Configure Application-Based Remote Access VPN (Per App VPN) on Mobile Devices Using Cisco Secure Firewall Management Center

First Published: 2023-07-31

Last Modified: 2023-07-31

Configure Application-Based Remote Access VPN (Per App VPN) on Mobile Devices Using Cisco Secure Firewall Management Center

About Per App VPN

When a remote user establishes a VPN connection from a mobile device using Secure Client, all the traffic including traffic from personal applications is routed through the VPN.

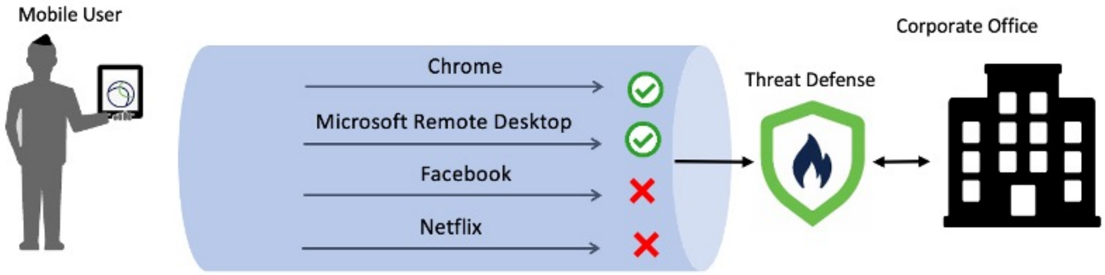
For mobile devices that run on Android or iOS, you can restrict the applications that traverse the VPN tunnel. This application-based remote access VPN is called Per App VPN.

To use Per App VPN, you must perform the following actions:

1. Install and configure a third-party Mobile Device Manager (MDM) server.
2. Define the list of approved applications that can go over the VPN tunnel in the MDM server.
3. Deploy the Per App configurations from the MDM server to the mobile devices.
4. Configure Per App VPN on the managed headend threat defense.

When an MDM-managed mobile device connects to the VPN using Secure Client, the client validates the applications before tunneling the traffic. The Per App policy configured on the threat defense performs this validation.

The following illustration shows an example of Per App VPN using the threat defense:



Benefits

- Limit VPN traffic over the corporate network and free up resources of the VPN headend. You can prevent:
  - Applications such as Netflix, Facebook, and YouTube over the VPN.
  - Trusted cloud applications such as Outlook, and Webex over the VPN.
- Optimize traffic.
- Minimize latency.
- Protect the corporate VPN tunnel from unapproved malicious applications on the mobile device.

Is this Guide for You?

This use case is for network administrators who use the management center to configure Per App VPN for remote workers connecting to their organization's network using remote access VPN.

In versions 6.4 to 6.7, you can enable Per App VPN on an FTD using FlexConfig. For more information, see Configure Application-Based (Per App) Remote Access VPN on Mobile Devices. In version 7.0 and later, you can enable Per App VPN on the threat defense using the management center UI.

System Requirements

The table below shows the supported platforms for this feature.

Product	Version	Version used in this document
Cisco Secure Firewall Threat Defense (formerly Firepower Threat Defense/FTD)	7.0 and later	7.3
Cisco Secure Firewall Management Center (formerly Firepower Management Center/FMC)	7.0 and later	7.3
Cisco Secure Client (formerly AnyConnect)	4.0 and later	5.0
Android Devices	Android 5.0 and later	-
Apple iOS devices	Apple iOS 8.3 and later	-

Prerequisites for Configuring Per App VPN Tunnels

Ensure that you have:

- Configured a remote access VPN policy in the management center.
- Set up an MDM server and enrolled each mobile device to the MDM server.

  For more information, see the MDM documentation.

We recommend that you configure the applications that can traverse the VPN tunnel in the MDM server. This configuration simplifies the headend configuration.

- Downloaded and installed the Cisco AnyConnect Enterprise Application Selector from the Cisco Software Download Center to your local host.

  You need this tool to define the Per App VPN policy.

Licenses:

- You need one of the following Secure Client licenses:

  Secure Client Premier or Secure Client Advantage.

- Your management center Essentials license must allow export-controlled functionality.

  Choose **System** > **Licenses** > **Smart Licenses** to verify this functionality in the management center.

