Configure Client Provisioning

Enable Client Provisioning in Cisco ISE

Client provisioning functions in Cisco ISE allow you to download client provisioning resources and configure agent profiles for Windows and MAC OS X clients, and native supplicant profiles for your own personal devices. Client provisioning resource policies enable users to download and install resources on client devices.

Enable client provisioning to allow users to download client provisioning resources and configure agent profiles. You can configure agent profiles for Windows clients, Mac OS X clients, and native supplicant profiles for personal devices. 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.

Before You Begin

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

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

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

Step 3 Click **Save**.

What to Do Next

Add client provisioning resources for posture agents in Cisco ISE and configure client provisioning policies to enable users to download and install client provisioning resources on client machines.

Client Provisioning Resources

Client provisioning resources are downloaded to endpoints after the endpoint connects to the network. Client provisioning resources consist of compliance and posture agents for desktops, and native supplicant profiles for phones and tablets. Client provisioning policies assign these provisioning resources to endpoints to start a network session.

Client provisioning resources are listed on **Policy Elements** > **Results** > **Client Provisioning** > **Resources**. The following resource types can be added to the list by clicking the **Add** button:

- **Agent resources from Cisco Site—**Select the NAC, AnyConnect, and Supplicant Provisioning wizards you want to make available for client provisioning policies. Cisco periodically updates this list of resources, adding new ones and updating existing ones. You can also set up ISE to download all the Cisco resources and resource updates automatically, see Download Client Provisioning Resources Automatically.

- **Agent resources from local disk—**Select resources on your PC that you want to upload to ISE, see Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 4.
- **AnyConnect Configuration—**Select the AnyConnect PC clients that you want to make available for client provisioning. See Create AnyConnect Configuration for more information.
- **Native Supplicant Profile—**Configure a supplicant profile for phones and tablets that contains settings for your network. For more information, see Create Native Supplicant Profiles.
- **NAC Agent or AnyConnect ISE Posture Profile—**Configure the NAC agent and AnyConnect ISE Posture here when you don't want to create and distribute agent XML profiles. For more information about the AnyConnect ISE Posture agent, see AnyConnect Adminstrators Guide, ISE Posture Profile Editor. For more information about the NAC agent profile, see Create an Agent Customization File for the Cisco NAC Agent, on page 34.

After creating client provisioning resources, create client provisioning policies that apply the client provisioning resources to the endpoints. See Configure Client Provisioning Resource Policies, on page 46.

Add Client Provisioning Resources from Cisco

You can add client provisioning resources from Cisco.com for AnyConnect and Cisco NAC Agent for Windows and MAC OS x clients, and Cisco Web agent. Depending on the resources that you select and available network bandwidth, Cisco ISE can take a few seconds or even a few minutes to download client provisioning resources to Cisco ISE.

Before You Begin

- Ensure that you have the correct proxy settings configured in Cisco ISE.
- Enable client provisioning in Cisco ISE.

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

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

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

Step 4 Click **Save**.

What to Do Next

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

Download Client Provisioning Resources Automatically

Downloading automatically uploads all available software from Cisco to Cisco ISE, many items of which may not be pertinent to your deployment. Cisco recommends manually uploading resources whenever possible rather than opting to download them automatically from Cisco.

Before You Begin

Ensure that you have the correct proxy settings configured in Cisco ISE and you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE.

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

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

Step 3 Specify the URL where Cisco ISE searches for system updates in the Update Feed URL text box. For example, the default URL for downloading client-provisioning resources is https://www.cisco.com/web/secure/pmbu/provisioning-update.xml.
If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the default URL, try also pointing your Cisco ISE to the following URL: https://www.perfigo.com/ise/provisioning-update.xml.

Step 4 Click **Save**.

What to Do Next

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

Add Cisco Provided Client Provisioning Resources from a Local Machine

You can add client provisioning resources from the local disk, which you might have previously downloaded from Cisco.

Before You Begin

Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources (older versions of the Cisco NAC Agent, for example) will likely cause serious issues for client access.

If you are downloading the resource files manually from the Cisco.com, refer to "Cisco ISE Offline Updates" section in the Release Notes.

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

Step 2 Choose **Add** > **Agent resources from local disk**.

Step 3 Choose **Cisco Provided Packages** from the Category drop-down.

Step 4 Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.
You can add AnyConnect, Cisco NAC Agent, and Cisco Web Agent resources that you have previously downloaded from Cisco site in your local machine.

Step 5 Click **Submit**.

What to Do Next

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

Add Customer Created Resources for AnyConnect from a Local Machine

Add customer created resources like AnyConnect customization and localization packages and AnyConnect profiles from the local machine to Cisco ISE.

Before You Begin

Ensure that customer created resources for AnyConnect are zipped files and available in your local disk.

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

Step 2 Click **Add**.

Step 3 Choose **Agent Resources from local disk**.

Step 4 Choose **Customer Created Packages** from the Category drop-down.

Step 5 Enter the name and description for AnyConnect resources.

Step 6 Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

Step 7 Choose the following AnyConnect resources to upload to Cisco ISE:

- AnyConnect customization bundle
- AnyConnect localization bundle
- AnyConnect profile
- Advanced Malware Protection (AMP) Enabler Profile

Step 8 Click **Submit**.
The Uploaded AnyConnect Resources table displays AnyConnect resources that you add to Cisco ISE.

What to Do Next

Create AnyConnect agent profile

Configure 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 example, Research In Motion Blackberry devices).

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

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

a) **Allow Network Access—**Users are allowed to register their device on the network without having to install and launch the native supplicant wizard.

b) **Apply Defined Authorization Policy—**Users must try to access the Cisco ISE network via standard authentication and authorization policy application (outside of the native supplicant provisioning process). If you enable this option, the user device goes through standard registration according to any client-provisioning policy applied to the user's ID. If the user's device requires a certificate to access the Cisco ISE network, you must also provide detailed instructions to the user describing how to obtain and apply a valid certificate using the customizable user-facing text fields, as described in the "Adding a Custom Language Template" section in the Chapter 15, Setting up and Customizing End_User Web Portals.

Step 3 Click **Save**.

What to Do Next

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

Create Native Supplicant Profiles

You can create native supplicant profiles to enable users to bring their own devices into the Cisco ISE network. When the user signs in, Cisco ISE uses the profile that you associated with that user's authorization requirements to choose the necessary supplicant provisioning wizard. The wizard runs and sets up the user's personal device to access the network.

Note The provisioning wizard only configures interfaces which are active. Because of this, users with Wired and Wireless connections will not be provisioned for both interfaces, unless they are both active.

