CHAPTER 18

Configuring Client Provisioning Policies

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

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:

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

After Cisco ISE classifies a client machine, it uses client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary.

Cisco ISE Agents

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 web site links to web sites in order 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).**

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.

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.

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.

Note If you require MAC address bypass (MAB) users to authenticate and access the network via an agent, you must configure your access policy to specify the Cisco NAC Web Agent only.

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 1.0.4*.

Adding and Removing Agents and Other Resources

- Viewing and Displaying Client Provisioning Resources, page 18-3
- Adding Client Provisioning Resources to Cisco ISE, page 18-4
- Creating Agent Profiles, page 18-10
- Deleting Client Provisioning Resources, page 18-23

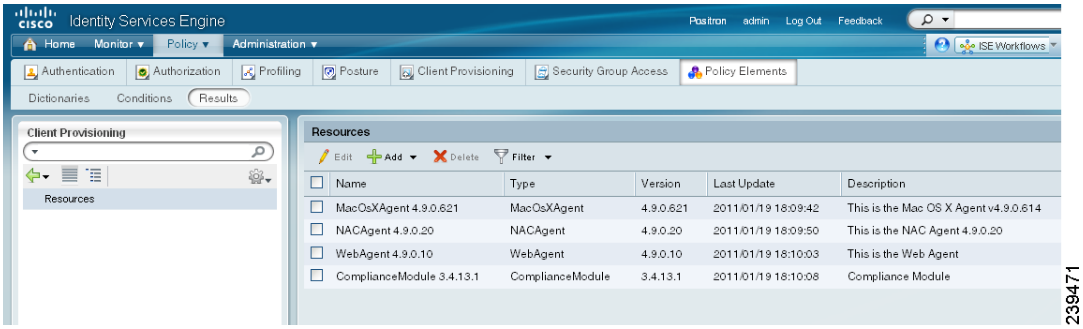
Viewing and Displaying Client Provisioning Resources

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 Client Provisioning Resources List 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
- Agent profiles
- Agent compliance modules
- Agent customization package

Figure 18-1 shows the Client Provisioning Resources List page.

Figure 18-1 Policy > Policy Elements > Results > Client Provisioning > Resources



Resources

□	Name	Type	Version	Last Update	Description
□	MacOsXAgent 4.9.0.621	MacOsXAgent	4.9.0.621	2011/01/19 18:09:42	This is the Mac OS X Agent v4.9.0.614
□	NACAgent 4.9.0.20	NACAgent	4.9.0.20	2011/01/19 18:09:50	This is the NAC Agent 4.9.0.20
□	WebAgent 4.9.0.10	WebAgent	4.9.0.10	2011/01/19 18:10:03	This is the Web Agent
□	ComplianceModule 3.4.13.1	ComplianceModule	3.4.13.1	2011/01/19 18:10:08	Compliance Module

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 18-3.

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 18-1.
- Agent profiles
- Agent compliance modules
- Agent customization package

Note If you require MAC address bypass (MAB) users to authenticate and access the network via an agent, you must configure your access policy to specify the Cisco NAC Web Agent only.

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 18-4
- Adding Client Provisioning Resources from a Local Machine, page 18-5
- Creating Agent Customization Files to Add to Cisco ISE, page 18-6

Note You can also configure Cisco ISE to automatically update client provisioning resources. For details, see Downloading Client Provisioning Resources Automatically, page 18-26.

Adding Client Provisioning Resources from a Remote Source

Prerequisites

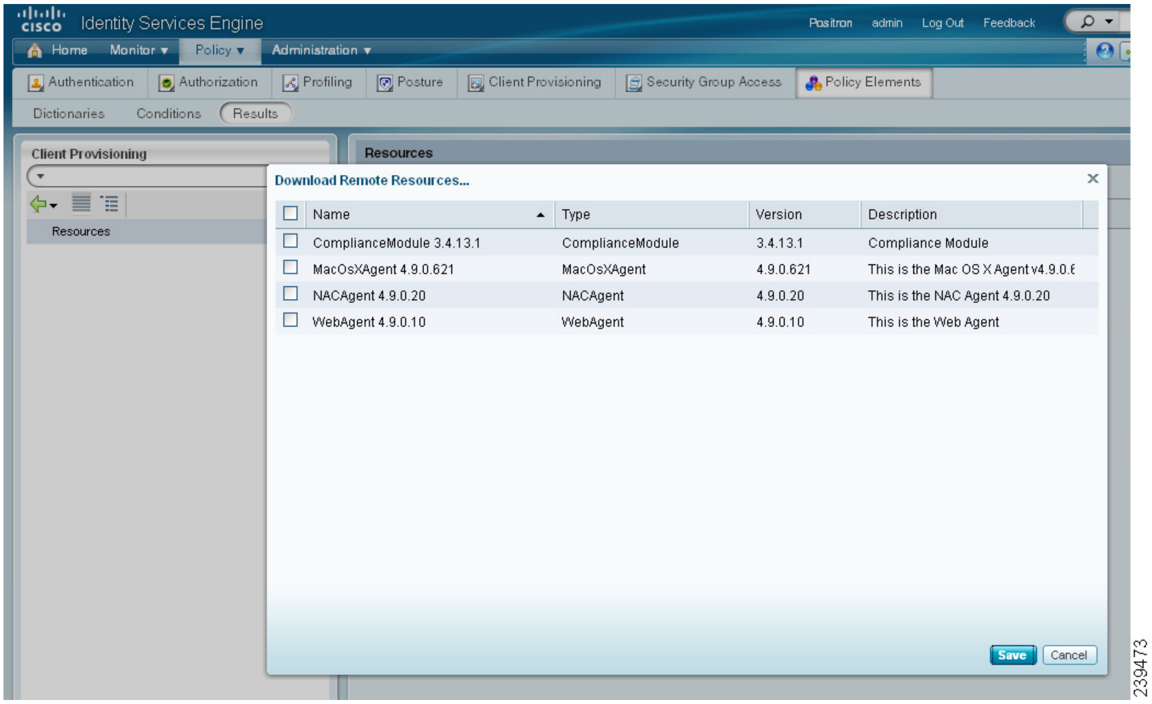
To ensure you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE, you may need to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE, page 18-24.

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 18-2).

Figure 18-2 Add resources from Cisco site



Download Remote Resources...

□	Name	Type	Version	Description
□	ComplianceModule 3.4.13.1	ComplianceModule	3.4.13.1	Compliance Module
□	MacOsXAgent 4.9.0.621	MacOsXAgent	4.9.0.621	This is the Mac OS X Agent v4.9.0.6
□	NACAgent 4.9.0.20	NACAgent	4.9.0.20	This is the NAC Agent 4.9.0.20
□	WebAgent 4.9.0.10	WebAgent	4.9.0.10	This is the Web Agent

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 18-27.

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Adding Client Provisioning Resources from a Local Machine

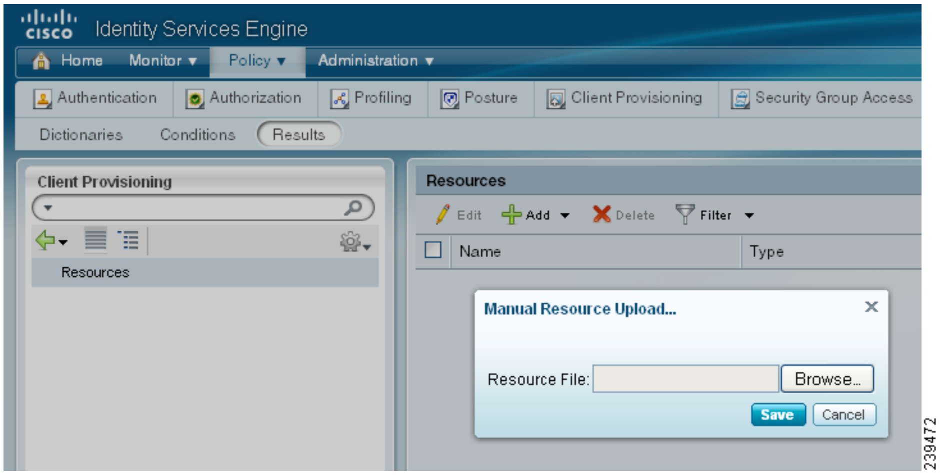
Caution Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources (older versions of the Cisco NAC Agent, for example) will likely cause serious issues for client access. For details, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.0.4*.

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 18-3).

Figure 18-3 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 18-27.

Creating Agent Customization Files to Add to Cisco ISE

This section describes how to customize various Cisco NAC Agent features by specifying settings within the Agent customization file (**branding.tar.gz**).

The "**branding.tar.gz**" 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

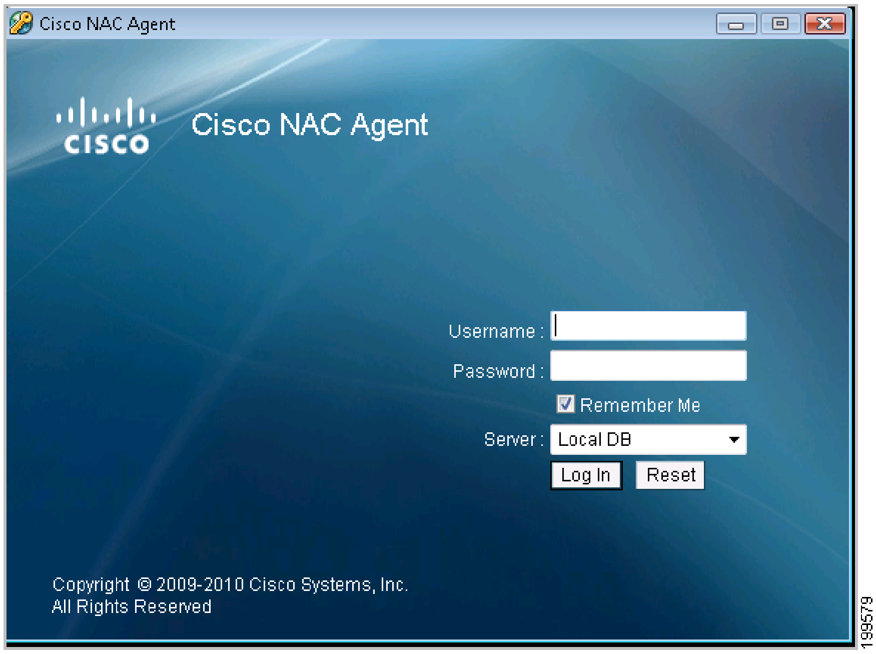
Logo

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 18-4.

