CHAPTER 13

Administering AnyConnect for Mobile Devices

This chapter provides you with device information, configuration information, support information, as well as other administrative tasks specific to AnyConnect 3.0 for Apple iOS and Android devices.

AnyConnect on Apple iOS Devices

Supported Apple iOS Devices

(with Retina

Device	Apple iOS Release Required
iPad Air	7.0 or later
iPad 2	6.0 or later
iPad (3rd generation)	6.0 or later
iPad (4th generation)	6.0 or later
iPad mini	6.0 or later
iPad mini (with Retina display)	7.0 or later
iPhone 3GS	6.0 or later
iPhone 4	6.0 or later
iPhone 4S	6.0 or later
iPhone 5	6.0 or later

Device	Apple iOS Release Required
iPhone 5C	7.0 or later
iPhone 5S	7.0 or later
iPod Touch (4th generation)	6.0 or later
iPod Touch (5th generation)	6.0 or later

Note AnyConnect on the iPod Touch appears and operates as on the iPhone. Use the *iPhone User Guide for Cisco AnyConnect Secure Mobility Client* for this device.

AnyConnect Features Supported on Apple iOS Devices

The following AnyConnect features are supported in AnyConnect 3.0.x for Apple iOS:

- Tunnel Protocols
  - Cisco SSL Tunneling Protocol (CSTP)
  - Cisco DTLS Tunneling Protocol (CDTP)
  - IPsec IKEv2
- SSL Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - DES-CBC-SHA
- Suite B (IPsec only)
- FIPS 140-2 Level 1
- Authentication
- Client Certificate Authentication
- Auto Reconnect (regardless of the Auto Reconnect profile specification, AnyConnect Mobile always attempts to maintain the VPN as users move between cellular and WiFi networks)
- Routing Policy
  - Tunnel All

  - Split Include
  - Split Exclude
- Rekey
- Network Roaming
- TLS Compression
- Cisco Profile Support
- Profile Update
- IPv6 over IPv4
- Post-Login Banner
- Dead Peer Detection
- Tunnel Keepalive
- Backup Server List
- Default Domain
- Cluster Support
- DNS Server Configuration
- Private-side Proxy Support
- Network Change Monitoring
- Statistics
- Graphical User Interface
- Pre-login Banner
- Secure Certificate Enrollment Protocol (SCEP)
- SCEP Proxy
- Certificate Management
  - Import a certificate using the client interface or URI command.
  - Delete a certificate or all certificates on the device.
- Connect on Demand (compatible with Apple iOS Connect on Demand)
- Mobile Posture
- Localization

Installing and Upgrading AnyConnect on Apple iOS Devices

End users install or upgrade the AnyConnect Secure Mobility Client for Apple iOS devices like any other iPad, iPhone, or iPod Touch app, by visiting the Apple App Store and downloading the app. The AnyConnect client app is free. For detailed installation steps, see the iPhone or iPad AnyConnect user guide.

The AnyConnect UI on Apple iOS Devices

For a description of the AnyConnect app, its user interface, and all activities carried out in the app, see the iPhone or iPad AnyConnect user guide.

Apple iOS Specific Considerations

Take the following considerations into account when supporting AnyConnect on Apple iOS devices:

- The SCEP references in this document apply exclusively to AnyConnect SCEP, not Apple iOS SCEP.
- Push e-mail notifications do not work via 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.

Using the Connect on Demand Feature

The Apple iOS Connect On Demand feature starts a VPN connection when a user attempts to access any destination with a hostname specified in the appropriate domains list. For example, if *.example.com is in the Always Connect list, when a user goes to internal.example.com, the client starts a VPN connection regardless of the network to which the device is currently connected.

Apple has introduced a Trusted Network Detection (TND) enhancement to the Connect On Demand feature in iOS 6. This enhancement:

- Extends the Connect on Demand functionality by determining whether the 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 a VPN should be connected.
- 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.

Note Releases prior to iOS 6 do not support discerning between trusted and untrusted networks.

Configuration Notes for Connect on Demand

- For mobile devices that have Connect on Demand configured, certificate-based authentication tunnel groups should 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 need not always 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.
- We recommend using the Connect if Needed option if you configure rules. A Connect if Needed rule initiates 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.
- Apple iOS 7 no longer supports *Always Connect* domains. When running AnyConnect on Apple iOS 7 devices, any domains listed as *Always Connect* will be treated as *Connect if Needed* domains.

See the "Apple iOS Connect On Demand" section for detailed configuration procedures and feature information.

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.

AnyConnect for Apple iOS supports the optional **split-dns** command to specify the DNS queries to resolve; however, the command works differently than it does on other devices if you also configure split tunnel VPN.

The **split-dns** command, entered in group-policy configuration mode, lists the domains to be resolved through the VPN session, as follows:

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2 ...
domain-nameN] | none}
```

If the **split-dns** command is not present, the group policy inherits the spilt 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 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 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 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.

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 is done in place of configuring an AnyConnect XML client profile on the secure gateway.

The existing IPCU GUI, controlled by Apple, does not have knowledge of the AnyConnect IPsec capabilities. You configure IPsec VPN connections within the existing AnyConnect GUI in IPCU by using the following URI syntax, as defined in RFC 2996, in the Server field:

```
[ipsec://][<AUTHENTICATION>[":"<IKE-IDENTITY>"@"]] <HOST>[":"<PORT>]["/"<GROUP-URL>]
```

Note This Server field syntax is backward compatible with the documented usage for configuring SSL VPN connections.

Parameters are specified as described:

- **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:
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - 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
```

AnyConnect on Android Devices

Supported Android Devices

Cisco provides AnyConnect brand-specific apps to support mobile devices from the following manufacturers:

- Samsung Devices
- HTC Devices
- Kindle Devices

Cisco also provides the following AnyConnect apps to support Android devices:

- AnyConnect for Android 4.0 Devices and later (ICS+)
- AnyConnect for Rooted Devices

Note Cisco no longer provides or supports the brand-specific AnyConnect apps for Lenovo and Motorola devices. Lenovo and Motorola devices that run Android version 4.0 (Ice Cream Sandwich) or later can use the AnyConnect ICS+ app. Uninstall the old brand-specific AnyConnect package before upgrading to AnyConnect 3.0.

