Configuring Client Provisioning

This chapter describes client-provisioning functions in Cisco ISE that allows you to download client-provisioning resources and configure agent profiles for Windows and MAC OS X clients, and native supplicant profiles for your own personal devices.

Client Provisioning Resource Types

Client-provisioning resource policies enable users to download and install resources on client devices. These resources must be installed on Cisco ISE before users can access them and include:

- Persistent and temporal agents:
  - Windows and Mac OS X Cisco Network Admission Control (NAC) Agents

  - Cisco NAC Web Agent
- Native supplicant profiles
- Agent profiles
- Native supplicant provisioning/installation wizards
- Agent compliance modules
- Agent customization packages

Related Topics

- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4
- Configuring Client Provisioning Resource Policies, page 23-45
- *Posture Services on the Cisco ISE Configuration Guide*

Enabling and Disabling Client Provisioning

Before You Begin

To ensure that you are able to access the appropriate remote location from which you can download client-provisioning resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network.

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

Step 2 From the Enable Provisioning drop-down list, choose **Enable** or **Disable**.

Step 3 Click **Save**.

When you choose to disable this function of Cisco ISE, users who attempt to access the network will receive a warning message indicating that they are not able to download client-provisioning resources.

What To Do Next

Set up system-wide client-provisioning functions according to the guidelines in the following topics:

- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4
- Configuring Client Provisioning Resource Policies, page 23-45

Related Topics

- Specifying Proxy Settings in Cisco ISE, page 6-3
- Cannot Download Remote Client Provisioning Resources, page G-14

Adding Client Provisioning Resources from Remote Sources

You can add client-provisioning resources from a remote source like Cisco.com. Depending on the resources that you select and available network bandwidth, Cisco ISE can take a few seconds or even a few minutes to download the new items and display them in the list of available client-provisioning resources.

Before You Begin

Ensure that you are able to access the appropriate remote location to download client-provisioning resources to Cisco ISE, by verifying that the proxy settings for your network are correctly configured.

Step 1 **Choose Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > Agent resources from Cisco site**.

Step 3 Select one or more required resources from the list available in the Downloaded Remote Resources dialog box.

Step 4 Click **Save**.

What To Do Next

After you have successfully added client-provisioning resources to Cisco ISE, you can begin to configure client-provisioning resource policies.

Related Topics

- Specifying Proxy Settings in Cisco ISE, page 6-3
- Client Provisioning Resource Types, page 23-1
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4
- Creating an Agent Customization File, page 23-20
- Configuring Client Provisioning Resource Policies, page 23-45
- Cannot Download Remote Client Provisioning Resources, page G-14

Adding Client Provisioning Resources from a Local Machine

You can add existing client-provisioning resources from a local machine (for example, files that you may have already downloaded from Cisco.com to your laptop).

Before You Begin

Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources (older versions of the Cisco NAC Agent, for example) will likely cause serious issues for client access. For details, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.2*.

If you are downloading the resource files manually from the Cisco.com, refer to “Cisco ISE Offline Updates” section in the *Release Notes for the Cisco Identity Services Engine, Release 1.2*.

Step 1 **Choose Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > Add resource from local disk**.

Step 3 Click **Browse** and navigate to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

Step 4 Highlight the resource file in the search window and click **Save**.

What To Do Next

After you have successfully added client-provisioning resources to Cisco ISE, you can begin to configure client-provisioning resource policies.

Related Topics

- Specifying Proxy Settings in Cisco ISE, page 6-3
- Client Provisioning Resource Types, page 23-1
- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4
- Creating an Agent Customization File, page 23-20
- Agent Profile Configuration Guidelines, page 23-21
- Configuring Client Provisioning Resource Policies, page 23-45

Downloading Client Provisioning Resources Automatically

This function automatically uploads *all* available software from Cisco, many items of which may not be pertinent to your deployment.

Before You Begin

To ensure that you are able to access the appropriate remote location from which you can download client-provisioning resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network. If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the default URL, try also pointing your Cisco ISE to https://www.perfigo.com/ise/provisioning-update.xml.

The default URL for downloading client-provisioning resources is https://www.cisco.com/web/secure/pmbu/provisioning-update.xml.

Cisco recommends manually uploading resources whenever possible rather than opting to upload them automatically.

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

Step 2 From the **Enable Automatic Download** drop-down list, choose **Enable**.

Step 3 Specify the URL where Cisco ISE searches for system updates in the Update Feed URL text box.

Step 4 Click **Save**.

What To Do Next

Set up system-wide client-provisioning functions according to the guidelines in the following topics:

- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4
- Configuring Client Provisioning Resource Policies, page 23-45

Related Topics

- Specifying Proxy Settings in Cisco ISE, page 6-3
- Cannot Download Remote Client Provisioning Resources, page G-14

Client Login Session Criteria

Cisco Identity Services Engine (ISE) looks at various elements when classifying the type of login session through which users access the internal network, including:

- Client machine operating system and version
- Client machine browser type and version
- Group to which the user belongs
- Condition evaluation results (based on applied dictionary attributes)

After Cisco ISE classifies a client machine, it uses client-provisioning resource policies to ensure that the client machine is 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, if necessary.

Cisco ISE Agents

Agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the Cisco NAC Agent or Mac OS X Agent) and remain on the client machine after installation, even when the client is not logged into the network, or Agents can be temporal (like the Cisco NAC Web Agent), removing themselves from the client machine after the login session has terminated. In either case, the Agent helps the user log in to the network, receive the appropriate access profile, and even perform posture assessment on the client machine to ensure it complies with network security guidelines before accessing the core of the network.

Note Currently Cisco NAC Agent and Cisco NAC Web Agent support Client Provisioning Portal and Native Supplicant Provisioning. Cisco NAC Web Agent supports Central Web Authentication flow (CWA), but Cisco NAC Agent does not support CWA.

Cisco NAC Agent for Windows Clients

The Cisco NAC Agent provides the posture assessment and remediation for client machines.

Users can download and install the Cisco NAC Agent (read-only client software), which can check the host registry, processes, applications, and services. The Cisco NAC Agent can be used to perform Windows updates or antivirus and antispyware definition updates, launch qualified remediation programs, distribute files uploaded to the Cisco ISE server, distribute website links to websites for users to download files to fix their system, or simply distribute information and instructions.

Cisco strongly recommends that you ensure that the latest Windows hotfixes and patches are installed on Windows XP clients so that the Cisco NAC Agent can establish a secure and encrypted communication with Cisco ISE (via SSL over TCP).

Uninstalling Cisco NAC Agent for Windows Clients

The NAC Agent installs to **C:\Program Files\Cisco\Cisco NAC Agent** on the Windows client. You can uninstall the Agent in the following ways:

- By double-clicking the **Uninstall Cisco NAC Agent** desktop icon
- By going to **Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Cisco NAC Agent**
- By going to **Start Menu > Control Panel > Add or Remove Programs > Cisco NAC Agent**

To uninstall Cisco NAC Agent in a Windows 8 client, execute the following:

Step 1 Switch to Metro Mode.

Step 2 Right-Click **Cisco NAC Agent** tile.

Step 3 Select **Un-Install** from the options available at the bottom of the screen.

Step 4 The system automatically switches to Desktop mode and opens **Add/Remove** control panel.

Step 5 In the **Add/Remove** control panel, perform one of the following:

- Double Click **Cisco NAC Agent**.
- Select **Cisco NAC Agent** and click **Uninstall**.
- Right Click **Cisco NAC Agent** and select **Uninstall**.

Related Topics

- *Cisco Identity Services Engine Network Component Compatibility, Release 1.2*.

Windows 8 Metro and Metro App Support —Toast Notifications

The **Enable Toast Notification** option is available on the Cisco NAC Agent Tray Icon, only for clients using Windows 8 as Operating System. You can enable this option to send relevant notifications to the user.

In Cisco NAC Agent scenarios where the user does not get network access, like “Remediation Failed” or “Network Access expired”, the Agent displays the following toast notification:

Network not available, Click “OK” to continue

To get more details, you can select the toast and you will be redirected to Desktop mode and the NAC agent dialog is displayed.

Toast Notification is displayed for all positive recommended actions that the user needs to perform to gain network access. The following are some examples:

- For Network Acceptance policy, toast will be displayed as: “Click Accept to gain network access”
- For Agent/Compliance Module Upgrade, toast will be displayed as: “Click OK to Upgrade/Update”
- In the “user logged out” event, when “Auto Close” option for Logoff is not enabled in CAM, toast notification is provided. This toast enables the users to know that they have been logged out and that they need to login again to get network access.

Cisco NAC Agent for Macintosh Clients

The Mac OS X Agent provides the posture assessment and remediation for Macintosh client machines.

Users can download and install the Mac OS X Agent (read-only client software), which can check antivirus and antispyware definition updates.

After users log in to the Mac OS X Agent, the agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client, the user is allowed network access. If requirements are not met, the agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept restricted network access while the user tries to remediate the client system.

Related Topics

- *Cisco Identity Services Engine Network Component Compatibility, Release 1.2*.

Uninstalling Cisco NAC Agent for Macintosh Clients

You can uninstall the NAC Agent for Mac OS X clients by running the uninstall script as follows:

Step 1 Open the navigator pane and navigate to <*local drive ID*> **> Applications**.

Step 2 Highlight and right-click the **CCAAgent** icon to bring up the selection menu.

Step 3 Choose **Show Package Contents** and double-click **NacUninstall.**

Step 4 This will uninstall the Agent on Mac OS X.

Cisco NAC Web Agent

The Cisco NAC Web Agent provides temporal posture assessment for client machines.

Users can launch the Cisco NAC Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet. The Web Agent is available only for Windows clients and not for Mac OSX clients.

After users log in to the Cisco NAC Web Agent, the Web Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client machine, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each requirement that is not satisfied. The dialog

provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

Note ActiveX is supported only on the 32-bit versions of Internet Explorer. You cannot install ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Related Topics

- *Cisco Identity Services Engine Network Component Compatibility, Release 1.2*.

Custom nac_login.xml File Template

This is one of the files that is required in your Agent customization package, which allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties screen, to suit your specific Windows client network access requirements.

Use the following template to construct an appropriate “nac_login.xml” file.

The following example shows a customized file.

```
<tr class="nacLoginMiddleSectionContainerInput">
 <td colspan="2">
 <fieldset width="100%" id="nacLoginCustomAlert"
style="display:block" class="nacLoginAlertBox">
 <table width="100%">
 <tr>
 <td id="nacLoginCustomAlert.img" valign="top" width="32px">
 <img src="./cues_icons/Status_warning_icon.png" align="absmiddle"
onload="cuesFixPNG(null,this)"></img>
 </td>
 <td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
 <cues:localize key="login.customalert"/>
 </td>
 </tr>
 </table>
 </fieldset>
 </td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
 <td>
 <cues:localize key="cd.nbsp"/>
 </td>
 <td class="cuesLoginField">
 <nobr>
 <input type="checkbox" alt="" title="" name="rememberme"
 id="rememberme" checked="true"/>
 <cues:localize key="login.remember_me"/>
 </nobr>
 </td>
</tr>
```

Related Topics

- Using a Custom Corporate/Company Logo, page 23-9
- Custom nacStrings_xx.xml File Template, page 23-9
- UpdateFeed.xml Descriptor File Template, page 23-19

- UpdateFeed.xml Descriptor File Template, page 23-19
- Creating an Agent Customization File, page 23-20
- Agent XML File Installation Directories, page 23-20

Using a Custom Corporate/Company Logo

You can replace the Cisco logo that appears in all the Cisco NAC Agent screens with your corporate/company logo.

