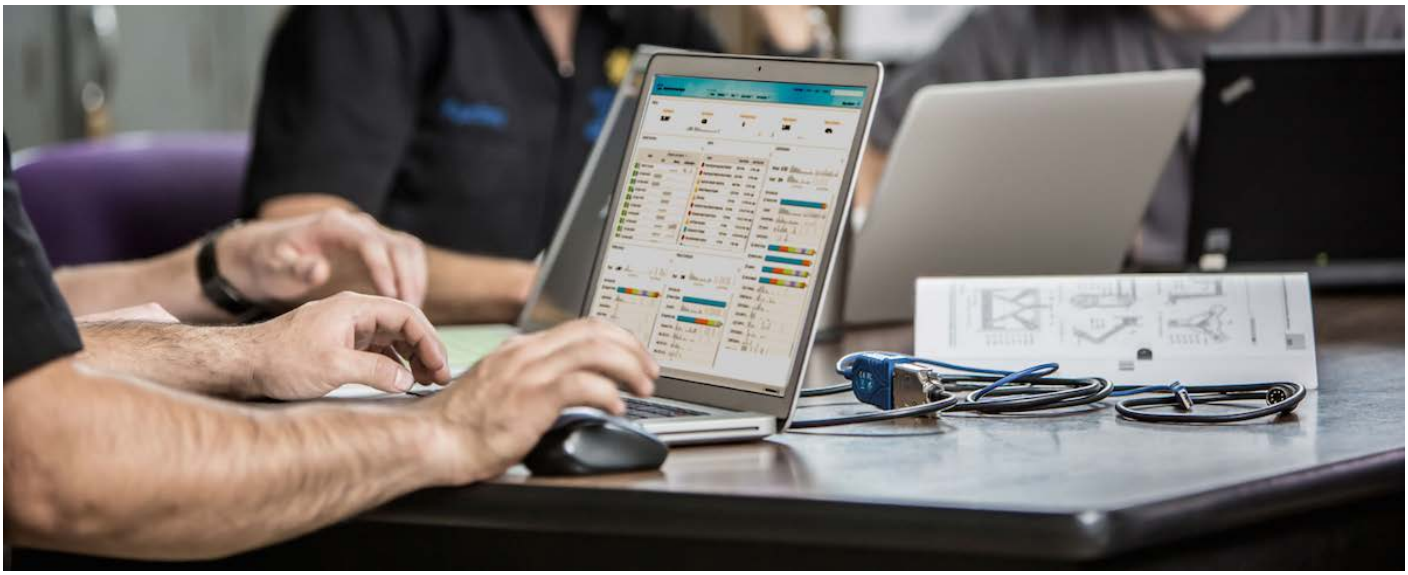


Cisco AnyConnect PerApp VPN

How to Implement PerApp for iOS devices with MobileIron MDM/EMM

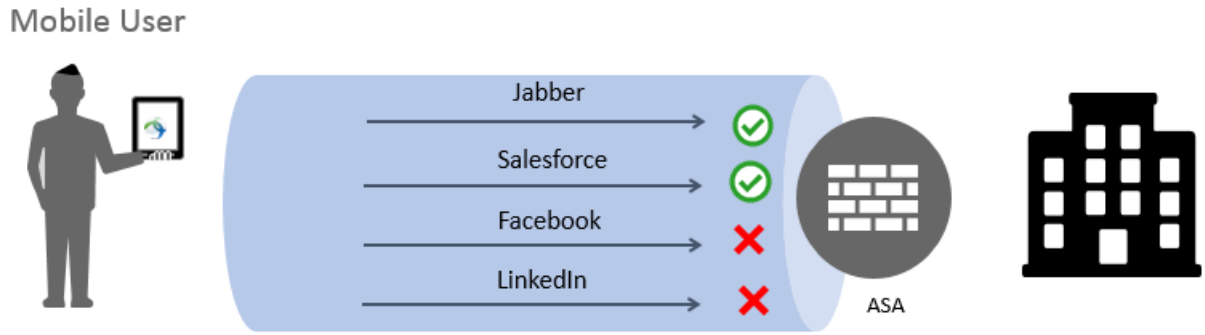


Table of Contents

PerApp Overview

AnyConnect Per-Application VPN (PerApp VPN) solves the problem of providing BYOD VPN support to AnyConnect on mobile devices where tunneling only applications defined by a policy to the corporate network is desired. PerApp not only protects the targeted corporate data but also protects the user's personal data and applications since only applications explicitly permitted by the ASA administrator will be permitted access to VPN head-end and ultimately the corporate network. This solution is essentially split-tunneling at Layer 7 without the inherent risks associated with L3 split-tunneling.

This use case focuses on Apple iOS devices which are required to be managed by an MDM/EMM solution. MDM servers such as MobileIron are able to push PerApp VPN configurations when managing devices. When devices are managed the AnyConnect VPN Client behaves as an application filter and performs validation of the application prior to allowing the traffic to be tunneled. This validation is accomplished using a PerApp Policy applied to the ASA. Applications not permitted by the PerApp policy will not have its packets forwarded to the ASA.

In this case the applications that are permitted to traverse the tunnel are defined and configured by MobileIron. The ASA will utilize a wildcard perapp policy in DAP to enforce, although this can also be done using an ASA group-policy. The difference between Managed and Unmanaged which is only supported by Android devices is that in the case of unmanaged the PerApp policy would configure and enforce. Since MobileIron will specify the 2 apps permitted in this example we can simply use the wildcard and put the onus on the Mobile Device Management to configure the policy and the ASA using the PerApp policy created using the Cisco AnyConnect Enterprise Application Selector tool.

Cisco Systems © 2016

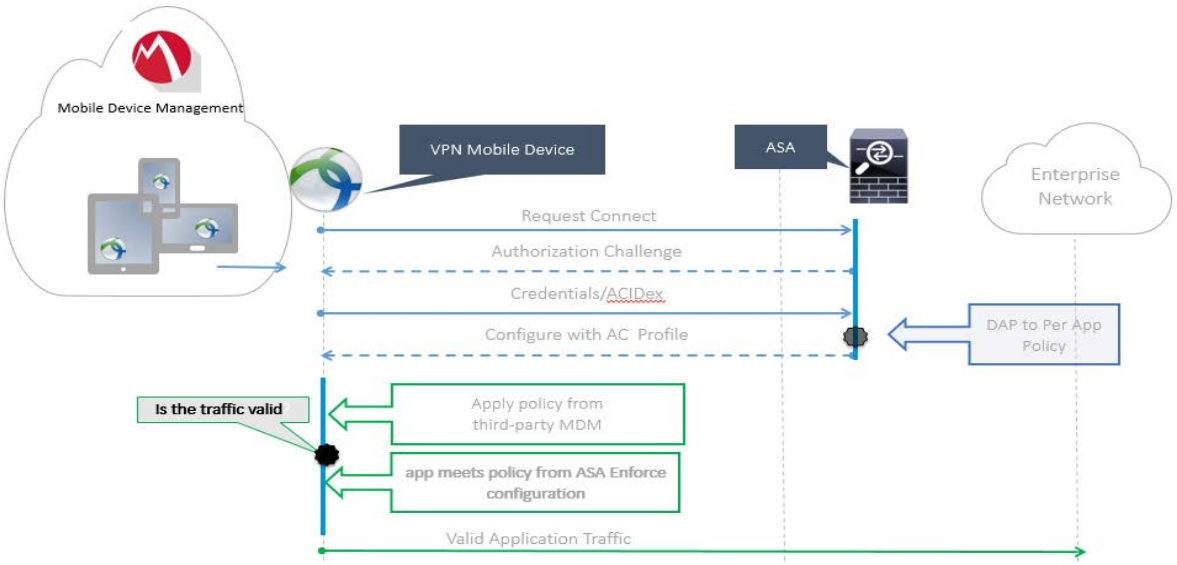


Figure 1. PerApp flow

MobileIron Configuration

Create VPN Policy

We have defined a VPN Configuration in MobileIron for the users accessing our ASA headend. This configuration contains the FQDN of the ASA, AnyConnect as the connection type with PerApp enabled. To create this configuration access '**Policies & Configs' > 'Configurations' > 'VPN' > Connection Type = AnyConnect**

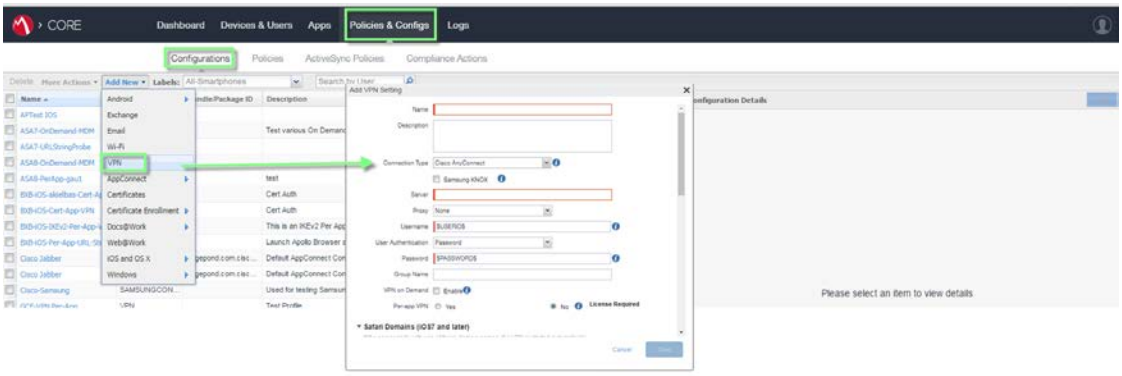


Figure 2. New VPN Configuration

For additional MobileIron VPN Configuration help please reference:

https://help.mobileiron.com/customer/apex/AwsHelp?topic=ProductGuides/AdminGuideCore71/appsettings/VPN_settings.htm .