Before You Begin

- If you intend to use a TLS device protocol for remote device registration, set up at least one Simple Certificate Enrollment Protocol (SCEP) profile.
- Open up TCP port 8909 and UDP port 8909 to enable installation of Cisco NAC Agent, Cisco NAC Web Agent, and supplicant provisioning wizard. For more information about port usage, see the "Cisco

ISE Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

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

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

Step 3 Create a profile, using the descriptions described in Native Supplicant Profile Settings, on page 7

What to Do Next

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

Native Supplicant Profile Settings

When you choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning Resources**, and add a Native Supplicant Profile, you will see the following settings.

- **Name—**Name of the native supplicant profile that you are creating, and select which operating system(s) this profile should apply to. Each profile defines settings for a network connection that ISE will apply to the client's native supplicant.

Wireless Profile(s)

Configure one or more Wireless profiles, one for each SSID that you want to make available to the client.

- **SSID Name—** Name of the SSID that the client will connect to.
- **Security—**Configure the client to use WPA or WPA2.
- **Allowed Procotol—**Configure which protocol the client should use to connect to the authentication server; PEAP or EAP-TLS.
- **Certificate Template—**For TLS, choose one of the certificate templates defined on **Administration** > **System Certificates** > **Certificate Authority** > **Certificate Templates**.

Optional Settings are described in the section *Optional Settings - for Windows*.

iOS Settings

- **Enable if target network is hidden**

Wired Profile

- **Allowed Protocol—**Configure which protocol the client should use to connect to the authentication server; PEAP or EAP-TLS.
- **Certificate Template—**For TLS, choose one of the certificate templates that defined on Administration System Certificates Certificate Authority Certificate Templates

Optional Settings - for Windows

If you expand **Optional**, the following fields are also available for Windows clients.

- **Automatically use logon name and password (and domain if any)—**If you selected User for authentication mode, use the logon and password to without prompting the user, if that information is available.
- **Enable Fast Reconnect—**Allow a PEAP session to resume without checking user credentials when the session resume feature is enabled in the PEAP protocol options, which is configured on **Administration** > **System** > **Settings** > **Protocols** > **PEAP**.
- **Enable Quarantine Checks—** Check if the client has been quarantined.
- **Disconnect if server does not present cryptobinding TLV—**Disconnect if cryptobinding TLV is not supported for the network connection.
- **Do not prompt user to authorize new servers or trusted certification authorities—**Automatically accept user certificates; do not prompt the user.
- **Connect even if the network is not broadcasting its name (SSID)—**For Wireless profiles only.

AMP Enabler Profile Settings

The following table describes the fields in the Advanced Malware Protection (AMP) Enabler Profile page. The navigation path is: **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Click the **Add** drop-down arrow and select the **AMP Enabler Profile**.

Table 1: AMP Enabler Profile Page

Fields	Usage Guidelines
Name	Enter the name of the AMP enabler profile that you want to create.
Description	Enter a description for the AMP enabler profile.
Install AMP Enabler	• **Windows Installer—**Specify the URL of the local server that hosts the AMP for Windows OS software. The AnyConnect module uses this URL to download the .exe file to the endpoint. The file size is approximately 25 MB. • **Mac Installer—**Specify the URL of the local server that hosts the AMP for Mac OSX software. The AnyConnect module uses this URL to download the .pkg file to the endpoint. The file size is approximately 6 MB. The **Check** button communicates with the server to verify if the URL is valid. If the URL is valid, a "File found" message is displayed or else an error message is displayed.
Uninstall AMP Enabler	Uninstalls the AMP for endpoint software from the endpoint.

Fields	Usage Guidelines
Add to Start Menu	Adds a shortcut for the AMP for endpoint software in the Start menu of the endpoint, after the AMP for endpoint software is installed on the endpoint.
Add to Desktop	Adds an icon for the AMP for endpoint software on the desktop of the endpoint, after the AMP for endpoint software is installed on the endpoint.
Add to Context Menu	Adds the Scan Now option in the right-click context menu of the endpoint, after the AMP for endpoint software is installed on the endpoint.

Create an AMP Enabler Profile Using the Embedded Profile Editor

You can create the AMP enabler profile using the ISE embedded profile editor or the standalone editor.

To create the AMP enable profile using the ISE embedded profile editor:

Before You Begin

- Download the AMP for Endpoint software from the SOURCEfire portal and host it on a local server.
- Import the certificate of the server that hosts the AMP for endpoint software to the ISE certificate store by navigating to **Administration** > **Certificates** > **Trusted Certificates**.
- Ensure that the **AMP Enabler** options are selected in the **AnyConnect Module Selection** and **Profile Selection** sections in the **AnyConnect Configuration** page (Policy > Policy Elements > Results > Client provisioning > Resources > Add > AnyConnect Configuration > Select AnyConnect Package).
- You must log in to the SOURCEfire portal, create policies for endpoint groups, and download the AMP for endpoint software. The software comes preconfigured with the policies that you have chosen. You must download two images, namely, the redistributable version of the AMP for endpoint software for Windows OS and AMP for endpoint software for Mac OSX. The downloaded software is hosted on a server that is accessible from the enterprise network.

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

Step 2 Click the **Add** drop-down.

Step 3 Choose **AMP Enabler Profile** to create a new AMP enabler profile.

Step 4 Enter the appropriate values in the fields.

Step 5 Click **Submit** to save the profile in the **Resources** page.

Create an AMP Enabler Profile Using the Standalone Editor

To create an AMP enabler profile using the AnyConnect standalone editor.

Before You Begin

You can create an AMP enabler profile by uploading the XML format of the profile using the AnyConnect 4.1 standalone editor.

- Download the AnyConnect standalone profile editor for Windows and Mac OS from Cisco.com.
- Launch the standalone profile editor and enter the fields as specified in the AMP Enabler Profile Settings.
- Save the profile as an XML file in your local disk.
- Ensure that the **AMP Enabler** options are selected in the **AnyConnect Module Selection** and **Profile Selection** sections in the **AnyConnect Configuration** page (Policy > Policy Elements > Results > Client provisioning > Resources > Add > AnyConnect Configuration > Select AnyConnect Package).

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

Step 2 Click **Add**.

Step 3 Choose **Agent resources from local disk**.

Step 4 Choose **Customer Created Packages** from the **Category** drop-down.

Step 5 Choose **AMP Enabler Profile** from the **Type** drop-down.

Step 6 Enter a **Name** and **Description**.

