AnyConnect on Mobile Devices

AnyConnect on mobile devices is similar to AnyConnect on Windows, macOS, 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
- Chromebook
- Windows Phone

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

AnyConnect mobile apps contain the core VPN client only. They do not include other AnyConnect modules such as the Network Access Manager or Posture. 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 31 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 29.

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 APIs 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 for details.
- Added after the user clicks a link provided by the administrator to import a certificate.

  See Import Certificates, on page 36 to provide this kind of certificate deployment to your users.

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 translated when AnyConnect starts.

Downloaded Localization

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

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

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

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

More Ways to Provide Localization on Mobile Devices

Localize the AnyConnect UI and Messages, on page 37 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.

VPN Authentication Using SAML

Follow these guidelines when using SAML:

- If you are using always-on VPN in failover mode, external SAML IdP is not supported (however, with internal SAML IdP, the ASA proxies all traffic to IdP and is supported)
- (Mobile only) Single logout is not supported.
- 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.
- 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) if you want users to re-authenticate with the Identity Provider (IdP) every time they establish a VPN session via SAML.

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.

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 HostScan 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 Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.x for Android for features and updates by release.

Refer to the AnyConnect Mobile Platforms and Feature Guide for features and devices supported by this release.

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 macOS 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.
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.

Manifest Permission	Description
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the broadcast after the system finishes booting.

Configure AnyConnect for Android on Chromebooks

Google recently announced a deprecation of all native Chromebook applications. This documentation is designed to help you migrate from the native Chromebook applications and help you with configuring AnyConnect for Android on Chromebooks.

You can access this Google documentation for additional information.

Procedure

Step 1 Sign in to your Google administrator console using an administrator account.

Step 2 From the Google Admin console Home page, go to **Devices** > **Chrome**.

Step 3 Click **Apps & entensions** > **Users & browsers**.

Step 4 Leave the top organizational unit selected if you want to apply the setting to everyone. Otherwise, apply a child organizational unit.

Step 5 Click **Add** > **Add from Google Play**.

Step 6 Choose AnyConnect as the application you'd like to manage.

Step 7 The only managed configuration is the JSON file, which you can paste in or upload by clicking the upload icon.

What to do next

Keys are defined in the .apk package file for Android. The only required field is vpn_connection_host, but if you are pushing an AnyConnect XML profile, the JSON key is vpn_connection_profile. AnyConnect supports all of the managed configuration keys listed in the next section.

Managed Configuration Keys Supported by AnyConnect

Managed Restrictions (Root)

vpn_connection_name

- Title—Connection name
- Type—String
- Description—User friendly name (for display only). If not set, defaults to the host.

vpn_connection_host

- Title—Host
- Type—string
- Description—URL to the headend. This field is required.

vpn_connection_profile

- Title—protocol
- Type—choice
- Possible Values—SSL | IPsec
- Description—VPN tunnel protocol (SSL or IPsec). Defaults to SSL

vpn_connection_ipsec_auth_mode

- Title—IPsec Authentication Mode
- Type—choice
- Description—(Optional) Authentication mode to use if tunnel protocol is IPsec. Defaults to EAP-AnyConnect

vpn_connection_ipsec_ike_identity

- Title—IKE identity
- Type—string
- Description—(Optional) Only applicable if IPsec authentication mode is EAP_GTC, EAP-Md5, or EAP-MSCHAPv2

vpn_connection_ipsec_ike_identity

- Title—IKE identity
- Type—string
- Description—(Optional) Only applicable if IPsec authentication mode is EAP_GTC, EAP-MD5, or EAP-MSCHAPv2.

vpn_connection_keychain_cert_alias

- Title—Keychain Certificate Alias
- Type—string
- Description—(Optional) Keychain alias of the client certificae to use for this VPN configuration

vpn_connection_perapp

- Title—Per App VPN Allowed Apps
- Type—string
- Description—(Deprecated) Use vpn_connection_allowed_apps instead.

vpn_connection_allowed_apps

- Title—Per App VPN Allowed Apps
- Type—string

- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should be tunneled, thus enabling per app VPN. All other apps are NOT tunneled. This setting requires a per app VPN to be enabled on the headend.

vpn_connection_disallowed_apps

- Title—Per App VPN Disallowed Apps
- Type—string
- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should NOT be tunneled, thus enabling per app VPN. All other apps are tunneled. This setting requires a per app VPN to be enabled on the headend.