Before You Begin

This is one of the files that is required in your Agent screen customization package, which allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties screen, to suit your specific Windows client network access requirements.

Be sure the image is a .gif file, not exceeding 67 x 40 pixels. Be sure to name the image “nac_logo.gif.”

Related Topics

- Custom nac_login.xml File Template, page 23-8
- Custom nacStrings_xx.xml File Template, page 23-9
- UpdateFeed.xml Descriptor File Template, page 23-19
- UpdateFeed.xml Descriptor File Template, page 23-19
- Creating an Agent Customization File, page 23-20
- Agent XML File Installation Directories, page 23-20

Custom nacStrings_*xx*.xml File Template

This is one of the files that is required in your Agent screen customization package, allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties screen, to suit your specific Windows client network access requirements.

Use the following template to construct a one or more nacStrings_xx.xml files, where the *xx* is a two-character identifier for the specific language.

The following example shows a customized nacStrings_xx.xml file.

```
<cueslookup:appstrings xmlns:cueslookup="http://www.cisco.com/cues/lookup">
  <cueslookup:name key="nac.brand.legal_name">Cisco Systems, Inc.</cueslookup:name>
  <cueslookup:name key="nac.brand.full_name">Cisco Systems</cueslookup:name>
  <cueslookup:name key="nac.brand.short_name">Cisco</cueslookup:name>
  <cueslookup:name key="nac.brand.abbreviation">Cisco</cueslookup:name>
  <cueslookup:name key="nac.copyright">Copyright </cueslookup:name>
  <cueslookup:name key="nac.copyright.period">2009-2013</cueslookup:name>
  <cueslookup:name key="nac.copyright.arr">All Rights Reserved</cueslookup:name>
<cueslookup:name key="updateagent.rqst">NAC Agent %1 is available.%br% Do you want to
install this update now?</cueslookup:name>
<cueslookup:name key="updateagent.rqst.retry">Unable to update NAC Agent. Please try
again.</cueslookup:name>
<cueslookup:name key="downloadagent.report">Downloading the update of NAC
Agent.</cueslookup:name>
<cueslookup:name key="downloadagent.packagename.label">Package Name</cueslookup:name>
<cueslookup:name key="downloadagent.completed.label">Completed</cueslookup:name>
<cueslookup:name key="downloadagent.completed.value">%1 of %2 bytes</cueslookup:name>
```

```
<cueslookup:name key="downloadagent.speed.label">Speed</cueslookup:name>
<cueslookup:name key="downloadagent.speed.value">%1 bytes/sec</cueslookup:name>
<cueslookup:name key="updateopswat.rqst">NAC Agent Posture component version %1 is
available.%br% Do you want to install this update now?</cueslookup:name>
<cueslookup:name key="updateopswat.rqst.retry">Unable to update NAC Agent Posture
component. Please try again.</cueslookup:name>
<cueslookup:name key="downloadopswat.report">Downloading the update of NAC Agnet Posture
component.</cueslookup:name>
 <cueslookup:name key="login.productname">Education First Compliance
Check</cueslookup:name>
<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.opswatversion">Posture Component Version</cueslookup:name>
<cueslookup:name key="login.username">Enter your username</cueslookup:name>
<cueslookup:name key="login.password">Enter your PIN</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
 <cueslookup:name key="login.customalert">Custom EF package version 2.1.1.1 with EF
Logo</cueslookup:name>
  <cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
  <cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
  <cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
 <cueslookup:name key="menu_devtools">Dev Tools</cueslookup:name>
<cueslookup:name key="c.sso.ad">Performing Windows Domain automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.generic">Unknown authentication type</cueslookup:name>
<cueslookup:name key="c.sso.macauth">Performing device filter automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.vpn">Performing automatic login into NAC environment for
remote user</cueslookup:name>
<cueslookup:name key="c.title.status.authenticating">Authenticating User</cueslookup:name>
<cueslookup:name key="c.title.status.answeringchallenge">Sending
Response</cueslookup:name>
<cueslookup:name key="c.title.status.checking">Checking Requirements</cueslookup:name>
<cueslookup:name key="c.title.status.checkcomplete">System Check
Complete</cueslookup:name>
<cueslookup:name key="c.title.status.loggedin">NAC Process Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netaccess.none">NAC Process
Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netpolicy">Network Usage Policy</cueslookup:name>
<cueslookup:name key="c.title.status.properties">Agent Properties &#x0026;
Information</cueslookup:name>
<cueslookup:name key="c.title.status.remediating">Remediating System</cueslookup:name>
<cueslookup:name key="c.title.status.session.expired">Session has
Expired</cueslookup:name>
<cueslookup:name key="c.title.status.update.available">Update Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.downloading">Downloading
Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.available">Update Posture
Component</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.downloading">Downloading Posture
Component</cueslookup:name>
 <cueslookup:name key="scanning">Checking</cueslookup:name>
<!-- <cueslookup:name key="scanningitemcomplete">Finished Checking</cueslookup:name> -->
<cueslookup:name key="ph.about">About</cueslookup:name>
<cueslookup:name key="ph.cancel">Cancel</cueslookup:name>
<!-- <cueslookup:name key="ph.details">Details</cueslookup:name> -->
  <cueslookup:name key="ph.logout">Logout</cueslookup:name>
<cueslookup:name key="title_remediating">Remediating System</cueslookup:name>
<cueslookup:name key="title_check_conplete">System Check Complete</cueslookup:name>
<cueslookup:name key="title_full_access_granted">Logged In</cueslookup:name>
<cueslookup:name key="title_access_denied">Network Access Denied</cueslookup:name>
<cueslookup:name key="tempNetAccess">Temporary Network Access</cueslookup:name>
```

```
<cueslookup:name key="announcePleaseBePatient">Please be patient while your system is
checked against the network security policy
</cueslookup:name>
<cueslookup:name key="bttn.accept">Accept</cueslookup:name>
<cueslookup:name key="bttn.apply">Apply</cueslookup:name>
<cueslookup:name key="bttn.cancel">Cancel</cueslookup:name>
<cueslookup:name key="bttn.continue">Update Later</cueslookup:name>
<cueslookup:name key="bttn.close">Close</cueslookup:name>
<cueslookup:name key="bttn.detailshide">Hide Compliance</cueslookup:name>
<cueslookup:name key="bttn.detailsshow">Show Compliance</cueslookup:name>
<cueslookup:name key="bttn.download">Download</cueslookup:name>
<cueslookup:name key="bttn.guestAccess">Guest Access</cueslookup:name>
<cueslookup:name key="bttn.go2link">Go To Link</cueslookup:name>
<cueslookup:name key="bttn.launch">Launch</cueslookup:name>
<cueslookup:name key="bttn.login">Log In</cueslookup:name>
<cueslookup:name key="bttn.next">Re-Scan</cueslookup:name>
<cueslookup:name key="bttn.ok">OK</cueslookup:name>
<cueslookup:name key="bttn.propertieshide">Hide Properties</cueslookup:name>
<cueslookup:name key="bttn.reject">Reject</cueslookup:name>
<cueslookup:name key="bttn.remediate">Repair</cueslookup:name>
<cueslookup:name key="bttn.rescan">Rescan</cueslookup:name>
<cueslookup:name key="bttn.reset">Reset</cueslookup:name>
<cueslookup:name key="bttn.restrictedNet">Get Restricted NET access This one comes down
from the network</cueslookup:name>
<cueslookup:name key="bttn.savereport">Save Report</cueslookup:name>
<cueslookup:name key="bttn.skip">Skip</cueslookup:name>
<cueslookup:name key="bttn.skipao">Skip All Optional</cueslookup:name>
<cueslookup:name key="bttn.submit">Submit</cueslookup:name>
<cueslookup:name key="bttn.update">Update</cueslookup:name>
 <cueslookup:name key="cd.days">
    days
  </cueslookup:name>
  <cueslookup:name key="cd.nbsp">
     
  </cueslookup:name>
  <cueslookup:name key="cd.tempNetAccess.counting">
    There is approximately %1 left until your temporary network access expires
  </cueslookup:name>
  <cueslookup:name key="cd.tempNetAccess.expired">
    Your Temporary Network Access has Expired!
  </cueslookup:name>
  <cueslookup:name key="cd.tempNetAccessShort.counting">
    %1 left
  </cueslookup:name>
  <cueslookup:name key="cd.tempNetAccessShort.expired">
    Expired!
  </cueslookup:name>
  <cueslookup:name key="cd.window.counting">
    This window will close in  %1 secs
  </cueslookup:name>
  <cueslookup:name key="dp.status.fullNetAccess">
   Full Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">
   Your device conforms with all the security policies for this protected
   network
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">
  Only optional requirements are failing.
  It is recommended that you update your system at
  your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">
   Refreshing IP address. Please Wait ...
```

```
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">
  Refreshing IP address succeeded.
</cueslookup:name>
  <cueslookup:name key="dp.status.vlanchange.progress.verbose">
   Connecting to protected Network. Please Wait ...
  </cueslookup:name>
  <cueslookup:name key="dp.status.guestNetAccess">
   Guest Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">
   Network Access Denied
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">
  There is at least one mandatory requirement failing.
  You are required to update your system before
  you can access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">
  Network Usage Terms and Conditions are rejected. You will not be
  allowed to access the network.
</cueslookup:name>
  <cueslookup:name key="dp.status.RestrictedNetAccess">
    Restricted Network Access granted.
  </cueslookup:name>
  <cueslookup:name key="dp.status.RestrictedNetAccess.verbose">
    You have been granted restricted network access because your device
    did not conform with all the security policies for this protected
    network and you have opted to defer updating your system. It is recommended
    that you update your system at your earliest convenience.
  </cueslookup:name>
   <cueslookup:name key="dp.status.temporaryNetAccess">
   Temporary Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">
   Please be patient while your system is checked against the network security policy.
</cueslookup:name>
  <cueslookup:name key="dp.status.pra.mandatoryfailure">
    Performing Re-assessment
  </cueslookup:name>
  <cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">
    There is at least one mandatory requirement failing.
    You are required to update your system otherwise
    your network access will be restricted.
  </cueslookup:name>
  <cueslookup:name key="dp.status.pra.optionalfailure">
    Performing Re-assessment
  </cueslookup:name>
  <cueslookup:name key="dp.status.pra.optionalfailure.verbose">
    Only optional requirements are failing.
    It is recommended that you update your system at
    your earliest convenience.
  </cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">
   Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">
   Temporary Access to the network has expired.
</cueslookup:name>
  <cueslookup:name key="dp.status.Unauthenticated">
    Logged out
  </cueslookup:name>
  <cueslookup:name key="dp.status.Unauthenticated.verbose">
     
```

```
  </cueslookup:name>
 <cueslookup:name key="ia.status.checkcomplete">
    Finished Checking Requirements
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress">
    Please be patient while we determine if your system is compliant with the security
policy
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress.01">
    Checking %1 out of %2
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicy">
    Access to the network requires that you view and accept the following
    Network Usage Policy
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicylinktxt">
    Network Usage Policy Terms and Conditions
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.inprogress">
    Remediating
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.start">
    Please Remediate
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.checkinprogress">
    Checking for compliance with Requirement
</cueslookup:name>
<cueslookup:name key="ia.table.name">
   Name
</cueslookup:name>
<cueslookup:name key="ia.table.location">
    Location
</cueslookup:name>
<cueslookup:name key="ia.table.software">