Step 7 Click **Browse** and select the saved profile (XML file) from the local disk. The following example shows a customized install file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

The following example shows a customized uninstall file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

Step 8 Click **Submit**.

The newly created AMP Enabler profile is displayed in the **Resources** page.

Troubleshoot Common AMP Enabler Installation Errors

When you enter the SOURCEfire URL in the Windows or MAC Installer text box and click **Check**, you might encounter any of the following errors:

- Error Message: The certificate for the server containing the Mac/Windows installer file is not trusted by ISE. Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.

  This error message appears if you have not imported the SOURCEfire trusted certificate in to the Cisco ISE certificate store. Obtain a SOURCEfire trusted certificate and import it in to the Cisco ISE trusted certificate store (Administration > Certificates > Trusted Certificates).

- Error Message: The installer file is not found at this location, this may be due to a connection issue. Enter a valid path in the Installer text box or check your connection.

  This error message appears when the server hosting the AMP for Endpoint software is down or if there is a typographic error in the Windows Installer or MAC Installer text box.

- Error Message: The Windows/Mac installer text box does not contain a valid URL.

  This error message appears when you enter a syntactically incorrect URL format.

Create AnyConnect Configuration

AnyConnect configuration includes AnyConnect software and its associated configuration files. This configuration can be used in the client provisioning policy that allows users to download and install AnyConnect resources on the clients. If you use both ISE and an ASA to deploy AnyConnect, then the configurations must match on both headends.

Before You Begin

You must upload the AnyConnect package, compliance module, profiles, and optionally any customization and localization bundles before configuring an AnyConnect Configuration object.

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

Step 2 Click **Add** to create an AnyConnect configuration.

Step 3 Choose **AnyConnect Configuration**.

Step 4 Choose an AnyConnect Package, which you previously uploaded. For example, AnyConnectDesktopWindows xxx.x.xxxxx.x.

Step 5 Enter the name for the current AnyConnect Configuration. For example, AC Config xxx.x.xxxxx.x.

Step 6 Choose the compliance module, which you previously uploaded. For example, AnyConnectComplianceModulewindows x.x.xxxx.x

Step 7 Check one or more AnyConnect modules check boxes. For example, choose one or more modules from the following: ISE Posture, VPN, Network Access Manager, Web Security, AMP Enabler, ASA Posture, Start Before Log on (only for Windows OS), and Diagnostic and Reporting Tool.

Note Un-checking the VPN module under AnyConnect Module Selection does not disable the VPN tile in the provisioned client. You must configure VPNDisable_ServiceProfile.xml to disable the VPN tile on AnyConnect GUI. VPNDisable_ServiceProfile.xml is on CCO with the other AnyConnect files.

Step 8 Choose AnyConnect profiles for selected AnyConnect modules. For example, ISE Posture, VPN, NAM, and Web Security.

Step 9 Choose AnyConnect customization and localization bundles.

Step 10 Click **Submit**.

Create AnyConnect and Cisco NAC Agent Profiles

Use this procedure to create an AnyConnect or a NAC posture agent profile where you can specify parameters that define the agent behavior, parameters that are related to whether or not to refresh the client IP address, and for the posture protocol.

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

Step 2 Click **Add**.

Step 3 Choose **NAC AnyConnect Agent Posture Profile**.

Step 4 Choose **AnyConnect** or **NAC Agent**.

Step 5 Configure parameters for the following:

- Cisco ISE posture agent behavior
- Client IP Address Changes
- Cisco ISE posture protocol

Step 6 Click **Submit**.

Agent Profile Configuration Guidelines

Cisco recommends configuring agent profiles to control remediation timers, network transition delay timers, and the timer that is used to automatically close 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** to accomplish the same goal.

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

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

Agent Behavior Configuration

The following table describes the fields in the NAC or AnyConnect Posture Profile page, which allows you to configure parameters for the posture agent (AnyConnect and Cisco NAC Agent). The navigation path for this page is **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **NAC or AnyConnect Posture Profile**.

Field	Default Value	Mode (Applies only to Cisco ISE NAC Agent)	Usage Guidelines
Disable Agent Exit. (Not applicable for a Mac OS X client)	No	Merge	If the value is set to Yes, this setting prevents users from exiting the agent via the system tray.

Field	Default Value	Mode (Applies only to Cisco ISE NAC Agent)	Usage Guidelines
Enable Accessibility Mode (Not applicable for a Mac OS X client)	No—Agent does not interact with the Job Access with Speech (JAWS)	Merge	If the value is set to Yes, this setting enables compatibility with the JAWS screen reader. Users may experience a slight impact on performance when this feature is enabled. The agent still functions normally if this feature is enabled on a client machine that does not have the JAWS screen reader installed.
Enable signature check(Not applicable for a Mac OS X client)	No	Overwrite	If the value is set to Yes, this setting enables Windows to check the digital signature of the executables before launching the programs for remediation.
Bypass Summary Screen(Not applicable for a Mac OS X client)	Yes	Merge	

Field	Default Value	Mode (Applies only to Cisco ISE NAC Agent)	Usage Guidelines
Locale(Not applicable for a Mac OS X client)	Default	Merge	The default setting enables the agent to use the locale settings from the client operating system. If this setting is either the ID, the abbreviated name, or the full name of a supported language, the agent automatically displays the appropriate localized text in the agent dialogs on the client machine.
Posture report filter(Not applicable for a Mac OS X client)	Display Failed	Merge	If the value is set to Display Failed, the client posture assessment report display only remediation errors when the user clicks Show Details in the agent dialog. If the value is set to Display All, the client posture assessment report displays all the results when the user clicks Show Details in the agent dialog.

Field	Default Value	Mode (Applies only to Cisco ISE NAC Agent)	Usage Guidelines
Remediation timer	4	Overwrite	This setting specifies the time to remediate any failed posture assessment checks on the client machine before having to go through the entire login process again. The valid range is 1 to 300 minutes.
Network transition delay	3	Overwrite	This setting specifies the time to wait for the network transition (IP address change) to occur before beginning the remediation timer countdown. The vaild range is 2- 30 seconds.

Field	Default Value	Mode (Applies only to Cisco ISE NAC Agent)	Usage Guidelines
Log file size	5	Merge	This setting specifies file size in megabytes for the agent log files on the client machine. If the log file size is set to zero, the agent does not record any login or operation information for the user session on the client machine. If the log file size is other than zero, the agent records login and session information up to the specified number of megabytes.
Enable Auto Close. (Not applicable for AnyConnect)	No	Overwrite	if this setting is set to Yes, this setting allows the agent login dialog to close automatically following the user authentication.

