NIST SPECIAL PUBLICATION 1800-21C

Mobile Device Security

Corporate-Owned Personally-Enabled (COPE)

Volume C:
How-to Guides

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

**Former employee; all work for this publication was done while at employer.*

July 2019

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-21C Natl. Inst. Stand. Technol. Spec. Publ. 1800-21C, 169 pages, (July 2019), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: mobile-nccoe@nist.gov.

Public comment period: July 22, 2019 through September 23, 2019

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Mobile devices provide access to workplace data and resources that are vital for organizations to accomplish their mission while providing employees the flexibility to perform their daily activities. Securing these devices is essential to the continuity of business operations.

While mobile devices can increase organizations' efficiency and employee productivity, they can also leave sensitive data vulnerable. Addressing such vulnerabilities requires mobile device management tools to help secure access to the network and resources. These tools are different from those required to secure the typical computer workstation.

To address the challenge of securing mobile devices while managing risks, the NCCoE at NIST built a reference architecture to show how various mobile security technologies can be integrated within an enterprise's network.

This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-based, commercially available products to help meet their mobile device security and privacy needs.

KEYWORDS

Bring your own device; BYOD; corporate-owned personally-enabled; COPE; mobile device management; mobile device security, on-premise.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Donna Dodson	NIST
Vincent Sritapan	Department of Homeland Security, Science and Technology Directorate
Jason Frazell	Appthority (acquired by Symantec)
Joe Midtlyng	Appthority (acquired by Symantec)
Chris Gogoel	Kryptowire
Tom Karygiannis	Kryptowire
Tim LeMaster	Lookout
Victoria Mosby	Lookout
Michael Carr	MobileIron
Walter Holda	MobileIron
Farhan Saifudin	MobileIron

Name	Organization
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Lura Danley	The MITRE Corporation
Eileen Durkin	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Marisa Harriston	The MITRE Corporation
Nick Merlino	The MITRE Corporation
Doug Northrip	The MITRE Corporation
Titilayo Ogunyale	The MITRE Corporation
Oksana Slivina	The MITRE Corporation
Tracy Teter	The MITRE Corporation
Paul Ward	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Appthority	Appthority Cloud Service, Mobile Threat Intelligence
Kryptowire	Kryptowire Cloud Service, Application Vetting
Lookout	Lookout Cloud Service/Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android), Mobile Threat Defense
MobileIron	MobileIron Core Version 9.7.0.1, MobileIron Agent Version 11.0.1A (iOS), 10.2.1.1.3R (Android), Enterprise Mobility Management
Palo Alto Networks	Palo Alto Networks PA-220
Qualcomm	Qualcomm Trusted Execution Environment (version is device dependent)

Contents

List of Figures

List of Tables

1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the mobile device security products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate addressing mobile device security (MDS) implementation challenges. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-21A: *Executive Summary*
- NIST SP 1800-21B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-21C: *How-To Guides* – instructions for building the example solution **(you are here)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-21A*, which describes the following topics:

- challenges that enterprises face in securely deploying mobile devices within their organization
- example solution built at the National Cybersecurity Center of Excellence (NCCoE)
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-21B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, describes the risk analysis we performed.
- Section 4.3, Security Control Map, discusses the security mappings of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-21A*, with your leadership team members to help them understand the importance of adopting standards-based solutions when addressing MDS implementation challenges.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-21C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of this guide's example solution for on-premises mobile device security management. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to mobile-nccoe@nist.gov.

1.2 Build Overview

When a business is on the go, mobile devices can serve as a temporary workstation replacement. They provide convenience of use, portability, and functionality. However, in many ways, mobile devices are different from the common computer workstation, and alternative management tools are required to secure their interactions with the enterprise. To address this security challenge, the NCCoE worked with its Community of Interest and build team partners and developed a real-world scenario for mobile deployment within an enterprise. The scenario presents a range of security challenges that an enterprise may experience when deploying mobile devices.

The lab environment used in developing this solution includes the architectural components, functionality, and standard best practices, which are described in Volume B. The build team partners provided the security technologies used to deploy the architecture components and functionality. The standard best practices are applied to the security technologies to ensure the appropriate security controls are put in place to meet the challenges presented in the devised scenario.

This section of the guide documents the build process and discusses the specific configurations used to develop a secure mobile deployment.

Note: Android for Work has been re-branded as Android Enterprise. At the time of writing this document, it was named Android for Work.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

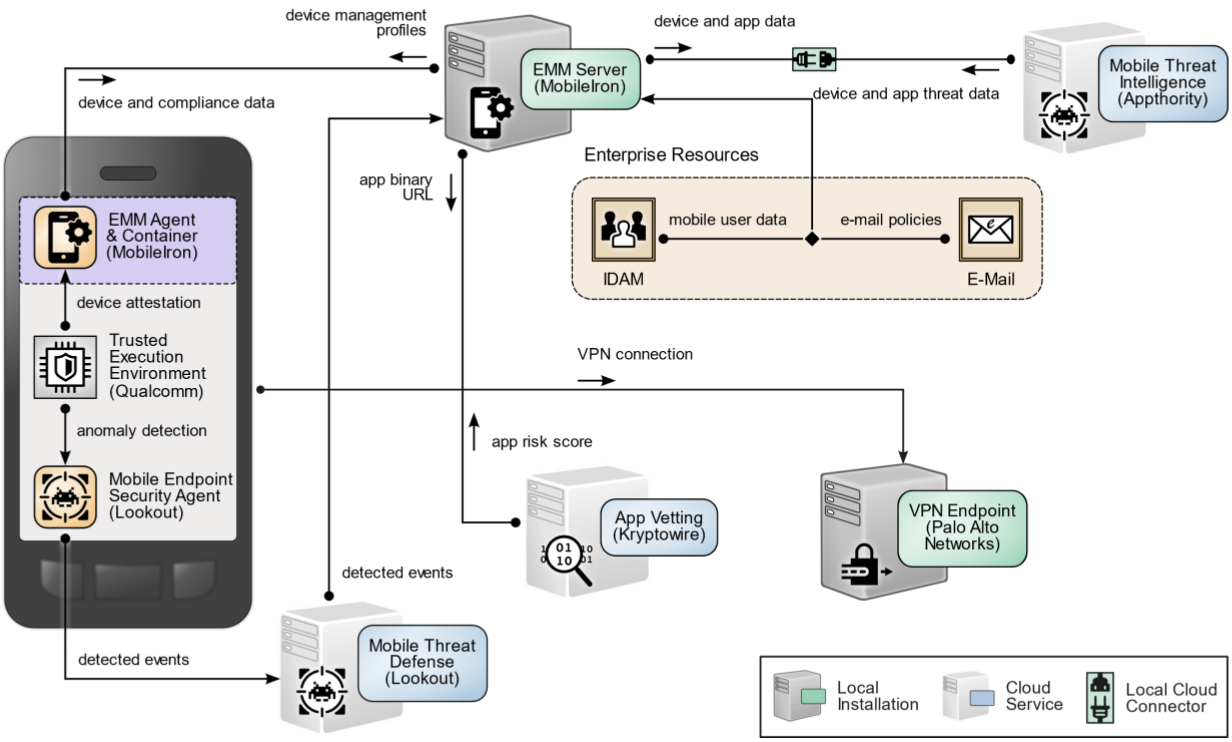
Table 1-1 Typographic Conventions

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

1.4 Logical Architecture Summary

The following graphic illustrates the main components of this example implementation and provides a simplified view of how they interact.

Figure 1-1 Logical Architecture Summary


device management profiles
device and app data
EMM Server (MobileIron)
Mobile Threat Intelligence (Appthority)
device and compliance data
device and app threat data
Enterprise Resources
app binary URL
EMM Agent & Container (MobileIron)
mobile user data
e-mail policies
IDAM
E-Mail
device attestation
Trusted Execution Environment (Qualcomm)
VPN connection
anomaly detection
app risk score
Mobile Endpoint Security Agent (Lookout)
App Vetting (Kryptowire)
VPN Endpoint (Palo Alto Networks)
detected events
detected events
Mobile Threat Defense (Lookout)
Local Installation
Cloud Service
Local Cloud Connector

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring key products used for the architecture illustrated below.

In our lab environment, the example solution was logically separated by a virtual local area network (VLAN) wherein each VLAN represented a separate mock enterprise environment. The network perimeter for this example implementation was enforced by a Palo Alto Networks virtual private network (VPN)/firewall appliance. It maintains three zones: one each for the internet/wide area network (WAN), a demilitarized zone (DMZ), and the organizational local area network (LAN).

2.1 Appthority Mobile Threat Detection

Appthority contributed a test instance of its Mobile Threat Detection service. Contact Appthority (Symantec) (https://www.symantec.com/) to establish an instance for your organization.

2.2 Kryptowire EMM+S

Kryptowire contributed a test instance of its EMM+S application-vetting service. Contact Kryptowire (https://www.kryptowire.com/mobile-app-security/) to establish an instance for your organization.

2.3 Lookout Mobile Endpoint Security

Lookout contributed a test instance of its Mobile Endpoint Security (MES) service. Contact Lookout (https://www.lookout.com/products/mobile-endpoint-security) to establish an instance for your organization.

2.4 MobileIron Core

MobileIron Core is the central product in the MobileIron suite. The following sections describe the steps for installation, configuration, and integration with Active Directory (AD).

2.4.1 Installation of MobileIron Core and Stand-Alone Sentry

Follow the steps below to install MobileIron Core:

1. Obtain a copy of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* from the MobileIron support portal.

2. Follow the MobileIron Core predeployment and installation steps in Chapter 1 of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* for the version of MobileIron being deployed in your environment. In our lab implementation, we deployed MobileIron Core 9.5.0.0 as a Virtual Core running on VMware 6.0. Post-installation, we performed an upgrade to MobileIron Core 9.7.0.1 following guidance provided in *CoreConnectorReleaseNotes9701_Rev12Apr2018*. Direct installations to MobileIron Core 9.7.0.1 will experience slightly different results, as some added features in this version are not used with earlier versions of configuration files.

2.4.2 General MobileIron Core Setup

The following steps are necessary for mobile device administrators or users to register devices with MobileIron.

1. Obtain a copy of *MobileIron Core Device Management Guide for iOS Devices* from the MobileIron support portal.

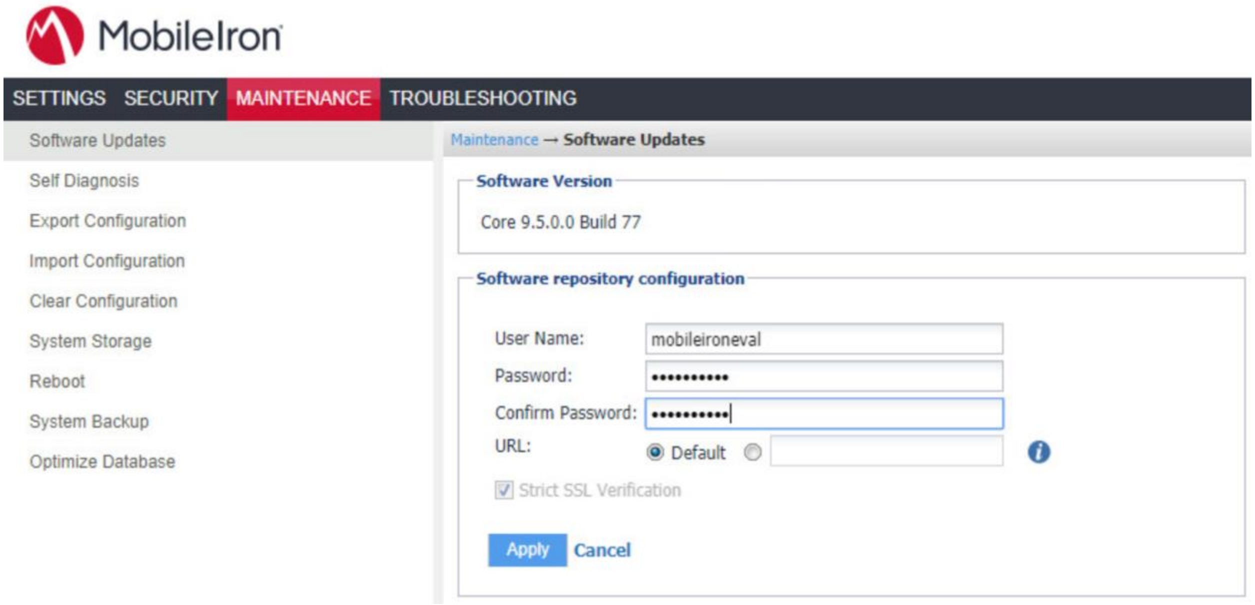
2. Complete all instructions provided in Chapter 1, Setup Tasks.

2.4.3 Upgrade MobileIron Core

The following steps were used to upgrade our instance of MobileIron Core from 9.5.0.0 to 9.7.0.1. Note there was no direct upgrade path between these two versions; our selected upgrade path was 9.5.0.0 > 9.5.0.1 > 9.7.0.1.

1. Obtain upgrade credentials from MobileIron Support.
2. In **MobileIron Core System Manager,** navigate to **Maintenance > Software Updates.**
3. In the **Software repository configuration** section:
    a. In the **User Name** field, enter the username provided by MobileIron Support.
    b. In the **Password** field, enter the password provided by MobileIron Support.
    c. In the **Confirm Password** field, reenter the password provided by MobileIron Support.
    d. Select **Apply.**

Figure 2-1 MobileIron Repository Configuration



Software Version

Core 9.5.0.0 Build 77

Software repository configuration

User Name: mobileironeval

Password: ••••••••••

Confirm Password: ••••••••••

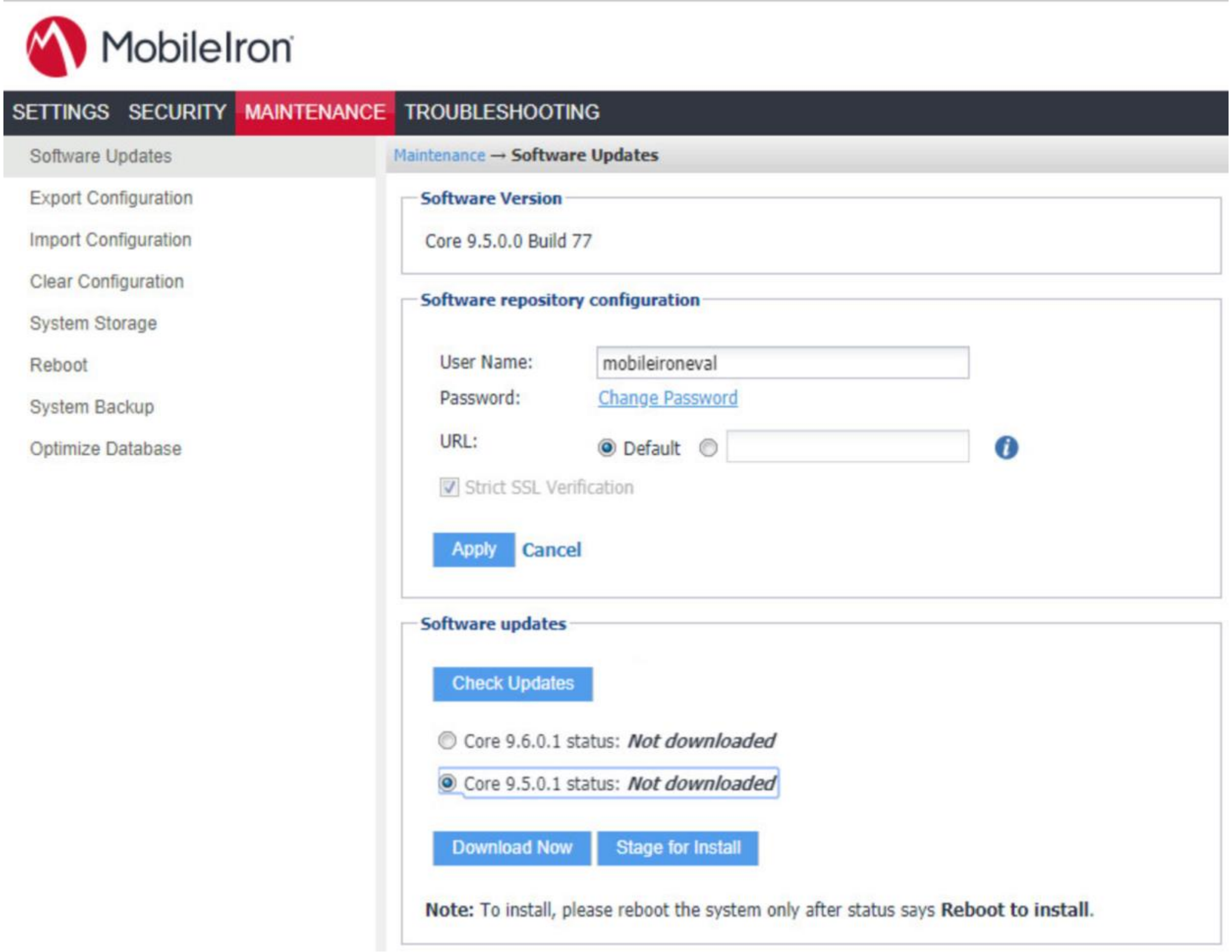
URL: ● Default ○

☑ Strict SSL Verification

4. In the **Software Updates** section:
    a. Select **Check Updates;** after a few seconds, the available upgrade path options will appear.
    b. Select the **Core 9.5.0.1 status: Not Downloaded option.**

c. Select **Download Now.** After a delay, the Software Download dialogue will appear.

Figure 2-2 MobileIron Core Version



Software Version

Core 9.5.0.0 Build 77

Software repository configuration

User Name: mobileironeval

Password: Change Password

URL: ● Default ○

☑ Strict SSL Verification

Software updates

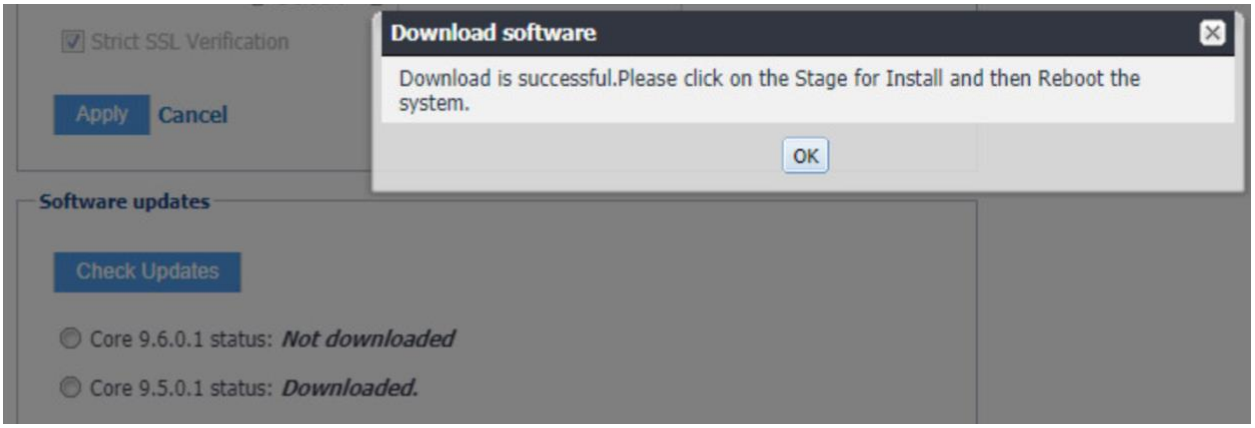
○ Core 9.6.0.1 status: ***Not downloaded***

● Core 9.5.0.1 status: ***Not downloaded***

Note: To install, please reboot the system only after status says **Reboot to install**.

5. In the **Download Software** dialogue, select **OK.**

Figure 2-3 MobileIron Download Status



☑ Strict SSL Verification

Download software

Download is successful.Please click on the Stage for Install and then Reboot the system.

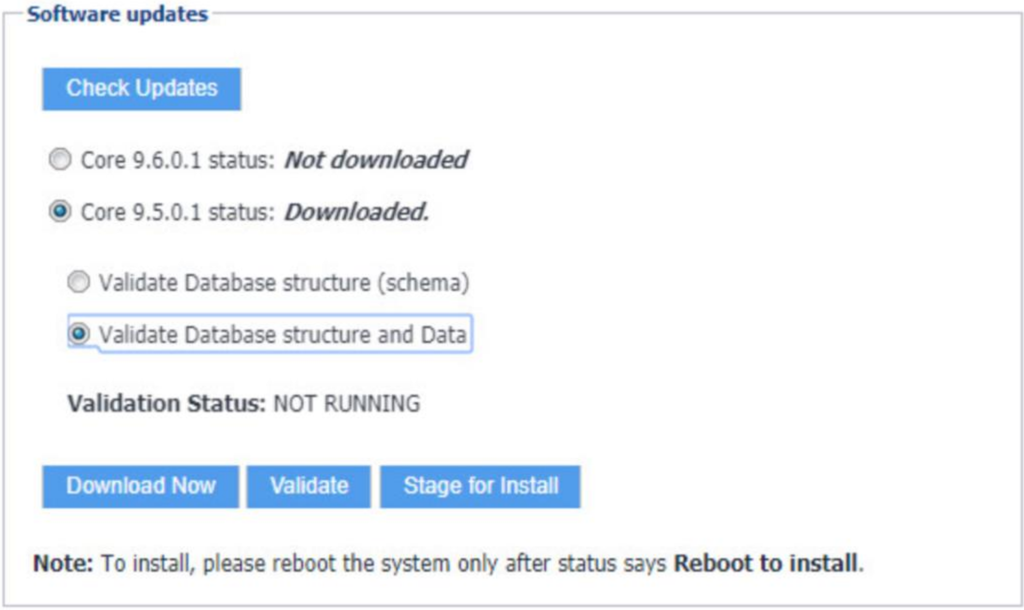
Software updates

○ Core 9.6.0.1 status: ***Not downloaded***

○ Core 9.5.0.1 status: ***Downloaded.***

6. In the **Software updates** section:
   a. Select the **Core 9.5.0.1 status: Downloaded** option.
   b. Select the **Validate Database Structure and Data** option.
   c. Select **Validate.**

Figure 2-4 Validating Database Data



Software updates

○ Core 9.6.0.1 status: ***Not downloaded***

● Core 9.5.0.1 status: ***Downloaded.***

○ Validate Database structure (schema)

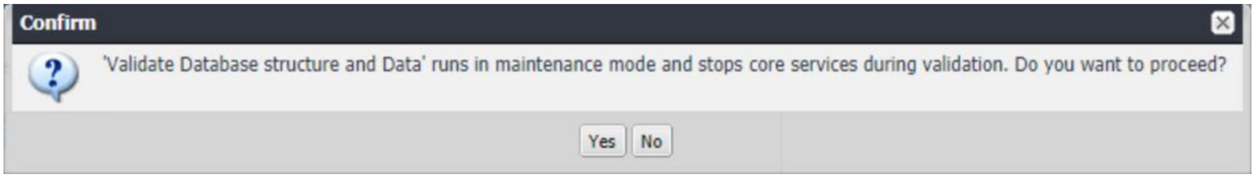
● Validate Database structure and Data

Validation Status: NOT RUNNING

Note: To install, please reboot the system only after status says **Reboot to install**.

7. In the **Confirm** dialogue, select **Yes** to validate database structure and data.

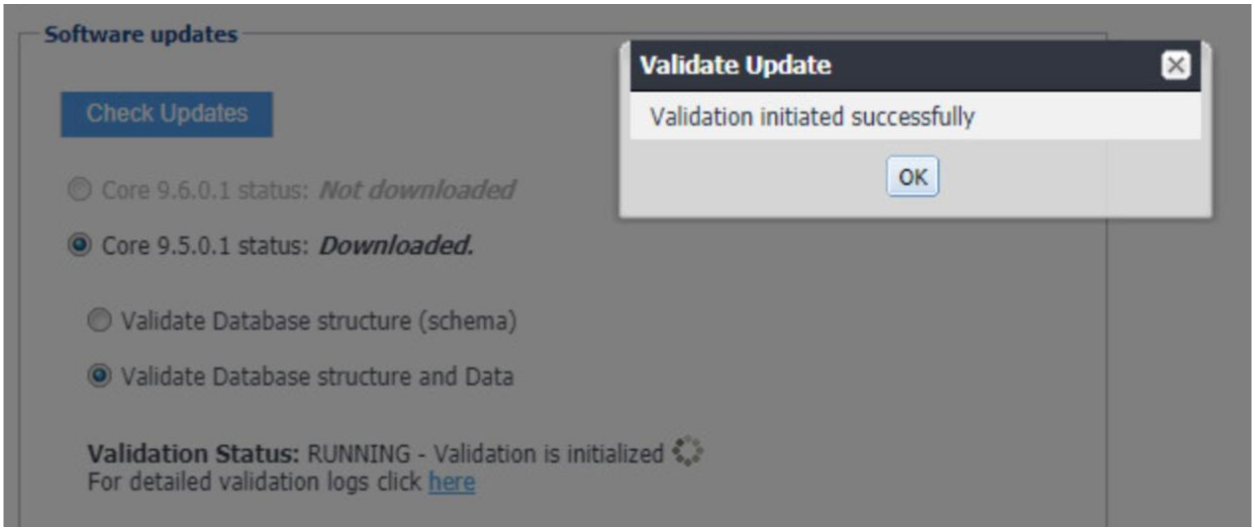
Figure 2-5 Validating Database Data Confirmation



'Validate Database structure and Data' runs in maintenance mode and stops core services during validation. Do you want to proceed?

8. In the **Validate Update** dialogue, select **OK.**

Figure 2-6 Database Data Validation Initiation Confirmation



Validation initiated successfully

○ Core 9.6.0.1 status: *Not downloaded*

● Core 9.5.0.1 status: ***Downloaded.***

○ Validate Database structure (schema)

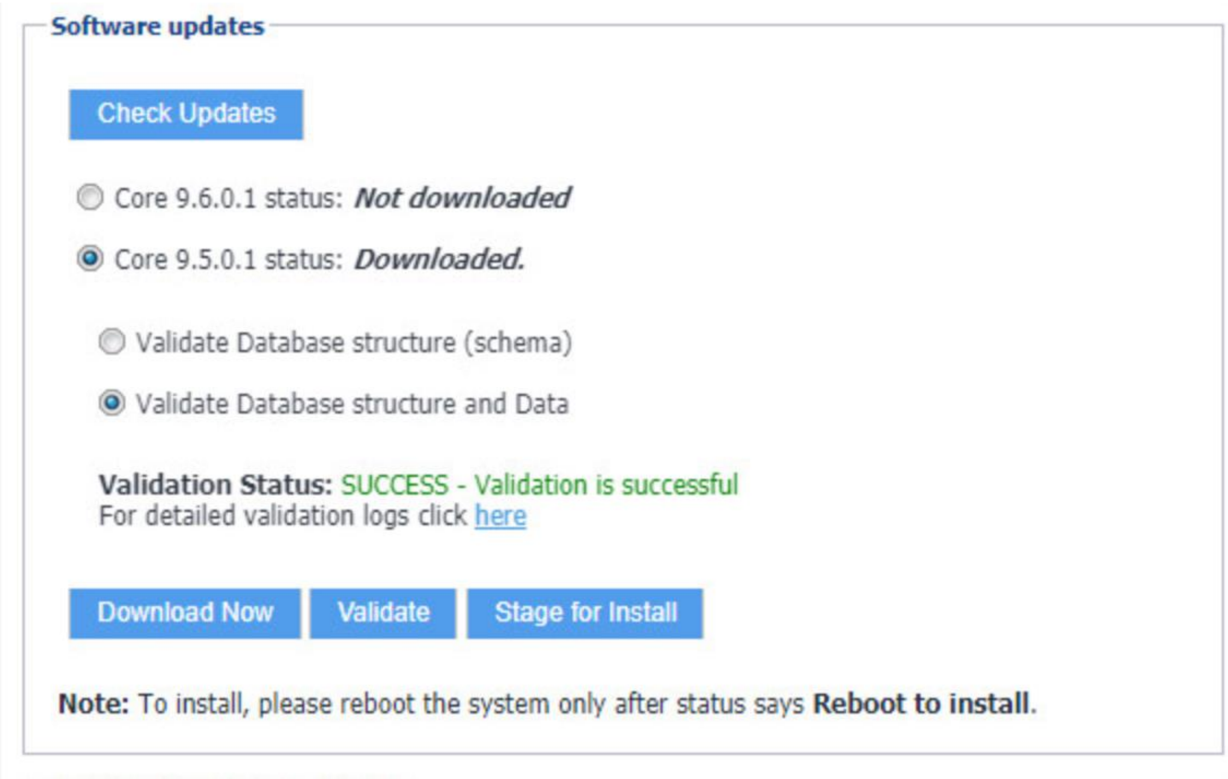
● Validate Database structure and Data

Validation Status: RUNNING - Validation is initialized

For detailed validation logs click here

9. In the **Software updates** section, select **Stage for Install;** the **Download Updates** dialogue will appear.

Figure 2-7 Database Data Validation Status



Software updates

Check Updates

○ Core 9.6.0.1 status: *Not downloaded*

● Core 9.5.0.1 status: *Downloaded.*

○ Validate Database structure (schema)

● Validate Database structure and Data

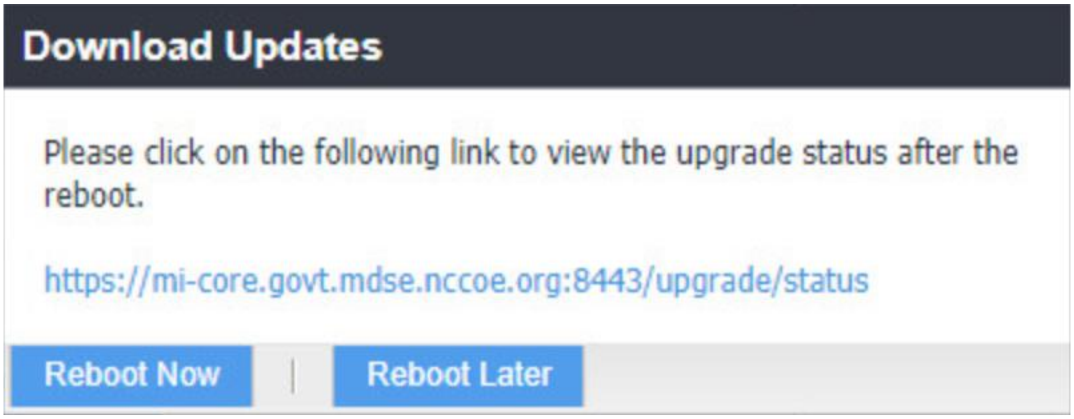
Validation Status: SUCCESS - Validation is successful
For detailed validation logs click here

Download Now | Validate | Stage for Install

Note: To install, please reboot the system only after status says **Reboot to install**.

10. In the **Download Updates** dialogue, select **Reboot Now;** a series of dialogues will appear.

Figure 2-8 Software Updates Reboot Prompt



Download Updates

Please click on the following link to view the upgrade status after the reboot.

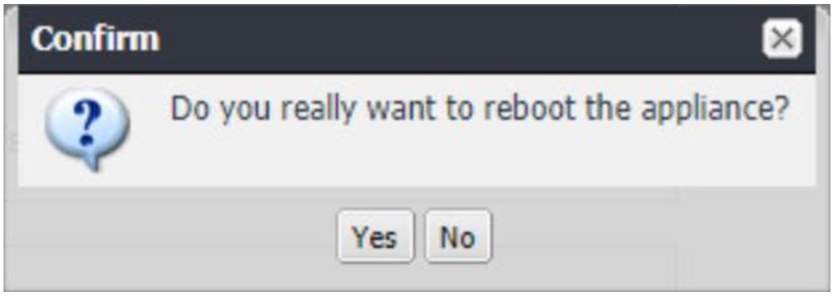
https://mi-core.govt.mdse.nccoe.org:8443/upgrade/status

Reboot Now | Reboot Later

11. In the **Confirm** dialogues:

    a. Select **Yes** to confirm reboot of the appliance.

Figure 2-9 Software Update Reboot Confirmation

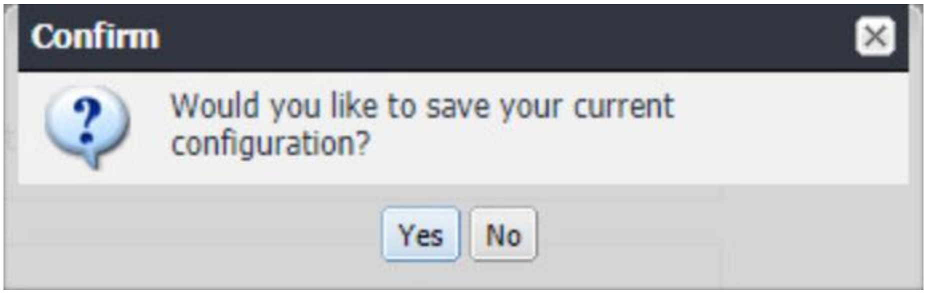


Confirm

Do you really want to reboot the appliance?

b. Select **Yes** to confirm saving the current configuration.

Figure 2-10 Reboot Configuration Save Prompt

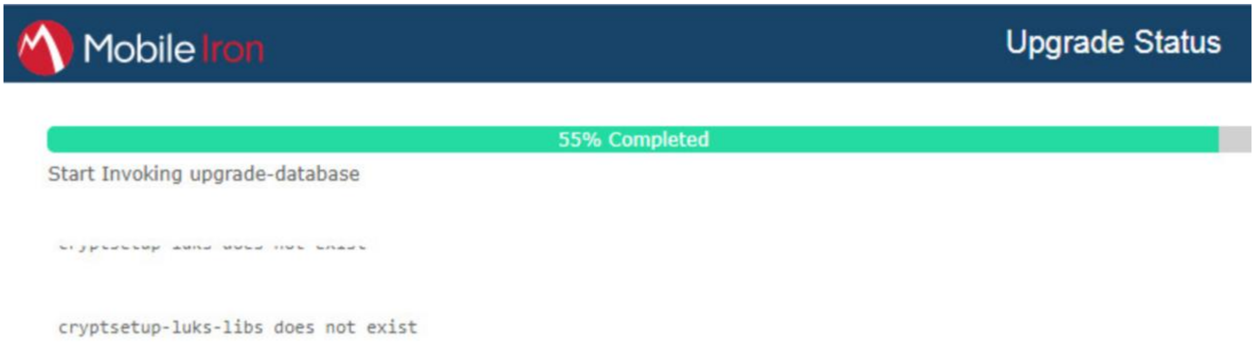


Confirm

Would you like to save your current configuration?

12. The Upgrade Status website hosted by Core will automatically open.

Figure 2-11 Upgrade Status



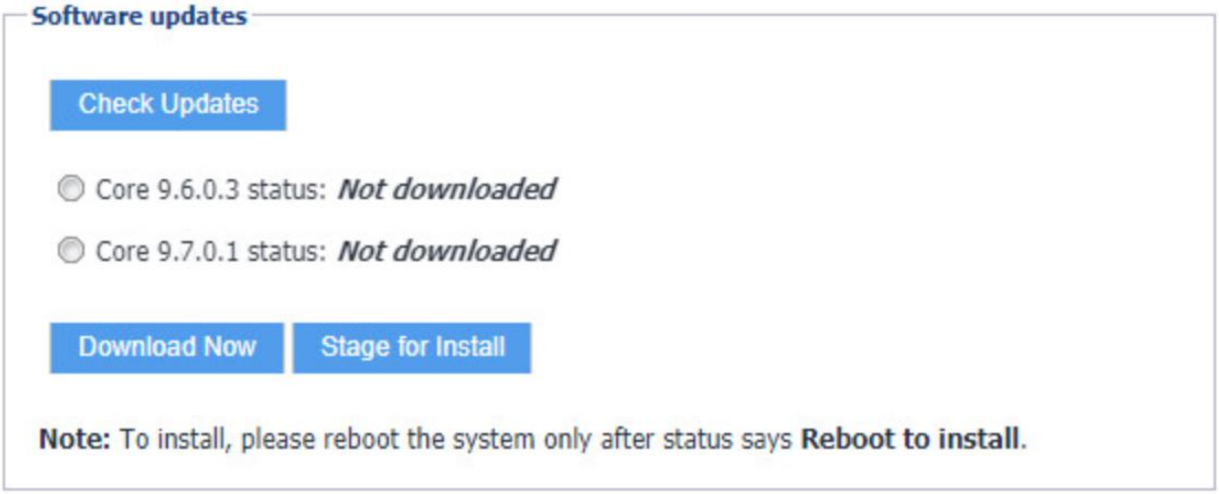
55% Completed

Start Invoking upgrade-database

```
cryptsetup-luks does not exist

cryptsetup-luks-libs does not exist
```

13. Once the upgrade is complete, **System Manager > Maintenance > Software Updates > Software Updates** now shows the capability to upgrade to 9.7.0.1.

Figure 2-12 Ability to Upgrade to 9.7.0.1



Software updates

○ Core 9.6.0.3 status: ***Not downloaded***

○ Core 9.7.0.1 status: ***Not downloaded***

Note: To install, please reboot the system only after status says **Reboot to install**.

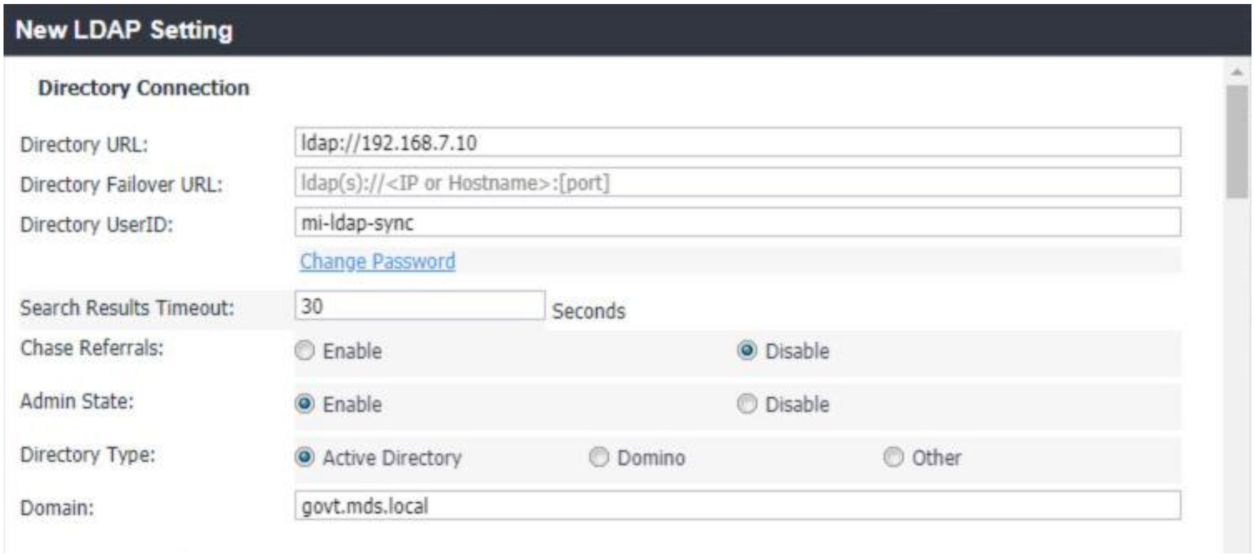
14. Repeat **Steps 4b** through **11** above, replacing 9.5.0.1 with **9.7.0.1** during **Steps 4b** and **6;** this will complete the upgrade path from MobileIron Core 9.5.0.0 to 9.7.0.1.

2.4.4 Integration with Microsoft Active Directory

In our implementation, we chose to integrate MobileIron Core with Active Directory using lightweight directory access protocol (LDAP). This is optional. General instructions for this process are covered in the *Configuring LDAP Servers* section in Chapter 2 of *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector*. The configuration details used during our completion of selected steps (retaining the original numbering) from that guide are given below:

1. From Step 4 in the MobileIron guide, in the **New LDAP Server** dialogue:
   a. Directory Connection:

461 **Figure 2-13 LDAP Settings**



New LDAP Setting

Directory Connection

Directory URL: ldap://192.168.7.10

Directory Failover URL: ldap(s)://<IP or Hostname>:[port]

Directory UserID: mi-ldap-sync

Change Password

Search Results Timeout: 30 Seconds

Chase Referrals: ○ Enable ● Disable

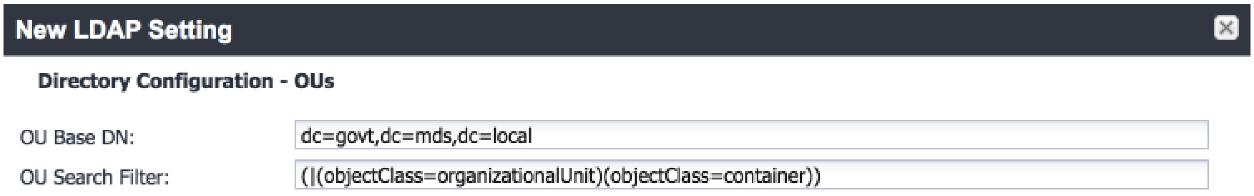
Admin State: ● Enable ○ Disable

Directory Type: ● Active Directory ○ Domino ○ Other

Domain: govt.mds.local

462 b. Directory Configuration—OUs:

463 **Figure 2-14 LDAP OUs**



New LDAP Setting

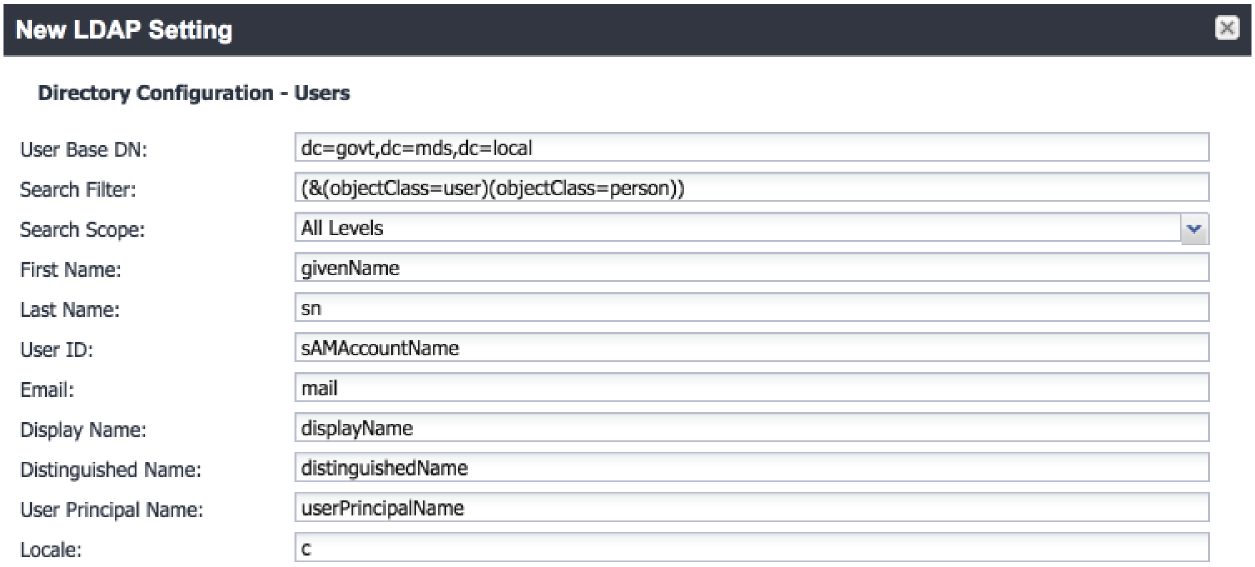
Directory Configuration - OUs

OU Base DN: dc=govt,dc=mds,dc=local

OU Search Filter: (|(objectClass=organizationalUnit)(objectClass=container))

464 c. Directory Configuration—Users:

Figure 2-15 LDAP User Configuration



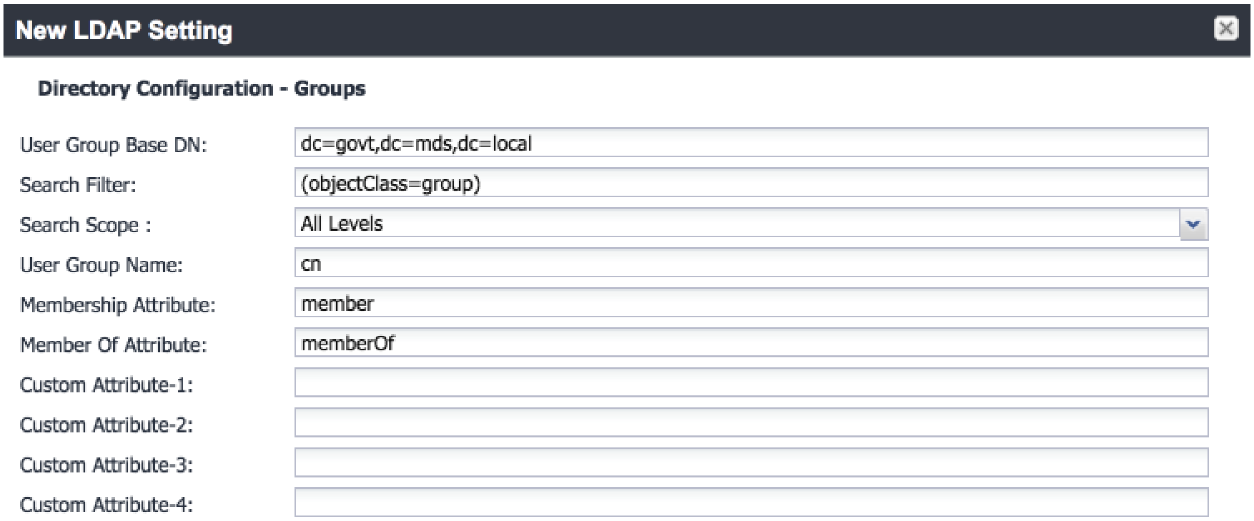
New LDAP Setting

Directory Configuration - Users

User Base DN:	dc=govt,dc=mds,dc=local
Search Filter:	(&(objectClass=user)(objectClass=person))
Search Scope:	All Levels
First Name:	givenName
Last Name:	sn
User ID:	sAMAccountName
Email:	mail
Display Name:	displayName
Distinguished Name:	distinguishedName
User Principal Name:	userPrincipalName
Locale:	c

d. Directory Configuration—Groups:

Figure 2-16 LDAP Group Configuration



New LDAP Setting

Directory Configuration - Groups

User Group Base DN:	dc=govt,dc=mds,dc=local
Search Filter:	(objectClass=group)
Search Scope :	All Levels
User Group Name:	cn
Membership Attribute:	member
Member Of Attribute:	memberOf
Custom Attribute-1:	
Custom Attribute-2:	
Custom Attribute-3:	
Custom Attribute-4:	

e. LDAP Groups:

   i. As a preparatory step, we used Active Directory Users and Computers to create a new security group for mobile-authorized users on the Domain Controller for the *govt.mds.local* domain. In our example, this group is named **Mobile Users.**

   ii. In the search bar, enter the name of the LDAP group for mobile-authorized users.

   iii. Select the **magnifying glass** button; the group name should be added to the **Available** list.

   iv. In the **Available** list box:

      1) Select the **Mobile Users** list item.

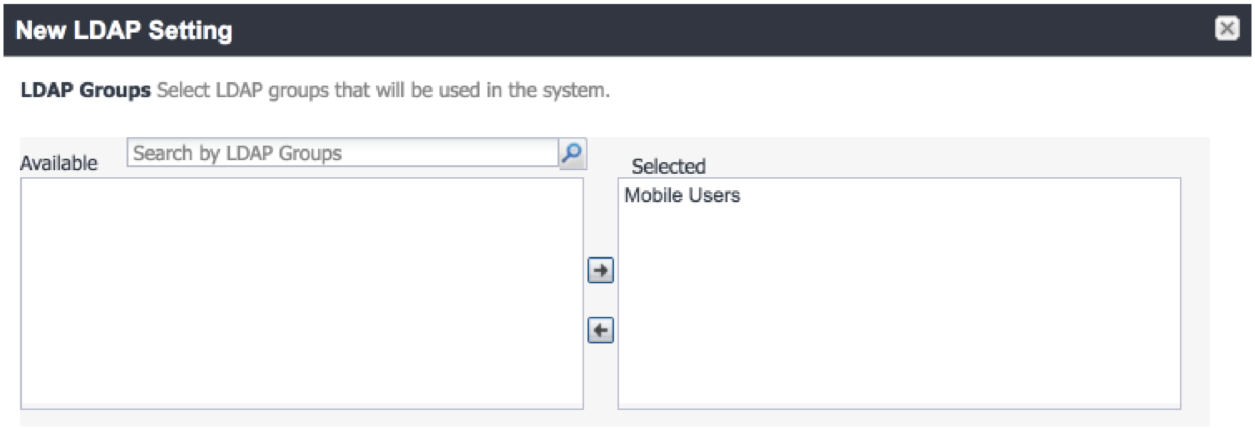
      2) Select the **right-arrow** button; the Mobile Users list item should move to the **Selected** list box.

   v. In the **Selected** list:

      1) Select the default **Users** group list item.

      2) Select the **left-arrow** button; the Users list item should move to the **Available** list box.

Figure 2-17 Selected LDAP Group



New LDAP Setting

LDAP Groups Select LDAP groups that will be used in the system.

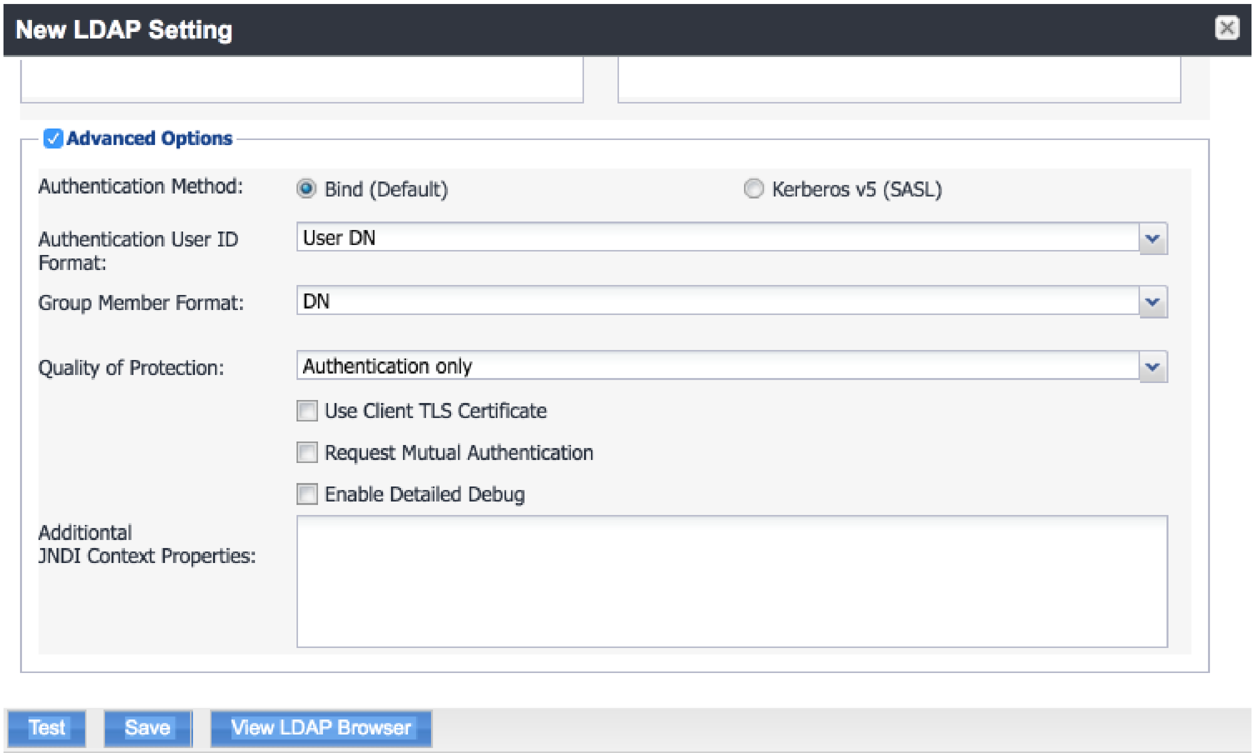
Available: Search by LDAP Groups

Selected: Mobile Users

f. Custom Settings: Custom settings were not specified.

g. Advanced Options: Advanced options were configured as shown in Figure 2-18.

Figure 2-18 LDAP Advanced Options



New LDAP Setting

☑ Advanced Options

Authentication Method: ● Bind (Default) ○ Kerberos v5 (SASL)

Authentication User ID Format: User DN

Group Member Format: DN

Quality of Protection: Authentication only

□ Use Client TLS Certificate

□ Request Mutual Authentication

□ Enable Detailed Debug

Additiontal JNDI Context Properties:

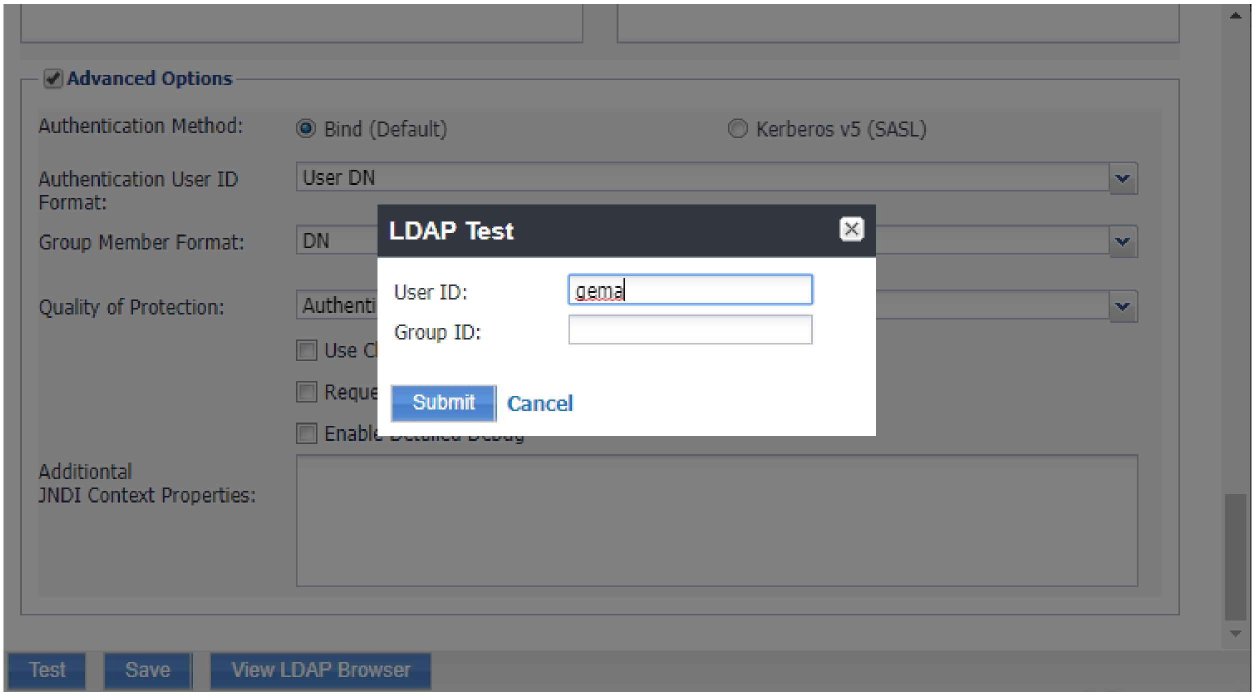
Note: In our lab environment, we did not enable stronger Quality of Protection or enable the Use of Client Transport Layer Security Certificate or Request Mutual Authentication features. However, we recommend that implementers consider using those additional mechanisms to secure communication with the LDAP server.

2. From **Steps 19** through **21** from the MobileIron guide, we tested that MobileIron can successfully query LDAP for Derived Personal Identity Verification Credential (DPC) Users.

   a. In the **New LDAP Setting** dialogue, click the **Test** button to open the **LDAP Test** dialogue.

   b. In the **LDAP Test** dialogue, enter a **User ID** for a member of the DPC Users group, then click the **Submit** button. A member of the Mobile Users group in our environment is **gema.**

Figure 2-19 Testing LDAP Configuration



☑ Advanced Options

Authentication Method: ● Bind (Default) ○ Kerberos v5 (SASL)

Authentication User ID Format: User DN

Group Member Format: DN

Quality of Protection: Authenti

□ Use C

□ Reque

□ Enable

Additional JNDI Context Properties:

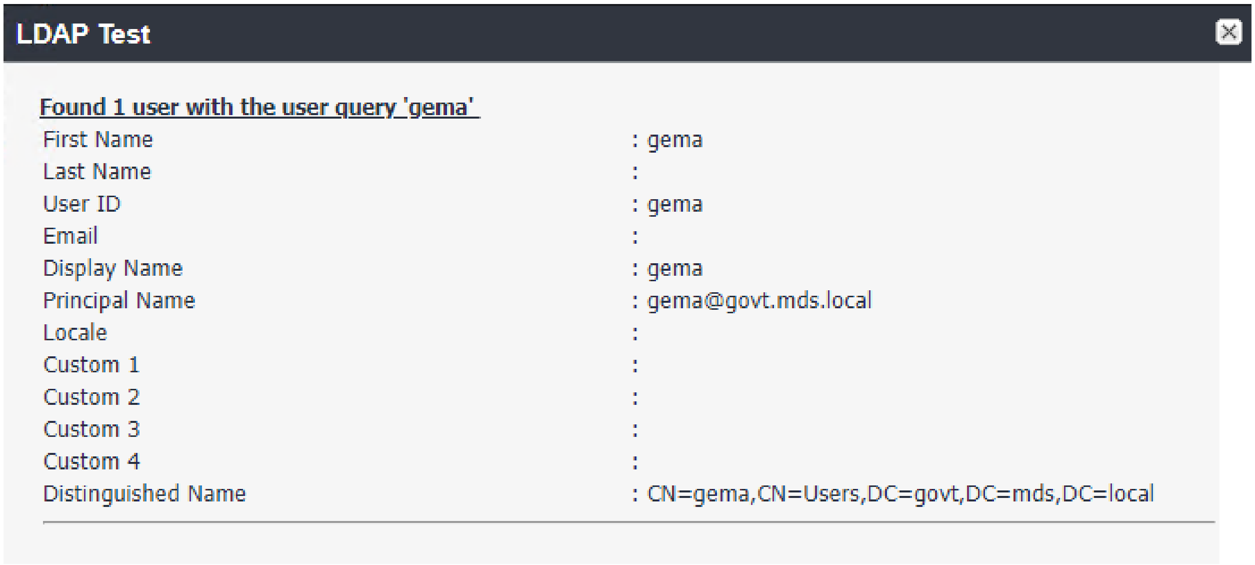
LDAP Test

User ID: gema

Group ID:

c. The **LDAP Test** dialogue indicates the query was successful:

Figure 2-20 LDAP Test Result



LDAP Test

Found 1 user with the user query 'gema'

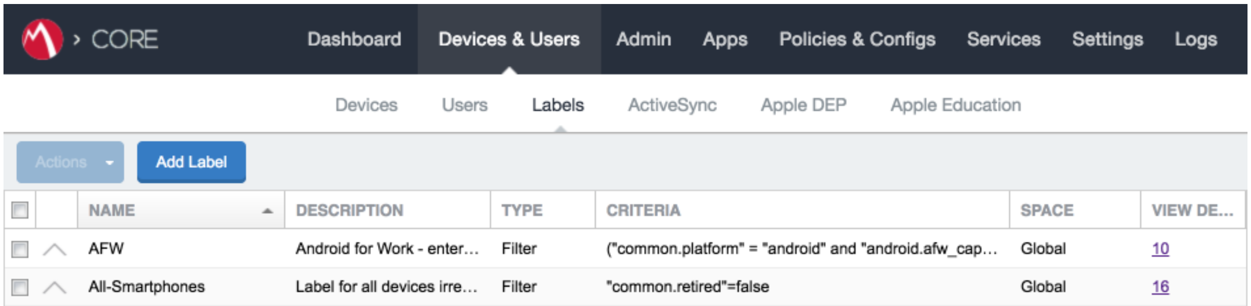
First Name	: gema
Last Name	:
User ID	: gema
Email	:
Display Name	: gema
Principal Name	: gema@govt.mds.local
Locale	:
Custom 1	:
Custom 2	:
Custom 3	:
Custom 4	:
Distinguished Name	: CN=gema,CN=Users,DC=govt,DC=mds,DC=local

2.4.5 Create a Mobile Users Label

MobileIron uses labels to link policies and device configurations with users and mobile devices. Creating a unique label for each category of authorized mobile user allows mobile device administrators to apply a consistent set of controls applicable to users with a common mobile use case. Our limited usage scenario only required a single MobileIron label to be created.

1. In the **MobileIron Core Admin Portal,** navigate to **Devices & Users > Labels.**
2. Select **Add Label.**

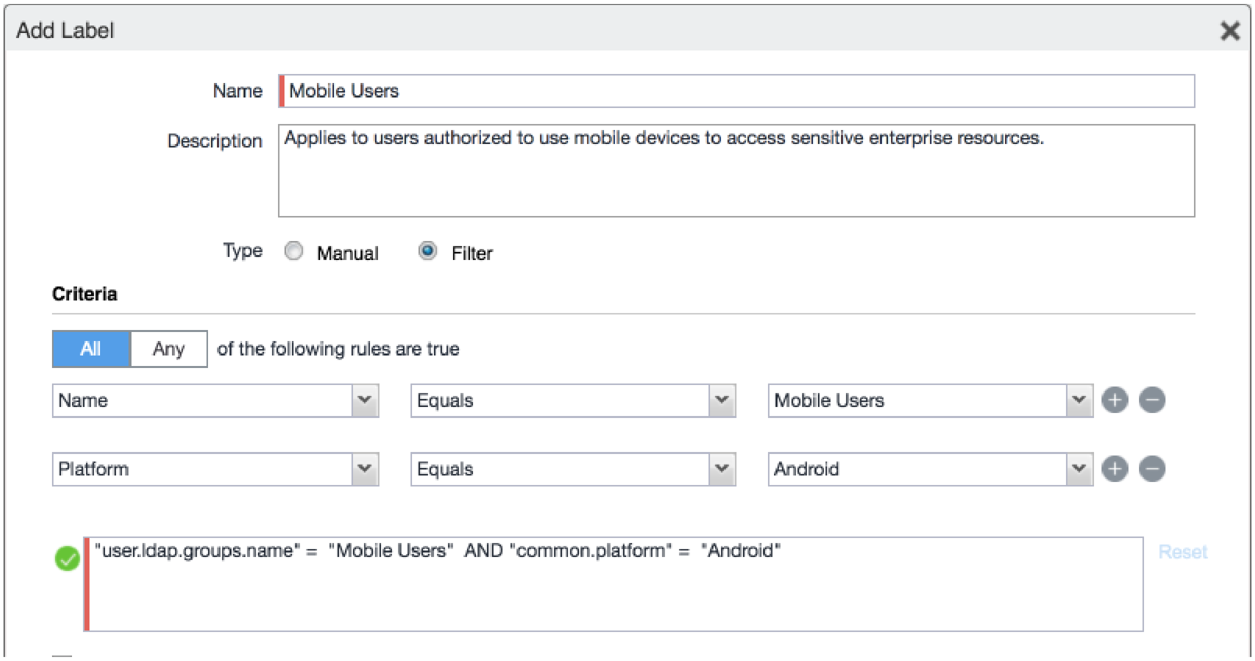
Figure 2-21 MobileIron Device Labels



☐		NAME	DESCRIPTION	TYPE	CRITERIA	SPACE	VIEW DE...
☐		AFW	Android for Work - enter...	Filter	("common.platform" = "android" and "android.afw_cap...	Global	10
☐		All-Smartphones	Label for all devices irre...	Filter	"common.retired"=false	Global	16

3. In the **Name** field, enter a unique name for this label (**Mobile Users** in this example).
4. In the **Description** field, enter a meaningful description to help others identify its purpose.
5. Under the **Criteria** section:
   a. In the blank rule:
      i. In the **Field** drop-down menu, select **User > LDAP > Groups > Name.**
      ii. In the **Value** drop-down menu, select the Active Directory group created to support mobile user policies (named **Mobile User** in this example).
   b. Select the **plus sign icon** to add a blank rule.
   c. In the newly created blank rule:
      i. In the **Field** drop-down menu, select **Common > Platform.**
      ii. In the **Value** drop-down menu, select **Android.**

520 **Figure 2-22 Adding a Device Label**



Add Label

Name: Mobile Users

Description: Applies to users authorized to use mobile devices to access sensitive enterprise resources.

Type: ○ Manual ● Filter

Criteria

All | Any of the following rules are true

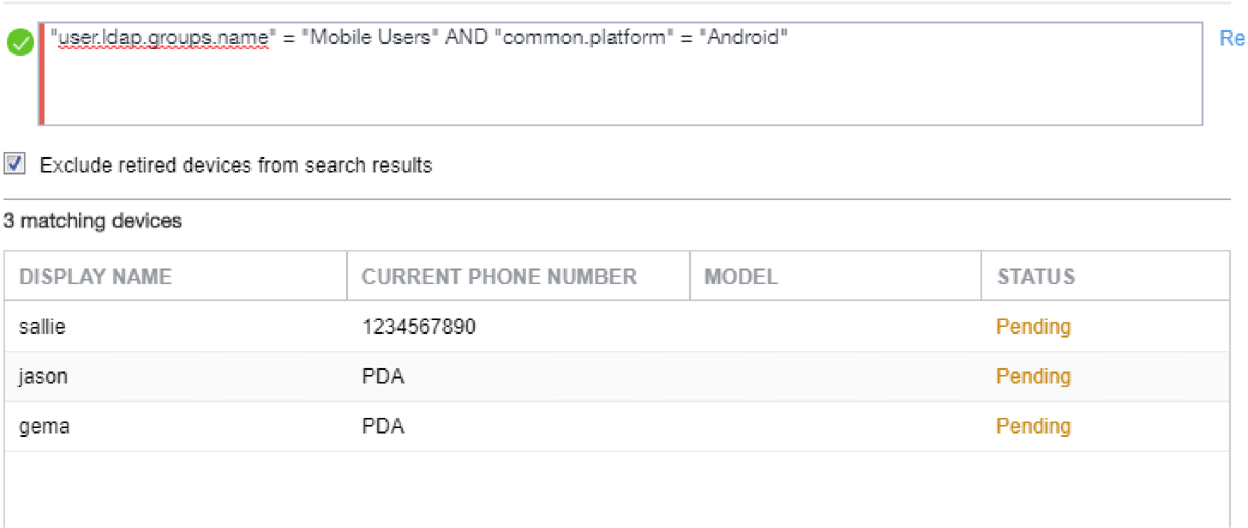
Name	Equals	Mobile Users
Platform	Equals	Android

```
"user.ldap.groups.name" =  "Mobile Users"  AND "common.platform" =  "Android"
```

521 d. The list of matching devices will appear below the specified criteria.