    Software
</cueslookup:name>
<cueslookup:name key="ia.table.software.programs">
    program(s)
</cueslookup:name>
<cueslookup:name key="ia.table.update">
    Update
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.nochange">
    Do not change current setting
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforedownload">
    Notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforeinstall">
    Notify before install
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.scheduledinstallation">
    Download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforedownload">
    Change to notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforeinstall">
    Change to notify before installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcescheduledinstall">
    Change to download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.description">
```

```
    Description
</cueslookup:name>
<cueslookup:name key="scs.table.title">
    Security Compliance Summary
</cueslookup:name>
<cueslookup:name key="scs.table.header1.scan_rslt">
    Scan Result
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_name">
    Requirement Name
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_details">
    Requirement Description - Remediation Suggestion
</cueslookup:name>
  <cueslookup:name key="scs.table.data.mandatory">
    Mandatory
  </cueslookup:name>
  <cueslookup:name key="scs.table.data.optional">
    Optional
  </cueslookup:name>
  <cueslookup:name key="scs.table.data.pass">
    Passed
  </cueslookup:name>
 <cueslookup:name key="ia.rem_inst_optional_download">
Please download and install the optional software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_download">
Please download and install the required software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_launch">
Please launch the optional remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_launch">
Please launch the required remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_av">
Please update the virus definition file of the specified antivirus software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_av">
Please update the virus definition file of the specified antivirus software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_win_update">
Please download and install the optional windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_win_update">
Please download and install the required windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_prog">
Launching Remediation Program(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_url">
Launching Remediation URL ...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_av">
```

```
Updating Virus Definition ...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_as">
Updating Spyware Definition ...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_win_update">
Launching Windows auto Update(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_launch_downloaded_file">
  Downloaded at %1. %br% Please open this folder &#x0026; double-click executable file to
install the required software.
</cueslookup:name>
   <cueslookup:name key="discoveryhost.label">
    Discovery Host
  </cueslookup:name>
   <cueslookup:name key="properties.table.title">
    List of Antivirus &#x0026; Anti-Spyware Products Detected by the Agent
  </cueslookup:name>
  <cueslookup:name key="properties.table.header1.index">
    No.
  </cueslookup:name>
  <cueslookup:name key="properties.table.header1.description">
    Description
  </cueslookup:name>
  <cueslookup:name key="properties.table.header1.value">
    Value
  </cueslookup:name>
  <cueslookup:name key="properties.table.data.product_type">
    Product Type
  </cueslookup:name>
  <cueslookup:name key="properties.table.data.product_name">
    Product Name
  </cueslookup:name>
  <cueslookup:name key="properties.table.data.product_version">
    Product Version
  </cueslookup:name>
  <cueslookup:name key="properties.table.data.def_version">
    Definition Version
  </cueslookup:name>
  <cueslookup:name key="properties.table.data.def_date">
    Definition Date
  </cueslookup:name>
 <cueslookup:name key="reboot.mandatory.001">
    Mandatory System Reboot Required
  </cueslookup:name>
  <cueslookup:name key="reboot.optional.001">
    You need to reboot your system in order for the changes to take effect.
  </cueslookup:name>
 <cueslookup:name key="rem.error.001">
    Unable to remediate particular requirement
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_access_denied">
    The remediation you are attempting is reporting an access denied error. This is
usually due to a privilege issue. Please contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_buffer_too_small">
    The remediation you are attempting has failed with an internal error. Please contact
your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_elevation_required">
    The remediation you are attempting requires elevation. Please contact your system
administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_failed">
```

```
    The remediation you are attempting had a failure. If the problem persists contact your
system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_internal_error">
    The remediation you are attempting has reported an internal error.  If this problem
persists please contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_not_implemented">
    The remediation you are attempting is not implemented for this product. Please contact
your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_not_supported">
    The remediation you are attempting is not supported for this product. Please contact
your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_update_faile">
    The AV/AS update has failed.  Please try again and if this message continues to
display contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_update_failed_due_to_network">
    The AV/AS update failed due to a networking issue. Please try again and if this
message continues to display contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.av_timeout">
    The remediation you are attempting has timed out waiting for the operation to finish.
If this continues please contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.file_dist_size_error">
    The size of the downloaded file does not match the package! Please discard downloaded
file and check with your administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.file_is_not_signed">
    The file that has been requested was not digitally signed.  Please try again and if
this message continues to display contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.file_save_location_error">
    The location for the file to be saved to can not be written.  Please choose a
different location.
  </cueslookup:name>
  <cueslookup:name key="rem.error.http_file_not_found">
    The requested file is not found.  Please try again and if this problem persists,
contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.launch_file_not_found">
    The file that has been requested could not be launched either because it could not be
found or there was a problem launching it.  Please contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.malformed_URL">
    The file that is trying to be downloaded has an incorrect URL. Please contact your
system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.network_error">
    There has been a network error, please try the remediation again.  If this message
continues to be seen contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.update_fail_for_non_admin">
    The remediation you are trying to do can not be accomplished at your user level.
Please contact your system administrator.
  </cueslookup:name>
  <cueslookup:name key="rem.error.wsus_search_failure">
    The WSUS search failed.  This is probably due to a network issue.  Please try again
and if this message continues to display contact your system administrator.
  </cueslookup:name>
 <cueslookup:name key="server.error.generic">
```

```
    Agent encountered problems logging user
  </cueslookup:name>
  <cueslookup:name key="server.error.255">
    Network Error: NAC Server could not establish a secure connection to NAC Manager.
    This could be due to one or more of the following reasons:
    1) NAC Manager certificate has expired or
    2) NAC Manager certificate cannot be trusted or
    3) NAC Manager cannot be reached or
    4) NAC Manager is not responding
    Please report this to your network administrator.
  </cueslookup:name>
  <cueslookup:name key="server.error.5000">
    Invalid provider name
  </cueslookup:name>
  <cueslookup:name key="server.error.5001">
    Failed to add user to online list
  </cueslookup:name>
  <cueslookup:name key="server.error.5002">
    Server communication error
  </cueslookup:name>
  <cueslookup:name key="server.error.5003">
    Invalid username or password
  </cueslookup:name>
  <cueslookup:name key="server.error.5004">
    Unknown user
  </cueslookup:name>
  <cueslookup:name key="server.error.5005">
    Account expired
  </cueslookup:name>
  <cueslookup:name key="server.error.5006">
    Account currently disabled
  </cueslookup:name>
  <cueslookup:name key="server.error.5007">
    Exceed quota limit
  </cueslookup:name>
  <cueslookup:name key="server.error.5008">
    Insufficient Clean Access packages installed
  </cueslookup:name>
  <cueslookup:name key="server.error.5009">
    Access to network is blocked by the administrator
  </cueslookup:name>
  <cueslookup:name key="server.error.5010">
    Vulnerabilities not fixed
  </cueslookup:name>
  <cueslookup:name key="server.error.5011">
    This client version is old and not compatible. Please login from web browser to see
the download link for the new version.
  </cueslookup:name>
  <cueslookup:name key="server.error.5012">
    Network policy is not accepted
  </cueslookup:name>
  <cueslookup:name key="server.error.5013">
    Invalid switch configuration
  </cueslookup:name>
  <cueslookup:name key="server.error.5014">
    Too many users using this account
  </cueslookup:name>
  <cueslookup:name key="server.error.5015">
    Invalid session
  </cueslookup:name>
  <cueslookup:name key="server.error.5016">
    Null session
  </cueslookup:name>
  <cueslookup:name key="server.error.5017">
```

```
    Invalid user role
  </cueslookup:name>
  <cueslookup:name key="server.error.5018">
    Invalid login page
  </cueslookup:name>
  <cueslookup:name key="server.error.5019">
    Encoding failure
  </cueslookup:name>
  <cueslookup:name key="server.error.5020">
    A security enhancement is required for your Agent. Please upgrade your Agent or
contact your network administrator.
  </cueslookup:name>
  <cueslookup:name key="server.error.5021">
    Can not find server reference
  </cueslookup:name>
  <cueslookup:name key="server.error.5022">
    User role currently disabled
  </cueslookup:name>
  <cueslookup:name key="server.error.5023">
    Authentication server is not reachable
  </cueslookup:name>
  <cueslookup:name key="server.error.5024">
    Agent user operating system is not supported
  </cueslookup:name>
  <cueslookup:name key="server.error.generic_emergency">
    The Agent has encountered an unexpected error and is restarting.
  </cueslookup:name>
  <cueslookup:name key="server.error.http_error">
    Clean Access Server is not available on the network.
  </cueslookup:name>
  <cueslookup:name key="server.error.nw_interface_chg">
    Authentication interrupted due to network status change. Press OK to retry.
  </cueslookup:name>
  <cueslookup:name key="server.error.svr_misconfigured">
    Clean Access Server is not properly configured.
  </cueslookup:name>
  <cueslookup:name key="server.clarification.generic_emergency">
    Please contact your administrator if the problem persists.
  </cueslookup:name>
  <cueslookup:name key="announce.savingreport">
    Saving Report
  </cueslookup:name>
  <cueslookup:name key="announce.savingreport.failed">
    Unable to save report
  </cueslookup:name>
  <cueslookup:name key="announce.cancelremediationack">
Clicking Cancel may change your network connectivity and interrupt download or required
updates.<p> Do you want to continue?</p>
  </cueslookup:name>
  <cueslookup:name key="announce.dismiss.default">
    Dismiss to continue
  </cueslookup:name>
 <cueslookup:name key="announce.logoutconfirm">
    Successfully logged out from the network!
  </cueslookup:name>
</cueslookup:appstrings>
```