Field	Default Value	Mode (Applies only to Cisco ISE NAC Agent)	Usage Guidelines
Auto close timer (Not applicable for AnyConnect)	0	Overwrite	This setting enables the agent login screen to wait for a specified period of time and close automatically following the user authentication. The valid range is 0 yo 30 seconds.

Note Merge parameter values with existing agent profile settings or overwrite them to appropriately configure agent behavior on Windows and Mac OS X clients.

Note Agent log files are stored in a directory on the client machine. After the first login session, two files reside in the directory: one backup file from the previous log in session, and one new file containing login and operation from the current session. If the log file for the current 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.

Supported Languages

Table 2: Supported Languages

Language	ID	Abbreviated Name	Full Name
English US	1033	en	English
Catalan	1027	ca	Catalan (Spain)
ChineseSimplified	2052	zh_cn	Chinese (Simplified)
ChineseTraditional	1028	zh_tw	Chinese (Traditional)
Czech	1029	cs	Czech
Danish	1030	da	Danish
Dutch	1043	nl	Dutch (Standard)

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

Client IP Address Refresh Configuration

The following table describes the fields in the NAC AnyConnect Posture Profile page, which allows you to configure parameters for the client to renew or refresh its IP address after VLAN change. The navigation path for this page is **Policy** > **Policy Elements** > **Resilts** > **Client Provisioning** > **Resources** > **Add** > **NAC or AnyConnect Posture Profile**.

Field	Default Value	Mode (Applies only to Cisco NAC Agent)	Usage Guidelines
VLAN detection interval	0, 5	Merge	

Field	Default Value	Mode (Applies only to Cisco NAC Agent)	Usage Guidelines
			This setting is the interval at which the agent check for the VLAN change. For the Windows NAC agent, the default value is 0. By default, the access to authentication VLAN change feature is disabled for Windows. The valid range is 0 to 5 seconds. For the Mac OS X agent, the default value is 5. By default, the access to authentication VLAN change feature is enabled with VlanDetectInteval as 5 seconds for Mac OS X. The valid range is 5 to 900 seconds. 0 —Access to Authentication VLAN change feature is disabled. 1 to 5—Agent sends an Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) query every 5 seconds. 6 to 900—An ICMP or ARP query is sent

Field	Default Value	Mode (Applies only to Cisco NAC Agent)	Usage Guidelines
			every x seconds.
Enable VLAN detection without UI (Not applicable for a Mac OS X client)	No	Merge	This setting enables or disables VLAN detection even when the user is not logged in. No—VLAN detect feature is disabled. Yes—VLAN detect feature is enabled.
Retry detection count	3	Merge	If the 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 or ARP	0 The valid range is 0 to 2.	Merge	This setting specifies the method used for detecting the client IP address change. 0—Poll using ICMP 1—Poll using ARP 2—Poll using ICMP first, then (if ICMP fails) ARP

Field	Default Value	Mode (Applies only to Cisco NAC Agent)	Usage Guidelines
Maximum timeout for ping	1 The valid range is 1 to 10 seconds.	Merge	Poll using ICMP, and if there is no response within the specified time, then declare an ICMP polling failure.
Enable agent IP refresh	Yes (Default)	Overwrite	This setting specifies whether or not the client machine to renew or refresh its IP address after the switch (or WLC) changes the VLAN for the login session of the client on the respective switch port.
DHCP renew delay	0 The valid range is 0 to 60 seconds.	Overwrite	This setting specifies that the client machine waits before attempting to request for a new IP address from the network DHCP server.
DHCP release delay	0 The valid range is 0 to 60 seconds.	Overwrite	The setting specifies that the client machine waits before releasing its current IP address.

Note Merge parameter values with existing agent profile settings or overwrite them to appropriately configure clients on Windows and Mac OS X clients for refreshing IP addresses.

Posture Protocol Settings

The following table describes the fields in the NAC AnyConnect Profile page, which allows you to configure the posture protocol settings. The navigation path for this page is **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **NAC Agent or AnyConnect Posture Profile**.

Field	Value	Mode	Usage Guidelines
Allow CRL Checks (Not applicable for a Mac OS X client)	Yes	Overwrite	If the value is set to No, this setting turns off checking the certificate revocation list (CRL) during discovery and negotiation.
MAC Address Exemption List (Not applicable for a Mac OS X client)	Enter MAC addresses separated by a comma. For example, AA:BB:CC:DD:EE:FF, 11:22:33:44:55:66	Merge	If you specify one or more MAC addresses in ths setting, the agent does not advertise those MAC addresses to Cisco ISE during login and authentication to help prevent sending unnecessary MAC addresses over th network.
Discovery Host (Not applicable for a Mac OS X client)	Enter the IP address or the fully qualified domain name (FQDN)	Overwrite	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.
Enable Discovery Host (Not applicable for a Mac OS X client)	Yes	Overwrite	Yes—User can specify a custom value in the Discovery Host field in the agent Properties dialog box. No—Ensure that the user cannot update the value in the Discovery Host field on the client machine.

Field	Value	Mode	Usage Guidelines
Server Name Rules	Enter the fully qualified domain name (FQDN) of the Cisco ISE server that are separated by a comma.	Merge	This field consists of comma-separated names of associated Cisco ISE servers. The agent uses the names in this list to authorize Cisco ISE access points. If this list is empty, then authorization is not performed. if any of the names is not found, then an error is reported.
Auto-generated MAC Address (Not applicable for a Mac OS X client)	—	Merge	This setting supports Evolution-Data Optimized connects on the client machine. if the client machine does not have an active network interface card, the agent creates a dummy MAC address for the system.
SWISS Timeout (Not applicable for a Mac OS X client)	1—Agent performs SWISS discovery as designed and no additional UDP response packet delay time out value is introduced.	Merge	If the value is set to greater than one, 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 makes this action to ensure that the network latency is not delaying the response packet en route. (SWISS Timeout only for UDP SWISS Timeouts)

Field	Value	Mode	Usage Guidelines
Disable L3 SWISS delay (Not applicable for a Mac OS X client)	No	Merge	If this setting is set to Yes, the agent disables the 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.
HTTP Discovery Timeout (Not applicable for a Mac OS X client)	30 (Default for Windows clients) The valid range is 3 seconds and above.	Merge	This setting specifies the HTTP discovery timeout for which the HTTPS discovery from the agent waits for the discovery response from Cisco ISE. if there is no response for the specified time, then the discovery process times out. If the value is set to 0, then the default client machine operating system timeout settings are used. If the value is set to 1 or 2, automatically the value is set to 3.