522 e. Select **Save.**

523 **Figure 2-23 Device Label Matches**



```
"user.ldap.groups.name" = "Mobile Users" AND "common.platform" = "Android"
```

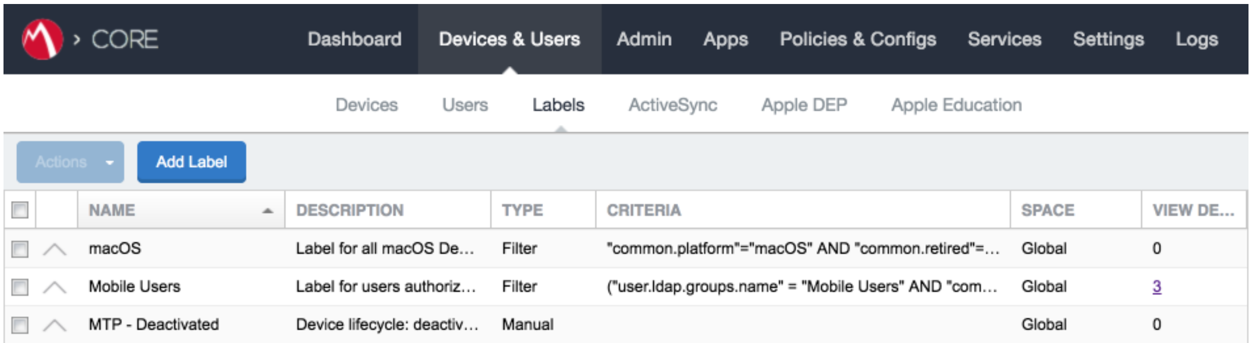
☑ Exclude retired devices from search results

3 matching devices

DISPLAY NAME	CURRENT PHONE NUMBER	MODEL	STATUS
sallie	1234567890		Pending
jason	PDA		Pending
gema	PDA		Pending

524 6. Navigate to **Devices & Users > Labels** to confirm the label was successfully created.

Figure 2-24 MobileIron Label List



□		NAME	DESCRIPTION	TYPE	CRITERIA	SPACE	VIEW DE...
□		macOS	Label for all macOS De...	Filter	"common.platform"="macOS" AND "common.retired"=...	Global	0
□		Mobile Users	Label for users authoriz...	Filter	("user.ldap.groups.name" = "Mobile Users" AND "com...	Global	3
□		MTP - Deactivated	Device lifecycle: deactiv...	Manual		Global	0

2.5 Integration of Palo Alto Networks GlobalProtect with MobileIron

The following steps detail how to integrate MobileIron Core, Microsoft Certificate Authority (CA), and Palo Alto Networks GlobalProtect to allow mobile users to authenticate to the GlobalProtect gateway using user-aware device certificates issued to mobile devices by Microsoft CA during enrollment with MobileIron Core.

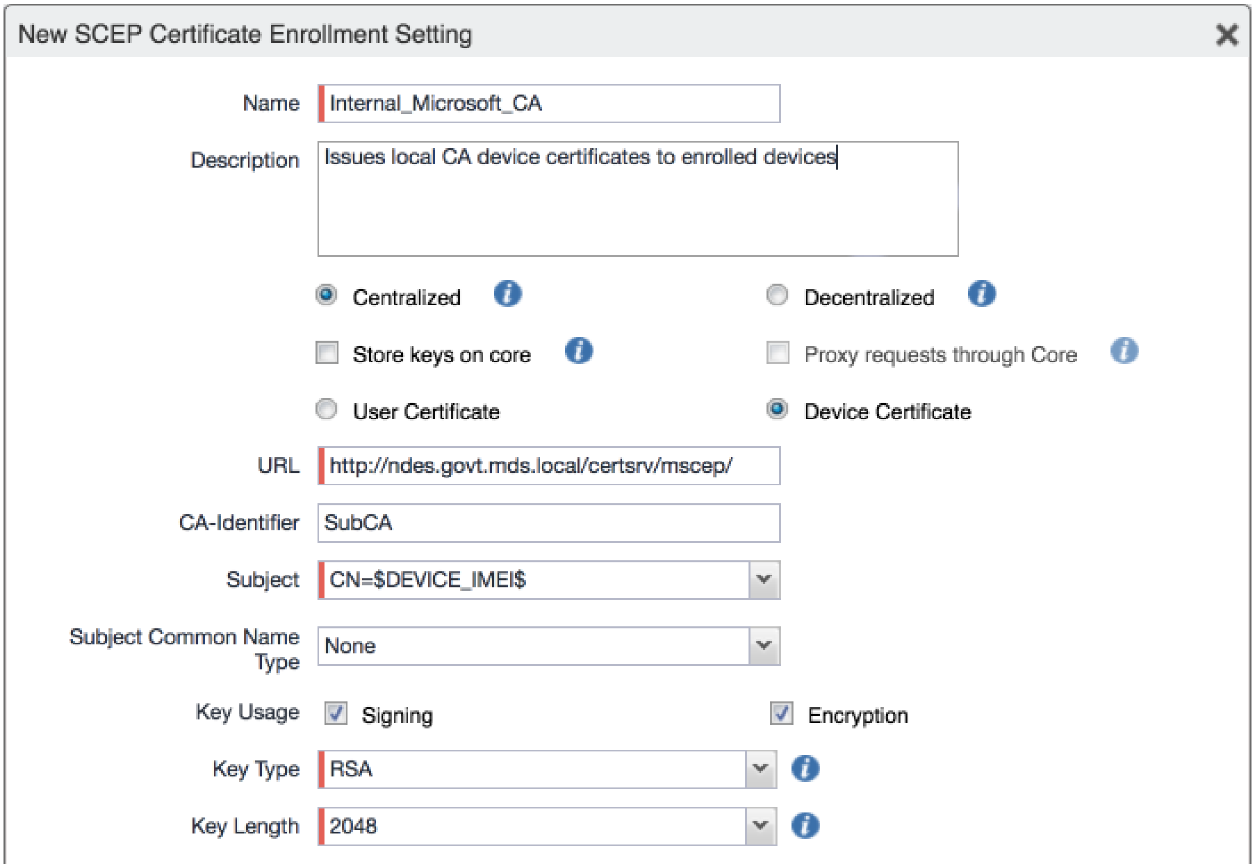
2.5.1 MobileIron Configuration

The following steps create the MobileIron Core configurations necessary to support integration with Palo Alto GlobalProtect and Microsoft CA.

2.5.1.1 Create Simple Certificate Enrollment Protocol (SCEP) Configuration

1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.
2. Select **Add New > Certificate Enrollment > SCEP**; the **New SCEP Configuration Enrollment Setting** dialogue will open.
3. In the **New SCEP Certificate Enrollment Setting** dialogue:
    a. For the **Name** field, enter a unique name to identify this configuration.
    b. Enable the **Device Certificate** option.
    c. In the **URL** field, enter the URL where SCEP is hosted within your environment.
    d. In the **CA-Identifier (ID)** field, enter the subject name of the Microsoft CA that will issue the device certificates.
    e. In the **Subject** drop-down menu, select **$DEVICE_IMEI$.**

Figure 2-25 MobileIron SCEP Configuration



New SCEP Certificate Enrollment Setting

Name: Internal_Microsoft_CA

Description: Issues local CA device certificates to enrolled devices

● Centralized ○ Decentralized

□ Store keys on core □ Proxy requests through Core

○ User Certificate ● Device Certificate

URL: http://ndes.govt.mds.local/certsrv/mscep/

CA-Identifier: SubCA

Subject: CN=$DEVICE_IMEI$

Subject Common Name Type: None

Key Usage: ☑ Signing ☑ Encryption

Key Type: RSA

Key Length: 2048

f. In the **Fingerprint** field, enter the fingerprint of the Microsoft CA that will issue the device certificates.

g. For the **Challenge Type** drop-down menu, select **Microsoft SCEP.**

h. Below the **Subject Alternative Names** list box, select **Add;** a new list item will appear.

i. For the new list item:

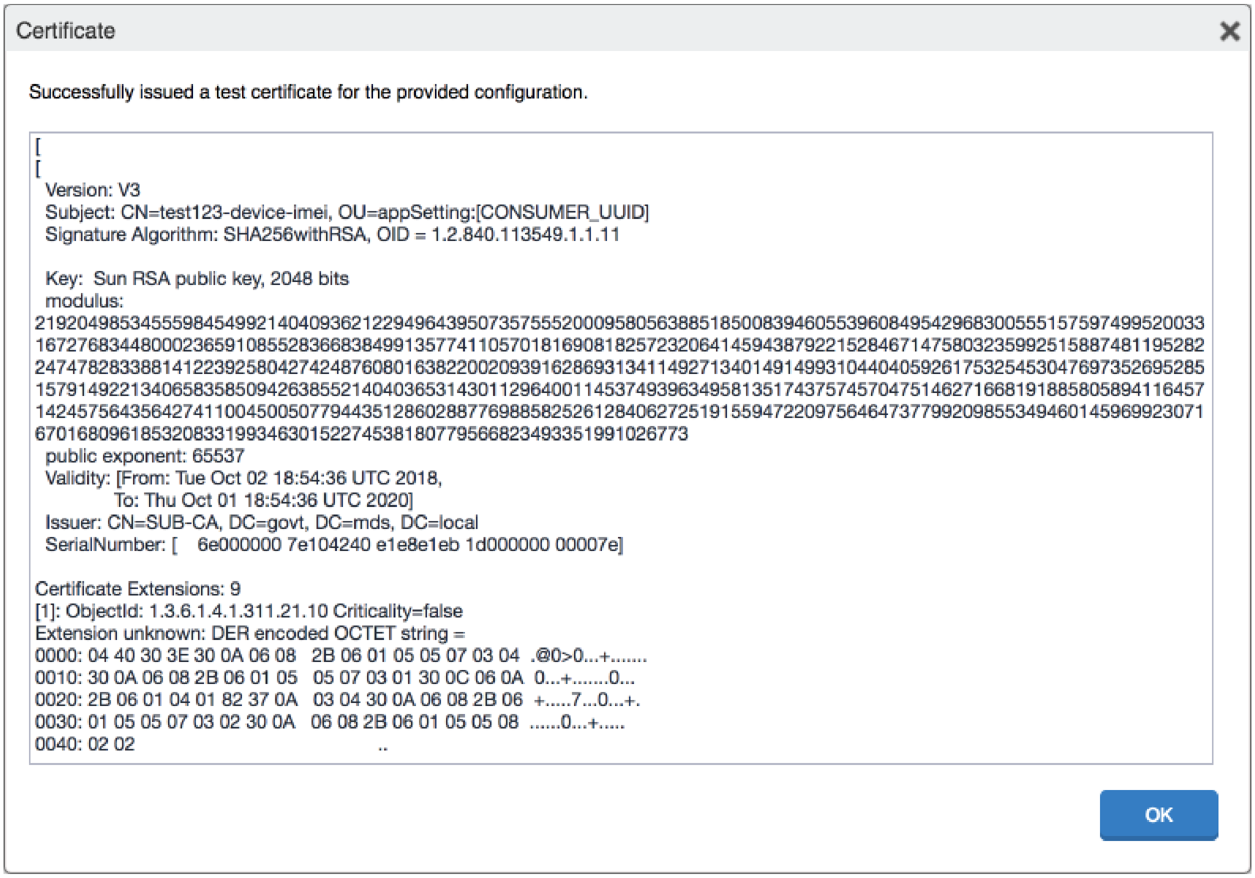
   i. For the **Type** drop-down menu, select **NT Principal Name.**

   ii. For the **Value** drop-down menu, select **$USER_UPN$.**

j. Select **Issue Test Certificate;** the **Certificate** dialogue should indicate success.

k. In the **Certificate** dialogue, select **OK.**

Figure 2-26 Test SCEP Certificate

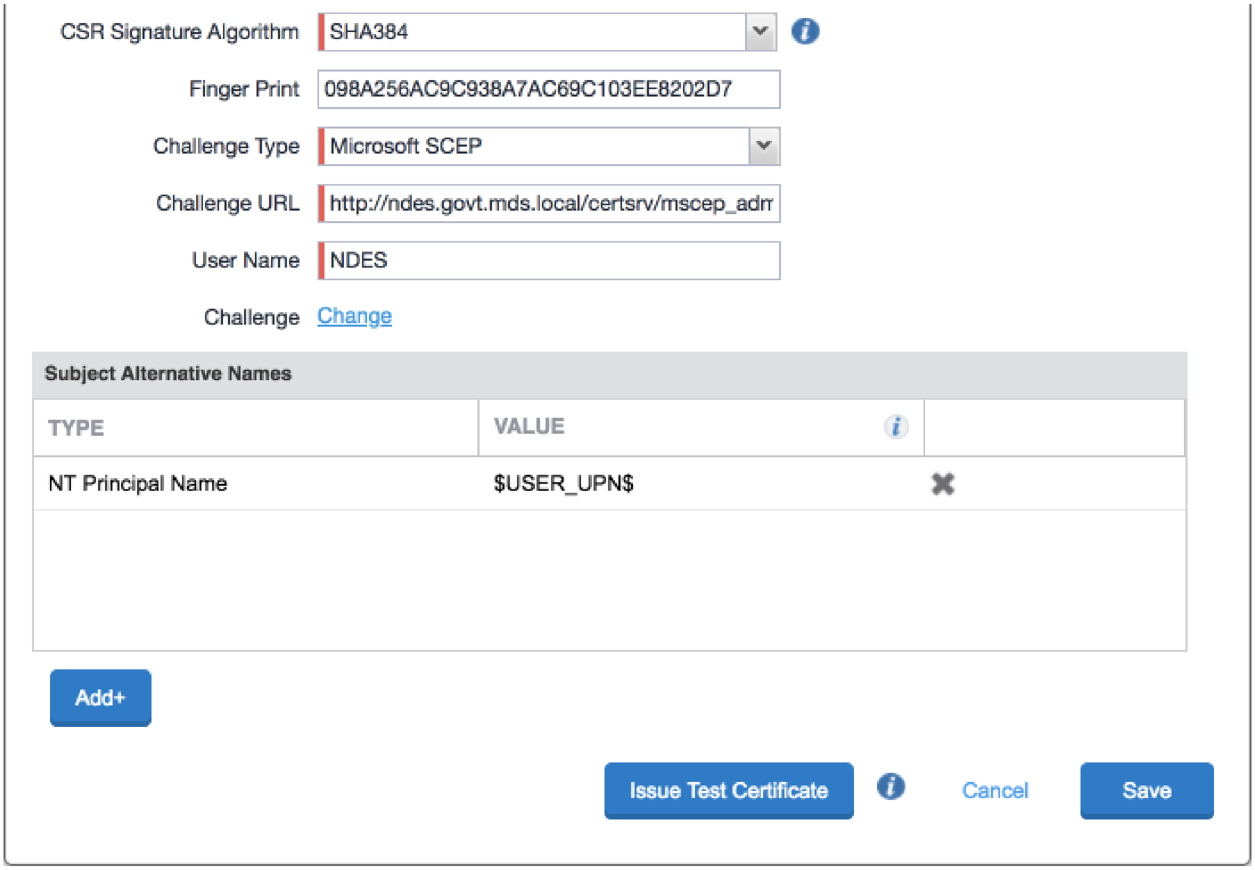


Successfully issued a test certificate for the provided configuration.

```
[
[
  Version: V3
  Subject: CN=test123-device-imei, OU=appSetting:[CONSUMER_UUID]
  Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

  Key:  Sun RSA public key, 2048 bits
  modulus:
219204985345559845499214040936212294964395073575552000958056388518500839460553960849542968300555157597499520033
167276834480002365910855283668384991357741105701816908182572320641459438792215284671475803235992515887481195282
247478283388141223925804274248760801638220020939162869313411492713401491499310440405926175325453047697352695285
157914922134065835850942638552140403653143011296400114537493963495813517437574570475146271668191885805894116457
142457564356427411004500507794435128602887769885825261284062725191559472209756464737799209855349460145969923071
67016809618532083319934630152274538180779566823493351991026773
  public exponent: 65537
  Validity: [From: Tue Oct 02 18:54:36 UTC 2018,
               To: Thu Oct 01 18:54:36 UTC 2020]
  Issuer: CN=SUB-CA, DC=govt, DC=mds, DC=local
  SerialNumber: [    6e000000 7e104240 e1e8e1eb 1d000000 00007e]

Certificate Extensions: 9
[1]: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 40 30 3E 30 0A 06 08   2B 06 01 05 05 07 03 04  .@0>0...+.......
0010: 30 0A 06 08 2B 06 01 05   05 07 03 01 30 0C 06 0A  0...+.......0...
0020: 2B 06 01 04 01 82 37 0A   03 04 30 0A 06 08 2B 06  +.....7...0...+.
0030: 01 05 05 07 03 02 30 0A   06 08 2B 06 01 05 05 08  ......0...+.....
0040: 02 02                                              ..
```

4. Select **Save.**

Figure 2-27 Test SCEP Certificate Configuration



CSR Signature Algorithm: SHA384

Finger Print: 098A256AC9C938A7AC69C103EE8202D7

Challenge Type: Microsoft SCEP

Challenge URL: http://ndes.govt.mds.local/certsrv/mscep_adr

User Name: NDES

Challenge: Change

Subject Alternative Names

TYPE	VALUE
NT Principal Name	$USER_UPN$

2.5.1.2 Create Palo Alto Networks GlobalProtect Configuration

The GlobalProtect configuration instructs the mobile client to connect to use the provisioned device certificate and to automatically connect to the correct VPN URL; mobile users will not need to manually configure the application. The following steps will create the GlobalProtect configuration.

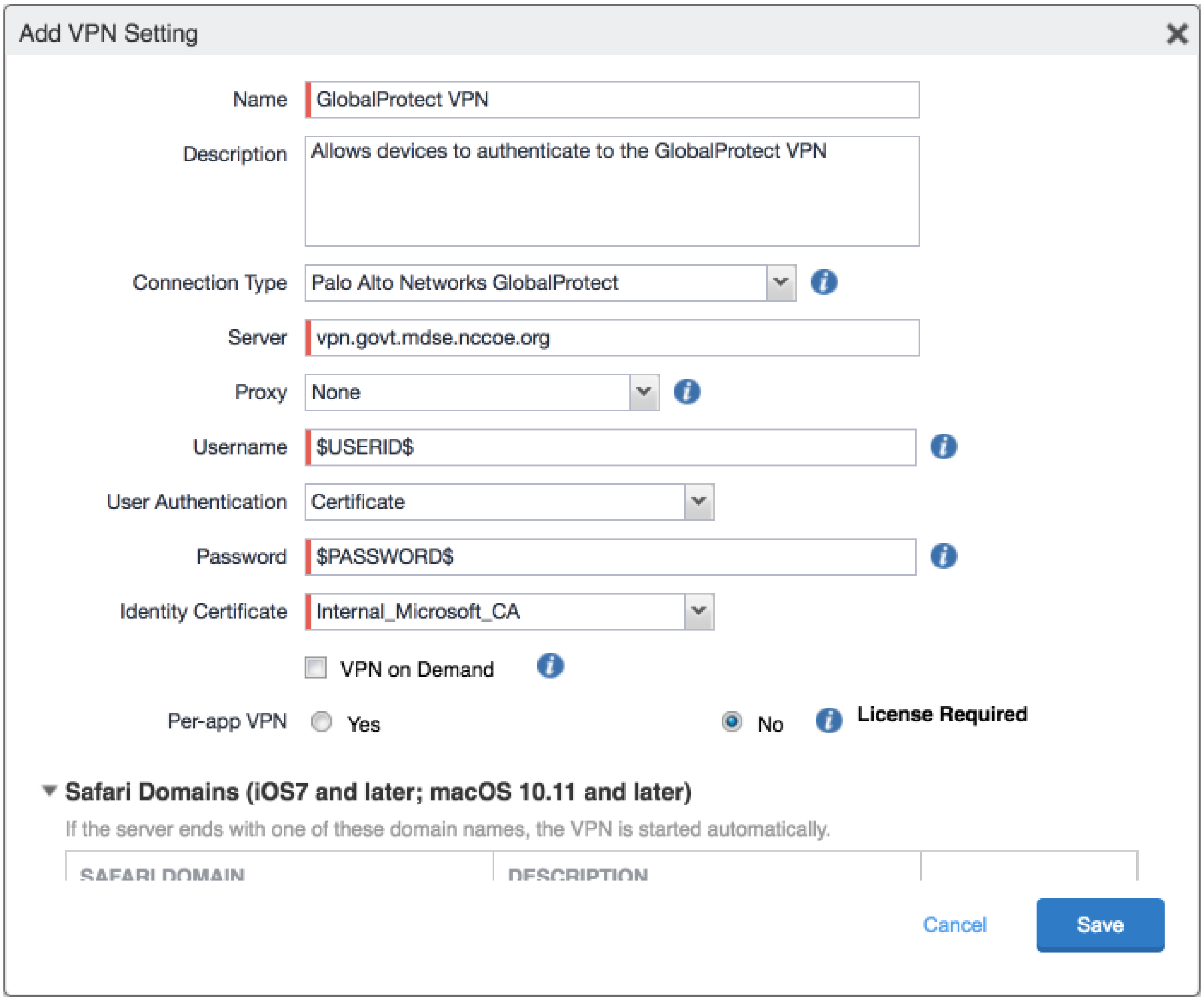
1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.
2. Select **Add New > VPN**; the **Add VPN Setting** dialogue will appear.
3. In the **Add VPN Setting** dialogue:
    a. In the **Name** field, enter a unique name to identify this VPN setting.
    b. In the **Connection Type** drop-down menu, select **Palo Alto Networks GlobalProtect.**
    c. In the **Server** field, enter the fully qualified domain name (FQDN) of your Palo Alto Networks appliance; our sample implementation uses **vpn.govt.mdse.nccoe.org.**

d. For the **User Authentication** drop-down menu, select **certificate.**

e. For the **Identity Certificate** drop-down menu, select the SCEP enrollment profile created in the previous section.

f. Select **Save.**

Figure 2-28 MobileIron VPN Configuration



Add VPN Setting

Name	GlobalProtect VPN
Description	Allows devices to authenticate to the GlobalProtect VPN
Connection Type	Palo Alto Networks GlobalProtect
Server	vpn.govt.mdse.nccoe.org
Proxy	None
Username	$USERID$
User Authentication	Certificate
Password	$PASSWORD$
Identity Certificate	Internal_Microsoft_CA
	☐ VPN on Demand
Per-app VPN	○ Yes ● No License Required

▾ Safari Domains (iOS7 and later; macOS 10.11 and later)

If the server ends with one of these domain names, the VPN is started automatically.

2.5.2 Basic Palo Alto Networks Configuration

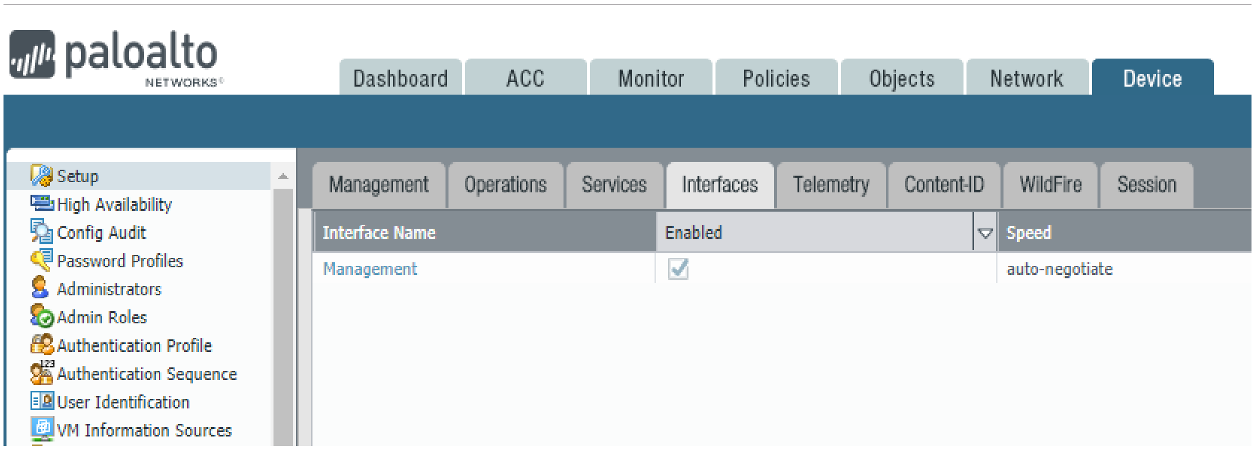
During basic configuration, internet protocol (IP) addresses are assigned to the management interface, domain name system (DNS), and network time protocol (NTP). The management interface allows the administrator to configure and implement security rules through this interface.

2.5.2.1 Configure Management Interface

The following steps will configure the Palo Alto Networks appliance management interface.

1. In the Palo Alto Networks portal, navigate to **Device > Setup > Interfaces.**
2. On the Interfaces tab, enable the **Management** option; the Management Interface Setting page will open.

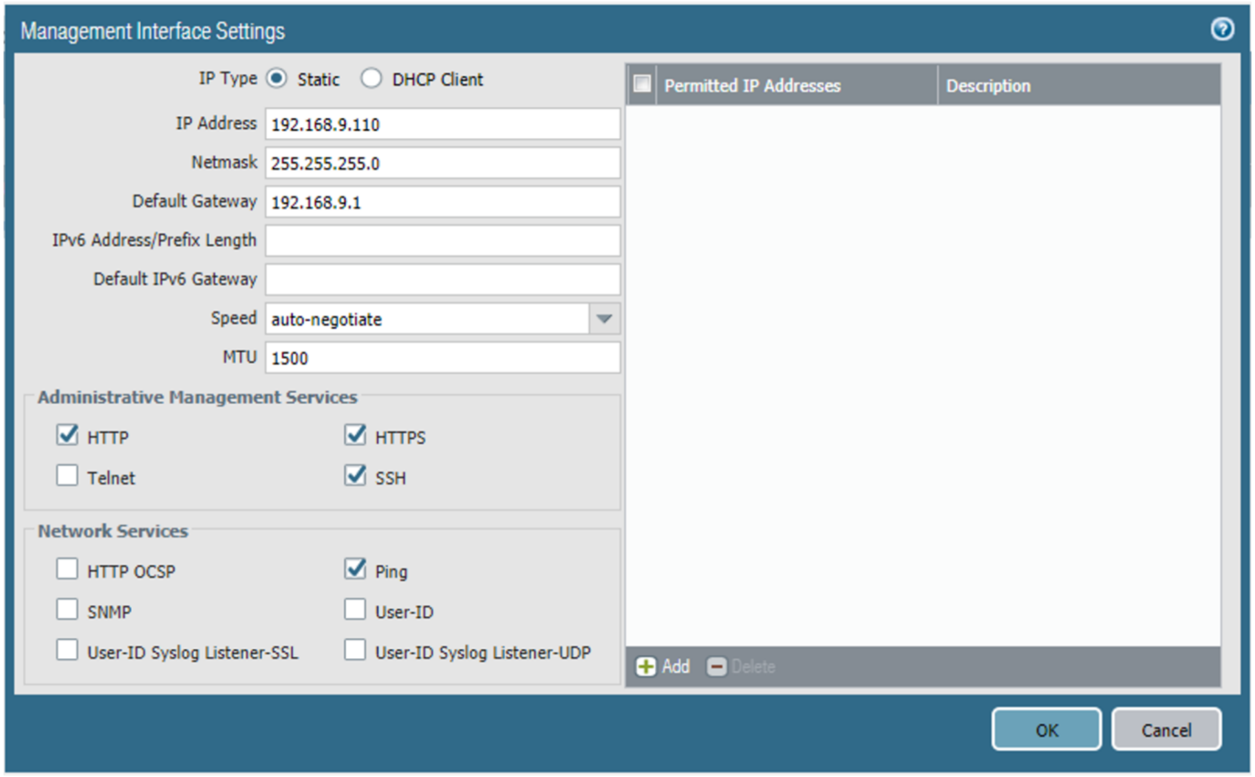
Figure 2-29 Palo Alto Networks Management Interface Enabled



Interface Name	Enabled	Speed
Management	☑	auto-negotiate

3. On the Management Interface Setting screen:
   a. In the **IP Address** field, enter the IP address for the Palo Alto Networks appliance.
   b. In the **Netmask** field, enter the netmask for the network.
   c. In the **Default Gateway** field, enter the IP address of the router that provides the appliance with access to the internet.
   d. Under **Administrative Management Services:** Enable the **Hypertext Transfer Protocol (HTTP)**, **Hypertext Transfer Protocol Secure (HTTPS)**, **Secure Shell (SSH)**, and **Ping** options.
   e. Click **OK.**

Figure 2-30 Management Interface Configuration



Management Interface Settings

IP Type ● Static ○ DHCP Client

IP Address 192.168.9.110

Netmask 255.255.255.0

Default Gateway 192.168.9.1

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed auto-negotiate

MTU 1500

Administrative Management Services

☑ HTTP ☑ HTTPS

□ Telnet ☑ SSH

Network Services

□ HTTP OCSP ☑ Ping

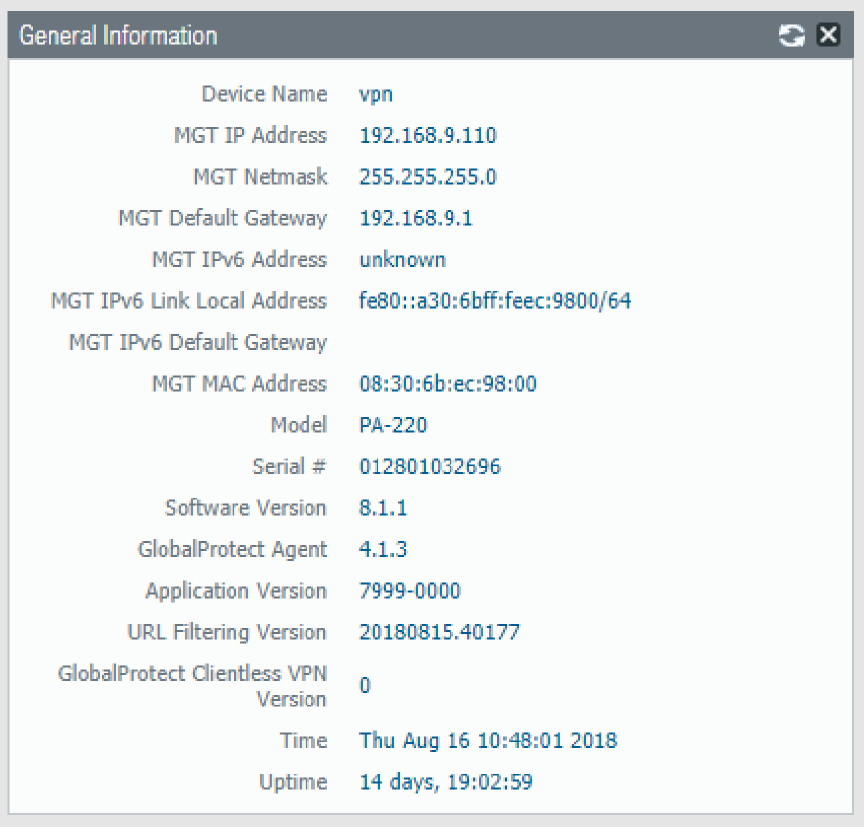
□ SNMP □ User-ID

□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	Permitted IP Addresses	Description

4. To verify the configuration, navigate to **Palo Alto Networks Portal > Dashboard;** the **General Information** section should reflect the appliance's network configuration.

Figure 2-31 Palo Alto Networks Firewall General Information



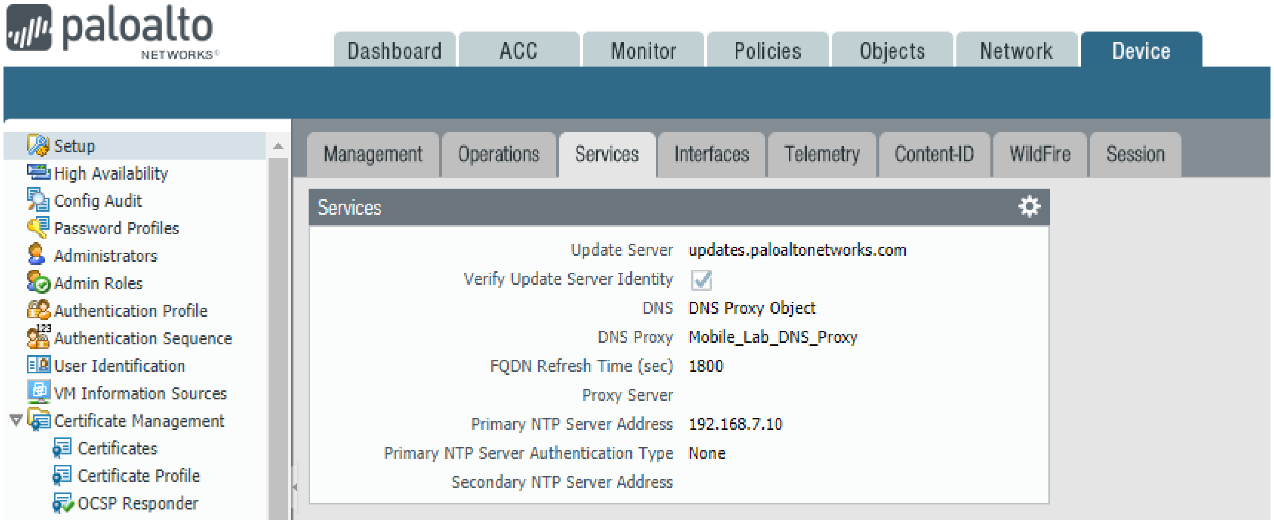
General Information

Device Name	vpn
MGT IP Address	192.168.9.110
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.9.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::a30:6bff:feec:9800/64
MGT IPv6 Default Gateway	
MGT MAC Address	08:30:6b:ec:98:00
Model	PA-220
Serial #	012801032696
Software Version	8.1.1
GlobalProtect Agent	4.1.3
Application Version	7999-0000
URL Filtering Version	20180815.40177
GlobalProtect Clientless VPN Version	0
Time	Thu Aug 16 10:48:01 2018
Uptime	14 days, 19:02:59

2.5.2.2 Configure DNS and NTP

1. In the **Palo Alto Networks Portal**, navigate to **Device > Setup > Services.**
2. In the **Services** tab, select the settings icon.

Figure 2-32 Palo Alto Networks Services Configuration



Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	☑
DNS	DNS Proxy Object
DNS Proxy	Mobile_Lab_DNS_Proxy
FQDN Refresh Time (sec)	1800
Proxy Server	
Primary NTP Server Address	192.168.7.10
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	

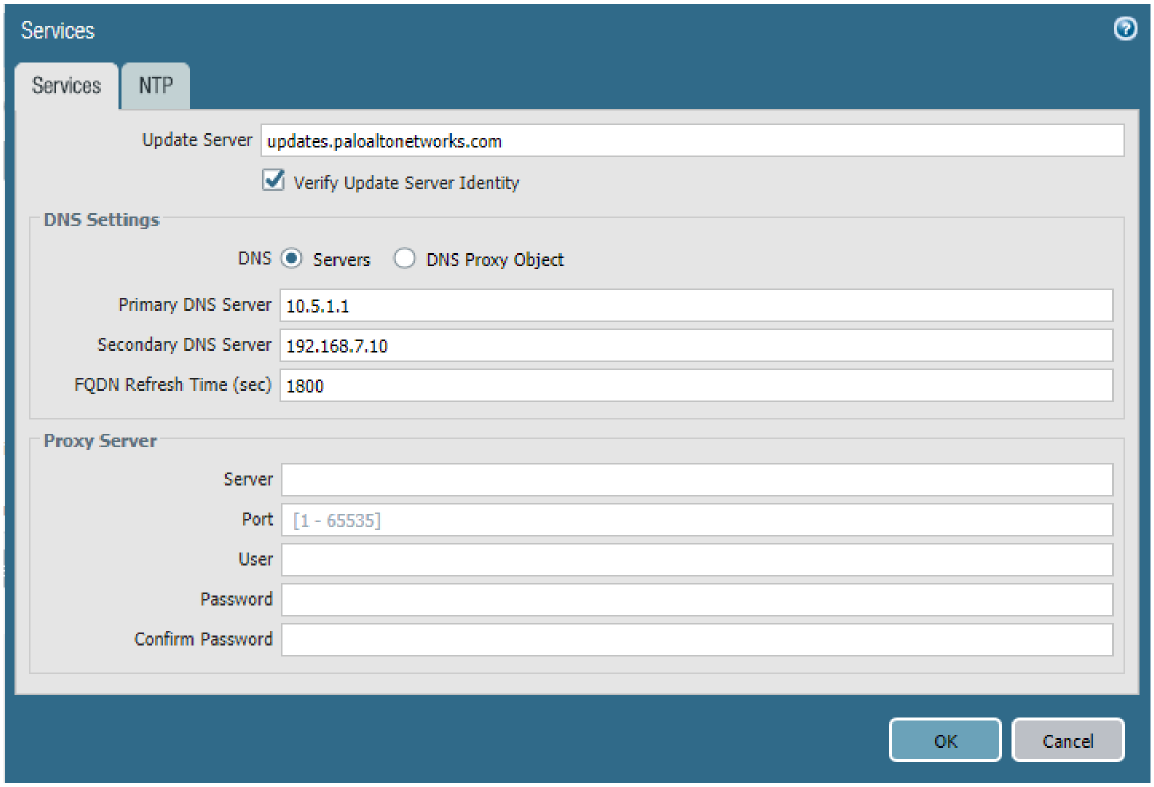
3. On the Services > Services tab:

    a. For the **Primary DNS Server** field, enter the primary DNS server IP address.

    b. For the **Secondary DNS Server** field, enter the secondary DNS server IP address, if applicable.

4. Select the **NTP** tab.

Figure 2-33 DNS Configuration



Update Server: updates.paloaltonetworks.com

☑ Verify Update Server Identity

DNS Settings

DNS ● Servers ○ DNS Proxy Object

Primary DNS Server: 10.5.1.1

Secondary DNS Server: 192.168.7.10

FQDN Refresh Time (sec): 1800

Proxy Server

Server:

Port: [1 - 65535]

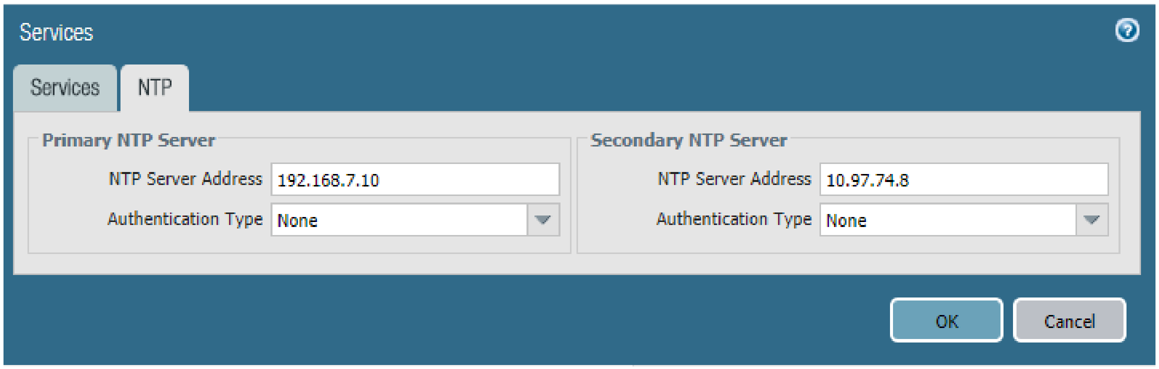
User:

Password:

Confirm Password:

5. On the **NTP** tab:
    a. For the **Primary NTP Server > NTP Server Address** field, enter the IP address of the primary NTP server to use.
    b. For the **Secondary NTP Server > NTP Server Address** field, enter the IP address of the backup NTP server to use, if applicable.
6. Select **OK.**

Figure 2-34 NTP Configuration



Primary NTP Server

NTP Server Address: 192.168.7.10

Authentication Type: None

Secondary NTP Server

NTP Server Address: 10.97.74.8

Authentication Type: None

2.5.3 Palo Alto Networks Interfaces and Zones Configuration

Palo Alto Networks firewall model PA-220 has eight interfaces that can be configured as trusted (inside) or untrusted (outside) interfaces. This section describes creating a zone and assigning an interface to it.

2.5.3.1 Create Ethernet Interfaces and Addresses

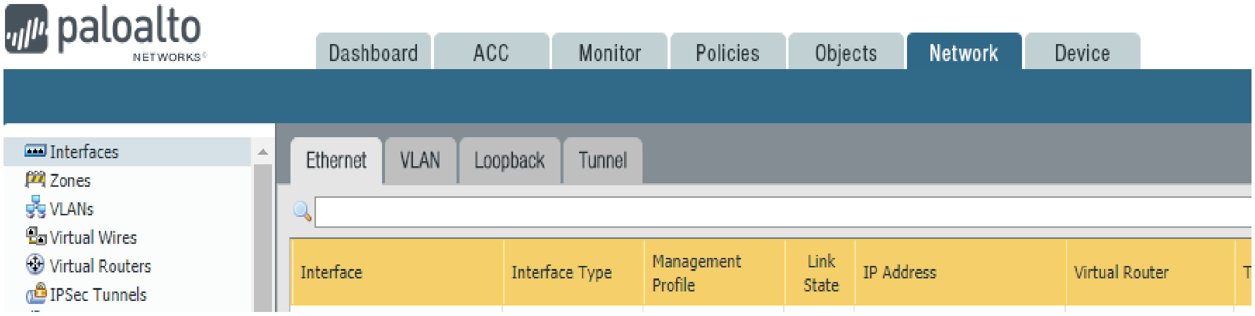
Our example implementation uses three interfaces:

- LAN: Orvilia’s LAN, which hosts intranet web and mail services
- DMZ: Orvilia’s DMZ network subnet, which hosts MobileIron Core and MobileIron Sentry
- WAN: provides access to the internet and is the inbound interface for secure sockets layer (SSL) VPN connections

To create and configure Ethernet interfaces:

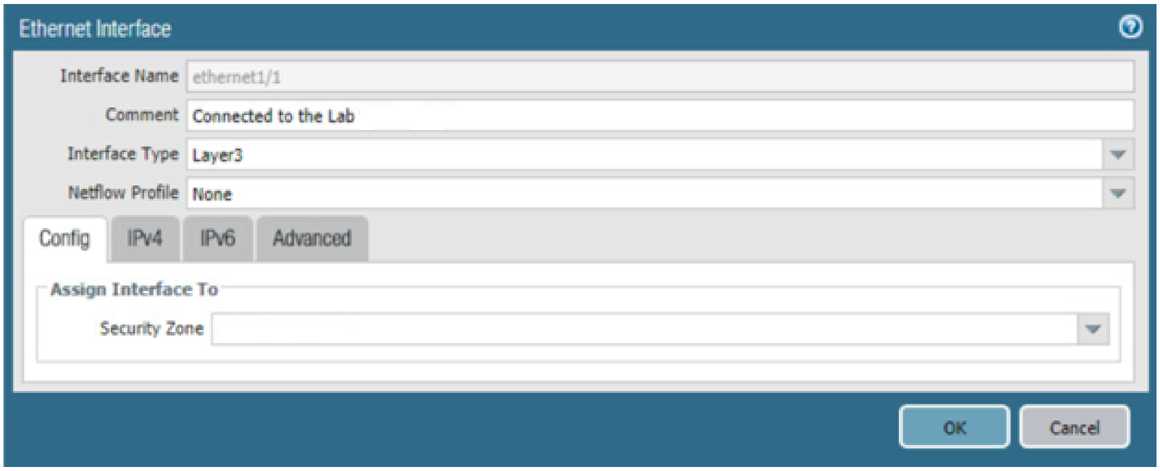
1. Navigate to **Palo Alto Networks Portal > Network > Ethernet > Interfaces > Ethernet.**

Figure 2-35 Ethernet Interfaces



2. In the **Ethernet** tab, select the name of the interface to configure; the Ethernet Interface dialogue will appear.
3. In the **Ethernet Interface** dialogue:
   a. In the **Comment** field, enter a description for this interface.
   b. For the **Interface Type** drop-down menu, select **Layer3.**

Figure 2-36 Ethernet Interface Configuration

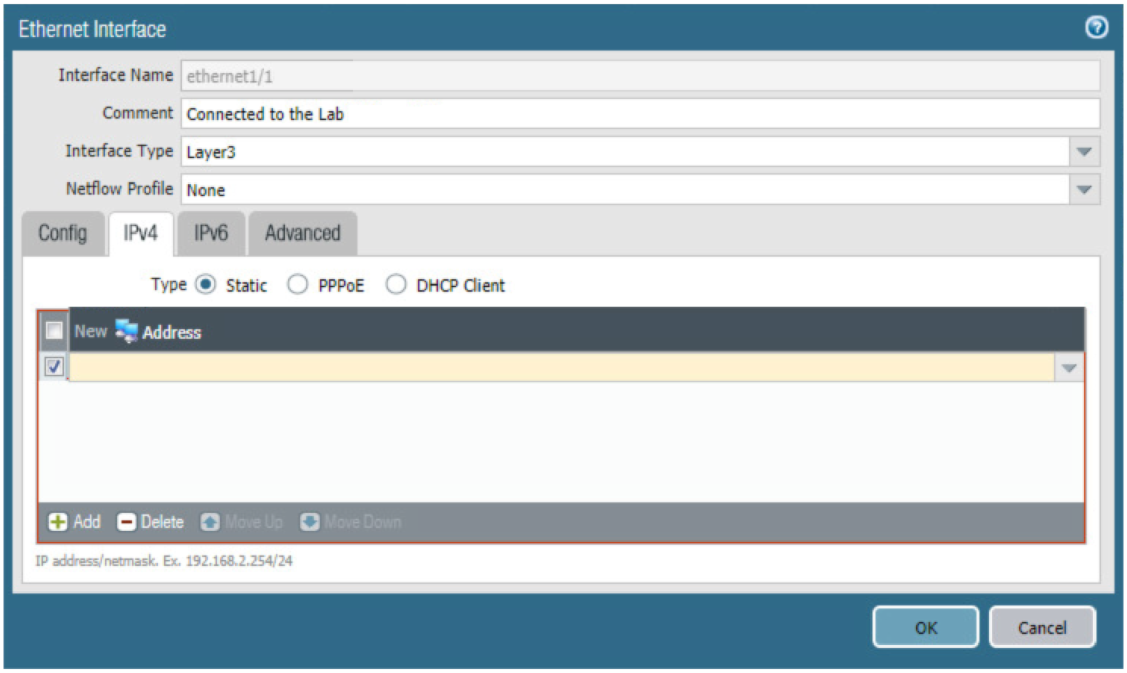


Ethernet Interface

Interface Name: ethernet1/1
Comment: Connected to the Lab
Interface Type: Layer3
Netflow Profile: None

   c. Select the **IPv4** tab.
   d. On the **IPv4** tab:
      i. In the **IP** list box, select **Add;** a blank list item will appear.
      ii. In the blank list item, select **New Address;** the Address dialogue will appear.

Figure 2-37 WAN Interface IPv4 Configuration



Ethernet Interface

Interface Name: ethernet1/1

Comment: Connected to the Lab

Interface Type: Layer3

Netflow Profile: None

Type: ● Static ○ PPPoE ○ DHCP Client

IP address/netmask. Ex. 192.168.2.254/24

iii. In the **Address** dialogue:

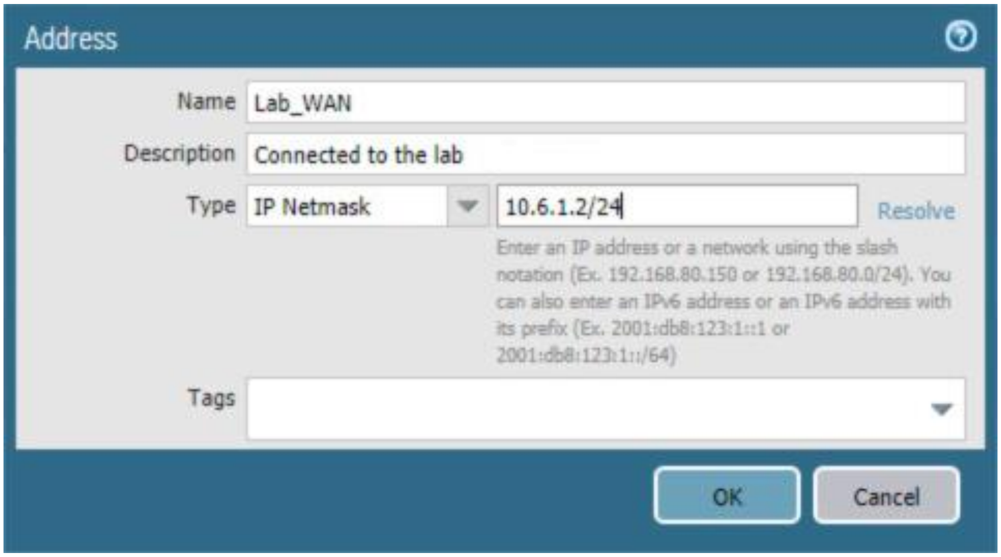
1) For the **Name** field, enter a unique name to identify this address.

2) For the **Description** field, enter a meaningful description of the purpose of this address.

3) In the unnamed field following the **Type** drop-down menu, enter the IPv4 address that this interface will use in **Classless Inter-Domain Routing** notation. This example uses **10.6.1.2/24** for the WAN interface in our lab environment.

4) Select **OK.**

Figure 2-38 WAN Interface IP Address Configuration



Name: Lab_WAN

Description: Connected to the lab

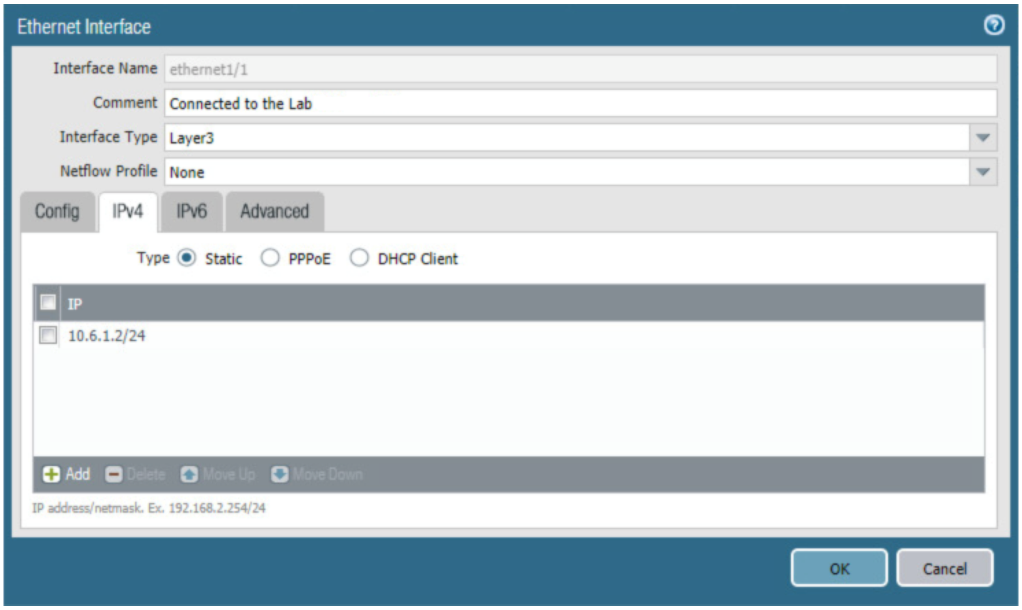
Type: IP Netmask — 10.6.1.2/24

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags:

e. The address should now appear as an item in the IP list box; select **OK;** the Address dialogue will close.

Figure 2-39 Completed WAN Interface Configuration



Interface Name: ethernet1/1

Comment: Connected to the Lab

Interface Type: Layer3

Netflow Profile: None

Type ● Static ○ PPPoE ○ DHCP Client

□	IP
□	10.6.1.2/24

IP address/netmask. Ex. 192.168.2.254/24

4. Select **OK.**

5. Repeat **Steps 2** and **3** for each of the additional Ethernet/Layer3 interfaces.

2.5.3.2 Create Security Zones

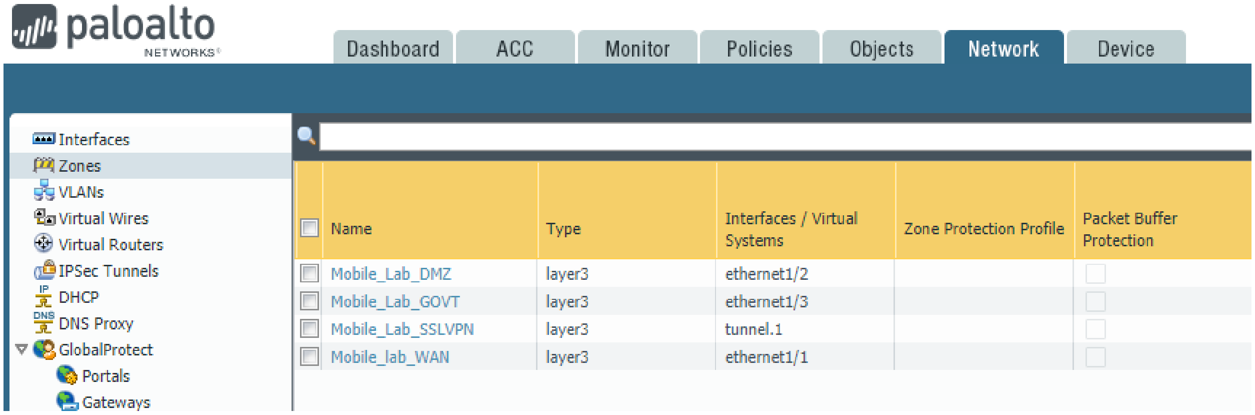
The PA Security Zone is a collection of single or multiple interfaces that have the same security rules. For this setup, four different zones have been configured:

- *Mobile_Lab_GOVT:* inside (trusted) interface connecting to the government (GOVT) segment
- *Mobile_Lab_DMZ*: inside (trusted) interface connecting to the DMZ segment
- *Mobile_Lab_WAN:* outside (untrusted) interface to permit trusted inbound connections (e.g., Lookout cloud service) from the untrusted internet and allow internet access to on-premises devices
- *Mobile_Lab_SSLVPN:* outside (untrusted) interface for VPN connections by trusted mobile devices originating from untrusted networks (e.g., public Wi-Fi)

To configure each zone:

1. Navigate to **Palo Alto Networks Portal > Network > Zones.**

Figure 2-40 Security Zone List

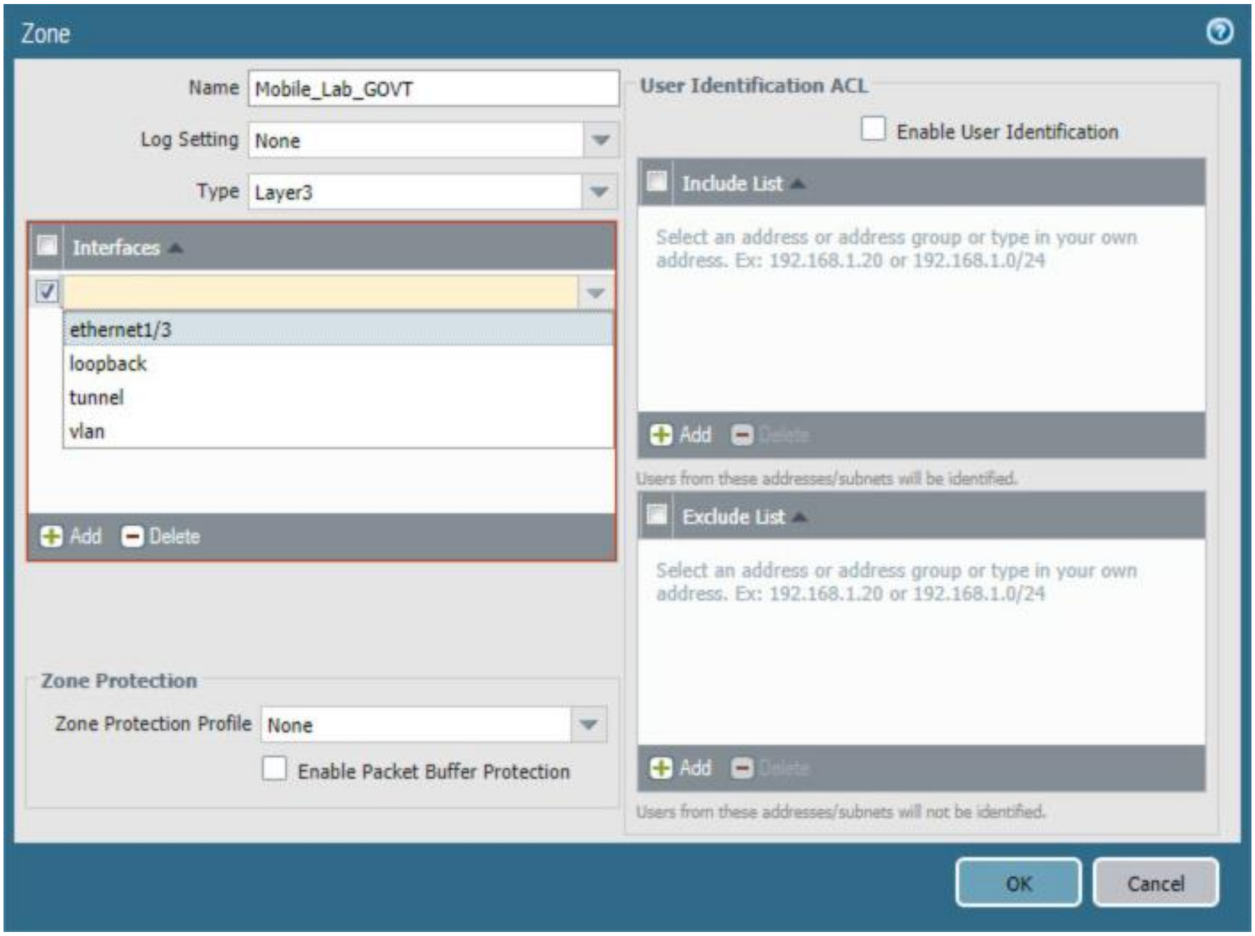


☐	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection
☐	Mobile_Lab_DMZ	layer3	ethernet1/2		☐
☐	Mobile_Lab_GOVT	layer3	ethernet1/3		☐
☐	Mobile_Lab_SSLVPN	layer3	tunnel.1		☐
☐	Mobile_lab_WAN	layer3	ethernet1/1		☐

2. In the **Zones** pane, select **Add;** the Zones page will open.
3. On the **Zones** page:
   a. For the **Name** field, provide a unique name for the zone.
   b. For the **Type** drop-down menu, select **Layer 3.**
   c. Under **Interfaces,** select **Add;** a blank drop-down menu will appear.
   d. In the drop-down menu, select the interface to assign to this zone; this example shows selection of **ethernet 1/3,** which is associated with the LAN interface.

e. Select **OK.**

Figure 2-41 LAN Security Zone Configuration



Zone

Name: Mobile_Lab_GOVT

Log Setting: None

Type: Layer3

☐ Interfaces ▲

☑

ethernet1/3
loopback
tunnel
vlan

Add Delete

Zone Protection

Zone Protection Profile: None

☐ Enable Packet Buffer Protection

User Identification ACL

☐ Enable User Identification

☐ Include List ▲

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will be identified.

☐ Exclude List ▲

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will not be identified.

OK Cancel

f. Repeat **Step b** for each zone.

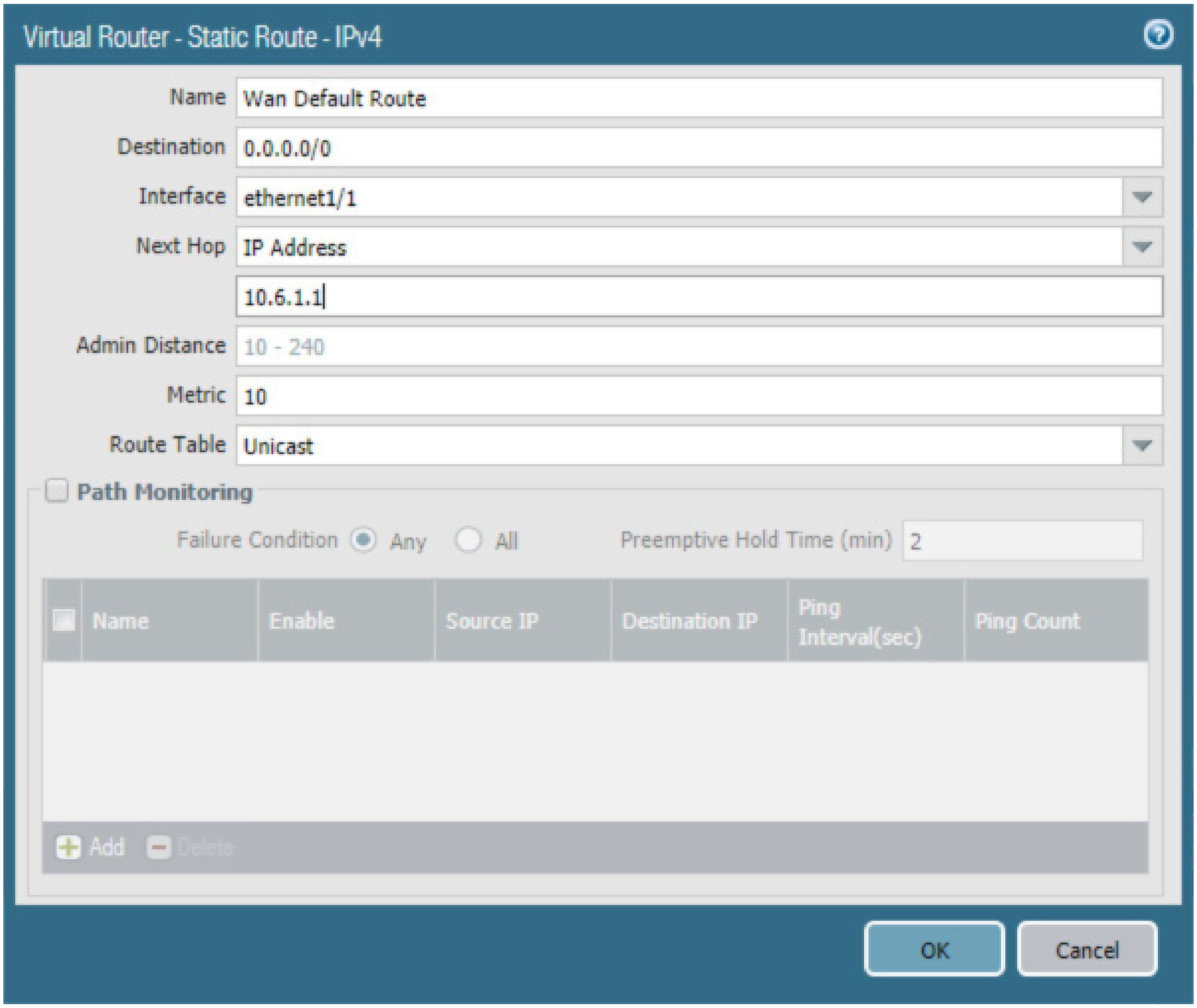
2.5.4 Configure Router

Palo Alto Networks uses a virtual router to emulate physical connectivity between interfaces in different zones. To permit systems to reach systems in other zones, the following steps will create a virtual router and add interfaces to it. The router also sets which of these interfaces will act as the local gateway to the internet.

1. In the **Palo Alto Networks Portal,** navigate to **Network > Virtual Routers.**
2. Below the details pane, select **Add;** the Virtual Router form will open.