Figure 18-4 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 the above 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 Cisco recommends to make changes in the **nacStrings_xx.xml** file.

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

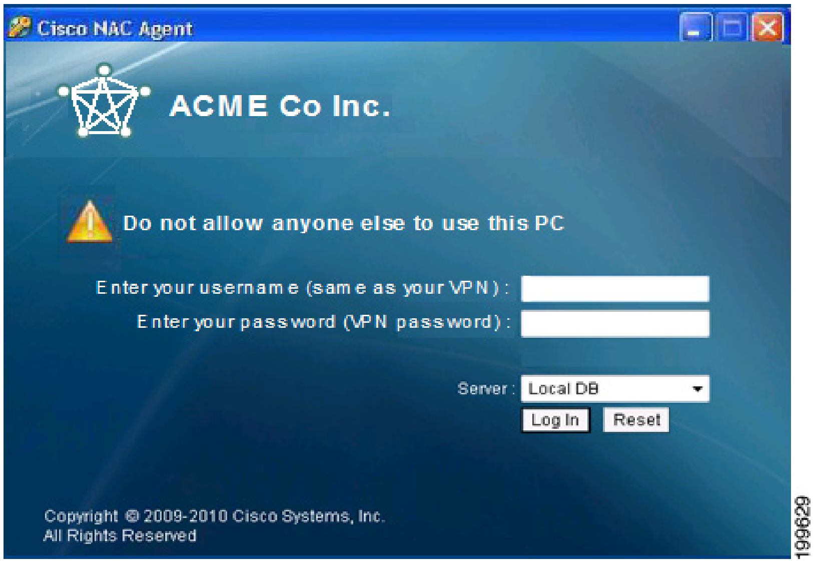
```
<tr class="nacLoginMiddleSectionContainerInput">
   <td colspan="2">
      <fieldset width="100%" id="nacLoginCustomAlert"
                style="display:block" class="nacLoginAlertBox">
          <table width="100%">
             <tr>
                <td id="nacLoginCustomAlert.img" valign="top"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

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"> ACME 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 above file has been modified to customize the login screen as shown in Figure 18-5.

Figure 18-5 Cisco NAC Agent Login—Customized Screen


Cisco NAC Agent
ACME Co Inc.
Do not allow anyone else to use this PC
Enter your username (same as your VPN):
Enter your password (VPN password):
Server:
Local DB
Log In
Reset
Copyright © 2009-2010 Cisco Systems, Inc.
All Rights Reserved
199629

Notice that the "Remember Me" checkbox has been removed. In addition, you can find more text for the "Username" and "Password" fields.

Note Though there is no limit for the number of characters used for the customized text, Cisco recommends restricting them so that they are not occupying 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 is a 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>
```

Note The strings need to be replaced in every locale for which the customization is required. If customization is required for more than one locales, then the modification has to be done in more than one **nacStrings_xx.xml** file.

After modifying the required files, tar all the files and save the tarred file as **branding.tar.gz**. The following is an example of the required tar command lane:

```
tar cvzf branding.tar.gz nac_login.xml nac_logo.gif nacStrings_en.xml
```

Upload the tar file to Cisco ISE using the guidelines described in Adding Client Provisioning Resources from a Local Machine, page 18-5.

Creating Agent Profiles

- Creating Windows Agent Profiles in Cisco ISE, page 18-11
- Creating Mac OS X Agent Profiles in Cisco ISE, page 18-13
- Modifying Windows and Mac OS X Agent Profiles in Cisco ISE, page 18-14
- Agent Profile Parameters and Applicable Values, page 18-15

Cisco recommends configuring agent profiles to control remediation timers, network transition delay timers, and the timer used to control the login success screen on client machines so that these settings are policy based. However, when there are no agent profiles configured to match 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 19-10 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, Cisco recommends you upload agent software to Cisco ISE per the guidelines at:

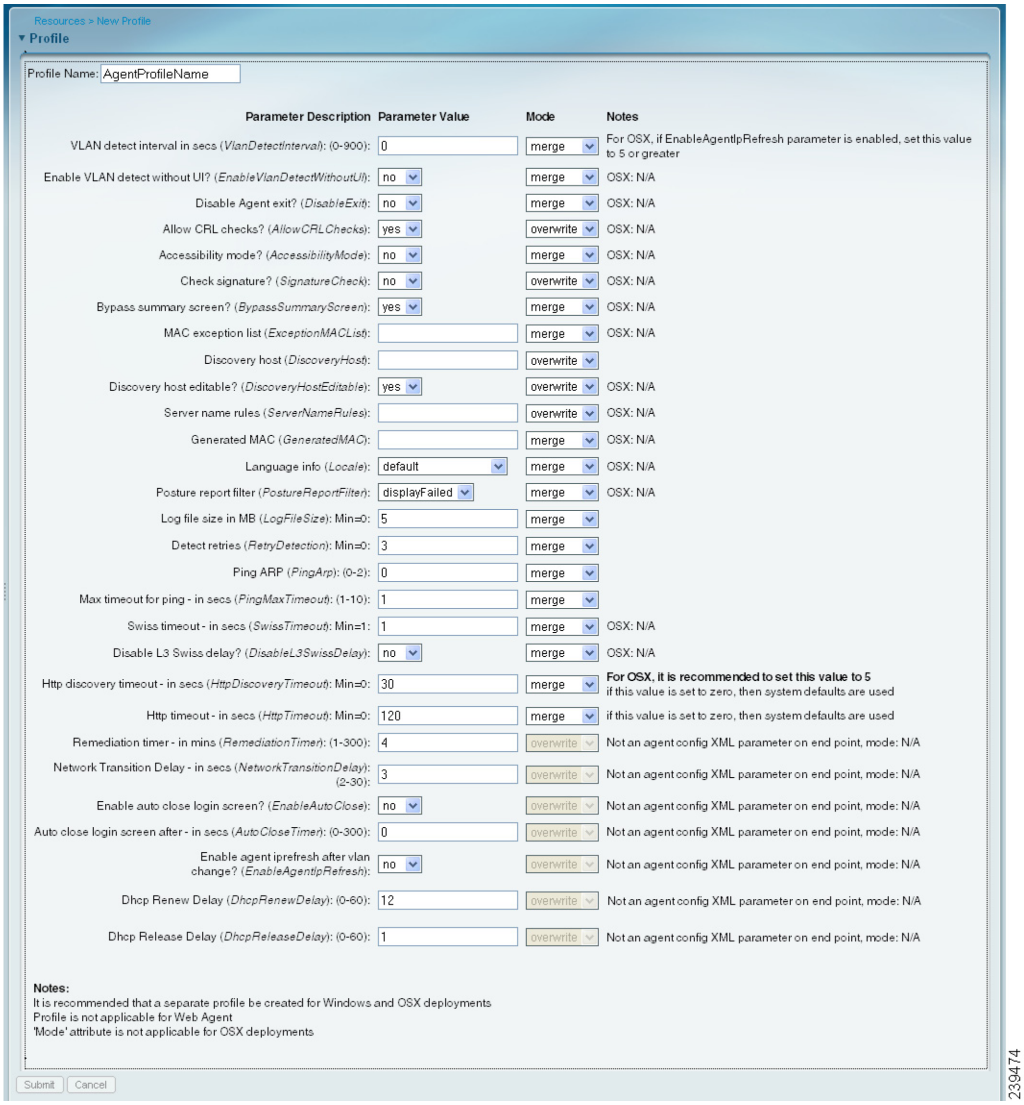
- Adding Client Provisioning Resources from a Remote Source, page 18-4
- Adding Client Provisioning Resources from a Local Machine, page 18-5

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 18-6).

Figure 18-6 ISE Posture Agent Profile



Profile Name: AgentProfileName

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

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 18-15.

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 18-27.

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. Cisco recommends 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, Cisco recommends you upload agent software to Cisco ISE per the guidelines at:

- Adding Client Provisioning Resources from a Remote Source, page 18-4
- Adding Client Provisioning Resources from a Local Machine, page 18-5

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** > **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 18-15.

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 18-27.

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:

- Creating Windows Agent Profiles in Cisco ISE, page 18-11
- Creating Mac OS X Agent Profiles in Cisco ISE, page 18-13

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 18-15.

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 18-27.

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 18-1 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	• 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 sec. • If this setting is 6-900, an ICMP or ARP query is sent every *x* sec.
Enable VLAN detect without UI?	no	yes or no	• 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. **Note** This setting does not apply to Mac OS X client machine agents.

