Deleting a Link Remediation

This section describes the procedures to add, duplicate, edit, or delete link remediations from the Link Remediations page.

To add a link remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations.

Step 5 Click **Add**.

The New Link Remediation page appears.

Caution Once created and saved, the name of the link remediation is not editable.

Step 6 Modify the values in the New Link Remediation page to add a new link remediation, as shown in Table 20-34.

Step 7 Click **Submit**.

The new link remediation appears in the Link Remediations page.

To duplicate a link remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations.

Step 5 Check the check box to choose a link remediation, and click **Duplicate** to duplicate a link remediation in the Link Remediations page. You cannot duplicate a link remediation with the same name.

Step 6 Click **Submit**.

A copy of a link remediation appears in the Link Remediations page.

To edit a link remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations.

Step 5 Check the check box to choose a link remediation from the Link Remediations page, and click **Edit** to edit a link remediation.

Step 6 Click **Save**.

The link remediation will be available in the Link Remediations page after you edit the link remediation.

To delete a link remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations.

Step 5 Check the check box to choose a link remediation from the Link Remediations page, and click **Delete** to delete a link remediation from the Link Remediations page.

Table 20-34 describes the fields that allow you to create a link remediation in the New Link Remediation page.

Table 20-34 Link Remediation

Field Name	Field Description
Link Remediation Name	Enter the name of the link remediation that you want to create.
Link Remediation Description	Enter the description of the link remediation that you want to create.
Remediation Type	Click the Remediation Type drop-down list to choose a mode that are predefined for a link remediation: • **Automatic** • **Manual**—when selected, Retry Count and Interval fields are not editable
Retry Count	Enter the number of attempts that clients can try to remediate from the link.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate from the link after previous attempts.
URL	Enter a valid URL that clients can access a remediation page or resource to remediate.

Filtering Link Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Link remediations page. A quick filter is a simple filter that can be used to filter link remediations in the Link Remediations page. The quick filter filters link remediations based on the field description such as the name of the link remediation, description, and the mode of remediation in the Link Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Link Remediations page. The advanced filter filters link remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Link Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Link Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter link remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Link Remediation**.

The Link Remediations page appears, which lists all the file remediations.

Step 5 In the Link Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering.

Step 6 In the Link Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-35.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-122 and To filter by using the Advanced Filter option, complete the following steps:, page 20-122.

Note To return to the Link Remediations page, choose **All** from the Show drop-down list to display all the link remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters link remediations based on each field description in the Link Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Link Remediations page. If you clear the field, it displays the list of all the link remediations in the Link Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Link Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter link remediations by using variables that are more complex. It contains one or more filters, which filter link remediations based on the values that match the field description. A filter on a single row filters link remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter link remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-35 describes the fields that allow you to filter link remediations.

Table 20-35 Filtering Link Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter link remediations by the name of the link remediation.
	Description	This field enables you to filter link remediations by the description of the link remediation.
	Type	This field enables you to filter link remediations by the mode of remediation.
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter link remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter link remediations from the Value drop-down list.

Antivirus Remediation

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

You can filter, add, duplicate, edit, or delete antivirus remediations in the AV Remediations page. The AV Remediations page displays all the antivirus remediations along with their names, description, and their modes of remediation.

This section describes the following procedures to configure and filter antivirus remediations.

- Adding, Duplicating, Editing, and Deleting an Antivirus Remediation
- Filtering Antivirus Remediations

Adding, Duplicating, Editing, and Deleting an Antivirus Remediation

This section describes the procedures to add, duplicate, edit, or delete antivirus remediations from the AV Remediations page.

To add an antivirus remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations.

Step 5 Click **Add**.

The New AV Remediation page appears.

Caution Once created and saved, the name of the antivirus remediation is not editable.

Step 6 Modify the values in the New AV Remediation page to add a new antivirus remediation, as shown in Table 20-36.

Step 7 Click **Submit**.

The new antivirus remediation appears in the AV Remediations page.

To duplicate an antivirus remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations.

Step 5 Check the check box to choose an antivirus remediation, and click **Duplicate** to duplicate an antivirus remediation in the AV Remediations page. You cannot duplicate an antivirus remediation with the same name.

Step 6 Click **Submit**.

A copy of an antivirus remediation appears in the AV Remediations page.

To edit an antivirus remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations.

Step 5 Click the check box to choose an antivirus remediation, and click **Edit** to edit an antivirus remediation.

Step 6 Click **Save**.

The antivirus remediation will be available in the AV Remediations page after you edit the antivirus remediation.

To delete an antivirus remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations.

Step 5 Check the check box to choose an antivirus remediation, and click **Delete** to delete an antivirus remediation from the AV Remediations page.

Table 20-36 describes the fields that allow you to create an antivirus remediation.

Table 20-36 Antivirus Remediation

Field Name	Field Description
Name	Enter the name of an antivirus remediation that you want to create.
Description	Enter the description of an antivirus remediation.
Remediation Type	Click the Remediation Type drop-down list to choose a mode that are predefined for an antivirus remediation: • **Automatic** • **Manual**—when selected, Interval and Retry Count fields are not editable
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antivirus definition.

Table 20-36 Antivirus Remediation (continued)

Field Name	Field Description
Operating System	Choose one of the following options: • **Windows** • **Macintosh**—when selected Remediation Type, Interval, and Retry Count fields are not editable This option specifies the operating system to which AV remediations apply.
AV Vendor Name	Click the drop-down list to view the predefined values for antivirus vendors.

Filtering Antivirus Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the AV Remediations page. A quick filter is a simple filter that can be used to filter antivirus remediations in the AV Remediations page. The quick filter filters antivirus remediations based on the field description such as the name of the antivirus remediation, description, and as well as the mode of remediation in the AV Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the AV Remediations page. The advanced filter filters antivirus remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the AV Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the AV Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter antivirus remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations.

Step 5 In the AV Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-37.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-127 and To filter by using the Advanced Filter option, complete the following steps:, page 20-127.

Note To return to the AV Remediations page, choose **All** from the Show drop-down list to display all the antivirus remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antivirus remediations based on each field description in the AV Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the AV Remediations page. If you clear the field, it displays the list of all the antivirus remediations in the AV Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the AV Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antivirus remediations by using variables that are more complex. It contains one or more filters, which filter antivirus remediations based on the values that match the field description. A filter on a single row filters antivirus remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antivirus remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-37 describes the fields that allow you to filter antivirus remediations.