3. In the **Virtual Router** form, on the **Router Settings** tab:
    a. For the **Name** field, enter a unique name to identify this router.
    b. On the **Router Settings > General** tab:
        i. Under the **Interfaces** list box, select **Add;** a new list item will appear.
        ii. In the new list item drop-down menu, select an existing interface.
        iii. Repeat **Steps 3a** and **3b** to add all existing interfaces to this router.
4. Select the **Static Routes** tab.
5. On the **Static Routes > IPv4** tab:
    a. Below the list box, select **Add;** the Virtual Router - Static Route - IPv4 form will open.
    b. In the **Virtual Router—Static Route—IPv4** form:
        i. For the **Name** field, enter a unique name to identify this route.
        ii. For the **Destination** field, enter **0.0.0.0/0.**
        iii. For the **Interface** drop-down menu, select the interface that provides access to the internet.
        iv. For the **Next Hop** drop-down menu, select **IP Address.**
        v. In the field below **Next Hop,** enter the IP address of the gateway that provides access to the internet.
        vi. Select **OK.**

701 **Figure 2-42 Virtual Router Configuration**



Virtual Router - Static Route - IPv4

Name	Wan Default Route
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	10.6.1.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

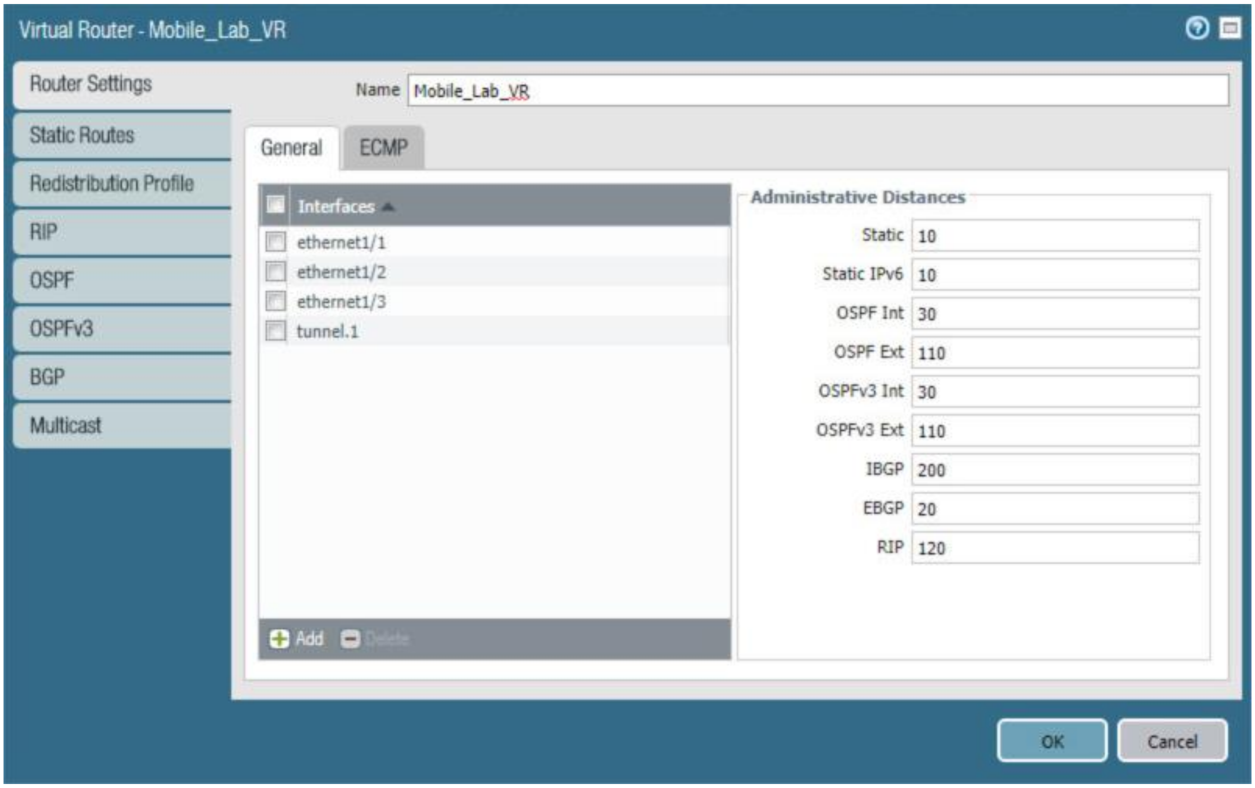
□ Path Monitoring

Failure Condition ● Any ○ All   Preemptive Hold Time (min) 2

□	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

702 6. Select **OK.**

Figure 2-43 Virtual Router General Settings



Virtual Router - Mobile_Lab_VR

Name: Mobile_Lab_VR

Interfaces:
- □ ethernet1/1
- □ ethernet1/2
- □ ethernet1/3
- □ tunnel.1

Administrative Distances

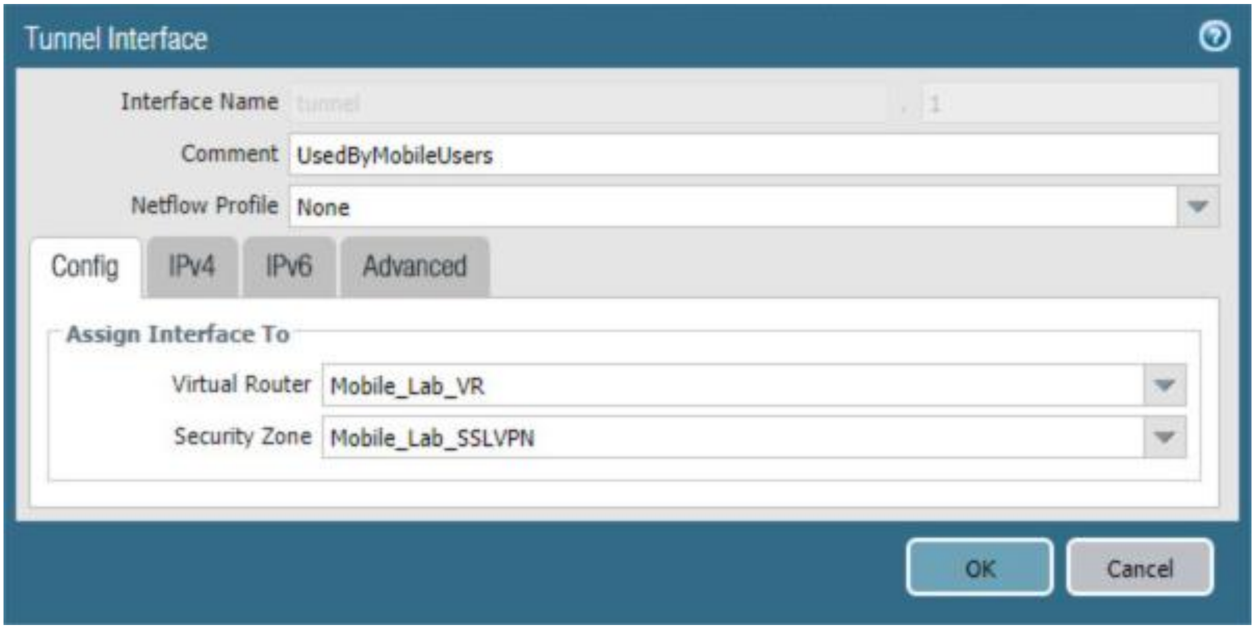
Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

2.5.5 Configure Tunnel Interface

The SSL VPN uses a tunnel interface to secure traffic from the external zone to the internal zone where organizational resources available to mobile users are maintained. To configure the tunnel interface:

1. Navigate to **Palo Alto Networks Portal > Network > Ethernet > Interfaces > Tunnel.**
2. Below the details pane, select **Add;** the Tunnel Interface form will open.
3. In the **Tunnel Interface** form on the **Config** tab:
   a. In the **Assign Interface To** section:
      i. For the **Virtual Router** drop-down menu, select the virtual router created in the previous section.
      ii. For the **Security Zone** drop-down menu, select the security zone created for the SSL VPN.
   b. Select **OK.**

Figure 2-44 SSL VPN Tunnel Interface



Interface Name: tunnel . 1

Comment: UsedByMobileUsers

Netflow Profile: None

Assign Interface To

Virtual Router: Mobile_Lab_VR

Security Zone: Mobile_Lab_SSLVPN

2.5.6 Configure Applications and Security Policies

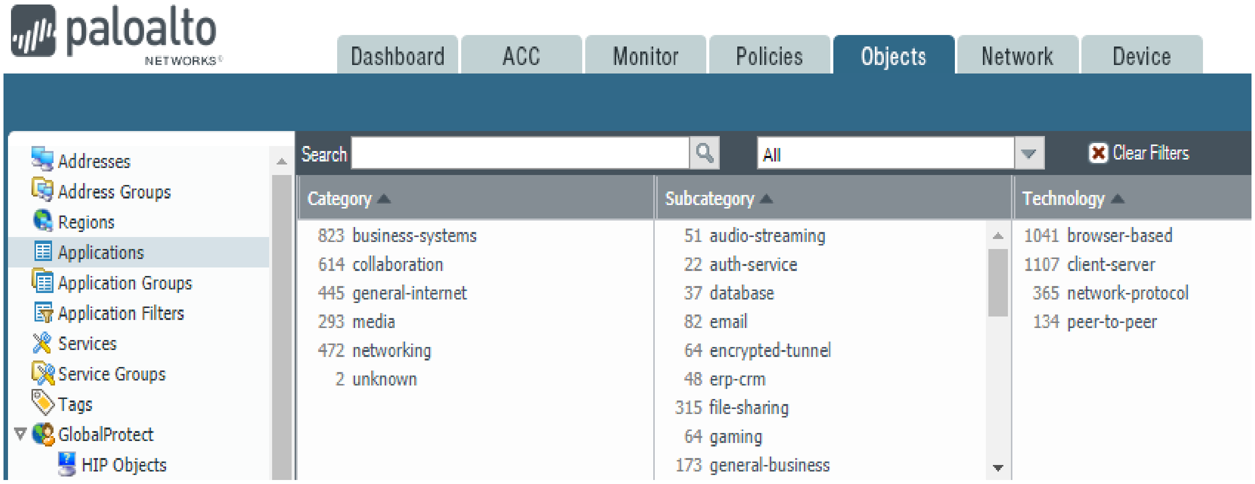
Security policies work similarly to firewall rules; they block or allow traffic between defined zones identified by a source, destination, and application(s) (contextually, Palo Alto Networks' objects define network protocols and ports). Palo Alto Networks has built-in applications for a large number of standard and well-known protocols and ports (e.g., LDAP and Secure Shell), but we defined custom applications for MobileIron-specific traffic.

2.5.6.1 Configure Applications

The following steps will create an application:

1. In the **Palo Alto Networks Portal,** navigate to **Objects > Applications.**

Figure 2-45 Application Categories



Category	Subcategory	Technology
823 business-systems	51 audio-streaming	1041 browser-based
614 collaboration	22 auth-service	1107 client-server
445 general-internet	37 database	365 network-protocol
293 media	82 email	134 peer-to-peer
472 networking	64 encrypted-tunnel	
2 unknown	48 erp-crm	
	315 file-sharing	
	64 gaming	
	173 general-business	

2. On the **Applications** screen:

3. Select **Add;** the Application form will open.

4. On the **Application > Configuration** screen:

   a. In the **General > Name** field, provide a unique name to identify this application.

   b. In the **General > Description** field, enter a meaningful description of its purpose.

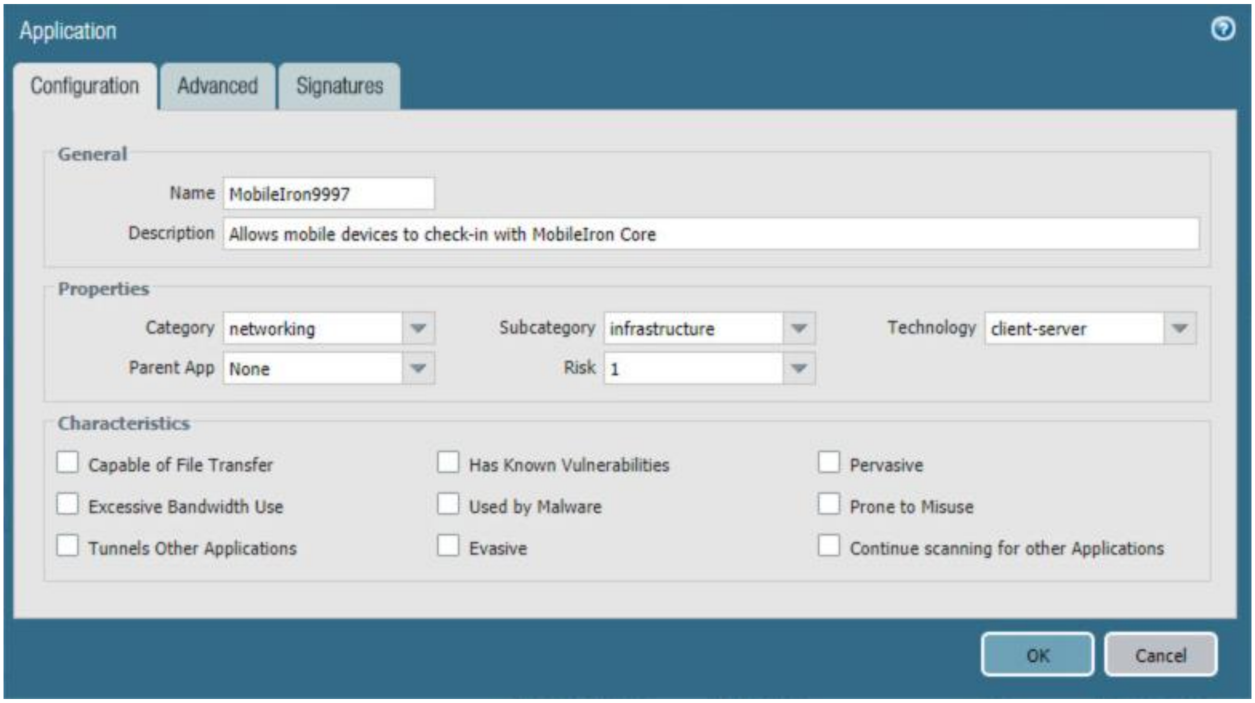
   c. For the **Properties > Category** drop-down menu, select a category appropriate to your environment; our sample implementation uses **networking.**

   d. For the **Properties > Subcategory** drop-down menu, select a subcategory appropriate to your environment; our sample implementation uses **infrastructure.**

   e. For the **Properties > Technology** drop-down menu, select a technology appropriate to your environment; our sample implementation uses **client-server.**

5. Select the **Advanced** tab.

Figure 2-46 MobileIron Core Palo Alto Networks Application Configuration



General

Name: MobileIron9997

Description: Allows mobile devices to check-in with MobileIron Core

Properties

Category: networking

Subcategory: infrastructure

Technology: client-server

Parent App: None

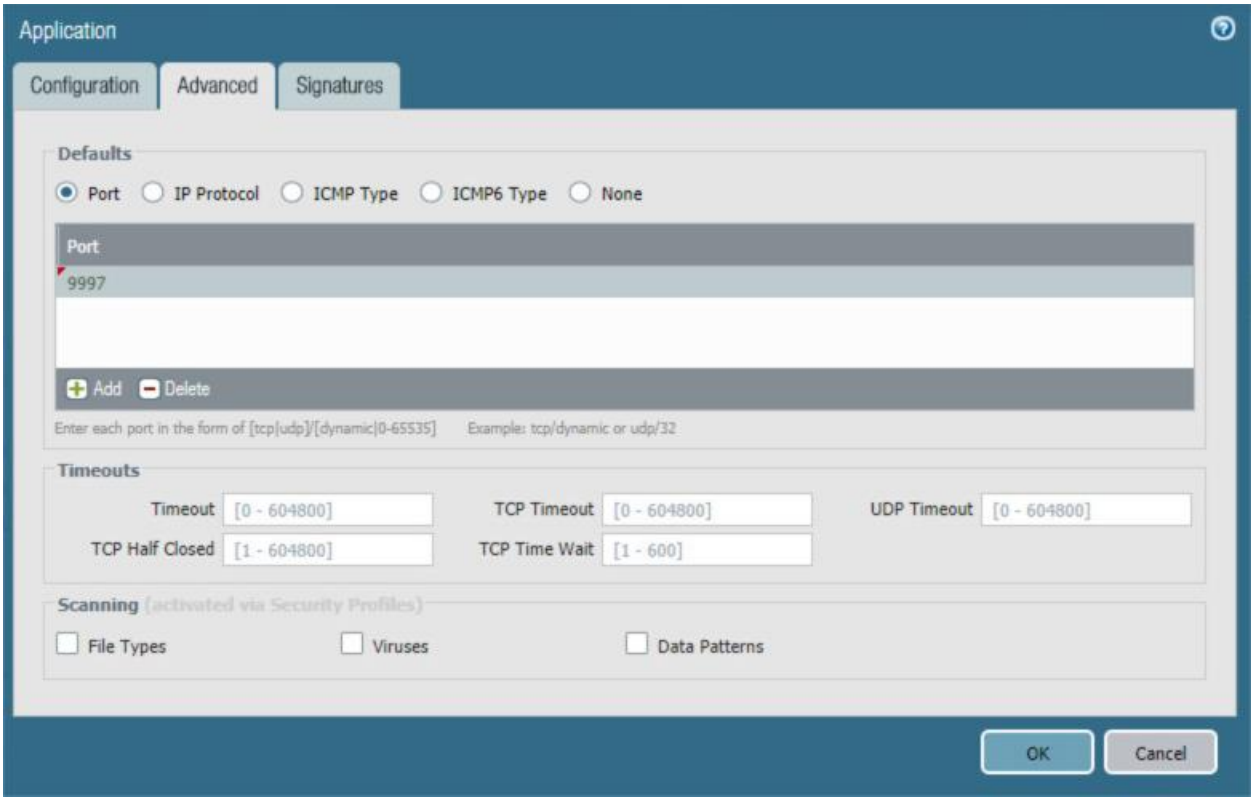
Risk: 1

Characteristics

□ Capable of File Transfer
□ Excessive Bandwidth Use
□ Tunnels Other Applications
□ Has Known Vulnerabilities
□ Used by Malware
□ Evasive
□ Pervasive
□ Prone to Misuse
□ Continue scanning for other Applications

6. On the **Application > Advanced** screen:
   a. Select **Defaults > Port.**
   b. Under the Ports list box, select **Add;** a blank list item will appear.
   c. In the blank list item, enter the port number used by the application; this example uses **9997**.
7. Select **OK.**

Figure 2-47 MobileIron Application Port Configuration



Application

Configuration | Advanced | Signatures

Defaults

● Port ○ IP Protocol ○ ICMP Type ○ ICMP6 Type ○ None

Port
9997

Add Delete

Enter each port in the form of [tcp|udp]/[dynamic|0-65535]   Example: tcp/dynamic or udp/32

Timeouts

Timeout [0 - 604800]   TCP Timeout [0 - 604800]   UDP Timeout [0 - 604800]

TCP Half Closed [1 - 604800]   TCP Time Wait [1 - 600]

Scanning (activated via Security Profiles)

□ File Types □ Viruses □ Data Patterns

8. Repeat **Steps 2** through **7** with the following modifications to create an application for MobileIron Core system administration console:
   a. **Configuration > General > Name is MobileIron8443.**
   b. **Configuration > Default > Category is business-systems.**
   c. **Configuration > Default > Subcategory is management.**
   d. **Advanced > Defaults > Ports > entry_1 is 8443.**

2.5.6.2 Configure Security Policies

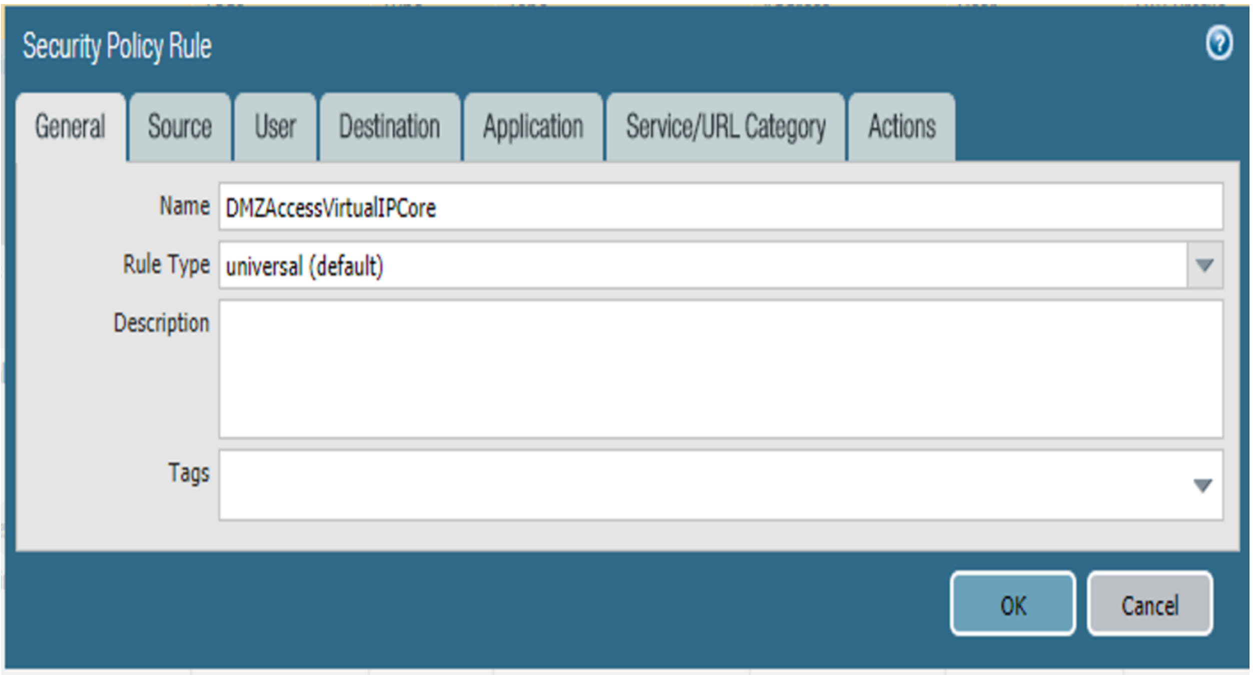
Security policies allow or explicitly deny communication within, between, or (externally) to or from Palo Alto Networks zones. For this sample implementation, several security policies were created to support communication by other components of the architecture. The first subsection covers the steps to create a given security policy. The second subsection provides a table illustrating the security policies we used; these policies would need to be adapted to host names and IP addresses specific to your network infrastructure.

2.5.6.2.1 Create Security Policies

To create a security policy:

1. In the **Palo Alto Networks Portal,** navigate to **Policies > Security.**
2. Select **Add;** the **Security Policy Rule** form will open.
3. In the **Security Policy Rule** form:
    a. In the **Name** field, enter a unique name for this security rule.
    b. For the **Rule Type** drop-down menu, select the scope of the rule.

Figure 2-48 DMZ Access to MobileIron Firewall Rule Configuration



Name: DMZAccessVirtualIPCore

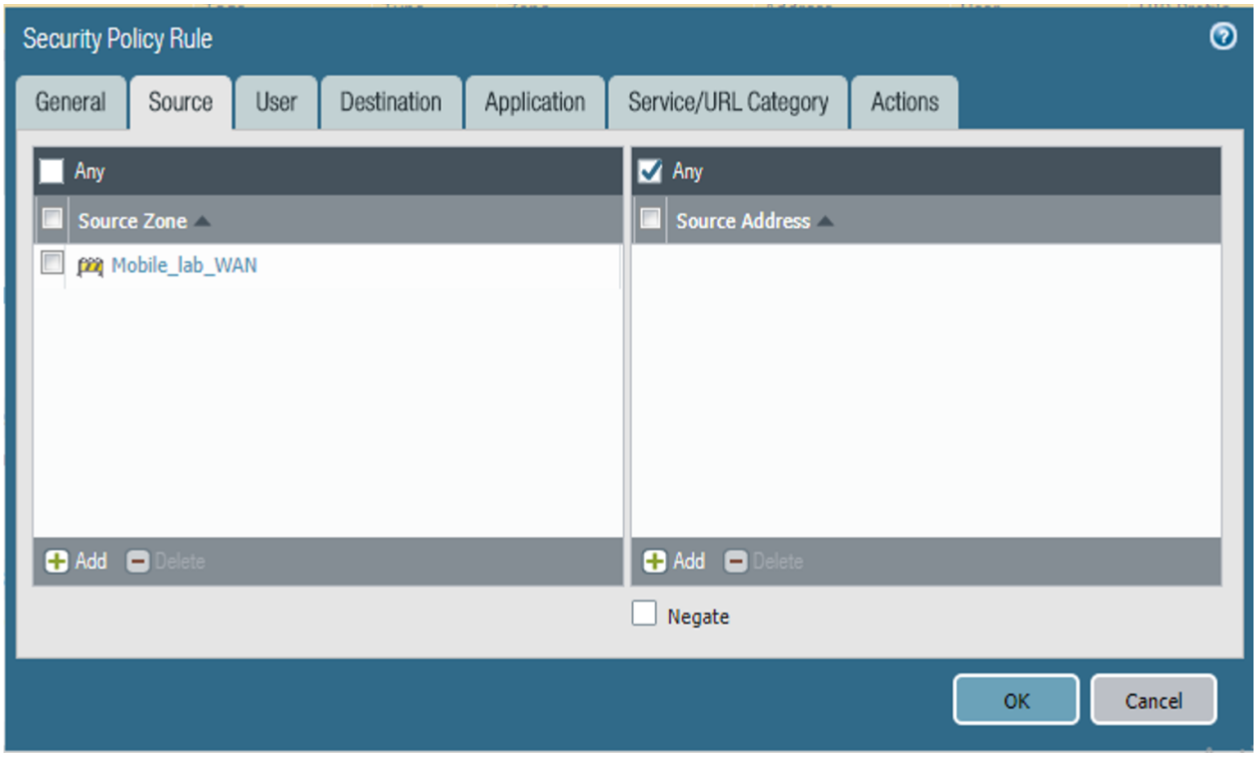
Rule Type: universal (default)

4. Select the **Source** tab.
5. On the **Source** tab:
    a. If the security rule applies to a specific source zone:
        i. Under the **Source Zone** list box, select **Add;** a new entry will appear in the list box.
        ii. For the new list item, select the source zone for this rule.
    b. If the rule applies to only specific source IP addresses:

i. Under the **Source Address** list box, select **Add;** a new list item will appear.

ii. For the new list item, select the source address for this rule.

Figure 2-49 DMZ Access to MobileIron Security Rule Source Zone Configuration



Security Policy Rule

□ Any

□ Source Zone ▲

□ Mobile_lab_WAN

☑ Any

□ Source Address ▲

□ Negate

6. Select the **Destination** tab.

7. On the **Destination** tab:

   a. If the security rule applies to a specific destination zone:

      i. Under the **Destination Zone** list box, select **Add;** a new destination list item will appear.

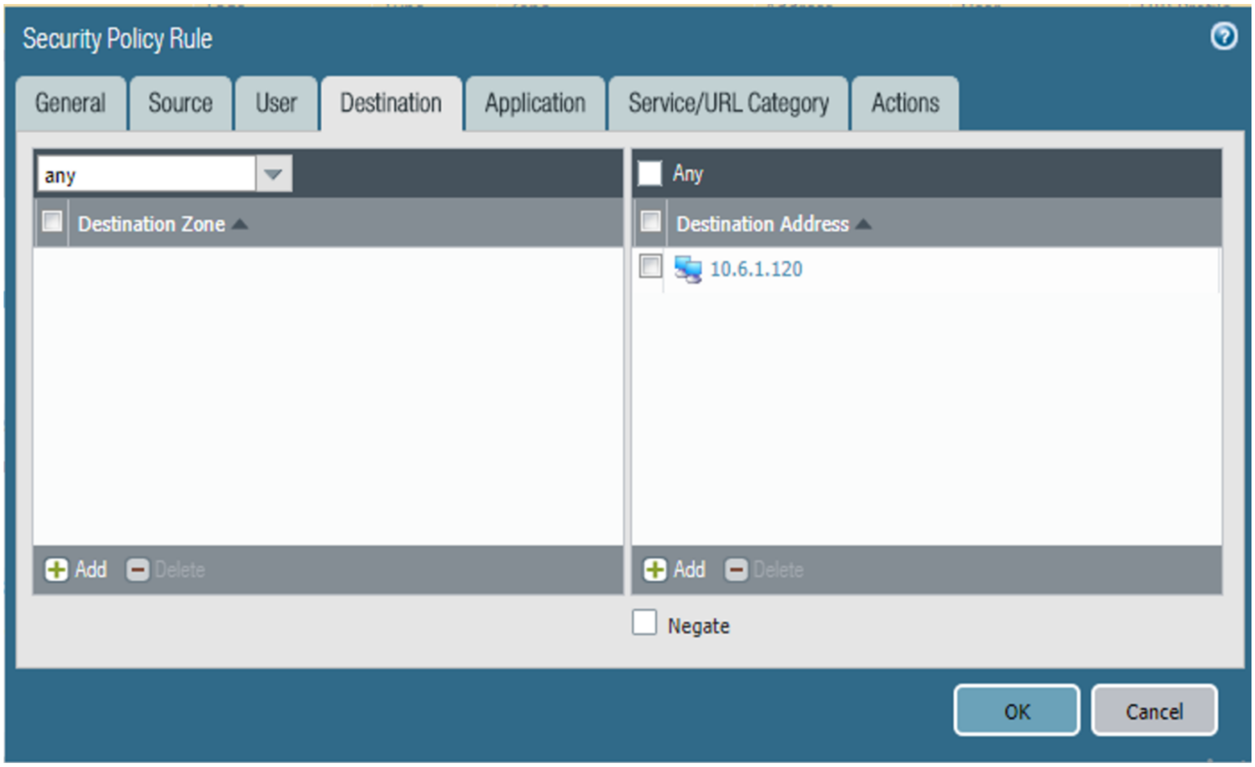
      ii. For the new **Source Zone** list item, select the destination zone for this rule.

   b. If the rule applies to only specific destination IP addresses:

      i. Under the **Destination Address** list box, select **Add;** a new list item will appear.

      ii. For the new list item, select the destination address for this rule.

Figure 2-50 DMZ Access to MobileIron Security Rule Destination Address Configuration



any

□ Destination Zone

□ Any

□ Destination Address

□ 10.6.1.120

□ Negate

8. Select the **Application** tab.

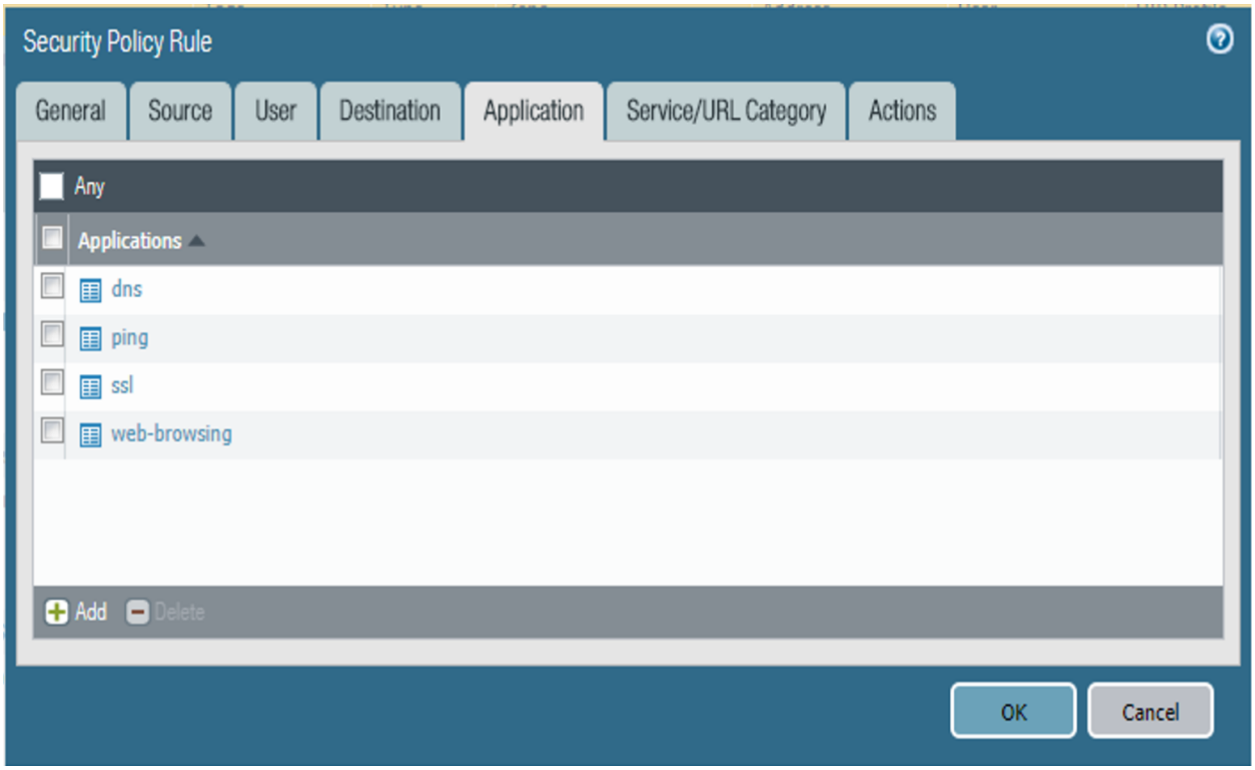
9. On the **Application** tab:

   a. Under the **Applications** list box, select **Add;** a new list item will appear.

   b. For the new **Applications** list item, select the application representing the protocol and port combination of the traffic to control.

   c. Repeat **Steps 9a** and **9b** for each application involving the same source and destination that would also have its traffic allowed or explicitly blocked (if otherwise allowed by a more permissive security rule).

Figure 2-51 DMZ Access to MobileIron Security Rule Application Protocol Configuration

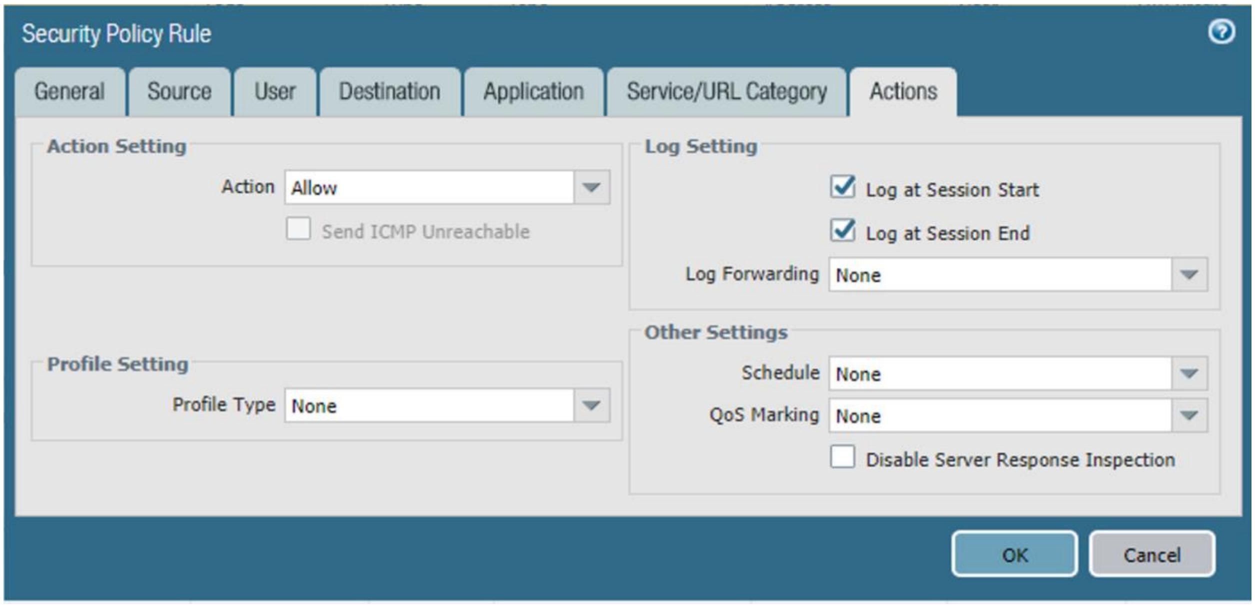


□ Any

□	Applications ▲
□	dns
□	ping
□	ssl
□	web-browsing

10. Select the **Actions** tab.
11. On the **Actions** tab: Unless explicitly blocking traffic permitted by a more permissive security rule, ensure that the **Action Setting > Action** drop-down menu is set to **Allow.**

Figure 2-52 DMZ Access to MobileIron Security Rule Action Configuration



Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

12. Select **OK.**

2.5.6.2.2 Implemented Security Policies

The implemented security policies are provided in Table 2-1, Table 2-2, and Table 2-3. Configuration options that aren't shown were left as their default values.

Table 2-1 Implemented Security Policies

Name	Tags	Type	Source Zone	Source Address
DMZAccessVirtualIPCore	none	universal	Mobile_lab_WAN	any
CoretoAppleSrvs	none	universal	Mobile_Lab_DMZ	MI_Core
AdminAccessToMI	none	interzone	Mobile_Lab_GOVT	MDS.govt.admin
ApphorityConnectorAccessToMI-Core	none	interzone	Mobile_Lab_GOVT	govt.appthority
MICoreObtainDeviceCERT	none	interzone	Mobile_Lab_DMZ	MI_Core
MICoreAccessDNS	none	interzone	Mobile_Lab_DMZ	MI_Core
MICoreRelaySMSNotifications	none	interzone	Mobile_Lab_DMZ	MI_Core
MICoreSyncLDAP	none	interzone	Mobile_Lab_DMZ	MI_Core

807 **Table 2-2 Implemented Security Policies**

Name	Source User	Source Host Information Protocol Profile	Destination Zone	Destination Address
DMZAccessVirtualIPCore	any	any	any	10.6.1.120
CoretoAppleSrvs	any	any	any	17.0.0.0/8
AdminAccessToMI	any	any	Mobile_Lab_DMZ	MI_Core;MI_Sentry
AppthorityConnectorAccessToMI-Core	any	any	Mobile_Lab_DMZ	MI_Core
MICoreObtainDeviceCERT	any	any	Mobile_Lab_GOVT	SCEP_server
MICoreAccessDNS	any	any	Mobile_Lab_GOVT	DNS_Server
MICoreRelaySMSNotifications	any	any	Mobile_Lab_GOVT	SMTP_Relay
MICoreSyncLDAP	any	any	Mobile_Lab_GOVT	LDAP_Server

808 **Table 2-3 Implemented Security Policies**

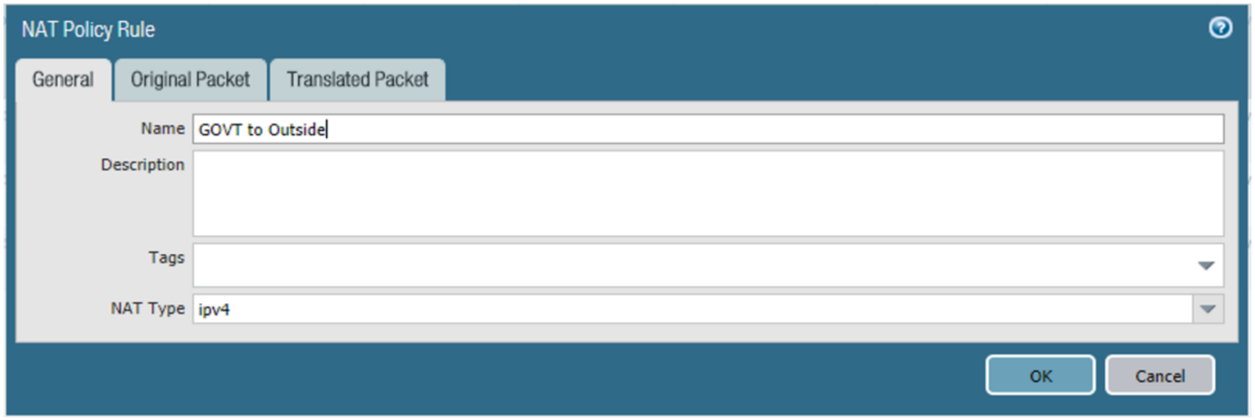
Name	Application	Service	Action	Profile	Options
DMZAccessVirtualIPCore	dns;ping;ssl;web-browsing	any	allow	none	none
CoretoAppleSrvs	any	any	allow	none	none
AdminAccessToMI	AdminAccessMI;ssh;ssl	any	allow	none	none
AppthorityConnectorAccessToMI-Core	AdminAccessMI;ssl;web-browsing	any	allow	none	none
MICoreObtainDeviceCERT	scep;web-browsing	application-default	allow	none	none
MICoreAccessDNS	dns	application-default	allow	none	none
MICoreRelaySMSNotifications	smtp	application-default	allow	none	none
MICoreSyncLDAP	ldap	application-default	allow	none	none

809 2.5.7 Network Address Translation (NAT)

810 To allow communication with external networks over the internet, the appliance also needs to be
811 configured with NAT rules. To configure NAT:

1. In the **Palo Alto Networks Portal,** navigate to **Policies > NAT.**
2. Below the details pane, select **Add;** the **NAT Policy Rule** form will open.
3. In the **NAT Policy Rule** form, on the **General** tab:
   a. In the **Name** field, provide a unique name for this NAT policy rule.
   b. Ensure the **NAT Type** drop-down menu is set to **ipv4.**

Figure 2-53 Outbound NAT Rule



Name: GOVT to Outside

NAT Type: ipv4

4. Select the **Original Packet** tab.
5. On the **Original Packet** tab:
   a. Under the **Source Zone** list box, select **Add;** a new Source Zone list item will appear.
   b. For the new **Source Zone** list item, select the zone that represents your LAN subnet; in this sample implementation, that is **Mobile_Lab_GOVT.**
   c. Repeat **Steps 5a** and **5b** to add the zone that represents your DMZ; in this sample implementation, that is **Mobile_Lab_DMZ.**
   d. Repeat **Steps 5a** and **5b** to add the zone that represents your SSL VPN; in this sample implementation, that is **Mobile_Lab_SSLVPN.**
   e. For the **Destination Zone** drop-down menu, select the zone that represents the internet; in this sample implementation, that is **Mobile_lab_WAN.**
   f. For the **Destination Interface,** select the adapter that is physically connected to the same subnet as your internet gateway; in this sample implementation, that is **ethernet1/1.**

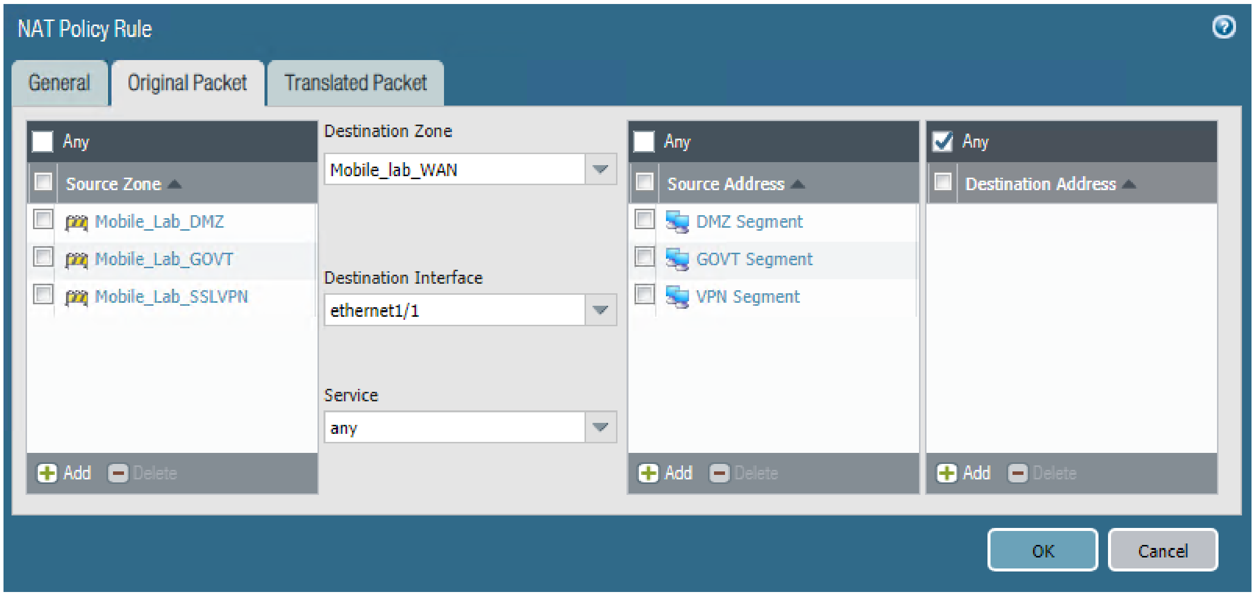
g. Under the **Source Address** list box, select **Add;** a new Source Address list item will appear.

h. For the new **Source Address** list item, select the address that represents the subnet (IP address range) for the LAN.

i. Repeat **Steps 5f** and **5g** to add the address representing the DMZ subnet.

j. Repeat **Steps 5f** and **5g** to add the address representing the SSL VPN subnet.

Figure 2-54 Outbound NAT Original Packet Configuration



□ Any

□ Source Zone ▲
- □ Mobile_Lab_DMZ
- □ Mobile_Lab_GOVT
- □ Mobile_Lab_SSLVPN

Destination Zone: Mobile_lab_WAN

Destination Interface: ethernet1/1

Service: any

□ Any

□ Source Address ▲
- □ DMZ Segment
- □ GOVT Segment
- □ VPN Segment

☑ Any

□ Destination Address ▲

6. Select the **Translated Packet** tab.

7. On the **Translated Packet** tab, under **Source Address Translation:**

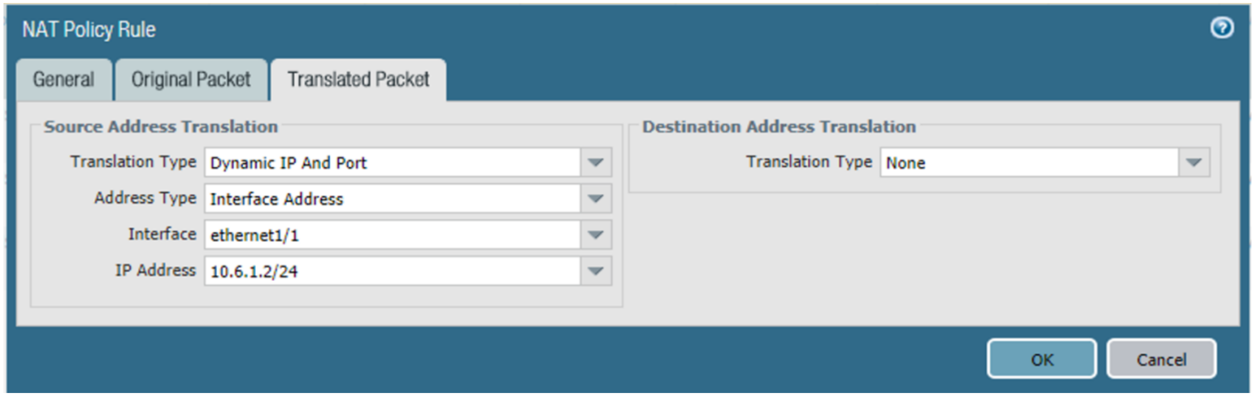
   a. For the **Translation Type** drop-down menu, select **Dynamic IP and Port.**

   b. For the **Address Type** drop-down menu, select **Interface Address.**

   c. For the **Interface** drop-down menu, select the same interface selected in **Step 5e.**

   d. For the **IP Address** drop-down menu, select the IPv4 address on the same subnet as your internet gateway.

Figure 2-55 Outbound NAT Translated Packet Configuration



Source Address Translation

Translation Type: Dynamic IP And Port
Address Type: Interface Address
Interface: ethernet1/1
IP Address: 10.6.1.2/24

Destination Address Translation

Translation Type: None

8. Select **OK.**

2.5.8 Configure SSL VPN

The SSL VPN enables remote mobile device users to create an encrypted connection to the enterprise from unencrypted networks (e.g., public Wi-Fi hot spots).

2.5.8.1 Configure End-User Authentication

The following steps establish the integrations and configurations related to mobile user identification and authentication.

2.5.8.1.1 Configured Server Profile

The following steps integrate this appliance with Microsoft Active Directory Domain Services to manage mobile user permissions via AD groups and roles.

1. In the **Palo Alto Networks Portal,** navigate to **Devices > Server Profiles > LDAP.**
2. Below the details pane, select **Add;** the **LDAP Server Profile** form will open.
3. In the **LDAP Server Profile** form:
    a. In the **Profile Name** field, enter a unique name to identify this profile.
    b. Under the **Service List** box, select **Add;** a new **Server List** item will appear.
    c. In the new **Service List** item:
        i. In the **Name** column, enter a name to identify the server.
        ii. In the **LDAP Server** column, enter the IP address of the LDAP server.

iii. The value in the **Port** column defaults to 389; change this if your LDAP server communicates over a different port number.

iv. Repeat **Steps 3ci** through **3ciii** for each LDAP server that you intend to use.

d. Under **Server Settings**:

i. In the **Type** drop-down menu, select **active-directory.**

ii. In the **Base DN** drop-down menu, select the DN for your Active Directory domain users who will use the SSL VPN.

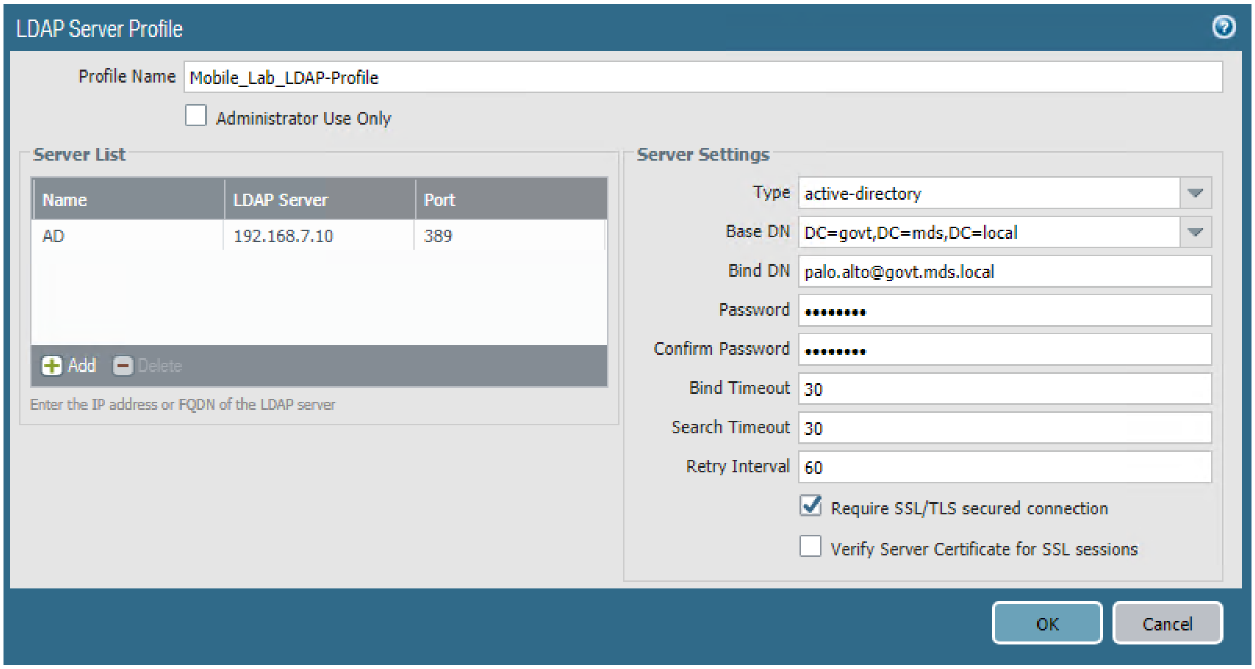
iii. In the **Bind DN** field, enter the Active Directory domain user account that will authenticate to LDAP to perform queries.

iv. In the **Password** field, enter the password for the Active Directory user account specified in the previous step.

v. In the **Confirm Password** field, reenter the password entered in the previous step.

4. Select **OK.**

Figure 2-56 LDAP Profile



LDAP Server Profile

Profile Name: Mobile_Lab_LDAP-Profile

□ Administrator Use Only

Server List

Name	LDAP Server	Port
AD	192.168.7.10	389

Enter the IP address or FQDN of the LDAP server

Server Settings

Type	active-directory
Base DN	DC=govt,DC=mds,DC=local
Bind DN	palo.alto@govt.mds.local
Password	••••••••
Confirm Password	••••••••
Bind Timeout	30
Search Timeout	30
Retry Interval	60

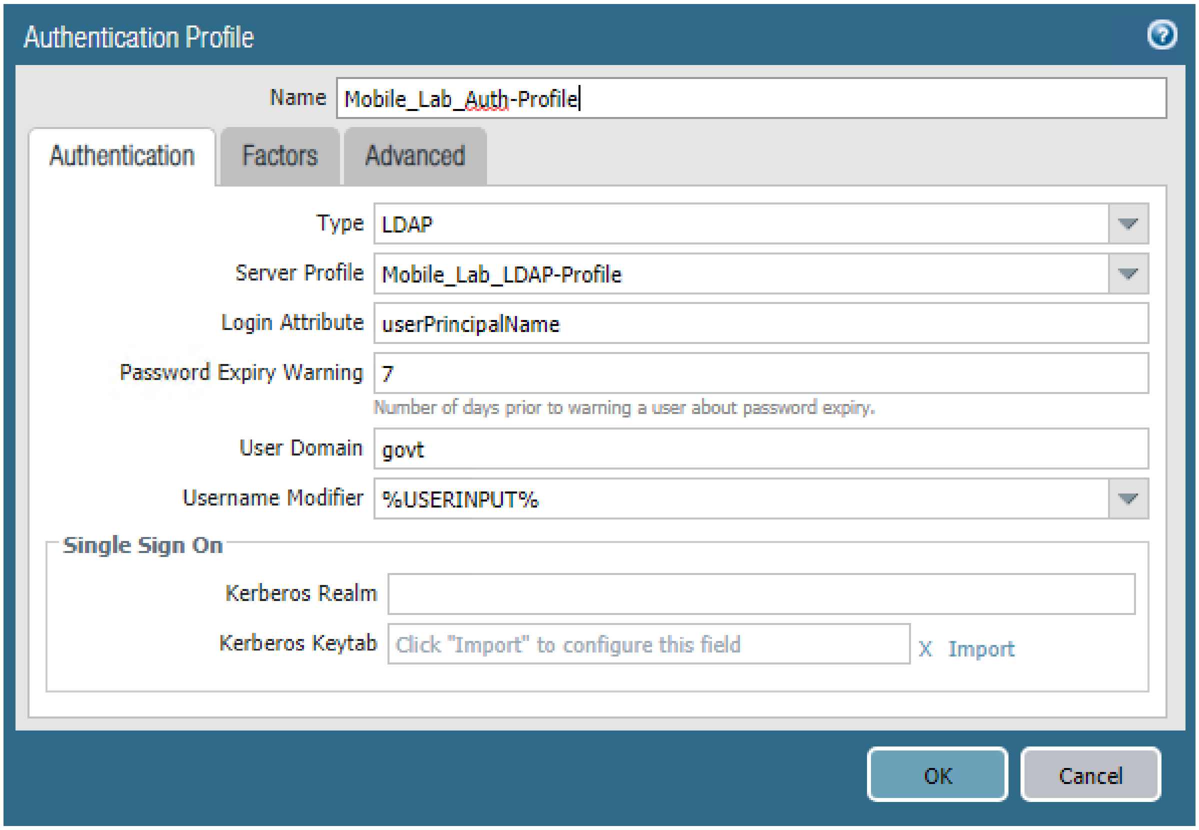
☑ Require SSL/TLS secured connection

□ Verify Server Certificate for SSL sessions

2.5.8.2 Configure Authentication Profile

1. In the **Palo Alto Networks Portal,** navigate to **Device > Authentication Profile.**
2. Under the details pane, select **Add;** the **Authentication Profile** form will open.
3. In the **Authentication Profile** form:
    a. In the **Name** field, provide a unique name to identify this authentication profile.
    b. On the **Authentication** tab:
        i. For the **Type** drop-down menu, select **LDAP.**
        ii. For the **Server Profile** drop-down menu, select the name of the LDAP Server Profile created in the previous section.
        iii. For the **Login Attribute** field, enter **userPrincipalName.**
        iv. For the **User Domain,** enter the name of your enterprise domain; our sample implementation uses **govt.**

Figure 2-57 Authentication Profile



Authentication Profile

Name: Mobile_Lab_Auth-Profile

Type: LDAP

Server Profile: Mobile_Lab_LDAP-Profile

Login Attribute: userPrincipalName

Password Expiry Warning: 7

Number of days prior to warning a user about password expiry.

User Domain: govt

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field

c. Select the **Advanced** tab.

d. On the **Advanced** tab:

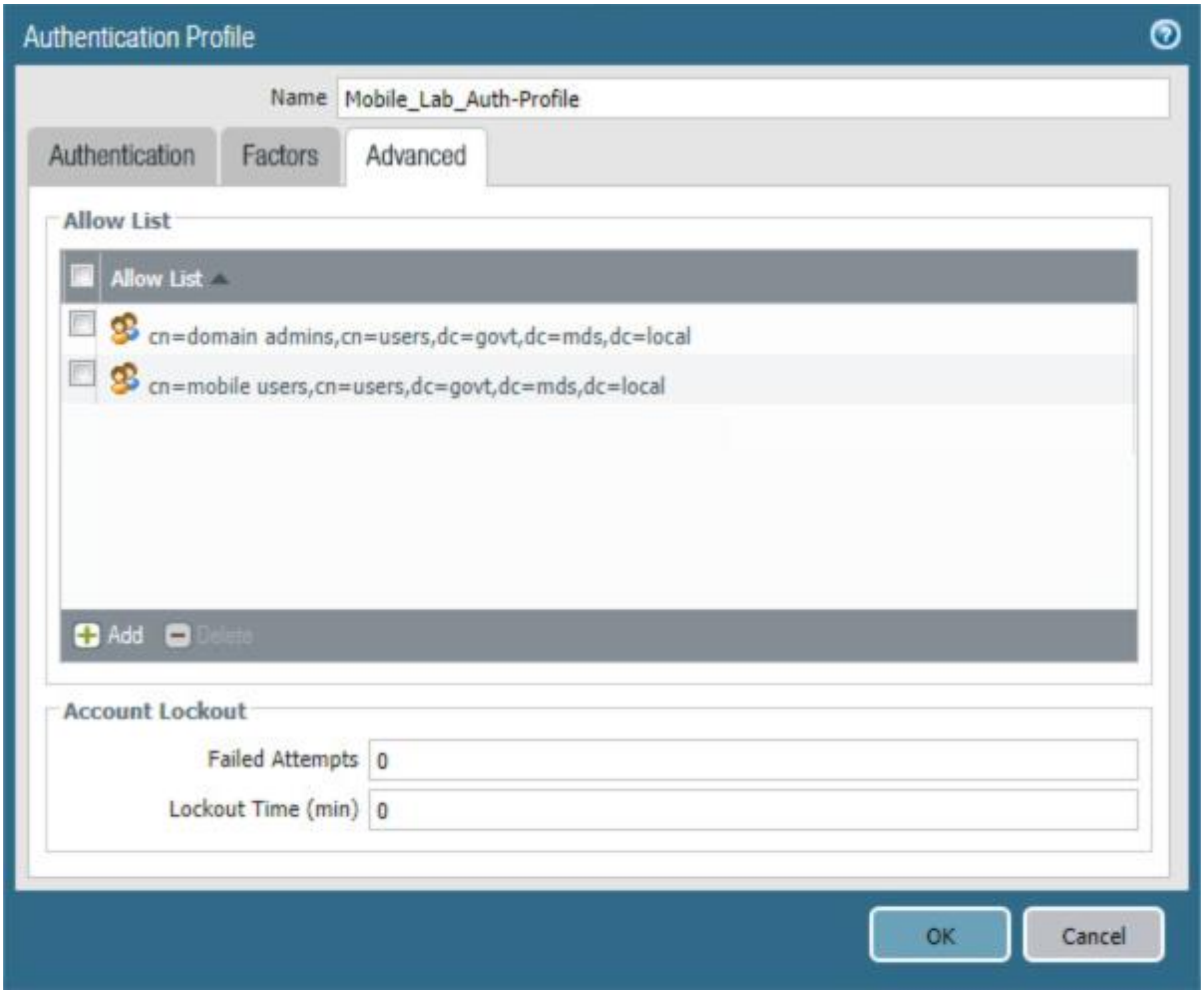
   i. Under the **Allow List** box, select **Add;** this will create a new list item.

   ii. In the new list item, select the Active Directory group for your mobile users.

   iii. Repeat **Steps 3di** and **3dii** for any additional groups that should authenticate to the SSL VPN.

e. Select **OK.**

Figure 2-58 Advanced Authentication Profile Settings



Authentication Profile

Name: Mobile_Lab_Auth-Profile

Allow List

Allow List
cn=domain admins,cn=users,dc=govt,dc=mds,dc=local
cn=mobile users,cn=users,dc=govt,dc=mds,dc=local

Account Lockout

Failed Attempts: 0

Lockout Time (min): 0

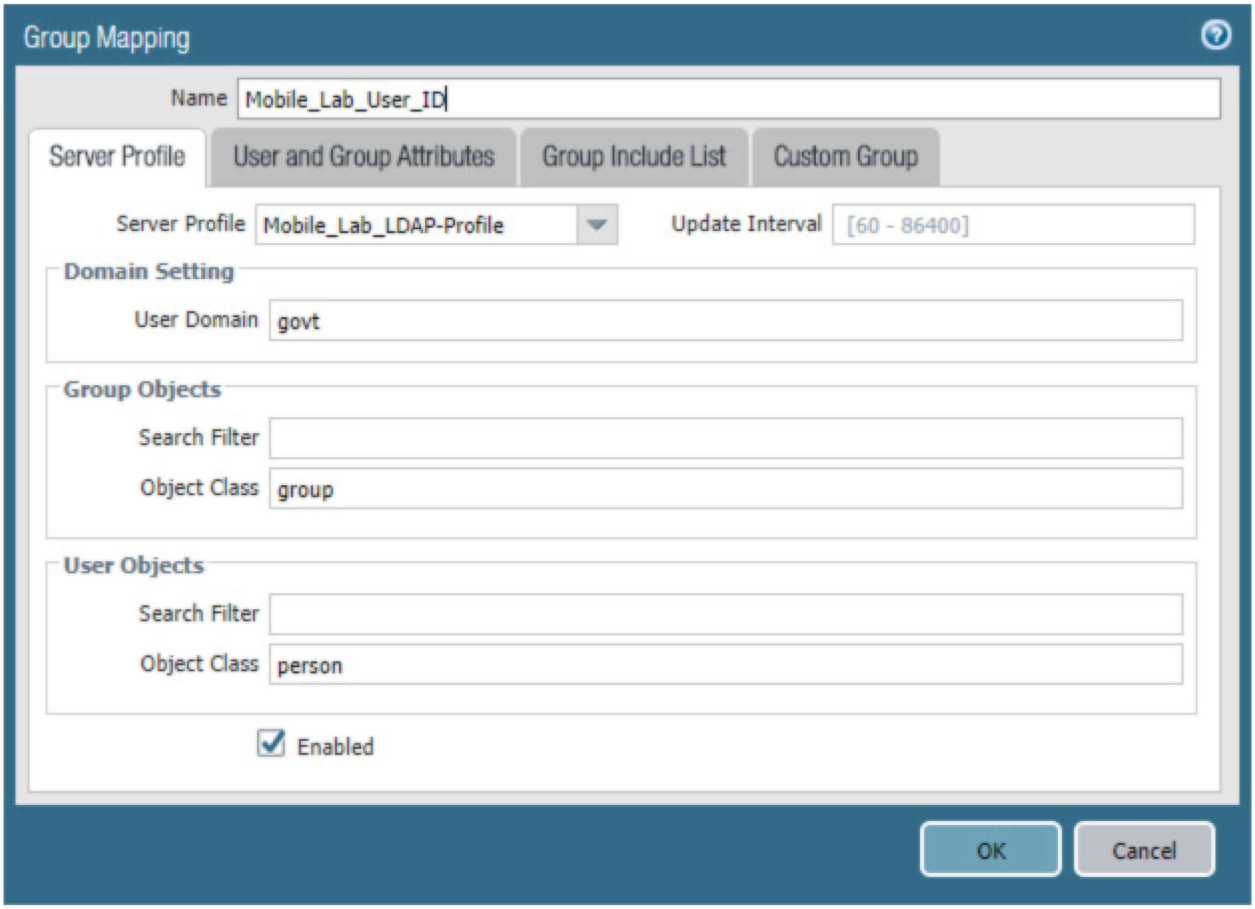
2.5.8.3 Configure User Identification

1. In the **Palo Alto Networks Portal,** navigate to **Device & User Identification.**
2. In the details pane, select the **Group Mapping Settings** tab.
3. Below the details pane, select **Add** the **Group Mapping** form will open.
4. In the **Group Mapping** form:
    a. In the **Name** field, enter a unique name to identify this group mapping.
    b. In the **Server Profile** tab:

i. For the **Server Profile** drop-down menu, select the LDAP Server Profile created previously.

ii. For **Domain Setting > User Domain,** enter the name of your Active Directory domain; this sample implementation uses **govt.**

Figure 2-59 LDAP Group Mapping



Group Mapping

Name: Mobile_Lab_User_ID

Server Profile: Mobile_Lab_LDAP-Profile

Update Interval: [60 - 86400]

Domain Setting

User Domain: govt

Group Objects

Search Filter:

Object Class: group

User Objects

Search Filter:

Object Class: person

☑ Enabled

c. Select the **Group Includes List** tab.

d. On the **Group Includes List** tab:

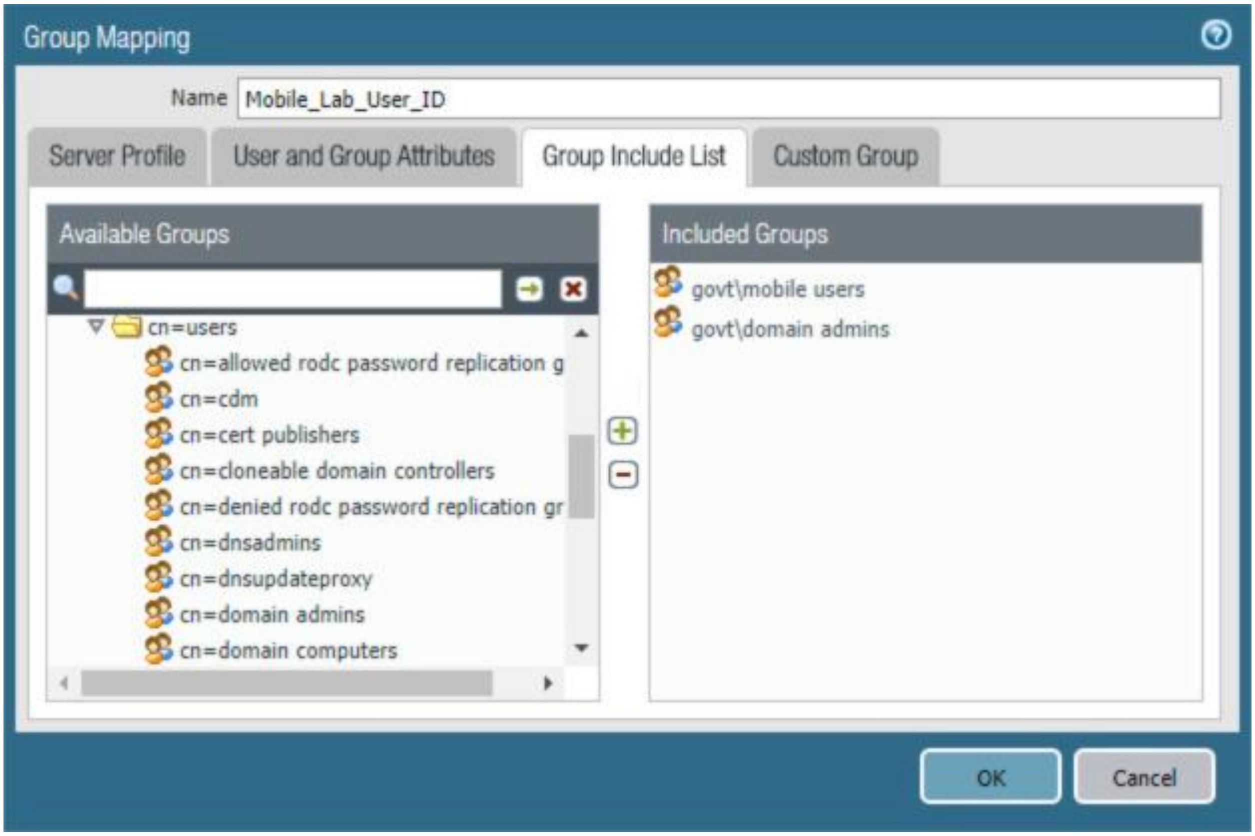
i. In the **Available Groups** list box, expand the Active Directory domain to reveal configured user groups.

ii. For each Active Directory group to be included in this User Identification configuration:

1) Select the **Active Directory** group.

2) Select the **plus icon** to transfer the group to the **Included Groups** list box.

