



MobileIron

MobileIron Cloud

Cisco Security Connector Setup Guide

October 2018

Version 1.0

www.mobileiron.com

Confidential Information of MobileIron, Inc

Copyright Notice

© 2018 MobileIron, Inc. All rights reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited.

Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication.

"MobileIron," the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

Contents

MobileIron and Cisco Security Connector Setup Guide	4
Introduction	4
Requirements	4
Overview and Integration workflow	5
Settings and Configuration	5
DEP and VPP in MobileIron	5
Enabling the Cisco Security Connector app with the Clarity AMP Dashboard	9
Enabling the Cisco Security Connector app with the Umbrella Dashboard	11
Reference	14
Contact Information	14

MobileIron and Cisco Security Connector Setup Guide

Introduction

Cisco Security Connector provides visibility and control for enterprise-owned and Unified Endpoint Management (UEM) managed Apple IOS system devices, such as iPhones and iPads. This increases security and compliance of mobile devices by providing the capability to audit workflow by users and applications. In addition, organizations can gain control over their mobile endpoints by regulating connectivity to the Internet through [DNS and IP requests](#)

MobileIron Unified Endpoint Management (UEM) solution will configure and manage iOS devices using Apple Device Enrollment Program (DEP) framework. This ensures all corporate security controls are enabled and applied. Along with this, MobileIron UEM solution will also manage application distribution via Apple Volume Purchase Program (VPP) and publish apps, in this case, the Cisco Security Connector app. MobileIron UEM solution will then help to configure the app on the device by pushing the mobileconfig file (a custom xml payload) that was provided by Cisco's Umbrella and Clarity.

Requirements

The following are the minimum system requirements for the Cisco Security Connector and MobileIron:

- A device running IOS system version 11.2 or higher:
 - running in supervised mode with Device Enrollment Program (DEP)
 - managed by MobileIron Cloud or On-Premise solution leveraging the Volume Purchase Program (VPP) to purchase, distribute and manage the app lifecycle.
 - having 5 MB free space on the device.
- Access to Cisco Advanced Malware Protector (AMP) for Endpoints and Cisco Umbrella instances
- If your devices are used on wifi networks behind a firewall, the Cisco Security Connector needs access to certain servers over specific ports.
 - The firewall must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):
 - Event Server - intake.amp.cisco.com/event/
 - Management Server - mgmt.amp.cisco.com/agent/v1/
 - Cloud Host - cloud-ios-asn.amp.cisco.com
 - Enrollment Server - cloud-ios-est.amp.cisco.com

- For IPv4 DNS protection, direct access to the IPv4 IP addresses 208.67.222.222 or 208.67.220.220 is required.
- For IPv6 DNS protection, direct access to the IPv6 IP addresses 2620:119:35::35 or 2620:119:53::53, or access to IPv4 addresses via NAT64/DNS64 translation is required
- **Note:** if DNS protection fails to engage then DNS traffic is not encrypted
- The device must be able to communicate with *.opendns.com for registration & validation purposes at least once a day.

Overview and Integration workflow

1. Enable and configure the DEP and VPP settings on the MobileIron On-Premise / Cloud solution
2. Register the devices into MobileIron UEM and push the apps to the devices
3. Enable the Cisco Security Connector app with Clarity AMP Dashboard
 - a. Export MobileIron's custom xml payload from AMP Dashboard.
 - b. Upload the custom XML payload (.mobileconifg) to MobileIron.
 - c. Apply the payload to the device in order to configure the app
4. Enable the Cisco Security Connector app with Umbrella Dashboard
 - a. Export MobileIron's custom xml payload from the Umbrella Dashboard.
 - b. Upload the custom XML payload (.mobileconifg) to MobileIron.
 - c. Apply the payload to the device to configure the app

Settings and Configuration

DEP and VPP in MobileIron

For more about DEP, VPP and their configurations on MobileIron see:

- [DEP Getting Started](#)
- [How to distribute apps with VPP](#)

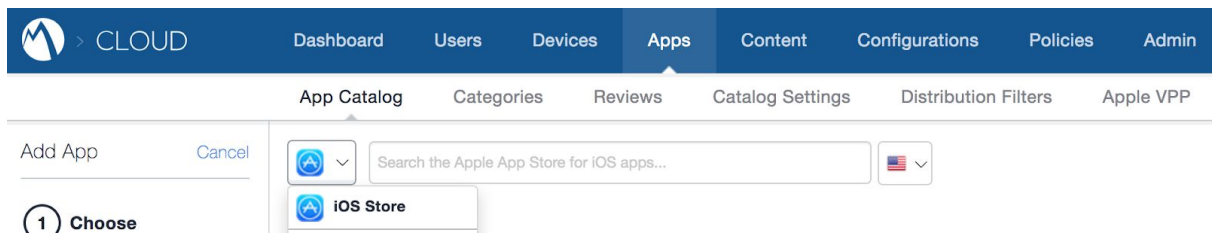
Note : As part of the VPP, get the free licenses for Cisco Cisco Security Connector app and distribute them to the devices.

On MobileIron Cloud start by identifying the user group you will deploy the Cisco Security Connector app to. To create a new user group for the deployment:

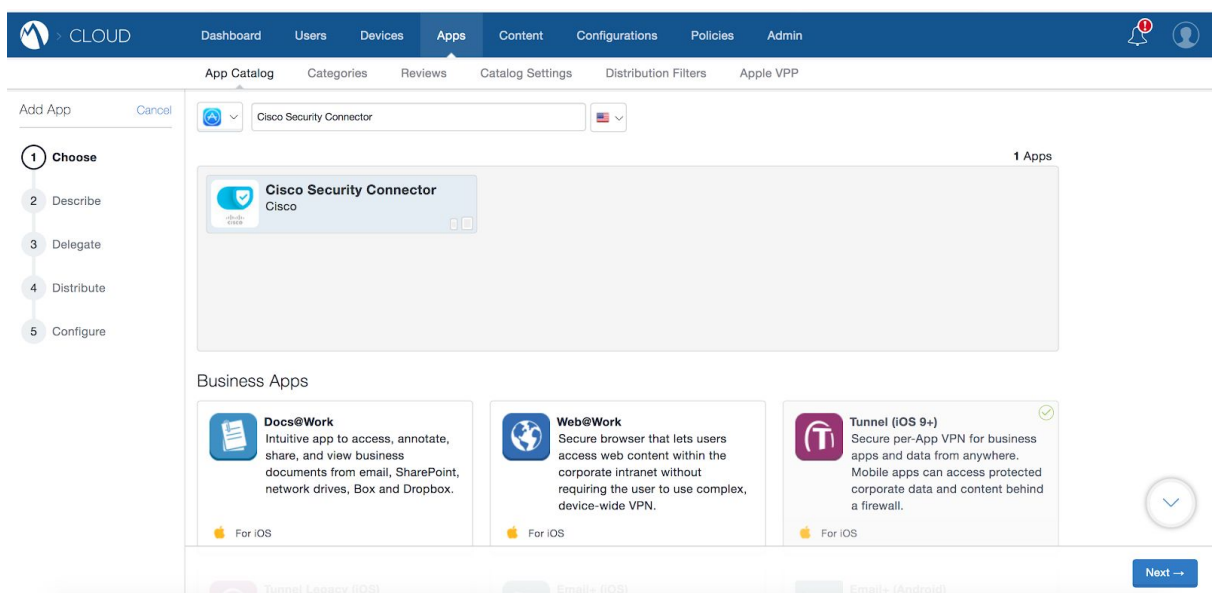
1. Login to MobileIron Cloud
2. Select users > user group and create a new user group
3. Build the criteria to obtain and add users to the group either manually or by using filters

To import the Cisco Security Connector app:

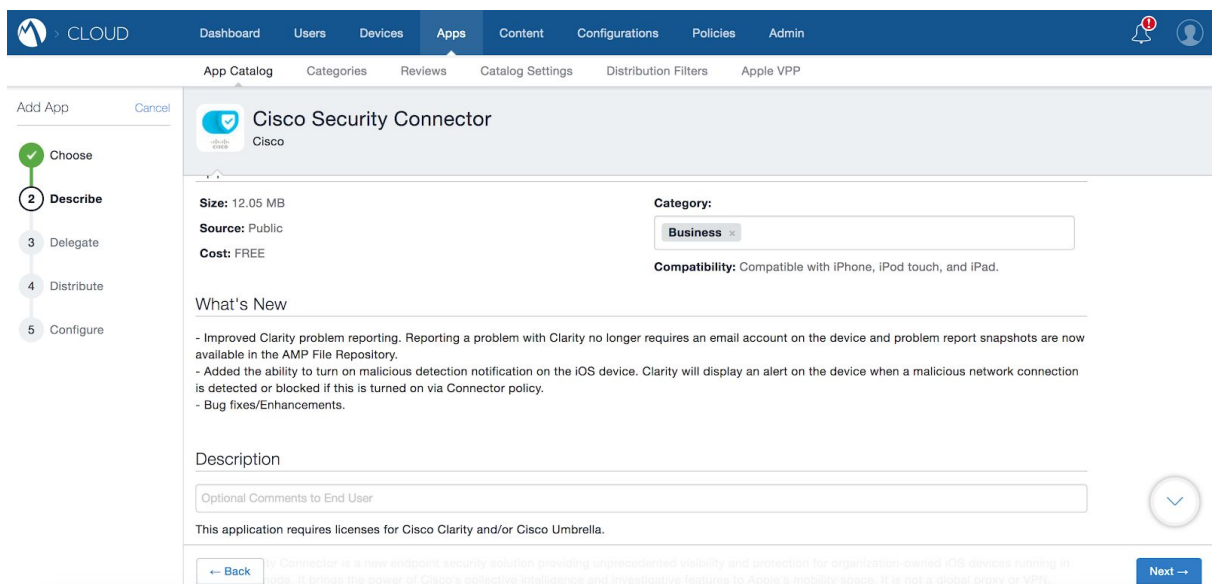
1. Go to apps > **Add** >> Select IOS system Store



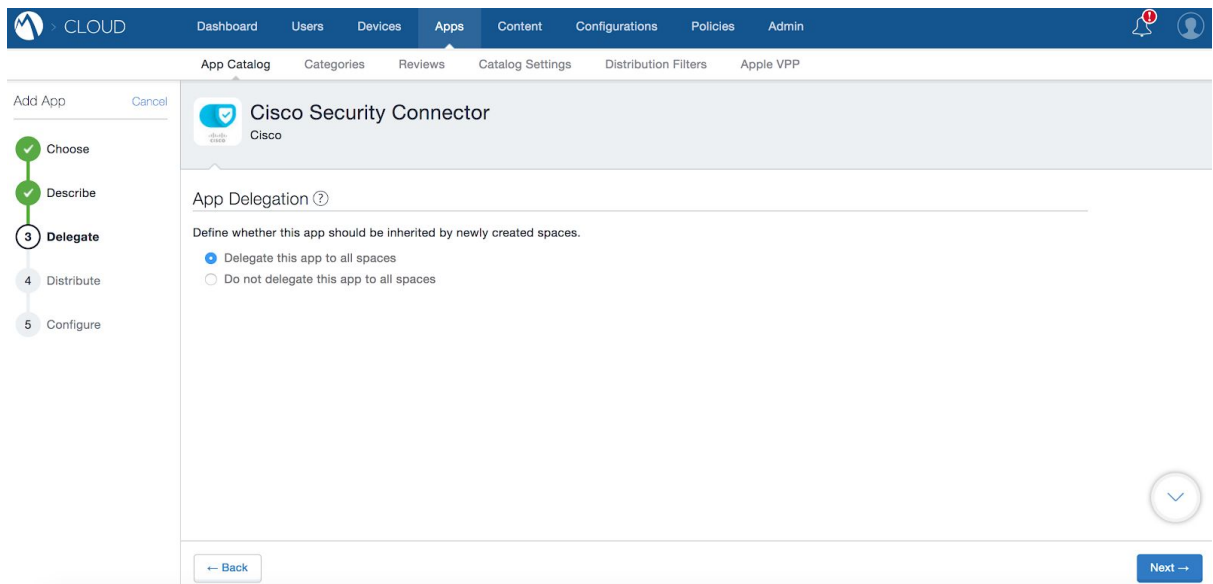
2. Search for Cisco Security Connector app, select it and hit **Next** in the bottom right corner



3. Add a description (optional)

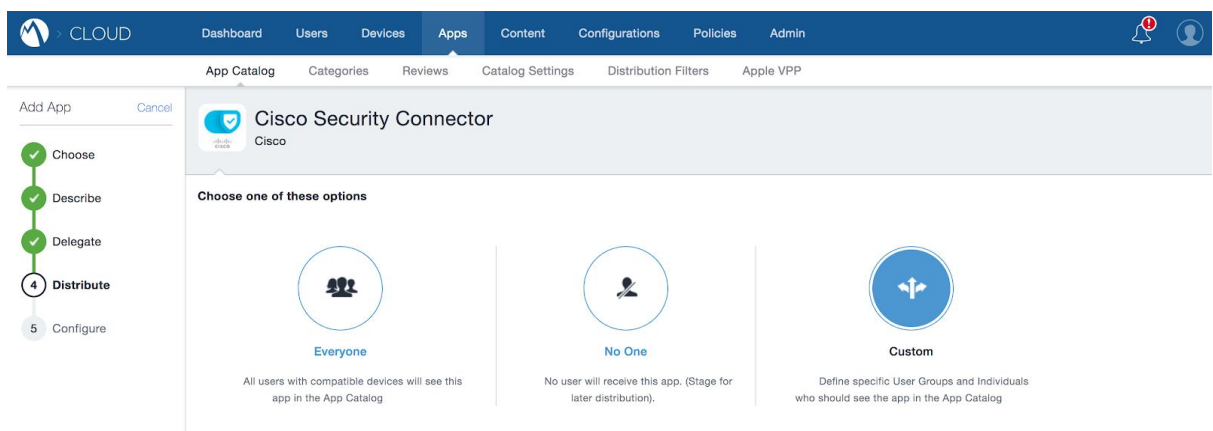


4. Select the admin space where you want to deploy to the Cisco Security Connector app



5. To deploy the Cisco Security Connector app, select the target user group. If you would like to do this for a particular group, then select **custom** and choose the user group you created earlier at the beginning. If a custom group is already created then select that and click **Next**.

Note : It is always recommended, for scalability, visibility and better control, that you use specific distribution groups and deploy the configuration and apps to only those devices.



6. Next you will taken to the app configuration page. Here, click “**Done**” at the bottom right corner to finish the app import process.

Note: It may take few moments for the server to pull the metadata and reflect it on the MobileIron console.

Enabling the Cisco Security Connector app with the Clarity AMP Dashboard

1. Export MobileIron's custom xml payload from AMP Dashboard.

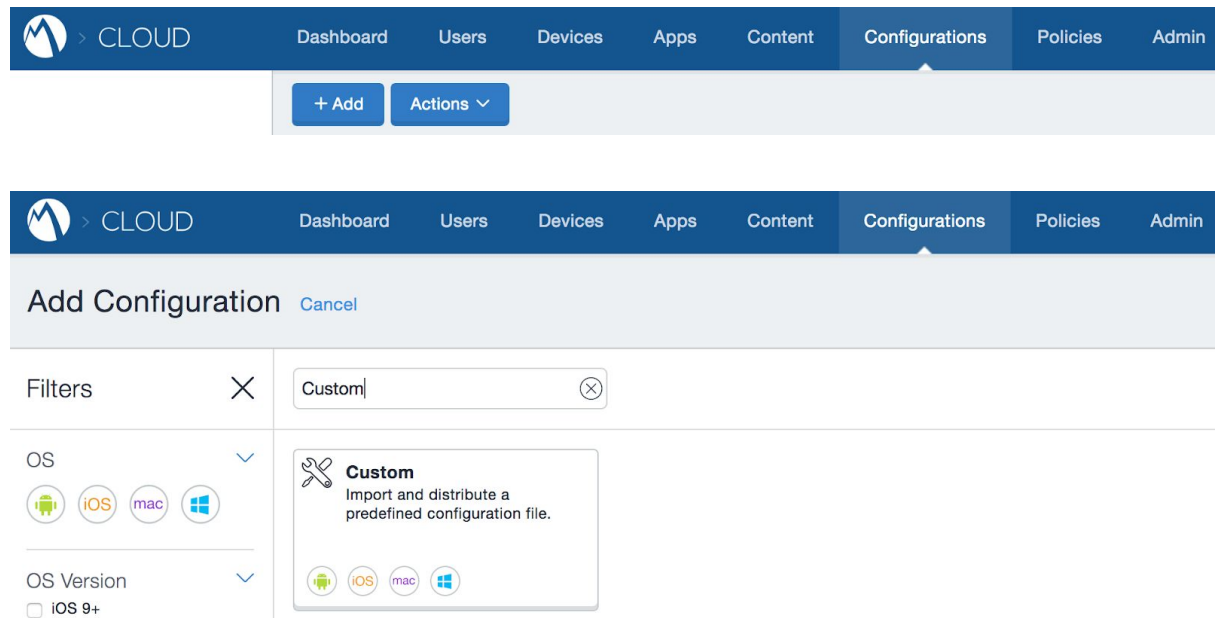
From the AMP Console:

- Go to Management > Deploy Clarity for IOS system.
- Select the AMP for Endpoints Group which is assigned to your intended IOS system policy.
- Click Download MobileIron Profile.

2. Upload the custom XML payload (.mobileconifg) to MobileIron and deploy to devices.

For MobileIron Cloud:

1. Identify the device group that will receive the configuration. If you choose to create a new device group, then go to **devices > device group** and create one with the necessary filter criteria, or manually add devices into the device group.
2. Next on the MobileIron Cloud console, navigate to Configurations, click on **Add** and search for "**Custom**" configuration. Select that option to import and distribute a predefined configuration file to the device by clicking **next** at the bottom right corner.




3. Give the configuration a name and choose iOS as the operating system.

The screenshot shows the 'Create Custom Configuration' page in a web application. The top navigation bar includes 'Dashboard', 'Users', 'Devices', 'Apps', 'Content', 'Configurations' (active), 'Policies', and 'Admin'. On the left, a sidebar shows 'Add Config' and 'Cancel' buttons, with a progress indicator for '1 Create Settings' and '2 Distribute'. The main content area has a title 'Create Custom Configuration' with a subtitle 'Import and distribute a predefined configuration file.' Below this, there is a 'Name' field containing 'Cloud Security Connector - Clarity AMP Dashboard' and a '+ Add Description' link. The 'Choose OS' section displays four circular icons: 'iOS' (selected), 'macOS', 'Android', and 'Windows'.

4. Click **Choose** or **drag and drop** the mobileconfig file you downloaded from the AMP console and click **next**

The screenshot shows a 'Configuration Setup' dialog box. It contains the text 'Upload .plist or .mobileconfig file to create the custom configuration settings.' Below this, a file upload area shows the file 'MICloud-Certify-withCSC_amp_ios.mobileconfig' with a green checkmark and the text 'File successfully added!'. A 'Choose a different file' link is also present. At the bottom right of the dialog is a circular arrow icon. Below the dialog, there are 'Back' and 'Next' buttons.

5. Select the device group to publish the configuration to. The recommended approach is to define a group specifically for the Cisco Security Connector app deployment. To do this, select that group under “Custom” and click **done**.


 CLOUD

DashboardUsersDevicesAppsContentConfigurationsPoliciesAdmin

Add ConfigCancel

✓ Create Settings

2 Distribute


 Create Custom Configuration

Import and distribute a predefined configuration file.

☒ Enable this configuration


This configuration will be applied to selected devices.

Choose one of these options




All Devices

All compatible devices will have this configuration sent to them



No Devices

Stage this configuration for later distribution



Custom

Define specific Device Groups that will have this configuration sent to them

Define Device Group Distribution

Select options below to distribute Configuration.

Search Device Groups

All (6)

Selected (0)

☐ Android Devices (0)

☐ Android Enterprise Devices (0)

☐ iOS Devices (1)

☐ Windows Devices (0)

☐ macOS Devices (0)

☐ tvOS Devices (0)

Distribution Summary

List of device users as they are added to the distribution.

NAME	PHONE #	DEVICE TYPE
There is no information to display.		

← Back

Done

Enabling the Cisco Security Connector app with the Umbrella Dashboard

1. Export MobileIron's custom xml payload from the Umbrella Dashboard.

To deploy from MobileIron you will need to download a Mobileconfig file from the Umbrella dashboard first.

Navigate to **Identities > Mobile Devices** and click the **MobileIron Config** download button. **Save** the file downloaded.



Next, download the Umbrella Root Certificate. Navigate to **Policies > Root Certificate**. Then click **Download Certificate** and **save** the resulting .cer file.

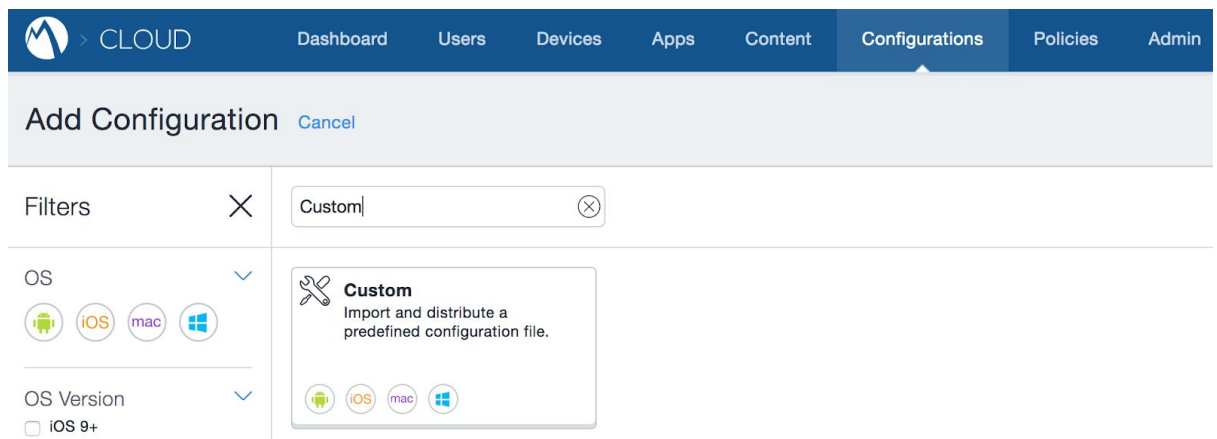
2. Upload the custom XML payload (.mobileconfig) to MobileIron and deploy it to the device along with the root certificate.

For MobileIron Cloud,

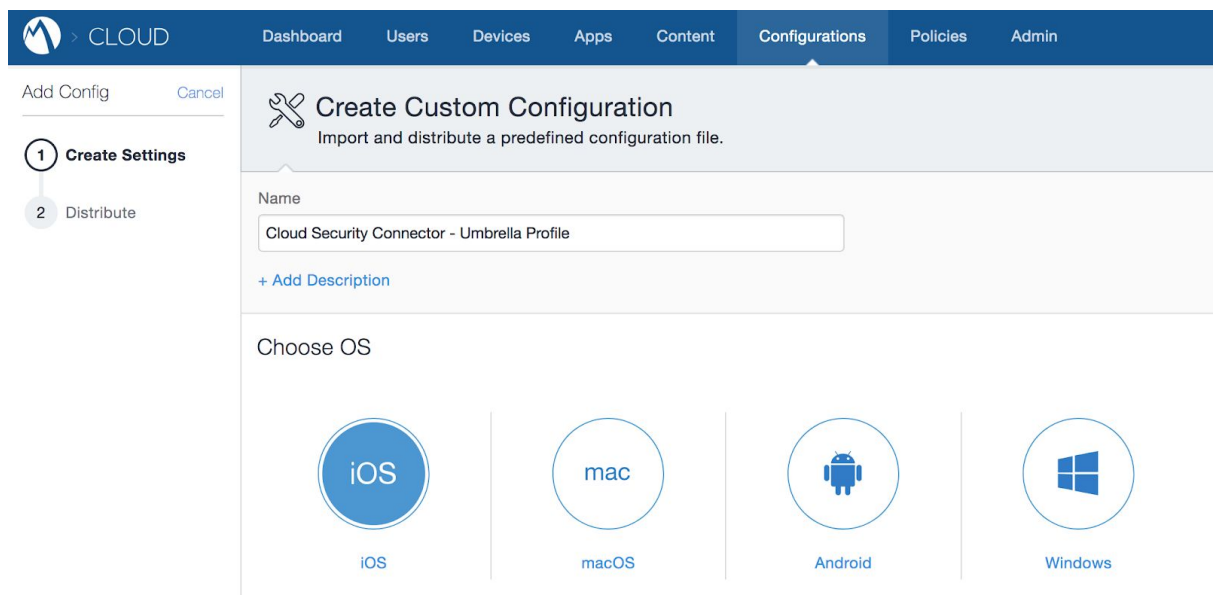
1. First identify the device group to publish the configuration to. If you choose to create a new device group, then go to devices > device group and create one with the necessary filter criteria or manually add devices into the device group.
2. Edit the mobileconfig downloaded from Umbrella dashboard with the help of any text editor and find and replace "\$DEVICE_SN\$" value with "\${deviceSN}" and **save** the changes in the file

```
<key>serialNumber</key>
<string>${deviceSN}</string>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Cisco Security</string>
<key>PayloadIdentifier</key>
<string>com.cisco.ciscosecurity.app.CiscoUmbrella.DB2A157-E134-3E8C-B4FB-23EDF48A0CD1</string>
```

- Next on the Mobileiron console, navigate to **Configurations** and click on **add** and search for “**Custom**” configuration. Select the option to import and distribute the configuration file by clicking on **next** at the bottom right corner of the screen

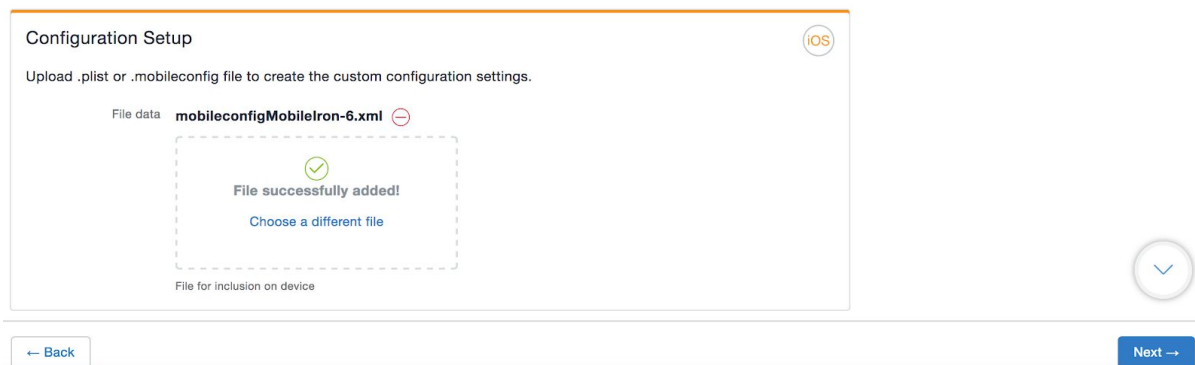


- Give the configuration a friendly name and choose the operating system as iOS



- Click **Choose** or **drag and drop** the mobileconfig file you edited with text editor to reflect the device Serial number variable and click **next**.

Note : If this is for MobileIron Core (On Premise solution) then you do not need to edit the variable.

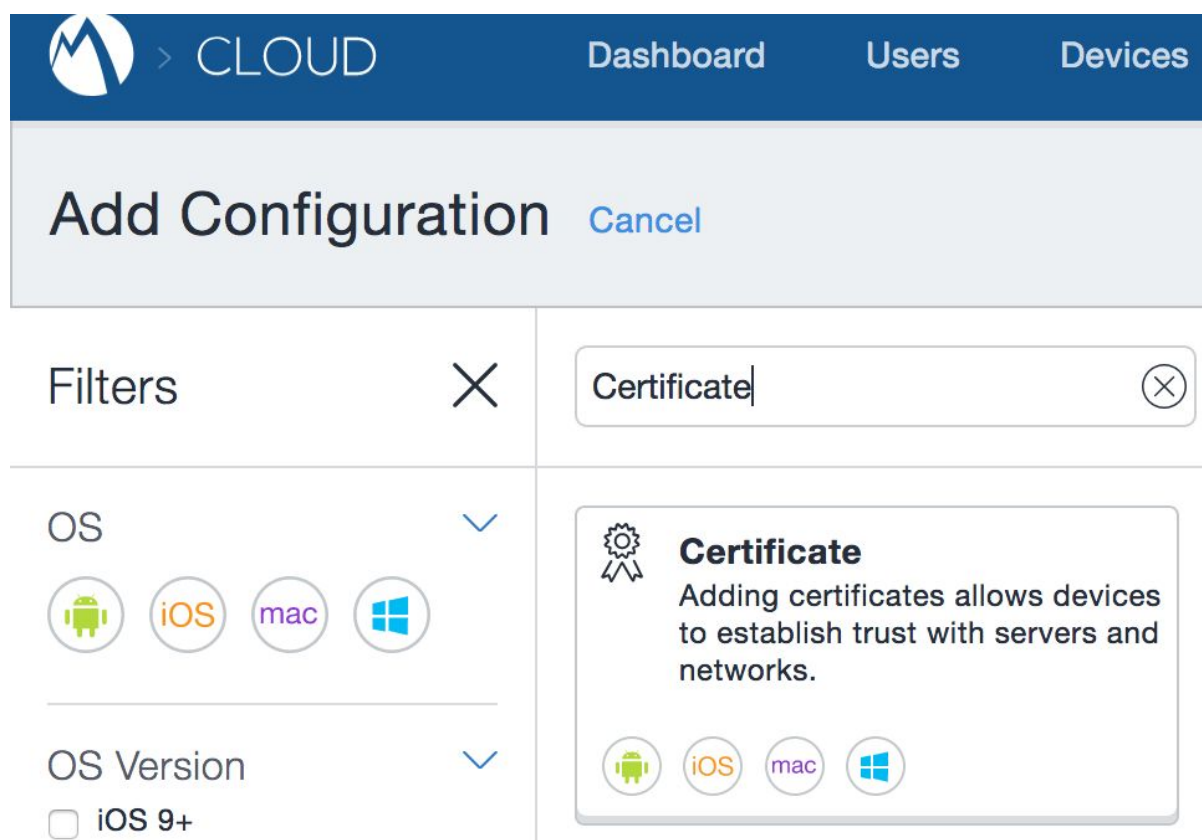


The screenshot shows a 'Configuration Setup' window with an 'iOS' icon in the top right. The text inside says 'Upload .plist or .mobileconfig file to create the custom configuration settings.' Below this, 'File data' is listed as 'mobileconfigMobileIron-6.xml' with a minus icon. A dashed box contains a green checkmark and the text 'File successfully added!' with a link 'Choose a different file'. At the bottom, it says 'File for inclusion on device'. Navigation buttons 'Back' and 'Next' are at the bottom.

- Select the device group you wish to publish the configuration. If you have created a device group specifically for Cisco security Connector app deployment (which is recommended approach) then select that under “**Custom**” section and click **done**.

To upload and distribute the Cisco Umbrella root certificate in MobileIron’s MI Cloud:

- For MobileIron Cloud, navigate to Configurations on the console and click on **add**. Search for “**Certificate**” and click **next**.



The screenshot shows the 'Add Configuration' screen in the MobileIron Cloud console. The top navigation bar includes the MobileIron logo, 'CLOUD', and links to 'Dashboard', 'Users', and 'Devices'. The main heading is 'Add Configuration' with a 'Cancel' link. Below this is a 'Filters' section with a search bar containing 'Certificate'. The 'OS' filter shows icons for Android, iOS, mac, and Windows. The 'OS Version' filter shows a checkbox for 'iOS 9+'. On the right, a card titled 'Certificate' with a ribbon icon explains that adding certificates allows devices to establish trust with servers and networks, and includes the same OS icons at the bottom.

2. Name the configuration

The screenshot shows the Cisco Umbrella Cloud console. The top navigation bar has a 'CLOUD' header and tabs for Dashboard, Users, Devices, Apps, Content, Configurations, Policies, and Admin. The left sidebar shows a progress indicator with '1 Create Settings' and '2 Distribute'. The main content area is titled 'Create Certificate Configuration' and includes a description: 'Adding certificates on devices allows devices to establish trust with servers and networks such as Wi-Fi. Often, these systems are already set up with publicly verifiable certificates, in which case the trust these systems is more secure and improves the user experience.' Below this, there is a 'Name' field with the text 'Cisco Umbrella Root Cert' and a '+ Add Description' link.

3. Click **Choose** or **drag and drop** the rootcert file you downloaded from the Umbrella console and click **next**

The screenshot shows the 'Configuration Setup' screen. The 'Certificate data' section shows the file 'Cisco_Umbrella_Root_CA.cer' with a red minus icon. Below this, a message box says 'File successfully added!' with a green checkmark and a 'Choose a different file' link. The bottom of the screen has a 'Back' button and a 'Next' button.

4. Again, select the device group you wish to publish the rootcert. If you have created a device group specifically for Cisco security Connector app deployment (which is recommended approach) then select that under “Custom” settings section and click done.

References

More information about Cisco Security Connector can be found at these links:

<https://www.cisco.com/c/en/us/products/security/security-connector/index.html>

<https://docs.umbrella.com/deployment-umbrella/docs/cisco-mobile-security-setup-guide>

<https://docs.umbrella.com/deployment-umbrella/docs/mobileiron-configuration> (contains steps that can be followed when using MobileIron Core)

ARE there MobileIron links we should add?

Contact Information

Please contact the MobileIron Technology Ecosystem team at ecosystem@mobileiron.com with any questions.