Table 20-37 Filtering AV Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter antivirus remediations by the name of an antivirus remediation.
	Description	This field enables you to filter antivirus remediations by the description of an antivirus remediation.
	Type	This field enables you to filter antivirus remediations by the mode of remediation.
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter antivirus remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter antivirus remediations from the Value drop-down list.

Antispyware Remediation

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

You can filter, add, duplicate, edit, or delete antispyware remediations in the AS Remediations page. The AS Remediations page displays all the antivirus remediations along with their names, description, and their modes of remediation.

This section describes the following procedures to configure and filter antispyware remediations.

- Adding, Duplicating, Editing, and Deleting an Antispyware Remediation
- Filtering Antispyware Remediations

Adding, Duplicating, Editing, and Deleting an Antispyware Remediation

This section describes the procedures to add, duplicate, edit, or delete antispyware remediations from the AS Remediations page.

To add an antispyware remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations.

Step 5 Click **Add**.

The New AS Remediation page appears.

⚠ **Caution** Once created and saved, the name of the antispyware remediation is not editable.

Step 6 Modify the values in the New AS Remediations page to add a new antispyware remediation, as shown in Table 20-38.

Step 7 Click **Submit**.

The new antispyware remediation appears in the AS Remediations page.

To duplicate an antispyware remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations.

Step 5 Check the check box to choose an antispyware remediation, and click **Duplicate** to duplicate an antispyware remediation in the AS Remediations page. You cannot duplicate an antispyware remediation with the same name.

Step 6 Click **Submit**.

A copy of an antispyware remediation appears in the AS Remediations page.

To edit an antispyware remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations.

Step 5 Check the check box to choose an antispyware remediation, and click **Edit** to edit an antispyware remediation.

Step 6 Click **Save**.

The antispyware remediation will be available in the AS Remediations page after you edit the antispyware remediation.

To delete an antispyware remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations.

Step 5 Check the check box to choose an antispyware remediation, and click **Delete** to delete an antispyware remediation.

Table 20-38 describes the fields that allow you to create an antispyware remediation:

Table 20-38 Antispyware Remediation

Field Name	Field Description
Name	Enter the name of an antispyware remediation that you want to create.
Description	Enter the description of an antispyware remediation.
Remediation Type	Click the Remediation Type drop-down list, choose a mode that are predefined for an antispyware remediation: • **Automatic** • **Manual**—when selected, Interval and Retry Count fields are not editable
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antispyware definition.
Operating System	Choose one of the following options: • **Windows** • **Macintosh**—when selected, Remediation Type, Interval, and Retry Count fields are not editable This option specifies the operating system to which AS remediations apply.
AS Vendor Name	Click the drop-down list to view the predefined values for antispyware vendors.

Filtering Antispyware Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the AS remediations page. A quick filter is a simple filter that can be used to filter antispyware remediations in the AS Remediations page. The quick filter filters antispyware remediations based on the field description such as the name of the antispyware remediation, description, and as well as the mode of remediation in the AS Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the AS Remediations page. The advanced filter filters antispyware remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the AS Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the AS Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter antispyware remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations.

Step 5 In the AS Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-39.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-131 and To filter by using the Advanced Filter option, complete the following steps:, page 20-132.

Note To return to the AS Remediations page, choose **All** from the Show drop-down list to display all the antispyware remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antispyware remediations based on each field description in the AS Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the AS Remediations page. If you clear the field, it displays the list of all the antispyware remediations in the AS Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the AS Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antispyware remediations by using variables that are more complex. It contains one or more filters, which filter antispyware remediations based on the values that match the field description. A filter on a single row filters antispyware remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antispyware remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-39 describes the fields that allow you to filter antispyware remediations.

Table 20-39 Filtering AS Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter antispyware remediations by the name of an antispyware remediation.
	Description	This field enables you to filter antispyware remediations by the description of an antispyware remediation.
	Type	This field enables you to filter antispyware remediations by the mode of remediation.

Table 20-39 Filtering AS Remediations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter antispyware remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter antispyware remediations from the Value drop-down list.

Launch Program Remediation

A launch program remediation launches one, or more programs on clients for compliance. You can create a launch program remediation, where the NAC Agents and Web Agents remediate clients by launching one, or more applications on clients for compliance.

You can filter, add, duplicate, edit, or delete launch program remediations in the Launch Program Remediations page. The Launch Program Remediations page displays all the launch program remediations along with their names, description, and their modes of remediation.

This section describes the following procedures to configure and filter launch program remediations.

- Adding, Duplicating, Editing, and Deleting a Launch Program Remediation
- Filtering Launch Program Remediations

Adding, Duplicating, Editing, and Deleting a Launch Program Remediation

This section describes the procedures to add, duplicate, edit, delete launch program remediations from the Launch Program Remediations page.

To add a launch program remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations.

Step 5 Click **Add**.

The New Launch Program Remediation page appears.

Caution Once created and saved, the name of the launch program remediation is not editable.

Step 6 Modify the values in the New Launch Program Remediation page to add a new launch program remediation, as shown in Table 20-40.

Step 7 Click **Submit**.

The new launch program remediation appears in the Launch Program Remediations page.

To duplicate a launch program remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations.

Step 5 Check the check box to choose a launch program remediation, and click **Duplicate** to duplicate a launch program remediation in the Launch Program Remediations page. You cannot duplicate a launch program remediation with the same name.

Step 6 Click **Submit**.

A copy of a launch program remediation appears in the Launch Program Remediations page.

To edit a launch program remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations.

Step 5 Check the check box to choose a launch program remediation, and click **Edit** to edit a launch program remediation.

Step 6 Click **Save**.

The launch program remediation will be available in the Launch Program Remediations page after you edit the launch program remediation.

To delete a launch program remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon to navigate to Remediation Actions.

Step 4 Click **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations.

Step 5 Check the check box to choose a launch program remediation, and click **Delete** to delete a launch program remediation.

Table 20-40 describes the fields that allow you to create a launch program remediation.