Figure 2-60 LDAP Group Include List



Name: Mobile_Lab_User_ID

Available Groups:

- cn=users
  - cn=allowed rodc password replication g
  - cn=cdm
  - cn=cert publishers
  - cn=cloneable domain controllers
  - cn=denied rodc password replication gr
  - cn=dnsadmins
  - cn=dnsupdateproxy
  - cn=domain admins
  - cn=domain computers

Included Groups:

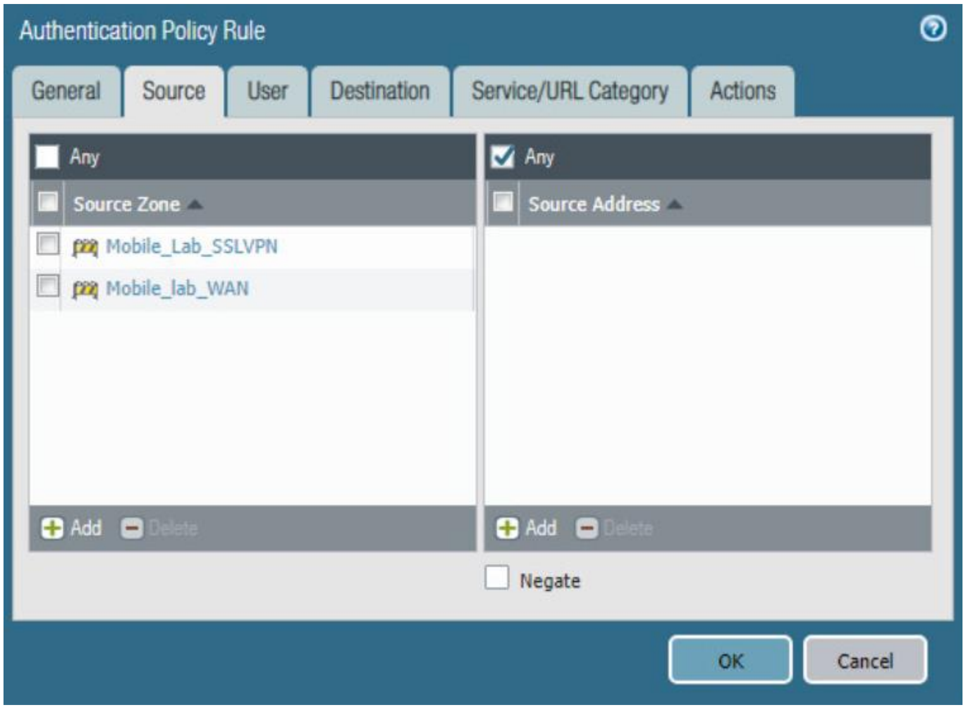
- govt\mobile users
- govt\domain admins

5. Select **OK.**

2.5.8.4 Configure Authentication Policy Rule

1. Navigate to **Policies** > **Authentication.**
2. Click **Add.**
3. Give the policy a name. In this implementation, **Mobile_Lab_Auth_Rule** was used.
4. Click **Source.**
5. Under Source Zone, click **Add.** Select the **SSL VPN** zone.
6. Under Source Zone, click **Add.** Select the **WAN** zone.

Figure 2-61 Authentication Policy Source Zones



☐ Any

☐	Source Zone ▲
☐	Mobile_Lab_SSLVPN
☐	Mobile_lab_WAN

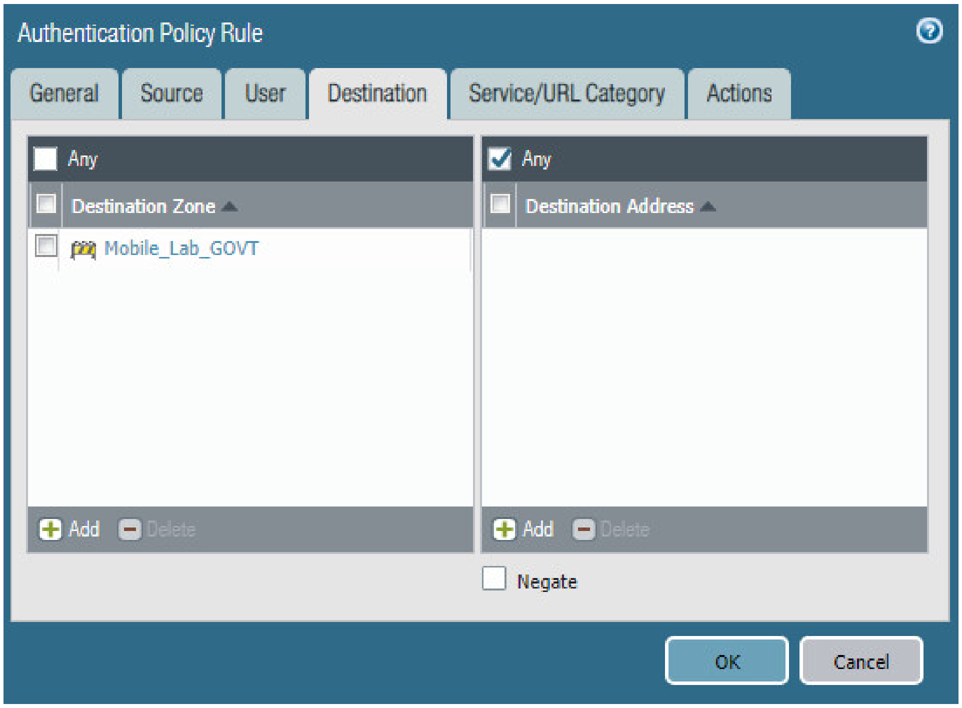
☑ Any

☐	Source Address ▲

☐ Negate

7. Click **Destination.**
8. Under Destination Zone, click **Add.**
9. Select the **LAN** zone.

Figure 2-62 Authentication Policy Destination Zones



Authentication Policy Rule

General | Source | User | Destination | Service/URL Category | Actions

□ Any

Destination Zone

□ Mobile_Lab_GOVT

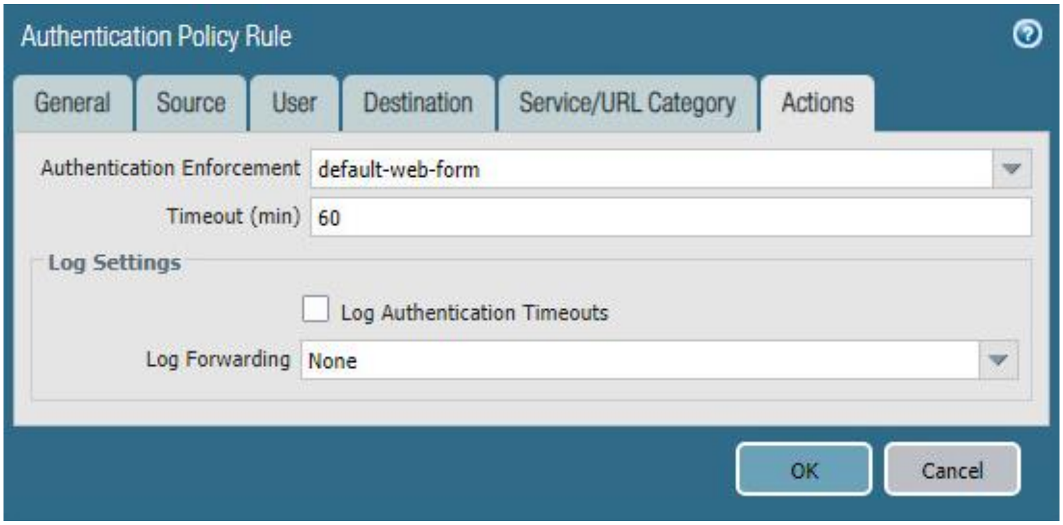
☑ Any

Destination Address

□ Negate

10. Click **Service/URL Category.**
11. Under service, click **Add.**
12. Select **service-http.**
13. Under service, click **Add.**
14. Select **service-https.**
15. Click **Actions.**
16. Next to Authentication Enforcement, select **default-web-form.**
17. Leave Timeout and Log Settings as their default values.

Figure 2-63 Authentication Profile Actions



Authentication Enforcement: default-web-form

Timeout (min): 60

□ Log Authentication Timeouts

Log Forwarding: None

18. Click **OK** and commit the changes.

2.5.9 Import Certificates

Certificates need to be imported into the appliance to configure certificate profiles that will affect how they are used in supporting communication with other systems. In particular, device certificates issued to mobile devices will be used to identify and authenticate mobile users.

Note: The certificate private keys must be password-protected to import them into the firewall.

1. In the **Palo Alto Networks Portal,** navigate to **Device > Certificate Management > Certificates.**
2. Under the details pane, select **Import;** the **Import Certificate** form will open.
3. In the **Import Certificate** form:
   a. For the **Certificate Type,** select **Local.**
   b. For the **Certificate Name** field, enter a unique name to identify this certificate.
   c. Next to the **Certificate File** field, Select **Browse...** to specify the full path to the file containing the certificate.
   d. For the **File Format** drop-down menu, select the certificate encoding appropriate to the certificate file; this example assumes the certificate and private key are in separate files, and select **PEM.** Note: The certificate’s private key must be password-protected to import it into Palo Alto Networks appliances.

   e. If the certificate identifies the Palo Alto Networks appliance:

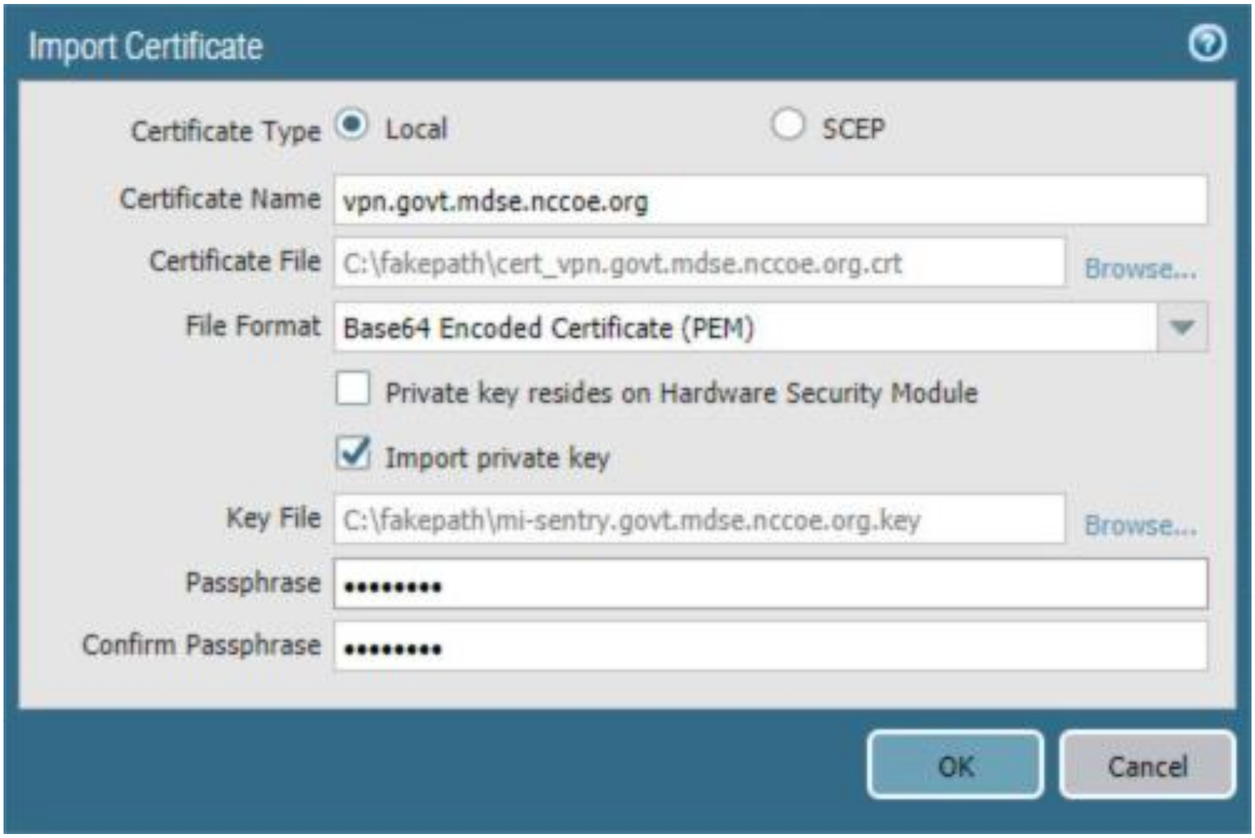
      i. Enable the **Import private key** checkbox.

      ii. Next to **Key File,** select **Browse...** to specify the full path to the file containing the private key for the uploaded certificate.

      iii. For the **Passphrase** field, enter the pass phrase protecting the private key.

      iv. For the **Confirm Passphrase** field, re-enter the pass phrase protecting the private key.

Figure 2-64 Import MobileIron Certificate



Certificate Type ● Local ○ SCEP

Certificate Name vpn.govt.mdse.nccoe.org

Certificate File C:\fakepath\cert_vpn.govt.mdse.nccoe.org.crt

File Format Base64 Encoded Certificate (PEM)

□ Private key resides on Hardware Security Module

☑ Import private key

Key File C:\fakepath\mi-sentry.govt.mdse.nccoe.org.key

Passphrase •••••••••

Confirm Passphrase •••••••••

   f. Select **OK.**

4. Repeat **Step 3** for each certificate to import into the Palo Alto Networks appliance. This will include all certificates that the appliance will use to identify itself or authenticate to remote systems, all certificates in the chain of trust for each such certificate, and any chain-of-trust certificates supporting identity verification for remote systems to which this appliance will

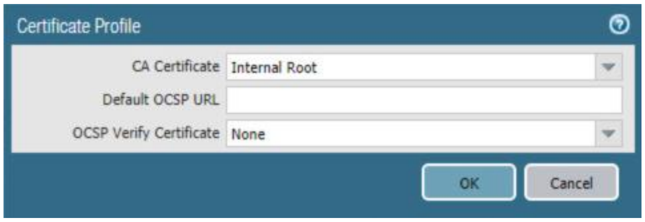
require certificate-based identification and authentication. This sample implementation uses certificates for the following systems:

- server certificate for this appliance issued by DigiCert
- DigiCert root CA certificate
- DigiCert subordinate CA certificate
- Microsoft CA enterprise root certificate
- Microsoft CA enterprise subordinate CA certificate

2.5.10 Configure Certificate Profile

1. In the **Palo Alto Networks Portal,** navigate to **Device > Certificate Management > Certificate Profile.**
2. Under the details pane, select **Add;** the **Certificate Profile** form will open.
3. In the **Certificate Profile** form:
    a. In the **Name** field, enter a unique name to identify this certificate profile.
    b. In the **Username Field** drop-down menu, select **Subject Alt.**
    c. Select the **Principal Name** option.
    d. In the **User Domain** field, enter the Active Directory domain name for your enterprise; this sample implementation uses **govt.**
    e. Under the **CA Certificate** list box, select **Add;** a secondary Certificate Profile form will appear.
    f. In the secondary **Certificate Profile** form, in the **CA Certificate** drop-down menu, select the Microsoft Active Directory Certificate Services root certificate uploaded in **Section 2.5.6.**
    g. Select **OK.**
    h. Repeat **Step 3f** for each intermediary certificate in the trust chain between the root certificate and the subordinate CA certificate that issues certificates to mobile devices.
    i. Select **OK.**

Figure 2-65 Internal Root Certificate Profile



Certificate Profile

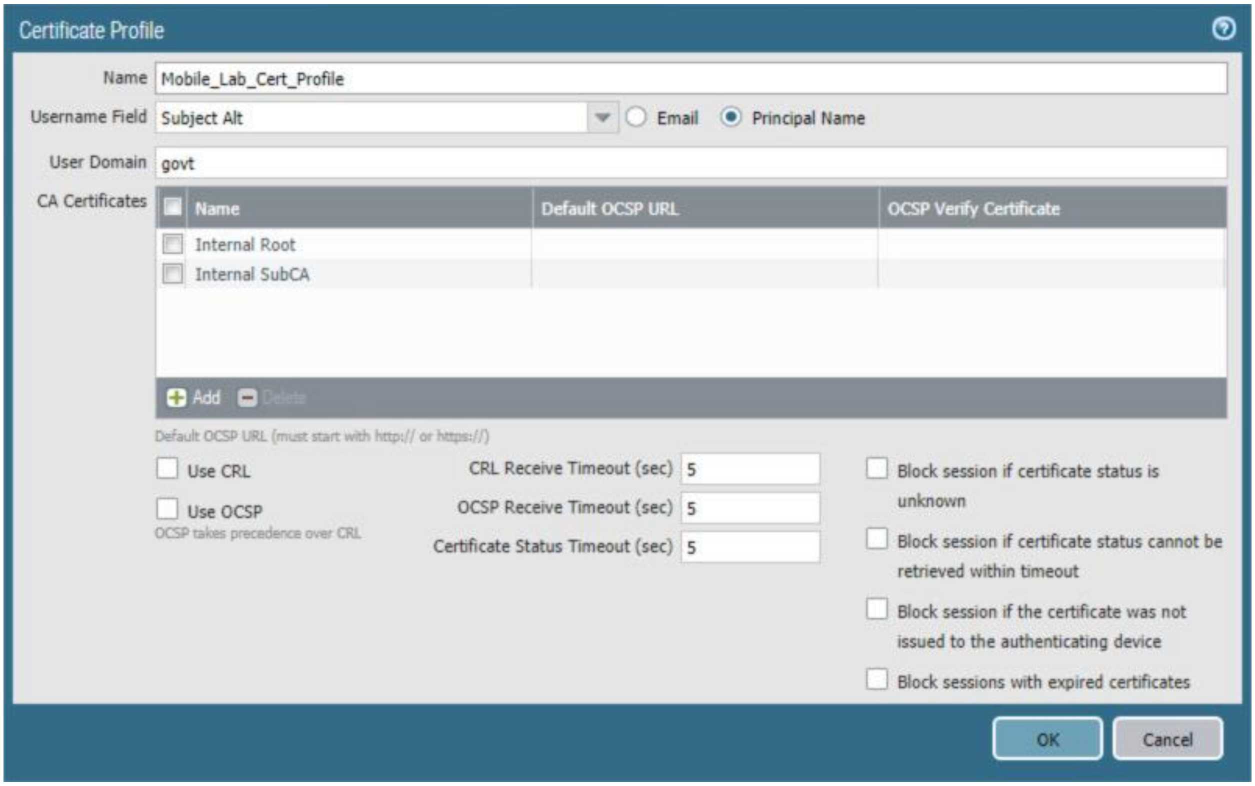
CA Certificate: Internal Root

Default OCSP URL:

OCSP Verify Certificate: None

4. Select **OK.**

Figure 2-66 Certificate Profile



Certificate Profile

Name: Mobile_Lab_Cert_Profile

Username Field: Subject Alt ○ Email ● Principal Name

User Domain: govt

CA Certificates

☐ Name	Default OCSP URL	OCSP Verify Certificate
☐ Internal Root		
☐ Internal SubCA		

Default OCSP URL (must start with http:// or https://)

☐ Use CRL

☐ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

☐ Block session if certificate status is unknown

☐ Block session if certificate status cannot be retrieved within timeout

☐ Block session if the certificate was not issued to the authenticating device

☐ Block sessions with expired certificates

2.5.11 Configure SSL/TLS Service Profile

The following steps will configure the SSL/TLS profile, which determines what certificates to trust when mobile devices are connecting to the VPN and what certificate to use when establishing outbound SSL/TLS connections.

1. In the **Palo Alto Networks Portal,** navigate to **Device > Certificate Management > SSL/TLS Service Profile.**

2. Below the details pane, select **Add;** the **SSL/TLS Service Profile** form will open.

3. In the **SSL/TLS Service Profile** form:

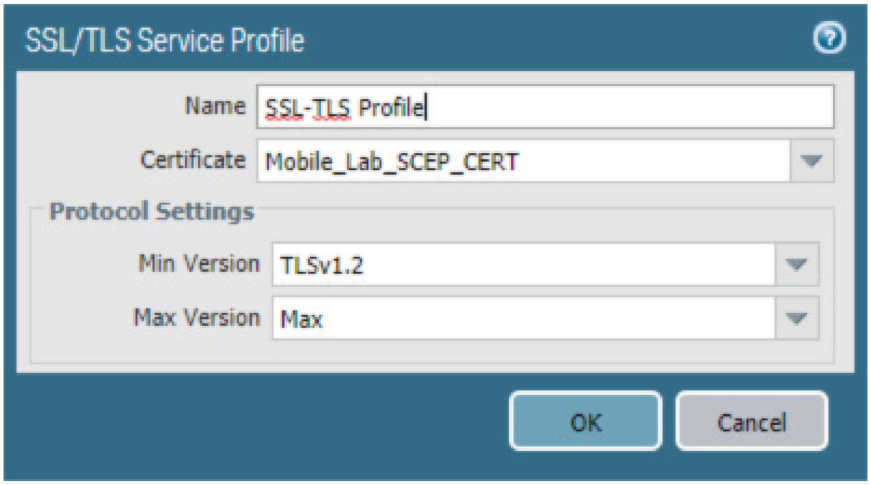
    a. In the **Name** field, enter a unique name to identify this service profile.

    b. For the **Certificate** drop-down menu, select the certificate to use for this SSL/TLS service profile; our sample implementation uses a client certificate obtained from a Microsoft enterprise CA via SCEP.

    c. For the **Min Version** drop-down menu, select **TLSv1.2.**

    d. Select **OK.**

Figure 2-67 SSL/TLS Service Profile



SSL/TLS Service Profile

Name: SSL-TLS Profile

Certificate: Mobile_Lab_SCEP_CERT

Protocol Settings

Min Version: TLSv1.2

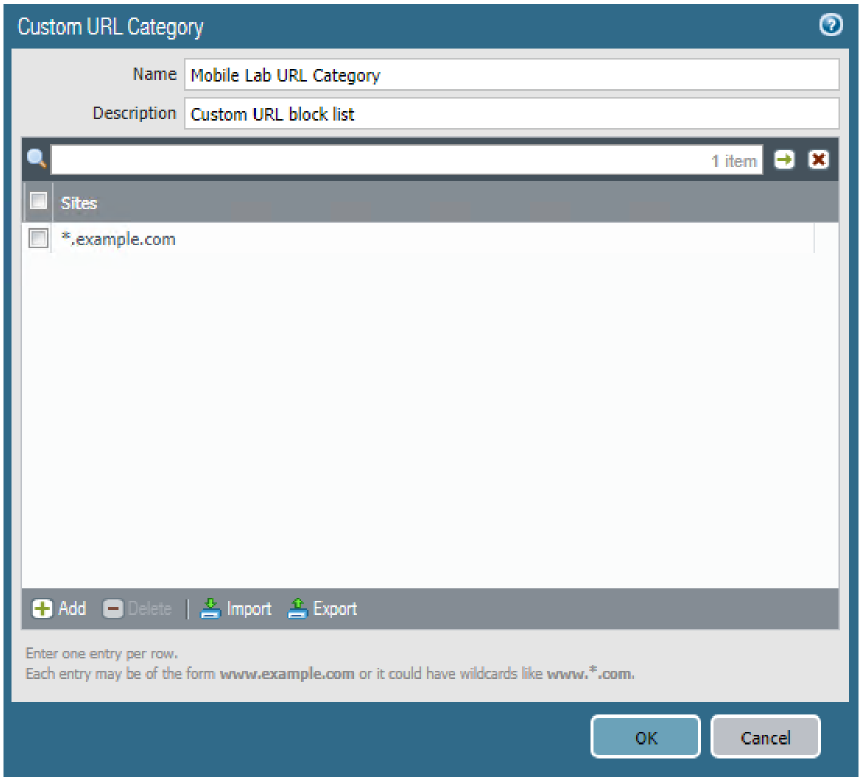
Max Version: Max

4. Repeat **Step 3** to add an identical SSL/TLS service profile for this appliance's server certificate issued through DigiCert.

2.5.12 URL Filtering Configuration

1. Navigate to **Objects > Custom Objects > URL Category.**
2. Click **Add.**
3. Give the category a name and description.
4. Add sites to be blocked. For this example, ***.example.com** was used.

Figure 2-68 Custom URL Category



Name: Mobile Lab URL Category

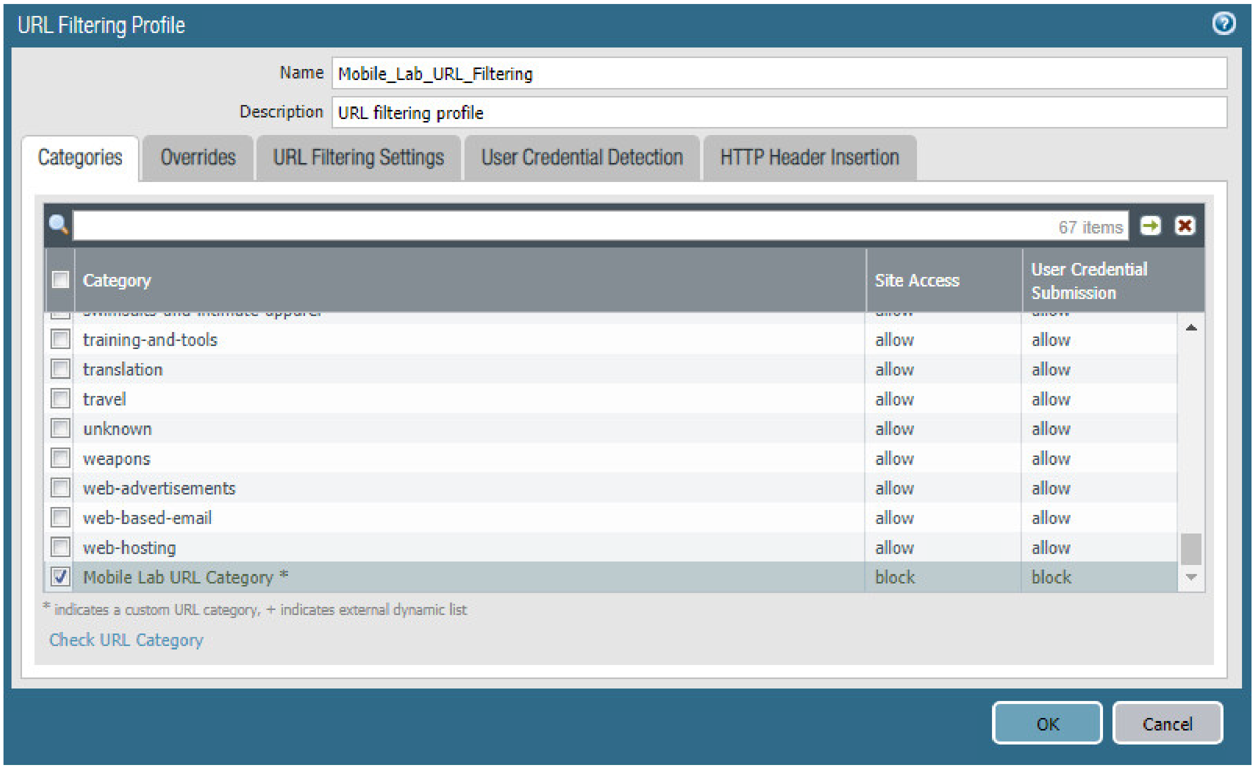
Description: Custom URL block list

□ Sites
□ *.example.com

Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

5. Click **OK.**
6. Navigate to **Objects > Security Profiles > URL Filtering.**
7. Check the box next to default and click **Clone.**
8. Select **default** from the window that appears.
9. Click **OK.**
10. Click the newly created profile, **default-1.**
11. Give the policy a meaningful name and description.
12. Scroll to the bottom of the list. The name of the created category will be last on the list.
13. Click the option below **Site Access** and next to your created URL category.
14. Set the Site Access option to **block.**

Figure 2-69 URL Filtering Profile



URL Filtering Profile

Name: Mobile_Lab_URL_Filtering

Description: URL filtering profile

	Category	Site Access	User Credential Submission
□	training-and-tools	allow	allow
□	translation	allow	allow
□	travel	allow	allow
□	unknown	allow	allow
□	weapons	allow	allow
□	web-advertisements	allow	allow
□	web-based-email	allow	allow
□	web-hosting	allow	allow
☑	Mobile Lab URL Category *	block	block

* indicates a custom URL category, + indicates external dynamic list

15. Click **OK.**

16. Navigate to **Policies > Security.**

17. Click the default outbound policy for the internal network (not VPN).

18. Click **Actions.**

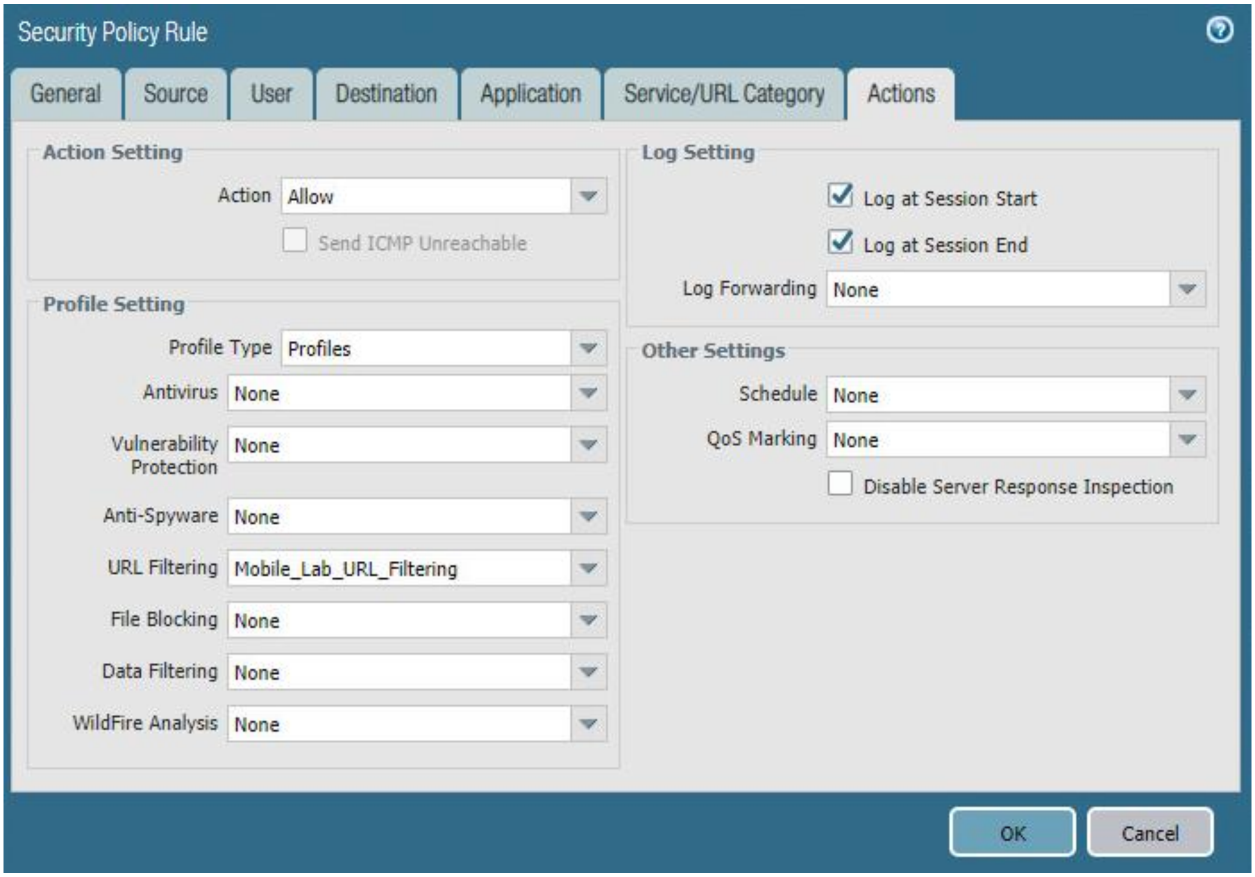
19. Next to Profile Type, select **Profiles.**

20. Next to URL Filtering, select the newly created profile.

21. Click **OK.**

22. Repeat **Steps 18** through **21** for the SSL VPN outbound traffic.

Figure 2-70 URL Filtering Security Policy



Action Setting

Action: Allow

☐ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: Mobile_Lab_URL_Filtering

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

23. Commit the changes.

2.5.13 GlobalProtect Gateway and Portal Configuration

The SSL VPN configuration requires creation of both a GlobalProtect gateway and a GlobalProtect portal, the latter of which could be used to manage VPN connections across multiple gateways. In this sample implementation, only a single gateway and portal are configured.

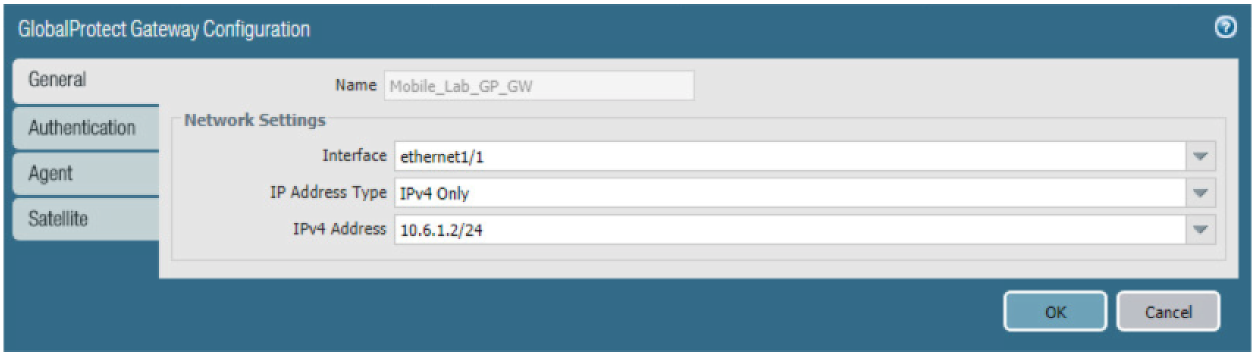
2.5.13.1 Configure GlobalProtect Gateway

The GlobalProtect gateway provides remote users with secure access to internal resources based on their Microsoft AD group. To configure the GlobalProtect gateway:

1. In the **Palo Alto Networks Portal,** navigate to **Network > GlobalProtect > Gateways.**
2. Below the details pane, select **Add;** the **GlobalProtect Gateway Configuration** form will open.

3. In the **GlobalProtect Gateway Configuration** form, on the **General** tab:
   a. In the **Name** field, enter a unique name to identify this GlobalProtect Gateway.
   b. Under **Network Settings**:
      i. In the **Interface** drop-down menu, select the physical interface connected to the subnet on which the internet gateway device is located.
      ii. In the **IPv4 Address** drop-down menu, select the IP address associated with the physical interface specified in the previous step.

Figure 2-71 General GlobalProtect Gateway Configuration



GlobalProtect Gateway Configuration

Name: Mobile_Lab_GP_GW

Network Settings

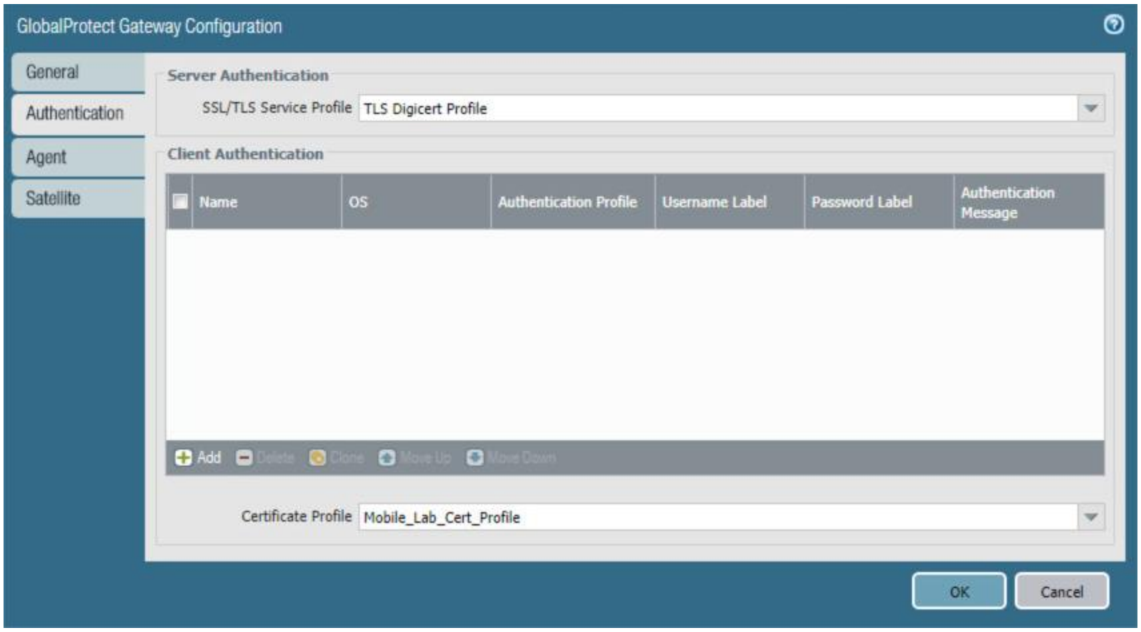
Interface: ethernet1/1

IP Address Type: IPv4 Only

IPv4 Address: 10.6.1.2/24

   c. Select the **Authentication** tab.
   d. In the **Authentication** tab:
      i. For the **Server Authentication > SSL/TLS Service Profile** drop-down menu, select the TLS/SSL profile associated with the publicly trusted server certificate for this appliance.
      ii. For the **Client Authentication > Certificate Profile** drop-down menu, select the client TLS/SSL profile associated with the internally trusted client certificates issued to mobile devices.

Figure 2-72 GlobalProtect Authentication Configuration



Server Authentication

SSL/TLS Service Profile: TLS Digicert Profile

Client Authentication

Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message

Certificate Profile: Mobile_Lab_Cert_Profile

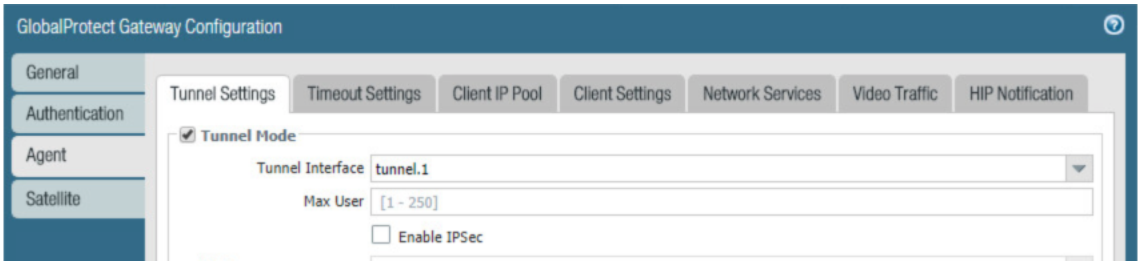
e. Select the **Agent** tab.

f. On the **Agent > Tunnel Settings** tab:

i. Select the **Tunnel Mode** checkbox.

ii. Select the **Enable IPSec** checkbox to disable IPSec.

Figure 2-73 GlobalProtect Tunnel Configuration



☑ Tunnel Mode

Tunnel Interface: tunnel.1

Max User: [1 - 250]

□ Enable IPSec

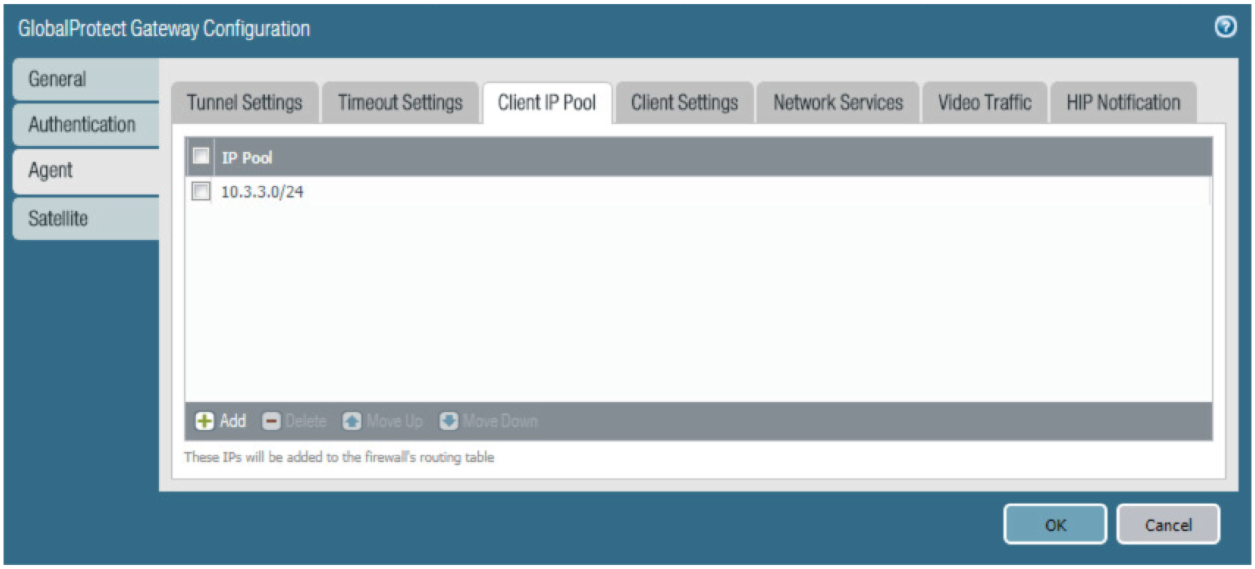
g. Select the **Agent > Client IP Pool** tab.

h. On the **Agent > Client IP Pool** tab:

i. Below the **IP Pool** list box, select **Add;** a new list item will appear.

ii. For the new **IP Pool** list item, enter the network address for the IP address pool from which connected devices will be allocated an IP address.

Figure 2-74 VPN Client IP Pool



IP Pool
10.3.3.0/24

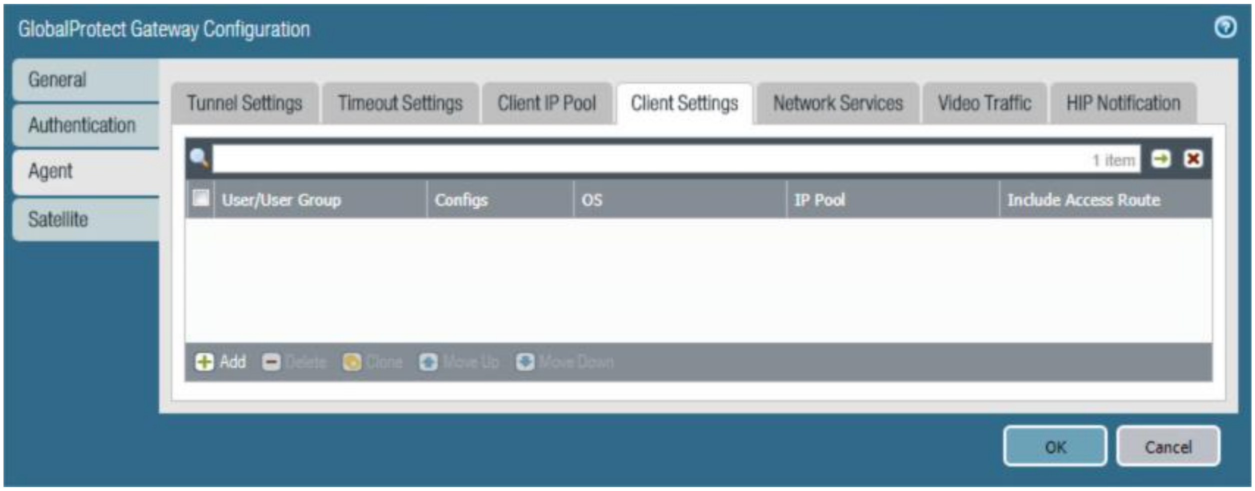
These IPs will be added to the firewall's routing table

i. Select the **Agent > Client Settings** tab.

j. On the **Agent > Client Settings** tab:

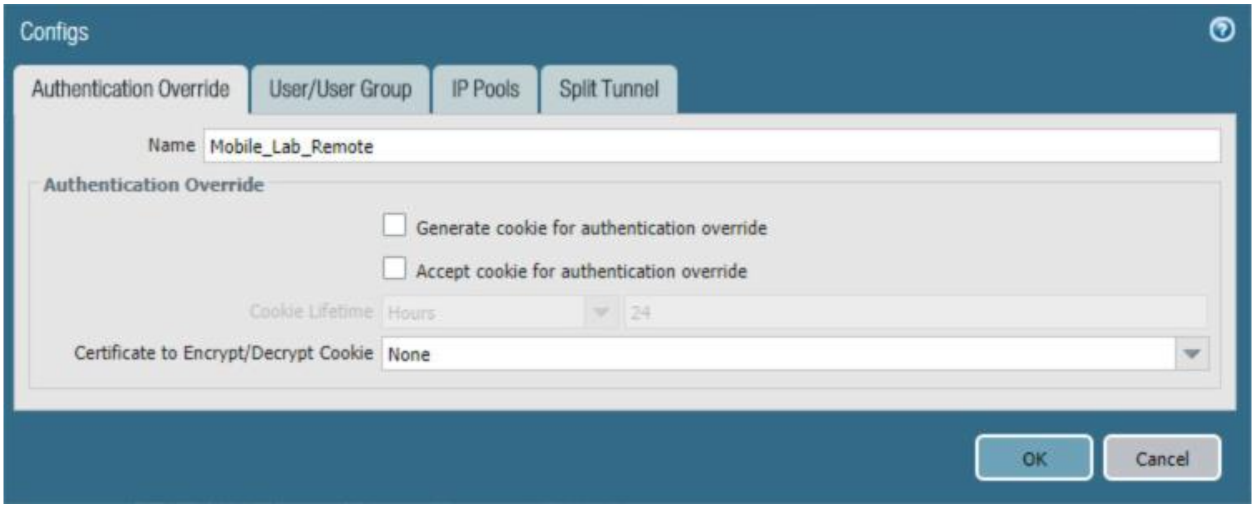
   i. Under the **Client Settings** list box, select **Add;** the **Configs** form will open.

Figure 2-75 VPN Client Settings



   ii. In the **Configs** form on the **Authorization Override** tab, enter a unique name to identify this client configuration.

Figure 2-76 VPN Authentication Override Configuration



Name Mobile_Lab_Remote

Authentication Override

□ Generate cookie for authentication override

□ Accept cookie for authentication override

Cookie Lifetime Hours 24

Certificate to Encrypt/Decrypt Cookie None

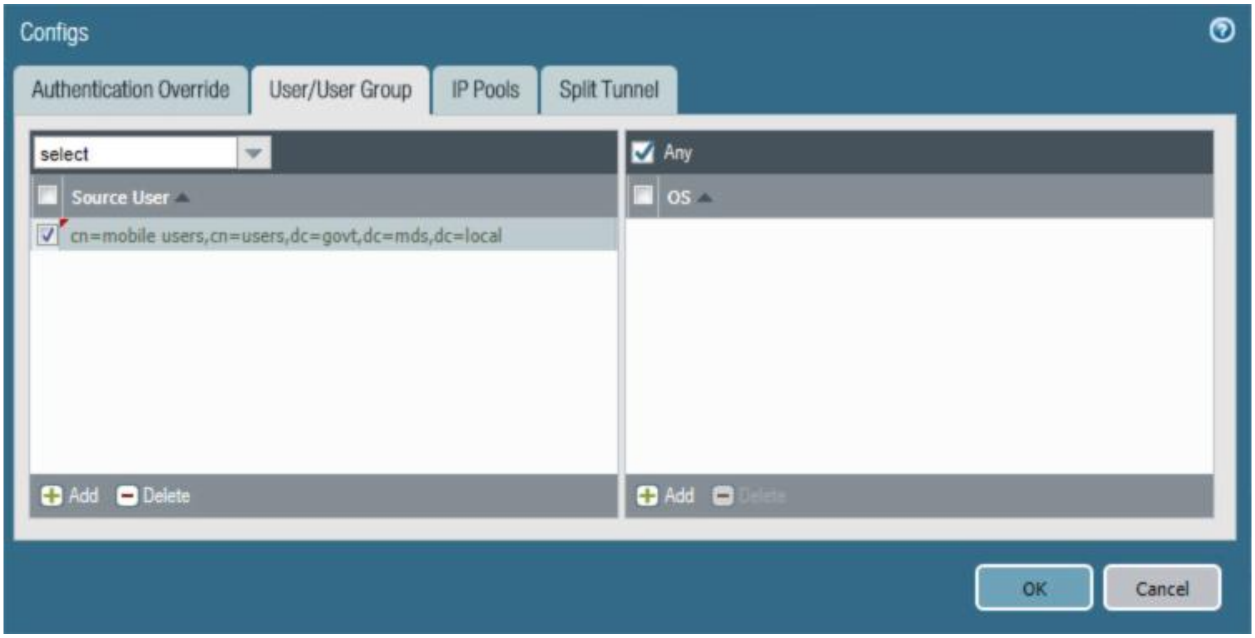
iii. Select the **User/User Group** tab.

iv. On the **User/User Group** tab:

1) Below the **Source User** list box, select **Add;** a new list item will appear.

2) In the **Source User** list item, select the Microsoft AD user group to grant access to internal resources through this GlobalProtect gateway.

Figure 2-77 VPN User Group Configuration



□ Source User
☑ cn=mobile users,cn=users,dc=govt,dc=mds,dc=local

☑ Any

□ OS

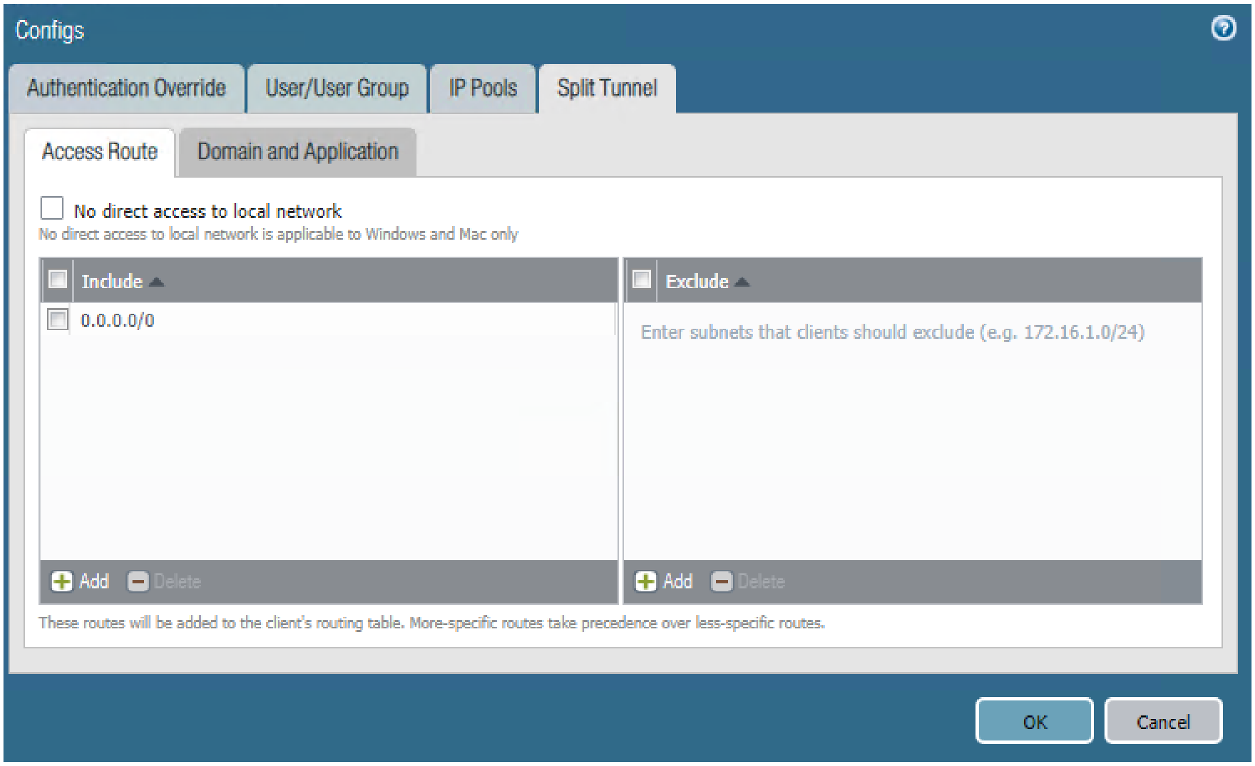
v. Select the **Split Tunnel** tab.

vi. On the **Split Tunnel** tab, on the **Access Route** tab:

1) Under the **Include** list box, select **Add;** a new list item will appear.

2) In the new **Include** list item, enter **0.0.0.0/0.** This enforces full tunneling.

Figure 2-78 VPN Split Tunnel Configuration



□ No direct access to local network

No direct access to local network is applicable to Windows and Mac only

□ Include ▲	□ Exclude ▲
□ 0.0.0.0/0	Enter subnets that clients should exclude (e.g. 172.16.1.0/24)

These routes will be added to the client's routing table. More-specific routes take precedence over less-specific routes.

vii. Select **OK.**

k. Select **OK.**

2.5.13.2 Configure GlobalProtect Portal

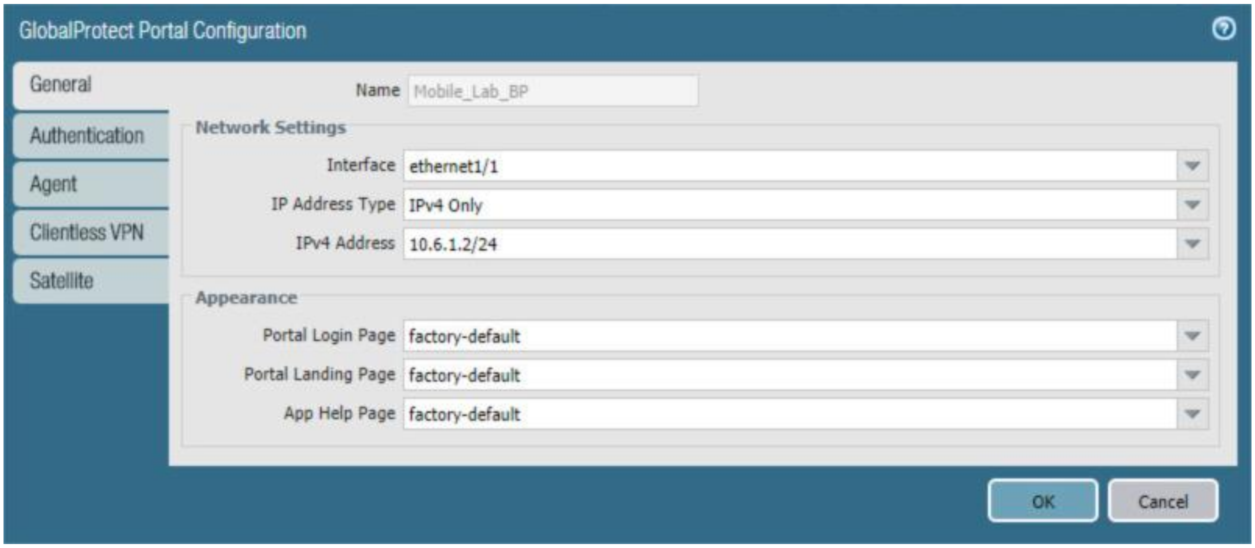
1. In the **Palo Alto Networks Portal**, navigate to **Network > GlobalProtect > Portal.**
2. Below the details pane, select **Add;** the **GlobalProtect Portal Configuration** form will open.
3. In the **GlobalProtect Portal Configuration** form, on the **General** tab:

a. In the **Name** field, enter a unique name to identify this GlobalProtect portal.

b. In the **Interface** drop-down menu, select the physical interface connected to the subnet on which the internet gateway device is located.

c. In the **IP Address Type** drop-down menu, select **IPv4 Only.**

Figure 2-79 GlobalProtect Portal Configuration



GlobalProtect Portal Configuration

Name: Mobile_Lab_BP

Network Settings

Interface: ethernet1/1

IP Address Type: IPv4 Only

IPv4 Address: 10.6.1.2/24

Appearance

Portal Login Page: factory-default

Portal Landing Page: factory-default

App Help Page: factory-default

4. Select the **Authentication** tab.

5. In the **Authentication** tab:

a. For the **Server Authentication > SSL/TLS Service Profile** drop-down menu, select the SSL/TLS service profile based on your third-party server certificate.

b. For the **Certificate Profile** drop-down menu, select the client TLS/SSL profile associated with the internally trusted client certificates issued to mobile devices.

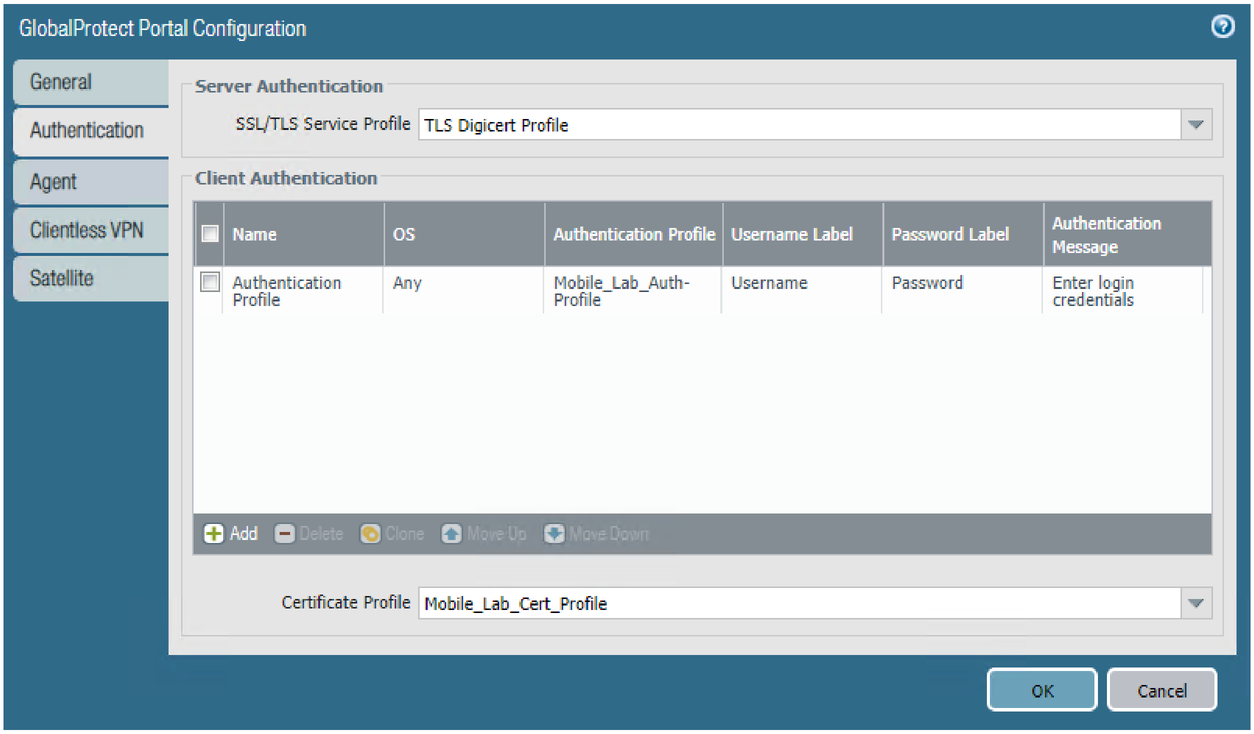
c. Click **Add.**

d. Enter a profile name. In this example implementation, Client Authentication was used.

e. For the **Authentication Profile** drop-down menu, select the previously created authentication profile.

f. Click **OK.**

Figure 2-80 GlobalProtect Portal SSL/TLS Configuration



Server Authentication

SSL/TLS Service Profile: TLS Digicert Profile

Client Authentication

□	Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message
□	Authentication Profile	Any	Mobile_Lab_Auth-Profile	Username	Password	Enter login credentials

Certificate Profile: Mobile_Lab_Cert_Profile

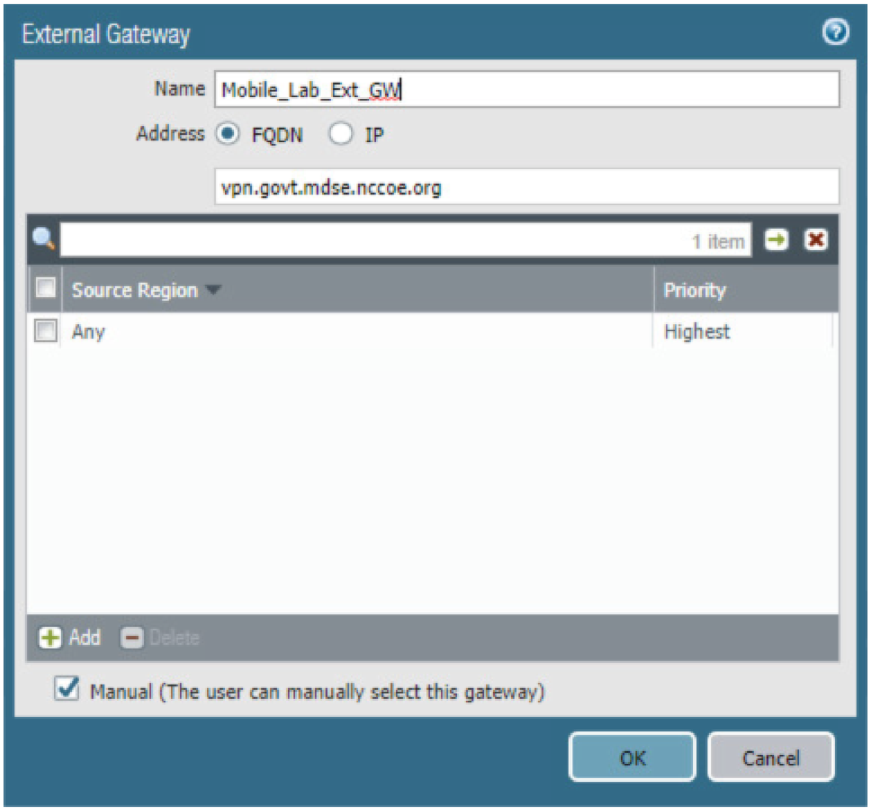
6. Select the **Agent** tab.
7. On the **Agent** tab:
   a. Below the **Agent** list box, select **Add;** the Configs form will open.
   b. In the **Configs** form:
      i. In the **Authentication** tab, below **Components that Require Dynamic Passwords,** check the box next to **Portal.**
      ii. In the **External** tab, under the **External Gateways** list box select **Add;** the **External Gateway** form will open.
      iii. In the External Gateway form:
         1) In the **Name** field, enter a unique name to identify this external gateway.
         2) For the **Address** option, enter the FQDN for this appliance; in this sample implementation, the FQDN is **vpn.govt.mdse.nccoe.org.**
         3) Below the **Source Region** list box, select **Add;** a new list item will appear.

4) In the new **Source Region** list item, select **Any.**

5) Select the **Manual** checkbox.

6) Select **OK.**

Figure 2-81 GlobalProtect External Gateway Configuration



External Gateway

Name: Mobile_Lab_Ext_GW

Address: ● FQDN ○ IP

vpn.govt.mdse.nccoe.org

1 item

□	Source Region	Priority
□	Any	Highest

☑ Manual (The user can manually select this gateway)

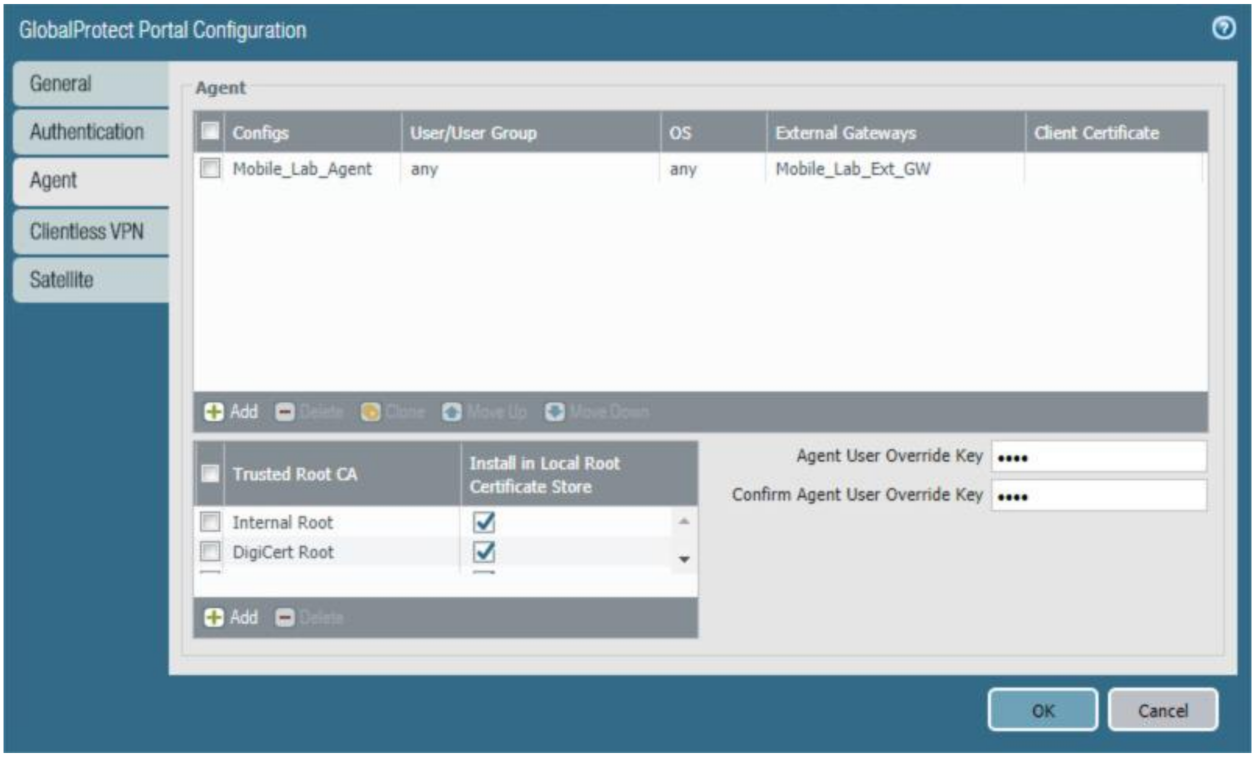
iv. Below the **Trusted Root CA** list box, select **Add;** a new list item will appear.

v. In the new **Trusted Root CA** list item, select your internal CA root certificate.

vi. Repeat **Steps 7biii** and **7biv** to add each certificate in your internal or third-party certificate trust chains used when mobile devices contact the GlobalProtect portal.

c. Click **App.** Ensure that Connect Method is set to **User-logon (Always On).**

Figure 2-82 GlobalProtect Portal Agent Configuration



Agent

□ Configs	User/User Group	OS	External Gateways	Client Certificate
□ Mobile_Lab_Agent	any	any	Mobile_Lab_Ext_GW	

□ Trusted Root CA	Install in Local Root Certificate Store
□ Internal Root	☑
□ DigiCert Root	☑

Agent User Override Key ••••

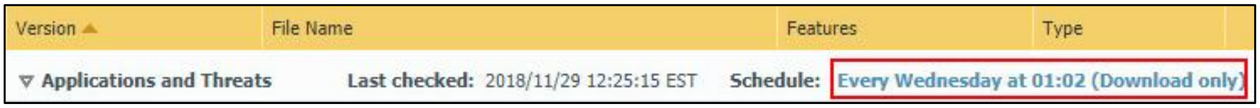
Confirm Agent User Override Key ••••

d. Select **OK.**

2.5.14 Configure Automatic Threat and Application Updates

1. In the **PAN-OS portal,** navigate to **Device > Dynamic Updates.**
2. Click **Check Now** at the bottom of the page.
3. Under Applications and Threats, click **Download** next to the last item in the list, with the latest Release Date. It will take a minute to download the updates.
4. When the download completes, click **Done.**
5. Click **Install** next to the downloaded update.
6. Click **Continue Installation.**
7. When installation completes, click **Close.**
8. Next to Schedule, click the link with the date and time.