Field	Value	Mode	Usage Guidelines
HTTP Timeout (Not applicable for a Mac OS X client)	120 (Default for Windows clients) The valid range is 3 seconds and above.	Merge	This setting specifies the HTTP timeout for which the HTTP request from the agent waits for the response. if there is no response for the specified time, then the request times out, and the discovery process times out. If the value is set to 0, then the default client machine operating system timeout settings are used. If the value is set to 1 or 2, automatically the value is set to 3.

Client Login Session Criteria

Cisco 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.

Agent Download Issues on Client Machine

Problem

The client machine browser displays a “no policy matched” error message after user authentication and authorization. This issue applies to user sessions during the client provisioning phase of authentication.

Possible Causes

The client provisioning policy is missing required settings.

Posture Agent Download Issues

Remember that downloading the posture agent installer requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. (The client provisioning download page prompts for this.)
- The client machine must have Internet access.

Resolution

- Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent(s) defined in the policy. (Also ensure whether or not there is any agent profile configured under **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **NAC or AnyConnect Posture Profile**, even a profile with all default values.)
- Try re-authenticating the client machine by bouncing the port on the access switch.

Provision Client Machines with the Cisco NAC Agent MSI Installer

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

Step 1 Download the **nacagentsetup-win.msi** or **nacagentsetup-win.zip** installer file from the Cisco Software Download site from http://software.cisco.com/download/navigator.html and navigate to **Security** > **Access Control and Policy > Cisco Identityt Services Engine** > **Cisco Identity Services Engine Software > Release 1.x**.

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

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

Step 3 Place an Agent configuration XML file in the same directory as the Cisco NAC Agent MSI package.
If you are not connected to Cisco ISE, you can copy the **NACAgentCFG.xml** file from a client that has already been successfully provisioned. The file is located at C:\Program Files\Cisco\Cisco NAC Agent\NACAgentCFG.xml.

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

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

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

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

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

Cisco ISE Posture Agents

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

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

Posture Agent Discovery Request and Cisco ISE Response

Cisco ISE supports coexistence of AnyConnect and legacy Cisco ISE NAC agents on Windows and Mac OS x clients. Agents start the posture discovery probe only when there is any change in the network on the clients. Cisco ISE responds to the client's posture discovery probe based on the client provisioning policy and the corresponding agent will get the discovery response, which results in only one agent being active.

Based on the client provisioning policy, Cisco ISE differs in responding to the agents posture discovery probe as below:

- If the endpoint is configured to use the legacy agent (Cisco ISE NAC agent for Windows and Mac OS x), the agent receives the discovery response with a string "X-perfigo-CAS=FQDN" in the existing format. AnyConnect stops discovery, if the discovery response is received for the legacy agent.
- If the endpoint is configured to use AnyConnect, Cisco ISE responds in a different format. This will be the Cisco ISE Policy Service node FQDN and the AnyConnect Configuration URL, AnyConnect package location and version based on the client provisioning policy. The legacy agent stops discovery, if the response is received for AnyConnect.

Web Agent Posture Discovery Request and Cisco ISE Response

The Web agent does not do discovery probe. if an endpoint is configured to use the Web agent, Cisco ISE responds using the format, X-ISE-PDP-WEBAGENT=FQDN". The webagent discovery response is used to invoke the Cisco NAC Agent on the client, if the client provisioning policy is configured to use the Web agent.

Agent Displays “Temporary Access”

Problem

A client machine is granted “Temporary Access” to the network following login and authentication, but administrator and users expect full network access.

Possible Causes

This issue is applicable to any client machine login session using an agent to connect.

If the Cisco NAC Agent is running on the client and:

- The interface on the client machine goes down
- The session is terminated

Resolution

The user must try to verify network connectivity and then try to log in again (and pass through posture assessment, as well) to attempt to reestablish the connection.

Agent Fails to Initiate Posture Assessment

Problem

The user is presented with a “Clean access server not available” message. This issue applies to any agent authentication session from Cisco ISE.

Possible Cause

This error could mean that either the session has terminated or Cisco ISE is no longer reachable on the network.

Resolution

- The user can try to log into the network again.
- The user can try to ping the default gateway or the RADIUS server IP address or FQDN supplied by the network administrator.
- The administrator can check network access attributes for the user (like the assigned VLAN, ACLs, routing, execute the **nslookup** command on the client, client machine DNS connection, and so on).

AnyConnect

Cisco ISE uses an integrated module in AnyConnect for Cisco ISE posture requirements. AnyConnect is the posture agent that coexists with Cisco ISE NAC Agent on the same endpoint. Based on the client provisioning policy configuration in Cisco ISE, only one of the agents will be active at a time.

Note Cisco AnyConnect is not supported in CWA flow. It cannot be provisioned from the Guest portal using the **Require guest device compliance** field in the **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Device Compliance Settings** page. Instead, AnyConnect should be provisioned from the Client Provisioning portal as a result of redirection configured in authorization permissions.

To leverage Cisco ISE for integration with AnyConnect agent, Cisco ISE:

- Serves as a staging server to deploy AnyConnect, Version 4.0 and its future releases
- Interacts with AnyConnect posture component for Cisco ISE posture requirements
- Supports deployment of AnyConnect profiles, customization/language packages, and OPSWAT library updates for Windows and Mac OS x operating systems
- Supports AnyConnect and legacy agents at the same time

Cisco NAC Agent XML File Installation Directories

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

- The nac_login.xml file is available in the “C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login” directory.
- In the nacStrings_xx.xml file, the “xx” indicates the locale. You can find a complete list of the files in the “C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility” directory.

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

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 web sites for users to download files to fix their system, or simply distribute information and instructions.

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

Uninstall the Cisco NAC Agent from Windows 7 and Earlier Clients

The Cisco NAC Agent installs to **C:\Program Files\Cisco\Cisco NAC Agent** on the Windows client.

You can uninstall the agent in the following ways:

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

Uninstall the Cisco NAC Agent in a Windows 8 Client

You can uninstall Cisco NAC Agent in a Windows 8 client in Metro mode.

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:

a) Double Click **Cisco NAC Agent** and click **Uninstall**.
b) Select **Cisco NAC Agent** and click **Uninstall**.
c) Right Click **Cisco NAC Agent** and select **Uninstall**.

Windows 8 Metro and Metro App Support —Toast Notifications

The Enable Toast Notification option is available on the Cisco NAC Agent Tray Icon that can send relevant notifications to users on Windows 8 clients .
In Cisco NAC Agent scenarios where the user does not get network access, like "Remediation Failed" or "Network Access expired", the Agent displays the following toast notification:Network not available, Click "OK" to continue.

