# Cisco AnyConnect Mobile Platforms Administrator Guide, Release 4.0

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# CONTENTS

CHAPTER 1

# 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:

- Android
- Apple iOS
- BlackBerry
- Chromebook

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.
- Added after the user clicks a link provided by the administrator to configure connection entries.

  See Generate a VPN Connection Entry, on page 25 to provide this kind of connection entry configuration to your users.
- 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 21.

# 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.

### OCSP Revocation

The AnyConnect client supports OCSP (Online Certificate Status Protocol). This allows the client to query the status of individual certificates in real time by making a request to the OCSP responder and parsing the OCSP response to get the certificate status. OCSP is used to verify the entire certificate chain. There is a five second timeout interval per certificate to access the OCSP responder.

The user can enable or disable OCSP verification in the Anyconnect settings activity, for details see the Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0. We have also added new API's in our framework which can be used by MDM administrators to control this feature remotely. Currently we support Samsung and Google MDM.

### Strict Certificate Trust

If enabled by the user, when authenticating remote security gateways, AnyConnect disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect to security gateways.

**Note** This setting overrides **Block Untrusted Server**.

If not selected, the client prompts the user to accept the certificate. This is the default behavior.

We strongly recommend that you enable Strict Certificate Trust for the AnyConnect client for the following reasons:

- With the increase in targeted exploits, enabling Strict Certificate Trust in the local policy helps prevent “man in the middle” attacks when users are connecting from untrusted networks such as public-access networks.
- Even if you use fully verifiable and trusted certificates, the AnyConnect client, by default, allows end users to accept unverifiable certificates. If your end users are subjected to a man-in-the-middle attack, they may be prompted to accept a malicious certificate. To remove this decision from your end users, enable Strict Certificate Trust.

## 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, on page 97 for details.
- Added after the user clicks a link provided by the administrator to import a certificate.

  See Import Certificates, on page 30 to provide this kind of certificate deployment to your users.

# VPN Authentication Using SAML

You can use SAML 2.0 integrated with ASA release 9.7.1 for initial session authentication. To provide a seamless reconnect without disruption, AnyConnect intentionally skips the repeating of the SAML authentication process. Additionally, if the user logs out of the IdP using a browser, the AnyConnect session remains intact.

Follow these guidelines when using SAML:

- You must synchronize your ASA's Network Time Protocol (NTP) server with the IdP NTP server in order to use the SAML feature.
- The VPN Wizard on ASDM does not currently support SAML configurations.
- You cannot access internal servers with SSO after logging in using an internal IdP.
- The SAML IdP *NameID* attribute determines the user's username and is used for authorization, accounting, and VPN session database.
- You should set Auto Reconnect to *ReconnectAfterResume* in the AnyConnect Profile Editor, Preferences (Part 1), on page 44 if you want users to re-authenticate with the Identity Provider (IdP) every time they establish a VPN session via SAML.

For AnyConnect Mobile the following platforms and versions are supported:

- Chrome OS 4.0.10151

Refer to the *SSO Using SAML 2.0* section in the appropriate release, 9.7 or later, of the Cisco ASA Series VPN Configuration Guide for additional configuration 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, on page 7 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

Localize the AnyConnect UI and Messages, on page 31 by providing a URI link to the user.

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.

## Import Translation Tables to the Adaptive Security Appliance

#### 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 AnyConnect clients with this preferred language. Localization will be applied after AnyConnect restarts and connects.

**Note** For AnyConnect running on non-mobile devices, the Cisco Secure Desktop translation table must also be imported onto the Adaptive Security Appliance for Host Scan messages to be localized, even if Cisco Secure Desktop is not being used.

# 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.

### 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 Android Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.0.x for Android for features and devices supported by this release.

Refer to the Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0 to install, upgrade, and use the AnyConnect app.

## Guidelines and Limitations for AnyConnect on Android

- AnyConnect for Android supports only the VPN features that are strictly related to remote access.
- AnyConnect for Android supports only the Network Visibility Module, it does not support any other AnyConnect modules.
- The ASA does not provide distributions and updates for AnyConnect for Android. They are available only on Google Play.
- AnyConnect for Android supports connection entries that the user adds and connection entries populated by an AnyConnect profile pushed by an ASA. The Android device supports no more than one AnyConnect profile, which is the last one received from a headend. However, a profile can consist of multiple connection entries.
- If users attempt to install AnyConnect on devices that are not supported, they receive the pop-up message`Installation Error: Unknown reason -8`. This message is generated by the Android OS.
- When users have an AnyConnect widget on their home screen, the AnyConnect services are automatically started (but not connected) regardless of the "Launch at startup" preference.
- AnyConnect for Android requires UTF-8 character encoding for extended ASCII characters when using pre-fill from client certificates. The client certificate must be in UTF-8 if you want to use prefill, per the instructions in KB-890772 and KB-888180.
- AnyConnect blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection per the inherent nature of EDGE and other early radio technology.

- Some known file compression utilities do not successfully decompress log bundles packaged with the use of the AnyConnect Send Log button. As a workaround, use the native utilities on Windows and Mac OS X to decompress AnyConnect log files.

# Android Specific Considerations

## Android Mobile Posture Device ID Generation

Upon a fresh installation, or after the user clears the application data, AnyConnect now generates a unique 256-byte device ID, which is based on the Android ID. This ID replaces the legacy 40-byte device ID based on the IMEI and MAC address generated in earlier releases.

If an earlier version of AnyConnect is installed, a legacy ID has already been generated. After upgrading to this version of AnyConnect, this legacy ID continues to be reported as the Device Unique ID until the user clears the application data or uninstalls AnyConnect.

Generated device IDs can be viewed after the initial application launch from the AnyConnect **Diagnostics** > **Logging and System Information** > **System** > **Device Identifiers** screen, or inside the AnyConnect log in the `device_identifiers.txt` file, or on the **About** Screen.

**Note** DAP policies on the secure gateway will need to be updated to use the new device IDs.

The `Device-ID` is determined as follows:

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

Where the `Android-ID` and `bytesToHexString` are defined as follows:

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

## Android Device Permissions

The following permissions are declared in the Android manifest file for AnyConnect operation:

| Manifest Permission | Description |
|---|---|
| uses-permission: android.permission.ACCESS_NETWORK_STATE | Allows applications to access information about networks. |
| uses-permission: android.permission.ACCESS_WIFI_STATE | Allows applications to access information about Wi-Fi networks. |

| Manifest Permission | Description |
|---|---|
| uses-permission: android.permission.BROADCAST_STICKY | Allows an application to broadcast sticky intents. These are broadcasts whose data is held by the system after being finished, so that clients can quickly retrieve that data without having to wait for the next broadcast. |
| uses-permission: android.permission.INTERNET | Allows applications to open network sockets. |
| uses-permission: android.permission.READ_EXTERNAL_STORAGE | Allows an application to read from external storage. |
| uses-permission: android.permission.READ_LOGS | Allows an application to read the low-level system log files. |
| uses-permission: android.permission.READ_PHONE_STATE | Allows read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device. |
| uses-permission: android.permission.RECEIVE_BOOT_COMPLETED | Allows an application to receive the broadcast after the system finishes booting. |

# AnyConnect on Apple iOS Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.0.x for Apple iOS for features and devices supported by this release.

Refer to the Apple iOS User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x to install, upgrade, and use the AnyConnect app.

## Guidelines and Limitations for AnyConnect on Apple iOS

AnyConnect for Apple iOS supports only features that are related to remote VPN access such as:

- AnyConnect can be configured by the user (manually), by the AnyConnect VPN Client Profile, generated by the iPhone Configuration Utility (http://www.apple.com/support/iphone/enterprise/), or using an Enterprise Mobile Device Manager.
- The Apple iOS device supports no more than one AnyConnect VPN client profile. The contents of the generated configuration always match the most recent profile. For example, you connect to vpn.example1.com and then to vpn.example2.com, the AnyConnect VPN client profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.
- This release supports the tunnel keepalive feature; however, it reduces battery life of the device. Increasing the update interval value mitigates this issue.

Apple iOS Connect On-Demand Considerations:

- VPN sessions that are automatically connected as a result of iOS On-Demand logic and have Disconnect on Suspend configured, are disconnected when the device sleeps. After the device wakes up, On-Demand logic will reconnect the VPN session when it is necessary again.
- AnyConnect collects device information when the UI is launched and a VPN connection is initiated. Therefore, there are circumstances in which AnyConnect can misreport mobile posture information if the user relies on iOS's Connect On-Demand feature to make a connection initially, or after device information, such has the OS version, has changed.
- This only applies in your environment if you are running a Legacy AnyConnect release earlier than 4.0.05032, or an Apple iOS release earlier than 9.3 while using Apple Connect-on-Demand capabilities. To ensure proper establishment of Connect On-Demand VPN tunnels after updating AnyConnect, users must manually start the AnyConnect app and establish a connection. If this is not done, upon the next iOS system attempt to establish a VPN tunnel, the error message "The VPN Connection requires an application to start up" displays.

Cisco AnyConnect and Legacy AnyConnect are different apps with different app IDs. Hence:

- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to the new 4.0.07x version. Cisco AnyConnect 4.0.07x is a separate app, installed with a different name and icon.
- The different versions of AnyConnect can co-exist on the mobile device, but this is not supported by Cisco. The behavior may not be as expected if you attempt to connect while having both versions of AnyConnect installed. Make sure you have only one AnyConnect app on your device and it is the appropriate version for your device and environment.
- Certificates imported using Legacy AnyConnect version 4.0.05069 and any earlier release, cannot be accessed or used by the new AnyConnect app release 4.0.07072 or later. MDM deployed certificates can be accessed and used by both app versions.
- App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. Otherwise they will continue to show in the system VPN settings. Remove app data before uninstalling the Legacy AnyConnect app.
- Current MDM profiles will not trigger the new app. EMM vendors must support VPNType (VPN), VPNSubType (com.cisco.anyconnect) and ProviderType (packet-tunnel). For integration with ISE, they must be able to pass the UniqueIdentifier to AnyConnect since AnyConnect no longer has access to this in the new framework. Please consult with your EMM vendor for how to set this up, some may require a custom VPN type and others may not have support available at release time.

Using the New Extension Framework in AnyConnect 4.0.07x and later causes the following changes in behavior from Legacy AnyConnect 4.0.05x:

- The Device ID sent to the head end is no longer the UDID in the new version, and it is different after a factory reset unless your device is restored from a backup made by the same device.
- You may use MDM deployed certificates, as well as certificates imported using one of the methods available in AnyConnect: SCEP, manually through the UI, or via the URI handler. The new version of AnyConnect can no longer use certificates imported via email or any other mechanism beyond these identified ones.
- When creating a connection entry using the UI, the user must accept the iOS security message displayed.
- A user-created entry with the same name as a downloaded host entry from the AnyConnect VPN profile will not be renamed until it disconnects, if it is active. Also, the downloaded host connection entry will appear in the UI after this disconnect, not while it remains connected.

# Apple iOS Specific Considerations

When supporting AnyConnect on Apple iOS devices, consider:

- The SCEP references in this document apply exclusively to AnyConnect SCEP, not Apple iOS SCEP.
- Push email notifications do not work over VPN because of Apple iOS constraints. However, AnyConnect works in parallel with externally accessible ActiveSync connections, when the tunnel policy excludes these from the session.

### The Apple iPhone Configuration Utility

The iPhone Configuration Utility (IPCU), available from Apple for Windows or Mac OS X, is used to create and deploy configurations to an Apple iOS device. This can be done in place of configuring an AnyConnect client profile on the secure gateway.

The existing IPCU GUI, controlled by Apple, does not know of the AnyConnect IPsec capabilities. Configure IPsec VPN connections within the existing AnyConnect GUI in IPCU. Use the following URI syntax, as defined in RFC 2996 in the Server field. This Server field syntax is backward compatible with the documented usage for configuring SSL VPN connections.

[**ipsec**://][<**AUTHENTICATION**>[“:”<**IKE-IDENTITY**>“@”]] <**HOST**>[“:”<**PORT**>][“/”<**GROUP-URL**>]

| Parameter | Description |
|---|---|
| ipsec | : Indicates that this is an IPsec connection. If omitted, SSL is assumed. |
| AUTHENTICATION | Specifies the authentication method for an IPsec connection. If omitted, EAP-AnyConnect is assumed. Valid values are:<br>• EAP-AnyConnect<br>• EAP-GTC<br>• EAP-MD5<br>• EAP-MSCHAPv2<br>• IKE-RSA |
| IKE-IDENTITY | Specifies the IKE identify when AUTHENTICATION is set to EAP-GTC, EAP-MD5, or EAP-MSCHAPv2. This parameter is invalid when used for other authentication settings. |
| HOST | Specifies the server address. The hostname or IP address to be used. |
| PORT | Currently ignored, included for consistency with the HTTP URI scheme. |
| GROUP=URL | Tunnel group name appended to the server name. |

Examples:

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

To connect to a standards-compliant Cisco IOS router only, use the following:

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

### Connect-on-Demand Usage Guidelines

The Apple iOS Connect-on-Demand feature lets other applications, such as Safari, start a VPN connection. Apple iOS evaluates the domain requested by the application against the rules configured for the device's active connection entry. Apple iOS establishes a VPN connection on behalf of an application only if all of the following are true:

- A VPN connection is not already established.
- An application compatible with the Apple iOS Connect-on-Demand framework requests a domain.
- The connection entry is configured to use a valid certificate.
- Connect On Demand is enabled in the connection entry.
- Apple iOS fails to match a string in the Never Connect list to the domain request.
- Either of the following is true: Apple iOS matches a string in the Always Connect list to the domain request (on Apple iOS 6 only). Or a DNS lookup failed, and Apple iOS matches a string in the Connect if Needed list to the domain request.

Keep in mind the following when using the Connect-on-Demand feature:

- After a VPN connection is initiated using iOS's Connect on Demand, iOS disconnects the tunnel if the tunnel is inactive for a particular time interval. See Apple’s VPN Connect-on-Demand documentation for more information.
- We recommend using the Connect if Needed option if you configure rules. A Connect if Needed rule starts a VPN connection if the DNS lookup to an internal host fails. It requires a correct DNS configuration so that hostnames within the enterprise are resolved using internal DNS servers only.
- For mobile devices that have Connect on Demand configured, certificate-based authentication tunnel groups have a short (60 second) idle timeout (vpn-idle-timeout). Set a short idle timeout if your VPN session is not critical for an application and does not always need to be connected. The Apple device closes the VPN connection when it is no longer needed, for example, when the device goes into sleep mode. The default idle timeout for a tunnel group is 60 minutes.
- Always connect behavior is release dependent:
    - ◦ On Apple iOS 6, iOS always starts 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.
- Apple has introduced a Trusted Network Detection (TND) enhancement to theConnect-on-Demand feature. This enhancement:
    - ◦ Extends the Connect-on-Demand functionality by determining whether the device user is on a trusted network.
    - ◦ Applies to Wi-Fi connectivity only. When operating over other types of network connections, Connect on Demand does not use TND to determine whether to connect a VPN.

  - ◦ Is not a separate feature and cannot be configured or used outside the Connect-on-Demand capabilities.

  Contact Apple for more information about Connect on Demand Trusted Network Detection in iOS 6.

- The integrated Apple iOS IPsec client and AnyConnect both use the same Apple iOS VPN Connect-on-Demand framework.

### Split DNS Resolution Behavior with Split Tunnel

The ASA split tunneling feature lets you specify which traffic goes over the VPN tunnel and which traffic goes in the clear. An associated feature called split DNS lets you specify which DNS traffic is eligible for DNS resolution over the VPN tunnel and which DNS traffic the endpoint DNS resolver handles (in the clear). Split DNS works differently on Apple iOS devices than on other devices if you also configure split tunneling. AnyConnect for Apple iOS responds to this command as follows:

- Encrypts only DNS queries for domains in the split-dns list.

  AnyConnect tunnels only the DNS queries for the domains specified in the command. It sends all other DNS queries to the local DNS resolver for resolution in-the-clear. For example, AnyConnect tunnels only the DNS queries for example1.com and example2.com in response to the following command:

  ```
  hostname(config-group-policy)# split-dns value example1.com example2.com
  ```

- Encrypts only DNS queries for the domain in the default-domain command.

  If the **split-dns none** command is present and the **default-domain** command specifies a domain, AnyConnect tunnels only DNS queries for that domain and sends all other DNS queries to the local DNS resolver for resolution in-the-clear. For example, AnyConnect tunnels only the DNS queries for example1.com in response to the following commands:

  ```
  hostname(config-group-policy)# split-dns none
  hostname(config-group-policy)# default-domain value example1.com
  ```

- Sends all DNS queries in-the-clear. If the **split-dns none** and **default-domain none** commands are present in the group policy, or if these commands are absent from the group policy but present in the default group policy, AnyConnect sends all DNS queries to the local DNS resolver for resolution in-the-clear.

**Note** If split-dns is not specified, the group policy inherits the spit tunneling domain lists that are present in the default group policy. To prevent inheriting a split tunneling domain list, use the split-dns none command.

# AnyConnect on BlackBerry Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.0.x for BlackBerry for features and devices supported by this release.

Refer to the BlackBerry User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x to install, upgrade, and use the AnyConnect app.

## Guidelines and Limitations for AnyConnect on BlackBerry

- Enabling Split DNS can break VPN connections. Blackberry supports a maximum of two DNS servers. Our ASA configured DNS server takes precedence because it is prepended in the DNS server list, so our ASA configured DNS server is applied to the tun adapter. If the ASA configures two private DNS servers without DNS forwarding in the ASA side, then DNS resolution of public network will fail.

  Work around: Until BlackBerry supports more than 2 DNS servers, the Admin should configure only one private DNS server on the ASA end.

- AnyConnect VPN profiles which are pushed to devices from an ASA headend, block all untrusted servers by default. This may be preventing a successful VPN connection. Disable this setting to provide the user with the option to accept or deny connections to untrusted servers

- IPsec IKEv2 VPN connections must be enabled and configured manually on the device by the user. Only EAP authentication is supported when connecting to the ASA headend.

# AnyConnect on Chrome OS Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.0.x for Google Chrome OS for features and devices supported by this release.

Refer to the Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0 to install, upgrade, and use the AnyConnect app.

## Guidelines and Limitations for AnyConnect on Chrome OS

- When the Chromebook device is managed (enrolled in an Enterprise Chrome Management service), then AnyConnect cannot access client certificates: client certificate authentication does not work.

- There is limited VPN performance on low-end Chromebooks (chromium issue #514341).

- Auto reconnect, reconnecting the VPN session when the network interface goes down and up, is supported when using AnyConnect release 4.0.10113 or later with Chrome OS 51 or later. Prior to Chrome 51 and this AC release, if you lost Wi-Fi, or put your device to sleep, AnyConnect would not be able to reconnect on its own.

- Unless you are using Chrome OS 45 or later, all server certificates, even fully trusted and valid ones, received from the secure gateway are seen as untrusted.

- After installing or upgrading AnyConnect on Chrome OS, wait until initializing is complete to configure AnyConnect. "Initializing, please wait..." is displayed in the AnyConnect app. This process may take a few minutes.