vpn_connection_allow_bypass

- Title—Allow Apps to Bypass VPN Tunnel
- Type—bool
- Description—(Optional) Allow apps to bypass this VPN connection. By default, this is disabled.

vpn_setting_replace_existing_profile

- Title—Replace Existing Profile
- Type—bool
- Description—(Optional) Only applicable if vpn_connection_profile is set. Specifies whether the managed configuration profile should replace any already installed profile on the client. Disabling this may be desirable to avoid conflicts with ASA pushed profiles. By default, this is enabled.

vpn_setting_apply_perapp_to_profile

- Title—Apply Per App Rules to Profile Imported Configurations
- Type—bool
- Description—(Optional) Specifies whether to apply managed configuration per-app VPN rules (if they exist) to configurations imported from AnyConnect profile XML. By default, this is disabled.

vpn_connection_set_active

- Title—Set Active
- Type—bool
- Default value—true
- Description—(Optional) Sets this as the last selected VPN configuration if there was none.

vpn_setting_fips_mode

- Title—Fips mode
- Type—bool
- Description—(Optional) Whether to enable FIPS mode for AnyConnect.

vpn_setting_uri_external_control

- Title—URI External Control
- Type—string
- Description—(Optional) Configure URI Handling (External Control). Valid options are prompted, enabled, and disabled.

vpn_setting_strict_mode

- Title—Strict Mode
- Type—bool
- Description—(Optional) Whether to enable Strict Certificate Trust mode for AnyConnect.

vpn_setting_certificate_revocation

- Title—Certificate Revocation
- Type—bool
- Description—(Optional) Whether to enable OCSP server certificate checking AnyConnect.

vpn_connection_profile

- Title—AnyConnect profile
- Type—string
- Description—(Optional) AnyConnect Profile (XML format or Base64 encoding of XML) to import

vpn_connection_device_id

- Title—Device Identifier
- Type—string
- Description—(Optional) Identifier of the device report to the headend. If not set, AnyConnect will generate a random persistent device identifier.

vpn_connection_report_hardware_id

- Title—Report Hardware Identifiers (MAC address and IMEI) for VPN authentication
- Type—bool
- Description—(Optional) Whether AnyConnect should attempt to report hardware identifiers to the headend. By default, AnyConnect tries to report hardware identifiers if they are accessible.

vpn_setting_allowed_saved_credentials

- Title—Allow users to save credentials
- Type—bool
- Default value—false

- Description—(Optional) Whether to allow user to save credentials (requires a screen lock). By default, user is not allowed to save credentials.

vpn_configuration_list

- Title—VPN Connection List
- Type—bundle_array
- Description—(Optional) Use this to configure more than one connection entries. Each entry is a vpn_configuration bundle.

umbrella_org_id

- Title—Umbrella Organization Id
- Type—string
- Description—The organization id to which customer belongs and it is as seen in the configuration file downloaded from Cisco Umbrella dashboard.

umbrella_reg_token

- Title—Umbrella Registration Token
- Type—string
- Description—The unique regToken issued to an organization, and the value is as seen in the configuration file downloaded from Cisco Umbrella dashboard.

umbrella_va_fqdns

- Title—Umbrella VA FQDNs list
- Type—string
- Description—This is the FQDN list of the VAs present in the connected network.

admin_email

- Title—Administrator Email Address
- Type—string
- Description—(Optional) Set a default administrator email address for sending logs.

vpn_always_on_umbrella_only

- Title—Enable Always On VPN Mode for Umbrella Protection Only
- Type—bool
- Default value—false
- Description—(Only applicable if using Umbrella) If set to true, always-on VPN will only apply Umbrella protection. If set to false, always-on VPN will apply to both Umbrella and remote access.