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

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

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

Cisco NAC Agent for Macintosh Clients

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

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

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

Uninstall the Cisco NAC Agent from Macintosh Clients

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

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

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

Step 3 Choose **Show Package Contents** and double-click **NacUninstall** to uninstall the Cisco NAC Agent on Mac OS X.

Cisco Web Agent

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

Users can launch the Cisco 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 in to the Cisco Web Agent, the Web Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client machine, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

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

Cisco NAC Agent Logs

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

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

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

Create an Agent Customization File for the Cisco NAC Agent

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

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

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

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

Step 2 Create a zip file called “brand-win.zip” that contains the assembled files. For example, in a Linux or Unix environment, execute the following: **zip -r brand-win.zip nac_login.xml nac_logo.gif nacStrings_en.xml nacStrings_cy.xml nacStrings_el.xml**

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

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

Custom nac_login.xml File Template

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

Use the following template to construct an appropriate "nac_login.xml" file to customize the logo, fields, and message text contained in a Cisco NAC Agent screen.

The following example shows a customized file.

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

Custom nacStrings_*xx*.xml File Template

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

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

The following example shows a customized nacStrings_xx.xml file.

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

```
again.</cueslookup:name>
<cueslookup:name key="downloadagent.report">Downloading the update of NAC
Agent.</cueslookup:name>
<cueslookup:name key="downloadagent.packagename.label">Package Name</cueslookup:name>
<cueslookup:name key="downloadagent.completed.label">Completed</cueslookup:name>
<cueslookup:name key="downloadagent.completed.value">%1 of %2 bytes</cueslookup:name>
<cueslookup:name key="downloadagent.speed.label">Speed</cueslookup:name>
<cueslookup:name key="downloadagent.speed.value">%1 bytes/sec</cueslookup:name>
<cueslookup:name key="updateopswat.rqst">NAC Agent Posture component version %1 is
available.%br% Do you want to install this update now?</cueslookup:name>
<cueslookup:name key="updateopswat.rqst.retry">Unable to update NAC Agent Posture component.
 Please try again.</cueslookup:name>
<cueslookup:name key="downloadopswat.report">Downloading the update of NAC Agnet Posture
component.</cueslookup:name>
<cueslookup:name key="login.productname">Education First Compliance Check</cueslookup:name>

<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.opswatversion">Posture Component Version</cueslookup:name>
<cueslookup:name key="login.username">Enter your username</cueslookup:name>
<cueslookup:name key="login.password">Enter your PIN</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Custom EF package version 2.1.1.1 with EF
Logo</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
<cueslookup:name key="menu_devtools">Dev Tools</cueslookup:name>
<cueslookup:name key="c.sso.ad">Performing Windows Domain automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.generic">Unknown authentication type</cueslookup:name>
<cueslookup:name key="c.sso.macauth">Performing device filter automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.vpn">Performing automatic login into NAC environment for remote
 user</cueslookup:name>
<cueslookup:name key="c.title.status.authenticating">Authenticating User</cueslookup:name>

<cueslookup:name key="c.title.status.answeringchallenge">Sending Response</cueslookup:name>

<cueslookup:name key="c.title.status.checking">Checking Requirements</cueslookup:name>
<cueslookup:name key="c.title.status.checkcomplete">System Check Complete</cueslookup:name>

<cueslookup:name key="c.title.status.loggedin">NAC Process Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netaccess.none">NAC Process Completed</cueslookup:name>

<cueslookup:name key="c.title.status.netpolicy">Network Usage Policy</cueslookup:name>
<cueslookup:name key="c.title.status.properties">Agent Properties &#x0026;
Information</cueslookup:name>
<cueslookup:name key="c.title.status.remediating">Remediating System</cueslookup:name>
<cueslookup:name key="c.title.status.session.expired">Session has Expired</cueslookup:name>

<cueslookup:name key="c.title.status.update.available">Update Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.downloading">Downloading Agent</cueslookup:name>

<cueslookup:name key="c.title.status.update.opswat.available">Update Posture
Component</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.downloading">Downloading Posture
Component</cueslookup:name>
<cueslookup:name key="scanning">Checking</cueslookup:name>
<!-- <cueslookup:name key="scanningitemcomplete">Finished Checking</cueslookup:name> -->
<cueslookup:name key="ph.about">About</cueslookup:name>
<cueslookup:name key="ph.cancel">Cancel</cueslookup:name>
<!-- <cueslookup:name key="ph.details">Details</cueslookup:name> -->
<cueslookup:name key="ph.logout">Logout</cueslookup:name>
<cueslookup:name key="title_remediating">Remediating System</cueslookup:name>
<cueslookup:name key="title_check_conplete">System Check Complete</cueslookup:name>
<cueslookup:name key="title_full_access_granted">Logged In</cueslookup:name>
<cueslookup:name key="title_access_denied">Network Access Denied</cueslookup:name>
<cueslookup:name key="tempNetAccess">Temporary Network Access</cueslookup:name>
<cueslookup:name key="announcePleaseBePatient">Please be patient while your system is checked
 against the network security policy
</cueslookup:name>
```

