



CHAPTER 19

Configuring Client Provisioning Policies

This chapter describes how to manage client provisioning resources and create client provisioning policies for your network.

- [Client Provisioning Overview, page 19-1](#)
- [Adding and Removing Agents and Other Resources, page 19-3](#)
- [Setting Up Global Client Provisioning Functions, page 19-28](#)
- [Configuring Client Provisioning Resource Policies, page 19-31](#)
- [Client-side Agent Installation and Login—Cisco NAC Agent, page 19-33](#)
- [Accessing the Network and Registering Personal Devices, page 19-39](#)
- [Viewing Client Provisioning Reports and Events, page 19-48](#)

Client Provisioning Overview

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

- 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 antispysware vendor support, and correct agent customization packages and profiles, if necessary.

Cisco ISE Agents

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.



Warning

The NAC Agents cannot communicate with the Cisco ISE server securely and the Cisco ISE server throws an error when the Windows XP clients do not have the latest Windows hotfixes and patches installed in them. You must ensure that the latest Windows hotfixes and patches are installed on Windows XP clients so that NAC Agents can establish a secure and encrypted communication with the Cisco ISE server (SSL over TCP).

Uninstalling Cisco NAC Agent for Windows Clients

The 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**.
-

Cisco NAC Agent for Macintosh Clients

The Macintosh 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 antivirus and antispyware definition updates.

After users log into the Cisco NAC 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 the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

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 <i><local drive ID></i> > 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.



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.

After users log into 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, 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.

Agent and Client Machine Operating System Compatibility

For a complete list of supported client machine operating systems and agents, see [Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x](#).

Adding and Removing Agents and Other Resources

- [Viewing and Displaying Client Provisioning Resources, page 19-4](#)

- [Adding Client Provisioning Resources to Cisco ISE, page 19-5](#)
- [Creating Agent Profiles, page 19-12](#)
- [Creating Native Supplicant Profiles, page 19-24](#)
- [Deleting Client Provisioning Resources, page 19-26](#)
- [Provisioning Client Machines with the Cisco NAC Agent MSI Installer, page 19-26](#)

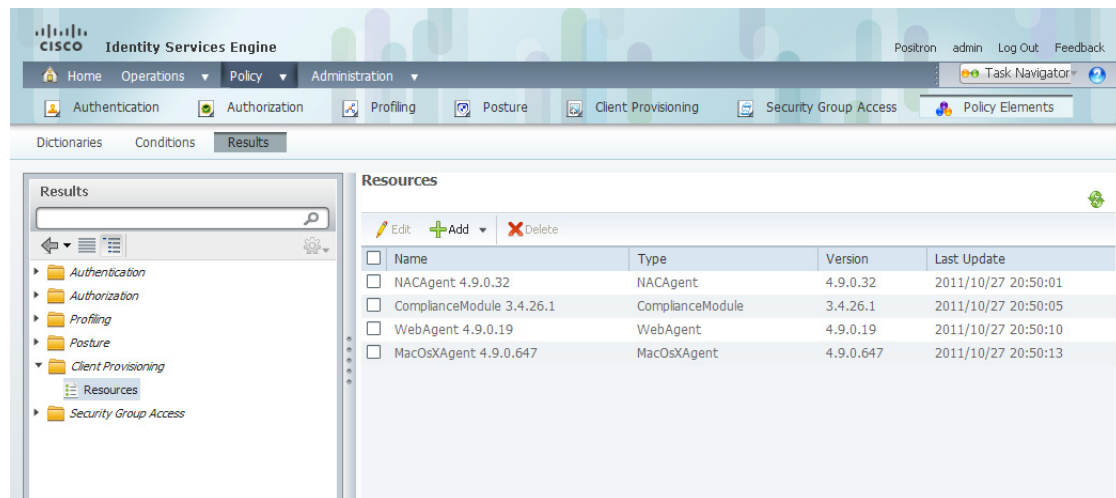
Viewing and Displaying Client Provisioning Resources

To display the list of existing resources that are available to configure client provisioning resource policies, open the Cisco ISE web console user interface and choose **Policy > Policy Elements > Results > Client Provisioning > Resources**. The Resources page displays the following types of resources:

- 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 wizards
- Agent compliance modules
- Agent customization packages

Figure 19-1 shows the Resources page.

Figure 19-1 *Policy > Policy Elements > Results > Client Provisioning > Resources*



If this display is empty (that is, if there are no client provisioning resources that are available on Cisco ISE), you can add resources using the procedures in [Adding and Removing Agents and Other Resources, page 19-3](#).

Adding Client Provisioning Resources to Cisco ISE

Before you can configure client provisioning resource policies that enable users to download and install resources on client machines, you must ensure that those resources are already present on the Cisco ISE appliance. You can use the resource download and creation functions described here to ensure the following Cisco ISE resources are available in Cisco ISE:

- Persistent and temporal agents (Windows and Mac OS X Cisco NAC Agents, Cisco NAC Web Agent). For detailed information on agent types available in Cisco ISE, see [Cisco ISE Agents, page 19-2](#).
- Agent profiles
- Agent compliance modules
- Agent customization packages
- Native supplicant installation wizards

The following topics describe how to add client provisioning resources from a remote source or from a local machine:

- [Adding Client Provisioning Resources from a Remote Source, page 19-5](#)
- [Adding Client Provisioning Resources from a Local Machine, page 19-6](#)

**Note**

You can also configure Cisco ISE to automatically update client provisioning resources. For details, see [Downloading Client Provisioning Resources Automatically, page 19-29](#).

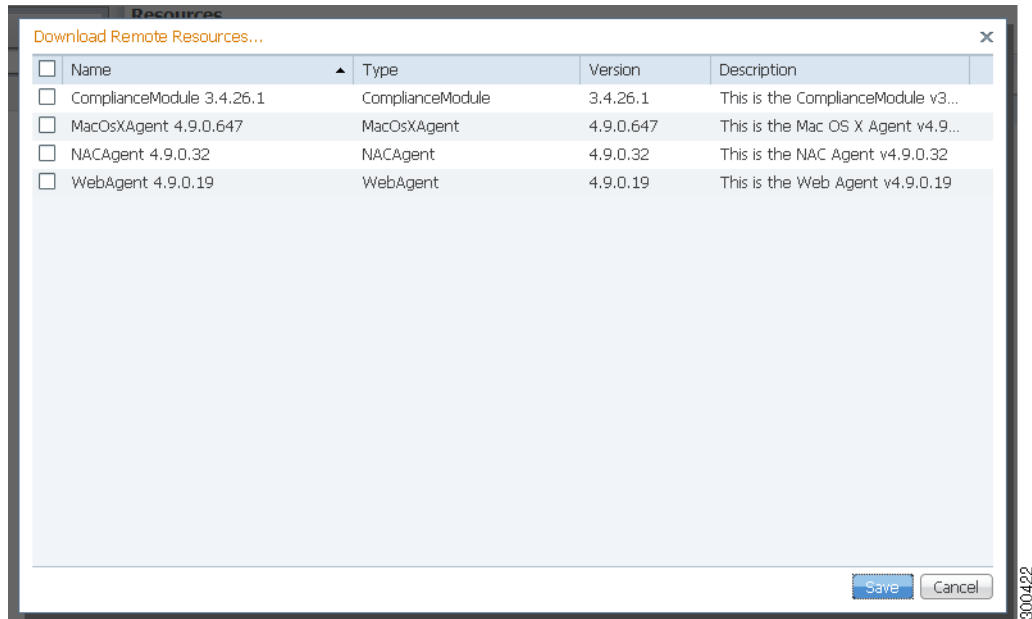
Adding Client Provisioning Resources from a Remote Source

Prerequisites

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 need to verify that you have the correct proxy settings configured for your network as described in [Specifying Proxy Settings in Cisco ISE, page 8-17](#).

To add client provisioning resources from a remote source like Cisco.com, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
- Step 2** Choose **Add > Add resources from Cisco site** ([Figure 19-2](#)).

Figure 19-2 Add resources from Cisco site

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

Step 4 Click **Save** to download the selected resources to Cisco ISE.

Depending on the type and number of resources that you select, and available network bandwidth, Cisco ISE can take a few seconds (or even a few minutes, depending on the size and type of resource) to download the new resources and display them in its list of available client provisioning resources.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure resource policies, as described in [Configuring Client Provisioning Resource Policies](#), page 19-31.

Troubleshooting Topics

- [Cannot Download Remote Client Provisioning Resources](#), page D-10

Adding Client Provisioning Resources from a Local Machine



Caution

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 1.1.x](#).

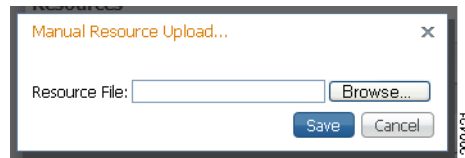
We recommend uploading only Agent customization packages and Agent profiles using this function of Cisco ISE. See [Creating Agent Customization Files to Add to Cisco ISE](#), page 19-7 and [Creating Agent Profiles](#), page 19-12. For other resource types, be sure to use the guidelines described in [Adding Client Provisioning Resources from a Remote Source](#), page 19-5.

For downloading the resource files manually from the CCO, refer to “Cisco ISE Offline Updates” section in the [Release Notes for the Cisco Identity Services Engine, Release 1.1.x](#).

To add existing client provisioning resources from a local machine (for example, files that you may have already downloaded from CCO to your laptop), complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
- Step 2** Choose **Add > Add resource from local disk** (Figure 19-3).

Figure 19-3 Add resources 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**.

Depending on the type of resource file that you select, and the available network bandwidth between Cisco ISE and your local machine, Cisco ISE can take a few seconds to a few minutes to download the new resource file and display it in its list of available client provisioning resources.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure resource policies, as described in [Configuring Client Provisioning Resource Policies, page 19-31](#).

Creating Agent Customization Files to Add to Cisco ISE

A customization package is a zip file that contains an XML descriptor file and another zip with the contents of the customized options. There are three steps required for creating a new customization package.

-
- Step 1** After modifying the required files like logo.gif, create a zip file called brand-win.zip. For example, in a Linux or Unix environment, execute the following:

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

The brand-win.zip file usually contains the following files:

- nac_logo.gif
- nac_login.xml
- nacStrings_xx.xml

The following parameters can be customized:

- [Logo](#)
- [Agent Login Screen](#)
- [Predetermined Set of Agent Strings and Fields](#)

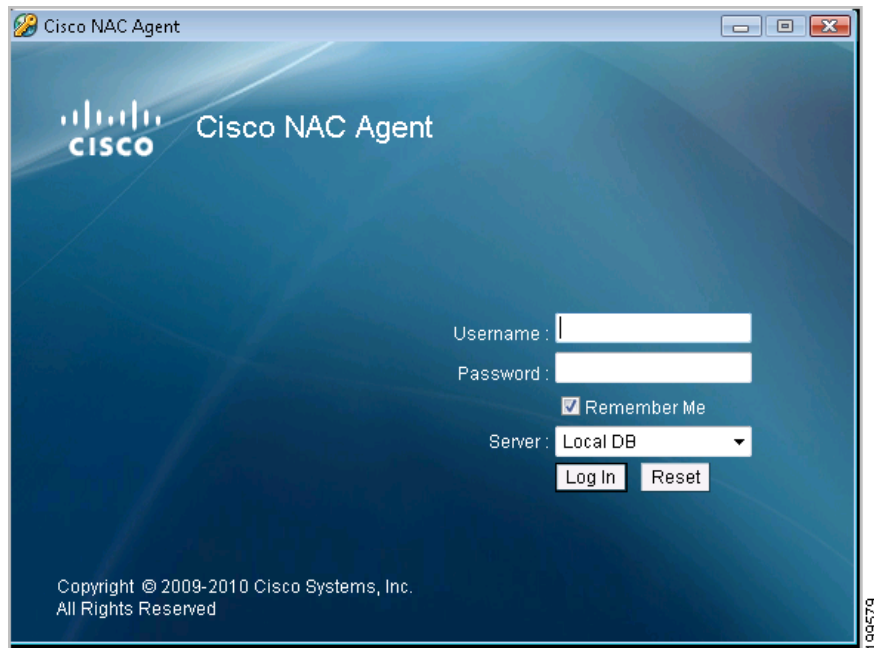
Logo

The Cisco logo that appears in all the Cisco NAC Agent screens can be replaced with your brand logo. The image should be a .gif file, not exceeding 67 x 40 pixels. The logo image should be named `nac_logo.gif`.