Managed Restrictions for vpn_configuration Bundle

vpn_name

- Title—Display Name
- Type—string
- Description—User friendly name (for display only). If not set, defaults to the host.

vpn_host

- Title—Host
- Type—string
- Description—URL to the headend. This field is required.

vpn_protocol

- Title—Protocol
- Type—choice
- Possible values—SSL | IPsec
- Description—VPN tunnel protocol (SSL or IPsec). Defaults to SSL.

vpn_ipsec_auth_mode

- Title—IPsec Authentication Mode
- Type—choice
- Possible Values—EAP-AnyConnect | EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | IKE RSA
- Description—(Optional) Authentication mode to use if tunnel protocol is IPsec. Defaults to EAP-Connect.

vpn_ipsec_ike_identity

- Title—IKE identity
- Type—string
- Description—(Optional) Only applicable if IPsec authentication mode is EAP_GTC, EAP-MD5, or EAP-MSCHAPv2.

vpn_keychain_cert_alias

- Title—Keychain Certificate Alias
- Type—string
- Description—(Optional) Keychain alias of the client certificate to use for this VPN configuration.

vpn_allowed_apps

- Key—vpn_allowed_apps
- Title—Per App VPN Allowed Apps

- Type—string
- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should be tunneled, thus enabling per app VPN. All other apps are NOT tunneled. This setting requires a per-app VPN to be enabled on the headend.

vpn_diallowed_apps

- Title—Per App VPN Disallowed Apps
- Type—string
- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should NOT be tunneled, thus enabling per-app VPN. All other apps are tunneled. This setting requires a per-app VPN to be enabled on the headend.

vpn_allow_bypass

- Title—Allow Apps to Bylass VPN Tunnel
- Type—bool
- Description—(Optional) Allow apps to bypass this VPN connection. By default, this is disabled.

vpn_set_active

- Title—Set Active:
- Type—bool
- Default value—false
- Description—(Optional) Sets this as the last selected VPN configuration if there was none.

AnyConnect on Apple iOS Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.x for Apple iOS for features and devices supported by this release.

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, which 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 as 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:

- Using the new extension framework in AnyConnect 4.0.07x (and later) causes the following changes in behavior from legacy AnyConnect 4.0.05x: AnyConnect considers traffic for tunnel DNS server to be tunneled, even if it is not in split-include network.
- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to AnyConnect 4.0.07x or 4.6.x (or later). Cisco AnyConnect 4.0.07x (or 4.6.x and later) 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. Consult 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.
- AnyConnect considers traffic for tunnel DNS server to be tunneled even if it is not in split-include network.

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 macOS, 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: • EAP-AnyConnect • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • IKE-RSA

Parameter	Description
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 the Connect-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 Chrome OS Devices

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.x for Google Chrome OS for features and devices supported by this release.

Guidelines and Limitations for AnyConnect on Chrome OS

- We are not planning any future Chrome OS releases. Because all current ChromeBooks support Android Apps, we advise you to use the AnyConnect Android App instead.
- 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.

AnyConnect on Universal Windows Platform

Refer to the Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9.x for Universal Windows Platform for features and devices supported by this release.

Guidelines and Limitations for AnyConnect on Universal Windows Platform

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

`with error code 602`. Please contact your administrator and ensure that a valid mobile license is installed on the secure gateway

Configure Mobile Device VPN Connectivity on the ASA Secure Gateway

Procedure

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

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

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

Step 2 Configure Mobile Posture (also called AnyConnect Identity Extensions, ACIDex) to accept, deny, or restrict mobile connections as desired.

See the *Configuring Endpoint Attributes Used in DAPs* procedure, in the appropriate release of Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides.

Example:

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

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

Step 3 (Optional) Configure Per App VPN tunneling mode.

See Configure Per App VPN, on page 23.

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 24.

Step 2 Determine Which Apps Should Be Allowed in the Tunnel, on page 25.

Step 3 Determine the Application IDs for Mobile Apps, on page 25.

Step 4 Configure Per App VPN, on page 23.

Step 5 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 26
- Define a Per App VPN Policy for Apple iOS Devices, on page 27

Step 6 Create Per App Custom Attributes, on page 27 on the ASA.

Step 7 Assign a Custom Attribute to a Policy on the ASA, on page 28.

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`*`\`.

Determine Which Apps Should Be Allowed in the Tunnel

When you support mobile devices, such as phones running Android or iOS, you can use Mobile Device Manager (MDM) applications to fine-tune VPN access so that only supported applications are allowed to use the VPN tunnel. By restricting the remote access VPN to approved applications, you can reduce the load on the VPN headend and also protect the corporate network from malicious applications installed on these mobile devices.