[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 18-2 Customize Agent Login/Logout Dialog Behavior

Parameter	Default Value	Valid Range	Description or Behavior
Disable Agent Exit?	no	yes or no	If this parameter is set to yes, users cannot exit the agent via the system tray icon. **Note** This setting does not apply to Mac OS X client machine agents.
Allow CRL Checks?	yes	yes or no	Setting this parameter to no turns off certificate revocation list (CRL) checking for the agent during discovery and negotiation with the Cisco ISE node. **Note** This setting does not apply to Mac OS X client machine agents.
Accessibility mode?	no	yes or no	• 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. **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. **Note** This setting does not apply to Mac OS X client machine agents.
Check signature?	no	yes or no	The Check signature setting looks for a digital signature that the agent uses to determine whether Windows can trust the executable before launching. For more information, see Adding, Duplicating, Editing, and Deleting a Launch Program Remediation, page 19-124. **Note** This setting does not apply to Mac OS X client machine agents.
Bypass summary screen?	yes	yes or no	If you are employing autoremediation for agent requirements, this setting enables you to make the agent session dialog more automated by skipping the agent posture assessment summary screen and proceeding directly to the first autoremediation function. Avoidance of this step reduces or eliminates user interaction during the agent login and remediation session. **Note** This setting does not apply to Mac OS X client machine agents.

Table 18-3 Manage Client-side MAC Address and Agent Discovery Host

Parameter	Default Value	Valid Range	Description or Behavior
MAC Exception list	—	Valid MAC address	If you specify one or more MAC addresses in this setting, the agent does not advertise those MAC addresses to Cisco ISE during login and authentication to help prevent sending unnecessary MAC addresses over the network. The text string that you specify must be a comma-separated list of MAC addresses including colons. For example: `AA:BB:CC:DD:EE:FF,11:22:33:44:55:66` **Note** This setting does not apply to Mac OS X client machine agents.
Discovery host	—	IP address or fully qualified domain name (FQDN)	This setting specifies the Discovery Host address or resolvable domain name that the agent uses to connect to Cisco ISE in a Layer 3 deployment.
Discovery host editable?	yes	yes or no	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. **Note** This setting does not apply to Mac OS X client machine agents.
Server name rules	—	FQDN	This parameter consists of comma-separated names of associated Cisco ISE nodes. The agent uses the names in this list to authorize Cisco ISE access points. If this list is empty, then the authorization is not performed. If any of the names are not found, then an error is reported. 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. **Note** This setting does not apply to Mac OS X client machine agents.
Generated MAC	—	Valid MAC address	This parameter supports Evolution-Data Optimized (EVDO) connections on the client machine. If the client machine does not have an active network interface card (NIC), the agent creates a dummy MAC address for the system. **Note** This setting does not apply to Mac OS X client machine agents.

Table 18-4 Specify Agent Localization Settings

Parameter	Default Value	Valid Range	Description or Behavior
Language Info	OS setting (“**default**”)	—	• 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. **Note** This setting does not apply to Mac OS X client machine agents.

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 18-5 Report and Log Display Settings

Parameter	Default Value	Valid Range	Description or Behavior
Posture Report Filter	displayFailed	—	This parameter controls the level and type of results that appear to the user when the client machine undergoes posture assessment. • 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. **Note** This setting does not apply to Mac OS X client machine agents.
Log file size in MB	5	0 and above	This setting specifies the file size (in megabytes) for agent log files on the client machine. • 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 18-6 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 *x* times before refreshing the client IP address.
Ping ARP	0	0-2	• 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 no response in *x* sec, then declare an ICMP polling failure.

Table 18-7 Additional SWISS Discovery Customization

Parameter	Default Value	Valid Range	Description or Behavior
Swiss timeout	1	1 and above	• 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. **Note** SwissTimeout works only for UDP SWISS timeouts. **Note** This setting does not apply to Mac OS X client machine agents.
Disable L3 Swiss Delay?	no	yes or no	If this setting is yes, the agent disables its ability to increase the transmission interval for Layer 3 discovery packets. Therefore, the Layer 3 discovery packets repeatedly go out every 5 sec, just like Layer 2 packets. The default setting is no. **Note** This setting does not apply to Mac OS X client machine agents.

Table 18-8 HTTP Discovery Customization

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

Table 18-8 HTTP Discovery Customization (continued)

Parameter	Default Value	Valid Range	Description or Behavior
Http timeout	120	0, 3 and above	Set by default at 120 sec, 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 18-9 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 *both*.

Table 18-10 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 19-10 for more information.

Table 18-11 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	⚠ **Caution** Cisco does not recommend enabling this option for Windows client machines accessing the network via native Windows, Cisco Secure Services Client, or AnyConnect supplicants. Specify whether or not the client machine should renew its IP address after the switch or WLC changes the VLAN for the login session of the client on the respective switch port. Check the "Enable agent IP refresh after VLAN change" parameter to refresh Windows client IP address in both wired and wireless environments for MAB with posture. To ensure the Mac OS X client IP address is refreshed when the assigned VLAN changes, this parameter is required for Mac OS X client machines accessing the network via the native Mac OS X supplicant in both wired and wireless environments. **Note** When you use the "Enable agent IP refresh after VLAN change" option, Cisco ISE sends "DHCP release delay" and "DHCP renew delay" settings (as specified below) instead of using the "Network transition delay" setting used for Windows agent profiles. If you do not use the "Enable agent IP refresh after VLAN change" option, Cisco ISE sends "Network transition delay" timer settings to client machines, but Cisco ISE will not send *both*.
DHCP renew delay	0	0-60	The number of seconds the client machine waits before attempting to request a new IP address from the network DHCP server.
DHCP release delay	0	0-60	The number of seconds the client machine waits before releasing its current IP address.

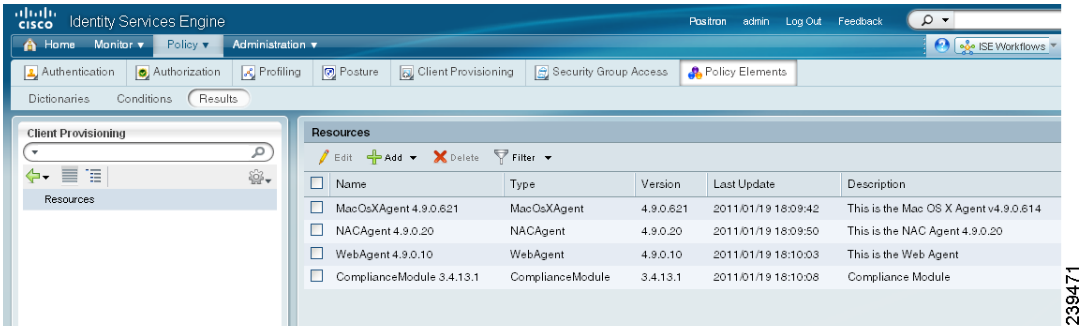
Deleting Client Provisioning Resources

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 18-7 Policy > Policy Elements > Results > Client Provisioning > Resources



cisco Identity Services Engine
Positron admin Log Out Feedback
Home Monitor ▾ Policy ▾ Administration ▾
ISE Workflows
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Client Provisioning
Resources
Edit Add ▾ Delete Filter ▾
239471

Resources

□	Name	Type	Version	Last Update	Description
□	MacOsXAgent 4.9.0.621	MacOsXAgent	4.9.0.621	2011/01/19 18:09:42	This is the Mac OS X Agent v4.9.0.614
□	NACAgent 4.9.0.20	NACAgent	4.9.0.20	2011/01/19 18:09:50	This is the NAC Agent 4.9.0.20
□	WebAgent 4.9.0.10	WebAgent	4.9.0.10	2011/01/19 18:10:03	This is the Web Agent
□	ComplianceModule 3.4.13.1	ComplianceModule	3.4.13.1	2011/01/19 18:10:08	Compliance Module

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

Setting Up Global Client Provisioning Functions

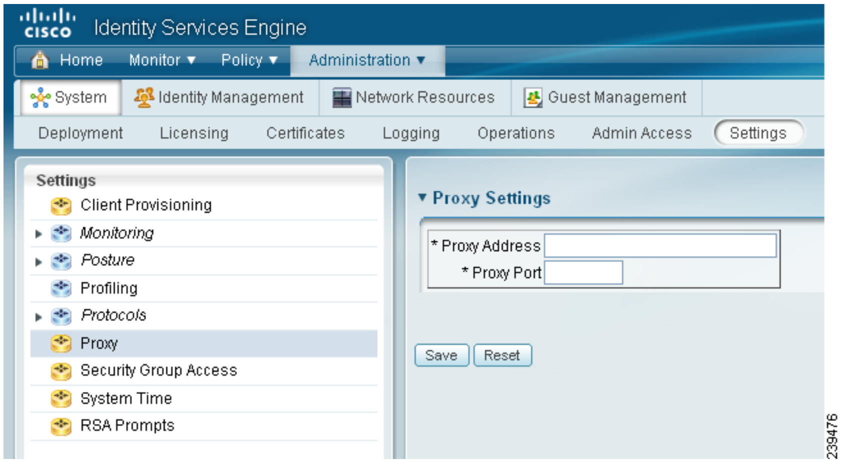
Specifying Proxy Settings in Cisco ISE

If your existing network topology requires you to use a proxy for Cisco ISE to access external resources (like the remote download site where you can find client provisioning and posture-related resources), you can use the Cisco ISE user interface to specify proxy properties.

To specify proxy settings for Cisco ISE, complete the following steps:

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

Figure 18-8 Administration > System > Settings > Proxy



Step 2 Enter the proxy IP address or DNS-resolvable host name in the Proxy Address field and specify the port through which proxy traffic travels to-and-from Cisco ISE in the Proxy Port field.

Step 3 Click **Save**.