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

```
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">
There is at least one mandatory requirement failing.
You are required to update your system before
you can access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">
Network Usage Terms and Conditions are rejected. You will not be
allowed to access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">
Restricted Network Access granted.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">
You have been granted restricted network access because your device
did not conform with all the security policies for this protected
network and you have opted to defer updating your system. It is recommended
that you update your system at your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">
Temporary Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">
Please be patient while your system is checked against the network security policy.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">
There is at least one mandatory requirement failing.
You are required to update your system otherwise
your network access will be restricted.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">
Temporary Access to the network has expired.
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose">
 
</cueslookup:name>
<cueslookup:name key="ia.status.checkcomplete">
Finished Checking Requirements
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress">
Please be patient while we determine if your system is compliant with the security policy
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress.01">
Checking %1 out of %2
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicy">
Access to the network requires that you view and accept the following
Network Usage Policy
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicylinktxt">
Network Usage Policy Terms and Conditions
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.inprogress">
Remediating
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.start">
```

```
Please Remediate
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.checkinprogress">
Checking for compliance with Requirement
</cueslookup:name>
<cueslookup:name key="ia.table.name">
Name
</cueslookup:name>
<cueslookup:name key="ia.table.location">
Location
</cueslookup:name>
<cueslookup:name key="ia.table.software">
Software
</cueslookup:name>
<cueslookup:name key="ia.table.software.programs">
program(s)
</cueslookup:name>
<cueslookup:name key="ia.table.update">
Update
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.nochange">
Do not change current setting
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforedownload">
Notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforeinstall">
Notify before install
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.scheduledinstallation">
Download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforedownload">
Change to notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforeinstall">
Change to notify before installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcescheduledinstall">
Change to download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.description">
Description
</cueslookup:name>
<cueslookup:name key="scs.table.title">
Security Compliance Summary
</cueslookup:name>
<cueslookup:name key="scs.table.header1.scan_rslt">
Scan Result
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_name">
Requirement Name
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_details">
Requirement Description - Remediation Suggestion
</cueslookup:name>
<cueslookup:name key="scs.table.data.mandatory">
Mandatory
</cueslookup:name>
<cueslookup:name key="scs.table.data.optional">
Optional
</cueslookup:name>
<cueslookup:name key="scs.table.data.pass">
Passed
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_download">
Please download and install the optional software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_download">
Please download and install the required software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_launch">
Please launch the optional remediation program(s) before accessing the network
```

```
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_launch">
Please launch the required remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
 the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
 the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_win_update">
Please download and install the optional windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_win_update">
Please download and install the required windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_prog">
Launching Remediation Program(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_url">
Launching Remediation URL...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_av">
Updating Virus Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_as">
Updating Spyware Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_win_update">
Launching Windows auto Update(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_launch_downloaded_file">
Downloaded at %1. %br% Please open this folder &#x0026; double-click executable file to
install the required software.
</cueslookup:name>
<cueslookup:name key="discoveryhost.label">
Discovery Host
</cueslookup:name>
<cueslookup:name key="properties.table.title">
List of Antivirus &#x0026; Anti-Spyware Products Detected by the Agent
</cueslookup:name>
<cueslookup:name key="properties.table.header1.index">
No.
</cueslookup:name>
<cueslookup:name key="properties.table.header1.description">
Description
</cueslookup:name>
<cueslookup:name key="properties.table.header1.value">
Value
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_type">
Product Type
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_name">
Product Name
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_version">
Product Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_version">
Definition Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_date">
```

```
Definition Date
</cueslookup:name>
<cueslookup:name key="reboot.mandatory.001">
Mandatory System Reboot Required
</cueslookup:name>
<cueslookup:name key="reboot.optional.001">
You need to reboot your system in order for the changes to take effect.
</cueslookup:name>
<cueslookup:name key="rem.error.001">
Unable to remediate particular requirement
</cueslookup:name>
<cueslookup:name key="rem.error.av_access_denied">
The remediation you are attempting is reporting an access denied error. This is usually due
 to a privilege issue. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_buffer_too_small">
The remediation you are attempting has failed with an internal error. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_elevation_required">
The remediation you are attempting requires elevation. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_failed">
The remediation you are attempting had a failure. If the problem persists contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_internal_error">
The remediation you are attempting has reported an internal error. If this problem persists
 please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_implemented">
The remediation you are attempting is not implemented for this product. Please contact your
 system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_supported">
The remediation you are attempting is not supported for this product. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_faile">
The AV/AS update has failed. Please try again and if this message continues to display
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_failed_due_to_network">
The AV/AS update failed due to a networking issue. Please try again and if this message
continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_timeout">
The remediation you are attempting has timed out waiting for the operation to finish. If
this continues please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_dist_size_error">
The size of the downloaded file does not match the package! Please discard downloaded file
 and check with your administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_is_not_signed">
The file that has been requested was not digitally signed. Please try again and if this
message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_save_location_error">
The location for the file to be saved to can not be written. Please choose a different
location.
</cueslookup:name>
<cueslookup:name key="rem.error.http_file_not_found">
The requested file is not found. Please try again and if this problem persists, contact
your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.launch_file_not_found">
The file that has been requested could not be launched either because it could not be found
 or there was a problem launching it. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.malformed_URL">
The file that is trying to be downloaded has an incorrect URL. Please contact your system
```

```
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.network_error">
There has been a network error, please try the remediation again. If this message continues
 to be seen contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.update_fail_for_non_admin">
The remediation you are trying to do can not be accomplished at your user level. Please
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.wsus_search_failure">
The WSUS search failed. This is probably due to a network issue. Please try again and if
this message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="server.error.generic">
Agent encountered problems logging user
</cueslookup:name>
<cueslookup:name key="server.error.255">
Network Error: NAC Server could not establish a secure connection to NAC Manager.
This could be due to one or more of the following reasons:
1) NAC Manager certificate has expired or
2) NAC Manager certificate cannot be trusted or
3) NAC Manager cannot be reached or
4) NAC Manager is not responding
Please report this to your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5000">
Invalid provider name
</cueslookup:name>
<cueslookup:name key="server.error.5001">
Failed to add user to online list
</cueslookup:name>
<cueslookup:name key="server.error.5002">
Server communication error
</cueslookup:name>
<cueslookup:name key="server.error.5003">
Invalid username or password
</cueslookup:name>
<cueslookup:name key="server.error.5004">
Unknown user
</cueslookup:name>
<cueslookup:name key="server.error.5005">
Account expired
</cueslookup:name>
<cueslookup:name key="server.error.5006">
Account currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5007">
Exceed quota limit
</cueslookup:name>
<cueslookup:name key="server.error.5008">
Insufficient Clean Access packages installed
</cueslookup:name>
<cueslookup:name key="server.error.5009">
Access to network is blocked by the administrator
</cueslookup:name>
<cueslookup:name key="server.error.5010">
Vulnerabilities not fixed
</cueslookup:name>
<cueslookup:name key="server.error.5011">
This client version is old and not compatible. Please login from web browser to see the
download link for the new version.
</cueslookup:name>
<cueslookup:name key="server.error.5012">
Network policy is not accepted
</cueslookup:name>
<cueslookup:name key="server.error.5013">
Invalid switch configuration
</cueslookup:name>
<cueslookup:name key="server.error.5014">
Too many users using this account
</cueslookup:name>
<cueslookup:name key="server.error.5015">
```

```
Invalid session
</cueslookup:name>
<cueslookup:name key="server.error.5016">
Null session
</cueslookup:name>
<cueslookup:name key="server.error.5017">
Invalid user role
</cueslookup:name>
<cueslookup:name key="server.error.5018">
Invalid login page
</cueslookup:name>
<cueslookup:name key="server.error.5019">
Encoding failure
</cueslookup:name>
<cueslookup:name key="server.error.5020">
A security enhancement is required for your Agent. Please upgrade your Agent or contact
your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5021">
Can not find server reference
</cueslookup:name>
<cueslookup:name key="server.error.5022">
User role currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5023">
Authentication server is not reachable
</cueslookup:name>
<cueslookup:name key="server.error.5024">
Agent user operating system is not supported
</cueslookup:name>
<cueslookup:name key="server.error.generic_emergency">
The Agent has encountered an unexpected error and is restarting.
</cueslookup:name>
<cueslookup:name key="server.error.http_error">
Clean Access Server is not available on the network.
</cueslookup:name>
<cueslookup:name key="server.error.nw_interface_chg">
Authentication interrupted due to network status change. Press OK to retry.
</cueslookup:name>
<cueslookup:name key="server.error.svr_misconfigured">
Clean Access Server is not properly configured.
</cueslookup:name>
<cueslookup:name key="server.clarification.generic_emergency">
Please contact your administrator if the problem persists.
</cueslookup:name>
<cueslookup:name key="announce.savingreport">
Saving Report
</cueslookup:name>
<cueslookup:name key="announce.savingreport.failed">
Unable to save report
</cueslookup:name>
<cueslookup:name key="announce.cancelremediationack">
Clicking Cancel may change your network connectivity and interrupt download or required
updates.<p> Do you want to continue?</p>
</cueslookup:name>
<cueslookup:name key="announce.dismiss.default">
Dismiss to continue
</cueslookup:name>
<cueslookup:name key="announce.logoutconfirm">
Successfully logged out from the network!
</cueslookup:name>
</cueslookup:appstrings>
```