# 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.<br>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.<br>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";
```

**Step 3** (Optional) Configure Per App VPN tunneling mode.
See Configure Per App VPN, on page 17.

If Per App VPN tunneling mode is not configured, the AnyConnect app operates in system-tunneling mode.

# Configure Per App VPN

### Before You Begin

AnyConnect Per App VPN tunneling requires:

- ASA 9.3.1 or later to configure Per App VPN tunneling.
- An AnyConnect v4.0 Plus or Apex license.

AnyConnect Per App VPN supports the following mobile platforms:

- Android devices running Android 5.0 (Lollipop) or later.
- Apple iOS devices running Apple iOS 8.3 or later configured to use Per App VPN in a Mobile Device Management (MDM) solution.

### Procedure

**Step 1** Install the Cisco AnyConnect Enterprise Application Selector Tool, on page 18.

**Step 2** Use the Application Selector tool to specify an AnyConnect Per App VPN policy for your platform:

- Define a Per App VPN Policy for Android Devices, on page 19
- Define a Per App VPN Policy for Apple iOS Devices, on page 20

**Step 3** Create Per App Custom Attributes, on page 20 on the ASA.

**Step 4** Assign a Custom Attribute to a Policy on the ASA, on page 21.

# Install the Cisco AnyConnect Enterprise Application Selector Tool

The Application Selector Tool is a standalone application that supports policy generation for both Android and Apple iOS devices.

### Before You Begin

The Cisco AnyConnect Enterprise Application Selector requires Java 7 or later.

### Procedure

**Step 1** Download the Cisco AnyConnect Enterprise Application Selector tool from the Cisco.com AnyConnect Secure Mobility Client v4.x Software Center.

**Step 2** If you are using Android apps in your policy, you must have the Android SDK and the Android SDK Build-tools installed on your system. If you do not, install them as follows.

a) Install the latest version of the Android SDK Tools for the platform you are running the Application Selector Tool on.
Install the recommended **SDK Tools Only** package for your platform using the default paths and settings, including: Install for All Users, so access to package entities is as described.

b) Using the Android SDK Manager, install the latest version of the **Android SDK Build-tools**.

### What to Do Next

**Note** If prompted in the application selector tool, configure access to the Android Asset Packaging Tool, **aapt**, by specifying its installed location, `*Android SDK installation directory*\build-tools\*build-tools version number*\`.

# Define a Per App VPN Policy for Android Devices

Your Per App VPN policy consists of a set of rules, where each rule identifies an app whose data flows over the tunnel. Specify the rule options to more stringently identify the allowable app and its use in your mobile device environment. The Application Selector tool uses information from the app's package file, `*.apk`, to set rule options. See http://developer.android.com/guide/topics/manifest/manifest-element.html for Android package manifest information.

### Before You Begin

The Cisco AnyConnect Enterprise Application Selector requires Java 7 or later.

### Procedure

**Step 1** Start the application selector and choose the **Android** mobile device platform.

**Step 2** Set the required **App ID** field.

- Choose **Import from Disk** to obtain app-specific package information from an app stored on your local system.

  The APP ID field (a string in reverse-DNS format) is automatically filled in. For example, if choosing the Chrome app for an Apple iOS policy, the APP ID field is set to com.google.chrome.ios. For Chrome on Android, it would be set to com.android.chrome.

- Alternatively, you may enter this app-specific information directly.

- Specify reverse-DNS format using a wildcard, for example, specify com.cisco.* to tunnel all Cisco apps, instead of listing each one in its own rule. The wildcard must be the last character in the APP ID entry.

  When configuring Per App VPN in a managed environment, verify that the ASA policy allows the same apps to tunnel as the MDM policy. Specifying *.* as the APP ID allows ALL apps to tunnel and ensures that the MDM policy is the only arbiter of tunneled apps.

**Step 3** (Optional) Select a listed app and configure more parameters if desired.

- Minimum Version—The minimum version of the chosen app as specified in the package's manifest attribute *android: versionCode*.

- Match Certificate ID—A digest of the application signing certificate.

- Allow Shared UID—Default value is true. If set to false, applications with an *android: sharedUserId* attribute specified in the package manifest will not match this rule, and are prevented from accessing the tunnel.

**Step 4** Click **File** > **Save** to save this Per App VPN policy.

**Step 5** Select **Policy** > **View Policy** to view the representation of the defined policy.
Copy this string, it is the string that becomes the value of a *perapp* custom attribute on the ASA.

# Define a Per App VPN Policy for Apple iOS Devices

The policy for Per App VPN on Apple iOS devices is entirely controlled by the MDM facilities. Therefore, AnyConnect must allow ALL apps, and MDM must configure per app policies to specify the particular apps that can be tunneled.

### Before You Begin

The Cisco AnyConnect Enterprise Application Selector requires Java 7 or later.

### Procedure

**Step 1** Start the application selector and choose the **Apple iOS** mobile device platform.

**Step 2** Set the required **App ID** field to *.*.
This setting allows ALL apps to tunnel through AnyConnect and ensures that the MDM per app policy is the only arbiter of tunneled apps.

**Step 3** Click **File > Save** to save this Per App VPN policy.

**Step 4** Select **Policy > View Policy** to view the representation of the defined policy.
Copy this string, it is the string that becomes the value of a *perapp* custom attribute on the ASA.

# Create Per App Custom Attributes

### Procedure

**Step 1** In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** to configure a custom attribute type.

**Step 2** Choose **Add** or **Edit** and set the following in the **Create / Edit Custom Attribute Type** pane:

a) Enter *perapp* as the type.
The type must be *perapp*, it is the only type of attribute understood by the AnyConnect client for Per App VPN.

b) Enter a description of your choosing.

**Step 3** Click **OK** to close this pane.

**Step 4** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** to configure a custom attribute.

**Step 5** Choose **Add** or **Edit** and set the following in the **Create / Edit Custom Attribute Name** pane:

a) Choose the *perapp* attribute **Type**.

b) Enter a **Name**. This name is used to assign this attribute to a policy.

c) **Add** one or more values by copying the BASE64 format from the policy tool and pasting it here.
Each value cannot exceed 420 characters. If your value exceeds this length, add multiple values for the additional value content. The configured values are concatenated before being sent to the AnyConnect client.

## Assign a Custom Attribute to a Policy on the ASA

The perapp custom attribute can be assigned to a Group Policy or a Dynamic Access Policy.

### Procedure

**Step 1** Open the policy on the ASA:

- For a Group Policy navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add** / **Edit** > **Advanced** > **AnyConnect Client** > **Custom Attributes**.
- For a Dynamic Access Policy navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies Add** / **Edit** . In the **Access/Authorization Policy Attributes** section select the **AnyConnect Custom Attributes** tab.

**Step 2** Click **Add** or **Edit** an existing attribute to open the **Create / Edit Custom Attribute** pane.

**Step 3** Select the predefined *perapp* attribute type from the drop-down list.

**Step 4** Choose **Select Value** and select a predefined value from the drop-down list

**Step 5** Click **OK** to close the open configuration panes.

## 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, on page 67 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.<br>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 22.
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, on page 41 chapter for instructions on how to import the VPN client profile to the ASA and associate it with a group policy.

- Provide the user with an AnyConnect URI link to import a client profile. (Android and Apple iOS only)

  See Import a VPN Client Profile, on page 31 to provide this kind of deployment procedure to your users.

- Have the user import an AnyConnect profile using **Profile Management** on the mobile device. (Android and Apple iOS only)

  See the appropriate mobile device User Guide for device-specific procedures.

# AnyConnect Profile Editor, Mobile Settings

Related Topics: Configure Mobile Device Connections in the AnyConnect VPN Profile, on page 21

### 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.

  Related Topics: Apple iOS Specific Considerations, on page 12

- **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.

# Automate AnyConnect Actions Using the URI Handler

The URI handler in AnyConnect lets other applications pass action requests in the form of Universal Resource Identifiers (URIs) to AnyConnect. To simplify the AnyConnect user setup process, embed URIs as links on web pages or e-mail messages, and give users instructions to access them.

### Before You Begin

- URI handling in the AnyConnect application is disabled by default. Mobile device users allow this functionality by setting the **External Control** app setting to Enable or Prompt. When enabled, external control allows all URI commands without user interaction. When set for prompting, the user is notified of URI activity and allows or disallows it at request time. You should inform your users how to respond to prompts associated with URI handling if you are using them.
- You must use URL encoding when entering URI handler parameter values. Use a tool such as the one in this link to encode an action request. Also, refer to provided examples below.
- In the URI, `%20` represents a space, `%3A` represents a colon (:), `%2F` represents a forward slash (/), and `%40` represents an ampersand (@).

- Slashes in the URI are optional.

Provide your users with any of the following actions.

# Generate a VPN Connection Entry

Use this AnyConnect URI handler to simplify the generation of an AnyConnect connection entry for users.

**anyconnect:**[//]**create**[/]**?name**=*Description***&host**=*ServerAddress*[**&Parameter1**=*Value***&Parameter2**=*Value* ...]

### Guidelines

- The *host* parameter is required, all other parameters are optional. When the action runs on the device, AnyConnect saves all the parameter values that you enter to the connection entry associated with that *name* and *host*.
- Use a separate link for each connection entry that you want to add to the device. Specifying multiple create connection entry actions in a single link is not supported.

### Parameters

- **name—**Unique name for the connection entry to appear in the connection list of the AnyConnect home screen and the Description field of the AnyConnect connection entry. AnyConnect responds only if the name is unique. We recommend using a maximum of 24 characters to ensure that they fit in the connection list. Use letters, numbers, or symbols on the keyboard displayed on the device when you enter text into a field. The letters are case-sensitive.
- **host—**Enter the domain name, IP address, or Group URL of the ASA with which to connect. AnyConnect inserts the value of this parameter into the Server Address field of the AnyConnect connection entry.

  ```
  anyconnect://create/?name=SimpleExample&host=vpn.example.com
  anyconnect:create?name=SimpleExample&host=vpn.example.com
  ```

- **protocol** (optional, defaults to SSL if unspecified)**—**The VPN protocol used for this connection. The valid values are:
  - SSL
  - IPsec

  ```
  anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
  ```

- **authentication** (optional, applies when protocol specifies IPsec only, defaults to EAP-AnyConnect)**—**The authentication method used for an IPsec VPN connection. The valid values are:
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA

- **ike-identity** (required if authentication is set to EAP-GTC, EAP-MD5, or EAP-MSCAPv2)—The IKE identify when AUTHENTICATION is set to EAP-GTC, EAP-MD5, or EAP-MSCHAPv2. This parameter is invalid when used for other authentication settings.

  ```
  anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
  &authentication=eap-md5&ike-identity=012A4F8B29A9BCD
  ```

- **netroam** (optional, applies to Apple iOS only)—Determines whether to limit the time that it takes to reconnect after the device wakes up or after a change to the connection type (such as EDGE, 3G, or Wi-Fi).This parameter does not affect data roaming or the use of multiple mobile service providers. The valid values are:

  - true—(Default) This option optimizes VPN access. AnyConnect inserts the value ON into the Network Roaming field of the AnyConnect connection entry. If AnyConnect loses a connection, it tries to establish a new one until it succeeds. This setting lets applications rely on a sustained connection to the VPN. AnyConnect does not impose a limit on the time that it takes to reconnect.

  - false—This option optimizes battery life. AnyConnect associates this value with the OFF value in the Network Roaming field of the AnyConnect connection entry. If AnyConnect loses a connection, it tries to establish a a new one for 20 seconds and then stops trying. The user or application must start a new VPN connection if one is necessary.

  ```
  anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
  ```

- **keychainalias** (optional)—Imports a certificate from the System Certificate Store to the AnyConnect Certificate Store. This option is for the Android mobile platform only.

  If the named certifiate is not already in the system store, the user will be prompted to choose and install it before being prompted to allow or deny it being copied into the AnyConnect store. External Control must be enabled on the mobile device.

  The following example creates a new connection entry named *SimpleExample* whose IP address is set to *vpn.example.com* with the certificate named *client* assigned to it for authentication.

  ```
  anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
  ```

- **usecert** (optional)—Determines whether to use a digital certificate installed on the device when establishing a VPN connection to the host. The valid values are:

  - true (default setting)—Enables automatic certificate selection when establishing a VPN connection with the host. Turning usecert to true without specifying a certcommonname value sets the Certificates field to Automatic, selecting a certificate from the AnyConnect certificate store at connection time.

  - false—Disables automatic certificate selection.

  ```
  anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
  ```

- **certcommonname** (optional, but requires the usecert parameter)—Matches the Common Name of a valid certificate pre-installed on the device. AnyConnect inserts the value into the Certificate field of the AnyConnect connection entry.

  To view this certificate installed on the device, tap **Diagnostics** > **Certificates**. You might need to scroll to view the certificate required by the host. Tap the detail disclosure button to view the Common Name parameter read from the certificate, as well as the other values.

- **useondemand** (optional, applies to Apple iOS only and requires the usecert, certcommonname parameters, and domain specifications below)—Determines whether applications, such as Safari, can start VPN connections. Valid values are:

- ◦ false (Default)—Prevents applications from starting a VPN connection. Using this option is the only way to prevent an application that makes a DNS request from potentially triggering a VPN connection. AnyConnect associates this option with the OFF value in the Connect on Demand field of the AnyConnect connection entry.
- ◦ true—Lets an application use Apple iOS to start a VPN connection. If you set the useondemand parameter to true, AnyConnect inserts the value ON into the Connect on Demand field of the AnyConnect connection entry. (domainlistalways or domainlistifneeded parameter required if useondemand=true)

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever** (optional, requires useondemand=true)—Lists the domains to evaluate for a match to disqualify the use of the Connect on Demand feature. This list is the first one AnyConnect uses to evaluate domain requests for a match. If a domain request matches, AnyConnect ignores the domain request. AnyConnect inserts this list into the Never Connect field of the AnyConnect connection entry. This list lets you exclude certain resources. For example, you might not want an automatic VPN connection over a public-facing web server. An example value is `www.example.com`.
- **domainlistalways**(domainlistalways or domainlistifneeded parameter required if useondemand=true)—Lists the domains to evaluate for a match for the Connect on Demand feature. This list is the second one AnyConnect uses to evaluate domain requests for a match. If an application requests access to one of the domains specified by this parameter and a VPN connection is not already in progress, Apple iOS attempts to establish a VPN connection. AnyConnect inserts this list into the Always Connect field of the AnyConnect connection entry. An example value list is `email.example.com,pay.examplecloud.com`.
- **domainlistifneeded** (domainlistalways or domainlistifneeded parameter required if useondemand=true)—AnyConnect evaluates a domain request for a match against this list if a DNS error occurred. If a string in this list matches the domain, Apple iOS attempts to establish a VPN connection. AnyConnect inserts this list into the Connect if Needed field of the AnyConnect connection entry. The most common use case for this list is to obtain brief access to an internal resource that is not accessible in a LAN within the corporate network. An example value is `intranet.example.com`.

Use a comma-delimited list to specify multiple domains. The Connect-on-Demand rules support only domain names, not IP addresses. However, AnyConnect is flexible about the domain name format of each list entry, as follows:

| Match | Instruction | Example Entry | Example Matches | Example Match Failures |
|---|---|---|---|---|
| Exact prefix and domain name only. | Enter the prefix, dot, and domain name. | email.example.com | email.example.com | www.example.com<br>email.1example.com<br>email.example1.com<br>email.example.org |

| Match | Instruction | Example Entry | Example Matches | Example Match Failures |
|---|---|---|---|---|
| Any prefix with the exact domain name. The leading dot prevents connections to hosts ending with *example.com, such as notexample.com. | Enter a dot followed by the domain name to be matched. | .example.org | anytext.example.org | anytext.example.com<br>anytext.1example.org<br>anytext.example1.org |
| Any domain name ending with the text you specify. | Enter the end of the domain name to be matched. | example.net<br>anytext. | anytext-example.net<br>anytext.example.net | anytext.example1.net<br>anytext.example.com |

# Establish a VPN Connection

Use this AnyConnect URI handler to connect to a VPN allowing users to easily establish VPN connections. You can also embed additional information in the URI to perform the following tasks:

- Prefill a Username and Password
- Prefill Usernames and Passwords for Double Authentication
- Prefill a Username and Password, and Specify a Connection Profile Alias

This action requires either the name or the host parameters, but allows both using one of the following syntaxes:

**anyconnect:**[//]**connect**[/]**?**[**name=***Description*|**host=***ServerAddress*]
[**&Parameter1**=*Value***&Parameter2**=*Value* ..]
or

**anyconnect:**[//]**connect**[/]**?name=***Description***&host=***ServerAddress*
[**&Parameter1**=*Value***&Parameter2**=*Value* ..]

### Guidelines

- If all the parameter values in the statement match those of an AnyConnect connection entry on the device, AnyConnect uses the remaining parameters to establish the connection.
- If AnyConnect does not match all parameters in the statement to those in a connection entry and the name parameter is unique, it generates a new connection entry and then attempts the VPN connection.
- Specifying a password when establishing a VPN connection using a URI should be used only in conjunction with a One Time Password (OTP) infrastructure.

### Parameters

- **name—**Name of the connection entry as it appears in the connection list of the AnyConnect home window. AnyConnect evaluates this value against the Description field of the AnyConnect connection entries, also called name if you used the previous instructions to create the connection entry on the device. This value is case-sensitive.

- **host—**Enter the domain name, IP address, or Group URL of the ASA to match the Server Address field of an AnyConnect connection entry, also called the host if you used the previous instructions to generate the connection entry on the device.

  The Group URL is configured in ASDM by selecting **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Advanced > Group Alias/Group URL > Group-URL**.

- **onsuccess—**Execute this action if the connection is successful. Platform specific behavior:
  - For Apple iOS devices, specify the URL to be opened when this connection transitions into the connected state, or use the anyconnect:close command to close the AnyConnect GUI.
  - For Android devices, specify the URL to opened when this connection transitions into or is already in the connected state. Multiple onsuccess actions can be specified. AnyConnect always closes the GUI after a successful connection on Android devices.

- **onerror—**Execute this action if the connection fails. Platform specific behavior:
  - For Apple iOS devices, specify the URL to be opened when this connection fails, or use the anyconnect:close command to close the AnyConnect GUI.
  - For Android devices, specify the URL to be opened when this connection fails. Multiple onerror actions can be specified. AnyConnect always closes the GUI after a failed connection on Android devices.

- **prefill_username—**Provides the username in the connect URI and prefills it in connection prompts.
- **prefill_password—**Provides the password in the connect URI and pre-fills it in connection prompts. This field should only be used with connection profiles configured for one-time passwords.
- **prefill_secondary_username—**In environments that are configured to require double authentication, this parameter provides the secondary username in the connect URI and prefills it in the connection prompts.
- **prefill_secondary_password—**In environments that are configured to require double authentication, this parameter provides the password for the secondary username in the connect URI and pre-fills it in the connection prompts.
- **prefill_group_list—**The connection alias defined in ASDM by selecting **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Advanced > Group Alias/Group URL > Connection Aliases**.

### Examples

- Provide the Connection Name and Hostname or Group URL in a URI:

```
anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example&host=hr.example.com
anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- Provide Actions For Success or Failure

Use the onsuccess or onerror parameters to initiate the opening of a specified URL based on the results of the connect action:

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

On Android you can specify multiple onsuccess actions:

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

On Apple iOS devices, the anyconnect://close command can be used in the onsuccess or onerror parameter to close the AnyConnect GUI:

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- Provide Connection Information and Prefill a Username and Password in a URI:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- Provide Connection Information and Prefill Usernames and Passwords for Double Authentication:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- Provide Connection Information, Prefill a Username and Password, and Specify a Connection Profile Alias:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

# Disconnect from a VPN

Use this AnyConnect URI handler to disconnect the user from a VPN.

**anyconnect:**[//]**disconnect**[/]**&onsuccess**=URL

### Parameters

The onsuccess parameter applies to Android devices only. Specify the URL to opened when this connection disconnects or is already in the disconnected state.

### Example

```
anyconnect:disconnect
```

# Import Certificates

Use this URI handler command to import a PKCS12 encoded certificate bundle to the endpoint. The AnyConnect client authenticates itself to the ASA using a PKCS12 encoded certificate that has been installed on the endpoint. Only pkcs12 certificate type is supported.

**anyconnect:**[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

### Parameters

- **type**—Only pkcs12 certificate type is supported.
- **uri**—URL encoded identifier where the certificate is found.

### Examples

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

## Import a VPN Client Profile

Use this URI handler method to distribute client profiles to AnyConnect clients.

**anyconnect:**[//]**import**[/]**?type=profile&uri**=*filename.xml*

### Example

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

## Localize the AnyConnect UI and Messages

Use this URI handler method to localize the AnyConnect client.

**anyconnect:**[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=***ServerAddress*

### Parameters

The import action requires all parameters.

- **type**—The import type, in this case localization.
- **lang**—The two- or four-character language tag representing the language provided in the anyconnect.po file. For example, the language tag may simply be fr for “French” or fr-ca for “Canadian French.”
- **host**—Enter the domain name or IP address of the ASA to match the Server Address field of an AnyConnect connection entry.

### Example

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

# Configure the Network Visibility Module

## About Network Visibility Module

Because users are increasingly operating on unmanaged devices, enterprise administrators have less visibility into what is going on inside and outside of the network. The Network Visibility Module (NVM) collects rich flow context from an endpoint on or off premise and provides visibility into network connected devices and user behaviors when coupled with a Cisco solution such as Stealthwatch, or a third-party solution such as

Splunk. The enterprise administrator can then do capacity and service planning, auditing, compliance, and security analytics. NVM provides the following services:

- Monitors application use to enable better informed improvements (expanded IPFIX collector elements in VzFlow protocol specification) in network design.
- Classifies logical groups of applications, users, or endpoints.
- Finds potential anomalies to help track enterprise assets and plan migration activities.

This feature allows you to choose whether you want the telemetry targeted as opposed to whole infrastructure deployment. The NVM collects the endpoint telemetry for better visibility into the following:

- The device—the endpoint, irrespective of its location
- The user—the one logged into the endpoint
- The application—what generates the traffic
- The location—the network location the traffic was generated on
- The destination—the actual FQDN to which this traffic was intended

When on a trusted network, AnyConnect NVM exports the flow records to a collector such as Cisco Stealthwatch or a third-party vendor such as LiveAction, which performs the file analysis and provides a UI interface. Another third-party vendor such as Splunk may also provide a UI interface to see the reports. Since most enterprise IT administrator want to build their own visualization templates with the data, we provide some sample base templates through a Splunk app plugin.

## NVM on Mobile AnyConnect

The Network Visibility Module (NVM) is included in the latest version of the Cisco AnyConnect Secure Mobility Client for Android, Release 4.0.09xxx, available in the Google playstore. NVM is supported on Samsung devices running Samsung Knox version 2.8 or later. No other mobile devices are currently supported.

Network Visibility on Android is part of the service profile configurations. To configure NVM on Android, an AnyConnect NVM profile is generated by the AnyConnect NVM Profile Editor, and then pushed to the Samsung mobile device using Mobile Device Management (MDM). The AnyConnect NVM Profile Editor from AnyConnect release 4.4.3 or later is required to configure NVM for mobile devices.

### Guidelines

- NVM is supported on Samsung devices running Samsung Knox version 2.8 or later. No other mobile devices are currently supported.
- On mobile devices, connectivity to the collector is supported over IPv4 only. IPv6 is not supported.
- Data collection on Java based apps is not supported.

# Configure NVM for Mobile

### Before You Begin

NVM for Mobile requires the following:

- Samsung devices that are running Samsung Knox 2.8 or later, which requires Android 7.0 or later. These devices must also be configured using an MDM solution.
- The AnyConnect Profile Editor from AnyConnect 4.4.3 or later. Earlier releases do not support mobile NVM configurations.
- TND (Trusted Network Detection) configured in the AnyConnect VPN Profile, and we recommend you set your Trusted Servers.

### Procedure

**Step 1** Open the NVM Profile Editor.

**Step 2** Set the parameters and options for your network environment.
See the NVM Profile Editor, on page 33 topic for details, field definitions, and choices. Be sure to specify this is a **Mobile** NVM Profile.

**Note** Some collected fields are empty because they do not apply to Android or are unsupported. See the field descriptions for details.

The following are the mobile specific fields:

- **KNOX only—**To specify collection of data from the KNOX workspace only.
- **Acceptable Use Policy—**To make the remote user aware of data collection activities.

**Step 3** **Save** the NVM Profile.
The profile is saved as a Base64 encoded file with extension `.b64`.

**Step 4** Use the .b64 NVM profile with your MDM facilities to push this configuration to your mobile devices.

**Note** Using MDM is the only way to configure the mobile NVM capabilities. The NVM Profile cannot be obtained at connectivity time like the VPN Profile.

### What to Do Next

Verify that the collector is receiving data.

## NVM Profile Editor

In the profile editor, configure the IP address or FQDN of the collection server. You can also customize the data collection policy choosing what type of data to send, and whether data is anonymized or not.

The mobile Network Visibility Module can establish a connection using IPv4 only. IPv6 connectivity is not supported.

**Note** The Network Visibility Module sends flow information only when it is on the trusted network. By default, no data is collected. Data is collected only when configured as such in the profile, and the data continues to be collected when the endpoint is connected. If collection is done on an untrusted network, it is cached and sent when the endpoint is on a trusted network. NVM uses the TND feature of VPN to learn if the endpoint is in a trusted network. Also, if VPN is in a connected state, then the endpoint is considered to be on the trusted network, and the flow information is sent. The NVM-specific system logs show TND use. Refer to AnyConnect Profile Editor, Preferences (Part 2), on page 47 for information about setting the TND parameters.

- **Desktop** or **Mobile—**Determines whether you are setting up NVM on a desktop or mobile device. **Desktop** is the default.
- **Collector Configuration**
  - **IP Address/FQDN—**Specifies the IPv4 address/FQDN of the collector.
  - **Port—**Specifies at which port number the collector is listening.
- **Cache Configuration**
  - **Max Size—**Specify the maximum size the database can reach. The cache size previously had a pre-set limit, but you can now configure it within the profile. The data in the cache is stored in an encrypted format, and only processes with root privileges are able to decrypt the data.