Samsung Devices

Samsung AnyConnect Release 3.0.x and Samsung AnyConnect Legacy Release 3.0.x support the Samsung product lines listed below. The devices must be running the latest software update from Samsung. See the installation instructions in the *AnyConnect for Android User Guide* to determine which package applies to your device.

- ACE+
- ACE II
- Conquer 4G
- Galaxy Appeal
- Galaxy Beam
- Galaxy Exhilarate
- Galaxy Mini
- Galaxy Note
- Galaxy Note II
- Galaxy NoteIII
- Galaxy Tab 7 (WiFi only)
- Galaxy Tab 7.0 Plus & 7.7
- Galaxy Tab 8.9
- Galaxy Tab 10.1
- Galaxy Tab 2 7.0
- Galaxy Tab 2 10.1
- Galaxy W
- Galaxy Xcover
- Galaxy Y Pro
- Illusion

- Galaxy Note 10.1
- Galaxy Rush
- Galaxy S
- Galaxy S II
- Galaxy S III
- Galaxy S 4
- Galaxy Stellar
- Infuse
- Rugby
- Stratosphere
- Stratosphere II
- Transform Ultra

Note Samsung rebrands devices in these product lines for each mobile service provider.

HTC Devices

HTC AnyConnect Release 3.0.x supports the HTC product lines listed at http://www.htcpro.com/enterprise/VPN. These devices must be running the minimum software required as shown in the table. Go to **Settings > About phone > Software information > Software number** to determine the software number running on your device.

Note

- Currently, HTC devices running Android 4.3 and later should use the Cisco AnyConnect ICS+ package. Uninstall HTC AnyConnect before installing this package.
- Currently, all AT&T HTC devices should use the Cisco AnyConnect ICS+ package. Uninstall HTC AnyConnect before installing this package.
- The HTC Raider, also know as the HTC Holiday, does not work with Cisco AnyConnect. Cisco and HTC are working to address this issue.

Kindle Devices

Cisco AnyConnect (Kindle Tablet Edition) Release 3.0.x is available from Amazon for the following devices:

- Kindle Fire HD
- New Kindle Fire
- Kindle Fire HDX

Anyconnect for Kindle is supported by the Android VPN Framework and is equivalent in functionality to the AnyConnect ICS+ package.

AnyConnect for Android 4.0 Devices and later (ICS+)

AnyConnect ICS+ Release 3.0.x offers VPN connectivity supported by the Android VPN Framework (AVF) in Android 4.0 (Ice Cream Sandwich) or later. This package can be used on any Android device that is running ICS or later.

The AVF provides only basic VPN connectivity. The AnyConnect AVF client, dependent upon these basic VPN capabilities, is unable to provide the full set of VPN features available in the brand-specific packages.

Note Cisco recommends the AnyConnect AVF client for unsupported devices running Android 4.0 or later. Supported devices should use the brand-specific AnyConnect client regardless of the version of the Android operating system.

AnyConnect for Rooted Devices

Cisco provides Rooted AnyConnect Release 3.0.x for rooted Android mobile devices running Android 2.1 or later, for preview and testing purposes only.

Cisco does not support this client, but it works on most rooted devices running 2.1or later. If you encounter issues, please report them to android-mobile-feedback@cisco.com, and we will make our best effort to resolve them.

Both a tun.ko module and iptables are required. AnyConnect displays an error message, informing you about what is missing when you attempt to establish a VPN connection. If the tun.ko module is missing, obtain or build it for your corresponding device kernel and place it in the `/data/local/kernel_modules/` directory.

Caution Rooting your device voids your device warranty. Cisco does not support rooted devices, nor do we provide instructions to root your device. If you choose to root your device, you do so at your own risk.

AnyConnect Features Supported on Android Devices

Android Brand-Specific AnyConnect

For Samsung, HTC and Motorola supported and qualified devices, Cisco provides brand-specific AnyConnect packages that offer a full-featured VPN experience across Android operating systems. These brand-specific AnyConnect packages are provided in partnership with device vendors and are the preferred AnyConnect clients for these devices.

Android AnyConnect Plus

For some Motorola supported and qualified devices (released after May 2012) Cisco provides this non-vendor specific packages that offers a full featured VPN experience that is equivalent in functionality to the brand-specific packages.

Android VPN Framework AnyConnect

For other Android devices that are unable to use the brand-specific AnyConnect package or AnyConnect Plus, Cisco provides an AnyConnect client that offers VPN connectivity supported by the Android VPN Framework (AVF) introduced in Android 4.0 (Ice Cream Sandwich). AVF provides only basic VPN connectivity. The AnyConnect AVF client, dependent upon these basic VPN capabilities, is unable to provide the full set of VPN features available in the device-specific packages. These discrepancies are shown in the table. Kinde devices use this package also.

