

Customize and Localize Secure Client and Installer

- Modify Cisco Secure Client Installation Behavior, on page 1
- Enable DSCP Preservation, on page 8
- Set Public DHCP Server Route, on page 9
- Customize the Cisco Secure Client GUI Text and Messages, on page 9
- Create Custom Icons and Logos for the Cisco Secure Client GUI, on page 17
- Create and Upload the Cisco Secure Client Help File, on page 23
- Write and Deploy Scripts, on page 24
- Write and Deploy Custom Applications with the Cisco Secure Client API, on page 28
- Use the Cisco Secure Client CLI Commands, on page 28

Modify Cisco Secure Client Installation Behavior

Disable Customer Experience Feedback

The Customer Experience Feedback module is enabled by default. This module provides Cisco with anonymous information about what features and modules customers have enabled and are using. This information gives us insight into the user experience so that Cisco can continue to improve quality, reliability, performance, and user experience.

To manually disable the Customer Experience Feedback module, create a CustomerExperience_Feedback.xml file using the standalone profile editor. You must stop the Cisco Secure Client service, name the file CustomerExperience_Feedback.xml, and put it in the C:\ProgramData\Cisco\Cisco Secure Client\CustomerExperienceFeedback\ directory. When the file is created with the disable flag set, you can manually deploy this to Cisco Secure Client. To check the results, open the Cisco Secure Client About menu and verify that the Customer Experience Feedback module is not listed in the Installed Module section.

You can disable the Customer Experience Feedback module using:

- A Customer Feedback Experience module client profile—Uncheck Enable Customer Experience Feedback Service, and distribute the profile.
- An MST file—Extract secureclient-win-disable-customer-experience-feedback.mst from secureclient-vpn-transforms-X.X.xxxxx.zip.

Modify Installation Behavior, Windows

Use the following Windows installer properties to modify Cisco Secure Client installation behavior. In the ISO image, the installer program setup.hta is HTML and can be edited.



Note Cisco Secure Client does not support Windows Installer ADVERTISE mode.

- Command-Line Parameters—One or more properties are passed as parameters on the command-line installer, msiexec. This method is for predeployment; it is not supported by web deployment.
- Installer Transform—You can modify the installer property table with a transform. Several tools are available to create transforms; one common tool is Microsoft Orca. The Orca tool is part of the Microsoft Windows Installer Software Development Kit (SDK), which is included in the Microsoft Windows SDK. To get the Windows SDK, browse to http://msdn.microsoft.com, and search for the SDK for your version of Windows.

  Transforms can be used for predeploy only. (Only Cisco signed transforms will work for web deploy when the downloader invokes the installer.) You can apply your own transforms through the out-of-band methods, but the details are outside the scope of this guide.

Limitations

The Cisco Secure Client uninstall prompt is not customizable.

Windows Installer Properties That Customize Client Installations

The following Windows installer properties customize Cisco Secure Client installations. Bear in mind that there are many other Windows installer properties supported by Microsoft that you can use.

- Restrict VPN upgrade—With an active VPN session, you can set the VPN installer property (RESTRICT_SOFTWARE_UPDATE_IF_VPN_SESSION_ACTIVE) to 1 to restrict an upgrade. By default, VPN upgrades occur when a session is active and a later released version is deployed using out-of-band mechanisms.
- Resetting the System MTU—When the VPN installer property (RESET_ADAPTER_MTU) is set to 1, the installer resets all Windows network adapter MTU settings to their default value. The system must be rebooted for the changes to take effect.
- Setting Windows Lockdown—Cisco recommends that end users be given limited rights to the Cisco Secure Client on their device. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping the Cisco Secure Client services. You can also stop the services from the command prompt with the service password.

  The MSI installers for VPN, Network Access Manager, Network Visibility Module, and Umbrella Roaming Security Module support a common property (LOCKDOWN). When LOCKDOWN is set to a non-zero value, Windows service(s) associated with that installer cannot be controlled by users or local administrators on the endpoint device. We recommend using the sample transform that we provide to set this property, and apply the transform to each MSI installer that you want to have locked down. You can download the sample transforms from the Cisco Secure Client software download page.

If you deploy the core client plus one or more optional modules, you must apply the LOCKDOWN property to each of the installers. This operation is one way only and cannot be removed unless you re-install the product.

- Hiding Cisco Secure Client from the Add/Remove Program List—You can hide the installed Cisco Secure Client modules from a user's Add/Remove Programs list in the Windows Control Panel. Passing ARPSYSTEMCOMPONENT=1 to the installer prevents that module from appearing in the list of installed programs.

  We recommend that you use the sample transform we provide to set this property, applying the transform to each MSI installer for each module that you want to hide. You can download the sample transforms from the Cisco Secure Client software download page.

Import a Customized Installer Transform to the Secure Firewall Adaptive Security Appliance

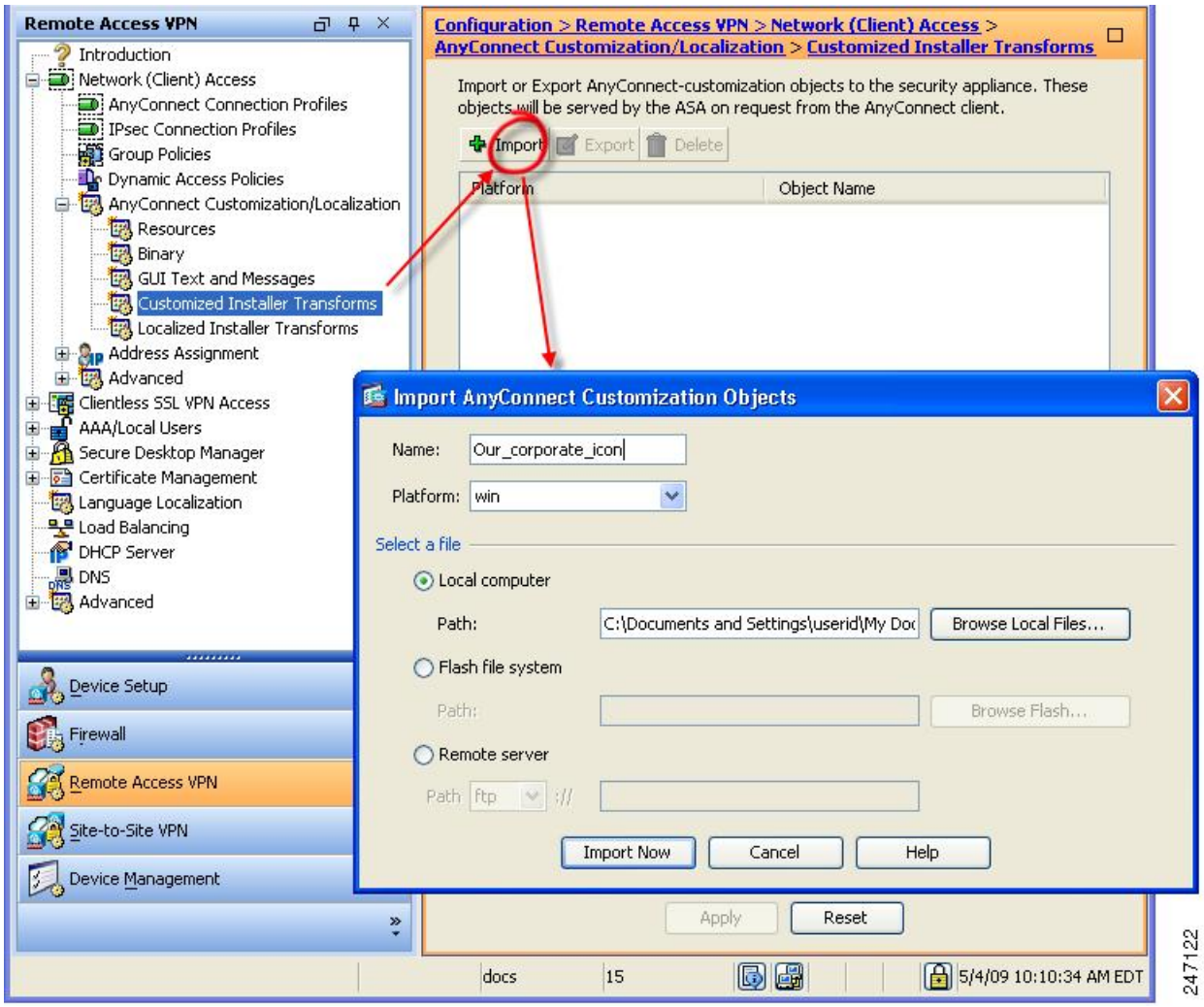
Importing a Cisco provided Windows transform to the Secure Firewall ASA allows you to use it for web deployment.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Customized Installer Transforms**.