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

Sample Extended 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>
```

UpdateFeed.xml Descriptor File Template

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

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

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:update="http://www.cisco.com/cpm/update/1.0">

<title>Provisioning Update</title>
<updated>2011-12-21T12:00:00Z</updated>
<id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
<author>
<name>Cisco Support</name>
```

```
<email>support@cisco.com</email>
</author>
<!-- Custom Branding -->
<entry>
<id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/7</id>
<title>Agent Customization Package</title>
<updated>2010-06-07T12:00:00Z</updated>
<summary>This is EF Agent Customization Package 1.1.1.7</summary>
<link rel="enclosure" type="application/zip" href="brand-win.zip" length="18884" />
<update:type>AgentCustomizationPackage</update:type>
<update:version>1.1.1.7</update:version>
<update:os>WINDOWS_ALL</update:os>
</entry>
</feed>
```

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

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

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.

Configure Client Provisioning Resource Policies

For clients, the 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.

For AnyConnect, resources can be selected either from the client provisioning resources page to create an AnyConnect configuration that you can use it the client provisioning policy page. AnyConnect configuration is the AnyConnect software and its association with different configuration files that includes AnyConnect binary package for Windows and Mac OS X clients, compliance module. module profiles, customization and language packages for AnyConnect.

For Cisco ISE NAC agents, resources can be selected from the client provisioning policy page.

Before You Begin

- Before you can create effective client-provisioning resource policies, ensure that you have added resources to Cisco ISE. When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.
- Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect to is hidden, check the **Enable if target network is hidden** check box from the iOS Settings area.

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

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

- **Enable—**Ensures Cisco ISE uses this policy to help fulfill client-provisioning functions when users log in to the network and conform to the client-provisioning policy guidelines.
- **Disable—**Cisco ISE does not use the specified resource policy to fulfill client-provisioning functions.
- **Monitor—**Disables the policy and “watches” the client-provisioning session requests to see how many times Cisco ISE tries to invoke based on the “Monitored” policy.

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

Step 4 Specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.
You can choose to specify the Any identity group type, or choose one or more groups from a list of existing Identity Groups that you have configured.

Step 5 Use the Operating Systems field to specify one or more operating systems that might be running on the client machine or device through which the user is logging into Cisco ISE.
You can choose to specify a single operating system like "Android" , "Mac iOS', and "Mac OS X" or an umbrella operating system designation that addresses a number of client machine operating systems like "Windows XP (All)" or "Windows 7 (All)."

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

Step 7 For client machines, use **Agent Configuration** to specify which agent type, compliance module, agent customization package, and/or profile to make available and provision on the client machine.

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

Step 8 Click **Save**.

What to Do Next

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

Configure Cisco ISE Posture Agent in the Client Provisioning Policy

For client machines, configure which agent type, compliance module, agent customization package, and/or profile to make available and provision for users to download and install on the client machine.

Before You Begin

You must have added client provisioning resources for AnyConnect and Cisco ISE NAC in Cisco ISE.

Step 1 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. The **Is Upgrade Mandatory** setting only applies to agent downloads. Agent profile, compliance module, and Agent customization package updates are always mandatory.

Step 2 Choose an existing agent profile from the **Profile** drop-down list.

Step 3 Choose an available compliance module to download to the client machine using the **Compliance Module** drop-down list.

Step 4 Choose an available agent customization package for the client machine from the **Agent Customization Package** drop-down list.

Configure Native Supplicants for Personal Devices

Employees can connect their personal devices to the network directly using native supplicants, which are available for Windows, Mac OS, iOS, and Android devices. For personal devices, specify which Native Supplicant configuration to make available and provision on the registered personal device.

Before You Begin

Create native supplicant profiles so that when user log in, based on the profile that you associate with that users authorization requirements , Cisco ISE provides the necessary supplicant provisioning wizard to set up the users personal devices to access the network.

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

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

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

Step 4 Specify the following:

- Use the Identity Groups field to specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.
- Use the Operating System field to specify one or more operating systems that might be running on the personal device through which the user is logging into Cisco ISE.
- Use the Other Conditions field to specify a new expression that you want to create for this particular resource policy.

Step 5 For personal devices, use **Native Supplicant Configuration** to choose the specific **Configuration Wizard** to distribute to these personal devices.

Step 6 Specify the applicable **Wizard Profile** for the given personal device type.

Step 7 Click **Save**.

Client Provisioning Reports

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

Client Provisioning Requests

The **Operations** > **ReportsISE ReportsEndpoints and UsersClient Provisioning** report displays statistics about successful and unsuccessful client provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data.

Supplicant Provisioning Requests

The **Operations** > **Reports** > **ISE Reports** > **Endpoints and Users** > **Supplicant Provisioning** window displays information about recent successful and unsuccessful user device registration and supplicant provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting supplicant provisioning data.

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 at Date and Time,

Identity (user ID), IP Address, MAC Address (endpoint ID), Server, profile, Endpoint Operating System, SPW Version, Failure Reason (if any), and the Status of the registration.

Client Provisioning Event Logs

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