Optional AnyConnect Configuration and Management

Modifying and Deleting Connection Entries

Modifying a Connection Entry

Change a VPN connection entry to correct a configuration error or comply with an IT policy change.

Note You cannot modify the description or server address of connection entries downloaded from a secure gateway.

Procedure

Step 1 From the AnyConnect home window, long-press the VPN connection entry to be modified.

AnyConnect displays the **Select Action** window.

Step 2 Tap **Edit connection**.

The **Connection Editor** window displays the parameter values assigned to the connection entry.

Step 3 Tap the value to be modified, use the on-screen keyboard to enter the new value, and tap **OK**.

Step 4 Tap **Done**.

AnyConnect saves the modified connection entry and reopens the AnyConnect home window.

Related Topics

About AnyConnect Connection Entries

Deleting Connection Entries

This procedure deletes a manually configured VPN connection entry.

Note The only way to remove a connection entry imported from a VPN secure gateway is to remove the downloaded AnyConnect profile that contains the connection entries.

Procedure

Step 1 Open the AnyConnect home window and long-press the connection entry to be deleted.

AnyConnect displays the **Select Action** window.

Step 2 Tap **Delete connection**.

AnyConnect removes the connection entry and reopens the AnyConnect home window.

Related Topics

About AnyConnect Connection Entries

Configuring Certificates

About Certificates on Your Android Device

Certificates are used to digitally identify each end of the VPN connection: the secure gateway, or the server, and the AnyConnect client, or the user. A server certificate identifies the secure gateway to AnyConnect, and a user certificate identifies the AnyConnect user to the secure gateway. Certificates are obtained from and verified by Certificate Authorities (CAs).

When establishing a connection, AnyConnect always expects a server certificate from the secure gateway. The secure gateway expects a certificate from AnyConnect only if it has been configured to do so. Expecting

the AnyConnect user to manually enter credentials is another way to authenticate a VPN connection. In fact, the secure gateway can be configured to authenticate AnyConnect users with a digital certificate, with manually entered credentials, or with both. Certificate-only authentication allows VPNs to connect without user intervention.

Distribution to and use of certificates by, the secure gateway and your device, are directed by your administrator. Follow directions provided by your administrator to import, use, and manage server and user certificates for AnyConnect VPNs. Information and procedures in this document related to certificates and certificate management are provided for your understanding and reference.

AnyConnect stores both user and server certificates for authentication in its own certificate store on the Android device. The AnyConnect certificate store is managed from the **Menu** > **Diagnostics** > **Certificate Management** screen; you can also view Android System certificates here.

About User Certificates

In order for you, the AnyConnect user, to authenticate to the secure gateway using a digital certificate, you need a user certificate in the AnyConnect certificate store on your device. User certificates are imported using one of the following methods, as directed by your administrator:

- Imported automatically after clicking a hyperlink provided by your administrator in an e-mail or on a web page.
- Imported manually by you from the device's file system, from the device's credential storage, or from a network server.
- Imported when connecting to a secure gateway that has been configured by your administrator to provide you with a certificate.

Once imported, the certificate can be associated with a particular connection entry or selected automatically during connection establishment to authenticate.

You can delete user certificates from the AnyConnect store if they are no longer needed for authentication.

Related Topics

Importing Certificates from Hyperlinks
Importing Certificates Manually
Importing Certificates Provided by a Secure Gateway
Viewing Certificates, on page 4
Removing Certificates, on page 4

About Server Certificates

A server certificate received from the secure gateway during connection establishment automatically authenticates that server to AnyConnect, if and only if it is valid and trusted. Otherwise:

- A valid, but untrusted server certificate can be reviewed, authorized, and imported to the AnyConnect certificate store. Once a server certificate is imported into the AnyConnect store, subsequent connections made to the server using this digital certificate are automatically accepted.
- An invalid certificate cannot be imported into the AnyConnect store. It can be accepted to complete the current connection, but this is not recommended.

Server certificates in the AnyConnect store can be deleted if they are no longer needed for authentication.

Related Topics

Responding to Untrusted VPN Server Notifications
Viewing Certificates, on page 4
Removing Certificates, on page 4

Viewing Certificates

View user and server certificates that have been imported into the AnyConnect certificate store, and Android system certificates.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** or **Server** tab to view certificates in the AnyConnect certificate store.