Figure 2-83 Schedule Link



Version ▲	File Name	Features	Type

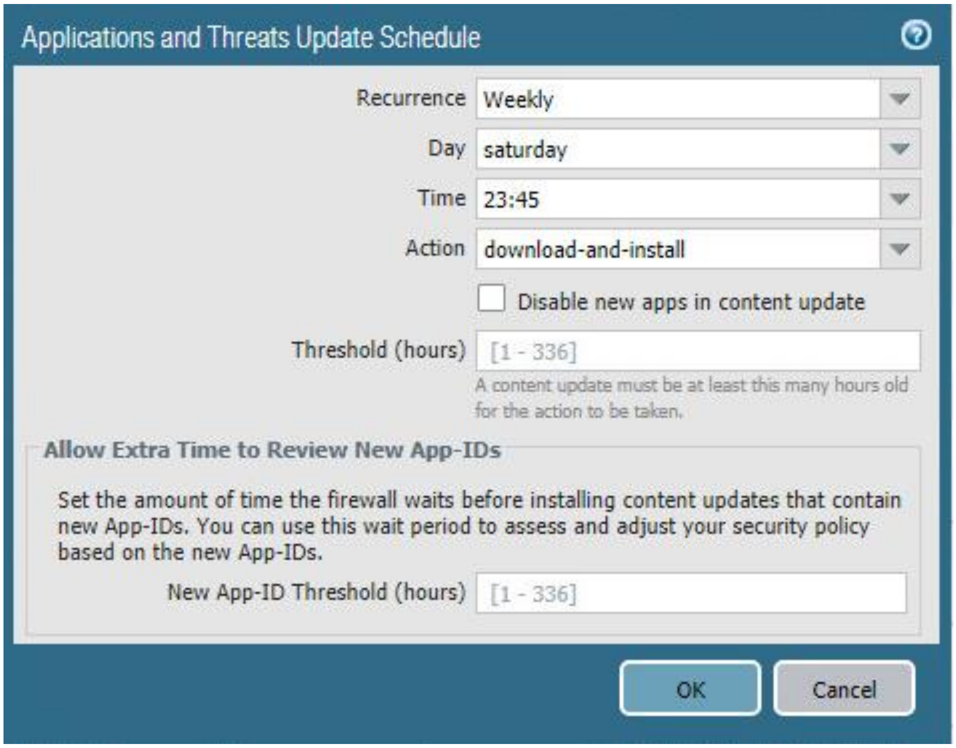
▽ Applications and Threats Last checked: 2018/11/29 12:25:15 EST Schedule: Every Wednesday at 01:02 (Download only)

9. Select the desired recurrence. For this implementation, Weekly was used.

10. Select the desired day and time. For this implementation, Saturday at 23:45 was used.

11. Next to Action, select **download-and-install.**

Figure 2-84 Threat Update Schedule



Applications and Threats Update Schedule

Recurrence: Weekly

Day: saturday

Time: 23:45

Action: download-and-install

□ Disable new apps in content update

Threshold (hours): [1 - 336]

A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours): [1 - 336]

12. Click **OK.**

13. Commit the changes.

2.6 Integration of Kryptowire EMM+S with MobileIron

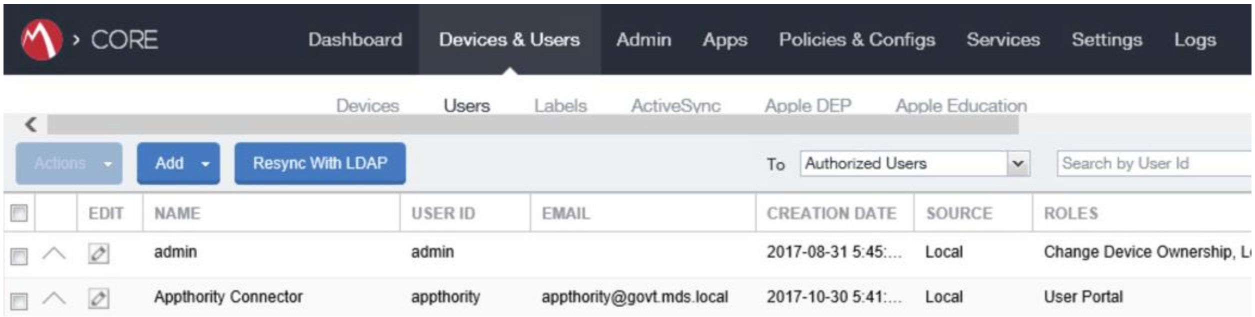
Kryptowire's application vetting service uses the MobileIron application programming interface (API) to regularly pull current device application inventory information from MobileIron Core. Updated analysis results are displayed in the Kryptowire portal.

2.6.1 Add MobileIron API Account for Kryptowire

The following steps will create an administrative account that will grant Kryptowire the specific permissions it requires within MobileIron.

1. In the **MobileIron Admin Portal,** navigate to **Devices & Users > Users.**
2. On the **Users** page:
   a. Select **Add > Add Local User;** the Add New User dialogue will open.

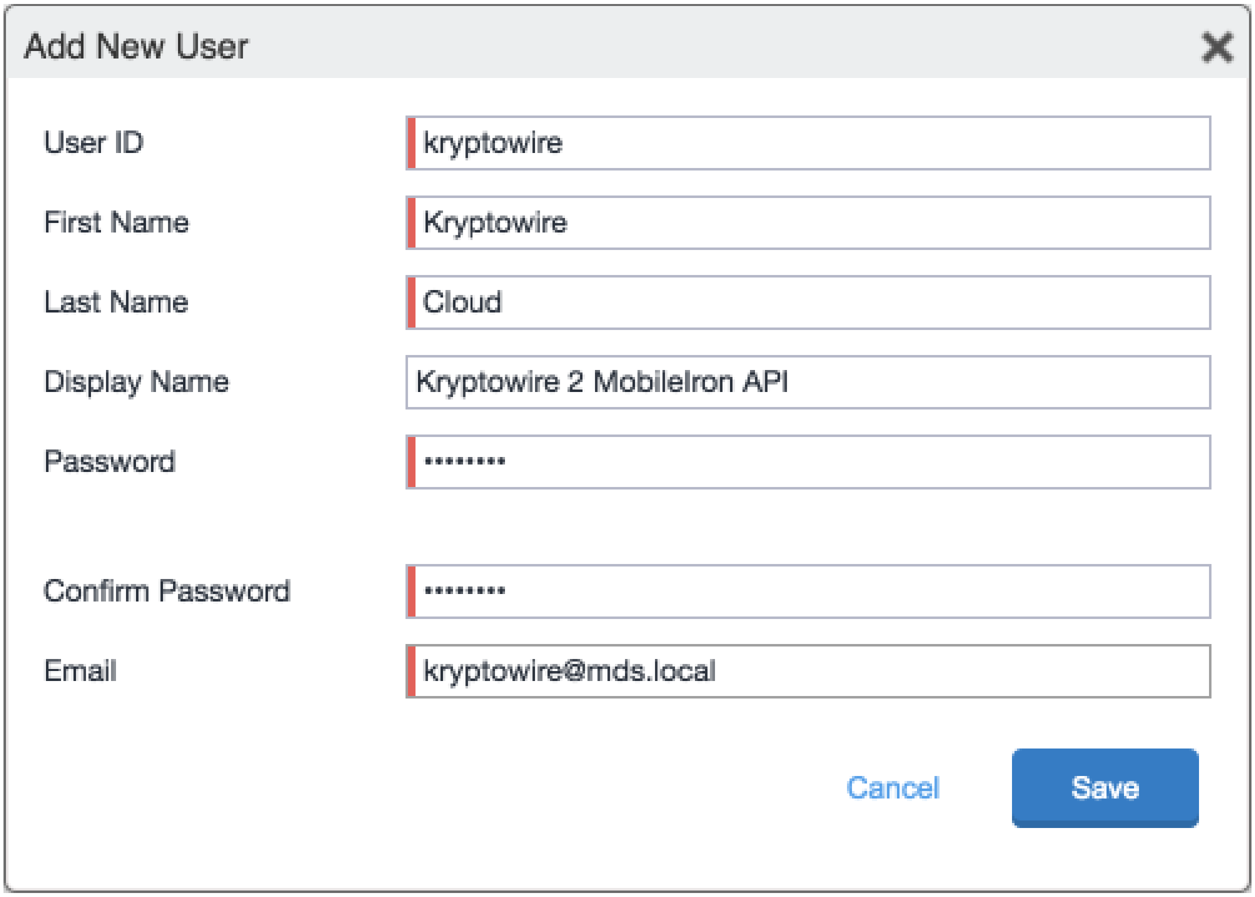
Figure 2-85 MobileIron Users



□		EDIT	NAME	USER ID	EMAIL	CREATION DATE	SOURCE	ROLES
□	^	✎	admin	admin		2017-08-31 5:45:...	Local	Change Device Ownership, L
□	^	✎	Appthority Connector	appthority	appthority@govt.mds.local	2017-10-30 5:41:...	Local	User Portal

   b. In the **Add New User** dialogue:
      i. In the **User ID** field, enter the user identity that the Kryptowire cloud will authenticate under; our implementation uses a value of **kryptowire.**
      ii. In the **First Name** field, enter a generic first name for **Kryptowire**.
      iii. In the **Last Name** field, enter a generic last name for **Kryptowire**.
      iv. In the **Display Name** field, optionally enter a displayed name for this user account.
      v. In the **Password** field, provide the password that the **Kryptowire** identity will use to authenticate to MobileIron.
      vi. In the **Confirm Password** field, enter the same password as in the preceding step.
      vii. In the **Email** field, provide an email account for the **Kryptowire** identity; this could be used in configuring automatic notifications and should be an account under the control of your organization.
      viii. Select **Save**

Figure 2-86 Kryptowire API User Configuration



Add New User

User ID: kryptowire

First Name: Kryptowire

Last Name: Cloud

Display Name: Kryptowire 2 MobileIron API

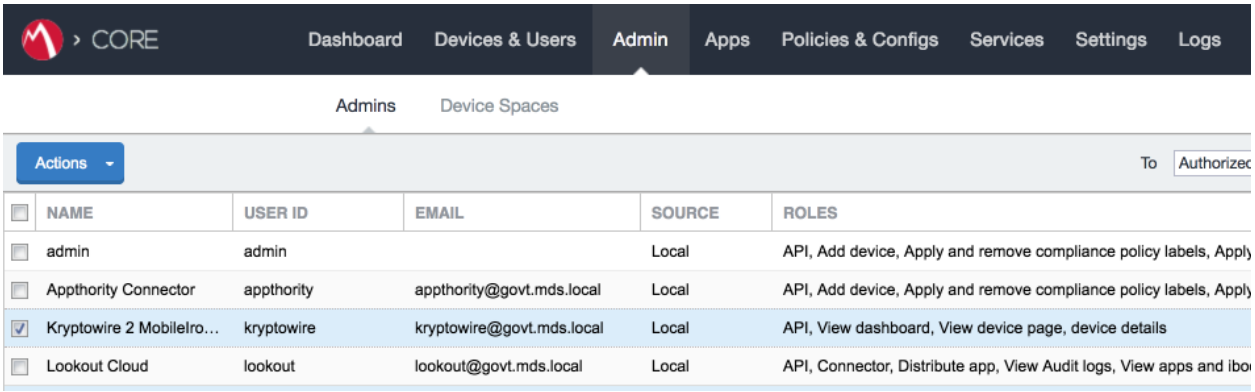
Password: •••••••••

Confirm Password: •••••••••

Email: kryptowire@mds.local

3. In the **MobileIron Admin Portal,** navigate to **Admin > Admins.**
4. On the **Admins** page:
   a. Enable the account you created for Kryptowire during **Step 2.**
   b. Select **Actions > Assign to Space;** this will open the Assign to Space dialogue for the Kryptowire account.

Figure 2-87 MobileIron User List

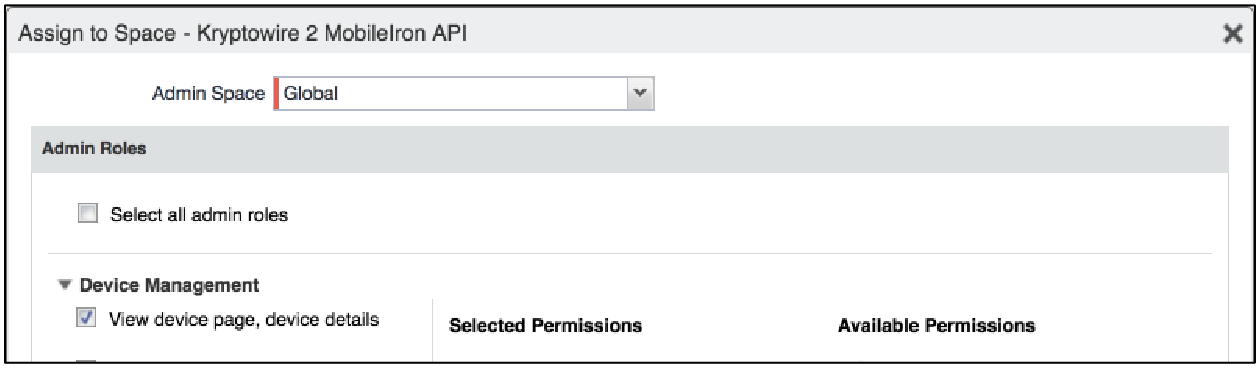


	NAME	USER ID	EMAIL	SOURCE	ROLES
□	admin	admin		Local	API, Add device, Apply and remove compliance policy labels, Apply
□	Appthority Connector	appthority	appthority@govt.mds.local	Local	API, Add device, Apply and remove compliance policy labels, Apply
☑	Kryptowire 2 MobileIro…	kryptowire	kryptowire@govt.mds.local	Local	API, View dashboard, View device page, device details
□	Lookout Cloud	lookout	lookout@govt.mds.local	Local	API, Connector, Distribute app, View Audit logs, View apps and ibo

c. In the **Assign to Space** dialogue:

i. In the **Select Space** drop-down menu, select **Global.**

Figure 2-88 Kryptowire API User Space Assignment


Assign to Space - Kryptowire 2 MobileIron API

Admin Space: Global

Admin Roles

□ Select all admin roles

▼ Device Management

☑ View device page, device details

ii. Enable each of the following settings:

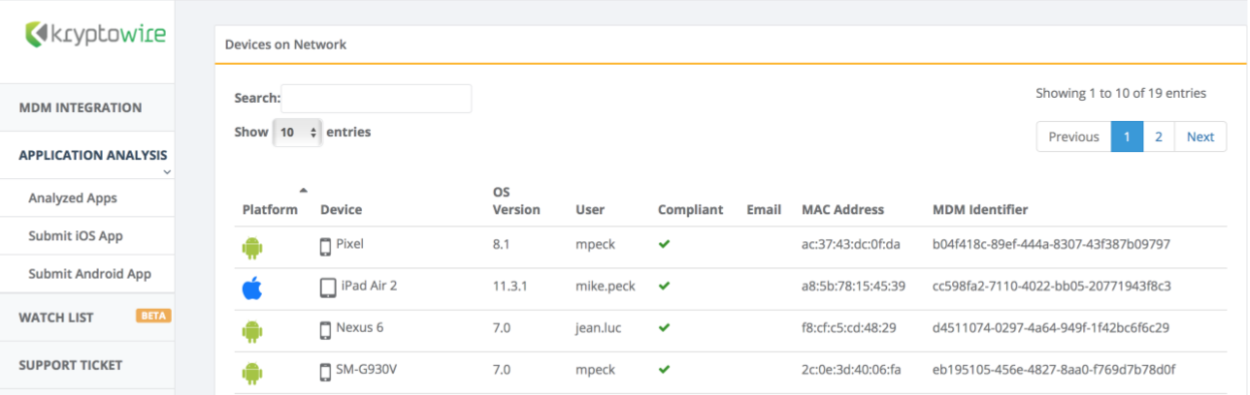
Admin Roles > Device Management > View device page, device details
Admin Roles > Device Management > View dashboard
Admin Roles > Privacy Control > View apps and ibooks in device details
Admin Roles > Privacy Control > View device IP and MAC address
Admin Roles > App Management > View app
Admin Roles > App Management > View app inventory
Other Roles > Common Services Provider (CSP)
Other Roles > API

iii. Select **Save.**

2.6.2 Contact Kryptowire to Create Inbound Connection

Once the MobileIron API account has been created, contact Kryptowire customer support to integrate your instance of MobileIron Core. Note that this will require creation of firewall rules that permit inbound connections from IP addresses designated by Kryptowire to MobileIron Core on port 443. Once the connection has been established, the Kryptowire portal will populate with information on devices registered with MobileIron. The EMM (Enterprise Mobility Management) ID presented by Kryptowire will be the same as the Universally Unique ID assigned to a device by MobileIron Core.

Figure 2-89 Kryptowire Device List



Showing 1 to 10 of 19 entries

Platform	Device	OS Version	User	Compliant	Email	MAC Address	MDM Identifier
🤖	Pixel	8.1	mpeck	✓		ac:37:43:dc:0f:da	b04f418c-89ef-444a-8307-43f387b09797
🍎	iPad Air 2	11.3.1	mike.peck	✓		a8:5b:78:15:45:39	cc598fa2-7110-4022-bb05-20771943f8c3
🤖	Nexus 6	7.0	jean.luc	✓		f8:cf:c5:cd:48:29	d4511074-0297-4a64-949f-1f42bc6f6c29
🤖	SM-G930V	7.0	mpeck	✓		2c:0e:3d:40:06:fa	eb195105-456e-4827-8aa0-f769d7b78d0f

2.7 Integration of Lookout Mobile Endpoint Security with MobileIron

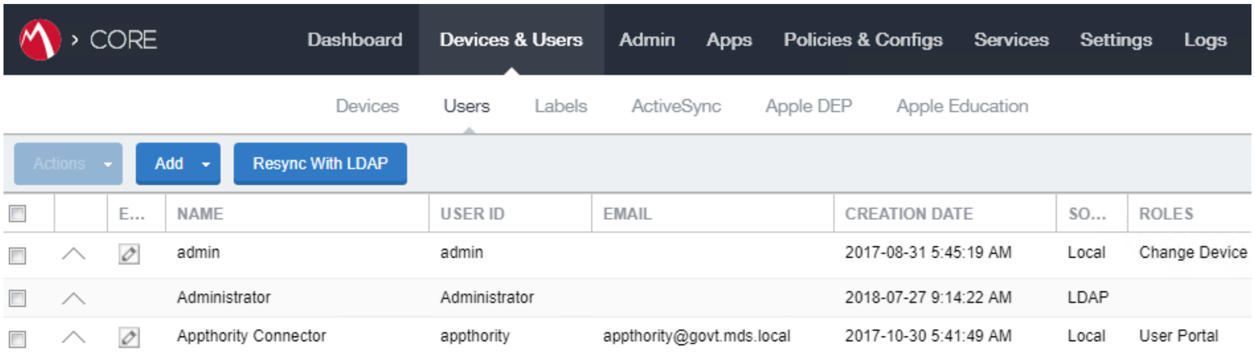
Lookout's Mobile Endpoint Security cloud service uses the MobileIron API to pull mobile device details and app inventory from MobileIron Core. Following analysis, Lookout uses the API to apply specific labels to devices to categorize them by the severity of any issues detected. MobileIron can be configured to automatically respond to the application of specific labels per built-in compliance actions.

2.7.1 Add MobileIron API Account for Lookout

The following steps will create an administrative account that will grant to Lookout the specific permissions it requires within MobileIron.

1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Users**.
2. On the **Users** page:
    a. Select **Add > Add Local User**; the Add New User dialogue will open.

Figure 2-90 MobileIron User List



☐		E...	NAME	USER ID	EMAIL	CREATION DATE	SO...	ROLES
☐	︿	✎	admin	admin		2017-08-31 5:45:19 AM	Local	Change Device
☐	︿		Administrator	Administrator		2018-07-27 9:14:22 AM	LDAP	
☐	︿	✎	Appthority Connector	appthority	appthority@govt.mds.local	2017-10-30 5:41:49 AM	Local	User Portal

b. In the **Add New User** dialogue:

i. In the **User ID** field, enter the user identity the Lookout cloud will authenticate under. Our implementation uses a value of **lookout**.

ii. In the **First Name** field, enter a generic first name for **Lookout**.

iii. In the **Last Name** field, enter a generic last name for **Lookout**.

iv. In the **Display Name** field, optionally enter a displayed name for this user account.

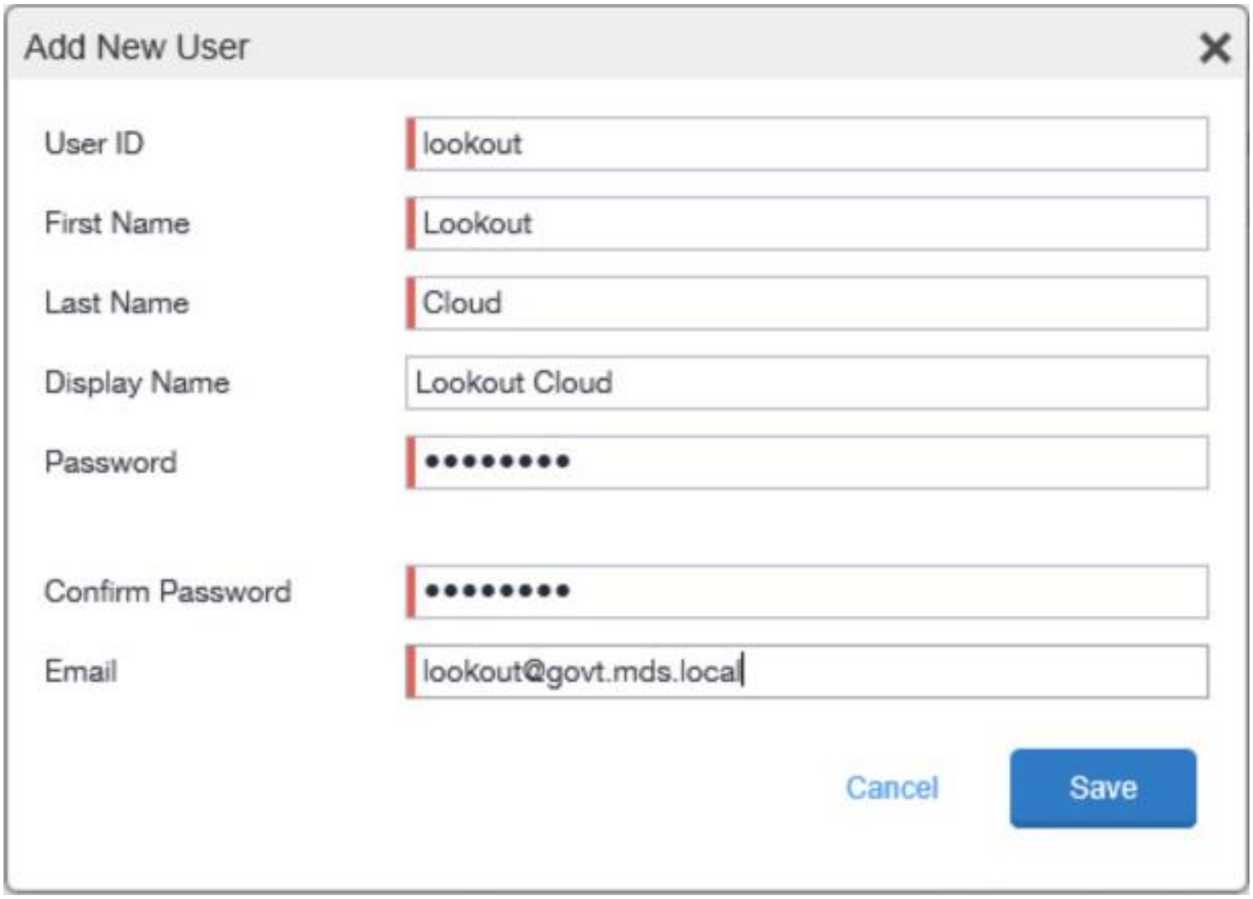
v. In the **Password** field, provide the password the Lookout identity will use to authenticate to MobileIron.

vi. In the **Confirm Password** field, enter the same password as in the preceding step.

vii. In the **Email** field, provide an email account for the Lookout identity; since this may be used for alerts, it should be an account under the control of your organization.

viii. Select **Save**.

Figure 2-91 MobileIron Lookout User Configuration

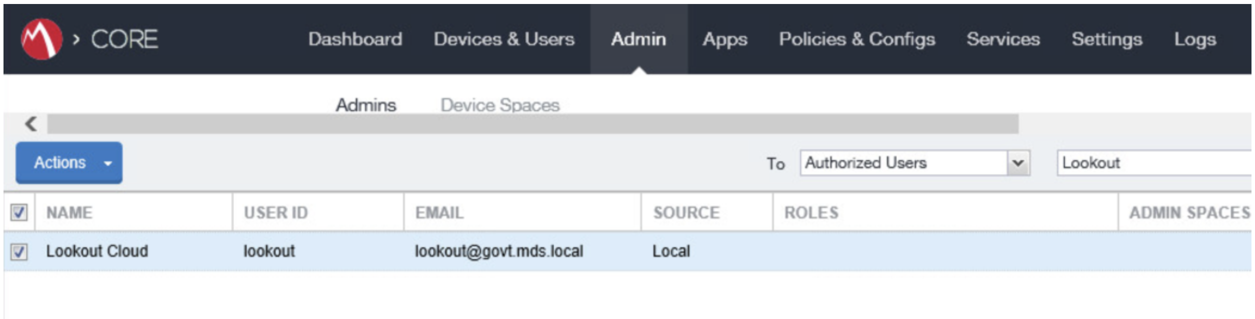


Add New User

User ID	lookout
First Name	Lookout
Last Name	Cloud
Display Name	Lookout Cloud
Password	●●●●●●●●
Confirm Password	●●●●●●●●
Email	lookout@govt.mds.local

3. In the **MobileIron Admin Portal**, navigate to **Admin**.
4. On the **Admin** page:
    a. Enable the account you created for Lookout during **Step 2**.
    b. Select **Actions > Assign to Space**; this will open the **Assign to Space** dialogue for the Lookout account.

Figure 2-92 Lookout MobileIron Admin Account



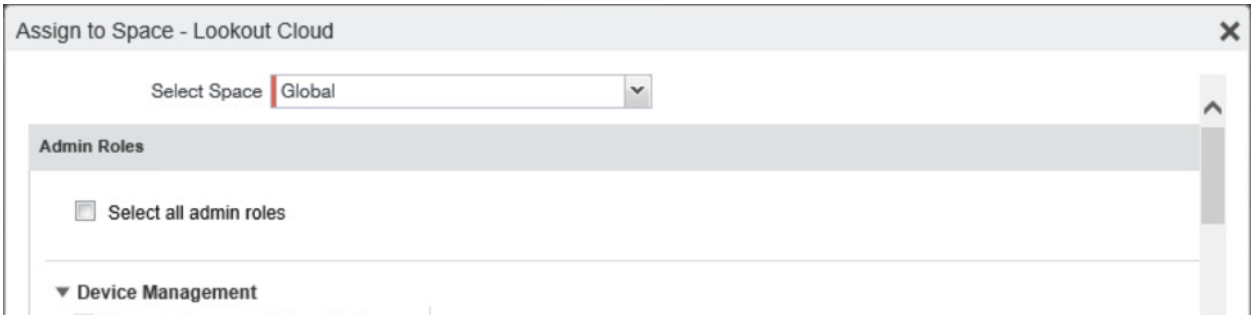
To: Authorized Users | Lookout

☑	NAME	USER ID	EMAIL	SOURCE	ROLES	ADMIN SPACES
☑	Lookout Cloud	lookout	lookout@govt.mds.local	Local		

c. In the **Assign to Space** dialogue:

i. In the **Select Space** drop-down menu, select **Global.**

Figure 2-93 Lookout Account Space Assignment



Assign to Space - Lookout Cloud

Select Space: Global

Admin Roles

□ Select all admin roles

▼ Device Management

ii. Enable each of the following settings:

Admin Roles > Device Management > View device page, device details
Admin Roles > Device Management > View dashboard
Admin Roles > Label Management > View Label
Admin Roles > Label Management > Manage Label
Admin Roles > Privacy Control > View apps and ibooks in device details
Admin Roles > Privacy Control > View device IP and MAC address
Admin Roles > App Management > Distribute app
Admin Roles > Logs and Event Management > View Audit logs
Admin Roles > Logs and Event Management > View events
Other Roles > CSP
Other Roles > Connector
Other Roles > API

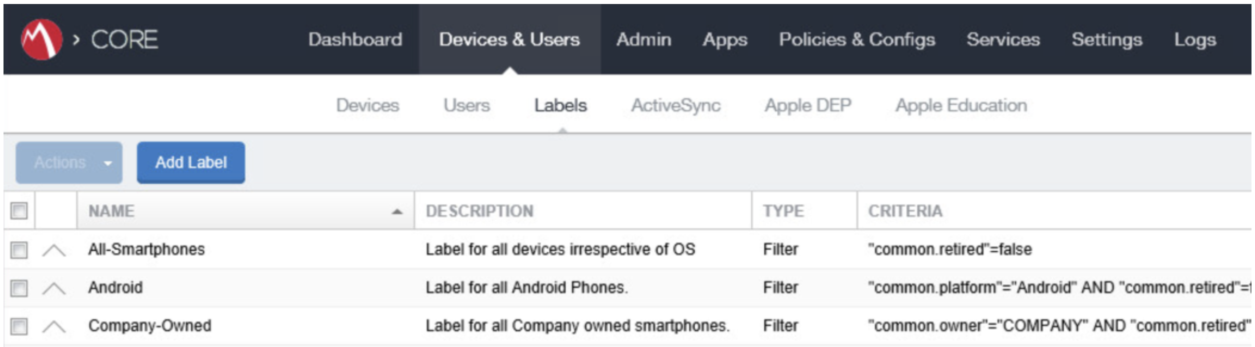
iii. Select **Save**.

2.7.2 Add MobileIron Labels for Lookout

Lookout will dynamically apply MobileIron labels to protected devices to communicate information about their current state. The following steps will create a group of Lookout-specific labels.

1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Labels**.
2. On the **Labels** page:
    a. Select **Add Label**; the **Add Label** dialogue will appear.

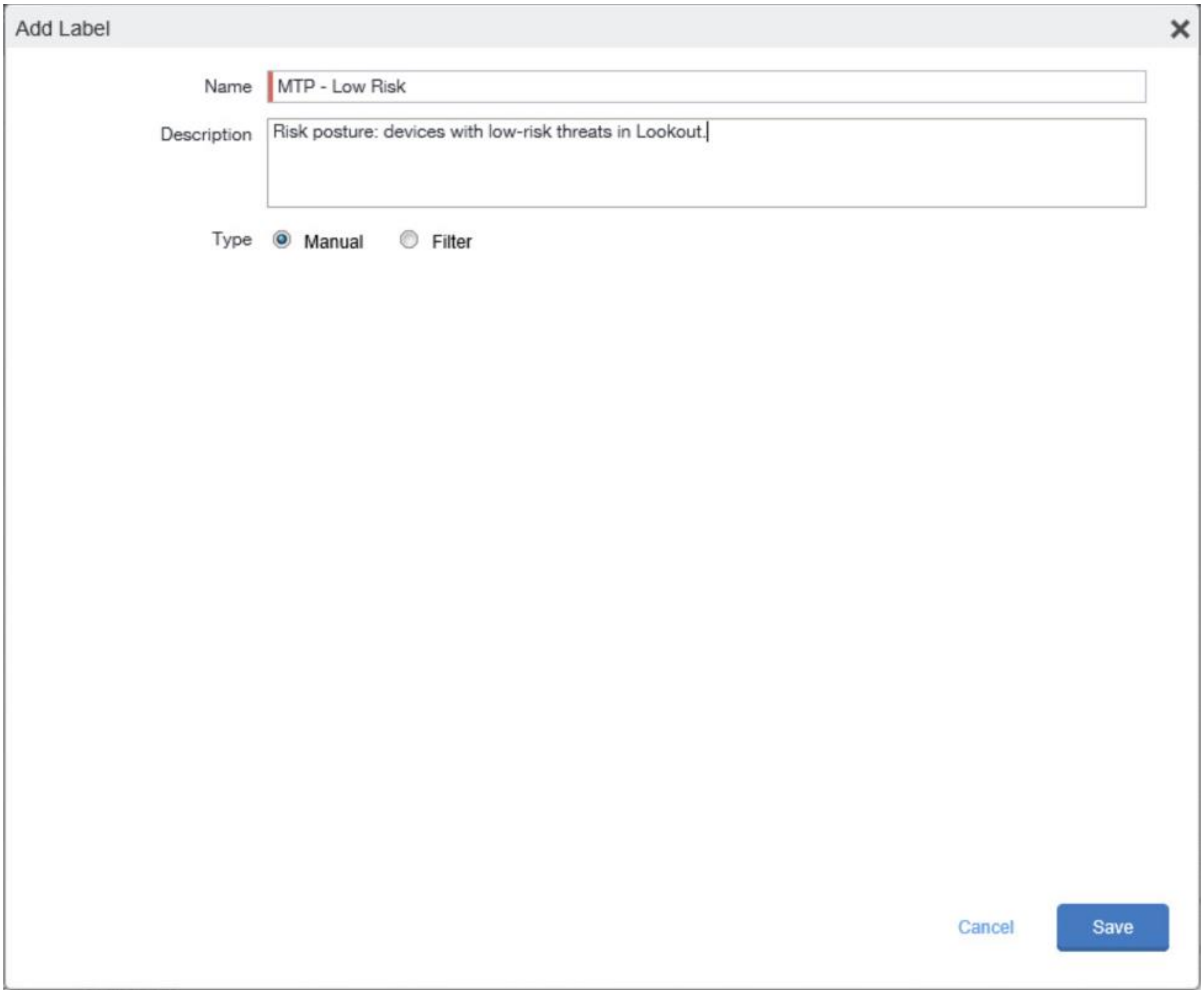
Figure 2-94 MobileIron Label List



NAME	DESCRIPTION	TYPE	CRITERIA
All-Smartphones	Label for all devices irrespective of OS	Filter	"common.retired"=false
Android	Label for all Android Phones.	Filter	"common.platform"="Android" AND "common.retired"=
Company-Owned	Label for all Company owned smartphones.	Filter	"common.owner"="COMPANY" AND "common.retired"

    b. In the **Add Label** dialogue:
        i. In the **Name** field, enter the name of the label. Note: future steps will use the Label Names presented here but use of these names is optional.
        ii. In the **Description** field, enter a brief description for this label.
        iii. For the **Type** option, select **Manual**; this will hide all other form inputs.
        iv. Select **Save.**

1269 **Figure 2-95 MTP Low Risk Label Configuration**



Name: MTP - Low Risk

Description: Risk posture: devices with low-risk threats in Lookout.

Type: ● Manual ○ Filter

c. Complete **Step 3** for each label in the following table:

Label Name	Purpose
Lookout for Work	Device enrollment
MTP - Pending	Lifecycle management: devices with Lookout not yet activated
MTP - Secured	Lifecycle management: devices with Lookout activated
MTP - Threats Present	Lifecycle management: devices with threats detected by Lookout

MTP - Deactivated	Lifecycle management: devices with Lookout deactivated
MTP - Low Risk	Risk posture: devices with a low risk score in Lookout
MTP - Moderate Risk	Risk posture: devices with a moderate risk score in Lookout
MTP - High Risk	Risk posture: devices with a high risk score in Lookout

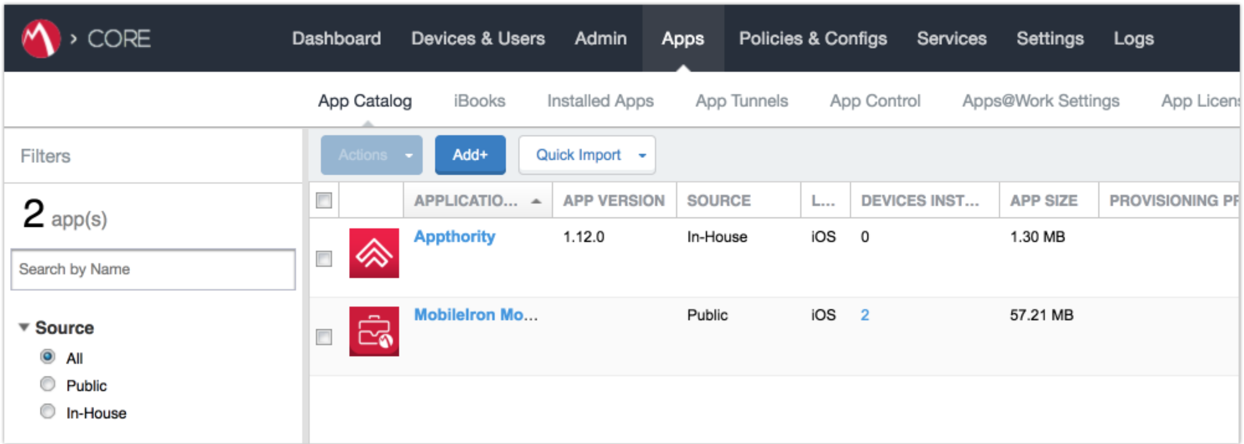
Note: Administrators can choose to alter the label names to something more appropriate for their environment.

2.7.3 Add Lookout for Work for Android to MobileIron App Catalog

The following steps will add the Lookout for Work app for Android to MobileIron.

1. In the **MobileIron Admin Portal**, navigate to **Apps > App Catalog**.
2. On the **App Catalog** page, select **Add**; this will start the workflow to add a new app to the app catalog.

Figure 2-96 MobileIron App Catalog



2 app(s)

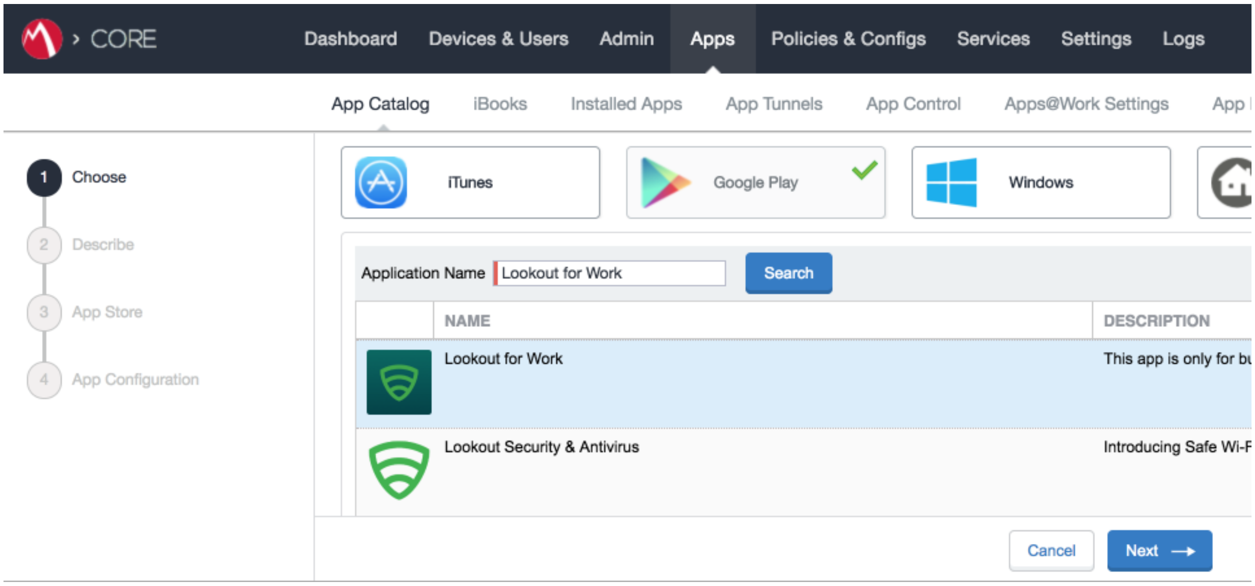
	APPLICATIO...	APP VERSION	SOURCE	L...	DEVICES INST...	APP SIZE	PROVISIONING PF
□	Appthority	1.12.0	In-House	iOS	0	1.30 MB	
□	MobileIron Mo...		Public	iOS	2	57.21 MB	

3. On the **App Catalog > Choose** page:
   a. Select **Google Play**; additional controls will be displayed.
   b. In the **Application Name** field, enter **Lookout for Work**.
   c. Select **Search**; search results will be displayed in the lower pane.

d. In the list of search results, select the **Lookout for Work** app.

e. Select **Next**.

Figure 2-97 Adding Lookout for Work to the MobileIron App Catalog



Application Name: Lookout for Work

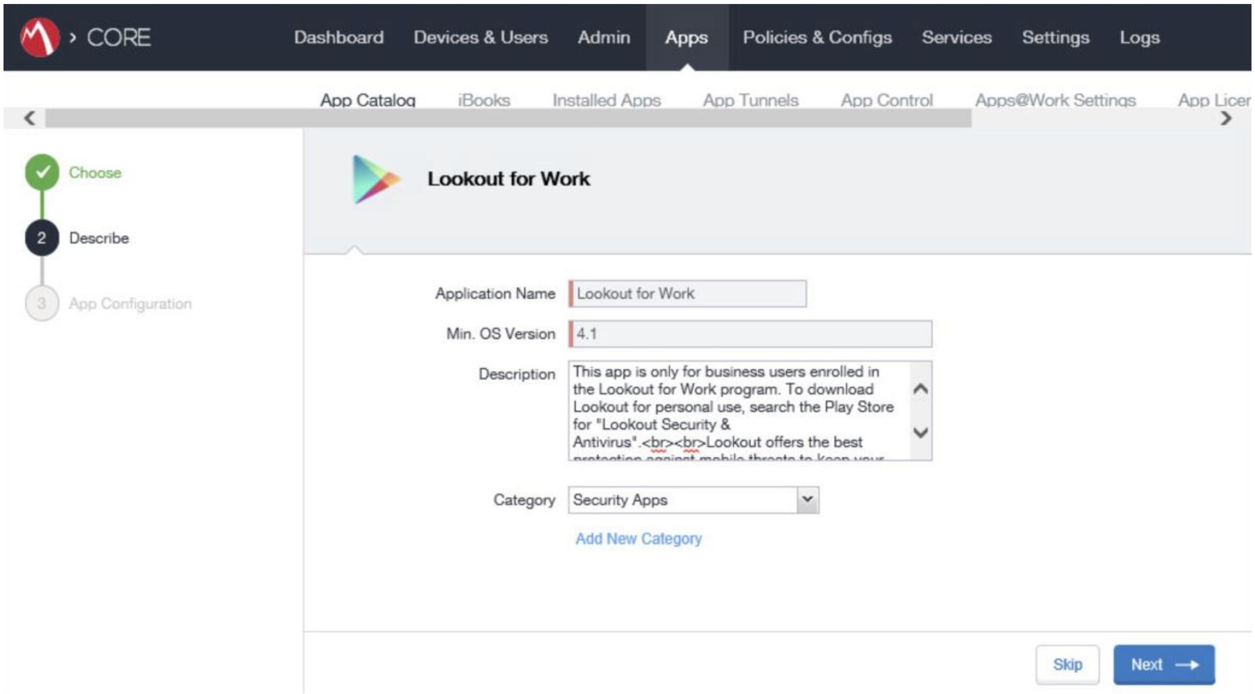
NAME	DESCRIPTION
Lookout for Work	This app is only for bu
Lookout Security & Antivirus	Introducing Safe Wi-F

4. On the **App Catalog > Describe** page:

   a. In **Category** drop-down menu, optionally assign the app to a category as appropriate to your MobileIron deployment strategy.

   b. Select **Next.**

Figure 2-98 Lookout for Work Application Configuration



Application Name: Lookout for Work

Min. OS Version: 4.1

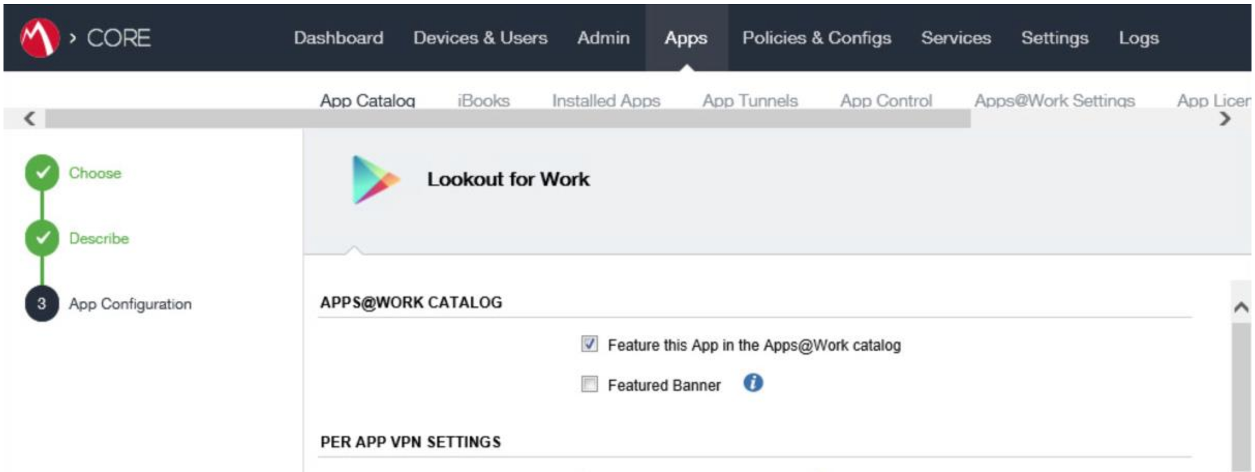
Description: This app is only for business users enrolled in the Lookout for Work program. To download Lookout for personal use, search the Play Store for "Lookout Security & Antivirus".

Lookout offers the best protection against mobile threats to keep your

Category: Security Apps

5. On the **App Catalog > App Configuration** page:
   a. In the **Apps@Work Catalog** section, Enable **Feature this App in the Apps@Work catalog.**

Figure 2-99 Lookout for Work Application Configuration



APPS@WORK CATALOG

☑ Feature this App in the Apps@Work catalog

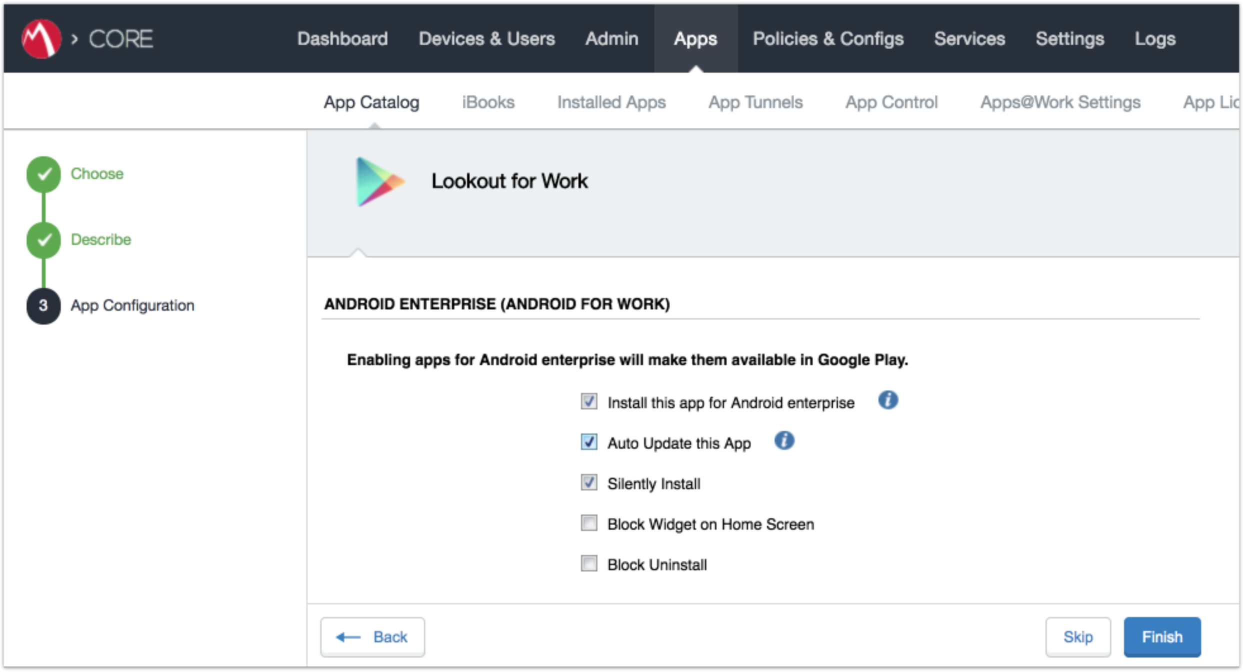
□ Featured Banner

   b. In the **Android Enterprise (Android for Work [AFW])** section:

   i. Enable **Install this app for Android enterprise**; additional controls will be made visible.
   ii. Enable **Auto Update this App.**
   iii. Ensure **Silently Install** is enabled.

  c. Select **Finish.**

Figure 2-100 Lookout for Work AFW Configuration



Lookout for Work

ANDROID ENTERPRISE (ANDROID FOR WORK)

Enabling apps for Android enterprise will make them available in Google Play.

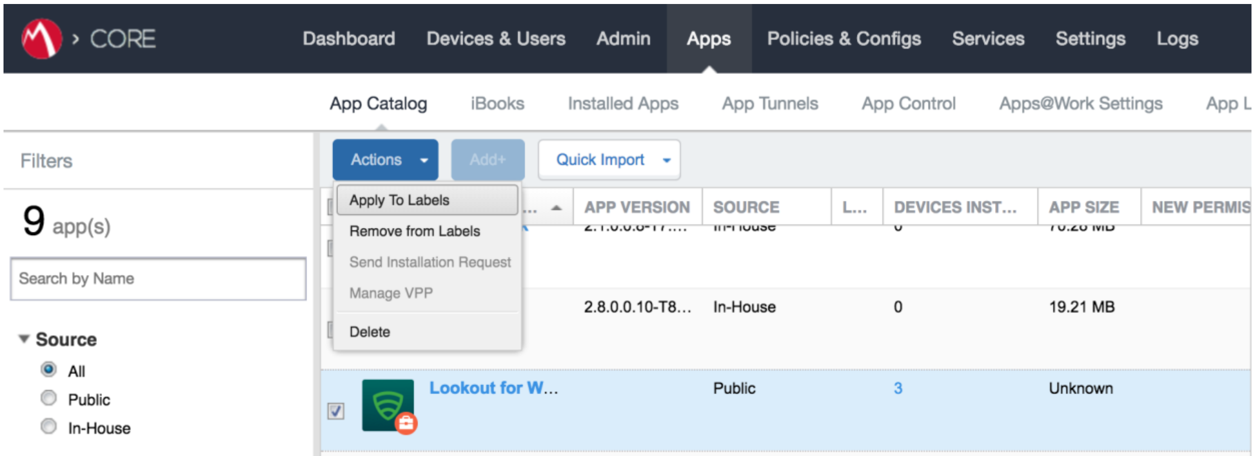
- ☑ Install this app for Android enterprise
- ☑ Auto Update this App
- ☑ Silently Install
- □ Block Widget on Home Screen
- □ Block Uninstall

6. The **Lookout for Work** app should now appear in the App Catalog with the AFW indicator.

2.7.4 Apply Labels to Lookout for Work for Android

1. On the **App Catalog** page:
   a. Enable Lookout for Work.
   b. Select **Actions > Apply To Labels**; the Apply To Labels dialogue will appear.

Figure 2-101 Apply Lookout for Work to Android Devices

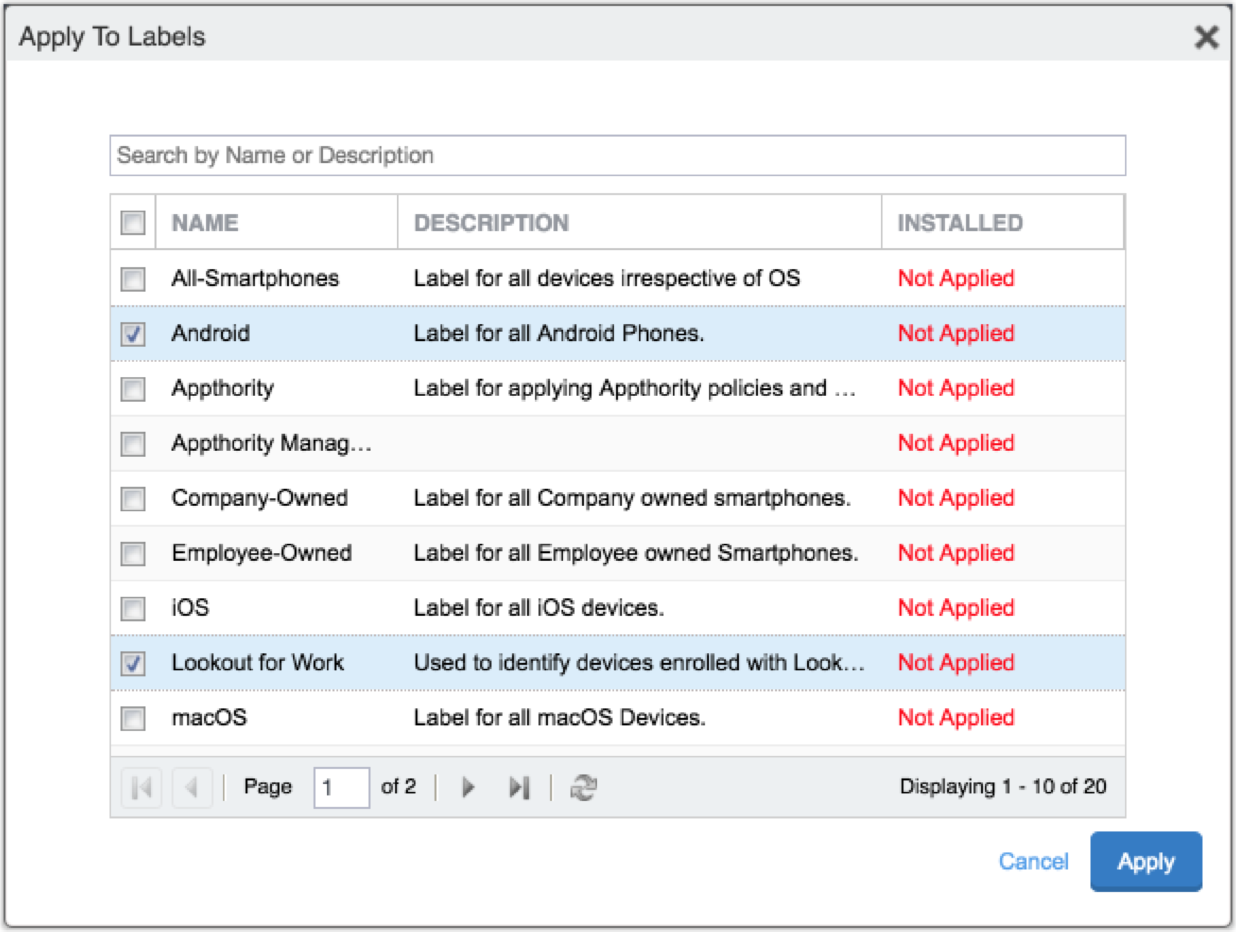


c. In the **Apply To Labels** dialogue:

i. Enable the **Lookout for Work** and **Android** labels, plus any other labels appropriate to your organization's mobile security policies.

ii. Select **Apply.**

1312 **Figure 2-102 Apply To Labels Dialogue**



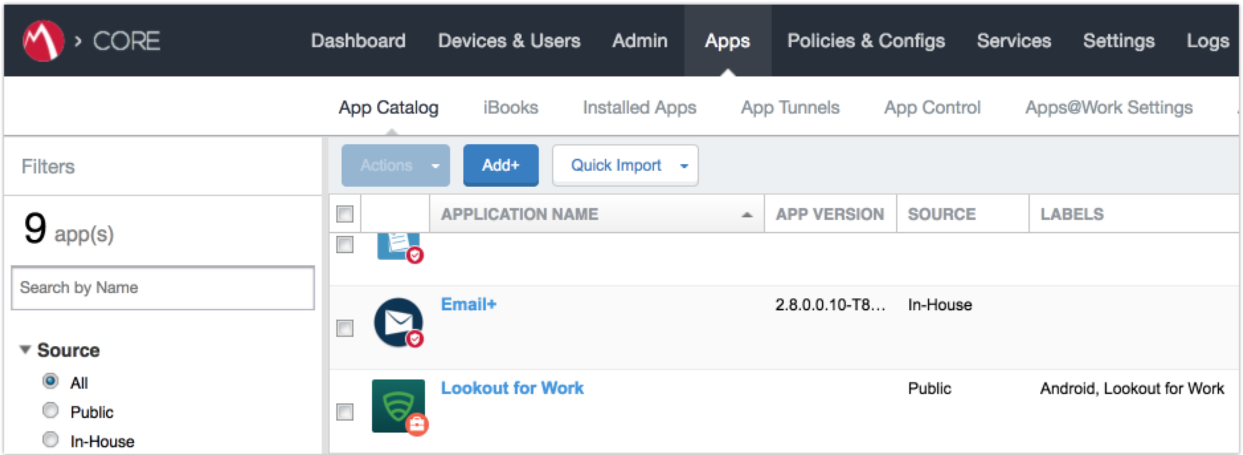
Apply To Labels

Search by Name or Description

☐	NAME	DESCRIPTION	INSTALLED
☐	All-Smartphones	Label for all devices irrespective of OS	Not Applied
☑	Android	Label for all Android Phones.	Not Applied
☐	Apppthority	Label for applying Apppthority policies and …	Not Applied
☐	Apppthority Manag…		Not Applied
☐	Company-Owned	Label for all Company owned smartphones.	Not Applied
☐	Employee-Owned	Label for all Employee owned Smartphones.	Not Applied
☐	iOS	Label for all iOS devices.	Not Applied
☑	Lookout for Work	Used to identify devices enrolled with Look…	Not Applied
☐	macOS	Label for all macOS Devices.	Not Applied

1313 d. The **Lookout for Work** app should now appear with the **Lookout for Work** and **Android**
1314 labels applied.

Figure 2-103 Lookout for Work with Applied Labels



□		APPLICATION NAME	APP VERSION	SOURCE	LABELS
□					
□		Email+	2.8.0.0.10-T8...	In-House	
□		Lookout for Work		Public	Android, Lookout for Work

2.7.5 Add Lookout for Work app for iOS to MobileIron App Catalog

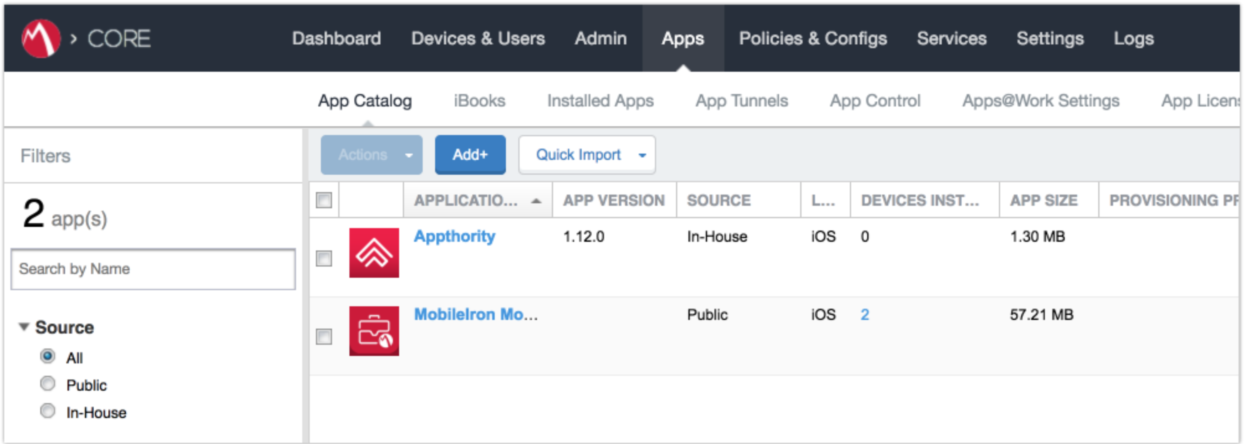
The following steps will add the Lookout for Work app for iOS to MobileIron, apply appropriate MobileIron labels, and create and upload a configuration file for one-touch activation of the app.

2.7.5.1 Import Lookout for Work App

1. In the **MobileIron Admin Portal**, navigate to **Apps > App Catalog**.

2. On the **App Catalog** page, select **Add**; this will start the workflow to add a new app to the app catalog.

Figure 2-104 MobileIron App Catalog



□		APPLICATIO...	APP VERSION	SOURCE	L...	DEVICES INST...	APP SIZE	PROVISIONING PF
□		Appthority	1.12.0	In-House	iOS	0	1.30 MB	
□		MobileIron Mo...		Public	iOS	2	57.21 MB	

3. On the **App Catalog > Choose** page:

a. Select **iTunes**; additional controls will be displayed.

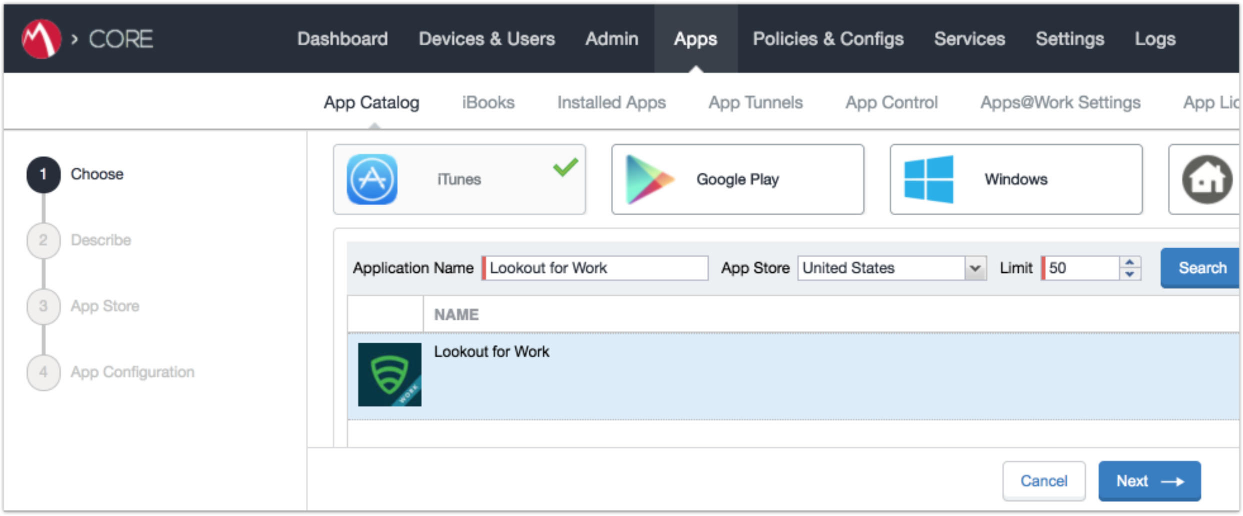
b. In the **Application Name** field, enter **Lookout for Work**.

c. Select **Search**; search results will be displayed in the lower pane.

d. In the list of search results, select the **Lookout for Work** app.

e. Select **Next**.

Figure 2-105 Lookout for Work Selected From iTunes



Application Name: Lookout for Work
App Store: United States
Limit: 50

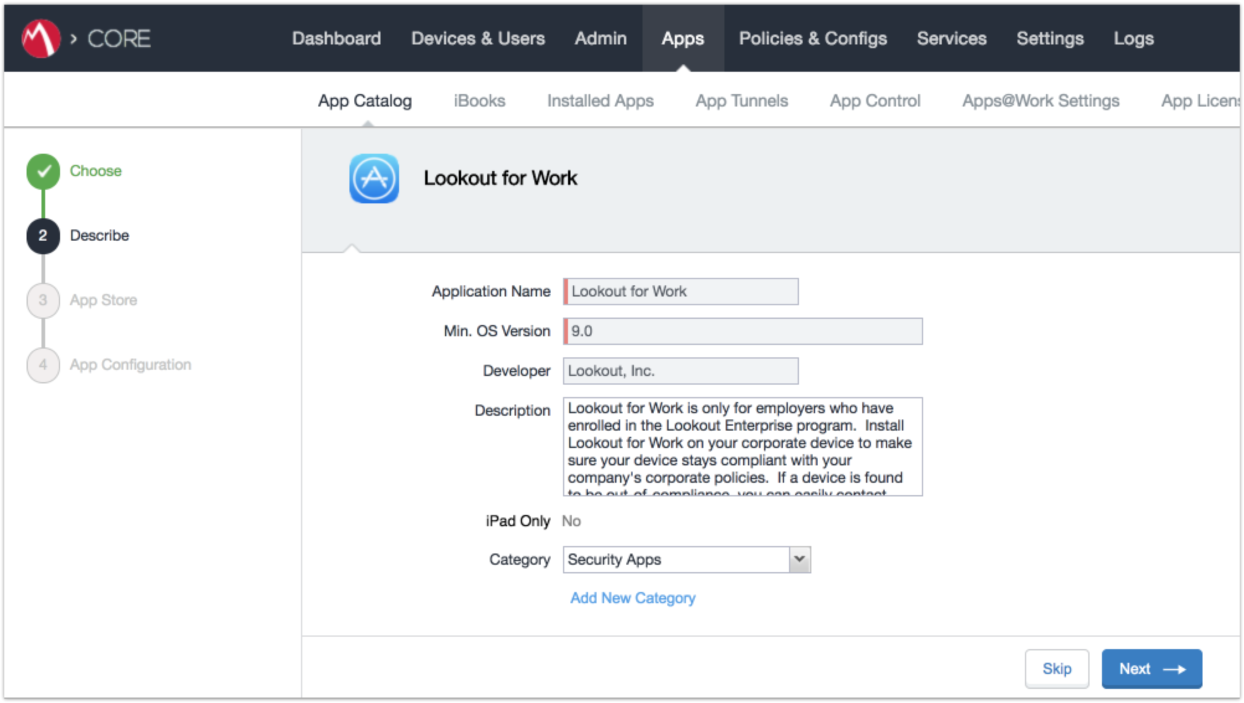
NAME
Lookout for Work

4. On the **App Catalog > Describe** page:

a. In **Category** drop-down menu, optionally assign the app to a category as appropriate to your MobileIron deployment strategy.

b. Select **Next**.