Next Steps

Once you have specified your proxy settings, you can optionally enable the following system-wide client provisioning functions:

- Enabling and Disabling the Client Provisioning Service, page 18-25
- Downloading Client Provisioning Resources Automatically, page 18-26

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Enabling and Disabling the Client Provisioning Service

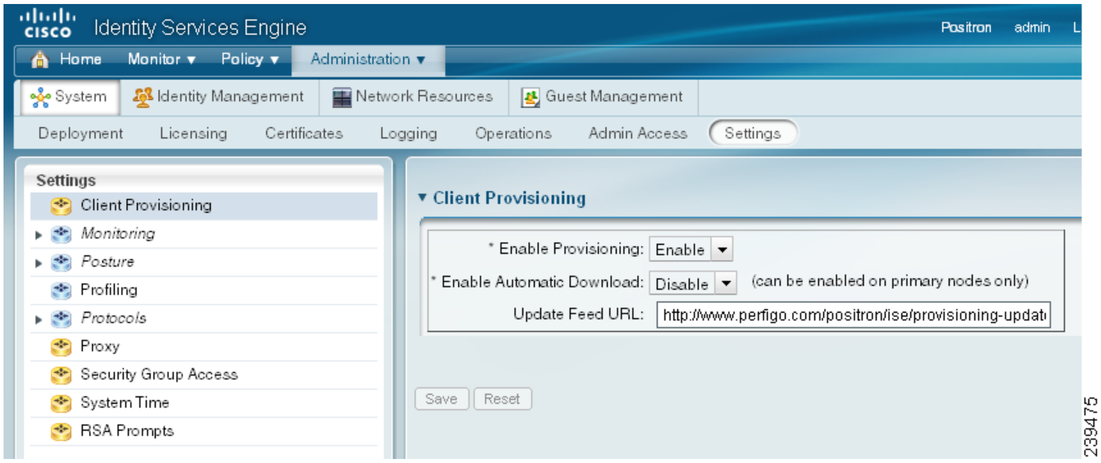
Prerequisites

To ensure 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 18-24.

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 18-9 Administration > System > Settings > Client Provisioning



* Enable Provisioning: Enable
* Enable Automatic Download: Disable (can be enabled on primary nodes only)
Update Feed URL: http://www.perfigo.com/positron/ise/provisioning-updat

Step 2 Click the **Enable Provisioning** drop-down menu and choose **Enable** or **Disable**.

Step 3 Click **OK**.

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:

- Adding and Removing Agents and Other Resources, page 18-3
- Configuring Client Provisioning Resource Policies, page 18-27

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Downloading Client Provisioning Resources Automatically

Note Cisco recommends that you manually upload resources whenever possible according to the guidelines in Adding Client Provisioning Resources to Cisco ISE, page 18-4, 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.

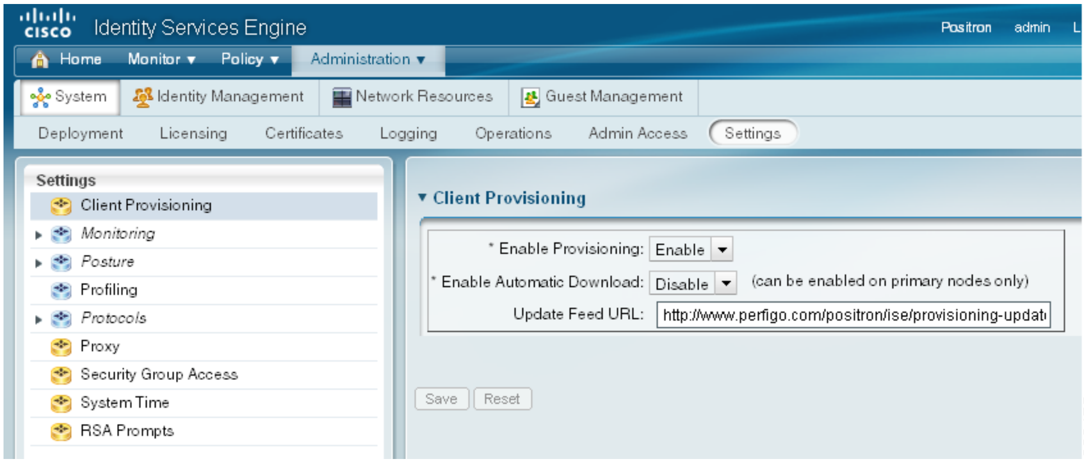
Prerequisites

To ensure 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 18-24.

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 18-10 Administration > System > Settings > Client Provisioning



* Enable Provisioning: Enable ▾

* Enable Automatic Download: Disable ▾ (can be enabled on primary nodes only)

Update Feed URL: http://www.perfigo.com/positron/ise/provisioning-updat

Step 2 Click the **Enable Automatic Download** drop-down menu and 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 field. 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 also access this URL and 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 18-5.

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:

- Adding and Removing Agents and Other Resources, page 18-3
- Configuring Client Provisioning Resource Policies, page 18-27

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

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.

Prerequisites

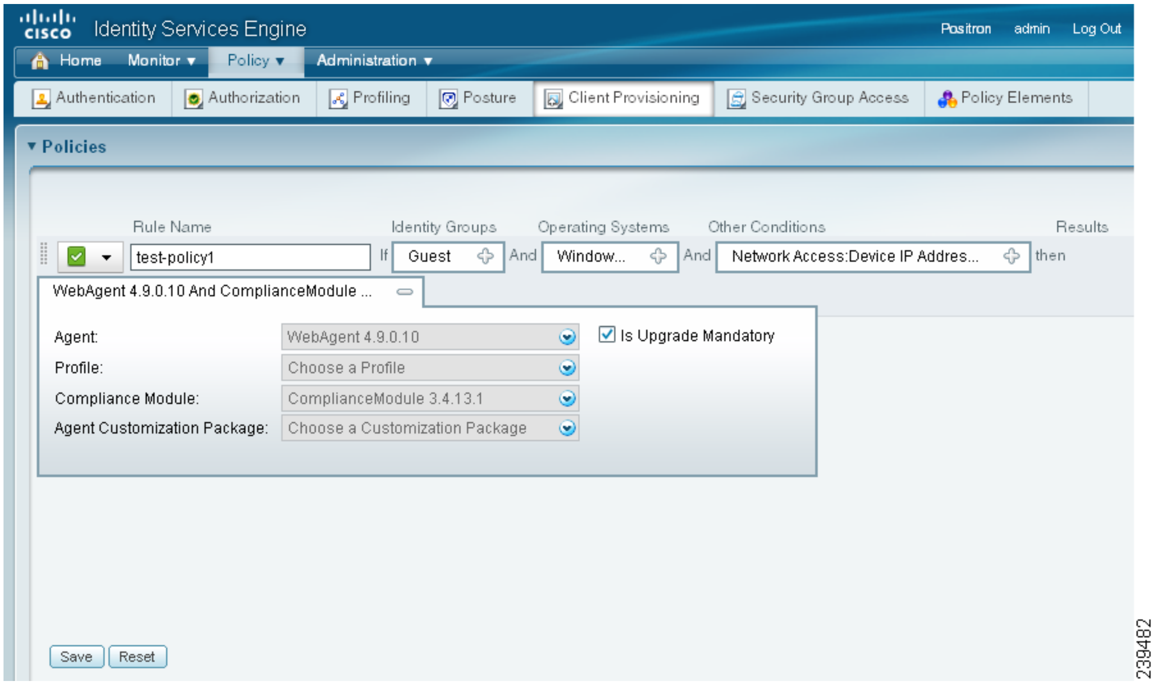
Before you can create effective client provisioning resource policies, ensure that you have set up system-wide client provisioning functions according to the following topics:

- Specifying Proxy Settings in Cisco ISE, page 18-24.
- Setting Up Global Client Provisioning Functions, page 18-24
- Adding and Removing Agents and Other Resources, page 18-3

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

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

Figure 18-11 Policy > Client Provisioning



☑ test-policy1 If Guest And Window... And Network Access:Device IP Addres... then WebAgent 4.9.0.10 And ComplianceModule ...

Agent: WebAgent 4.9.0.10 ☑ Is Upgrade Mandatory

Profile: Choose a Profile

Compliance Module: ComplianceModule 3.4.13.1

Agent Customization Package: Choose a Customization Package

Enable or Disable the Resource Policy

Step 2 Select the **Enable**, **Disable**, or **Monitor** option from the behavior drop-down menu on the left side of the client provisioning policy configuration window:

- **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 field.

Categorize the Client Machine

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 you have configured (for example, "Guest," sponsor-created, or administrator-created groups) at Configuring User Identity Groups, page 4-39.

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

You can choose to specify a single operating system like "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 1.0.4*.

Step 6 In the Other Conditions portion of the client provisioning resource policy, specify a new expression 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

Step 7 Specify which agent type, compliance module, customization package, and/or profile to make available and provision on the client machine based on the categorization defined above.

a. 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 customization package updates are always mandatory.

b. Choose an available agent from the Agent drop-down list.

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

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

Note You can also use the policy configuration process to download agent resources "on the fly" for the three resource types above by clicking the gear-shaped widget and selecting **Download Resource** or **Upload Resource** from the resulting pop-up menu. This method takes you to the Downloaded Remote Resources or Manual Resource Upload dialog box, respectively, where you can download one or more resources to Cisco ISE as described in Adding Client Provisioning Resources to Cisco ISE, page 18-4.

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

Step 8 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 19, "Configuring Client Posture Policies."

Client-side Installation and Log-In

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.