Android Rooted AnyConnect

Cisco also provides an AnyConnect package for rooted Android devices that is equivalent in functionality to the brand-specific packages. This package works on most rooted devices that are running Android 2.1 or later. Brand-specific AnyConnect packages do not work on rooted devices; therefore you must use the rooted version of AnyConnect on rooted devices.

Table 13-1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunneling	TLS/DTLS	Yes	Yes
	IPsec IKEv2	Yes	Yes
	IKEv2 - NAT-T	Yes	Yes
	IKEv2 - raw ESP	Yes	Yes
	Suite B support	Yes (IPsec only)	Yes (IPsec only)
	TLS compression	Yes	Yes
	Dead peer detection	Yes	Yes
	Tunnel keepalive	Yes	Yes
Tunnel Establishment	Optimal Gateway Selection	No	No
	VPN load balancing	Yes	Yes
	Backup server list	Yes	Yes
	Activate a connection on profile import	Yes	Yes
	URI connect credential pre-fill	Yes	Yes

Table 13-1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunnel Policy	All/full tunnel	Yes	Yes
	Split tunnel (split include)	Yes	Yes
	Local LAN (split exclude)	Yes	No
	Split-DNS	Yes	Will work with split include.
	Always-on enforcement	No	No
	Auto Reconnect	Yes, regardless of the Auto Reconnect profile specification, AnyConnect Mobile always attempts to maintain the VPN as users move between 3G and WiFi networks.	
	VPN on-demand (triggered by destination)	No	No
	VPN on-demand (triggered by application)	No	No
	Trusted Network Detection (TND)	Yes	No
	Rekey	Yes	Yes
	ASA group profile support	Yes, limited	Yes, limited
	IPv4 public transport	Yes	Yes
	IPv6 public transport	No	No
	IPv4 over IPv4 tunnel	Yes	Yes
	IPv6 over IPv4 tunnel	Yes	Yes
	Default domain	Yes	Yes
	DNS server configuration	Yes	Yes
	Private-side proxy support	No	No, WiFi proxies are disabled when the VPN is established.
	Pre-login banner	Yes	Yes
	Post-login banner	Yes	Yes
	Scripting	No	No
	Reconfigure VPN	Yes	Yes

Table 13-1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Tunnel Security	Network change monitoring	Yes	Yes
	Shim intercept/filtering	No	No
	Embedded firewall rules	No	No
	Filter support (iptables)	Yes	No
Authentication	Manual certificate import (get certificate)	Yes	Yes
	SCEP enrollment	Yes	Yes
	SCEP proxy	Yes	Yes
	Automatic certificate selection	Yes	Yes
	Manual certificate selection	Yes	Yes
	Non-exportable certificate	N/A	N/A
	Smart card support	No	No
	Username and password	Yes	Yes
	Tokens/challenge	Yes	Yes
	Double authentication	Yes	Yes
	Group selection	Yes	Yes
	Credential prefill	Yes	Yes
	Save password	No	No

Table 13-1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
User interface	Standalone GUI	Yes	Yes
	Native OS GUI	No	No
	CLI	No	No
	API	Yes, Java not C++	Yes, Java not C++
	UI customization	Yes (themes)	Yes (themes)
	UI localization	Yes	Yes
	User preferences	Yes	Yes
	Certificate confirmation reasons	Yes	Yes
	Home screen widgets for one-click VPN access	Yes	Yes
	Paused icon when connection suspended for TND	Yes	Yes
	Hide AnyConnect icon when idle	Yes	Yes
	Launch on startup of mobile device	Yes	Yes
	Exit AnyConnect	Yes	Yes
	User certificate management	Yes	Yes
	User profile management	Yes	Yes
	User localization management	Yes	Yes
Deployment	WebLaunch (browser-initiated)	No	No
	Web redirect to application store	No	No
	Standalone installer	No	No
	Preinstalled by OEM	No	No
	Install or upgrade from the ASA	No	No
	Install or upgrade from Android Market	Yes	Yes
	Pre-packaged localization for some languages	Yes	Yes

Table 13-1 AnyConnect Android Features

AnyConnect Feature	Subfeature	Android Brand-Specific, Anyconnect Plus, & Rooted AnyConnect Packages	Android VPN Framework & Kindle AnyConnect Packages
Configuration	XML Client Profile import on connect.	Yes	Yes
	URI handler support for importing XML Client Profile	Yes	Yes
	User-configured connection entries	Yes	Yes
Posture Assessment	Device check (pin lock, encryption, etc.)	No	No
	Running or installed apps	No	No
	Serial number or unique ID check	No	No
	Mobile Posture	Yes	Yes
URI Handling	Add connection entry	Yes	Yes
	Connect to a VPN	Yes	Yes
	Credential pre-fill on connect	Yes	Yes
	Disconnect VPN	Yes	Yes
	Import certificate	Yes	Yes
	Import localization data	Yes	Yes
	Import XML client profile	Yes	Yes
	External (user) control of URI commands	Yes	Yes
Troubleshooting	Statistics	Yes	Yes
	Logging	Yes	Yes
	Email statistics, log messages, and system information	Yes	Yes
	Direct feedback to Cisco	Yes	Yes
	DART	No	No
Certifications	FIPS 140-2 Level 1	Yes	Yes
	Common criteria	No	No

Installing and Upgrading AnyConnect on Android Devices

AnyConnect for Android devices is available from the Android Market only. AnyConnect cannot be downloaded from the ASA. For instructions on downloading the appropriate AnyConnect package for an Android device, see the *Android User Guide for Cisco AnyConnect Secure Mobility Client*.