How to Configure Per App VPN Using Management Center

Step	Do This	More Info
1	Ensure that you meet the prerequisites.	Prerequisites for Configuring Per App VPN Tunnels, on page 2
2	Determine which applications should be allowed in the tunnel.	-
3	Determine the application IDs for the mobile applications.	Determine the Application IDs for Mobile Applications, on page 3
4	Define a Per App VPN policy for Android and Apple iOS devices.	Define a Per App VPN Policy for Android and Apple iOS Devices, on page 5
5	Assign the Per App VPN policy to a remote access VPN in the management center.	Assign the Per App VPN Policy to a Remote Access VPN in the Management Center, on page 8
6	Deploy the configuration on the threat defense.	On the management center menu bar, click **Deploy** and then select **Deployment**.

Determine the Application IDs for Mobile Applications

If you decide to configure the list of allowed applications on the headend, you must determine the application IDs for each application on each type of endpoint.

Note We recommend that you configure the Per App policy in the MDM server. This configuration simplifies the headend configuration.

The application ID, or 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.

To determine the application IDs:

- **Android**

  1. In a web browser, go to Google Play (https://play.google.com/store/).
  2. Click the **Apps** tab.
  3. Click an application that you want to allow in the VPN tunnel.

     The application ID is part of the URL.

  4. Copy the string after the ‘id=’ parameter.

     For Microsoft Remote Desktop, the URL is:

     https://play.google.com/store/apps/details?id=com.microsoft.rdc.androidx, and the app id is com.microsoft.rdc.androidx.

  For applications that are not available on Google Play, download a package name viewer application to extract the app ID.

- **iOS**

  1. In a web browser, go to Apple App Store (https://www.apple.com/in/app-store/).
  2. In the search results, search for an application.

     The application ID is part of the URL.

  3. Copy the number after the ‘id’ string.

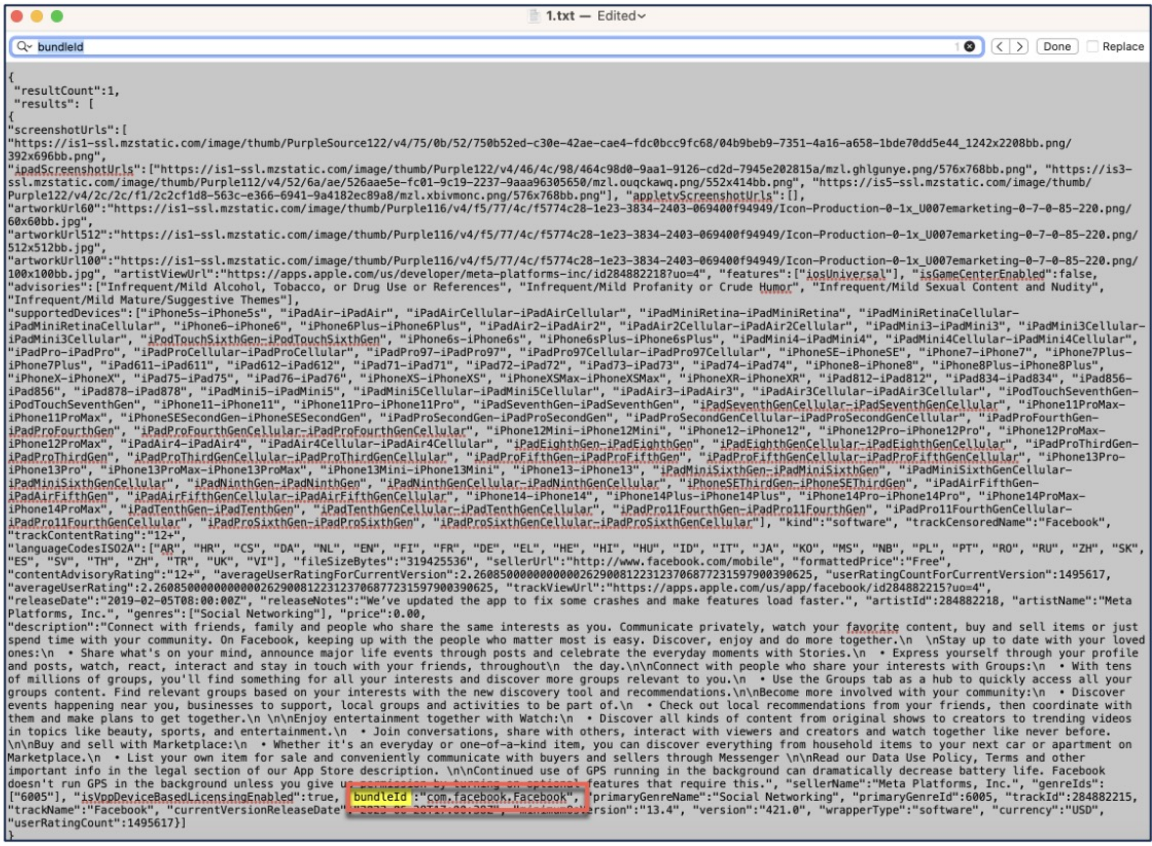
     For Facebook, the URL is:

     https://apps.apple.com/in/app/facebook/id284882215 and the application ID is 284882215.