Agent Login Screen

By default, the Cisco NAC Agent login screen appears as shown in [Figure 19-4](#).

Figure 19-4 Cisco NAC Agent Login—Default Screen



The elements that appear on the Cisco NAC Agent login screen can be customized by using either one of the following methods:

- Modify the `nac_login.xml` file
- Modify the `nacStrings_xx.xml` file



Note

You can replace the default logo by using the `nac_logo.gif` file.

In a system that has the Cisco NAC Agent installed at the default location, you can find these 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.

**Note**

The files are available in the directories mentioned above when the agent is installed at the default location. 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”.

**Tip**

We recommend making changes in the nacStrings_xx.xml file.

The following example shows part of the nac_login.xml file. The customized text is shown in boldface.

```
<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>
          </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>
```

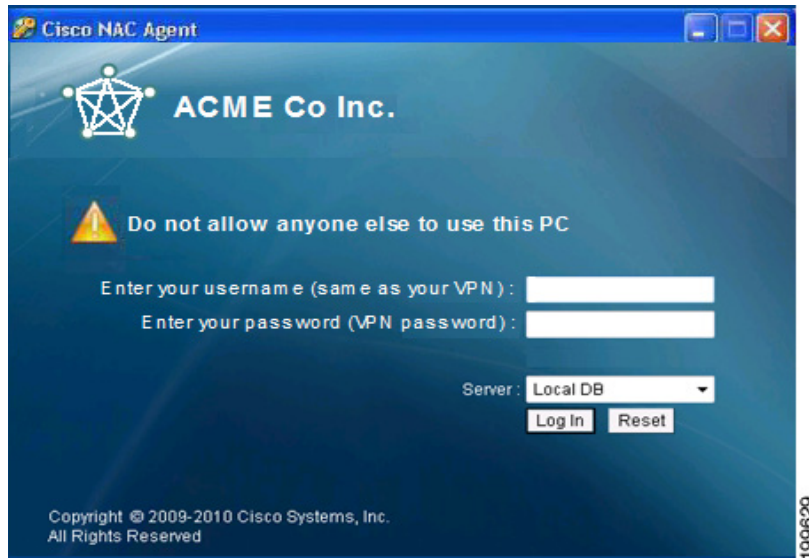
The following example shows a part of contents of the nacStrings_xx.xml file. The customized text is shown in boldface.

```
<cueslookup:name key="login.productname"> XYZ Co Inc. </cueslookup:name>
<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.username"> Enter your username (same as your VPN)
</cueslookup:name>
<cueslookup:name key="login.password">Enter your password (VPN password)</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">Do not allow anyone else to use this
PC</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>
```

The previous file has been modified to customize the login screen as shown in [Figure 19-5](#).

Figure 19-5 Cisco NAC Agent Login—Customized Screen



Notice that the Remember Me check box has been removed, and the Username and Password fields have more text.



Note

There is no limit for the number of characters used for the customized text. However, we recommend restricting the length so that these fields do not take up too much of space in the login screen.

Predetermined Set of Agent Strings and Fields

Modify the `nacStrings_xx.xml` file to replace the Device Posture Status (DPS) details. The following example shows part of the `nacStrings_xx.xml` file with DPS values.

Example `nacStrings_xx.xml` File:

```
<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>

```

Step 2 Create an XML descriptor file like the following and name it **updateFeed.xml**:

```

<?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/1/1/1/1</id> -- This
id can be anything, but should be unique within an ISE deployment
    <title>Agent Customization Package</title>
    <updated>2010-06-07T12:00:00Z</updated>
    <summary>This is the agent customization package </summary> - Can be
anything
    <link rel="enclosure" type="application/zip" href="brand-windows.zip"
length="18884" />
    <update:type>AgentCustomizationPackage</update:type>
    <update:version>1.1.1.0</update:version> -- Important to have this as 4
digit
    <update:os>Win</update:os>
  </entry>
</feed>

```

Step 3 Create another zip file that contains the descriptor file above and the zip file created in [Step 1](#). For example, in a Linux or Unix environment, execute the following:

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

Step 4 Upload the new custom.zip file to Cisco ISE using the guidelines described in [Adding Client Provisioning Resources from a Local Machine](#), page 19-6.

Creating Agent Profiles

- [Creating Windows Agent Profiles in Cisco ISE](#), page 19-12
- [Creating Mac OS X Agent Profiles in Cisco ISE](#), page 19-14
- [Modifying Windows and Mac OS X Agent Profiles in Cisco ISE](#), page 19-15
- [Agent Profile Parameters and Applicable Values](#), page 19-16

We recommend 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. See [Posture General Settings](#), page 20-10 for more details.



Note

Once you configure and upload an agent profile to a client machine via policy enforcement or other method, that agent profile remains on the client machine and affects the client machine 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 client machines. 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 machine and upload it via policy enforcement.

Creating Windows Agent Profiles in Cisco ISE

Prerequisites

Before you create a Windows agent profile, we recommend that you upload agent software to Cisco ISE per the guidelines in the following topics:

- [Adding Client Provisioning Resources from a Remote Source](#), page 19-5
- [Adding Client Provisioning Resources from a Local Machine](#), page 19-6

To create a Windows agent profile, complete the following steps:

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

Step 2 Choose **Add > ISE Posture Agent Profile** ([Figure 19-6](#)).

Figure 19-6 ISE Posture Agent Profile

Resources > New Profile

▼ ISE Posture Agent Profile

Profile Name:

| Parameter Description | Parameter Value | Mode | Notes |
|---|----------------------------------|-----------|---|
| VLAN detect interval in secs (<i>VlanDetectInterval</i>): (0-900): | <input type="text" value="0"/> | merge | For OSX, if <i>EnableAgentIpRefresh</i> parameter is enabled, set this value to 5 or greater |
| Enable VLAN detect without UI? (<i>EnableVlanDetectWithoutUI</i>): | no | merge | OSX: N/A |
| Disable Agent exit? (<i>DisableExit</i>): | no | merge | OSX: N/A |
| Allow CRL checks? (<i>AllowCRLChecks</i>): | yes | overwrite | OSX: N/A |
| Accessibility mode? (<i>AccessibilityMode</i>): | no | merge | OSX: N/A |
| Check signature? (<i>SignatureCheck</i>): | no | overwrite | OSX: N/A |
| Bypass summary screen? (<i>BypassSummaryScreen</i>): | yes | merge | OSX: N/A |
| MAC exception list (<i>ExceptionMACList</i>): | <input type="text"/> | merge | OSX: N/A |
| Discovery host (<i>DiscoveryHost</i>): | <input type="text"/> | overwrite | |
| Discovery host editable? (<i>DiscoveryHostEditable</i>): | yes | overwrite | OSX: N/A |
| Server name rules (<i>ServerNameRules</i>): | <input type="text"/> | overwrite | OSX: N/A |
| Generated MAC (<i>GeneratedMAC</i>): | <input type="text"/> | merge | OSX: N/A |
| Language info (<i>Locale</i>): | default | merge | OSX: N/A |
| Posture report filter (<i>PostureReportFilter</i>): | displayFailed | merge | OSX: N/A |
| Log file size in MB (<i>LogFileSize</i>): Min=0: | <input type="text" value="5"/> | merge | |
| Detect retries (<i>RetryDetection</i>): Min=0: | <input type="text" value="3"/> | merge | |
| Ping ARP (<i>PingArp</i>): (0-2): | <input type="text" value="0"/> | merge | |
| Max timeout for ping - in secs (<i>PingMaxTimeout</i>): (1-10): | <input type="text" value="1"/> | merge | |
| Swiss timeout - in secs (<i>SwissTimeout</i>): Min=1: | <input type="text" value="1"/> | merge | OSX: N/A |
| Disable L3 Swiss delay? (<i>DisableL3SwissDelay</i>): | no | merge | OSX: N/A |
| Http discovery timeout - in secs (<i>HttpDiscoveryTimeout</i>): Min=0: | <input type="text" value="30"/> | merge | For OSX, it is recommended to set this value to 5 if this value is set to zero, then system defaults are used |
| Http timeout - in secs (<i>HttpTimeout</i>): Min=0: | <input type="text" value="120"/> | merge | if this value is set to zero, then system defaults are used |
| Remediation timer - in mins (<i>RemediationTimer</i>): (1-300): | <input type="text" value="4"/> | overwrite | Not an agent config XML parameter on end point, mode: N/A |
| Network Transition Delay - in secs (<i>NetworkTransitionDelay</i>): (2-30): | <input type="text" value="3"/> | overwrite | Not an agent config XML parameter on end point, mode: N/A |
| Enable auto close login screen? (<i>EnableAutoClose</i>): | no | overwrite | Not an agent config XML parameter on end point, mode: N/A |
| Auto close login screen after - in secs (<i>AutoCloseTimer</i>): (0-300): | <input type="text" value="0"/> | overwrite | Not an agent config XML parameter on end point, mode: N/A |
| Enable agent iprefresh after vlan change? (<i>EnableAgentIpRefresh</i>): | no | overwrite | Not an agent config XML parameter on end point, mode: N/A |
| Dhcp Renew Delay (<i>DhcpRenewDelay</i>): (0-60): | <input type="text" value="12"/> | overwrite | Not an agent config XML parameter on end point, mode: N/A |
| Dhcp Release Delay (<i>DhcpReleaseDelay</i>): (0-60): | <input type="text" value="1"/> | overwrite | Not an agent config XML parameter on end point, mode: N/A |

Notes:
It is recommended that a separate profile be created for Windows and OSX deployments
'Mode' attribute is not applicable for OSX deployments

300423

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.

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. For details regarding the various parameters and their settings, see [Agent Profile Parameters and Applicable Values](#), page 19-16.

Step 5 Click **Submit** to save the agent profile to Cisco ISE. The new file now appears in the list of available client provisioning resources.

Next Steps

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, as described in [Configuring Client Provisioning Resource Policies](#), page 19-31.

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 machine. If Cisco ISE has a different agent profile than what is present on the client machine (determined using MD5 checksum), then Cisco ISE downloads the new agent profile to the client machine. If the agent customization file originating from Cisco ISE is different, Cisco ISE downloads the new agent customization file to the client machine, as well.

Creating Mac OS X Agent Profiles in Cisco ISE

The parameters available to configure for Mac OS X client machines are only a subset of those available for Windows client machines. We recommend 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 client machines.

Prerequisites

Before you create a Mac OS X agent profile, we recommend that you upload agent software to Cisco ISE per the guidelines in the following topics:

- [Adding Client Provisioning Resources from a Remote Source](#), page 19-5
- [Adding Client Provisioning Resources from a Local Machine](#), page 19-6

To create a Mac OS X agent profile, complete the following steps:

-
- 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.

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. For details regarding the various parameters and their settings, see [Agent Profile Parameters and Applicable Values](#), page 19-16.

- Step 5** Click **OK** to save the Mac OS X agent profile to Cisco ISE. The new file now appears in the list of available client provisioning resources.
-

Next Steps

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, as described in [Configuring Client Provisioning Resource Policies](#), page 19-31.

Modifying Windows and Mac OS X Agent Profiles in Cisco ISE

Prerequisites

To modify a Windows or Mac OS X agent profile, you must have already manually created one or more agent profiles according to the guidelines in the following topics:

- [Creating Windows Agent Profiles in Cisco ISE](#), page 19-12
- [Creating Mac OS X Agent Profiles in Cisco ISE](#), page 19-14

To modify an existing Windows or Mac OS X agent profile, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
- Step 2** Select an existing agent profile entry, and click **Edit**.
- Step 3** Make any necessary changes in the existing agent profile, and click **Save**. For details regarding the various parameters and their settings, see [Agent Profile Parameters and Applicable Values](#), page 19-16.



Note If you choose the **Reset** option, all parameter values are automatically reset to their respective default settings.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE and configured or modified one or more existing optional agent profiles, you can begin to configure resource policies, as described in [Configuring Client Provisioning Resource Policies](#), page 19-31.