Figure 2-106 Lookout for Work App Configuration



Lookout for Work

Application Name: Lookout for Work

Min. OS Version: 9.0

Developer: Lookout, Inc.

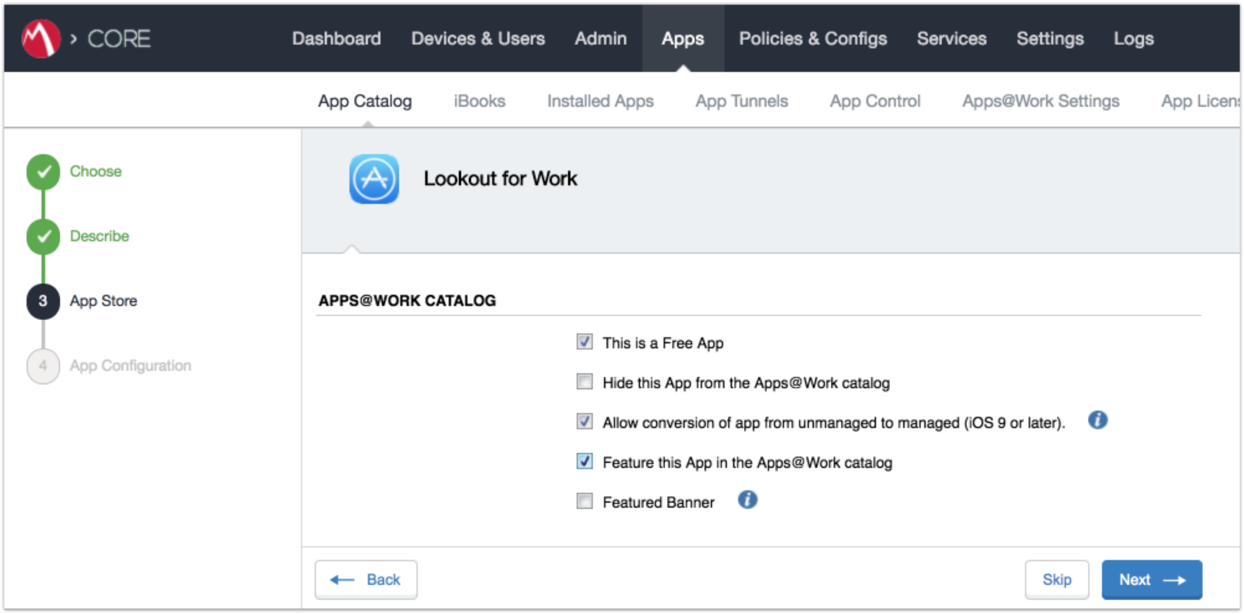
Description: Lookout for Work is only for employers who have enrolled in the Lookout Enterprise program. Install Lookout for Work on your corporate device to make sure your device stays compliant with your company's corporate policies. If a device is found to be out of compliance, you can easily contact

iPad Only: No

Category: Security Apps

5. On the **App Catalog > App Store** page:
   a. In the **Apps@Work Catalog** section:
      i. Enable **Allow conversion of app from unmanaged to managed (iOS 9 or later).**
      ii. Enable **Feature this App in the Apps@Work catalog.**
      iii. Select **Next.**

Figure 2-107 Lookout for Work App Configuration



APPS@WORK CATALOG

☑ This is a Free App

□ Hide this App from the Apps@Work catalog

☑ Allow conversion of app from unmanaged to managed (iOS 9 or later).

☑ Feature this App in the Apps@Work catalog

□ Featured Banner

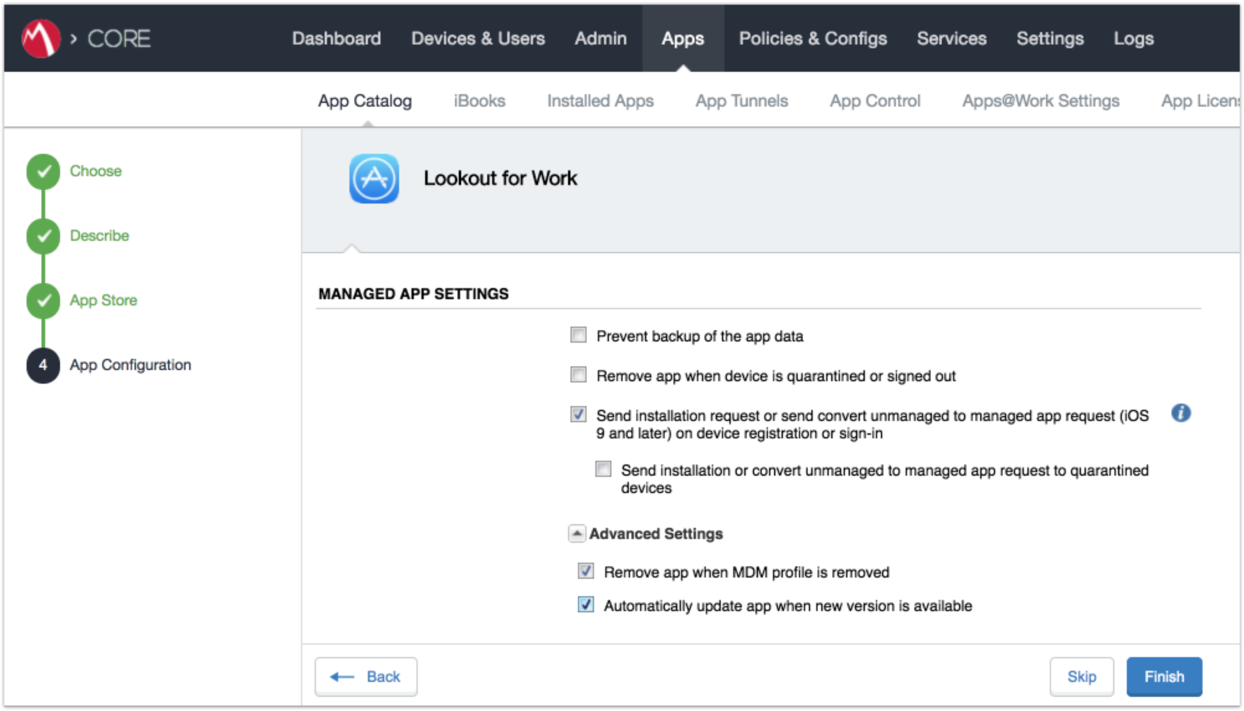
b. In the **App Catalog > App Configuration** section:

   i. Enable **Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in.**

   ii. Enable **Advanced Settings > Automatically update app when new version is available.**

c. Select **Finish**.

Figure 2-108 Lookout for Work Managed App Settings



Lookout for Work

MANAGED APP SETTINGS

☐ Prevent backup of the app data

☐ Remove app when device is quarantined or signed out

☑ Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in

☐ Send installation or convert unmanaged to managed app request to quarantined devices

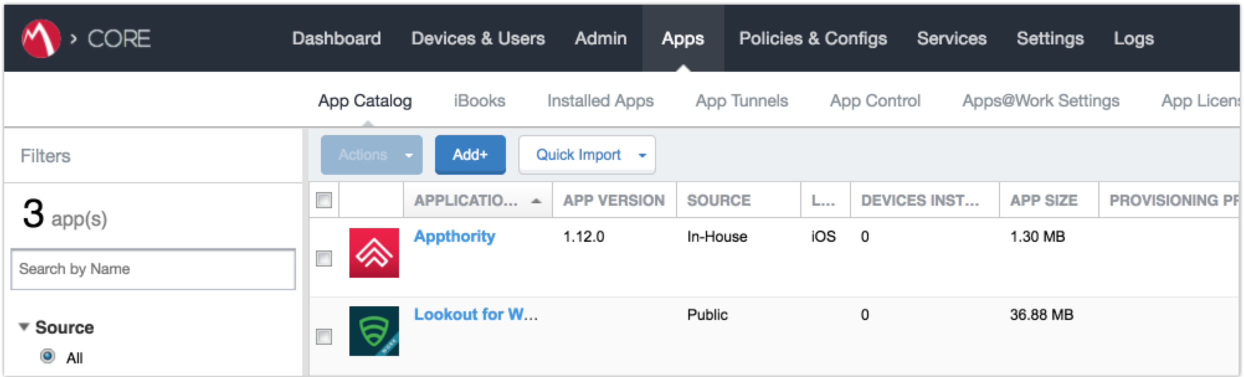
Advanced Settings

☑ Remove app when MDM profile is removed

☑ Automatically update app when new version is available

6. The **Lookout for Work** app should now appear in the App Catalog with AFW indicator.

Figure 2-109 App Catalog With Lookout for Work



3 app(s)

☐		APPLICATIO...	APP VERSION	SOURCE	L...	DEVICES INST...	APP SIZE	PROVISIONING PF
☐		Appthority	1.12.0	In-House	iOS	0	1.30 MB	
☐		Lookout for W...		Public		0	36.88 MB	

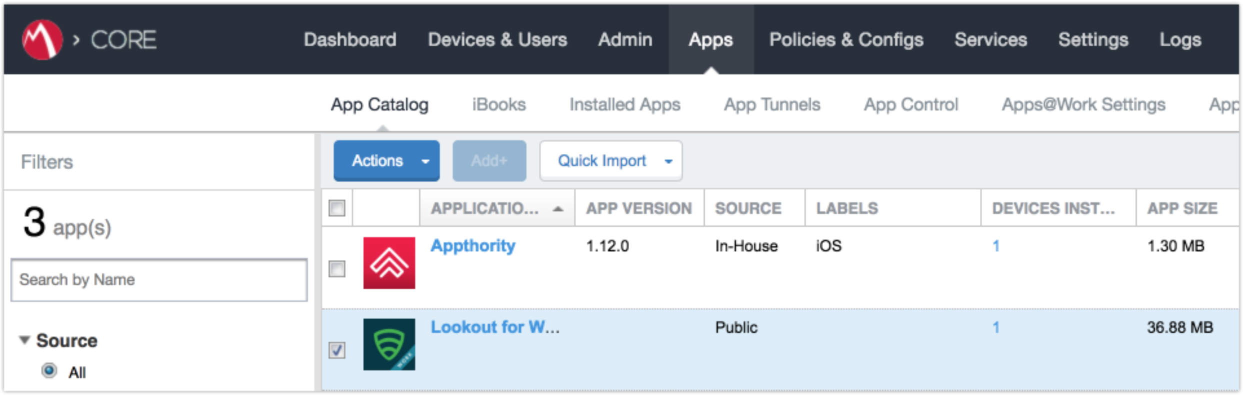
2.7.5.2 Apply MobileIron Labels to Lookout for Work App

1. On the **App Catalog** page:

   a. Enable Lookout for Work.

b. Select **Actions > Apply To Labels**; the Apply To Labels dialogue will appear.

Figure 2-110 Lookout for Work Selected



3 app(s)

Search by Name

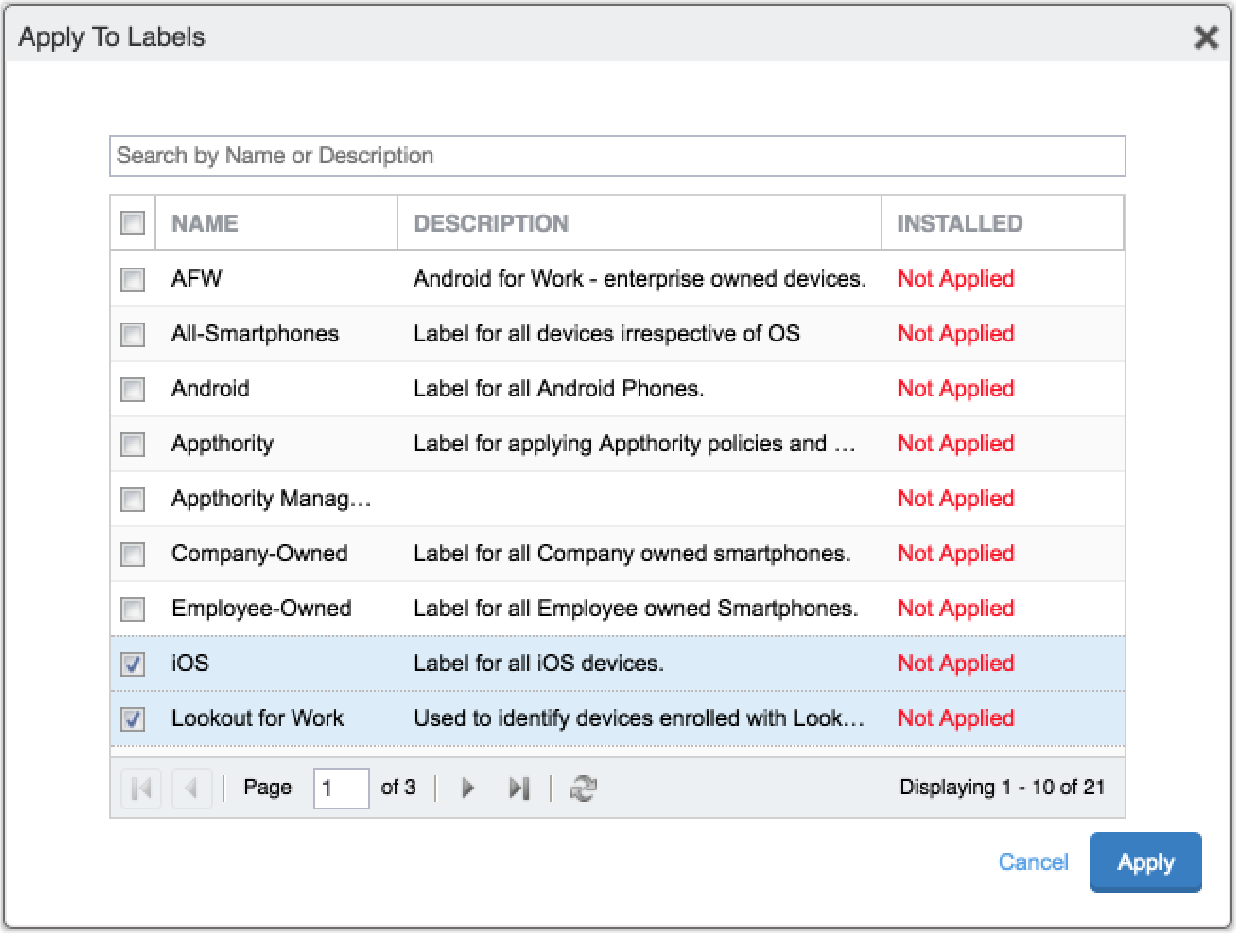
☐		APPLICATIO...	APP VERSION	SOURCE	LABELS	DEVICES INST...	APP SIZE
☐		Appthority	1.12.0	In-House	iOS	1	1.30 MB
☑		Lookout for W...		Public		1	36.88 MB

c. In the **Apply To Labels** dialogue:

i. Enable the **Lookout for Work** and **iOS** labels, plus any other labels appropriate to your organization's mobile security policies.

ii. Select **Apply.**

Figure 2-111 Apply To Labels Dialogue



Apply To Labels ✕

Search by Name or Description

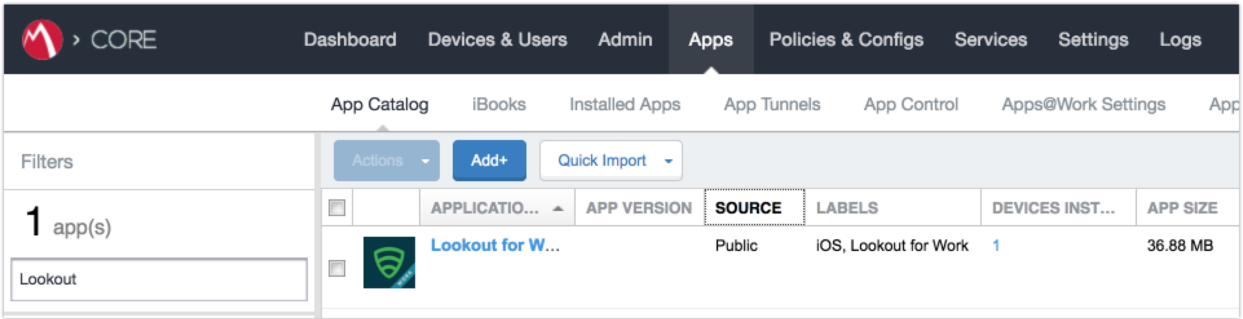
☐	NAME	DESCRIPTION	INSTALLED
☐	AFW	Android for Work - enterprise owned devices.	Not Applied
☐	All-Smartphones	Label for all devices irrespective of OS	Not Applied
☐	Android	Label for all Android Phones.	Not Applied
☐	Appthority	Label for applying Appthority policies and …	Not Applied
☐	Appthority Manag…		Not Applied
☐	Company-Owned	Label for all Company owned smartphones.	Not Applied
☐	Employee-Owned	Label for all Employee owned Smartphones.	Not Applied
☑	iOS	Label for all iOS devices.	Not Applied
☑	Lookout for Work	Used to identify devices enrolled with Look…	Not Applied

Page 1 of 3 Displaying 1 - 10 of 21

Cancel Apply

d. The **Lookout for Work** app should now appear with the Lookout for Work and iOS labels applied.

Figure 2-112 App Catalog With Lookout for Work



1 app(s)

Lookout

☐		APPLICATIO…	APP VERSION	SOURCE	LABELS	DEVICES INST…	APP SIZE
☐		Lookout for W…		Public	iOS, Lookout for Work	1	36.88 MB

2.7.5.3 Create Managed App Configuration File for Lookout for Work

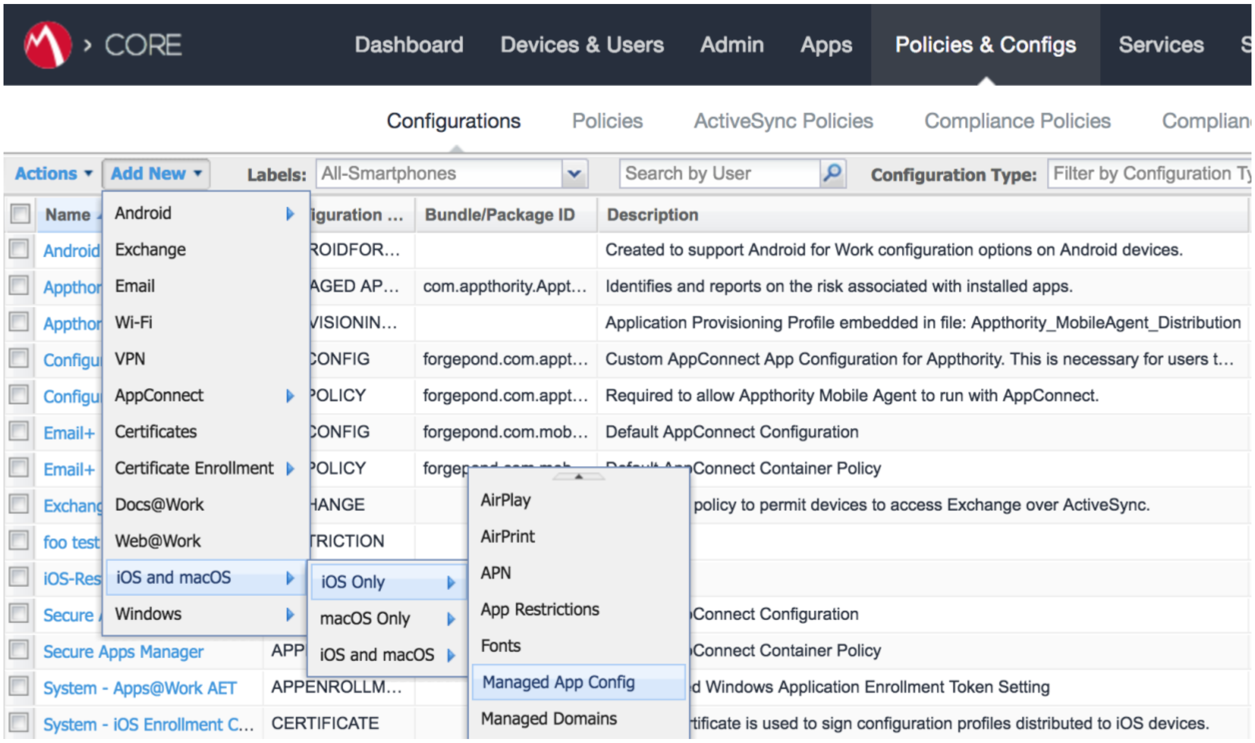
MobileIron can push a configuration file down to managed iOS devices to allow users easy activation of Lookout for Work. The following steps will create and upload the necessary file.

1. Using a **plain text** editor, create the following text file by **replacing the asterisks on line 13** with your organization's Global Enrollment Code.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"https://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>MDM</key>
    <string>MOBILEIRON</string>
    <key>DEVICE_UDID</key>
    <string>$DEVICE_UDID$</string>
    <key>EMAIL</key>
    <string>$EMAIL$</string>
    <key>GLOBAL_ENROLLMENT_CODE</key>
    <string>*******</string>
  </dict>
</plist>
```

2. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.
3. On the **Configurations** Page:
   a. Select **Add New > iOS and OS X > iOS Only > Managed App Config**; the New Managed App Config Setting dialogue will open.

1389 **Figure 2-113 Importing Managed Application Configuration**



Name	iguration ...	Bundle/Package ID	Description
Android	ROIDFOR...		Created to support Android for Work configuration options on Android devices.
Appthor	AGED AP...	com.appthority.Appt...	Identifies and reports on the risk associated with installed apps.
Appthor	VISIONIN...		Application Provisioning Profile embedded in file: Appthority_MobileAgent_Distribution
Configu	CONFIG	forgepond.com.appt...	Custom AppConnect App Configuration for Appthority. This is necessary for users t...
Configu	POLICY	forgepond.com.appt...	Required to allow Appthority Mobile Agent to run with AppConnect.
Email+	CONFIG	forgepond.com.mob...	Default AppConnect Configuration
Email+	POLICY	forgep	Connect Container Policy
Exchang	HANGE		policy to permit devices to access Exchange over ActiveSync.
foo test	TRICTION		
iOS-Res			
Secure			Connect Configuration
Secure Apps Manager	APP		Connect Container Policy
System - Apps@Work AET	APPENROLLM...		d Windows Application Enrollment Token Setting
System - iOS Enrollment C...	CERTIFICATE		tificate is used to sign configuration profiles distributed to iOS devices.

1390 b. In the **Managed App Config Setting** dialogue:

1391 i. In the **Name** field, provide a name for this configuration; our implementation
1392 used **Activate Lookout**.

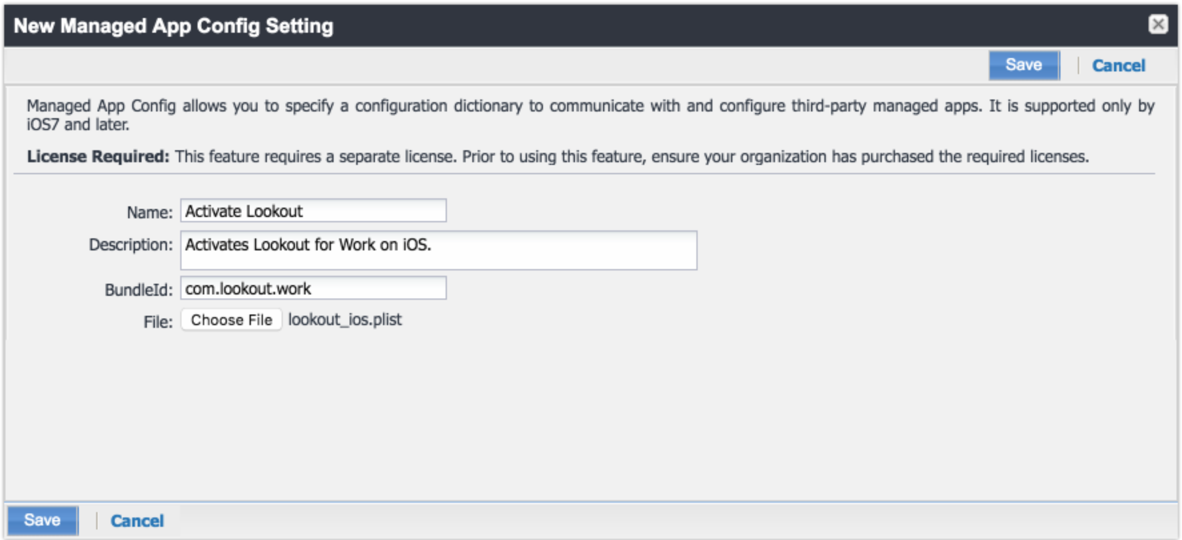
1393 ii. In the **Description** field, provide the purpose for this configuration.

1394 iii. In the **BundleId** field, enter the bundle ID for Lookout at Work, which for our
1395 version was **com.lookout.work**.

1396 iv. Select **Choose File...** to upload the plist file created during **Step 1.**

1397 v. Select **Save.**

Figure 2-114 plist Import Configuration



Managed App Config allows you to specify a configuration dictionary to communicate with and configure third-party managed apps. It is supported only by iOS7 and later.

License Required: This feature requires a separate license. Prior to using this feature, ensure your organization has purchased the required licenses.

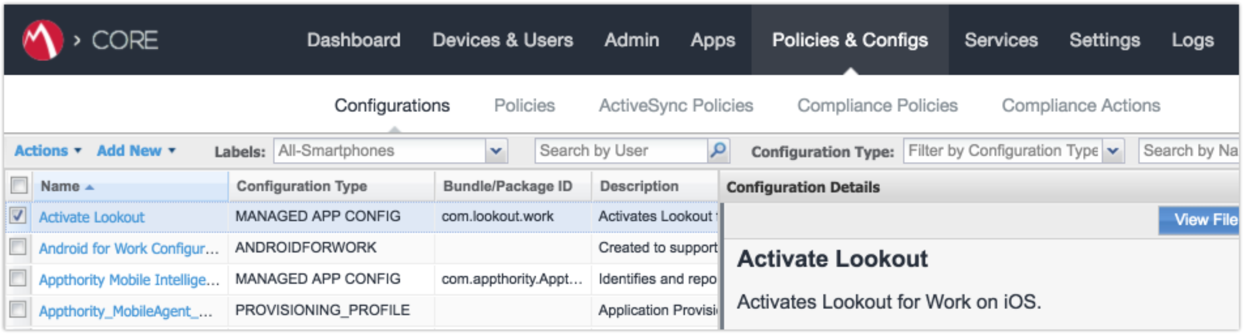
Name: Activate Lookout
Description: Activates Lookout for Work on iOS.
BundleId: com.lookout.work
File: Choose File lookout_ios.plist

2.7.5.4 Apply Labels to Managed App Configuration for Lookout for Work

The following steps will apply the managed app configuration created in the previous section to labels.

1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.
2. On the **Configurations** page:
   a. Enable the **Lookout Activation** managed app configuration created in the previous section.
   b. Select **Actions > Apply To Label**; the Apply To Label dialogue will open.

Figure 2-115 Lookout Configuration Selected



Labels: All-Smartphones
Configuration Type: Filter by Configuration Type

	Name	Configuration Type	Bundle/Package ID	Description
☑	Activate Lookout	MANAGED APP CONFIG	com.lookout.work	Activates Lookout
□	Android for Work Configur...	ANDROIDFORWORK		Created to support
□	Appthority Mobile Intellige...	MANAGED APP CONFIG	com.appthority.Appt...	Identifies and repo
□	Appthority_MobileAgent_...	PROVISIONING_PROFILE		Application Provisi

Configuration Details

Activate Lookout

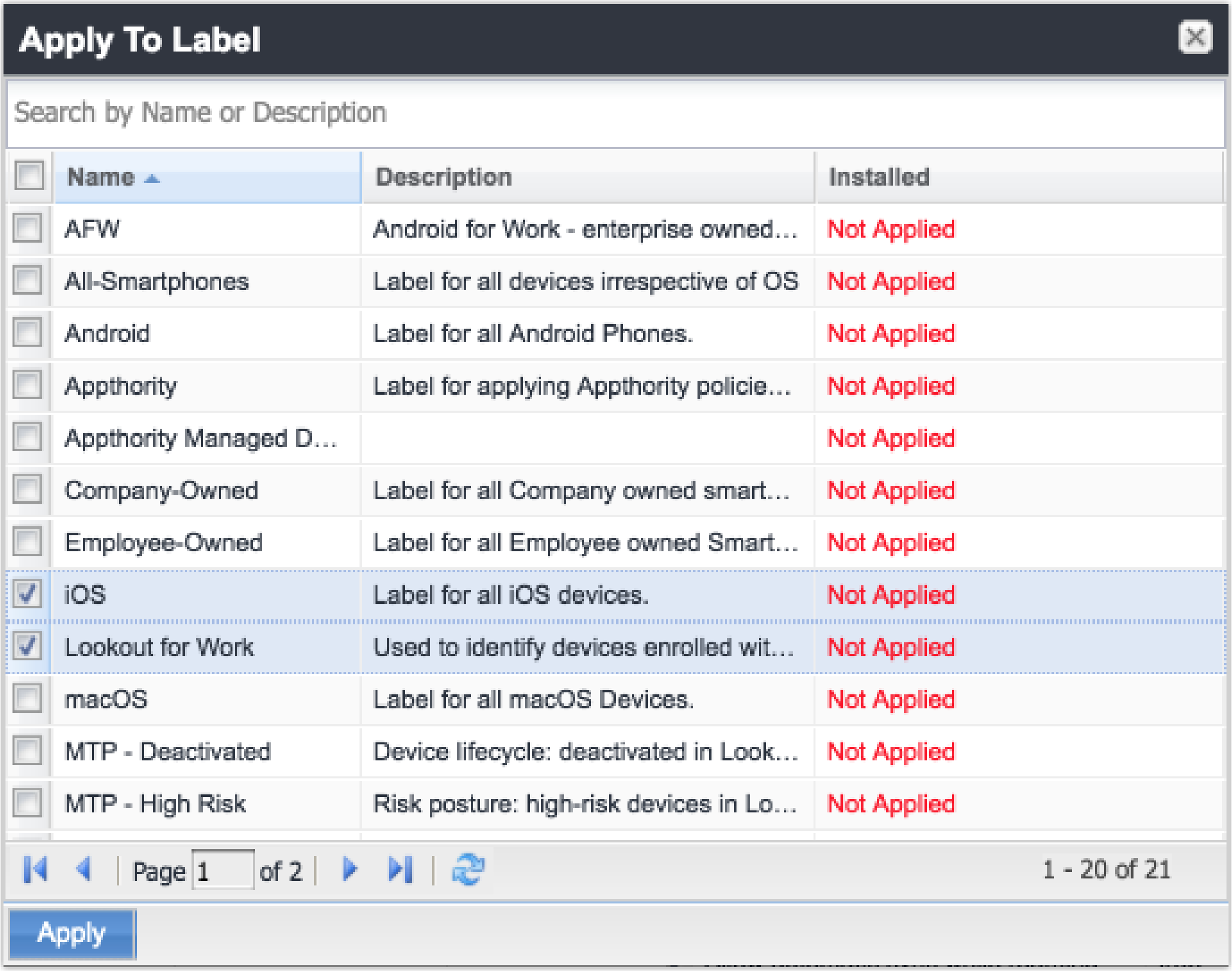
Activates Lookout for Work on iOS.

   c. In the **Apply To Label** dialogue:

i. Enable the iOS and Lookout for Work labels.

ii. Select **Apply.**

Figure 2-116 Apply To Label Dialogue



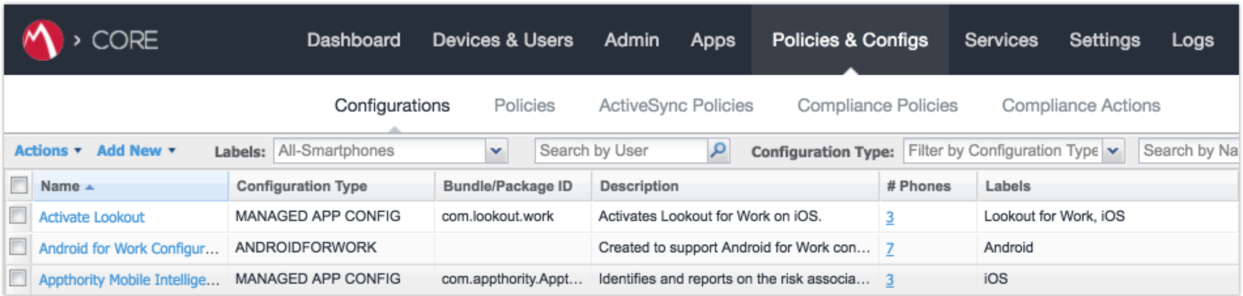
Apply To Label

Search by Name or Description

☐	Name ▲	Description	Installed
☐	AFW	Android for Work - enterprise owned…	Not Applied
☐	All-Smartphones	Label for all devices irrespective of OS	Not Applied
☐	Android	Label for all Android Phones.	Not Applied
☐	Appthority	Label for applying Appthority policie…	Not Applied
☐	Appthority Managed D…		Not Applied
☐	Company-Owned	Label for all Company owned smart…	Not Applied
☐	Employee-Owned	Label for all Employee owned Smart…	Not Applied
☑	iOS	Label for all iOS devices.	Not Applied
☑	Lookout for Work	Used to identify devices enrolled wit…	Not Applied
☐	macOS	Label for all macOS Devices.	Not Applied
☐	MTP - Deactivated	Device lifecycle: deactivated in Look…	Not Applied
☐	MTP - High Risk	Risk posture: high-risk devices in Lo…	Not Applied

d. The system should now reflect the **Lookout for iOS** and **iOS** labels have been applied to the **Activate Lookout** configuration.

Figure 2-117 Lookout Configuration With Labels



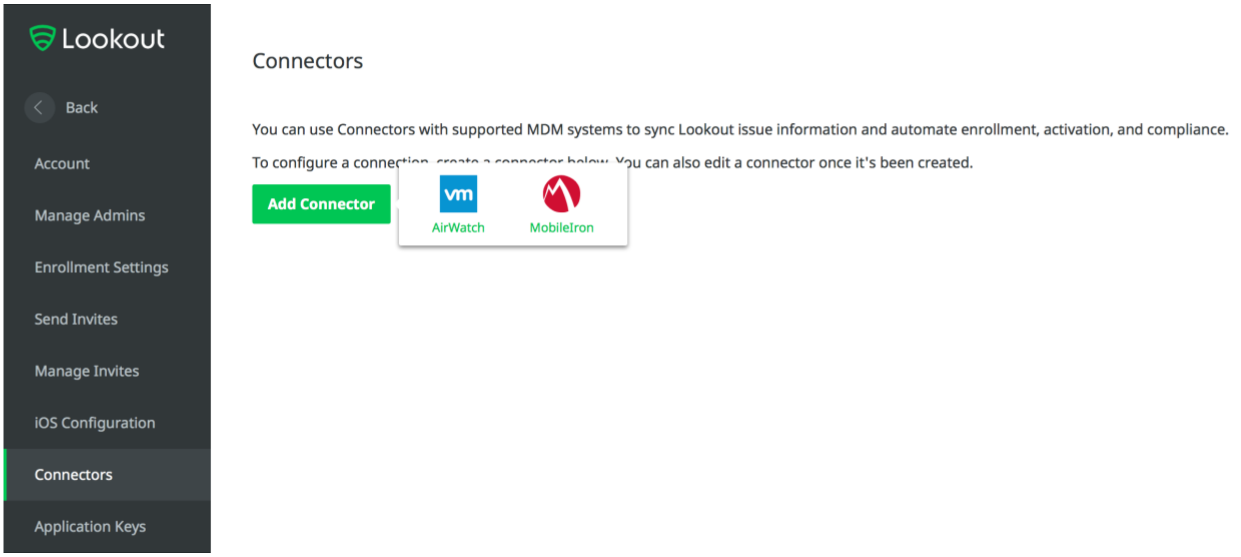
□	Name ▴	Configuration Type	Bundle/Package ID	Description	# Phones	Labels
□	Activate Lookout	MANAGED APP CONFIG	com.lookout.work	Activates Lookout for Work on iOS.	3	Lookout for Work, iOS
□	Android for Work Configur…	ANDROIDFORWORK		Created to support Android for Work con…	7	Android
□	Apptthority Mobile Intellige…	MANAGED APP CONFIG	com.appthority.Appt…	Identifies and reports on the risk associa…	3	iOS

2.7.6 Add MDM Connector for MobileIron to Lookout MES

The following instructions will connect Lookout with your MobileIron instance and associate Lookout device states with the MobileIron labels created previously.

1. Using the most-recent version of *MDM Service IP Whitelisting* available from the Lookout support portal, configure your organization's firewalls to permit inbound connections from the IP addresses provided on port 443 to your instance of MobileIron Core.
2. In the **Lookout MES portal**, navigate to **Lookout > System > Connectors**.
3. On the **Connectors** page:
   a. Select **Add Connector > MobileIron**; this will open a new form.

Figure 2-118 Add Lookout Connector Display



Connectors

You can use Connectors with supported MDM systems to sync Lookout issue information and automate enrollment, activation, and compliance.

To configure a connection, create a connector below. You can also edit a connector once it's been created.

b. In the **Connector Settings** section of the form:

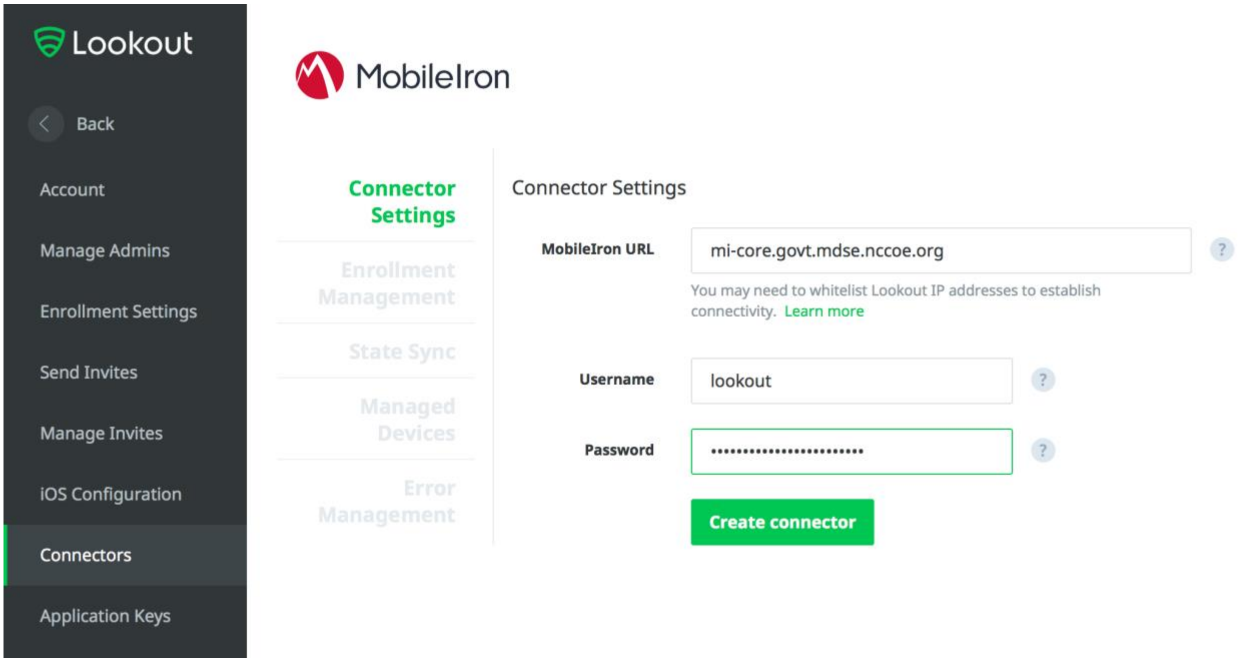
i. For the **MobileIron URL** field, enter the FQDN for your instance of MobileIron. In our example implementation, the URL was **mi-core.govt.mdse.nccoe.org.**

ii. For the **Username** field, enter the User ID of the MobileIron admin account created in 2.7.1. In our example implementation, the **User ID** is **lookout.**

iii. For the **Password** field, enter the password associated with that MobileIron admin account.

iv. Select **Create Connector**; this will enable additional sections of the form.

Figure 2-119 Connector Settings



Connector Settings

MobileIron URL: mi-core.govt.mdse.nccoe.org

You may need to whitelist Lookout IP addresses to establish connectivity. Learn more

Username: lookout

Password: ••••••••••••••••••••••••

c. In the **Enrollment Management** section of the form:

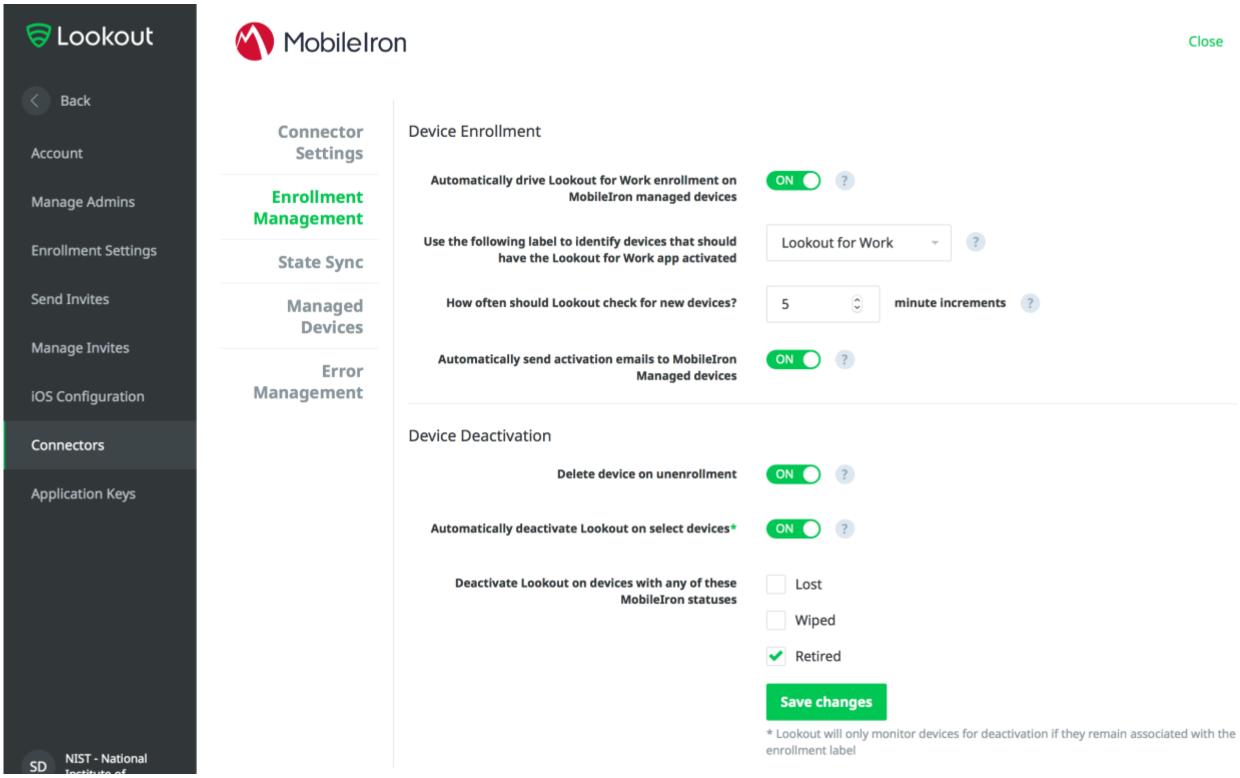
i. Toggle **Device Enrollment > Automatically** drive Lookout for Work enrollment on MobileIron managed devices to **On.**

ii. For the **Device Enrollment > Use the following label to identify devices that should have the Lookout for Work app activated** drop-down menu, select the **Lookout for Work** label.

iii. Toggle **Device Enrollment > Automatically send activation emails to MobileIron managed devices** to **On.**

iv. Select **Save Changes.**

Figure 2-120 Connector Enrollment Settings



Device Enrollment

Automatically drive Lookout for Work enrollment on MobileIron managed devices: ON

Use the following label to identify devices that should have the Lookout for Work app activated: Lookout for Work

How often should Lookout check for new devices? 5 minute increments

Automatically send activation emails to MobileIron Managed devices: ON

Device Deactivation

Delete device on unenrollment: ON

Automatically deactivate Lookout on select devices*: ON

Deactivate Lookout on devices with any of these MobileIron statuses:

☐ Lost

☐ Wiped

☑ Retired

Save changes

* Lookout will only monitor devices for deactivation if they remain associated with the enrollment label

d. In the **State Sync** section of the form:

i. Toggle **State Sync > Synchronize Device Status to MobileIron** to **On**.

ii. For each entry in the table below:

1) Toggle the control to **On.**

2) From the drop-down menu, select the **MobileIron Label** with the associated Purpose from the table in **Section 2.6.2 Add MobileIron Labels for Lookout.** We provide the Label Name we used for each Purpose in our example implementation.

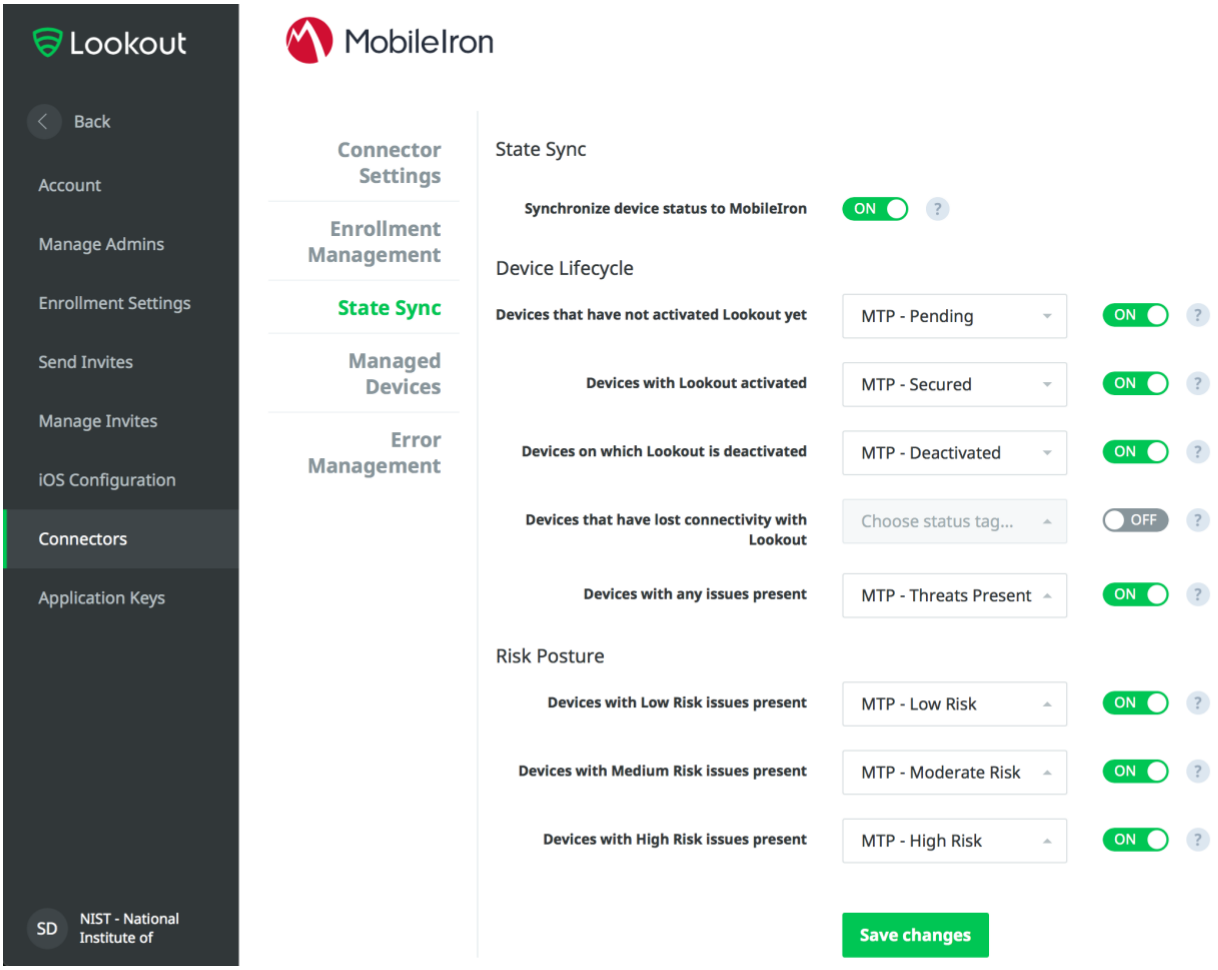
State	Purpose	Label Name
Devices that have not activated Lookout yet	Lifecycle management: devices with Lookout not yet activated	MTP - Pending

Devices with Lookout activated	Lifecycle management: devices with Lookout activated	MTP - Secured
Devices on which Lookout is deactivated	Lifecycle management: devices with Lookout deactivated	MTP - Deactivated
Devices with any issues present	Lifecycle management: devices with threats detected by Lookout	MTP - Threats Detected
Devices with Low Risk issues present	Risk posture: devices with a low risk score in Lookout	MTP - Low Risk
Devices with Medium Risk issues present	Risk posture: devices with a moderate risk score in Lookout	MTP - Moderate Risk
Devices with High Risk issues present	Risk posture: devices with a high risk score in Lookout	MTP - High Risk

Note: Administrators can choose to alter the label names to something more appropriate for their environment.

iii. Select **Save Changes**.

Figure 2-121 Connector Sync Settings



State Sync

Synchronize device status to MobileIron: ON

Device Lifecycle

Devices that have not activated Lookout yet	MTP - Pending	ON
Devices with Lookout activated	MTP - Secured	ON
Devices on which Lookout is deactivated	MTP - Deactivated	ON
Devices that have lost connectivity with Lookout	Choose status tag...	OFF
Devices with any issues present	MTP - Threats Present	ON

Risk Posture

Devices with Low Risk issues present	MTP - Low Risk	ON
Devices with Medium Risk issues present	MTP - Moderate Risk	ON
Devices with High Risk issues present	MTP - High Risk	ON

2.7.7 Configure MobileIron Risk Response

The following steps will allow MobileIron to generate responses to various device states as assigned to devices by Lookout (e.g. MTP - High Risk).

2.7.7.1 Add MobileIron App Control Rule

1. In the **MobileIron Admin Portal**, navigate to **Apps > App Control**.
2. Select **Add**; the Add App Control Rule dialogue will appear.
3. In the **Add App Control Rule** dialogue:
    a. In the **Name** field, enter **Threats Present Trigger**.

b. Of the **Type** options, select **Required.**

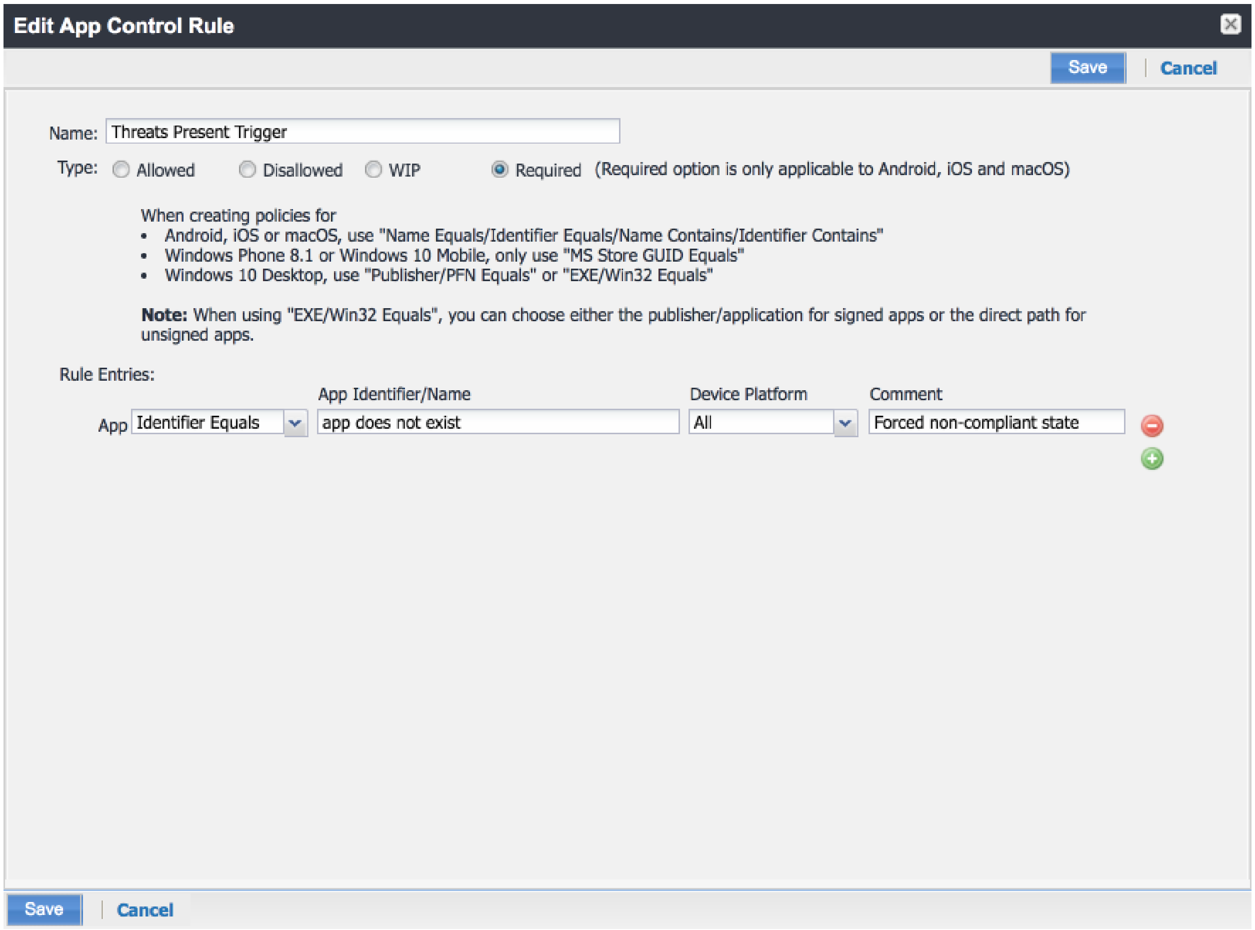
c. In the **App Identifier/Name** field enter **app does not exist.**

d. In the **Device Platform** drop-down menu, select **All**.

e. In the **Comment** field, optionally enter **Forces non-compliant state.**

f. Select **Save.**

Figure 2-122 MobileIron App Control Rule



Name: Threats Present Trigger

Type: ○ Allowed ○ Disallowed ○ WIP ● Required (Required option is only applicable to Android, iOS and macOS)

When creating policies for

- Android, iOS or macOS, use "Name Equals/Identifier Equals/Name Contains/Identifier Contains"
- Windows Phone 8.1 or Windows 10 Mobile, only use "MS Store GUID Equals"
- Windows 10 Desktop, use "Publisher/PFN Equals" or "EXE/Win32 Equals"

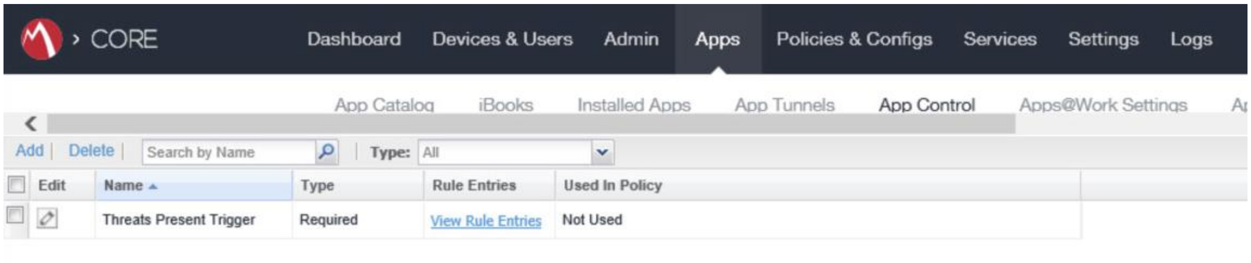
Note: When using "EXE/Win32 Equals", you can choose either the publisher/application for signed apps or the direct path for unsigned apps.

Rule Entries:

	App Identifier/Name	Device Platform	Comment
App Identifier Equals	app does not exist	All	Forced non-compliant state

4. The new app control rule should now appear on the **Apps > App Control** page.

Figure 2-123 MobileIron App Control Rule



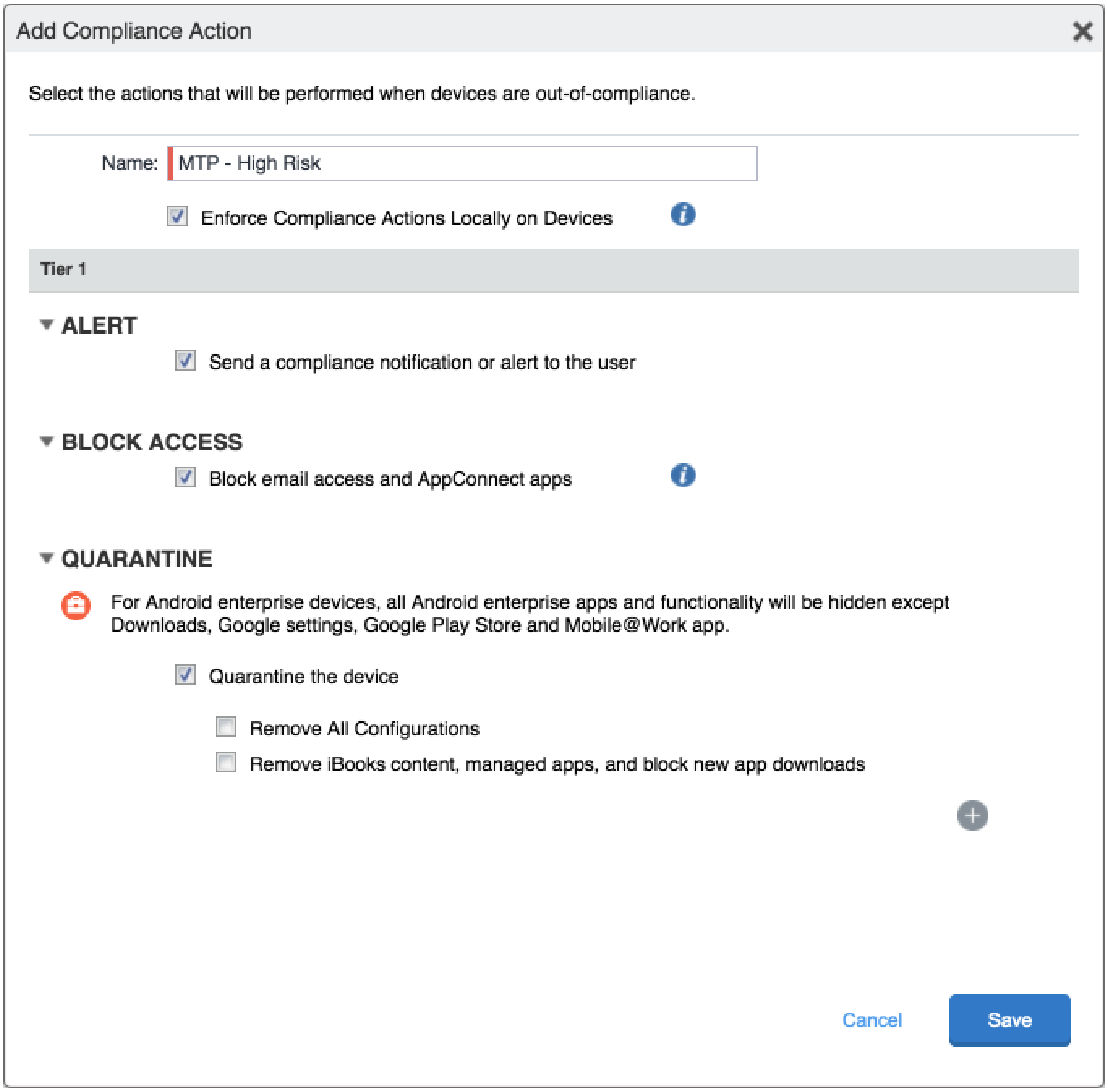
□	Edit	Name	Type	Rule Entries	Used In Policy
□		Threats Present Trigger	Required	View Rule Entries	Not Used

2.7.7.2 Add MobileIron Compliance Actions

A Compliance Action defines what actions MobileIron will take when an App Control policy, like the one created in the previous section, is violated by a managed mobile device. The following steps will create and configure an example Compliance Action in response to the MTP - High Risk App Control rule. Note that a single Compliance Action can be associated with multiple App Control rules if the same response would be configured for each. Otherwise, a new Compliance Action should be created.

1. In the **MobileIron Admin Portal,** navigate to **Policies & Configs > Compliance Actions.**
2. Select **Add;** the **Add Compliance Action** dialogue will open.
3. In the **Add Compliance Action** dialogue:
   a. In the **Name** field, add a description of the compliance action; we recommend indicating the kind of action taken. This example illustrates creating a compliance action that will be associated with the **MTP - High Risk** label.
   b. Select the **Enforce Compliance Actions Locally on Devices** check box.
   c. Select the **Send a compliance notification or alert to the user** check box.
   d. Select the **Block email access and AppConnect apps** check box.
   e. Select the **Quarantine the device** check box.
   f. Deselect the **Remove All Configurations** check box.
   g. Select **Save.**

Figure 2-124 MTP High Risk Compliance Action



Add Compliance Action

Select the actions that will be performed when devices are out-of-compliance.

Name: MTP - High Risk

☑ Enforce Compliance Actions Locally on Devices

Tier 1

ALERT

☑ Send a compliance notification or alert to the user

BLOCK ACCESS

☑ Block email access and AppConnect apps

QUARANTINE

For Android enterprise devices, all Android enterprise apps and functionality will be hidden except Downloads, Google settings, Google Play Store and Mobile@Work app.

☑ Quarantine the device

□ Remove All Configurations

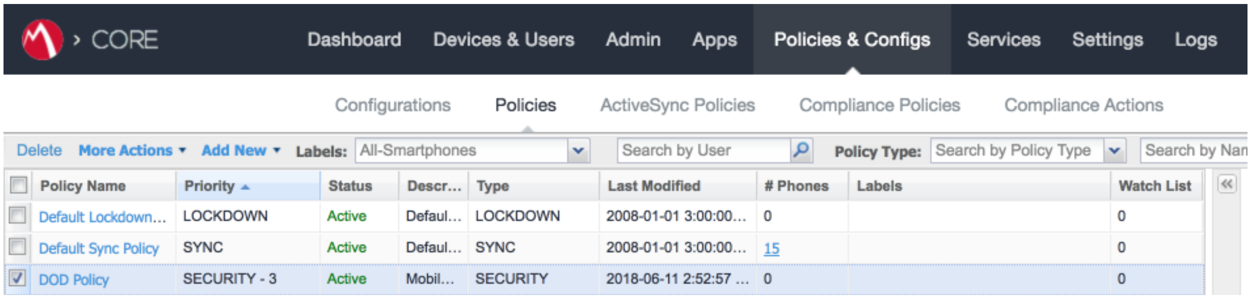
□ Remove iBooks content, managed apps, and block new app downloads

2.7.7.3 Create MobileIron Security Policy for Lookout MES

In addition to potentially defining other controls, such as password requirements, a Security Policy can map a Compliance Action to an App Control rule, enabling MobileIron to execute the configured actions whenever a device that applies the policy violates the App Control rule. The following steps will create a new Security Policy for Lookout MES High Risk devices using an existing policy as a baseline from which to apply more stringent controls.

1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Policies.**
2. On the **Policies** page:
    a. Select the security policy to use as a baseline.
    b. Select **More Actions > Save As**; this will open the **New Security Policy** dialogue.

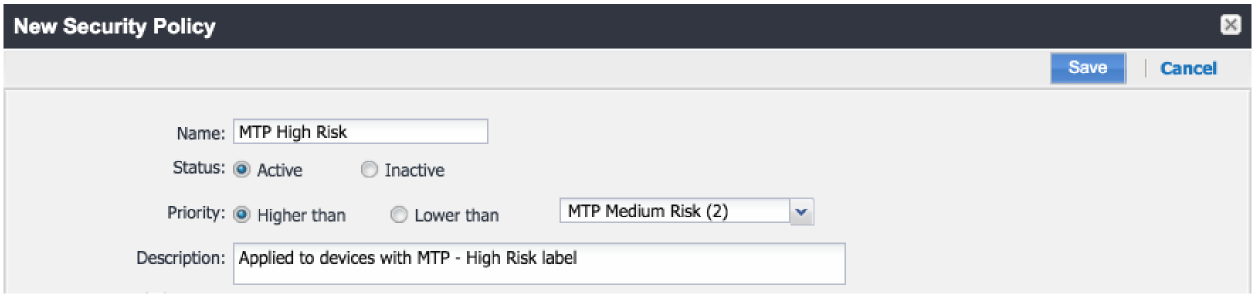
Figure 2-125 Baseline Policy Selection



□	Policy Name	Priority ▲	Status	Descr...	Type	Last Modified	# Phones	Labels	Watch List
□	Default Lockdown...	LOCKDOWN	Active	Defaul...	LOCKDOWN	2008-01-01 3:00:00...	0		0
□	Default Sync Policy	SYNC	Active	Defaul...	SYNC	2008-01-01 3:00:00...	15		0
☑	DOD Policy	SECURITY - 3	Active	Mobil...	SECURITY	2018-06-11 2:52:57 ...	0		0

    c. In the **New Security Policy** dialogue:
        i. In the **Name** field, rename the policy to **MTP - High Risk.**
        ii. In the **Priority** drop-down menu, select the security policy this policy will be prioritized in relation to; in this example, it is higher than the **MTP Medium Risk** policy. **Note:** for ease of setting priority, it is recommended to add new security policies in ascending order (lowest to highest priority).

Figure 2-126 MTP High Risk Policy



Name: MTP High Risk

Status: ● Active ○ Inactive

Priority: ● Higher than ○ Lower than MTP Medium Risk (2)

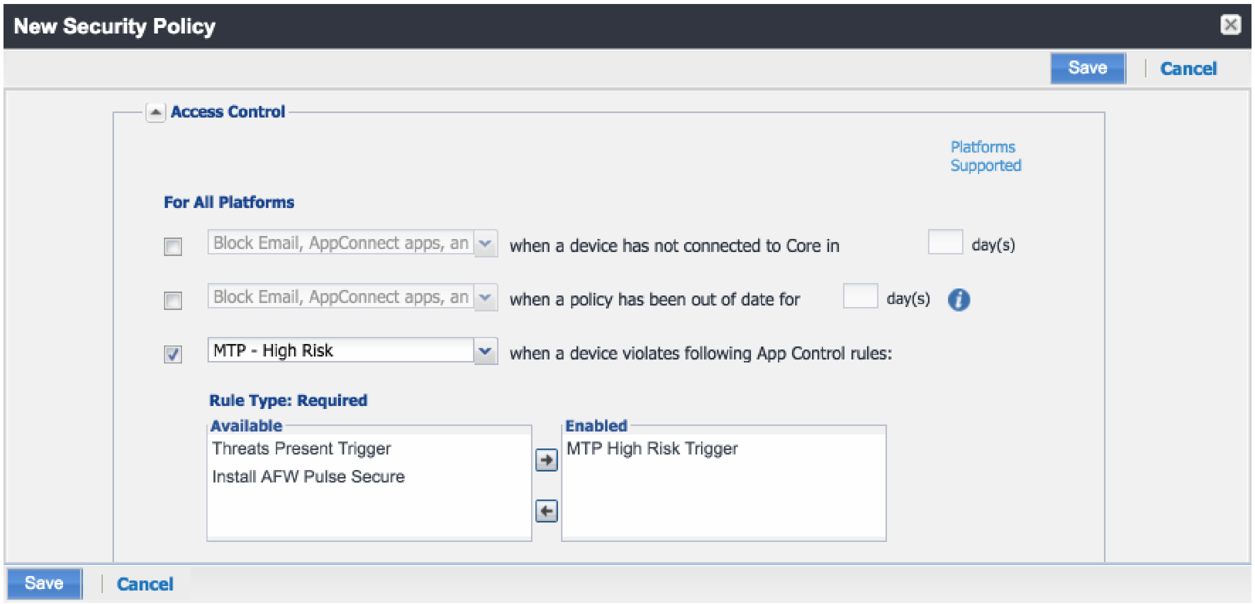
Description: Applied to devices with MTP - High Risk label

        iii. Under **Access Control > For All Platforms** section:

1. For the **when a device violates the following app control rules** drop-down menu, select the **MTP - High Risk** compliance action.
2. In the **Available** list of app control rules, highlight **MTP High Risk Trigger.**
3. Select the **right arrow** to move MTP High Risk Trigger item into the **Enabled List.**

iv. Select **Save.**

Figure 2-127 Security Policy Trigger



New Security Policy

Save | Cancel

Access Control

Platforms Supported

For All Platforms

☐ Block Email, AppConnect apps, an when a device has not connected to Core in day(s)

☐ Block Email, AppConnect apps, an when a policy has been out of date for day(s)

☑ MTP - High Risk when a device violates following App Control rules:

Rule Type: Required

Available	Enabled
Threats Present Trigger	MTP High Risk Trigger
Install AFW Pulse Secure	

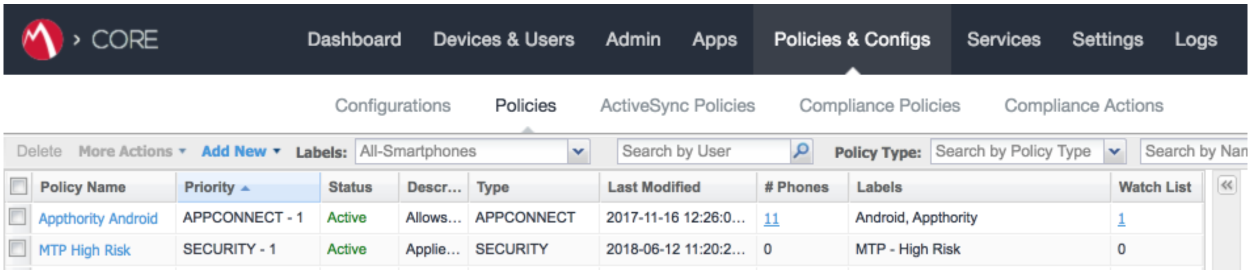
Save | Cancel

2.7.7.4 Apply Lookout MES Label to MobileIron Security Policy

The following steps will apply the MTP - High Risk label to the security policy created in the previous section. As a result, once the Lookout cloud service applies the label to any device with a detected high-risk threat and such a device checks in with MobileIron, the security policy will automatically be applied to it (provided it is of higher priority than the policy currently applied). In turn that will cause the MTP High Risk Trigger App Control policy to be violated and the MTP - High Risk Compliance Action to be taken. Once Lookout detects that the threat has been resolved, the Lookout service will remove the MTP - High Risk label and on device check-in, MobileIron will then apply the next-lower-priority security policy.

1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Policies.**
2. On the **Policies** page:
    a. Select the check box in the **MTP High Risk** security policy item.
    b. Select More **Actions > Apply to Label**; the Apply to Label dialogue will open.

Figure 2-128 Policy List



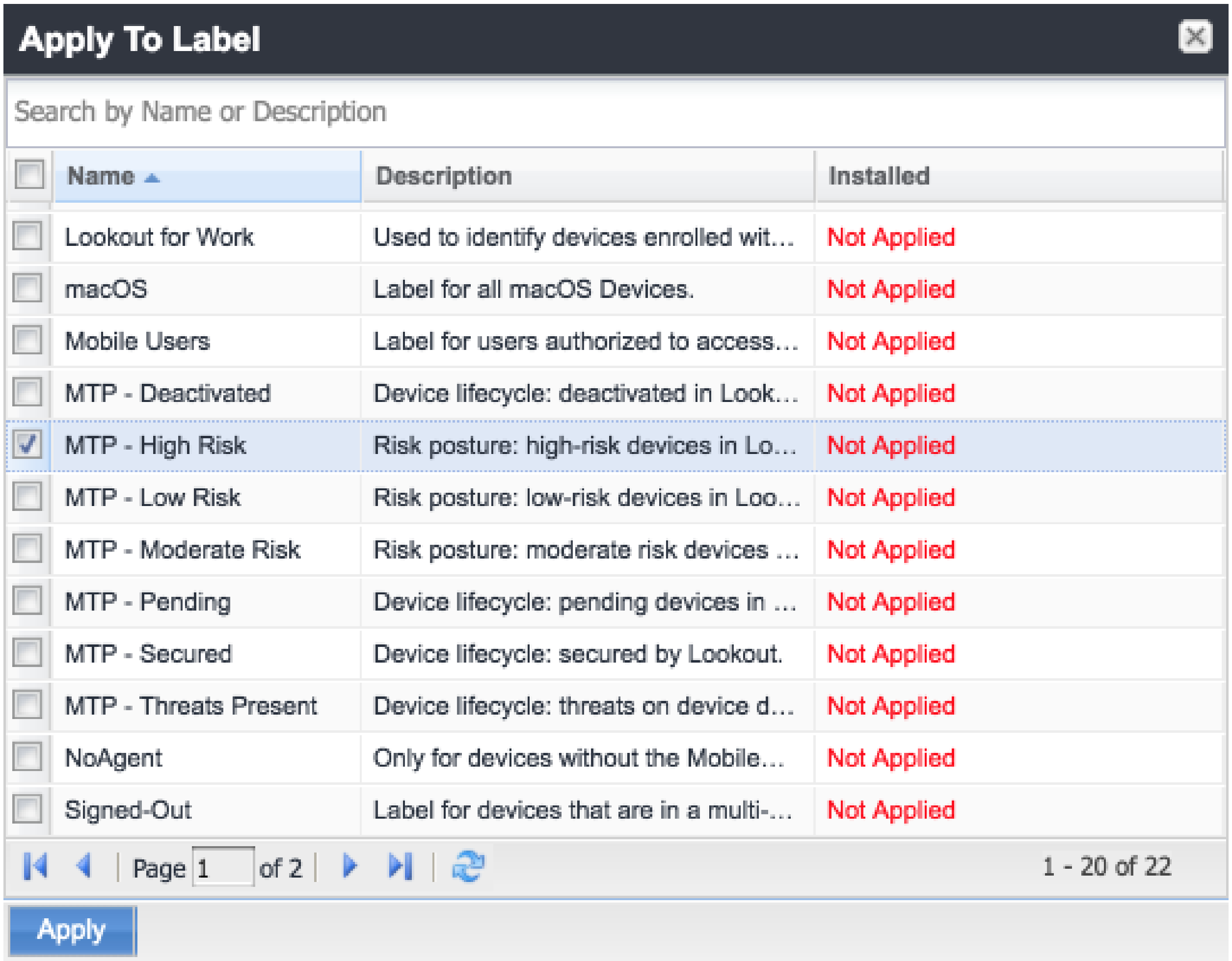
☐	Policy Name	Priority ▴	Status	Descr…	Type	Last Modified	# Phones	Labels	Watch List
☐	Appthority Android	APPCONNECT - 1	Active	Allows…	APPCONNECT	2017-11-16 12:26:0…	11	Android, Appthority	1
☐	MTP High Risk	SECURITY - 1	Active	Applie…	SECURITY	2018-06-12 11:20:2…	0	MTP - High Risk	0

c. In the **Apply to Label** dialogue:

i. Select the check box for the **MTP - High Risk** item.

ii. Select **Apply.**

Figure 2-129 Apply To Label Dialogue



☐	Name ▲	Description	Installed
☐	Lookout for Work	Used to identify devices enrolled wit…	Not Applied
☐	macOS	Label for all macOS Devices.	Not Applied
☐	Mobile Users	Label for users authorized to access…	Not Applied
☐	MTP - Deactivated	Device lifecycle: deactivated in Look…	Not Applied
☑	MTP - High Risk	Risk posture: high-risk devices in Lo…	Not Applied
☐	MTP - Low Risk	Risk posture: low-risk devices in Loo…	Not Applied
☐	MTP - Moderate Risk	Risk posture: moderate risk devices …	Not Applied
☐	MTP - Pending	Device lifecycle: pending devices in …	Not Applied
☐	MTP - Secured	Device lifecycle: secured by Lookout.	Not Applied
☐	MTP - Threats Present	Device lifecycle: threats on device d…	Not Applied
☐	NoAgent	Only for devices without the Mobile…	Not Applied
☐	Signed-Out	Label for devices that are in a multi-…	Not Applied

2.8 Integration of Appthority Mobile Threat Detection with MobileIron

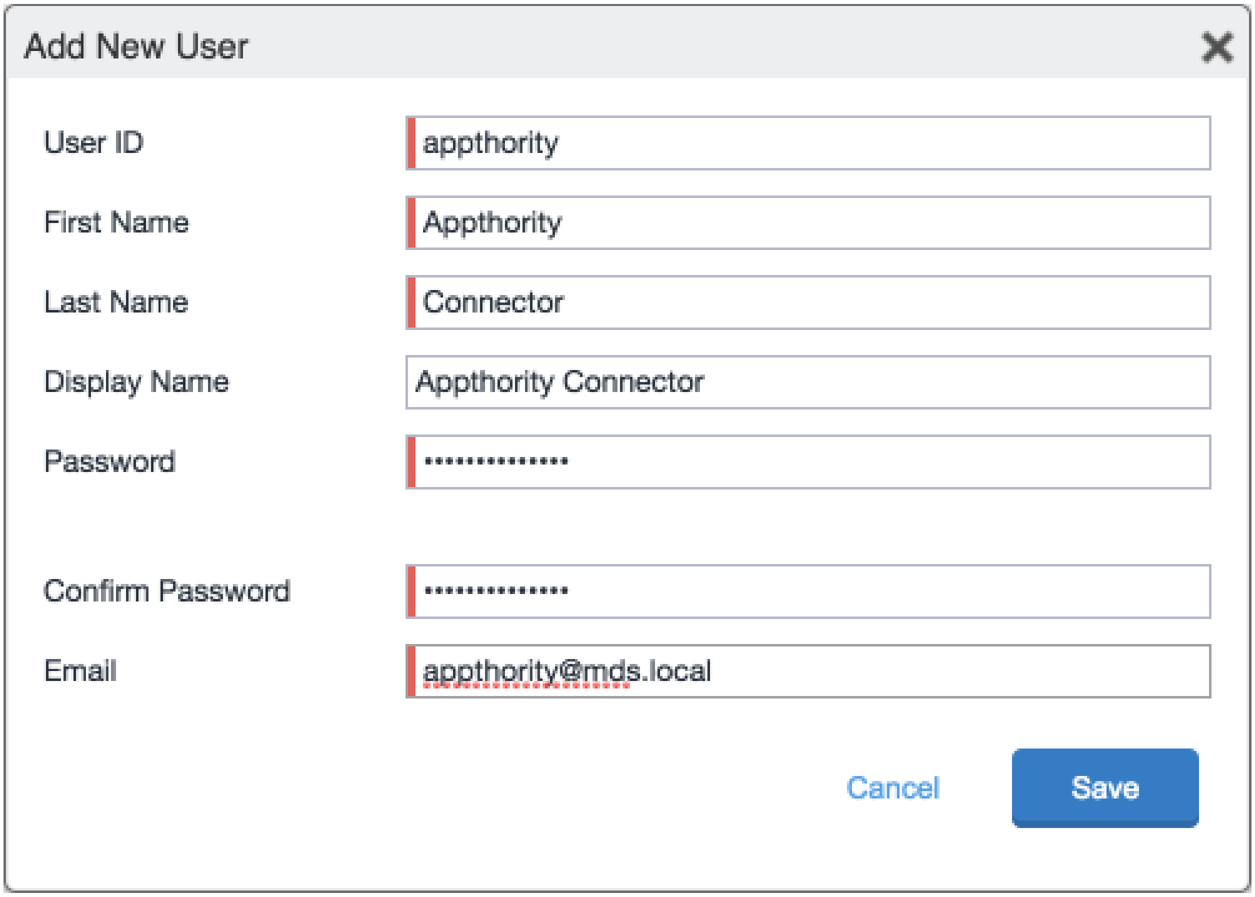
Appthority provides an on-premises connector for MobileIron that runs as a Docker container on RedHat Linux. The connector uses the MobileIron API to obtain information on managed devices and their installed apps, which is then synchronized with the cloud service instance to obtain app and device risk scores, which are assigned to devices using custom attributes. The following sections provide the steps to create a MobileIron API account and deploy and configure the Appthority connector.

2.8.1 Create MobileIron API Account for Appthority Connector

The following steps will create an administrative account that will grant Appthority the specific permissions it requires within MobileIron.

1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Users.**
2. On the **Users** page:
    a. Select **Add > Add Local User**; the **Add New User** dialogue will open.
    b. In the **Add New User** dialogue:
        i. In the **User ID** field, enter the **user identity** the Appthority connector will authenticate under. Our implementation uses a value of **Appthority.**
        ii. In the **First Name** field, enter a generic first name for **Appthority.**
        iii. In the **Last Name** field, enter a generic last name for **Appthority.**
        iv. In the **Display Name** field, optionally enter a displayed name for this user account.
        v. In the **Password** field, provide the password the **Appthority** identity will use to authenticate to MobileIron.
        vi. In the **Confirm Password** field, enter the same password as in the preceding step.
        vii. In the **Email** field, provide an email account for the **Appthority** identity; this should be an account under the control of your organization.
        viii. Select **Save.**

Figure 2-130 Apptherity User Settings



Add New User

User ID: appthority

First Name: Appthority

Last Name: Connector

Display Name: Appthority Connector

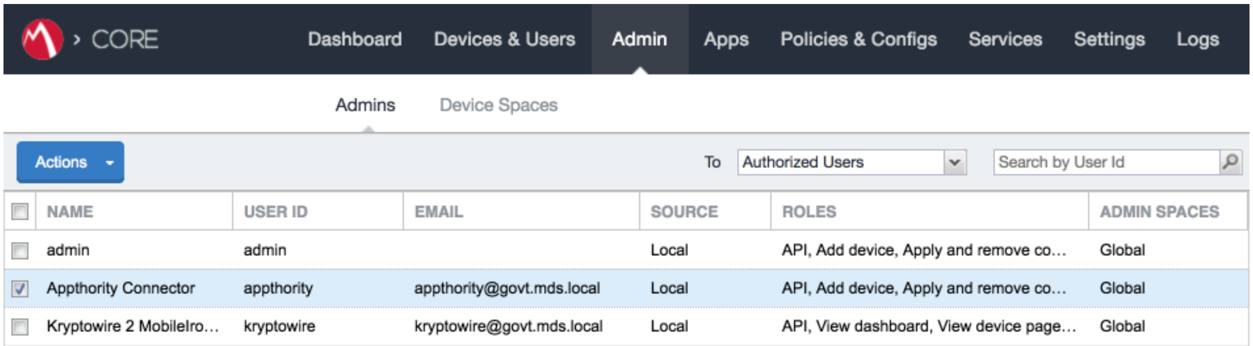
Password: •••••••••••••••

Confirm Password: •••••••••••••••

Email: appthority@mds.local

1. In the **MobileIron Admin** Portal, navigate to **Admin.**
2. On the **Admin** page:
   a. Enable the account you created for **Appthority** during **Step 2.**
   b. Select **Actions > Assign to Space**; this will open the **Assign to Space** dialogue for the **Appthority** account.

Figure 2-131 Apprority Connector User

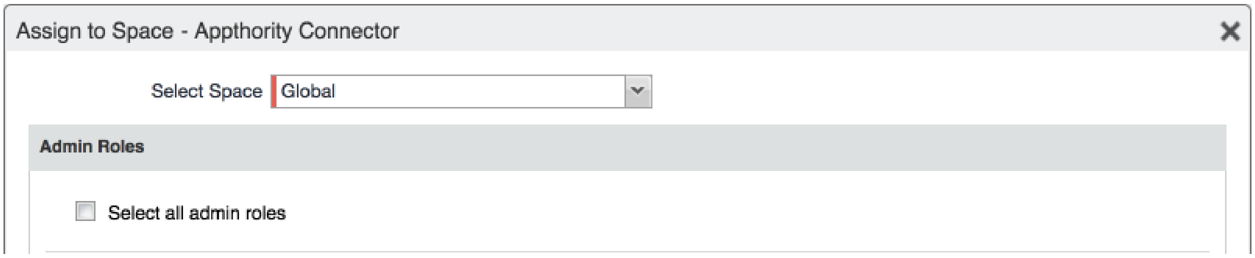


☐	NAME	USER ID	EMAIL	SOURCE	ROLES	ADMIN SPACES
☐	admin	admin		Local	API, Add device, Apply and remove co…	Global
☑	Apprority Connector	apprority	apprority@govt.mds.local	Local	API, Add device, Apply and remove co…	Global
☐	Kryptowire 2 MobileIro…	kryptowire	kryptowire@govt.mds.local	Local	API, View dashboard, View device page…	Global

c. In the **Assign to Space** dialogue:

i. In the **Select Space** drop-down menu, select **Global.**

Figure 2-132 Apprority Connector Space Assignment


Assign to Space - Apprority Connector

Select Space: Global

Admin Roles

☐ Select all admin roles

ii. **Enable** each of the following settings:

Device Management > View device page, device details
Privacy Control > View apps and ibooks in device details
App Management > Apply and remove application label
Other Roles > API

iii. Select **Save.**

2.8.2 Deploy Apprority Connector Open Virtualization Appliance

One deployment option for the Apprority connector is a pre-built RedHat virtual machine distributed as an Open Virtualization Appliance (OVA). We imported the OVA into our virtual lab environment following guidance provided in *Connector On-Premises: Virtual Machine Setup* available from the Apprority support portal: https://support.apprority.com/.

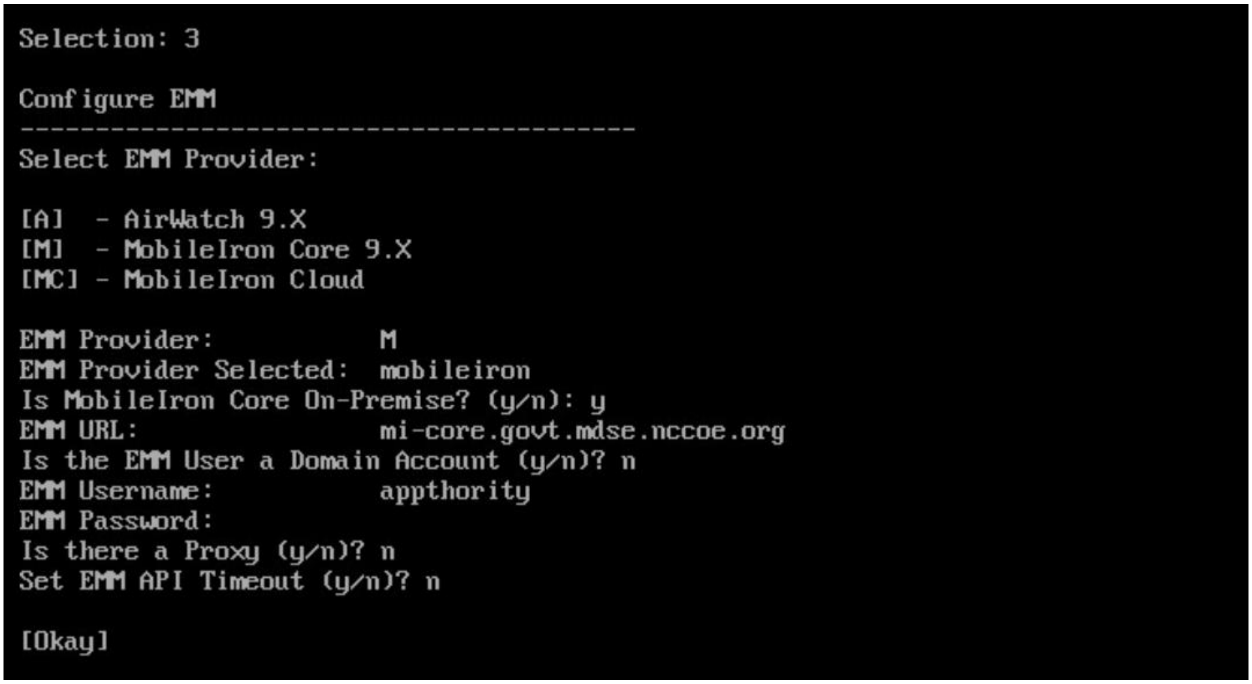
2.8.3 Run the Enterprise Mobility Management Connector Deployment Script

Once the Appthority docker container is running, the setup script will configure it to use the MobileIron API account created previously. Detailed instructions on using the script are available on the Appthority support portal at [https://help-mtp.appthority.com/SetUp/EMM/EMM_Script/RunEMMDeployScript.html.](https://help-mtp.appthority.com/SetUp/EMM/EMM_Script/RunEMMDeployScript.html) The first two steps ask for Appthority-supplied credentials necessary to verify your subscription and to link the connector with the correct instance of their cloud service. In the third step you will provide details to integrate with your on-premises instance of MobileIron core. Our results from completing the third step are shown below.

1. **Obtain** a copy of *Run the EMM Connector Deployment Script* from the Appthority support portal at https://help-mtp.appthority.com/SetUp/EMM/EMM_Script/RunEMMDeployScript.html (authentication to the portal is required).

2. **Execute** the script. The third step in the script involves providing settings to enable the Appthority Connector to communicate with MobileIron Core. The results of our completion of that step are provided below as a reference.

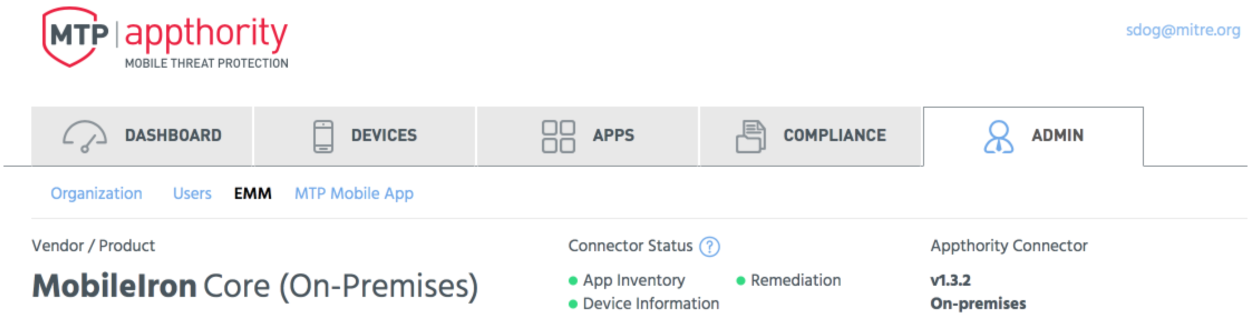
Figure 2-133 Appthority Connector CLI Configuration