  4. Open a new browser window, and add the number to the end of the following URL: https://itunes.apple.com/lookup?id=

     For Facebook the URL is https://itunes.apple.com/lookup?id=284882215.

  5. Download the text file, usually named 1.txt.
  6. Open the file in a text editor, and search for ‘bundleId’. For Facebook, the ‘bundleId’ is " com.facebook.Facebook". Use this bundle ID as the app ID.



```
{
 "resultCount":1,
 "results": [
{
"screenshotUrls":[
"https://is1-ssl.mzstatic.com/image/thumb/PurpleSource122/v4/75/0b/52/750b52ed-c30e-42ae-cae4-fdc0bcc9fc68/04b9beb9-7351-4a16-a658-1bde70dd5e44_1242x2208bb.png/
392x696bb.png",
"ipadScreenshotUrls":["https://is1-ssl.mzstatic.com/image/thumb/Purple122/v4/46/4c/98/464c98d0-9aa1-9126-cd2d-7945e202815a/mzl.ghlgunye.png/576x768bb.png", "https://is3-
ssl.mzstatic.com/image/thumb/Purple112/v4/52/6a/ae/526aae5e-fc01-9c19-2237-9aaa96305650/mzl.ouqckawq.png/552x414bb.png", "https://is5-ssl.mzstatic.com/image/thumb/
Purple122/v4/2c/2c/f1/2c2cf1d8-563c-e366-6941-9a4182ec89a8/mzl.xbivmonc.png/576x768bb.png"], "appletvScreenshotUrls":[],
"artworkUrl60":"https://is1-ssl.mzstatic.com/image/thumb/Purple116/v4/f5/77/4c/f5774c28-1e23-3834-2403-069400f94949/Icon-Production-0-1x_U007emarketing-0-7-0-85-220.png/
60x60bb.jpg",
"artworkUrl512":"https://is1-ssl.mzstatic.com/image/thumb/Purple116/v4/f5/77/4c/f5774c28-1e23-3834-2403-069400f94949/Icon-Production-0-1x_U007emarketing-0-7-0-85-220.png/
512x512bb.jpg",
"artworkUrl100":"https://is1-ssl.mzstatic.com/image/thumb/Purple116/v4/f5/77/4c/f5774c28-1e23-3834-2403-069400f94949/Icon-Production-0-1x_U007emarketing-0-7-0-85-220.png/
100x100bb.jpg", "artistViewUrl":"https://apps.apple.com/us/developer/meta-platforms-inc/id284882218?uo=4", "features":["iosUniversal"], "isGameCenterEnabled":false,
"advisories":["Infrequent/Mild Alcohol, Tobacco, or Drug Use or References", "Infrequent/Mild Profanity or Crude Humor", "Infrequent/Mild Sexual Content and Nudity",
"Infrequent/Mild Mature/Suggestive Themes"],
"supportedDevices":["iPhone5s-iPhone5s", "iPadAir-iPadAir", "iPadAirCellular-iPadAirCellular", "iPadMiniRetina-iPadMiniRetina", "iPadMiniRetinaCellular-
iPadMiniRetinaCellular", "iPhone6-iPhone6", "iPhone6Plus-iPhone6Plus", "iPadAir2-iPadAir2", "iPadAir2Cellular-iPadAir2Cellular", "iPadMini3-iPadMini3", "iPadMini3Cellular-
iPadMini3Cellular", "iPodTouchSixthGen-iPodTouchSixthGen", "iPhone6s-iPhone6s", "iPhone6sPlus-iPhone6sPlus", "iPadMini4-iPadMini4", "iPadMini4Cellular-iPadMini4Cellular",
"iPadPro-iPadPro", "iPadProCellular-iPadProCellular", "iPadPro97-iPadPro97", "iPadPro97Cellular-iPadPro97Cellular", "iPhoneSE-iPhoneSE", "iPhone7-iPhone7", "iPhone7Plus-
iPhone7Plus", "iPad611-iPad611", "iPad612-iPad612", "iPad71-iPad71", "iPad72-iPad72", "iPad73-iPad73", "iPad74-iPad74", "iPhone8-iPhone8", "iPhone8Plus-iPhone8Plus",
"iPhoneX-iPhoneX", "iPad75-iPad75", "iPad76-iPad76", "iPhoneXS-iPhoneXS", "iPhoneXSMax-iPhoneXSMax", "iPhoneXR-iPhoneXR", "iPad812-iPad812", "iPad834-iPad834", "iPad856-
iPad856", "iPad878-iPad878", "iPadMini5-iPadMini5", "iPadMini5Cellular-iPadMini5Cellular", "iPadAir3-iPadAir3", "iPadAir3Cellular-iPadAir3Cellular", "iPodTouchSeventhGen-
iPodTouchSeventhGen", "iPhone11-iPhone11", "iPhone11Pro-iPhone11Pro", "iPadSeventhGen-iPadSeventhGen", "iPadSeventhGenCellular-iPadSeventhGenCellular", "iPhone11ProMax-
iPhone11ProMax", "iPhoneSESecondGen-iPhoneSESecondGen", "iPadProSecondGen-iPadProSecondGen", "iPadProSecondGenCellular-iPadProSecondGenCellular", "iPadProFourthGen-
iPadProFourthGen", "iPadProFourthGenCellular-iPadProFourthGenCellular", "iPhone12Mini-iPhone12Mini", "iPhone12-iPhone12", "iPhone12Pro-iPhone12Pro", "iPhone12ProMax-
iPhone12ProMax", "iPadAir4-iPadAir4", "iPadAir4Cellular-iPadAir4Cellular", "iPadEighthGen-iPadEighthGen", "iPadEighthGenCellular-iPadEighthGenCellular", "iPadProThirdGen-
iPadProThirdGen", "iPadProThirdGenCellular-iPadProThirdGenCellular", "iPadProFifthGen-iPadProFifthGen", "iPadProFifthGenCellular-iPadProFifthGenCellular", "iPhone13Pro-
iPhone13Pro", "iPhone13ProMax-iPhone13ProMax", "iPhone13Mini-iPhone13Mini", "iPhone13-iPhone13", "iPadMiniSixthGen-iPadMiniSixthGen", "iPadMiniSixthGenCellular-
