AnyConnect on Mobile Devices

AnyConnect on mobile devices is similar to AnyConnect on Windows, Mac and Linux platforms. This chapter provides device information, configuration information, support information, as well as other administrative tasks specific to AnyConnect for mobile devices.

AnyConnect Operation and Options on Mobile Devices

About AnyConnect Mobile VPN Connections

This release of the AnyConnect Secure Mobility Client is available on the following mobile platforms:

-
- Windows Phone

Cisco AnyConnect is provided on the app store for each supported platform, it is not available on www.cisco.com or distributed from a secure gateway.

AnyConnect mobile apps contain the core VPN client only, they do not include other AnyConnect modules such as the Network Access Manager, Posture, or Web Security. Posture information, referred to as Mobile Posture, is provided to the headend using AnyConnect Identify Extensions (ACIDex) when the VPN is connecting.

An AnyConnect VPN connection can be established in one of the following ways:

- Manually by a user.
- Manually by the user when they click an automated connect action provided by the administrator (Android and Apple iOS only).

- Automatically by the Connect On-Demand feature (Apple iOS only).

AnyConnect VPN Connection Entries on Mobile Devices

A connection entry identifies the address of the secure gateway by its fully qualified domain name or IP address, including the tunnel group URL if required. It can also include other connection attributes.

AnyConnect supports multiple connection entries on a mobile device addressing different secure gateways and/or VPN tunnel groups. If multiple connection entries are configured, it is important that the user knows which one to use to initiate the VPN connection. Connection entries are configured in one of the following ways:

- Manually configured by the user. See the appropriate platform user guide for procedures to configure a connection entry on a mobile device.
- Defined by the Anyconnect VPN Client Profile.

  The AnyConnect VPN Client Profile specifies client behavior and defines VPN connection entries. For details refer to Configure Mobile Device Connections in the AnyConnect VPN Profile, on page 8.

Tunneling Modes

AnyConnect can operate, in a managed or an unmanaged BYOD environment. VPN tunneling in these environments operates exclusively in one of the following modes:

- System-tunneling mode—The VPN connections are used to tunnel all data (full-tunneling), or only data flowing to and from particular domains or addresses (split-tunneling). This mode is available on all mobile platforms.
- Per App VPN mode—The VPN connection is used for a specific set of apps on the mobile device (Android and Apple iOS only)

  AnyConnect allows the set of apps defined by the administrator on the headend. This list is defined using the ASA Custom Attributes mechanism. This list is sent to the AnyConnect client, and enforced on the device. For all other apps, data is sent outside of the tunnel or in the clear.

  On Apple iOS, a managed environment is required to run in this mode. On Android, both managed and unmanaged environments are supported. On both platforms, in a managed environment, the Mobile Device Manager must also configure the device to tunnel the same list of apps that AnyConnect is configured to tunnel.

AnyConnect operates in the mode determined by the configuration information received from the ASA headend. Specifically, the presence or absence of a Per App VPN list in the Group Policy or Dynamic Access Policy (DAP) associated with the connection. If the Per App VPN list is present, AnyConnect operates in Per App VPN mode; if it is absent, AnyConnect operates in system-tunneling mode.

Secure Gateway Authentication on Mobile Devices

Block Untrusted Servers

When establishing a VPN connection, AnyConnect uses the digital certificate received from the secure gateway to verify the server's identify. If the server certificate is invalid (there is a certificate error due to an expired or invalid date, wrong key usage, or a name mismatch), or if it is untrusted (the certificate cannot be verified by a Certificate Authority), or both, the connection is blocked. A blocking message displays, and the user must choose how to proceed.

The **Block Untrusted Servers** application setting determines how AnyConnect reacts if it cannot identify the secure gateway. This protection is ON by default; it can be turned OFF by the user, but this is not recommended.

When **Block Untrusted Servers** is ON, a blocking **Untrusted VPN Server** notification alerts the user to this security threat. The user can choose:

- **Keep Me Safe** to terminate this connection and remain safe.
- **Change Settings** to turn the Block Untrusted Servers application preference OFF, but this is not recommended. After the user disables this security protection, they must reinitiate the VPN connection.