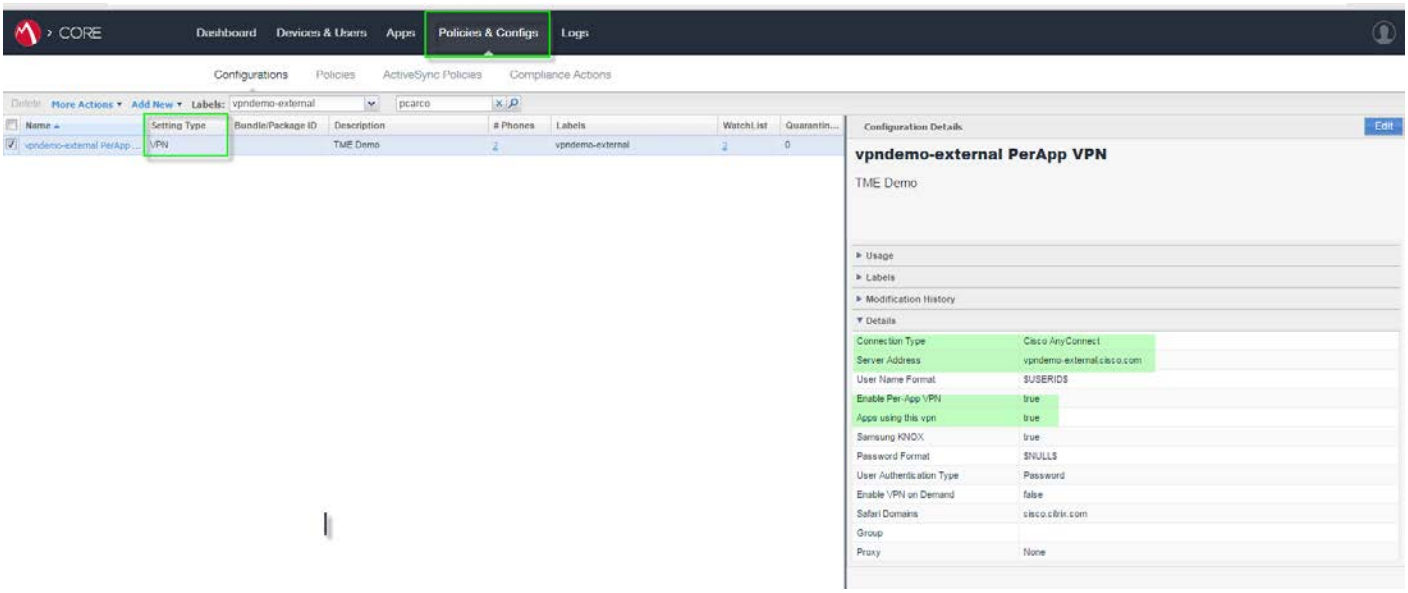


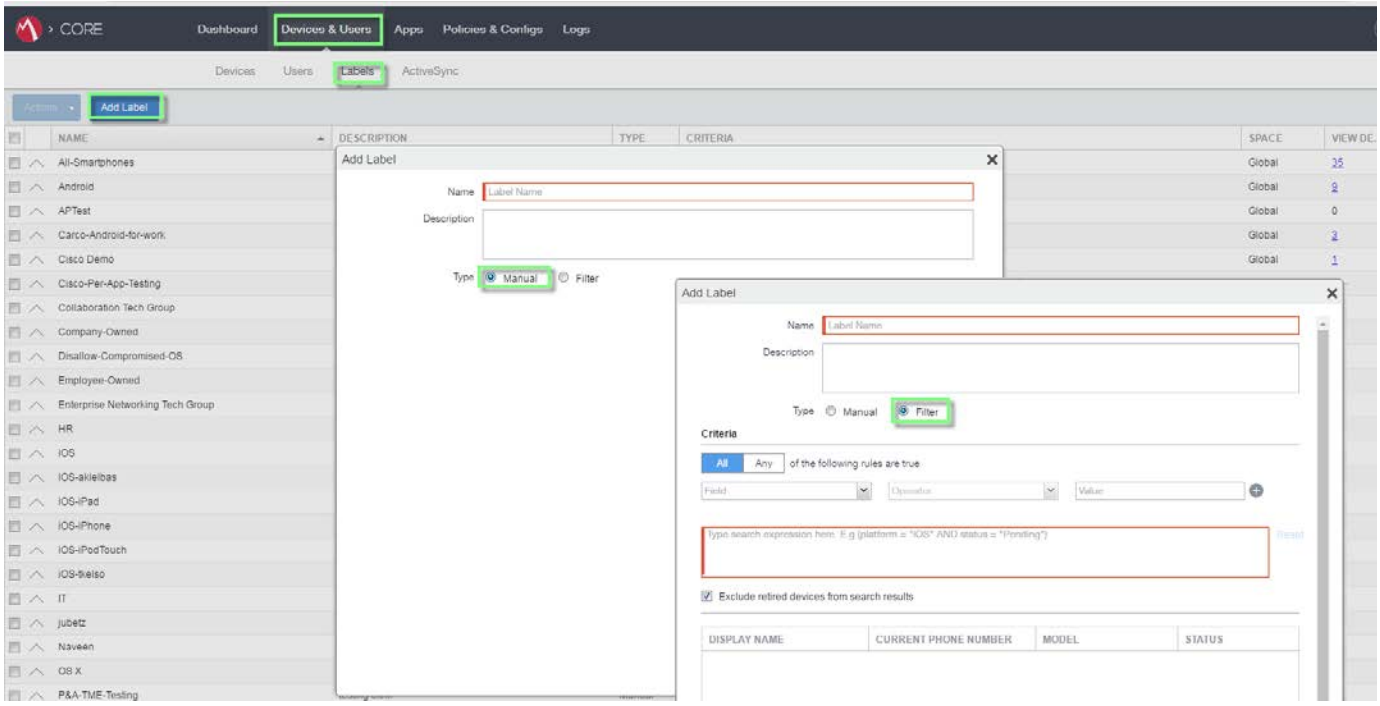
Figure 3. Completed VPN Policies' & Configuration

Create a Label

MobileIron provides labels to create a virtual grouping of objects found on the system. Labels are a key component used to distribute a policy to a select subset of devices. A label must be created before it can be applied. Labels are managed under 'Users & Devices'. We have created a manual label named vpndemo-external. Manual labels are manually applied to devices – the administrator must select the devices in the Users & Devices tab and then apply the manual label to those devices in order to assign policies, settings, or apps to those devices. Filter labels are dynamic and use specific criteria to specify a group of devices. Manual labels have no criteria associated with them.

For additional help with using and creating labels with MobileIron please reference:

https://help.mobileiron.com/customer/apex/AwsHelp?topic=ProductGuides/AdminGuideCore71/mgphones/Using_labels_to_establish_groups.htm



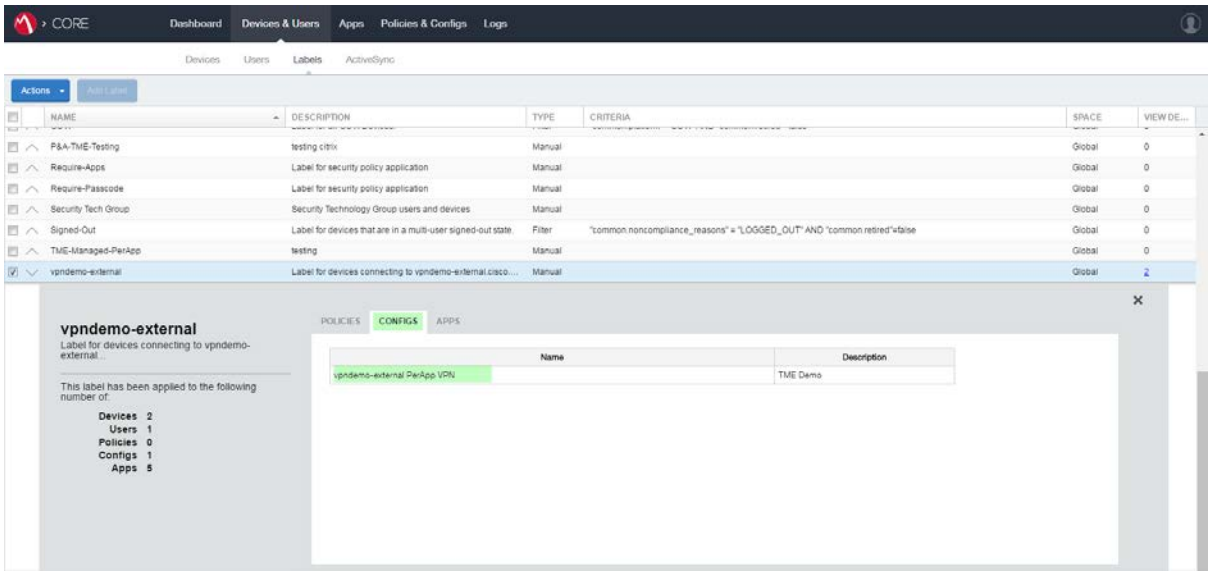


Figure 4. Manual Label linked to VPN configuration

Associate the apps that are permitted over VPN by specifying the VPN configuration for the app. It is necessary to access the App Catalog and configure the Apps with a label, this ties the app to the VPN Configuration since the label has also been tied to the VPN Configuration.

In the MobileIron Admin Portal,

1. Go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Select the app you want to work with.
4. Click **Actions > Apply to Label**.
5. Select the label that represents the iOS devices for which you want the selected app to be displayed.
6. Click **Apply**.

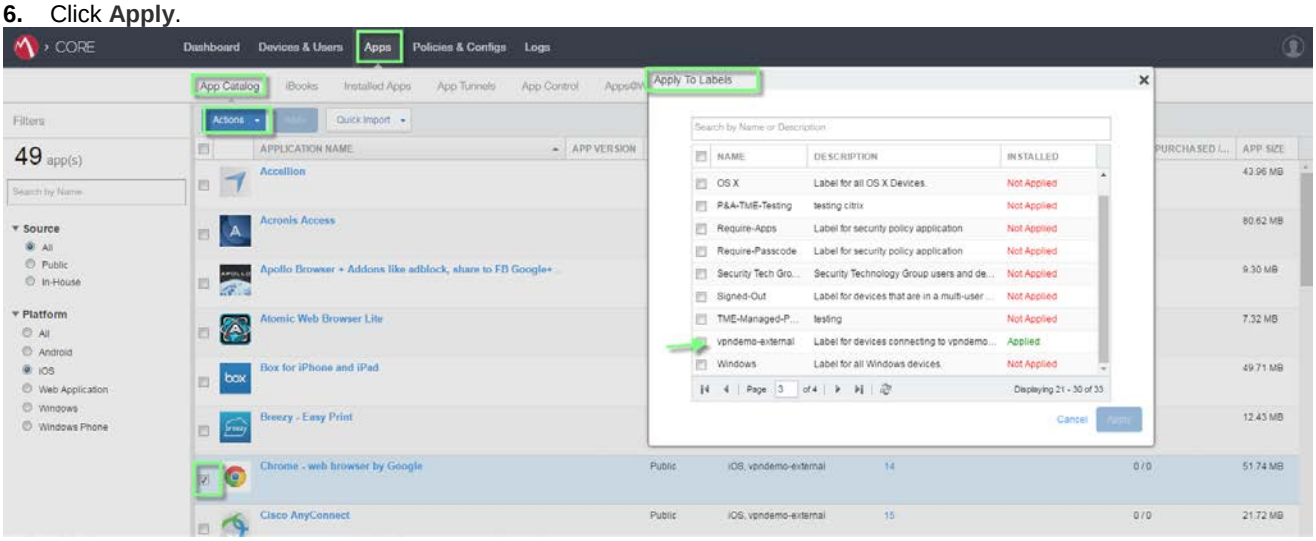


Figure 5. Apply label to App(s)

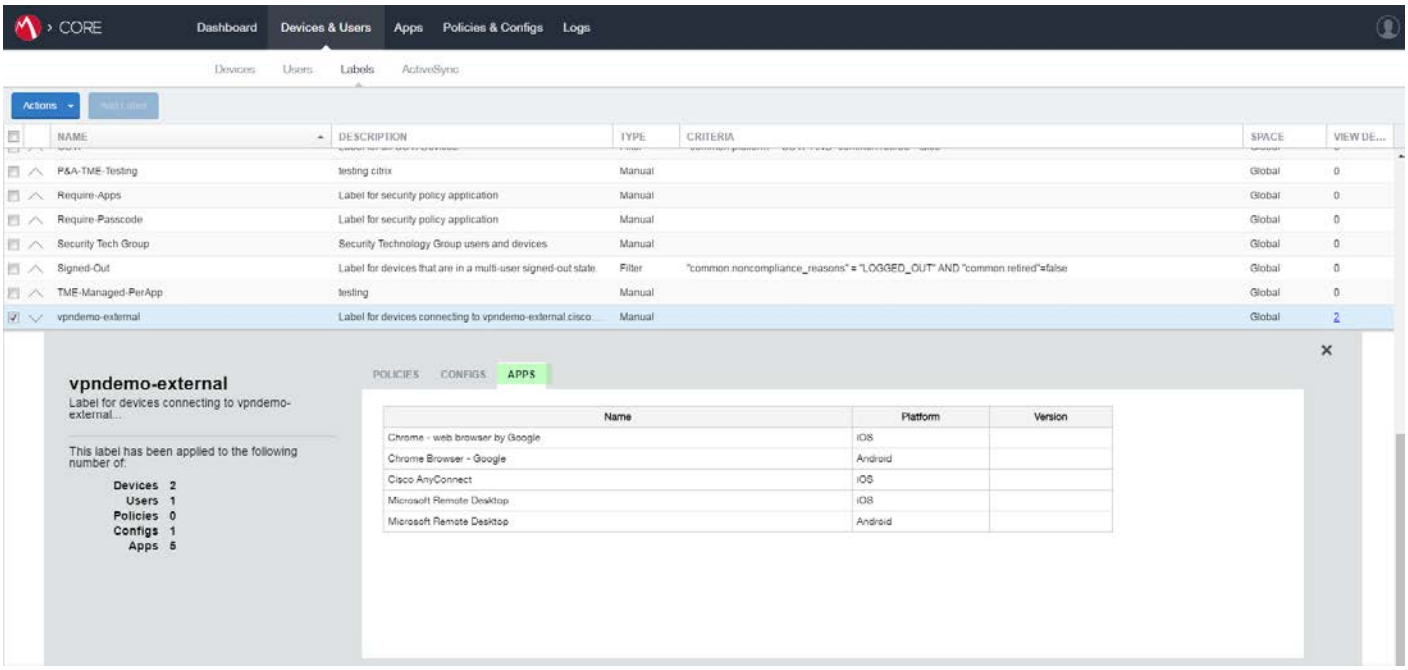


Figure 6. List of Apps assigned to label

Users & Devices

The Users and Devices pages enable you to manage enterprise devices. Use these pages to:

- Register/enroll a new device and associate it with a user
- Register/enroll devices in bulk mode
- Display a list of registered devices
- View and manage devices connected through ActiveSync
- **Apply labels in order to group devices** ←
- Create, edit, and delete labels
- Locate, Lock, Wipe or perform other administrative actions on a device.