    Once a size limit is reached, the oldest data is dropped from the space for the most recent data.
  - **Max Duration—**Specify how many days of data you want to store. If you also set a max size, the limit which reaches first takes precedence.

    Once the day limit is reached, the oldest day's data is dropped from the space for the most recent day. If only Max Duration is configured, there is no size cap; if both are disabled, the size is capped at 50MB.
- **Periodic Flow Reporting**(Optional, applies to desktop only)—Check to enable periodic flow reporting. Reporting of flows (such as server connections or downloads) will occur at the interval you configure, while on a trusted network or over VPN. Periodic flow reporting is disabled by default.
- **Aggregation Interval—**You can customize the NVM timer to define when Cisco nvzFlow exports the data. Specify the interval so that the collector environment is not overrun. The default is 5 seconds.
- **Throttle Rate—**Throttling controls at what rate to send data from the cache to the collector so that the end user is minimally impacted. You can apply throttling on both real time and cached data, as long as there is cached data. Enter the throttle rate in Kbps. The default is 500 Kbps.

  The cached data is exported after this fixed period of time. Enter 0 to disable this feature.
- **Collection Mode—**Specify when data from the endpoint should be collected by choosing collection mode is off, trusted network only, untrusted network only, or all networks.
- **Collection Criteria—** You can reduce unnecessary broadcasts during data collection so that you have only relevant data to analyze. Control collection of data with the following options:
  - **Broadcast packets** and **Multicast packets** (Applies to desktop only)—By default, and for efficiency, broadcast and multicast packet collection are turned off so that less time is spent on

backend resources. Click the check box to enable collection for broadcast and multicast packets and to filter the data.

  - **KNOX only** (Optional and mobile specific)—When checked, data is collected from the KNOX workspace only. By default, this field is not checked, and data from inside and outside the workspace is collected.

- **Data Collection Policy—**You can add data collection policies and associate them with a network type or connectivity scenario. You can apply one policy to VPN and another to non-VPN traffic since multiple interfaces can be active at the same time.

  When you click Add, the Data Collection Policy window appears. Keep these guidelines in mind when creating policies:

  - By default, all fields are reported and collected if no policy is created or associated with a network type.
  - Each data collection policy must be associated with at least one network type, but you cannot have two policies for the same network type.
  - The policy with the more specific network type takes precedence. For example, since VPN is part of the trusted network, a policy containing VPN as a network type takes precedence over a policy which has trusted as the network specified.
  - You can only create a data collection policy for the network that applies based on the collection mode chosen. For example, if the **Collection Mode** is set to **Trusted Network Only**, you cannot create a **Data Collection Policy** for an **Untrusted Network Type**.

  - **Name—**Specify a name for the policy you are creating.
  - **Network Type—**Determine the collection mode, or the network to which a data collection policy applies, by choosing VPN, trusted, or untrusted. If you choose trusted, the policy applies to the VPN case as well.
  - **Include/Exclude**

    - **Type—**Determine which fields you want to **Include** or **Exclude** in the data collection policy. The default is **Exclude**. All fields not checked are collected, and no fields are checked.
    - **Fields—**Determine which fields will be part of your data collection policy. Based on the network type and the fields included or excluded, NVM collects the appropriate data on the endpoint.

      See Collection Parameters for NVM, on page 36 for details.

      For AnyConnect release 4.4 (and later), you can now choose Interface State and SSID, which specifies whether the network state of the interface is trusted or untrusted.

    - **Optional Anonymization Fields—**If you want to correlate records from the same endpoint while still preserving privacy, choose the desired fields as anonymized, and they are sent as the hash of the value rather than actual values. A subset of the fields is available for anonymization.

      Fields marked for include or exclude are not available for anonymization; likewise, fields marked for anonymization are not available for include or exclude.

- **Acceptable Use Policy** (Optional and mobile specific)—Click **Edit** to define an Acceptable Use Policy for mobile devices in the dialog box. Once complete, click **OK**. A maximum of 4000 characters is allowed.

  This message is shown to the user once after NVM is configured. The remote user does not have a choice to decline NVM activities. The network administrator controls NVM using MDM facilities.

# Collection Parameters for NVM

The following parameters are collected at the endpoint and exported to the collector:

*Table 1: Endpoint Identity*

| Parameter | Description / Notes |
|---|---|
| Virtual Station Name | Empty for Android, not provided by Samsung. |
| UDID | Universally Unique Identifier. Uniquely identifies the endpoint corresponding to each flow. This UDID value is also reported by Hostscan in Desktop, and ACIDex in Mobile. |
| OS Name | |
| OS Version | |
| SystemManufacturer | |
| System Type | Set to `arm` for Android.<br>`x86` or `x64` for other platforms. |
| OS Edition | |

*Table 2: Interface Information*

| Parameter | Description / Notes |
|---|---|
| Endpoint UDID | Same as UDID. |
| Interface UID | |
| Interface Index | |
| Interface Type | |
| Interface Name | |

| Parameter | Description / Notes |
|---|---|
| Interface Details List | State and SSID, attributes of InterfaceDetailsList. Indicate the network state of the interface (trusted or untrusted), and the SSID of the connection. |
| Interface MAC address | Windows and Mac OS only<br>Empty for Android, not supported. |

*Table 3: Flow Information*

| Protocol Identifier | Description / Notes |
|---|---|
| Source IPv4 Add | |
| Destination IPv4 Addr | |
| Source Transport Port | |
| Destination Transport Port | |
| Source IPv6 Addr | Empty for Android, not supported. |
| Destination IPv6 Addr | Empty for Android, not supported. |
| Start Sec<br>End Sec | The absolute timestamp of the start or end of the flow. |
| Flow UDID | Same as UDID. |
| Logged In User | Empty for Android, not supported. |
| Logged In User Account Type | Windows and Mac OS only.<br>Empty for Android, not supported. |
| Process Account | Empty for Android, not supported. |
| Process Account type | Windows and Mac OS only.<br>Empty for Android, not supported. |
| Process Name | |
| Process Hash | |
| Parent Process Account | Empty for Android, not supported. |

| Protocol Identifier | Description / Notes |
|---|---|
| Parent Process Account Type | Windows and Mac OS only.<br>Empty for Android, not supported. |
| Parent Process Name | |
| Parent Process Hash | Set to 0 for Android. |
| DNS Suffix | Configured on the interface associated with the flow on the endpoint. |
| L4ByteCountIn | |
| L4ByteCountOut | |
| Destination Hostname | Actual FQDN that resolved to the destination IP on the endpoint |
| Interface UID | |
| Module Name List | Empty for Android, not supported. |
| Module Hash List | Empty for Android, not supported. |

# Troubleshoot AnyConnect on Mobile Devices

### Before You Begin

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

- Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0
- Apple iOS User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x
- BlackBerry User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.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.

**Step 4** On Apple iOS devices, check the following.

a) If the VPN connection is not restored after the device wakes up, ensure that Network Roaming is enabled.

b) If using Connect on Demand, verify certificate-only authentication and a Group URL are configured.

### 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.

CHAPTER 2

# The AnyConnect Profile Editor

## About the Profile Editor

The Cisco AnyConnect Secure Mobility Client software package contains a profile editor for all operating systems. ASDM activates the profile editor when you load the AnyConnect client image on the ASA. You can upload a client profile from local or flash.

If you load multiple AnyConnect packages, ASDM activates the client profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

There is also a stand-alone profile editor which runs on Windows.

### Add a New Profile from ASDM

**Note** You must first upload a client image before creating a client profile.

Profiles are deployed to administrator-defined end user requirements and authentication policies on endpoints as part of AnyConnect, and they make the preconfigured network profiles available to end users. Use the profile editor to create and configure one or more profiles. AnyConnect includes the profile editor as part of ASDM and as a stand-alone Windows program.

To add a new client profile to the ASA from ASDM:

### Procedure

**Step 1** Open ASDM and select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

**Step 2** Click **Add**.

**Step 3** Enter a profile name.

**Step 4** From the Profile Usage drop-down list, choose the module for which you are creating a profile.

**Step 5** (Optional) In the Profile Location field, click **Browse Flash** and select a device file path for the XML file on the ASA.

**Step 6** (Optional) If you created a profile with the stand-alone editor, click **Upload** to use that profile definition.

**Step 7** (Optional) Choose an AnyConnect group policy from the drop-down list.

**Step 8** Click **OK**.

# Stand-Alone Profile Editor

In addition to the profile editors in ASDM, you can use stand-alone versions of the profile editors for Windows. When predeploying the client, you use the stand-alone profile editors to create profiles for the VPN service and other modules that you deploy to computers using your software management system.

You can modify the stand-alone Cisco AnyConnect Profile Editor installation or uninstall the VPN or other profile editors using Add or Remove Programs.

**Requirements**

- Java—A minimum of JRE 1.6 is a prerequisite for the profile editor, but administrators must deploy it on their own.

  **Note** JRE 1.6 is not uninstalled automatically when uninstalling the stand-alone profile editor. You must uninstall it separately.

- Supported Operating Systems—This application has been tested on Windows 7. The MSI only runs on Windows.

- Supported Browsers—The help files in this application are supported by Firefox and Internet Explorer. They have not been tested in other browsers.

- Required Hard Drive Space—The Cisco AnyConnect Profile Editor application requires less than five megabytes of hard drive space. JRE 1.6 requires less than 100 megabytes of hard drive space.

- You must include the ASA in the VPN profile’s server list in order for the client GUI to display all user controllable settings on the first connection. If you do not add the ASA address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a certificate match and the certificate properly matches the criteria, but you do not add the ASA as a host entry in that profile, the certificate match is ignored.

# Install the Stand-Alone AnyConnect Profile Editor

The stand-alone AnyConnect profile editor is distributed as a Windows executable msi file, separately from the AnyConnect ISO and .pkg files, and has this file naming convention: `anyconnect-profileeditor-win-<version>-k9.msi`.

### Procedure

**Step 1** Download the `anyconnect-profileeditor-win-<version>-k9.msi` from https://software.cisco.com/download/release.html?mdfid=286281283&flowid=72322&softwareid=282364313&release=4.0.00061&relind=AVAILABLE&rellifecycle=&reltype=latest.

**Step 2** Double-click `anyconnect-profileeditor-win-<version>-k9.msi` to launch the installation wizard.

**Step 3** At the Welcome screen, click **Next**.

**Step 4** At the Choose Setup Type window, click one of the following buttons and click **Next**:

- **Typical—**Installs only the Network Access Manager profile editor automatically.
- **Custom—**Allows you to choose any of the profile editors to install.
- **Complete—**Automatically installs all of the profile editors.

**Step 5** If you clicked **Typical** or **Complete** in the previous step, skip to the next step. If you clicked Custom in the previous step, click the icon for the stand-alone profile editor you want to install and select Will be installed on local hard drive or click Entire Feature will be unavailable to prevent the stand-alone profile editor from being installed. Click **Next**.

**Step 6** At the Ready to Install screen, click **Install**.

**Step 7** Click **Finish**.

- The stand-alone AnyConnect profile editor is installed in the `C:\Program Files\Cisco\Cisco AnyConnect` Profile Editor directory.
- You can launch the profile editors by selecting **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** and then clicking the stand-alone profile editor you want from the submenu or by clicking the appropriate profile editor shortcut icon installed on the desktop.

# Edit a Client Profile Using the Stand-Alone Profile Editor

For reasons of security, you cannot manually edit the client profile XML files outside of the stand-alone profile editor. Any profile XML file that is edited outside the stand-alone profile editor will not be accepted by the ASA.

### Procedure

**Step 1** Launch the desired profile editor by double-clicking the shortcut icon on the desktop or by navigating to **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** and selecting the desired profile editor from the submenu.

**Step 2** Select **File** > **Open** and navigate to the client profile XML file that you want to edit.

If you mistakenly try to open a client profile of one kind of feature, such as Web Security, using the profile editor of another feature, such as VPN, you receive a **Schema Validation failed** message and you will not be able to edit the profile.

If you inadvertently try to edit the same client profile in two instances of the same kind of profile editor, the last edits made to the client profile are saved.

**Step 3** Make your changes to the profile and select **File** > **Save** to save your changes.

# The AnyConnect VPN Profile

Cisco AnyConnect Secure Mobility Client features are enabled in the AnyConnect profiles. These profiles contain configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, ISE posture, customer experience feedback, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

You can configure the ASA or ISE to deploy profiles globally for all AnyConnect users or to users based on their group policy. Usually, a user has a single profile file for each AnyConnect module installed. In some cases, you might want to provide more than one VPN profile for a user. Someone who works from multiple locations might need more than one VPN profile.

Some profile settings are stored locally on the user's computer in a user preferences file or a global preferences file. The user file has information the AnyConnect client needs to display user-controllable settings in the Preferences tab of the client GUI and information about the last connection, such as the user, the group, and the host.

The global file has information about user-controllable settings so that you can apply those settings before login (since there is no user). For example, the client needs to know if Start Before Logon and/or AutoConnect On Start are enabled before login.

## AnyConnect Profile Editor, Preferences (Part 1)

- **Use Start Before Logon—**(Windows Only) Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears. After authenticating, the login dialog box appears and the user logs in as usual.
- **Show Pre-connect Message—**Enables an administrator to have a one-time message displayed prior to a users first connection attempt. For example, the message can remind users to insert their smart card into its reader. The message appears in the AnyConnect message catalog and is localized.

- **Certificate Store—**Controls which certificate store(s) AnyConnect uses for storing and reading certificates. The default setting (All) is appropriate for most cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.
  - All—(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.
  - Machine—Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.
  - User—Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.
- **Certificate Store Override—**Allows an administrator to direct AnyConnect to search for certificates in the Windows machine certificate store when the users do not have administrator privileges on their device.

**Note** You must have a pre-deployed profile with this option enabled in order to connect with Windows using a machine certificate. If this profile does not exist on a Windows device prior to connection, the certificate is not accessible in the machine store, and the connection fails.

- **Auto Connect on Start—**AnyConnect, when started, automatically establishes a VPN connection with the secure gateway specified by the AnyConnect profile, or to the last gateway to which the client connected.
- **Minimize On Connect—**After establishing a VPN connection, the AnyConnect GUI minimizes.
- **Local LAN Access—**Allows the user complete access to the local LAN connected to the remote computer during the VPN session to the ASA.

**Note** Enabling local LAN access can potentially create a security weakness from the public network through the user computer into the corporate network. Alternatively, you can configure the security appliance (version 8.4(1) or later) to deploy an SSL client firewall that uses the AnyConnect Client Local Print firewall rule included in the default group policy. In order to enable this firewall rule, you also must enable Automatic VPN Policy, Always on, and Allow VPN Disconnect in this editor, Preferences (Part 2).

-
- **Auto Reconnect—**AnyConnect attempts to reestablish a VPN connection if you lose connectivity. If you disable Auto Reconnect, it does not attempt to reconnect, regardless of the cause of the disconnection.

**Note** Use Auto Reconnect in scenarios where the user has control over the behavior of the client. This feature is not supported with AlwaysOn.

  - **Auto Reconnect Behavior**
    - DisconnectOnSuspend—AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resumes.

    - ReconnectAfterResume (Default)—AnyConnect attempts to reestablish a VPN connection if you lose connectivity.

- **Auto Update—**When checked, enables the automatic update of the client. If you check User Controllable, the user can override this setting in the client.
- **RSA Secure ID Integration** (Windows only)—Controls how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction (automatic setting: both software or hardware tokens accepted).
- **Windows Logon Enforcement—**Allows a VPN session to be established from a Remote Desktop Protocol (RDP) session. Split tunneling must be configured in the group policy. AnyConnect disconnects the VPN connection when the user who established the VPN connection logs off. If the connection is established by a remote user, and that remote user logs off, the VPN connection terminates.
    - Single Local Logon (Default)—Allows only one local user to be logged on during the entire VPN connection. Also, a local user can establish a VPN connection while one or more remote users are logged on to the client PC. This setting has no effect on remote user logons from the enterprise network over the VPN connection.

    **Note** If the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection.

    - Single Logon—Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection terminates. No additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.

    **Note** Multiple simultaneous logons are not supported.

- **Windows VPN Establishment—**Determines the behavior of AnyConnect when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:
    - Local Users Only (Default)—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of AnyConnect.
    - Allow Remote Users—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the client PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.
- **Clear SmartCard PIN**

- **IP Protocol Supported**—For clients with both an IPv4 and IPv6 address attempting to connect to the ASA using AnyConnect, AnyConnect needs to decide which IP protocol to use to initiate the connection. By default AnyConnect initially attempts to connect using IPv4. If that is not successful, AnyConnect attempts to initiate the connection using IPv6.

  This field configures the initial IP protocol and order of fallback.

  - IPv4—Only IPv4 connections can be made to the ASA.
  - IPv6—Only IPv6 connections can be made to the ASA.
  - IPv4, IPv6—First, attempt to make an IPv4 connection to the ASA. If the client cannot connect using IPv4, then try to make an IPv6 connection.
  - IPv6, IPv4—First attempt to make an IPv6 connection to the ASA. If the client cannot connect using IPv6 then try to make an IPv4 connection.

  **Note** The IPv4 to IPv6 and IPv6 to IPv4 protocol failover can also happen during the VPN session. If the primary IP protocol is lost, the VPN session will be re-established via the secondary IP protocol, if possible.

## AnyConnect Profile Editor, Preferences (Part 2)

- **Disable Automatic Certificate Selection** (Windows only)—Disables automatic certificate selection by the client and prompts the user to select the authentication certificate.

  Related Topics: Configure Certificate Selection

- **Proxy Settings**—Specifies a policy in the AnyConnect profile to control client access to a proxy server. Use this when a proxy configuration prevents the user from establishing a tunnel from outside the corporate network.

  - Native—Causes the client to use both proxy settings previously configured by AnyConnect, and the proxy settings configured in the browser. The proxy settings configured in the global user preferences are pre-pended to the browser proxy settings.
  - IgnoreProxy—Ignores the browser proxy settings on the user's computer.
  - Override—Manually configures the address of the Public Proxy Server. Public proxy is the only type of proxy supported for Linux. Windows also supports public proxy. You can configure the public proxy address to be User Controllable.

- **Allow Local Proxy Connections**—By default, AnyConnect lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Uncheck this parameter if you want to disable support for local proxy connections. Some examples of elements that provide a transparent proxy service include acceleration software provided by some wireless data cards, and network component on some antivirus software

- **Enable Optimal Gateway Selection** (OGS), (IPv4 clients only)—AnyConnect identifies and selects which secure gateway is best for connection or reconnection based on the round trip time (RTT), minimizing latency for Internet traffic without user intervention. OGS is not a security feature, and it performs no load balancing between secure gateway clusters or within clusters. You control the activation and deactivation of OGS and specify whether end users may control the feature themselves. Automatic Selection displays in the Connect To drop-down list on the Connection tab of the client GUI.

  - **Suspension Time Threshold** (hours)—Enter the minimum time (in hours) that the VPN must have been suspended before invoking a new gateway-selection calculation. By optimizing this value in combination with the next configurable parameter (Performance Improvement Threshold), you can find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.
  - **Performance Improvement Threshold** (%)—The percentage of performance improvement that triggers the client to re-connect to another secure gateway following a system resume. Adjust these values for your particular network to find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials. The default is 20%.

When OGS is enabled, we recommend that you also make the feature user-controllable.

OGS has the following limitations:

  - It cannot operate with Always On
  - It cannot operate with automatic proxy detection
  - It cannot operate with proxy auto-configuration (PAC) files
  - If AAA is used, users may have to re-enter their credentials when transitioning to a different secure gateway. Using certificates eliminates this problem.

- **Automatic VPN Policy** (Windows and macOS only)—Enables Trusted Network Detection allowing AnyConnect to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection.
  - **Trusted Network Policy**—Action AnyConnect automatically takes on the VPN connection when the user is inside the corporate network (the trusted network).
    - Disconnect (Default)—Disconnects the VPN connection upon the detection of the trusted network.
    - Connect—Initiates a VPN connection upon the detection of the trusted network.
    - Do Nothing—Takes no action in the untrusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
    - Pause—AnyConnect suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
  - **Untrusted Network Policy**—AnyConnect starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.

- ◦ Connect (Default)—Initiates the VPN connection upon the detection of an untrusted network.
- ◦ Do Nothing—Takes no action in the trusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.

◦ **Trusted DNS Domains**—DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *.cisco.com. Wildcards (*) are supported for DNS suffixes.

◦ **Trusted DNS Servers**—DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1. Wildcards (*) are supported for IPv4 DNS server addresses. (They are not supported for IPv6 DNS server addresses.)

◦

**Note** You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. The Network Visibility Module sends flow information only when this feature is enabled so that data is sent over a secure TND connection. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

◦ **Always On**—Determines whether AnyConnect automatically connects to the VPN when the user logs in to a computer running one of the supported Windows or macOS operating systems. You can enforce corporate policies, protecting the computer from security threats by preventing access to Internet resources when it is not in a trusted network. You can set the Always-On VPN parameter in group policies and dynamic access policies to override this setting by specifying exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables Always-On and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions, as long as its criteria match the dynamic access policy or group policy on the establishment of each new session. After enabling, you will be able to configure additional parameters.

**Note** AlwaysOn is used for scenarios where the connection establishment and redundancy run without user intervention; therefore, while using this feature, you need not configure or enable Auto Reconnect in Preferences, part 1.

Related Topics: Require VPN Connections Using Always-On

- ◦ **Allow VPN Disconnect**—Determines whether AnyConnect displays a Disconnect button for Always-On VPN sessions. Users of Always-On VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as performance issues with the current VPN session or reconnection issues following the interruption of a VPN session.

The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

- **Connect Failure Policy—**Determines whether the computer can access the Internet if AnyConnect cannot establish a VPN session (for example, when an ASA is unreachable). This parameter applies only if Always-On and Allow VPN Disconnect are enabled. If you choose Always-On, the fail-open policy permits network connectivity, and the fail-close policy disables network connectivity.
  - Closed—Restricts network access when the VPN is unreachable. The purpose of this setting is to help protect corporate assets from network threats when resources in the private network responsible for protecting the endpoint are unavailable.
  - Open—Permits network access when the VPN is unreachable.

⚠

**Caution** A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. It is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access. It prevents all network access except for local resources such as printers and tethered devices permitted by split tunneling and limited by ACLs. It can halt productivity if users require Internet access beyond the VPN if a secure gateway is unavailable. AnyConnect detects most captive portals. If it cannot detect a captive portal, a connect failure closed policy prevents all network connectivity.