When **Block Untrusted Servers** is OFF, a non-blocking **Untrusted VPN Server** notification alerts the user to this security threat. The user can choose to:

- **Cancel** the connection and remain safe.
- **Continue** the connection, but this is not recommended.
- **View Details** of the certificate to visually determine acceptability.

  If the certificate that the user is viewing is valid but untrusted, the user can:

  - Import the server certificate into the AnyConnect certificate store for future use and continue the connection by selecting **Import and Continue**.

    Once this certificate is imported into the AnyConnect store, subsequent connections made to the server using this digital certificate are automatically accepted.
  - Go back to the previous screen and choose **Cancel** or **Continue**.

  If the certificate is invalid, for any reason, the user can only return to the previous screen and choose **Cancel** or **Continue**.

Leaving the Block Untrusted Servers setting ON (default setting), having a valid and trusted server certificate configured on your secure gateway, and instructing your mobile users to always choose Keep Me Safe is the safest configuration for VPN connectivity to your network.

Note **Strict Certificate Trust** overrides this setting, see description below.

Client Authentication on Mobile Devices

To complete a VPN connection, the user must authenticate by providing credentials in the form of a username and password, a digital certificate, or both. The administrator defines the authentication method on the tunnel group. For the best user experience on mobile devices, Cisco recommends using multiple AnyConnect connection profiles depending on the authentication configuration. You will have to decide how best to balance user experience with security. We recommend the following:

- For AAA-based authentication tunnel groups for mobile devices, the group policy should have a very long idle timeout, such as 24 hours, to let the client remain in a reconnecting state without requiring the user to re-authenticate.
- To achieve the most transparent end user experience, use certificate-only authentication. When a digital certificate is used, a VPN connection is established without user interaction.

In order to authenticate the mobile device to the secure gateway using a certificate, end users must import a certificate onto their device. This certificate is then available for automatic certificate selection, or it can be associated with a particular connection entry manually. Certificates are imported using the following methods:

- Imported manually by the user. See the appropriate user guide for procedures to import certificates to your mobile device.
- Using SCEP. See Configure Certificate Enrollment for details.

Localization on Mobile Devices

AnyConnect Secure Mobility Client for Android and Apple iOS supports localization, adapting the AnyConnect user interface and messages to the user's locale.

Prepackaged Localization

The following language translations are included in the AnyConnect Android and Apple iOS apps:

- Canadian French (fr-ca)
- Chinese (Taiwan) (zh-tw)
- Czech (cs-cz)
- Dutch (nl-nl)
- French (fr-fr)
- German (de-de)
- Hungarian (hu-hu)
- Italian (it-it)
- Japanese (ja-jp)
- Korean (ko-kr)
- Latin American Spanish (es-co)
- Polish (pl-pl)

- Portuguese (Brazil) (pt-br)
- Russian (ru-ru)
- Simplified Chinese (zh-cn)
- Spanish (es-es)

Localization data for these languages is installed on the mobile device when AnyConnect is installed. The local specified on your mobile device determines the displayed language. 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 translatednyConnect when AnyConnect starts.

Downloaded Localization

For languages not in the AnyConnect package, administrators add localization data to the ASA to be downloaded to the device upon AnyConnect VPN connectivity.

Cisco provides the anyconnect.po file, including all localizable AnyConnect strings, on the product download center of Cisco.com. AnyConnect administrators download the anyconnect.po file, provide translations for the available strings, and then upload the file to the ASA. AnyConnect administrators that already have an anyconnect.po file installed on the ASA will download this updated version.

Initially, the AnyConnect user interface and messages are presented to the user in the installed language. When the device user establishes the first connection to the ASA, AnyConnect compares the device's preferred language to the available localization languages on the ASA. If AnyConnect finds a matching localization file, it downloads the localized file. Once the download is complete, AnyConnect presents the user interface and user messages using the translated strings added to anyconnect.po file. If a string was not translated, AnyConnect presents the default English strings.