iPadMiniSixthGenCellular", "iPadNinthGen-iPadNinthGen", "iPadNinthGenCellular-iPadNinthGenCellular", "iPhoneSEThirdGen-iPhoneSEThirdGen", "iPadAirFifthGen-
iPadAirFifthGen", "iPadAirFifthGenCellular-iPadAirFifthGenCellular", "iPhone14-iPhone14", "iPhone14Plus-iPhone14Plus", "iPhone14Pro-iPhone14Pro", "iPhone14ProMax-
iPhone14ProMax", "iPadTenthGen-iPadTenthGen", "iPadTenthGenCellular-iPadTenthGenCellular", "iPadPro11FourthGen-iPadPro11FourthGen", "iPadPro11FourthGenCellular-
iPadPro11FourthGenCellular", "iPadProSixthGen-iPadProSixthGen", "iPadProSixthGenCellular-iPadProSixthGenCellular"], "kind":"software", "trackCensoredName":"Facebook",
"trackContentRating":"12+",
"languageCodesISO2A":["AR", "HR", "CS", "DA", "NL", "EN", "FI", "FR", "DE", "EL", "HE", "HI", "HU", "ID", "IT", "JA", "KO", "MS", "NB", "PL", "PT", "RO", "RU", "ZH", "SK",
"ES", "SV", "TH", "ZH", "TR", "UK", "VI"], "fileSizeBytes":"319425536", "sellerUrl":"http://www.facebook.com/mobile", "formattedPrice":"Free",
"contentAdvisoryRating":"12+", "averageUserRatingForCurrentVersion":2.26085000000000026290081223123706877231597900390625, "userRatingCountForCurrentVersion":1495617,
"averageUserRating":2.26085000000000026290081223123706877231597900390625, "trackViewUrl":"https://apps.apple.com/us/app/facebook/id284882215?uo=4",
"releaseDate":"2019-02-05T08:00:00Z", "releaseNotes":"We've updated the app to fix some crashes and make features load faster.", "artistId":284882218, "artistName":"Meta
Platforms, Inc.", "genres":["Social Networking"], "price":0.00,
"description":"Connect with friends, family and people who share the same interests as you. Communicate privately, watch your favorite content, buy and sell items or just
spend time with your community. On Facebook, keeping up with the people who matter most is easy. Discover, enjoy and do more together.\n  \nStay up to date with your loved
ones:\n  • Share what's on your mind, announce major life events through posts and celebrate the everyday moments with Stories.\n  • Express yourself through your profile
and posts, watch, react, interact and stay in touch with your friends, throughout\n  the day.\n\nConnect with people who share your interests with Groups:\n  • With tens
of millions of groups, you'll find something for all your interests and discover more groups relevant to you.\n  • Use the Groups tab as a hub to quickly access all your
groups content. Find relevant groups based on your interests with the new discovery tool and recommendations.\n\nBecome more involved with your community:\n  • Discover
events happening near you, businesses to support, local groups and activities to be part of.\n  • Check out local recommendations from your friends, then coordinate with
them and make plans to get together.\n \n\nEnjoy entertainment together with Watch:\n  • Discover all kinds of content from original shows to creators to trending videos
in topics like beauty, sports, and entertainment.\n  • Join conversations, share with others, interact with viewers and creators and watch together like never before.
\n\nBuy and sell with Marketplace:\n  • Whether it's an everyday or one-of-a-kind item, you can discover everything from household items to your next car or apartment on
Marketplace.\n  • List your own item for sale and conveniently communicate with buyers and sellers through Messenger \n\nRead our Data Use Policy, Terms and other
important info in the legal section of our App Store description. \n\nContinued use of GPS running in the background can dramatically decrease battery life. Facebook
doesn't run GPS in the background unless you give us permission by turning on optional features that require this.", "sellerName":"Meta Platforms, Inc.", "genreIds":
["6005"], "isVppDeviceBasedLicensingEnabled":true, "bundleId":"com.facebook.Facebook", "primaryGenreName":"Social Networking", "primaryGenreId":6005, "trackId":284882215,
"trackName":"Facebook", "currentVersionReleaseDate":"[illegible]", "minimumOsVersion":"13.4", "version":"421.0", "wrapperType":"software", "currency":"USD",
"userRatingCount":1495617}]
}
```