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy Always-On VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

Related Topics: About Captive Portals

If Connect Failure Policy is Closed, then you can configure the following settings:

- **Allow Captive Portal Remediation—**Lets AnyConnect lift the network access restrictions imposed by the closed connect failure policy when the client detects a captive portal (hotspot). Hotels and airports typically use captive portals to require the user to open a browser and satisfy conditions required to permit Internet access. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.
- **Remediation Timeout—**Number of minutes AnyConnect lifts the network access restrictions. This parameter applies if the Allow Captive Portal Remediation parameter is checked and the client detects a captive portal. Specify enough time to meet typical captive portal requirements (for example, 5 minutes).

        - ◦ **Apply Last VPN Local Resource Rules**—If the VPN is unreachable, the client applies the last client firewall it received from the ASA, which may include ACLs allowing access to resources on the local LAN.

    Related Topics: Configure a Connect Failure Policy

- **Allow Manual Host Input**—Enables users to enter different VPN addresses than those listed in the drop-down box of the AnyConnect UI. If you uncheck this checkbox, the VPN connection choices are only those in the drop-down box, and users are restricted from entering a new VPN address.
- **PPP Exclusion**—For a VPN tunnel over a PPP connection, specifies whether and how to determine the exclusion route. The client can exclude traffic destined for the secure gateway from the tunneled traffic intended for destinations beyond the secure gateway. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI. If you make this feature user controllable, users can read and change the PPP exclusion settings.
    - ◦ Automatic—Enables PPP exclusion. AnyConnect automatically uses the IP address of the PPP server. Instruct users to change the value only if automatic detection fails to get the IP address.
    - ◦ Disabled—PPP exclusion is not applied.
    - ◦ Override—Also enables PPP exclusion. Choose if automatic detection fails to get the IP address of the PPP server, and you configured PPP exclusion as user controllable.

  If PPP Exclusion is enabled also set:

    - ◦ **PPP Exclusion Server IP**—The IP address of the security gateway used for PPP exclusion.

  Related Topics: Instruct Users to Override PPP Exclusion

- **Enable Scripting**—Launches OnConnect and OnDisconnect scripts if present on the security appliance flash memory.
    - ◦ **Terminate Script On Next Event**—Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends, and terminates a running OnDisconnect script if the client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.
    - ◦ **Enable Post SBL On Connect Script**—Launches the OnConnect script if present, and SBL establishes the VPN session. (Only supported if VPN endpoint is running Microsoft Windows.)
- **Retain VPN On Logoff**—Determines whether to keep the VPN session when the user logs off a Windows OS.
    - ◦ **User Enforcement**—Specifies whether to end the VPN session if a different user logs on. This parameter applies only if "Retain VPN On Logoff" is checked, and the original user logged off Windows when the VPN session was up.
- **Authentication Timeout Values**—By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Enter a number of seconds in the range of 0 to 120.

# AnyConnect Profile Editor, Backup Servers

You can configure a list of backup servers the client uses in case the user-selected server fails. If the user-selected server fails, the client attempts to connect to the optimal server's backup at the top of the list. If that fails, the client attempts each remaining server in the Optimal Gateway Selection list, ordered by its selection results.

**Note** Any backup servers that you configure here are **only** attempted when no backup servers are defined in AnyConnect Profile Editor, Add/Edit a Server List, on page 57. Those servers configured in the Server List take precedence, and backup servers listed here are overwritten.

**Host Address**—Specifies an IP address or a Fully-Qualified Domain Name (FQDN) to include in the backup server list.

- **Add**—Adds the host address to the backup server list.
- **Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- **Move Down**—Moves the selected backup server down in the list.
- **Delete**—Removes the backup server from the server list.

# AnyConnect Profile Editor, Certificate Matching

Enable the definition of various attributes that can be used to refine automatic client certificate selection on this pane.

If no certificate matching criteria is specified, AnyConnect applies the following certificate matching rules:

- Key Usage: Digital_Signature
- Extended Key Usage: Client Auth

If any criteria matching specifications are made in the profile, neither of these matching rules are applied unless they are specifically listed in the profile.

- **Key Usage**—Use the following Certificate Key attributes for choosing acceptable client certificates:
  - Decipher_Only—Deciphering data, and that no other bit (except Key_Agreement) is set.
  - Encipher_Only—Enciphering data, and any other bit (except Key_Agreement) is not set.
  - CRL_Sign—Verifying the CA signature on a CRL.
  - Key_Cert_Sign—Verifying the CA signature on a certificate.
  - Key_Agreement—Key agreement.
  - Data_Encipherment—Encrypting data other than Key_Encipherment.
  - Key_Encipherment—Encrypting keys.

    - Non_Repudiation—Verifying digital signatures protecting against falsely denying some action, other than Key_Cert_sign or CRL_Sign.
    - Digital_Signature—Verifying digital signatures other than Non_Repudiation, Key_Cert_Sign or CRL_Sign.

- **Extended Key Usage—**Use these Extended Key Usage settings. The OIDs are included in parenthesis:
    - ServerAuth (1.3.6.1.5.5.7.3.1)
    - ClientAuth (1.3.6.1.5.5.7.3.2)
    - CodeSign (1.3.6.1.5.5.7.3.3)
    - EmailProtect (1.3.6.1.5.5.7.3.4)
    - IPSecEndSystem (1.3.6.1.5.5.7.3.5)
    - IPSecTunnel (1.3.6.1.5.5.7.3.6)
    - IPSecUser (1.3.6.1.5.5.7.3.7)
    - TimeStamp (1.3.6.1.5.5.7.3.8)
    - OCSPSign (1.3.6.1.5.5.7.3.9)
    - DVCS (1.3.6.1.5.5.7.3.10)
    - IKE Intermediate

- **Custom Extended Match Key** (Max 10)**—**Specifies custom extended match keys, if any (maximum 10). A certificate must match all of the specified key(s) you enter. Enter the key in the OID format (for example, 1.3.6.1.5.5.7.3.11).

**Note** If a Custom Extended Match Key is created with the OID size greater than 30 characters, it is unaccepted when you click the OK button. The limit for the maximum characters for an OID is 30.

- **Distinguished Name** (Max 10):**—**Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates.
    - **Name—**The distinguished name (DN) to use for matching:
        - CN—Subject Common Name
        - C—Subject Country
        - DC—Domain Component
        - DNQ—Subject Dn Qualifier
        - EA—Subject Email Address
        - GENQ—Subject Gen Qualifier
        - GN—Subject Given Name

  - I—Subject Initials
  - L—Subject City
  - N—Subject Unstruct Name
  - O—Subject Company
  - OU—Subject Department
  - SN—Subject Sur Name
  - SP—Subject State
  - ST—Subject State
  - T—Subject Title
  - ISSUER-CN—Issuer Common Name
  - ISSUER-DC—Issuer Component
  - ISSUER-SN—Issuer Sur Name
  - ISSUER-GN—Issuer Given Name
  - ISSUER-N—Issuer Unstruct Name
  - ISSUER-I—Issuer Initials
  - ISSUER-GENQ—Issuer Gen Qualifier
  - ISSUER-DNQ—Issuer Dn Qualifier
  - ISSUER-C—Issuer Country
  - ISSUER-L—Issuer City
  - ISSUER-SP—Issuer State
  - ISSUER-ST—Issuer State
  - ISSUER-O—Issuer Company
  - ISSUER-OU—Issuer Department
  - ISSUER-T—Issuer Title
  - ISSUER-EA—Issuer Email Address

- **Pattern**—Specifies the string to match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.

  For example, if a sample string was abc.cisco.com and the intent is to match cisco.com, the pattern entered should be cisco.com.

- **Operator**—The operator to use when performing matches for this DN.

  - Equal—equivalent to ==
  - Not Equal—equivalent to !=

  - **Wildcard—**Enabled includes wildcard pattern matching. With wildcard enabled, the pattern can be anywhere in the string.
  - **Match Case—**Check to enable case-sensitive pattern matching.

### Related Topics

Configure Certificate Matching, on page 108

## AnyConnect Profile Editor, Certificate Enrollment

Certificate Enrollment enables AnyConnect to use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate for client authentication.

- **Certificate Expiration Threshold—**The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported by RADIUS password-management). The default is zero (no warning displayed). The range of values is zero to 180 days.
- **Certificate Import Store—**Select which Windows certificate store to save enrollment certificates to.
- **Automatic SCEP Host—**For Legacy SECP, specifies the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name scep_eng.
- **CA URL—**For Legacy SCEP, identifies the SCEP CA server. Enter an FQDN or IP Address of the CA server. For example, http://ca01.cisco.com.
  - **Prompt For Challenge PW—**Enable to let the user make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
  - **Thumbprint—**The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

  **Note** Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in the issued server certificate.

- **Certificate Contents—**Specifies certificate contents to include in the SCEP enrollment request:
  - Name (CN)—Common Name in the certificate.
  - Department (OU)—Department name specified in certificate.
  - Company (O)—Company name specified in certificate.
  - State (ST)—State identifier named in certificate.
  - State (SP)—Another state identifier.
  - Country (C)—Country identifier named in certificate.

    - Email (EA)—Email address. In the following example, Email (EA) is %USER%@cisco.com. %USER% corresponds to the user's ASA username login credential.
    - Domain (DC)—Domain component. In the following example, Domain (DC) is set to cisco.com.
    - SurName (SN)—The family name or last name.
    - GivenName (GN)—Generally, the first name.
    - UnstructName (N)—Undefined name.
    - Initials (I)—The initials of the user.
    - Qualifier (GEN)—The generation qualifier of the user. For example, "Jr." or "III."
    - Qualifier (DN)—A qualifier for the entire DN.
    - City (L)—The city identifier.
    - Title (T)—The person's title. For example, Ms., Mrs., Mr.
    - CA Domain—Used for the SCEP enrollment and is generally the CA domain.
    - Key size—The size of the RSA keys generated for the certificate to be enrolled.

- **Display Get Certificate Button**—Enables the AnyConnect GUI to display the Get Certificate button under the following conditions:
    - The certificate is set to expire within the period defined by the Certificate Expiration Threshold (not supported with RADIUS).
    - The certificate has expired.
    - No certificate is present.
    - The certificate fails to match.

### Related Topics

Configure Certificate Enrollment, on page 97

## AnyConnect Profile Editor, Mobile Policy

AnyConnect version 3.0 and later does not support Windows Mobile devices. See *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*, for information related to Windows Mobile devices.

## AnyConnect Profile Editor, Server List

You can configure a list of servers that appear in the client GUI. Users can select servers in the list to establish a VPN connection.

Server List Table Columns:

- Hostname—The alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- Host Address—IP address or FQDN of the server.

- User Group—Used in conjunction with Host Address to form a group-based URL.
- Automatic SCEP Host—The Simple Certificate Enrollment Protocol specified for provisioning and renewing a certificate used for client authentication.
- CA URL—The URL this server uses to connect to certificate authority (CA).

**Add/Edit**—Launches the Server List Entry dialog where you can specify the above server parameters.

**Delete**—Removes the server from the server list.

**Details**—Displays more details about backup servers or CA URLs for the server.

### Related Topics

Configure VPN Connection Servers, on page 69

## AnyConnect Profile Editor, Add/Edit a Server List

- **Host Display Name**—Enter an alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- **FQDN or IP Address**— Specify an IP address or an FQDN for the server.
  - If you specify an IP address or FQDN in the Host Address Field, then the entry in the Host Name field becomes a label for the server in the connection drop-down list of the AnyConnect Client tray fly-out.
  - If you only specify an FQDN in the Hostname field, and no IP address in the Host Address field, then the FQDN in the Hostname field will be resolved by a DNS server.
  - If you enter an IP address, use the Public IPv4 or the Global IPv6 address of the secure gateway. Use of the link-local secure gateway address is not supported.
- **User Group**—Specify a user group.

  The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.
- **Additional mobile-only settings**—Select to configure Apple iOS and Android mobile devices.
- **Backup Server List**
  We recommend that you configure a list of backup servers the client uses in case the user-selected server fails. If the server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.

  **Note** Conversely, the backup servers configured in AnyConnect Profile Editor, Backup Servers, on page 52 are global entries for all connection entries. Any entries put in the Backup Servers location are overwritten with what is entered here for an individual server list entry. This setting takes precedence and is the recommended practice.

  - **Host Address**—Specifies an IP address or an FQDN to include in the backup server list. If the client cannot connect to the host, it attempts to connect to the backup server.

    - **Add—**Adds the host address to the backup server list.
    - **Move Up—**Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
    - **Move Down—**Moves the selected backup server down in the list.
    - **Delete—**Removes the backup server from the server list.

- **Load Balancing Server List**
  If the host for this server list entry is a load balancing cluster of security appliances, and the Always-On feature is enabled, specify the backup devices of the cluster in this list. If you do not, Always-On blocks access to backup devices in the load balancing cluster.
    - **Host Address—**Specifies an IP address or an FQDN of a backup device in a load-balancing cluster.
    - **Add—**Adds the address to the load balancing backup server list.
    - **Delete—**Removes the load balancing backup server from the list.

- **Primary Protocol—**Specifies the protocol for connecting to this server, either SSL or IPsec with IKEv2. The default is SSL.
    - **Standard Authentication Only (IOS Gateways)—**When you select IPsec as the protocol, you are able to select this option to limit the authentication methods for connections to IOS servers.

      **Note** If this server is an ASA, then changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

    - **Auth Method During IKE Negotiation** Select one of the standard-based authentication methods.
        - **IKE Identity—**If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*.

- **Automatic SCEP Host—**This host is used for legacy SCEP.
- **CA URL—**Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, http://ca01.cisco.com.
- **Prompt For Challenge PW—**Enable to let the user make certificate requests manually. When the user clicks Get Certificate, the client prompts the user for a username and one-time password.
- **CA Thumbprint—**The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

**Note** Your CA server administrator can provide the CA URL and thumbprint. The thumprint should be retrieved directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

### Related Topics

Configure VPN Connection Servers, on page 69

## AnyConnect Profile Editor, Mobile Settings

Related Topics: Configure Mobile Device Connections in the AnyConnect VPN Profile, on page 21

### 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.

  Related Topics: Apple iOS Specific Considerations, on page 12

- **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.

# The AnyConnect Local Policy

AnyConnectLocalPolicy.xml is an XML file on the client containing security settings. This file is not deployed by the ASA. You must install it manually or deploy it to a user computer using an enterprise software deployment system. If you make changes to an existing local policy file on a user's system, that system should be rebooted.

## Local Policy Parameters and Values

The following parameters are elements in the VPN Local Policy Editor and in the `AnyConnectLocalPolicy.xml` file. XML elements are shown in angle brackets.

**Note** If you manually edit the file and omit a policy parameter, that feature resorts to default behavior.

- <acversion>

  Specifies the minimum version of the AnyConnect client capable of interpreting all of the parameters in this file. If a client running a version of AnyConnect that is older than this version reads the file, it issues an event log warning.

  The format is acversion="<version number>".

- **FIPS Mode** <FipsMode>

  Enables FIPS mode for the client. This setting forces the client to only use algorithms and protocols approved by the FIPS standard.

- **Bypass Downloader** <BypassDownloader>

  When selected, disables the launch of the VPNDownloader.exe module, which is responsible for detecting the presence of and updating the local versions of dynamic content. The client does not check for dynamic content present on the ASA, including translations, customizations, optional modules, and core software updates.

  When Bypass Downloader is selected, one of two things happens upon client connection to an ASA:

  - If the VPN client profile on the ASA is different than the one on the client, the client aborts the connection attempt.

  - If there is no VPN client profile on the ASA, the client makes the VPN connection, but it uses its hard-coded VPN client profile settings.

  **Note** If you configure VPN client profiles on the ASA, they must be installed on the client before the client connects to an ASA with BypassDownloader set to true. Because the profile can contain an administrator defined policy, the BypassDownloader true setting is only recommended if you do not rely on the ASA to centrally manage client profiles.

- **Restrict Web Launch** <RestrictWebLaunch>

Prevents users from using a non-FIPS-compliant browser to initiate WebLaunch. It does this by preventing the client from obtaining the security cookie that is used to initiate an AnyConnect tunnel. The client displays an informative message to the user.

- **Strict Certificate Trust** <StrictCertificateTrust>

  If selected, when authenticating remote security gateways, AnyConnect disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect to security gateways using self-signed certificates and displays`Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.`. If not selected, the client prompts the user to accept the certificate. This is the default behavior.

  We strongly recommend that you enable Strict Certificate Trust for the AnyConnect client for the following reasons:

  - With the increase in targeted exploits, enabling Strict Certificate Trust in the local policy helps prevent "man in the middle" attacks when users are connecting from untrusted networks such as public-access networks.
  - Even if you use fully verifiable and trusted certificates, the AnyConnect client, by default, allows end users to accept unverifiable certificates. If your end users are subjected to a man-in-the-middle attack, they may be prompted to accept a malicious certificate. To remove this decision from your end users, enable Strict Certificate Trust.

- **Restrict Preference Caching** <RestrictPreferenceCaching>

  By design, AnyConnect does not cache sensitive information to disk. Enabling this parameter extends this policy to any type of user information stored in the AnyConnect preferences.

  - Credentials—The user name and second user name are not cached.
  - Thumbprints—The client and server certificate thumbprints are not cached.
  - CredentialsAndThumbprints—Certificate thumbprints and user names are not cached.
  - All—No automatic preferences are cached.
  - false—All preferences are written to disk (default).

- **Exclude Pem File Cert Store** (Linux and macOS) <ExcludePemFileCertStore>

  Prevents the client from using the PEM file certificate store to verify server certificates and search for client certificates.

  The store uses FIPS-capable OpenSSL and has information about where to obtain certificates for client certificate authentication. Permitting the PEM file certificate store ensures remote users are using a FIPS-compliant certificate store.

- **Exclude Mac Native Cert Store** (macOS only) <ExcludeMacNativeCertStore>

  Prevents the client from using the Mac native (keychain) certificate store to verify server certificates and search for client certificates.

- **Exclude Firefox NSS Cert Store** (Linux and macOS) <ExcludeFirefoxNSSCertStore>

  Prevents the client from using the Firefox NSS certificate store to verify server certificates and search for client certificates.

  The store has information about where to obtain certificates for client certificate authentication.

- **Update Policy** <UpdatePolicy>

  Controls which headends the client can get software or profile updates from.

  - **Allow Software Updates From AnyServer** <AllowSoftwareUpdatesFromAnyServer>

    Allow or disallow software updates of the VPN core module and other optional modules from unauthorized servers (ones not listed in the Server Name list).

  - **Allow VPN Profile Updates From AnyServer** <AllowVPNProfileUpdatesFromAnyServer>

    Allow or disallow VPN Profile updates from unauthorized servers (ones not listed in the Server Name list).

  - **Allow Service Profile Updates From AnyServer** <AllowServiceProfileUpdatesFromAnyServer>

    Allow or disallow other service module profile updates from unauthorized servers (ones not listed in the Server Name list).

  - **Allow ISE Posture Profile Updates From Any Server**<AllowISEProfileUpdatesFromAnyServer>

    Allow or disallow ISE Posture Profile updates from unauthorized servers (ones not listed in the Server Name list).

  - **Allow Compliance Module Updates From Any Server**<AllowComplianceModuleUpdatesFromAnyServer>

    Allow or disallow Compliance Module updates from unauthorized servers (ones not listed in the Server Name list).

  - **Server Name** <ServerName>

    Specify authorized servers in this list. These headends are allowed full updates of all AnyConnect software and profiles upon VPN connectivity. ServerName can be an FQDN, IP address, domain name, or wildcard with domain name.

# Change Local Policy Parameters Manually

### Procedure

**Step 1** Retrieve a copy of the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml) from a client installation.

*Table 4: Operating System and AnyConnect Local Policy File Installation Path*

| Operating System | Installation Path |
|---|---|
| Windows | C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client |
| Linux | /opt/cisco/anyconnect |
| macOS | /opt/cisco/anyconnect |

**Step 2** Edit the parameter settings. You can either edit the AnyConnectLocalPolicy file manually, or use the VPN Local Policy editor, which is distributed with the AnyConnect Profile Editor installer.

**Step 3** Save the file as `AnyConnectLocalPolicy.xml` and deploy the file to remote computers using a corporate software deployment system.

**Step 4** Reboot the remote computers so that the changes to the local policy file take effect.

# Enable Local Policy Parameters in an MST File

See Local Policy Parameters and Values for the descriptions and values that you can set.

Create an MST file to change local policy parameters. The MST parameter names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml):

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

**Note** AnyConnect installation does not automatically overwrite an existing local policy file on the user computer. You must delete the existing policy file on user computers first, so the client installer can create a new policy file.

**Note** Any changes to the local policy file require the system to be rebooted.

# Enable Local Policy Parameters with the Enable FIPS Tool

For all operating systems, you can use Cisco's Enable FIPS tool to create an AnyConnect Local Policy file with FIPS enabled. The Enable FIPS tools is a command line tool that runs on Windows using administrator privileges or as a root user for Linux and macOS.

For information about where you can download the Enable FIPS tool, see the licensing information you received for the FIPS client.

You run the Enable FIPS tool by entering the command EnableFIPS <arguments> from the command line of the computer. The following usage notes apply to the Enable FIPS tool:

- If you do not supply any arguments, the tool enables FIPS and restarts the vpnagent service (Windows) or the vpnagent daemon (macOS and Linux).
- Separate multiple arguments with spaces.

The following example shows the Enable FIPS tool command, run on a Windows computer:

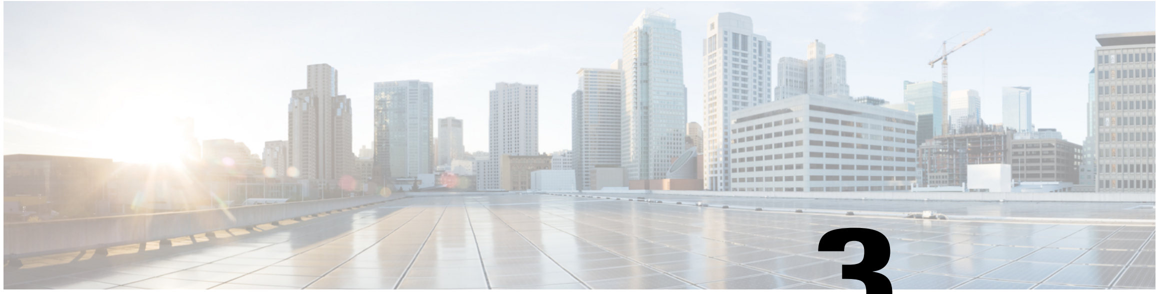
```
EnableFIPS rwl=false sct=true bd=true fm=false
```

The next example shows the command, run on a Linux or macOS computer:

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

The next table shows the policy settings you can configure with the Enable FIPS tool. The arguments match the parameters in the AnyConnect local policy file.

| Policy Setting | Argument and Syntax |
|---|---|
| FIPS mode | fm=[true \| false] |
| Bypass downloader | bd=[true \| false] |
| Restrict weblaunch | rwl=[true \| false] |
| Strict certificate trust | sct=[true \| false] |
| Restrict preferences caching | rpc=[Credentials \| Thumbprints \| CredentialsAndThumbprints \| All \| false] |
| Exclude FireFox NSS certificate store (Linux and macOS) | efn=[true \| false] |
| Exclude PEM file certificate store (Linux and macOS) | epf=[true \| false] |
| Exclude Mac native certificate store (macOS only) | emn=[true \| false] |



CHAPTER 3

# Configure VPN Access

# Connect and Disconnect to a VPN

## AnyConnect VPN Connectivity Options

The AnyConnect client provides many options for automatically connecting, reconnecting, or disconnecting VPN sessions. These options provide a convenient way for your users to connect to your VPN, and they also support your network security requirements.