Table 20-40 Launch Program Remediation

Field Name	Field Description
Name	Enter the name of the launch program remediation that you want to create.
Description	Enter the description of the launch program remediation that you want to create.
Remediation Type	Click the Remediation Type drop-down list to choose a mode that are predefined for launch program remediations: • **Automatic** • **Manual**
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to launch required programs.
Program Installation Path	Choose the path in which a remediation program has to be installed from the Program Installation Path drop-down list. Click the Program Installation Path drop-down list to view the following predefined paths to installing programs: • **ABSOLUTE_PATH**—remediation program is installed in the fully qualified path of the file. For example, C:\<directory>\ • **SYSTEM_32**—remediation program is installed in the C:\WINDOWS\system32 directory • **SYSTEM_DRIVE**—remediation program is installed in the C:\ drive • **SYSTEM_PROGRAMS**—remediation program is installed in the C:\Program Files • **SYSTEM_ROOT**—remediation program is installed in the root path for Windows system
Program Executable	Enter the name of the remediation program executable, or an installation file.
Program Parameters	Optional. Enter required parameters for the remediation programs.
Existing Programs	Existing Programs table displays the installation paths of remediation programs, the name of the remediation programs installed, and parameters if any. Add—Click to add remediation programs to the list after entering program executable, or an installation file. Delete—Click to delete remediation programs from the list.

Filtering Launch Program Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Launch Program Remediations page. A quick filter is a simple and quick filter that can be used to filter launch program remediations in the Launch Program Remediations page. The quick filter filters launch program remediations based on the field description such as the name of the launch program remediations, description, as well as the mode of remediation in the Launch Program Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Launch Program Remediations page. The advanced filter filters launch program remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Launch Program Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Launch Program Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter launch program remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Launch Program Remediation**.

The Launch Program Remediation page appears, which lists all the launch program remediations.

Step 5 In the Launch Programs Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-41.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-136 and To filter by using the Advanced Filter option, complete the following steps:, page 20-137.

Note To return to the Launch Program Remediations page, choose **All** from the Show drop-down list to display all the launch program remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters launch program remediations based on each field description in the Launch Program Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Launch Program Remediations page. If you clear the field, it displays the list of all the launch program remediations in the Launch Program Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Launch Program Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter launch program remediations by using variables that are more complex. It contains one or more filters, which filter launch program remediations based on the values that match the field description. A filter on a single row filters launch program remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter launch program remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-41 describes the fields that allow you to filter launch program remediations.

Table 20-41 Filtering Launch Program Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter launch program remediations by the name of the program remediation.
	Description	This field enables you to filter launch program remediations by the description of the program remediation.
	Type	This field enables you to filter launch program remediations by type.

Table 20-41 Filtering Launch Program Remediations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter launch program remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter launch program remediations from the Value drop-down list.

Windows Update Remediation

A Windows update remediation ensures that Automatic Updates configuration is turned on Windows clients per your security policy, and helps you to ensure that Automatic Updates remediates Windows clients to result in successful posture assessments for compliance.

You can filter, add, duplicate, edit, or delete Windows update remediations from the Windows Update Remediations page. The Windows Update Remediations page displays all the Windows update remediations along with their names, description, as well as their modes of remediation.

Windows Automatic Updates

The Windows administrators have an option to turn on or turn off Automatic Updates on Windows clients. The Microsoft Windows uses this feature to regularly check for important updates and install them on your clients. If the Automatic Updates feature is turned on, then the Windows automatically updates Windows-recommended updates before any other updates.

Windows XP provides the following settings for configuring Automatic Updates:

- Automatic (recommended)—Windows allows clients automatically download recommended Windows updates for their computers and install them
- 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 them
- Notify me but don’t automatically download or install them—Windows only notifies clients, but does not automatically download, or install them
- Turn off Automatic Updates—Windows allows clients to turn off Windows Automatic Updates feature. Here, clients are vulnerable unless clients install updates regularly. They can install updates from the Windows Update Web site link.

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

You can create a Windows update remediation to check for the Windows updates service (wuaserv) whether the service is started or stopped in any Windows client by using the **pr_AutoUpdateCheck_Rule**. It is a predefined Cisco rule, which can be used to create a posture requirement. If the posture requirement fails, the remediation action (Windows update remediation) that you associate to the requirement enforces the Windows client to remediate by using one of the automatic updates options.

Override User's Windows Update Setting With Administrator's Option in Windows Update Remediations

You can enable the "Override User's Windows Update setting with administrator's" option to override the user's with remediation settings, or else you can disable the option.

Note The users setting are not restored back here to their original setting even after they exit from NAC Agents, or when they reboot their Windows clients, or when they restart the Windows Automatic Updates service on their Windows clients.

If "Override User's Windows update setting with administrator's" option is disabled, Windows update remediations will not be enforced except for "Turn Off Automatic Updates" settings on Windows clients.

Windows update remediations will fail when you want to change the Windows Automatic Updates setting:

- From Automatic (recommended) to Download updates for me, but let me choose when to install them and vice versa.
- From Automatic (recommended) to Notify me but don't automatically download or install them and vice versa.
- From Notify me but don't automatically download or install them to Download updates for me, but let me choose when to install them and vice versa.

This section describes the following procedures to configure and filter Windows update remediations.

- Adding, Duplicating, Editing, and Deleting a Windows Update Remediation
- Filtering Windows Update Remediations

Adding, Duplicating, Editing, and Deleting a Windows Update Remediation

This section describes the procedures to add, duplicate, edit, or delete Windows update remediations from the Windows Update Remediations page.

To add a Windows update remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations.

Step 5 Click **Add**.

The New Windows Update Remediation page appears.

Caution Once created and saved, the name of the Windows update remediation is not editable.

Step 6 Modify the values in the New Windows Update Remediation page to add a new Windows update remediation, as shown in Table 20-42.

Step 7 Click **Submit**.

The new Windows update remediation appears in the Windows update remediations page.

To duplicate a Windows update remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations.

Step 5 Check the check box to choose a Windows update remediation, and click **Duplicate** to duplicate a Windows update remediation in the Windows Update Remediations page. You cannot duplicate a Windows update remediation with the same name.

Step 6 Click **Submit**.

A copy of a Windows update remediation appears in the Windows Update Remediations page.

To edit a Windows update remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations.

Step 5 Check the check box to choose a Windows update remediation, and click **Edit** to edit a Windows update remediation.

Step 6 Click **Save**.

The Windows update remediation will be available in the Windows Update Remediations page after you edit the Windows update Remediation.

To delete a Windows update remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations.

Step 5 Check the check box to choose a Windows update remediation, and click **Delete** to delete a Windows update remediation.

Table 20-42 describes the fields that allow you to create a Windows update remediation:

Table 20-42 Windows Update Remediation

Field Name	Field Description
Name	Enter the name of the Windows update remediation that you want to create.
Description	Enter the description of the Windows update remediation that you want to create.
Remediation Type	Click the Remediation Type drop-down list to choose a mode that are predefined for Windows updates: • **Automatic** • **Manual**—when selected, Interval and Retry Count fields are not editable
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that Windows clients can try for Windows updates.