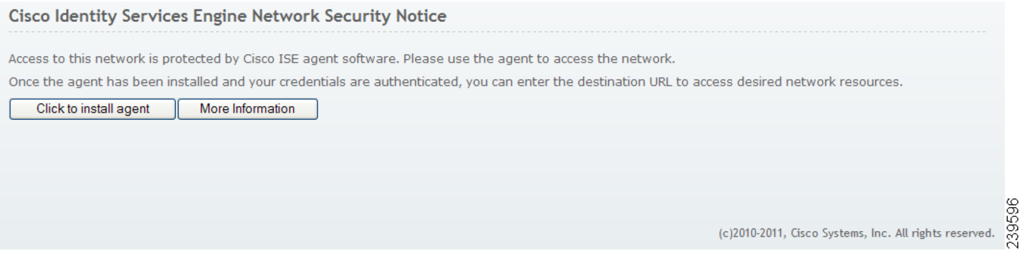
To download agents and other client provisioning resources, users must have administrator privileges on their client machines and the browser session through which they are attempting to log into Cisco ISE. In addition, to successfully install the agent, users will likely need to explicitly accept ActiveX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

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).

Note If you require MAC address bypass (MAB) users to authenticate and access the network via an agent, you must configure your access policy to specify the Cisco NAC Web Agent only.

Figure 18-12 shows a Cisco ISE welcome screen, prompting the user to download and install the Cisco NAC Agent on the client machine.

Figure 18-12 Cisco ISE Agent Download and Installation



Cisco Identity Services Engine Network Security Notice

Access to this network is protected by Cisco ISE agent software. Please use the agent to access the network.

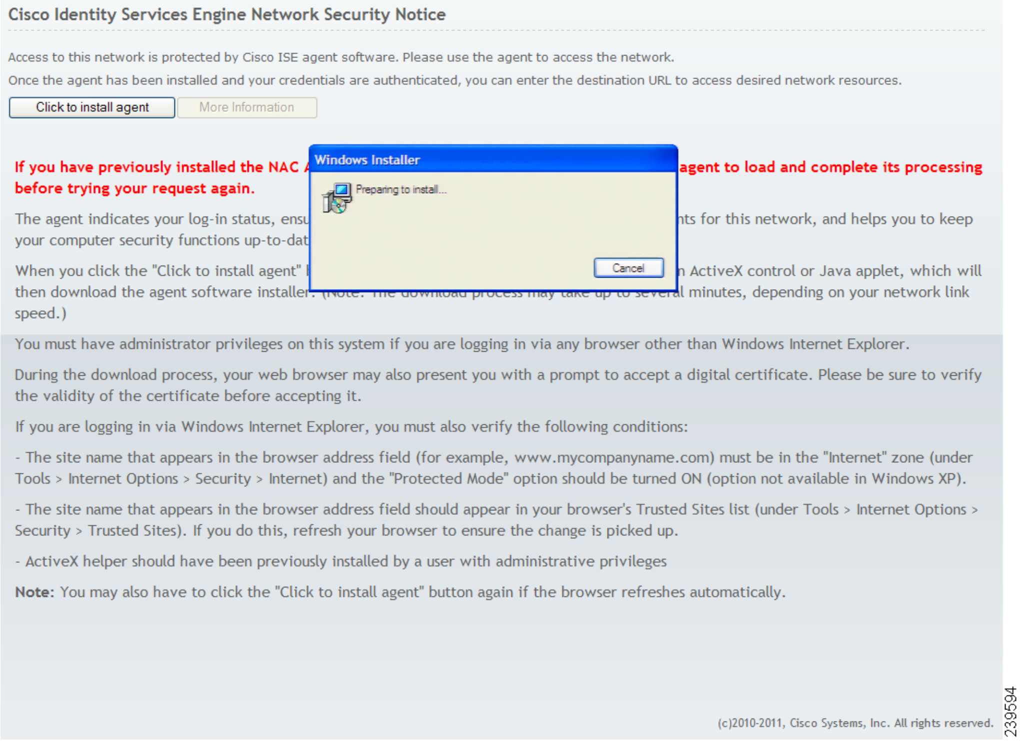
Once the agent has been installed and your credentials are authenticated, you can enter the destination URL to access desired network resources.

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://1.1.1.1. For detailed information on testing Cisco ISE installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*.

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 18-13 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 18-13 Preparing to Install Cisco NAC Agent



Cisco Identity Services Engine Network Security Notice

Access to this network is protected by Cisco ISE agent software. Please use the agent to access the network.

Once the agent has been installed and your credentials are authenticated, you can enter the destination URL to access desired network resources.

If you have previously installed the NAC A agent to load and complete its processing before trying your request again.

The agent indicates your log-in status, ensu nts for this network, and helps you to keep your computer security functions up-to-dat

When you click the "Click to install agent" I n ActiveX control or Java applet, which will then download the agent software installer. (Note: The download process may take up to several minutes, depending on your network link speed.)

You must have administrator privileges on this system if you are logging in via any browser other than Windows Internet Explorer.

During the download process, your web browser may also present you with a prompt to accept a digital certificate. Please be sure to verify the validity of the certificate before accepting it.

If you are logging in via Windows Internet Explorer, you must also verify the following conditions:

- The site name that appears in the browser address field (for example, www.mycompanyname.com) must be in the "Internet" zone (under Tools > Internet Options > Security > Internet) and the "Protected Mode" option should be turned ON (option not available in Windows XP).

- The site name that appears in the browser address field should appear in your browser's Trusted Sites list (under Tools > Internet Options > Security > Trusted Sites). If you do this, refresh your browser to ensure the change is picked up.

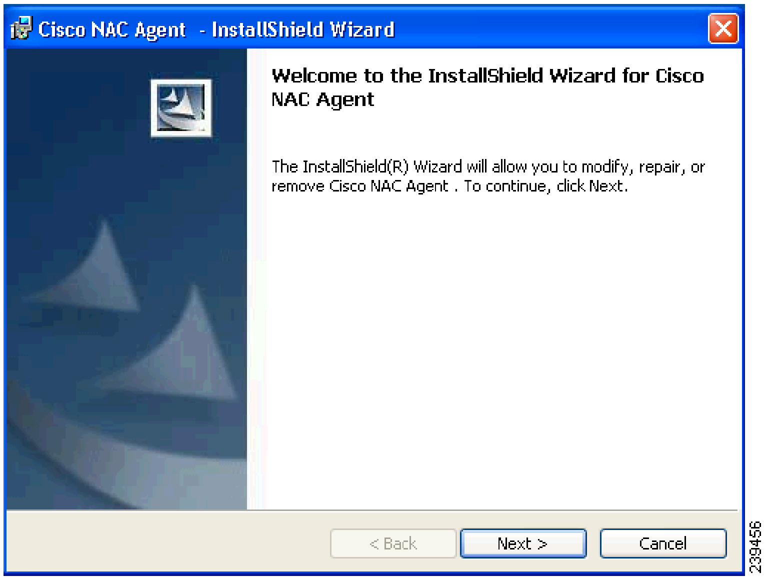
- ActiveX helper should have been previously installed by a user with administrative privileges

Note: You may also have to click the "Click to install agent" button again if the browser refreshes automatically.

(c)2010-2011, Cisco Systems, Inc. All rights reserved.

The agent **InstallShield Wizard** dialog appears (Figure 18-14).

Figure 18-14 Cisco NAC Agent InstallShield Wizard—Welcome



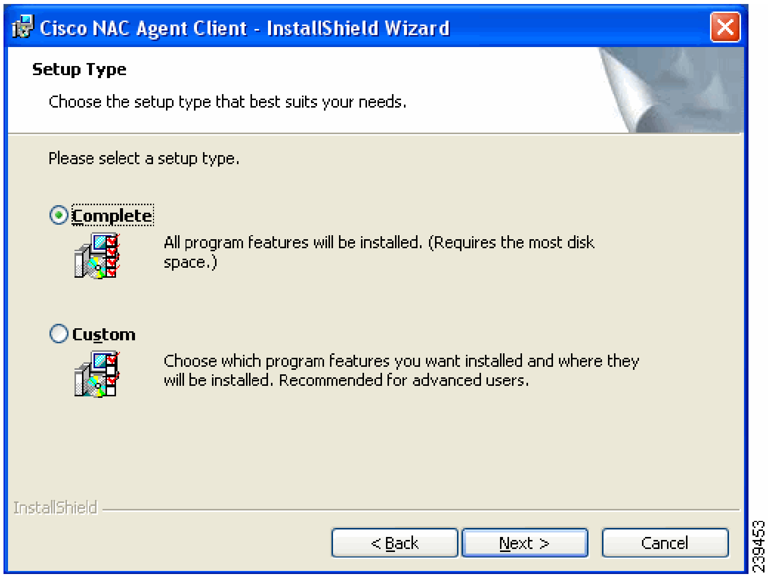
Cisco NAC Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for Cisco NAC Agent

The InstallShield(R) Wizard will allow you to modify, repair, or remove Cisco NAC Agent . To continue, click Next.

The user has the option to install the complete collection of agent files or specify one or more items by choosing the **Custom** option and clicking **Next** (Figure 18-15).

Figure 18-15 Cisco NAC Agent Installation—Setup Type



Cisco NAC Agent Client - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Complete

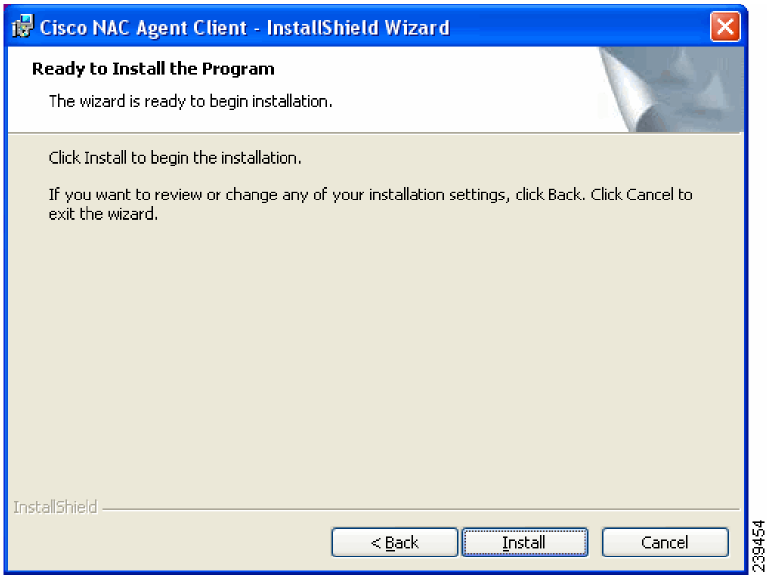
All program features will be installed. (Requires the most disk space.)