For additional help with managing Devices & Users please reference:

https://help.mobileiron.com/customer/apex/AwsHelp?topic=ProductGuides/AdminGuideVSP70/mgphones/Overview_of_managing_devices_and_users.htm

The next step is to associate an iPad with the label associated with the VPN Configuration to complete our MobileIron configuration for this use case. This is done by selecting the device, clicking on 'Actions' and then 'Apply to Label'

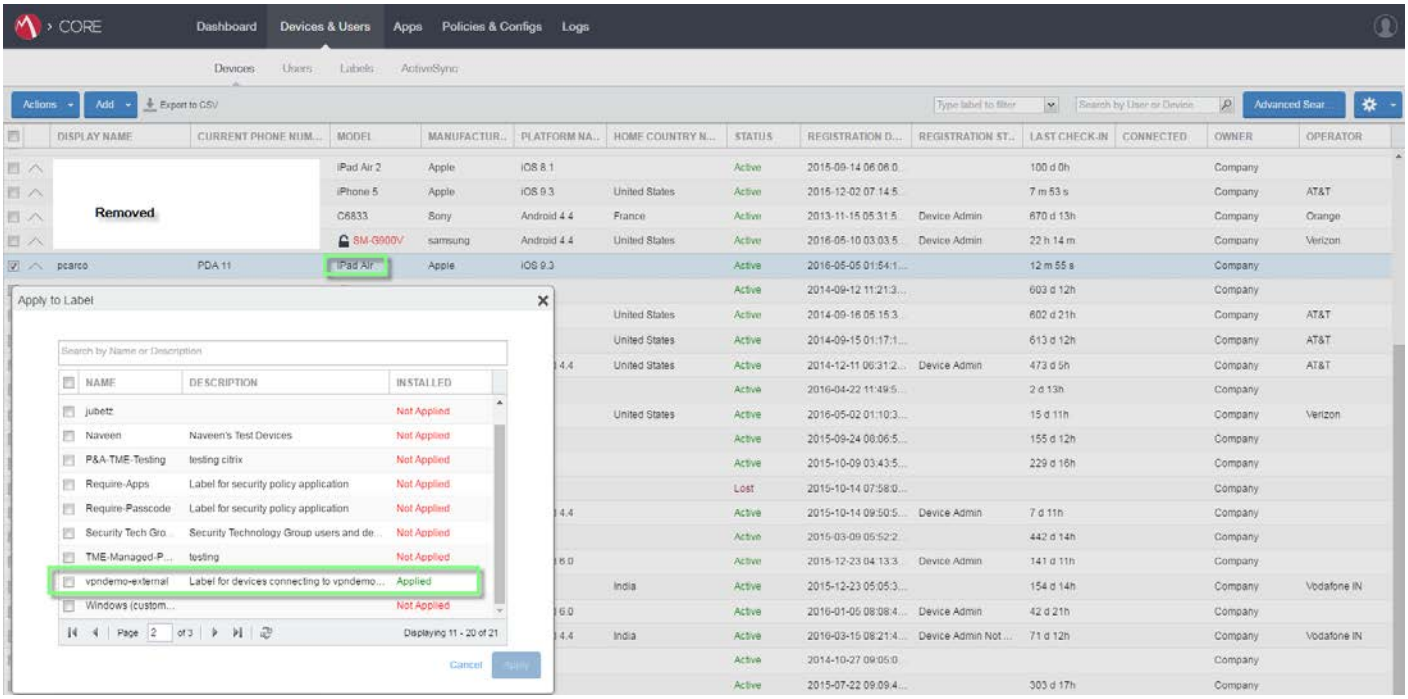


Figure 7. Applying a label to a device

Cisco Enterprise Application Selector Tool

The Application Selector Tool is a standalone application that supports policy generation for both Android and Apple iOS devices. Download the Cisco AnyConnect Enterprise Application Selector tool from the Cisco.com AnyConnect Secure Mobility Client v4.x Software Center.

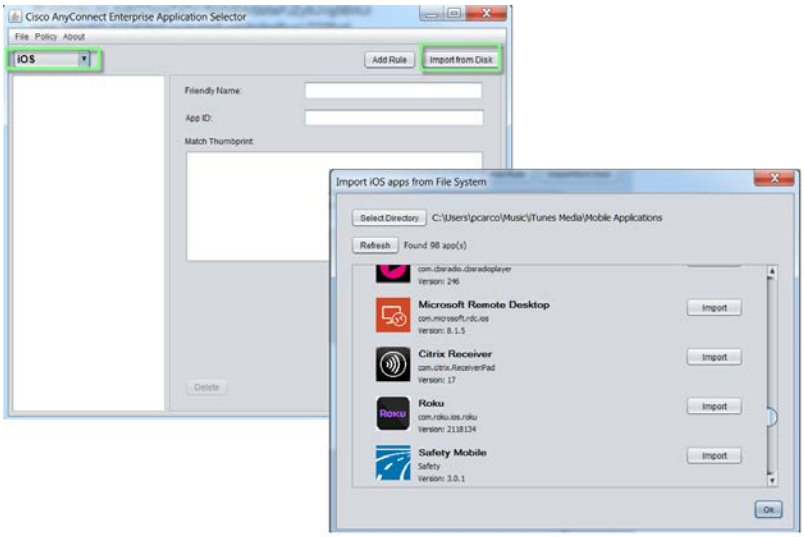


Figure 8. Cisco Enterprise Application Selector Tool

The Per App VPN policy consists of a set of rules, where each rule identifies an app whose data flows over the tunnel. We will use the Selector Tool to create the PerApp policy and then ultimately apply it to the ASA. This tool allows you to import specific applications as shown above in Figure 8. In this use case and since our MDM solution is configuring the permitted Apps for the device we will simply use a wildcard policy and the ASA will permit any Application specified by the MobileIron configuration

Configuration Options:

http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/anyconnect-mobile-devices.html

• 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`.

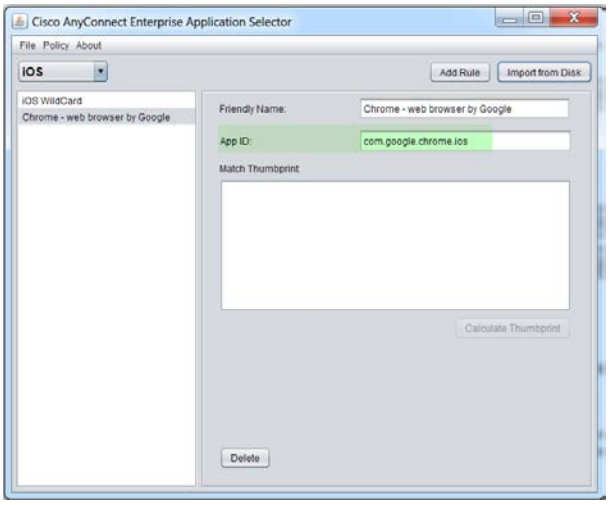


Figure 9. App ID reverse-DNS format

• Alternatively, you may enter this app-specific information directly, an example would be to import from your local iTunes directory.

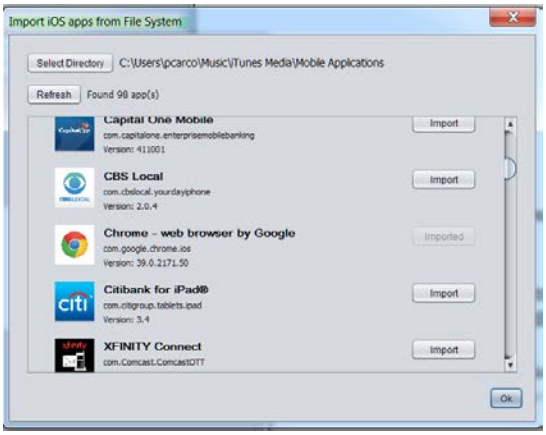


Figure 10. Import IOS apps from File System

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

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

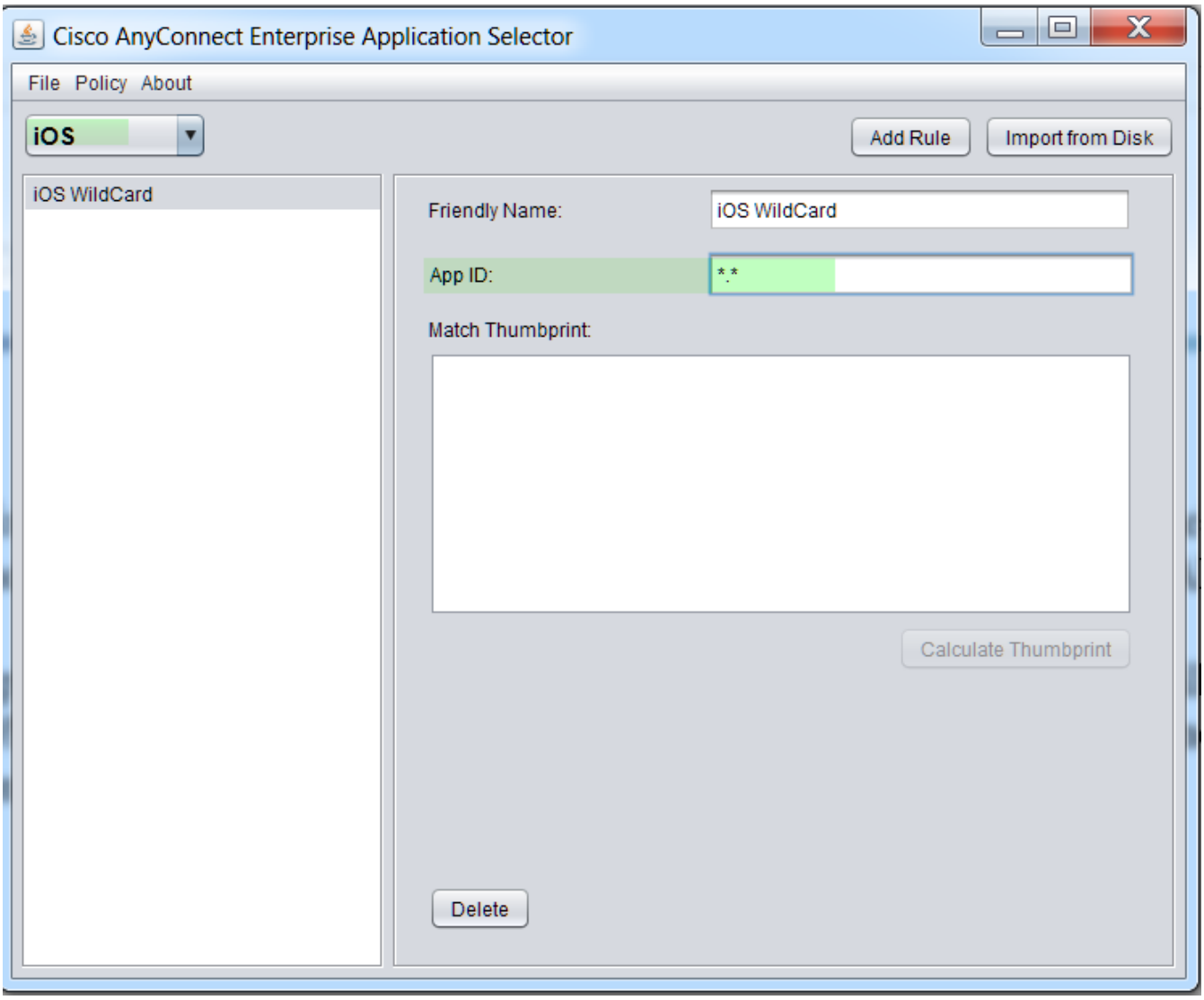


Figure 11. iOS Wildcard

The content of the PerApp policy will first be compressed and then Base64 encoded. The PerApp policy will be delivered as a custom attribute which is provided by the ASA as part of the Aggregate Authentication config message which is an XML exchange used between the ASA and AnyConnect for several reasons not only specific to PerApp. If the custom attribute for PerApp is received by AnyConnect then full tunneling is not allowed, if there is no PerApp custom attribute received by AnyConnect then the client assumes full tunneling operation.