The AnyConnect UI on Android Devices

For a description of the AnyConnect app, its user interface, and all activities, see the *Android User Guide for Cisco AnyConnect Secure Mobility Client*.

Android Specific Considerations

Android Mobile Posture Device ID Generation

Note The algorithm to generate mobile posture Device IDs on Android changed in AnyConnect 3.0. If you have DAP rules defined that use Device IDs generated from previous versions of AnyConnect, they will have to be updated to bind to the newly generated Device IDs.

AnyConnect 3.0 generates a unique 40-byte device ID at installation time. The generated device ID is based on the Android ID and one or both of the following values if they are available at installation time:

- MEID/IMEI (Mobile Equipment Identifier / International Mobile Equipment Identity)
- MAC-ADDRESS (MAC address of the device)

The device ID is generated depending on the availability of these values:

Available values	Generation Algorithm
If both values are retrievable at installation time:	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI + MAC-ADDRESS))`
If only the MEID/IMEI is retrievable at installation time:	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI))`
If only the MAC-ADDRESS is retrievable at installation time	`device-ID = bytesToHexString(SHA1(Android-ID + MAC-ADDRESS))`

Where:

- The Android-ID is set as follows:

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

- And the `bytesToHexString` function is:

```
String bytesToHexString(byte[] sha1rawbytes)
{
     String hashHex = null;
      if (sha1rawbytes != null)
     {
         StringBuffer sb = new StringBuffer(sha1rawbytes.length * 2);
         for (int i = 0; i < sha1rawbytes.length; i++)
         {
             String s = Integer.toHexString(0xFF & sha1rawbytes[i]).toUpperCase();
             if (s.length() < 2)
             {
                 sb.append("0");
             }
             sb.append(s);
         }
         hashHex = sb.toString();
```

```
        }
         return hashHex;
    }
```

Note If neither the MEID/IMEI nor MAC-ADDRESS values are retrievable at installation time, a random number is used with the `Android-ID` to generate the device-ID.

Generated device IDs can be viewed after the initial AnyConnect 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.

In AnyConnect 2.5, the MEID/IMEI is used as the device ID. If the MEID/IMEI is not available, AnyConnect will try to use the MAC-ADDRESS. If this value is also not available, AnyConnect installation fails.

AnyConnect Operation and Options

VPN Connections

To initiate a VPN connection, the user selects a connection entry on the mobile device identifying the server address of the secure gateway, as well as other connection attributes. The server address is the fully qualified domain name or IP address of the secure gateway, including the tunnel group URL if required. 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 user guide for procedures to configure a connection entry on a mobile device.

- Defined by the Anyconnect VPN Client Profile.

  The AnyConnect VPN Client Profile 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 as well as other connection attributes, policies and constraints. For details, see the "Configuring Mobile Device Connections in the AnyConnect Profile" section and the "Deploying the AnyConnect Profile" section.

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

  See the "Using the URI Handler to Generate a VPN Connection Entry" section to provide this kind of connection entry configuration to your users.

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.

- For AAA-based authentication tunnel groups for mobile devices, the tunnel group 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.

Client Certificates

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:

- Added after the user clicks a link provided by the administrator to import a certificate. See Using the URI Handler to Import Certificates to provide this kind certificate deployment to your users.
- Using SCEP. See the "Configuring Certificate Enrollment using SCEP" section in the "Configuring VPN Access" chapter of the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* manual for administrator configuration.
- Imported manually by the user. See the appropriate user guide procedures to import certificates to your mobile device.

Server Certificates

A valid, trusted server certificate configured on the secure gateway provides an easy and safe VPN connection for the user.

AnyConnect on mobile devices provides improved security protection when accessing a secure gateway by blocking the VPN connection if the certificate presented by the secure gateway is invalid or untrusted, or both.

A new **Block Untrusted Servers** application setting determines how AnyConnect blocks connections 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.

AnyConnect uses the digital certificate received from the server to verify its identify. If the 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.

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 nonblocking **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.

  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, having a valid, 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.

Deploying the AnyConnect Profile

After creating a VPN client profile with mobile device connection entries, administrators must choose how to distribute the client profile in one of the following ways:

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

  See the "Deploying the AnyConnect Profile" section in the "Configuring VPN Access" chapter of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for instructions on how to import the VPN client profile to the ASA and associate it with a group policy.
- Providing the user with an AnyConnect URI link to import a client profile.

  See the "Using the URI Handler to Import a VPN Client Profile " section for details.
- Importing an AnyConnect profile using Profile Management on the mobile device.

  See the appropriate mobile device user guide for device-specific procedures.

When administrators create and distribute these profiles, end users cannot modify the defined connection entries. End users can modify only the connection entries that they create manually.

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

- The user manually imports a profile. The imported profile replaces the current profile.
- Upon startup of an automatic or manual VPN connection, the new connection's profile replaces the current profile.
- The user manually deletes the current profile, the current profile is removed, and all connection entries defined in this profile are deleted.

Configuring Mobile Device Connections in the AnyConnect Profile

Step 1 Refer to Configuring VPN Access for the configuration procedures that are common to desktop and mobile endpoints taking into account the following exceptions:

Profile attribute	Exception
Auto Reconnect	Regardless of your Auto Reconnect specification, AnyConnect Mobile always attempts to ReconnectAfterResume.

Step 2 Configure the mobile-specific attributes explained in this chapter.