Agent Profile Parameters and Applicable Values

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. Agent configuration parameters are grouped by function and appear in the following tables:

- [Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs](#)
- [Customize Agent Login/Logout Dialog Behavior](#)
- [Manage Client-side MAC Address and Agent Discovery Host](#)
- [Specify Agent Localization Settings](#)
- [Report and Log Display Settings](#)
- [Recurring Client Machine Connection Verification](#)
- [Additional SWISS Discovery Customization](#)
- [HTTP Discovery Customization](#)
- [Remediation Timeout Customization](#)
- [Agent Dialog Behavior on User Logout or Shutdown](#)
- [IP Address Behavior Settings for Client Machines](#)

Table 19-1 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

| Parameter | Default Value | Valid Range | Description or Behavior |
|--------------------------------|---------------------------------|-------------|---|
| Vlan detect interval | 0 ¹ , 5 ² | 0, 5-900 | <ul style="list-style-type: none"> • If this setting is 0, the Access to Authentication VLAN change feature is disabled. • If this setting is 1-5, the agent sends ICMP or ARP queries every 5 seconds. • If this setting is 6-900, an ICMP or ARP query is sent every <i>x</i> seconds. |
| Enable VLAN detect without UI? | no | yes or no | <ul style="list-style-type: none"> • If this value is set to no, the VLAN detect feature is disabled. • If this value is set to yes, the VLAN detect feature is enabled. <p>Note This setting does not apply to Mac OS X client machine agents.</p> |

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 19-2 Customize Agent Login/Logout Dialog Behavior

| Parameter | Default Value | Valid Range | Description or Behavior |
|------------------------|---------------|-------------|---|
| Disable Agent Exit? | no | yes or no | <p>If this parameter is set to yes, users cannot exit the agent via the system tray icon.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Allow CRL Checks? | yes | yes or no | <p>Setting this parameter to no turns off certificate revocation list (CRL) checking for the agent during discovery and negotiation with the Cisco ISE node.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Accessibility mode? | no | yes or no | <ul style="list-style-type: none"> • If this setting is 1, the agent is compatible with the Job Access with Speech (JAWS) screen reader. • If this setting is 0, the agent does not interact with the JAWS screen reader. <p>Note 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.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Check signature? | no | yes or no | <p>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, Duplicating, Editing, and Deleting a Launch Program Remediation, page 20-133.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Bypass summary screen? | yes | yes or no | <p>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. Avoidance of this step reduces or eliminates user interaction during the agent login and remediation session.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |

Table 19-3 Manage Client-side MAC Address and Agent Discovery Host

| Parameter | Default Value | Valid Range | Description or Behavior |
|--------------------------|---------------|--|--|
| MAC Exception list | — | Valid MAC address | <p>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:</p> <p>AA:BB:CC:DD:EE:FF,11:22:33:44:55:66</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Discovery host | — | IP address or fully qualified domain name (FQDN) | <p>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.</p> |
| Discovery host editable? | yes | yes or no | <p>If this parameter is set to yes (the default value), then the user can specify a custom value in the Discovery Host field in the agent Properties dialog box. You can change this entry to no to ensure that the user cannot update the value in the Discovery Host field on the client machine.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Server name rules | — | FQDN | <p>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 the authorization is not performed. If any of the names are not found, then an error is reported.</p> <p>The server names should be FQDN names. The wildcard character (an asterisk [*]) can be used to specify Cisco ISE node names with similar characters. For example, *.cisco.com matches all the servers in the Cisco.com domain.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Generated MAC | — | Valid MAC address | <p>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.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |

Table 19-4 Specify Agent Localization Settings

| Parameter | Default Value | Valid Range | Description or Behavior |
|---------------|------------------------|-------------|---|
| Language Info | OS setting (“default”) | — | <ul style="list-style-type: none"> If this setting is default, the 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. <p>Note This setting does not apply to Mac OS X client machine agents.</p> |

| 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) |
| 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 |
| Portuguese | 2070 | pl | 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 19-5 Report and Log Display Settings

| Parameter | Default Value | Valid Range | Description or Behavior |
|-----------------------|---------------|-------------|---|
| Posture Report Filter | displayFailed | — | <p>This parameter controls the level and type of results that appear to the user when the client machine undergoes posture assessment.</p> <ul style="list-style-type: none"> If this setting is displayAll, the client posture assessment report appears, displaying all results when the user clicks Show Details in the agent dialog. If this setting is displayFailed, the client posture assessment report only displays remediation errors when the user clicks Show Details in the agent dialog. <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Log file size in MB | 5 | 0 and above | <p>This setting specifies the file size (in megabytes) for agent log files on the client machine.</p> <ul style="list-style-type: none"> If this setting is 0, the agent does not record any login or operation information for the user session on the client machine. If the administrator specifies any other integer, the 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 19-6 Recurring Client Machine Connection Verification

| Parameter | Default Value | Valid Range | Description or Behavior |
|----------------------|---------------|-------------|--|
| 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 <i>x</i> times before refreshing the client IP address. |
| Ping ARP | 0 | 0-2 | <ul style="list-style-type: none"> If this value is set to 0, poll using ICMP. If this value is set to 1, poll using ARP. If this value is set to 2, poll using ICMP first, then (if ICMP fails) use ARP. |
| Max Timeout for Ping | 1 | 1-10 | Poll using ICMP, and if there is no response in <i>x</i> seconds, then declare an ICMP polling failure. |

Table 19-7 Additional SWISS Discovery Customization

| Parameter | Default Value | Valid Range | Description or Behavior |
|-------------------------|---------------|-------------|--|
| Swiss timeout | 1 | 1 and above | <ul style="list-style-type: none"> If this setting is 1, the agent performs SWISS discovery as designed and no additional UDP response packet delay timeout value is introduced. If the setting is an integer greater than 1, the 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. <p>Note SwissTimeout works only for UDP SWISS timeouts.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |
| Disable L3 Swiss Delay? | no | yes or no | <p>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.</p> <p>Note This setting does not apply to Mac OS X client machine agents.</p> |

Table 19-8 HTTP Discovery Customization

| Parameter | Default Value | Valid Range | Description or Behavior |
|------------------------|---------------|----------------|--|
| Http discovery timeout | 30 | 0, 3 and above | <ul style="list-style-type: none"> 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—We recommend that setting this value to 5 secs for Mac OS X client machine agent profiles. <p>If this value is set to 0, then default client machine operating system timeout settings are used.</p> |

Table 19-8 HTTP Discovery Customization (continued)

| Parameter | Default Value | Valid Range | Description or Behavior |
|--------------|---------------|----------------|---|
| 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. 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. If this value is set to 0, then default client machine operating system timeout settings are used. |

Table 19-9 Remediation Timeout Customization

| Parameter | Default Value | Valid Range | Description or Behavior |
|--------------------------|---------------|-------------|---|
| 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 over 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 <i>both</i> . |


Table 19-10 Agent Dialog Behavior on User Logout or Shutdown

| Parameter | Default Value | Valid Range | Description or Behavior |
|---------------------------------------|---------------|-------------|--|
| Enable auto close login screen? | no | yes or no | Allows you to determine whether or not the agent login dialog into 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. |

**Note**

When there are no agent profiles configured to match client provisioning policies, you can use the settings specified in the **Administration > System > Settings > Posture > General Settings** page to perform the same functions. See [Posture General Settings, page 20-10](#) for more information.

Table 19-11 IP Address Behavior Settings for Client Machines

| Parameter | Default Value | Valid Range | Description or Behavior |
|--|---------------|-------------|---|
| Enable agent IP refresh after VLAN change? | no | yes or no | <div>  Caution We do not recommend enabling this option for Windows client machines accessing the network via native Windows, Cisco Secure Services Client, or AnyConnect supplicants. </div> <p>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.</p> <p>Check the “Enable agent IP refresh after VLAN change” parameter to refresh Windows client IP address in both wired and wireless environments for MAB with posture.</p> <p>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.</p> <div> 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 <i>both</i>. </div> |
| 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. |

Creating Native Supplicant Profiles

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.

Prerequisites:

- 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 13-25.
- 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 3300 Series Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

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

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

Figure 19-7 Creating Native Supplicant Profiles

Native Supplicant Profile > New Supplicant Profile

Native Supplicant Profile

* Name:

Description:

* Operating System:

* Connection Type: ☐ Wired ☒ Wireless

* SSID:

Security:

* Allowed Protocol:

▼ Optional Settings

▼ Windows Settings

☐ Automatically use logon name and password (and domain if any)

☒ Enable Fast Reconnect

☐ Enable Quarantine checks

☐ Disconnect if server does not present cryptobinding TLV

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. The available options are ALL, Android, Mac OS X (for Apple Macintosh machines), Apple iOS All (for Apple iPhones and iPads), Windows All, Windows 7 (All), Windows Vista (All), and Windows XP (All).

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
- The wireless Security type: either WPA2 Enterprise or WPA Enterprise

Step 7 Choose the Allowed Protocol for the device profile:

- 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 13-25](#).
- 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.

Step 8 Enable or disable other **Optional Settings** as appropriate for this profile. Available optional settings include Windows, Mac OS X, and iPhone/iPad settings.

Step 9 Click **Submit**.

Next Steps

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network as described in [Hosting Multiple Portals, page 21-48](#).

Deleting Client Provisioning Resources



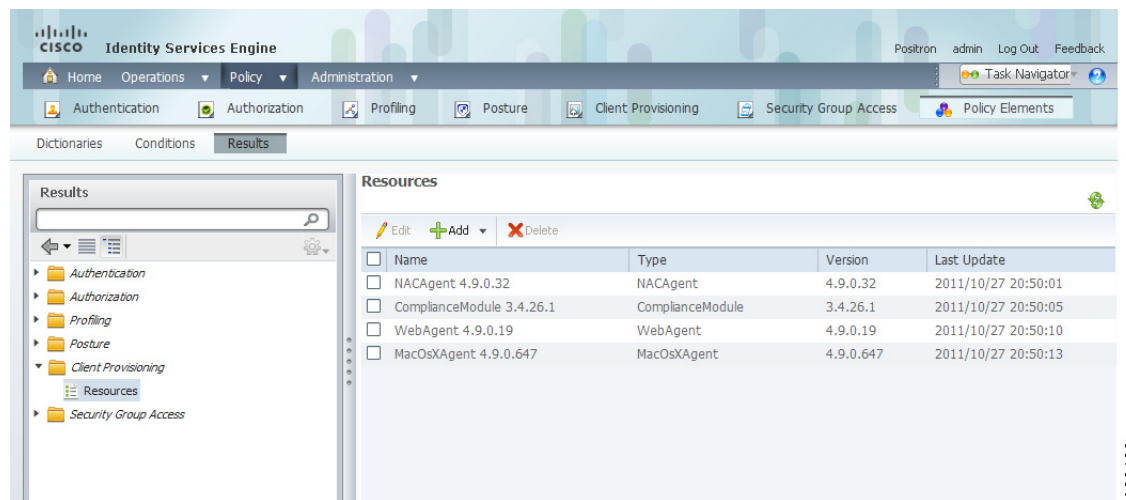
Caution

Before you delete an existing resource from Cisco ISE, ensure that none of your client provisioning resource policies requires that resource.

To remove an existing client provisioning resource from Cisco ISE, complete the following steps:

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

Figure 19-8 Policy > Policy Elements > Results > Client Provisioning > Resources



Step 2 Select one or more existing resources from the client provisioning resources list, and click **Delete**.

Step 3 Confirm that you want to remove the specified resource (or resources) in the confirmation pop-up that appears. The resources that you specify no longer appear in the client provisioning resources list.

Troubleshooting Topics

- [Cannot Download Remote Client Provisioning Resources, page D-10](#)

Provisioning Client Machines with the Cisco NAC Agent MSI Installer

Cisco provides an MSI (Microsoft Installer format) installer for the Cisco NAC Agent (called **nacagentsetup-win.msi**) on Windows client machines. There is also a zip version of the same installer package that uses up less local memory on file transfer. You can download the MSI and/or zip package from the Cisco Software Download Site at <http://www.cisco.com/public/sw-center/index.shtml>. When you have obtained the Cisco NAC Agent MSI or zip package, you can place the MSI installer in a

directory 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://www.cisco.com/public/sw-center/index.shtml>.
- 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. For information on the Agent configuration XML file and its parameters and syntax, see [Creating Windows Agent Profiles in Cisco ISE, page 19-12](#), and [Example XML File Generated Using the Create Profile Function, page 19-14](#).

If you are not connected to 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.

**Note**

The Discovery Host field can be made editable or not by changing the DiscoveryHostEditable parameter in the Agent configuration XML file. See [Agent Profile Parameters and Applicable Values, page 19-16](#), for more details.