Step 2 Click **Import**.

The Import AnyConnect Customization Objects windows displays:



Step 3 Enter the name of the file to import. The name of the transform file determines to which module the installer transform file applies. You can apply transforms globally or per module with the following syntax:

a) *_name*.mst: applied to all installers

b) <moduleid>*_name*.mst: applied to a single module installer

c) *name*.mst: applied to the VPN installer only

Step 4 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table of installer transforms.

What to do next

If the transform file is incorrect, the installation/upgrade process for remote Windows users may fail with a *Failed to install Cisco Secure Client* error. This error represents itself in the DART file as DOWNLOADER_ERROR_INTEGRITY_CHECK_FAILED.

Localize the Cisco Secure Client Installer Screens

You can translate the messages displayed by the Cisco Secure Client installer. The Secure Firewall ASA uses a transform to translate the messages displayed by the installer. The transform alters the installation but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.



Note Every release of Cisco Secure Client includes a localized transform that administrators can upload to the Secure Firewall ASA whenever they upload Cisco Secure Client packages with new software. If you are using our localization transform, make sure to update them with the latest release from cisco.com whenever you upload a new Cisco Secure Client package.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the Cisco Secure Client software download page at cisco.com:

`secureclient-win-<VERSION>-webdeploy-k9-lang.zip`

In this file, <VERSION> is the version of Cisco Secure Client release.

The archive contains the transforms (.mst files) for the available translations. If you need to provide a language to remote users that is not one of the 30 languages we provide, you can create your own transform and import it to the Secure Firewall ASA as a new language. With Orca, the database editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK.

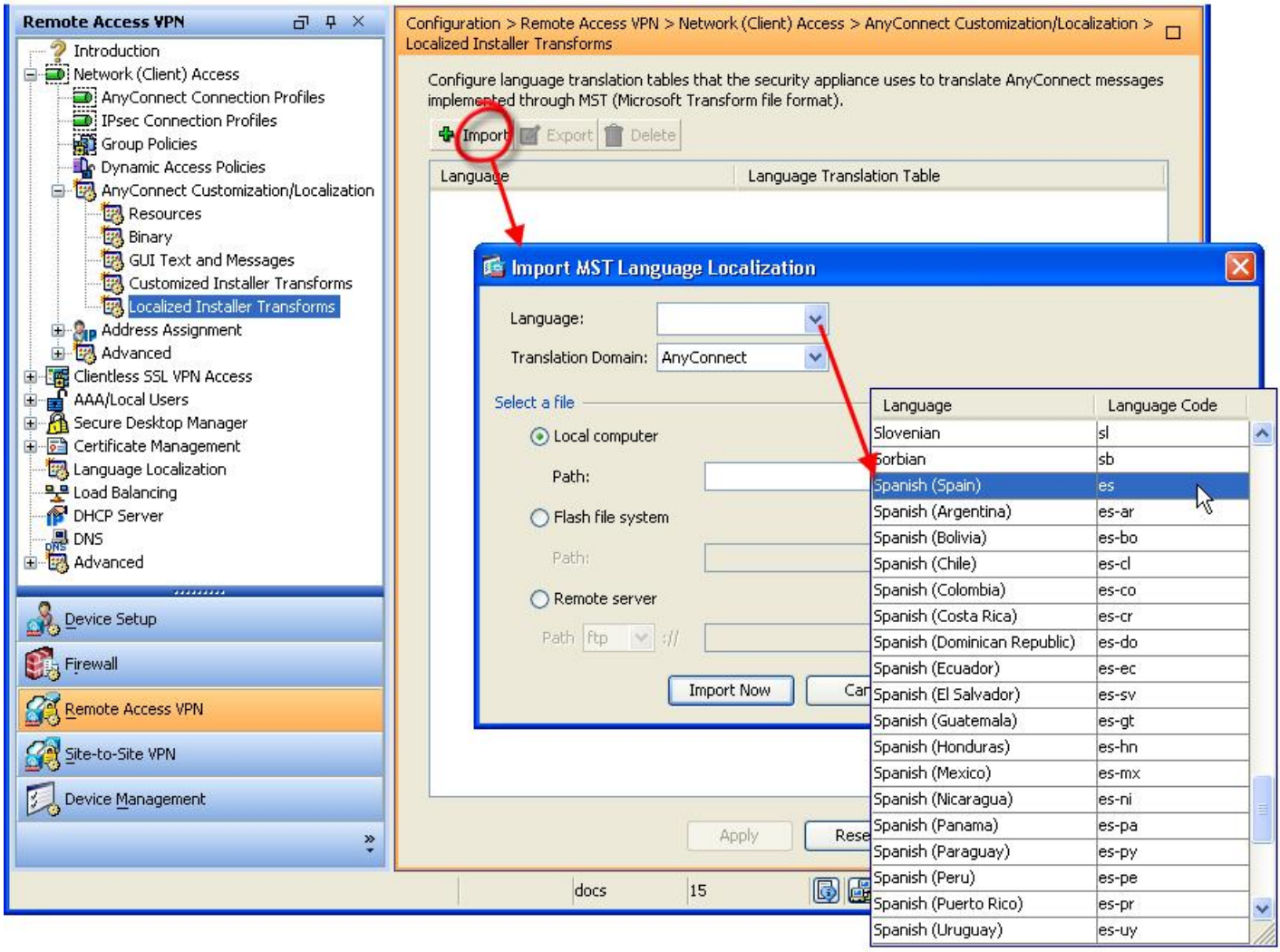
Import a Localized Installer Transform to the Secure Firewall ASA

The following procedure shows how to import a transform to the Secure Firewall ASA using ASDM.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Localized Installer Transforms**.

Step 2 Click **Import**. The Import MST Language Localization window opens:



Step 3 Click the **Language** drop-down list to choose a language (and the industry-recognized abbreviation) for this transform. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

Step 4 Click **Import Now**.
A message displays saying you successfully imported the table.

Step 5 Click **Apply** to save your changes.

In this procedure we specified the language as Spanish (es). The following illustration shows the new transform for Spanish in the list of Languages for Cisco Secure Client.



Modify Installation Behavior, macOS

The Cisco Secure Client installer cannot be localized. The strings used by the installer come from the macOS installer application, not the Cisco Secure Client installer.