Downloading the AnyConnect Profile Editor

Use the AnyConnect Profile Editor Release 3.0.1047 or later to create a VPN client profile that includes host connection entries for mobile devices. The Profile Editor is a standalone tool. To download the Profile Editor:

Step 1 Connect to the AnyConnect Secure Mobility Client page on www.cisco.com and click **Download Software**.

Step 2 Expand the **All Releases** and **3.0** directories and select **3.0.1047** or a later version of AnyConnect.

Step 3 In the column on the right, look for a file with the naming convention **anyconnect-profileeditor-win-<*version*>-k9.exe**. If you were downloading the AnyConnect Profile Editor released with AnyConnect 3.0.1047, you would find **anyconnect-profileeditor-win-3.0.1047-k9.exe**.

Step 4 Click **Download now** and follow the instructions on the site to complete the download process.

Mobile-Specific Attributes

Certificate Authentication

The **Certificate Authentication** policy attribute associated with a connection entry specifies how certificates are handled for this connection. Valid values are Automatic, Manual, or Disabled:

- **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 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 will be 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.

Activate on Import

Activate on Import, or **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 Network Roaming

This attribute applies to Apple iOS device connections only.

Network Roaming, or **Reconnect when roaming between 3G/Wifi networks**, is enabled by default. When enabled, 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 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.

Apple iOS Connect On Demand

This attributes applies to Apple iOS device connections only.

The Apple iOS Connect On Demand feature lets an application, such as Safari, initiate a VPN connection. Apple iOS evaluates the domain requested by the application against the strings in the domain lists within the *active* connection entry—the entry with the check mark next to it.

When a VPN connection is initiated via iOS's Connect on Demand, iOS disconnects the tunnel if the tunnel is inactive (no traffic through the tunnel) for a particular time interval. See Apple's VPN On Demand documentation for more information.

You define the domain lists that Apple iOS evaluates.

- **Never Connect**—Apple iOS evaluates domain requests for a match against the contents of this list first. If a string in this list matches the domain, Apple iOS ignores the domain request. 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`.

Note If you or the user enables Connect On Demand, AnyConnect adds the server address in the VPN configuration to the Never Connect list to prevent VPN connections from starting when you use a web browser to connect to a secure gateway. Leaving the rule in place does not have an adverse effect on Connect On Demand.

- **Always Connect**—Apple iOS evaluates domain requests for a match against the contents of this list next. If a string in this list matches the domain, Apple iOS attempts to establish a VPN connection. The most common use case for this list is to obtain brief access to internal resources. An example value is `email.example.com`.

Note Apple iOS 7 no longer supports *Always Connect* domains. When running AnyConnect on Apple iOS 7 devices, any domains listed as *Always Connect* will be treated as *Connect if Needed* domains.

- **Connect if Needed**—Apple iOS 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. 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`.

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.
  - A DNS lookup failed, and Apple iOS matches a string in the Connect if Needed list to the domain request.

The Connect On Demand rules support only domain names, not IP addresses; however, the domain names specified within the rules may be partial or whole domain strings.

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

Also see Configuring Connect-On-Demand Rules in the iPad or iPhone user guide or Using the URI Handler to Generate a VPN Connection Entry later in this document for additional information and instructions.

Configuring Mobile Specific Attributes

Step 1 In the VPN Client Profile, select **Server List**.

Step 2 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.

Step 3 In the Server List Entry dialog box, check **Additional mobile-only settings** and click **Edit**.

Step 4 In the **Apple iOS / Android Settings** area, configure the following attributes for devices that are running Apple iOS or Android operating systems:

a. Choose the **Certificate Authentication** type: **Automatic, Manual**, or **Disabled**.

b. Check or uncheck the **Make this Server List Entry active when profile is imported** checkbox as desired.

Step 5 In the **Apple iOS Only Settings** area, configure the following attributes for devices that are running Apple iOS operating systems only:

a. Check or uncheck the **Reconnect when roaming between 3G/Wifi networks** checkbox as desired.

b. Check or uncheck the **Connect on Demand** checkbox as desired.

Connect on Demand is enabled if the Certificate Authentication field is set to **Manual** or **Automatic**. If the Certificate Authentication field is set to **Disabled**, this checkbox is grayed out. 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 checkbox is grayed out.

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.

c. In the **Match Domain or Host** field, 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.

d. In the **On Demand Action** field, specify one of the following actions when a user attempts to connect to the domain or host defined in the previous step: **Always connect, Connect if needed**, or **Never connect.**

e. Click **Add**.

The rule is displayed in the rules list below.

Step 6 Click **OK**.

Recommended ASA Configurations

Step 1 Refer to General VPN Setup in the "*Cisco ASA Series VPN ASDM Configuration Guide*" for the configuration procedures that are common to desktop and mobile endpoints taking into account the following exceptions:

Attribute	ASDM Location	Exception
Homepage URL	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add** or **Edit > Advanced > AnyConnect Client > Customization**.	AnyConnect Mobile ignores the Homepage 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**	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".

Step 2 Configure the following attributes as explained in this chapter.

- Setting Dead Peer Detection, page 13-23
- Disabling Keepalive Messages, page 13-23
- Configuring Mobile Posture, page 13-24

Setting Dead Peer Detection

Server-side dead peer detection should be switched off 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, when the quality of transmission is too low or unavailable to continue sending traffic over the VPN connection.

Disabling Keepalive Messages

We recommend disabling keepalive messages to conserve the battery life of mobile devices, especially if client-side dead peer detection is enabled. To access the Keepalive Messages parameter in ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add** or **Edit > Advanced > AnyConnect Client**.