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

The agent **InstallShield Wizard** dialog appears (Figure 18-16).

Figure 18-16 Cisco NAC Agent InstallShield Wizard—Ready to Install



Cisco NAC Agent Client - InstallShield Wizard

Ready to Install the Program

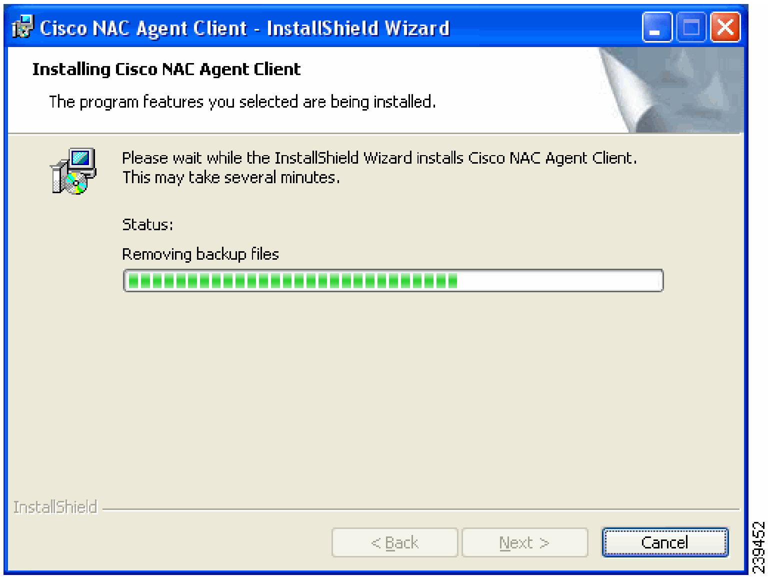
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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 18-17 Cisco NAC Agent Installation In Progress



Cisco NAC Agent Client - InstallShield Wizard

Installing Cisco NAC Agent Client

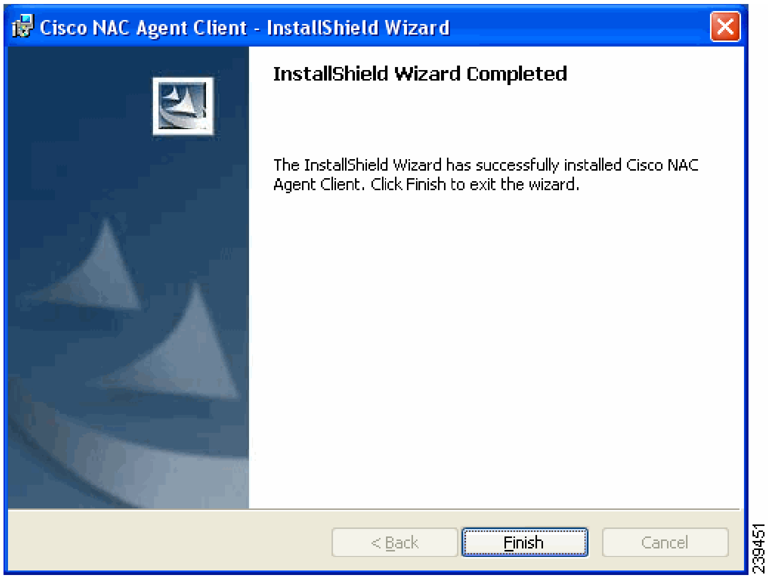
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Cisco NAC Agent Client. This may take several minutes.

Status:

Removing backup files

Figure 18-18 Cisco NAC Agent Installation Complete



Cisco NAC Agent Client - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Cisco NAC Agent Client. Click Finish to exit the wizard.

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.

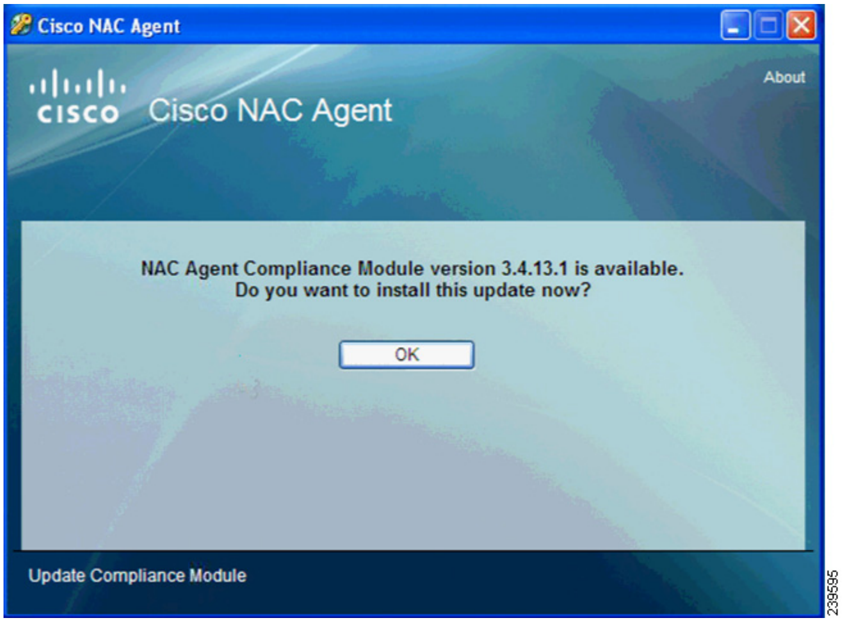
Note The server certificate on the client helps ensure the client machine can perform DNS resolution, allowing services like Cisco ISE client provisioning and posture assessment. If you change the Cisco ISE domain name (by logging into the Cisco ISE CLI and manually specifying a new domain name, for 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 package

Figure 18-19 displays an example of an agent compliance module update (which is always mandatory) at the time of agent installation on the client machine.

Figure 18-19 Cisco NAC Agent—Updating Agent Compliance Module



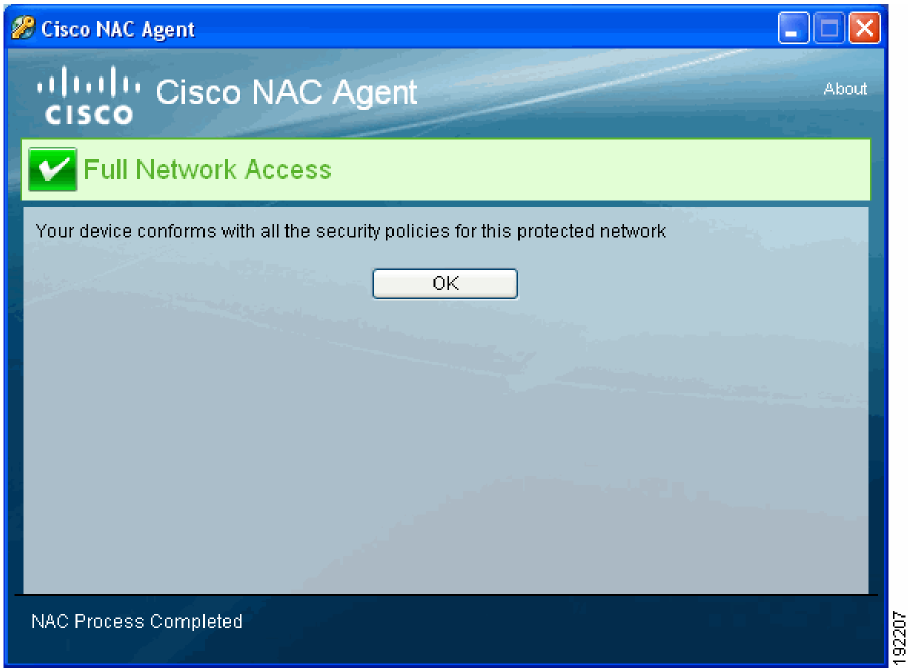
NAC Agent Compliance Module version 3.4.13.1 is available.
Do you want to install this update now?

If you have not enabled the Is Upgrade Mandatory setting in the client provisioning resource policy, then the agent upgrade dialog would display 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 18-27.

Following successful agent installation, client posture assessment, and remediation, the agent notifies the user that their login session is complete and 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.