### Starting and Restarting AnyConnect Connections

Configure VPN Connection Servers to provide the names and addresses of the secure gateways your users will manually connect to.

Choose from the following AnyConnect capabilities to provide convenient, automatic VPN connectivity:

- Automatically Start Windows VPN Connections Before Logon
- Automatically Start VPN Connections When AnyConnect Starts
- Automatically Restart VPN Connections

Also, consider using the following Automatic VPN Policy options to enforce greater network security or restrict network access to the VPN only:

- About Trusted Network Detection
- Require VPN Connections Using Always-On
- Use Captive Portal Hotspot Detection and Remediation

### Renegotiating and Maintaining the AnyConnect Connection

You can limit how long the ASA keeps an AnyConnect VPN connection available to the user even with no activity. If a VPN session goes idle, you can terminate the connection or re-negotiate the connection.

- Keepalive—The ASA sends keepalive messages at regular intervals. These messages are ignored by the ASA, but are useful in maintaining connections with devices between the client and the ASA.

  For instructions to configure Keepalive with the ASDM or CLI, see the *Enable Keepalive* section in the Cisco ASA Series VPN Configuration Guide.

- Dead Peer Detection—The ASA and AnyConnect client send "R-U-There" messages. These messages are sent less frequently than IPsec's keepalive messages. You can enable both the ASA (gateway) and the AnyConnect client to send DPD messages, and configure a timeout interval.

  - If the client does not respond to the ASA's DPD messages, the ASA tries once more before putting the session into "Waiting to Resume" mode. This mode allows the user to roam networks, or enter sleep mode and later recover the connection. If the user does not reconnect before the idle timeout occurs, the ASA will terminate the tunnel. The recommended gateway DPD interval is 300 seconds.

  - If the ASA does not respond to the client's DPD messages, the client tries again before terminating the tunnel. The recommended client DPD interval is 30 seconds.

    For instructions to configure DPD within the ASDM, refer to *Configure Dead Peer Detection* in the appropriate release of the Cisco ASA Series VPN Configuration Guide.

- Best Practices:

  - Set Client DPD to 30 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).

  - Set Server DPD to 300 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).

  - Set Rekey, for both SSL and IPsec to 1 hour (Group Policy > Advanced > AnyConnect Client > Key Regeneration).

### Terminating an AnyConnect Connection

Terminating an AnyConnect connection requires the user to re-authenticate their endpoint to the secure gateway and create a new VPN connection.

The following connection parameters terminate the VPN session based on timeouts:

- Maximum Connect Time—Sets the maximum user connection time in minutes. At the end of this time, the system terminates the connection. You can also allow unlimited connection time(default).

- VPN Idle Timeout—Terminates any user's session when the session is inactive for the specified time. If the VPN idle timeout is not configured, then the default idle timeout is used.

- Default Idle Timeout—Terminates any user's session when the session is inactive for the specified time. The default value is 30 minutes. The default is 1800 second.

See the *Specify a VPN Session Idle Timeout for a Group Policy* section in the appropriate release of the Cisco ASA Series VPN Configuration Guide to set these parameters.

# Configure VPN Connection Servers

The AnyConnect VPN server list consists of host name and host address pairs identifying the secure gateways that your VPN users will connect to. The host name can be an alias, an FQDN, or an IP address.

The hosts added to the server list display in the Connect to drop-down list in the AnyConnect GUI. The user can then select from the drop-down list to initiate a VPN connection. The host at the top of the list is the default server, and appears first in the GUI drop-down list. If the user selects an alternate server from the list, the selected server becomes the new default server.

Once you add a server to the server list, you can view its details and edit or delete the server entry. To add a server to the server list, follow this procedure.

### Procedure

**Step 1** Open the VPN Profile Editor and choose **Server List** from the navigation pane.

**Step 2** Click **Add**.

**Step 3** Configure the server's host name and address:

a) Enter a **Host Display Name**, an alias used to refer to the host, an FQDN, or an IP address. Do not use "&" or "<" characters in the name. If you enter an FQDN or an IP address, you do not need to enter the **FQDN** or **IP Address** in the next step.
If you enter an IP address, use the Public IPv4 or the Global IPv6 address of the secure gateway. Use of the link-local secure gateway address is not supported.

b) (Optional) Enter the host's **FQDN** or **IP Address** if not entered in the Host Display Name.

c) (Optional) Specify a **User Group**.
AnyConnect uses the FQDN or IP Address in conjunction with User Group to form the Group URL.

**Step 4** Enter the server to fall back to as the backup server in the **Backup Server List**. Do not use "&" or "<" characters in the name.

**Note** Conversely, the Backup Server tab on the Server menu is a global entry for all connection entries. Any entries put in that Backup Server location are overwritten with what is entered here for an individual server list entry. This setting takes precedence and is the recommended practice.

**Step 5** (Optional) Add load balancing servers to the **Load Balancing Server List.** Do not use "&" or "<" characters in the name.
If the host for this server list entry specifies a load balancing cluster of security appliances, and the Always-On feature is enabled, add the load balancing devices in the cluster to this list. If you do not, Always-On blocks access to the devices in the load balancing cluster.

**Step 6** Specify the **Primary Protocol** for the client to use for this ASA:

a) Choose SSL (default) or IPsec.
If you specify IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.

b) If you specify IPsec, select **Standard Authentication Only** to disable the default authentication method (proprietary AnyConnect EAP), and choose a method from the drop-down list.

**Note** Changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

**Step 7** (Optional) Configure SCEP for this server:

a) Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, http://ca01.cisco.com.

b) Check **Prompt For Challenge PW** to enable the user to make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.

c) Enter the certificate thumbprint of the CA. Use SHA1 or MD5 hashes. Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

**Step 8** Click **OK**.

### Related Topics

AnyConnect Profile Editor, Server List, on page 56

AnyConnect Profile Editor, Add/Edit a Server List, on page 57

# Automatically Start Windows VPN Connections Before Logon

## About Start Before Logon

This feature called Start Before Logon (SBL) allows users to establish their VPN connection to the enterprise infrastructure before logging onto Windows.

When SBL is installed and enabled, AnyConnect starts before the Windows logon dialog box appears, ensuring users are connected to their corporate infrastructure before logging on. After VPN authentication, the Windows logon dialog appears, and the user logs in as usual.

SBL also includes the Network Access Manager tile and allows connections using user configured home network profiles. Network profiles allowed in SBL mode include all media types employing non-802-1X authentication modes.

SBL is available on Windows systems only, and is implemented using different mechanisms depending on the version of Windows:

- On Windows, the Pre-Login Access Provider (PLAP) is used to implement AnyConnect SBL.

  With PLAP, the Ctrl+Alt+Del key combination opens a window where the user can choose either to log in to the system or activate Network Connections (PLAP components) using the Network Connect button in the lower-right corner of the window.

  PLAP supports 32-bit and 64-bit versions of the Windows.

Reasons you might consider enabling SBL for your users include:

- The user’s computer is joined to an Active Directory infrastructure.
- A user has network-mapped drives that require authentication with the Microsoft Active Directory infrastructure.
- The user cannot have cached credentials on the computer (the group policy disallows cached credentials). In this scenario, users must be able to communicate with a domain controller on the corporate network for their credentials to be validated before gaining access to the computer.
- The user must run logon scripts that execute from a network resource or need access to a network resource. With SBL enabled, the user has access to the local infrastructure and logon scripts that would

normally run when a user is in the office. This includes domain logon scripts, group policy objects and other Active Directory functionality that normally occurs when users log on to their system.

- Networking components (such as MS NAP/CS NAC) exist that might require connection to the infrastructure.

## Limitations on Start Before Logon

- AnyConnect is not compatible with fast user switching.
- AnyConnect cannot be started by third-party Start Before Logon applications.

## Configure Start Before Logon

**Procedure**

**Step 1** Install the AnyConnect Start Before Logon Module.

**Step 2** Enable SBL in the AnyConnect Profile.

### Install the AnyConnect Start Before Logon Module

The AnyConnect installer detects the underlying operating system and places the appropriate AnyConnect DLL from the AnyConnect SBL module in the system directory. On Windows 7, or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component, vpnplap.dll or vpnplap64.dll.

**Note** If you uninstall AnyConnect while leaving the VPNGINA or PLAP component installed, the VPNGINA or PLAP component is disabled and not visible to the remote user.

You can pre-deploy the SBL module or configure the ASA to download it. When pre-deploying AnyConnect, the Start Before Logon module requires that the core client software is installed first. If you are pre-deploying AnyConnect Core and the Start Before Logon components using MSI files, you must get the order right.

**Procedure**

**Step 1** In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

**Step 2** Select a group policy and click **Edit** or **Add** a new group policy.

**Step 3** Select **Advanced** > **AnyConnect Client** in the left navigation pane.

**Step 4** Uncheck **Inherit** for the Optional Client Module for Download setting.

**Step 5** Select the **AnyConnect SBL** module in the drop-down list.

## Enable SBL in the AnyConnect Profile

### Before You Begin

- SBL requires a network connection to be present at the time it is invoked. In some cases, this might not be possible, because a wireless connection might depend on credentials of the user to connect to the wireless infrastructure. Since SBL mode precedes the credential phase of a logon, a connection would not be available in this scenario. In this case, the wireless connection needs to be configured to cache the credentials across logon, or another wireless authentication needs to be configured, for SBL to work.
- If the Network Access Manager is installed, you must deploy machine connection to ensure that an appropriate connection is available.

### Procedure

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

**Step 2** Select **Use Start Before Logon**.

**Step 3** (Optional) To give the remote user control over SBL, select **User Controllable**.

**Note** The user must reboot the remote computer before SBL takes effect.

## Troubleshoot Start Before Logon

### Procedure

**Step 1** Ensure that the AnyConnect profile is loaded on the ASA, ready to be deployed.

**Step 2** Delete prior profiles (search for them on the hard drive to find the location, *.xml).

**Step 3** Using Windows Add/Remove Programs, uninstall the SBL Components. Reboot the computer and retest.

**Step 4** Clear the user's AnyConnect log in the Event Viewer and retest.

**Step 5** Browse back to the security appliance to install AnyConnect again.

**Step 6** Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt.

**Step 7** Collect a DART bundle and send it to your AnyConnect Administrator.

**Step 8** If you see the following error, delete the user's AnyConnect profile:

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application
Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not
available.
```

**Step 9** Go back to the .tmpl file, save a copy as an.xml file, and use that XML file as the default profile.

# Automatically Start VPN Connections When AnyConnect Starts

This feature called Auto Connect On Start, automatically establishes a VPN connection with the secure gateway specified by the VPN client profile when AnyConnect starts.

Auto Connect On Start is disabled by default, requiring the user to specify or select a secure gateway.

### Procedure

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

**Step 2** Select **Auto Connect On Start**.

**Step 3** (Optional) To give the user control over Auto Connect on Start, select **User Controllable**.

# Configure Start Before Logon (PLAP) on Windows Systems

The Start Before Logon (SBL) feature starts a VPN connection before the user logs in to Windows. This ensures that users connect to their corporate infrastructure before logging on to their computers.

The SBL AnyConnect feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets programmatic network administrators perform specific tasks, such as collecting credentials or connecting to network resources before logon. PLAP provides SBL functions on all of the supported Windows operating systems. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP functions supports x86 and x64.

## Install PLAP

The vpnplap.dll and vpnplap64.dll components are part of the existing installation, so you can load a single, add-on SBL package on the security appliance, which then installs the appropriate component for the target platform. PLAP is an optional feature. The installer software detects the underlying operating system and places the appropriate DLL in the system directory. On Windows 7 or later, or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component.

**Note** If you uninstall AnyConnect while leaving the PLAP component installed, the PLAP component is disabled and is not visible to the remote user.

Once installed, PLAP is not active until you modify the user profile <profile.xml> file to activate SBL. See Enable SBL in the AnyConnect Profile, on page 72. After activation, the user invokes the Network Connect component by clicking Switch User, then the Network Connect icon in the lower, right part of the screen.

**Note** If the user mistakenly minimizes the user interface, the user can restore it by pressing the **Alt + Tab** key combination.

## Log on to a Windows PC Using PLAP

### Procedure

**Step 1** At the Windows start window, users press the **Ctrl+Alt+Del** key combination.
The logon window appears with a Switch User button.

**Step 2** The user clicks **Switch User**. The Network Connect window displays. If the user is already connected through an AnyConnect connection and clicks **Switch User**, that VPN connection remains. If the user clicks **Network Connect**, the original VPN connection terminates. If the user clicks **Cancel**, the VPN connection terminates.

**Step 3** The user clicks the **Network Connect** button in the lower-right corner of the window to launch AnyConnect.
The AnyConnect logon window opens.

**Step 4** The user uses this GUI to log in as usual.
This example assumes AnyConnect is the only installed connection provider. If there are multiple providers installed, the user must select the one to use from the items displayed on this window.

**Step 5** When the user connects, the user sees a screen similar to the Network Connect window, except that it has the Microsoft Disconnect button in the lower-right corner. This button is the only indication that the connection was successful.

**Step 6** The user clicks the icon associated with their logon.
Once the connection is established, you have a few minutes to log on. The user logon session times out after approximately a two minute idle timeout and a disconnect is issued to the AnyConnect PLAP component, causing the VPN tunnel to disconnect.

## Disconnect from AnyConnect Using PLAP

After successfully establishing a VPN session, the PLAP component returns to the original window, this time with a Disconnect button displayed in the lower-right corner of the window.

When the user clicks **Disconnect**, the VPN tunnel disconnects.

In addition to explicitly disconnecting in response to the **Disconnect** button, the tunnel also disconnects in the following situations:

- When a user logs on to a PC using PLAP but then presses **Cancel**.
- When the PC is shut down before the user logs on to the system.
- When Windows times out the user logon session and returns to the "Press CTRL + ALT + DEL to log on" screen.

This behavior is a function of the Windows PLAP architecture, not AnyConnect.

# Automatically Restart VPN Connections

When Auto Reconnect is enabled (default), AnyConnect recovers from VPN session disruptions and reestablishes a session, regardless of the media used for the initial connection. For example, it can reestablish a session on wired, wireless, or 3G. When Auto Reconnect is enabled, you also specify the reconnect behavior upon system suspend or system resume. A system suspend is a low-power standby, such as Windows “hibernation” or macOS or Linux “sleep.” A system resume is a recovery following a system suspend.

If you disable Auto Reconnect, the client does not attempt to reconnect regardless of the cause of the disconnection. Cisco highly recommends using the default setting (enabled) for this feature. Disabling this setting can cause interruptions in VPN connectivity over unstable connections.

#### Procedure

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

**Step 2** Select **Auto Reconnect**.

**Step 3** Choose the Auto Reconnect Behavior:

- Disconnect On Suspend—(Default) AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
- Reconnect After Resume—The client retains resources assigned to the VPN session during a system suspend and attempts to reconnect after the system resume.

# Use Trusted Network Detection to Connect and Disconnect

## About Trusted Network Detection

Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network).

TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.

You configure TND in the AnyConnect VPN Client profile. No changes are required to the ASA configuration. You need to specify the action or policy AnyConnect takes when recognizing it is transitioning between trusted and untrusted networks, and identify your trusted networks and servers.

## Guidelines for Trusted Network Detection

- Because the TND feature controls the AnyConnect GUI and automatically starts connections, the GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.
- If AnyConnect is also running Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes.
- Trusted Network Detection with or without Always-On configured is supported on IPv6 and IPv4 VPN connections to the ASA over IPv4 and IPv6 networks.

- Multiple profiles on a user computer may present problems if the TND configuration is different.

  If the user has received a TND-enabled profile in the past, upon system restart, AnyConnect attempts to connect to the security appliance it was last connected to, which may not be the behavior you desire. To connect to a different security appliance, they must manually disconnect and re-connect to that headend. The following workarounds will help you prevent this problem:

  - Enable TND in the client profiles loaded on all the ASAs on your corporate network.
  - Create one profile listing all the ASAs in the host entry section, and load that profile on all your ASAs.
  - If users do not need to have multiple, different profiles, use the same profile name for the profiles on all the ASAs. Each ASA overrides the existing profile.

## Configure Trusted Network Detection

### Procedure

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

**Step 2** Select **Automatic VPN Policy**.

**Step 3** Choose a **Trusted Network Policy.**
This is the action the client takes when the user is inside the corporate network (the trusted network). The options are:

- Disconnect—(Default) The client terminates the VPN connection in the trusted network.
- Connect—The client starts a VPN connection in the trusted network.
- Do Nothing—The client takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection (TND).
- Pause—AnyConnect suspends the VPN session (instead of disconnecting it) if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

**Step 4** Choose an **Untrusted Network Policy**.
This is the action the client takes when the user is outside the corporate network. The options are:

- Connect—The client starts a VPN connection upon the detection of an untrusted network.
- Do Nothing—The client takes no action upon detection of an untrusted network. This option disablesAlways-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to **Do Nothing** disables Trusted Network Detection.

**Step 5** Specify **Trusted DNS Domains**.
Specify the DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. You can assign multiple DNS suffixes if you add them to the split-dns list and specify a default domain on the ASA.

The AnyConnect client builds the DNS suffix list in the following order:

- The domain passed by the head end.
- The split-DNS suffix list passed by the head end.
- The public interface's DNS suffixes, if configured. If not, the primary and connection-specific suffixes, along with the parent suffixes of the primary DNS suffix (if the corresponding box is checked in the Advanced TCP/IP Settings).

| To Match This DNS Suffix: | Use This Value for TrustedDNSDomains: |
|---|---|
| example.com (only) | *example.com |
| example.com AND anyconnect.cisco.com | *.example.com OR example.com, anyconnect.example.com |
| asa.example.com AND example.cisco.com | *.example.com OR asa.example.com, anyconnect.example.com |

Wildcards (*) are supported for IPv4 DNS suffixes. (They are not supported for IPv6 DNS suffixes.

**Step 6** Specify **Trusted DNS Servers**.
All DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 203.0.113.1,2001:DB8::1. Wildcards (*) are supported for IPv4 DNS server addresses. (They are not supported for IPv6 DNS server addresses.)

You must have a DNS entry for the headend server that is resolvable via DNS. If your connections are by IP address, you need a DNS server that can resolve mus.cisco.com. If mus.cisco.com is not resolvable via DNS, captive portal detection will not work as expected.

**Note** You can configure either TrustedDNSDomains, TrustedDNSServers, or both. If you configure TrustedDNSServers, be sure to enter all your DNS servers, so your site(s) will all be part of the Trusted Network.

An active interface will be considered as an In-Trusted-Network if it matches *all* the rules in the VPN profile.

**Step 7** Specify a host URL that you want to add as trusted. You must have a secure web server that is accessible with a trusted certificate to be considered trusted. After you click **Add**, the URL is added and the certificate hash is pre-filled. If the hash is not found, an error message prompts the user to enter the certificate hash manually and click **Set**.

**Note** You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

# Require VPN Connections Using Always-On

## About Always-On VPN

Always-On operation prevents access to Internet resources when the computer is not on a trusted network, unless a VPN session is active. Enforcing the VPN to always be on in this situation protects the computer from security threats.

When Always-On is enabled, it establishes a VPN session automatically after the user logs in and upon detection of an untrusted network. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer (specified in the ASA group policy) expires. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

When Always-On is enabled in the VPN Profile, AnyConnect protects the endpoint by deleting all the other downloaded AnyConnect profiles and ignores any public proxies configured to connect to the ASA.

The following AnyConnect options also need to be considered when enabling Always-On:

- Allowing the user to Disconnect the Always-On VPN session: AnyConnect provides the ability for the user to disconnect Always-On VPN sessions. If you enable **Allow VPN Disconnect**, AnyConnect displays a Disconnect button upon the establishment of a VPN session. By default, the profile editor enables the Disconnect button when you enableAlways-On VPN.

  Pressing the Disconnect button locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. Users of Always-On VPN sessions may want to click Disconnect so they can choose an alternative secure gateway due to performance issues with the current VPN session, or reconnection issues following the interruption of a VPN session.

- Setting a Connect Failure Policy: The connect failure policy determines whether the computer can access the internet if Always-On VPN is enabled and AnyConnect cannot establish a VPN session. See Set a Connect Failure Policy for Always-On.

- Handling Captive Portal Hotspots: See Use Captive Portal Hotspot Detection and Remediation.

## Limitations of Always-On VPN

- If Always-On is enabled, but the user does not log on, AnyConnect does not establish the VPN connection. AnyConnect starts the VPN connection only post-login.

- Always-On VPN does not support connecting though a proxy.

## Guidelines for Always-On VPN

To enhance protection against threats, we recommend the following additional protective measures if you configure Always-On VPN:

- We strongly recommend purchasing a digital certificate from a certificate authority (CA) and enrolling it on the secure gateways. The ASDM provides an **Enroll ASA SSL VPN with Entrust** button on the **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** panel to facilitate enrollment of a public certificate.

- Pre-deploy a profile configured with Always-On to the endpoints to limit connectivity to the pre-defined ASAs. Predeployment prevents contact with a rogue server.
- Restrict administrator rights so that users cannot terminate processes. A PC user with admin rights can bypass an Always-On policy by stopping the agent. If you want to ensure fully-secure Always-On, you must deny local admin rights to users.
- Restrict access to the Cisco sub-folders on Windows computers, typically `C:\ProgramData`.
- Users with limited or standard privileges may sometimes have write access to their program data folders. They could use this access to delete the AnyConnect profile file and thereby circumvent the Always-On feature.
- Pre-deploy a group policy object (GPO) for Windows users to prevent users with limited rights from terminating the GUI. Predeploy equivalent measures for macOS users.

## Configure Always-On VPN

### Procedure

**Step 1** Configure Always-On in the AnyConnect VPN Client Profile.

**Step 2** (Optional) Add Load-Balancing Backup Cluster Members to the Server List.

**Step 3** (Optional) Exempt Users from Always-On VPN.

### Configure Always-On in the AnyConnect VPN Client Profile

#### Before You Begin

Always-On VPN requires that a valid, trusted server certificate be configured on the ASA; otherwise, it fails and logs an event indicating the certificate is invalid. In addition, ensuring that the server certificate can pass Strict Certificate Trust mode prevents the download of an Always-On VPN profile that locks a VPN connection to a rogue server.

#### Procedure

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

**Step 2** Select **Automatic VPN Policy**.

**Step 3** Configure Trusted Network Detection.

**Step 4** Select **Always On**.

**Step 5** (Optional) Select or un-select **Allow VPN Disconnect**.

**Step 6** (Optional) Configure a Connect Failure Policy.

**Step 7** (Optional) Configure Captive Portal Remediation.

### Add Load-Balancing Backup Cluster Members to the Server List

Always-On VPN affects the load balancing of AnyConnect VPN sessions. With Always-On VPN disabled, when the client connects to a master device within a load balancing cluster, the client complies with a redirection from the master device to any of the backup cluster members. With Always-On enabled, the client does not comply with a redirection from the master device unless the address of the backup cluster member is specified in the server list of the client profile. Therefore, be sure to add any backup cluster members to the server list.

To specify the addresses of backup cluster members in the client profile, use ASDM to add a load-balancing backup server list by following these steps:

#### Procedure

**Step 1** Open the VPN Profile Editor and choose **Server List** from the navigation pane.

**Step 2** Choose a server that is a master device of a load-balancing cluster and click **Edit**.

**Step 3** Enter an FQDN or IP address of any load-balancing cluster member.

### Exempt Users from Always-On VPN

You can configure exemptions to override an Always-On policy. For example, you might want to let certain individuals establish VPN sessions with other companies or exempt the Always-On policy for noncorporate assets.

Exemptions set in group policies and dynamic access policies on the ASA override the Always-On policy. You specify exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables Always-On and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

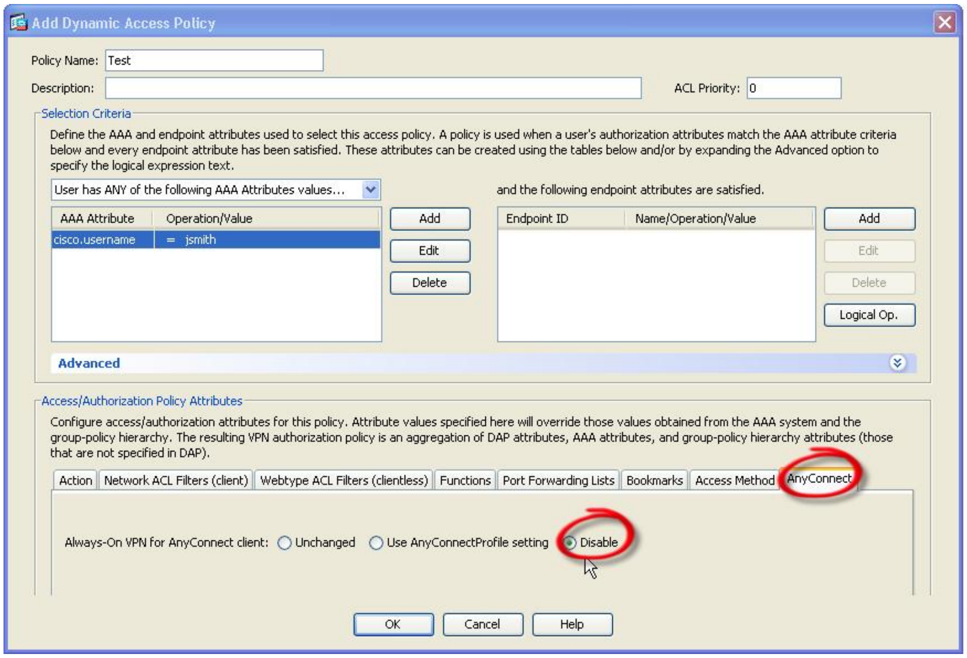
This procedure configures a dynamic access policy that uses AAA endpoint criteria to match sessions to noncorporate assets.

#### Procedure

**Step 1** Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** or **Edit**.

**Step 2** Configure criteria to exempt users from Always-On VPN. For example, use the Selection Criteria area to specify AAA attributes to match user logon IDs.

**Step 3** Click the **AnyConnect** tab on the bottom half of the Add or Edit Dynamic Access Policy window.



Policy Name: Test

Description:

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

| AAA Attribute | Operation/Value |
|---|---|
| cisco.username | = jsmith |

and the following endpoint attributes are satisfied.

| Endpoint ID | Name/Operation/Value |
|---|---|

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Always-On VPN for AnyConnect client: ○ Unchanged ○ Use AnyConnectProfile setting ● Disable

**Step 4** Click **Disable** next to “Always-On VPN for AnyConnect client."

## Set a Connect Failure Policy for Always-On

### *About the Connect Failure Policy*

The connect failure policy determines whether the computer can access the internet if Always-On VPN is enabled and AnyConnect cannot establish a VPN session. This can occur when a secure gateway is unreachable, or when AnyConnect fails to detect the presence of a captive portal hotspot.

An open policy permits full network access, letting users continue to perform tasks where access to the Internet or other local network resources is needed.

A closed policy disables all network connectivity until the VPN session is established. AnyConnect does this by enabling packet filters that block all traffic from the endpoint that is not bound for a secure gateway to which the computer is allowed to connect.

Regardless of the connect failure policy, AnyConnect continues to try to establish the VPN connection.

### *Guidelines for Setting the Connect Failure Policy*

Consider the following when using an open policy which permits full network access:

- Security and protection are not available until the VPN session is established; therefore, the endpoint device may get infected with web-based malware or sensitive data may leak.
- An open connect failure policy does not apply if you enable the Disconnect button and the user clicks **Disconnect**.

Consider the following when using a closed policy which disables all network connectivity until the VPN session is established:

- A closed policy can halt productivity if users require Internet access outside the VPN.
- The purpose of closed is to help protect corporate assets from network threats when resources in the private network that protect the endpoint are not available.The endpoint is protected from web-based malware and sensitive data leakage at all times because all network access is prevented except for local resources such as printers and tethered devices permitted by split tunneling.
- This option is primarily for organizations where security persistence is a greater concern than always-available network access.
- A closed policy prevents captive portal remediation unless you specifically enable it.
- You can allow the application of the local resource rules imposed by the most recent VPN session if **Apply Last VPN Local Resources** is enabled in the client profile. For example, these rules could determine access to active sync and local printing.
- The network is unblocked and open during an AnyConnect software upgrade when Always-On is enabled regardless of a closed policy.
- If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy Always-On with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

**Caution** A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. Use extreme caution when implementing a connect failure closed policy.

### *Configure a Connect Failure Policy*

You configure a Connect Failure Policy only when the Always-On feature is enabled. By default, the connect failure policy is closed, preventing Internet access if the VPN is unreachable. To allow Internet access in this situation the connect failure policy must be set to open.

#### Procedure

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

**Step 2** Set the **Connect Failure Policy** parameter to one of the following settings:

- Closed—(Default) Restricts network access when the secure gateway is unreachable.
- Open—Permits network access by browsers and other applications when the client cannot connect to the secure gateway.

**Step 3** If you specified a closed policy:

a) Configure Captive Portal Remediation.

b) Select **Apply Last VPN Local Resources** if you would like to retain the last VPN session's local device rules while network access is disabled.

# Use Captive Portal Hotspot Detection and Remediation

## About Captive Portals

Many facilities that offer Wi-Fi and wired access, such as airports, coffee shops, and hotels, require the user to pay before obtaining access, to agree to abide by an acceptable use policy, or both. These facilities use a technique called captive portal to prevent applications from connecting until the user opens a browser and accepts the conditions for access. Captive portal detection is the recognition of this restriction, and captive portal remediation is the process of satisfying the requirements of a captive portal hotspot in order to obtain network access.

Captive portals are detected automatically by AnyConnect when initiating a VPN connection requiring no additional configuration. Also, AnyConnect does not modify any browser configuration settings during captive portal detection and does not automatically remediate the captive portal. It relies on the end user to perform the remediation. AnyConnect reacts to the detection of a captive portal depending on the current configuration:

- If Always-On is disabled, or if Always-On is enabled and the Connect Failure Policy is open, the following message is displayed on each connection attempt:

  ```
  The service provider in your current location is restricting access to the Internet.
  You need to log on with the service provider before you can establish a VPN session.
  You can try this by visiting any website with your browser.
  ```

  The end user must perform captive portal remediation by meeting the requirements of the provider of the hotspot. These requirements could be paying a fee to access the network, signing an acceptable use policy, both, or some other requirement defined by the provider.

- If Always-On is enabled and the connect failure policy is closed, captive portal remediation needs to be explicitly enabled. If enabled, the end user can perform remediation as described above. If disabled, the following message is displayed upon each connection attempt, and the VPN cannot be connected.

  ```
  The service provider in your current location is restricting access to the Internet.
  The AnyConnect protection settings must be lowered for you to log on with the service
   provider. Your current enterprise security policy does not allow this.
  ```

## Configure Captive Portal Remediation

You configure captive portal remediation only when the Always-On feature is enabled and the Connect Failure Policy is set to closed. In this situation, configuring captive portal remediation allows AnyConnect to connect to the VPN when a captive portal is preventing it from doing so.

If the Connect Failure Policy is set to open or Always-On is not enabled, your users are not restricted from network access and are capable of remediating a captive portal without any specific configuration in the AnyConnect VPN client profile.

By default, captive portal remediation is disabled to provide the greatest security.

### Procedure

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

**Step 2** Select **Allow Captive Portal Remediation.**
This setting lifts the network access restrictions imposed by the closed connect failure policy.

**Step 3** Specify the Remediation Timeout.
Enter the number of minutes for which AnyConnect lifts the network access restrictions. The user needs enough time to satisfy the captive portal requirements.

## Troubleshoot Captive Portal Detection and Remediation

AnyConnect can falsely assume that it is in a captive portal in the following situations.

- If AnyConnect attempts to contact an ASA with a certificate containing an incorrect server name (CN), then the AnyConnect client will think it is in a “captive portal” environment.

  To prevent this, make sure the ASA certificate is properly configured. The CN value in the certificate must match the name of the ASA server in the VPN client profile.

- If there is another device on the network before the ASA, and that device responds to the client's attempt to contact an ASA by blocking HTTPS access to the ASA, then the AnyConnect client will think it is in a “captive portal” environment. This situation can occur when a user is on an internal network, and connects through a firewall to connect to the ASA.

  If you need to restrict access to the ASA from inside the corporation, configure your firewall such that HTTP and HTTPS traffic to the ASA’s address does not return an HTTP status. HTTP/HTTPS access to the ASA should either be allowed or completely blocked (also known as black-holed) to ensure that HTTP/HTTPS requests sent to the ASA will not return an unexpected response.

If users cannot access a captive portal remediation page, ask them to try the following:

- Terminate any applications that use HTTP, such as instant messaging programs, e-mail clients, IP phone clients, and all but one browser to perform the remediation.

  The captive portal may be actively inhibiting DoS attacks by ignoring repetitive attempts to connect, causing them to time out on the client end. The attempt by many applications to make HTTP connections exacerbates this problem.

- Disable and re-enable the network interface. This action triggers a captive portal detection retry.

- Restart the computer.

# Configure AnyConnect over L2TP or PPTP

ISPs in some countries require support of the Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).

To send traffic destined for the secure gateway over a Point-to-Point Protocol (PPP) connection, AnyConnect uses the point-to-point adapter generated by the external tunnel. When establishing a VPN tunnel over a PPP connection, the client must exclude traffic destined for the ASA from the tunneled traffic intended for destinations beyond the ASA. To specify whether and how to determine the exclusion route, use the PPP Exclusion setting in the AnyConnect profile. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI.

### Procedure

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

**Step 2** Choose a **PPP Exclusion** method. Also, check **User Controllable** for this field to let users view and change this setting:

- Automatic**—**Enables PPP exclusion. AnyConnect automatically uses the IP address of the PPP server. Instruct users to change the value only if automatic detection fails to get the IP address.
- Override**—**Also enables PPP exclusion. If automatic detection fails to get the IP address of the PPP server, and the PPP Exclusion UserControllable value is true, instruct users to follow the instructions in the next section to use this setting.
- Disabled**—**PPP exclusion is not applied.

**Step 3** In the **PPP Exclusion Server IP** field, enter the IP address of the PPP server used for the connection. Checking **User Controllable** for this field lets users change this IP address of the PPP Server via the preferences.xml file.

### What to Do Next

Refer to the *"Instruct Users to Override PPP Exclusion"* section for information about changing the preferences.xml file.

## Instruct Users to Override PPP Exclusion

If automatic detection does not work and you configured the PPP Exclusion fields as user controllable, the user can override the setting by editing the AnyConnect preferences file on the local computer.

### Procedure

**Step 1** Use an editor such as Notepad to open the preferences XML file.
This file is at one of the following paths on the user's computer:

- Windows: %LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml. For example,
- macOS: /Users/username/.anyconnect
- Linux: /home/username/.anyconnect

**Step 2** Insert the PPPExclusion details under `<ControllablePreferences>`, while specifying the Override value and the IP address of the PPP server. The address must be a well-formed IPv4 address. For example:

```
<AnyConnectPreferences>
```

```
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

**Step 3** Save the file.

**Step 4** Exit and restart AnyConnect.

# Configure AnyConnect Proxy Connections

## About AnyConnect Proxy Connections

AnyConnect supports VPN sessions through Local, Public, and Private proxies:

- Local Proxy Connections:

  A local proxy runs on the same PC as AnyConnect, and is sometimes used as a transparent proxy. Some examples of a transparent proxy service include acceleration software provided by some wireless data cards, or a network component on some antivirus software, such as Kaspersky.

  The use of a local proxy is enabled or disabled in the AnyConnect VPN client profile, see Allow a Local Proxy Connection.

- Public Proxy Connections:

  Public proxies are usually used to anonymize web traffic. When Windows is configured to use a public proxy, AnyConnect uses that connection. Public proxy is supported on macOS and Linux for both native and override.

  Configuring a public proxy is described in Configure a Public Proxy Connection, Windows.

- Private Proxy Connections:

  Private proxy servers are used on a corporate network to prevent corporate users from accessing certain Web sites based on corporate usage policies, for example, pornography, gambling, or gaming sites.

  You configure a group policy to download private proxy settings to the browser after the tunnel is established. The settings return to their original state after the VPN session ends. See Configure a Private Proxy Connection.

**Note** AnyConnect SBL connections through a proxy server are dependent on the Windows operating system version and system (machine) configuration or other third-party proxy software capabilities; therefore, refer to system wide proxy settings as provided by Microsoft or whatever third-party proxy application you use.

### Control Client Proxy with VPN Client Profile

The VPN Client profile can block or redirect the client system's proxy connection. For Windows and Linux, you can configure, or you can allow the user to configure, the address of a public proxy server.

For more information about configuring the proxy settings in the VPN client profile, see AnyConnect Profile Editor, Preferences (Part 2)

### Proxy Auto-Configuration File Generation for Clientless Support

Some versions of the ASA require AnyConnect configuration to support clientless portal access through a proxy server after establishing an AnyConnect session. AnyConnect uses a proxy auto-configuration (PAC) file to modify the client-side proxy settings to let this occur. AnyConnect generates this file only if the ASA does not specify private-side proxy settings.

## Requirements for AnyConnect Proxy Connections

OS support of proxy connections varies as shown:

| Proxy Connection Type | Windows | macOS | Linux |
|---|---|---|---|
| Local Proxy | Yes | No | No |
| Private Proxy | Yes (on Internet Explorer) | Yes (on Safari) | No |
| Public Proxy | Yes (IE and Override) | No | Yes (Override) |

## Limitations on Proxy Connections

- IPv6 proxies are not supported for any type of proxy connection.
- Connecting through a proxy is not supported with the Always-On feature enabled.
- A VPN client profile is required to allow access to a local proxy.

## Allow a Local Proxy Connection

### Procedure

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

**Step 2** Select (default) or unselect **Allow Local Proxy Connections**. Local proxy is disabled by default.

## Configure a Public Proxy Connection, Windows

Follow these steps to configure a public proxy connection on Windows.

### Procedure

**Step 1** Open **Internet Options** from Internet Explorer or the Control Panel.

**Step 2** Select the **Connections** Tab, and click the **LAN Settings** button.

**Step 3** Configure the LAN to use a proxy server, and enter the IP address of the proxy server.

## Configure a Private Proxy Connection

### Procedure

**Step 1** Configure the private proxy information in the ASA group policy. See the Configuring a Browser Proxy for an Internal Group Policy section in the *Cisco ASA Series VPN Configuration Guide*.

**Note** In a macOS environment, the proxy information that is pushed down from the ASA (upon a VPN connection) is not viewed in the browser until you open up a terminal and issue a scutil --proxy.

**Step 2** (Optional) Configure the Client to Ignore Browser Proxy Settings.

**Step 3** (Optional) Lock Down the Internet Explorer Connections Tab.

### Configure the Client to Ignore Browser Proxy Settings

You can specify a policy in the AnyConnect profile to bypass the Microsoft Internet Explorer or Safari proxy configuration settings on the user's PC. This prevents the user from establishing a tunnel from outside the corporate network, and prevents AnyConnect from connecting through an undesirable or illegitimate proxy server.

### Procedure

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

**Step 2** In the Proxy Settings drop-down list, choose **IgnoreProxy**. Ignore Proxy causes the client to ignore all proxy settings. No action is taken against proxies that are downloaded from the ASA.

### Lock Down the Internet Explorer Connections Tab

Under certain conditions, AnyConnect hides the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown is reversed on disconnect, and it is superseded by any administrator-defined policies applied to that tab. The conditions under which this lock down occurs are the following:

- The ASA configuration specifies Connections tab lockdown.

- The ASA configuration specifies a private-side proxy.
- A Windows group policy previously locked down the Connections tab (overriding the no lockdown ASA group policy setting).

You can configure the ASA to allow or not allow proxy lockdown, in the group policy. To do this using ASDM, follow this procedure:

**Procedure**

**Step 1** In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

**Step 2** Select a group policy and click **Edit** or **Add** a new group policy.

**Step 3** In the navigation pane, go to **Advanced** > **Browser Proxy**. The Proxy Server Policy pane displays.

**Step 4** Click **Proxy Lockdown** to display more proxy settings.

**Step 5** Uncheck **Inherit** and select **Yes** to enable proxy lockdown and hide the Internet Explorer Connections tab for the duration of the AnyConnect session or; select **No** to disable proxy lockdown and expose the Internet Explorer Connections tab for the duration of the AnyConnect session.

**Step 6** Click **OK** to save the Proxy Server Policy changes.

**Step 7** Click **Apply** to save the Group Policy changes.

### Verify the Proxy Settings

- For Windows: Find the proxy settings in the registry under:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- For macOS: Open a terminal window, and type:

```
scutil --proxy
```

# Select and Exclude VPN Traffic

## Configure IPv4 or IPv6 Traffic to Bypass the VPN

You can configure how the AnyConnect client manages IPv4 traffic when the ASA is expecting only IPv6 traffic or how AnyConnect manages IPv6 traffic when the ASA is only expecting IPv4 traffic using the Client Bypass Protocol setting.

When the AnyConnect client makes a VPN connection to the ASA, the ASA can assign the client an IPv4, IPv6, or both an IPv4 and IPv6 address.

If Client Bypass Protocol is enabled for an IP protocol and an address pool is not configured for that protocol (in other words, no IP address for that protocol was assigned to client by the ASA), any IP traffic using that protocol will not be sent through the VPN tunnel. It will be sent outside the tunnel.

If Client Bypass Protocol is disabled, and an address pool is not configured for that protocol, the client drops all traffic for that IP protocol once the VPN tunnel is established.

For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped. If Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

You configure the Client Bypass Protocol on the ASA in the group policies.

### Procedure

**Step 1** In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

**Step 2** Select a group policy and click **Edit** or **Add** a new group policy.

**Step 3** Select **Advanced** > **AnyConnect**.

**Step 4** Next to **Client Bypass Protocol**, uncheck **Inherit** if this is a group policy other than the default group policy.

**Step 5** Choose one of these options:

- Click **Disable** to drop IP traffic for which the ASA did not assign an address.
- Click **Enable** to send that IP traffic in the clear.

**Step 6** Click **OK**.

**Step 7** Click **Apply**.

## Configure a Client Firewall with Local Printer and Tethered Device Support

See the Client Firewall with Local Printer and Tethered Device Support section in the *Cisco ASA Series Configuration Guide*.

## Configure Split Tunneling

Split tunneling is configured in a Network (Client) Access group policy. See the *Configure Split Tunneling for AnyConnect Traffic* section in the Cisco ASA Series VPN Configuration Guide.

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy**.

## Split DNS

When split DNS is configured in the Network (Client) Access group policy, AnyConnect tunnels specific DNS queries to the private DNS server (also configured in the group policy). All other DNS queries go to the DNS resolver on the client operating system, in the clear, for DNS resolution. If split DNS is not configured, AnyConnect tunnels all DNS queries.

## Requirements for Split DNS

Split DNS supports standard and update queries (including A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR, and CNAME). PTR queries matching any of the tunneled networks are allowed through the tunnel.

AnyConnect split DNS is supported on Windows and macOS platforms.

For macOS, AnyConnect can use true split-DNS for a certain IP protocol only if one of the following conditions is met:

- Split-DNS is configured for one IP protocol (such as IPv4), and Client Bypass Protocol is configured for the other IP protocol (such as IPv6) in the group policy (with no address pool configured for the latter IP protocol).
- Split-DNS is configured for both IP protocols.

## Configure Split DNS

To configure split DNS in the group policy, do the following:

### Procedure

**Step 1** Configure at least one DNS server.
See the *Configure Server Attributes for an Internal Group Policy* section in the Cisco ASA Series VPN Configuration Guide.

Ensure the private DNS servers specified do not overlap with the DNS servers configured for the client platform. If they do, name resolution does not function properly and queries may be dropped.

**Step 2** Configure split-include tunneling:
On the **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Advanced** > **Split Tunneling** pane, choose the **Tunnel Network List Below** policy, and specify a **Network List** of addresses to be tunneled.

Split-DNS does not support the Exclude Network List Below split-tunneling policy. You must use the Tunnel Network List Below split-tunneling policy to configure split-DNS.