Configuring Mobile Posture

ASAs that are running release 8.2(5+) and 8.4(2) feature AnyConnect Mobile Posture for mobile device detection. Mobile Posture lets you accept, deny, or restrict mobile connections. It requires an AnyConnect Premium and AnyConnect Mobile license.

Configure dynamic access policies (DAPs) based on the following attributes of a mobile device:

- Client Version—The AnyConnect client version.
- Platform—The operating system including Android and Apple iOS.
- Platform Version—The operating system version number.
- Device Type—The mobile device type, such as iPad or Samsung GT-I9000.
- Device Unique ID—The mobile device's unique ID. See "Android Mobile Posture Device ID Generation" for important information about device IDs on the Android platform.

For complete instructions, see the "Adding Mobile Posture Attributes to a DAP" section in *Cisco 5500 Series Configuration Guide using ASDM, 6.4* or see the "Add/Edit Endpoint Attributes" section in *Cisco Security Appliance Configuration Guide using ASDM, 6.2*.

Restricting Mobile Devices from Establishing VPN Connections

If an AnyConnect Mobile license is not activated on an ASA, it automatically denies connection attempts from mobile devices.

An ASA activated with an AnyConnect Mobile license supports mobile device VPN connections. By default, any user who authenticates can log in from a mobile device that is running AnyConnect.

Configure an ASA to prevent these connections; the configuration depends on the ASA release:

- On ASAs that are running release 8.2(5+) and 8.4(2), AnyConnect Mobile Posture is used for mobile device detection.
- For earlier releases, ASA Releases 8.0(4) through 8.2(4), and 8.4(1), a different DAP specification, Cisco Secure Desktop, and an AnyConnect Premium license are required.

To configure an ASA to prevent VPN mobile device connections, add a dynamic access policy as follows:

Procedure for Using Mobile Posture

Step 1 Establish an ASDM session with the ASA.

Step 2 Choose **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add** or **Edit**.

Step 3 **Choose Add** to the right of the Endpoint Attributes table.

Step 4 Change the Endpoint Attribute Type to **AnyConnect**.

Step 5 Change the Platform to **Android** or **Apple iOS**.

Step 6 Enter the model name into the Device Type field.

ASDM displays a drop-down list next to Device Type; however, the drop-down options are not supported.

Step 7 Add one endpoint attribute to a DAP for each device to assign a policy to it.

Step 8 Use the tabs in the Access/Authorization Policy Attributes section of the Add or Edit Dynamic Access Policy window to continue, terminate, or impose restrictions on Android connections.

Procedure for Earlier ASA Releases

Step 1 Establish an ASDM session with the ASA.

Step 2 Choose **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add**.

Step 3 Name the policy, for example: `Deny Apple iOS`, or `Deny Android`.

Step 4 Click **Advanced**.

Step 5 Enter one of the following into the Logical Expressions text box:

```
EVAL(endpoint.os.version, "EQ", "Apple Plugin", "string")
```

or

```
EVAL(endpoint.os.version, "EQ", "Android", "string")
```

Step 6 Use the tabs in the Access/Authorization Policy Attributes section of the Add or Edit Dynamic Access Policy window to continue, terminate, or impose restrictions on Android connections.

Step 7 Click **OK** and **Apply**.

FIPS and Suite B Cryptography

AnyConnect 3.0 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.

In AnyConnect 3.0 for mobile devices, 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 settings. When FIPS Mode is disabled, AnyConnect also accepts non-FIPS cryptography algorithms for VPN connections.

AnyConnect 3.0 for mobile devices includes the following Suite B algorithms:

- AES-GCM support (128-, 192-, and 256-bit keys) for symmetric encryption and integrity
  - IKEv2 payload encryption and authentication (AES-GCM only)
  - ESP packet encryption and authentication
- SHA-2 (SHA with 256/384/512 bits) support for hashing
  - IKEv2 payload authentication
  - ESP packet authentication
- ECDH support for key exchange

  - Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS
- ECDSA support (256-, 384-, 512-bit elliptic curves) for digital signature, asymmetric encryption, and authentication
  - IKEv2 user authentication and server certificate verification
- Other cipher suite dependencies between algorithms promote support for the following:
  - Diffie-Hellman Groups 14 and 24 for IKEv2
  - RSA certificates with 4096 bit keys for DTLS and IKEv2

Requirements

- FIPS and/or Suite B support is required on the secure gateway. Cisco provides Suite B capability on the ASA version 9.0 and later, and FIPS capability on the ASA version 8.4.1 and later.
- An AnyConnect Premium license is required for FIPS or Suite B remote access connections to the ASA.

Note

- At AnyConnect 3.0 for Mobile release time, Apple iOS does not support ECDSA certificates. This problem is being addressed by Apple. Once fixed, the following requirement will apply:

  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.
- VPN connections require server certificates that contain Key Usage attributes of Digital Signature and Key Encipherment, as well as an Enhanced Key Usage attribute of Server Authentication, or IKE Intermediate for IPsec. Server certificates not containing a Key Usage are considered invalid for all Key Usages. Similarly, a server certificate not containing an Enhanced Key Usage is considered invalid for all Enhanced Key Usages.

Guidelines and Limitations

- Suite B is available only for IKEv2/IPsec.
- A device that is running in FIPS mode is not compatible with using SCEP to provide mobile users with digital certificates, proxy method or legacy method. Plan your deployment accordingly.
- No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.
- ECDSA certificates must have a Digest strength equal to or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
- VPN connections perform name verification on server certificates. The following rules are applied to name verification:
  - If a Subject Alternative Name extension is present with relevant attributes, name verification uses only the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates and also 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 uses 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 must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.