Note You cannot manipulate the optional module selection that is seen by the user in the installer UI. Changing the default optional module selection in the installer UI requires editing of the installer, which would then invalidate the signature.

Customize Installer Behavior on macOS with ACTransforms.xml

No standard way to customize .pkg behavior is provided for macOS, so we created ACTransforms.xml. When this XML file is positioned with the installer, the installer reads this file before running the installation. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

1. In a “Profile” directory in the same directory as the .pkg installer file.
2. In a “Profile” directory in the root of a mounted disk image volume.
3. In a “Profile” directory in the root of a mounted disk image volume.

The XML file has this format:

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

For example, the macOS ACTransforms.xml property is DisableVPN to create a “stand-alone” deployment of Network Visibility Module. ACTransforms.xml is in the Profiles directory in the DMG file.

Disable the Customer Experience Feedback Module

The Customer Experience Feedback module is enabled by default. To switch this feature off on macOS:

Procedure

Step 1 Convert the dmg package from read-only to read-write using Disk Utility or hdiutil. For example:

```
hdiutil convert cisco-secure-client-macosx-version-predeploy-k9.dmg -format UDRW -o
cisco-secure-client-macosx-version-predeploy-k9-rw.dmg
```

Step 2 Edit ACTransforms.xml, and set or add the following value, if it is not already set.

```
<DisableCustomerExperienceFeedback>false</DisableCustomerExperienceFeedback>
```

Modify Installation Behavior, Linux

Customizing Installer Behavior on Linux with ACTransform.xml

No standard way to customize .pkg behavior is provided for Linux, so we created ACTransforms.xml. When this XML file is positioned with the installer, the installer reads this file before running the installation. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

- In a “Profile” directory in the same directory as the .rpm/.deb installer file
- In a “Profile” directory in the root of a mounted disk image volume

The XML file, ACTransforms.xml, in the Profiles directory in the predeployment package has this format:

```
<ACTransforms>

<PropertyName1>Value</PropertyName1>

<PropertyName2>Value</PropertyName2>

</ACTransforms>
```

Enable DSCP Preservation

You can set a custom attribute to control Differentiated Services Code Point (DSCP) on Windows or macOS platforms for DTLS connection only. DSCP preservation allows devices to prioritize latency sensitive traffic; the router takes into account whether this is set and marks prioritized traffic to improve outbound connection quality.

The custom attribute type is DSCPPreservationAllowed, and the valid values are True or False.

Note By default Cisco Secure Client performs DSCP preservation (True). To disable it, set the custom attribute value to false on the headend and reinitiate the connection.

This feature is configured in ASDM at **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes**. Refer to the *Enable DSCP Preservation* section in the appropriate release of the Cisco ASA Series VPN ASDM Configuration Guide for the configuration process.

Set Public DHCP Server Route

To allow local DHCP traffic to flow in the clear when Tunnel All Network is configured, Cisco Secure Client adds a specific route to the local DHCP server when the client connects. To prevent data leakage on this route, Cisco Secure Client also applies an implicit filter on the LAN adapter of the host device, blocking all traffic for that route except DHCP traffic. If you are connecting to the external interface and using a local DHCP server once a connection is established, a specific route to that server is created, pointing to the NIC and not the virtual adapter. If other services are running on the same server (such as WINS or DNS), this route breaks these services after the VPN session is established.

On Windows, by setting a group policy custom attribute, you can control the creation of the public DHCP server route. The no-dhcp-server-route custom attribute must be present and set to true to avoid creating the public DHCP server route upon tunnel establishment.

This feature is configured in ASDM at **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes**. Refer to the appropriate release of the Cisco ASA Series VPN ASDM Configuration Guide for the configuration process.

Customize the Cisco Secure Client GUI Text and Messages

The Secure Firewall ASA uses translation tables to translate user messages displayed by Cisco Secure Client. The translation tables are text files with strings of translated message text. You can edit existing messages or add additional languages using ASDM or using transforms (for Windows).

The following Windows sample transforms for localization are available on www.cisco.com:

- Language localization transform files for predeploy package for Windows platforms
- Language localization transform files for web-deploy package for Windows platforms

The Cisco Secure Client package file for Windows contains a default English language template for Cisco Secure Client messages. The Cisco Secure Firewall ASA automatically imports this file when you load the Cisco Secure Client package on the ASA. This template contains the latest changes to message strings in the Cisco Secure Client software. You can use it to create new translation tables for other languages, or you can import one of the following translation tables available on www.cisco.com (see Import Translation Tables to the Secure Firewall ASA, on page 13):

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Dutch
- French
- French (Canadian)
- German
- Hungarian
- Italian

- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Russian
- Spanish (Latin American)

In Cisco Secure Client release 5.0, default localization files for various languages are included with installation. Refer to Localization on Desktop Devices, on page 11.

The following sections contain procedures for translating GUI text and messages if the desired languages are not available or if you wish to further customize imported translation tables:

- Add or Edit the AnyConnect Text and Messages. You can make changes to the message file by adding or editing the file to change message text for one or more message IDs in one of the following ways:
  - Typing your changes into the text in the open dialog.
  - Copying the text in the open dialog to a text editor, making your changes, and pasting the text back into the dialog.
- Import Translation Tables to the Secure Firewall ASA, on page 13. You can export the message file by clicking Save to File, editing the file, and importing it back into the ASDM.

After you update the translation table on the Secure Firewall ASA, the updated messages are not applied until the client is restarted and makes another successful connection.



Note If you are not deploying the client from the Secure Firewall ASA and are using a corporate software deployment system such as Altiris Agent, you can manually convert the Cisco Secure Client translation table (anyconnect.po) to a .mo file using a catalog utility such as Gettext and install the .mo file to the proper folder on the client computer. See "Create Message Catalogs for Enterprise Deployment" section on page 3-22 for more information.

Guidelines and Limitations

Cisco Secure Client is not fully compliant with all internationalization requirements, exceptions include:

- Date/Time formats do not always follow locale requirements.
- Right to left languages are not supported.
- Some strings are truncated in the UI due to hardcoded field lengths.
- A few hardcoded English strings remain such as:
  - Status messages, when updating.
  - Untrusted server messages.
  - Deferred update messages.

Localization on Desktop Devices

With Cisco Secure Client installation, default localization files for various languages are included. The Secure Client will use string localization from ASDM if available. If that language file is not available, the Secure Client uses the default embedded language matching the provided system locale language. If no match is found, English is used.