Note There is no limit to the number of characters you can use for the customized text. However, Cisco recommends restricting the length so that these fields do not take up too much space in the resulting customized login screen as it appears on the client.

Related Topics

- Custom nac_login.xml File Template, page 23-8
- Using a Custom Corporate/Company Logo, page 23-9
- UpdateFeed.xml Descriptor File Template, page 23-19
- Creating an Agent Customization File, page 23-20
- Agent XML File Installation Directories, page 23-20

UpdateFeed.xml Descriptor File Template

This is one of the files that is required in your Agent screen customization package, allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties screen, to suit your specific Windows client network access requirements.

Before you can complete your Agent screen customization package, you must construct a suitable **updateFeed.xml** XML descriptor file. Use the following example as a template to set up the updateFeed.xml file required for your customization package.

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:update="http://www.cisco.com/cpm/update/1.0">
 <title>Provisioning Update</title>
 <updated>2011-12-21T12:00:00Z</updated>
<id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
 <author>
 <name>Cisco Support</name>
 <email>support@cisco.com</email>
 </author>
 <!-- Custom Branding -->
 <entry>
<id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/7</id>
 <title>Agent Customization Package</title>
 <updated>2010-06-07T12:00:00Z</updated>
 <summary>This is EF Agent Customization Package 1.1.1.7</summary>
 <link rel="enclosure" type="application/zip" href="brand-win.zip" length="18884" />
 <update:type>AgentCustomizationPackage</update:type>
 <update:version>1.1.1.7</update:version>
 <update:os>WINDOWS_ALL</update:os>
 </entry>
</feed>
```

Note the following points while creating the updateFeed.xml descriptor file:

- <update:os>—You must always set this attribute to “WINDOWS_ALL” to include all the Windows OS versions that are supported by Cisco NAC Agent. See Support Information for Cisco NAC Appliance Agents for the list of Windows OS versions that are supported by Cisco NAC Agent.
- <update:version>—This refers to the Agent Customization Package version that you want to upgrade to. This value should be four digit <n.n.n.n> and should be greater than the package version that is currently installed.
- <id>—This id can be anything, but should be unique for each Agent Customization Package.

Related Topics

- Custom nac_login.xml File Template, page 23-8
- Using a Custom Corporate/Company Logo, page 23-9

- Custom nacStrings_xx.xml File Template, page 23-9
- Creating an Agent Customization File, page 23-20
- Agent XML File Installation Directories, page 23-20

Creating an Agent Customization File

An agent customization file allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent screen dialog to suit your specific Windows client network access requirements.

You can create a customization package as a .zip file that contains an XML descriptor file and another .zip file with the contents comprising the customized options.

Step 1 Assemble the files required to comprise your Agent screen customization package:

- Customized nac_login.xml file
- Customized corporate/company logo as a .gif file
- One or more customized nacStrings_*xx*.xml files
- Customized updateFeed.xml descriptor file

Step 2 Create a zip file called “brand-win.zip” that contains the assembled files. For example, in a Linux or Unix environment, execute the following:

zip -r brand-win.zip nac_login.xml nac_logo.gif nacStrings_en.xml nacStrings_cy.xml nacStrings_el.xml

Step 3 Create a “custom.zip” file that contains an appropriate updateFeed.xml descriptor file and the .zip file created above. For example, in a Linux or Unix environment, execute the following:

zip -r custom.zip updateFeed.xml brand-win.zip

Step 4 Save the resulting “custom.zip” file to a location on a local machine that you can access when uploading the file to Cisco ISE.

Related Topics

- Custom nac_login.xml File Template, page 23-8
- Using a Custom Corporate/Company Logo, page 23-9
- Custom nacStrings_xx.xml File Template, page 23-9
- UpdateFeed.xml Descriptor File Template, page 23-19
- Agent XML File Installation Directories, page 23-20

Agent XML File Installation Directories

In a system where the Cisco NAC Agent installed at the default location, you can find these .xml files in the following directories:

- The nac_login.xml file is available in the “C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login” directory.

- In the nacStrings_xx.xml file, the "xx" indicates the locale. You can find a complete list of the files in the "C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility" directory.

If the agent is installed at a different location, then the files would be available at "<*Agent Installed path*>\Cisco\Cisco NAC Agent\UI\nac_divs\login" and "<*Agent Installed path*>\Cisco\Cisco NAC Agent\cues_utility".

Related Topics

- Custom nac_login.xml File Template, page 23-8
- Using a Custom Corporate/Company Logo, page 23-9
- Custom nacStrings_xx.xml File Template, page 23-9
- UpdateFeed.xml Descriptor File Template, page 23-19
- Creating an Agent Customization File, page 23-20

Agent Profile Configuration Guidelines

Cisco recommends configuring agent profiles to control remediation timers, network transition delay timers, and the timer that is 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 client-provisioning policies, you can use the settings in the Administration > System > Settings > Posture > General Settings configuration page to accomplish the same goal.

Once you configure and upload an agent profile to a client device via policy enforcement or another method, that agent profile remains on the client and affects login and operation behavior until you change it to something else. Therefore, deleting an agent profile from Cisco ISE does not remove that behavior from previously affected clients. To alter the login and operational behavior, you must define a new agent profile that *overwrites* the values of existing agent profile parameters on the client and upload it via policy enforcement.

If Cisco ISE has a different agent profile than what is present on the client (which is determined using MD5 checksum), then Cisco ISE downloads the new agent profile to the client. If the agent customization file originating from Cisco ISE is different, Cisco ISE also downloads the new agent customization file to the client. See for more details.

Related Topics

- Posture Administration Settings, page 24-5
- Creating an Agent Customization File, page 23-20

Agent Profile Parameters and Applicable Values

Agent configuration parameters are grouped by function.

This section provides descriptions, default values, and allowable ranges for the Agent profile parameters used to customize login, operational, and logout behavior for Agents that are installed on a client machine.

Table 23-1 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

Parameter	Default Value	Valid Range	Usage Guidelines
VLAN detect interval	0 [1], 5 [2]	0, 5-900	• 0—Access to Authentication VLAN change feature is disabled • 1-5—Agent sends ICMP or ARP queries every 5 seconds • 6-900—An ICMP or ARP query is sent every *x* seconds
Enable VLAN detect without UI?	no	yes or no	• **no**—VLAN detect feature is disabled • **yes**—VLAN detect feature is enabled **Note** This setting does not apply to Mac OS X clients.

1. For the Cisco NAC Windows Agent, the default value is 0. By default, the Access to Authentication VLAN change feature is disabled for Windows.
2. For the Mac OS X Agent, the default value is 5. By default, the Access to Authentication VLAN change feature is enabled with VlanDetectInterval as 5 seconds for Mac OS X.

Table 23-2 Customize Agent Login/Logout Dialog Behavior

Parameter	Default Value	Valid Range	Usage Guidelines
Disable Agent Exit?	no	yes or no	**yes**—Users cannot exit the Agent via the system tray icon **Note** This setting does not apply to Mac OS X clients.
Allow CRL Checks?	yes	yes or no	**no**—Turns off certificate revocation list (CRL) checking during discovery and negotiation **Note** This setting does not apply to Mac OS X clients.
Accessibility mode?	no	yes or no	• 1—Agent is compatible with the Job Access with Speech (JAWS) screen reader • 0—Agent does not interact with the JAWS screen reader Users may experience a slight impact on performance when this feature is enabled. The Agent still functions normally if this feature is enabled on a client machine that does not have the JAWS screen reader installed. **Note** This setting does not apply to Mac OS X clients.

Table 23-2 Customize Agent Login/Logout Dialog Behavior (continued)

Parameter	Default Value	Valid Range	Usage Guidelines
Check signature?	no	yes or no	The Check signature setting looks for a digital signature that the Agent uses to determine whether Windows can trust the executable before launching. For more information, see Adding a Launch Program Remediation, page 24-16. **Note** This setting does not apply to Mac OS X clients.
Bypass summary screen?	yes	yes or no	If you are employing autoremediation for Agent requirements, this setting enables you to make the Agent session dialog more automated by skipping the Agent posture assessment summary screen and proceeding directly to the first autoremediation function. Avoiding this step reduces or eliminates user interaction during the Agent login and remediation session. **Note** This setting does not apply to Mac OS X clients.

Table 23-3 Manage Client-side MAC Address and Agent Discovery Host

Parameter	Default Value	Valid Range	Usage Guidelines
MAC Exception list	—	Valid MAC address	If you specify one or more MAC addresses in this setting, the Agent does not advertise those MAC addresses to Cisco ISE during login and authentication to help prevent sending unnecessary MAC addresses over the network. The text string that you specify must be a comma-separated list of MAC addresses including colons. For example: `AA:BB:CC:DD:EE:FF,11:22:33:44:55:66` **Note** This setting does not apply to Mac OS X clients.
Discovery host	—	IP address or fully qualified domain name (FQDN)	This setting specifies the Discovery Host address or resolvable domain name that the Agent uses to connect to Cisco ISE in a Layer 3 deployment.
Discovery host editable?	yes	yes or no	**yes**—(default value) User can specify a custom value in the Discovery Host field in the Agent **Properties** dialog box **no**—Ensure that the user cannot update the value in the Discovery Host field on the client machine **Note** This setting does not apply to Mac OS X clients.

Table 23-3 Manage Client-side MAC Address and Agent Discovery Host (continued)

Parameter	Default Value	Valid Range	Usage Guidelines
Server name rules	—	FQDN	This parameter consists of comma-separated names of associated Cisco ISE nodes. The Agent uses the names in this list to authorize Cisco ISE access points. If this list is empty, then authorization is not performed. If any of the names are not found, then an error is reported. The server names should be FQDN names. You can use wildcard characters (asterisks [*]) to specify Cisco ISE node names with similar characters. For example, ***.cisco.com** matches all servers in the Cisco.com domain. **Note** This setting does not apply to Mac OS X clients.
Generated MAC	—	Valid MAC address	This parameter supports Evolution-Data Optimized (EVDO) connections on the client machine. If the client machine does not have an active network interface card (NIC), the Agent creates a dummy MAC address for the system. **Note** This setting does not apply to Mac OS X clients.

Table 23-4 Specify Agent Localization Settings

Parameter	Default Value	Valid Range	Usage Guidelines
Language Info	OS setting (“**default**”)	—	• **default**—Agent uses the locale settings from the client operating system • If this setting is either the ID, abbreviated name, or full name of a supported language, the Agent automatically displays the appropriate localized text in Agent dialogs on the client machine. See Table 23-5. “Supported Languages”. **Note** This setting does not apply to Mac OS X clients.

Table 23-5 Supported Languages

Language	ID	Abbreviated Name	Full Name
English US	1033	en	English
Catalan	1027	ca	Catalan (Spain)
ChineseSimplified	2052	zh_cn	Chinese (Simplified)
ChineseTraditional	1028	zh_tw	Chinese (Traditional)

Table 23-5 Supported Languages

Language	ID	Abbreviated Name	Full Name
Czech	1029	cs	Czech
Danish	1030	da	Danish
Dutch	1043	nl	Dutch (Standard)
Finnish	1035	fi	Finnish
French	1036	fr	French
FrenchCanadian	3084	fr-ca	French-Canadian
German	1031	de	German
Hungarian	1038	hu	Hungarian
Italian	1040	it	Italian
Japanese	1041	ja	Japanese
Korean	1042	ko	Korean (Extended Wansung)
Norwegian	1044	no	Norwegian
Polish	1045	pl	Polish
Portuguese	2070	pt	Portuguese
Russian	1049	ru	Russian
SerbianLatin	2074	sr	Serbian (Latin)
SerbianCyrillic	3098	src	Serbian (Cyrillic)
Spanish	1034	es	Spanish (Traditional)
Swedish	1053	sv	Swedish
Turkish	1055	tr	Turkish

Table 23-6 Report and Log Display Settings

Parameter	Default Value	Valid Range	Usage Guidelines
Posture Report Filter	displayFailed	—	This parameter controls the level and type of results that appear to the user when the client machine undergoes posture assessment. • **displayAll**—Client posture assessment report appears, displaying all results when the user clicks Show Details in the Agent dialog • **displayFailed**—(default value) Client posture assessment report only displays remediation errors when the user clicks Show Details in the Agent dialog **Note** This setting does not apply to Mac OS X clients.
Log file size in MB	5	0 and above	This setting specifies the file size (in megabytes) for Agent log files on the client machine. • 0—Agent does not record any login or operation information for the user session on the client machine • any other integer—Agent records login and session information up to the number of megabytes that is specified[1]

1. Agent log files are recorded and stored in a directory on the client machine. After the first Agent login session, two files reside in this directory: one backup file from the previous login session, and one new file containing login and operation information from the current session. If the log file for the current Agent session grows beyond the specified file size, the first segment of Agent login and operation information automatically becomes the backup file in the directory, and the Agent continues to record the latest entries in the current session file.

Table 23-7 Recurring Client Machine Connection Verification

Parameter	Default Value	Valid Range	Usage Guidelines
Detect Retries	3	0 and above	If Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) polling fails, this setting configures the Agent to retry *x* times before refreshing the client IP address.
Ping ARP	0	0-2	• 0—Poll using ICMP • 1—Poll using ARP • 2—Poll using ICMP first, then (if ICMP fails) ARP
Max Timeout for Ping	1	1-10	Poll using ICMP, and if there is no response in *x* seconds, then declare an ICMP polling failure.

Table 23-8 Additional SWISS Discovery Customization

Parameter	Default Value	Valid Range	Usage Guidelines
Swiss timeout	1	1 and above	• 1—Agent performs SWISS discovery as designed and no additional UDP response packet delay timeout value is introduced • an integer greater than 1—Agent waits the additional number of seconds for a SWISS UDP discovery response packet from Cisco ISE before sending another discovery packet. The Agent takes this action to ensure that network latency is not delaying the response packet en route. (SwissTimeout works only for UDP SWISS timeouts.) **Note** This setting does not apply to Mac OS X clients.
Disable L3 Swiss Delay?	no	yes or no	If this setting is yes, the Agent disables its ability to increase the transmission interval for Layer 3 discovery packets. Therefore, the Layer 3 discovery packets repeatedly go out every 5 seconds, just like Layer 2 packets. The default setting is no. **Note** This setting does not apply to Mac OS X clients.

Table 23-9 HTTP Discovery Customization

Parameter	Default Value	Valid Range	Description or Behavior
Http discovery timeout	30	0, 3 and above	• Windows—Set by default at 30 seconds, the Http discovery timeout is the time for which the HTTPS discovery from Agent waits for the response from Cisco ISE. If there is no response for the specified time, then the discovery process times out. The valid range is 3 secs and above. Entering a value of 1 or 2 automatically sets the parameter value to 3. • Mac OS X—Cisco recommends setting this value to 5 secs for Mac OS X client machine Agent profiles. If this value is set to 0, then default client machine operating system timeout settings are used.
Http timeout	120	0, 3 and above	Set by default at 120 seconds, the Http timeout is the time for which the HTTP request from the Agent waits for a response. If there is no response for the specified time, the request times out, and the discovery process times out. The valid range is 3 seconds and above. (Entering a value of 1 or 2 automatically sets the parameter value to 3.) If this value is set to 0, then default client machine operating system timeout settings are used.

Table 23-10 Remediation Timeout Customization

Parameter	Default Value	Valid Range	Usage Guidelines
Remediation timer	4	1-300	Specifies the number of minutes the user has to remediate any failed posture assessment checks on the client machine before having to go through the entire login process again.
Network Transition Delay	3	2-30	Specifies the number of seconds the Agent should wait for network transition (IP address change) before beginning the remediation timer countdown. **Note** When you use the "Enable Agent IP refresh after VLAN change" option, Cisco ISE sends "DHCP release delay" and "DHCP renew delay" settings (as specified below) instead of using the "Network transition delay" setting used for Windows Agent profiles. If you do not use the "Enable Agent IP refresh after VLAN change" option, Cisco ISE sends "Network transition delay" timer settings to client machines, but Cisco ISE will not send *both*.

Table 23-11 Agent Dialog Behavior on User Logout or Shutdown

Parameter	Default Value	Valid Range	Usage Guidelines
Enable auto close login screen?	no	yes or no	Allows you to determine whether or not the Agent login dialog in to which the client machine user enters their login credentials closes automatically following authentication.
Auto close login screen after <*x*> sec	0	0-300	Specifies the number of seconds the Agent waits to automatically close following user credential authentication on the client machine.

Table 23-12 IP Address Behavior Settings for Client Machines

Parameter	Default Value	Valid Range	Usage Guidelines
Enable Agent IP refresh after VLAN change?	no	yes or no	**Caution** Cisco does not recommend enabling this option for Windows client machines accessing the network via native Windows, Cisco Secure Services Client, or AnyConnect supplicants. Specify whether or not the client machine should renew its IP address after the switch or WLC changes the VLAN for the login session of the client on the respective switch port. Check the "Enable Agent IP refresh after VLAN change" parameter to refresh the Windows client IP address in both wired and wireless environments for MAB with posture. To ensure the Mac OS X client IP address is refreshed when the assigned VLAN changes, this parameter is required for Mac OS X client machines accessing the network via the native Mac OS X supplicant in both wired and wireless environments. **Note** When you use the "Enable Agent IP refresh after VLAN change" option, Cisco ISE sends "DHCP release delay" and "DHCP renew delay" settings (as specified below) instead of using the "Network transition delay" setting used for Windows Agent profiles. If you do not use the "Enable Agent IP refresh after VLAN change" option, Cisco ISE sends "Network transition delay" timer settings to client machines, but Cisco ISE will not send *both*.
DHCP renew delay	0	0-60	The number of seconds the client machine waits before attempting to request a new IP address from the network DHCP server.
DHCP release delay	0	0-60	The number of seconds the client machine waits before releasing its current IP address.

Example XML File Generated Using the Create Profile Function