Long-press a certificate and tap:

- **View certificate details** to see the contents of a certificate.
- **Delete certificate** to remove this certificate from the AnyConnect store.

Step 3 Tap the **System** tab to view certificates in the Android Credential Storage.

Long-press a certificate and tap **View certificate details** to see the contents of a certificate.

Related Topics

About User Certificates
About Server Certificates, on page 3

Removing Certificates

Remove certificates from the AnyConnect certificate store only; certificates in the System certificate store cannot be removed.

Certificates are deleted individually or cleared from the AnyConnect certificate store all at once.

Related Topics

About User Certificates
About Server Certificates, on page 3

Deleting a Single Certificate

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** or **Server** tab to display user or server certificates in the AnyConnect certificate store.

Step 3 Long-press a certificate.

The **Certificate Options** display.

Step 4 Choose **Delete certificate** and confirm that you want to delete this particular certificate.

Clearing All Certificates

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Certificate Management**.

Step 2 Tap the **User** or **Server** tab to display user or server certificates in the AnyConnect certificate store.

Step 3 Tap **Clear All** to remove all certificates from the AnyConnect certificate store.

Specifying Application Preferences

Procedure

From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Changing the AnyConnect Theme

AnyConnect provides the following themes:

- Cisco Default Theme (default)—Color contrast, emphasizing shades of blue.
- Android—Android-like alternative to the Cisco default theme.

Note The assignment of the Android theme to AnyConnect has issues such as the whiteout of field values on some devices. Reapply the default theme if the Android theme is difficult to use.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Step 2 Tap **Application Style**.

AnyConnect shows a green button next to the theme currently in use.

Step 3 Tap the theme that you want displayed.

Launching AnyConnect at Startup

You have control over when AnyConnect launches on your device. By default, AnyConnect does not automatically launch at device startup. If checked, Launch at Startup is enabled.

Note Launch at Startup is automatically enabled if a profile specifying Trusted Network Detection is download or imported.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Step 2 Tap the **Launch at Startup** checkbox to enable or disable this preference.

Hiding the AnyConnect Status Bar Icon

The AnyConnect icon in the notification bar can be hidden when AnyConnect is not active.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Step 2 Tap the **Hide Icon** checkbox.

If left unchecked, the icon displays persistently.

Controlling External Use of AnyConnect

The External Control application preference specifies how the AnyConnect application responds to external URI requests. External requests create connection entries; connect or disconnect a VPN; and import client profiles, certificates, or localization files.

External requests are URIs, typically provided by your administrator in e-mails or on web pages. Your administrator will instruct you to set this preference to one the following values:

- Enabled: The AnyConnect application automatically allows all URI commands.
- Disabled: The AnyConnect application automatically disallows all URI commands.
- Prompt: The AnyConnect application prompts you each time an AnyConnect URI is accessed on the device. You allow or disallow the URI request.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Step 2 Tap **External Control**.

Step 3 Tap **Enabled**, **Disabled**, or **Prompt**.

Blocking Untrusted Servers

This application setting determines if AnyConnect blocks connections when it cannot identify the secure gateway. This protection is ON by default; it can be turned OFF, but this is not recommended.

AnyConnect uses the certificate received from the server to verify its identify. If there is a certificate error due to an expired or invalid date, wrong key usage, or a name mismatch, the connection is blocked.

When this setting is ON, a blocking **Untrusted VPN Server!** notification alerts you to this security threat.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Step 2 Tap the **Block Untrusted Servers** checkbox to enable or disable this preference.

Setting FIPS Mode

FIPS Mode makes use of Federal Information Processing Standards (FIPS) cryptography algorithms for all VPN connections.

Before You Begin

Your administrator will inform you if you need to enable FIPS mode on your mobile device for connectivity to your network.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

Step 2 Tap the **FIPS Mode** checkbox to enable or disable this preference.

Upon confirmation of your FIPS mode change, AnyConnect exits and must be restarted manually. Upon restart, your FIPS mode setting is in effect.

Setting Trusted Network Detection

Trusted Network Detection (TND) allows automatic initiation of a VPN connection when the device is outside of a trusted network and automatic suspension of the VPN connection when the device returns to a trusted network.