When Cisco Secure Client gets the translations from ASA, it will try to fill in any translation gaps using the default translations. For example, if administrators have strings that they didn't provide, Cisco Secure Client will still translate, if the string is part of the default translations. Localization data is provided for these languages by default:

- Canadian French (Canada) — (fr-CA)
- Chinese (China) — (zh-CN)
- Chinese (Simplified) — (zh-HANS)
- Chinese (Taiwan) — (zh-TW)
- Chinese (Traditional) — (zh-HANT)
- Czech (Czech Republic) — (cs-CZ)
- Dutch (Netherlands) — (nl-nNL)
- French (France) — (fr-FR)
- German (Germany) — (de-DE)
- Hungarian (Hungary) — (hu-HU)
- Italian (Italy) — (it-IT)
- Japanese (Japan) — (ja-JP)
- Korean (Korea) — (ko-KR)
- Polish (Poland) — (pl-PL)
- Portuguese (Brazil) — (pt-BR)
- Russian (Russia) — (ru-RU)
- Spanish (Spain) — (es-ES)

Add or Edit the Cisco Secure Client Text and Messages

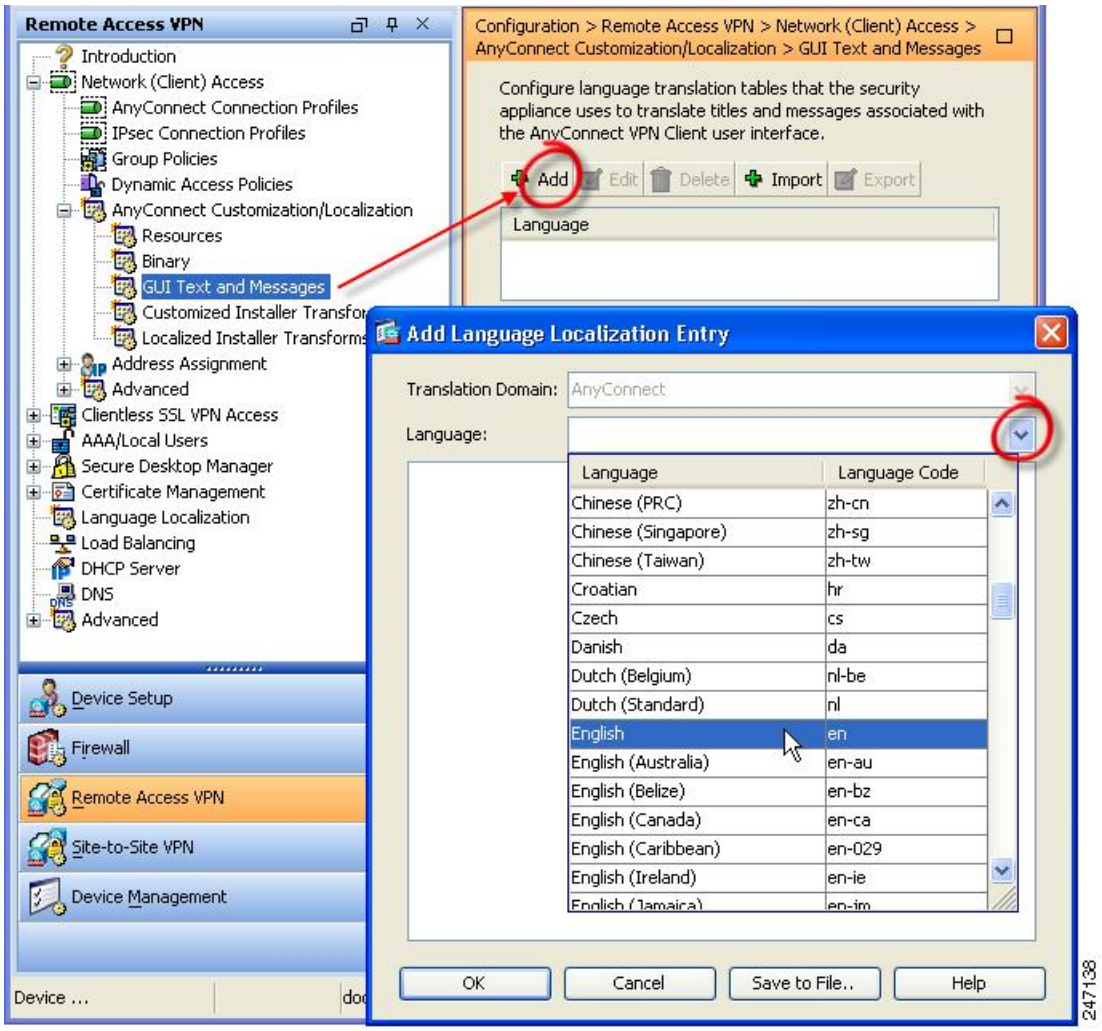
You can make changes to the English messages displayed on the Cisco Secure Client GUI by adding or editing the English translation table and changing message text for one or more message IDs. After you open the message file, you can edit it by:

- Typing your changes into the text in the open dialog.
- Copying the text in the open dialog to a text editor, making your changes, and pasting the text back into the dialog.
- Exporting the message file by clicking Save to File, editing the file, and importing it into the ASDM.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **GUI Text and Messages**.

Step 2 Click **Add**. The Add Language Localization Entry window displays.

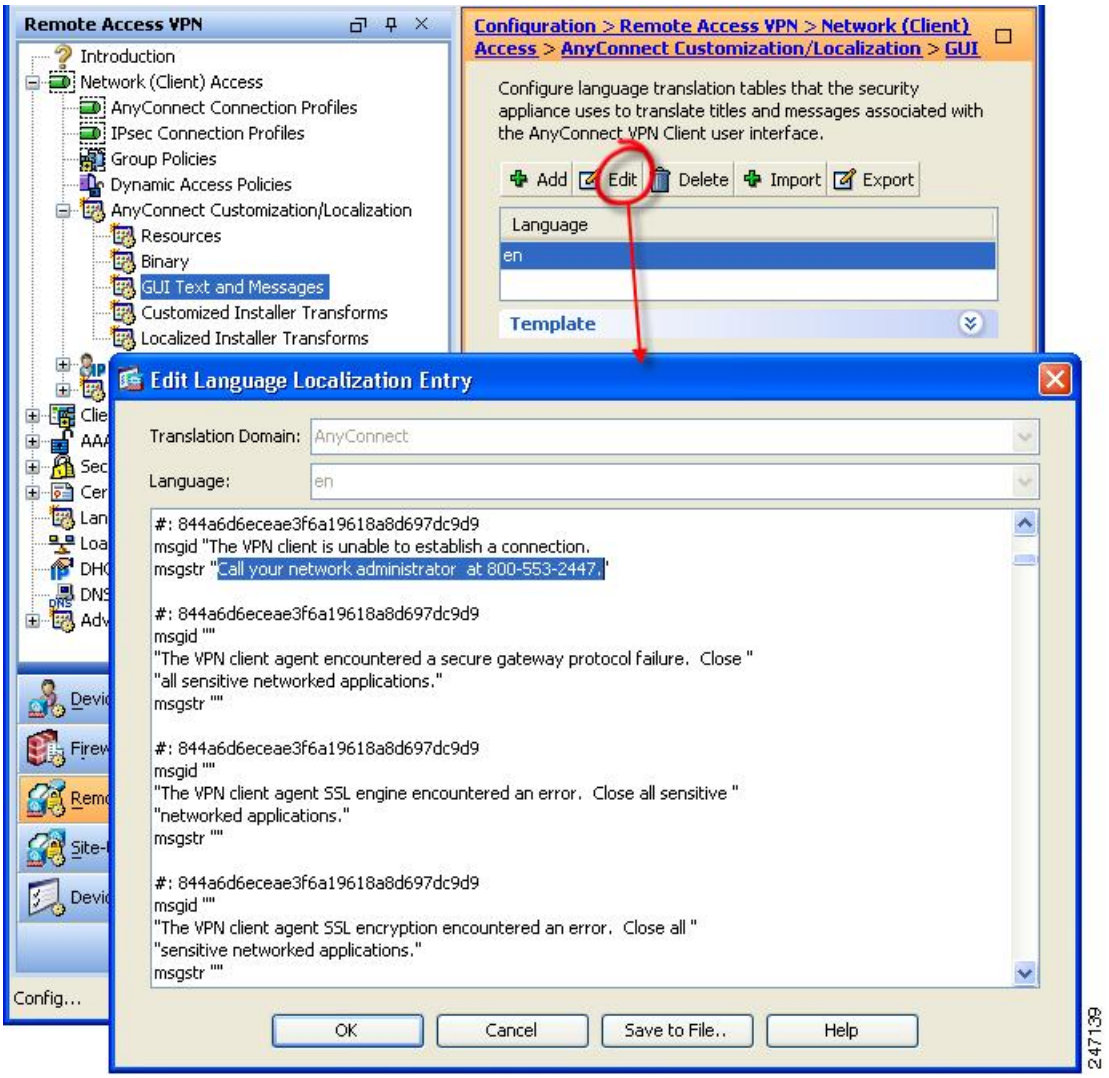


Step 3 Click the Language drop-list and specify the language as English (en). The translation table for English displays in the list of languages in the pane.