Full Network Access

Your device conforms with all the security policies for this protected network

NAC Process Completed

Viewing Client Provisioning Reports and Events

- Viewing Client Provisioning Reports in Cisco ISE, page 18-35
- Viewing Client Provisioning Event Logs in Cisco ISE, page 18-39

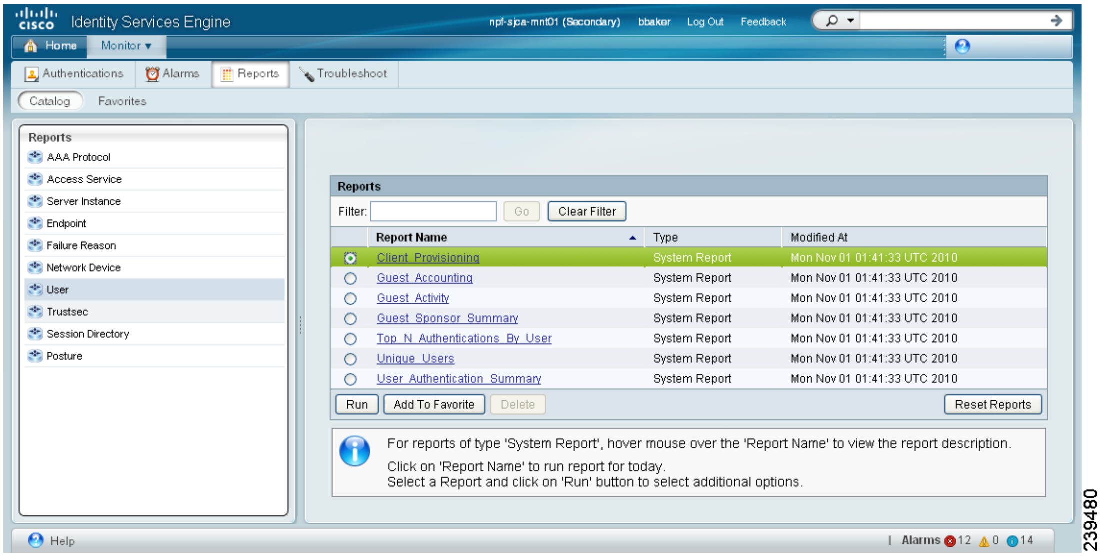
Viewing Client Provisioning Reports in Cisco ISE

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 22, "Monitoring and Troubleshooting" for more details on using the Cisco ISE monitoring and troubleshooting capabilities to maximize the tools within your network deployment.

The **Monitor > Reports > Catalog > User > Client Provisioning** window displays statistics about successful and unsuccessful client provisioning requests (Figure 18-20).

Figure 18-20 Monitor > Reports > Catalog > User > Client Provisioning



Reports

Filter: Go Clear Filter

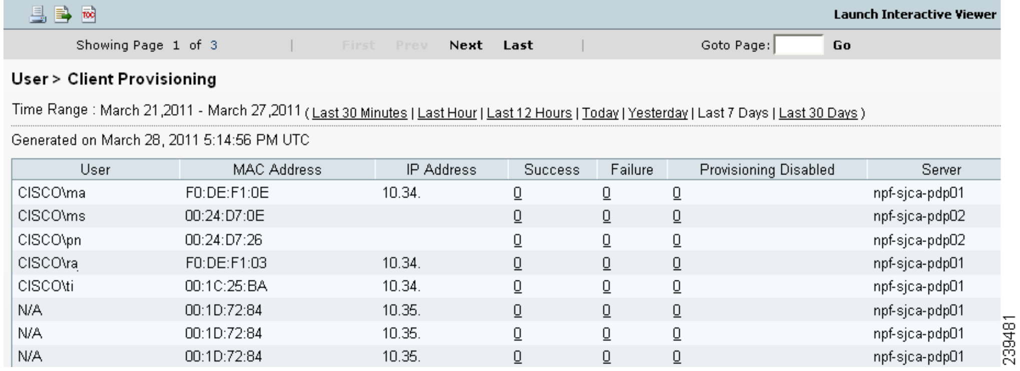
	Report Name	Type	Modified At
●	Client_Provisioning	System Report	Mon Nov 01 01:41:33 UTC 2010
○	Guest_Accounting	System Report	Mon Nov 01 01:41:33 UTC 2010
○	Guest_Activity	System Report	Mon Nov 01 01:41:33 UTC 2010
○	Guest_Sponsor_Summary	System Report	Mon Nov 01 01:41:33 UTC 2010
○	Top_N_Authentications_By_User	System Report	Mon Nov 01 01:41:33 UTC 2010
○	Unique_Users	System Report	Mon Nov 01 01:41:33 UTC 2010
○	User_Authentication_Summary	System Report	Mon Nov 01 01:41:33 UTC 2010

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.

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 18-21).

Figure 18-21 Client Provisioning Report Results



User > Client Provisioning

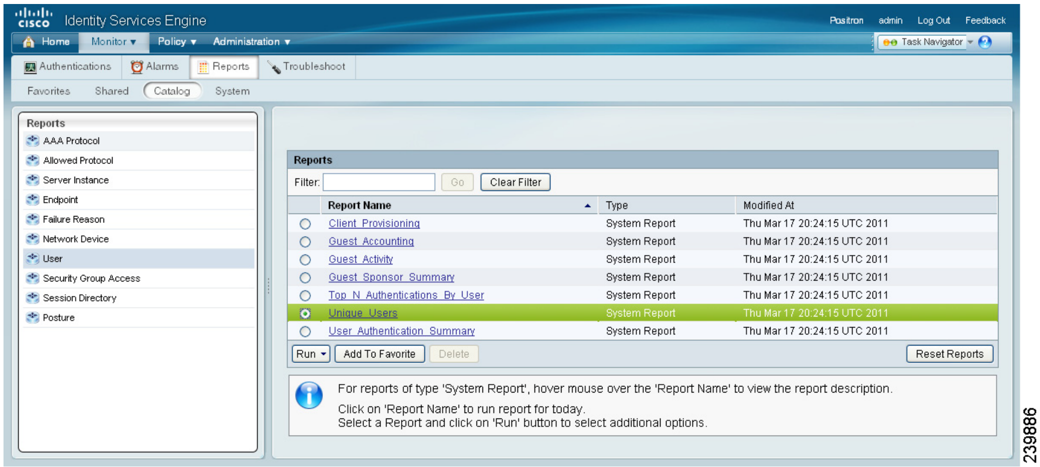
Time Range : March 21,2011 - March 27,2011 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

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.	0	0	0	npf-sjca-pdp01
CISCO\ms	00:24:D7:0E		0	0	0	npf-sjca-pdp02
CISCO\pn	00:24:D7:26		0	0	0	npf-sjca-pdp02
CISCO\ra	F0:DE:F1:03	10.34.	0	0	0	npf-sjca-pdp01
CISCO\ti	00:1C:25:BA	10.34.	0	0	0	npf-sjca-pdp01
N/A	00:1D:72:84	10.35.	0	0	0	npf-sjca-pdp01
N/A	00:1D:72:84	10.35.	0	0	0	npf-sjca-pdp01
N/A	00:1D:72:84	10.35.	0	0	0	npf-sjca-pdp01

The **Monitor > Reports > Catalog > User > Unique Users** window displays statistics about known specific client access sessions initiated during the specified time period (Figure 18-22).

Figure 18-22 Monitor > Reports > Catalog > User > Unique Users

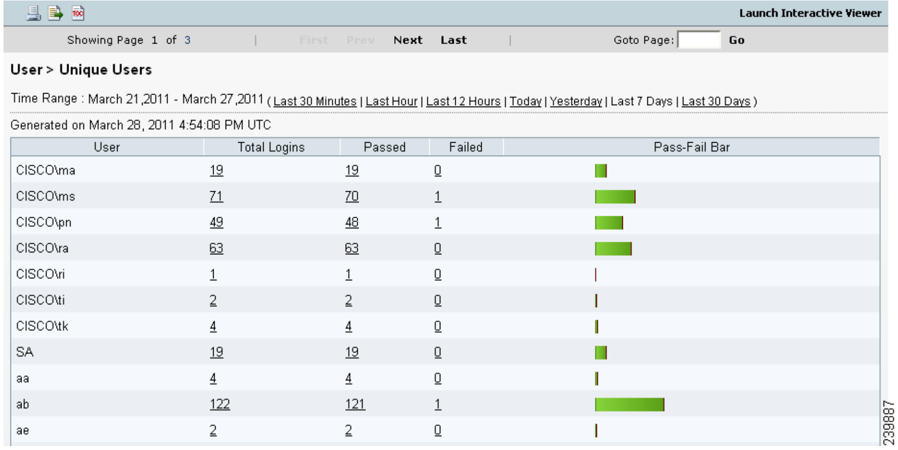


	Report Name	Type	Modified At
○	Client_Provisioning	System Report	Thu Mar 17 20:24:15 UTC 2011
○	Guest_Accounting	System Report	Thu Mar 17 20:24:15 UTC 2011
○	Guest_Activity	System Report	Thu Mar 17 20:24:15 UTC 2011
○	Guest_Sponsor_Summary	System Report	Thu Mar 17 20:24:15 UTC 2011
○	Top_N_Authentications_By_User	System Report	Thu Mar 17 20:24:15 UTC 2011
●	Unique_Users	System Report	Thu Mar 17 20:24:15 UTC 2011
○	User_Authentication_Summary	System Report	Thu Mar 17 20:24:15 UTC 2011

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 client provisioning data (Figure 18-23).