```
<?xml version="1.0" ?>
<cfg>
   <VlanDetectInterval>0</VlanDetectInterval>
   <RetryDetection>3</RetryDetection>
   <PingArp>0</PingArp>
   <PingMaxTimeout>1</PingMaxTimeout>
   <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
```

```
    <SignatureCheck>0</SignatureCheck>
    <DisableExit>0</DisableExit>
    <PostureReportFilter>displayFailed</PostureReportFilter>
    <BypassSummaryScreen>1</BypassSummaryScreen>
    <LogFileSize>5</LogFileSize>
    <DiscoveryHost></DiscoveryHost>
    <DiscoveryHostEditable>1</DiscoveryHostEditable>
    <Locale>default</Locale>
    <AccessibilityMode>0</AccessibilityMode>
    <SwissTimeout>1</SwissTimeout>
    <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
    <HttpTimeout>120</HttpTimeout>
    <ExceptionMACList></ExceptionMACList>
    <GeneratedMAC></GeneratedMAC>
    <AllowCRLChecks>1</AllowCRLChecks>
    <DisableL3SwissDelay>0</DisableL3SwissDelay>
    <ServerNameRules></ServerNameRules>
</cfg>
```

Note This file also contains two static (that is, uneditable by the user or Cisco ISE administrator) “AgentCfgVersion” and “AgentBrandVersion” parameters used to identify the current version of the agent profile and agent customization file, respectively, on the client.

Creating Windows Agent Profiles

You can configure Agent profiles in Cisco ISE that specify how Windows clients behave when logging into your protected network. When you set one or more of the parameters to merge with any existing agent profile, new (previously undefined) parameters are set according to the merged value, but existing parameter settings in an agent profile are maintained.

Before You Begin

Before you create a Windows agent profile, Cisco recommends uploading agent software to Cisco ISE:

- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > ISE Posture Agent Profile**.

Step 3 Specify a name for the Windows agent profile.

Step 4 Specify values for parameters, and specify whether these settings should merge with or overwrite existing profile settings as necessary to appropriately configure Windows client machine agent behavior.

Step 5 Click **Submit**.

What To Do Next

After you have successfully added client-provisioning resources to Cisco ISE and configured one or more optional agent profiles, you can begin to configure resource policies.

Related Topics

- Agent Profile Configuration Guidelines, page 23-21
- Agent Profile Parameters and Applicable Values, page 23-21
- Example XML File Generated Using the Create Profile Function, page 23-30
- Configuring Client Provisioning Resource Policies, page 23-45

Creating Mac OS X Agent Profiles

You can configure Agent profiles in Cisco ISE that specify how Mac OS X clients behave when logging into your protected network. When you set one or more of the parameters to merge with any existing agent profile, new (previously undefined) parameters are set according to the merged value, but existing parameter settings in an agent profile are maintained.

The parameters available to configure for Mac OS X client machines are only a subset of those available for Windows client machines. Cisco recommends that you avoid specifying settings for any parameters that feature a note reading "Mac platform: N/A," as these settings have no effect on agent behavior on Mac OS X clients.

Before You Begin

Before you create a Mac OS X agent profile, Cisco recommends uploading agent software to Cisco ISE:

- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > ISE Posture Agent Profile**.

Step 3 Specify a name for the agent profile.

Step 4 Specify values for parameters, and specify whether these settings should merge with or overwrite existing profile settings as necessary to appropriately configure Mac OS X client machine agent behavior.

Step 5 Click **Submit**.

What To Do Next

After you have successfully added client-provisioning resources to Cisco ISE and configured one or more optional agent profiles, you can begin to configure resource policies.

Related Topics

- Configuring Client Provisioning Resource Policies, page 23-45
- Agent Profile Configuration Guidelines, page 23-21
- Agent Profile Parameters and Applicable Values, page 23-21
- Example XML File Generated Using the Create Profile Function, page 23-30

Performing Data Encryption Checks for Windows OS

Cisco ISE performs a series of steps to check data encryption using OPSWAT Gears.

Create the Registry conditions.

Note You can apply Steps 1 through 15 to create the Registry conditions.

Step 1 Choose **Policy > Conditions > Posture > Registry Condition**.

Step 2 Click **Add**.

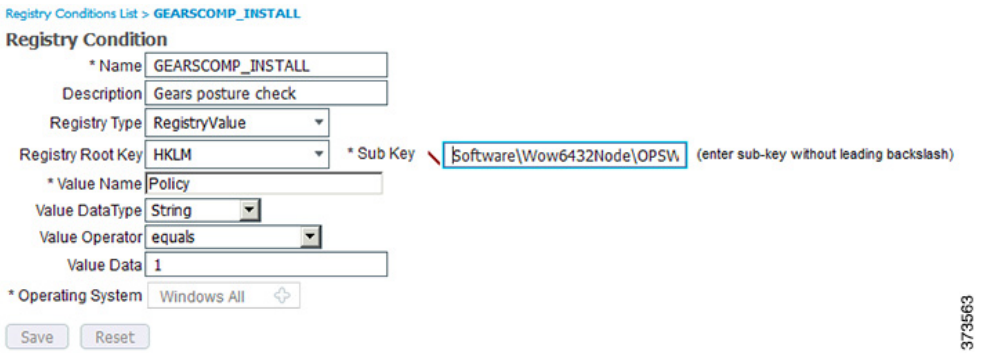
The Registry Condition page appears. You can create the first posture registry condition.

Step 3 Enter the **Name, Description, Registry Type, Registry Root Key, Value Name, Value Data Type, Value Operator, Value Data, and Operating System.**

Step 4 Enter the following Sub Key: Software\Wow6432Node\OPSWAT\Gears Client\Status in the **Sub Key** text box.

Step 5 Click **Submit**.

The OPSWAT Persistent Agent performs a posture compliance check. If the disk is encrypted, the OPSWAT Persistent Agent sets the Registry Value Data to 1. Or, the Registry Value Data is set to zero.

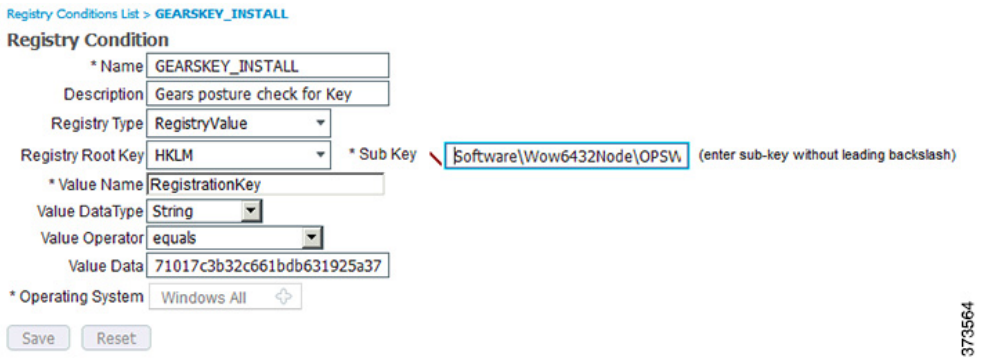


Step 6 In the **Registry Condition** page, click **Add**, to create the second posture registry condition.

Step 7 Enter the **Name, Description, Registry Type, Registry Root Key, Value Name, Value Data Type, Value Operator, Value Data,** and **Operating System** text boxes.

Step 8 In the **Sub Key** text box, enter the following **Sub Key: Software\Wow6432Node\OPSWAT\Gears Client\Config**.

The registry check for OPSWAT key ensures that it matches the Corporate Account key. If the Corporate Account key is not included, it may result in unauthorized users gaining access to the OPSWAT account.

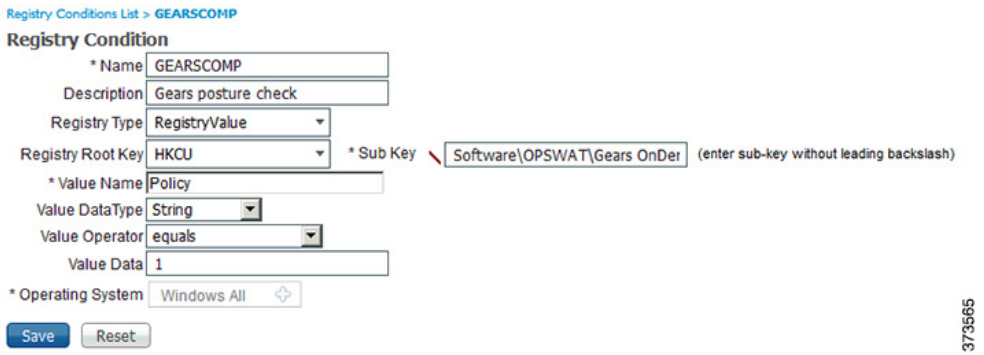


Step 9 In the **Registry Condition** page, click **Add**, to create the third posture registry condition.

Step 10 Enter the **Name, Description, Registry Type, Registry Root Key, Value Name, Value Data Type, Value Operator, Value Data,** and **Operating System**.