Once your policy is created click on 'Policy' and 'View Policy' and the compressed Base64 format will be revealed. It is a good time to cut and paste to your clipboard since you will need this when configuring the ASA.

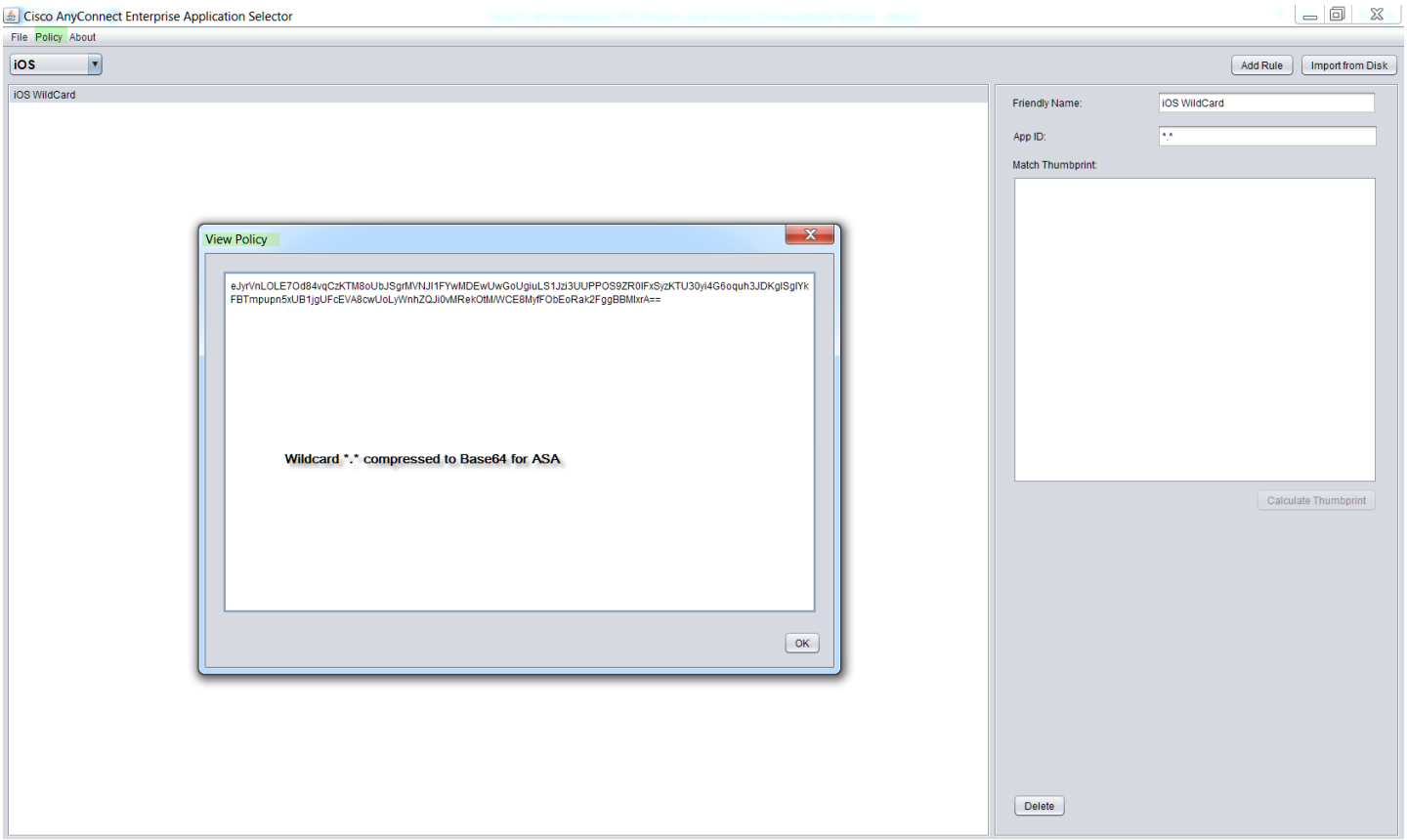


Figure 12. PerApp View Policy

Cisco ASA Configuration

Configuring PerApp VPN is a relatively easy task and the following steps will help you enable your ASA to support the solution.

Note: The following steps assume all other required configurations to support AnyConnect sessions are in place including the AnyConnect Client Profile. The AnyConnect Client Profile is an XML file that allows the Administrator to configure client features such as the server list which is a list of head ends (ASA's) that the user will connect to and receive a PerApp configuration.

Please see the following for more information regarding AnyConnect Client Profiles

http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30/ac02asaconfig.html#17671

Custom Attribute Configuration

Step 1:

In this step we will add the **PerApp** custom attribute **Type**. This is only defined once but used for each PerApp policy the Admin creates.

- In ASDM navigate to Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes
  - Select 'Add' and enter 'perapp' (must be all lowercase) in the box labeled 'Type' and enter anything you would prefer in the 'Description' field
  - Click 'Ok' , 'Apply' and 'Save'

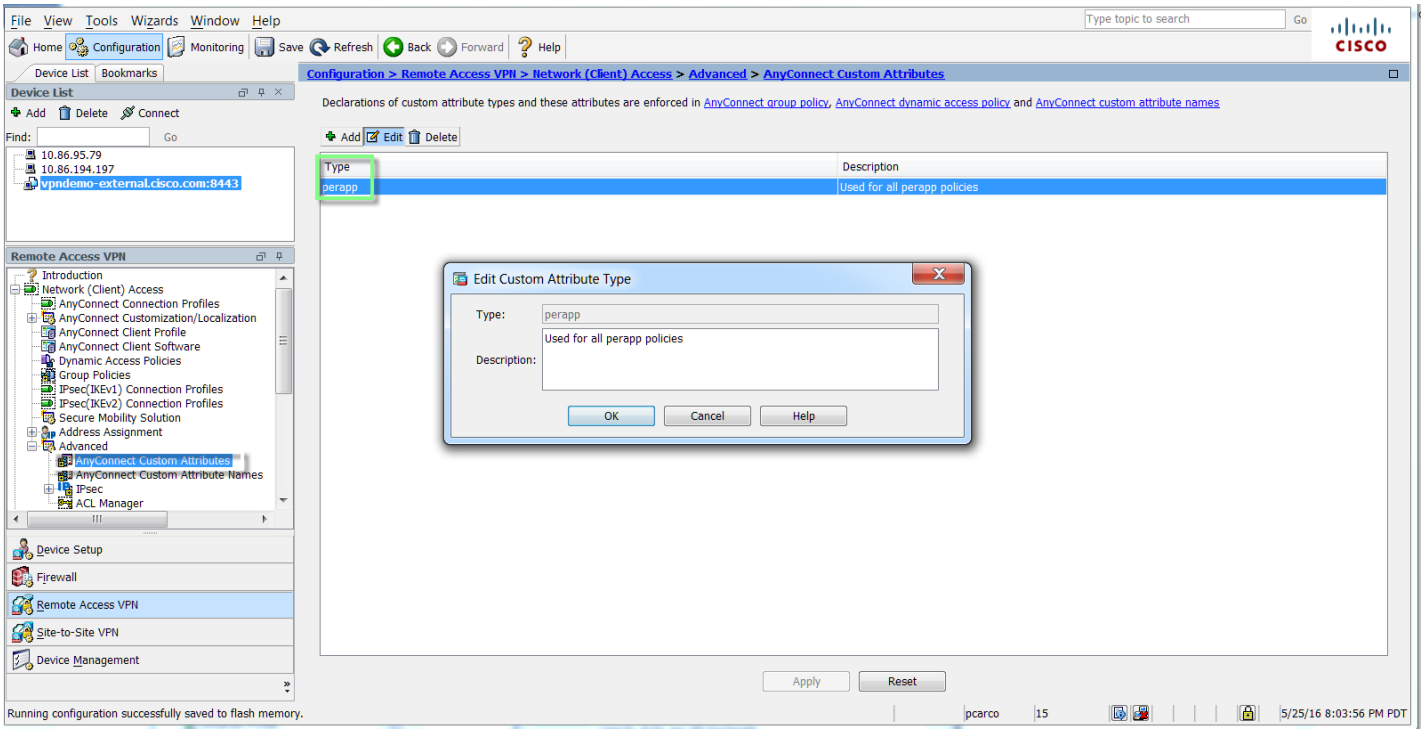


Figure 13. AnyConnect Custom Attribute – PerApp

Step 2:

In this step we create the actual PerApp policy that will apply to a Dynamic Access Policy later in this guide.

Using ASDM Navigate to:

Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names

Click on '**Add**', Ensure the **Type** is set to '**perapp**', Name the policy and cut/paste the Base64 blob from the Cisco AnyConnect Enterprise Application Selector Tool

Click Ok, Ok, Apply & Save and now we have a perapp policy we can either apply to the ASA Group-Policy or DAP. We will use DAP in this guide.

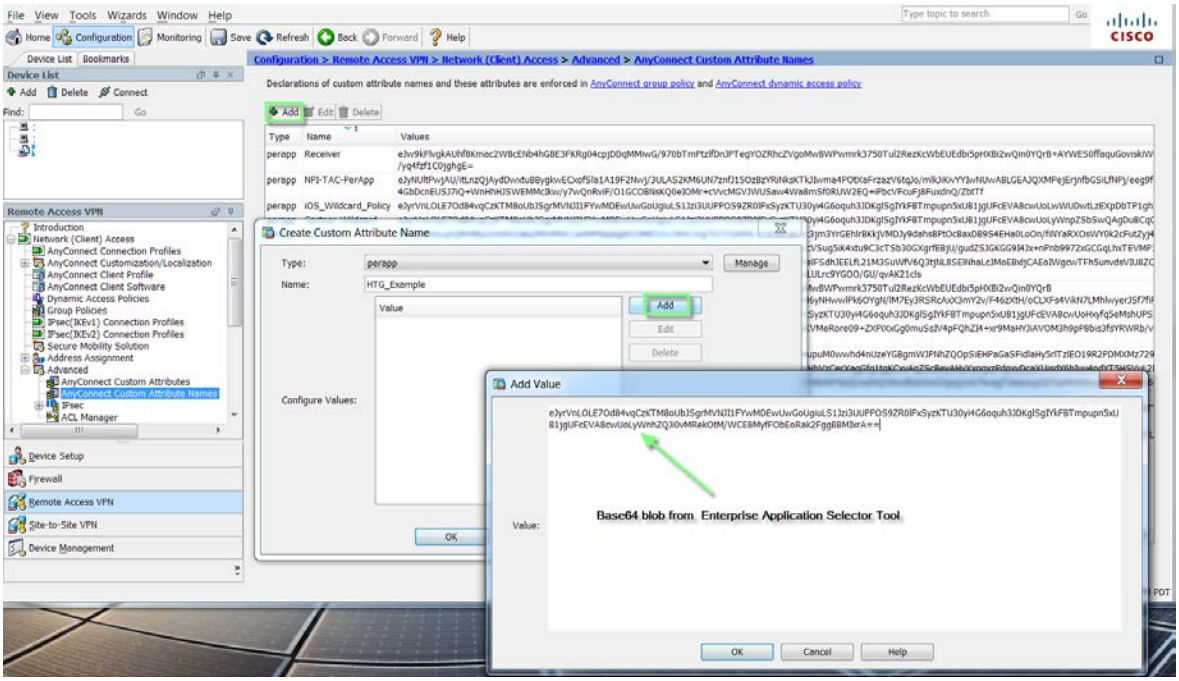


Figure 14. Adding new PerApp Policy to ASA

The final result is that the PerApp policy is added to a list of available policies and can be referenced by a Group-policy or DAP

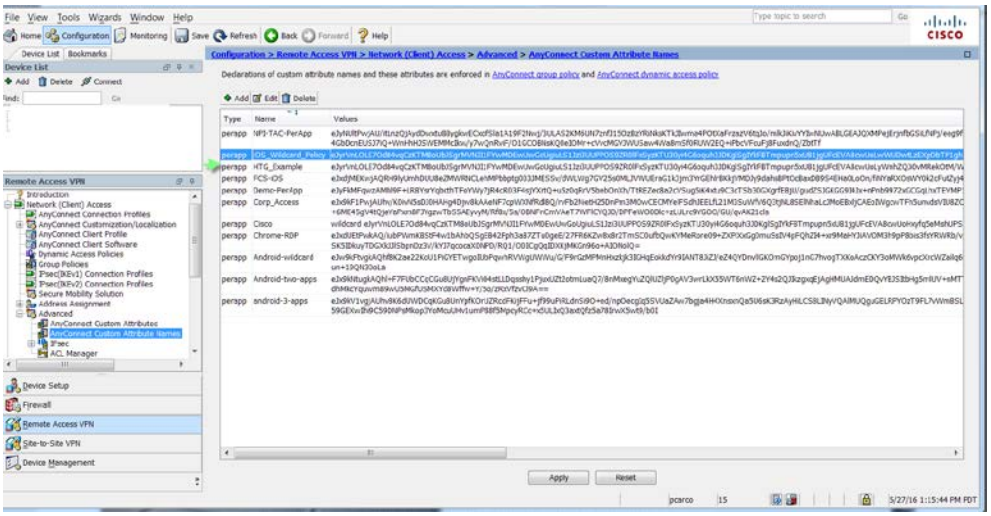


Figure 15. List of PerApp polices (Custom Attribute Names)

Group-Policy and Dynamic Access Policies

The PerApp Policy can be assigned to either an ASA Group-Policy or Dynamic Access Policy (DAP). It is important to understand the hierarchy in which the ASA uses to assign configuration attributes to a user. There are multiple ways users can be assigned attributes but when working with PerApp only the Group-Policy and DAP are possible. Keep in mind if you apply PerApp policy to a group-policy as well as DAP and the user is assigned to both DAP will always win out and the user will receive the PerApp policy from DAP.