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

```
msiexec.exe /i NACAgentSetup-win.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.

The Cisco NAC Agent is installed on the client machine and automatically launches in the background using the Discovery Host supplied in the Agent configuration XML file to contact the Cisco ISE network.

If you are using Altiris/SMS to distribute the MSI installer, perform the following to enforce Agent Customization:

- 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.

Setting Up Global Client Provisioning Functions

- [Enabling and Disabling the Client Provisioning Service, page 19-28](#)
- [Downloading Client Provisioning Resources Automatically, page 19-29](#)
- [Configuring Personal Device Registration Behavior, page 19-30](#)

Enabling and Disabling the Client Provisioning Service

Prerequisites

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 as described in [Specifying Proxy Settings in Cisco ISE, page 8-17](#).

To configure Cisco ISE to automatically discover and download client provisioning resources, complete the following steps:

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

Figure 19-9 Administration > System > Settings > Client Provisioning

The screenshot shows the 'Client Provisioning' configuration page. It contains the following settings:

- * Enable Provisioning: **Enable** (dropdown menu)
- * Enable Automatic Download: **Disable** (dropdown menu)
- * Update Feed URL: **https://www.cisco.com/web/secure/pmbu/provisioning** (text field)
- * Native Supplicant Provisioning Policy Unavailable: **Allow Network Access** (dropdown menu)

At the bottom left, there are **Save** and **Reset** buttons. A vertical label '300424' is visible on the right side of the form.

- 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.

Next Steps

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

- [Adding and Removing Agents and Other Resources, page 19-3](#)

- [Configuring Client Provisioning Resource Policies, page 19-31](#)

Troubleshooting Topics

- [Cannot Download Remote Client Provisioning Resources, page D-10](#)

Downloading Client Provisioning Resources Automatically



Note

We recommend that you manually upload resources whenever possible according to the guidelines in [Adding Client Provisioning Resources to Cisco ISE, page 19-5](#), rather than opting to upload them automatically. This function automatically uploads *all* available software from Cisco, many items of which may not be pertinent to your deployment.

Prerequisites

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 as described in [Specifying Proxy Settings in Cisco ISE, page 8-17](#).

To configure Cisco ISE to automatically discover and download all known available client provisioning resources, complete the following steps:

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

Figure 19-10 Administration > System > Settings > Client Provisioning

The screenshot shows the 'Client Provisioning' configuration page. It contains the following settings:

- * Enable Provisioning: **Enable** (dropdown menu)
- * Enable Automatic Download: **Disable** (dropdown menu)
- * Update Feed URL: **https://www.cisco.com/web/secure/pmbu/provisioning** (text box)
- * Native Supplcant Provisioning Policy Unavailable: **Allow Network Access** (dropdown menu)

At the bottom left, there are 'Save' and 'Reset' buttons. A small '300464' is visible in the bottom right corner of the form area.

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

- Step 3** When enabling automatic downloads, be sure to specify the URL where Cisco ISE searches for system updates in the Update Feed URL text box. The default URL for downloading client provisioning resources is <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml>.

If you choose not to use the Enable Automatic Download function, you can manually download the client provisioning resource files to a local system before importing them into Cisco ISE via the guidelines described in [Adding Client Provisioning Resources from a Local Machine, page 19-6](#).

- Step 4** Click **Save**. Cisco ISE automatically checks for updated resources every 24 hours, based on the time Cisco ISE was first installed.

Next Steps

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

- [Adding and Removing Agents and Other Resources](#), page 19-3
- [Configuring Client Provisioning Resource Policies](#), page 19-31

Troubleshooting Topics

- [Cannot Download Remote Client Provisioning Resources](#), page D-10

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. For more information on the supported user login methods via a personal device, see [Accessing the Network and Registering Personal Devices](#), page 19-39.

To configure Cisco ISE to manage login sessions where users access the network via personal devices on which no supplicant provisioning wizard may be installed or launched:

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

Figure 19-11 Administration > System > Settings > Client Provisioning

Client Provisioning

* Enable Provisioning:

* Enable Automatic Download: ⓘ

* Update Feed URL: ⓘ

* Native Supplicant Provisioning Policy Unavailable:

300424

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. See [Logging In Without Supplicant Provisioning](#), page 19-47 for more information.
- **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 in described in [Adding a Custom Sponsor Language Template](#), page 21-36 and [Adding a Custom Guest Language Template](#), page 21-45.

Step 3 Click **Save**.

Next Steps

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network as described in [Hosting Multiple Portals](#), page 21-48.

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.

Prerequisites

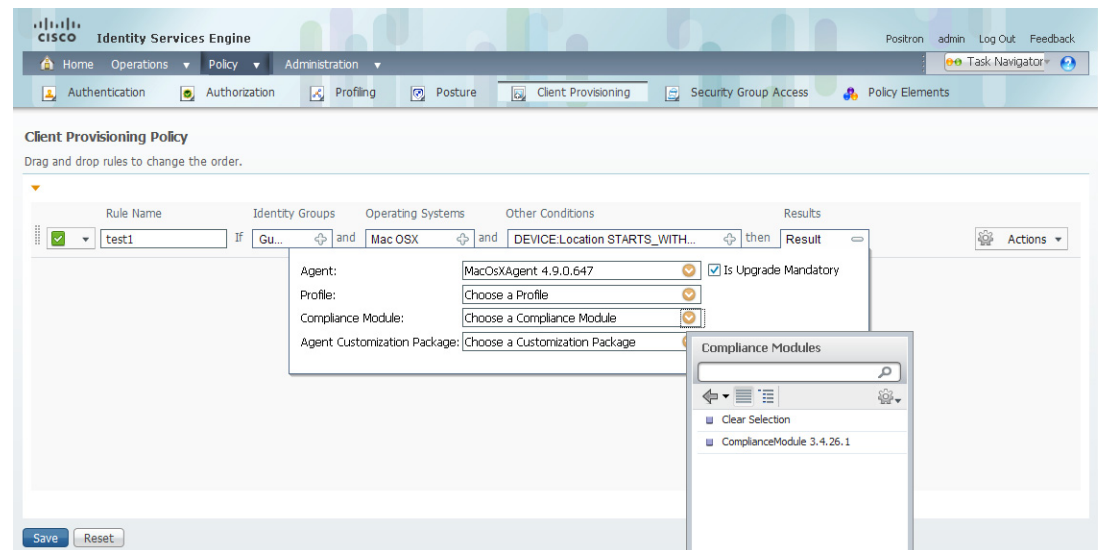
Before you can create effective client provisioning resource policies, ensure that you have set up system-wide client provisioning functions according to the following topics:

- [Specifying Proxy Settings in Cisco ISE](#), page 8-17.
- [Setting Up Global Client Provisioning Functions](#), page 19-28
- [Adding and Removing Agents and Other Resources](#), page 19-3

To configure a client provisioning resource policy, complete the following steps:

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

Figure 19-12 Policy > Client Provisioning



Enable or Disable the Resource Policy

Step 2 Choose **Enable**, **Disable**, or **Monitor** from the behavior drop-down list. This list contains a green check mark:

- **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.

Define the Resource Policy

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

Categorize the Client Machine or Device

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 (for example, “Guest,” sponsor-created, or administrator-created groups) at [Configuring User Identity Groups, page 4-41](#).