Table 20-42 Windows Update Remediation (continued)

Field Name	Field Description
Windows Update Setting	Cisco ISE provides the following four options for Windows update remediations: **a.** Do not change setting—If selected, the Windows Automatic Updates client configuration does not change during, or after Windows update remediation. **b.** Notify to download and install—Windows only notifies clients, but does not automatically download, or install them. If selected, Windows only notifies clients to download, or install Windows updates. **c.** Automatically download and notify to install—Windows downloads updates for clients, and allows them to choose when to install them. If selected, Windows automatically downloads, and notifies clients to install Windows updates. **d.** Automatically download and install—Windows allows clients automatically download recommended Windows updates for their computers and install them. If selected, Windows automatically downloads, and installs Windows updates. This is the highly recommended setting from Windows for Windows clients. Click the drop-down list to choose an option for Automatic Updates setting on Windows clients.
Override User's Windows Update setting with administrator's check box.	A check box, which allows Cisco ISE administrators to override Automatic Updates configuration of Windows clients. If checked, the setting enforces the Cisco ISE administrator-specified setting for Windows Automatic Updates on all the client machines during, and after Windows update remediation. If unchecked, the setting enforces the following: • The Cisco ISE administrator-specified setting only when Automatic Updates are disabled on Windows clients. • The Windows clients-specified setting only when Windows Automatic Updates are enabled on the client.

Filtering Windows Update Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Windows Update Remediations page. A quick filter is a simple and quick filter that can be used to filter Windows update remediations in the Windows Update Remediations page. The quick filter filters Windows update remediations based on the field description such as the name of the Windows update remediations, description, as well as the mode of remediation in the Windows Update Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Windows Update Remediations page. The advanced filter filters Windows update remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Windows Update Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Windows Update Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter Windows update remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations.

Step 5 In the Windows Update Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-43.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-143 and To filter by using the Advanced Filter option, complete the following steps:, page 20-143.

Note To return to the Windows Update Remediations page, choose **All** from the Show drop-down list to display all the Windows update remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters Windows update remediations based on each field description in the Windows Update Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Windows Update Remediations page. If you clear the field, it displays the list of all the Windows update remediations in the Windows Update Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Windows Update Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter Windows update remediations by using variables that are more complex. It contains one or more filters, which filter Windows update remediations based in the values that match the field description. A filter on a single row filters Windows update remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter Windows update remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-43 describes the fields that allow you to filter Windows update remediations:.

Table 20-43 Filtering Windows Update Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter Windows update remediations by the name of the Windows update remediation.
	Description	This field enables you to filter Windows update remediations by the description of the Windows update remediation.
	Type	This field enables you to filter Windows update remediations by type.
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter Windows update remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter Windows update remediations from the Value drop-down list.

Windows Server Update Services Remediation

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

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.

The Windows Server Update Services (WSUS) Remediations page displays all the WSUS remediations along with their names, description, and as well as their modes of remediation. You can filter, add, duplicate, edit, or delete WSUS remediations from the remediations list.

Note When you associate a WSUS remediation action to a posture requirement to validate Windows updates by using the severity level option, you must choose the pr_WSUSRule (a dummy compound condition) compound condition in the posture requirement. When the posture requirement fails, the NAC Agent enforces the remediation action (Windows updates) based on the severity level that you define in the WSUS remediation.

This section describes the following procedures to configure and filter WSUS remediations.

- Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation
- Filtering Windows Server Update Services Remediations

Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation

This section describes the procedures to add, duplicate, edit, or delete WSUS remediations from the Windows Server Update Services Remediations page.

To add a Windows server update services remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations.

Step 5 Click **Add**.

The New Windows Server Update Services Remediation page appears.

Caution Once created and saved, the name of the Windows server update services remediation is not editable.

Step 6 Modify the values in the New Windows Server Update Services Remediation page to add a new WSUS remediation, as shown in Table 20-44.

Step 7 Click **Submit**.

The new WSUS remediation appears in the Windows Server Update Services Remediations page.

To duplicate a Windows server update services remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations.

Step 5 Check the check box to choose a WSUS remediation, and click **Duplicate** to duplicate a WSUS remediation in the Windows Server Update Services Remediations page. You cannot duplicate a WSUS remediation with the same name.

Step 6 Click **Submit**.

A copy of a WSUS remediation appears in the Windows Server Update Services Remediations page.

To edit a Windows server update services remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations.

Step 5 Check the check box to choose a WSUS remediation, and click **Edit** to edit a WSUS remediation.

Step 6 Click **Save**.

The WSUS remediation will be available in the Windows Server Update Services Remediations after you edit the WSUS remediation.

To delete a Windows server update services remediation, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker icon (right arrow) to navigate to Remediation Actions.

Step 4 Click **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations.

Step 5 Check the check box to choose a WSUS remediation, and click **Delete** to delete a WSUS remediation from the Windows Server Update Services Remediations page.

Table 20-44 describes the fields that allow you to create a WSUS remediation.

Table 20-44 WSUS Remediation

Field Name	Field Description
Name	Enter the name of the WSUS remediation that you want to create.
Description	Enter the description of the WSUS remediation that you want to create.
Remediation Type	Click the Remediation Type drop-down list to choose a mode that are predefined for WSUS remediations. The following options are available: • **Automatic**—The NAC Agents automatically updates Windows clients with the latest WSUS updates. • **Manual**—When it is selected, Interval and Retry Count fields are nor editable. The user manually updates the Windows client with the latest WSUS updates from a Microsoft-managed WSUS server, or from the locally administered WSUS server for compliance.
Interval (in seconds)	Enter the interval in seconds (the default interval is 0) to delay WSUS updates before the NAC Agents and Web Agents attempt to retry after the previous attempt.
Retry Count	Enter the number of attempts that the NAC Agents and web Agents retry to update Windows clients with WSUS updates.
Validate Windows updates using	The validation method that you use to check the Windows operating system that is installed on the client for Windows updates. The available options are: • **Cisco Rules** • **Severity Level**
Cisco Rules	The validation method that you will use to check the client Windows operating system to meet minimum security standards as a result of dynamic posture updates downloaded to the Cisco ISE server. Click the Cisco Rules radio button to validate WSUS updates using Cisco Rules. If selected, custom or preconfigured rules must be selected as conditions in the posture requirement.