Step 4 Click **Edit** to begin editing the messages.

The Edit Language Localization Entry window displays. The text between the quotes of msgid is the default English text displayed by the client and must not be changed. The msgstr string contains text that the client uses to replace the default text in msgid. Insert your own text between the quotes of the msgstr.

In the example below, we insert “Call your network administrator at 800-553-2447.”



Step 5 Click **OK** and then **Apply** to save your changes.

Import Translation Tables to the Secure Firewall ASA

Procedure

Step 1 Download the desired translation table from www.cisco.com.

Step 2 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **GUI Text and Messages**.

Step 3 Click **Import**. The Import Language Localization Entry window displays.

Step 4 Choose the appropriate Language from the drop-down list.

Step 5 Specify where the translation table will be imported from.

Step 6 Click **Import Now**. This translation table will be deployed to Cisco Secure Client clients with this preferred language. Localization will be applied after Cisco Secure Client restarts and connects.

Create Message Catalogs for Enterprise Deployment

If you are not deploying the client with the Secure Firewall ASA, and are using an enterprise software deployment system such as Altiris Agent, you can manually convert the Cisco Secure Client translation table to a message catalog using a utility such as Gettext. After converting the table from a .po file to a .mo file, you then place the file in the proper folder on the client computer.



Note GetText and PoeEdit are third-party software applications. The recommended method for Cisco Secure Client GUI customization is to take the default .mo file from the Secure Firewall ASA and edit it as necessary for any deployments to the client. Using the default .mo avoids potential conversion issues resulting from third-party applications such as GetText and PoeEdit.

Gettext is a utility from The GNU Project and runs in the command window. See the GNU website at gnu.org for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net. This procedure creates a message catalog using Gettext:

Cisco Secure Client Message Template Directories

Cisco Secure Client message templates are located in the folders listed below for each operating system:



Note The `\l10n` directory is part of each directory path listed below. The directory name is spelled: lower case l (“el”), one, zero, lower case n.

- For Windows— `<DriveLetter>:\ProgramData\Cisco\Cisco Secure Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES`
- For macOS and Linux— `/opt/cisco/secureclient/l10n/<LANGUAGE-CODE>/LC_MESSAGES`

Procedure

Step 1 Download the Gettext utilities from http://www.gnu.org/software/gettext/ and install Gettext on a computer that you use for administration (not a remote user computer).

Step 2 Retrieve a copy of the Cisco Secure Client message template AnyConnect.po on a computer with Cisco Secure Client installed.

Step 3 Edit the AnyConnect.po file (use notepad.exe or any plain text editor) to change strings as desired.

Step 4 Run the Gettext message file compiler to create the .mo file from the .po file:

msgfmt -o AnyConnect.mo AnyConnect.po

Step 5 Place a copy of the .mo file in the correct message template directory on the user's computer.

Merge New Messages into a Customized Translation Table on the Secure Firewall ASA

New user messages are added to some releases of Cisco Secure Client. To enable translation of these new messages, new message strings are added to the translation template that is packaged with the latest client image. If you have created translation tables based on the template included with the previous client, the new messages are not automatically displayed to remote users. You must merge the latest template with your translation table to ensure your translation table has these new messages.

There are free third-party tools to perform the merge. Gettext utilities from The GNU Project is available for Windows and runs in the command window. See the GNU website at gnu.org for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net. Both methods are covered in the procedure below.



Note This procedure assumes that you have already loaded the latest Cisco Secure Client image package to the Secure Firewall ASA. The template is not available for export until you do.

Procedure

Step 1 Export the latest Cisco Secure Client Translation Template from **Remote Access VPN** > **Language Localization** > **Templates**. Export the template with the filename as `AnyConnect.pot`. This filename ensures that the msgmerge.exe program recognizes the file as a message catalog template.

Step 2 Merge the Cisco Secure Client Template and Translation Table.

If you are using the Gettext utilities for Windows, open a command prompt window and run the following command. The command merges the Cisco Secure Client translation table (.po) and the template (.pot), creating the new `AnyConnect_merged.po` file:

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

The following example shows the results of the command:

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
..................................... done.
```

If you are using Poedit, first open the AnyConnect.po file; go to **File > Open > <AnyConnect.po>**. Then merge it with the template; go to **Catalog > Update** from POT file <AnyConnect.pot>. Poedit displays an Update Summary window with both new and obsolete strings. Save the file, which you will import in the next step.

Step 3 Import the merged translation table to **Remote Access VPN** > **Language Localization**. Click **Import**, specify a language, and select **AnyConnect** as the Translation Domain. Specify the file to import as `AnyConnect_merged.po`.

Determining the Language on the Client

When the remote user connects to the Secure Firewall ASA and downloads the client, Cisco Secure Client determines the preferred language of the device and applies the appropriate translation table, by detecting the specified system locale. If no localization is established from ASA, it attempts one of the 17 default translations that come with Secure Client. If none of those translations are a match,English is used.

If you want to bypass the default localization files embedded within the client (stored in the Program Files), refer to the Bypass Default Localization preference in Local Policy. When this preference in the Local Policy is changed to *true*, it skips the usage of translations that come with Secure Client and instead uses English.

View/Change the Specified System Locale in Windows

Procedure

Step 1 Navigate to the **Control Panel** > **Region > Administrative > Change system locale** > **.**

Step 2 Choose the desired language from the **Current system locale** drop down.

When the system locale is changed, Windows requires a restart for the changes to take effect. Refer to the documentation associated with your specific operating system for additional details.

View/Change the Specified System Locale in macOS

Procedure

Step 1 Navigate to the **System Settings** > **General > Language & Region > Region** > **.**

Step 2 Change to the desired region.

Step 3 Add Cisco Secure Client as an application in the Language & region and set the desired language.

When the system locale is changed, macOS requires a restart for the changes to take effect. Refer to the documentation associated with your specific operating system for additional details.

View/Change the Specified System Locale in Linux

Procedure

Step 1 Navigate to the **Settings** > **Region > Language** > **.**

Step 2 Change to the desired language.

Step 3 Change to the desired region.

When the system locale is changed, Linux requires a restart for the changes to take effect. Refer to the documentation associated with your specific operating system for additional details.

Create Custom Icons and Logos for the Cisco Secure Client GUI

The tables in this section list the Cisco Secure Client files that you can replace for each operating system. The images in the tables are used by the Cisco Secure Client core VPN and Network Access Manager module.

Restrictions

- The filenames of your custom components must match the filenames used by the Cisco Secure Client GUI, which are different for each operating system and are case sensitive for macOS and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as company_logo.png. If you import it as a different filename, the Cisco Secure Client installer does not change the component. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.
- If you import an image as a resource file (such as company_logo.bmp), the image that you import customizes Cisco Secure Client until you reimport another image using the same filename. For example, if you replace company_logo.bmp with a custom image and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.

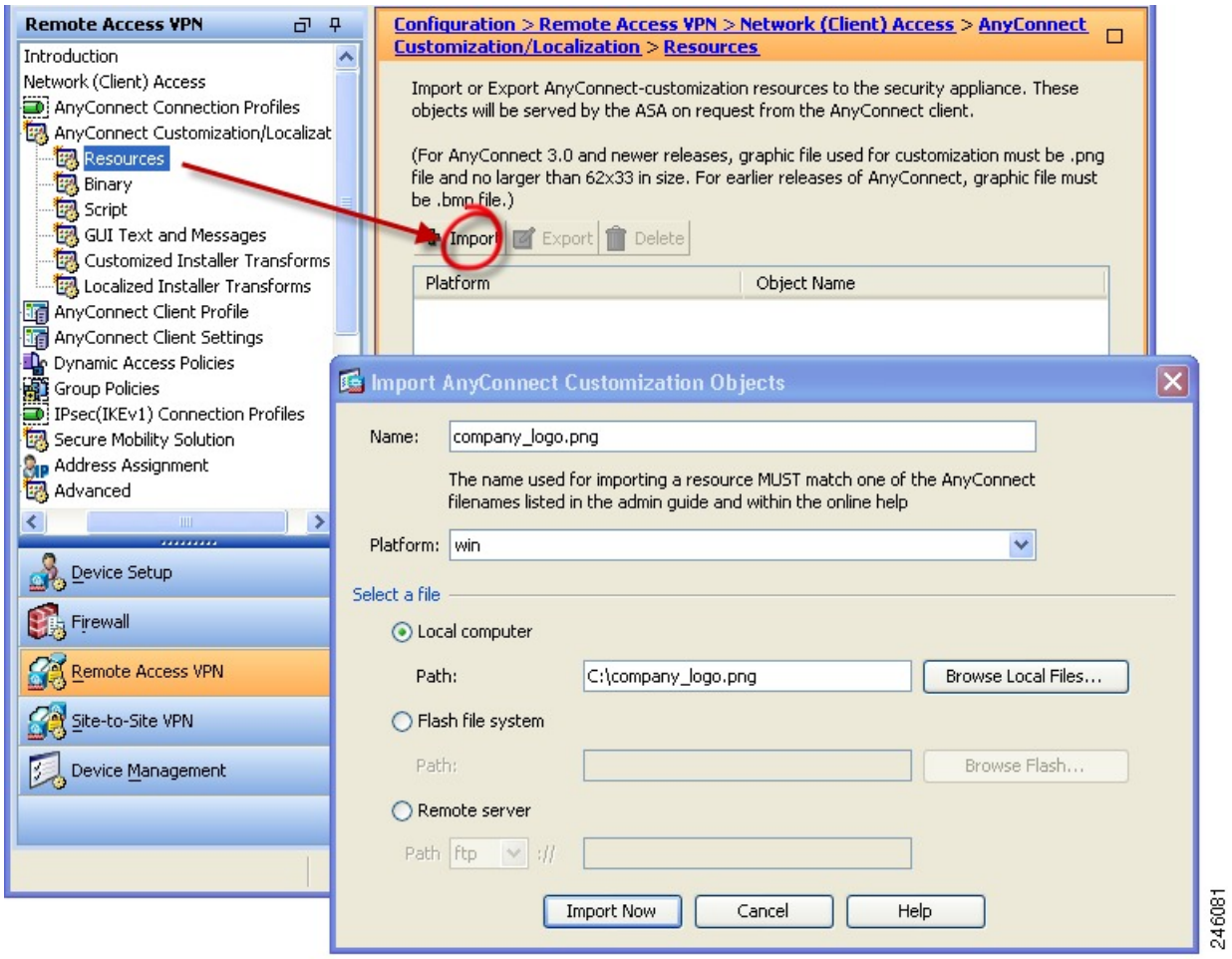
Replace Cisco Secure Client GUI Components

You can customize Cisco Secure Client by importing your own custom files to the security appliance, which deploys the new files with the client.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Resources**.

Step 2 Click **Import**. The **Import AnyConnect Customization Objects** window displays.



Step 3 Enter the name of the file to import.

Step 4 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the list of objects.

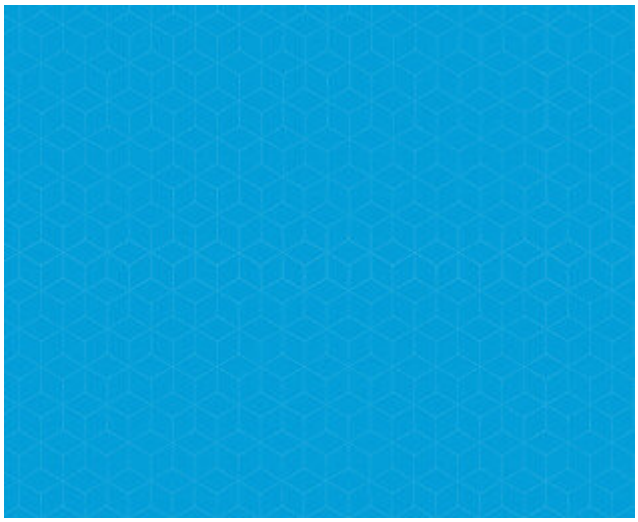
Cisco Secure Client Icons and Logos for Windows

All files for Windows are located in:

`%PROGRAMFILES%\Cisco\Cisco Secure Client\res\`

Note %PROGRAMFILES% refers to the environment variable by the same name. In most Windows installations, this is `C:\Program Files`.

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
about.png The About button in the upper-right corner of the Advanced dialog. The size is not adjustable. 	24 x 24 PNG
about_hover.png The About button in the upper-right corner of the Advanced dialog. The size is not adjustable. 	24 x 24 PNG
app_logo.png 128 x 128 is the maximum size. If your custom file is not that size, it is resized to 128 x 128 in the application. If it is not in the same ratio, it is stretched. 	128 x 128 PNG
attention.ico System tray icon alerting the user to a condition requiring attention or interaction. For example, a dialog about the user credentials. The size is not adjustable. 	16 x 16 ICO
company_logo.png The company logo displayed in the top-left corner of the tray flyout and Advanced dialog. 97 x 58 is the maximum size. If your custom file is not that size, it is resized to 97 x 58 in the application. If it is not in the same ratio, it is stretched. 	97 x 58 (maximum) PNG

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
company_logo_alt.png The company logo displayed in the bottom-right corner of the About dialog. 97 x 58 is the maximum size. If your custom file is not that size, it is resized to 97 x 58 in the application. If it is not in the same ratio, it is stretched. 	97 Xx58 PNG
cues_bg.jpg The background image for the tray flyout, Advanced window, and About dialog. Because images are not stretched, using a replacement image that is too small results in black space. 	1260 x 1024 JPEG
error.ico System tray icon alerting the user that something is critically wrong with one or more components. The size is not adjustable. 	16 x 16 ICO
neutral.ico System tray icon indicating that client components are operating correctly. The size is not adjustable. 	16 x 16 ICO

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
transition_1.ico System tray icon that displays along with transition_2.ico and transition_3.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 ICO
transition_2.ico System tray icon that displays along with transition_1.ico and transition_3.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 ICO
transition_3.ico System tray icon that displays along with transition_1.ico and transition_2.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when the Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 ICO
vpn_connected.ico System tray icon indicating that the VPN is connected. The size is not adjustable. 	16 x 16 ICO

Cisco Secure Client Icons and Logos for Linux

All files for Linux are located in:

/opt/cisco/secureclient/resources

The following table lists the files that you can replace and the client GUI area that is affected.

Filename and Description in Linux Installation	Image Size (Pixels, L x H) and Type
company-logo.png Corporate logo that appears on each tab of the user interface. Use PNG images no bigger than 62x33 pixels. 	142 x 92 PNG
cvc-about.png Icon that appears on the About tab. 	16 x 16 PNG
cvc-connect.png Icon that appears next to the Connect button, and on the Connection tab. 	16 x 16 PNG
cvc-disconnect.png Icon that appears next to the Disconnect button. 	16 x 16 PNG
cvc-info.png Icon that appears on the Statistics tab. 	16 x 16 PNG
systray_connected.png Tray icon that displays when the client is connected. 	16 x 16 PNG
systray_notconnected.png Tray icon that displays when the client is not connected. 	16 x 16 PNG

Filename and Description in Linux Installation	Image Size (Pixels, L x H) and Type
systray_disconnecting.png Tray icon that displays when the client is disconnecting. 	16 x 16 PNG
systray_quarantined.png Tray icon that displays when the client is quarantined. 	16x16 PNG
systray_reconnecting.png Tray icon that displays when the client is reconnecting. 	16 x 16 PNG
vpnui48.png Main program icon. 	48 x 48 PNG

Cisco Secure Client Icons and Logos for macOS

Cisco Secure Client icons and logos for macOS GUI resource customization on macOS are currently not supported.

Create and Upload the Cisco Secure Client Help File

To provide Cisco Secure Client users with help, create a help file with instructions about your site and load it on the Secure Firewall ASA. When users connect with Cisco Secure Client, the help file is downloaded, and the help icon displays on the Cisco Secure Client user interface. When the user clicks the help icon, the browser opens the help file. PDF and HTML files are supported.

Procedure

Step 1 Create an HTML file named `help_AnyConnect.html`.

Step 2 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Binary**.

Step 3 Import the **help_AnyConnect.xxx** file. The supported formats are: PDF, HTML, HTM, and MHT.

Step 4 On your device, bring up Cisco Secure Client and connect to your Secure Firewall ASA. The help file will be downloaded to the client device.
You should see that the help icon is added to the UI automatically.

Step 5 Click the help icon to open the help file in the browser.

If the help icon does not appear, check the help directory to see if the Cisco Secure Client downloader was able to retrieve the help file.

The "help_" part of the filename is removed by the downloader, so you should see AnyConnect.html in one of the following directories, depending on the operating system:

- Windows—`C:\ProgramData\Cisco\Cisco Secure Client\Help`
- macOS—`/opt/cisco/secureclient/help`

Write and Deploy Scripts

Cisco Secure Client lets you download and run scripts when the following events occur:

- Upon the establishment of a new client VPN session with the security appliance. We refer to a script triggered by this event as an *OnConnect* script because it requires this filename prefix.
- Upon the tear-down of a client VPN session with the security appliance. We refer to a script triggered by this event as an *OnDisconnect* script because it requires this filename prefix.

The establishment of a new client VPN session initiated by Trusted Network Detection triggers the OnConnect script (assuming the requirements are satisfied to run the script), but the reconnection of a persistent VPN session after a network disruption does not trigger the OnConnect script.

Some examples that show how you might want to use this feature include:

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.
- Logging on to a service upon VPN connection, and logging off after disconnection.

Cisco Secure Client supports script launching during WebLaunch and stand-alone launches.

These instructions assume you know how to write scripts and run them from the command line of the targeted endpoint to test them.