**Step 3** Configure split DNS:
On the **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Advanced** > **Split Tunneling** pane, uncheck **Send All DNS lookups through tunnel**, and specifying the names of the domains whose queries will be tunneled in **DNS Names**.

### What to Do Next

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles** > **Add/Edit** > **Group Policy**.

### Verify Split DNS Using AnyConnect Logs

To verify if split-DNS is enabled, search the AnyConnect logs for an entry containing "Received VPN Session Configuration Settings." That entry indicates Split DNS is enabled. There are separate log entries for IPv4 and IPv6 split DNS.

### Check Which Domains Use Split DNS

You can use any tool or application that relies on the operating system's DNS resolver for domain name resolution. For example, you can use a ping or web browser to test the split DNS solution. Other tools such as nslookup or dig circumvent the OS DNS resolver.

To use the client to check which domains are used for split DNS, follow these steps:

**Procedure**

**Step 1** Run **ipconfig/all** and record the domains listed next to DNS Suffix Search List.

**Step 2** Establish a VPN connection and again check the domains listed next to DNS Suffix Search List.
Those extra domains added after establishing the tunnel are the domains used for split DNS.

**Note** This process assumes that the domains pushed from the ASA do not overlap with the ones already configured on the client host.

# Manage VPN Authentication

## Important Security Considerations

- We do not recommend using a self-signed certificate on your secure gateway because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.
- We strongly recommend that you enable Strict Certificate Trust for the AnyConnect client for the following reasons:

  To configure **Strict Certificate Trust** , see the *Local Policy Parameters and Values* section: Local Policy Parameters and Values, on page 61.

## Configure Server Certificate Handling

### Server Certificate Verification

- The AnyConnect client does not support certificate verification using certificate revocation lists (CRL).

Many sites position the Certificate Authority they use to validate server certificates inside the corporate network. That means that a client cannot verify CRL when it is trying to connect to a headend, since the CRL is not accessible on the public network. The client operating system can be configured to verify CRL in Windows and Mac OS X, but we ignore that setting.

- (Windows only) For both SSL and IPsec VPN connections, you have the option to perform Certificate Revocation List (CRL) checking. When enabled in the profile editor, AnyConnect retrieves the updated CRL for all certificates in the chain. It then verifies whether the certificate in question is among those revoked certificates which should no longer be trusted; and if found to be a certificate revoked by the Certificate Authority, it does not connect. Refer to Local Policy Parameters and Values, on page 61 for further information.
- When a user connects to an ASA that is configured with a server certificate, the checkbox to trust and import that certificate will still display, even if there is a problem with the trust chain (Root, Intermediate, etc.) If there are any other certificate problems, that checkbox will not display.
- SSL connections being performed via FQDN do not make a secondary server certificate verification with the FQDN's resolved IP address for name verification if the initial verification using the FQDN fails.
- IPsec and SSL connections require that if a server certificate contains Key Usage, the attributes must contain DigitalSignature AND (KeyAgreement OR KeyEncipherment). If the server certificate contains an EKU, the attributes must contain serverAuth (for SSL and IPsec) or ikeIntermediate (for IPsec only). Note that server certificates are not required to have a KU or an EKU to be accepted.
- IPsec connections perform name verification on server certificates. The following rules are applied for the purposes of IPsec name verification:
    - If a Subject Alternative Name extension is present with relevant attributes, name verification is performed solely against the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates, and additionally include IP address attributes if the connection is being performed to an IP address.
    - If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification is performed against any Common Name attributes found in the Subject of the certificate.
    - If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.
- For OSX, expired certificates are displayed only when Keychain Access is configured to “Show Expired Certificates.” Expired certificates are hidden by default, which may confuse users.

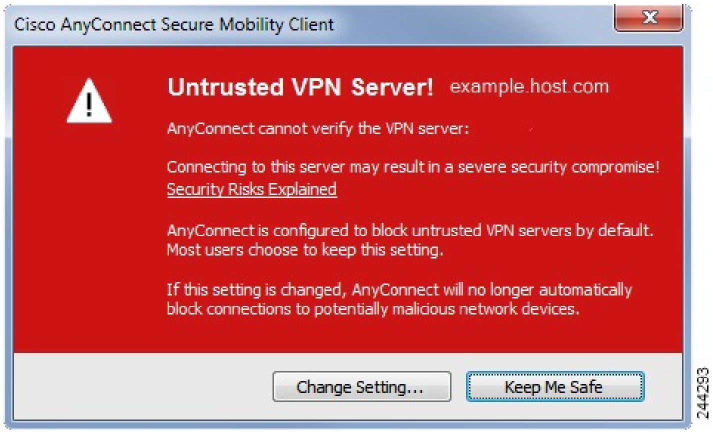
## Invalid Server Certificate Handling

In response to the increase of targeted attacks against mobile users on untrusted networks, we have improved the security protections in the client to help prevent serious security breaches. The default client behavior has been changed to provide an extra layer of defense against Man-in-the-middle attacks.

### User Interaction

When the user tries to connect to a secure gateway, and there is a certificate error (due to expired, invalid date, wrong key usage, or CN mismatch), the user sees a red-colored dialog with Change Settings and Keep Me Safe buttons.

**Note** The dialogs for Linux may look different from the ones shown in this document.



Cisco AnyConnect Secure Mobility Client

**Untrusted VPN Server!** example.host.com

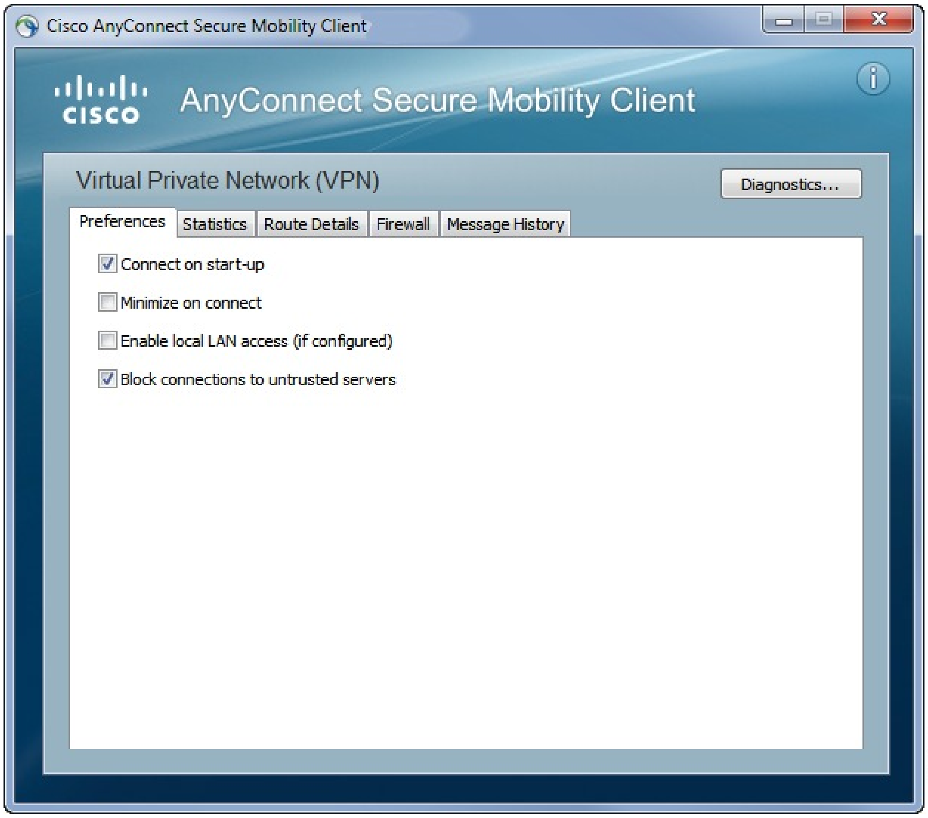
AnyConnect cannot verify the VPN server:

Connecting to this server may result in a severe security compromise!
Security Risks Explained

AnyConnect is configured to block untrusted VPN servers by default.
Most users choose to keep this setting.

If this setting is changed, AnyConnect will no longer automatically block connections to potentially malicious network devices.

- Clicking **Keep Me Safe** cancels the connection.
- Clicking **Change Settings** opens AnyConnect's Advanced > VPN >Preferences dialog, where the user can enable connections to untrusted servers. The current connection attempt is canceled.



Cisco AnyConnect Secure Mobility Client

AnyConnect Secure Mobility Client

Virtual Private Network (VPN)

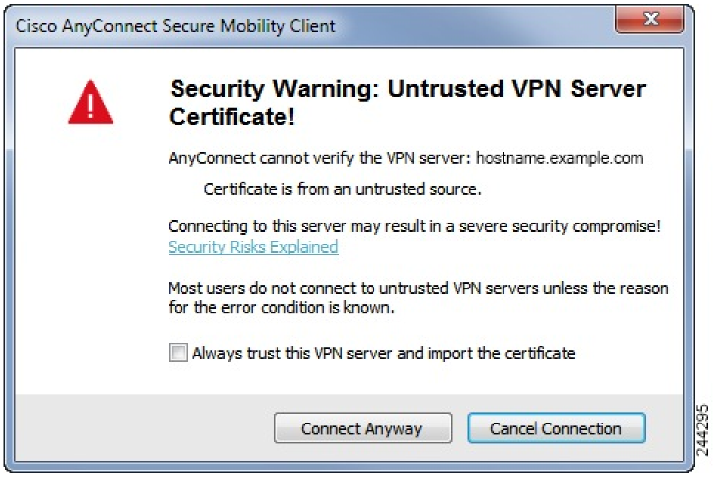
☑ Connect on start-up

□ Minimize on connect

□ Enable local LAN access (if configured)

☑ Block connections to untrusted servers

If the user un-checks **Block connections to untrusted servers**, and the only issue with the certificate is that the CA is untrusted, then the next time the user attempts to connect to this secure gateway, the user will not see the Certificate Blocked Error Dialog dialog; they only see the following dialog:



Cisco AnyConnect Secure Mobility Client

**Security Warning: Untrusted VPN Server Certificate!**

AnyConnect cannot verify the VPN server: hostname.example.com

Certificate is from an untrusted source.

Connecting to this server may result in a severe security compromise!
Security Risks Explained

Most users do not connect to untrusted VPN servers unless the reason for the error condition is known.

□ Always trust this VPN server and import the certificate

If the user checks **Always trust this VPN server and import the certificate**, then future connections to this secure gateway will not prompt the user to continue.

Note

If the user checks **Block connections to untrusted servers** in **AnyConnect Advanced > VPN > Preferences**, or if the user's configuration meets one of the conditions in the list of the modes described under the guidelines and limitations section, then AnyConnect rejects invalid server certificates.

### Improved Security Behavior

When the client accepts an invalid server certificate, that certificate is saved in the client's certificate store. Previously, only the thumbprint of the certificate was saved. Note that invalid certificates are saved only when the user has elected to always trust and import invalid server certificates.

There is no administrative override to make the end user less secure automatically. To completely remove the preceding security decisions from your end users, enable **Strict Certificate Trust** in the user's local policy file. When Strict Certificate Trust is enabled, the user sees an error message, and the connection fails; there is no user prompt.

For information about enabling Strict Certificate Trust in the local policy file, see the *AnyConnect Local Policy Parameters and Values* section: Local Policy Parameters and Values, on page 61.

### Guidelines and Limitations

Invalid server certificates are rejected when:

- Always On is enabled in the AnyConnect VPN client profile and is not turned off by an applied group policy or DAP.
- The client has a Local Policy with Strict Certificate Trust enabled.
- AnyConnect is configured to start before logon.
- A client certificate from the machine certificate store is used for authentication.

## Configure Certificate-Only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password.

To support certificate-only authentication in an environment where multiple groups are used, you may provision more than one group-url. Each group-url would contain a different client profile with some piece of customized data that would allow for a group-specific certificate map to be created. For example, the Department_OU value of Engineering could be provisioned on the ASA to place the user in this group when the certificate from this process is presented to the ASA.

Note

The certificate used to authenticate the client to the secure gateway must be valid and trusted (signed by a CA). A self-signed client certificate will not be accepted.

### Procedure

**Step 1** Go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**. Select a connection profile and click Edit. The Edit AnyConnect Connection Profile window opens.

**Step 2** If it is not already, click the **Basic** node of the navigation tree on the left pane of the window. In the right pane of the window, in the **Authentication** area, enable the method **Certificate**.

**Step 3** Click **OK** and apply your changes.

# Configure Certificate Enrollment

The Cisco AnyConnect Secure Mobility Client uses the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate as part of client authentication. Certificate enrollment using SCEP is supported by AnyConnect IPsec and SSL VPN connections to the ASA in the following ways:

- SCEP Proxy: The ASA acts as a proxy for SCEP requests and responses between the client and the Certificate Authority (CA).
    - The CA must be accessible to the ASA, not the AnyConnect client, since the client does not access the CA directly.
    - Enrollment is always initiated automatically by the client. No user involvement is necessary.
- Legacy SCEP: The AnyConnect client communicates with the CA directly to enroll and obtain a certificate.
    - The CA must be accessible to the AnyConnect client, not the ASA, through an established VPN tunnel or directly on the same network the client is on.
    - Enrollment is initiated automatically by the client and may be initiated manually by the user if configured.

### Related Topics

AnyConnect Profile Editor, Certificate Enrollment, on page 55

## SCEP Proxy Enrollment and Operation

The following steps describe how a certificate is obtained and a certificate-based connection is made when AnyConnect and the ASA are configured for SCEP Proxy.

1. The user connects to the ASA headend using a connection profile configured for both certificate and AAA authentication. The ASA requests a certificate and AAA credentials for authentication from the client.
2. The user enters his/her AAA credentials, but a valid certificate is not available. This situation triggers the client to send an automatic SCEP enrollment request after the tunnel has been established using the entered AAA credentials.
3. The ASA forwards the enrollment request to the CA and returns the CA’s response to the client.

4 If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.

If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact his/her administrator.

Other SCEP Proxy operational considerations:

- If configured to do so, the client automatically renews the certificate before it expires, without user intervention.
- SCEP Proxy enollment uses SSL for both SSL and IPsec tunnel certificate authentication.

## Legacy SCEP Enrollment and Operation

The following steps describe how a certificate is obtained and a certificate-based connection is made when AnyConnect is configured for Legacy SCEP.

1 When the user initiates a connection to the ASA headend using a tunnel group configured for certificate authentication, the ASA requests a certificate for authentication from the client.

2 A valid certificate is not available on the client. The connection cannot be established. This certificate failure indicates that SCEP enrollment needs to occur.

3 The user must then initiate a connection to the ASA headend using a tunnel group configured for AAA authentication only whose address matches the Automatic SCEP Host configured in the client profile. The ASA requests the AAA credentials from the client.

4 The client presents a dialog box for the user to enter AAA credentials.

If the client is configured for manual enrollment and the client knows it needs to initiate SCEP enrollment (see Step 2), a **Get Certificate** button displays on the credentials dialog box. If the client has direct access to the CA on his/her network, the user will be able to manually obtain a certificate by clicking this button at this time.

**Note** If access to the CA relies on the VPN tunnel being established, manual enrollment cannot be done at this time because there is currently no VPN tunnel established (AAA credentials have not been entered).

5 The user enters AAA credentials and establishes a VPN connection.

6 The client knows it needs to initiate SCEP enrollment (see Step 2). It initiates an enrollment request to the CA through the established VPN tunnel, and a response is received from the CA.

7 If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.

If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact his/her administrator.

Other Legacy SCEP operational considerations:

- If the client is configured for manual enrollment and the **Certificate Expiration Threshold** value is met, a **Get Certificate** button displays on a presented tunnel group selection dialog box. Users can manually renew their certificate by clicking this button.

- If the certificate expires and the client no longer has a valid certificate, the client repeats the Legacy SCEP enrollment process.

## Certificate Authority Requirements

- All SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA, are supported.
- The CA must be in auto-grant mode; polling for certificates is not supported.
- You can configure some CAs to email users an enrollment password for an additional layer of security. The CA password is the challenge password or token that is sent to the certificate authority to identify the user. The password can then be configured in the AnyConnect client profile, which becomes part of SCEP request that the CA verifies before granting the certificate. If you use manual Legacy SCEP enrollment, we recommend that you enable the CA password in the client profile.

## Guidelines for Certificate Enrollment

- Clientless (browser-based) VPN access to the ASA does not support SCEP proxy, but WebLaunch (clientless-initiated AnyConnect) does.
- ASA Load balancing is supported with SCEP enrollment.
- The ASA does not indicate why an enrollment failed, although it does log the requests received from the client. Connection problems must be debugged on the CA or the client.
- Certificate-Only Authentication and Certificate Mapping on the ASA:

  To support certificate-only authentication in an environment where multiple groups are used, you may provision more than one group-url. Each group-url would contain a different client profile with some piece of customized data that would allow for a group-specific certificate map to be created. For example, the Department_OU value of Engineering could be provisioned on the ASA to place the user in this tunnel group when the certificate from this process is presented to the ASA.
- Identifying Enrollment Connections to Apply Policies:

  On the ASA, the aaa.cisco.sceprequired attribute can be used to catch the enrollment connections and apply the appropriate policies in the selected DAP record.
- Windows Certificate Warning:

  When Windows clients first attempt to retrieve a certificate from a certificate authority they may see a warning. When prompted, users must click Yes. This allows them to import the root certificate. It does not affect their ability to connect with the client certificate.

## Configure SCEP Proxy Certificate Enrollment

### Configure a VPN Client Profile for SCEP Proxy Enrollment

#### Procedure

**Step 1** Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.

**Step 2** Select **Certificate Enrollment**.

**Step 3** Configure the **Certificate Contents** to be requested in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment.

**Note**
- If you use %machineid%, then Hostscan/Posture must be loaded for the desktop client.
- For mobile clients, at least one certificate field must be specified.

### Configure the ASA to Support SCEP Proxy Enrollment

For SCEP Proxy, a single ASA connection profile supports certificate enrollment and the certificate authorized VPN connection.

#### Procedure

**Step 1** Create a group policy, for example, cert_group. Set the following fields:

- On General, enter the URL to the CA in **SCEP Forwarding URL**.
- On the Advanced > AnyConnect Client pane, uncheck **Inherit** for Client Profiles to Download and specify the client profile configured for SCEP Proxy. For example, specify the ac_vpn_scep_proxy client profile.

**Step 2** Create a connection profile for certificate enrollment and certificate authorized connection, for example, cert_tunnel.

- Authentication: Both (AAA and Certificate).
- Default Group Policy: cert_group.
- On Advanced > General, check **Enable SCEP Enrollment for this Connction Profile**.
- On Advanced > GroupAlias/Group URL, create a Group URL containing the group (cert_group) for this connection profile.

# Configure Legacy SCEP Certificate Enrollment

## Configure a VPN Client Profile for Legacy SCEP Enrollment

### Procedure

**Step 1** Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.

**Step 2** Select **Certificate Enrollment.**

**Step 3** Specify an **Automatic SCEP Host** to direct the client to retrieve the certificate.
Enter the FQDN or IP address, and the alias of the connection profile (tunnel group) that is configured for SCEP certificate retrieval. For example, if asa.cisco.com is the host name of the ASA and scep_eng is the alias of the connection profile, enter asa.cisco.com/scep-eng.

When the user initiates the connection, the address chosen or specified must match this value exactly for Legacy SCEP enrollment to succeed. For example, if this field is set to an FQDN, but the user specifies an IP address, SCEP enrollment will fail.

**Step 4** Configure the Certificate Authority attributes:

**Note** Your CA server administrator can provide the CA URL and thumbprint. Retrieve the thumbprint directly from the server, not from a "fingerprint" or "thumbprint" attribute field in an issued certificate.

a) Specify a CA URL to identify the SCEP CA server. Enter an FQDN or IP address. For example: http://ca01.cisco.com/certsrv/mscep/mscep.dll.
b) (Optional) Check **Prompt For Challenge PW** to prompt users for their username and one-time password.
c) (Optional) Enter a thumbprint for the CA certificate. Use SHA1 or MD5 hashes. For example: `8475B661202E3414D4BB223A464E6AAB8CA123AB`.

**Step 5** Configure which **Certificate Contents** to request in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment.

**Note** If you use %machineid%, load HostScan/Posture on the client.

**Step 6** (Optional) Check **Display Get Certificate Button** to permit users to manually request provisioning or renewal of authentication certificates. The button is visible to users if the certificate authentication fails.

**Step 7** (Optional) Enable SCEP for a specific host in the server list. Doing this overrides the SCEP settings in the Certificate Enrollment pane described above.

a) Choose **Server List** from the navigation pane.
b) **Add** or **Edit** a server list entry.
c) Specify the Automatic SCEP Host and Certificate Authority attributes as described in Steps 5 and 6 above.

## Configure the ASA to Support Legacy SCEP Enrollment

For Legacy SCEP on the ASA, you must create a connection profile and group policy for certificate enrollment and a second connection profile and group policy for the certificate authorized VPN connection.

### Procedure

**Step 1** Create a group policy for enrollment, for example, cert_enroll_group. Set the following fields:
On the Advanced > AnyConnect Client pane, uncheck **Inherit** for Client Profiles to Download and specify the client profile configured for Legacy SCEP. For example, specify the ac_vpn_legacy_scep client profile.

**Step 2** Create a second group policy for authorization, for example, cert_auth_group.

**Step 3** Create a connection profile for enrollment, for example, cert_enroll_tunnel. Set the following fields:

- On the Basic pane, set the Authentication Method to AAA.
- On the Basic pane, set the Default Group Policy to cert_enroll_group.
- On Advanced > GroupAlias/Group URL, create a Group URL containing the enrollment group (cert_enroll_group) for this connection profile.
- Do not enable the connection profile on the ASA. It is not necessary to expose the group to users in order for them to have access to it.

**Step 4** Create a connection profile for authorization, for example, cert_auth_tunnel. Set the following fields.

- On the Basic pane, set the Authentication Method to Certificate.
- On the Basic pane, set the Default Group Policy to cert_auth_group.
- Do not enable this connection profile on the ASA. It is not necessary to expose the group to users in order for them to access it.

**Step 5** (Optional) On the General pane of each group policy, set **Connection Profile (Tunnel Group) Lock** to the corresponding SCEP connection profile, which restricts traffic to the SCEP-configured connection profile.

## Set Up a Windows 2008 Server Certificate Authority for SCEP

If your Certificate Authority software is running on a Windows 2008 server, you may need to make one of the following configuration changes to the server to support SCEP with AnyConnect.

### Disable the SCEP Password on the Certificate Authority

The following steps describe how to disable the SCEP challenge password, so that clients will not need to provide an out-of-band password before SCEP enrollment.