The ASA applies attributes in the following order:

1. **Dynamic Access Policy attributes**—Take precedence over all others.

2. User attributes—The AAA server returns these after successful user authentication or authorization.

3. **Group policy attributes** —These attributes come from the group policy associated with the user. You identify the user group policy name in the local database by the vpn-group-policy attribute or from a RADIUS/LDAP server by the value of the RADIUS CLASS attribute (25) in the OU=GroupName. The group policy provides any attributes that are missing from the DAP or user attributes.

4. Connection profile (tunnel group) default-group-policy attributes — These attributes come from the default group policy associated with the connection profile. This group policy provides any attributes that are missing from the DAP, user or group policy.

5. System default attributes—System default attributes provide any values that are missing from the DAP, user, group policy, or connection profile.

Policy Enforcement of Permissions and Attributes Hierarchy

Group-Policy PerApp Configuration

For a Group Policy navigate to: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Custom Attributes.

Here the Admin will be able configure the group-policy to apply a certain PerApp policy to users that are assigned to this group-policy. It is possible to have multiple group-policies each with its own PerApp policy.

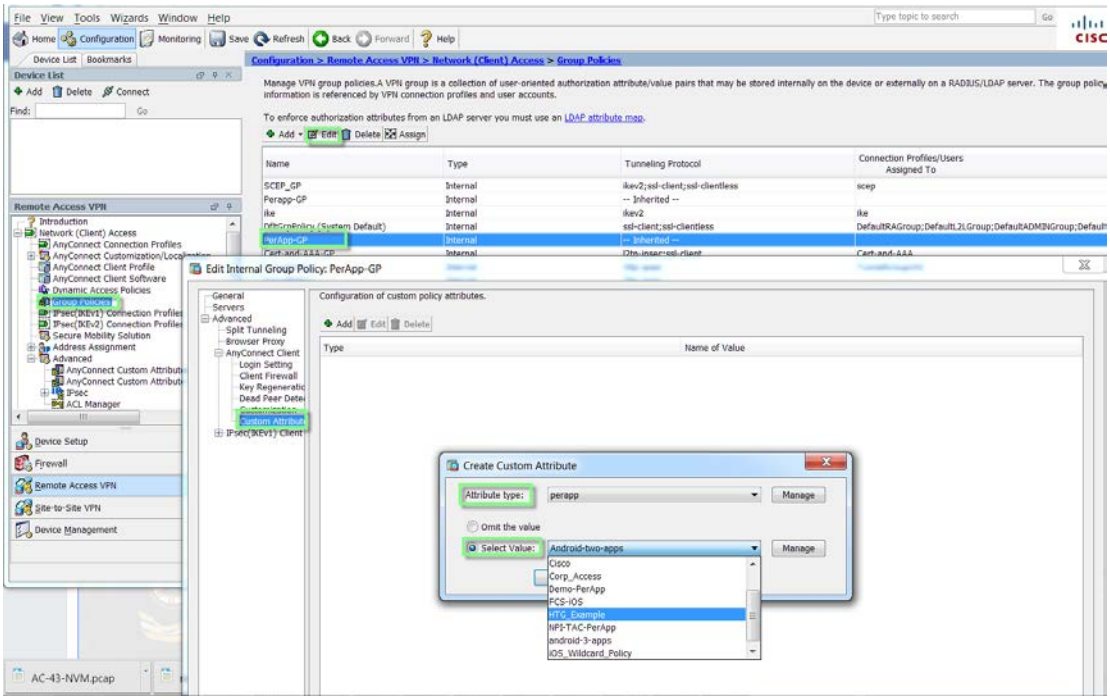


Figure 16. Group-Policy PerApp Configuration

Dynamic Access Policy (DAP)

Dynamic access policies (DAP) on the ASA allows you to create an authorization policy based on AAA and Endpoint criteria and then apply certain permissions to the devices matching the DAP Record.

Please reference the following document for more details regarding Dynamic Access Policies
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/vpn/asdm_71_vpn_config/vpn_asdm_dap.html#15525

To configure 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 (Fig 18) select the AnyConnect Custom Attributes tab and Add the PerApp policy to the DAP record. Users that are assigned this DAP record will have this PerApp Policy applied to the session. In the example below (Fig 17) the DAP record is configured to match any iOS device that is running iOS 9.3.1 and then apply the iOS_Wildcard_Policy. Note: there could also be AAA criteria as well as other Endpoint criteria defined in this DAP record but for the sake of simplicity we have kept it at a minimum.

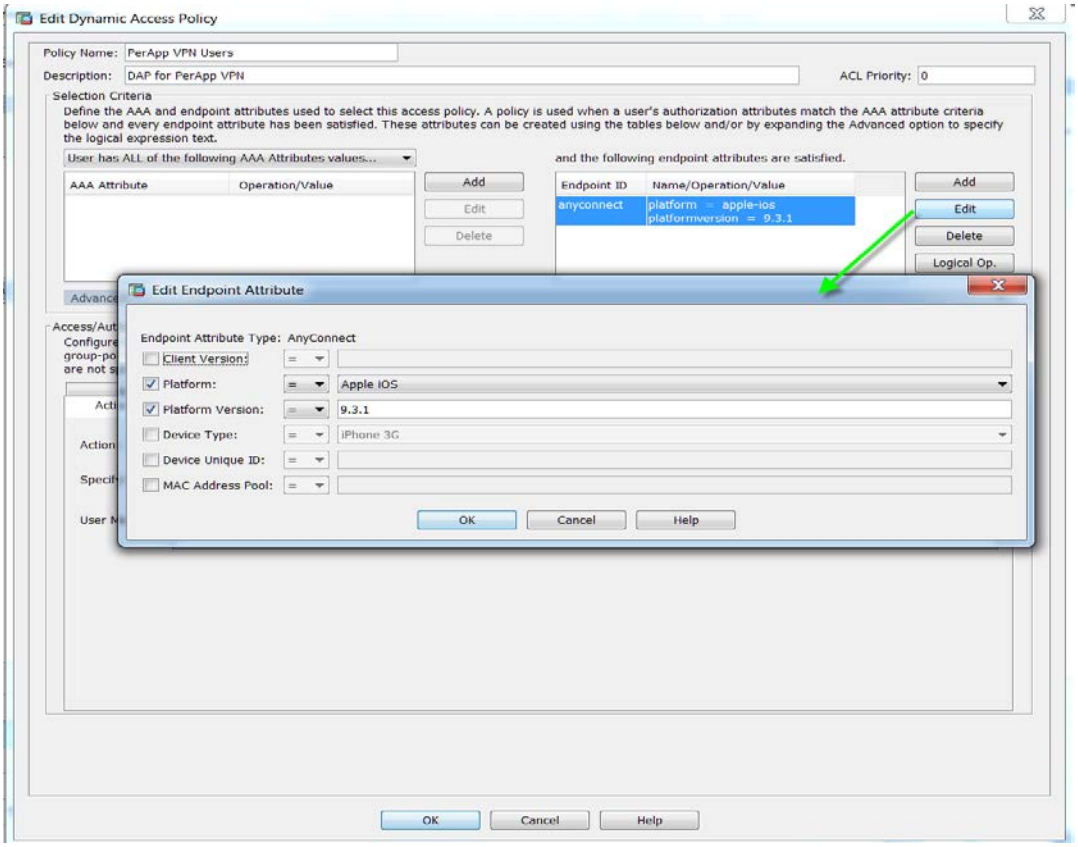


Figure 17. Dynamic Access Policy - Endpoint ID defined

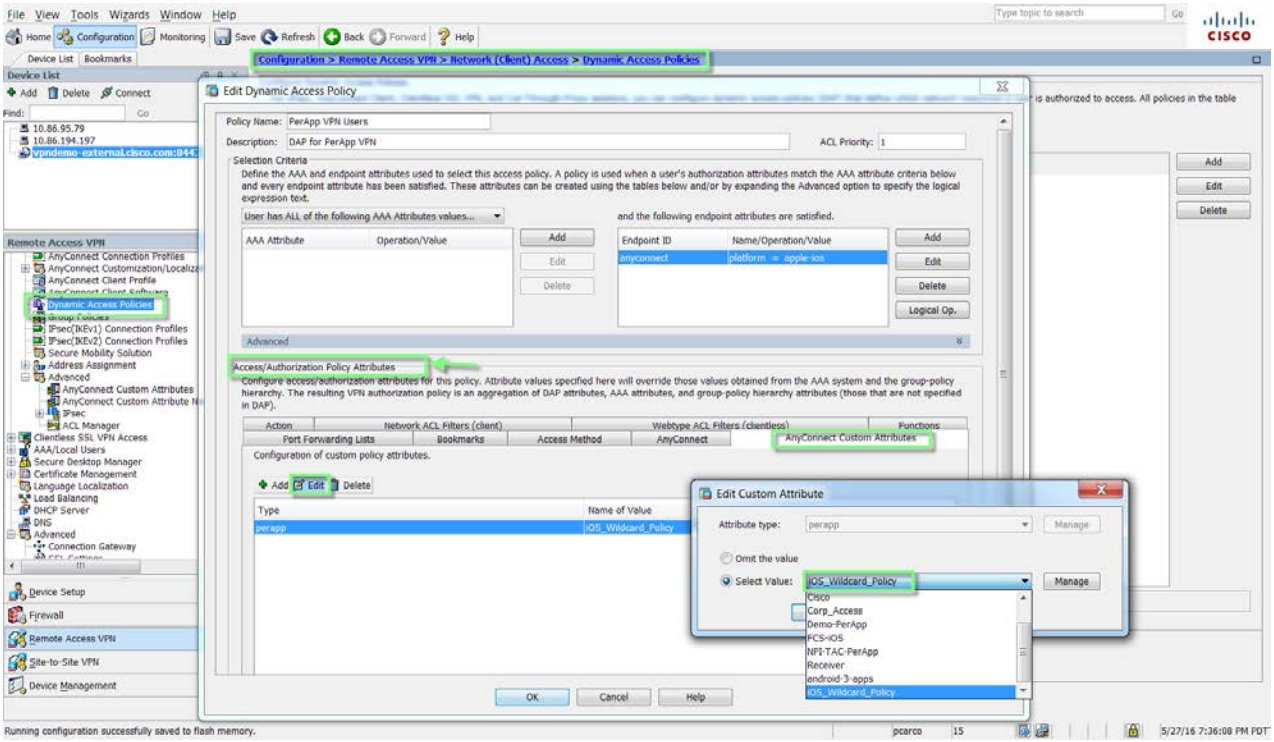


Figure 18. Dynamic Access Policy – PerApp Configuration

iOS Device Configuration & Testing

In this section we will focus on an actual iOS device and the configuration required to allow PerApp to function properly.

Test Setup:

- Apple **iPad** Air **MD789LL/A**
- **iOS version 9.3.1**
- AnyConnect v4.0.05038
- ASA 9.6.1(3)
- ASDM 7.6(1)
- MobileIron Mobile@Work App v.7.2.0

MobileIron Mobile@Work

The iPad being used for this test has been registered with MobileIron using the Mobile@Work App that can be downloaded from iTunes for iOS or Google Play for Android. Mobile@Work works in conjunction with MobileIron Core shown earlier in this guide. The Administrator of the MobileIron Core solution will need to provide a registration URL and credentials for the initial onboarding to users in order to become registered and compliant.

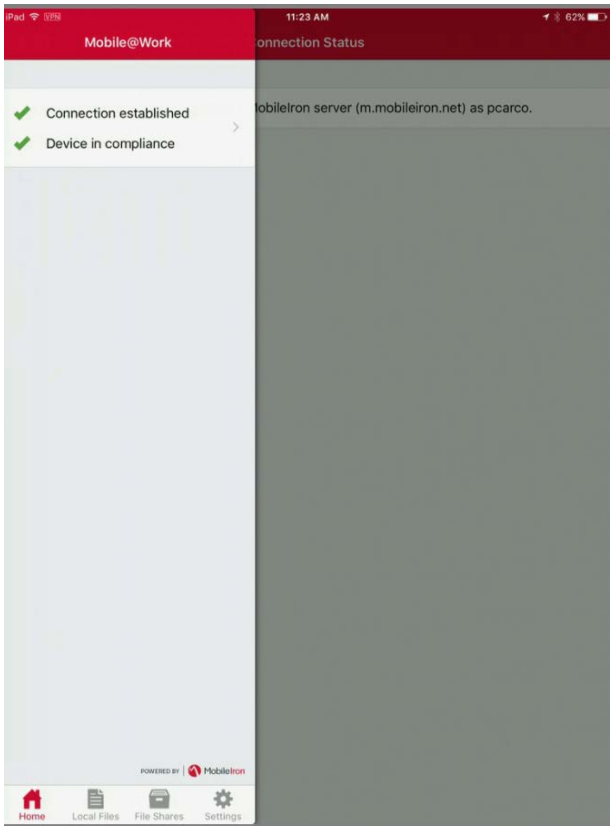


Figure 19. Mobile@Work iOS App

MobileIron Apps@Work

Apps@Work provides the tools for distributing and managing mobile apps. You can use Apps@Work tools to facilitate installation of standard corporate apps, as well as to help regulate the apps that your users are bringing into the enterprise. Apps@Work tools consist of: • App Catalog (previously called “app distribution library”) • App Control • Installed Apps (previously called “device app inventory”)

Source: https://community.mobileiron.com/docs/DOC-4290

The Apps@Work container is pushed once the registration of the endpoint takes place and allows the user to download apps from the MobileIron Core App Catalog. This iPad matched both the Manual label we created earlier as well as other dynamic labels which results in this list of applications. Note: Only Chrome and the Microsoft RDP are allowed by the PerApp configuration.

Figure 20. MobileIron Apps@Work

AnyConnect

AnyConnect v4.0.x is the first release which is compatible with Apple iOS Per App VPN. This capability must be used in conjunction with a MDM/EMM vendor and requires at a minimum ASA 9.3(2) or later licensed with AnyConnect Plus, Apex or VPN Only license. The iOS device must be running iOS 8.3 or later. AnyConnect for Mobile devices is downloadable from the respective stores depending on the OS i.e., iTunes for iOS.

Figure 21. AnyConnect for iOS

).

The AnyConnect Connections section will show you all the profiles either received by an ASA, or from the MDM. This iPad matched several labels defined on MobileIron Core. The connections with PerApp enabled are grouped together at the bottom. The vpndemo-external PerApp VPN was the VPN configuration defined earlier (Figure 3.) and is currently active.

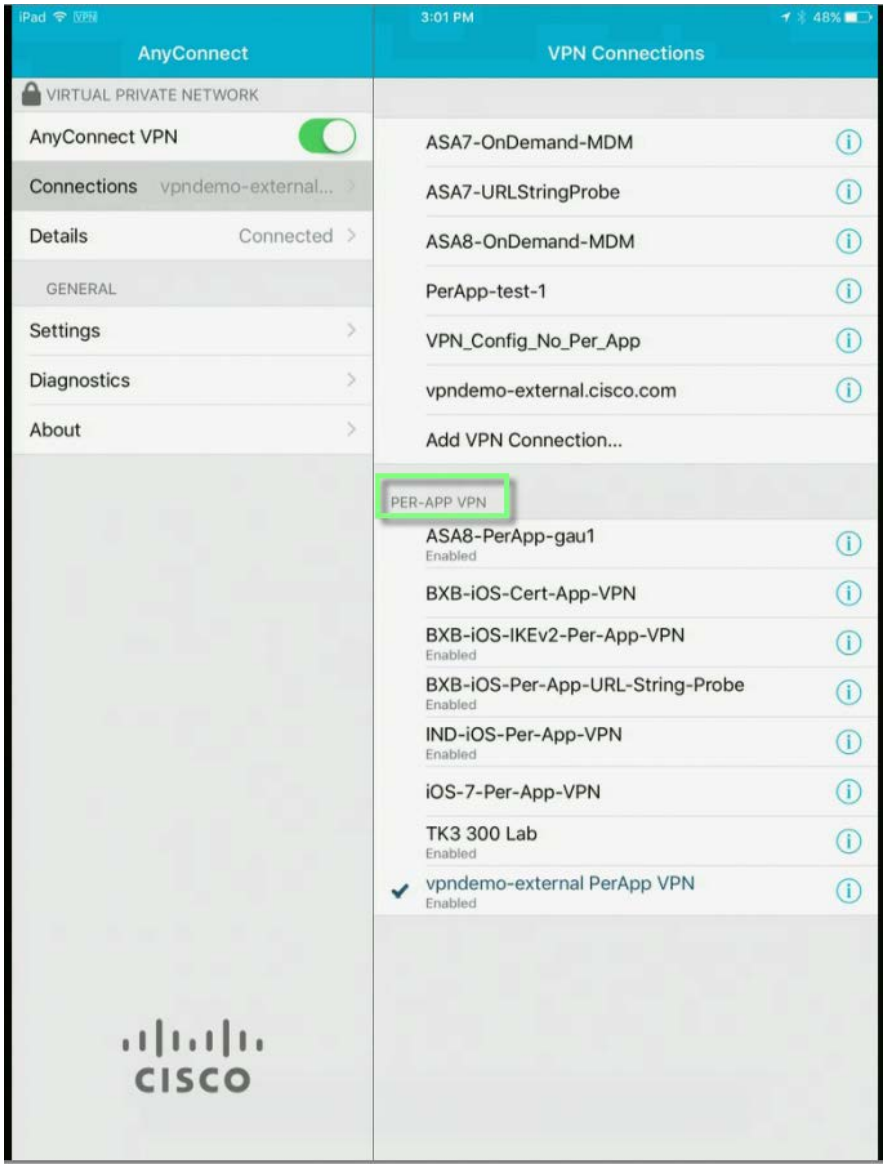


Figure 22. AnyConnect Connections list

With a check next to the connection and by clicking on the information symbol to the right of the connection name ‘vpndemo-external PerApp VPN will open up another window that will allow you to view the /**Advanced**’ settings and then click on ‘**App Rules’** you notice the two apps we defined; Chrome and Microsoft RDP.

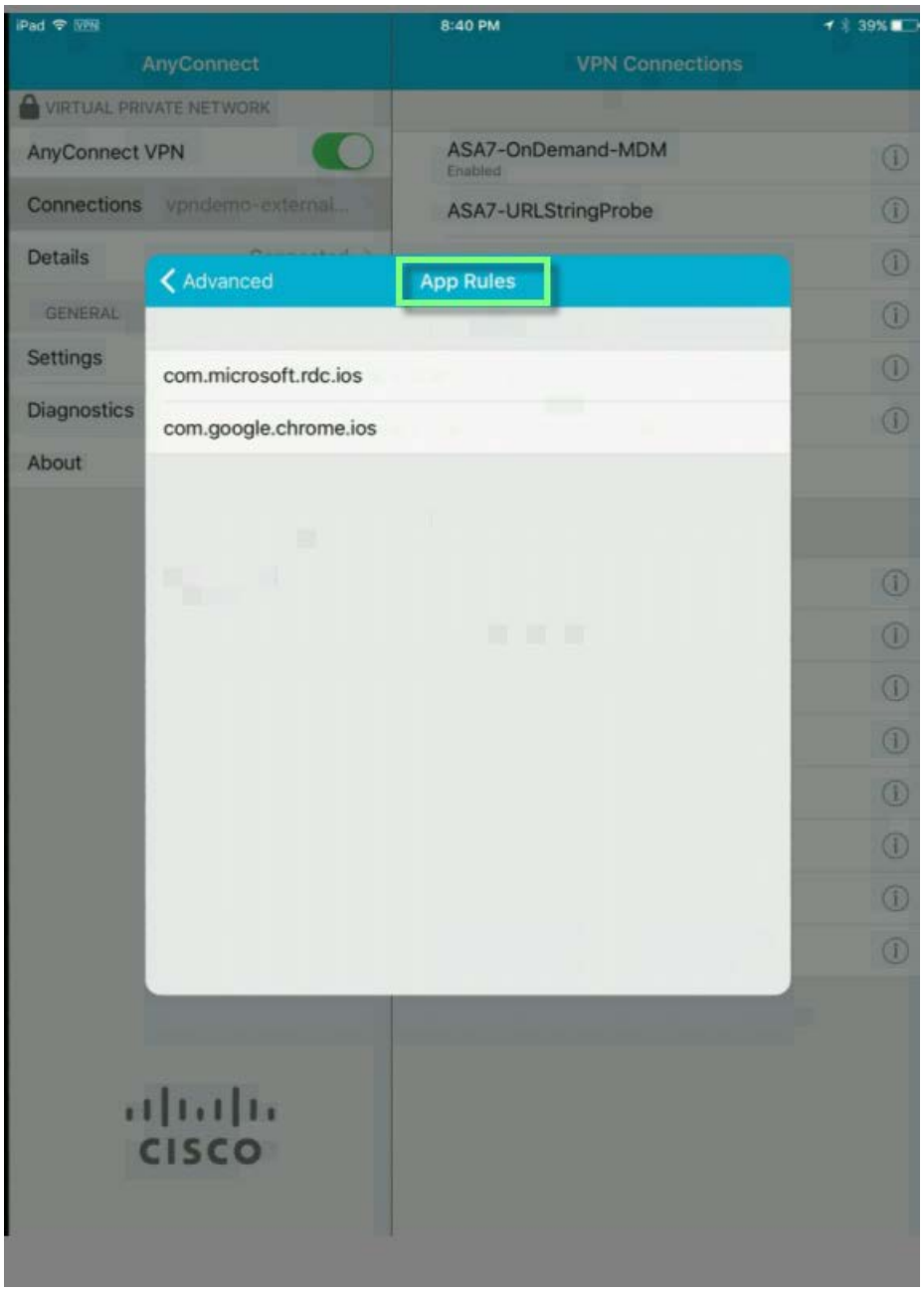
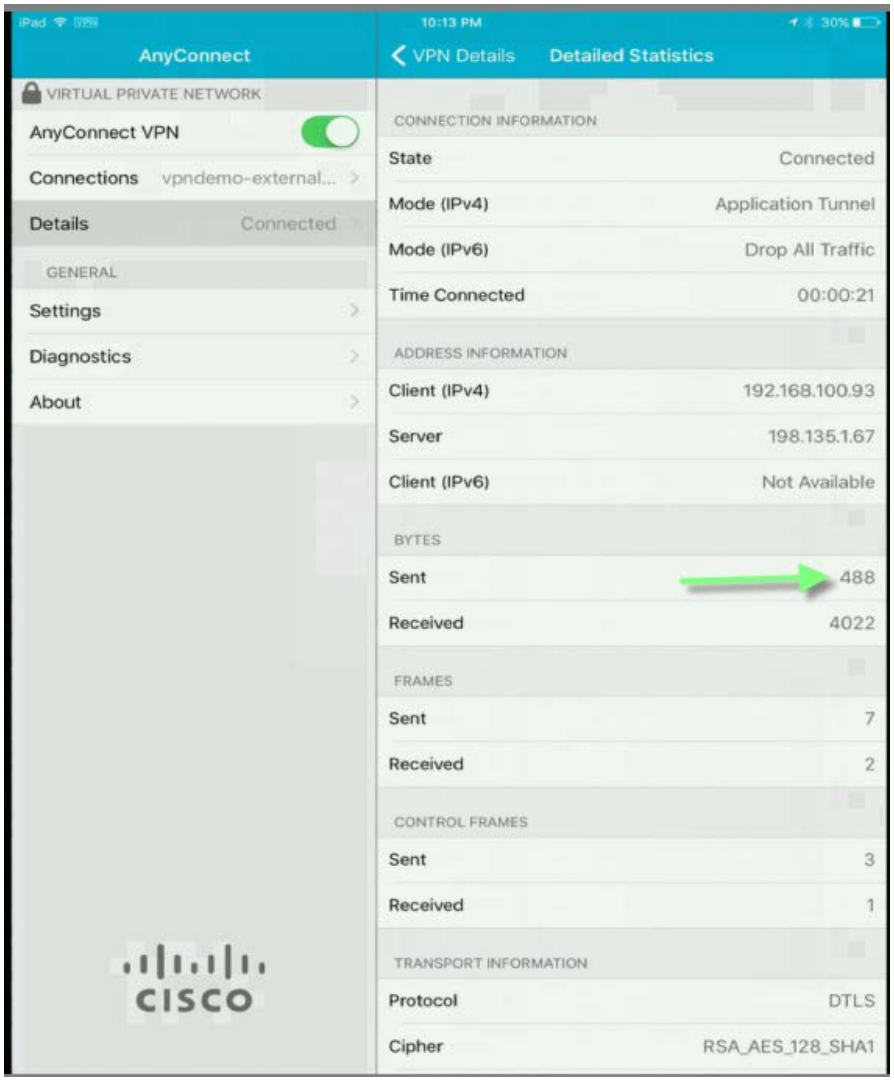


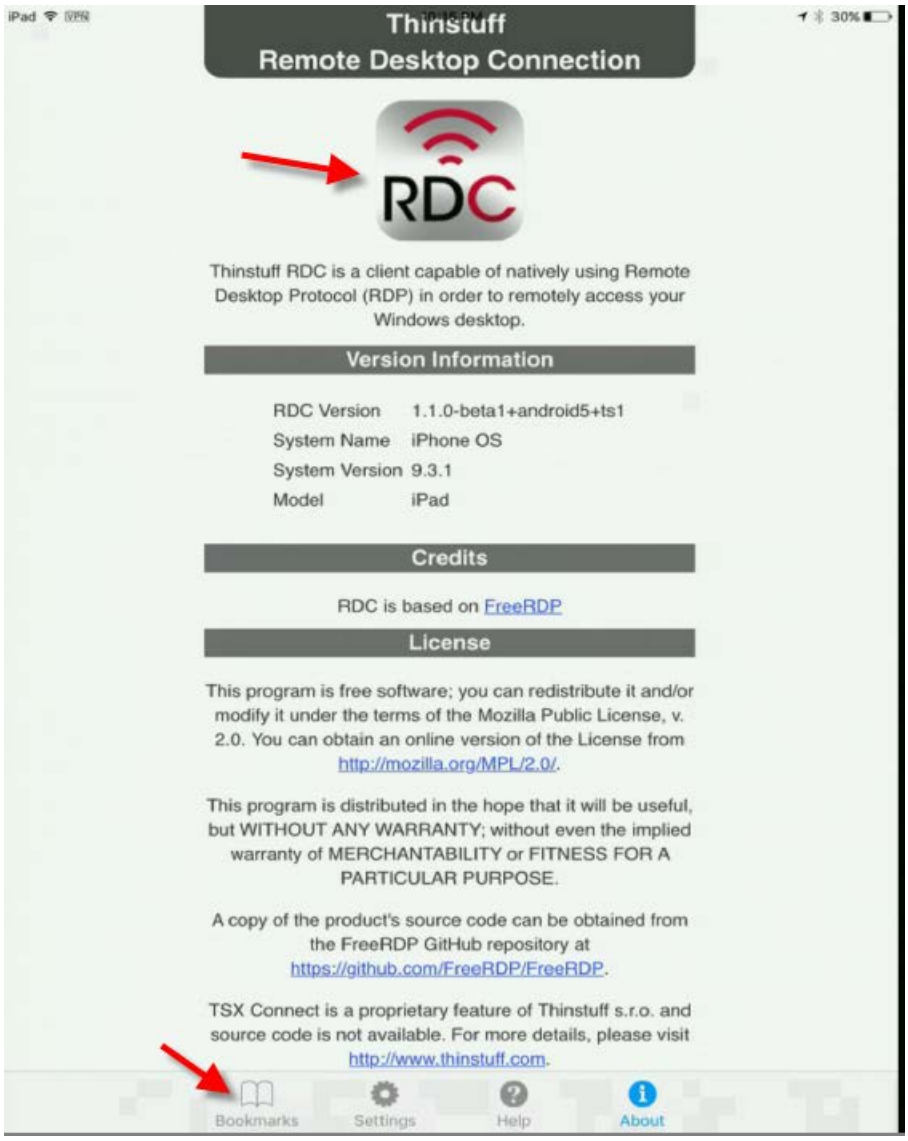
Figure 23. AnyConnect App Rules

Testing/Demo

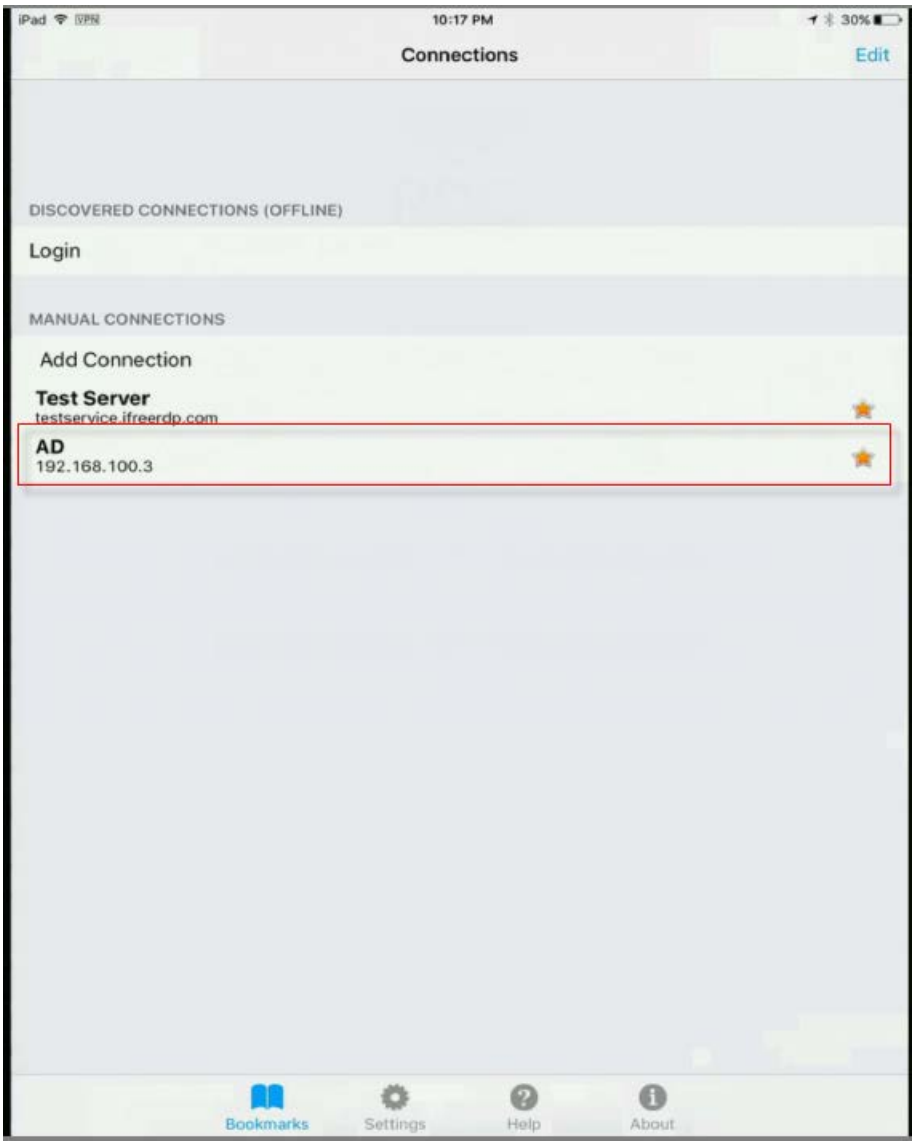
This is a simple test to demonstrate that configuration in place operates as expected. The PerApp policy permits the two Apps Microsoft RDP and the Chrome browser. We will attempt to use an RDP app other than the Microsoft RDP app which should fail. We will then use the MS RDP App which should be able to traverse the tunnel.



Note Sent Byte count. No traffic has been sent since tunnel was established

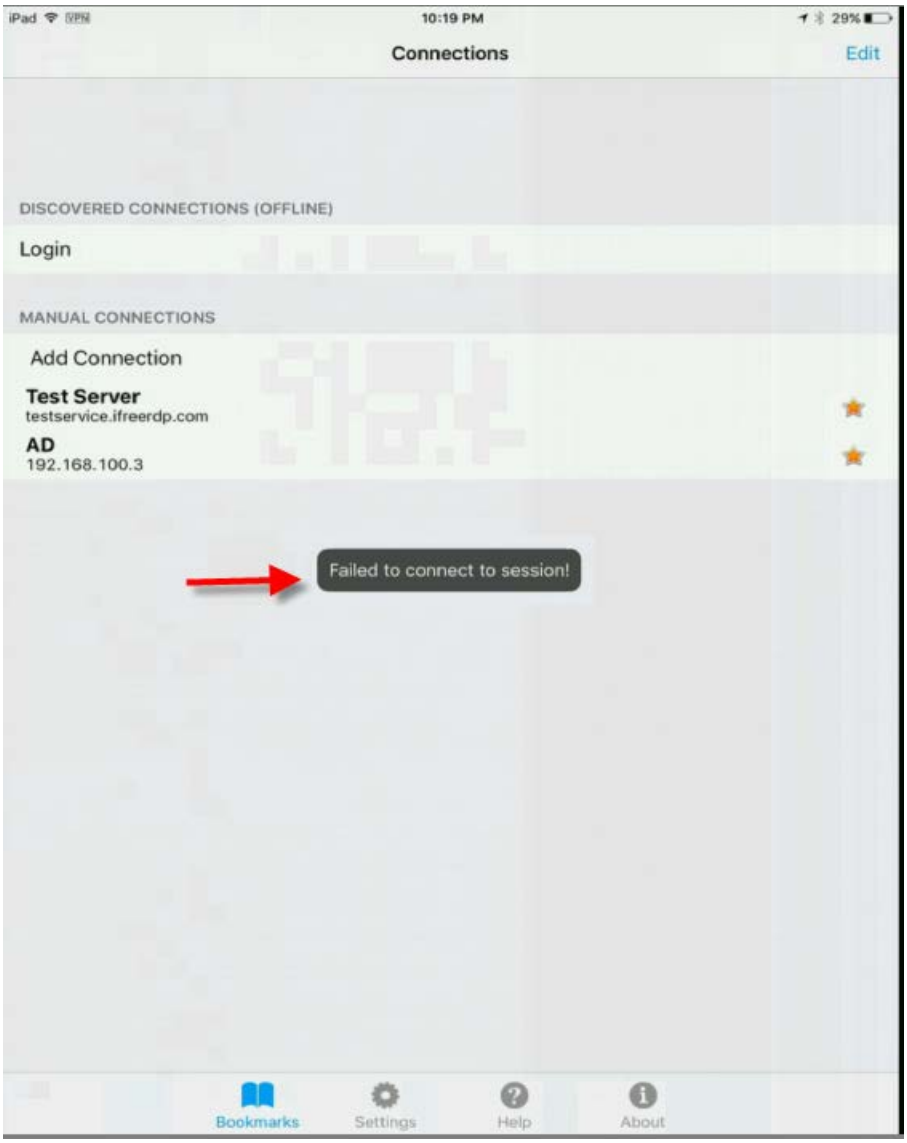


With the session established to the ASA we attempt to use another RDP application that is not one of the permitted apps

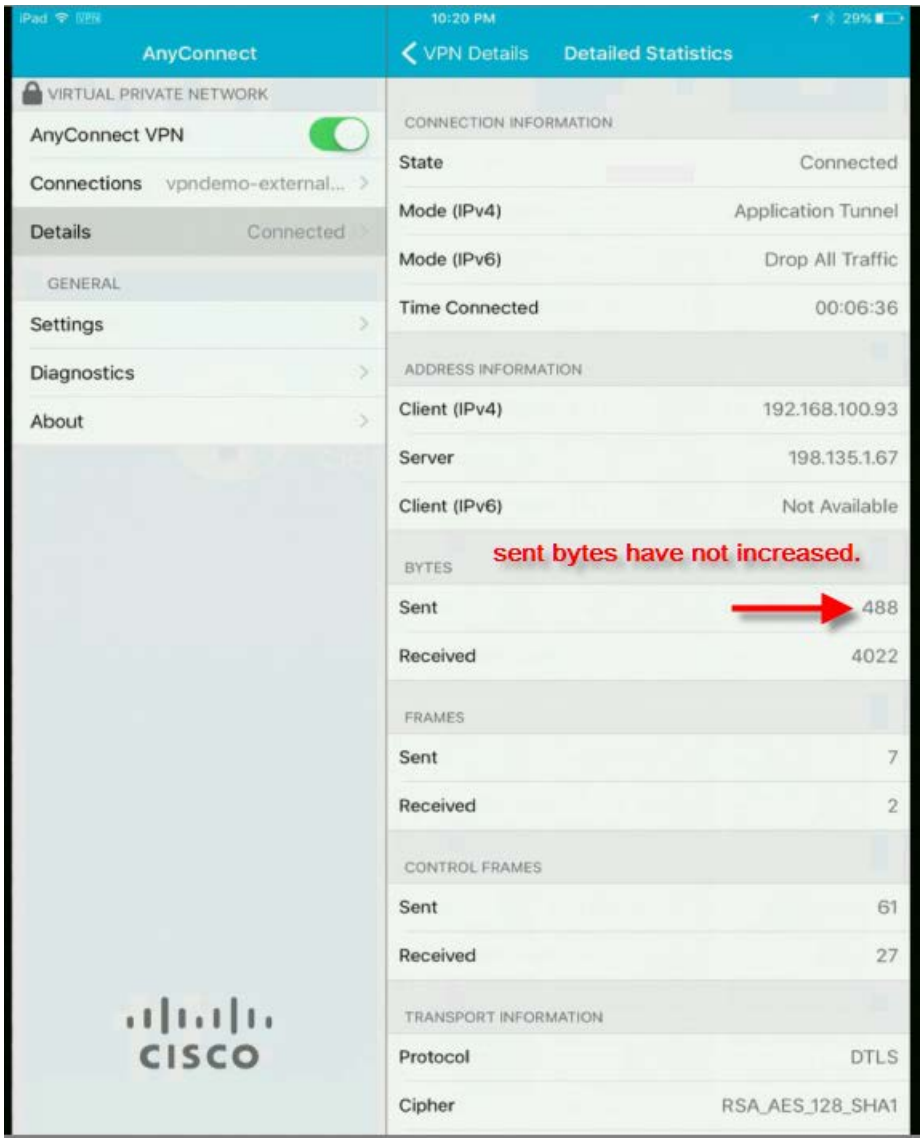


Attempt to establish RDP session to host on inside network.

RDP is attempting to connect.

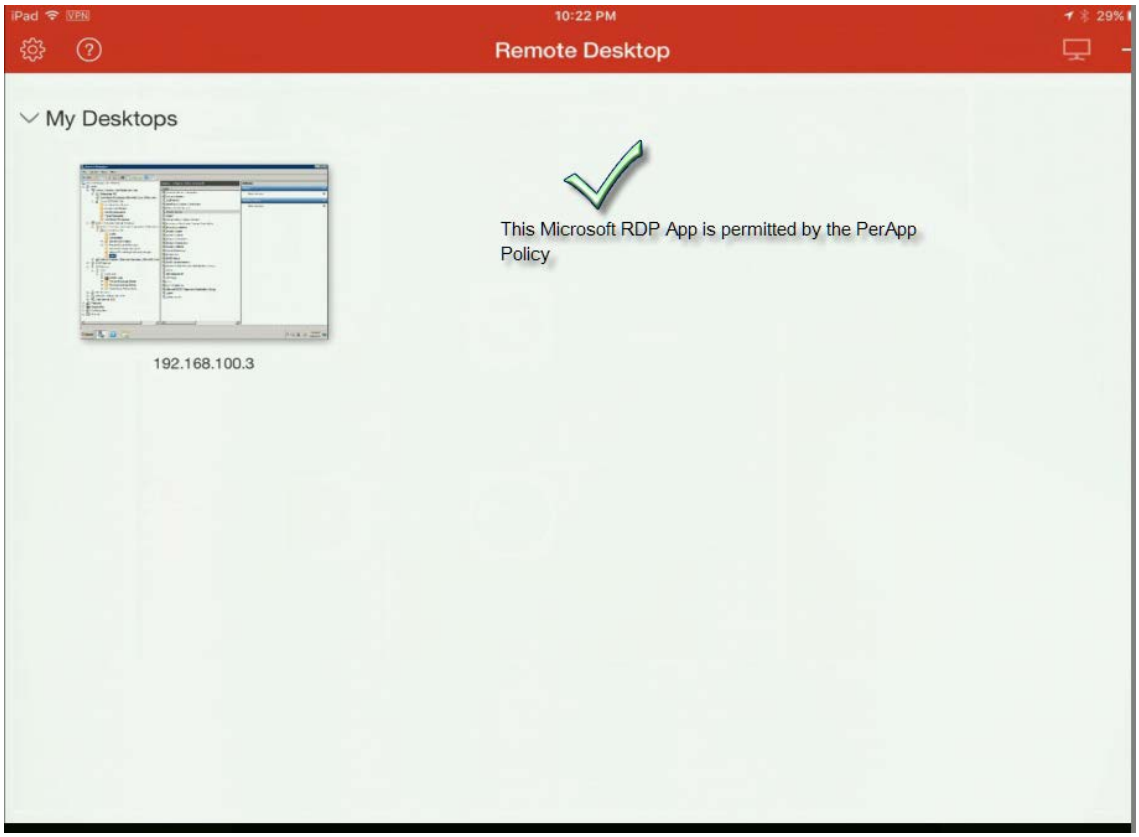


RDP attempt fails.

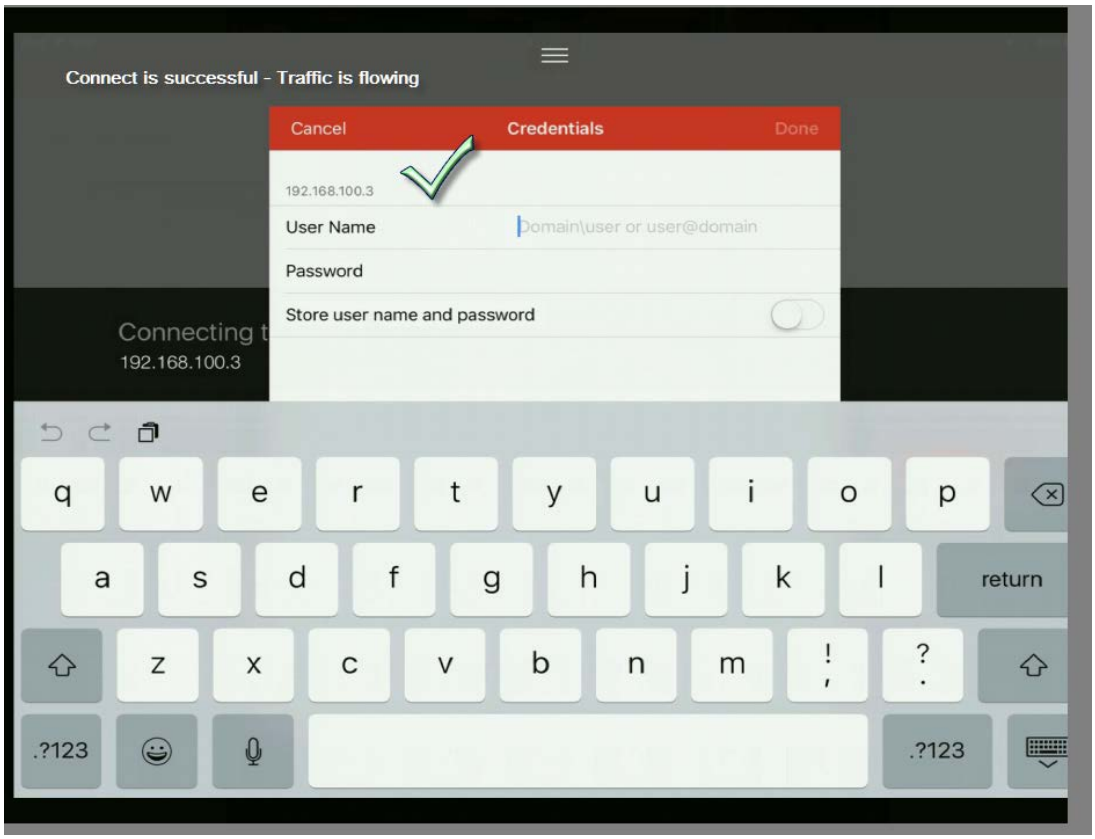


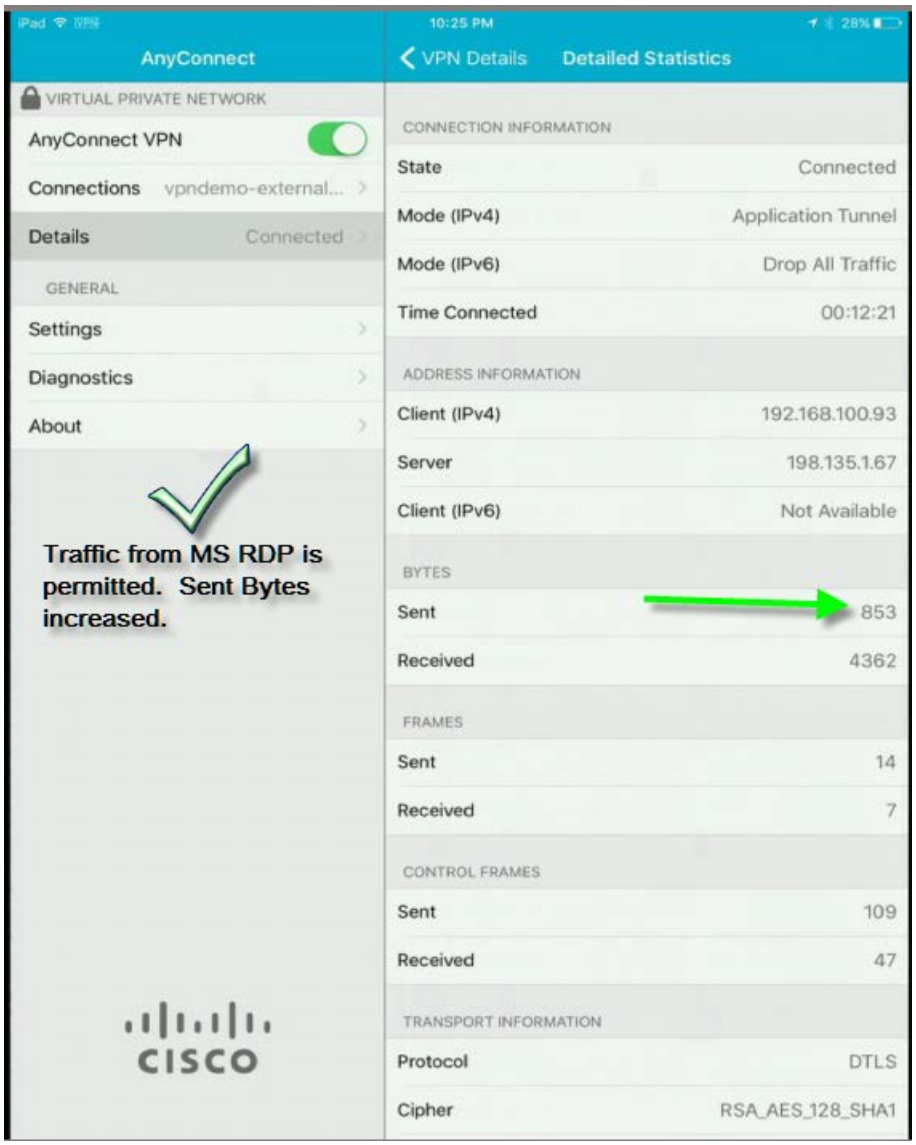
Note that the Sent Bytes has not increased.

We will now test with the MS RDP App which is permitted.



RDP Session is established immediately





Note that Sent Bytes have increased due to the MS RDP App being permitted.