Figure 18-23 Unique Users Report Results



User > Unique Users

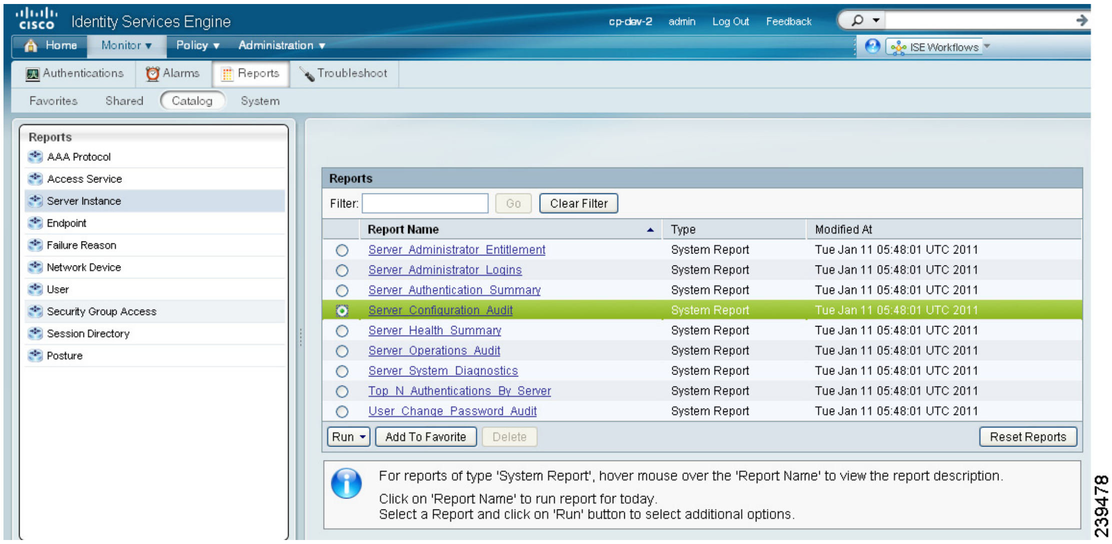
Time Range : March 21,2011 - March 27,2011 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on March 28, 2011 4:54:08 PM UTC

User	Total Logins	Passed	Failed	Pass-Fail Bar
CISCO\ma	19	19	0	
CISCO\ms	71	70	1	
CISCO\pn	49	48	1	
CISCO\ra	63	63	0	
CISCO\ri	1	1	0	
CISCO\ti	2	2	0	
CISCO\tk	4	4	0	
SA	19	19	0	
aa	4	4	0	
ab	122	121	1	
ae	2	2	0	

The **Monitor > Reports > Catalog > Server Instance > Server Configuration Audit** window displays information about recent client provisioning resource configuration changes (Figure 18-24).

Figure 18-24 Monitor > Reports > Catalog > Server Instance > Server Configuration Audit



Reports

Filter: Go Clear Filter

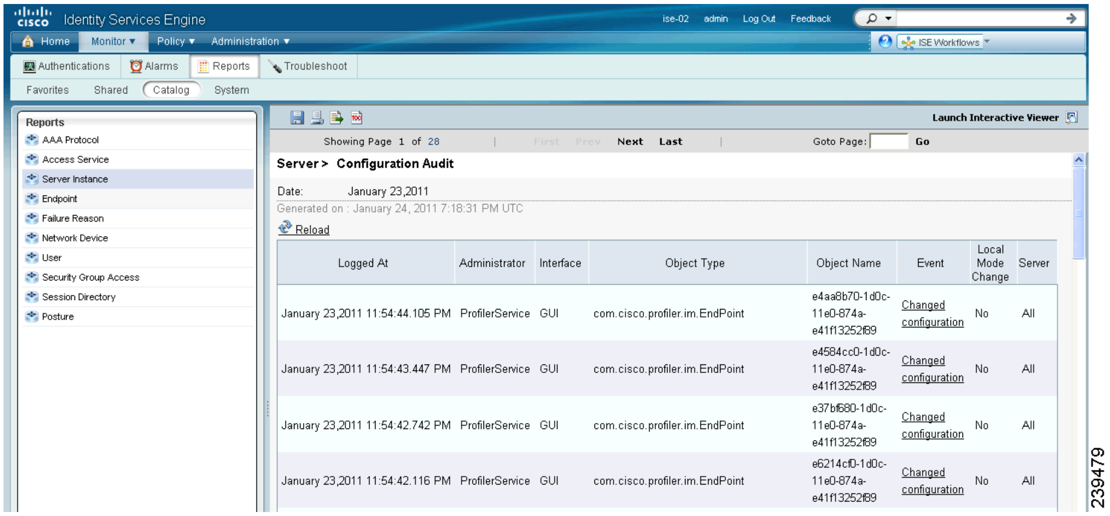
	Report Name	Type	Modified At
○	Server_Administrator_Entitlement	System Report	Tue Jan 11 05:48:01 UTC 2011
○	Server_Administrator_Logins	System Report	Tue Jan 11 05:48:01 UTC 2011
○	Server_Authentication_Summary	System Report	Tue Jan 11 05:48:01 UTC 2011
●	Server_Configuration_Audit	System Report	Tue Jan 11 05:48:01 UTC 2011
○	Server_Health_Summary	System Report	Tue Jan 11 05:48:01 UTC 2011
○	Server_Operations_Audit	System Report	Tue Jan 11 05:48:01 UTC 2011
○	Server_System_Diagnostics	System Report	Tue Jan 11 05:48:01 UTC 2011
○	Top_N_Authentications_By_Server	System Report	Tue Jan 11 05:48:01 UTC 2011
○	User_Change_Password_Audit	System Report	Tue Jan 11 05:48:01 UTC 2011

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 18-25).

Figure 18-25 Server Configuration Audit Report Results



Server > Configuration Audit

Date: January 23,2011
Generated on : January 24, 2011 7:18:31 PM UTC

Reload

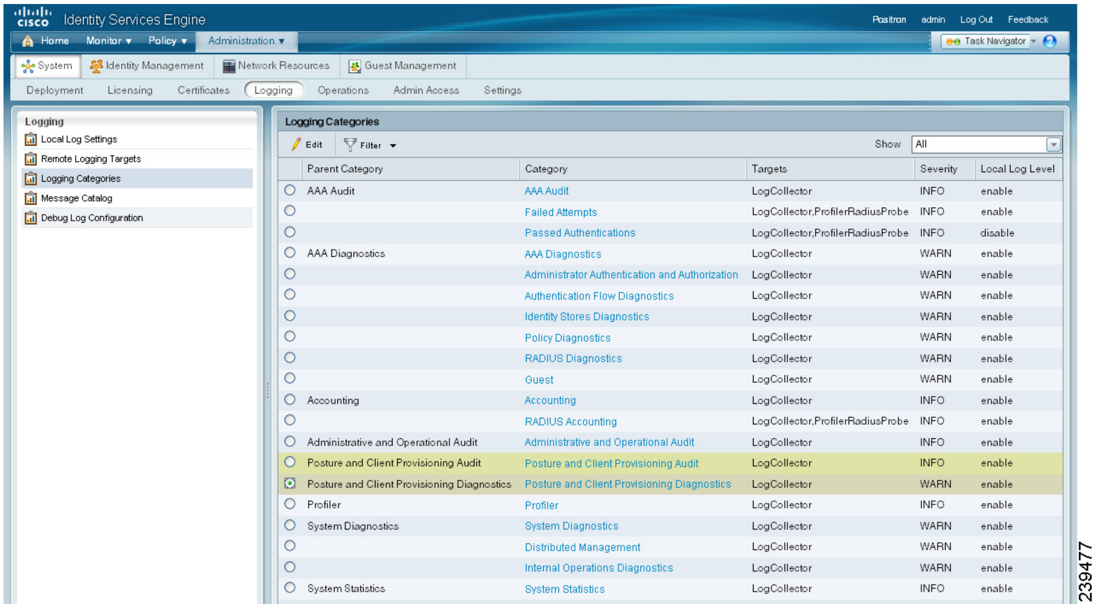
Logged At	Administrator	Interface	Object Type	Object Name	Event	Local Mode Change	Server
January 23,2011 11:54:44.105 PM	ProfilerService	GUI	com.cisco.profiler.im.EndPoint	e4aa8b70-1d0c-11e0-874a-e41f13252f89	Changed configuration	No	All
January 23,2011 11:54:43.447 PM	ProfilerService	GUI	com.cisco.profiler.im.EndPoint	e4584cc0-1d0c-11e0-874a-e41f13252f89	Changed configuration	No	All
January 23,2011 11:54:42.742 PM	ProfilerService	GUI	com.cisco.profiler.im.EndPoint	e37bf680-1d0c-11e0-874a-e41f13252f89	Changed configuration	No	All
January 23,2011 11:54:42.116 PM	ProfilerService	GUI	com.cisco.profiler.im.EndPoint	e6214cf0-1d0c-11e0-874a-e41f13252f89	Changed configuration	No	All

Viewing Client Provisioning Event Logs in Cisco ISE

During Cisco ISE operation, you may need to search event log entries in order 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 13, “Logging” for more specific information on using the Cisco ISE log compilation capabilities to maximize the tools within your network deployment.

Figure 18-26 Administration > System > Logging > Categories > Posture and Client Provisioning Diagnostics



	Parent Category	Category	Targets	Severity	Local Log Level
○	AAA Audit	AAA Audit	LogCollector	INFO	enable
○		Failed Attempts	LogCollector,ProfilerRadiusProbe	INFO	enable
○		Passed Authentications	LogCollector,ProfilerRadiusProbe	INFO	disable
○	AAA Diagnostics	AAA Diagnostics	LogCollector	WARN	enable
○		Administrator Authentication and Authorization	LogCollector	WARN	enable
○		Authentication Flow Diagnostics	LogCollector	WARN	enable
○		Identity Stores Diagnostics	LogCollector	WARN	enable
○		Policy Diagnostics	LogCollector	WARN	enable
○		RADIUS Diagnostics	LogCollector	WARN	enable
○		Guest	LogCollector	WARN	enable
○	Accounting	Accounting	LogCollector	INFO	enable
○		RADIUS Accounting	LogCollector,ProfilerRadiusProbe	INFO	enable
○	Administrative and Operational Audit	Administrative and Operational Audit	LogCollector	INFO	enable
○	Posture and Client Provisioning Audit	Posture and Client Provisioning Audit	LogCollector	INFO	enable
●	Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagnostics	LogCollector	WARN	enable
○	Profiler	Profiler	LogCollector	INFO	enable
○	System Diagnostics	System Diagnostics	LogCollector	WARN	enable
○		Distributed Management	LogCollector	WARN	enable
○		Internal Operations Diagnostics	LogCollector	WARN	enable
○	System Statistics	System Statistics	LogCollector	INFO	enable