Once you have your list of application IDs, you can define the policy for the mobile device as explained in the procedure below.

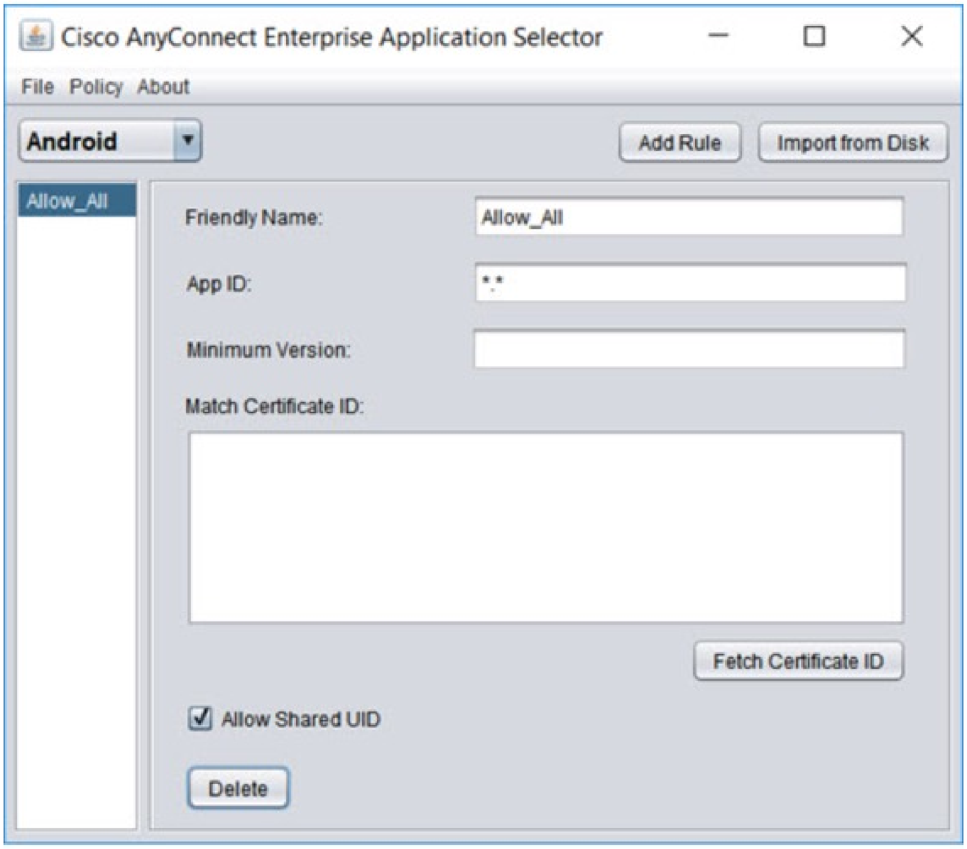
Define a Per App VPN Policy for Android and Apple iOS Devices

Use the Cisco AnyConnect Enterprise Application Selector to define the Per App VPN policy.