See Import Translation Tables to the Adaptive Security Appliance for instructions on configuring localization on an ASA. If the ASA does not contain localization data for the device's locale, the preloaded localization data from the AnyConnect application package continues to be used.

More Ways to Provide Localization on Mobile Devices

Ask your mobile device users to manage localization data on their own device. See the appropriate User Guide for procedures to perform the following localization activities:

- Import localization data from a specified server. The user chooses to import localization data and specifies 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 prepackaged, installed localization data.
- Restore default localization data. This restores the use of the preloaded localization data from the AnyConnect package and deletes all imported localization data.

FIPS and Suite B Cryptography on Mobile Devices

AnyConnect for mobile devices incorporates Cisco Common Cryptographic Module (C3M), the Cisco SSL implementation which includes FIPS 140-2 compliant cryptography modules and NSA Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms. Suite B cryptography is available for IPsec VPNs only; FIPS-compliant cryptography is available for both IPsec and SSL VPNs.

Use of cryptography algorithms is negotiated with the headend while connecting. Negotiation is dependent on the capabilities of both ends of the VPN connection. Therefore, the secure gateway must also support FIPS-compliant and Suite B cryptography.

The user configures AnyConnect to accept only NGE algorithms during negotiation by enabling **FIPS Mode** in the AnyConnect app settings. When FIPS Mode is disabled, AnyConnect also accepts non-FIPS cryptography algorithms for VPN connections.

See About FIPS, NGE, and AnyConnect for general support information.

Additional Mobile Guidelines and Limitations

- Apple iOS 5.0 or later is required for Suite B cryptography; this is the minimum Apple iOS version that supports ECDSA certificates used in Suite B.
- Android 4.0 (Ice Cream Sandwich) or later is required for Suite B cryptography; this is the minimum Android version that supports ECDSA certificates used in Suite B.
- A device that is running in FIPS mode is not compatible with using SCEP to provide mobile users with digital certificates by proxy method or legacy method. Plan your deployment accordingly.

AnyConnect on Windows Phone Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.1.x for Windows Phone for features and devices supported by this release.

Refer to the Windows Phone User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.1.x to install, upgrade, and use the AnyConnect app.

Guidelines and Limitations for AnyConnect on Windows 10 and Windows Phone 8.1

- Performance is limited due to non-support of DTLS and IPsec/IKEv2.
- VPN roaming (transitioning between WiFi and 3/4G networks) is not supported.
- AnyConnect does not receive or process the AnyConnect VPN Profile from the Secure Gateway.
- A user initiated disconnect does not cleanly disconnect from the head end. Cisco recommends you connect to ASA VPN groups with a small idle timeout to clear orphaned sessions on the ASA.
- When the mobile device user is connecting to an ASA that does not have a valid mobile license, the user will get into a login loop, where after entering credentials the authentication will restart and eventually (after 5 attempts) send the user a generic error message: `The VPN connection has failed with error code 602`. Please contact your administrator and ensure that a valid mobile license is installed on the secure gateway

Configure Mobile Device VPN Connectivity on the ASA Secure Gateway

Procedure

Step 1 Refer to the appropriate release of the Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides for configuration procedures that are common to desktop and mobile endpoints. Consider the following for mobile devices:

Attribute	ASDM Location	Exception
Home page URL	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Customization**	AnyConnect Mobile ignores the home page URL setting, you cannot redirect mobile clients after successful authentication.
Name and Aliases of the AnyConnect Connection Profile	**Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add / Edit**	Do not use special characters in the Name or Aliases fields of tunnel groups (connection profiles) that are used for AnyConnect mobile client connectivity. Use of special characters may cause the AnyConnect client to display the error message: `Connect attempt has failed` after logging that it is `Unable to process response from Gateway`.
Dead Peer Detection	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client**	Switch off server-side dead peer detection because it prevents the device from sleeping. However, client-side dead peer detection should remain switched on because it enables the client to determine when the tunnel is terminated due to a lack of network connectivity.
SSL Keepalive Messages	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client**	We recommend disabling these keepalive messages to conserve the battery life of mobile devices, especially if client-side dead peer detection is enabled.