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” (for iPhones/iPads), 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).” For a complete list of supported client machine operating systems, see [Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x](#).

Step 6 In the Other Conditions field, specify a new expression that you want to create for this particular resource policy. When you develop a new condition for this resource policy, specify the components of the new expression for this resource policy per the guidelines outlined in [Dictionary and Attribute User Interface, page 7-2](#).

Define Which Resources to Distribute to Windows and Mac OS X Client Machines

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.

- 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.

- Choose an existing agent profile from the **Profile** drop-down list.
- Choose an available compliance module to download to the client machine using the **Compliance Module** drop-down list.



Note

Starting from Compliance Module version 3.5.2101.2, a new fallback detection mechanism using Windows Security Center has been included. This provides new capabilities for detecting the AV/AS products that are not yet supported by the current Compliance Module. This feature allows you to perform installation verification for the AV/AS products on the endpoint that are yet to be supported by the Compliance Module.

From Compliance Module version 3.5.2101.2, the AV SDK and AS SDK contain an additional product

that represents the Windows Security Center fallback detection name, which is available at the bottom of each vendor list as “Other Vendor AV/AS product.” For example, refer to [Cisco NAC Appliance Supported Windows AV/AS Products Compliance Module Version 3.5.2101.2](#).

If a particular version of a AV/AS is unsupported, the administrator can choose to configure the installation check for “Other Vendor AV/AS product.”

- d. Choose an available agent customization package for the client machine from the **Agent Customization Package** 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 [Adding Client Provisioning Resources to Cisco ISE](#), page 19-5.

Define Which Resources to Distribute to Personal Devices (Androids or iPhones/iPads)

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**.

Next Steps

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 according to the topics in [Chapter 20, “Configuring Client Posture Policies.”](#)

Client-side Agent Installation and Login—Cisco NAC Agent

When users first log into a network that is managed by Cisco ISE and requires access via an agent, they are prompted to install temporal or persistent agents (as well as possible associated client provisioning resources) on the client machine to facilitate network access, client posture assessment, and other Cisco ISE network services.

To download agents and other client provisioning resources, users must have administrator privileges on their client machines and the browser session through which they are attempting to log into Cisco ISE. In addition, to successfully install the agent, users will likely need to explicitly accept ActiveX or Java applet installer functions.

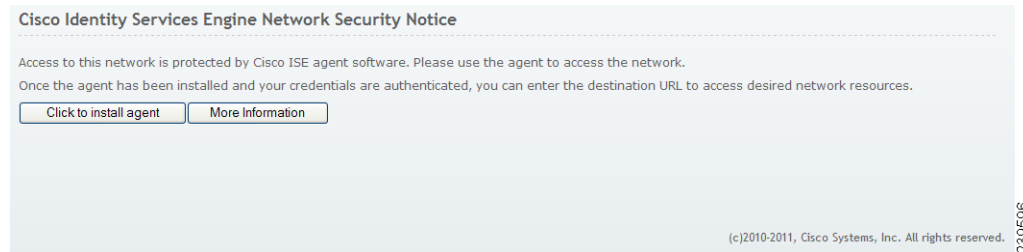
**Note**

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.

Once the browser session from that client machine reaches the specified access portal, Cisco ISE prompts the user to download and install a persistent agent (like the Cisco NAC Agent or Mac OS X Agent) or temporal agent (like the Cisco NAC Web Agent).

Figure 19-13 shows a Cisco ISE welcome screen, prompting the user to download and install the Cisco NAC Agent on the client machine.

Figure 19-13 Cisco ISE Agent Download and Installation



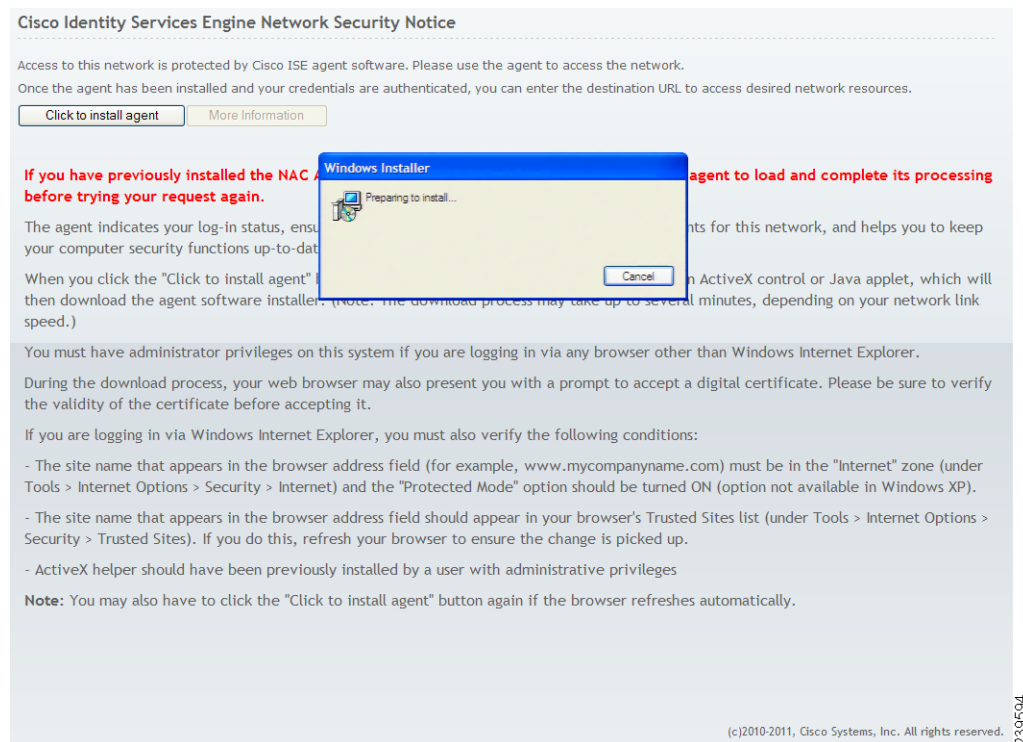
Note

During Cisco ISE hardware and software installation, you can test network connectivity from remote client machines. You can perform this test by launching a browser window on a test client machine that is connected to the user access part of your Cisco ISE network and navigating to a dummy IP address like <https://a.b.c.d>. For detailed information on testing Cisco ISE installation, see the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x](#).

Once the user validates and accepts any certificate (or certificates) required to facilitate agent download and installation on the client machine, the ActiveX or Java applet installer process launches and provisions the agent installation package on the client machine.

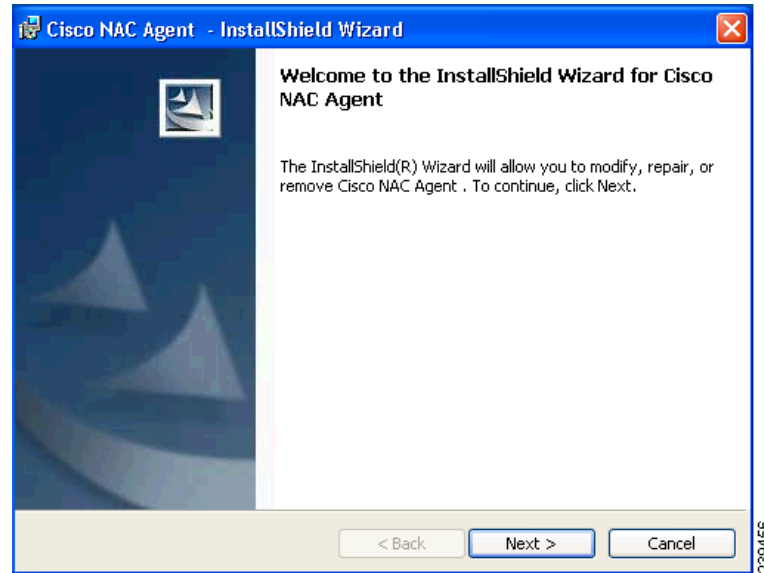
Figure 19-14 shows an example of the user Cisco ISE browser session when the agent installation files have been downloaded, and the installer is preparing to install the Cisco NAC Agent application files on the client machine.

Figure 19-14 Preparing to Install Cisco NAC Agent



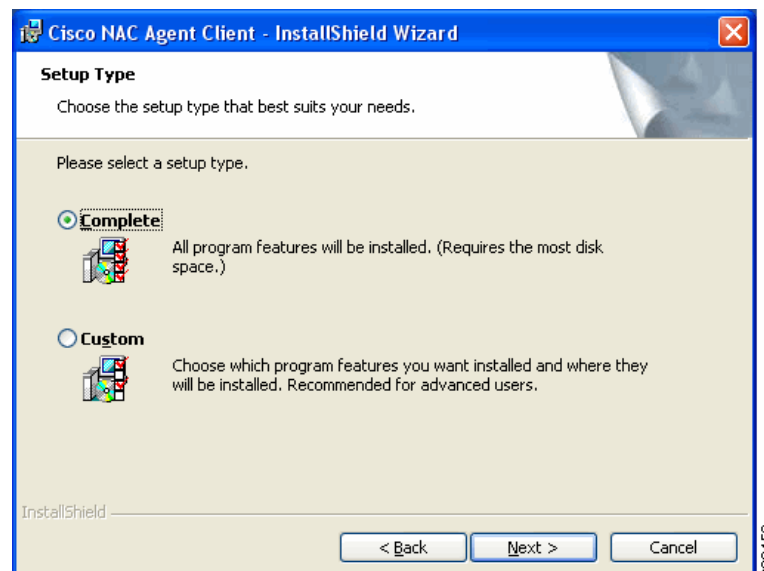
The agent **InstallShield Wizard** screen appears (Figure 19-15).

Figure 19-15 Cisco NAC Agent InstallShield Wizard—Welcome

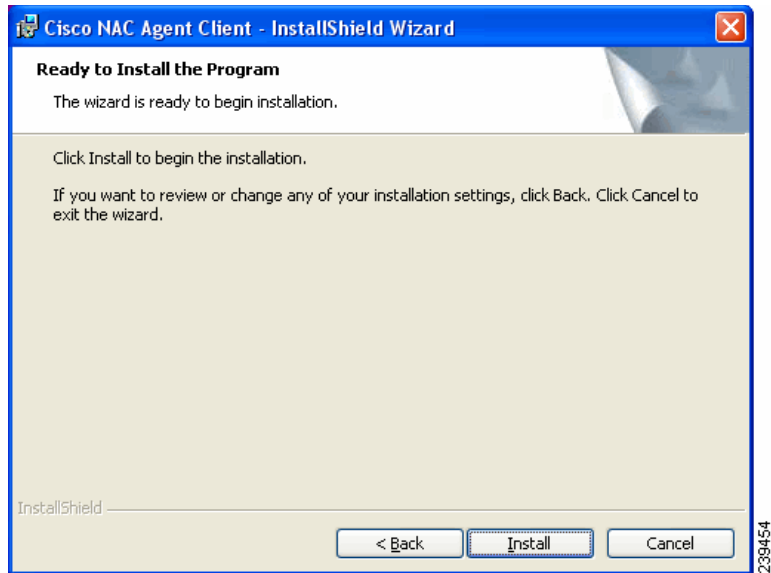


The user has the option to install the complete collection of agent files or specify one or more items by selecting **Custom** and clicking **Next** (Figure 19-16).

Figure 19-16 Cisco NAC Agent Installation—Setup Type



The agent **InstallShield Wizard** screen appears (Figure 19-17).

Figure 19-17 Cisco NAC Agent InstallShield Wizard—Ready to Install

The setup wizard prompts the user through the short installation steps to install the agent to the C:\Program Files\Cisco\Cisco NAC Agent directory on the client machine.

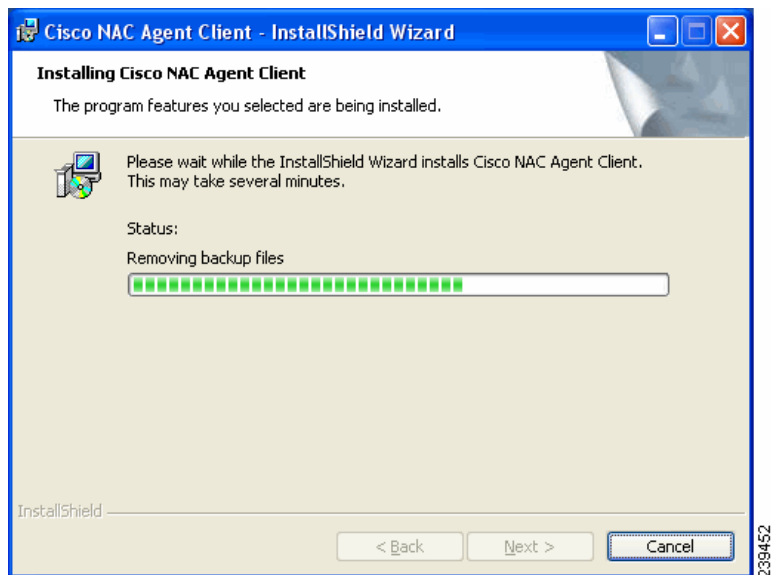
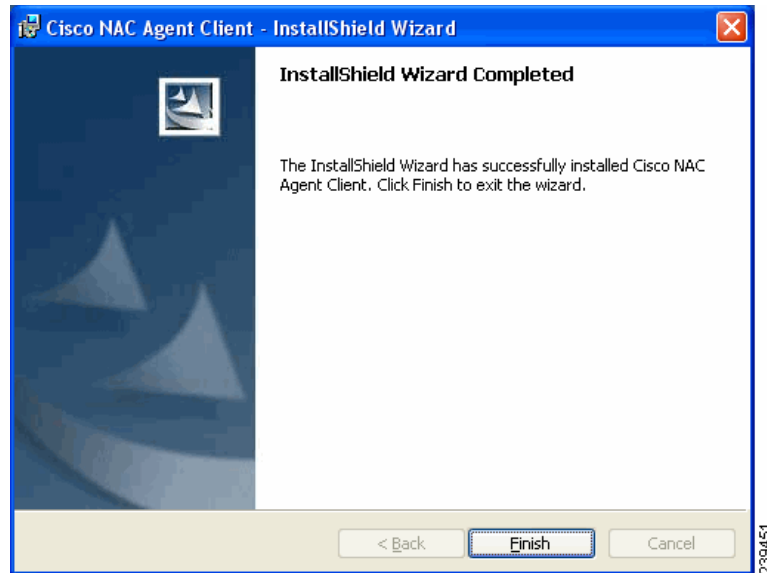
Figure 19-18 Cisco NAC Agent Installation In Progress

Figure 19-19 Cisco NAC Agent Installation Complete

When the InstallShield Wizard completes and the user clicks **Finish**, the agent automatically transmits the native operating system login credentials of the user to Cisco ISE for authentication and access to the internal network.

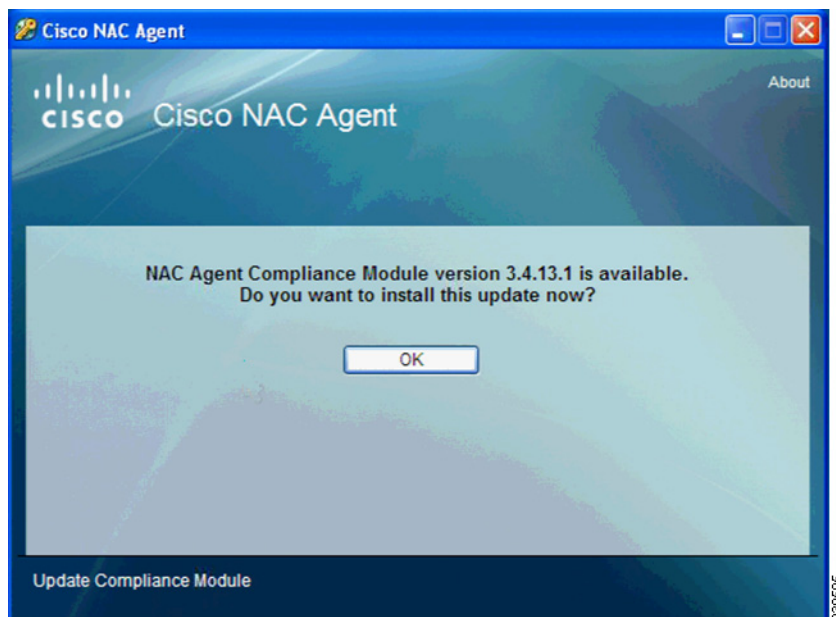
**Note**

The server certificate on the client helps to ensure that the client machine can perform DNS resolution, allowing services like Cisco ISE client provisioning and posture assessment. If you change the Cisco ISE domain name (by logging into the Cisco ISE CLI and manually specifying a new domain name, for example), you must generate a new server certificate to reflect the same domain name change.

If you have associated any posture assessment or profiling policies with the user role to which the user in question is assigned, those services initiate at this time. Users accessing the network via Cisco ISE (except for registered “guests”) must also agree to the Acceptable Use Policy each time they log in. Additionally, these other client provisioning resources that you may have specified for the user role are now downloaded to the client machine to help facilitate network access:

- Agent profiles
- Agent compliance modules
- Agent customization packages

Figure 19-20 displays an example of an agent compliance module update (which is always mandatory) at the time of agent installation on the client machine.

Figure 19-20 Cisco NAC Agent—Updating Agent Compliance Module

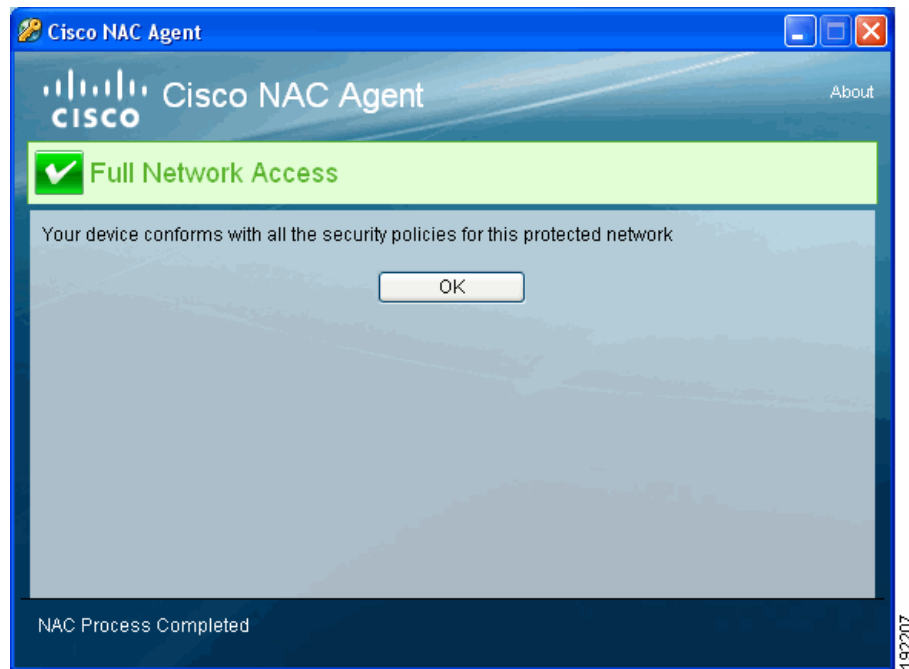
If you have not enabled the Is Upgrade Mandatory setting in the client provisioning resource policy, then the agent upgrade dialog displays a Cancel button as well as the **OK** button. This allows end users the option to cancel an agent upgrade if a more current version is available.

For details, see [Configuring Client Provisioning Resource Policies, page 19-31](#).

Following successful agent installation, client posture assessment, and remediation, the agent notifies the user that their login session is complete and that they are granted access to the network based on the assigned user role.

**Note**

If the agent is not able to reach the primary Discovery Host address configured in the associated client provisioning policy (after attempting to connect per the number of retries configured in the agent profile), the agent automatically tries the Discovery Host address received from the access switch via URL redirection to successfully connect to the network.



Accessing the Network and Registering Personal Devices

There are two paths users with personal devices can follow to log in and register their devices on the Cisco ISE network:

- [Logging In Via Standard Native Supplicant Provisioning, page 19-39](#)
- [Logging In Without Supplicant Provisioning, page 19-47](#)

Logging In Via Standard Native Supplicant Provisioning

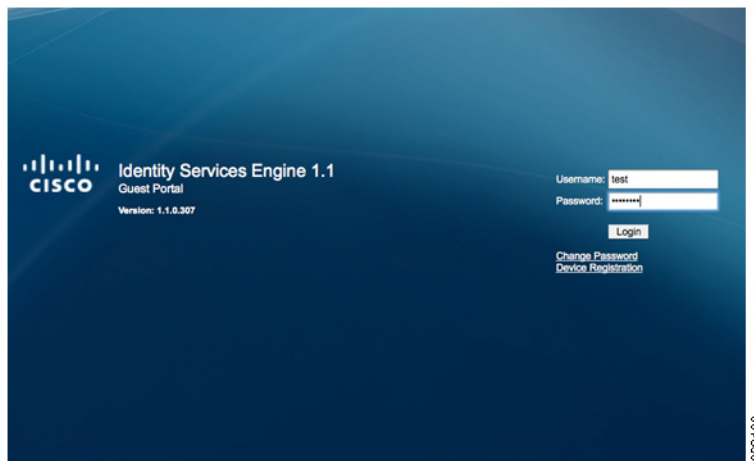
1. Users with a supported device access the network and are redirected to the Cisco ISE Guest portal where they are asked to enter their network access credentials (unless the network access session is authenticated via PEAP where those same credentials are passed automatically).
2. Users then reach a registration page where the device ID (MAC address) is automatically determined and the user is asked to enter an optional device description. At this point users may choose to cancel or submit their registration.
 - Submitting the registration information registers the device and launches the appropriate Supplicant Provisioning Wizard which ensures that the device then has correct credentials and supplicant profiles required to access the protected network.
 - Choosing to cancel the registration process terminates the login session and the device is not registered with Cisco ISE. (Subsequent attempts to access the network with the same device result in the user encountering the Cisco ISE Guest portal redirection process described above.)
3. For supported devices, the result of this process changes the device's "active" network to the protected network and the device state switches to "Registered" in the Cisco ISE database.

- For unsupported devices, the result of this process changes the device's "active" network to the protected network and the device state switches to "Registered" in the Cisco ISE database (just as for supported devices), but Cisco ISE also issues a change of authorization (CoA) event to force the device to reauthenticate with the protected network before access is granted.

For examples of supported device login and registration flows, see [Chapter 22, "Device Access Management."](#)

When Android or iPhone/iPad users attempt to access the network, they are automatically presented with the existing Guest Registration portal to enter their user credentials.

Figure 19-21 *User Accesses the Cisco ISE Network with Personal Device*

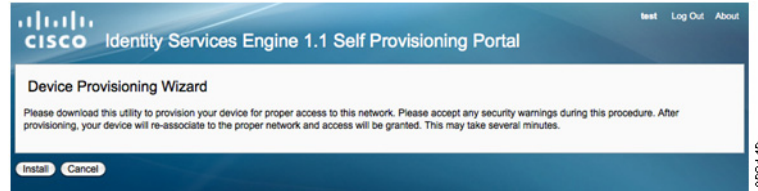


If the device is not yet registered on the network, Cisco ISE directs the device session to the self-registration portal, where the user is asked to specify information about the device.

Figure 19-22 *User Specifies Device Registration Information*



Based on the profile to which the user has been assigned and the authentication methods that are configured for that profile (see [Creating Native Supplicant Profiles](#), page 19-24 for more configuration guidelines), Cisco ISE asks the user to install the appropriate native supplicant setup wizard for the device.

Figure 19-23 User Installs Native Supplicant Wizard on Personal Device

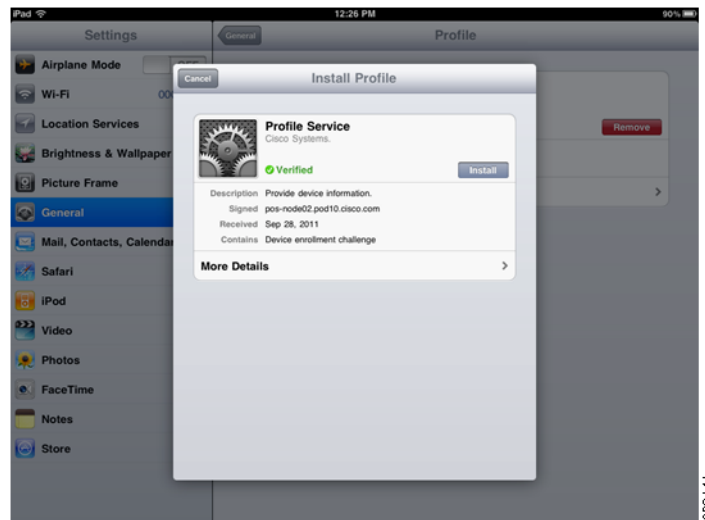
Upon installation, users are able to access the network using their personal devices. The two main native supplicants that are supported in Cisco ISE are the iPhone/iPad and Android supplicants:

- [Accessing the Network with an iPhone or iPad, page 19-41](#)
- [Accessing the Network with an Android Device, page 19-44](#)

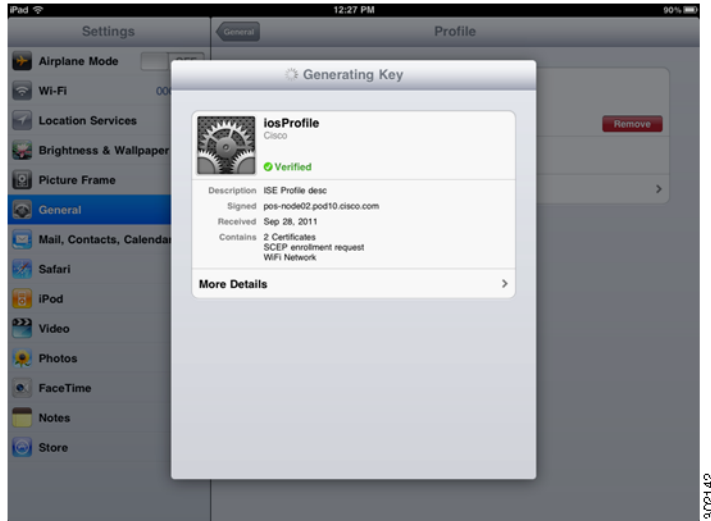
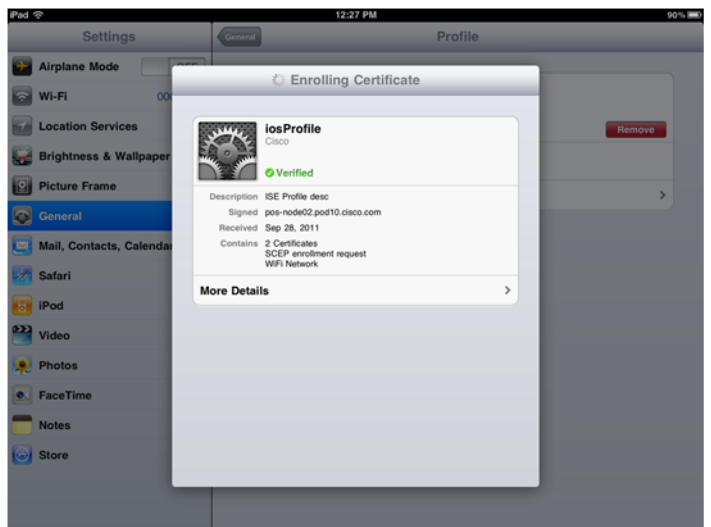
Accessing the Network with an iPhone or iPad

The iPhone/iPad users are presented with a prompt to install the wizard that will take them through the negotiation and registration process.

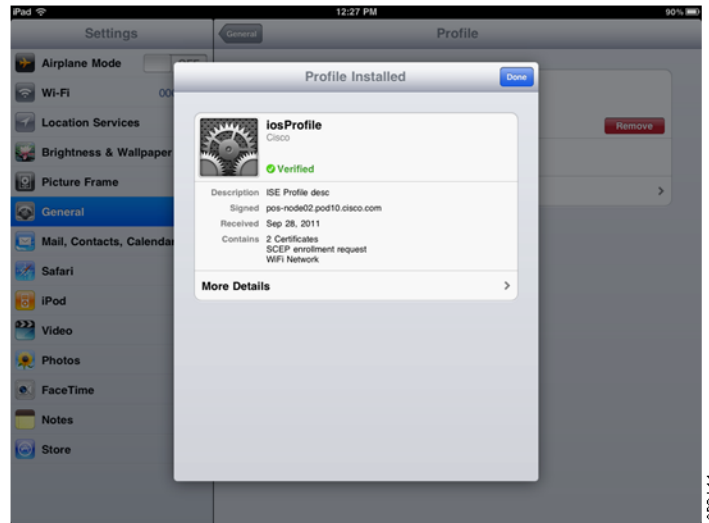
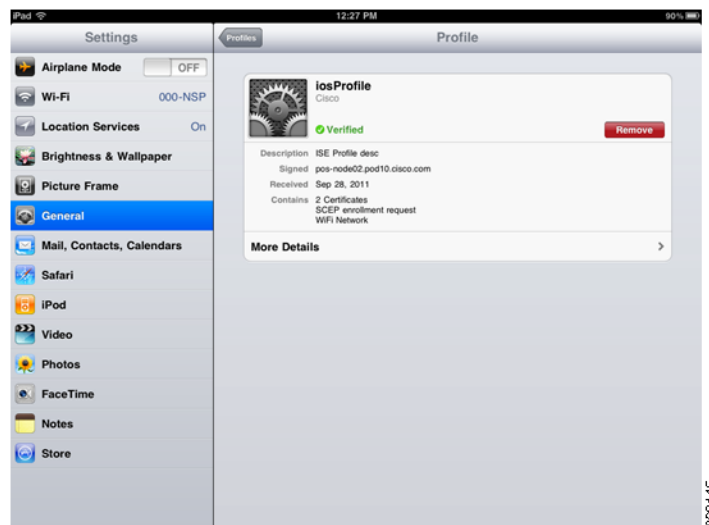
If users try to access the network and register an iPhone or iPad device running iOS version 4.0 or earlier where only a Single SSID is employed for access, you must then ensure that, after users register the iOS device, you present users with a custom message explaining that users must manually set the profile and connect to the network, according to the guidelines described in [Adding a Custom Sponsor Language Template, page 21-36](#) and [Adding a Custom Guest Language Template, page 21-45](#).

Figure 19-24 iPhone/iPad User Installs the Wizard

The wizard generates authentication keys and initiates an SCEP request for the device certificate.

Figure 19-25 *iPhone/iPad Key Generation***Figure 19-26** *iPhone/iPad SCEP Certificate Enrollment*

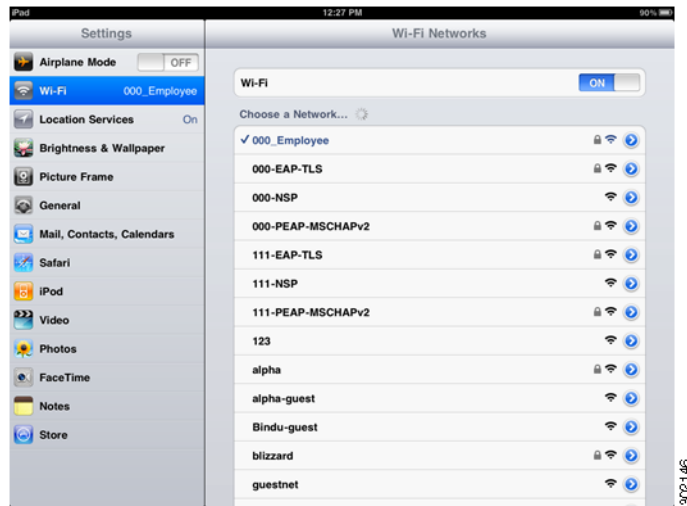
The wizard completes the registration and enrollment process and connects the iPhone/iPad to the Cisco ISE-managed network.

Figure 19-27 *Installation and Registration Complete***Figure 19-28** *Installation Verified*

After profile installation, an on-screen message instructs the user to navigate to the original network address location where they can then join the network.

**Note**

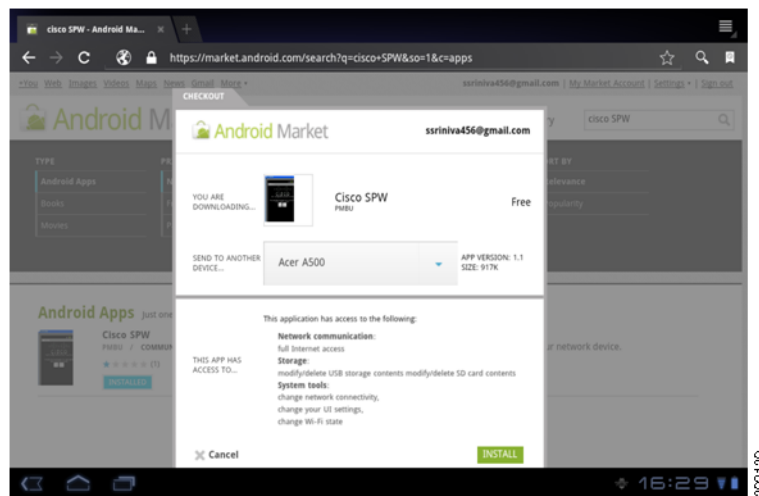
If the network in question is hidden/closed to general user access (that is, if it does not appear in the list of known local available networks), the user may have to manually enter the specified network name in order to connect to the network as instructed by the iOS messages that are presented.

Figure 19-29 *iPhone/iPad Connected to the Network*

Accessing the Network with an Android Device

In order for users to access the Cisco ISE network via an Android personal device, users must navigate to the Android App Store and download the installation app for the Cisco Setup Assistant.