Note The Cisco Secure Client software download site provides some example scripts; if you examine them, remember that they are only examples. They may not satisfy the local computer requirements for running them and are unlikely to be usable without customizing them for your network and user needs. Cisco does not support example scripts or customer-written scripts.

Scripting Requirements and Limitations

Be aware of the following requirements and limitations for scripts:

- Number of Scripts Supported—Cisco Secure Client runs only one OnConnect and one OnDisconnect script; however, these scripts may launch other scripts.
- File Formats—Cisco Secure Client identifies the OnConnect and onDisconnect script by the filename. It looks for a file whose name begins with OnConnect or OnDisconnect regardless of file extension. The first script encountered with the matching prefix is executed. It recognizes an interpreted script (such as VBS, Perl, or Bash) or an executable.
- Script Language—The client does not require the script to be written in a specific language but does require an application that can run the script to be installed on the client computer. Thus, for the client to launch the script, the script must be capable of running from the command line.
- Restrictions on Scripts by the Windows Security Environment—On Microsoft Windows, Cisco Secure Client can only launch scripts after the user logs onto Windows and establishes a VPN session. Thus, the restrictions imposed by the user's security environment apply to these scripts; scripts can only execute functions that the user has rights to invoke. Cisco Secure Client hides the cmd window during the execution of a script on Windows, so executing a script to display a message in a .bat file for testing purposes does not work.
- Enabling the Script—By default, the client does not launch scripts. Use the Cisco Secure Client profile EnableScripting parameter to enable scripts. The client does not require the presence of scripts if you do so.



Note Although there is no requirement for XML profiles beyond setting this *EnableScripting* parameter, it is expected by the vpnagent that the profile be pushed from the headend. Because the *EnableScripting* setting is enforced after the VPN session is established, the setting remains at the default (EnableScripting set to *false*) if no VPN profile was pushed from the headend via the Group-Policy attributes. Even though the XML profile is loaded prior to the VPN establishment, features like certificate store override, SBL, certificate store, and such require the OnConnect/OnDisconnect script to operate based on the VPN headend Group-Policy attributes.

- Client GUI Termination—Client GUI termination does not necessarily terminate the VPN session; the OnDisconnect script runs after session termination.
- Running Scripts on 64-bit Windows—The Cisco Secure Client is a 32-bit application. When running on a 64-bit Windows version, it uses the 32-bit version of cmd.exe.

  Because the 32-bit cmd.exe lacks some commands that the 64-bit cmd.exe supports, some scripts could stop executing when attempting to run an unsupported command, or run partially and stop. For example, the msg command, supported by the 64-bit cmd.exe, may not be understood by the 32-bit version of Windows 7 (found in %WINDIR%\SysWOW64).

  Therefore, when you create a script, use commands supported by the 32-bit cmd.exe.

Write, Test, and Deploy Scripts

Write and test your scripts on the targeted operating system. If a script cannot run properly from the command line on the native operating system, then Cisco Secure Client cannot run it properly.

Procedure

Step 1 Write and test your scripts.

Step 2 Choose how to deploy the scripts:

- Use ASDM to import the script as a binary file to the Secure Firewall ASA.

  Go to **Network (Client) Access** > **AnyConnect Customization/Localization** > **Script**.

  If you use ASDM version 6.3 or later, the Secure Firewall ASA adds the prefix scripts_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script. When the client connects, the security appliance downloads the script to the proper target directory on the remote computer, removes the scripts_ prefix and leaves the OnConnect or OnDisconnect prefix. For example, if you import the script myscript.bat, the script appears on the security appliance as scripts_OnConnect_myscript.bat. On the remote computer, the script appears as OnConnect_myscript.bat.

  If you use an ASDM version earlier than 6.3, you must import the scripts with the following prefixes:

  - scripts_OnConnect
  - scripts_OnDisconnect

    To ensure the scripts run reliably, configure all Secure Firewall ASAs to deploy the same scripts. If you modify or replace a script, use the same name as the previous version and assign the replacement script to all of the Secure Firewall ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Use an enterprise software deployment system to deploy scripts manually to the VPN endpoints.

  If you use this method, use the script filename prefixes below:

  - OnConnect
  - OnDisconnect

    Install the scripts in the following directory:

Table 1: Required Script Locations

OS	Directory
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\Script
Linux (On Linux, assign execute permissions to the file for User, Group and Other.)	/opt/cisco/secureclient/vpn/script

OS	Directory
macOS	/opt/cisco/secureclient/vpn/script

Configure the Cisco Secure Client Profile for Scripting

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Check **Enable Scripting**. The client launches scripts on connecting or disconnecting the VPN connection.

Step 3 Check **User Controllable** to let users enable or disable the running of On Connect and OnDisconnect scripts.

Step 4 Check **Terminate Script On Next Event** to enable the client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running On Connect script if the VPN session ends and terminates a running OnDisconnect script if Cisco Secure Client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the On Connect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the On Connect or OnDisconnect script; it does not terminate child scripts.

Step 5 Check **Enable Post SBL On Connect Script** (enabled by default) to let the client launch the On Connect script (if present) if SBL establishes the VPN session.

Note Be sure to add the client profile to the Secure Firewall ASA group policy to download it to the VPN endpoint.

Troubleshoot Scripts

If a script fails to run, try resolving the problem as follows:

Procedure

Step 1 Make sure that the script has an `OnConnect` or `OnDisconnect` prefix name. Write, Test and Deploy Scripts shows the required scripts directory for each operating system.

Step 2 Try running the script from the command line. The client cannot run the script if it cannot run from the command line. If the script fails to run on the command line, make sure the application that runs the script is installed, and try rewriting the script on that operating system.

Step 3 Verify that there is only one OnConnect script and only one OnDisconnect script in the scripts directory on the VPN endpoint. If the client downloads an OnConnect script from the Secure Firewall ASA, then downloads a second OnConnect script with a different filename suffix for another Secure Firewall ASA, then the client might not run the script you intended to run. If the script path contains more than one OnConnect or OnDisconnect script, and you are using the Secure

Firewall ASA to deploy scripts, then remove the contents of the scripts directory and re-establish a VPN session. If the script path contains more than one OnConnect or OnDisconnect script, and you are using the manual deployment method, then remove the unwanted scripts and re-establish a VPN session.

Step 4 If the operating system is Linux, make sure that the script file permissions are set to execute.

Step 5 Make sure that the client profile has scripting enabled.

Write and Deploy Custom Applications with the Cisco Secure Client API

For Windows, Linux, and macOS computers, you can develop your own executable User Interface (UI) with the Cisco Secure Client API. Deploy your UI by replacing the Cisco Secure Client binary files.

The following table lists the filenames of the client executable files for the different operating systems.

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
macOS	Not supported by the Secure Firewall ASA deployment. However, you can deploy an executable for the macOS that replaces the client GUI using other means, such as Altiris Agent.	vpn

Your executable can call any resource files that you import to the Secure Firewall ASA, such as logo images. When you deploy your own executable, you can use any filenames for your resource files.

Restrictions

- You cannot deploy updated Cisco Secure Client software from the Secure Firewall ASA. If you place an updated version of the Cisco Secure Client package on the Secure Firewall ASA, the Cisco Secure Client downloads the update, which replaces your custom UI. You must manage distribution of your custom client and related Cisco Secure Client software. Even though ASDM allows you to upload binaries to replace Cisco Secure Client, this deployment function is not supported when using custom applications.
- If you deploy the Network Access Manager, use the Cisco Secure Client GUI.
- Start Before Login is not supported.

Use the Cisco Secure Client CLI Commands

The Cisco Secure Client provides a command line interface (CLI) for users who prefer to enter client commands instead of using the graphical user interface. The following sections describe how to launch the CLI command prompt and the commands available through the CLI:

• Launch the Client CLI Prompt, on page 29
• Use the Client CLI Commands, on page 29
• Prevent a Windows Popup Message When Secure Firewall ASA Terminates a Session, on page 31



Note In Windows and macOS, the same downloader is used for profile updates in both VPN UI or CLI connections. In Linux, the downloader for the VPN UI can display warnings and popups, such as the Untrusted Certificate warning we often see when connecting or when downloading a profile or other component. However, a second Linux downloader for the VPN CLI is not capable of displaying such popups and warnings, and you receive a connection failure message as expected behavior.

Launch the Client CLI Prompt

To launch the CLI command prompt:

- (Windows) Locate the file *vpncli.exe* in the Windows folder C:\Program Files (x86)\Cisco\Cisco Secure Client. Double click vpncli.exe.
- (Linux and macOS) Locate the file *vpn* in the folder /opt/cisco/secureclient/bin/. Execute the file *vpn*.

Use the Client CLI Commands

If you run the CLI in interactive mode, it provides its own prompt. You can also use the command line.

- connect *IP address or alias*—Client establishes a connection to a specific Secure Firewall ASA
- disconnect—Client closes a previously established connection
- stats—Displays statistics about an established connection
- quit—Exits the CLI interactive mode
- exit—Exits the CLI interactive mode

  The following examples show the user establishing and terminating a connection from the command line:

Windows