Your administrator enables this feature, defines which networks are trusted or untrusted, and determines AnyConnect behavior when it detects network transitions. For example, your administrator may configure TND to automatically connect while you are on your home network and then disconnect when you move into the corporate network.

If this feature has been enabled by your administrator, you are given the option to disable it on your own device. Keep in mind that this feature is provided for you convenience, automatically connecting and disconnecting the VPN so that you do not have to do so manually. Enable TND to reinstate this functionally.

TND does not interfere with your ability to manually establish a VPN connection or disconnect a VPN connection started while on a trusted network. TND disconnects the VPN session only if the device first connects (automatically or manually) in an untrusted network and then moves into a trusted network.

Before You Begin

Trusted Network Detection requires the AnyConnect app to be running. If you have exited the application using **Menu** > **Exit** or forced the app to stop using the Android settings, AnyConnect will be unable to detect a trusted network.

Note The Trusted Network Detection feature is not available in the AnyConnect ICS+ package, the Android VPN Framework package. It is only available in the brand-specific and rooted AnyConnect packages.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Settings** > **Application Preferences**.

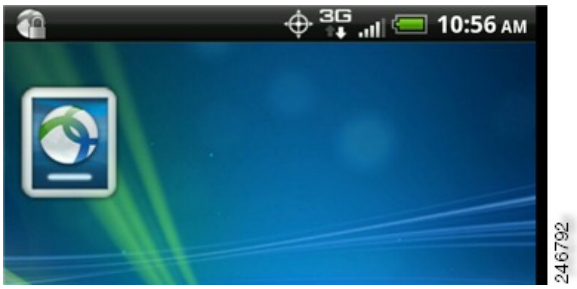
Step 2 Tap the **Trusted Network Detection** checkbox to enable or disable this preference.

Using AnyConnect Widgets

About AnyConnect Widgets

AnyConnect provides widgets to add to your home screen:

- The smallest widget is the same size as the AnyConnect apps icon. The color of the bar below the icon reflects the VPN status. Tap the widget to connect to or disconnect from the current VPN connection.



- The larger widget shows the AnyConnect icon and name, the current VPN connection, and the VPN status. Tap the widget to connect to or disconnect from the VPN connection.

Placing a Widget on your Android Home Window

The instructions for placing a widget may vary, depending on the device and the Android version that you are using. Example instructions are provided.

Procedure

Step 1 Go to an Android home screen that has enough space for the widget that you want to use.

Step 2 Tap **Menu** > **Personalize** > **Widgets**.

Step 3 Tap the AnyConnect widget that you want to use.

Android adds the widget to the home screen.

Step 4 Long-press the widget if you want to reposition it. Move it after it responds.

Managing the AnyConnect Client Profile

About AnyConnect Client Profiles

The AnyConnect VPN Client Profile is an XML file that specifies client behavior and identifies VPN connections. Each connection entry in the VPN Client Profile specifies a secure gateway that is accessible to this device, as well as other connection attributes, policies, and constraints. These connection entries, in addition to the VPN connections that you configured locally on the device, are listed on the AnyConnect home screen to choose from when initiating a VPN connection.

AnyConnect retains only one VPN Client Profile on the Android device at a time. The following are some key scenarios that cause the current profile, if it exists, to be replaced or deleted:

- Manually importing a profile replaces the current profile with the imported profile.
- Upon startup of an automatic or manual VPN connection, the new connection's profile replaces the current profile.
- If a VPN connection does not have a profile associated with it, the existing profile is deleted upon startup of that VPN.

View or delete the AnyConnect profile currently on the device, or import a new one.

Related Topics

Viewing the AnyConnect Profile, on page 10
Importing an AnyConnect Profile, on page 11
Removing the AnyConnect Profile, on page 11

Viewing the AnyConnect Profile

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Profile Management**.

Step 2 Tap the expansion icon for the **Current Profile Details**. The XML file is displayed. Scroll down to see the whole file.

Related Topics

About AnyConnect Client Profiles, on page 10

Importing an AnyConnect Profile

Before You Begin

A profile file must be present on the Android device to import it in this way. Your administrator provides you with the name of the profile file to be installed on your device.

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Profile Management**.