Localizing AnyConnect Interface and Messages

Starting in release 2.5, AnyConnect Secure Mobility Client for Android and Apple iOS supports localization, adapting the AnyConnect user interface and messages to the user's locale.

Pre-packaged Localization

The following language translations are included in the AnyConnect package:

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

Localization data for these languages is installed on the mobile device when AnyConnect is installed. The displayed language is determined by the locale specified on your mobile device. AnyConnect uses the language specification, then the region specification, to determine the best match. For example, after installation, a French-Switzerland (fr-ch) locale setting results in a French-Canadian (fr-ca) display. AnyConnect UIs and messages are translated as soon as AnyConnect starts.

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. See Localizing the AnyConnect GUI 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.

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 should download this updated version.

Initially, the AnyConnect user interface and messages are presented to the user in the installed language. When the end 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.

If the ASA does not contain localization data for the device's locale, the installed localization data from the AnyConnect application package continues to be used.

Procedure

Step 1 Begin at the **Select a Product** page.

Step 2 Select **Products > Security > Virtual Private Networks (VPN) > Cisco VPN Clients > Cisco AnyConnect Secure Mobility Client**.

Step 3 Expand the **All Releases** folder in the release folder tree, expand **3.0**, and then open the folder of the latest AnyConnect 3.0 release.

Step 4 In the list of downloadable files, find **anyconnect.po** and click **Download Now**.

Step 5 Follow the prompts to download the file.

Additional Localization

An additional way to get localization data onto a user's device is for the administrator to provide the user with an AnyConnect URI for importing localization data. For example:

```
anyconnect://import?type=localization&host=asa.example.com&lang=ja-jp
```

See Using the URI Handler to Localize the AnyConnect UI and Messages for a full explanation.

User Localization Management

Mobile device users 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 pre-loaded localization data from the AnyConnect package and deletes all imported localization data.

Using the URI Handler to Automate AnyConnect Actions

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. You use URIs to:

- Generate VPN connection entries.
- Establish a connection to a VPN and disconnect from a VPN.
- Import localization files, certificates, and AnyConnect profiles.

URI handling in the AnyConnect application is Disabled by default. Mobile device users allow this functionality by setting the AnyConnect Application Preference External Control to Enable or Prompt. Enabling external control allows all URI commands without user interaction.

The user is notified of URI activity and allows or disallows it at request time by choosing Prompt**.** 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.

Note Android users cannot enter these URIs into the address bar of the web browser. The user needs to access these URIs from a remote web server or, depending on their e-mail client, they may be able to click a link in e-mail.

Using the URI Handler to Generate a VPN Connection Entry

Use the AnyConnect URI handler **create** action to simplify the generation of an AnyConnect connection entry for users.

Insert 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.

Use the following URI syntax to add an AnyConnect connection entry to the endpoint configuration:

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

Examples:

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

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

To match a space, enter **%20**. For example, to match a connection entry named `Example Connection 1`, enter **Example%20Connection%201**.

The create action requires the `host` parameter, 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`.

Create parameter options:

- **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.
- **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).

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

  Note 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.

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

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

  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.

- **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` and `certcommonname` parameters)—Determines whether applications, such as Safari, can start VPN connections.
  - **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.
  - **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.

```
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 email.1example.com email.example1.com email.example.org
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 anytext.1example.org anytext.example1.org
Any domain name ending with the text you specify.	Enter the end of the domain name to be matched.	example.net	anytext.anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

Using the URI Handler to Establish a VPN Connection

Embed connection information in URIs and provide these URIs to users to easily establish VPN connections. Create URI strings that perform the following tasks:

- Provide the Connection Name and Hostname in a URI
- Provide Connection Information and Prefill a Username and Password in a URI
- Provide Connection Information and Prefill Usernames and Passwords for Double Authentication
- Provide Connection Information, Prefill a Username and Password, and Specify a Connection Profile Alias

See also, Connect Parameter and Syntax Descriptions.

Note Specifying a password when establishing a VPN connection using a URI should be used only in conjunction with a One Time Password (OTP) infrastructure.

Provide the Connection Name and Hostname in a URI

Use either syntax expression to insert the **name** and **host** parameter in the connect action:

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]
anyconnect:[//]connect[/]?name=Description&host=ServerAddress
```

Examples of Completed URIs

```
anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example&host=hr.example.com
```

See Connect Parameter and Syntax Descriptions for expanded descriptions of the parameters and additional syntax requirements.

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**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]
[**&onsuccess**=URL**&onerror**=URL]

anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress*[**&onsuccess**=URL**&onerror**=URL]

Examples

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

In addition, the **anyconnect://close** command is used in the onsuccess or onerror parameter to close the AnyConnect GUI:

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

See Connect Parameter and Syntax Descriptions for expanded descriptions of the parameters and additional syntax requirements.

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

Use either syntax to specify the prefilled username and prefilled password parameters in addition to name and host parameter in the connect action:

anyconnect:[**//**]**connect**[**/**]**?**[**name=**Description|**host=**ServerAddress]**&prefill_username**=username**&prefill_password**=password

anyconnect:[**//**]**connect**[**/**]**?name=**Description**&host=**ServerAddress**&prefill_username**=username**&prefill_password**=password

Examples of Completed URIs

anyconnect://connect/?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1

anyconnect:connect?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password**=password1

See Connect Parameter and Syntax Descriptions for expanded descriptions of the parameters and additional syntax requirements.