Table 20-44 WSUS Remediation (continued)

Field Name	Field Description
Severity Level	The validation method that you will use to check the client Windows operating system to meet minimum security standards by using a Microsoft-managed WSUS server, or locally administered WSUS server. Click the Security Level radio button to validate WSUS updates based on the Security Level set on the WSUS server. If selected, custom or preconfigured rules can be selected as conditions in the posture requirement, but they are not used. For this purpose, the pr_WSUSRule can be used as a placeholder condition (a dummy condition) in the posture requirement that specifies a WSUS remediation.
Windows Updates Severity Level	The severity level of Windows updates that you select to install on Windows clients. The following are the severity levels of WSUS updates that you can install on Windows clients: • **Critical**—Installs only critical Windows updates • **Express**—Installs important and critical Windows updates • **Medium**—Installs all critical, important and moderate Windows updates • **All**—Installs all critical, important, moderate and low Windows updates
Update to latest OS Service Pack	If checked, then the WSUS remediation installs the latest service pack available for the client's operating system automatically. **Note** The operating system service packs are updated automatically irrespective of the Medium and All severity level options selected in WSUS remediation.
Windows Updates Installation Source	This selection specifies the source from where you install WSUS updates on Windows clients: • **Microsoft server**—Microsoft-managed WSUS server • **Managed server**—Locally administered WSUS server
Installation Wizard Interface Setting	An option to display the installation wizard on the client during WSUS updates: • **Show UI**—An option to display the Windows Update Installation Wizard progress on Windows clients. (Users must have Administrator privileges on client machines in order to see the installation wizard user interface during WSUS updates.) • **No UI**—An option to hide the Windows Update Installation Wizard progress on Windows clients.

Filtering Windows Server Update Services Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well in the Windows Server Update Services Remediations page. A quick filter is a simple and quick filter that can be used to filter WSUS remediations in the Windows Server Update Services Remediations page. The quick filter filters WSUS remediations based on the field description such as the name of the WSUS remediations, description, and the mode of remediation in the Windows Server Update Services Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results in the Windows Server Update Services Remediations page. The advanced filter filters WSUS remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the Windows Server Update Services Remediations page. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results in the Windows Server Update Services Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter WSUS remediations, complete the following steps:

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

Step 2 In the Results navigation pane, expand **Posture**.

Step 3 Click **Remediation Actions** or click the quick picker (right arrow) icon to navigate to Remediation Actions.

Step 4 Click **WSUS Server Update Services Remediation**.

Step 5 In the Windows Server Update Services Remediations page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 20-45.

For more information, see the To filter by using the Quick Filter option, complete the following steps:, page 20-149 and To filter by using the Advanced Filter option, complete the following steps:, page 20-150.

Note To return to the Windows Server Update Services Remediations page, choose **All** from the Show drop-down list to display all the WSUS remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters WSUS remediations based on each field description in the Windows Server Update Services Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results in the Windows Server Update Services Remediations page. If you clear the field, it displays the list of all the WSUS remediations in the Windows Server Update Services Remediations page.

Step 1 To filter, click **Go** within each field to refresh the page with the results that are displayed in the Windows Server Update Services Remediations page.

Step 2 To clear the field, click **Clear** within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter WSUS remediations by using variables that are more complex. It contains one or more filters, which filter WSUS remediations based on the values that match the field description. A filter on a single row filters WSUS remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter WSUS remediations by using any one or all the filters within a single advanced filter.

Step 1 To choose the field description, click the drop-down arrow.

Step 2 To choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click **Add Row** (plus [+] sign) to add the filtered lists, or click **Remove Row** (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Step 8 Click **Clear Filter** after filtering.

Table 20-45 describes the fields that allow you to filter WSUS remediations.

Table 20-45 Filtering Windows Server Update Services Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter WSUS remediations by the name of the WSUS remediation.
	Description	This field enables you to filter WSUS remediations by the description of the WSUS remediation.
	Type	This field enables you to filter WSUS remediations by type.

Table 20-45 Filtering Windows Server Update Services Remediations

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down list to choose the field description.
	Operator	Choose an operator that can be used to filter WSUS remediations from the Operator drop-down list.
	Value	Choose the value for the field description that you selected against which to filter WSUS remediations from the Value drop-down list.

Client Posture Assessment Requirements

Prerequisite

You must have an understanding of Acceptable Use Policy (AUP) for a posture as you create posture requirements. Refer to the following location on AUP with respect to posture compliance:

Administration > System > Settings > Posture > Acceptable Use policy.

For more information on AUP, see Posture Acceptable Use Policy, page 20-25.

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role in conjunction with an operating system. All the clients that are connecting to your network must meet mandatory requirements during posture policies evaluation, which are associated to posture policies to become compliant on your network. If requirements are optional and clients fail these requirements, then the clients have an option to continue further so that end users can skip optional requirements even though they fail during policy evaluation.

If clients fail to meet mandatory requirements during posture policies evaluation, then they are denied network access to your network, and they are moved into a quarantine state. If clients are moved into the quarantine state, they will not be able to reauthenticate again to be postured successfully for compliance again. If clients need to come out of the quarantine state to become compliant, then the network access devices must be configured to restart a new RADIUS session after the session times out so that clients can reauthenticate again to meet mandatory requirements for compliance.

For information on configuration guidance of posture clients quarantine state, see “Authorization Profile Configuration Guidance for Posture Clients Quarantine State” section on page 20-25.

pr_WSUSRule

The pr_WSUSRule is a dummy compound condition, which is used in a posture requirement with a Windows Server Update Services (WSUS) remediation associated to it. The associated WSUS remediation action must be configured to validate Windows updates by using the severity level option. When this requirement fails, the NAC Agent that is installed on the Windows client enforces the WSUS remediation action based on the severity level that you define in the WSUS remediation.

Note The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.

You can use the Posture Requirements page to insert (create) a new requirement, or duplicate an existing requirement, or delete an existing requirement.

Creating User Defined Conditions and Remediation Actions

Cisco ISE allows you to create and associate user defined conditions, associate Cisco defined conditions, and create and associate remediation actions in the Requirements page itself that simplifies requirement configuration without navigating to their respective pages. Once created and saved in the Requirements page, these user defined conditions and remediation actions can be viewed from their respective lists.

Table 20-46 describes the fields in the Posture Requirements page that allow you to insert a new posture requirement, or duplicate an existing requirement or delete an existing posture requirement.