The Android users are presented with a prompt to install the wizard from the App Store, which takes them through the negotiation and registration process.

Figure 19-30 *Install Android Provisioning Wizard from App Store*

The user then launches the wizard app on the Android device, and the wizard connects to Cisco ISE to get the appropriate access profile for the user.

Figure 19-31 Setup Wizard Starts the Provisioning Process



The wizard generates authentication keys and initiates a certificate request (if required) for the device certificate.

Figure 19-32 User Password Required for Authentication Key Configuration

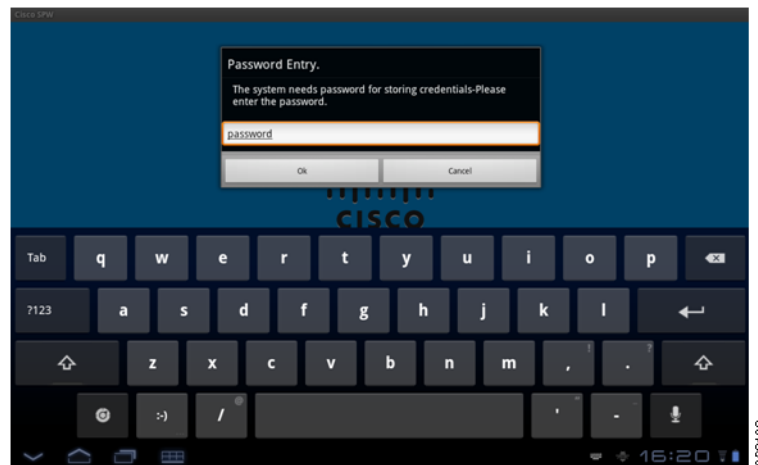


Figure 19-33 Certificate Request Process



Figure 19-34 User Names the Certificate

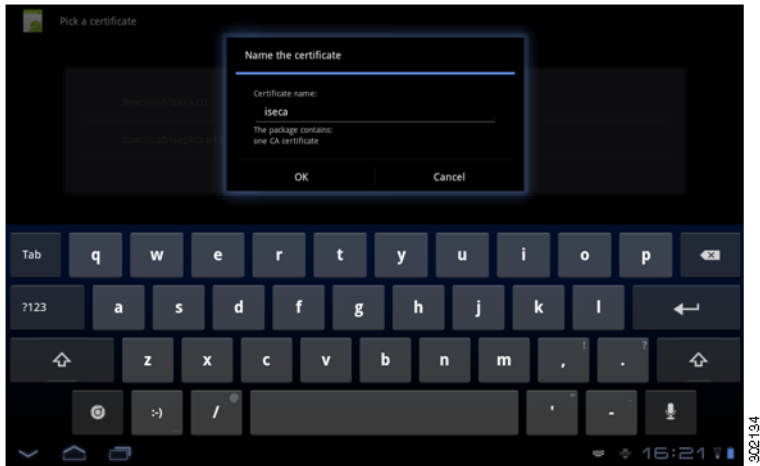
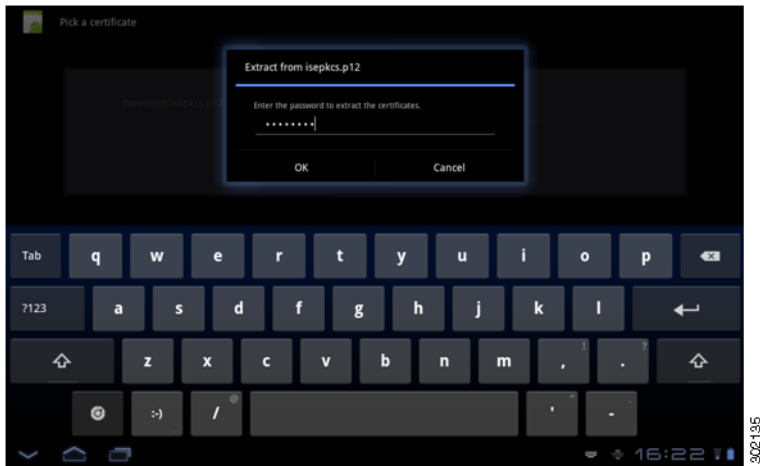


Figure 19-35 User Extracts the Certificate



Once the certificate authenticates the device, the user is able to connect the Android device to the network.

Figure 19-36 *Android Device Connects to the Network*

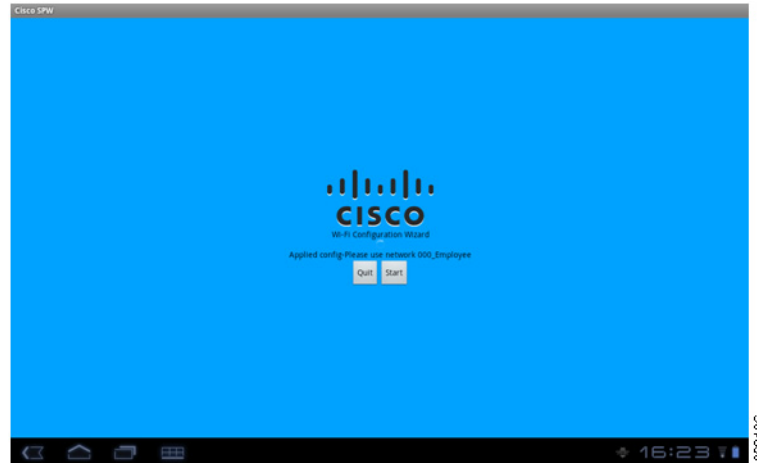
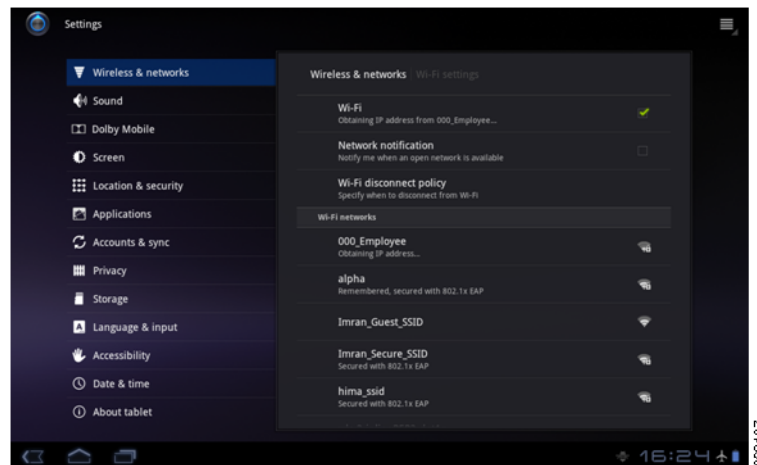


Figure 19-37 *Network Connection Verified*



Note

If the user “forgets” the secure network on their Android device, they must go through the setup process again to reconnect to the network.

Logging In Without Supplicant Provisioning

1. Users with a supported device access the network and are redirected to the Cisco ISE Guest portal where they are asked to enter their network access credentials (unless the network access session is authenticated via PEAP where those same credentials are passed automatically).
2. Users then reach a registration page where the device ID (MAC address) is automatically determined and the user is asked to enter an optional device description. At this point users may choose to cancel or submit their registration.

- Users will be able to submit registration information as long as you have enabled the “Allow network access” option in [Configuring Personal Device Registration Behavior, page 19-30](#).
 - Choosing to cancel the registration process terminates the login session and the device is not registered with Cisco ISE. (Subsequent attempts to access the network with the same device result in the user encountering the Cisco ISE Guest portal redirection process described above.)
3. The result of this process changes the device’s “active” network to the protected network and the device state switches to “Registered” in the Cisco ISE database (just as for supported devices), but Cisco ISE also issues a change of authorization (CoA) event to force the device to re-authenticate with the protected network before access is granted.

**Note**

Only the self-provisioning and native supplicant provisioning (NSP) are capable of extracting the device MAC address while registering your personal devices.

Viewing Client Provisioning Reports and Events

- [Viewing Client Provisioning Reports in Cisco ISE, page 19-48](#)
- [Viewing Client Provisioning Event Logs in Cisco ISE, page 19-53](#)

Viewing Client Provisioning Reports in Cisco ISE

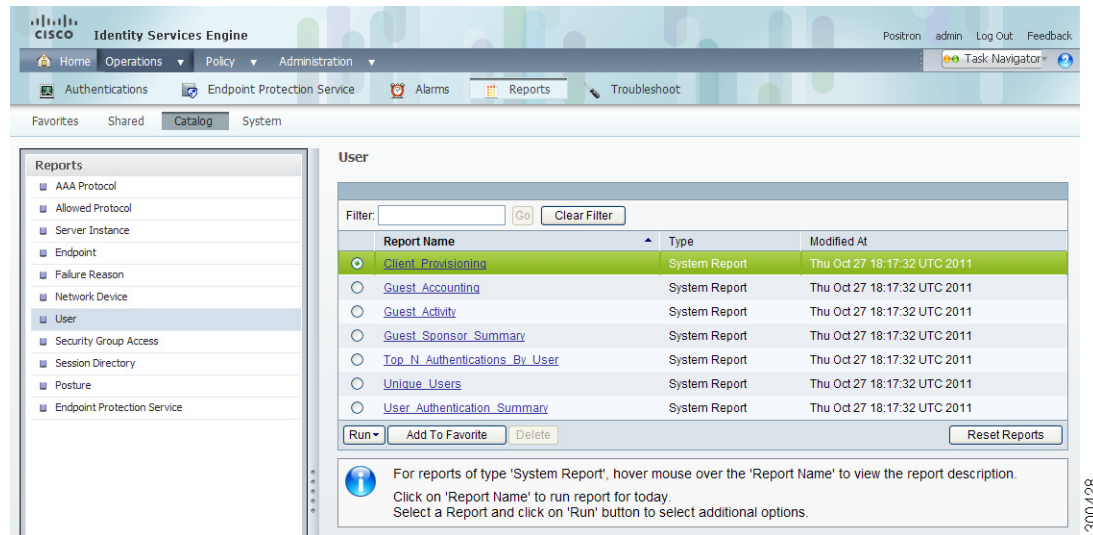
As a network administrator, you may need to access the Cisco ISE monitoring and troubleshooting functions to check on overall trends for successful or unsuccessful user login sessions, gather statistics about the number and types of client machines logging into the network during a specified time period,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

The following examples provide a couple of common scenarios, however you should see [Chapter 24, “Monitoring and Troubleshooting”](#) for more details on using the Cisco ISE monitoring and troubleshooting capabilities to maximize the tools within your network deployment.

Client Provisioning Requests

The **Operations > Reports > Catalog > User > Client Provisioning** page displays statistics about successful and unsuccessful client provisioning requests (Figure 19-38).

Figure 19-38 *Operations > Reports > Catalog > User > Client Provisioning*



When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data (Figure 19-39).

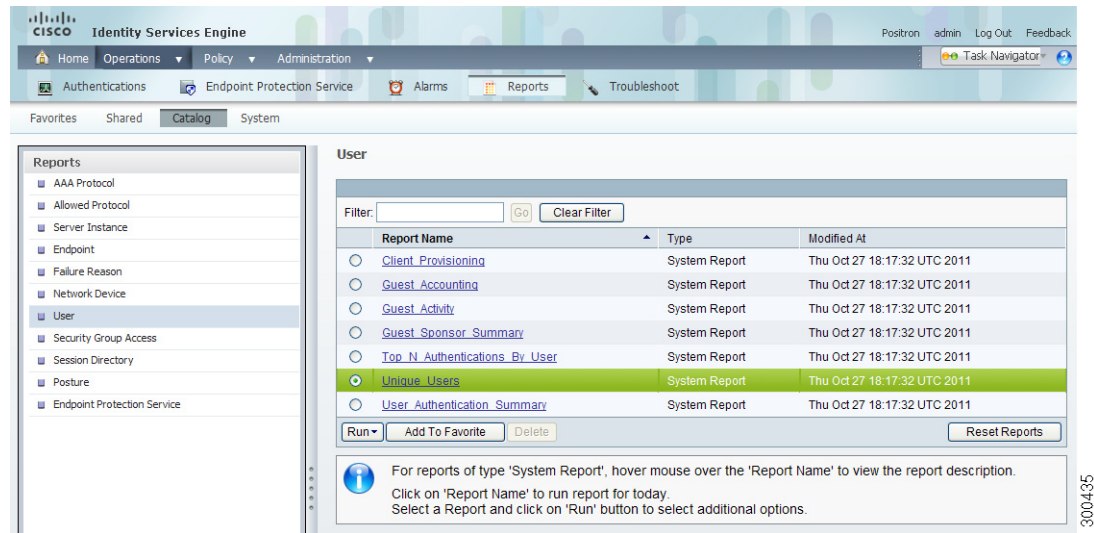
Figure 19-39 *Client Provisioning Report Results*

| Launch Interactive Viewer | | | | | | |
|---|-------------|------------|---------|---------|-----------------------|----------------|
| Showing Page 1 of 3 First Prev Next Last Goto Page: Go | | | | | | |
| User > Client Provisioning | | | | | | |
| Time Range : March 21,2011 - March 27,2011 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days) | | | | | | |
| Generated on March 28, 2011 5:14:56 PM UTC | | | | | | |
| User | MAC Address | IP Address | Success | Failure | Provisioning Disabled | Server |
| CISCO\ma | F0:DE:F1:0E | 10.34. | Q | Q | Q | npf-sjca-pdp01 |
| CISCO\ms | 00:24:D7:0E | | Q | Q | Q | npf-sjca-pdp02 |
| CISCO\pn | 00:24:D7:26 | | Q | Q | Q | npf-sjca-pdp02 |
| CISCO\va | F0:DE:F1:03 | 10.34. | Q | Q | Q | npf-sjca-pdp01 |
| CISCO\ti | 00:1C:25:BA | 10.34. | Q | Q | Q | npf-sjca-pdp01 |
| N/A | 00:1D:72:84 | 10.35 | Q | Q | Q | npf-sjca-pdp01 |
| N/A | 00:1D:72:84 | 10.35 | Q | Q | Q | npf-sjca-pdp01 |
| N/A | 00:1D:72:84 | 10.35 | Q | Q | Q | npf-sjca-pdp01 |

Client Access Sessions

The **Operations > Reports > Catalog > User > Unique Users** page displays statistics about known specific client access sessions initiated during the specified time period (Figure 19-40).

Figure 19-40 Operations > Reports > Catalog > User > Unique Users



When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data (Figure 19-41).

Figure 19-41 Unique Users Report Results

| Launch Interactive Viewer | | | | | |
|---|--------------|--------|--------|---------------|--|
| Showing Page 1 of 3 First Prev Next Last Goto Page: <input type="text"/> Go | | | | | |
| User > Unique Users | | | | | |
| Time Range : March 21, 2011 - March 27, 2011 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days) | | | | | |
| Generated on March 28, 2011 4:54:08 PM UTC | | | | | |
| User | Total Logins | Passed | Failed | Pass-Fail Bar | |
| CISCOvma | 19 | 19 | 0 | <div></div> | |
| CISCOvms | 71 | 70 | 1 | <div></div> | |
| CISCOpn | 49 | 48 | 1 | <div></div> | |
| CISCOva | 63 | 63 | 0 | <div></div> | |
| CISCOvi | 1 | 1 | 0 | <div></div> | |
| CISCOti | 2 | 2 | 0 | <div></div> | |
| CISCOtk | 4 | 4 | 0 | <div></div> | |
| SA | 19 | 19 | 0 | <div></div> | |
| aa | 4 | 4 | 0 | <div></div> | |
| ab | 122 | 121 | 1 | <div></div> | |
| ae | 2 | 2 | 0 | <div></div> | |

Client Provisioning Resource Configuration Changes

The **Operations > Reports > Catalog > Server Instance > Server Configuration Audit** page displays information about recent client provisioning resource configuration changes (Figure 19-42).

Figure 19-42 *Operations > Reports > Catalog > Server Instance > Server Configuration Audit*