### Procedure

**Step 1** On the Certificate Authority server, launch the Registry Editor. You can do this by selecting **Start** > **Run**, typing **regedit**, and clicking **OK**.

**Step 2** Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword. If the EnforcePassword key does not exist, create it as a new Key.

**Step 3** Edit EnforcePassword, and set it to '0'. If it does not exist, create it as a REG-DWORD.

**Step 4** Exit regedit, and reboot the certificate authority server.

### Setting the SCEP Template on the Certificate Authority

The following steps describe how to create a certificate template, and assign it as the default SCEP template.

#### Procedure

**Step 1** Launch the Server Manager. You can do this by selecting Start > Admin Tools > Server Manager.

**Step 2** Expand Roles > Certificate Services (or AD Certificate Services).

**Step 3** Navigate to CA Name > Certificate Templates.

**Step 4** Right-click **Certificate Templates > Manage**.

**Step 5** From the Cert Templates Console, right-click User template and choose **Duplicate**

**Step 6** Choose **Windows Server 2008 version** for new template, and click **OK**.

**Step 7** Change the template display name to something descriptive, such as NDES-IPSec-SSL.

**Step 8** Adjust the Validity Period for your site. Most sites choose three or more years to avoid expired certificates.

**Step 9** On the Cryptography tab, set the minimum key size for your deployment.

**Step 10** On the Subject Name tab, select **Supply in Request**.

**Step 11** On the Extensions tab, set the Application Policies to include at least:

- Client Authentication
- IP security end system
- IP security IKE intermediate
- IP security tunnel termination
- IP security user

These values are valid for SSL or IPsec.

**Step 12** Click **Apply**, then **OK** to save new template.

**Step 13** From Server manager > Certificate Services-CA Name, right-click Certificate Templates. Select New > Certificate Template to Issue, select the new template you created (in this example, NDES-IPSec-SSL), and click **OK**.

**Step 14** Edit the registry. You can do this by selecting Start > Run, regedit, and clicking **OK**.

**Step 15** Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.

**Step 16** Set the value of the following three keys to **NDES-IPSec-SSL**.

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

**Step 17** Click **Save**, and reboot the certificate authority server.

# Configure a Certificate Expiration Notice

Configure AnyConnect to warn users that their authentication certificate is about to expire. The **Certificate Expiration Threshold** setting specifies the number of days before the certificate's expiration date that AnyConnect warns users that their certificate is expiring. AnyConnect warns the user upon each connect until the certificate has actually expired or a new certificate has been acquired.

**Note** The Certificate Expiration Threshold feature cannot be used with RADIUS.

### Procedure

**Step 1** Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.

**Step 2** Select **Certificate Enrollment.**

**Step 3** Specify a **Certificate Expiration Threshold**.
This is the number of days before the certificate expiration date, that AnyConnect warns users that their certificate is going to expire.

The default is 0 (no warning displayed). The range is 0 to 180 days.

**Step 4** Click **OK**.

# Configure Certificate Selection

The following steps show all the places in the AnyConnect profiles where you configure how certificates are searched for and how they are selected on the client system. None of the steps are required, and if you do not specify any criteria, AnyConnect uses default key matching.

AnyConnect reads the browser certificate stores on Windows. For macOS and Unix, you must create a Privacy Enhanced Mail (PEM) formatted file store.

### Procedure

**Step 1** Windows and macOS:Configure Which Certificate Stores to Use, on page 105
Specify which certificate stores are used by AnyConnect in the VPN client profile.

**Step 2** Windows Only: Prompt Windows Users to Select Authentication Certificate, on page 106
Configure AnyConnect to present a list of valid certificates to users and let them choose the certificate to authenticate the session.

**Step 3** For macOS and Linux environments: Create a PEM Certificate Store for macOS and Linux, on page 107

**Step 4** For macOS and Linux environments: Select which certificate stores to exclude in the VPN Local Policy profile.

**Step 5** Configure Certificate Matching, on page 108

Configure keys that AnyConnect tries to match, when searching for a certificate in the store. You can specify keys, extended keys, and add custom extended keys. You can also specify a pattern for the value of an operator in a distinguished name for AnyConnect to match.

## Configure Which Certificate Stores to Use

Windows provides separate certificate stores for the local machine and for the current user. Specify which certificate stores are used by AnyConnect in the VPN client profile. By default, it searches both, but you can configure AnyConnect to use only one.

Users with administrative privileges on the computer have access to both certificate stores. Users without administrative privileges only have access to the user certificate store. Usually, Windows users do not have administrative privileges. Selecting **Certificate Store Override** allows AnyConnect to access the machine store, even when the user does not have administrative privileges.

**Note** Access-control for the machine store can vary depending on the Windows version and security settings. Because of this, the user may be unable to use certificates in the machine store even though they have administrative privileges. In this case, select **Certificate Store Override** to allow machine store access.

The following table describes how AnyConnect searches for certificates on a client based on what **Certificate Store** is searched, and whether **Certificate Store Override** is checked.

| Certificate Store Setting | Certificate Store Override Setting | AnyConnect Search Strategy |
|---|---|---|
| All (for Windows) | cleared | AnyConnect searches all certificate stores. AnyConnect is not allowed to access the machine store when the user does not have administrative privileges.<br>This setting is the default. This setting is appropriate for most cases. Do not change this setting unless you have a specific reason or scenario requirement to do so. |
| All (for Windows) | checked | AnyConnect searches all certificate stores. AnyConnect is allowed to access the machine store when the user does not have administrative privileges. |
| Machine<br>(not a multi-cert option) | checked | AnyConnect searches the machine certificate store. AnyConnect is allowed to search the machine store when the user does not have administrative privileges. |

| Certificate Store Setting | Certificate Store Override Setting | AnyConnect Search Strategy |
|---|---|---|
| Machine<br>(not a multi-cert option) | cleared | AnyConnect searches the machine certificate store. AnyConnect is not allowed to search the machine store when the user does not have administrative privileges.<br>**Note** This configuration can be used when only a limited group of users is allowed to authenticate using a certificate. |
| User (for Windows) | does not apply | AnyConnect searches in the user certificate store only. The certificate store override is not applicable because users without administrative rights can have access to this certificate store. |

### With Basic Certificate Authentication

#### Procedure

**Step 1** Set **Certificate Store**.

- All—(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.
- Machine—Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.
- User—Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.

**Step 2** Choose **Certificate Store Override** if you want to allow AnyConnect to search the machine certificate store when users do not have administrative privileges.

## Prompt Windows Users to Select Authentication Certificate

You can configure the AnyConnect to present a list of valid certificates to users and let them choose the certificate to authenticate the session. An expired certificate is not necessarily considered invalid. For example, if you are using SCEP, the server might issue a new certificate to the client. Eliminating expired certificates might keep a client from connecting at all; thus requiring manual intervention and out-of-band certificate distribution. AnyConnect only restricts the client certificate based on security-related properties, such as key usage, key type and strength, and so on, based on configured certificate matching rules. This configuration is available only for Windows. By default, user certificate selection is disabled.

### Procedure

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

**Step 2** To enable certificate selection, uncheck **Disable Certificate Selection**.

**Step 3** Uncheck **User Controllable**, unless you want users to be able to turn automatic certificate selection on and off in the **Advanced** > **VPN** > **Preferences** pane.

## Create a PEM Certificate Store for macOS and Linux

AnyConnect supports certificate retrieval from a Privacy Enhanced Mail (PEM) formatted file store. AnyConnect reads PEM-formatted certificate files from the file system on the remote computer, verifies, and signs them.

### Before You Begin

In order for the client to acquire the appropriate certificates under all circumstances, ensure that your files meet the following requirements:

- All certificate files must end with the extension .pem.
- All private key files must end with the extension .key.
- A client certificate and its corresponding private key must have the same filename. For example: client.pem and client.key.

**Tip** Instead of keeping copies of the PEM files, you can use soft links to PEM files.

To create the PEM file certificate store, create the paths and folders listed below. Place the appropriate certificates in these folders:

| PEM File Certificate Store Folders | Type of Certificates Stored |
|---|---|
| ~/.cisco/certificates/ca(1) ~<br>**Note** This is the home directory. | Trusted CA and root certificates |
| ~/.cisco/certificates/client | Client certificates |
| ~/.cisco/certificates/client/private | Private keys |

Machine certificates are the same as PEM file certificates, except for the root directory. For machine certificates, substitute /opt/.cisco for ~/.cisco. Otherwise, the paths, folders, and types of certificates listed apply.

## Configure Certificate Matching

AnyConnect can limit its search of certificates to those certificates that match a specific set of keys. Certificate matchings are global criteria that are set in an AnyConnect VPN client profile, in the **Certificate Matching** pane. The criteria are:

- Key Usage
- Extended Key Usage
- Distinguished Name

### Related Topics

AnyConnect Profile Editor, Certificate Matching, on page 52

### Configure Key Usage

Selecting the **Key Usage** keys limits the certificates that AnyConnect can use to those certificates that have at least one of the selected keys. The supported set is listed in the **Key Usage** list on the VPN client profile, and it includes:

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

If one or more criteria are specified, a certificate must match at least one to be considered a matching certificate.

### Configure Extended Key Usage

Selecting the **Extended Key Usage** keys limits the certificates that AnyConnect can use to the certificates that have these keys. The following table lists the well-known set of constraints with their corresponding object identifiers (OIDs).

| Constraint | OID |
|---|---|
| ServerAuth | 1.3.6.1.5.5.7.3.1 |
| ClientAuth | 1.3.6.1.5.5.7.3.2 |
| CodeSign | 1.3.6.1.5.5.7.3.3 |

| Constraint | OID |
|---|---|
| EmailProtect | 1.3.6.1.5.5.7.3.4 |
| IPSecEndSystem | 1.3.6.1.5.5.7.3.5 |
| IPSecTunnel | 1.3.6.1.5.5.7.3.6 |
| IPSecUser | 1.3.6.1.5.5.7.3.7 |
| TimeStamp | 1.3.6.1.5.5.7.3.8 |
| OCSPSign | 1.3.6.1.5.5.7.3.9 |
| DVCS | 1.3.6.1.5.5.7.3.10 |
| IKE Intermediate | 1.3.6.1.5.5.8.2.2 |

### Configure Custom Extended Match Key

All other OIDs (such as 1.3.6.1.5.5.7.3.11, used in some examples in this document) are considered “custom.” As an administrator, you can add your own OIDs if the OID that you want is not in the well-known set.

### Configure Certificate Distinguished Name

The **Distinguished Name** table contains certificate identifiers that limit the certificates that the client can use to the certificates that match the specified criteria and criteria match conditions. Click the **Add** button to add criteria to the list and to set a value or wildcard to match the contents of the added criteria.

| Identifier | Description |
|---|---|
| CN | SubjectCommonName |
| SN | SubjectSurName |
| GN | SubjectGivenName |
| N | SubjectUnstructName |
| I | SubjectInitials |
| GENQ | SubjectGenQualifier |
| DNQ | SubjectDnQualifier |
| C | SubjectCountry |
| L | SubjectCity |

| Identifier | Description |
|---|---|
| SP | SubjectState |
| ST | SubjectState |
| O | SubjectCompany |
| OU | SubjectDept |
| T | SubjectTitle |
| EA | SubjectEmailAddr |
| DC | DomainComponent |
| ISSUER-CN | IssuerCommonName |
| ISSUER-SN | IssuerSurName |
| ISSUER-GN | IssuerGivenName |
| ISSUER-N | IssuerUnstructName |
| ISSUER-I | IssuerInitials |
| ISSUER-GENQ | IssuerGenQualifier |
| ISSUER-DNQ | IssuerDnQualifier |
| ISSUER-C | IssuerCountry |
| ISSUER-L | IssuerCity |
| ISSUER-SP | IssuerState |
| ISSUER-ST | IssuerState |
| ISSUER-O | IssuerCompany |
| ISSUER-OU | IssuerDept |
| ISSUER-T | IssuerTitle |
| ISSUER-EA | IssuerEmailAddr |
| ISSUER-DC | IssuerDomainComponent |

**Distinguished Name** can contain zero or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. **Distinguished Name** matching specifies that a certificate must or must not have the specified string, and whether wild carding for the string is allowed.

# VPN Authentication Using SDI Token (SoftID) Integration

AnyConnect integrates support for RSA SecurID client software versions 1.1 and later running on Windows 7 x86 (32-bit) and x64 (64-bit).

RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. RSA SecurID Software Tokens residing on a remote device generate a random one-time-use passcode that changes every 60 seconds. The term SDI stands for Security Dynamics, Inc. technology, which refers to this one-time password generation technology that uses hardware and software tokens.

Typically, users make an AnyConnect connection by clicking the AnyConnect icon in the tools tray, selecting the connection profile with which they wish to connect, and then entering the appropriate credentials in the authentication dialog box. The login (challenge) dialog box matches the type of authentication configured for the tunnel group to which the user belongs. The input fields of the login dialog box clearly indicate what kind of input is required for authentication.

For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, the RSA Authentication Manager validates the passcode and allows the user to gain access.

Users who use RSA SecurID hardware or software tokens see input fields indicating whether the user should enter a passcode or a PIN, a PIN, or a passcode and the status line at the bottom of the dialog box provides further information about the requirements. The user enters a software token PIN or passcode directly into the AnyConnect user interface.

The appearance of the initial login dialog box depends on the secure gateway settings: the user can access the secure gateway either through the main login page, the main index URL, a tunnel-group login page, or a tunnel group URL (URL/tunnel-group). To access the secure gateway via the main login page, the “Allow user to select connection” check box must be set in the Network (Client) Access AnyConnect Connection Profiles page. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down list in which the user selects a tunnel group; the tunnel-group login page does not, since the tunnel-group is specified in the URL.

In the case of a main login page (with a drop-down list of connection profiles or tunnel groups), the authentication type of the default tunnel group determines the initial setting for the password input field label. For example, if the default tunnel group uses SDI authentication, the field label is “Passcode;” but if the default tunnel group uses NTLM authentication, the field label is “Password.” In Release 2.1 and later, the field label is not dynamically updated with the user selection of a different tunnel group. For a tunnel-group login page, the field label matches the tunnel-group requirements.

The client supports input of RSA SecurID Software Token PINs in the password input field. If the RSA SecurID Software Token software is installed and the tunnel-group authentication type is SDI, the field label is “Passcode” and the status bar states “Enter a username and passcode or software token PIN.” If a PIN is used, subsequent consecutive logins for the same tunnel group and username have the field label “PIN.” The client retrieves the passcode from the RSA SecurID Software Token DLL using the entered PIN. With each successful authentication, the client saves the tunnel group, the username, and authentication type, and the saved tunnel group becomes the new default tunnel group.

AnyConnect accepts passcodes for any SDI authentication. Even when the password input label is “PIN,” the user may still enter a passcode as instructed by the status bar. The client sends the passcode to the secure gateway as is. If a passcode is used, subsequent consecutive logins for the same tunnel group and username have the field label "Passcode."

The RSASecureIDIntegration profile setting has three possible values:

- Automatic—The client first attempts one method, and if it fails, the other method is tried. The default is to treat the user input as a token passcode (HardwareToken), and if that fails, treat it as a software token pin (SoftwareToken). When authentication is successful, the successful method is set as the new SDI Token Type and cached in the user preferences file. For the next authentication attempt, the SDI Token Type defines which method is attempted first. Generally, the token used for the current authentication attempt is the same token used in the last successful authentication attempt. However, when the username or group selection is changed, it reverts to attempting the default method first, as shown in the input field label.

  **Note** The SDI Token Type only has meaning for the automatic setting. You can ignore logs of the SKI Token Type when the authentication mode is not automatic. HardwareToken as the default avoids triggering next token mode.

- SoftwareToken—The client always interprets the user input as a software token PIN, and the input field label is "PIN:".
- HardwareToken—The client always interprets the user input as a token passcode, and the input field label is "Passcode:".

**Note** AnyConnect does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the client uses the default selected via the RSA SecurID Software Token GUI.

## Categories of SDI Authentication Exchanges

All SDI authentication exchanges fall into one of the following categories:

- Normal SDI Authentication Login
- New User mode
- New PIN mode
- Clear PIN mode
- Next Token Code mode

### Normal SDI Authentication Login

A normal login challenge is always the first challenge. The SDI authentication user must provide a user name and token passcode (or PIN, in the case of a software token) in the username and passcode or PIN fields, respectively. The client returns the information to the secure gateway (central-site device), and the secure gateway verifies the authentication with the authentication server (SDI or SDI via RADIUS proxy).

If the authentication server accepts the authentication request, the secure gateway sends a success page back to the client, and the authentication exchange is complete.

If the passcode is not accepted, the authentication fails, and the secure gateway sends a new login challenge page, along with an error message. If the passcode failure threshold on the SDI server has been reached, then the SDI server places the token into next token code mode.

### New User, Clear PIN, and New PIN Modes

The PIN can be cleared only on the SDI server and only by the network administrator.

In the New User, Clear PIN, and New PIN modes, AnyConnect caches the user-created PIN or system-assigned PIN for later use in the "next passcode" login challenge.

Clear PIN mode and New User mode are identical from the point of view of the remote user and are both treated the same by the secure gateway. In both cases, the remote user either must enter a new PIN or be assigned a new PIN by the SDI server. The only difference is in the user response to the initial challenge.

For New PIN mode, the existing PIN is used to generate the passcode, as it would be in any normal challenge. For Clear PIN mode, no PIN is used at all for hardware tokens, with the user entering just a token code. A PIN of eight consecutive zeros (00000000) is used to generate a passcode for RSA software tokens. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Adding a new user to an SDI server has the same result as clearing the PIN of an existing user. In both cases, the user must either provide a new PIN or be assigned a new PIN by the SDI server. In these modes, for hardware tokens, the user enters just a token code from the RSA device. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

### Creating a New PIN

If there is no current PIN, the SDI server requires that one of the following conditions be met, depending on how the system is configured:

- The system must assign a new PIN to the user (Default)
- The user must create a new PIN
- The user can choose whether to create a PIN or have the system assign it

If the SDI server is configured to allow the remote user to choose whether to create a PIN or have the system assign a PIN, the login screen presents a drop-down list showing the options. The status line provides a prompt message.

For a system-assigned PIN, if the SDI server accepts the passcode that the user enters on the login page, then the secure gateway sends the client the system-assigned PIN. The client sends a response back to the secure gateway, indicating that the user has seen the new PIN, and the system continues with a "next passcode' challenge.

If the user chooses to create a new PIN, AnyConnect presents a dialog box on which to enter that PIN. The PIN must be a number from 4 to 8 digits long. Because the PIN is a type of password, anything the user enters into these input fields is displayed as asterisks.

With RADIUS proxy, the PIN confirmation is a separate challenge, subsequent to the original dialog box. The client sends the new PIN to the secure gateway, and the secure gateway continues with a "next passcode" challenge.

### "Next Passcode" and "Next Token Code" Challenges

For a "next passcode" challenge, the client uses the PIN value cached during the creation or assignment of a new PIN to retrieve the next passcode from the RSA SecurID Software Token DLL and return it to the secure gateway without prompting the user. Similarly, in the case of a “next Token Code” challenge for a software token, the client retrieves the next Token Code from the RSA SecurID Software Token DLL.

## Compare Native SDI with RADIUS SDI

The network administrator can configure the secure gateway to allow SDI authentication in either of the following modes:

- Native SDI refers to the native ability in the secure gateway to communicate directly with the SDI server for handling SDI authentication.
- RADIUS SDI refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

Native SDI and RADIUS SDI appear identical to the remote user. Because the SDI messages are configurable on the SDI server, the message text on the ASA must match the message text on the SDI server. Otherwise, the prompts displayed to the remote client user might not be appropriate for the action required during authentication. AnyConnect might fail to respond and authentication might fail.

RADIUS SDI challenges, with minor exceptions, essentially mirror native SDI exchanges. Since both ultimately communicate with the SDI server, the information needed from the client and the order in which that information is requested is the same.

During authentication, the RADIUS server presents access challenge messages to the ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA is communicating directly with an SDI server from when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to AnyConnect, the ASA must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. AnyConnect might fail to respond and authentication might fail.

## Configure the ASA to Support RADIUS/SDI Messages

To configure the ASA to interpret SDI-specific RADIUS reply messages and prompt the AnyConnect user for the appropriate action, you must configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server. Users authenticating to the SDI server must connect over this connection profile.

### Procedure

**Step 1** Go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**.

**Step 2** Select the connection profile you want to configure to interpret SDI-specific RADIUS reply messages and click **Edit**.

**Step 3** In the **Edit AnyConnect Connection Profile** window, expand the Advanced node in the navigation pane on the left and select **Group Alias / Group URL.**

**Step 4** Check **Enable the display of SecurID messages on the login screen**.

**Step 5** Click **OK**.

**Step 6** Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**.

**Step 7** Click **Add** to Add a AAA Server group.

**Step 8** Configure the AAA server group in the Edit AAA Server Group dialog and click **OK**.

**Step 9** In the **AAA Server Groups** area, select the AAA server group you just created and then click **Add** in the **Servers in the Selected Group** area.

**Step 10** In the SDI Messages area, expand the **Message Table** area. Double-click a message text field to edit the message. Configure the RADIUS reply message text on the ASA to match (in whole or in part) the message text sent by the RADIUS server.
The following table shows the message code, the default RADIUS reply message text, and the function of each message:

**Note** The default message text used by the ASA is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the ASA.

Because the security appliance searches for strings in the order in which they appear in the table, you must ensure that the string you use for the message text is not a subset of another string. For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN,” when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

| Message Code | Default RADIUS Reply Message Text | Function |
|---|---|---|
| next-code | Enter Next PASSCODE | Indicates the user must enter the NEXT tokencode without the PIN. |
| new-pin-sup | Please remember your new PIN | Indicates the new system PIN has been supplied and displays that PIN for the user. |
| new-pin-meth | Do you want to enter your own pin | Requests from the user which new PIN method to use to create a new PIN. |
| new-pin-req | Enter your new Alpha-Numerical PIN | Indicates a user-generated PIN and requests that the user enter the PIN. |

| Message Code | Default RADIUS Reply Message Text | Function |
|---|---|---|
| new-pin-reenter | Reenter PIN: | Used internally by the ASA for user-supplied PIN confirmation. The client confirms the PIN without prompting the user. |
| new-pin-sys-ok | New PIN Accepted | Indicates the user-supplied PIN was accepted. |
| next-ccode-and-reauth | new PIN with the next card code | Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate. |
| ready-for-sys- pin | ACCEPT A SYSTEM GENERATED PIN | Used internally by the ASA to indicate the user is ready for the system-generated PIN. |

**Step 11** Click **OK**, then **Apply**, then **Save**.