Step 11 In the **Sub Key** text box, enter the following **Sub Key: Software\OPSWAT\Gears OnDemand\Config**.

Step 12 The OPSWAT Dissolvable or On-Demand Agent performs a compliance check. If the disk is encrypted, the OPSWAT Persistent Agent sets the Registry Value Data to 1. Or, the Registry Value Data is set to zero.

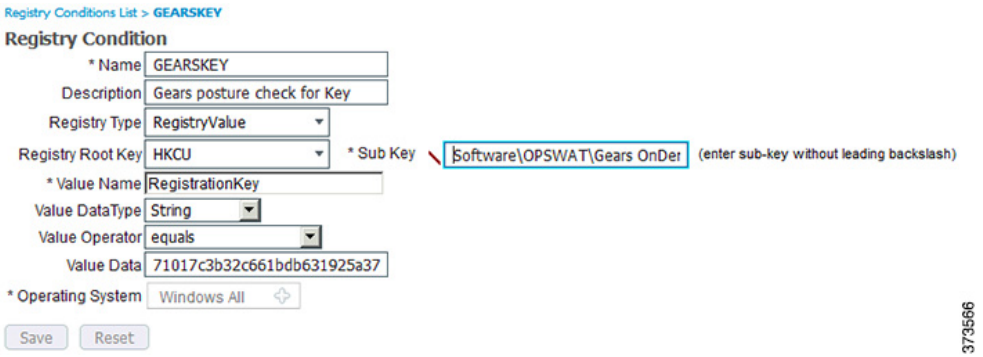


Step 13 In the **Registry Condition** page, click **Add**, to create the last posture registry condition.

Step 14 Enter the **Name, Description, Registry Type, Registry Root Key, Value Name, Value Data Type, Value Operator, Value Data**, and **Operating System.**

Step 15 In the **Sub Key** text box, enter the following **Sub Key: Software\OPSWAT\Gears OnDemand\Config**.

The Registry check for OPSWAT Key ensures that it matches the Corporate Account key. If the Corporate Account key is not included in the posture check, it may result in unauthorized users gaining access to the OPSWAT account.



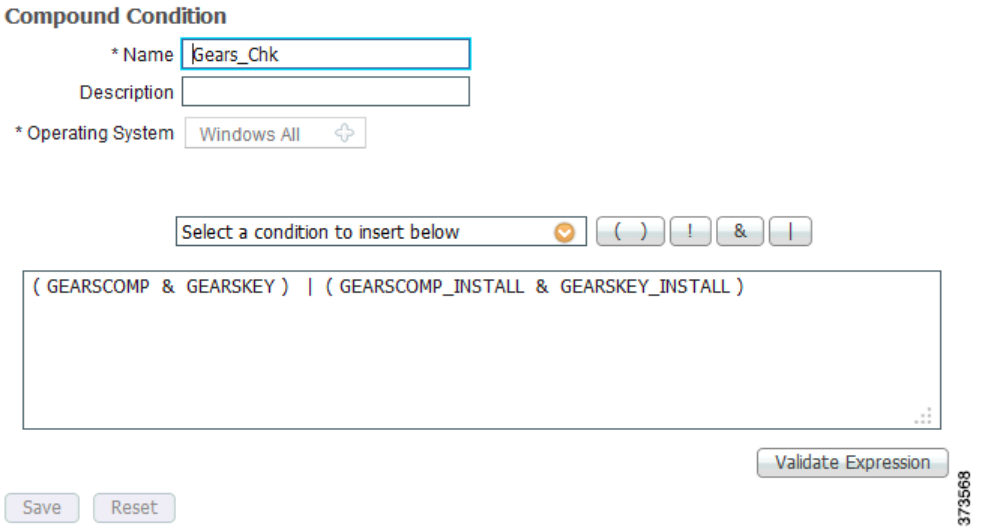
Create a compound condition to combine the Registry conditions that you created earlier.

Step 1 Choose **Policy > Conditions > Posture > Compound Condition** and click **Add**.

Step 2 Enter the **Name**, **Description**, and **Operating System**. In the **Select a condition to insert below** drop-down list, choose the Registry condition names that you have created in the previous steps, to create the compound condition.

Step 3 Click **Validate Expression** to receive the following message: **Server Response: Valid expression.**

Step 4 Click **Submit** to create the compound condition.



Create a posture requirement to use the conditions.

Step 1 Choose **Policy > Results > Posture > Requirements**, click the **Edit** drop-down list and choose the **Insert New Requirement** option.

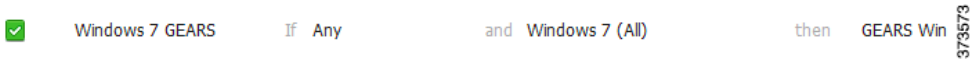
Step 2 In the newly inserted row, enter the **Requirements**. This ensures posture requirement check for Windows registry compliance and key check for OPSWAT Persistent or OPSWAT On-Demand.

Define the Posture policy.

Step 1 Choose **Policy > Posture**.

Step 2 Click the **Edit** drop-down list and choose the **Insert new policy** to display a new row.

Step 3 Enter **policy name, Identity Groups, Operating Systems**, and **Requirements**.



Note In case of an error with compound condition, you can create simple conditions such as, GEARS.

Create the Authorization profile.

Step 1 Choose **Policy > Results > Authorization > Authorization Profile**.

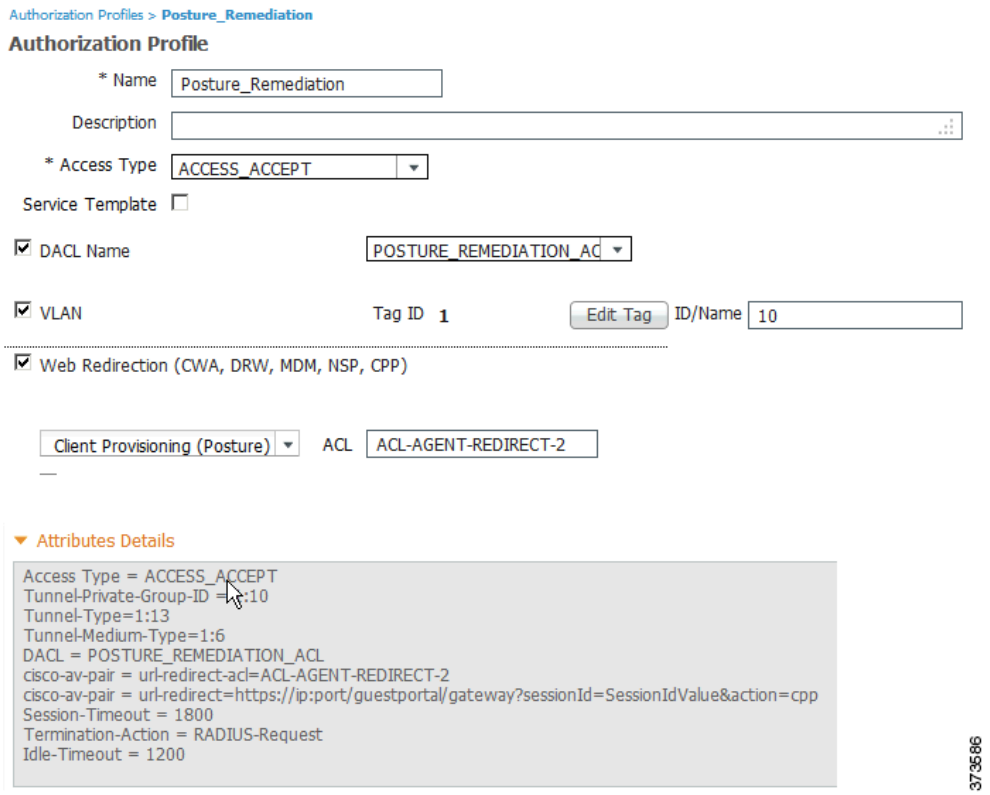
Step 2 Click **Add** to set the new authorization profile.

Step 3 Enter **Name** and **Access Type** in the **Authorization Profile** section.

Step 4 Enter **DACL Name** and **VLAN** in the **Common Tasks** section.

Step 5 Click **Submit**.

Step 6 View the **Attributes Details**.



Create a new Authorization Profile for employee access.

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

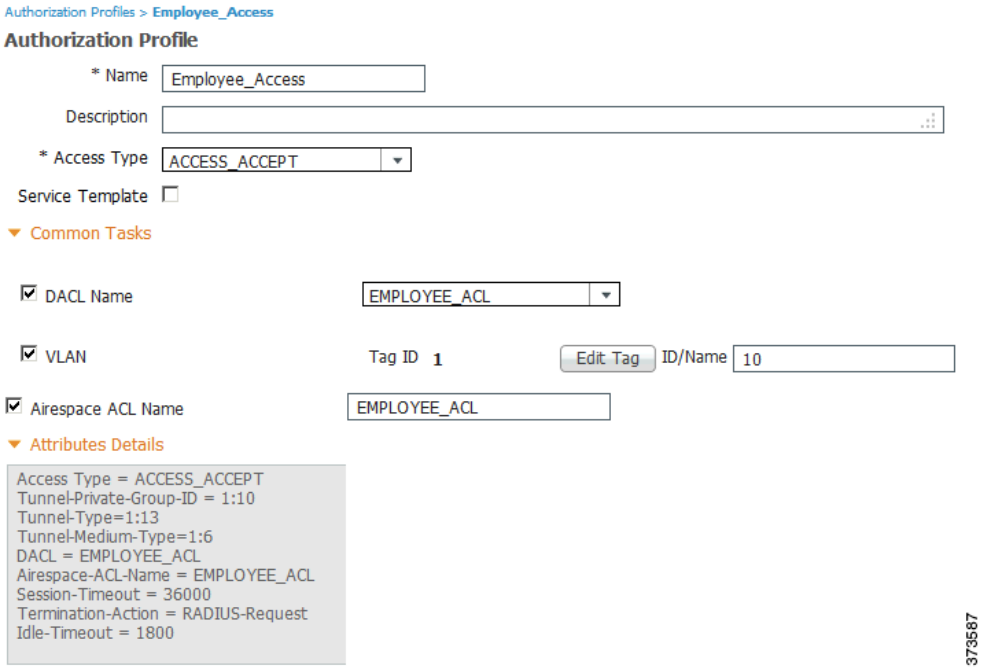
Step 2 Click **Add** to set the new authorization profile.

Step 3 Enter **Name** and **Access Type** in the **Authorization Profile** section.

Step 4 Enter **DACL Name, VLAN, and Airespace ACL Name** in the **Common Tasks** section.

Step 5 Click **Submit**.

Step 6 View the **Attributes Details**.

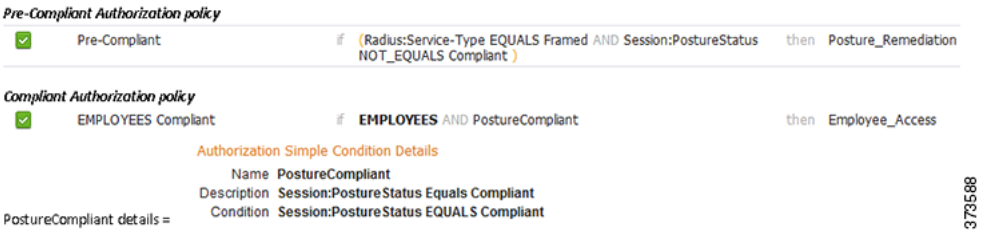


Create the Authorization Policy.

Step 1 Choose **Policy > Authorization**.

Step 2 Set the **Pre-Compliant Authorization** and **Compliant Authorization** policies.

Step 3 View the posture complaint details.



Performing Data Encryption Checks for Mac OS X

Cisco ISE performs a series of steps to check data encryption using OPSWAT Gears.

Create a compound condition to combine the AV conditions.

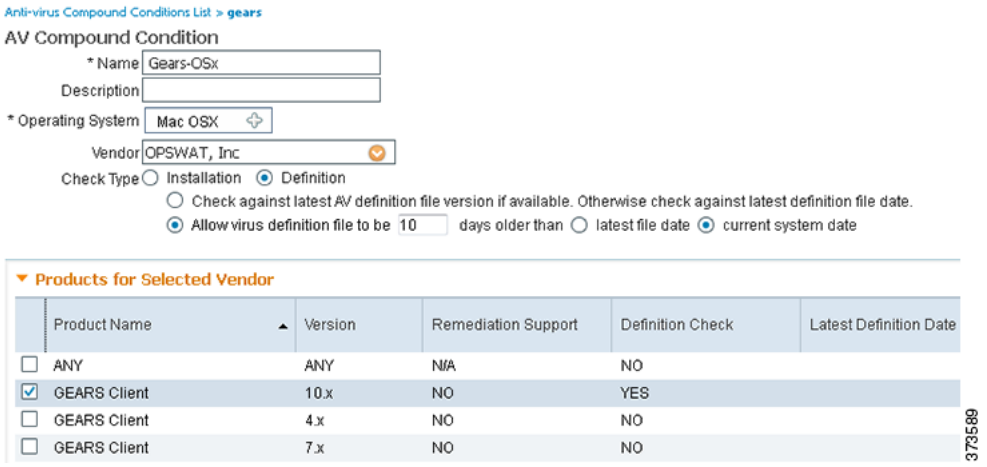
Step 1 Choose **Policy > Conditions > Posture > AV Compound Condition**.

Step 2 Click **Add**.

Step 3 Enter **Name, Description, Operating System, Vendor**, and **Check Type**.

Step 4 Select the desired product in the **Products for Selected Vendor** section.

Step 5 Click **Submit** to perform a definition check.



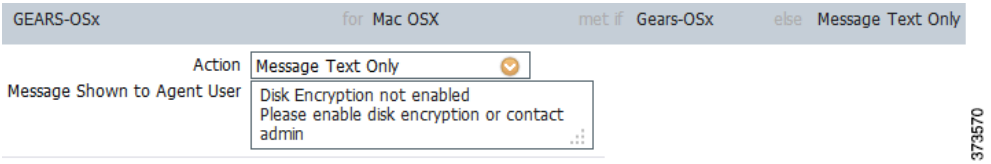
Create a posture requirement to use the conditions.

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

Step 2 Click the **Edit** drop-down list.

Step 3 Choose the **Insert New Requirement** option.

Step 4 Enter the **Requirements** in the newly inserted row. This ensures requirement check for Mac OS X leveraging the AV compound condition created in the previous step for OPSWAT definition check.



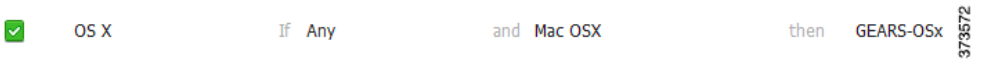
Define the posture policy.

Step 1 Choose **Policy > Posture**.

Step 2 Click the **Edit** drop-down list.

Step 3 Choose the **Insert new policy** to display a new row.

Step 4 Enter **policy name, Identity Groups, Operating Systems**, and **Requirements**.



Create the Authorization profile.

Step 1 Choose **Policy -> Results -> Authorization -> Authorization Profile**.

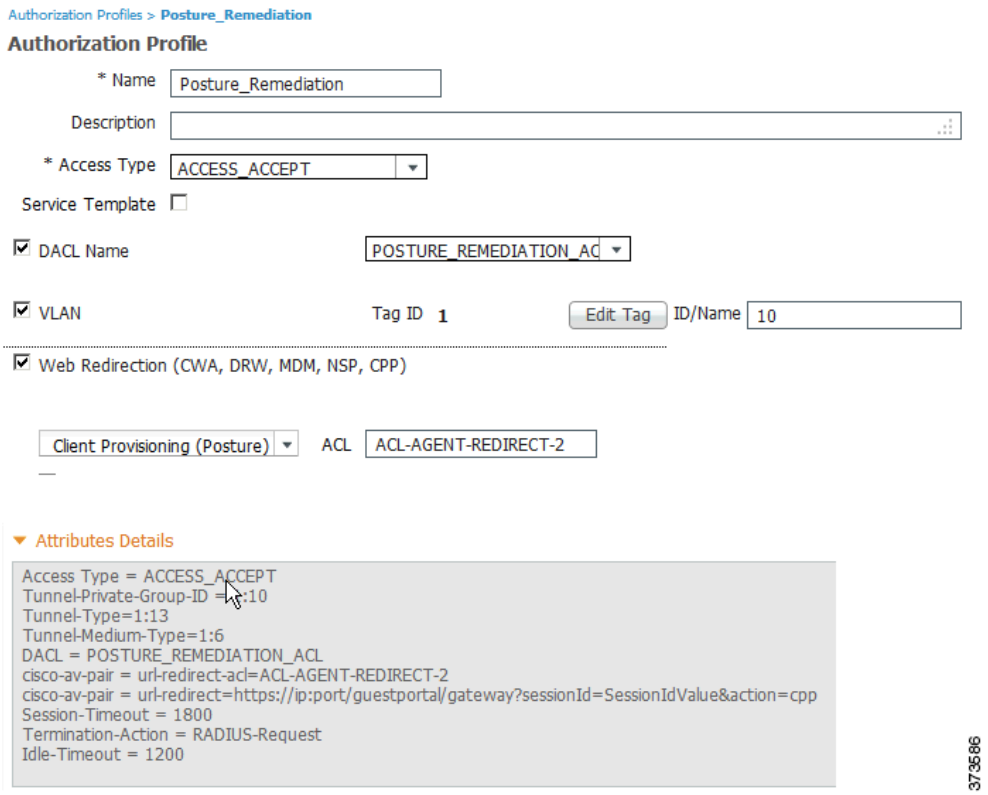
Step 2 Click **Add** to set the new authorization profile.

Step 3 Enter **Name** and **Access Type** in the **Authorization Profile** section.

Step 4 Enter **DACL Name** and **VLAN** in the **Common Tasks** section.

Step 5 Click **Submit**.

Step 6 View the **Attributes Details**.



Create a new Authorization Profile for employee access.

Step 1 Choose **Policy -> Results -> Authorization -> Authorization Profile**.

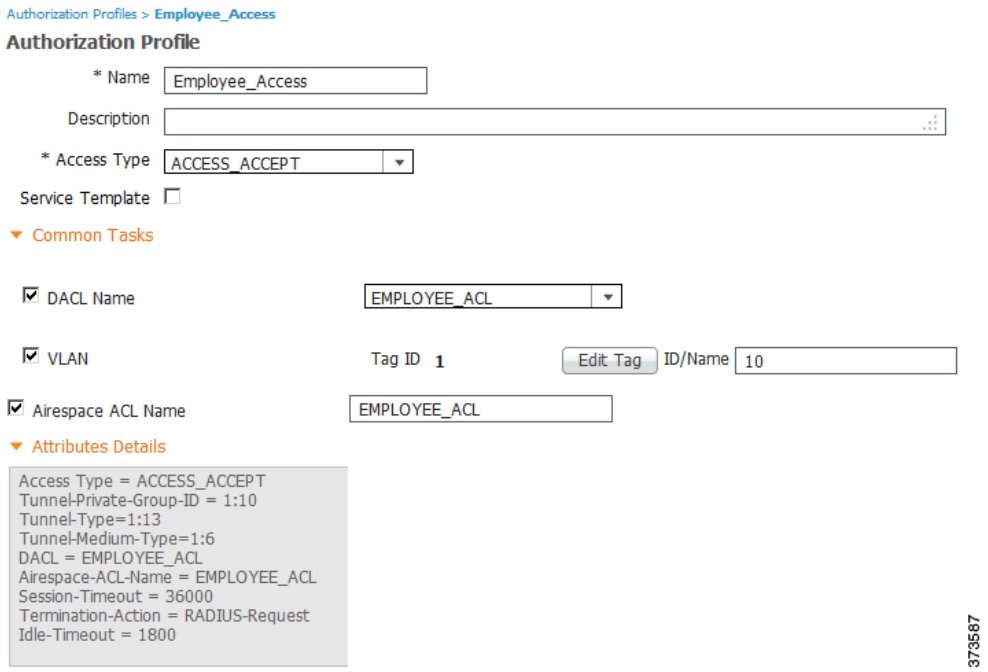
Step 2 Click **Add** to set the new authorization profile.

Step 3 Enter **Name** and **Access Type** in the **Authorization Profile** section.

Step 4 Enter **DACL Name, VLAN, and Airespace ACL Name** in the **Common Tasks** section.

Step 5 Click **Submit**.

Step 6 View the **Attributes Details**.

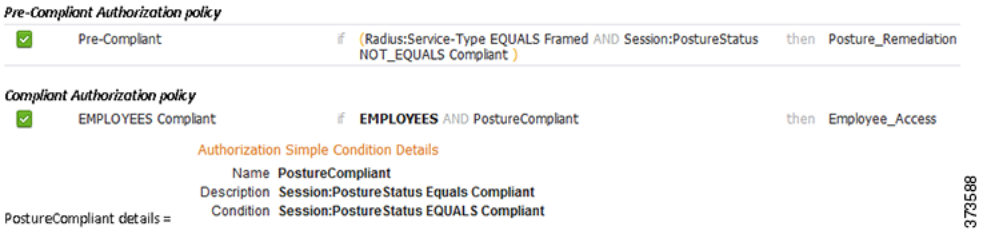


Create the Authorization Policy.

Step 1 Choose **Policy > Authorization**.

Step 2 Set the **Pre-Compliant Authorization** and **Compliant Authorization** policies.

Step 3 View the posture complaint details.



Creating Native Supplicant Profiles

You can create native supplicant profiles to enable users to bring their own devices into the Cisco ISE network. When the user logs in, based on the profile that you associate with that user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network.