Attribute	ASDM Location	Exception
IPsec over NAT-T Keepalive Messages	**Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters**	**Enable IPsec over NAT-T** must be selected for AnyConnect IPsec to work. When enabled, NAT Keepalive messages are sent every 20 seconds by default, causing excessive battery drainage on mobile devices. To minimally effect battery usage on mobile devices, we recommend you Set the NAT-T Keepalives to the maximum value of 3600 because these messages cannot be disabled. Use the `crypto isakmp nat-traversal 3600` command to specify this in the ASA CLI.

Step 2 Configure Mobile Posture (also called AnyConnect Identity Extensions, ACIDex) to accept, deny, or restrict mobile connections as desired.
See the *Configuring Endpoint Attributes Used in DAPs* procedure, in the appropriate release of Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides.

Example:
The following attributes are sent by AnyConnect on Apple iOS to the headend when establishing a connection:

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

Configure Mobile Device Connections in the AnyConnect VPN Profile

The AnyConnect VPN Client Profile is an XML file that specifies client behavior and defines VPN connection entries. Each connection entry specifies a secure gateway that is accessible to the endpoint device and other connection attributes, policies, and constraints. Use the AnyConnect Profile Editor to create a VPN client profile that includes host connection entries for mobile devices.

Connection entries defined in the VPN profile delivered to mobile devices from the ASA cannot be modified or deleted by the user. Users can modify and delete only the connection entries that they create manually.

AnyConnect retains only one current VPN Client Profile on the mobile device at a time. Upon startup of an automatic or manual VPN connection, the new VPN profile entirely replaces the current profile. If the user manually deletes the current profile, the profile is removed and all connection entries defined in this profile are deleted.

Procedure

Step 1 Configure basic VPN access.
See Configure VPN Access for procedures that are common to desktop and mobile endpoints considering the following exceptions:

Profile Attribute	Exception
Auto Reconnect	For all platforms except Apple iOS, regardless of your Auto Reconnect specification, AnyConnect Mobile always attempts to ReconnectAfterResume. For Apple iOS only, Disconnect On Suspend is supported. When Disconnect On Suspend is chosen, AnyConnect disconnects and then releases the resources assigned to the VPN session. It will only reconnect in response to a user's manual connection or an On Demand connection (if configured).
Local LAN Access	AnyConnect Mobile ignores the Local LAN Access setting, always allowing Local LAN Access regardless of the setting in the Client profile.

Step 2 Configure Mobile Specific Attributes:

a) In the VPN Client Profile, select **Server List** in the navigation pane.
b) Select **Add** to add a new server entry to the list, or select a server entry from the list and press **Edit** to open the Server List Entry dialog box.
c) Configure mobile specific parameters as described in AnyConnect Profile Editor, Mobile Settings, on page 9.
d) Click **OK**

Step 3 Distribute the VPN client profile in one of the following ways:

- Configure the ASA to upload a client profile onto the mobile device upon VPN connectivity.

  See The AnyConnect Profile Editor chapter for instructions on how to import the VPN client profile to the ASA and associate it with a group policy.

AnyConnect Profile Editor, Mobile Settings

Related Topics: Configure Mobile Device Connections in the AnyConnect VPN Profile, on page 8

Apple iOS / Android Settings

- **Certificate Authentication—**The Certificate Authentication policy attribute associated with a connection entry specifies how certificates are handled for this connection. Valid values are:
  - **Automatic—**AnyConnect automatically chooses the client certificate with which to authenticate when making a connection. In this case, AnyConnect views all the installed certificates, disregards

those certificates that are out of date, applies the certificate matching criteria defined in VPN client profile, and then authenticates using the certificate that matches the criteria. This happens every time the device user attempts to establish a VPN connection.

- **Manual—**AnyConnect searches for a certificate from the AnyConnect certificate store on the Android device when the profile is downloaded and does one of the following:
  - If AnyConnect finds a certificate based on the certificate matching criteria defined in the VPN client profile, it assigns that certificate to the connection entry and uses that certificate when establishing a connection.
  - If a matching certificate cannot be found, the Certificate Authentication policy is set to Automatic.
  - If the assigned certificate is removed from the AnyConnect certificate store for any reason, AnyConnect resets the Certificate Authentication policy to Automatic.
- **Disabled—**A client certificate is not used for authentication.