We recommend that you create a simple 'Allow All' policy, and define the allowed applications in the MDM. However, you can specify a list of applications to allow and control the list from the headend. If you want to include specific applications, create a separate rule for each application, using a unique name and the application's app ID.

To create an **Allow All** policy (wildcard policy) that supports both Android and iOS platforms using the AnyConnect Enterprise Application Selector:

1. Choose **Android** or **iOS** from the drop-down list as the platform type.
2. Configure the following options:
   - **Friendly Name**—Enter a name for the policy. For example, Allow_All.
   - **App ID**—Enter *.* to match all possible applications.
   - Leave the other options.



Android

Friendly Name: Allow_All

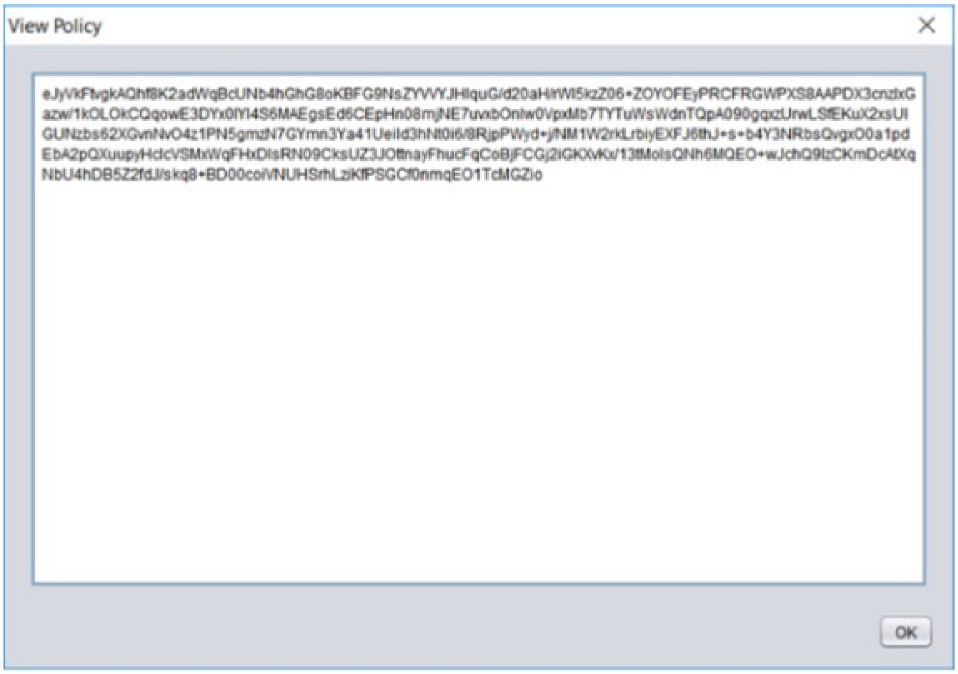
App ID: *.*

Minimum Version:

Match Certificate ID:

☑ Allow Shared UID

3. Choose **Policy** > **View Policy** to get the base64 encoded string for the policy. This string contains an encrypted XML file that allows the threat defense to see the policies. Copy this value. You need this string when you configure Per App VPN on the threat defense in the next step.



eJyVkFtvgkAQhf8K2adWqBcUNb4hGhG8oKBFG9NsZYVVYJHlquG/d20aHlrWI5kzZ06+ZOYOFEyPRCFRGWPXS8AAPDX3cnzlxG
azw/1kOLOkCQqowE3DYx0lYl4S6MAEgsEd6CEpHn08mjNE7uvxbOnlw0VpxMb7TYTuWsWdnTQpA090gqxzUrwLSfEKuX2xsUI
GUNzbs62XGvnNvO4z1PN5gmzN7GYmn3Ya41Ueild3hNt0i6/8RjpPWyd+j/NM1W2rkLrbiyEXFJ6thJ+s+b4Y3NRbsQvgxO0a1pd
EbA2pQXuupyHclcVSMxWqFHxDIsRN09CksUZ3JOttnayFhucFqCoBjFCGj2iGKXvKx/13tMolsQNh6MQEO+wJchQ9lzCKmDcAfXq
NbU4hDB5Z2fdJ/skq8+BD00coiVNUHSrhLziKfPSGCf0nmqEO1TcMGZio

To create a policy for the Microsoft Remote Desktop application using the AnyConnect Enterprise Application Selector:

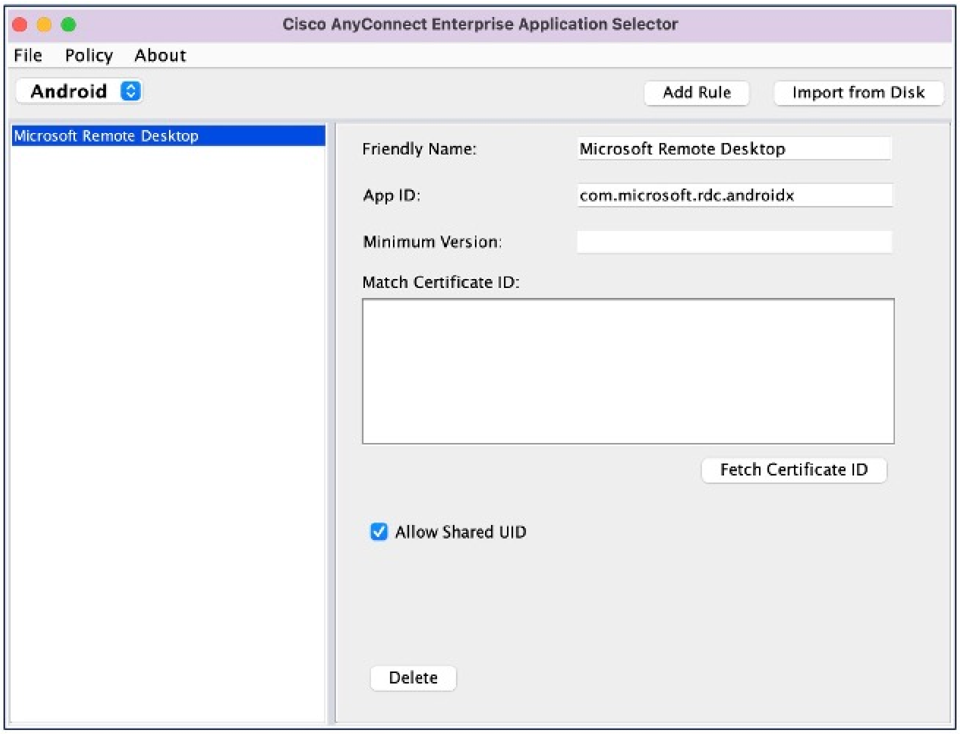
1. Choose **Android** from the drop-down list as the platform type.

2. Configure the following options:

   - **Friendly Name**—Enter the policy name.

   - **App ID**—For Android, enter com.microsoft.rdc.androidx.

   - Leave the other options.



Android

Microsoft Remote Desktop

Friendly Name: Microsoft Remote Desktop

App ID: com.microsoft.rdc.androidx

Minimum Version:

Match Certificate ID:

☑ Allow Shared UID

3. Choose **Policy** > **View Policy** to get the base64 encoded string for the policy.

Assign the Per App VPN Policy to a Remote Access VPN in the Management Center

Procedure

Step 1 Choose **Devices** > **Remote Access**.

Step 2 Select a remote access VPN policy and click **Edit**.

Step 3 Select a connection profile and click **Edit**.

Step 4 Click **Edit Group Policy**.

Step 5 Click the **Secure Client** tab.

Step 6 Click **Custom Attributes** and click **+**.

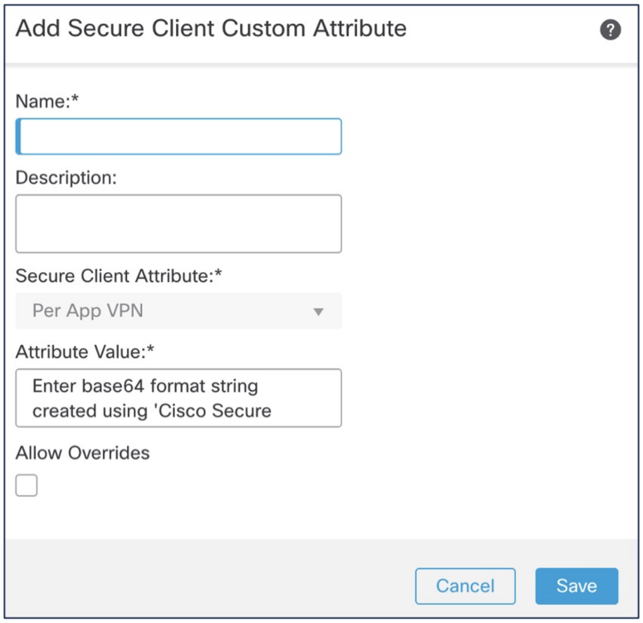
Step 7 Choose Per App VPN from the **Secure Client Attribute** drop-down list.