Before You Begin

- If you intend to use a TLS device protocol for remote device registration, be sure you set up at least one Simple Certificate Enrollment Protocol (SCEP) profile, as described in Simple Certificate Enrollment Protocol Profiles, page 9-30.
- Be sure to open up TCP port 8909 and UDP port 8909 to enable Cisco NAC Agent, Cisco NAC Web Agent, and supplicant provisioning wizard installation. For more information on port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*.

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > Native Supplicant Profile**.

Step 3 Specify a Name for the agent profile.

Step 4 Enter an optional Description for the Native Supplicant Profile.

Step 5 Select an Operating System for this profile.

Step 6 Enable the appropriate options for Wired or Wireless Connection Type (or both) for this profile. If you enable the Wireless connection option, be sure to also specify the device SSID and the wireless Security type (either WPA2 Enterprise or WPA Enterprise).

Step 7 Choose the Allowed Protocol for the device profile.

Step 8 Enable or disable other **Optional Settings** as appropriate for this profile.

Step 9 Click **Submit**.

What To Do Next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Related Topics

- Agent Profile Configuration Guidelines, page 23-21
- Support for Multiple Guest Portals, page 17-2

Allowed Protocol Settings

Table 23-13 Allowed Protocol Settings

Parameter	Description
TLS	Use the TLS protocol to provide the highest level of device registration security. When you specify the TLS method, Cisco ISE generates a Certificate Signing Request for the device certificate and forwards an SCEP request to the applicable certificate registration authority. For more information on configuring a connection to an SCEP certificate authority, see Simple Certificate Enrollment Protocol Profiles, page 9-30.
PEAP	In general, PEAP allows users to enter their access credentials when logging into the network, and accepts standard registration certificates in return.
EAP-FAST	Use EAP-FAST to connect Apple iOS and Mac OS X devices. Connection typically takes place independent of certificate type and presence. **Note** Due to Apple iOS default behavior on iPhones and iPads, Cisco ISE does not support using the EAP-FAST protocol in the native supplicant profile when connecting via a *single* Service Set Identifier (SSID). When logging into the Cisco ISE network, iOS-based devices automatically negotiate using the PEAP-MSCHAPv2 protocol by default, even if the supplicant provisioning profile that is installed on the device specifies the EAP-FAST protocol. In a dual SSID environment, iOS-based devices should not face this restriction.

Configuring Personal Device Registration Behavior

Use this function to specify how Cisco ISE should handle user login sessions via personal devices on which Cisco ISE cannot install a native supplicant provisioning wizard (like Research In Motion Blackberry devices).

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

Step 2 From the Native Supplicant Provisioning Policy Unavailable drop-down list, choose one of the following two options:

- **Allow Network Access**—Users are allowed to register their device on the network without having to install and launch the native supplicant wizard.
- **Apply Defined Authorization Policy**—Users must try to access the Cisco ISE network via standard authentication and authorization policy application (outside of the native supplicant provisioning process). If you enable this option, the user device goes through standard registration according to any client-provisioning policy applied to the user's ID. If the user's device requires a certificate to access the Cisco ISE network, you must also provide detailed instructions to the user describing how to obtain and apply a valid certificate using the customizable user-facing text fields, as described in the "Adding a Custom Language Template" section in the Chapter 15, Setting up and Customizing End_User Web Portals.

Step 3 Click **Save**.

What To Do Next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Related Topics

- Support for Multiple Guest Portals, page 17-2
- Adding a Custom Language Template, page 16-4

Provisioning Client Machines with the Cisco NAC Agent MSI Installer

You can place the MSI installer in a directory or a zip version of the same installer on the client machine along with an Agent configuration XML file (named **NACAgentCFG.xml**) containing the appropriate Agent profile information required to coincide with your network.

Step 1 Download the **nacagentsetup-win.msi** or **nacagentsetup-win.zip** installer file from the Cisco Software Download site at http://software.cisco.com/download/navigator.html.

Step 2 Place the **nacagentsetup-win.msi** file in a specific directory on the client machine (for example, C:\temp\nacagentsetup-win.msi):

- If you are copying the MSI installer directly over to the client, place the **nacagentsetup-win.msi** file into a directory on the client machine from which you plan to install the Cisco NAC Agent.
- If you are using the **nacagentsetup-win.zip** installer, extract the contents of the zip file into the directory on the client machine from which you plan to install the Cisco NAC Agent.

Step 3 Place an Agent configuration XML file in the same directory as the Cisco NAC Agent MSI package.

If you are not connected to Cisco ISE, you can copy the **NACAgentCFG.xml** file from a client that has already been successfully provisioned. The file is located at **C:\Program Files\Cisco\Cisco NAC Agent\NACAgentCFG.xml.**

As long as the Agent configuration XML file exists in the same directory as the MSI installer package, the installation process automatically places the Agent configuration XML file in the appropriate Cisco NAC Agent application directory so that the agent can point to the correct Layer 3 network location when it is first launched.

Step 4 Open a Command prompt on the client machine and enter the following to execute the installation:

```
msiexec.exe /i NACAgentSetup-win-<version>.msi /qn /l*v c:\temp\agent-install.log
```

(The `/qn` qualifier installs the Cisco NAC Agent completely silently. The `/l*v` logs the installation session in verbose mode.)

To uninstall the NAC Agent, you can execute the following command:

```
msiexec /x NACAgentSetup-win-<version>.msi /qn
```

Note Installing a new version of the Agent using MSI will uninstall the old version and install the new version using the above commands.

Step 5 If you are using Altiris/SMS to distribute the MSI installer, place the Agent customization files in a sub-directory named “brand” in the directory “%TEMP%/CCAA”. When the Cisco NAC Agent is installed in the client, the customization is applied to the Agent. To remove the customization, send a plain MSI without the customization files.

Related Topics

- Example XML File Generated Using the Create Profile Function, page 23-30
- Creating Windows Agent Profiles, page 23-31

Configuring Client Provisioning Resource Policies

Client-provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and/or agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

Before You Begin

Before you can create effective client-provisioning resource policies, ensure that you have set up system-wide client-provisioning functions according to the following topics:

- Specifying Proxy Settings in Cisco ISE, page 6-3.
- Adding Client Provisioning Resources from Remote Sources, page 23-3
- Adding Client Provisioning Resources from a Local Machine, page 23-3
- Downloading Client Provisioning Resources Automatically, page 23-4

Step 1 Choose **Policy > Client Provisioning**.

Step 2 Choose **Enable**, **Disable**, or **Monitor** from the behavior drop-down list:

- **Enable**—Ensures Cisco ISE uses this policy to help fulfill client-provisioning functions when users log in to the network and conform to the client-provisioning policy guidelines.
- **Disable**—Cisco ISE does not use the specified resource policy to fulfill client-provisioning functions.

- **Monitor**—Disables the policy and "watches" the client-provisioning session requests to see how many times Cisco ISE tries to invoke based on the "Monitored" policy.

Step 3 Enter a name for the new resource policy in the Rule Name text box.

Step 4 Specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.

You can choose to specify the *Any* identity group type, or choose one or more groups from a list of existing Identity Groups that you have configured.

Step 5 Use the Operating Systems field to specify one or more operating systems that might be running on the client machine or device through which the user is logging into Cisco ISE.

You can choose to specify a single operating system like "Android," "Mac iOS," and "Mac OS X," or an umbrella operating system designation that addresses a number of client machine operating systems like "Windows XP (All)" or "Windows 7 (All)."

Step 6 In the Other Conditions field, specify a new expression that you want to create for this particular resource policy.

Step 7 For client machines, specify which agent type, compliance module, agent customization package, and/or profile to make available and provision on the client machine based on the categorization defined in the preceding topic.

a. Choose an available agent from the **Agent** drop-down list and specify whether the agent upgrade (download) defined here is mandatory for the client machine by enabling or disabling the **Is Upgrade Mandatory** option, as appropriate.

Note The **Is Upgrade Mandatory** setting only applies to agent downloads. Agent profile, compliance module, and Agent customization package updates are always mandatory.

b. Choose an existing agent profile from the **Profile** drop-down list.

c. Choose an available compliance module to download to the client machine using the **Compliance Module** drop-down list.

Note You can also use the policy configuration process to download agent resources "on the fly" for these three resource types by clicking the Action icon and choosing **Download Resource** or **Upload Resource** from the drop-down list. This opens the Downloaded Remote Resources or Manual Resource Upload dialog box, where you can download one or more resources to Cisco ISE, as described in the "Adding Client_Provisioning Resources from Remote Sources" and "Adding Client_Provisioning Resources from a Local Machine" sections.

d. Choose an available agent customization package for the client machine from the **Agent Customization Package** drop-down list.

Starting from Cisco ISE Release 1.2, it is mandatory to include the client provisioning URL in authorization policy, to enable the NAC Agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

Step 8 For personal devices, specify which Native Supplicant Configuration to make available and provision on the registered personal device based on the categorization defined above:

a. Choose the specific **Configuration Wizard** to distribute to these personal devices.

b. Specify the applicable **Wizard Profile** for the given personal device type.

Step 9 Click **Save**.

What To Do Next

Once you have successfully configured one or more client-provisioning resource policies, you can start to configure Cisco ISE to perform posture assessment on client machines during login.

Related Topics

- Chapter 24, "Configuring Client Posture Policies."

Viewing Client Provisioning Reports

You can access the Cisco ISE monitoring and troubleshooting functions to check on overall trends for successful or unsuccessful user login sessions, gather statistics about the number and types of client machines logging into the network during a specified time period, or check on any recent configuration changes in client-provisioning resources.

Related Topics

- Viewing Client Provisioning Requests, page 23-47
- Viewing Client Provisioning Event Logs, page 23-47

Viewing Client Provisioning Requests

The **Operations > Reports > ISE Reports > Endpoints and Users > Client Provisioning** page displays statistics about successful and unsuccessful client-provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client-provisioning data.

Viewing Client Provisioning Event Logs

You can search event log entries to help diagnose a possible problem with client login behavior. For example, you may need to determine the source of an issue where client machines on your network are not able to get client-provisioning resource updates upon login. You can compile and view logging entries for Client Provisioning and Posture audit messages as well as diagnostics.

Related Topics

- Chapter 12, "Logging"

Collecting Cisco NAC Agent Logs

In Cisco NAC Agent for Windows, right-click the Agent Tray Icon and then click **Log Packager** to run the support package and collect the logs.

In Cisco NAC Agent for Mac OS X, in the Tools menu, right-click the Agent icon and click the **Collect Support Logs** option to collect the Agent logs and support information. The collected information is available as a zip file. The user can save the file by choosing the file location and filename. By default the file is saved on the desktop with the filename as *CiscoSupportReport.zip*.

If the Agent crashes or hangs, you can run the **CCAAgentLogPackager.app** to collect the logs. This file is available at **/Applications/CCAAgent.app**. You can right-click **CCAAgent.app**, select **Show Package Contents** and double-click **CCAAgentLogPackager** to collect the support information.“