```
Selection: 3

Configure EMM
-----------------------------------------
Select EMM Provider:

[A]  - AirWatch 9.X
[M]  - MobileIron Core 9.X
[MC] - MobileIron Cloud

EMM Provider:             M
EMM Provider Selected:    mobileiron
Is MobileIron Core On-Premise? (y/n): y
EMM URL:                  mi-core.govt.mdse.nccoe.org
Is the EMM User a Domain Account (y/n)? n
EMM Username:             appthority
EMM Password:
Is there a Proxy (y/n)? n
Set EMM API Timeout (y/n)? n

[Okay]
```

3. Once the script has been completed, verify successful synchronization with the Appthority cloud service by accessing the Appthority MTP portal and navigating to **Admin > EMM** and viewing items under **Connector Status.**

Figure 2-134 Apthority EMM Connector Status



Vendor / Product

MobileIron Core (On-Premises)

Connector Status

● App Inventory ● Remediation
● Device Information

Appthority Connector

v1.3.2
On-premises

2.9 Registering Devices with MobileIron Core

In this scenario, the employee manages their own personal apps, data, and many device functions. The organization manages work-related apps and data, and has control over specific device functions, such as requiring a complex device unlock PIN or being able to remotely wipe a lost device. The mechanisms to achieve similar security characteristics between iOS and Android devices differ.

2.9.1 Supervising and Registering iOS Devices

Many MDM-based security controls are only applicable to iOS devices that are running in Supervised Mode. The following steps outline how to place an iOS device into this mode, and then register with MobileIron Core.

2.9.1.1 Resetting the iOS Device

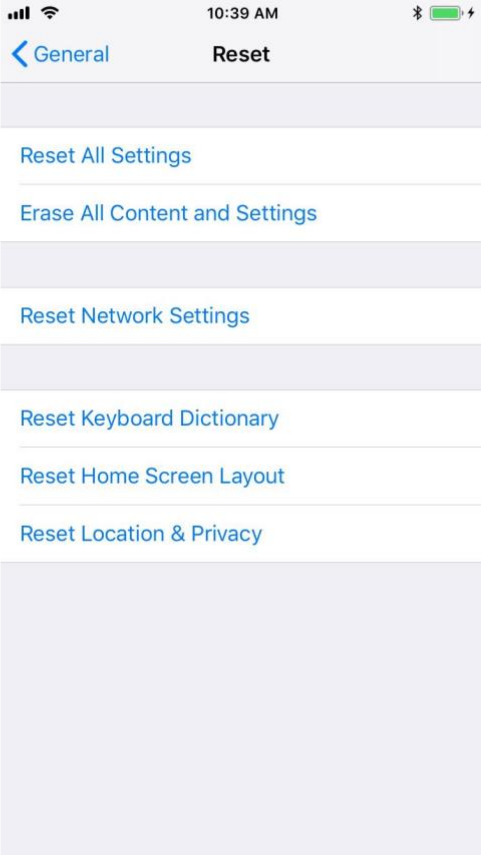
Before a device can be placed into Supervised Mode, it must be in a factory-reset state with the Activation Lock on the device removed. If Activation Lock is in-place, Configurator 2 will be unable to place the device into Supervised Mode.

2.9.1.1.1 Reset an Unsupervised Device Using Settings App

If a device is not already in Supervised Mode, it is recommended to have the current device user manually reset and activate the device to factory settings using the following steps:

1. Navigate to **Settings > General > Reset.**
2. Select **Erase All Content and Settings.**

Figure 2-135 iOS Reset Screen



10:39 AM

General

Reset

Reset All Settings

Erase All Content and Settings

Reset Network Settings

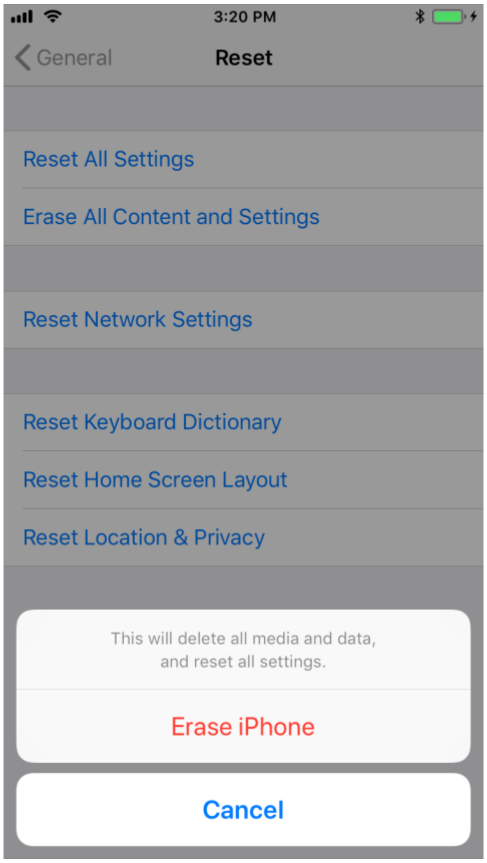
Reset Keyboard Dictionary

Reset Home Screen Layout

Reset Location & Privacy

1. At the warning that this will delete all media and data and reset all settings, select **Erase iPhone.**

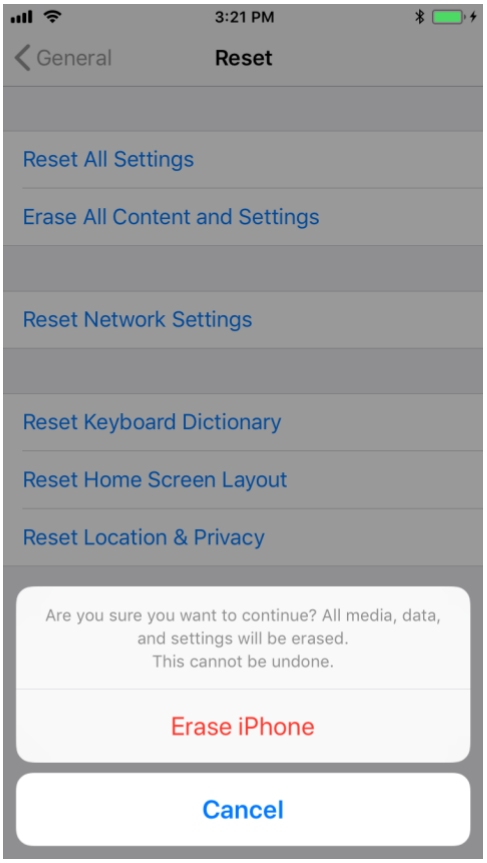
Figure 2-136 Erase iPhone Confirmation



This will delete all media and data,
and reset all settings.

1. At the warning that all media, data, and settings will be irreversibly erased, select **Erase iPhone.** Once the reset process is complete, the device will reboot and need to be activated.

Figure 2-137 Erase iPhone Final Confirmation



Are you sure you want to continue? All media, data, and settings will be erased.
This cannot be undone.

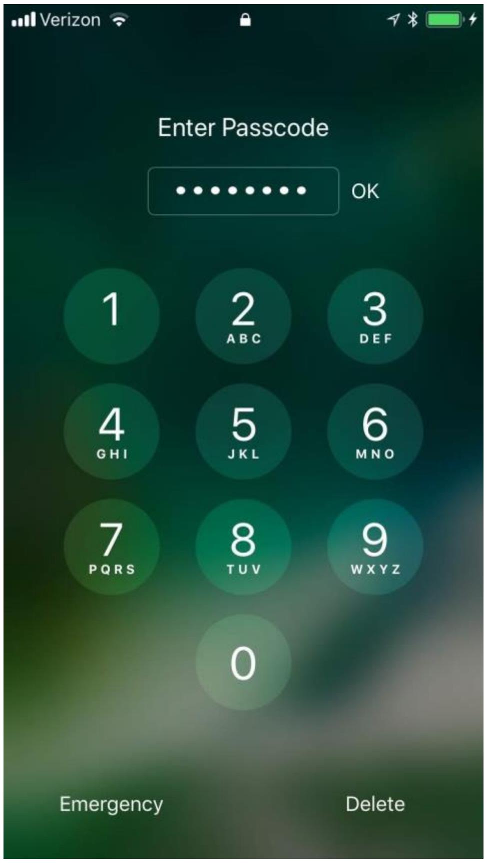
1. Once the device displays the **Hello** screen, press the **Home key.**
2. At the **Select Your Language** screen, select **English.**
3. At the **Select Your Country or Region** screen, select **United States.**
4. At the **Quick Start** screen select **Set up Manually.**
5. At the **Choose a Wi-Fi Network** screen, select the **Service Set Identifier (SSID)** for the network and authenticate to your on-premises SSID Wi-Fi network; the device should indicate it is being activated. **Note:** you may need to attempt activation again if there is a delay in the device establishing connectivity to the internet.
6. **Stop** at the **Data & Privacy** screen. At this point, the device should be placed into **Supervised Mode** using **Configurator 2.**

2.9.1.1.2 Reset a Supervised Device Using Configurator 2

1. **Connect** the iOS device with the system running **Configurator 2** over **Universal Serial Bus (USB).**

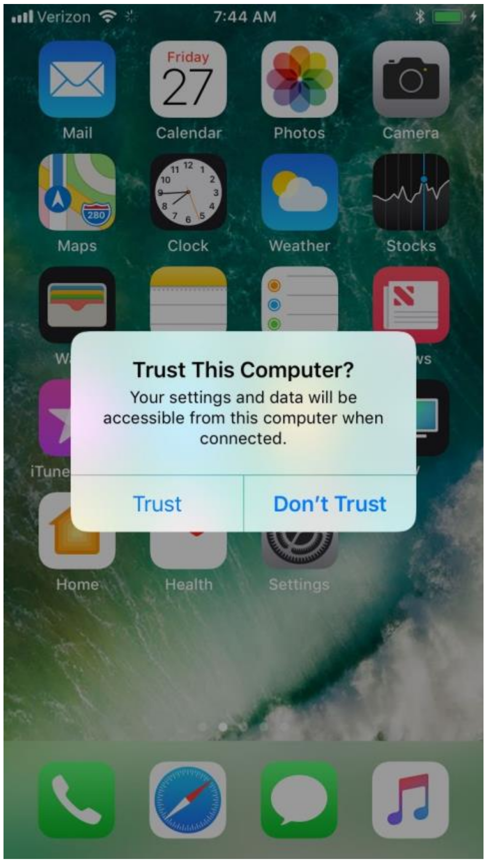
2. On the device at the **Enter Passcode** screen (if locked), enter the **device unlock passcode.**

Figure 2-138 Entering iOS Passcode



3. At the **Trust this Computer?** dialogue, select **Trust.** Note that this step, along with step that follows, is only encountered the first time a device is paired with a given system.

Figure 2-139 iOS Trust Computer Confirmation

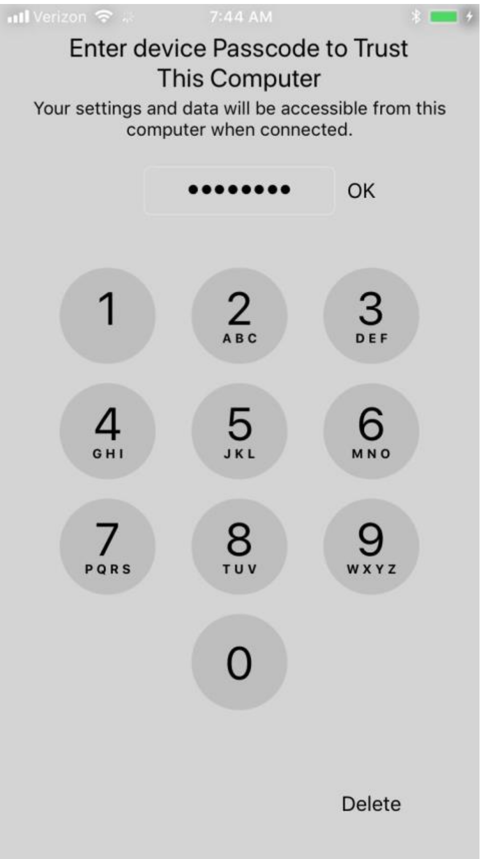


Trust This Computer?

Your settings and data will be accessible from this computer when connected.

4. At the **Enter Device Passcode to Trust This Computer** screen:
   a. **Enter** the device unlock passcode.
   b. Select **OK**.

Figure 2-140 Entering Passcode to Trust Computer

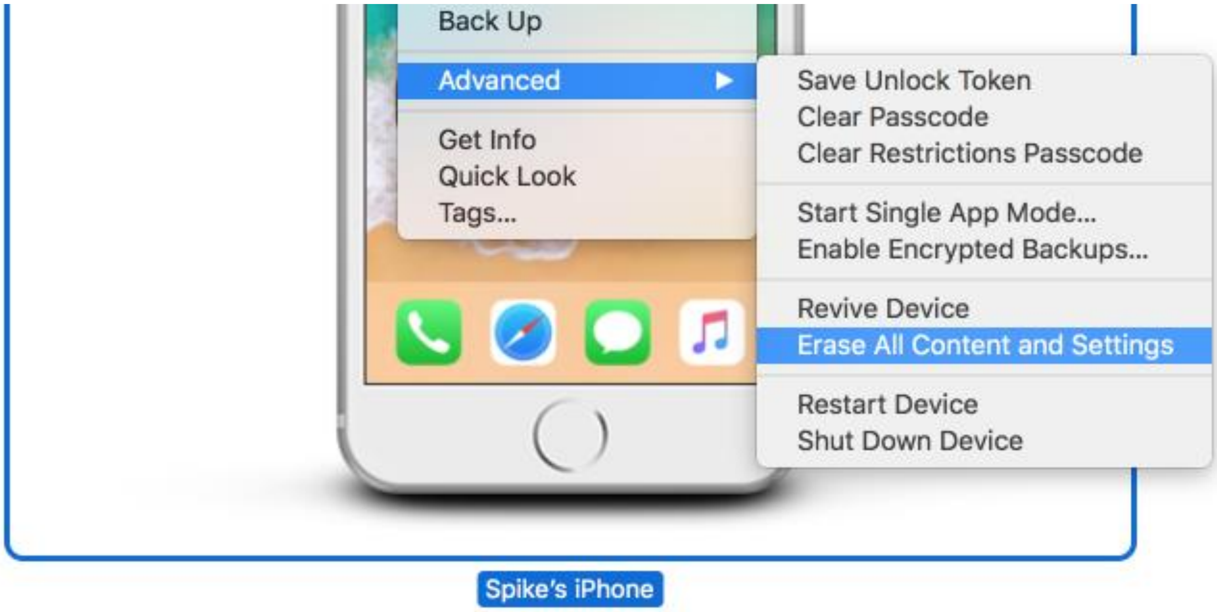


Enter device Passcode to Trust This Computer

Your settings and data will be accessible from this computer when connected.

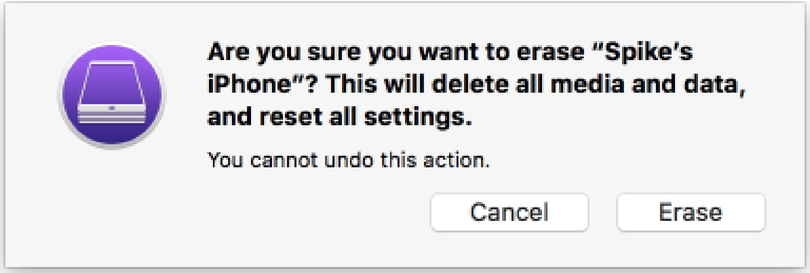
5. In **Configurator 2**, select the **representation** of the connected device.
6. From the **context** menu, select **Advanced > Erase All Content and Settings**.

Figure 2-141 Resetting iPhone in Configurator 2



7. At the **Are you sure you want to erase "<device name>"?** dialogue, select **Erase.**

Figure 2-142 Configurator 2 Erase Confirmation

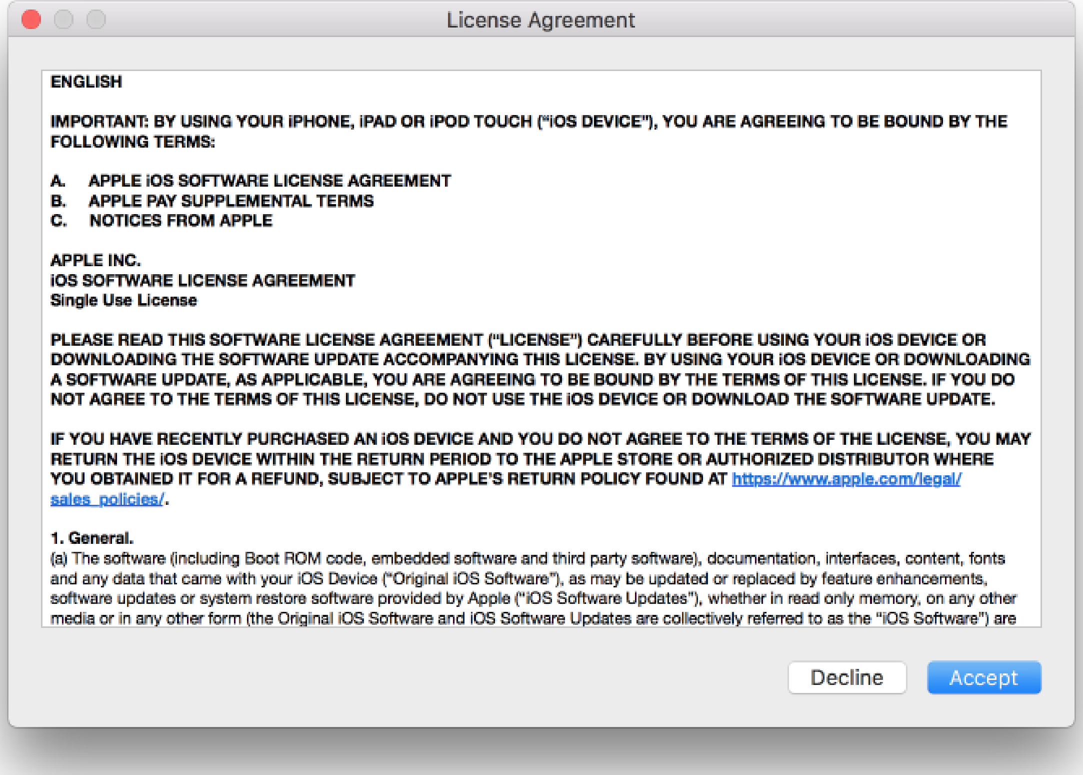


Are you sure you want to erase "Spike's iPhone"? This will delete all media and data, and reset all settings.

You cannot undo this action.

8. At the **License Agreement** screen:
   a. **Review** the license agreement.
   b. Select **Accept** to agree to the license and continue using the software**.**

Figure 2-143 Configurator 2 License Agreement



ENGLISH

IMPORTANT: BY USING YOUR iPHONE, iPAD OR iPOD TOUCH ("iOS DEVICE"), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS:

A. APPLE iOS SOFTWARE LICENSE AGREEMENT
B. APPLE PAY SUPPLEMENTAL TERMS
C. NOTICES FROM APPLE

APPLE INC.
iOS SOFTWARE LICENSE AGREEMENT
Single Use License

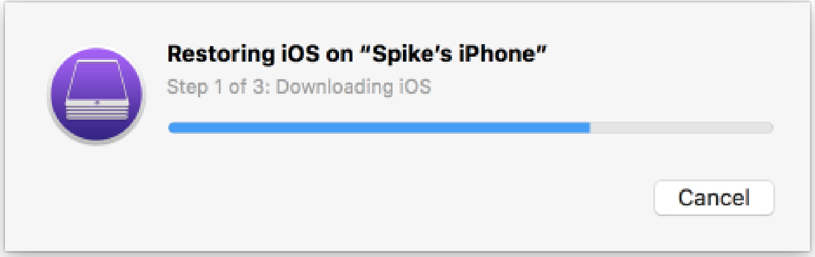
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR iOS DEVICE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR iOS DEVICE OR DOWNLOADING A SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE iOS DEVICE OR DOWNLOAD THE SOFTWARE UPDATE.

IF YOU HAVE RECENTLY PURCHASED AN iOS DEVICE AND YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE iOS DEVICE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT https://www.apple.com/legal/sales_policies/.

1. General.
(a) The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with your iOS Device ("Original iOS Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("iOS Software Updates"), whether in read only memory, on any other media or in any other form (the Original iOS Software and iOS Software Updates are collectively referred to as the "iOS Software") are

9. **Configurator 2** will take several minutes to restore the device to factory default settings. **Configurator 2** will also activate the device following restoration.

Figure 2-144 Restoring iPhone

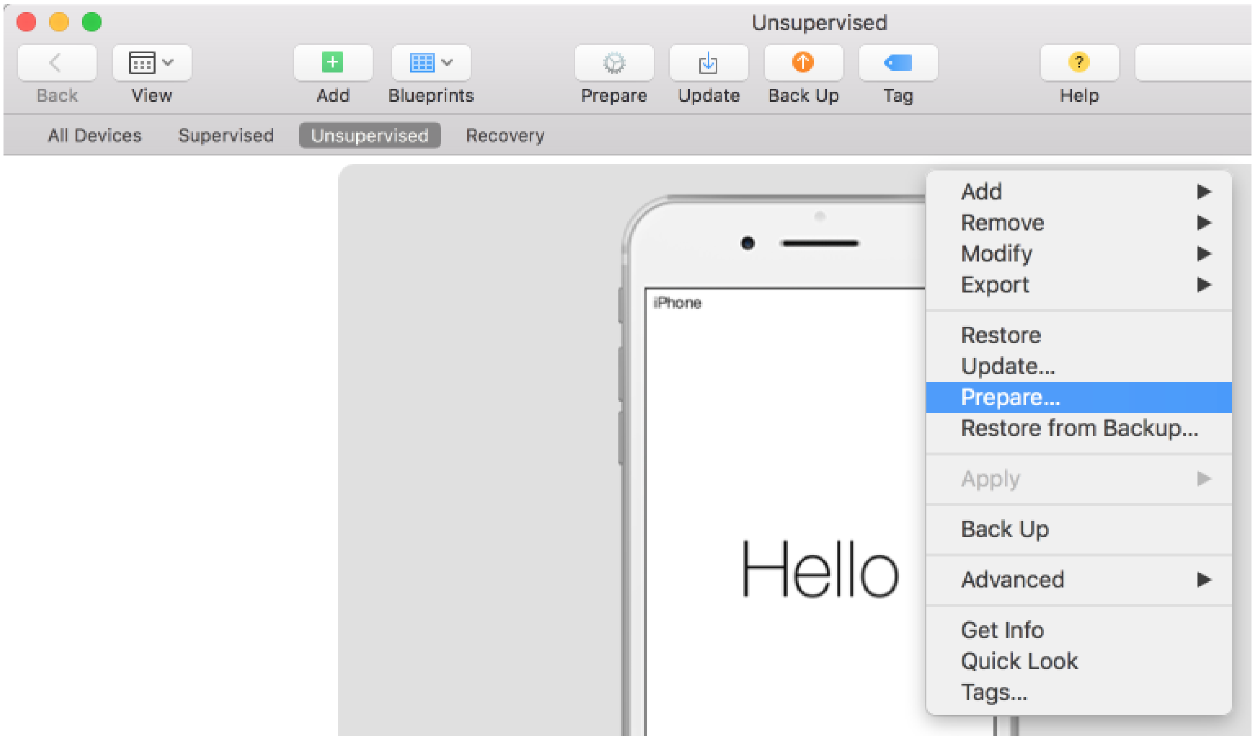

Restoring iOS on "Spike's iPhone"
Step 1 of 3: Downloading iOS
Cancel

2.9.1.2 Placing an iOS Device into Supervised Mode

iOS devices that have been factory reset and subsequently activated (the Activation Lock has been removed) can be placed into Supervised Mode using software available from Apple, Configurator 2, by the following steps:

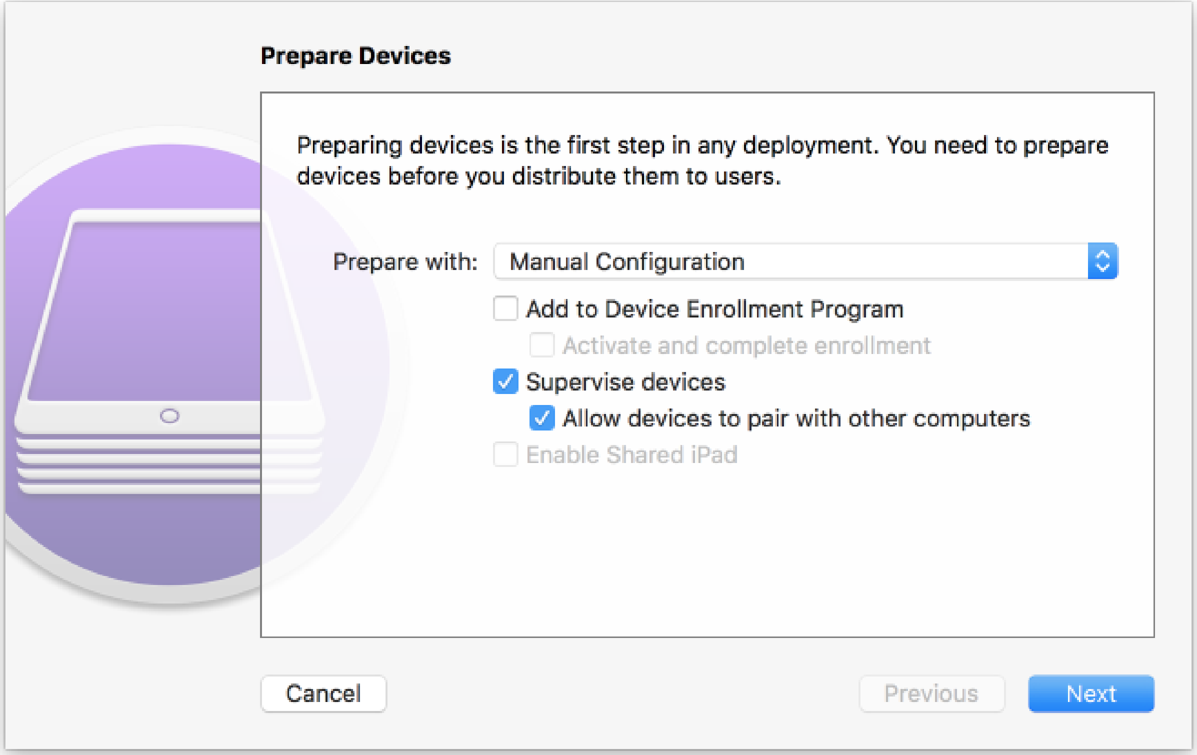
1. **Pair** the target iOS device with the system running Configurator 2 over USB.
2. Navigate to **Configurator 2 > Unsupervised**; a representation of the connected device should appear.
3. On the **All Devices** tab:
   a. **Select** the representation of the paired device.
   b. From the **context** menu, select **Prepare**; a wizard will open to guide the process.

Figure 2-145 Prepare Option in Configuration 2



4. For the **Prepare Devices** step:
   a. **Enable** Supervise Devices.
   b. Select **Next.**

1693 **Figure 2-146 Device Preparation Options**



Prepare Devices

Preparing devices is the first step in any deployment. You need to prepare devices before you distribute them to users.

Prepare with: Manual Configuration

□ Add to Device Enrollment Program

□ Activate and complete enrollment

☑ Supervise devices

☑ Allow devices to pair with other computers

□ Enable Shared iPad

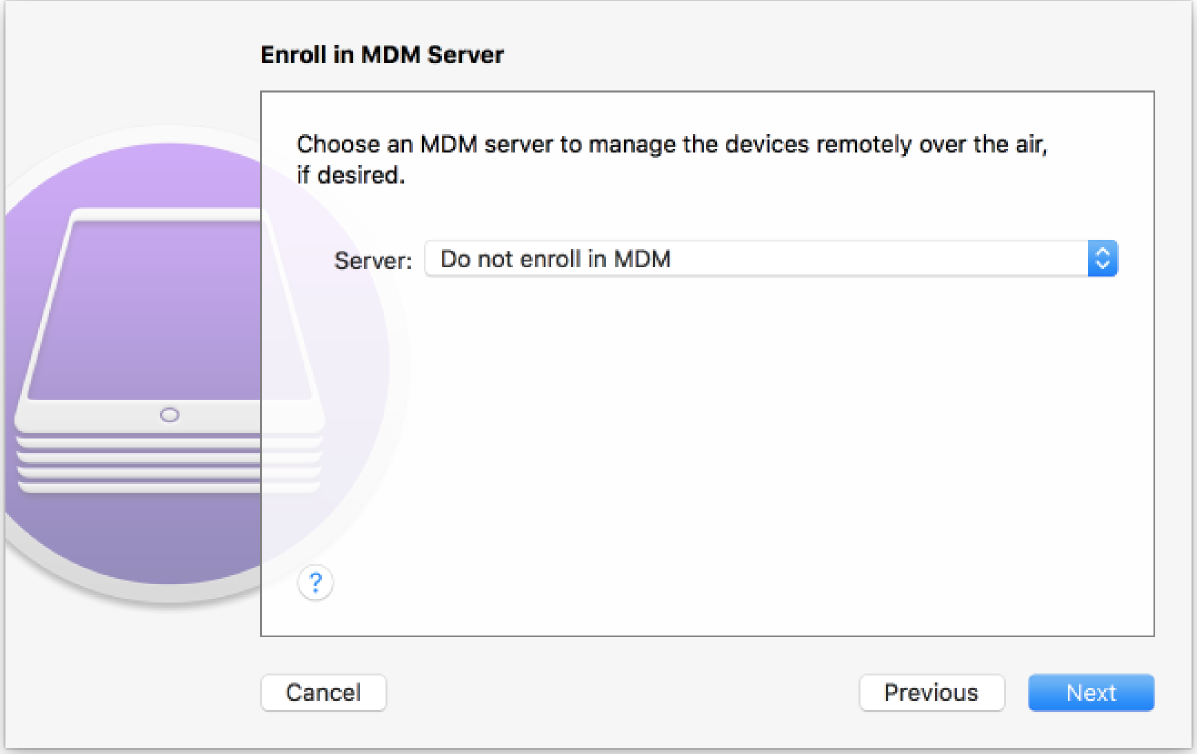
1694

1695 5. For the **Enroll in MDM Server** step:

1696 a. Ensure the **Server** drop-down menu has **Do not enroll in MDM** selected.

1697 b. Select **Next.**

1698 Figure 2-147 Preparation MDM Server Selection



Enroll in MDM Server

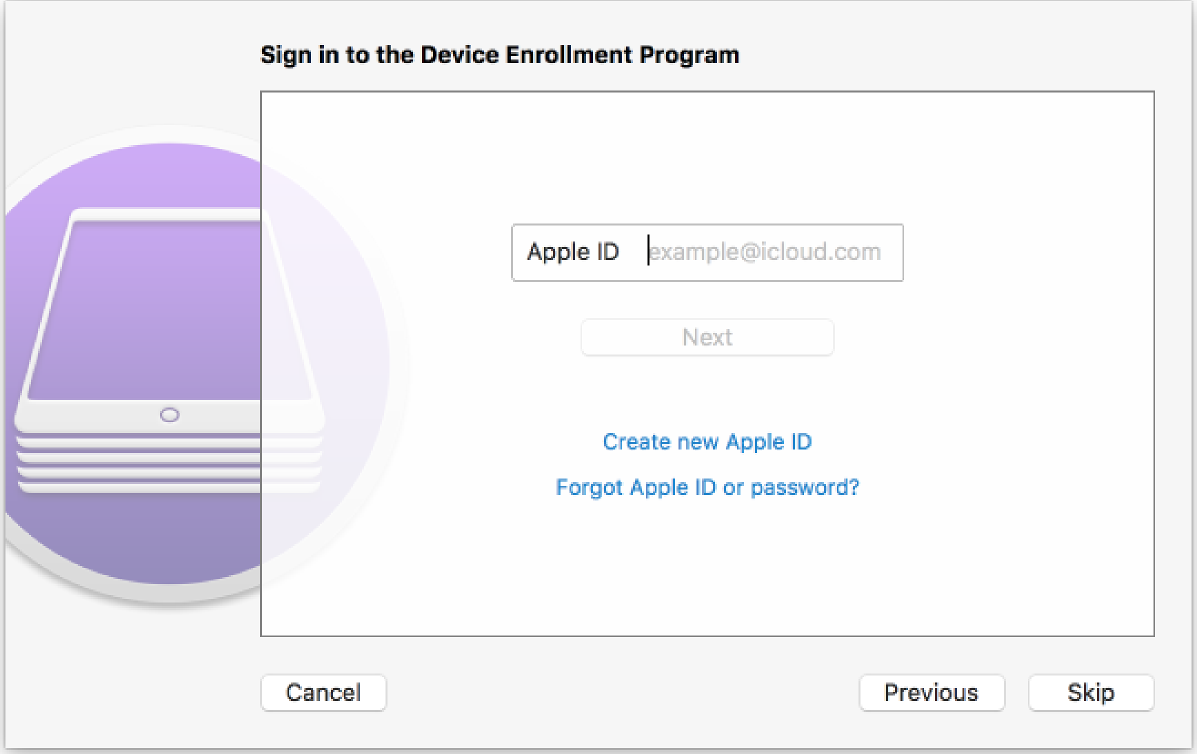
Choose an MDM server to manage the devices remotely over the air, if desired.

Server: Do not enroll in MDM

1699

1700 6. For the **Sign into the Device Enrollment Program** step, select **Skip.**

Figure 2-148 Signing into Apple Account

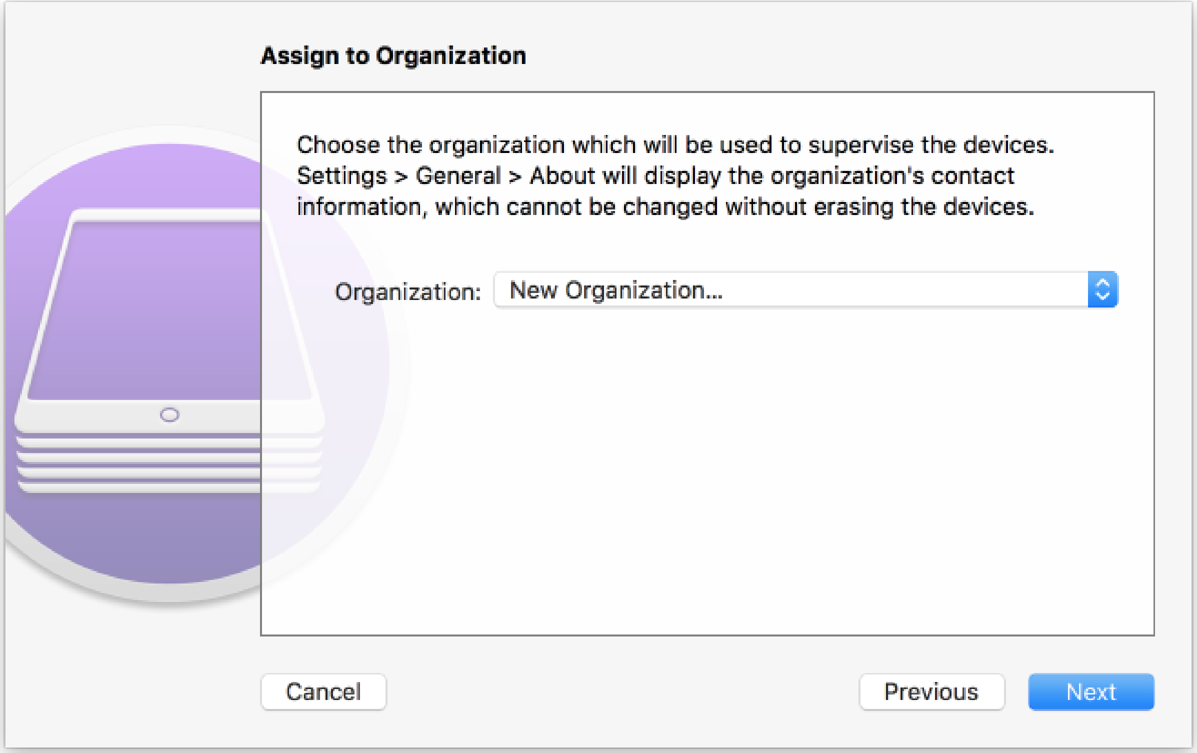


Sign in to the Device Enrollment Program

Apple ID example@icloud.com

7. For the **Assign to Organization** step:
    a. If you have previously created your organization, select **Next** and continue with **Step 9.**
    b. If you have not created your organization, from the **Organization** drop-down menu, select **New Organization...**

Figure 2-149 Organization Assignment Dialogue



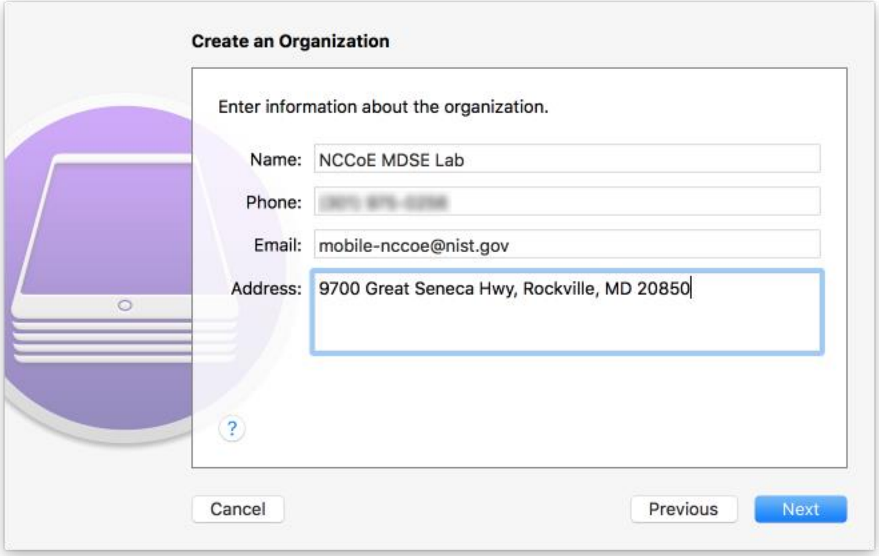
Assign to Organization

Choose the organization which will be used to supervise the devices. Settings > General > About will display the organization's contact information, which cannot be changed without erasing the devices.

Organization: New Organization...

8. At the **Create an Organization screen:**
   a. In the **Name** field, enter the name of your organization.
   b. In the **Phone** field, enter an appropriate support number for your mobility program.
   c. In the **Email** field, enter an appropriate support email for your mobility program.
   d. In the **Address** field, enter the address for your organization.
   e. Select **Next.**

Figure 2-150 Creating an Organization



Create an Organization

Enter information about the organization.

Name: NCCoE MDSE Lab

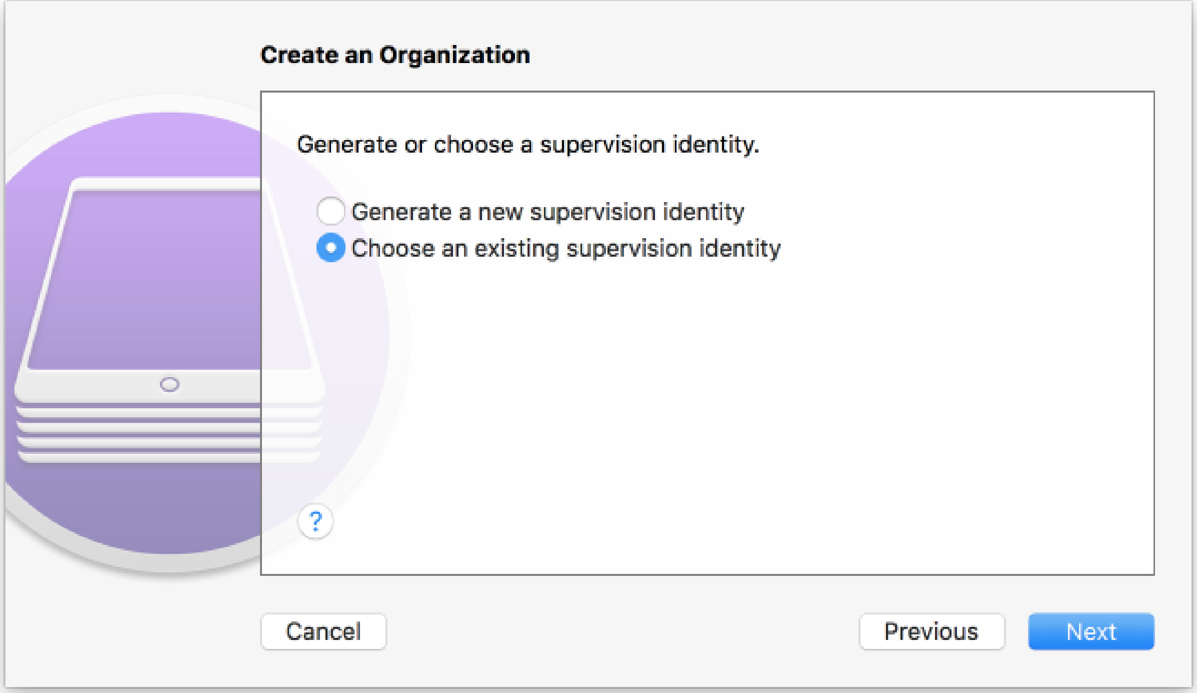
Phone: [redacted]

Email: mobile-nccoe@nist.gov

Address: 9700 Great Seneca Hwy, Rockville, MD 20850

9. If your organization has established a digital identity for placing devices into **Supervised Mode:**
   a. Continue with **Step 10. Note:** that the same digital identity must be used for any given device.
   b. Otherwise, continue with **Step 14**.
10. In the **Create an Organization** screen:
    a. For the **Generate or choose a supervision identity** option, select **Choose an existing supervision identity**.
    b. Select **Next.**

Figure 2-151 Supervisory Identity Configuration



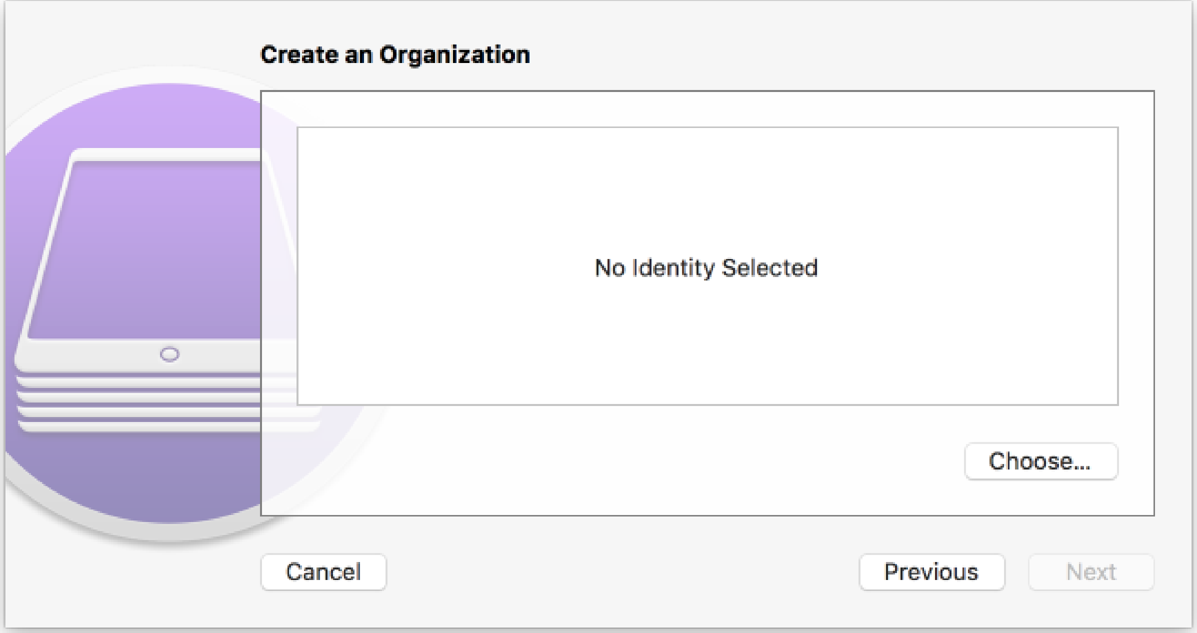
Create an Organization

Generate or choose a supervision identity.

○ Generate a new supervision identity
● Choose an existing supervision identity

11. Select **Choose...**

Figure 2-152 Organization Selection

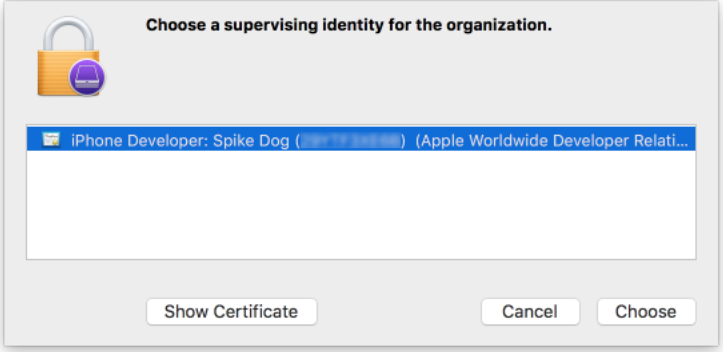


Create an Organization

No Identity Selected

12. At the **Choose a supervising identity for the organization** dialogue:
    a. **Select** the digital certificate from the list of those available to the system.
    b. Select **Choose.**

Figure 2-153 Supervising Identity Selection

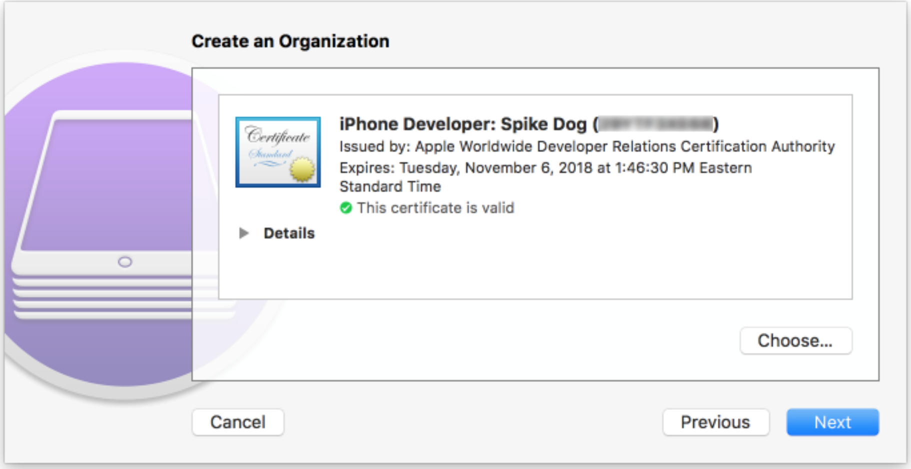


Choose a supervising identity for the organization.

iPhone Developer: Spike Dog ([redacted]) (Apple Worldwide Developer Relati...

13. At the **Create an Organization** screen, select **Next.**

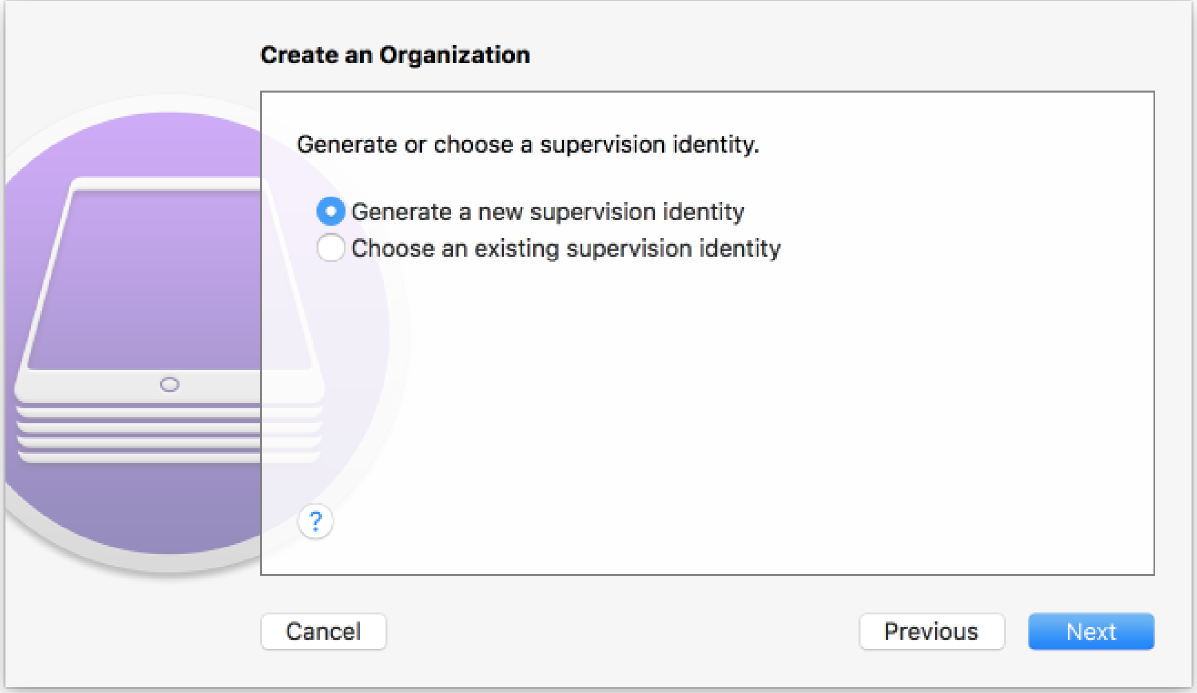
Figure 2-154 Selected Organization



iPhone Developer: Spike Dog ([redacted])
Issued by: Apple Worldwide Developer Relations Certification Authority
Expires: Tuesday, November 6, 2018 at 1:46:30 PM Eastern Standard Time
This certificate is valid

14. In the **Create an Organization** screen:
    a. For the **Generate or choose a supervision identity option**, select **Generate a new supervision identity**.
    b. Select **Next.**

Figure 2-155 Create an Organization Supervision Identity Configuration



Create an Organization

Generate or choose a supervision identity.

● Generate a new supervision identity
○ Choose an existing supervision identity

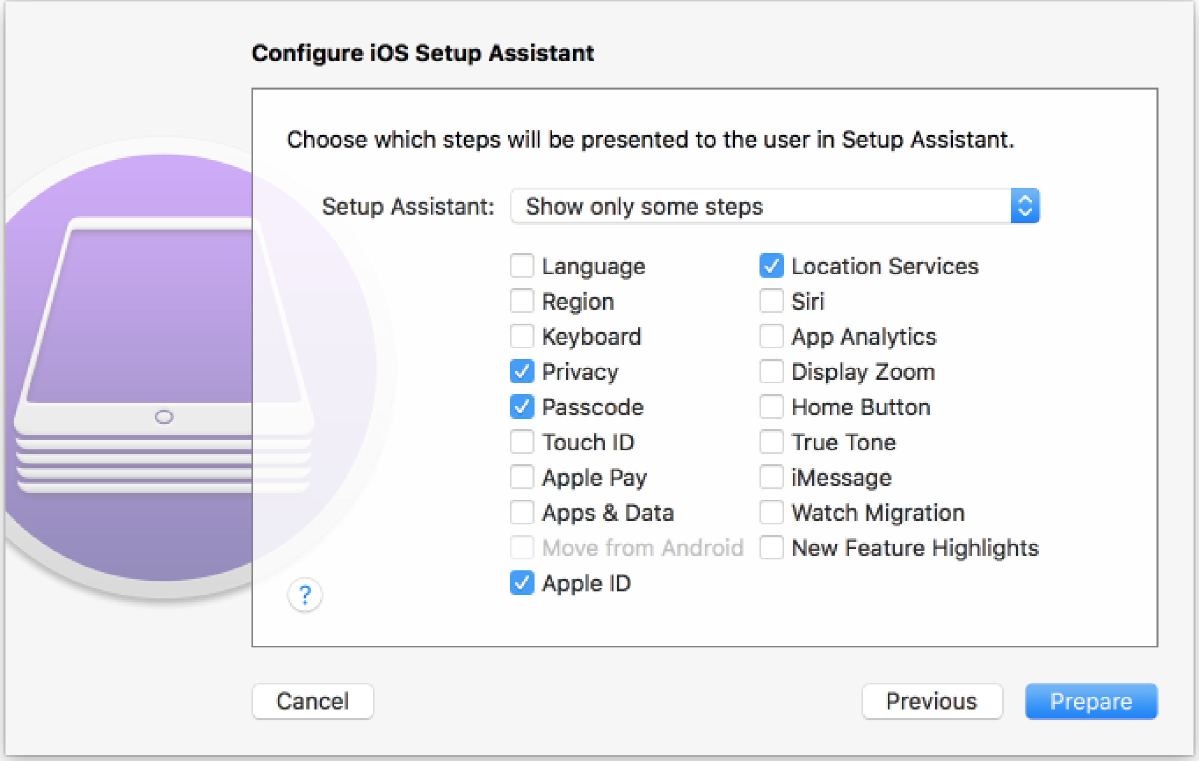
15. For the **Configure iOS Setup Assistant** step:

    a. Ensure the **Setup Assistant** drop-down menu shows **Show only some steps** selected; additional options will appear.

    b. Enable each of the **Privacy**, **Passcode**, **Apple ID**, and **Location Services** check-boxes.

    c. Select **Prepare**.

Figure 2-156 Setup Assistant Configuration



Configure iOS Setup Assistant

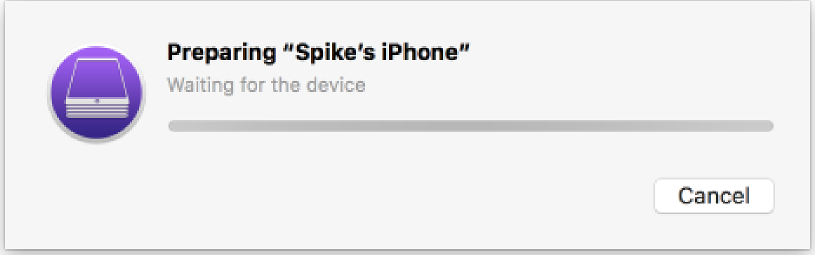
Choose which steps will be presented to the user in Setup Assistant.

Setup Assistant: Show only some steps

☐ Language
☐ Region
☐ Keyboard
☑ Privacy
☑ Passcode
☐ Touch ID
☐ Apple Pay
☐ Apps & Data
☐ Move from Android
☑ Apple ID
☑ Location Services
☐ Siri
☐ App Analytics
☐ Display Zoom
☐ Home Button
☐ True Tone
☐ iMessage
☐ Watch Migration
☐ New Feature Highlights

16. **Configurator 2** will take several minutes to prepare the device and place it into **Supervised Mode.**

Figure 2-157 Waiting for iPhone



Preparing "Spike's iPhone"

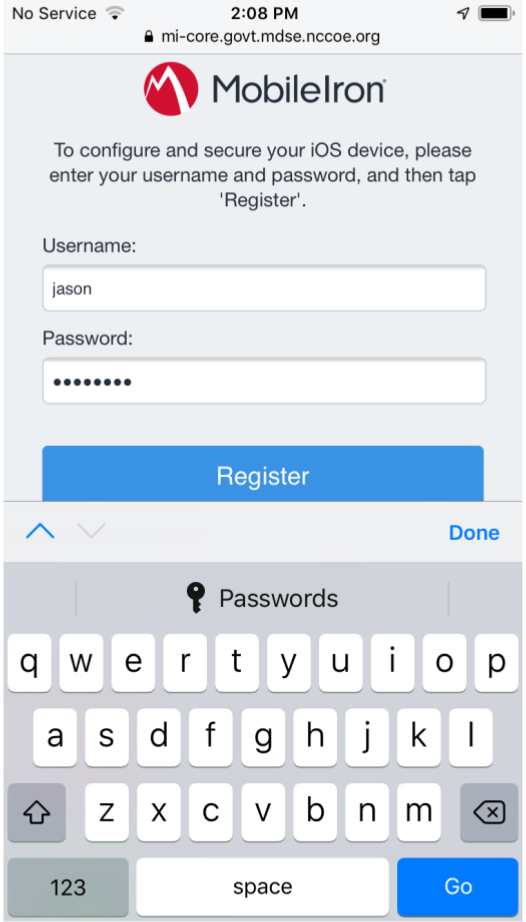
Waiting for the device

2.9.1.3 Registration with MobileIron Core

The following steps will register an iOS device in Supervised Mode with MobileIron Core, which uses a web-based process rather than the *Mobile@Work* app.

1. Using **Safari**, navigate to **MobileIron Core** page, substituting <FQDN> for that of your organization's instance of MobileIron Core. In our example implementation, the resulting URL is https://mi-core.govt.mdse.nccoe.org/go .

Figure 2-158 MobileIron Registration Page



No Service 2:08 PM

mi-core.govt.mdse.nccoe.org

MobileIron

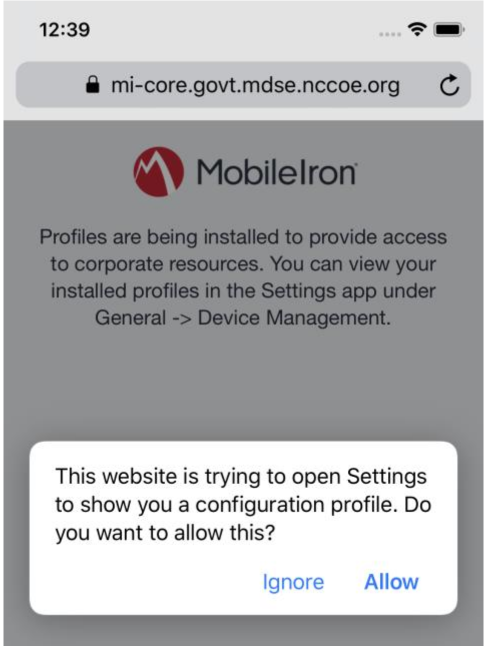
To configure and secure your iOS device, please enter your username and password, and then tap 'Register'.

Username: jason

Password: ••••••••

2. At the **warning** that the web site is trying to open **Settings** to show a configuration profile, select **Allow**; the **Settings** built-in app will open.

Figure 2-159 Opening Settings Confirmation



12:39

mi-core.govt.mdse.nccoe.org

MobileIron

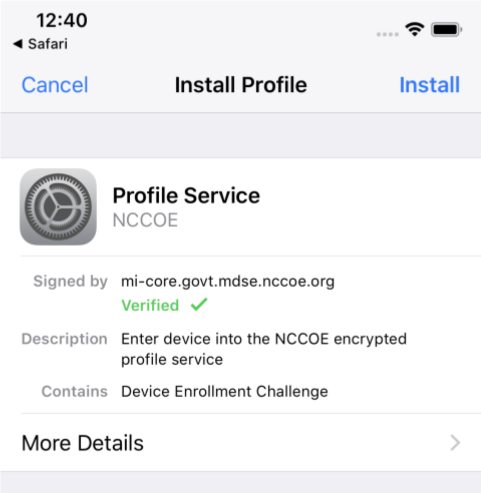
Profiles are being installed to provide access to corporate resources. You can view your installed profiles in the Settings app under General -> Device Management.

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

Ignore Allow

3. At the **Settings > Install Profile** screen:
    a. Verify the **Signed by** field indicates the server identity is **Verified.**
    b. Select **Install**.

Figure 2-160 Profile Installation



12:40

◀ Safari

Cancel Install Profile Install

Profile Service

NCCOE

Signed by mi-core.govt.mdse.nccoe.org

Verified ✓

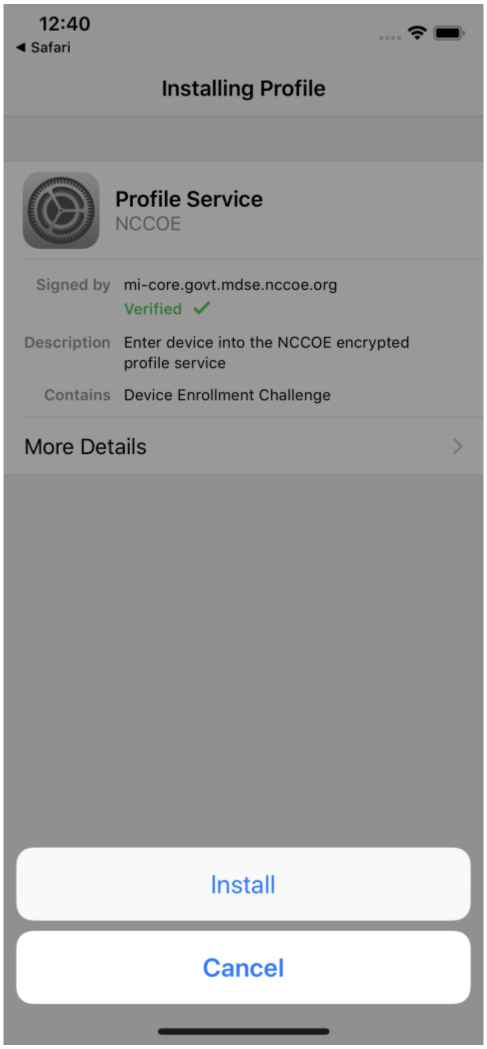
Description Enter device into the NCCOE encrypted profile service

Contains Device Enrollment Challenge

More Details >

4. At the **Installing Profile** screen, select **Install**.

Figure 2-161 Profile Installation



12:40
◂ Safari

Installing Profile

Profile Service
NCCOE

Signed by mi-core.govt.mdse.nccoe.org
Verified ✓

Description Enter device into the NCCOE encrypted profile service

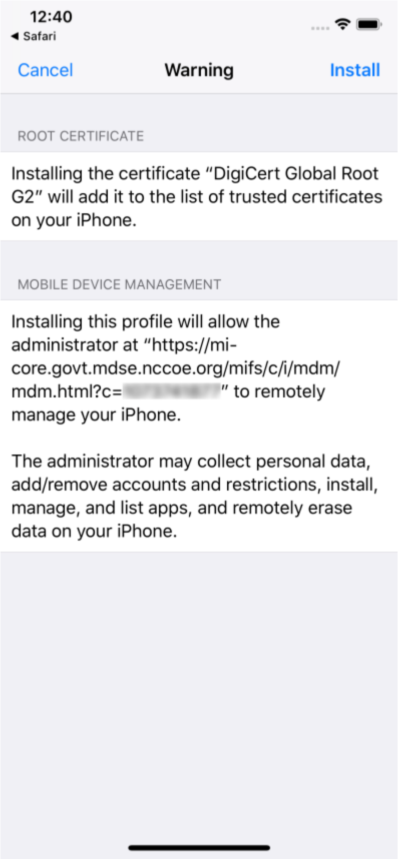
Contains Device Enrollment Challenge

5. At the **Warning** screen:

   a. Verify that information under **Root Certificate** and **MDM** is consistent with information provided by your mobile device administrator.

   b. Select **Install**.

Figure 2-162 Profile Installation Warning



ROOT CERTIFICATE

Installing the certificate “DigiCert Global Root G2” will add it to the list of trusted certificates on your iPhone.

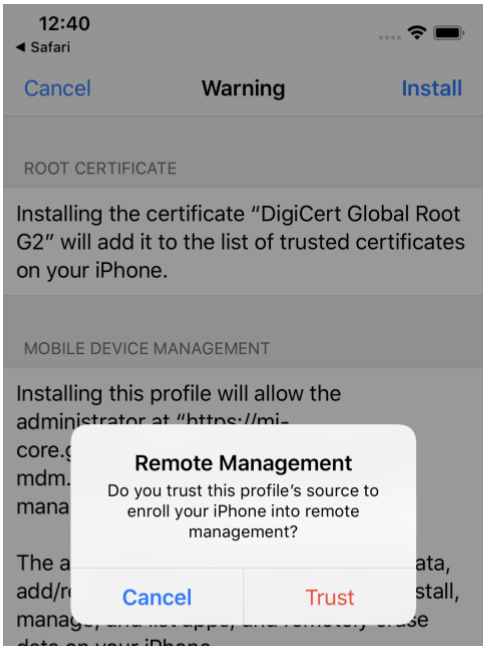
MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://mi-core.govt.mdse.nccoe.org/mifs/c/i/mdm/mdm.html?c=[redacted]” to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPhone.

6. In the **Remote Management** dialogue, select **Trust.**

Figure 2-163 Profile Installation Trust Confirmation



Installing the certificate “DigiCert Global Root G2” will add it to the list of trusted certificates on your iPhone.

Installing this profile will allow the administrator at “https://mi-core.g mdm. mana

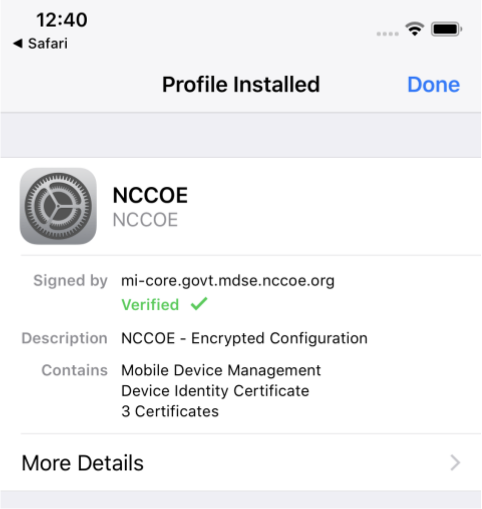
The a ata, add/r stall, manag e

Remote Management

Do you trust this profile’s source to enroll your iPhone into remote management?

7. At the **Profile Installed** screen, select **Done**. The device is now registered with MobileIron.

Figure 2-164 Profile Installation Confirmation



NCCOE
NCCOE

Signed by mi-core.govt.mdse.nccoe.org
Verified ✓

Description NCCOE - Encrypted Configuration

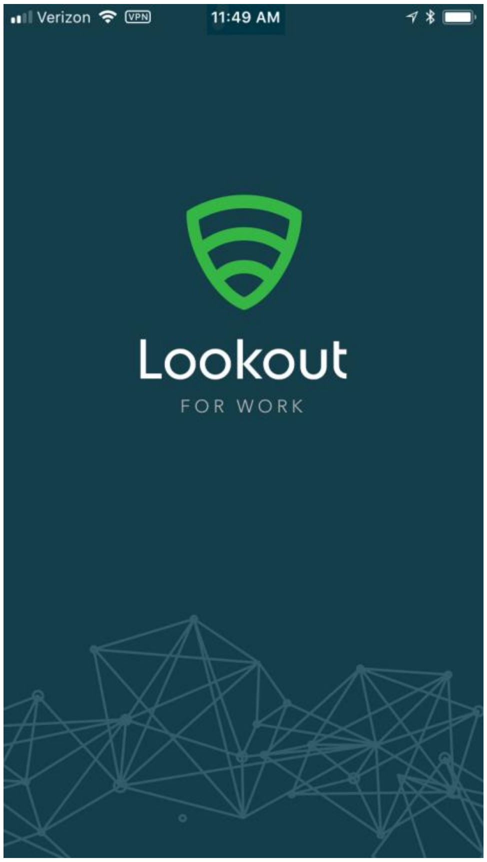
Contains Mobile Device Management