Provide Connection Information and Prefill Usernames and Passwords for Double Authentication

Use either syntax to specify the prefilled primary and secondary usernames and prefilled passwords in addition to the name and host parameters in the connect action:

anyconnect:[**//**]**connect**[**/**]**?**[**name=**Description|**host=**ServerAddress]**&prefill_username**=username**&prefill_password**=password**&prefill_secondary_username**=username2**&prefill_secondary_password=**password2

anyconnect:[**//**]**connect**[**/**]**?name=**Description**&host=**ServerAddress**&prefill_username**=username**&prefill_password**=password**&prefill_secondary_username**=username2**&prefill_secondary_password=**password2

Examples of Completed URIs

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

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

See Connect Parameter and Syntax Descriptions for expanded descriptions of the parameters and additional syntax requirements.

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

This example adds a connection profile alias to a URI that provides a prefilled username and prefilled password in addition to name and host parameter for the connect action:

anyconnect:[**//**]**connect**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]**&prefill_username=***username*&**prefill_password=***password***&prefill_group_list=**10.%20Single%20Authentication

anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress***&prefill_username=***username*&**prefill_password=***password***&prefill_group_list=**10.%20Single%20Authentication

Examples of Completed URIs

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

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

See Connect Parameter and Syntax Descriptions for expanded descriptions of the parameters and additional syntax requirements.

Connect Parameter and Syntax Descriptions

The connect action requires either the `name` or the `host` parameters, but allows both. 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.

These are descriptions of the connect parameter options:

- **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. The value is case-sensitive; AnyConnect does not match this field if the case of the letters in the statement differs from that in the connection entries.
- **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.

- **onsuccess**—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.
- **onerror**—Specify the URL to be opened when this connection transitions into the disconnected state, or use the **anyconnect:close** command to close the AnyConnect GUI.
- **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 prefills it in connection prompts.

Note The prefill_password 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 prefills 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**.

Using the URI Handler to Disconnect from a VPN

Use the following syntax to insert the disconnect action:

anyconnect:[**//**]**disconnect**[**/**]

Example:

anyconnect:disconnect

The slashes are optional. The disconnect action takes no parameters.

Using the URI Handler to Localize the AnyConnect UI and Messages

Note You must have Apple iOS 5, or later, installed on an Apple iOS device to use the URI handler to localize AnyConnect UI and messages.

Use the following syntax to use the **import** command in a URI:

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

Example:

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

The slashes are optional. The import action requires all parameters. The **type**, **lang**, and **host** parameters are defined below:

- **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.

Using the URI Handler to Import Certificates

The AnyConnect client authenticates itself to the ASA using a PKCS12 encoded certificate that has been installed on the endpoint. Use the URI handler **import** command to import a PKCS12 encoded certificate bundle to the endpoint.

Use the following syntax to import a PKCS12 certificate from a URL:

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

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

The slashes in the beginnings of the URI are optional.

To match a space, enter **%20**. For example, to match a string named `Example Connection 1`, enter Example**%20**Connection**%20**1.

To match a colon in a URI, use **%3A**. To match a forward slash in a URI, use **%2F**. For example, to match http://example.cisco.com/CertName.p12 enter `http%3A%2F%2Fexample.cisco.com%2FCertName.p12.`

The following describes the import parameter options:

- **type**—Only pkcs12 certificate type is supported.
- **uri**—URL Encoded identifier where the certificate is found. We support “http”, “https”, and “ftp”. In the URI, **%3A** represents a colon (:), **%2F** represents a forward slash (/), and **%40** represents an ampersand (@).

HTML Hyperlink Examples

To add the URI to an HTML page, you need to make it part of a hyperlink. Here are examples that show how to use the URI in an HTML hyperlink. The part of the example in bold is the URI.

HTTP Example

```
<p>
<a href="anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12>
click here to import certificate using http</a>
</p>
```

FTP Example

```
<p><ahref="anyconnect://import?type=pkcs12
&uri=ftp%3A%2F%2FAdministrator%3Apassword%40192.168.10.20%2Fcerts%2FCertName.pfx">click
here to import certificate using ftp </a>
</p>
```

Secure Digital Card Example

```
<p><a href="anyconnect://import?type=pkcs12
&uri=file%3A%2F%2Fsdcard%2CertName.pfx">click here to import certificate from sdcard
on mobile device</a>
</p>
```

Using the URI Handler to Import a VPN Client Profile

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

Use the following syntax to use this **import** command in a URI:

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

Example:

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

The slashes are optional. The import action requires the `uri` parameter.

Troubleshooting

Enable logging on the mobile device and follow the troubleshooting instructions in the appropriate user guide:

- *iPhone User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x*
- *iPad User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x*
- *Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 3.0.x*

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

- Determine whether the same problem occurs with the desktop client.
- Ensure that the AnyConnect Mobile license is installed on the ASAs.
- If certificate authentication fails, ensure that the correct certificate has been selected. Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage. 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 will not be used for authentication if it does not match the filtering rules in the profile. If your authentication mechanism uses any associated accounting policy to an ASA, verify that the user can successfully authenticate. If problems persist, enable logging on the client and enable debug logging on the ASA.
- 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. For details, refer to the release-apporpriate ASA administrator guide.

Apple iOS Specific Troubleshooting

- If the VPN connection is not restored after the device wakes up, ensure that Network Roaming is enabled.
- If Apple iOS prompts you to start a connection using the AnyConnect application when certificate authentication and the Apple iOS Connect On Demand feature are configured for the connection, configure the connection to use a Group URL. Both a Group URL and certificate-only authentication are requirements for Connect on Demand.