Table 20-46 Posture Requirement

Field	Field Description
Name	Enter the name of the requirement that you want to create.
Operating Systems	Choose an operating system. It allows you to select all, or specific Windows, or Macintosh operating systems to which the posture requirement is applied.
Conditions	Choose one or more dictionary simple conditions, and dictionary compound conditions to which the posture requirement should apply from the Conditions object selector. If more than one condition is selected, then all the conditions must be met (a logical AND operation) to form a compound condition. The system uses "&" as the AND operator. The conditions are defined in the following location: Policy > Policy Elements > Conditions > Posture. For more information on the posture conditions, see the Custom Conditions for Posture, page 20-42.
Remediation Actions	Choose a remediation from the Remediations object selector. The remediation action defines the action to be taken when the posture requirement fails on the client. The remediation actions are defined in the following location: Policy > Policy Elements > Results > Posture > Remediation Actions. For information on the posture remediation actions, see the Custom Posture Remediation Actions, page 20-113.

For more information on how to manage posture requirements, see the "Creating, Duplicating, and Deleting Client Posture Requirements" section on page 20-153.

Related Topics

Client Posture Assessment Policies, page 20-33

Custom Posture Remediation Actions, page 20-113

Creating, Duplicating, and Deleting Client Posture Requirements

This section describes the following procedures on how to insert (create) a new requirement, or duplicate an existing requirement, or delete an existing requirement in the Requirements page.

- Creating a New Posture Requirement, page 20-153
- Duplicating a Posture Requirement, page 20-157
- Deleting a Posture Requirement, page 20-157

Creating a New Posture Requirement

You can create a new posture requirement in the Requirements page.

To insert a new requirement, complete the following steps:

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

The Requirements page appears.

Step 2 Enter the requirement name.

Caution The operating system is not editable in the posture requirement after you have associated the newly created requirement to a posture policy. To edit the operating system in the requirement, you need to remove the posture requirement association from the posture policy.

Step 3 From the Operating Systems anchored overlay, choose **Select Operating Systems**.

To choose an operating system, complete the following steps:

a. Click the plus [+] sign to expand the operating systems anchored overlay.

The operating systems anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Operating Systems quick picker (down arrow) icon.

The parent groups for the operating systems appears in the Operating System Groups object selector.

c. Choose the parent operating system group.

- For Mac OS X (Macintosh), the group has three underlying versions. From the Mac OS X (Macintosh) group, choose the underlying Macintosh operating system.
- For Windows All, the group has the Windows 7 (All), Windows Vista (All), and Windows XP (All) groups that contain underlying versions for each of the groups. From the Windows All group, choose the underlying Windows group and the Windows version. Each Windows group contains its own underlying versions.

d. Click **Add** (plus [+] sign) to associate more than one operating system to the policy.

e. Click **Remove** (minus [-] sign) to remove the operating system from the policy.

Step 4 From the Conditions anchored overlay, choose **Select Conditions**.

To choose a condition, complete the following steps:

a. Click the plus [+] sign to expand the Conditions anchored overlay.

The Conditions anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Conditions quick picker (down arrow) icon.

The Conditions object selector appears. The Conditions object selector lists User Defined Conditions and Cisco Defined Conditions. You can create a user defined condition that can be saved to the respective user defined conditions list.

c. From the Conditions object selector, choose **User Defined Conditions**.

The row view button shows the list of user defined conditions in a row format in the right pane of the Conditions object selector. The tabbed view button shows the list of user defined conditions in a tree format under user defined conditions in the Conditions object selector.

To choose a user defined condition, complete the following steps:

d. Click the quick picker (right arrow) to view the list of user defined conditions.

Choose one of the following user defined conditions:

- File Conditions
- Registry Conditions
- Service Conditions
- Application Conditions
- Regular Compound Conditions
- AV Compound Conditions
- AS Compound Conditions

e. Click the quick picker (right arrow) to view the list of each user defined condition.

You can choose a user defined condition from the list.

You cannot edit the associated parent operating system while creating user defined conditions in the Requirements page.

To create a user defined condition from the Conditions object selector, complete the following steps:

a. Click the Select Conditions quick picker (right arrow) icon.

The Conditions object selector appears, which lists User Defined Conditions and Cisco Defined Conditions.

b. Click the quick picker (right arrow) on the **Action** icon.

You can create any user defined condition that allows you to save it to the existing list of respective user defined conditions, as well as associate it to the requirement from the Requirements page.

c. Choose one of the user defined conditions from the following conditions:

- Create File Condition

  The Add File Condition dialog appears. Here, you can create a file (simple) condition.

- Create Registry Condition

  The Add Registry Condition dialog appears. Here, you can create a registry (simple) condition.

- Create Application Condition

  The Add Application Condition dialog appears. Here, you can create an application (simple) condition.

- Create Service Condition

The Add Service Condition dialog appears. Here, you can create a service (simple) condition.

- Create Compound Condition

  The Add Compound Condition dialog appears. Here, you can create a regular compound condition where you can add simple file conditions, registry conditions, application conditions and service conditions and form a compound condition by using AND. OR, NOT logical operators.

- Create AV Compound Condition

  The Add AV Compound Condition dialog appears. Here, you can create an AV compound condition.

- Create AS Compound Condition

  The Add AS Compound Condition dialog appears. Here, you can create an AS compound condition.

d. Click **Save and Select**.

   Once created, the user defined condition can be saved to the existing list of respective user defined conditions, as well as associated to the requirements from the Requirements page.

To choose a Cisco defined condition, complete the following steps:

a. From the Conditions object selector, choose **Cisco Defined Conditions**.

   The row view button shows the list of Cisco defined conditions in a row format in the right pane of the Conditions object selector. The tabbed view button shows the list of Cisco defined conditions in a tree format in the Conditions object selector.

b. Click the quick picker (right arrow) to view the list of each Cisco defined conditions.

   Choose one of the following Cisco defined conditions:

   - File Conditions
   - Registry Conditions
   - Service Conditions
   - Application Conditions
   - Regular Compound Condition

     pr_WSUSRule is a dummy compound condition. For more information, see the pr_WSUSRule, page 20-151.

   - AV Compound Condition
   - AS Compound Condition

c. Choose a Cisco defined condition.

To associate one or more conditions to the requirement, complete the following steps:

a. Click **Add** (plus [+] sign) to associate more than one condition to the requirement.

b. Click **Remove** (minus [-] sign) to remove the condition from the requirement.

To validate associated conditions in a requirement, complete the following step:

a. Choose one of the following options:

   - All selected conditions succeed
   - Any selected condition succeeds
   - No selected condition succeeds

Step 5 From the Remediations Actions anchored overlay, choose **Select Remediations**.

To choose a remediation action, complete the following steps:

a. Click the plus [+] sign to expand the remediation anchored overlay.