Device Identity Certificate
3 Certificates

2.9.2 Activating Lookout for Work on iOS

The configuration of the Lookout for Work (iOS) app in the MobileIron app catalog causes a configuration file to be included during automatic install. As a result, when a user first launches Lookout for Work, it should be activated without any user interaction. Additional action is required to grant Lookout for Work the permissions necessary for it to provide optimal protection.

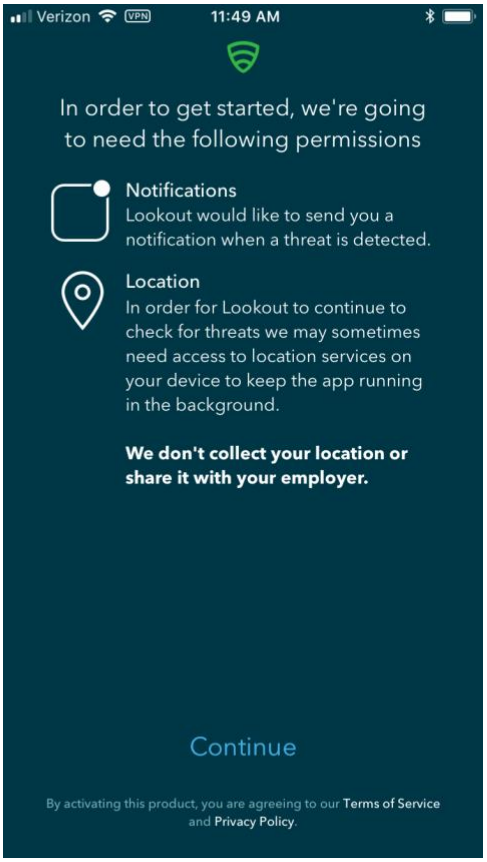
1. Launch the **Lookout for Work** app; activation occurs silently at the **splash** screen.

Figure 2-165 Lookout for Work Splash Screen



2. At the **welcome** screen, select **Continue.**

1797 **Figure 2-166 Lookout for Work Permission Information**



In order to get started, we're going to need the following permissions

Notifications
Lookout would like to send you a notification when a threat is detected.

Location
In order for Lookout to continue to check for threats we may sometimes need access to location services on your device to keep the app running in the background.

We don't collect your location or share it with your employer.

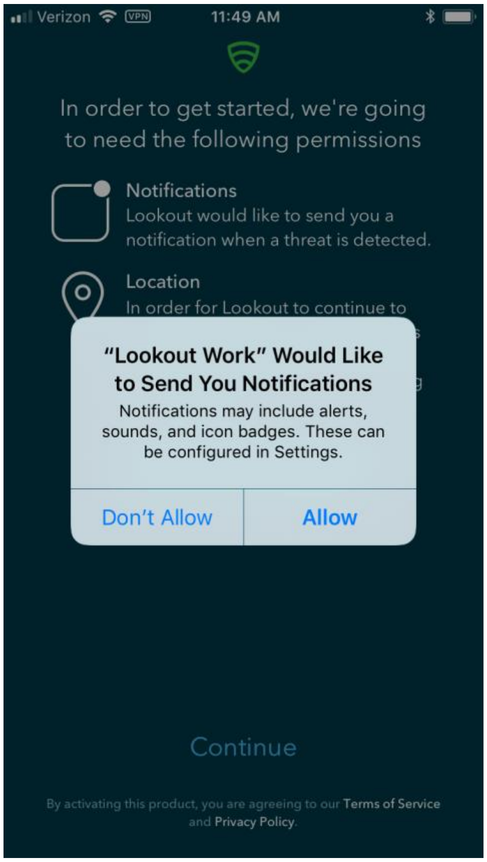
Continue

By activating this product, you are agreeing to our **Terms of Service** and **Privacy Policy**.

1798

1799 3. At the **"Lookout Work"** Would Like to Send You Notifications dialogue, select **Allow**.

Figure 2-167 Notifications Permissions Prompt



In order to get started, we're going to need the following permissions

Notifications
Lookout would like to send you a notification when a threat is detected.

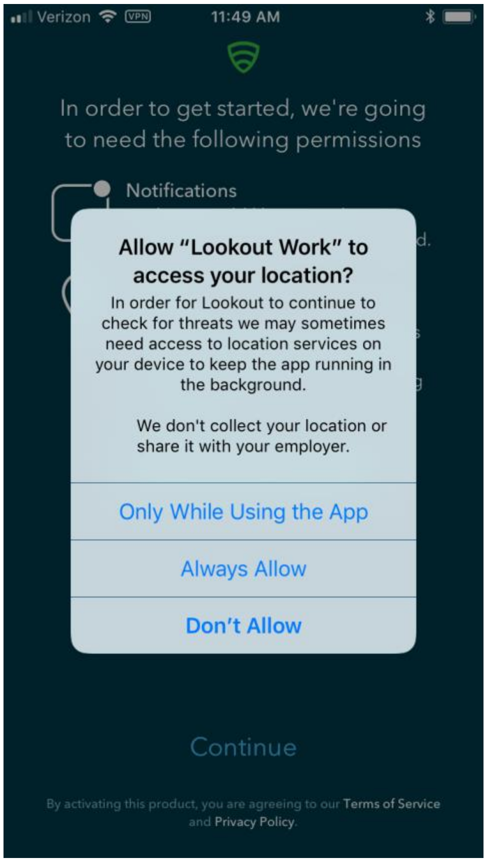
Location
In order for Lookout to continue to

"Lookout Work" Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

By activating this product, you are agreeing to our Terms of Service and Privacy Policy.

4. At the **Allow "Lookout Work" To Access Your Location?** dialogue, select **Always Allow**.

1803 **Figure 2-168 Locations Permission Prompt**



Verizon 11:49 AM

In order to get started, we're going to need the following permissions

Notifications

Allow "Lookout Work" to access your location?

In order for Lookout to continue to check for threats we may sometimes need access to location services on your device to keep the app running in the background.

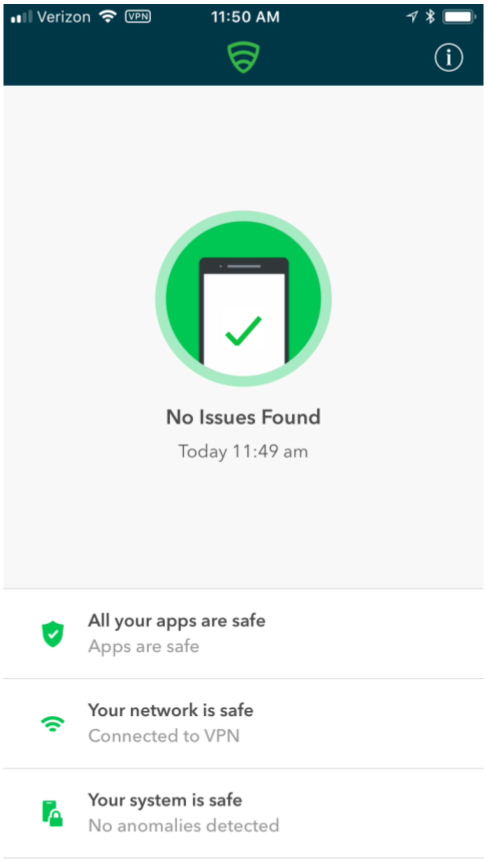
We don't collect your location or share it with your employer.

By activating this product, you are agreeing to our Terms of Service and Privacy Policy.

1804

1805 5. **Lookout for Work** should automatically perform scans of device and app activity and
1806 provide feedback to the user.

Figure 2-169 Lookout for Work Home Screen



Verizon VPN 11:50 AM

No Issues Found

Today 11:49 am

All your apps are safe

Apps are safe

Your network is safe

Connected to VPN

Your system is safe

No anomalies detected

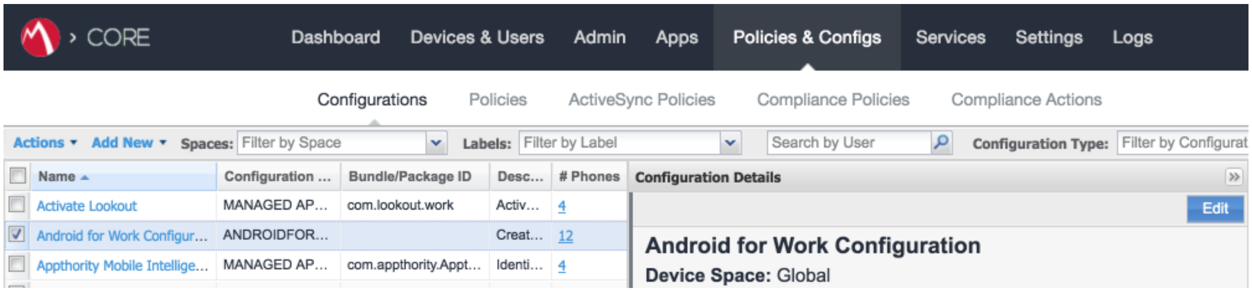
2.9.3 Provisioning Work-Managed Android Devices with a Work Profile

In this scenario, Android devices are deployed as work-managed with a work profile. Enabling this feature for AFW-capable devices requires a change to the AFW configuration. It also requires that the device user already has a personal Google account to provision the work profile; it is not created as part of the workflow to register a device with MobileIron Core.

2.9.3.1 Enable Work Profile on Work-Managed Devices

1. In the **MobileIron Admin** Portal, navigate to **Policies** > **Configs** > **Configurations**.
2. **Enable** the check box in the row for the **AFW** configuration.
3. In the **Configuration Details** pane, select **Edit**.

Figure 2-170 MobileIron AFW Configuration



	Name ▴	Configuration ...	Bundle/Package ID	Desc...	# Phones
□	Activate Lookout	MANAGED AP...	com.lookout.work	Activ...	4
☑	Android for Work Configur...	ANDROIDFOR...		Creat...	12
□	Appthority Mobile Intellige...	MANAGED AP...	com.appthority.Appt...	Identi...	4

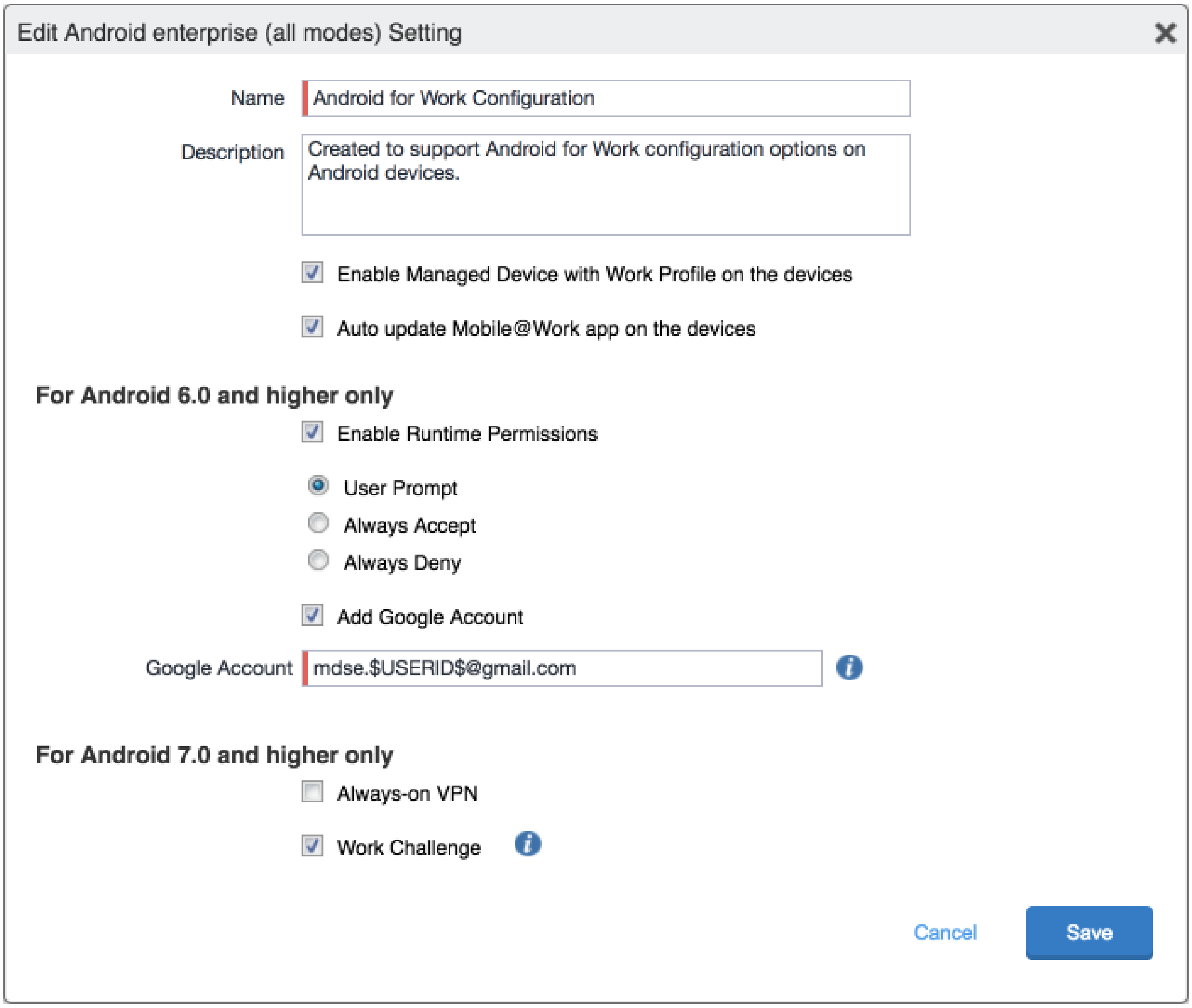
Configuration Details

Android for Work Configuration

Device Space: Global

4. In the **Edit Android enterprise (all modes) Setting** dialogue:
   a. Enable **Enable Managed Devices with Work Profile** on the devices.
   b. Enable **Add Google account**.
   c. In the **Google Account** text box, provide a valid Google domain account. The example in our reference implementation will map a MobileIron user ID of gema to and email address of **mdse.gema@gmail.com**. See *MobileIron Core 9.4.0.0 Device Management Guide for AFW* for a list of variables to appropriately adapt this field to your existing identity management strategy.
   d. Select **Save.**

Figure 2-171 AFW Configuration



Edit Android enterprise (all modes) Setting

Name: Android for Work Configuration

Description: Created to support Android for Work configuration options on Android devices.

☑ Enable Managed Device with Work Profile on the devices

☑ Auto update Mobile@Work app on the devices

For Android 6.0 and higher only

☑ Enable Runtime Permissions

● User Prompt
○ Always Accept
○ Always Deny

☑ Add Google Account

Google Account: mdse.$USERID$@gmail.com

For Android 7.0 and higher only

□ Always-on VPN

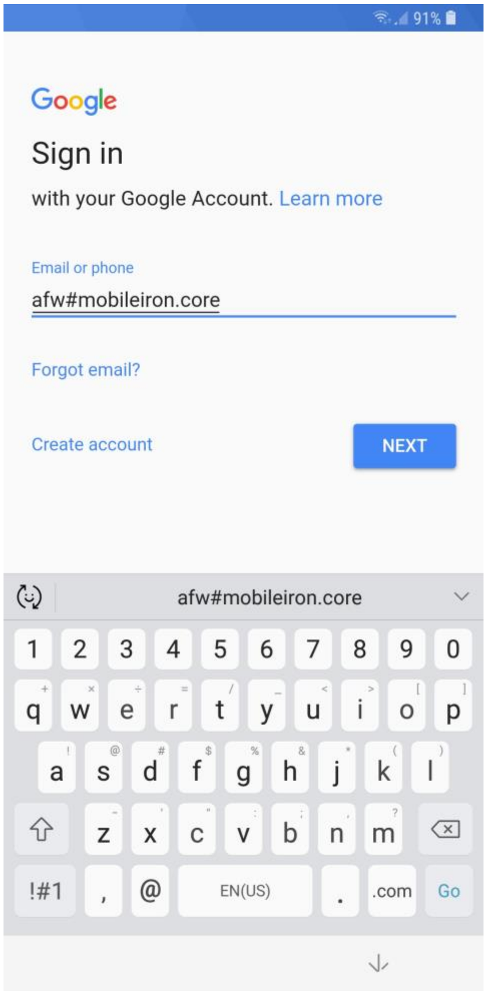
☑ Work Challenge

2.9.3.2 Registering Android Devices

The following steps can only be completed when working with an Android device that is still set to (or has been reset to) factory default settings.

5. When prompted to **sign in** with your Google Account:
    a. In the **Email or phone field,** enter **afw#mobileiron.core**.
    b. Select **Next.**

Figure 2-172 MobileIron Enrollment Process



Google

Sign in

with your Google Account. Learn more

Email or phone

afw#mobileiron.core

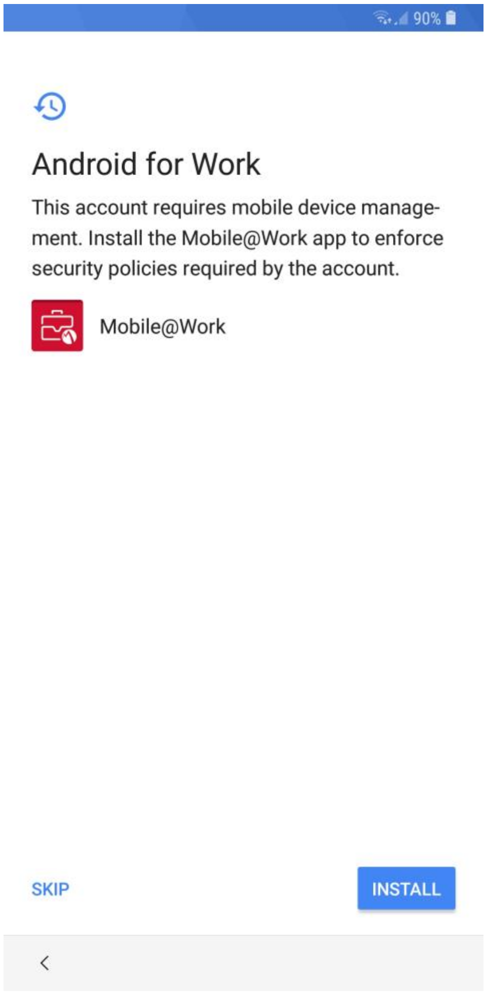
Forgot email?

Create account

NEXT

6. When **AFW** prompts you to install *Mobile@Work*, select **Install**; this will download the Mobile@Work client to the device.

1841 Figure 2-173 AFW Enrollment



Android for Work

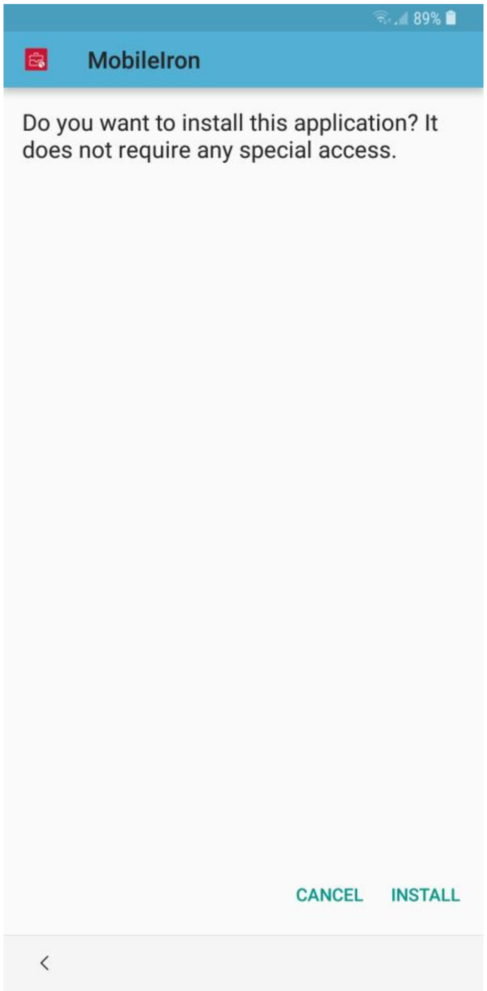
This account requires mobile device management. Install the Mobile@Work app to enforce security policies required by the account.

Mobile@Work

1842

1843 7. At the prompt to install MobileIron, select **Install.**

1844 Figure 2-174 MobileIron Installation

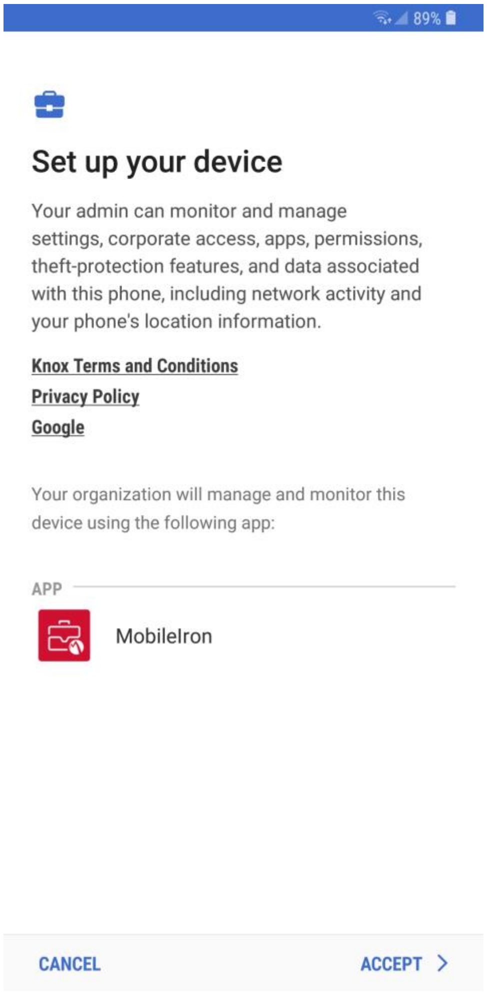


Do you want to install this application? It does not require any special access.

1845

1846 8. At the Set up your device screen, select **Accept**.

Figure 2-175 Accepting AFW Terms and Conditions



Set up your device

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information.

Knox Terms and Conditions

Privacy Policy

Google

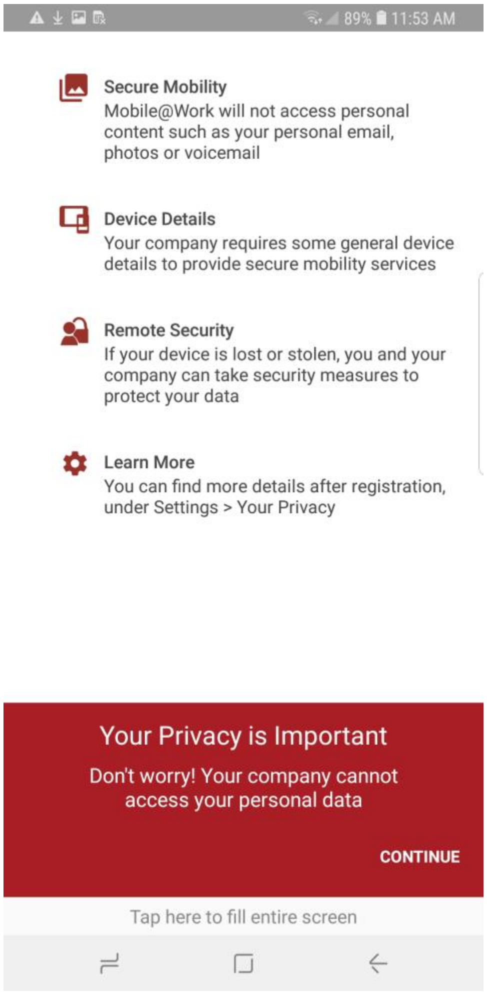
Your organization will manage and monitor this device using the following app:

APP

MobileIron

9. This screen notifies the user of the data that *Mobile@Work* collects and how it is used. When this information has been reviewed, select **Accept.** Mobile@Work will minimize and return to the operating system home screen.

Figure 2-176 MobileIron Privacy Information



Secure Mobility
Mobile@Work will not access personal content such as your personal email, photos or voicemail

Device Details
Your company requires some general device details to provide secure mobility services

Remote Security
If your device is lost or stolen, you and your company can take security measures to protect your data

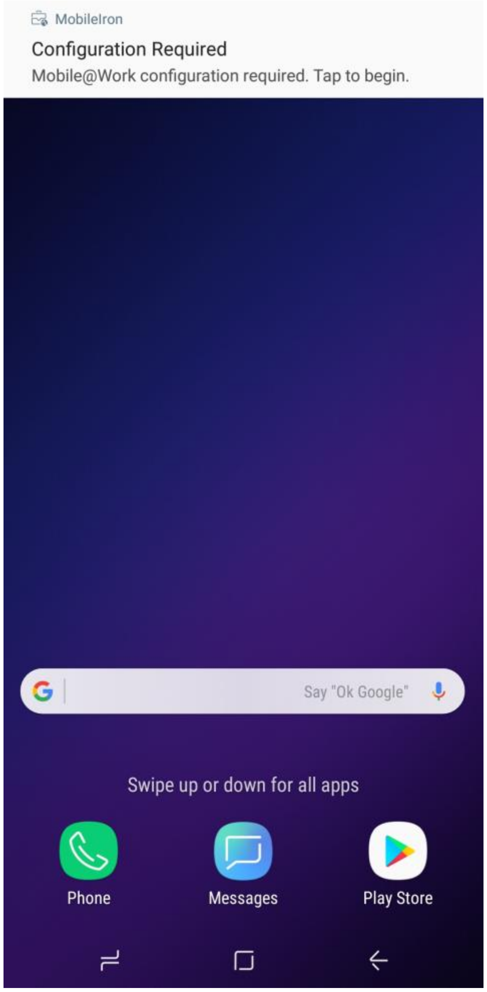
Learn More
You can find more details after registration, under Settings > Your Privacy

Your Privacy is Important

Don't worry! Your company cannot access your personal data

10. When MobileIron sends a **Configuration Required** notification, select the **notification.**

1855 **Figure 2-177 MobileIron Configuration Required Notification**

1856 

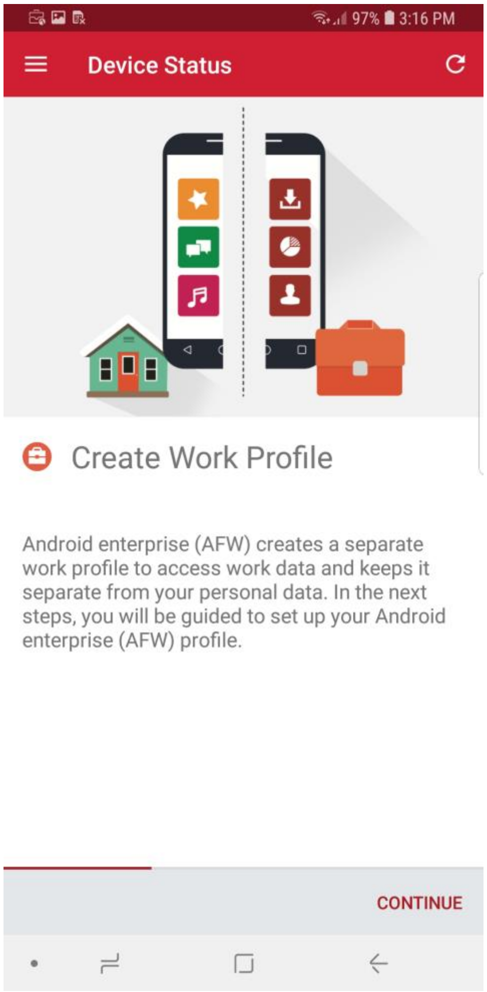
MobileIron

Configuration Required

Mobile@Work configuration required. Tap to begin.

1857 11. On the **Device Status** > **Create Work Profile** screen, select **Continue**.

1858 **Figure 2-178 MobileIron Device Status**



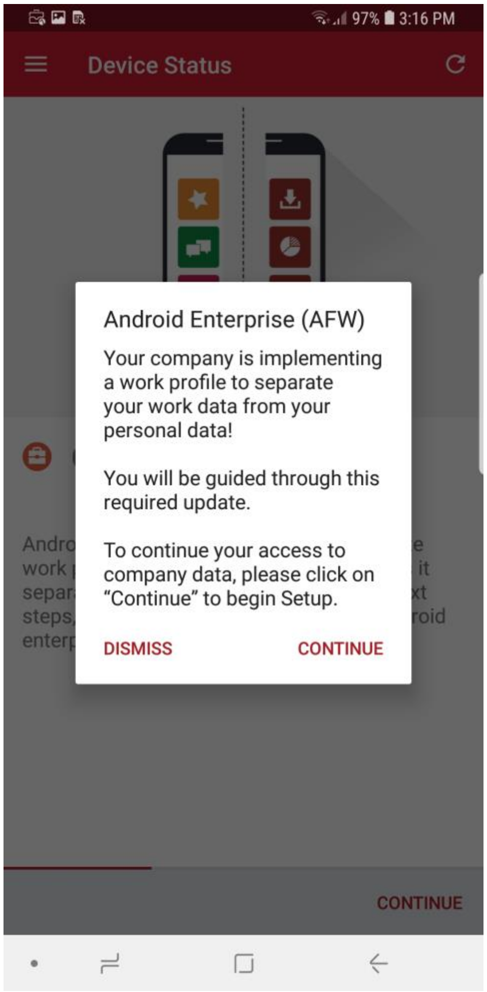
Create Work Profile

Android enterprise (AFW) creates a separate work profile to access work data and keeps it separate from your personal data. In the next steps, you will be guided to set up your Android enterprise (AFW) profile.

1859

1860 12. At the **AFW** prompt, select **Continue.**

Figure 2-179 AFW Configuration



Android Enterprise (AFW)

Your company is implementing a work profile to separate your work data from your personal data!

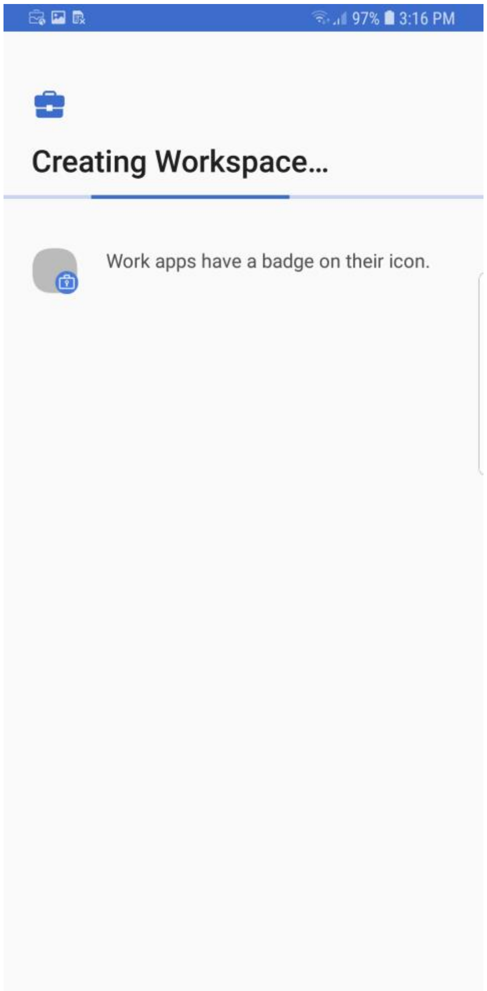
You will be guided through this required update.

To continue your access to company data, please click on "Continue" to begin Setup.

DISMISS CONTINUE

13. **AFW** will notify the user that it is creating the personal workspace. The next two screens repeat **Steps 7** and **8** as above.

1865 **Figure 2-180 AFW Workspace Creation**



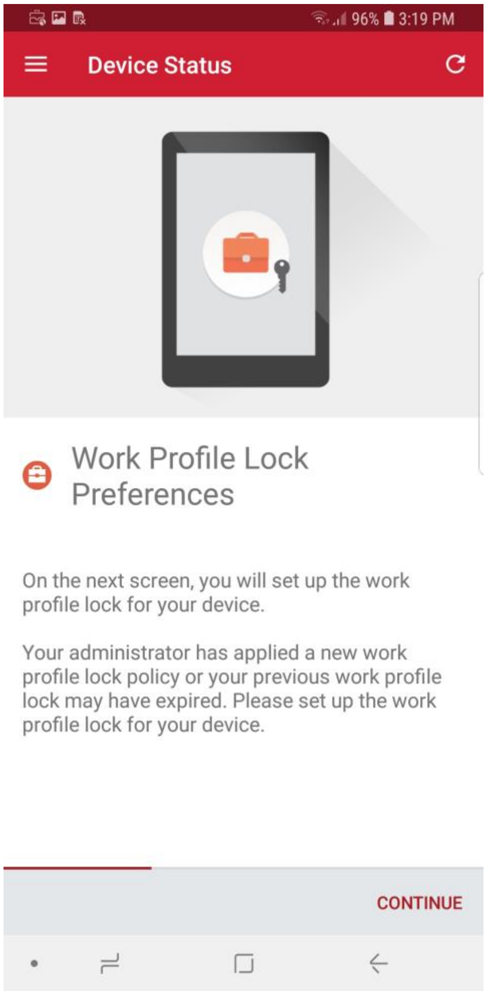
Creating Workspace...

Work apps have a badge on their icon.

1866

1867 14. At the **Device Status** > **Work Profile Lock Preferences** screen, select **Continue.**

Figure 2-181 MobileIron Work Profile Lock Preferences



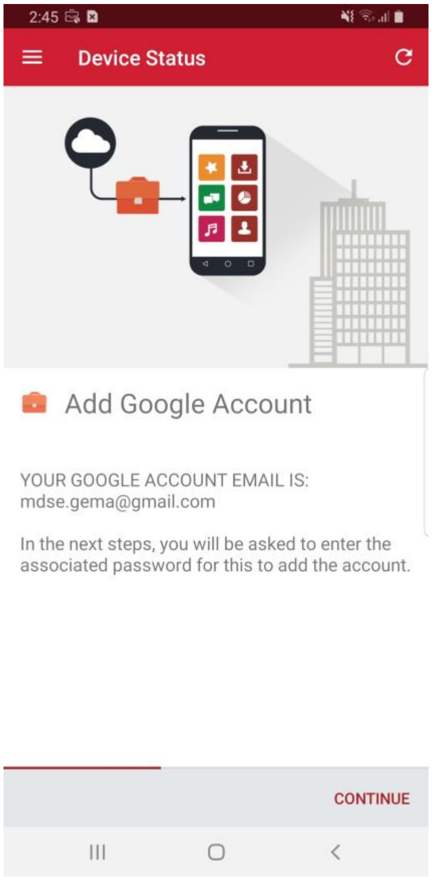
Work Profile Lock Preferences

On the next screen, you will set up the work profile lock for your device.

Your administrator has applied a new work profile lock policy or your previous work profile lock may have expired. Please set up the work profile lock for your device.

15. The user will be prompted to create a passcode to protect the AFW container.
16. At the **Device Status** > **Add Google Account** screen, select **Continue.**

Figure 2-182 MobileIron Google Account Configuration



Add Google Account

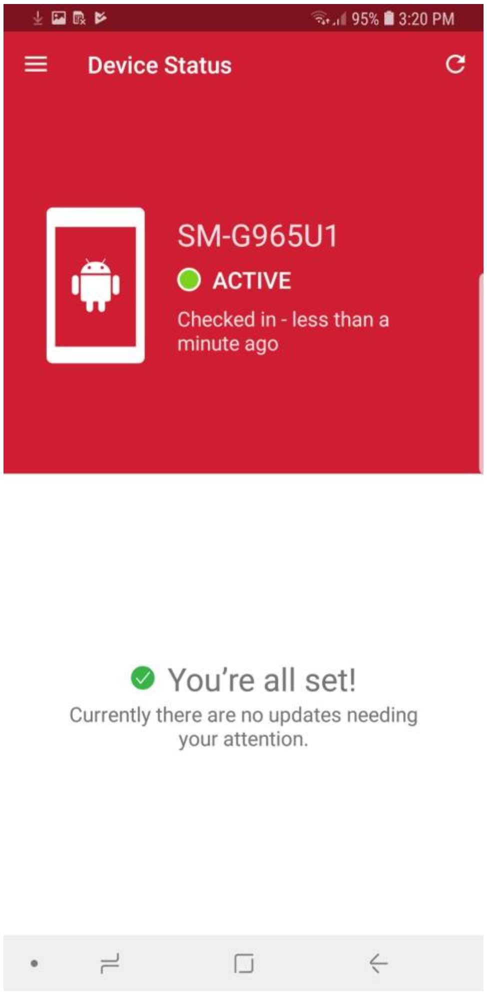
YOUR GOOGLE ACCOUNT EMAIL IS:
mdse.gema@gmail.com

In the next steps, you will be asked to enter the associated password for this to add the account.

17. The user will be prompted to authenticate to the same Google domain account mapped to their MobileIron account based on the email address set in the AFW configuration in MobileIron Core. In our example implementation, the mapped Google account is **mdse.gema@gmail.com**.

18. Once the *Mobile@Work* app has been provisioned with the user's account, the Device Status screen should appear; the device has now successfully been provisioned into MobileIron.

1881 **Figure 2-183 MobileIron Device Status**



SM-G965U1

● ACTIVE

Checked in - less than a minute ago

✓ You're all set!

Currently there are no updates needing your attention.

1882

Appendix A List of Acronyms

AD	Active Directory
AFW	Android for Work
API	Application Programming Interface
CA	Certificate Authority
CN	Common Name
CSP	Common Service Provider
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
DPC	Derived Personal Identity Verification Credential
EMM	Enterprise Mobility Management
FQDN	Fully Qualified Domain Name
GOVT	Government
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMEI	International Mobile Equipment Identity
ID	Identifier
IP	Internet Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MDS	Mobile Device Security
MES	Mobile Endpoint Security
MTP	Mobile Threat Posture
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OU	Organizational Unit
OVA	Open Virtualization Appliance
PLIST	Property List

SCEP	Simple Certificate Enrollment Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B Glossary

Application Programming Interface (API)

A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality [1]

App-Vetting Process

The process of verifying that an app meets an organization's security requirements. An app vetting process comprises app testing and app approval/rejection activities [2]

Authenticate

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system [3]

Certificate

A data structure that contains an entity’s identifier(s), the entity's public key (including an indication of the associated set of domain parameters) and possibly other information, along with a signature on that data set that is generated by a trusted party, i.e. a certificate authority, thereby binding the public key to the included identifier(s) [4]

Certificate Authority (CA)

A trusted entity that issues and revokes public key certificates [5]

Demilitarized Zone (DMZ)

An interface on a routing firewall that is similar to the interfaces found on the firewall’s protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. [6]

Derived Personal Identity Verification (PIV)

A credential issued based on proof of possession and control of the PIV Card, so as not to duplicate the identity proofing process as defined in [SP 800-63-2]. A Derived PIV Credential token is a hardware or software-based token that contains the Derived PIV Credential. [7]

Hypertext Transfer Protocol (HTTP)

A standard method for communication between clients and Web servers [8]

Hypertext Transfer Protocol Secure (HTTPS)

HTTP transmitted over TLS [9]

Internet Protocol (IP) addresses

Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks [10]

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol, or LDAP, is a directory access protocol. In this document, LDAP refers to the protocol defined by RFC 1777, which is also known as LDAP V2. LDAP V2 describes unauthenticated retrieval mechanisms. [11]

Local Area Network (LAN)

A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network [12]

Mutual Authentication

The process of both entities involved in a transaction verifying each other [13]

Passphrase

A passphrase is a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage, but is generally longer for added security. [14]

Personal Identity Verification (PIV)

A physical artifact (e.g., identity card, “smart” card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in FIPS PUB 201. [15]

Risk Analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. [16]

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. [17]

Root Certificate Authority (CA)

In a hierarchical public key infrastructure (PKI), the certification authority (CA) whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain [18]

Appendix C References

[1] National Institute of Standards and Technology (NIST). Information Technology Laboratory (ITL) Glossary, "Application Programming Interface Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Application-Programming-Interface. [Accessed 1 May 2019].

[2] NIST. ITL Glossary, "Application Programming Interface Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/App-Vetting-Process. [Accessed 1 May 2019].

[3] NIST. ITL Glossary, "Authenticate Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/authenticate. [Accessed 1 May 2019].

[4] NIST. ITL Glossary, "Certificate Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/certificate. [Accessed 1 May 2019].

[5] NIST. ITL Glossary, "Certificate Authority (CA) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Certificate-Authority. [Accessed 1 May 2019].

[6] NIST. ITL Glossary, "Demilitarized Zone (DMZ) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/demilitarized-zone. [Accessed 1 May 2019].

[7] NIST. ITL Glossary, "Derived Personal Identity Verification (PIV) Credential Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Derived-PIV-Credential. [Accessed 1 May 2019].

[8] NIST. ITL Glossary, "Hypertext Transfer Protocol (HTTP) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/HTTP. [Accessed 1 May 2019].

[9] NIST. ITL Glossary, "Hypertext Transfer Protocol over Transport Layer Security Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Hypertext-Transfer-Protocol-over-Transport-Layer-Security. [Accessed 1 May 2019].

[10] NIST. ITL Glossary, "Internet Protocol (IP) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/internet-protocol. [Accessed 1 May 2019].

[11] NIST. ITL Glossary, "Lightweight Directory Access Protocol Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Lightweight-Directory-Access-Protocol. [Accessed 1 May 2019].

[12] NIST. ITL Glossary, "Local Area Network (LAN) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Local-Area-Network. [Accessed 1 May 2019].

[13] NIST. ITL Glossary, "Mutual Authentication Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/mutual-authentication. [Accessed 1 May 2019].

[14] NIST. ITL Glossary, "Passphrase Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Passphrase. [Accessed 1 May 2019].

[15] NIST. ITL Glossary, "Personal Identity Verification (PIV)," [Online]. Available: https://csrc.nist.gov/glossary/term/personal-identity-verification. [Accessed 1 May 2019].

[16] NIST. ITL Glossary, "Risk Analysis," [Online]. Available: https://csrc.nist.gov/glossary/term/risk-analysis. [Accessed 1 May 2019].

[17] NIST. "NIST Special Publication 800-39, Managing Information Security Risk," March 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf. [Accessed 1 May 2019].

[18] NIST. "NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure," February 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf. [Accessed 1 May 2019].