Step 8 Choose an object from the **Custom Attribute Object** drop-down list or click **+** to add an object.

When you add a new custom attribute object for Per App VPN:

a. Enter the name, and description.

b. In the **Attribute Value** field, specify the base64 encoded policy string from the Cisco AnyConnect Enterprise Application Selector.



Add Secure Client Custom Attribute

Name:*

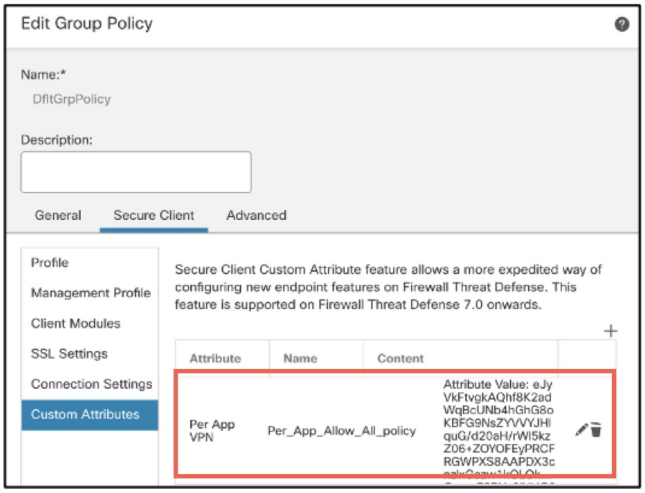
Description:

Secure Client Attribute:* Per App VPN

Attribute Value:* Enter base64 format string created using 'Cisco Secure

Allow Overrides □

Step 9 Click **Save** and click **Add**.



Edit Group Policy

Name:* DfltGrpPolicy

Description:

Secure Client Custom Attribute feature allows a more expedited way of configuring new endpoint features on Firewall Threat Defense. This feature is supported on Firewall Threat Defense 7.0 onwards.

Attribute	Name	Content
Per App VPN	Per_App_Allow_All_policy	Attribute Value: eJy VkFtvgkAQhf8K2ad WqBcUNb4hGhG8o KBFG9NsZYVVYJHI quG/d20aH/rWI5kz Z06+ZOYOFEyPRCF RGWPXS8AAPDX3c

Step 10 Click **Save**.

What to do next

1. Deploy the configuration on the threat defense.
2. Establish a VPN connection to the threat defense using the Secure Client.
3. Verify Per App VPN Configuration.

Verify Per App VPN Configuration

On the Threat Defense

Use the following commands on the threat defense to verify the Per App configuration:

Command	Description
show run webvpn	View details of the Secure Client configurations.
show run group-policy <group_policy_name>	View details of the remote access VPN group policy for Secure Client.
show vpn-sessiondb anyconnect	View details of the active Secure Client VPN sessions.
show run anyconnect-custom-data	View details of the Per App configuration.

Sample output for **sh run webvpn** is given below:

```
firepower# sh run webvpn
 webvpn
 enable inside
 anyconnect-custom-attr perapp description Per-App Allow
 http-headers
 hsts-server
 enable
 max-age 31536000
 include-sub-domains
 no preload
 hsts-client
 enable
 x-content-type-options
 x-xss-protection
 content-security-policy
 anyconnect image disk0:/csm/cisco-secure-client-win-5.0.03076-webdeploy-k9 1 regex "Windows"

 anyconnect enable
 tunnel-group-list enable
 cache
 no disable
 error-recovery disable
```

Sample output for **sh run anyconnect-custom-data** is given below:

```
firepower# sh run anyconnect-custom-data
anyconnect-custom-data perapp PerAppPolicy
eJw9kFtvgkAQhf8K2ae2GC+rqPFNgYjgBcUL2PRhCyuuZVlkuRv/
```

Sample output for **sh running-config group-policy** is given below:

```
firepower# sh running-config group-policy
 group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev2 ssl-client
 user-authentication-idle-timeout none
 anyconnect-custom perapp value PerAppPolicy
 webvpn
 anyconnect keep-installer none
 anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none
```

On the Endpoint

After the endpoint establishes a VPN connection with the threat defense, click the **Statistics** icon of the Secure Client:

- **Tunnel Mode** will be “Application Tunnel” instead of “Tunnel All Traffic.”
- **Tunneled Apps** will list the applications you enabled for tunneling in the MDM.