The Remediations anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Remediations quick picker (down arrow) icon.

The Remediations object selector appears.

c. Choose the remediation action.

For Message Text only action, enter appropriate information in text so that the NAC Agent displays it on the client. For more information, see the Message Text Only, page 20-113.

To create a remediation action, complete the following steps:

a. Click the Select Remediation quick picker (down arrow) icon.

The Remediations object selector appears, which lists all the remediation actions.

b. Click the quick picker (down arrow) on the **Action** icon.

You can create a remediation action that allows you to save it to the existing list of respective remediation actions, as well as associate it from the Requirements page.

c. Choose one of the remediation actions from the following:

- Create AV Remediation

  The Add AV Remediation dialog appears. Here, you can create an AV remediation.

- Create AS Remediation

  The Add AS Remediation dialog appears. Here, you can create an AS remediation.

- Create File Remediation

  The Add File Remediation dialog appears. Here, you can create a file remediation.

- Create Launch Program Remediation

  The Add Launch Program Remediation dialog appears. Here, you can create a launch program remediation.

- Create Link Remediation

  The Add Link Remediation dialog appears. Here, you can create a link remediation.

- Create Windows Server Update Services Remediation

  The Add Windows Server Update Services Remediation dialog appears. Here, you can create a WSUS remediation.

- Create Windows Update Remediation

  The Add Windows Update Remediation dialog appears. Here, you can create a Windows update remediation.

d. Click **Save and Select**.

Once created, the remediation actions can be saved to the existing list of respective remediation actions list, as well as associated to the requirements from the Requirements page.

Step 6 Click **Done** to save the posture requirement in read-only mode. To edit the posture requirement, click **Edit** to switch to edit mode.

Step 7 Click **Save**.

Duplicating a Posture Requirement

You can create a copy of a posture requirement that you want to duplicate in the Requirements page.

To duplicate a requirement, complete the following steps:

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

The Requirements page appears.

Step 2 Click the quick picker (down arrow) next to Edit.

Step 3 Click **Duplicate** to create a copy of the requirement that you want to duplicate.

Step 4 Click **Save**.

Deleting a Posture Requirement

You can also delete a posture requirement from the Requirements page.

To delete a requirement, complete the following steps:

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

The Requirements page appears

Step 2 Click the quick picker (down arrow) next to Edit.

Step 3 Click **Delete** to delete a requirement from the Requirements page.

Custom Authorization Policies for Posture

This section describes the standard authorization policies that you define for posture in the Cisco ISE appliance.

You can define two types of authorization policies in the Authorization Policy page, the standard authorization policies and the exceptions authorization policies. The standard authorization policies that are specific to posture in the Authorization Policy page are used to make policy decisions (enforce policies) based on the compliance status of endpoints such as unknown, compliant, and noncompliant. The standard authorization profiles (permissions) that you define in the Authorization Profiles page set access privileges based on the matching compliance status.

You can create posture-specific authorization policies for all wired, wireless, and guest deployments by specifying the Session:PostureStatus attribute in the authorization policies. This attribute has three values, unknown, compliant, and noncompliant, which you can use n the authorization policies.

First Matched Rule Applies

With this option selected, one or more authorization profiles (permissions) that are defined in the authorization policy set the access privileges (authorization) for an end user based on the first matching authorization policy during evaluation.

The selection of First Matched Rule Applies option allows you to configure authorization profiles for an end user by applying the first matching authorization policy from the standard authorization policies that are enabled in the Authorization Policy page. Cisco ISE evaluates the standard authorization policies that are enabled in the Authorization Policy page and then determines the authorization profile, or authorization profiles that are associated in the standard authorization policies. Once the first matching authorization policy is found, Cisco ISE stops evaluating the rest of the standard authorization policies in the Authorization Policy page.

Multiple Matched Rule Applies

With this option selected, one or more authorization profiles that are defined in the authorization policies determine the access privileges for an end user based on multiple matching authorization policies during evaluation.

The selection of Multiple Matched Rule Applies option allows you to configure authorization profiles for an end user by applying multiple matching authorization policies from the standard authorization policies that are enabled in the Authorization Policy page. Cisco ISE evaluates all the standard authorization policies that are enabled in the Authorization Policy page and finds all the matching authorization policies in the Authorization Policy page. When multiple matching authorization policies are found, Cisco ISE determines the authorization profile or profiles for the end user.

Prerequisites:

Before you begin, you should have an understanding of authorization policies in Cisco ISE.

For information on the authorization policies, see Chapter 17, “Managing Authorization Policies and Profiles.”

This section covers the following procedures:

- Standard Authorization Policies for a Posture, page 20-158
- Creating, Duplicating, and Deleting a Standard Authorization Policy for a Posture, page 20-159

Standard Authorization Policies for a Posture

This section describes the basic operations that allow you to manage the standard authorization policies that are specific to posture service.

The Authorization Policy page displays the list of exceptions authorization policies and the standard authorization policies. The Authorization Policy page allows you to configure the standard authorization policies that can be applied to the first matching rule (authorization policy) or multiple matching rules (authorization policies) in the Authorization Policy page.

When they are created and saved, you can also prioritize the standard authorization policies by moving the standard authorization policies up and down in the Authorization Policy page. If the policies are enabled within the standard authorization policy, then the standard authorization policies enforce policies based on the compliance status of the endpoints. If they are disabled, then the standard authorization policies do not enforce policies on the endpoints. You can also configure the standard authorization policies that can be set to only monitor policies based on the compliance status.

To create a standard authorization policy, complete the following steps:

Step 1 Choose **Policy > Authorization**.

The Authorization Policy page appears. This page displays the list of authorization policies for standard and exceptions types.

Step 2 Click the drop-down list to view the matching rule options.

The First Matched Rule Applies and Multiple Matched Rule Applies options appear.

Step 3 Click **First Matched Rule Applies** or **Multiple Matched Rule Applies** from the drop-down list.

The first matched rule applies option sets access privileges (standard authorization profiles) with a single authorization policy that is first matched during evaluation from the list of standard authorization policies.

The multiple matched rule applies option sets access privileges (standard authorization profiles) with multiple authorization policies that are matched during evaluation from the list of all the standard authorization policies.

Step 4 Click the quick picker (down arrow) next to Edit to insert a new authorization policy, duplicate an existing authorization policy, or delete an existing authorization policy.

You can do the following:

- Insert New Rule Above
- Insert New Rule Below
- Duplicate Above
- Duplicate Below
- Delete

Step 5 Click **Done** to create a new standard authorization policy.