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Reports' tab is active, showing a list of reports under the 'Server Instance' category. The 'Server Configuration Audit' report is selected and highlighted in green. The interface includes a left-hand navigation pane with 'Reports' and 'Catalog' tabs, and a main content area displaying a list of reports with columns for 'Report Name', 'Type', and 'Modified At'.

| Report Name | Type | Modified At |
|---|---------------|------------------------------|
| OCSP_Monitoring | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_Administrator_Entitlement | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_Administrator_Logins | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_Authentication_Summary | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_Configuration_Audit | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_Health_Summary | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_Operations_Audit | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Server_System_Diagnostics | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| Top_N_Authentications_By_Server | System Report | Thu Oct 27 18:17:32 UTC 2011 |
| User_Change_Password_Audit | System Report | Thu Oct 27 18:17:32 UTC 2011 |

Buttons: Run, Add To Favorite, Delete, Reset Reports

For reports of type 'System Report', hover mouse over the 'Report Name' to view the report description. Click on 'Report Name' to run report for today. Select a Report and click on 'Run' button to select additional options.

Choosing Run and specifying one of the preset time periods displays any configuration changes to client provisioning resources in Cisco ISE (for example, a newly uploaded agent version) within the time period specified (Figure 19-43).

Figure 19-43 *Server Configuration Audit Report Results*

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Reports' tab is active, showing a list of reports under the 'Server Instance' category. The 'Server Configuration Audit' report is selected, and the 'Launch Interactive Viewer' button is visible. The report results are displayed in a table with columns for 'Logged At', 'Administrator', 'Interface', 'Object Type', 'Object Name', 'Event', and 'Server'.

| Logged At | Administrator | Interface | Object Type | Object Name | Event | Server |
|---------------------------------|---------------|-----------|------------------------------|---|---------------------|--------|
| October 27, 2011 8:50:14.896 PM | admin | GUI | Client Provisioning Resource | MacOsXAgent 4.9.0.647 (downloaded from remote server) | Added configuration | All |
| October 27, 2011 8:50:12.152 PM | admin | GUI | Client Provisioning Resource | WebAgent 4.9.0.19 (downloaded from remote server) | Added configuration | All |

Supplicant Provisioning Requests

The **Operations > Reports > Catalog > User > Supplicant Provisioning** window displays information about recent successful and unsuccessful user device registration and supplicant provisioning requests. (Figure 19-44).

Figure 19-44 Operations > Reports > Catalog > User > Supplicant Provisioning

User

Filter:

| Report Name | Type | Modified At |
|---|---------------|------------------------------|
| Client Provisioning | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| Guest Accounting | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| Guest Activity | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| Guest Sponsor Summary | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| Supplicant Provisioning | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| Top N Authentications By User | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| Unique Users | System Report | Thu Apr 19 11:36:02 PDT 2012 |
| User Authentication Summary | System Report | Thu Apr 19 11:36:02 PDT 2012 |

For reports of type 'System Report', hover mouse over the 'Report Name' to view the report description.
Click on 'Report Name' to run report for today.
Select a Report and click on 'Run' button to select additional options.

When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting supplicant provisioning data (Figure 19-45).

Figure 19-45 Supplicant Provisioning Report Results

Launch Interactive Viewer

User > Supplicant Provisioning

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

User > Supplicant Provisioning

Time Range : March 25, 2012 - April 23, 2012 (Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on April 24, 2012 8:12:49 AM PDT

| Logged At | User | IP Address | MAC Address | Server | Profile | Operating System |
|-----------|------|------------|-------------|--------|---------|------------------|
|-----------|------|------------|-------------|--------|---------|------------------|

The Supplicant Provisioning report provides information about a list of endpoints that are registered through the device registration portal for a specific period of time, including data like the Logged In Date and Time, User ID, IP Address, MAC Address, Server, Operating System, SPW Version, Failure Reason (if any), and the Status of the registration.

Viewing Client Provisioning Event Logs in Cisco ISE

During Cisco ISE operation, you may need to 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. See [Chapter 14, “Logging”](#) for more specific information on using the Cisco ISE log compilation capabilities to maximize the tools within your network deployment.

Figure 19-46 Administration > System > Logging > Logging Categories > Posture and Client Provisioning Diagnostics

| Parent Category | Category | Targets | Severity |
|---|---|-----------------------------------|----------|
| AAA Audit | AAA Audit | LogCollector | INFO |
| | Failed Attempts | LogCollector, ProfilerRadiusProbe | INFO |
| | Passed Authentications | LogCollector, ProfilerRadiusProbe | INFO |
| AAA Diagnostics | AAA Diagnostics | LogCollector | WARN |
| | Administrator Authentication and Authoriza... | LogCollector | WARN |
| | Authentication Flow Diagnostics | LogCollector | WARN |
| | Identity Stores Diagnostics | LogCollector | WARN |
| | Policy Diagnostics | LogCollector | WARN |
| | RADIUS Diagnostics | LogCollector | WARN |
| | Guest | LogCollector | WARN |
| Accounting | Accounting | LogCollector | INFO |
| | RADIUS Accounting | LogCollector, ProfilerRadiusProbe | INFO |
| Administrative and Operational Audit | Administrative and Operational Audit | LogCollector | INFO |
| Posture and Client Provisioning Audit | Posture and Client Provisioning Audit | LogCollector | INFO |
| Posture and Client Provisioning Diagnostics | Posture and Client Provisioning Diagnostics | LogCollector | WARN |
| Profiler | Profiler | LogCollector | INFO |
| System Diagnostics | System Diagnostics | LogCollector | WARN |
| | Distributed Management | LogCollector | WARN |
| | Internal Operations Diagnostics | LogCollector | WARN |
| System Statistics | System Statistics | LogCollector | INFO |