Step 2 Tap **Import Profile** and choose the XML profile from the device's file system.

Connection entries defined in this profile appear in the AnyConnect home screen immediately, and AnyConnect client behavior conforms to this profile's specifications.

Related Topics

About AnyConnect Client Profiles, on page 10

Removing the AnyConnect Profile

Procedure

Step 1 From the AnyConnect home window, tap**Menu** > **Diagnostics** > **Profile Management** .

Step 2 Tap **Delete Profile** and confirm to delete the current profile.

Connection entries defined in the profile are cleared from the AnyConnect home screen, and AnyConnect client behavior conforms to default client specifications.

Related Topics

About AnyConnect Client Profiles, on page 10

Managing Localization

About Android Device Localization

Installed Localization

Upon AnyConnect installation, your Android device is localized if the specified device's locale matches one of the packaged language translations. The following language translations are included in the AnyConnect package:

- Czech (cs-cz)
- German (de-de)
- Latin American Spanish (es-co)
- Canadian French (fr-ca)
- Japanese (ja-jp)
- Korean (ko-kr)
- Polish (pl-pl)
- Simplified Chinese (zh-cn)

The displayed language is determined by the locale specified in **Settings** > **Language and Keyboard** > **Select locale**. AnyConnect uses the language specification, then the region specification, to determine the best match. For example, after installation, a French-Switzerland (fr-ch) locale setting results in a French-Canadian (fr-ca) display.

AnyConnect UIs and messages are translated as soon as AnyConnect starts. The selected localization is noted as Active in the AnyConnect **Menu** > **Diagnostics** > **Localization Management** screen.

Importing Localization

After installation, localization data for languages not supported in the AnyConnect package is imported by:

- Clicking on a hyperlink provided to you by an administrator that has been defined to import localization data.

  Your administrator can provide a hyperlink in e-mail, or on a web page, that imports localization data when clicked. This method uses the AnyConnect URI handler, a feature available to administrators for simplifying AnyConnect configuration and management.

Note You must allow this AnyConnect activity by setting External Control to either Prompt or Enable within the AnyConnect settings. See Controlling External Use of AnyConnect for how to set this.

- Connecting to a secure gateway that an administrator has configured to provide downloadable localization data upon VPN connection.

  If this method is to be used, your administrator will provide you with appropriate VPN connection information or a predefined connection entry in the XML profile. Upon VPN connection, localization data is downloaded to your device and put into play immediately.

- Manually imported using the **Import Localization** option on the AnyConnect Localization Management Activity Screen.

Restoring Localization

Restoring the use of the pre-loaded localization data from the AnyConnect package deletes all imported localization data. The restored language is chosen by matching the specified device locale to the installed localization data.

Managing Localization Data

Procedure

From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Localization Management**.

What to Do Next

- **Import Localization**: Import localization data from a specified server.
- **Restore Localization**: Restore default localization data.
- **Localization Files**: View the list of localization files.

Importing Localization Data from a Server

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Localization Management**.

Step 2 Tap **Import Localization**.

Specify the address of the secure gateway and the locale. The locale is specified per ISO 639-1, with the country code added if applicable (for example, en-US, fr-CA, ar-IQ, and so on).

This localization data is used in place of the pre-packaged, installed localization data.

Restoring Localization Data

Procedure

Step 1 From the AnyConnect home window, tap **Menu** > **Diagnostics** > **Localization Management**.

Step 2 Tap **Restore Localization**.

Restores the use of the pre-loaded localization data from the AnyConnect package and deletes all imported localization data.

The restored language is chosen based on the device's locale specified in **Settings** > **Language and Keyboard** > **Select locale**.

Exiting AnyConnect

Exiting AnyConnect terminates the current VPN connection and stops all AnyConnect processes. Use this action sparingly, other apps or processes on your device may be using the current VPN connection and exiting AnyConnect may adversely affect their operation.

Procedure

From the AnyConnect home window, tap **Menu** > **Exit**.

In the event that AnyConnect is unable to gracefully exit all of its processes, you will be detoured to the Android application management screen to manually terminate AnyConnect by tapping **Force Stop**.

Removing AnyConnect

Procedure

Step 1 Go to the Android Settings for your device and proceed to the app or applications management area.

Step 2 Tap **Uninstall**.