The standard authorization policy appears in read only-mode in the Authorization Policy page. Click **Edit** to switch the authorization policy row to edit mode.

Step 6 Click **Save**.

Creating, Duplicating, and Deleting a Standard Authorization Policy for a Posture

You can create a new authorization policy, duplicate an existing authorization policy, or delete an existing authorization policy in the Authorization Policy page. Exceptions and Standard items in the Authorization Policy page display the authorization policy widgets.

To create (insert) a standard authorization policy for posture, complete the following steps:

Step 1 Choose **Policy > Authorization**.

The Authorization Policy page lists standard and exceptions authorization policies.

Step 2 Click the quick picker (down arrow) next to Edit to open the menu.

Step 3 Click **Insert New Rule Above** from the default standard authorization policy row.

The new authorization policy row appears above the default standard authorization policy row.

Note The Insert new Rule Above is the only menu available from the default standard authorization policy row. Insert New Rule Above, Insert New Rule Below, Duplicate Above, Duplicate Below, and Delete menus will be available in the subsequent authorization policies row that you create.

Step 4 Click the drop-down list to view the predefined settings to enforce policies.

You can choose one of the following options to enforce the policies based on the compliance status.

The following options are available:

- Enabled—The standard authorization policies enforce policies based on the compliance status of the endpoints
- Disabled—The standard authorization policies do not enforce policies
- Monitor Only—The standard authorization policies monitor enforced policies on endpoints

Step 5 Enter the rule (standard authorization policy) name.

To choose an identity group, complete the following steps:

Step 6 Click the plus [+] sign to expand the identity groups anchored overlay.

The identity groups anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

a. Click the quick picker (down arrow) icon.

The Identity Groups object selector appears.

b. Choose an identity group in the Identity Groups object selector.

c. Click the plus [+] sign to associate more than one identity group.

To choose a condition, complete the following steps:

Step 7 Click the plus [+] sign to expand the conditions anchored overlay.

The conditions anchored overlay appears with the following options: Select Existing Condition from Library and Create new Condition (Advance Option). Click the minus [-] sign, or click outside the anchored overlay to close it.

To choose an attribute, complete the following steps:

Step 8 Choose **Select Existing Condition from Library** or **Create new Condition (Advance Option)**.

For information on selecting an existing condition, see the To select an existing condition from the library, complete the following steps:, page 20-161.

For information on creating a new condition, see the To create a new condition, complete the following steps:, page 20-161.

To choose a permission (standard authorization profile), complete the following steps:

Step 9 Click the plus [+] sign to expand the authzprofile(s) anchored overlay.

The authzprofile(s) anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

a. Click the quick picker (down arrow) icon.

The Profiles object selector appears. From the Profiles object selector, click the navigation arrow to view the authorization profiles in each category.

The Profiles object selector displays the following authorization profile categories:

- Inline Posture Node
- Security Group
- Standard

b. Choose **Standard**.

c. Click the navigation arrow to view the authorization profiles in the standard authorization profile category.

d. Choose an authorization profile from the standard category.

e. Click the plus [+] sign to associate more than one authorization profile from the standard category

Step 10 Click **Done** to create a new standard authorization policy in read-only mode.

The standard authorization policy appears in the Authorization Policy page. Click **Edit** to switch the authorization policy row to edit mode.

Step 11 Click **Save**.

To select an existing condition from the library, complete the following steps:

Step 1 Click **Select Existing Condition from Library**.

The conditions anchored overlay appears.

Step 2 Click the quick picker (down arrow) icon.

The Dictionaries object selector appears that lists the available dictionaries.

Step 3 From the Dictionaries object selector, click the navigation arrow to view the available dictionary conditions.

The following options appear:

- Simple Conditions
- Compound Conditions
- Time and Date Conditions

Step 4 Choose a condition.

Step 5 Click the **Action** icon to add a dictionary attribute and its value, add a condition from the library, or delete existing conditions or dictionary attributes.

Step 6 Choose an **AND** operator, or an **OR** operator from the drop-down list.

To create a new condition, complete the following steps:

You can use the **Save** icon to add all the new conditions to the policy elements library.

Step 1 **Create new Condition (Advance Option)**

The conditions anchored overlay appears.

Step 2 Click the quick picker (down arrow) icon.

The Dictionaries object selector appears that lists the available dictionaries.

Step 3 From the Dictionaries object selector, click the navigation arrow to view the available dictionary attributes.

The dictionary attributes appear for the dictionary.

Step 4 Choose the dictionary attribute, an operator and a value for the attribute.

For the posture status, you can use the Session:PostureStatus attribute, an operator, and the values such as Unknown, Compliant, and Noncompliant.

Step 5 Click **Save** to save all the conditions to the policy elements library.

Step 6 Click the **Action** icon.

You can do the following:

- Add Attribute/Value—Add a dictionary attribute and its value
- Add Condition from Library—Add a condition from the library that allows you to choose a condition that is already saved
- Duplicate—Duplicate a condition
- Add Condition to Library—Add a condition to the library
- Delete—Delete existing conditions or dictionary attributes

Step 7 Choose an **AND** operator, or an **OR** operator from the drop-down list.

You can create a copy of a standard authorization policy in the Authorization Policy page above or below the selected policy row.

To duplicate a standard authorization policy, complete the following steps:

Step 1 Click the arrow next to Edit to create a copy (duplicate) of a standard authorization policy.

Step 2 Click **Duplicate Above** to duplicate a standard authorization policy above the selected policy row or click **Duplicate Below** to duplicate a standard authorization policy below the selected policy row.

Step 3 Click **Done** to create a copy of the standard authorization policy in read-only mode.

Step 4 Click **Save**.

You can also delete a standard authorization policy in the Authorization Policy page.

To delete a standard authorization policy, complete the following steps:

Step 1 Click the arrow next Edit to delete a standard authorization policy.

Step 2 Click **Delete** in the confirmation dialog.

Custom Permissions for Posture

A custom permission is an authorization profile (standard authorization profile) that you define in the Cisco ISE appliance. The 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 and then associate them to three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

This section describes the standard authorization profiles that you can define in the Cisco ISE appliance.

Prerequisites:

Before you begin, you should have an understanding of the states for a posture.

Review the following states:

- Unknown Profile
- Compliant Profile
- Noncompliant Profile

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 to Cisco ISE by a NAC Agent. For an endpoint to have privileged network access on your network, the compliant status of the endpoint should be compliant.

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 the endpoint fails to meet all the mandatory requirements that are defined in the matching posture policy 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 to be compliant.