```
connect 209.165.200.224
```

Establishes a connection to a security appliance with the address 209.165.200.224. After contacting the requested host, Cisco Secure Client displays the group to which the user belongs and asks for the user's username and password. If you have specified that an optional banner be displayed, the user must respond to the banner. The default response is n, which terminates the connection attempt. For example:

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
>>notice: Please respond to banner.
```

```
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

stats

Displays statistics for the current connection; for example:

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
0.0.0.0 0.0.0.0
VPN>
```

disconnect

Closes a previously established connection; for example:

```
VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit or exit

Either command exits the CLI interactive mode; for example:

```
quit
goodbye
>>state: Disconnected
```

Linux or macOS

```
/opt/cisco/secureclient/bin/vpn connect 1.2.3.4
```

Establishes a connection to the Secure Firewall ASA with the address 1.2.3.4

```
/opt/cisco/secureclient/bin/vpn connect some_asa_alias
```

Establishes a connection to the Secure Firewall ASA by reading the profile and looking up the alias *some_asa_alias* in order to find its address

```
/opt/cisco/secureclient/bin/vpn stats
```

Displays statistics about the vpn connection

```
/opt/cisco/secureclient/bin/vpn disconnect
```

Disconnect the vpn session if it exists.

Prevent a Windows Popup Message When Secure Firewall ASA Terminates a Session

If you terminate the Cisco Secure Client session by issuing a session reset from the Secure Firewall ASA, the following Windows popup message displays to the end user:

```
The secure gateway has terminated the vpn connection. The following message was received
for the gateway: Administrator Reset
```

You may not want this message to appear (for example, when the VPN tunnel is initiated using the CLI command). You can prevent the message from appearing by restarting the client CLI after the client connects. The following example shows the CLI output when you do this:

```
C:\Program Files(x86)\Cisco\Cisco Secure Client>vpncli
Cisco Secure Client (version 5.x).
Copyright (c) 2022 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

Alternatively, in the Windows registry, you can create a 32-bit double value with the name SuppressModalDialogs on the endpoint device in the following locations. The client checks for the name but ignores its value:

- 64-bit Windows:

  HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\Cisco\ Cisco Secure Client

- 32-bit Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client