To use a per-app remote access VPN, you must install and configure a third-party MDM application. It is in the MDM that you define the list of approved applications that can be used over the VPN tunnel. Explaining how to configure and use the third-party MDM that you select is outside the scope of this document.

When you use AnyConnect to establish a VPN connection from a mobile device, all the traffic including the traffic from personal applications is routed through the VPN. If you instead want to route corporate applications only through the VPN, so that non-corporate traffic is excluded from the VPN, you can use per-app VPN to select which applications should be tunneled through the VPN.

Configure per-app VPN has the following main benefits:

- Performance—It limits traffic in the VPN to the traffic that needs to go to the corporate network. Thus, you free up resources at the head end of the RA VPN.
- Protection—Because only traffic from approved applications is allowed, it protects the corporate tunnel from unapproved malicious applications that a user might unwittingly install on the mobile device. Because these applications are not included in the tunnel, traffic from them is never sent to the headend.

The Mobile Device Manager (MDM) running on the mobile endpoint enforces the Per-app VPN policy on the applications.

Determine the Application IDs for Mobile Apps

We strongly recommend that you configure the per-app policy in the Mobile Device Manager (MDM) that you select to provide the service on the user's mobile device. This greatly simplifies the headend configuration.

If you instead decide that you also want to configure the list of allowed apps on the headend, you need to determine the application IDs for each application on each type of endpoint.

The application ID, called the bundle ID in iOS, is a reverse DNS name. You can use an asterisk as a wildcard. For example, *.* indicates all applications, com.cisco.* indicates all Cisco applications.

- Android—Go to Google play in a web browser and choose the Apps category. Click on (or hover over) an application that you want to allow, then look at the URL. The app id is in the URL, on the **id=** parameter. For example, the following URL is for Facebook Messenger, so the app id is com.facebook.orca:

  ```
  https://play.google.com/store/apps/details?id=com.facebook.orca
  ```

For applications that are not available through Google Play, such as your own applications, download a package name viewer application to extract the app ID. Cisco does not endorse any of the available applications, but one of them should provide what you need.

- iOS—One means to find the bundle ID:

  1. Use a desktop browser such as Chrome to search for the application name.

2. In the search results, look for the link to download the app from the Apple App Store. For example, Facebook messanger would be similar to https://apps.apple.com/us/app/messenger/id454638411.
3. Copy the nymber after the **id** string. In this example, **454638411.**
4. Open a new browser window, and add the number to the end of the following URL:

   `https://itunes.apple.com/lookup?id=`

   For this example, https://itunes.apple.com/lookup?id=454638411
5. You will be prompted to download a text file, usually named 1.txt. Download the file.
6. Open the file in a text editor such as WordPad and search for bundleId. For example: "bundleId":"com.facebook.Messenger". In this example, the bundle ID is com.facebook.Messenger. Use this as the app ID.

Once you have your list of application IDs, you can configure the policy.

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. You are required to configure some per-app policy (custom attribute) on the ASA in order for per-app to work, even if MDM has been configured for per-app. 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. We recommend specifying *.* as the APP ID to allow tunneling of ALL apps and to ensure that the MDM policy is the only arbiter of tunneled apps. Non *.* policies are not supported.

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. This string 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. This string 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* because it is the only type of attribute understood by the AnyConnect client for Per App VPN. Adding this attribute to remote access VPN group profile automatically limits the tunnel to the explicitly identified platforms. Traffic from all other application is automatically excluded from the tunnel.

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 for procedures that are common to desktop and mobile endpoints considering the following exceptions:

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

Step 2 Configure Mobile Specific Attributes:

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

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

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

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

- 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 37 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.

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

- The URI handler in AnyConnect lets other applications pass action requests in the form of Universal Resource Identifiers (URIs) to AnyConnect.

  In managed environment:

  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. The key and values for configuring the settings on MDM are:

  Key - *UriExternalControl*

  Values - *Enabled*, *Prompt*, or *Disabled*

  Note Once the configuration setting has been done in MDM and pushed down to the user device, the user is not allowed to make changes to this setting.

  In unmanaged environment:

  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 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 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

Match	Instruction	Example Entry	Example Matches	Example Match Failures
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

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
```

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

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

Procedure

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

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

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

a) Ensure that the correct certificate is being selected.
b) Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage.
c) Ensure that the certificate matching rules in the AnyConnect profile are not filtering out the user's selected certificate.

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

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

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.