- **Make this Server List Entry active when profile is imported—**Defines a server list entry as the default connection once the VPN profile has been downloaded to the device. Only one server list entry can have this designation. The default value is disabled.

Apple iOS Only Setting

- **Reconnect when roaming between 3G/Wifi networks—**When enabled (default), AnyConnect does not limit the time that it takes to try to reconnect after losing a connection, after the device wakes up, or after changes occur in the connection type (such as EDGE(2G), 1xRTT(2G), 3G, or Wi-Fi). This feature provides seamless mobility with a secure connection that persists across networks. It is useful for applications that require a connection to the enterprise, but consumes more battery life.

  If Network Roaming is disabled and AnyConnect loses a connection, it tries to re-establish a connection for up to 20 seconds if necessary. If it cannot, the device user or application must start a new VPN connection if one is necessary.

  Note Network Roaming does not affect data roaming or the use of multiple mobile service providers.

- **Connect on Demand (requires certificate authorization)—**This field allows you to configure the Connect on Demand functionality provided by Apple iOS. You can create lists of rules that are checked whenever other applications start network connections that are resolved using the Domain Name System (DNS).

  Connect on Demand is an option only if the Certificate Authentication field is set to Manual or Automatic. If the Certificate Authentication field is set to Disabled, this check box is dimmed. The Connect on Demand rules, defined by the Match Domain or Host and the On Demand Action fields, can still be configured and saved when the check box is dimmed.

- **Match Domain or Host—**Enter the hostnames (host.example.com), domain names (.example.com), or partial domains (.internal.example.com) for which you want to create a Connect on Demand rule. Do not enter IP addresses (10.125.84.1) in this field.

- **On Demand Action**Specify one of the following actions when a device user attempts to connect to the domain or host defined in the previous step:
  - **Never connect—**iOS will never start a VPN connection when rules in this list are matched. Rules in this list take precedence over all other lists

    Note When Connect On Demand is enabled, the application automatically adds the server address to this list. This prevents a VPN connection from being automatically established if you try accessing the server's clientless portal with a web browser. Remove this rule if you do not want this behavior.

  - **Connect if Needed—**iOS will start a VPN connection when rules in this list are matched only if the system could not resolve the address using DNS.
  - **Always Connect—**Always connect behaviour is release dependent:
    - On Apple iOS 6, iOS will always start a VPN connection when rules in this list are matched.
    - On iOS 7.x, Always Connect is not supported, when rules in this list are matched they behave as Connect If Needed rules.
    - On later releases, Always Connect is not used, configured rules are moved to the Connect If Needed list and behave as such.

- **Add or Delete—**Add the rule specified in the Match Domain or Host and On Demand Action fields to the rules table, or delete a selected rule from the rules table.

Troubleshoot AnyConnect on Mobile Devices

Before You Begin

Enable logging on the mobile device and follow the troubleshooting instructions in the appropriate User Guide:

- Windows Phone User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.1.x

If following those instructions does not resolve the issue, try the following:

Procedure

Step 1 Determine whether the same problem occurs with the desktop client or another mobile OS.

Step 2 Ensure that the proper licenses are installed on the ASAs.

Step 3 If certificate authentication is failing, check the following:

a) Ensure that the correct certificate is being selected.

b) Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage.

c) Ensure that the certificate matching rules in the AnyConnect profile are not filtering out the user's selected certificate.

Even if a user selected the certificate, it is not used for authentication if it does not match the filtering rules in the profile.

d) If your authentication mechanism uses any associated accounting policy to an ASA, verify that the user can successfully authenticate.
e) If you see an authentication screen when you are expecting to use certificate-only authentication, configure the connection to use a group URL and ensure that secondary authentication is not configured for the tunnel group.

What to Do Next

If problems persist, enable logging on the client and enable debug logging on the ASA. For details, refer to the release-appropriate Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides.