NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security

Corporate-Owned Personally-Enabled (COPE)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Joshua M. Franklin
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau
Dr. Behnam Shariati
Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security
Corporate-Owned Personally-Enabled (COPE)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

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.*

DRAFT

July 2019

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

NIST SPECIAL PUBLICATION 1800-21A

Mobile Device Security

Corporate-Owned Personally-Enabled (COPE)

Volume A:
Executive Summary

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

Executive Summary

- 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 National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore 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.

CHALLENGE

Mobile devices are a staple within modern workplaces. As employees use these devices to perform everyday enterprise tasks, organizations are challenged with ensuring that devices regularly process, modify, and store sensitive data securely. These devices bring unique threats to the enterprise and should be managed in a manner distinct from traditional desktop platforms. This includes securing against different types of network-based attacks on mobile devices that have an always-on connection to the internet.

Managing the security of workplace mobile devices and minimizing the risk posed can be challenging because there are many mobile device security tools available. Proper implementation is difficult to achieve for an end user because the method of implementation varies considerably from tool to tool. In addition, unfamiliarity with the threats to mobile devices can further compound these implementation difficulties.

SOLUTION

To address the challenge of securing mobile devices within an enterprise, NIST built an example solution in a lab environment at the NCCoE to demonstrate mobile management tools that enterprises can use to secure their networks. These technologies are configured to protect organizational assets and end-user privacy, providing methodologies to enhance the security and privacy posture of the adopting organization.

Both Apple iOS and Android devices are used in the example solution, which includes detailed device configurations and enterprise mobility management policies provisioned to the devices. The foundation of this architecture is based on federal U.S. guidance, including that from NIST 800 series publications, National Information Assurance Partnership, U.S. Department of Homeland Security, and the Federal

Chief Information Officers Council. These standards, best practices, and certification programs help ensure the confidentiality and integrity of enterprise data on mobile systems.

This guide provides:

- a detailed example solution and capabilities that address risk and implementation of security controls
- a demonstration of the approach using commercially available products
- how-to instructions for implementers and security engineers, with instructions on integrating and configuring the example solution into their organization's enterprise in a manner that can achieve security goals with minimum impact on operational processes

The NCCoE sought existing technologies that provided the following capabilities:

- enhanced protection of data that resides on the mobile device
- centralization of management systems to deploy policies and configurations to devices
- ability to evaluate the security of mobile applications
- inhibition of the eavesdropping of mobile device data when traversing a network
- privacy settings that protect end-user data
- protection from phishing attempts

Commercial, standards-based products such as the ones we used are readily available and interoperable with existing information technology (IT) infrastructure and investments.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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 a solution.

BENEFITS

The NCCoE's practice guide *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* can help your organization:

- reduce adverse effects on the organization if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- apply robust, standards-based technologies using industry best practices
- reduce privacy risks to users through privacy protections
- provide users with enhanced protection against loss of personal and business data when a device is stolen or misplaced
- deploy enterprise management technologies to improve the security of enterprise networks, devices, and applications

- reduce risk so that employees can access the necessary data from nearly any location, using a wide selection of mobile devices and networks
- enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implement government standards for mobile security

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at mobile-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

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.

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit http://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200

NIST SPECIAL PUBLICATION 1800-21B

Mobile Device Security

Corporate-Owned Personally-Enabled (COPE)

Volume B:
Approach, Architecture, and Security Characteristics

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

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-21B Natl. Inst. Stand. Technol. Spec. Publ. 1800-21B, 148 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 Summary

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide seeks to address mobile device security implementation challenges in several ways: by analyzing a set of mobile security and privacy threats; exploring mitigating technologies; and describing a reference design based upon those technologies to help mitigate the identified threats.

Incorporating mobile devices into the organizational enterprise provides greater flexibility in how employees access organizational resources. For some organizations, this flexibility supports a hybrid approach enhancing their traditional in-office processes with more responsive communication and adaptive workflows.

For others, this flexibility, combined with growing mobile functionality, fosters a mobile-first approach in which their employees primarily communicate and collaborate using mobile devices. However, some of the features that make mobile devices increasingly flexible and functional also make them challenging to deploy and manage with security in mind.

Further, organizations are becoming progressively cognizant of the privacy implications for their employees that arise from using mobile security technologies. Therefore, developing a successful mobile deployment strategy requires organizations to evaluate their security and privacy requirements.

Although organizations may be aware of the security and privacy risks that can be introduced by mobile devices, addressing them strategically and technically can pose a barrier to implementing mobile device security capabilities. This barrier is particularly challenging for businesses to overcome. As a result, they may choose to enable mobile access with minimal acceptable use policies, employee awareness, or security controls to limit implementation challenges.

To help address mobile device security and privacy risks, this document's reference design provides:

- a description of a mobile deployment strategy featuring an on-premises enterprise mobility management (EMM) solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities in support of a corporate-owned personally-enabled (COPE) mobile device usage scenario
- a series of How-To Guides—step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture—to help security engineers rapidly deploy and evaluate our example solution in their test environment

The example solution of our reference design uses standards-based, commercially available products. It can be used directly by any organization with a COPE usage scenario by implementing a security infrastructure that supports integration of on-premises with cloud-hosted mobile security technologies. Alternatively, an organization may use our reference design and example solution in whole or part as the basis for a custom solution that realizes the security and privacy characteristics that best support its unique mobile device usage scenario.

1.1 Challenge

Mobile devices are a staple within modern workplaces, and as employees use these devices to perform everyday enterprise tasks, organizations are challenged with ensuring that devices regularly process, modify, and store sensitive data securely. They bring unique threats to the enterprise and need to be managed differently from traditional desktop platforms.

Due to their unique capabilities, mobile devices' specific security challenges can include:

- securing their always-on-connections to the internet from network-based attacks
- securing the data on devices to prevent compromise via malicious applications
- protecting them from phishing attempts that try to collect user credentials or entice a user to install software
- selecting from the many mobile device management tools available and implementing their protection capabilities consistently
- identifying threats to mobile devices and how to mitigate them

Given these challenges, managing the security of workplace mobile devices and minimizing the risk posed can be complex. By providing an example solution that organizations can make immediate use of, this guide provides an example solution to help simplify deployment of mobile device security capabilities.

1.2 Solution

In our lab at the National Cybersecurity Center of Excellence (NCCoE), NIST engineers built an environment that contains an example solution for managing the security of mobile devices. In this guide, we show how an enterprise can leverage this infrastructure to implement on-premises enterprise mobility management (EMM), mobile threat defense (MTD), mobile threat intelligence (MTI), application vetting, secure boot/image authentication, and virtual private network (VPN) services.

Further, these technologies were configured to protect organizational assets and end-user privacy, providing methodologies to enhance the security posture of the adopting organization. The foundation of this architecture is based on federal United States guidance, including that from the NIST 800 series publications [1], the National Information Assurance Partnership (NIAP) [2], the Department of Homeland Security [3], and the Federal Chief Information Officers (CIO) Council [4]. These standards, best practices, and certification programs help ensure the confidentiality, integrity, and availability of enterprise data on mobile systems.

This guide provides:

- a detailed example solution with capabilities that mitigate common mobile threats
- a demonstration of an approach that uses commercially available products
- step-by-step installation how-to guidance for implementers, which is designed to easily integrate with existing systems to improve the organization's mobile security posture with minimal disruption to operations

The NCCoE sought existing technologies that provided the following capabilities:

- ability to help protect data resident on the mobile device
- utilization of centralized management systems to deploy policies and configurations to devices
- vetting the security of mobile applications
- ability to help protect data from eavesdropping while traversing a network
- privacy settings to enable the predictability, manageability, and disassociability of end-users' personally identifiable information (PII)

Commercial, standards-based products such as the ones we used are readily available and interoperable with existing information technology (IT) infrastructure and investments.

1.2.1 Standards and Guidance

The following standards and guidance have been consulted for this publication:

- NIST Cybersecurity Framework Version 1.1 [5]
- NIST Mobile Threat Catalogue [6]
- NIST Risk Management Framework [7]
- NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [8]
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [9]
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [10]
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [11]
- NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [12]
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [13]
- NIST SP 800-63-3, *Digital Identity Guidelines* [14]
- NIST SP 800-113, *Guide to SSL VPNs* [15]

- NIST SP 800-114 Revision 1, *User’s Guide to Telework and Bring Your Own Device (BYOD) Security* [16]
- NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [17]
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [18]
- NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [19]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [20]
- Center for Internet Security [21]
- Executive Office of the President, Bring Your Own Device Toolkit [22]
- Federal Chief Information Officers (CIO) Council and Department of Homeland Security (DHS) Mobile Security Reference Architecture, Version 1.0 [23]
- Digital Services Advisory Group and Federal Chief Information Officers Council, Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis [24]
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, *Information technology–Security techniques–Information security management systems–Requirements* [25]
- Mobile Computing Decision Example Case Study [26]
- Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), Mobility Strategy Development Guidelines Working Group Document [27]
- MSCT ATARC, Mobile Threat Protection App Vetting and App Security Working Group Document [28]
- MSCT, Device Procurement and Management Guidance [29]
- MSCT, Mobile Device Management (MDM), MDM Working Group Document [30]
- MSCT, Mobile Services Roadmap, MSCT Strategic Approach [31]
- NIAP U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 3.0 [32]
- NIAP U.S. Government Approved Protection Profile—Protection Profile for Mobile Device Fundamentals Version 3.1 [33]
- NIAP U.S. Government Approved Protection Profile—Protection Profile for Mobile Device Management Version 3.0 [34]
- NIAP Product Compliant List [35]

- United States Office of Management and Budget (OMB), Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services [36]
- The United States Government Configuration Baseline (USGCB) [37]
- United State Department of Homeland Security (DHS) Study on Mobile Device Security [38]

Note that Defense Federal Acquisition Regulation Supplement regulations are out of scope for this effort.

1.3 Benefits

The potential business benefits of the example solution explored by this project are to:

- provide users with enhanced protection against both malicious applications and loss of personal and business data when a device is stolen or misplaced
- reduce adverse effects on an organization if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- provide visibility for system administrators into mobile security events, enabling automated identification and notification of a compromised device
- provide modular architecture based on technology roles while remaining vendor-agnostic
- facilitate multiple mobile device usage scenarios using COPE devices
- apply robust, standards-based technologies using industry best practices
- demonstrate secure mobile access to organizational resources such as intranet, email, contacts, and calendar
- illustrate the application of the NIST Risk Management Framework to mobility scenarios

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate how to improve mobile device security with on-premises mobile device management solutions. 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 **(you are here)**

- NIST SP 1800-21C: *How-To Guides* – instructions for building the example solution

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 securing mobile devices from threats that are distinct from traditional desktop platforms
- example solution built at the 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 this part of the guide, *NIST SP 1800-21B,* which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed
- Section 4.3, Security Control Map, maps the security characteristics 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 to improve mobile device security with on-premises mobile device management solutions.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-21C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create 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 we used, and Appendix H 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.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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.

3 Approach

The NIST build team surveyed reports of mobile device security trends and openly invited the mobile device security community—including vendors, researchers, administrators, and users—to engage in a discussion about pressing cybersecurity challenges. The community expressed two significant messages.

First, administrators experienced confusion about which policies and standards—out of myriad sources—should be implemented. Second, mobile device users were frustrated by the degrees to which enterprises have control over their mobile devices and maintain visibility into their personal activity.

Therefore, the NIST build team reviewed the primary standards, best practices, and guidelines from government sources and implemented a COPE usage scenario within this build. Additionally, this effort highlights several security characteristics and capabilities that are documented within the Mobile Device Security for Enterprises building block [39].

3.1 Audience

This practice guide is for organizations that want to enhance mobile device deployment and management security, principally smartphones and tablets. It is intended for executives, security managers, engineers, administrators, and others who are responsible for acquiring, implementing, and maintaining mobile enterprise technology, including centralized device management, application vetting, and endpoint protection systems.

This document will be of particular interest to system architects already managing mobile deployment solutions and those looking to deploy mobile devices in the near term. It assumes readers have a basic understanding of mobile device technologies and enterprise security principles. Please refer to Section 2 for how different audiences can effectively use this guide.

3.2 Scope

The scope of this build includes managing mobile smartphones and tablets with on-premises EMM. Laptops are excluded from the scope of this publication, as the security controls available today for laptops differ significantly from those available for smartphones and tablets, although this is changing with the emergence of unified endpoint management capabilities.

Devices with minimal computing capability are also excluded, including feature phones, wearables, and devices classified as part of the Internet of Things. Classified systems, devices, data, and applications are not addressed within this publication.

The build team devised a fictional scenario centered around a mock organization (Orvilia Development) to provide context to our risk assessment and to enable us to architect a reference design to solve common enterprise mobile security challenges. Use of a scenario like Orvilia Development's exemplifies the issues that an organization may face when addressing common enterprise mobile security challenges. We intend for the example solution proposed in this practice guide to be broadly applicable to enterprises, including both the public and private sectors.

To focus specifically on mobile device threats that Orvilia may be exposed to with its recent organizational changes, the example solution does not specifically focus on insider threat events with corresponding mitigations.

Additional options for deployment of Android, Apple, and Samsung Knox managed devices are discussed in Appendix D.

3.2.1 Orvilia Development

The fictional organization, Orvilia Development, is a small start-up company providing IT services to many private sector organizations. Its service offerings include developing scalable web applications, improving existing IT systems, project management, and procurement. Orvilia recently won its first government contract. Given the organization's current security posture, particularly in its use of mobile devices, complying with government regulations and heightened cybersecurity standards presents it with new challenges.

Orvilia has a simple deployment of on-premises IT resources. It hosts its own Microsoft Active Directory domain, Microsoft Exchange email server, and web-based resources for employees, such as timekeeping and travel support. All enterprise resources can be directly accessed by employees locally or remotely from any internet-connected device by using password-based authentication. Orvilia also provides its employees with corporate-owned mobile devices. These may be used for personal activity, including phone calls, instant messaging, and installation and use of social applications. Employees also regularly work outside the office and frequently use public Wi-Fi networks at hotels, airports, and coffee shops.

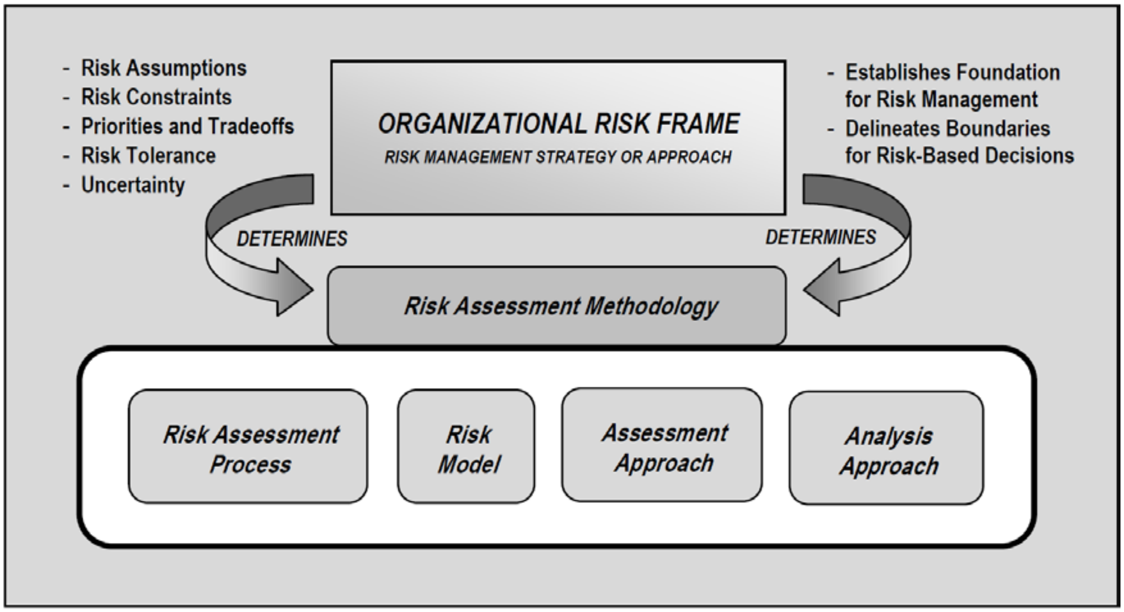
Orvilia's mobile device deployment practice is still developing; it has minimal mobile device policies and has not implemented any additional security mechanisms such as enterprise mobility management. All policy and security enforcement actions are performed manually on an ad-hoc basis. Employees are expected to secure their own COPE devices, for instance via the timely installation of operating system (OS) updates, and to exercise good judgment regarding any personal use.

However, no mechanisms have been put into place to prevent or detect misuse or device compromise. Further, corporate policy prohibits access to the corporate network from personally owned mobile devices, but no technical safeguards have been implemented to prevent employees from doing so. This posture had been promoted based on the organization's small size, high level of employee technical acumen, and lack of awareness that it has been significantly impacted by any cybersecurity incidents.

However, Orvilia's new status as a contractor to a civilian government agency calls for it to achieve and maintain compliance with government policies, which require compliance with cybersecurity best practices and applicable standards. For example, Orvilia is required to secure its access to and storage of sensitive government information, which its employees will need to access from their mobile devices, both locally at agency sites and remotely from Orvilia or during travel.

In addition to meeting compliance requirements rising from its contractual obligations to a government agency, Orvilia leadership is concerned about the potential for future incidents where nation-state malicious actors might obtain sensitive government data from unsecured devices and infrastructure. Therefore, a risk assessment as described in NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [9] was performed using the risk management concepts shown in Figure 3-1.

Figure 3-1 Risk Management Approach



The risk assessment revealed that Orvilia's current mobile infrastructure places the organization at risk of intrusion and compromise of sensitive data. The results of the risk assessment process are presented in Appendix E.

Based on the risk assessment findings, Orvilia chose to invest in security improvements to its mobile infrastructure. Details of Orvilia's new mobile device security infrastructure are provided in Section 4. As described in Section 4's architecture design, Orvilia's new infrastructure addressed the concerns identified in its risk assessment. Orvilia's risk assessment team reviewed guidance by standards organizations and government agencies as part of its process and identified the standards and guidance identified in Section 1.2.1 as applicable to its organizational mobile use case.

3.3 Assumptions

This project is guided by the following assumptions:

- The solution was developed in a lab environment based on a typical organization's IT enterprise. It does not reflect the complexity of a production environment.
- An organization has access to the skills and resources required to implement a mobile device security solution.
- The benefits of adopting this particular mobile device security solution outweigh any additional performance, reliability, or security risks that may be introduced. However, we draw the reader's attention to the fact that implementation of any security controls has the potential to

increase or decrease the attack surface within an enterprise, the actual impact of which will vary from organization to organization. Because the organizational environment in which this build could be implemented represents a greater level of complexity than is captured in the current guide, we assume that organizations will first examine the implications for their current environment before implementing any part of the proposed solution.

- Organizations have either already invested or are willing to invest in the security of mobile devices used within their organization and of their IT systems more broadly. As such, we assume they either have the technology in place to support this implementation or have access to the off-the shelf information security technology used in this build, which we assume will perform as described by the respective product vendor.
- Organizations have familiarized themselves with existing standards and any associated guidelines (e.g., NIST Cybersecurity Framework [5], NIST SP 800-124 Revision 1 [17], NIST SP 1800-4 [8]) relevant to implementation of the solution proposed in this practice guide. We also assume that any existing technology to be used in the proposed solution has been implemented in a manner consistent with these standards.
- Organizations have instituted relevant mobile device security policies and that these will be updated based on implementation of this solution.

3.3.1 Systems Engineering

Some organizations use a systems engineering-based approach in planning and implementing their IT projects. Organizations wishing to implement IT systems are encouraged to conduct robust requirements development, taking into consideration the operational needs of each system stakeholder.

The information contained within Section 4 of this volume provides architecture details to help understand the operational capabilities of the example solution. Guidance is also provided in standards such as the ISO/IEC/Institute of Electrical and Electronics Engineers 15288:2015, *Systems and software engineering–System life cycle processes* [40]; and NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [41], which provide guidance in this endeavor. With these standards, organizations can choose to adopt only those sections that are relevant to their environment and business context.

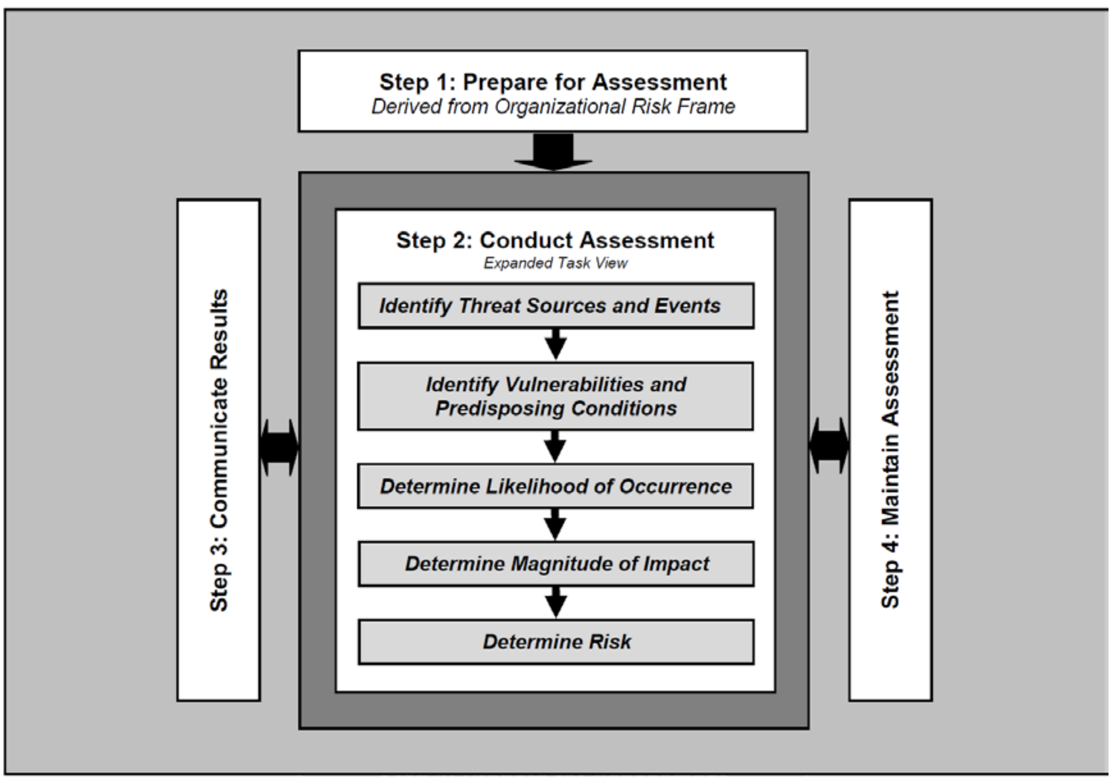
3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [9], states that risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing 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. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [10]–material that is available to the public. The Risk Management Framework (RMF) guidance [7], as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

This section provides information on the risk assessment process employed to improve the mobile security posture of Orvilia Development. Typically, a NIST SP 800-30 Revision 1-based risk assessment follows a four-step process as shown in Figure 3-2: Prepare for assessment, conduct assessment, communicate results, and maintain assessment. Full details of the risk assessment can be found in the Risk Assessment Appendix.

Figure 3-2 Risk Assessment Process



The purpose of the risk assessment of Orvilia Development is to identify and document new risks to its mission resulting from Orvilia's new status as a contractor to government agencies.

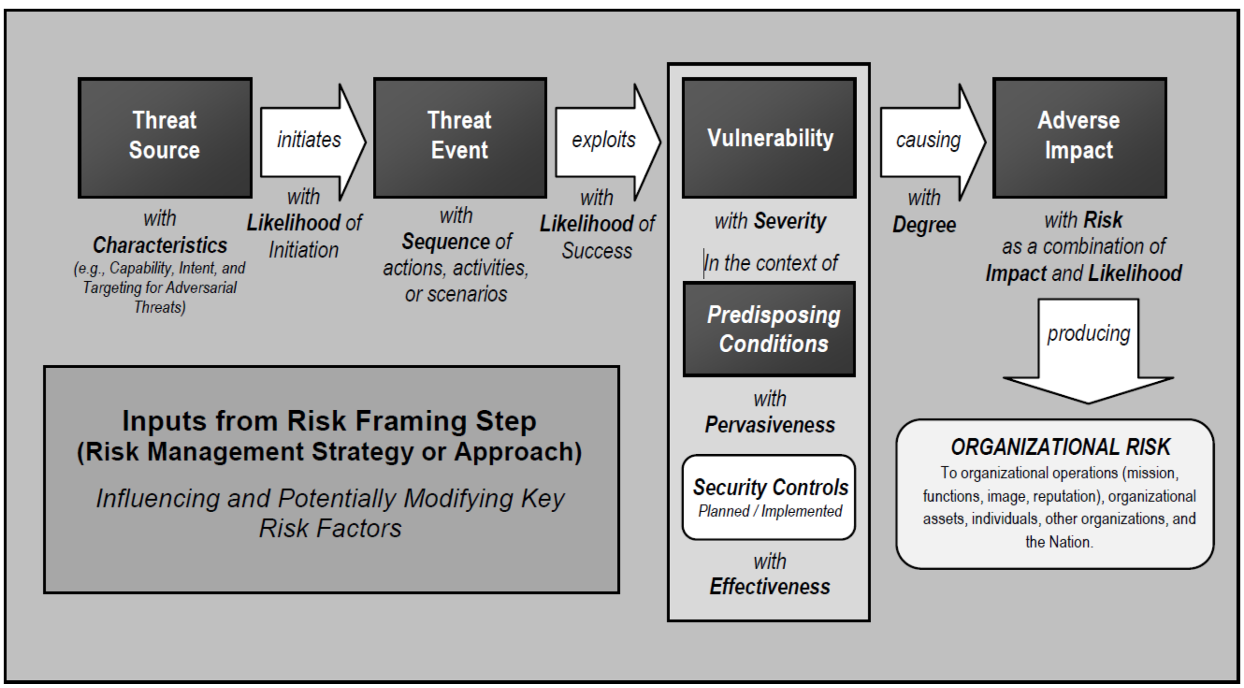
3.4.1 Risk Assessment of the Fictional Organization Orvilia Development

This risk assessment is scoped to Orvilia's mobile deployment, which consists of mobile devices used to access Orvilia enterprise resources along with any backend IT components used to manage or provide services to those mobile devices.

Risk assessment assumptions and constraints were developed using a NIST SP 800-30 Revision 1 Generic Risk Model as shown in Figure 3-3 to identify the following necessary components of the risk assessment:

- threat sources
- threat events
- vulnerabilities
- predisposing conditions
- security controls
- adverse impacts
- organizational risks

Figure 3-3 NIST 800-30 Generic Risk Model



3.4.2 Development of Threat Event Descriptions

Orvilia examined the sample tables in NIST SP 800-30 Revision 1—Table E-1, Table E-2, Table E-3, Table E-4, and Table E-5—and analyzed the sources of mobile threats. Using this process, Orvilia leadership identified the potential mobile device threat events that are described in the following subsections. A mapping of the threat events considered in this guide's example solution to the Mobile Threat Catalogue can be found in Table 3-1.

A note about selection of the threat events: These threat events were developed by identifying threats from the NIST Mobile Threat Catalogue [6] that would have the ability to significantly disrupt Orvilia's processes. In the interest of brevity, we limited our identified threat events of concern to those that were presumed to average a foreseeably high likelihood of occurrence and high potential for adverse impact in Orvilia's specific scenario. The threats from the NIST Mobile Threat Catalogue that could have less impact to Orvilia were not prioritized as high and did not become part of the following 12 threat events that Orvilia prioritized for inclusion in its mobile device security architecture.

Table 3-1 Threat Event Mapping to the Mobile Threat Catalogue

Threat Event	NIST Mobile Threat Catalogue Threat ID
TE-1	APP-2, APP-12
TE-2	AUT-9
TE-3	APP-5, AUT-10, APP-31, APP-40, APP-32, APP-2
TE-4	STA-9, APP-4, STA-16, STA-0, APP-26
TE-5	APP-32, APP-36
TE-6	STA-7, EMM-3
TE-7	CEL-18, APP-0, LPN-2
TE-8	AUT-2, AUT-4
TE-9	APP-9, AUT-0
TE-10	EMM-5
TE-11	PHY-0
TE-12	EMM-9

3.4.2.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

Summary: A mobile application can attempt to collect and exfiltrate any information to which it has been granted access. This includes any information generated during use of the application (e.g., user input), user-granted permissions (e.g., contacts, calendar, call logs, camera roll), and general device data available to any application (e.g., International Mobile Equipment Identity, device make and model, serial number). Further, if a malicious application exploits a vulnerability in other applications, the OS, or device firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or otherwise accessible through the device.

<u>Risk Assessment Analysis:</u>

Overall Likelihood: Very High

Justification: Employees have easy access to download any applications at any time. If an employee requires an application that provides a desired function, the employee can download that application from any available source (trusted or untrusted). If an application performs an employee's desired function, they may download an application from an untrusted source and have no regard for granted privacy intrusive permissions.

Level of Impact: High

Justification: Employees may download an application from an untrusted source and have no regard for granted privacy intrusive permissions. This poses a threat for sensitive corporate data, as some applications may include features that access corporate data, unbeknownst to the user.

3.4.2.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or Email Phishing Campaign

Summary: Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate ones and entice users to authenticate to them by distributing phishing messages over SMS or email. Effective use of social engineering techniques such as impersonating an authority figure or creating a sense of urgency may compel users to forgo scrutiny of the message and proceed to authenticate to the fraudulent website; it then captures and stores the user's credentials before (usually) forwarding them to the legitimate website to allay suspicion.

<u>Risk Assessment Analysis:</u>

Overall Likelihood: Very High

Justification: Phishing campaigns are a common threat that occurs almost daily.

Level of Impact: High

Justification: A successful phishing campaign could provide the malicious actor with corporate credentials, allowing access to sensitive corporate data, or personal credentials that could lead to compromise of corporate data or infrastructure via other means.

3.4.2.3 Threat Event 3—Malicious Applications Installed via Uniform Resource Locators (URLs) in SMS or Email Messages

Summary: Malicious actors may send users SMS or email messages that contain a URL where a malicious application is hosted. Generally, such messages are crafted using social engineering techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby increasing the likelihood they access the URL using their mobile device. If they do, it will attempt to download and install the application. Effective use of social engineering by the attacker will further compel an otherwise suspicious user to grant any trust required by the developer and all permissions requested by the application. Granting the former facilitates the installation of other malicious applications by the same developer, and granting the latter increases the potential for the application to do direct harm.

<u>Risk Assessment Analysis:</u>

Overall Likelihood: High

Justification: Installation of malicious applications via URLs is less common than traditional phishing attempts. The process for sideloading applications requires much more user input and consideration (e.g., trusting the developer certificate) than standard phishing, which solely requests a username and password. A user may proceed through the process of sideloading an application to acquire a desired capability from an application.

Level of Impact: High

Justification: Once a user installs a malicious sideloaded application, this could provide a malicious actor with full access to a mobile device, and therefore access to corporate data and credentials, without the user’s knowledge.

3.4.2.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known Vulnerability in the OS or Firmware

Summary: When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and then issues commands in the context of the root user or the OS kernel. These commands may be enough for some to accomplish their goal, but advanced malicious actors will usually attempt to install additional malicious tools and to establish a persistent presence. If successful, the malicious actor will be able to launch further attacks against the user, the device, or any other systems the device connects to. As a result, any data stored on, generated by, or accessible to the device at that time–or in the future–may be compromised.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Many public vulnerabilities specific to mobile devices have been seen over the years, such as Stagefright. Users jailbreak iOS devices and root Android devices to download third-party applications and apply unique settings/configurations that the device would not typically be able to apply/access.

Level of Impact: High

Justification: Exploiting a vulnerability allows circumventing traditional security controls and modifying protected device data that should not be modified. Jailbroken and rooted devices exploit kernel vulnerabilities and allow third-party applications/services root access that can also be used to bypass security controls built-in or applied to a mobile device.

3.4.2.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors

Summary: Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera, gyroscope, Global Positioning System [GPS] receiver, and radios) can use them to conduct surveillance. It may be directed at the user, as when tracking the device location, or it may be applied more generally, as when recording any nearby sounds. Captured sensor data may be immediately useful to a malicious actor, such as a recording of an executive meeting. Alternatively, the data may be analyzed in isolation or in combination with other data to yield sensitive information. For example, audio recordings of on-device or proximate activity can be used to probabilistically determine user inputs to touchscreens and keyboards–essentially turning the device into a remote keylogger.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: This has been seen on public application stores in the past, with simple applications allegedly being data collection applications for nation-states [42]. As mentioned in Threat Event 1, unbeknownst to the user, a downloaded application may be granted privacy intrusive permissions that allow access to device sensors.

Level of Impact: High

Justification: When the sensors are being misused, the user is typically not alerted. This allows collection of sensitive enterprise data, such as location, without knowledge of the user.

3.4.2.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or Certificates

Summary: Malicious actors who successfully install an EMM/MDM, network, or VPN profile or certificate onto a device will gain a measure of additional control over the device or its communications. Presence of an EMM/MDM profile will allow an attacker to misuse existing OS application programming interfaces (APIs) to send the device a wide variety of commands. This may allow a malicious actor to obtain device information; install or restrict applications; or remotely locate, lock, or wipe the device. Malicious network profiles may allow a malicious actor to automatically compel the device to connect to access points under their control to achieve a man-in-the-middle attack on all outbound connections. Alternatively, VPN profiles assist in the undetected exfiltration of sensitive data by encrypting it, thus hiding it from network scanning tools. Additionally, malicious certificates may allow the malicious actor to compel the device to automatically trust connections to malicious web servers, wireless access points, or installation of applications under the attacker's control.

<u>Risk Assessment Analysis:</u>

Overall Likelihood: Moderate

Justification: Unlike installation of an application, installation of EMM/MDM, network, VPN profiles, and certificates requires additional effort and understanding from the user to properly implement.

Level of Impact: Very High

Justification: If a malicious actor were able to install malicious configuration profiles or certificates, they would be able to perform actions such as decrypt network traffic and possibly even control the device.

3.4.2.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

Summary: Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is connected to such a network, a malicious actor would gain unauthorized access to any data sent or received by the device for any session not already protected by encryption at either the transport or application layers. Even if the transmitted data were encrypted, an attacker would be privy to the domains, internet protocol (IP) addresses, and services (as indicated by port numbers) to which the device connects; such information could be used in future watering hole attacks or man-in-the-middle attacks against the device user.

Additionally, visibility into network layer traffic enables a malicious actor to conduct side-channel attacks against its encrypted messages, which can still result in a loss of confidentiality. Further, eavesdropping on unencrypted messages during a handshake to establish an encrypted session with another host or endpoint may facilitate attacks that ultimately compromise security of the session.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Users require network access to retrieve email and access cloud services and other necessary data on the internet. Users can connect to readily available free internet access in public venues such as coffee shops, hotels, and airports.

Level of Impact: High

Justification: Users may connect to unencrypted wireless networks, and many applications do not properly encrypt network communications. Improper use of encryption, or lack thereof, allows a malicious actor to eavesdrop on network traffic.

3.4.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code

Summary: A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the device; only the third technique requires physical access. However, side-channel attacks that infer the unlock code by detecting taps and swipes to the screen can be attempted by applications with access to any peripherals that detect sound or motion (microphone, gyroscope, or accelerometer). Once the device unlock code has been obtained, a malicious actor with physical access to the device will gain immediate access to any data or functionality not already protected by additional access control mechanisms. Additionally, if the user employs the device unlock code as a credential to any other systems, the attacker may further gain unauthorized access to those systems.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: Unlike shoulder-surfing to observe a user's passcode, brute-force attacks are not as common or successful due to the built-in deterrent mechanisms. These mechanisms include exponential back-off/lockout period and device wipes after a certain number of failed unlock attempts.

Level of Impact: High

Justification: If a malicious actor can successfully unlock a device without the user's permission, they could have full control over the user's corporate account and thus gain unauthorized access to corporate data.

3.4.2.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

Summary: If a malicious actor gains unauthorized access to a mobile device, the attacker also has access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications and can subsequently gain access to sensitive data or backend services. This could result from weaknesses or vulnerabilities present in the authentication or credential storage mechanisms implemented within an in-house application.

<u>Risk Assessment Analysis:</u>

Overall Likelihood: Very High

Justification: Often applications include hard-coded credentials for the default password of the administrator account. Default passwords are readily available online. These passwords may not be changed to allow for ease of access and to eliminate the pressure of remembering a password.

Level of Impact: High

Justification: Successful extraction of the credentials allows an attacker to gain unauthorized access to enterprise data.

3.4.2.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

Summary: An employee who accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization's visibility into the state of a mobile device, including if the device is compromised by a malicious actor. Therefore, users who violate security policies to gain unauthorized access to enterprise resources from such devices risk providing attackers with access to sensitive organizational data, services, and systems.

<u>Risk Assessment Analysis:</u>

Overall Likelihood: Very High

Justification: This may occur accidentally when an employee attempts to access their email.

Level of Impact: High

Justification: Unmanaged devices pose a sizable security risk because the enterprise has no visibility into their security or risk posture. Due to this lack of visibility, a compromised device may allow an attacker to attempt to exfiltrate sensitive enterprise data.

3.4.2.11 Threat Event 11—Loss of Organizational Data Due to a Lost or Stolen Device

Summary: Due to the nature of the small form factor of mobile devices, they are easy to misplace or be stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

Risk Assessment Analysis:

Overall Likelihood: Very High

Justification: Mobile devices are small and very easy to misplace. Enterprise devices may be lost or stolen at the same frequency as personally owned devices.

Level of Impact: High

Justification: Similar to Threat Event 9, if a malicious actor can gain access to the device, they could potentially have access to sensitive corporate data.

3.4.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data Due to Its Unauthorized Storage in Non-Organizationally Managed Services

Summary: If employees violate data management policies by using unmanaged services to store sensitive organizational data, this data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Further, storage of sensitive data in an unmanaged service may subject the user or the organization to prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate efforts by the organization to achieve remediation or recovery from any future losses, such as those resulting from the public disclosure of trade secrets.

Risk Assessment Analysis:

Overall Likelihood: High

Justification: This could occur either intentionally or accidentally (e.g., taking a screenshot and backup up pictures to an unmanaged cloud service).

Level of Impact: High

Justification: Storage in unmanaged services presents a risk to the confidentiality and availability of corporate data because the corporation would no longer control it.

3.4.3 Identification of Vulnerabilities and Predisposing Conditions

In Section 3.2.1, we identified vulnerabilities and predisposing conditions that increase the likelihood that identified threat events will result in adverse impacts for Orvilia Development. Each vulnerability or predisposing condition is listed in Table 3-2 along with the corresponding threat events and ratings of threat pervasiveness. More details on the use of threat event ratings can be found in the Risk Assessment Appendix.

Table 3-2 Identify Vulnerabilities and Predisposing Conditions

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-1	Email and other enterprise resources can be accessed from anywhere, and only username/password authentication is required.	TE-2, TE-10, TE-11	Very High
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their corporate mobile devices.	TE-7	Very High
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on corporate mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-11, TE-12	Very High

3.4.4 Summary of Risk Assessment Findings

Table 3-3 summarizes the risk assessment findings. More detail about the methodology used to rate overall likelihood, level of impact, and risk can be found in the Risk Assessment Appendix.

Table 3-3 Summary of Risk Assessment Findings

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: Unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	Very High	High	High

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-2: Theft of credentials through an SMS or email phishing campaign	VULN-1	Very High	High	High
TE-3: Malicious applications installed via URLs in SMS or email messages	VULN-3	High	High	High
TE-4: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	VULN-3	High	High	High
TE-5: Violation of privacy via misuse of device sensors	VULN-3	Very High	High	High
TE-6: Compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates	VULN-3	Moderate	Very High	High
TE-7: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2, VULN-3	High	High	High
TE-8: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	High	High	High
TE-9: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	Very High	High	High
TE-10: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1	Very High	High	High

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-11: Loss of organizational data due to a lost or stolen device	VULN-1, VULN-3	Very High	High	High
TE-12: Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	VULN-3	High	High	High

Note 1: Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST Special Publication 800-30 Revision 1 [9].

Note 2: The risk rating itself is derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST Special Publication 800-30 Revision 1 [9]. Because these scales are not true interval scales, the combined overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two variables. This is demonstrated in the table above where levels of moderate weigh more heavily than other ratings.

Note 3: Ratings of risk relate to the probability and level of adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1, adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic effects (i.e., very high).

3.4.5 Privacy Risk Assessment

This section describes the privacy risk assessment conducted on Orvilia’s enterprise security architecture. To perform the privacy risk assessment, the NIST Privacy Risk Assessment Methodology (PRAM) was used. The PRAM is a tool for analyzing, assessing, and prioritizing privacy risks to help organizations determine how to respond and select appropriate solutions. The PRAM can also serve as a useful communication tool to convey privacy risks within an organization. A blank version of the PRAM is available for download on NIST’s website [43].

The PRAM uses the privacy risk model and privacy engineering objectives described in NIST Internal Report (NISTIR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [44], to analyze for problematic data actions. Data actions are any system operations that process PII. Processing can include collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of PII. A problematic data action is one that could cause an adverse effect for individuals. The PRAM activities identified the following potential problems for indivduals.

3.4.5.1 Potential Problems for Individuals

Three data actions were identified in the PRAM that have the potential to create problems for individuals. Those three data actions, along with their risk assessment analysis, follow:

- blocking access and wiping devices
- employee monitoring
- data sharing across parties

3.4.5.1.1 Data Action 1: Blocking Access and Wiping Devices

Employees are likely to use their devices for both personal and work-related purposes. Therefore, in a system that features the capability to wipe a device entirely, there could be an issue of employees losing personal data. This is a potential problem for individuals because employee use of work devices for both personal and work-related purposes is common.

Devices that might pose a risk to the organization's security posture can be blocked from accessing enterprise resources or wiped and reset to factory setting defaults, which could result in loss of information contained on the device. Potential options for minimizing the impact to the employee include:

- blocking the device's access to enterprise resources until it is granted access permission again
- selectively wiping elements of the device without removing all data on the device. Within the example solution, this option is available for iOS devices.
- advising employees to back up the personal data maintained on devices
- limiting staff with the ability to perform wipes or block access

3.4.5.1.2 Data Action 2: Employee Monitoring

Employees may not be aware of the monitoring of their interactions with the system and may not want this monitoring to occur. Employer-owned or -controlled networks like Orvilia's often can monitor activities, and many do on a regular basis.

The assessed infrastructure offers Orvilia a number of security capabilities, including reliance on comprehensive monitoring capabilities. A significant amount of data relating to employees, their devices, and their activities is collected and analyzed by multiple parties. Potential options for minimizing the impact to the employee include:

- limit staff with ability to review data about employees and their devices
- develop organization policies and techniques to limit collection of specific data elements

- develop organization policies and techniques regarding disposal of PII

3.4.5.1.3 Data Action 3: Data Sharing Across Parties

Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to different information about them.

The infrastructure involves several parties that serve different purposes supporting Orvilia's security objectives. As a result, a significant flow of data about individuals and their devices occurs across various parties.

If a wide audience of administrators and co-workers know which of their colleagues are conducting activity on their devices that triggers security alerts, it could lead to undesired outcomes such as employee embarrassment. Potential options for minimizing the impact to the employee include:

- developing organization policies and techniques for the de-identification of data
- using encryption
- limiting or disabling access to data
- developing organization policies and techniques to limit the collection of specific data elements
- using contracts to limit third-party data processing

Additional information regarding these potential problems for individuals and potential options for minimizing the impact to the employees is provided in the Privacy Risk Assessment Appendix.

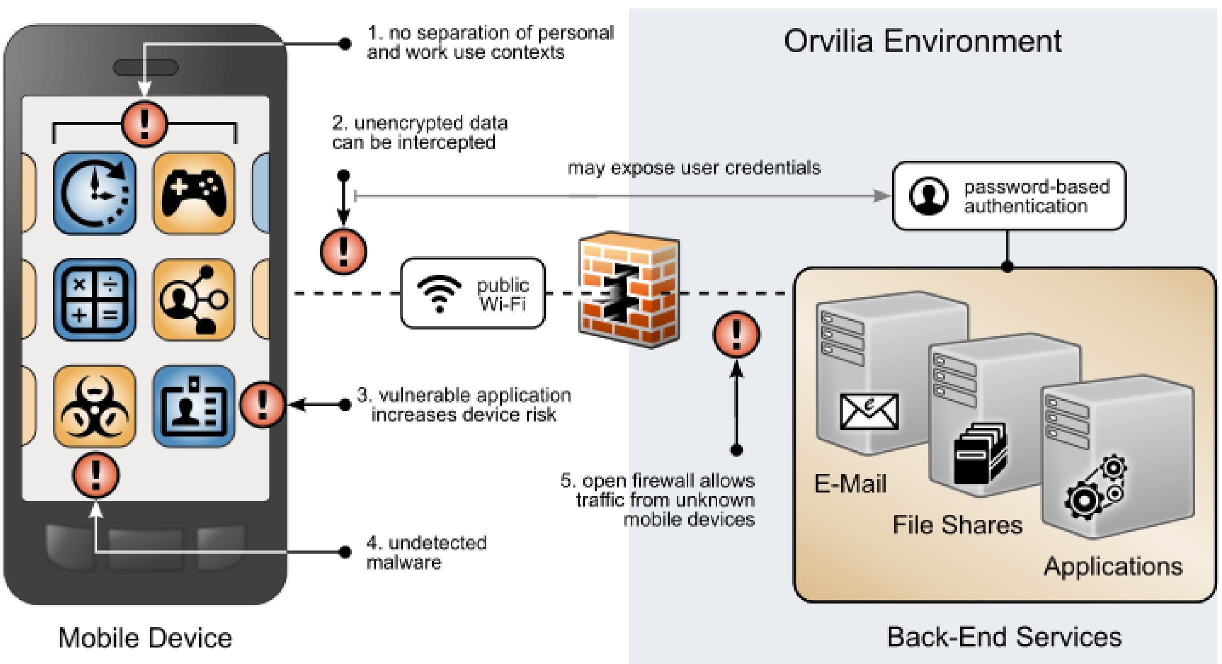
3.5 Preliminary Solution Goals

This section describes the preliminary solution goals for revising Orvilia's mobile security architecture. Here is an overview of the security issues identified within Orvilia's original (also known as current) mobile device infrastructure architecture. To address these issues, a list of security goals was developed to provide a high-level overview of factors that could be applied to improve the security of Orvilia's mobile architecture.

3.5.1 Current Architecture

Prior to investing in security improvements to their mobile infrastructure—as identified based on the aforementioned risk assessment—Orvilia Development had not implemented a mobile security strategy. Several weaknesses were identified based on their use of mobile devices. A subset of these weaknesses is presented in Figure 3-4.

Figure 3-4 Orvilia's Mobile Deployment Before Security Enhancements



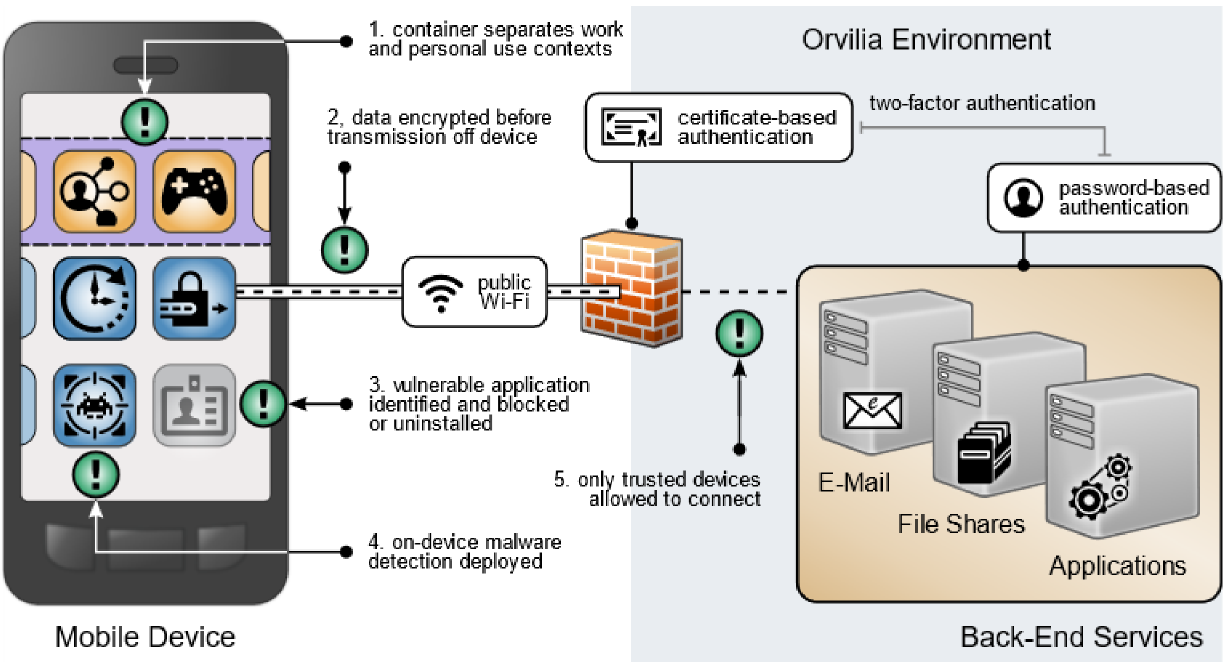
The following issues are highlighted in Figure 3-4 with a red exclamation mark:

1. Organizational and personal data can become commingled if either the same application is used in both contexts or if multiple applications access shared device resources (e.g., contacts or calendar).
2. Mobile devices are connecting to Orvilia from unencrypted public Wi-Fi hot spots; data transmitted prior to a secure connection is subject to eavesdropping, including passwords.
3. Applications for work or personal use may contain unidentified vulnerabilities or weaknesses that increase the risk of device compromise.
4. Applications may be obtained outside official application stores, increasing the risk that they are malware in disguise.
5. Because mobile devices can connect from unknown locations, firewall rules must allow inbound connections from unrecognized, potentially malicious IP addresses.

3.5.2 Preliminary Security Goals

In considering improvement to the security of their current deployment, Orvilia was able to identify high-level preliminary security goals to correct these shortcomings, as illustrated in Figure 3-5.

Figure 3-5 Orvilia's Preliminary Security Goals



The following strategies are highlighted in Figure 3-5 with a green exclamation mark:

1. Organizational and personal information can be separated by restricting data flow between organizationally managed and unmanaged applications. Sensitive data is protected from crossing between work and personal contexts.
2. Mobile devices can connect to Orvilia over a VPN or similar solution to encrypt all data before it is transmitted from the device, protecting otherwise unencrypted data from interception.
3. Identifying applications with significant vulnerabilities or weaknesses facilitates blocking or uninstalling those applications from managed devices, reducing their risk to the organization.
4. Malware detection could be deployed to devices to identify malicious applications and facilitate remediation.

5. Mobile devices can be provisioned with a security certificate that allows them to be identified and authenticated at the connection point, which combines with user credentials to create two-factor authentication from mobile devices.

These high-level goals, obtained from a review of their current mobile security posture, provide examples of why a thorough risk assessment process is beneficial to organizations implementing mobile device security capabilities.

3.6 Technologies

This section describes the mobile-specific technology components used within this example solution. These technologies were selected to address the preliminary security goals and threat events identified in the risk assessment. This section provides a brief description of each technology and discusses the security capabilities that each component provides to address Orvilia's security issues. For additional information, Appendix H provides the technologies used in this project and provides a mapping between the specific product used and the cybersecurity standards and best practices that the product provides in the example solution discussed in this guide.

3.6.1 Architecture Components

The security components in this section are combined into a cohesive enterprise security architecture to enable enterprises to address mobile security threats and provide secure access to enterprise resources from mobile devices. The security components described in this section provide protection for the following enterprise architecture components that are accessed by Orvilia's users with their mobile devices.

- email/Outlook Web Access–contacts
- private chat server
- travel support
- organization intranet (e.g., internal announcements, organizational charts, policies)
- time reporting

3.6.1.1 Trusted Execution Environment

A trusted execution environment (TEE) is "a tamper-resistant processing environment that runs on a separation kernel. It guarantees the authenticity of the executed code, the integrity of the runtime states (e.g., central processing unit registers, memory and sensitive I/O), and the confidentiality of its code, data and runtime states stored on a persistent memory. In addition, it shall be able to provide remote attestation that proves its trustworthiness for third-parties [45]."

3.6.1.2 Enterprise Mobility Management

Organizations use Enterprise Mobility Management solutions to secure the mobile devices of users who are authorized to access organizational resources. Such solutions generally have two main components. The first is a backend service that mobile administrators use to manage the policies, configurations, and security actions applied to registered mobile devices. The second is an on-device agent, usually in the form of a mobile application, that integrates between the mobile OS and solution's backend service. Alternatively, iOS supports a web-based EMM enrollment use case.

At a minimum, an EMM solution can perform MDM functions, which include the ability to provision configuration profiles to devices, enforce security policies on devices, and monitor compliance with those policies by devices. The on-device MDM agent can typically notify the device user of any noncompliant settings and may be able to remediate some noncompliant settings automatically. The organization can use policy compliance data to inform its access control decisions so that it grants access only to a device that demonstrates the mandated level of compliance with the security policy that applies to it.

EMM solutions commonly include any of the following: mobile application management, mobile content management, and implementations of or integrations with device- or mobile OS-specific containerization solutions, such as Samsung Knox. These capabilities can be used to manage installation and usage of applications based on the applications' trustworthiness and work relevance. Additionally, they can control how managed applications access and use organizational data and possibly strengthen the separation between a user's personal and professional usage of the device.

Further, EMM solutions often have integrations with a diverse set of additional tools and security technologies that enhance their capabilities. An example is an EMM embedded with a mobile threat defense tool that serves to perform on-device behavioral-based threat-detection and to trigger policy remediation without the need to communicate to any server or service outside the device. This type of integration allows one application, the EMM agent, to manage, detect, and remediate device, network, application, malware, and spear phishing attacks. Additionally, because the remediation is autonomous at the device (does not require reaching a policy server), it has the advantage in addressing network-based threat vectors such as Pineapple or Stingray impersonation of valid Wi-Fi or cellular networks [46].

For further reading, NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [17], provides additional information on mobile device management with EMM solutions. Further, NIAP's *Protection Profile for Mobile Device Management Version 4.0* [47] describe important capabilities and security requirements to look for in EMM systems.

3.6.1.3 Virtual Private Network

A VPN gateway increases the security of remote connections from authorized mobile devices to an organization's internal network. A VPN is a virtual network, built on top of existing physical networks, which can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the internet. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection, and access control that help reduce the risks of transmitting data between network components.

VPN connections apply an additional layer of encryption to the communication between remote devices and the internal network, and VPN gateways can enforce access control decisions by limiting which devices or applications can connect to it. Integration with other security mechanisms allows a VPN gateway to base access control decisions on more risk factors than it may be able to collect on its own; examples include a device's level of compliance with mobile security policies or the list of installed applications (blacklisted applications) as reported by an integrated EMM.

NIAP's *Extended Package for VPN Gateways* [48], in combination with the internationally and collaboratively developed *Protection Profile for Network Devices* [49], describes important capabilities and security requirements to expect from VPN gateways.

3.6.1.4 Mobile Application Vetting Service

Mobile application vetting services use a variety of static, dynamic, and behavioral techniques to determine if an application demonstrates any behaviors that pose a security or privacy risk. The risk may be to a device owner or user, to parties that own data on the device, or to external systems to which the application connects. The set of detected behaviors is often aggregated to generate a singular score that estimates the level of risk (or conversely, trustworthiness) attributed to an application. Clients can often adjust the values associated with given behaviors (e.g., hard-coded cryptographic keys) to tailor the score for their unique risk posture. Those scores may be further aggregated to present a score that represents the overall risk or trustworthiness posed by the set of applications currently installed on a given device.

Mobile applications, malicious or benign, have high potential to negatively impact both security and user privacy. A malicious application can contain code intended to exploit vulnerabilities present in potentially any targeted hardware, firmware, or software on the device. Alternatively, or in conjunction with exploit code, a malicious application may misuse any device, personal, or behavioral data to which it has been explicitly or implicitly granted access, such as contacts, clipboard data, or location services. Benign applications may still present vulnerabilities or weaknesses that malicious applications can exploit to gain unauthorized access to its data or functionality. Further, benign applications may place user privacy at risk by collecting more information than is necessary for the application to deliver functionality desired by the user.

While not specific to applications, some services may include device-based risks (e.g., lack of disk encryption or vulnerable OS version) in their analysis to provide a more comprehensive assessment of the risk or trustworthiness presented by a device when running an application or service.

NIAP does not provide a Protection Profile for application vetting services themselves. However, NIAP's *Protection Profile for Application Software* [50] describes security requirements to be expected from mobile applications. Many mobile application vetting vendors provide capabilities to automate evaluation of applications against NIAP's requirements.

3.6.1.5 Mobile Threat Defense

MTD generally takes the form of an application that is installed on the device, which provides the widest and most timely access to information about what activity is taking place. Ideally, the MTD solution will be able to detect unwanted activity and properly inform the user so they can act to prevent or limit the harm an attacker could cause. Additionally, MTD solutions may integrate with EMM solutions to leverage the EMM agent's on-device capabilities, such as blocking a malicious application from being launched until the user can remove it.

MTD products typically analyze device-based threats, application-based threats, and network-based threats. Device-based threats include outdated operating system versions and insecure configuration settings. Application-based threats include the issues discussed above regarding the mobile application vetting service, though sometimes without the same breadth or depth found in services dedicated to application vetting. Network-based threats include use of unencrypted or public Wi-Fi networks and attacks such as active attempts to intercept and decrypt network traffic.

3.6.1.6 Mobile Threat Intelligence

In this guide, we describe mobile threat intelligence as actionable information that mobile administrators can use to make changes to their security configuration to improve their posture relative to recent discoveries. Intelligence data include malicious URLs, IP addresses, domain names, and application names or package/bundle IDs, as well as malware signatures or vulnerabilities in applications, mobile devices, device platform services, or mobile security products. This list is not all-encompassing, as any recent information that could inform rapid changes to enable an enterprise to better secure a mobile deployment against novel or newly enhanced threats is equally applicable to the term. This capability may be found in various other types of technology, such as MTD and other network analysis tools.

3.6.1.7 Native Mobile OS Capabilities

Native mobile OS capabilities are available without the use of additional security features. They are included as part of the mobile device's core capabilities. The following mobile OS capabilities can be found in mobile devices, particularly smartphones.

3.6.1.7.1 Secure Boot

Secure boot is a general term that refers to a system architecture designed to prevent and detect any unauthorized modification to the boot process. A system that successfully completes a secure boot has loaded its start-up sequence information into a trusted operating system. A common mechanism is for the first program executed (a boot loader) to be immutable (stored on read-only memory or implemented strictly in hardware). Further, the integrity of mutable code is cryptographically verified prior to execution by either immutable or verified code. This process establishes a chain of trust that can be traced back to immutable, implicitly trustworthy code. Use of an integrated TEE as part of a secure boot process is preferable to an implementation that uses software alone [51].

3.6.1.7.2 Device Attestation

This is an extension of the secure boot process that involves the operating system (or more commonly, an integrated TEE) providing cryptographically verifiable proof that it has a known and trusted identity and is in a trustworthy state, which means all software running on the device is free from unauthorized modification.

Device attestation requires cryptographic operations using an immutable private key that can be verified by a trusted third party, which is typically the original equipment manufacturer of the TEE (e.g., Qualcomm or Samsung) or device platform vendor (e.g., Google, Apple, or Microsoft). Proof of possession of a valid key establishes the integrity of the first link in a chain of trust that preserves the integrity of all other pieces of data used in the attestation. It will include unique device identifiers, metadata, and the results of integrity checks on mutable software, and possibly metrics from the boot or attestation process itself [51].

3.6.1.7.3 Device Management and MDM API

Mobile operating systems and platform-integrated firmware (e.g., Samsung Knox) provide a number of built-in security features that are generally active by default. Examples include disk and file-level encryption, verification of digital signatures for installed software and updates, a device unlock code, remote device lock, and automatic device wipe following a series of failed device unlock attempts. Some of these features are directly configurable by the user via a built-in application or through a service provided by the device platform vendor (e.g., Google, Apple, or Microsoft).

Additionally, mobile operating systems expose an API to MDM products that allow an organization that manages a device to have greater control over these and many more settings that might not be directly accessible to the device user. Management APIs allow enterprises using integrated EMM or MDM products to manage devices more effectively and efficiently than they could by using the built-in application alone.

4 Architecture

This example solution consists of the six mobile security technologies described in Section 3.6: trusted execution environment, enterprise mobility management, virtual private network, mobile application vetting service, mobile threat defense, and mobile threat intelligence. Table 4-1, Commercially Available Products Used, identifies the commercially available products used in this example solution and how they aligned with the six mobile security technologies.

Table 4-1 Commercially Available Products Used

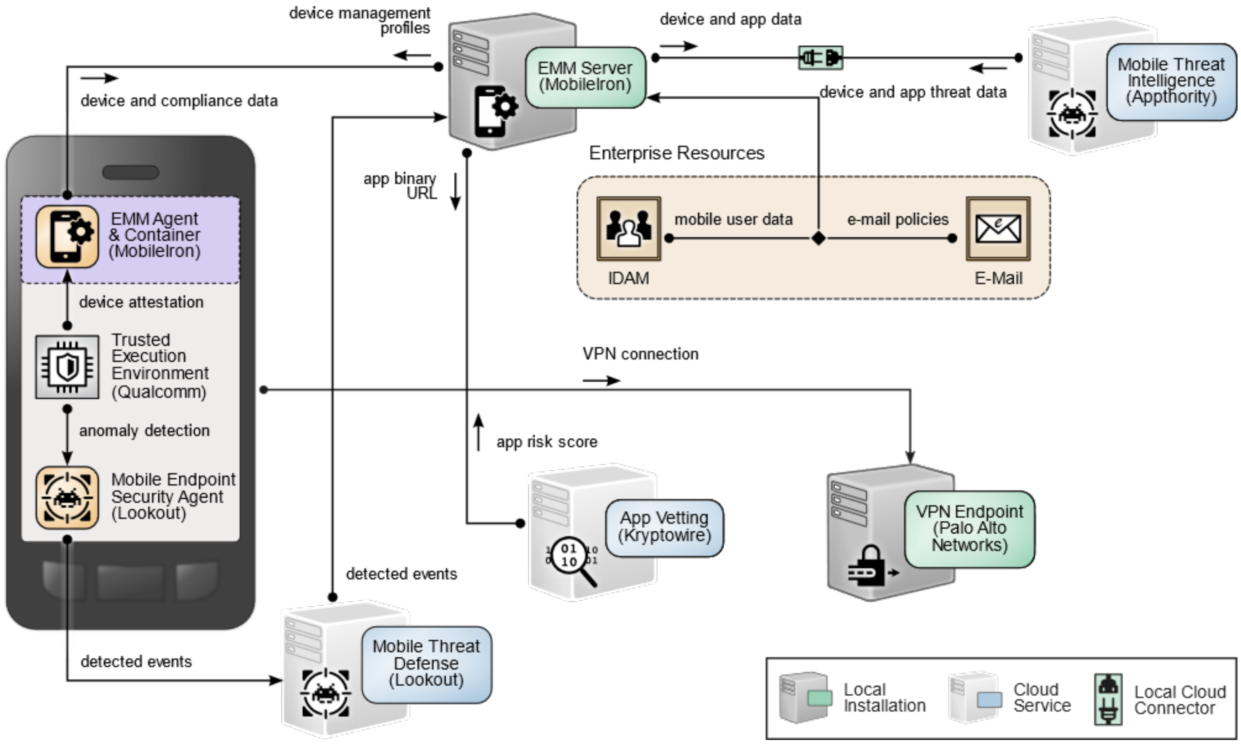
Commercially Available Product	Mobile Security Technology
Appthority Cloud Service	Mobile threat intelligence
Kryptowire Cloud Service	Mobile application vetting service
Lookout Cloud Service/Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android)	Mobile threat defense
MobileIron Core Version 9.7.0.1 MobileIron Agent Version 11.0.1A (iOS), 10.2.1.1.3R (Android)	Enterprise mobility management
Palo Alto, PA-220 Version 8.1.1	Virtual private network
Qualcomm, (version is mobile device dependent)	Trusted execution environment

These components are further integrated with broader on-premises security mechanisms and a VPN gateway as shown in Figure 4-1. This integrated solution provides a broad range of capabilities to help securely provision and manage devices, protect against and detect device compromise, and help provide security-enhanced access to enterprise resources by only authorized mobile users and devices.

Organizations exploring the use of on-premises EMM technology should be aware they will be responsible for installing and configuring the on-premises instances of the EMM technology. This will include the software licenses that must be paid for directly by the organization for any underlying platforms or components. Pre-built software images and containers may be available that can help ease installation and configuration work. As a recommended best practice, if prebuilt containers and images are used, it is recommended that they be checked for common software vulnerabilities.

On-premises mobile device management solutions offer the benefit that enterprise data resides within the organization. Allowed devices may still send and receive information from the mobile device solution that they are authorized to obtain. Organizations that are interested can explore monitoring data flows from the EMM to other devices. Additionally, on-premises mobile device management solutions provide the organization with the capability to maintain physical security of the EMM.

Figure 4-1 Example Solution Architecture



4.1 Architecture Description

The NCCoE worked with industry subject matter experts to develop an open, standards-based, commercially available architecture that addresses the risks identified during the risk assessment process in Section 3.4.

Where possible, the architecture uses components that are present on NIAP's Product Compliant List [35], meaning the product has been successfully evaluated against a NIAP-approved Protection Profile [50]. NIAP collaborates with a broad community, including industry, government, and international partners, to publish technology-specific security requirements and tests in the form of Protection Profiles. The requirements and tests in these Protection Profiles are intended to ensure that evaluated products address identified security threats.

The example solution architecture supports its desired security characteristics as a result of the following integrations.

4.1.1 Enterprise Integration

This example solution extends central identity and access management to mobile devices via an integration between both MobileIron Core and Palo Alto Networks GlobalProtect with Microsoft Active Directory Domain Services (ADDS). The integrity of identification and authentication by mobile devices to the enterprise is further enhanced by using device certificates issued by local Microsoft Active Directory Certificate Services (ADCS).

By integrating with Active Directory (AD), MobileIron Core allows administrators to authorize select groups of users to register a mobile device, limiting mobile access to only those users who require it. Additionally, different security policies, device configurations, and authorized applications can be deployed to different AD groups, allowing administrators to centrally manage distinct mobile use cases. MobileIron Core queries AD using the lightweight directory access protocol.

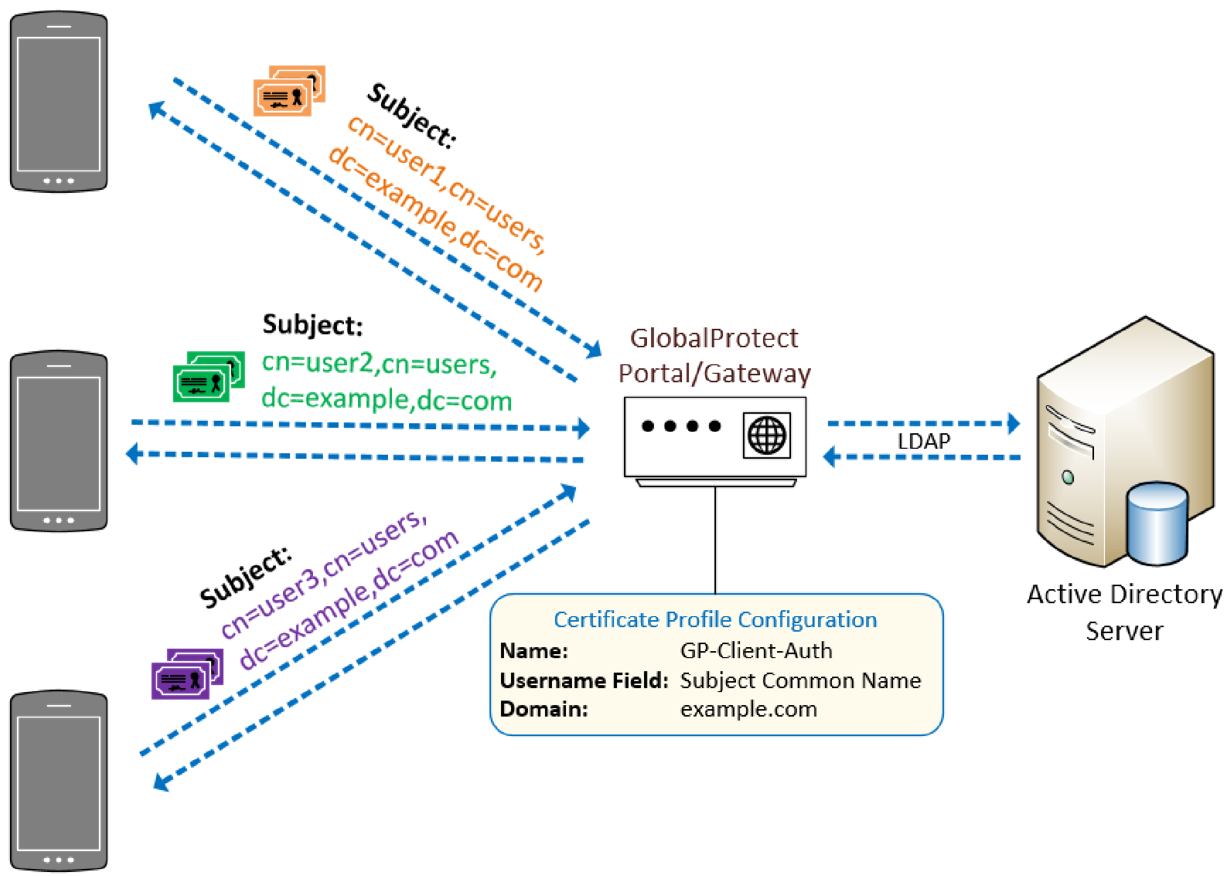
Through its integration with ADCS, MobileIron Core automatically configures devices to obtain locally managed device certificates by using the Simple Certificate Enrollment Protocol (SCEP). Our example solution mitigates the potential of remote exploitation of SCEP by restricting certificate enrollment to mobile devices that are connected to a dedicated enterprise-managed Wi-Fi network that allows devices to access only MobileIron Core and the Network Device Enrollment Service server. Further, this example solution uses a dynamic SCEP scheme, in which MobileIron Core supplies a registered mobile device with a onetime password to include in its SCEP request, thus helping prevent unknown and untrusted devices that gain unauthorized access to the dedicated Wi-Fi network from obtaining a trusted device certificate.

The example solution’s chosen certificate enrollment configuration includes the mobile user’s User Principal Name (UPN) in the device certificate’s Subject Alternative Name field, which the Palo Alto Networks GlobalProtect VPN gateway uses to perform identity verification and enforce access control for the unique combination of mobile user and device.

MobileIron Core-registered devices also utilize the device certificate indirectly to enhance the security of remote connections to the enterprise in two ways. First, communication with MobileIron Core (which must be accessible from the internet in the demilitarized zone) is secured using two-way Transport Layer Security (TLS). This protects MobileIron Core from establishing secure connections with untrusted mobile devices. Second, the device certificate is used in the GlobalProtect VPN configuration, which restricts access to the VPN to only trusted devices. Further, GlobalProtect uses the device user’s UPN to grant appropriate access to enterprise resources based on the device user’s UPN through its integration with ADDS.

As shown in Figure 4-2 [52], devices present the certificates to the VPN and EMM authentication services after the certificate have been successfully issued. The GlobalProtect VPN authenticates the device user by mapping the common name field in the client certificate to an account stored in the local ADDS. On successful authentication, the GlobalProtect application prompts the user to authenticate using a second factor–their Active Directory domain password. Once this is verified, GlobalProtect establishes a tunnel with the gateway and is assigned an IP address from the IP pool in the gateway's tunnel configuration.

Figure 4-2 Example Solution Gateway Architecture



4.1.2 Mobile Component Integration

This section describes how the various mobile technology components integrate with one another. The majority of these components integrate with the EMM, MobileIron. MobileIron supports the integration of third-party cloud services through a defined API. MobileIron Core authenticates external systems by using basic authentication, so TLS protects the confidentiality of API account credentials and

MobileIron's responses to clients' RESTful calls. MobileIron API client accounts for Kryptowire, Lookout Mobile Endpoint Security, and Appthority Mobile Threat Protection (MTP) are each assigned administrative roles that grant the minimum set of permissions necessary to achieve integration [53], [54].

4.1.2.1 Appthority–MobileIron

The Appthority application reputation service provides an integration with MobileIron Core systems through implementation of connector software provided by Appthority. The connector provides the code that exercises the APIs provided by MobileIron Core and the Appthority cloud service. In this integration, an API user was created within the MobileIron Core system and assigned specific roles required for successful operation of the application vetting service. Automatic syncing between the Appthority service and MobileIron Core system can occur on a configurable basis. Specifically, the application and device inventory data are synced between the two systems. In this integration, syncing occurs every hour, but this value should be adjusted to fit the needs of the organization.

In this example solution, the integration provides the primary security benefit of compliance enforcement and remediation escalation. In the initial step of the process, the application inventory is gathered from the MobileIron Core system, and each application is assigned a threat measurement score. If an application is installed on a device that is not compliant with the configured policy, Appthority MTP communicates with the MobileIron Core system to identify those devices, which triggers MobileIron compliance enforcement actions.

4.1.2.2 Lookout–MobileIron

The Lookout mobile threat defense service provides integration with MobileIron Core systems through implementation of connector software provided by Lookout. The connector provides the code that exercises the APIs provided by MobileIron Core and the Lookout cloud service. This integration allows Lookout to retrieve device details as well as application inventory information and to apply labels to devices as necessary.

Following analysis, Lookout uses the API to apply specific labels to devices to categorize them based on risk posture, which is calculated based on the severity of issues detected on the device. MobileIron can then automatically respond to application of specific labels based on built-in compliance actions. This allows administrators to configure exactly how MobileIron will respond to devices in the following categories:

- Pending–Lookout not yet activated
- Secured–Lookout active
- Threats Present–Lookout has detected threats
- Deactivated–Lookout has been deactivated

- Low Risk–devices with a low risk score in Lookout
- Moderate Risk–devices with a moderate risk score in Lookout
- High Risk–devices with a high-risk score in Lookout

4.1.2.3 Kryptowire–MobileIron

Kryptowire obtains device details, such as device platform, OS version, and the universally unique identifiers assigned to each registered device by MobileIron Core to enable clear identification of a particular device across systems. Kryptowire obtains the inventory of applications from all of the devices enrolled in MobileIron. Kryptowire performs static, dynamic, and behavioral binary code analysis on mobile applications against government (NIAP) and industry (The Open Web Application Security Project, or OWASP) [55] standards. Kryptowire provides both a detailed security analysis, provides pass/fail evidence down to the line of code, and provides a summary weighted risk score for each application. Mobile application administrators can use these detailed reports to inform decisions on which applications are trusted and compliant with enterprise security and privacy policies and which are restricted for enterprise or personal use.

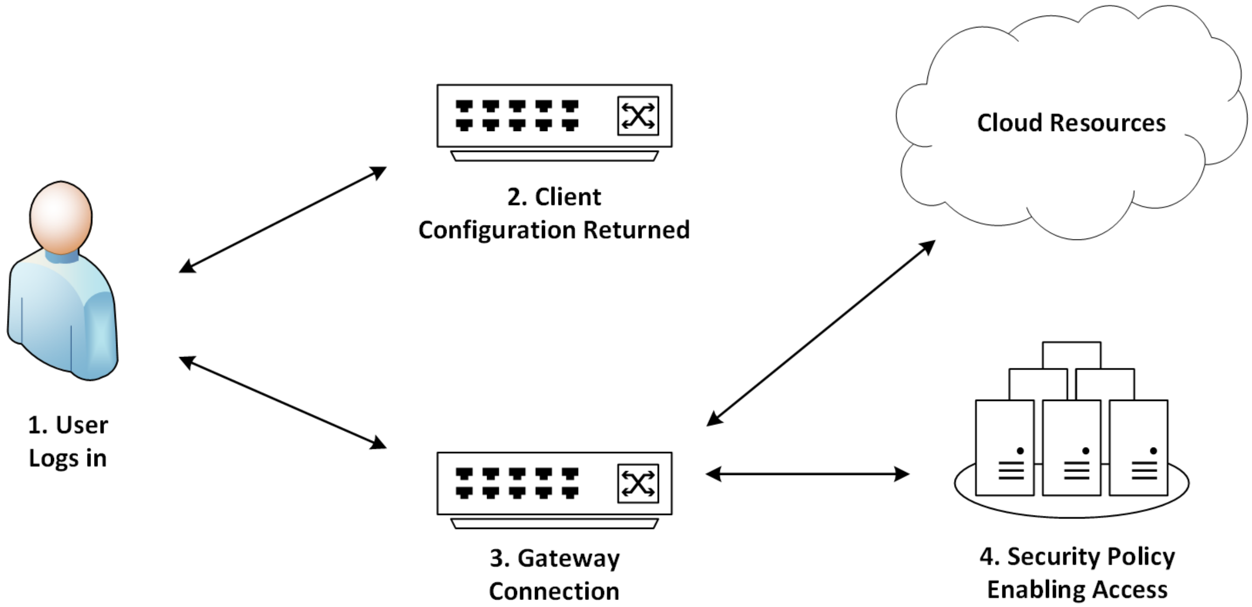
4.1.2.4 Palo Alto Networks–MobileIron

Palo Alto Networks' GlobalProtect VPN is used to secure remote connections from mobile devices. MobileIron Core offers specific configuration options for the GlobalProtect client available on Android and iOS that facilitates secure deployment of VPN clients and enablement of VPN access using certificate-based authentication to the GlobalProtect gateway. Details of the certificate enrollment process are provided in Section 4.1.1.

The VPN architecture used in this example solution is composed of two components of the Palo Alto Networks next-generation firewall–a GlobalProtect portal and a GlobalProtect gateway. The portal provides the management functions for VPN infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s). The gateway provides security enforcement for traffic from GlobalProtect applications. It is configured to provide access to specific enterprise resources only to mobile device users after a successful authentication and authorization decision.

The VPN tunnel negotiation between the VPN endpoint/mobile device and the VPN gateway is presented in Figure 4-3 [56]. It demonstrates a user logging into the system (1), the portal returning the client configuration (2), the agent automatically connecting to the gateway and establishing a VPN tunnel (3), and the gateway's security policy enabling access to internal and external applications (4).

Figure 4-3 Example Solution VPN Architecture



For our example solution, we chose to enforce an always-on VPN configuration. This configuration causes registered devices to establish a VPN connection to the GlobalProtect gateway whenever they have network connectivity–this occurs over cellular or Wi-Fi and is persistent across device reboot. This configuration affords devices with the greatest degree of protection, as additional Palo Alto Networks services can be extended to GlobalProtect. This example solution uses URL filtering, which blocks mobile devices from accessing blacklisted internet domains or any domain that Palo Alto Networks associates with active exploits (e.g., phishing campaigns, watering hole attacks, botnet command and control). NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and BYOD Security* [11], describes the most common VPN options used for remote workers.

4.1.2.4.1 FIPS Compliance

Any sensitive information passing over the internet, wireless networks, and other untrusted networks should have its confidentiality and integrity preserved through cryptography [11]. While federal agencies are required to use cryptographic algorithms that are NIST-approved and contained in Federal Information Processing Standards (FIPS)-validated modules, adoption of these standards is available to private and commercial organizations [57]. This example solution uses these best practices to the extent possible in the following ways:

- *FIPS-CC* mode in the GlobalProtect VPN appliance is enabled, which requires TLS 1.1 (or above) and limits the public key use to FIPS-approved algorithms. This example solution's implementation uses the highest version of TLS available, with TLS 1.2 being the minimum acceptable version. A full list of security functions can be found on the Palo Alto Networks FIPS-CC Security Functions documentation site [58].

- As described in Section 4.1.1, dynamic SCEP challenges are enabled.

To align our example solution with guidance in NIST SP 800-52 Revision 1. *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [12], this example solution implements the following configuration:

- The GlobalProtect portal and gateway restrict the list of cipher suites available to the client application by using a TLS service profile. The minimum version of TLS is set to 1.2 as recommended by NIST SP 800-52.
- The GlobalProtect portal and gateway server certificates use 2048-bit RSA key modulus signed with *sha256WithRSAEncryption* algorithm.

4.1.2.5 iOS and Android EMM Integration

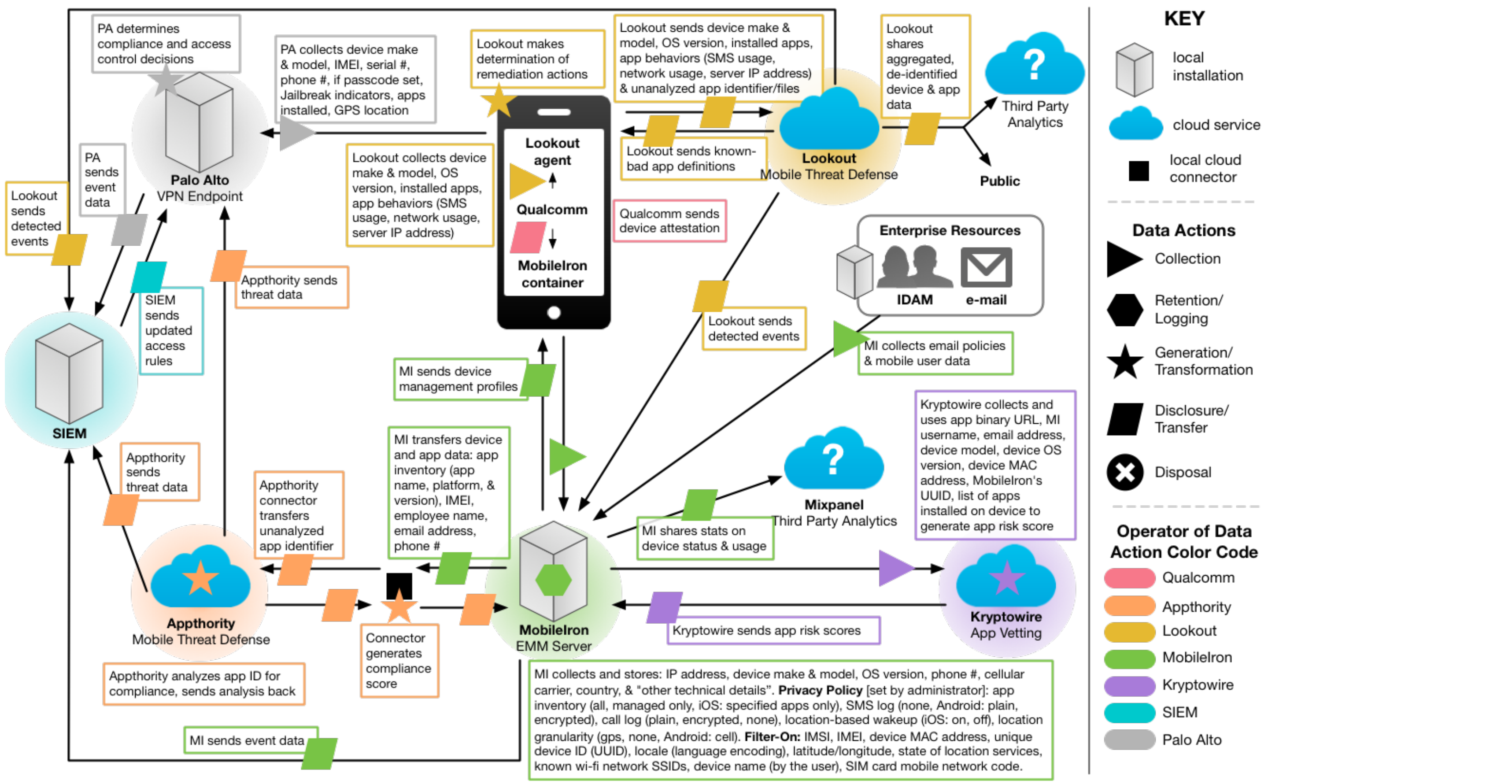
iOS and Android-based devices both integrate directly with EMM solutions, providing enterprise-level management of security controls based on policy. iOS devices are managed by configuration profiles. Configuration profiles can force security policies such as VPN usage, enterprise Kerberos support, and access to cloud services. iOS further incorporates a set of additional security controls in what is termed *supervised* mode, which denotes a corporately owned device. Typically, organizations choose to use the Device Enrollment Program [59] for large-scale deployments of iOS devices in *supervised* mode due to the reduction of labor involved in manually configuring each device. However, due to the small number of devices in our reference design, we have configured *supervised* mode using the Apple Configurator 2 tool [60]. A full description of iOS capabilities can be found in the iOS Security Guide [61].

Similarly, Android-based devices offer security controls that an EMM can leverage for enterprise deployments. The Android Enterprise program by Google is available on devices with Android 5.0 (Lollipop) and higher. An EMM deploys a device policy controller [62] as part of its on-device agent that controls local device policies and system applications on devices. Android Enterprise supports COPE and BYOD deployment scenarios through work-managed [63] and work-profile [64] device solutions. In work-managed mode, the device is corporately owned, and the entire device is managed by the enterprise, whereas work profiles can be added to personally owned devices. A newer mode introduced in Android 8.0 supports a combination of work-managed and work profiles on the same device [65]. In this scenario, the device is corporately owned, in that device level controls such as device wipe and reset to factory default settings are available. A work profile is also created to keep enterprise applications and data separate from any personal data. This scenario allows for some flexibility of the device owner to permit personal use of the device while retaining device controls and is the chosen deployment of this reference implementation.

4.2 Enterprise Security Architecture Privacy Data Map

Orvilia performed a privacy analysis using both the information gathered in the initial PRAM effort and the identified mobile security technologies included in the revised architecture. The output from the PRAM activities, including data flows between the components, along with their on-premises or cloud-based location, resulted in the information contained in Figure 4-4. For additional information on the PRAM activities, see the Privacy Risk Assessment Appendix.

Figure 4-4 NIST Privacy Risk Assessment Methodology Data Map for Orvilia's Enterprise Security Architecture



4.3 Security Control Map

Using the developed risk information as input, the security characteristics of the solution were identified. A security control map was developed documenting the example solution's capabilities with applicable Subcategories from the NIST Cybersecurity Framework Version 1.1 [5]; NIST SP 800-53 Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* [13]; International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, *Information technology–Security techniques–Information security management systems – Requirements* [25]; the Center for Internet Security's Control set [21] Version 6; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [20].

The security control map identifies the security characteristic standards mapping for the products as they were used in the example solution. The products may be capable of additional capabilities not used in this example solution. For that reason, it is recommended the mapping not be used as a reference for all of the security capabilities these products may be able to address. The security control map can be found in Table H-1.

5 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating how to increase the security of mobile devices within an enterprise by deploying EMM, MTD, MTI, application vetting, secure boot/image authentication, and VPN services.

5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed those systems are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

5.2 Build Testing

Functional testing was used to confirm the example solution's capabilities. We use the test activities to demonstrate Orvilia's susceptibility to the threat before implementing the architecture detailed in this practice guide. We use the test activities again after implementing the architecture to demonstrate that the threats have been appropriately addressed.

5.2.1 Threat Event 1 —Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

Summary: Unauthorized access to sensitive information via a malicious or privacy-intrusive application is tested. We tested this threat by placing a mock sensitive enterprise contact list and calendar entries on devices, then attempted to install and use applications on the Apple App Store and Google Play Store [66] that access and back up those entries. Ideally, the enterprise's security architecture would either detect or prevent use of these applications, or it would block the applications from accessing enterprise-controlled contact list and calendar entries.

Test Activity:

Install an iOS or Android application that accesses the contact and calendar entries and backs them up to a cloud service. We have no reason to believe these applications are malicious. However, the behavior of accessing and backing up enterprise-controlled data (contacts and calendar entries) without authorization presents an activity that should be mitigated by this example solution's security architecture.

Desired Outcome: The enterprise's security architecture should identify the presence of the applications and the fact that they access contact and calendar entries. The security architecture should block these applications from installing, block them from running, or detect their presence and cause another appropriate response to occur, such as blocking the mobile device from accessing enterprise resources until the applications are removed.

Alternatively, built-in device mechanisms such as Apple's managed applications functionality and Google's Android enterprise work profile functionality could be used to separate the contact and calendar entries associated with enterprise email accounts, so they can be accessed only by enterprise applications (applications authorized and managed by the EMM), not applications manually installed by the user. The user should not have the ability to manually provision their enterprise email account. The account should be able to be provisioned only by the EMM, enabling enterprise controls on the enterprise contact list and calendar data. However, in this practice guide build, we chose to make the devices fully managed, not divided into separate enterprise and personal areas.

Observed Outcome: Appthority identified the presence of applications that have access to sensitive data and updated the device labels in MobileIron Core.

5.2.2 Threat Event 2 —Theft of Credentials Through an SMS or Email Phishing Campaign

Summary: A fictitious phishing event was created where protection against theft of credentials through an SMS or email phishing campaign was tested.

Test Activity:

- Establish a web page with a form that impersonates an enterprise login prompt.
- Send the web page's URL via SMS or email and attempt to collect and use enterprise login credentials.

Desired Outcome: The enterprise's security architecture should block the user from browsing to known malicious websites. Additionally, the enterprise should use multifactor authentication or phishing-resistant authentication methods, such as those based on public key cryptography, so that either there is no password for a malicious actor to capture, or capturing the password is insufficient to obtain access to enterprise resources.

Observed Outcome: The example solution used Palo Alto Networks' next-generation firewall. The firewall includes PAN-DB, a URL filtering service that automatically blocks known malicious URLs. The URL filtering database is updated regularly to help protect users from malicious URLs. The next-generation firewall blocked the attempt to visit the phishing site. However, if the malicious URL were not present in PAN-DB, the user would be allowed to access the website.

5.2.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages

Summary: Unauthorized applications, not present on the official Apple App Store or Google Play Store, are installed via URL links in SMS, email messages, or third-party websites.

Test Activity (Android):

- Send an email to the user containing a link (https://f-droid.org/Fdroid.apk) to the F-Droid APK (Android Application Package) file with a message urging the user to click on the link to install the application.
- On the device, if not already enabled, attempt to enable the Unknown Sources toggle setting in the device security settings to allow installing applications from sources other than the Google Play Store.
- On the device, read the received email, click on the link, and attempt to install the F-Droid application.
- Observe whether the F-Droid application could be successfully installed. If so, observe whether the enterprise detected and responded to installation of the unauthorized application.

Test Activity (iOS):

- Send an email to the user containing a link to an iOS application available for installation from the iosninja.io website, along with a message urging the user to click on the link to install the application.
- On the device, read the received email, click on the link, and attempt to install the application.

- On the device, attempt to explicitly trust the developer's signing certificate. Then attempt to run the application.
- Observe whether the application could run. If so, observe whether the enterprise detected and responded to installation of the unauthorized application.

Desired Outcome: The device does not allow the user to install the unauthorized application. If the application is somehow installed, its presence should be detected, and an appropriate response should occur, such as blocking the device from accessing enterprise resources until the application is removed.

Observed Outcome: On iOS devices, Lookout detected that an application had been sideloaded, and it applied a label to the device. MobileIron then quarantined the device until the threat was resolved.

On iOS devices, MobileIron has a configuration option that prohibited the user from trusting the developer certificate.

On Android devices, MobileIron has a configuration option that prohibited the user from enabling Unknown Sources on the device.

5.2.4 Threat Event 4 —Confidentiality and Integrity Loss due to Exploitation of Known Vulnerability in the OS or Firmware

Summary: When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and issues commands in the context of the root user or the OS kernel.

Test Activity: Attempt to access enterprise resources from a mobile device with known vulnerabilities (e.g., running an older, unpatched version of iOS or Android).

Desired Outcome: The enterprise's security architecture should identify the presence of devices that are running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be possible, when warranted by the risks, to block devices from accessing enterprise resources until system updates are installed.

Observed Outcome: Lookout identified that devices were running outdated operating systems. This information was communicated to MobileIron, which subsequently automatically quarantined the devices until the operating system was updated.

5.2.5 Threat Event 5 —Violation of Privacy via Misuse of Device Sensors

Summary: There is collection of location, camera, or microphone data by an application that has no need to access this data.

Note: Not all applications that have access to location, camera, or microphone data are malicious. However, when an application is found to be collecting this information, additional vetting or testing may be required to determine the intent of its use and to then determine if the application is malicious.

Test Activity: Upload the application to Kryptowire; observe the output report.

Desired Outcome: Output report identifies the use of location, camera, or microphone use by the application.

Observed Outcome: The Kryptowire report identified the use of location sensor, camera, or microphone by the application.

5.2.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or Certificates

Summary: There is compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates using a man-in-the-middle approach.

Test Activity:

- Install mitmproxy (https://mitmproxy.org/) on a computer (we used a Mac) connected to the same Wi-Fi network as the mobile devices.
- Install mitmproxy's CA certificate (stored at *~/.mitmproxy/mitmproxy-ca-cert.cer* on our Mac) onto the mobile devices being tested. iOS- and Android-specific instructions are found below.
- Configure the computer as necessary to run mitmproxy in transparent mode, as described in https://docs.mitmproxy.org/stable/howto-transparent/.
- To illustrate a malicious actor's ability to manipulate network traffic, we downloaded the mitmproxy *internet_in_mirror* script from https://github.com/mitmproxy/mitmproxy/blob/master/examples/simple/internet_in_mirror.py. It performs a mirror reflection of the content of all websites.
- Run mitmproxy in transparent mode and using the *internet_in_mirror* script: `mitmproxy –mode transparent –ssl-insecure –showhost -s internet_in_mirror.py`
- Rather than perform an intrusive attack such as address resolution protocol spoofing, we manually configured each mobile device's Wi-Fi network settings to change the default gateway's (sometimes referred to as router in the network settings) IP address to the computer's IP address rather than the router's IP address. This configuration change forced all the network traffic from each device through the computer.

Test Activity (Android):

- Place mitmproxy's CA certificate as an attachment within an email message.
- Open the email message on the Android device and click on the attachment to attempt to install the CA certificate.
- Modify the device's Wi-Fi network settings to manually change the default gateway's IP address to the address of the computer running mitmproxy.
- Browse to a hypertext transfer protocol secure (https) website (e.g., https://www.nccoe.nist.gov), and observe whether the content has been reversed, illustrating that the man-in-the-middle attack on a TLS-protected connection was successful.

Test Activity (iOS):

- Use Apple Configurator 2 on a Mac, or another tool, to create an iOS configuration profile containing mitmproxy's CA certificate. The configuration profile used in testing was named Enterprise Access. The configuration profile was signed using a key associated with an Apple free developer account certificate. The signature was optional (Configuration profiles do not have to be signed).
- Send the configuration profile as an attachment within an email message.
- Open the email message and attempt to click on the attachment to install the configuration profile. Attempt to follow the prompts to complete the profile installation.
- Attempt to enable the CA certificate in the iOS device's Certificate Trust Settings.

Desired Outcome: The enterprise's security architecture should block installation of unauthorized configuration profiles (iOS) or CA certificates (Android). Alternatively, the security architecture may detect the presence of unauthorized configuration profiles or CA certificates and perform another appropriate action, such as blocking the device from accessing enterprise resources until the configuration profile or CA certificate is removed. The architecture should also detect attempted man-in-the-middle attacks.

Observed Outcome: Lookout detected a man-in-the-middle attack on both iOS and Android devices. Lookout also detected the unknown configuration profile on iOS.

5.2.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

Summary: Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is connected to such a network, a malicious actor would gain unauthorized access to any data sent or received by the device for any session not already protected by encryption at either the transport or application layers.

Test Activity: Test if applications will attempt to establish an http or unencrypted connection.

Desired Outcome: Be alerted when applications attempt to make an unencrypted connection or prevent the application from being able to do so.

Appthority can determine if applications will attempt to establish an http or unencrypted connection.

iOS and Android also can require a secure connection for an application. (When it tries to connect to the server if it is unencrypted, it will just drop the connection.)

Observed Outcome: On both iOS and Android, Appthority detected a “sends data unencrypted” threat for an application. Transferring data over unencrypted connections could result in the loss of confidentiality of information being transmitted by that application.

5.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced device Unlock Code

Summary: A malicious actor may be able to obtain a user’s device unlock code by direct observation, side-channel attacks, or brute-force attacks.

Test Activity:

- Attempt to completely remove the device unlock code. Observe whether the attempt succeeds.
- Attempt to set the device unlock code to “1234,” a weak four-digit personal identification number (PIN). Observe whether the attempt succeeds.
- Attempt to continuously unlock the device, confirming the device is factory reset after 10 failed attempts.

Desired Outcome: Policies set on the device by the EMM (MobileIron) should require a device unlock code to be set, prevent the device unlock code from being removed, require a minimum complexity for the device unlock code, and factory reset the device after 10 failed unlock attempts.

Additionally, Lookout can identify and report devices that have the lock screen disabled.

Observed Outcome: MobileIron applied a policy to the devices that enforced a mandatory PIN and device wipe capability after 10 failed unlock attempts. Further, Lookout reports when the device has the lock screen disabled. For both devices, all data was erased after 10 failed unlock attempts.

The option to remove the unlock PIN/passcode had been disabled. Upon attempting to set the PIN to something simple, such as a PIN with repetitious or consecutive characters, an error was displayed, informing the user they cannot use the PIN they entered.

5.2.9 Threat Event 9—Unauthorized Access to Backend Services via authentication or credential Storage Vulnerabilities in Internally Developed Applications

Summary: If a malicious actor gains unauthorized access to a mobile device, the attacker also has access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications and can subsequently gain access to sensitive data or backend services.

Test Activity: Application was submitted to Appthority for analysis of credential weaknesses.

Desired Outcome: Discover and report credential weaknesses.

Observed Outcome: Appthority recognized within an application that it uses hard-coded credentials. The application's use of hard-coded credentials could introduce vulnerabilities if the hard-coded credentials were used for access to enterprise resources by unauthorized entities.

5.2.10 Threat Event 10 —Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

Summary: An employee that accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization's visibility into the state of a mobile device, including if the device is compromised by an attacker.

Test Activity: Attempt to directly access enterprise services, e.g., Exchange email server or corporate VPN, on a mobile device that is not enrolled into the EMM system.

Desired Outcome: Enterprise services should not be accessible from devices that are not enrolled into the EMM system. Otherwise, the enterprise is not able to effectively manage devices to prevent threats.

Observed Outcome: Devices that were not enrolled in MobileIron were unable to access enterprise resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper client certificates, only obtainable through enrolling in the EMM.

5.2.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device

Summary: Due to the nature of the small form factor of mobile devices, they are easy to misplace or be stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

Test Activity: Attempt to download enterprise data onto a mobile device that is not enrolled into the EMM system (may be performed in conjunction with TE-10). Attempt to remove (in conjunction with TE-8) the device unlock code or demonstrate that the device does not have a device unlock code in place.

Attempt to locate and wipe the device through the EMM console (it will fail if the device is not enrolled in the EMM).

Desired Outcome: It should be possible to locate or wipe EMM-enrolled devices in response to a report that they have been lost or stolen. As demonstrated by TE-10, only EMM-enrolled devices should be able to access enterprise resources. As demonstrated by TE-8, EMM-enrolled devices can be forced to have a screen lock with a passcode of appropriate strength, which helps resist exploitation (including loss of organizational data) if the device has been lost or stolen.

Should the device be unreachable by the EMM (e.g., disconnected from all networking), EMM control and corporate data will be removed after 10 failed unlock attempts.

Observed Outcome (Enrolled Devices): Enrolled devices are protected. An enterprise policy requiring a personal identification number/lock screen is present, and therefore the enterprise data on the device could not be accessed. After 10 attempts to access the device, the device was wiped. Additionally, the device was remotely wiped after it was reported as lost to enterprise mobile device service management.

Observed Outcome (Unenrolled Devices): As shown in Threat Event 10, only enrolled devices can access enterprise services. When the device attempted to access enterprise data, no connection to the enterprise services was available. Because the device cannot access the enterprise, enterprise information would not be located on the device.

5.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its Unauthorized Storage in Non-Organizationally Managed Services

Summary: If employees violate data management policies by using unmanaged services to store sensitive organizational data, this data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Test Activity: Connect to the enterprise VPN. Open an enterprise website or application. Attempt to extract enterprise data by taking a screenshot, or copy/paste and send it via an unmanaged e-mail account.

Desired Outcome: Screenshots and other data-sharing actions will be prohibited by the EMM while using managed applications.

Observed Outcome: Through MobileIron restriction and lockdown policies, an administrator prevented the following actions on devices:

Android

- copy/paste
- screen capture
- data transfer over near-field communication
- data transfer over Universal Serial Bus
- Bluetooth

iOS

- screen capture and recording (iOS 9+)
- AirDrop
- iCloud Backup
- iCloud Documents and data access
- managed applications storing data in iCloud
- data flow between managed and unmanaged applications
- hand-off

These restrictions prohibited the user from executing common data leakage methods.

5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

This section provides the scenarios and findings for the security and privacy characteristics the example solution was intended to support. They include:

- development of the Cybersecurity Framework and NICE Framework mappings
- threat event scenarios and example solution architecture mitigations
- data action scenarios and potential mitigations that organizations could employ

5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings

While the example solution was being developed, the Cybersecurity Framework Subcategory mappings were developed into a table mapping for organizations implementing the example solution's capabilities.

As the example solution's products were installed, configured, and used in the example solution architecture, the example solution's functions and their corresponding Cybersecurity Framework Subcategories, along with other guidance alignment, were determined and documented.

This mapping became an important resource to the example solution contained in this practice guide because it provides the ability to communicate with the organization's stakeholders about the security controls that the example solution can help mitigate, and the workforce requirements that the example solution will require.

The example solution's products, security control, and workforce mapping can be found in Table H-1.

5.3.2 Threat Event Scenarios and Findings

As part of the findings, the threat events were mitigated in the example solution architecture using the concepts and technology shown in Table 5-1. Each threat event was matched with functions that helped mitigate the risks posed by the threat event.

Note: While not demonstrated in the table, TEE provided tamper-resistant processing environment capabilities that helped mitigate mobile device runtime and memory threats in the example solution.

Table 5-1 Threat Event Scenarios and Findings Summary

Threat Event	How the Example Solution Architecture Helps Mitigate the Threat Event	The Technology Function That Helps Mitigate the Threat Event
Threat Event 1: Unauthorized access to sensitive information via a malicious or privacy-intrusive application	Ensured administrators have insight into what corporate data applications can access.	MTI
Threat Event 2: Theft of credentials through an SMS or email phishing campaign	Utilized PAN-DB to block known malicious websites.	Firewall

Threat Event	How the Example Solution Architecture Helps Mitigate the Threat Event	The Technology Function That Helps Mitigate the Threat Event
Threat Event 3: Malicious applications installed via URLs in SMS or email messages	Disabled installing applications from unknown sources.	EMM
Threat Event 4: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	Quarantined noncompliant device until its operating system was updated.	EMM
Threat Event 5: Violation of privacy via misuse of device sensors	Application vetting reports indicated the sensors to which an application requested access.	MTI
Threat Event 6: Compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates	Detected a man-in-the-middle attack by using Lookout. Lookout detected the unauthorized configuration profile on iOS.	MTD
Threat Event 7: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	Application vetting reports indicated if an application sent data without proper encryption.	Application Vetting
Threat Event 8: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	Enforced mandatory device wipe capabilities after 10 failed unlock attempts.	EMM
Threat Event 9: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	Application vetting reports indicated if an application used credentials improperly.	MTI
Threat Event 10: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	Devices not enrolled in the EMM system were not able to connect to the corporate VPN.	VPN

Threat Event	How the Example Solution Architecture Helps Mitigate the Threat Event	The Technology Function That Helps Mitigate the Threat Event
Threat Event 11: Loss of organizational data due to a lost or stolen device	Enterprise data was protected by enforced passcode policies and device wipe capabilities.	EMM
Threat Event 12: Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	Policies that enforce data loss prevention were pushed to devices.	EMM

5.3.3 Data Action Scenarios and Findings

The results of the PRAM found that three data actions were especially relevant to the build. Potential mitigations that could be used by an organization to lessen their impact were identified by the PRAM as shown below. Further details on the PRAM's findings can be found in Appendix F.

Table 5-2 Data Action Scenarios and Findings Summary

Data Action	Data Action Description	How the Data Action Could Be Mitigated
Data Action 1: Blocking access and wiping devices	Employees are likely to use their devices for both personal and work-related purposes. Therefore, in a system that features the capability to wipe a device entirely, there could be an issue of employees losing personal data.	Block the device's access to enterprise resources until it is granted access permission again. Selectively wipe elements of the device without removing all data on the device. Within the example solution, this option is available for iOS devices. Advise employees to back up the personal data maintained on devices. Limit staff with the ability to perform wipes or block access.

Data Action	Data Action Description	How the Data Action Could Be Mitigated
Data Action 2: Employee monitoring	Employer-owned or controlled networks monitor activities on a regular basis. Employees may not be aware of the monitoring of their interactions with the system and may not want this monitoring to occur.	Limit staff with ability to review data about employees and their devices. Develop organizational policies and techniques to limit collection of specific data elements. Develop organizational policies and techniques regarding disposal of PII.
Data Action 3: Data sharing across parties	Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to different information about them.	Develop organizational policies and techniques for de-identification of data. Use encryption. Limit or disable access to data. Develop organizational policies and techniques to limit collection of specific data elements. Use contracts to limit third-party data processing.

6 Conclusion

This document provides an overview of the Risk Management Framework and the Privacy Risk Assessment Methodology, an explanation of mobile device security concepts, and an example solution for organizations implementing a COPE deployment.

Our fictitious Orvilia Development organization started with a mobile device infrastructure that was lacking mobile device security architecture concepts. It employed a risk management and privacy methodology to understand the current gaps in its architecture and methods to enhance the security of its systems.

After identifying the core threat events from the risk assessment, the appropriate mobile device security technologies were applied. These included an on-premises EMM solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities in support of a usage scenario.

The practice guide also includes in Volume C a series of How-To Guides—step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture—to help security engineers rapidly deploy and evaluate our example solution in their test environment.

The example solution of our reference design uses standards-based, commercially available products. It can be used directly by any organization with a COPE usage scenario by implementing a security infrastructure that supports an integration of on-premises with cloud-hosted mobile security technologies. The practice guide provides a reference design and example solution that an organization may use in whole or in parts as the basis for a custom solution that realizes the security and privacy characteristics that best support its unique mobile device usage scenario.

7 Future Build Considerations

A topic of interest for a future build is a BYOD scenario. This entails protecting corporate data on personally owned devices that employees will use for work as well as personal activity. Another area of interest is a thin client deployed to mobile devices. The thin client would allow the employee to access a virtual device contained within the corporate infrastructure to access enterprise data and resources, ensuring that no corporate data ever resides on the physical device.

Further, examination of emerging 5G technologies as they relate to mobile device security is a new field that presents a wide breadth of research opportunities.

Appendix A List of Acronyms

AD	Active Directory
ADCS	Active Directory Certificate Services
ADDS	Active Directory Domain Services
API	Application Programming Interface
ATARC	Advanced Technology Academic Research Center
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BYOD	Bring Your Own Device
CIO	Chief Information Officer
CIS	Center for Internet Security
COMSEC	Communications Security
COPE	Corporate-Owned Personally-Enabled
CSP	Credential Service Provider
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
EMM	Enterprise Mobility Management
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPS	Intrusion Protection System
IR	Interagency Report
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile Device Management
MTC	Mobile Threat Catalogue

MTD	Mobile Threat Defense
MTI	Mobile Threat Intelligence
MTP	Mobile Threat Protection
MSCT	Mobile Services Category Team
NCCoE	National Cybersecurity Center of Excellence
NIAP	National Information Assurance Partnership
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OS	Operating System
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
ROM	Read-only Memory
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Information and Event Management
SMS	Short Message Service
SP	Special Publication
TE	Threat Event
TEE	Trusted Execution Environment
TLS	Transport Layer Security
UPN	User Principal Name
URL	Uniform Resource Locator
VPN	Virtual Private Network

Appendix B Glossary

Access Management	Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [67].
Agent	A host-based IPS program that monitors and analyzes activity and performs preventive actions; OR a program or plug-in that enables an SSL VPN to access non-Web-based applications and services [15]
Application Layer	Layer of the TCP/IP protocol stack that sends and receives data for particular applications such as DNS, HTTP, and SMTP [15]
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 [18].
Blacklist	A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity [68]
Brute-Force Attack	In cryptography, an attack that involves trying all possible combinations to find a match [69]
Chief Information Officers (CIO) Council	The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources [70].
Cryptographic Algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output [68]
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification [71]

Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification [68]
Common Vulnerabilities and Exposures	A dictionary of common names for publicly known information system vulnerabilities [72]
Data Action	System operations that process PII [44]
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks [73].
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [44]
Encryption	The cryptographic transformation of data to produce ciphertext [68]
Enterprise Mobility Management	Enterprise Mobility Management (EMM) systems are a common way of managing mobile devices in the enterprise. Although not a security technology by itself, EMMs can help to deploy policies to an enterprise's device pool and to monitor device state [6].
Identity Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). Adapted from Verification [68].
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system [13]

Key Logger	A remote program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures [74]
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code [13].
Man-in-the-Middle Attack	An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP during enrollment, or between subscriber and CSP during authenticator binding [71].
Mobile Device Management (MDM)	The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices [18].
Network Layer	Layer of the TCP/IP protocol stack that is responsible for routing packets across networks [15]
Phishing	An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP [71]
Predisposing Conditions	A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation [9]

Privacy Risk Assessment Methodology (PRAM)	The PRAM is a tool that applies the risk model from NISTIR 8062 and helps organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions. The PRAM can help drive collaboration and communication between various components of an organization, including privacy, cybersecurity, business, and IT personnel [75].
Read-Only Memory	ROM is a pre-recorded storage medium that can only be read from and not written to [76].
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization [13]
Replay Resistance	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access [19]
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence [9]
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. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis [13]
Risk Management Framework	The Risk Management Framework (RMF) provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of systems into the mission and business processes of the organization [77].
Sandbox	A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized (Under Sandboxing) [68].

Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements [13]
Side-Channel Attacks	An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions [71].
Social Engineering	The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust [71]
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [9]
Threat Events	An event or situation that has the potential for causing undesirable consequences or impact [9]
Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes [78]
Threat Sources	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent [13]
Transport Layer	Layer of the TCP/IP protocol stack that is responsible for reliable connection-oriented or connectionless end-to-end communications [15]
Transport Layer Security (TLS)	A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol [68].

Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor” [79]
Unmanaged Device	A device inside the assessment boundary that is either unauthorized or, if authorized, not assigned to a person to administer [80]
Virtual Private Network	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line [68]
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [9]
Watering Hole	Watering hole attacks involve attackers compromising one or more legitimate Web sites with malware in an attempt to target and infect visitors to those sites [81].

1664 # Appendix C References

[1] National Institute of Standards and Technology (NIST), "NIST Computer Security Resource Center," [Online]. Available: https://csrc.nist.gov/publications/sp800. [Accessed 11 March 2019].

[2] National Information Assurance Partnership (NIAP), "NIAP Home Page," [Online]. Available: https://www.niap-ccevs.org. [Accessed 11 March 2019].

[3] Department of Homeland Security, "Home Page," [Online]. Available: https://www.dhs.gov/. [Accessed 15 May 2019].

[4] Federal Chief Information Officers (CIO) Council, "Federal CIO Home Page," [Online]. Available: https://www.cio.gov/. [Accessed 11 March 2019].

[5] National Institute of Standards and Technology (NIST), "NIST Cybersecurity Framework, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2018. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 20 April 2018].

[6] National Institute of Standards and Technology (NIST), "Mobile Threat Catalogue," [Online]. Available: https://pages.nist.gov/mobile-threat-catalogue/. [Accessed 8 March 2019].

[7] National Institute of Standards and Technology (NIST), "Risk Management Framework (RMF) Overview," [Online]. Available: https://csrc.nist.gov/Projects/Risk-Management/rmf-overview. [Accessed 8 March 2019].

[8] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-4, Mobile Device Security: Cloud and Hybrid Builds," 21 February 2019. [Online]. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid. [Accessed 8 March 2019].

[9] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. [Accessed 26 November 2018].

[10] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [Accessed 11 March 2019].

[11] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," July 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final. [Accessed 8 March 2019].

[12] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52, Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," April 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-52/rev-1/final. [Accessed 11 March 2019].

[13] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," 22 January 2015. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final. [Accessed 23 January 2019].

[14] National Institute of Standards and Technology (NIST), "Digital Identity Guidelines," June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. [Accessed 8 March 2019].

[15] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-113 Guide to SSL VPNs," July 2008. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-113/final. [Accessed 8 March 2019].

[16] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security," July 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final. [Accessed 8 March 2019].

[17] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. [Accessed 8 March 2019].

[18] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-163 Revision 1, Vetting the Security of Mobile Applications," April 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf. [Accessed 26 April 2019].

[19] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," December 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf. [Accessed 8 March 2019].

[20] National Institute of Standards and Technology (NIST), "NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," August 2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final. [Accessed 1 May 2019].

[21] Center for Internet Security, "Center for Internet Security Home Page," [Online]. Available: https://www.cisecurity.org/. [Accessed 29 April 2019].

[22] Executive Office of the President, "Bring Your Own Device, A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," 23 August 2012. [Online]. Available: https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device. [Accessed 15 April 2019].

[23] Federal CIO Council and Department of Homeland Security, "Mobile Security Reference Architecture Version 1.0," 23 May 2013. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf. [Accessed 8 March 2019].

[24] Digital Services Advisory Group and Federal Chief Information Officers Council, "Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis," December 2012. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf. [Accessed 8 March 2019].

[25] International Organization for Standardization, "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements," October 2013. [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed 26 June 2019].

[26] "Mobile Computing Decision," [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf. [Accessed 8 March 2019].

[27] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobility Strategy Development Guidelines Working Group Document," June 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12997/Agency_Mobility_Strategy_Deliverable.pdf. [Accessed 8 March 2019].

[28] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobile Threat Protection App Vetting and App Security Working Group Document," July 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12996/Mobile_Threat_Protection_Deliverable.pdf. [Accessed 8 March 2019].

[29] Mobile Services Category Team (MSCT), "Device Procurement and Management Guidance," November 2016. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/information-technology/4485/mobile-device-procurement-and-management-guidance. [Accessed 8 March 2019].

[30] Mobile Services Category Team (MSCT), "Mobile Device Management (MDM) MDM Working Group Document," August 2017. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf. [Accessed 8 March 2019].

[31] Mobile Services Category Team (MSCT), "Mobile Services Roadmap (MSCT Strategic Approach)," 23 September 2016. [Online]. Available: https://atarc.org/project/mobile-services-roadmap-msct-strategic-approach/. [Accessed 8 March 2019].

[32] National Information Assurance Partnership (NIAP), "NIAP U.S. Government Approved Protection Profile - Extended Package for Mobile Device Management Agents Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=403&id=403. [Accessed 8 March 2019].

[33] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals Version 3.1," 16 June 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed 8 March 2019].

[34] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Management Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed 8 March 2019].

[35] National Information Assurance Partnership (NIAP), "Product Compliant List," [Online]. Available: https://www.niap-ccevs.org/Product/. [Accessed 8 March 2019].

[36] United States Office of Management and Budget (OMB), "Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services," 4 August 2016. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_20.pdf. [Accessed 8 March 2019].

[37] National Institute of Standards and Technology (NIST), "United States Government Configuration Baseline (In Development)," [Online]. Available: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline. [Accessed 8 March 2019].

[38] Department of Homeland Security (DHS), "DHS Study on Mobile Device Security," April 2017. [Online]. Available: https://www.dhs.gov/publication/csd-mobile-device-security-study. [Accessed 8 March 2019].

[39] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Mobile Device Security for Enterprises Building Block Version 2 Final Draft," 12 September 2014. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/mds-project-description-final.pdf. [Accessed 26 November 2018].

[40] International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE), "International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, Systems and software engineering – System life cycle processes," 2015. [Online]. Available: https://www.iso.org/standard/63711.html. [Accessed 26 November 2018].

[41] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," November 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final. [Accessed 26 November 2018].

[42] Tech Times, "Flashlight apps are spying on users Android, iOS, Windows Phone smartphones, is yours on the list?," 26 October 2014. [Online]. Available: https://www.techtimes.com/articles/18762/20141026/flashlight-apps-are-spying-on-users-android-ios-windows-phone-smartphones-is-yours-on-the-list.htm. [Accessed 13 May 2019].

[43] National Institute of Standards and Technology (NIST), "NIST Privacy Risk Assessment Methodology (PRAM)," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources. [Accessed 17 July 2019].

[44] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems," January 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. [Accessed 28 November 2018].

[45] M. A. A. B. Mohamed Sabt, "Trusted Execution Environment: What It is, and What It is Not. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Helsinki, Finland," August 2015. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01246364/file/trustcom_2015_tee_what_it_is_what_it_is_not.pdf. [Accessed 28 November 2018].

[46] Zimperium, "MobileIron Threat Defense, Mobile Device Security & MDM," [Online]. Available: https://www.zimperium.com/partners/mobileiron. [Accessed 22 May 2019].

[47] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Extended Package for Mobile Device Management Agents Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed 28 November 2018].

[48] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Extended Package for VPN Gateways Version 2.1," 8 March 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed 28 November 2018].

[49] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile - Collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314," 14 March 2018. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed 28 November 2018].

[50] National Information Assurance Partnership, "Approved Protection Profiles," [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed 11 March 2019].

[51] Qualcomm, "Qualcomm Secure Boot and Image Authentication Technical Overview," [Online]. Available: https://www.qualcomm.com/media/documents/files/secure-boot-and-image-authentication-technical-overview.pdf. [Accessed 16 April 2019].

[52] Palo Alto Networks, "Remote Access VPN (Certificate Profile)," [Online]. Available: https://docs.paloaltonetworks.com/globalprotect/8-0/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-certificate-profile.html#. [Accessed 16 April 2019].

[53] MobileIron, "Admin Google Android Google Apps API," [Online]. Available: http://mi.extendedhelp.mobileiron.com/45/all/en/desktop/Google_Apps_API.htm. [Accessed 16 April 2019].

[54] MobileIron, "MobileIron unified endpoint security platform," [Online]. Available: https://www.mobileiron.com/en/unified-endpoint-management/platform. [Accessed 16 April 2019].

[55] Open Web Application Security Project (OWASP), [Online]. Available: https://www.owasp.org/index.php/Main_Page. [Accessed 3 May 2019].

[56] Palo Alto Networks, "Always On VPN Configuration," [Online]. Available: https://docs.paloaltonetworks.com/globalprotect/7-1/globalprotect-admin/globalprotect-quick-configs/always-on-vpn-configuration. [Accessed 4 April 2019].

[57] National Institute of Standards and Technology (NIST), "Cryptographic Module Validation Program," [Online]. Available: https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards. [Accessed 11 March 2019].

[58] Palo Alto Networks, "FIPS-CC Security Functions documentation site," [Online]. Available: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/certifications/fips-cc-security. [Accessed 11 March 2019].

[59] Apple Computer, "Apple at Work," [Online]. Available: https://www.apple.com/business/it/. [Accessed 11 March 2019].

[60] Apple Computer, "Apple Configurator 2," [Online]. Available: https://itunes.apple.com/us/app/apple-configurator-2/id1037126344?mt=12. [Accessed 13 March 2019].

[61] Apple Computer, "iOS Security iOS 12.3," November 2018. [Online]. Available: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf. [Accessed 19 July 2019].

[62] Android.com, "Build a device policy controller," [Online]. Available: https://developer.android.com/work/dpc/build-dpc. [Accessed 13 March 2019].

[63] Google.com, "Android Enterprise Fully managed device," [Online]. Available: https://developers.google.com/android/work/requirements/fully-managed-device. [Accessed 13 March 2019].

[64] Google.com, "Android Enterprise Work profile," [Online]. Available: https://developers.google.com/android/work/requirements/work-profile. [Accessed 13 March 2019].

[65] Android.com, "Work profiles on fully managed devices," [Online]. Available: https://developers.google.com/android/work/requirements/work-profile. [Accessed 13 March 2019].

[66] Google.com, "Backup Your Mobile," [Online]. Available: https://play.google.com/store/apps/details?id=com.backupyourmobile. [Accessed 13 March 2019].

[67] IDManagement.gov, "Federal Identity, Credential, and Access Management Architecture," [Online]. Available: https://arch.idmanagement.gov/services/access/. [Accessed 10 May 2019].

[68] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary, Publication 4009," 6 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/issuances/Instructions.cfm. [Accessed 1 May 2019].

[69] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8053, De-Identification of Personal Information," October 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. [Accessed 13 May 2019].

[70] General Services Administration, "Chief Information Officers Council (CIOC)," [Online]. Available: https://www.gsa.gov/about-us/organization/office-of-governmentwide-policy/office-of-shared-solutions-and-performance-improvement/chief-information-officers-council-cioc. [Accessed 13 May 2019].

[71] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines," 1 December 2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-63/3/final. [Accessed 31 January 2019].

[72] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-126 Revision 3, The Technical Specification for the Security Content Automation Protocol (SCAP)," February 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf. [Accessed 13 May 2019].

[73] National Institute of Standards and Technology (NIST), "NISTIR 7711 Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7711.pdf. [Accessed 13 May 2019].

[74] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security," May 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. [Accessed 1 May 2019].

[75] National Institute of Standards and Technology (NIST), "Risk Assessment Tools," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools. [Accessed 13 May 2019].

[76] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1, Guidelines for Media Sanitization," December 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. [Accessed 13 May 2019].

[77] National Institute of Standards and Technology (NIST), "Risk Management Framework: Quick Start Guide," [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides. [Accessed 13 May 2019].

[78] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing," October 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf. [Accessed 13 May 2019].

[79] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 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].

[80] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8011 Volume 1, Automation Support for Security Control Assessments," June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf. [Accessed 13 May 2019].

[81] United States Department of Homeland Security, "ICS-CERT Monitor," October, November, December 2013. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf. [Accessed 10 May 2019].

[82] Android, "Android zero-touch enrollment," [Online]. Available: https://www.android.com/enterprise/management/zero-touch/. [Accessed 8 April 2019].

[83] Google, "Android's enterprise requirements," [Online]. Available: https://support.google.com/work/android/answer/6174145?hl=en. [Accessed 16 April 2019].

[84] Apple, "Business Support," [Online]. Available: https://support.apple.com/business. [Accessed 8 April 2019].

[85] Apple, "Configuration Profile," 25 March 2019. [Online]. Available: https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf. [Accessed 16 April 2019].

[86] Samsung, "Knox Mobile Enrollment," [Online]. Available: https://www.samsungknox.com/en/solutions/it-solutions/knox-mobile-enrollment. [Accessed 16 April 2019].

[87] Samsung, "Secured by Knox," [Online]. Available: https://www.samsungknox.com/en/secured-by-knox. [Accessed 16 April 2019].

[88] Samsung, "Devices built on Knox," [Online]. Available: https://www.samsungknox.com/en/knox-platform/supported-devices. [Accessed 16 April 2019].

[89] The MITRE Corporation, "ATT&CK," 21 November 2018. [Online]. Available: https://attack.mitre.org/.

[90] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8144 (DRAFT), Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue," [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8144/draft. [Accessed 21 November 2018].

[91] The MITRE Corporation, "ATT&CK for Mobile," [Online]. Available: https://attack.mitre.org/resources/mobile-introduction/. [Accessed 21 November 2018].

[92] The MITRE Corporation, "Common Vulnerabilities and Exposures (CVEs)," [Online]. Available: http://cve.mitre.org/. [Accessed 24 02 2019].

[93] FedRAMP, "FedRAMP Home Page," [Online]. Available: https://www.fedramp.gov/. [Accessed 24 02 2019].

[94] National Institute of Standards and Technology (NIST), "NIST Information Technlogy Laboratory National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/. [Accessed 21 November 2018].

[95] Android Open Source Project, "Pixel / Nexus Security Bulletins," [Online]. Available: https://source.android.com/security/bulletin/pixel/. [Accessed 26 November 2018].

[96] Apple Computers, "Apple Security Updates," [Online]. Available: https://support.apple.com/en-us/HT201222. [Accessed 26 November 2018].

[97] Apple, "Managing Devices & Corporate Data on iOS," July 2018. [Online]. Available: https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf. [Accessed 6 March 2019].

[98] Samsung, "Android Security Updates," [Online]. Available: https://security.samsungmobile.com/securityUpdate.smsb. [Accessed 26 November 2018].

[99] Samsung, "Knox Mobile Enrollment," [Online]. Available: https://www.samsungknox.com/en/solutions/it-solutions/knox-mobile-enrollment. [Accessed 8 April 2019].

[100] Palo Alto Networks, "Wildfire Malware Analysis," [Online]. Available: https://www.paloaltonetworks.com/products/secure-the-network/wildfire.html. [Accessed 16 April 2019].

Appendix D Android, Apple, and Samsung Knox Mobile Enrollment

Device enrollment and management capabilities are available when deploying mobile devices in bulk. Certain settings can be preloaded, and devices can ship preconfigured for enterprise management. iOS-, Android-, and Samsung Knox-based devices integrate directly with Enterprise Mobility Management (EMM) solutions, providing enterprise-level management of security controls based on policy.

D.1 Android Devices

For Android devices, zero-touch enrollment provides an option different from the manual setup of Android devices. Android-based devices offer security controls that an EMM can leverage for enterprise deployments. The Android Enterprise program by Google is available on devices with Android 5.0 (Lollipop) and higher. An EMM deploys a device policy controller as part of its on-device agent that controls local device policies and system applications on devices. Android Enterprise supports corporate-owned personally-enabled and bring your own device deployment scenarios through work-managed and work-profile device solutions [82], [83].

D.2 iOS Devices

For iOS devices, Apple Configurator supports Volume Purchase and Device Enrollment Program scenarios. Apple Business Manager provides a mobile device management solution to assist organizations in deploying iOS devices. iOS devices are managed by configuration profiles. Configuration profiles can force security policies such as virtual private network usage, enterprise Kerberos support, and access to cloud services. iOS further incorporates a set of additional security controls in what is termed supervised mode, which denotes a corporately owned device. Typically, organizations choose to use the Device Enrollment Program for large-scale deployments of iOS devices in supervised mode due to the reduction of labor involved in manually configuring each device. However, due to the small number of devices in our reference design, we have configured supervised mode using the Apple Configurator 2 tool. A more detailed description of iOS capabilities can be found in the iOS Security Guide [84], [85].

D.3 Samsung Knox Devices

Samsung Knox Mobile Enrollment provides the ability to add Samsung devices to the enterprise without manually enrolling each device. Samsung Knox Mobile Enrollment works on Samsung Galaxy devices running Android Lollipop or higher. It allows remote provisioning of devices when they connect to Wi-Fi or cellular networks. Samsung Knox Mobile Enrollment works with a number of EMM solutions, including cloud-based options [86], [87], [88].

Appendix E Risk Assessment

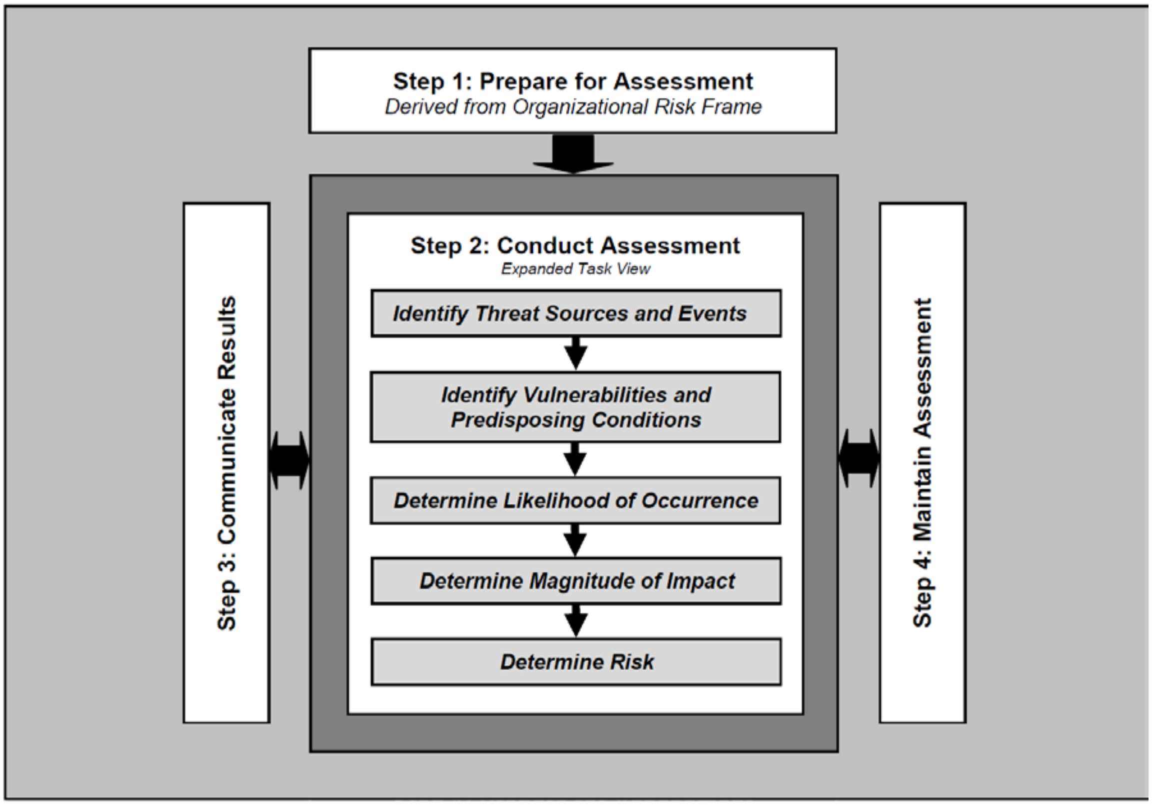
E.1 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* [9] states that risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing 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. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.”

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—material that is available to the public. The Risk Management Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

This section details the risk assessment undertaken to improve the mobile security posture of the fictional organization Orvilia Development. Typically, a National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1-based risk assessment follows a four-step process as shown in Figure E-1: Prepare for assessment, conduct assessment, communicate results, and maintain assessment.

Figure E-1 Risk Assessment Process



To provide the most value in this exercise:

- We focused on the preparation, which established the context of the risk assessment.
- We conducted the risk assessment, which produced a list of information security risks that were prioritized by risk level and used to inform risk response decisions.
- We followed the process detailed in Section 3 of NIST SP 800-30 Revision 1 [9] to perform a risk assessment of the current mobile infrastructure.

We recommend that organizations performing a risk assessment communicate results and perform maintenance of the risk assessment, but these activities were deemed out of scope for this project. The following tasks were used during the assessment process.

E.1.1 Task 1-1: Risk Assessment Purpose

Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

The purpose of the risk assessment of Orvilia Development was to identify and document new risks to its mission resulting from addition of a mobility program.

The results of the risk assessment informed decisions to Orvilia's mobility deployment that included:

- implementation of new security mechanisms
- configuration changes to existing infrastructure
- updates to security and appropriate-use policies relevant to their mobility program

E.1.2 Task 1-2: Risk Assessment Scope

Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.

Organizational Applicability:

The scope of this risk assessment was limited to systems impacted by inclusion of a mobility program; it did not include existing information technology (IT) infrastructure to which no impact was anticipated. With their original architecture, Orvilia deployed corporate-owned personally-enabled (COPE) devices. Orvilia employees utilized mobile devices for local and remote work activities and limited personal activities (e.g., phone calls, messaging, social applications, and personal emails).

With Orvilia's new government contract, this risk assessment also evaluated Orvilia's mobile deployment regarding its ability to access and store government data while meeting applicable information security and privacy requirements.

While not directly associated with risk assessment activities, Orvilia will be required to demonstrate compliance with government standards and policies established to improve data security. Therefore, Orvilia needed to determine how compliance with government policy and application of its standards would best align with its strategy to identify, protect again, detect, respond to, and recover from threats related to its mobility program.

Time Frame Supported:

Because this was the first risk assessment performed by Orvilia, the process was more time-intensive than it will be in future risk management cycles. Orvilia completed the initial risk assessment within six months.

Architectural and Technology Considerations:

This risk assessment was scoped to Orvilia's mobile deployment, which constitutes mobile devices used to access Orvilia enterprise resources along with any backend IT components used to manage or provide services to those mobile devices.

The following provide an overview of the mobile deployment components involved in the original (current) Orvilia architecture.

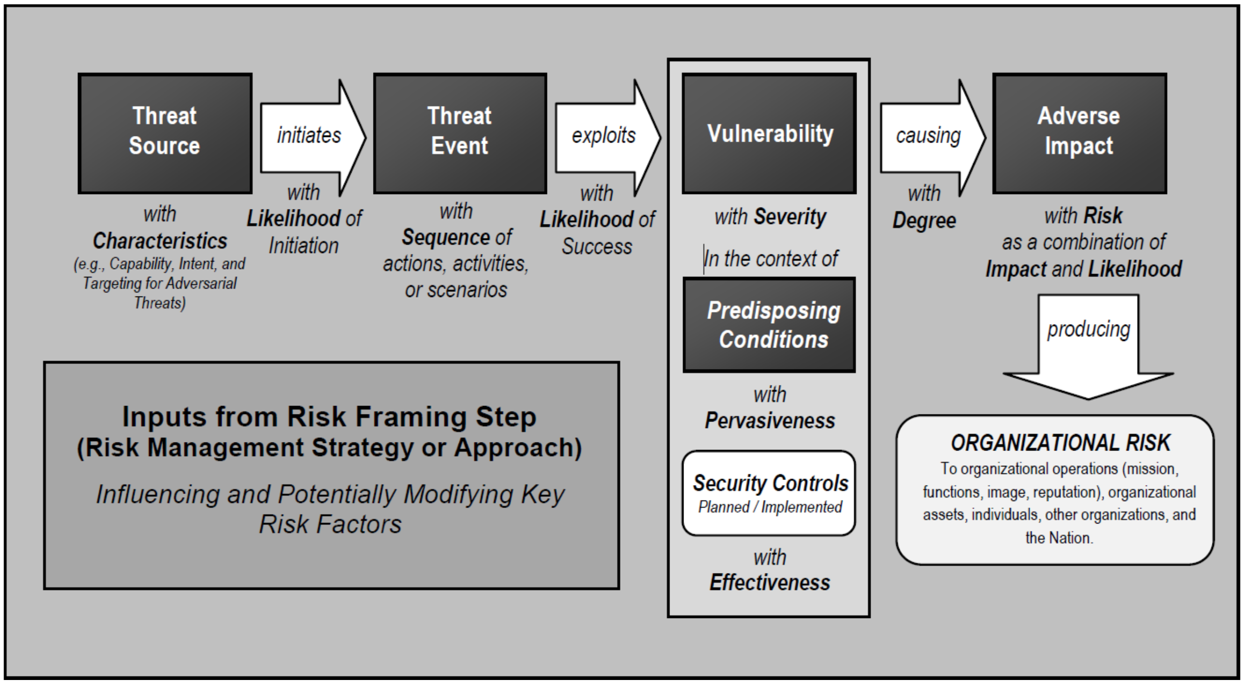
- **Mobile Device:** A mobile device is a small form factor device with a rich operating system, at least one wireless network interface, and the ability to run applications. These features are considered essential for Orvilia to have portable and efficient access to enterprise data.
- **Communication Networks and Data Transmission:** Mobile devices will establish connections to the internet by using their cellular or Wi-Fi adapters. As connections may be made to unsecured access points or may traverse untrusted networks, consideration will be given to the risks associated with the security of those connections and the data transmitted over them. Additionally, the organization will need to consider risks arising from permitting inbound connections by mobile devices via the internet.
- **Public Application Stores:** With a COPE deployment strategy, employees will have the option to download any mobile application available from official platform application stores (e.g., Google Play Store). While those platforms analyze applications for malicious behaviors, it is still possible for such applications to exceed Orvilia's needs for user privacy or pose a risk to the devices or data. Therefore, risks from such applications should be included in this assessment.
- **Device and Operating System (OS) Vendor Infrastructure:** The hardware, firmware, and software that compose each model of mobile device can vary, particularly those from different manufacturers and vendors, which may incorporate technology that is exclusive to their products. It will be important to select devices that demonstrate security mechanisms that align with the organization's risk mitigation strategy. However, risks that are specific to given device components (e.g., chipsets or driver versions) will be out of scope for this assessment.
- **Enterprise Systems:** If a potentially compromised mobile device can connect to the enterprise, it poses direct risks to any systems it can reach or data it can access. Such systems will reasonably include on-premises mobile application stores, mobile management technologies, email servers, file servers, and intranet web servers. Subsequent compromise of any of these systems may cascade to others not directly reachable by the mobile device. Risks to all such systems by a mobile device should be included in this assessment.

E.1.3 Task 1-3: Risk Assessment Assumptions and Constraints

Identify the specific assumptions and constraints under which the risk assessment is conducted.

Risk assessment assumptions and constraints were developed using a NIST SP 800-30 Revision 1 Generic Risk Model as shown in Figure E-2.

Figure E-2 NIST 800-30 Generic Risk Model



E.1.3.1 Risk Assessment Assumptions

Some of the threats and their resulting risks and impacts span several levels. In cases where these risks and impacts have several possible levels, it was assumed that Orvilia would document these using a high-water mark methodology. This assumption of greatest risk then provided the basis for risk mitigation activities. For example, where the threat risk could pose a moderate, high, or very high outcome, the very high outcome was selected, and these very high risks were prioritized for mitigation.

E.1.3.2 Risk Assessment Constraints

Information regarding the following were used as input for the constraints for the risk assessment.

- threat sources
- threat events
- vulnerabilities and predisposing conditions
- likelihood
- impacts
- risk assessment and analysis approaches
- resources available for the assessment

- skills and expertise

Threat Sources

Orvilia's executives and managers identified two threat sources as possible concerns. Orvilia's technical staff were provided security control mappings identified within this guide to help them understand the additional security that the example solution could provide to Orvilia as they implemented the example solution.

Additionally, due to the cybersecurity-focused scope of the risk assessment, non-adversarial threat sources (e.g., unintentional hardware, software, or system design and architecture shortcoming threats) were not considered.

As identified in Section E.1.6, Task 2-1: Identify and Characterize Threat Sources of Concern, the risk assessment identified the following threat sources of concern:

- Orvilia's competitors
- nation-state actors

Threat Events

- Threat events were described at a high level and in general terms within the risk assessment. Similar threat events were combined into a single, broader threat.
- Only those threat events that have been previously observed by an authoritative source were considered (e.g., reported as already having occurred by other organizations), drawing primarily from the NIST National Cybersecurity Center of Excellence Mobile Threat Catalogue [6].
- Threat events involving exploitation of vulnerabilities within the cellular network, including a mobile device's cellular baseband, reasonably exceeded Orvilia's ability to directly identify and mitigate them and were not further assessed.
- Threat events involving exploitation of vulnerabilities in low-level hardware, firmware, and device controllers reasonably exceeded Orvilia's ability to directly identify and mitigate them and were not further assessed.
- Threat events involving exploitation of vulnerabilities in the supply chain reasonably exceeded Orvilia's ability to directly identify and mitigate them and were not further assessed.

Vulnerabilities and Predisposing Conditions

- Mobile device vulnerabilities considered during this risk assessment included those in mobile operating systems and mobile applications, including third-party software libraries.
- Vulnerabilities in commonly used noncellular network protocols such as Bluetooth and Wi-Fi were considered.

- Vulnerabilities related to a potential Enterprise Mobility Management (EMM) system were considered.
- Additional information and determinations were made via Appendix F of NIST SP 800-30 Revision 1.

Likelihood

- Likelihood determinations were made via Appendix G of NIST SP 800-30 Revision 1.

Note: The rating of overall likelihood is derived from the Likelihood of Initiation and Likelihood that Threat Events Result from Adverse Impacts using Table G-5 of Appendix G in NIST SP 800-30 Revision 1 [9]. Ratings of the latter two variables relied heavily on the subjective judgment of Orvilia employees.

Impacts

- Impact determinations were made via Appendix H of NIST SP 800-30 Revision 1.

Note: Ratings of impact relied heavily on the subjective judgment of Orvilia employees.

Risk Assessment and Analysis Approaches

- This risk assessment focused on identifying an initial set of threats to Orvilia's mobile deployment.
- Approaches for describing threats and their impact were informed by the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework [89].
- The rating of Risk was derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [9].

Resources Available for the Assessment

- Orvilia ensured the appropriate staff with the requisite expertise were available to conduct the assessment within the time allotted.
- Orvilia provided funding for the risk analysis staff.
- Orvilia staff who conducted the risk assessment had the necessary information systems and software.

Skills and Expertise

- Risk assessments were conducted by experts leveraging industry best practices and NIST risk assessment frameworks.

E.1.4 Task 1-4: Risk Assessment Threat, Vulnerability, and Impact Sources

Identify the sources of descriptive threat, vulnerability, and impact information to be used in the risk assessment.

Orvilia used the following methods to identify mobile infrastructure threats, vulnerabilities, and impacts.

E.1.4.1 Sources of Threats

This risk assessment identified NIST's Mobile Threat Catalogue (MTC) [6], along with its associated NIST Interagency Report 8144, *Assessing Threats to Mobile Devices & Infrastructure* [90], and MITRE's ATT&CK Mobile Profile [91] as credible sources for threat information. Each entry in the MTC contains several pieces of information: an identifier, a category, a high-level description, details on its origin, exploit examples, Common Vulnerabilities and Exposures [92] examples, possible countermeasures, and academic references.

MITRE's ATT&CK is a curated knowledge base and model for cyber-adversary behavior. ATT&CK details specific techniques that can be used by cyber adversaries. Each technique entry typically includes a detailed technical description, mitigations, detection analytics, examples of use by malicious actors, and references. The ATT&CK model organizes these techniques into high-level malicious actor tactical objectives, referred to as tactics. A primary use case for ATT&CK is use by organizations to assess the state of their cybersecurity defenses and prioritize deployment of defensive capabilities. The ATT&CK Mobile Profile describes tactics and techniques specific to the mobile environment.

Due to Orvilia's current use of cloud services, it identified the outputs of the Federal Risk and Authorization Management Program [93] and associated NIST SP 800-53 security controls as being in scope for this risk assessment.

E.1.4.2 Sources of Vulnerabilities

Vulnerabilities are commonly associated with mobile operating systems, device drivers, mobile applications, and third-party libraries. However, vulnerabilities can be present in any level of the mobile technology stack. For up-to-date information regarding vulnerabilities, this risk assessment identified the National Vulnerability Database (NVD) [94] as a credible source of information. The NVD is the U.S. government repository of standards-based vulnerability management data. Use of NVD was supplemented by review of individual vendor vulnerability disclosures such as those published in the Pixel/Nexus Security Bulletins [95] for Android, Apple security updates [96] for iOS, Managing Devices & Corporate Data on iOS [97], and Android Security Updates [98] for Android-based Samsung devices.

E.1.4.3 Sources of Impacts

This risk assessment identified the scenario described in Section E.1.2 as the primary source of impact determination information. The scenario identified the following systems as being critical to the organization's mission:

- Microsoft Active Directory domain
- Microsoft Exchange email server

- timekeeping web application
- travel support web application
- corporately owned mobile devices

An example of a successful attack against a mobile device is one that could be used to glean the credentials for the travel support web application and use them to penetrate the application server. While Orvilia can absorb minimal downtime to the web application, the attacker could use this position to gain a foothold in the Orvilia infrastructure to laterally move to more critical systems in the environment, such as the email server. Compromise of the email server would have high impact, possibly causing serious harm to the organization.

E.1.5 Task 1-5: Risk Assessment Risk Model and Analytic Approach Identification

Identify the risk model and analytic approach to be used in the risk assessment.

In this risk assessment, the analytic approach used qualitative (i.e., subjective) ratings of risk (i.e., very low, low, moderate, high, and very high). The approach was primarily threat oriented, as described in section E.1.6.

E.1.6 Task 2-1: Identify and Characterize Threat Sources of Concern

Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.

Orvilia examined NIST SP 800-30 Revision 1's Table D-2: Taxonomy of Threat Sources [9] and identified the following threat sources of concern:

Table E-1 Threat Sources of Concern

Identifier	Threat Source	Description	Characteristic
TS-1	Adversarial, Organization, Competitor	Orvilia's competitors seek to exploit dependence on cyber resources, specifically the data entrusted by its customers to increase market share.	Capability, Intent, Targeting
TS-2	Adversarial, Nation-State	Nation-state actors stealing sensitive government data from unsecured devices and infrastructure	Capability, Intent, Targeting

Orvilia produced the following table as output of Task 2-1 to provide relevant inputs to the risk tables. It identifies the threat sources identified in NIST SP 800-30 Revision 1 with the associated risk rating of capability, intent, and targeting score (using the previously mentioned five-point scale: very low, low, moderate, high, and very high).

Orvilia's assessment found that all threat events could be initiated by both threat sources (Organization/Competitor and Nation-State).

Capability refers to the level of expertise of the malicious actor. Intent refers to the malicious actor's goal. Targeting refers to the reconnaissance and selection methods performed by the malicious actor.

Table E-2 Threat Sources Qualitative Scale

Identifier	Threat Events Relevant to Threat Sources	In Scope	Capability	Intent	Targeting
TS-1	All threat events (Threat Events 1-12)	Yes	High	High	High
TS-2	All threat events (Threat Events 1-12)	Yes	Very High	Very High	Very High

E.1.7 Task 2-2: Identify Potential Threat Events

Identify potential threat events, relevance of the events, and the threat sources that could initiate the events.

The threat events used for the example solution are described below. These threat events describe how the mobile devices in Orvilia might be compromised by malicious activities. All of the threat events map to both threat sources identified in Section E.1.6.

Orvilia examined the sample tables in NIST SP 800-30 Revision 1—Tables E-1, E-2, E-3, E-4, and E-5—and analyzed the sources of mobile threats identified in Task 1-4. Using this process, Orvilia leadership identified the following threat events.

E.1.7.1 Threat Event 1—Unauthorized Access to sensitive Information via a Malicious or Privacy-Intrusive Application

A mobile application can attempt to collect and exfiltrate any information to which it has been granted access. This includes any information generated during use of the application (e.g., user input), user-granted permissions (e.g., contacts, calendar, call logs, camera roll), and general device data available to any application (e.g., International Mobile Equipment Identity, device make and model, serial number). Further, if a malicious application exploits a vulnerability in other applications, the OS, or device firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or otherwise accessible through the device.

E.1.7.2 Threat Event 2—Theft of credentials Through an SMS or Email Phishing Campaign

Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate ones and entice users to authenticate to them by distributing phishing messages over short message service (SMS) or email. Effective use of social engineering techniques such as impersonating an authority figure or creating a sense of urgency may compel users to forgo scrutiny of the message and proceed to authenticate to the fraudulent website; it then captures and stores the user's credentials before (usually) forwarding them to the legitimate website to allay suspicion.

E.1.7.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages

Malicious actors may send users SMS or email messages that contain a uniform resource locator (URL) where a malicious application is hosted. Generally, such messages are crafted using social engineering techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby increasing the likelihood they access the URL by using their mobile device. If the URL is accessed, the device will attempt to download and install the application. Effective use of social engineering by the attacker will further compel an otherwise suspicious user to grant any trust required by the developer and all permissions requested by the application. Granting the former facilitates installation of other malicious applications by the same developer, and granting the latter increases the potential for the application to do direct harm.

E.1.7.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known Vulnerability in the OS or Firmware

When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and issues commands in the context of the root user or the OS kernel. This may be enough for some to accomplish their goal, but advanced malicious actors will usually attempt to install additional malicious tools and to establish a persistent presence. If successful, the attacker will be able to launch further attacks against the user, the device, or any other systems to which the device connects. As a result, any data stored on, generated by, or accessible to the device at that time—or in the future—may be compromised.

E.1.7.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors

Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera, gyroscope, Global Positioning System receiver, and radios) can use them to conduct surveillance. It may be directed at the user, as when tracking the device location, or it may be applied more generally, as when recording any nearby sounds. Captured sensor data, such as a recording of an executive meeting, may be immediately useful to a malicious actor. Alternatively, the data may be analyzed in isolation or in combination with other data to yield sensitive information. For example, audio recordings of on-device or proximate activity can be used to probabilistically determine user inputs to touchscreens and keyboards—essentially turning the device into a remote keylogger.

E.1.7.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or Certificates

Malicious actors who successfully install an EMM/mobile device management (MDM), network, or virtual private network (VPN) profile or certificate onto a device will gain a measure of additional control over the device or its communications. Presence of an EMM/MDM profile will allow an attacker to misuse existing OS application programming interfaces to send the device a wide variety of commands. This may allow a malicious actor to obtain device information, install or restrict applications, or remotely locate, lock, or wipe the device. Malicious network profiles may allow a malicious actor to automatically compel the device to connect to access points under their control to achieve a man-in-the-middle attack on all outbound connections. Alternatively, VPN profiles assist in the undetected exfiltration of sensitive data by encrypting it, thus hiding it from network scanning tools. Additionally, malicious certificates may allow the malicious actor to compel the device to automatically trust connections to malicious web servers, wireless access points, or installation of applications under their control.

E.1.7.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications

Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is connected to such a network, an attacker would gain unauthorized access to any data sent or received by the device for any session not already protected by encryption at either the transport or application layers. Even if the transmitted data were encrypted, an attacker would be privy to the domains, internet protocol addresses, and services (as indicated by port numbers) to which the device connects; such information could be used in future watering hole attacks or man-in-the-middle attacks against the device user. Additionally, visibility into network layer traffic enables a malicious actor to conduct side-channel attacks against its encrypted messages, which can still result in a loss of confidentiality. Further, eavesdropping on unencrypted messages during a handshake to establish an encrypted session with another host or endpoint may facilitate attacks that ultimately compromise the security of the session.

E.1.7.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code

A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the device; only the third technique requires physical access. However, side-channel attacks that infer the unlock code by detecting taps and swipes to the screen can be attempted by applications with access to any peripherals that detect sound or motion (e.g., microphone, gyroscope, or accelerometer). Once the device unlock code has been obtained, a malicious actor with physical access to the device will gain immediate access to any data or functionality not already protected by additional access control mechanisms. Additionally, if the user employs the device unlock code as a credential to any other systems, the malicious actor may further gain unauthorized access to those systems.

E.1.7.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

If a malicious actor gains unauthorized access to a mobile device, the malicious actor also has access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications and can subsequently gain access to sensitive data or backend services. This could result from weaknesses or vulnerabilities present in the authentication or credential storage mechanisms implemented within an in-house application.

E.1.7.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

An employee who accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization's visibility into the state of a mobile device, including if the device is compromised by a malicious actor. Therefore, users who violate security policies to gain unauthorized access to enterprise resources from such devices risk providing malicious actors with access to sensitive organizational data, services, and systems.

E.1.7.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device

Due to the nature of the small form factor of mobile devices, they are easy to misplace or be stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

E.1.7.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its Unauthorized Storage to Non-Organizationally Managed Services

If employees violate data management policies by using unmanaged services to store sensitive organizational data, the data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Further, storage of sensitive data in an unmanaged service may subject the user or the organization to prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate efforts by the organization to achieve remediation or recovery from any future losses, such as those resulting from the public disclosure of trade secrets.

E.1.8 Task 2-3: Identify Vulnerabilities and Predisposing Conditions

Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.

Drawing on the scenario described in Section 3.2.1 of NIST SP 800-30 Revision 1, there existed vulnerabilities and predisposing conditions that increased the likelihood that identified threat events would result in adverse impacts for Orvilia. Each vulnerability or predisposing condition is listed in the table below along with the corresponding threat events.

The methodology used to rate the level of pervasiveness was qualitative (i.e., subjective) and used a five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table E-3 Identify Vulnerabilities and Predisposing Conditions

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-1	Email and other enterprise resources can be accessed from anywhere, and only username/password authentication is required.	TE-2, TE-10, TE-11	Very High
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their corporate mobile devices.	TE-7	Very High

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on corporate mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-11, TE-12	Very High

Note 1: Ratings of the level of pervasiveness were based on the qualitative scale found in Table F-5 of Appendix F in NIST SP 800-30 Revision 1 [9].

Note 2: Ratings of pervasiveness indicate that the vulnerabilities apply few (i.e., very low), some (i.e., low), many (i.e., moderate), most (i.e., high), or all (i.e., very high) organizational missions/business functions and processes, or information systems.

E.1.9 Task 2-4: Determine Likelihood of a Threat and the Likelihood of the Threat Having Adverse Impacts

Determine the likelihood that threat events of concern result in adverse impacts, considering (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

In the interest of brevity, the threat events of concern identified in Task 2-2 were limited to those presumed to have a foreseeably high likelihood of occurrence.

The methodology used to identify the likelihood of threats of concern was qualitative (i.e., subjective) and used the following five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table E-4 Likelihood of Threat Events of Concern

Threat ID	Likelihood of Threat Event Initiation	Likelihood of Threat Event Resulting in Adverse Impacts	Overall Likelihood
TE-1	High	Very High	Very High
TE-2	Very High	High	Very High
TE-3	High	High	High
TE-4	Moderate	Very High	High
TE-5	High	Very High	Very High
TE-6	Moderate	High	Moderate
TE-7	High	High	High
TE-8	Moderate	High	High
TE-9	Moderate	High	Very High
TE-10	High	Very High	Very High
TE-11	Very High	Very High	Very High
TE-12	High	High	High

Note 1: For the Likelihood of Threat Event Initiation, the ratings translate as follows: Moderate = malicious actor is somewhat likely to initiate; High = malicious actor is highly likely to initiate; Very high = malicious actor is almost certain to initiate.

Note 2: For the Likelihood of Threat Event Resulting in Adverse Impacts, the ratings translate as follows: Moderate = if the threat is initiated, it is somewhat likely to have adverse impacts; High = if the threat is initiated, it is highly likely to have adverse impacts; Very high = if the threat is initiated, it is almost certain to have adverse impacts.

Note 3: Overall likelihood was calculated based on the qualitative scale found in Table G-3 of Appendix G in NIST SP 800-30 Revision 1 [9]. It is derived from both the Likelihood of Threat Event Initiation and

Likelihood of Threat Event Resulting in Adverse Impacts. Because these scales are not true interval scales, the combined overall ratings do not always reflect a strict mathematical average of the two ratings.

E.1.10 Task 2-5: Determine the Extent of Adverse Impacts

Determine the adverse impacts from threat events of concern considering (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Threat events with a high potential for adverse impacts were then identified in our specific scenario.

The methodology used to determine the extent of adverse impacts was qualitative (i.e., subjective) and used the following five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table E-5 Potential Adverse Impacts

Threat ID	Type of Impact	Impact Affected Asset	Maximum Impact
TE-1	Harm to Operations, Assets, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-2	Harm to Operations, Other Organizations	Inability, or limited ability, to perform missions/business functions in the future	High
TE-3	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future	High

Threat ID	Type of Impact	Impact Affected Asset	Maximum Impact
		Damage to or loss of information systems or networks	
TE-4	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-5	Harm to Operations, Assets, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Loss of personally identifiable information	High
TE-6	Harm to Operations, Assets, Other Organizations	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Damage to reputation (and hence future or potential trust relationships)	Very High
TE-7	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-8	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-9	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future	High

Threat ID	Type of Impact	Impact Affected Asset	Maximum Impact
		Damage to or loss of information systems or networks	
TE-10	Harm to Operations, Assets	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks	High
TE-11	Harm to Operations, Assets, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Damage to reputation (and hence future or potential trust relationships) Loss of personally identifiable information	High
TE-12	Harm to Operations, Assets, Other Organizations, Individuals	Inability, or limited ability, to perform missions/business functions in the future Damage to or loss of information systems or networks Loss of personally identifiable information Damage to reputation (and hence future or potential trust relationships)	High

Note 1: Ratings of maximum impact were based on the qualitative scale found in Appendix H, Table H-3 in NIST SP 800-30 Revision 1 [9].

Note 2: Ratings of maximum impact indicate the threat event could be expected to have negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), or multiple severe or catastrophic effects (i.e., very high).

Note 3: For specific examples of types of impact, see Appendix H of NIST SP 800-30, Revision 1 [9].

E.1.11 Task 2-6: Determine Risk to Organization

Determine the risk to the organization from threat events of concern considering (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.

In the interest of brevity, the threat events of concern identified in Task 2-2 were limited to those presumed to have a foreseeably high likelihood of occurrence and high potential for adverse impact in Orvilia's specific scenario.

Threat Source Characteristics

This table summarizes the risk assessment findings.

The methodology used to identify risk to organization was qualitative (i.e., subjective) and used the following five-point scale.

- Very High
- High
- Moderate
- Low
- Very Low

Table E-6 Summary of Risk Assessment Findings

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: Unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	Very High	High	High
TE-2: Theft of credentials through an SMS or email phishing campaign	VULN-1	Very High	High	High
TE-3: Malicious applications installed via URLs in SMS or email messages	VULN-3	High	High	High
TE-4: Confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	VULN-3	High	High	High

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-5: Violation of privacy via misuse of device sensors	VULN-3	Very High	High	High
TE-6: Compromise of the integrity of the device or its network communications via installation of malicious EMM/MDM, network, VPN profiles, or certificates	VULN-3	Moderate	Very High	High
TE-7: Loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2	High	High	High
TE-8: Compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	High	High	High
TE-9: Unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	Very High	High	High
TE-10: Unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1	Very High	High	High
TE-11: Loss of organizational data due to a lost or stolen device	VULN-3	Very High	High	High
TE-12: Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	VULN-3	High	High	High

Note 1: Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [9].

Note 2: The risk rating itself is derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [9]. Because these scales are not true interval scales, the combined overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two variables. This is demonstrated in the table above in which levels of Moderate weigh more heavily than other ratings.

Note 3: Ratings of risk relate to the probability and level of adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1, adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic effects (i.e., very high).

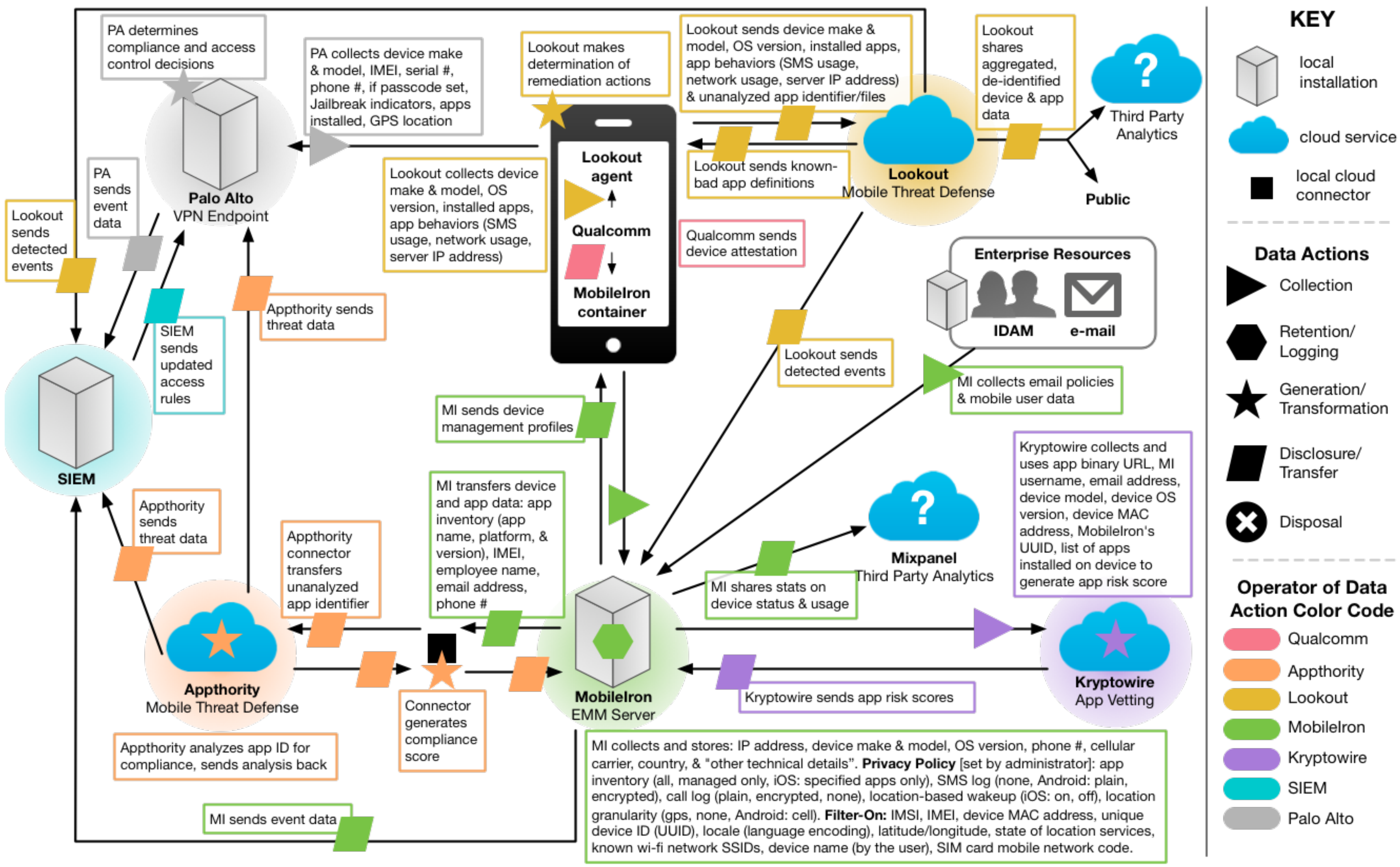
Appendix F Privacy Risk Assessment

This section describes the privacy risk assessment conducted on Orvilia's enterprise security architecture. To perform the privacy risk assessment, the National Institute of Standards and Technology (NIST) Privacy Risk Assessment Methodology (PRAM) was used, a tool for analyzing, assessing, and prioritizing privacy risks to help organizations determine how to respond and select appropriate solutions. The PRAM can also serve as a useful communication tool to convey privacy risks within an organization. A blank version of the PRAM is available for download on NIST's website [43].

The PRAM uses the privacy risk model and privacy engineering objectives described in NIST Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [44], to analyze potential problematic data actions. Data actions are any system operations that process personally identifiable information (PII). Processing can include collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of PII. A problematic data action is one that could cause an adverse effect for individuals.

The PRAM begins with framing the business objectives for the system, including the organizational needs served, and framing organizational privacy governance, including identification of privacy-related legal obligations and commitments to principles or other organizational policies. Next, create a data map to illustrate the data actions performed by the system and the PII processed by the data actions. These data actions, the PII being processed, and the contextual factors that describe the circumstances surrounding the system's processing of PII serve as inputs to the risk analysis. Then, assess the probability that a data action will become problematic for individuals, assess the secondary costs absorbed by the organization from a data action creating a problem for individuals, and use likelihood and impact calculations to determine the total estimated risk per data action. Finally, list potential mitigating technical and policy controls for the identified risks. The output from the PRAM activities resulted in the information contained in Figure F-1.

2181 **Figure F-1 PRAM Data Map for Orvilia's Enterprise Security Architecture**



As an output of the Orvilia PRAM, we identified three broad data actions with the potential to create problems for individuals and relevant mitigations. Some mitigations listed under a particular data action may provide privacy benefits to individuals beyond the scope of that data action. We also identified overarching training and support controls that can help mitigate risks associated with all three of these data actions.

While a security information and event management (SIEM) capability was not used in the reference implementation, SIEMs, as discussed here, can be extremely beneficial in understanding the privacy implications of the mobile device security data being logged, aggregated, and stored.

F.1 Data Action 1: Blocking Access and Wiping Devices

Devices that might pose a risk to the organization's security posture can be blocked from accessing enterprise resources or wiped and reset to factory setting defaults. Options are outlined in the following sections for how this might be accomplished.

F.1.1 Potential Problem for Individuals

In a corporate-owned personally-enabled or bring your own device environment, employees are likely to use their devices for both personal and work-related purposes. Therefore, in a system that features the capability to wipe a device entirely, there could be an issue of employees losing personal data—and employees may not even expect this possibility. A hypothetical example would be that an Orvilia employee stores pictures of their newborn child on their mobile device, but these photos are lost when their device is wiped after anomalous activity is detected.

F.1.2 Mitigations

Block access instead of wiping devices.

As an alternative to wiping data entirely, devices can be blocked from accessing enterprise resources, for example, until an unapproved application is removed. This temporary blocking of access helps ensure an individual will not lose personal data through a full wipe of a device. Taking this approach may help bring the system's capabilities into alignment with employees' expectations about what can happen to their devices, especially if they are unaware that devices can be wiped by administrators—providing for greater *predictability* in the system.

- Related mitigation: If this approach is taken, remediation processes should also be established and communicated to employees. It is important to have a clear remediation process in place to help employees regain access to resources on their devices at the appropriate time. It is equally important to clearly convey this remediation process to employees. A remediation process provides greater manageability in the system supporting employees' ability to access resources. If well communicated to employees, this also provides greater predictability, as employees will know the steps involved in regaining access.

Enable only selective wiping.

An alternative mitigation option for wiping is to specify the information to be wiped. Performing a selective wipe is an option that only removes enterprise data from the device instead of being a full factory reset. When configured this way, a wipe preserves employees' personal configurations, applications, and data while removing only the corporate configurations, applications, and data. Within the example solution, this option is available for iOS devices.

Advise employees to back up the personal data maintained on devices.

If device wiping remains an option for administrators, encourage employees to perform regular backups of their personal data to ensure it remains accessible in case of a wipe.

Limit staff with the ability to perform wipes or block access.

Limit staff with the ability to perform a wipe to only those with that responsibility by using role-based access controls. This can help decrease the chances of accidentally removing employee data or blocking access to resources.

F.2 Data Action 2: Employee Monitoring

The assessed infrastructure offers Orvilia a number of security capabilities, including reliance on comprehensive monitoring capabilities, as noted in Section 4, Architecture. A significant amount of data relating to employees, their devices, and their activities is collected and analyzed by multiple parties.

F.2.1 Potential Problem for Individuals

Employees may not be aware that their interactions with the system are being monitored and may not want this monitoring to occur. Collection and analysis of information might enable Orvilia or other parties to craft a narrative about an employee based on their interactions with the system, which could lead to a power imbalance between Orvilia and the employee and loss of trust in the employer if the employee discovers unanticipated monitoring.

F.2.2 Mitigations

Limit staff with ability to review data about employees and their devices.

This may be achieved using role-based access controls and by developing organizational policies to limit how employee data can be used by staff with access to that data. Access can be limited to any dashboard in the system containing data about employees and their devices but is most sensitive within the mobile management dashboard, which is the hub for data about employees, their devices, and threats. Minimizing access to sensitive information can enhance *disassociability* for employees using the system.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. Consider the configuration options for intrusive device features, such as location services, application inventory collection, and location-based wake-ups. When collecting application inventory data, ensure that information is gathered only from applications installed from the organization's corporate application store. While these administrative configurations may help provide for disassociability in the system, there are also some opportunities for employees to limit the data collected.

Organizations may allow their employees to manage certain aspects and configurations of their device. For example, employees may be able to disable location services in their device OS to prevent collection of location data. Each of these controls contributes to reducing the number of attributes collected regarding employees and their mobile devices. This reduction of collected data limits administrators' ability to associate information with specific individuals.

Dispose of PII.

Disposal of PII after an appropriate retention period can help reduce the risk of entities building profiles of individuals. Disposal can also help bring the system's data processing into alignment with employees' expectations and reduce the security risk associated with storing a large volume of PII. Disposal may be particularly important for certain parties in the system that collect a larger volume of data or more sensitive data. Disposal may be achieved using a combination of policy and technical controls. Parties in the system may identify what happens to data, when, and how frequently.

F.3 Data Action 3: Data Sharing Across Parties

The infrastructure involves several parties that serve different purposes supporting Orvilia's security objectives. As a result, there is a significant flow of data about individuals and their devices occurring across various parties. This includes sharing device and application data publicly and with third-party analytics services, and includes sharing device status and usage with third-party analytics.

F.3.1 Potential Problems for Individuals

Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to different information about them. If administrators and co-workers know what colleague is conducting activity on his or her device that triggers security alerts, it could cause employee embarrassment or emotional distress. This information being revealed and associated with specific employees could also lead to stigmatization and even impact Orvilia upper management in their decision-making regarding the employee. Further, clear text transmissions could leave information vulnerable to attackers and the unanticipated release of employee information.

F.3.2 Mitigations

Use de-identification techniques.

De-identification of data helps decrease the chances that a third party is aggregating information pertaining to one specific individual. While de-identification can help reduce privacy risk, there are residual risks of reidentification. De-identification techniques may be applied to aggregated data before sharing it with third-party analytics and publicly.

Use encryption.

Encryption decreases the chances of insecurity of information transmitted between parties. Organizations should keep this in mind when considering how their enterprise data is transmitted and stored. Mobile security systems share mobile device and application data with one another to optimize efficiency and leverage data to perform security functions. This data may include application inventory and employee name, email address, and phone number. Some systems offer multiple encryption options that allow an organization to choose the encryption level necessary for the type of data that is stored or transmitted.

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using access controls to limit staff access to compliance information, especially when associated with individuals, is important in preventing association of specific events with particular employees, which could cause embarrassment. Some mobile security systems offer options for restricting the amount of employee information that an administrator can access. These options may include hiding an employee's username and email address from the administrator console. Mobile application information may also include employee information. Organizations should consider how their mobile security systems hide application names, application binary analysis details, network names service set identifier, and network analysis details from administrators.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. Identifying the employee information collected and determining what data elements are stored assist in assessing the privacy risk of mobile security systems. Organizations should consider the mobile security system's ability to limit or reduce collection and storage of employee information, such as username, email address, Global Positioning System location, and application data.

Use contracts to limit third-party data processing.

Establish contractual policies to limit data processing by third parties to only the processing that facilitates delivery of security services, and no data processing beyond those explicit purposes.

F.4 Mitigations Applicable Across Various Data Actions

Several mitigations provide benefits to employees pertaining to all three data actions identified in the privacy risk assessment. These training and support mitigations can help Orvilia appropriately inform employees about the system and its data processing.

Mitigations:

Provide training to employees about the system, parties involved, data processing, and administrative actions that can be taken.

Training sessions can also highlight any privacy-preserving techniques used, such as for disclosures to third parties. Training should include confirmation from employees that they understand the actions that can be taken on their devices and the consequences—whether this involves blocking access or wiping data. Employees may also be informed of data retention periods and when their data will be disposed of. This can be more effective than simply sharing a privacy notice, which research has shown that individuals are unlikely to read.

Provide ongoing notifications or reminders about system activity.

This can be achieved using push notifications, similar to those pictured in screenshots in Appendix G, Threat Event 6, to help directly link administrative actions on devices to relevant threats and help employees understand why an action is being taken. Notifications of changes to policies can help increase system predictability by setting employee expectations appropriately with the way the system processes data and the resulting actions.

Provide a support point of contact.

By providing employees with a point of contact in the organization who can respond to inquiries and concerns regarding the system, employees can gain a better understanding of the system's processing of their data, which enhances predictability.

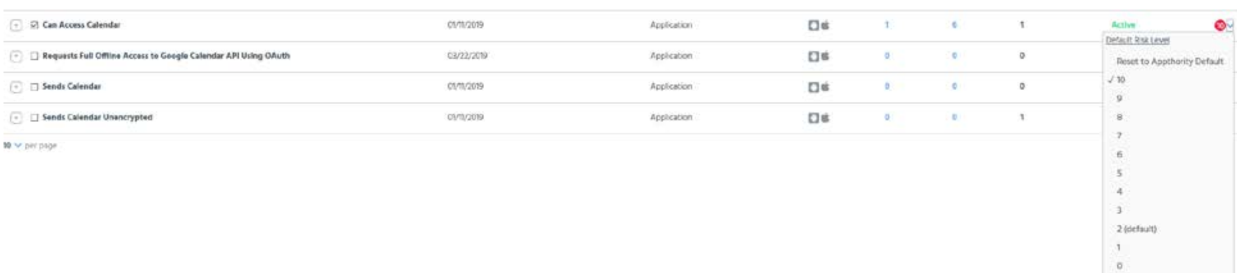
Appendix G Threat Event Test Information

Detailed information and screenshots for some of this practice guide's threat events and their testing results are provided below.

G.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or Privacy-Intrusive Application

A part of Threat Event 1's testing conclusions is shown in the following screen capture, where the calendar access permission is being set to a risk score of 10. This allows MobileIron to automatically apply the mobile threat protection high-risk label to the device and quarantine the device until the privacy-intrusive application is removed.

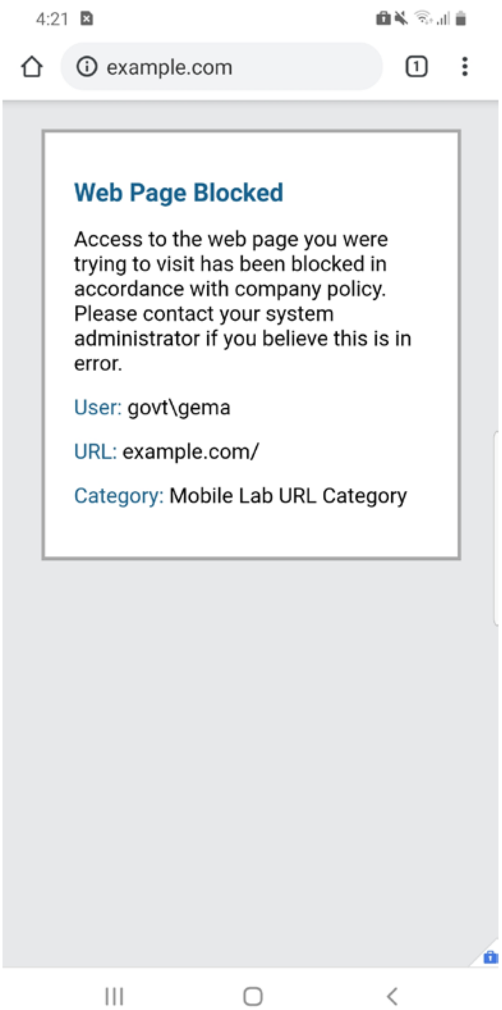
Figure G-1 Setting a Custom Risk Level in Appthority



G.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or Email Phishing Campaign

Threat Event 2's outcome is shown in the following screen capture, where PAN-DB is blocking a website manually added to the malicious uniform resource locator (URL) database.

Figure G-2 PAN-DB Blocked Website



G.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages

The following screenshots demonstrate enabling the Unknown Sources toggle and installing an application through a link in an email message.

Figure G-3 Lock Screen and Security

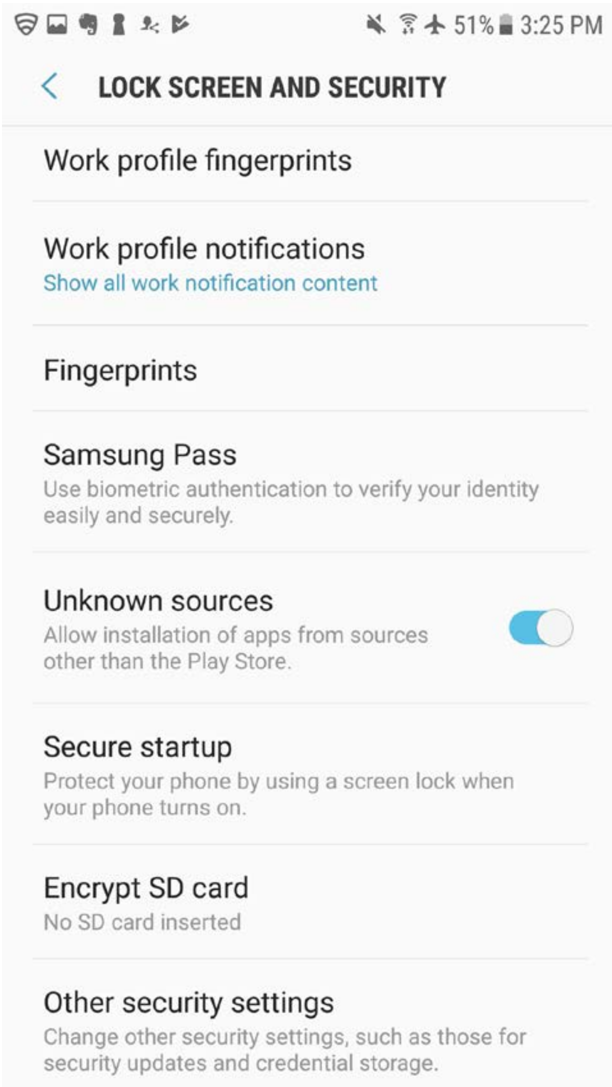
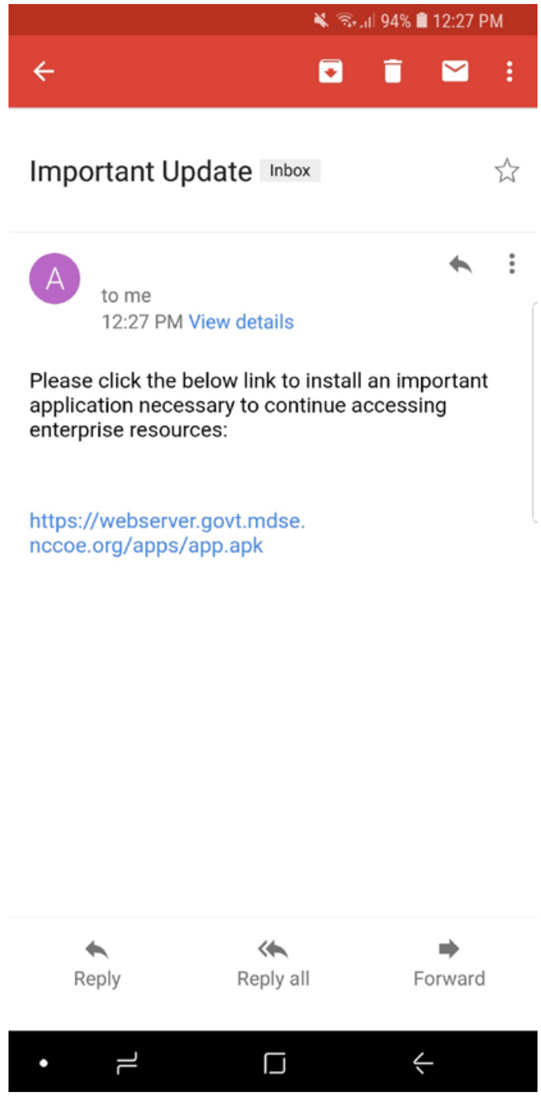


Figure G-4 Phishing Email on Android



2355 Figure G-5 depicts the iOS test activity of receiving an email containing a link to an application from a
2356 non-Apple App Store source.

Figure G-5 Phishing Email on iOS

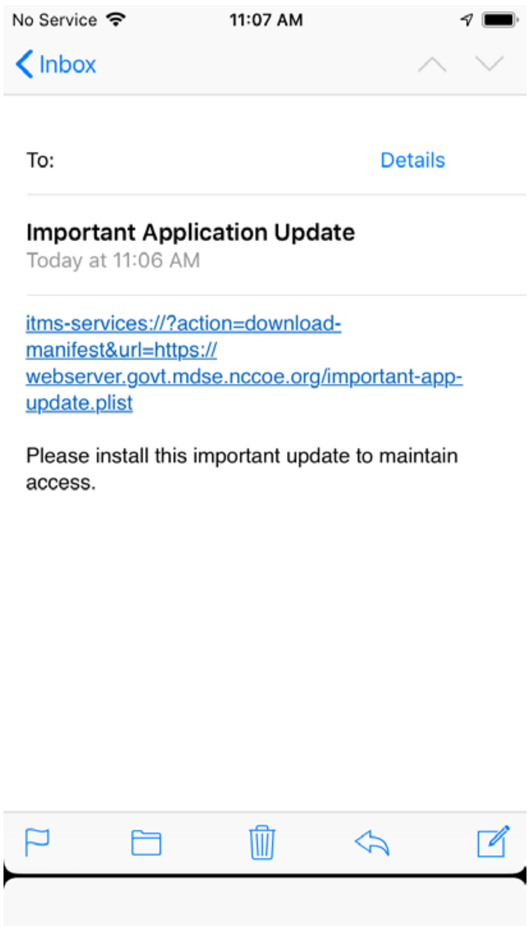
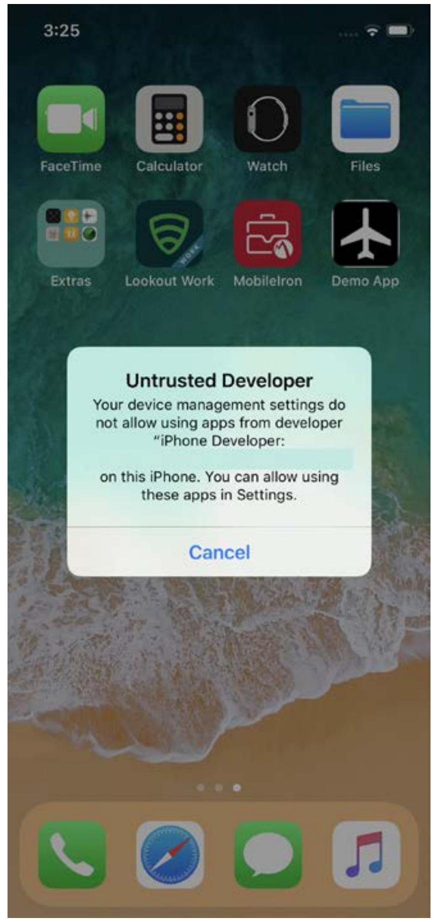


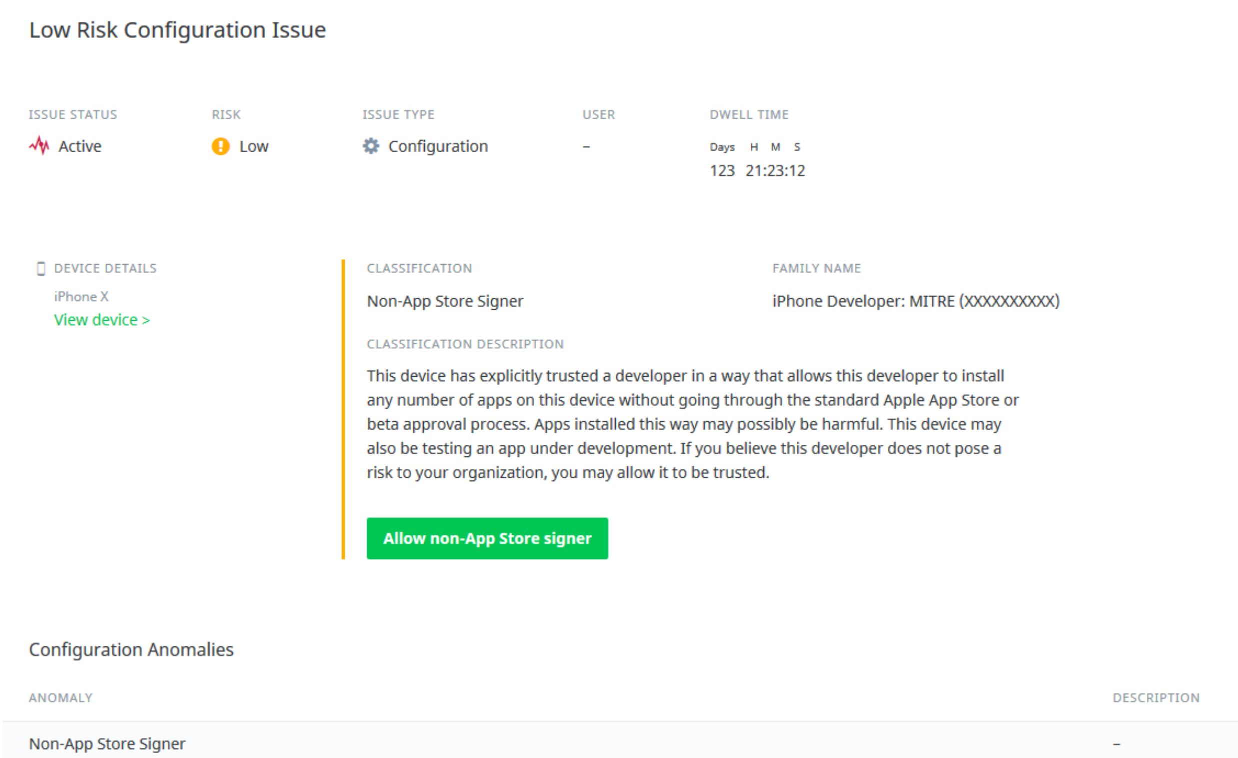
Figure G-6 Untrusted Developer Warning



After the application is installed, an untrusted developer notice appears as shown in Figure G-6 when the user attempts to launch the application.

Figure G-7 shows Lookout's ability to detect application signing certificates that have been trusted on a device by the user to execute applications from sources other than Apple's App Store.

Figure G-7 Application Signing Certificates



The following screenshots depict an attempt to install and run the unauthorized demo application on an iOS device with the `allowEnterpriseAppTrust` policy restriction set to false by an Enterprise Mobility Management (EMM) system. The user is not able to trust the developer when the policy restriction is active, and hence the application will not run.

Figure G-8 Restriction Setting Modification Screen

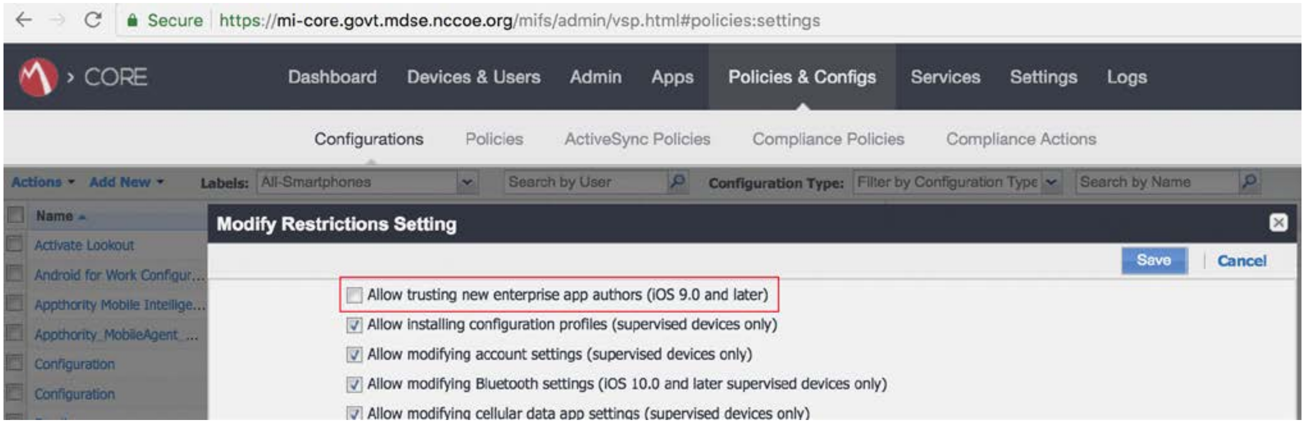
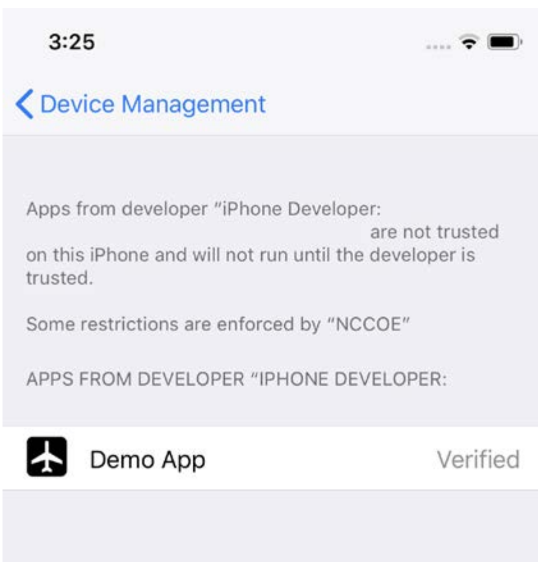


Figure G-9 Unable to Trust Developer

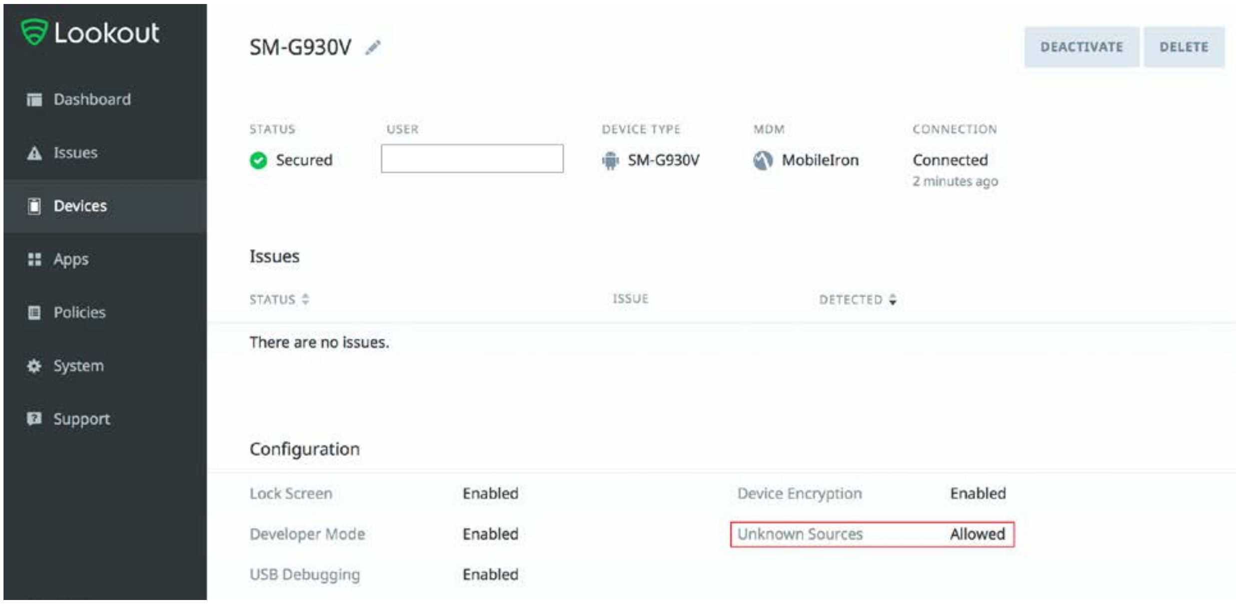


Android Device Testing

On Android devices, applications cannot be installed from sources other than the Google Play Store unless the Unknown Sources setting is enabled in the device's security settings. Lookout can identify when the Unknown Sources setting has been enabled and can communicate this information to MobileIron to enable automated response actions, such as blocking device access to enterprise resources until the situation is resolved. However, even if Unknown Sources is disabled, it is possible that the setting was previously enabled and that unauthorized applications were installed at that time.

Figure G-10 shows Lookout's ability to detect Android devices with Unknown Sources enabled.

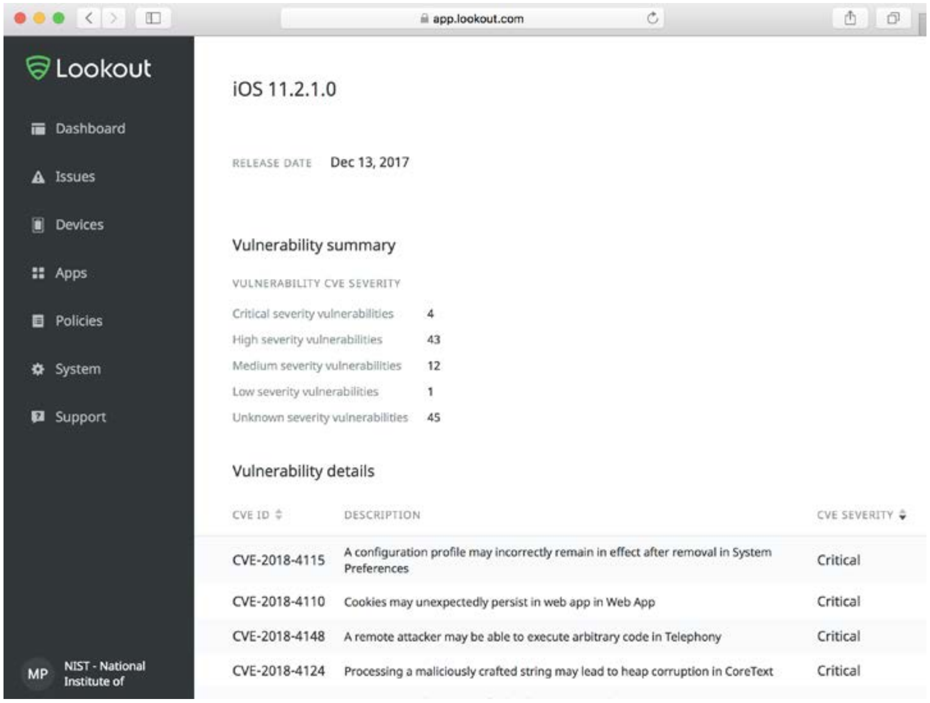
Figure G-10 Unknown Sources Detection



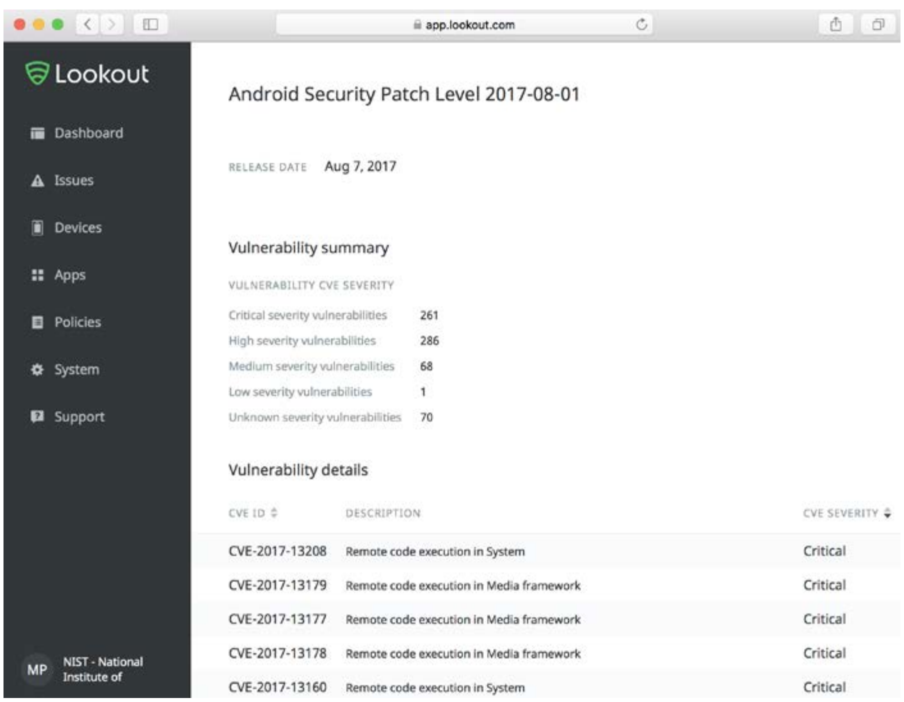
G.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known Vulnerability in the Operating System or Firmware

Figure G-11 demonstrates Lookout's ability to identify known vulnerabilities to which unpatched iOS and Android devices are susceptible. Figure G-12 shows the patch level of the device.

2381 **Figure G-11 Vulnerability Identification**



2382 **Figure G-12 Patch Level Display**



G.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors

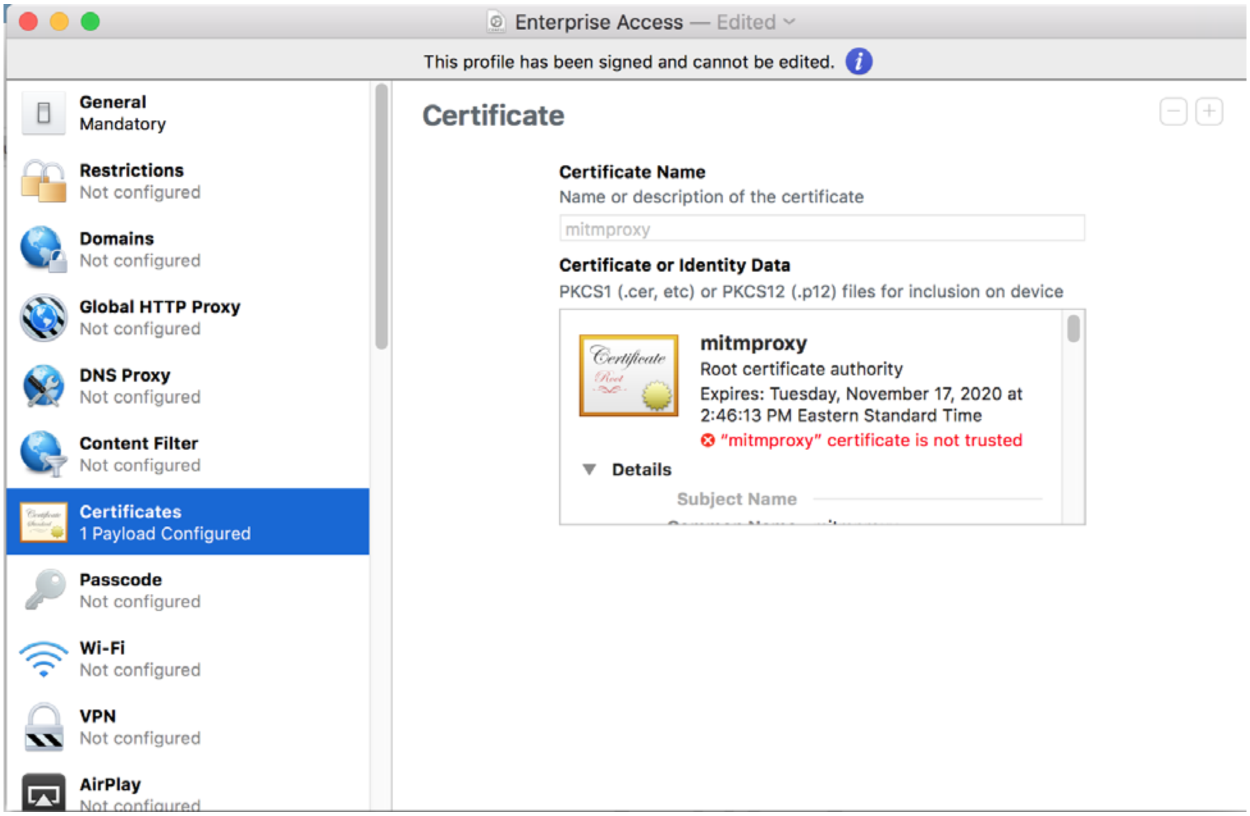
The following screenshot depicts a Kryptowire application analysis report and the reported permissions that this application was requesting.

Figure G-13 Kryptowire Analysis Report

G.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network Communications via Installation of Malicious EMM/Mobile Device Management, Network, Virtual Private Network (VPN) Profiles, or Certificates

The configuration profile used for configuring and testing Threat Event 6 is shown in Figure G-14.

2392 **Figure G-14 Configuration Profile Example**



2393 Figure G-15 shows the email containing a malicious device configuration profile, and Figure G-16 shows
2394 the warning displayed to the user when attempting to mark the malicious certificate as a trusted root.

Figure G-15 Configuration Profile Phishing Email

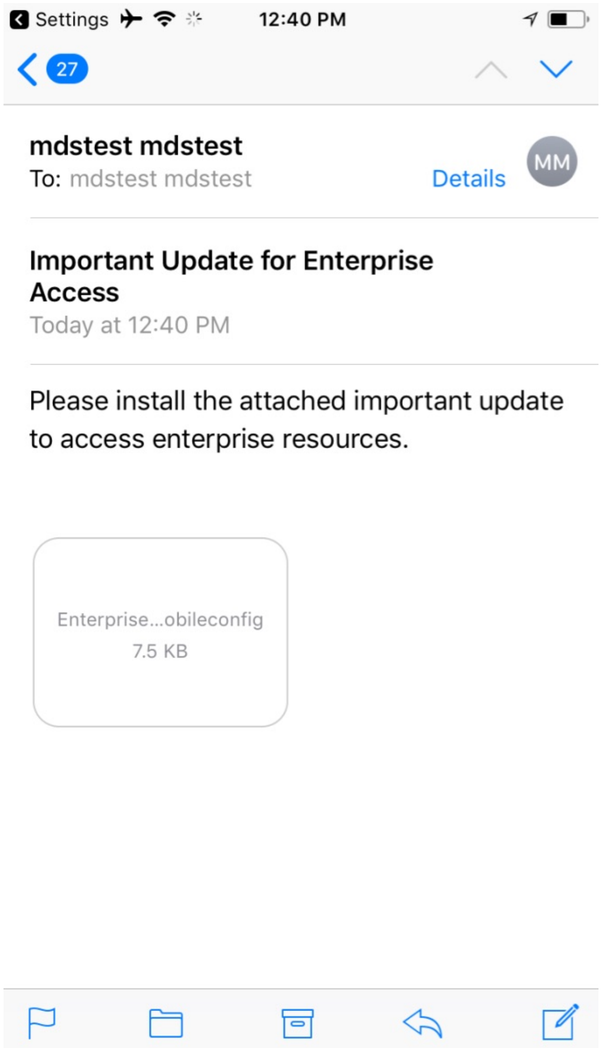


Figure G-16 Root Certificate Authority Enablement Warning

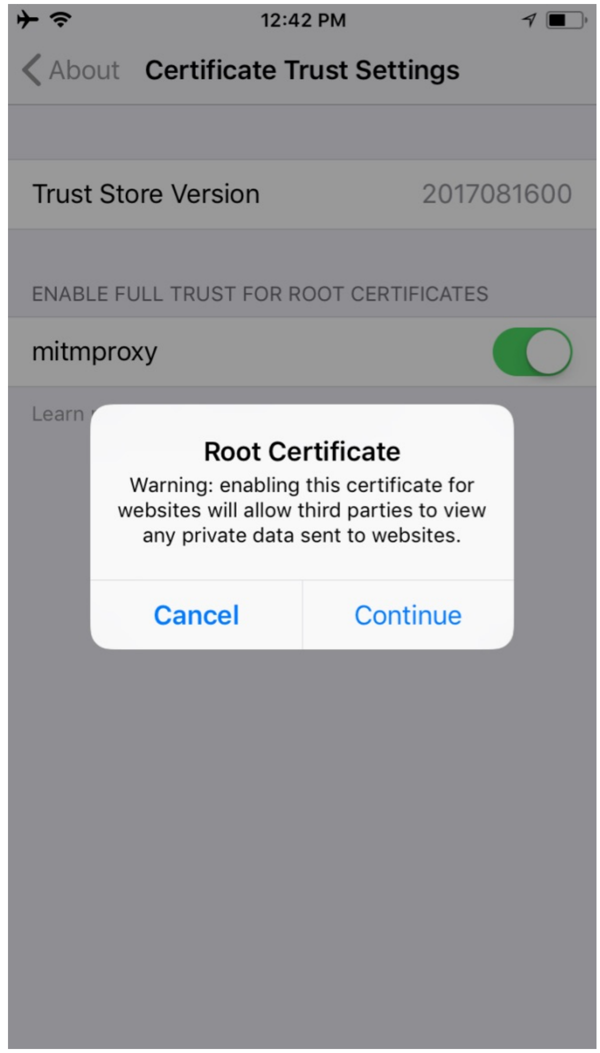


Figure G-17 Reversed Web Page

Browse to a hypertext transfer protocol secure (https) website from the mobile device and observe whether the content has been reversed. Figure G-17 illustrates that the man-in-the-middle attack on a Transport Layer Security-protected connection was successful.

The following screenshots demonstrate a man-in-the-middle attack on Android.

Figure G-18 Certificate Phishing Email

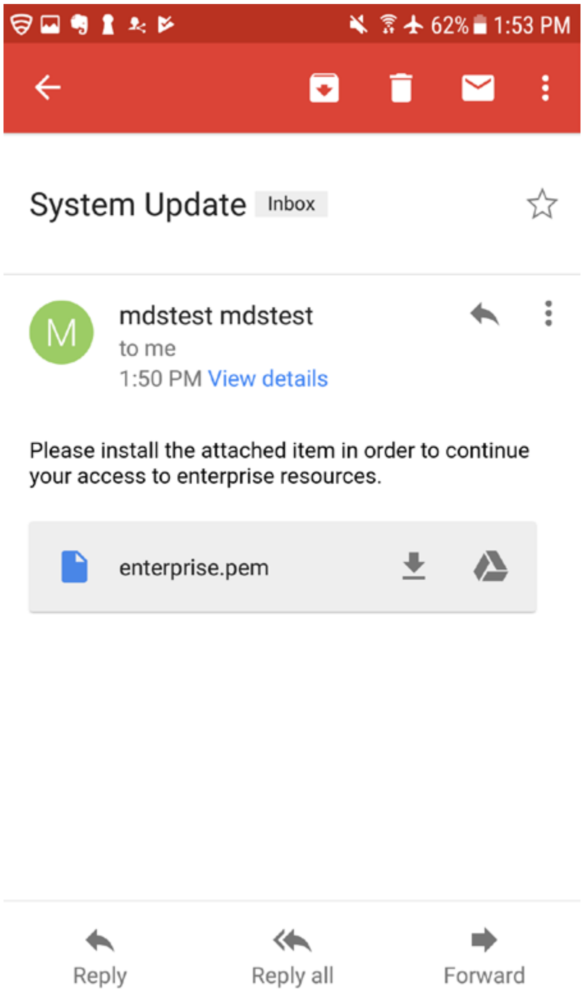
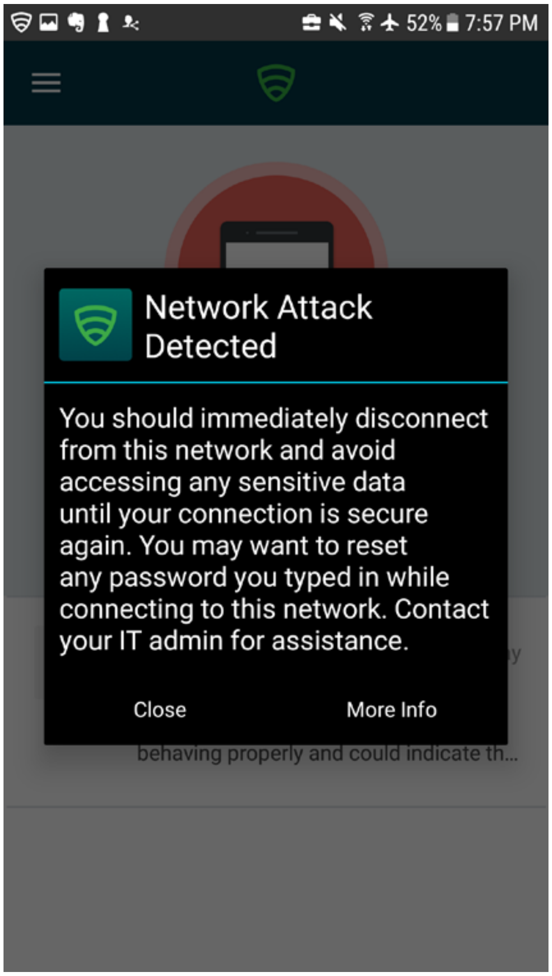


Figure G-19 Reversed Web Page

2400 Man-in-the-middle attack is detected by Lookout as shown in Figure G-20.

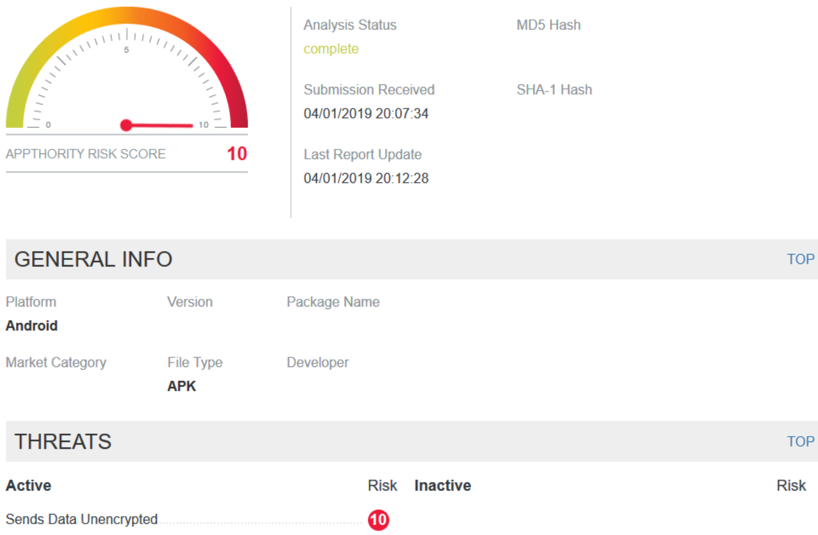
2401 **Figure G-20 Network Attack Detected**



2402 G.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via 2403 Eavesdropping on Unencrypted Device Communications

2404 The following screenshot shows Appthority detecting an application sending data unencrypted.

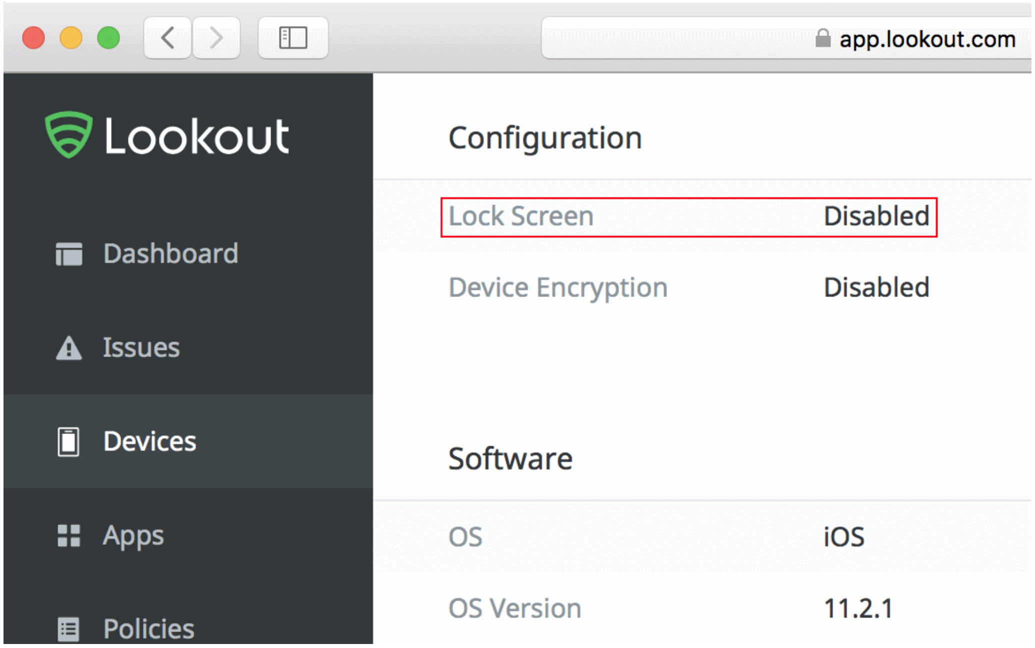
Figure G-21 Unencrypted Data Transfer



G.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code

MobileIron applies a policy to the devices to enforce a mandatory personal identification number and device-wipe capability. Lookout reports devices that have the lock screen disabled.

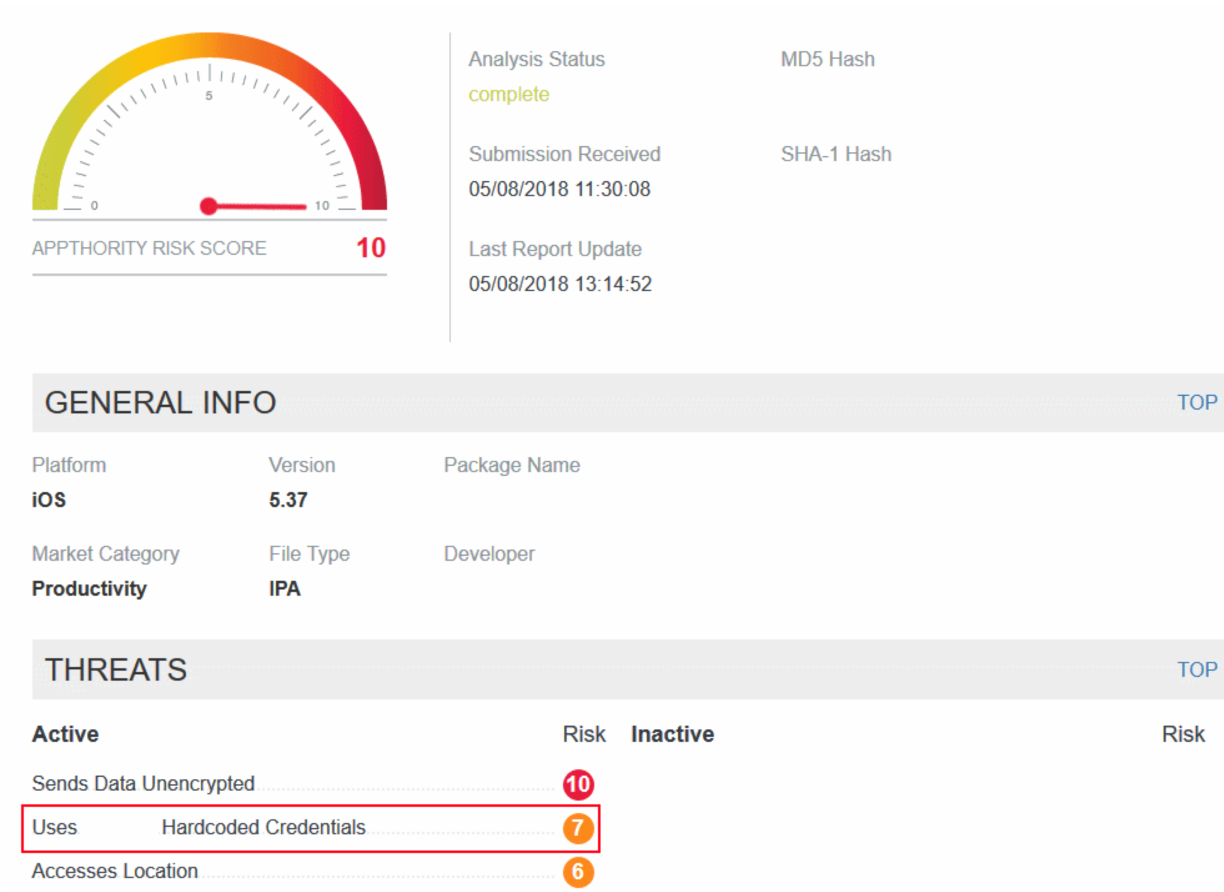
Figure G-22 Lock Screen Disabled Detection Notice



G.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

As shown in Figure G-23, Appthority recognized that an application used hard-coded credentials. The application's use of hard-coded credentials could introduce vulnerabilities if the hard-coded credentials were used for access to enterprise resources by unauthorized entities or for unauthorized actions.

Figure G-23 Hard-Coded Credentials



G.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device

The following two screenshots depict the inability to connect to the GlobalProtect VPN without the proper client certificates, obtainable only through enrolling the device in MobileIron.

Figure G-24 No Certificates Found on Android

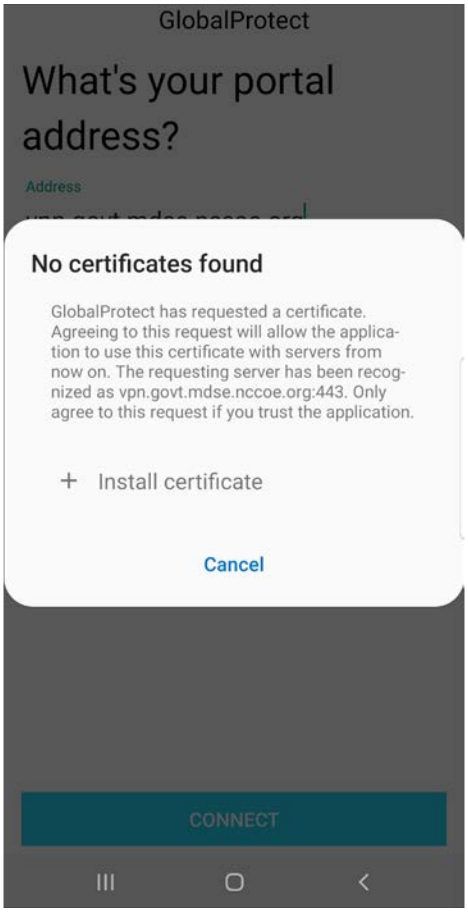
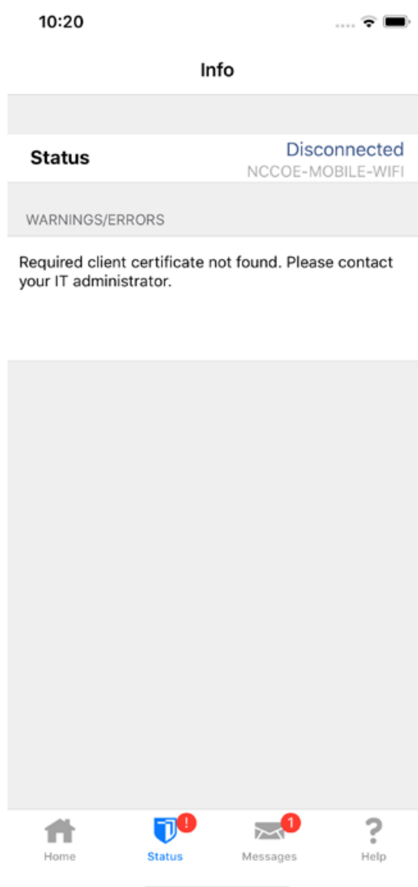


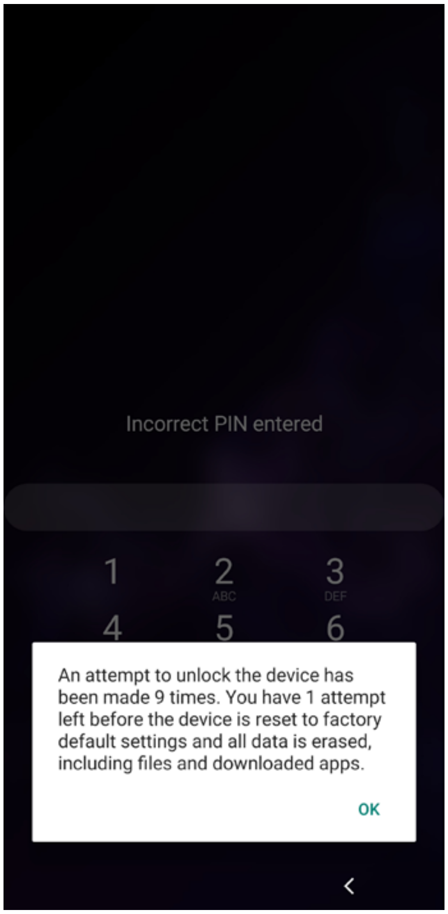
Figure G-25 No Certificates Found on iOS



G.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device

This screenshot depicts the final warning before Android factory-resets the device. In the event the device was stolen, all corporate data would be removed from the device after one more failed unlock attempt, thwarting the malicious actor's goal.

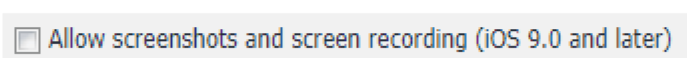
Figure G-26 Android Device Wipe Warning



G.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its Unauthorized Storage in Non-Organizationally Managed Services

The following screenshot shows one of the data loss prevention configuration options in MobileIron for iOS.

Figure G-27 Disallowing Screenshots and Screen Recording



Appendix H Example Security Control Map

Table H-1 lists the technologies used in this project and provides a mapping among the generic application term, the specific product used, the security control(s) the product provides, and a mapping to the relevant National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Work Roles*. From left to right, the columns in the table describe:

- **Specific product used:** vendor product used by the example solution
- **How the component functions in the build:** capability the component provides in the example solution. This is mapped to the general mobile technology component term.
- **Applicable Cybersecurity Framework Subcategories:** applicable Cybersecurity Framework Subcategory(s) that the component is providing in the example solution
- **Applicable NIST controls:** the NIST SP 800-53 Revision 4 controls that the component provided in the example solution
- **ISO/IEC 27001:2013:** International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013 mapping that the component provides in the example solution
- **CIS 6:** Center for Internet Security (CIS) version 6 controls mapping that the component provides in the example solution
- **NIST SP 800-181, *NICE Framework Work Roles:*** NICE Framework work role(s) that could be used to manage this component's use in the example solution. This mapping provides information on the workforce members who would be engaged in this part of the example solution's support.

2455 **Table H-1 Example Solution's Cybersecurity Standards and Best Practices Mapping**

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
Mobile Threat Defense						
Appthority Cloud Service	Mobile Threat Intelligence	ID.RA-1—Asset vulnerabilities are identified and documented.	Security Assessment and Authorization CA-2, CA-7, CA-8 Risk Assessment RA-3, RA-5 System and Services Acquisition SA-5, SA-11 System and Information Integrity SI-2, SI-4, SI-5	A.12.6.1 Control of Technical vulnerabilities A.18.2.3 Technical Compliance Review	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor SP-ARC-002 Security Architect OM-ANA-001 Systems Security Analyst PR-VAM-001 Vulnerability Assessment Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		ID.RA-3 - Threats, both internal and external, are identified and documented.	Risk Assessment RA-3 System and Information Integrity SI-5 Insider Threat Program PM-12, PM-16	Clause 6.1.2 Information Risk Assessment Process	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor PR-CDA-001 Cyber Defense Analyst OV-SPP-001 Cyber Workforce Developer and Manager OV-TEA-001 Cyber Instructional Curriculum Developer AN-TWA-001 Threat/Warning Analyst PR-VAM-001 Vulnerability Assessment Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
						OV-MGT-001 Information Systems Security Manager
		DE.CM-4—Malicious code is detected.	System and Information Integrity SI-3, SI-8	A.12.2.1 Controls Against Malware	CSC 4 Continuous Vulnerability Assessment and Remediation CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses CSC 12 Boundary Defense	PR-VAM-001 Vulnerability Assessment Analyst PR-CIR-001 Cyber Defense Incident Responder PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
		DE.CM-5—Unauthorized mobile code is detected.	Mobile Code SC-18, SC-44 System and Information Integrity SI-4	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on	CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses	PR-CDA-001 Cyber Defense Analyst OM-NET-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				Software Installation		Network Operations Specialist
Kryptowire Cloud Service	Application Vetting	ID.RA-1—Asset vulnerabilities are identified and documented.	Security Assessment and Authorization CA-2, CA-7, CA-8 Risk Assessment RA-3, RA-5 System and Services Acquisition SA-5, SA-11 System and Information Integrity SI-2, SI-4, SI-5	A.12.6.1 Control of Technical vulnerabilities A.18.2.3 Technical Compliance Review	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor SP-ARC-002 Security Architect OM-ANA-001 Systems Security Analyst PR-VAM-001 Vulnerability Assessment Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		ID.RA-3— Threats, both internal and external, are identified and documented.	Risk Assessment RA-3 System and Information Integrity SI-5 Insider Threat Program PM-12, PM-16	Clause 6.1.2 Information Risk Assessment Process	CSC 4 Continuous Vulnerability Assessment and Remediation	SP-RSK-002 Security Control Assessor OM-ANA-001 Systems Security Analyst OV-SPP-001 Cyber Workforce Developer and Manager OV-TEA-001 Cyber Instructional Curriculum Developer

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
						AN-TWA-001 Threat/Warning Analyst PR-VAM-001 Vulnerability Assessment Analyst PR-CDA-001 Cyber Defense Analyst OV-MGT-001 Information Systems Security Manager
		DE.CM-4—Malicious code is detected.	System and Information Integrity SI-3, SI-8	A.12.2.1 Controls Against Malware	CSC 4 Continuous Vulnerability Assessment and Remediation CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses CSC 12 Boundary Defense	PR-CIR-001 Cyber Defense Incident Responder PR-CDA-001 Cyber Defense Analyst PR-VAM-001 Vulnerability Assessment Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
						OM-NET-001 Network Operations Specialist
		DE.CM-5—Unauthorized mobile code is detected.	Mobile Code SC-18, SC-44 System and Information Integrity SI-4	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation	CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses	PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
Lookout Cloud Service/ Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android)	Mobile Threat Defense/Endpoint Security	PR.AC-5—Network integrity is protected (e.g., network segregation, network segmentation).	Access Control AC-4, AC-10 System and Communications Protection SC-7	A.13.1.1 Network Controls A.13.1.3 Segregation in Networks A.13.2.1 Information Transfer Policies and Procedures A.14.1.2 Securing	CSC 9 Imitation and Control of Network Ports, Protocols, and Services CSC 14 Controlled Access Based on the Need to Know CSC 15 Wireless Access Control	OM-ADM-001 System Administrator OV-SPP-002 Cyber Policy and Strategy Planner PR-CDA-001 Cyber Defense Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions	CSC 18 Application Software Security	OM-NET-001 Network Operations Specialist
		PR.PT-4—Communications and control networks are protected.	Access Control AC-4, AC-17, AC-18 Contingency Planning Policy and Procedures CP-8 System and Communications Protection SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	A.13.1.1 Network Controls A.13.1.3 Segregation in Networks A.14.1.3 Protecting Application Services Transactions	CSC 8 Malware Defenses CSC 12 Boundary Defense CSC 15 Wireless Access Control	OM-ADM-001 System Administrator OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager SP-ARC-0001 Enterprise Architect

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
						PR-CDA-001 Cyber Defense Analyst SP-ARC-002 Security Architect OM-NET-001 Network Operations Specialist
		DE.CM-5— Unauthorized mobile code is detected.	Mobile Code SC-18, SC-44 System and Information Integrity SI-4	A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation	CSC 7 Email and Web Browser Protections CSC 8 Malware Defenses	PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist
Enterprise Mobility Management						
MobileIron Core Version 9.7.0.1	Enterprise Mobility Management	ID.AM-1— Physical devices and systems within the organization are inventoried.	Information System Component Inventory CM-8	A.8.1.1 Inventory of Assets	CSC 1 Inventory of Authorized and Unauthorized Devices	OM-STS-001 Technical Support Specialist OM-ADM-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
			Information System Inventory PM-5	A.8.1.2 Ownership of Assets		System Administrator
		PR.AC-1—Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	Access Control AC-1, AC-2 Identification and Authentication IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	A.9.2.1 User Registration and De-Registration A.9.2.2 User Access Provisioning A.9.2.3 Management of Privileged Access Rights A.9.2.4 Management of Secret Authentication Information of Users A.9.2.6 Removal or Adjustment of Access Rights A.9.3.1 Use of Secret Authentication Information	CSC 1 Inventory of Authorized and Unauthorized Devices CSC 5 Controlled Use of Administrative Privileges CSC 15 Wireless Access Control CSC 16 Account Monitoring and Control	OV-SPP-002 Cyber Policy and Strategy Planner OM-ADM-001 System Administrator OV-MGT-002 Communications Security (COMSEC) Manager OM-STS-001 Technical Support Specialist OM-ANA-001 Systems Security Analyst PR-CDA-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				A.9.4.2 Secure Log-On Procedures A.9.4.3 Password Management System		Cyber Defense Analyst
		PR.AC-6—Identities are proofed and bound to credentials and asserted in interactions.	Access Control AC-1, AC-2, AC-3, AC-16, AC-19, AC-24 Identification and Authentication IA-1, IA-2, IA-4, IA-5, IA-8 Physical and Environmental Protection PE-2	A.7.1.1 Screening A.9.2.1 User Registration and De-Registration	CSC 16 Account Monitoring and Control	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OM-ADM-001

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
			Personnel Security PS-3			System Administrator
		PR.IP-1—A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	Information System Component Inventory CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9 System and Services Acquisition SA-10	A.12.1.2 Change Management A.12.5.1 Installation of Software on Operational Systems A.12.6.2 Restrictions on Software Installation A.14.2.2 System Change Control Procedures A.14.2.3 Technical Review of Applications After Operating	CSC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers CSC 9 Limitation and Control of Network Ports, Protocols, and Services CSC 11 Secure Configurations for Network Devices Such as Firewalls, Routers, and Switches	SP-ARC-002 Security Architect OV-SPP-002 Cyber Policy and Strategy Planner SP-SYS-001 Information Systems Security Developer OM-ADM-001 System Administrator PR-VAM-001 Vulnerability Assessment Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				Platform Changes A.14.2.4 Restrictions on Changes to Software Packages		OM-NET-001 Network Operations Specialist OV-MGT-001 Information Systems Security Manager OM-STS-001 Technical Support Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
MobileIron Agent Version 11.0.1A (iOS), 10.2.1.1.3R (Android)	EMM/Endpoint Agent	PR.DS-6—Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	System and Communications Protection SC-1 System and Information Integrity SI-7	A.12.2.1 Controls Against Malware A.12.5.1 Installation of Software on Operational Systems A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions A.14.2.4 Restrictions on Changes to Software Packages	CSC 2 Inventory of Authorized and Unauthorized Software CSC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	OV-SPP-002 Cyber Policy and Strategy Planner SP-ARC-0001 Enterprise Architect OV-MGT-001 Information Systems Security Manager OM-ADM-001 System Administrator OM-STS-001 Technical Support Specialist
Trusted Execution Environment						

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
Qualcomm (Version is mobile device dependent)	Trusted Execution Environment	PR.DS-1— Data at rest is protected.	Media Downgrading MP-8 System and Communications Protection SC-12, SC-28	A.8.2.3 Handling of Assets	CSC 13 Data Protection CSC 14 Controlled Access Based on the Need to Know	OV-SPP-002 Cyber Policy and Strategy Planner PR-INF-001 Cyber Defense Infrastructure Support Specialist OV-LGA-002 Privacy Officer/Privacy Compliance Manager OV-MGT-002 COMSEC Manager OM-NET-001 Network Operations Specialist OM-ANA-001 Systems Security Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.DS-6—Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	System and Communications Protection SC-16 System and Information Integrity SI-7	A.12.2.1 Controls Against Malware A.12.5.1 Installation of Software on Operational Systems A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions A.14.2.4 Restrictions on Changes to Software Packages	CSC 2 Inventory of Authorized and Unauthorized Software CSC 3 Secure Configurations for Hardware and Software on Mobile	OV-SPP-002 Cyber Policy and Strategy Planner PR-CDA-001 Cyber Defense Analyst SP-ARC-0001 Enterprise Architect OV-MGT-001 Information Systems Security Manager OM-STS-001 Technical Support Specialist OM-ADM-001 System Administrator

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.DS-8—Integrity-checking mechanisms are used to verify hardware integrity.	Developer Configuration Management SA-10 System and Information Integrity SI-7	A.11.2.4 Equipment Maintenance	Not applicable	OM-ADM-001 System Administrator SP-ARC-0001 Enterprise Architect
		DE.CM-4—Malicious code is detected.	System and Information Integrity SI-3, SI-8	A.12.2.1 Controls Against Malware	CSC 5 Controlled Use of Administrative Privileges CSC 7 Email and Web Browser Protections CSC 14 Controlled Access Based on the Need to Know CSC 16 Account Monitoring and Control	PR-CDA-001 Cyber Defense Analyst PR-INF-001 Cyber Defense Infrastructure Support Specialist PR-VAM-001 Vulnerability Assessment Analyst OM-NET-001 Network Operations Specialist PR-CDA-001 Cyber Defense Analyst

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
Virtual Private Network						
Palo Alto, PA-220 Version 8.1.1	Virtual Private Network	PR.AC-3—Remote access is managed.	Access Control AC-1, AC-17, AC-19, AC-20 System and Communications Protection SC-15	A.6.2.1 Mobile Device Policy A.6.2.2 Teleworking A.11.2.6 Security of Equipment and Assets Off-Premises A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies and Procedures	CSC 12 Boundary Defense	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OM-NET-001 Network Operations Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.AC-5—Network integrity is protected (e.g., network segregation, network segmentation).	Access Control AC-4, AC-10 System and Communications Protection SC-7	A.13.1.1 Network Controls A.13.1.3 Segregation in Networks A.13.2.1 Information Transfer Policies and Procedures A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions	CSC 9 Limitation and Control of Network Ports, Protocols, and Services CSC 14 Controlled Access Based on the Need to Know CSC 15 Wireless Access Control CSC 18 Application Software Security	PR-CDA-001 Cyber Defense Analyst OM-ADM-001 System Administrator OM-NET-001 Network Operations Specialist

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
		PR.AC-6—Identities are proofed and bound to credentials and asserted in interactions.	Access Control AC-1, AC-2, AC-3, AC-16, AC-19, AC-24 Identification and Authentication IA-1, IA-2, IA-4, IA-5, IA-8 Physical and Environmental Protection PE-2, PS-3	A.7.1.1 Screening A.9.2.1 User Registration and De-Registration	CSC 16 Account Monitoring and Control	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OM-ADM-001 System Administrator
		PR.DS-2— Data in transit is protected.	System and Communications Protection SC-8, SC-11, SC-12	A.8.2.3 Handling of Assets A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies and Procedures A.13.2.3 Electronic Messaging	CSC 13 Data Protection CSC 14 Controlled Access Based on the Need to Know	OV-SPP-002 Cyber Policy and Strategy Planner OV-MGT-002 Communications Security (COMSEC) Manager OV-LGA-002 Privacy Officer/Privacy Compliance Manager

Specific product used	How the component functions in the build	Applicable Cybersecurity Framework Version 1.1 Subcategories	Applicable NIST SP 800-53 Revision 4 Controls	ISO/IEC 27001:2013	CIS 6	NIST SP 800-181 NICE Framework Work Roles
				A.14.1.2 Securing Application Services on Public Networks A.14.1.3 Protecting Application Services Transactions		OM-NET-001 Network Operations Specialist
		PR.PT-4—Communications and control networks are protected.	Access Control AC-4, AC-17, AC-18 Contingency Planning CP-8 System and Communications Protection SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies and Procedures A.14.1.3 Protecting Application Services Transactions	CSC 8 Malware Defenses CSC 12 Boundary Defense CSC 15 Wireless Access Control	PR-INF-001 Cyber Defense Infrastructure Support Specialist OV-SPP-002 Cyber Policy and Strategy Planner PR-CDA-001 Cyber Defense Analyst OM-NET-001 Network Operations Specialist

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

NCCOE
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.

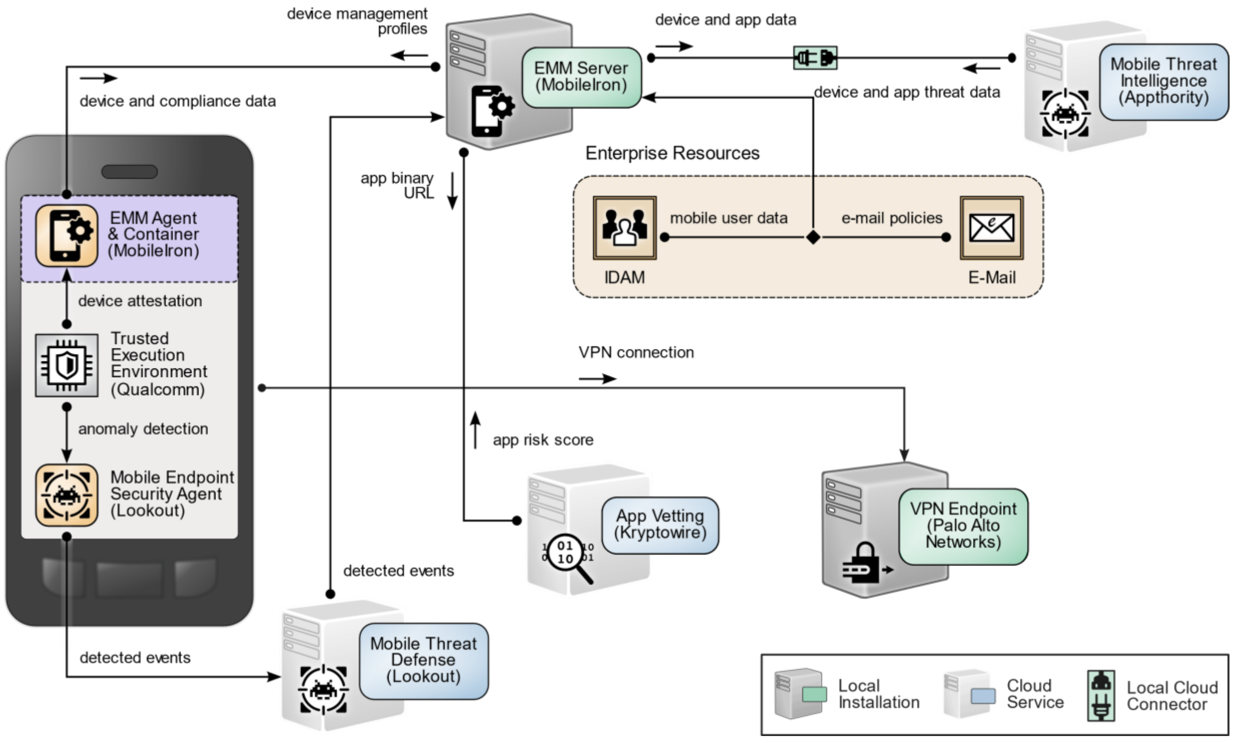
Table 1-1 Typographic Conventions

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



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.

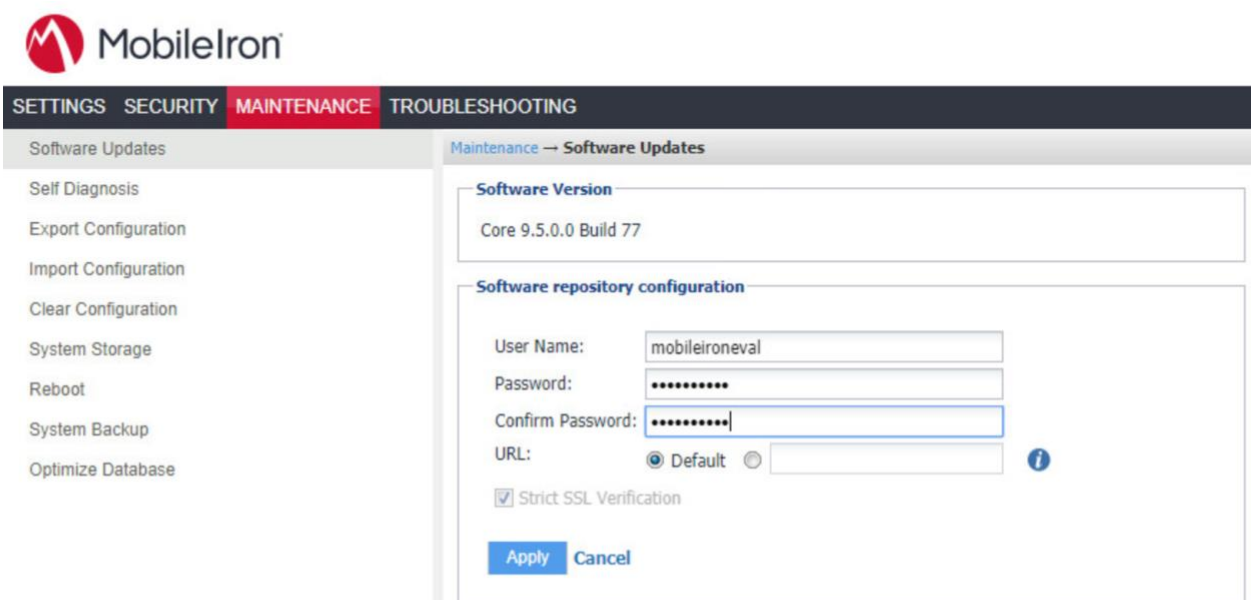
1. Obtain a copy of *MobileIron Core Device Management Guide for iOS Devices* from the MobileIron support portal.
2. Complete all instructions provided in Chapter 1, Setup Tasks.

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.**

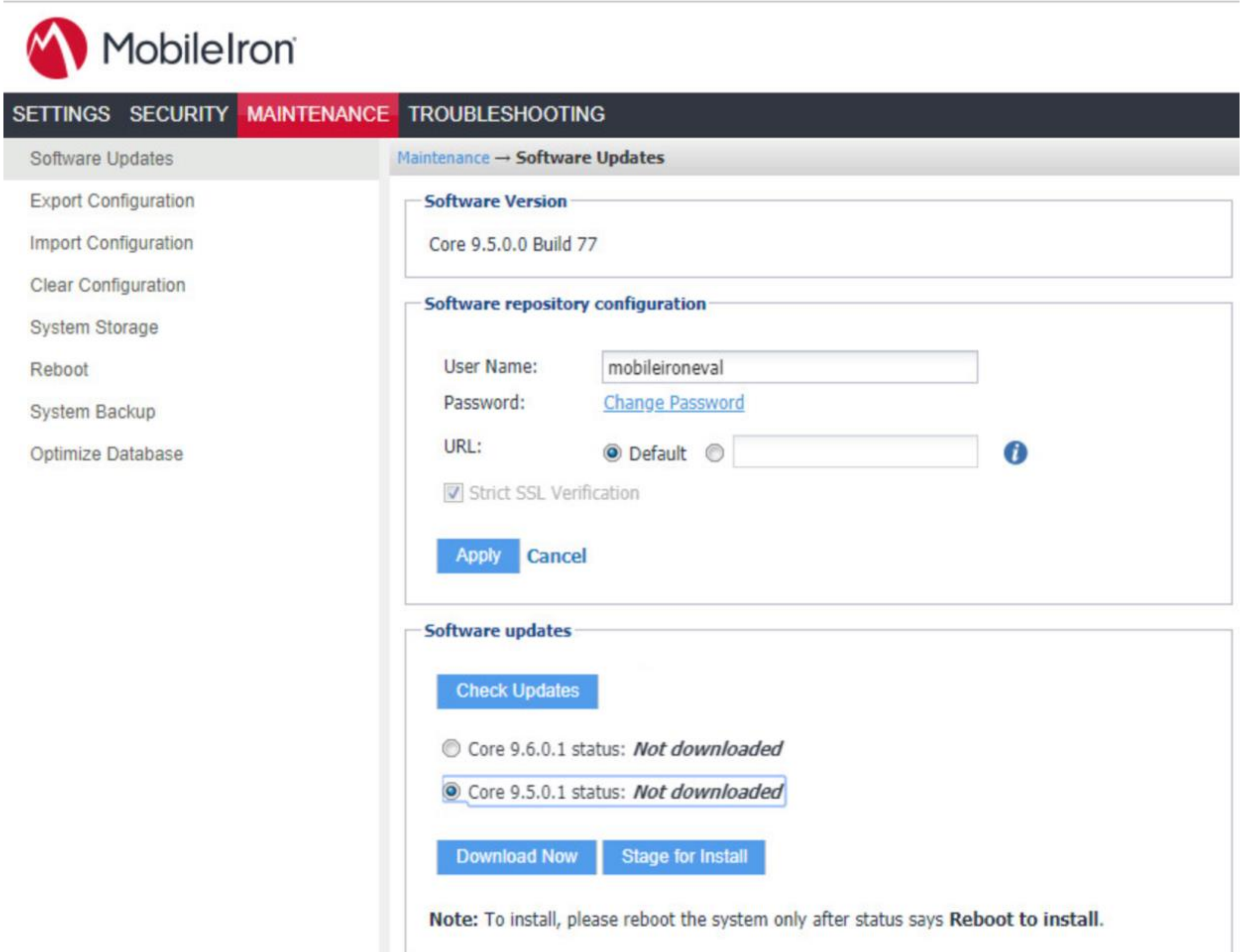
Figure 2-1 MobileIron Repository Configuration



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.**

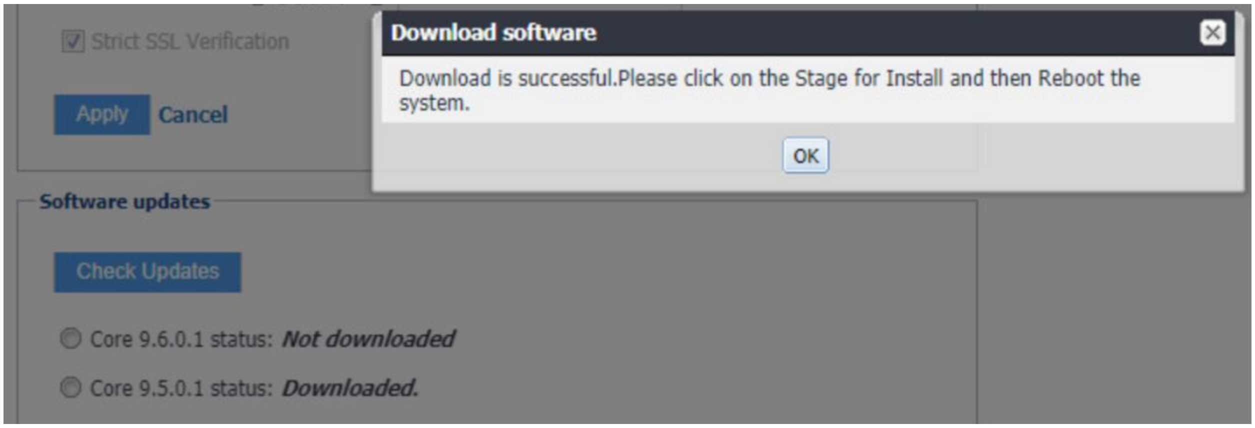
c. Select **Download Now.** After a delay, the Software Download dialogue will appear.

Figure 2-2 MobileIron Core Version



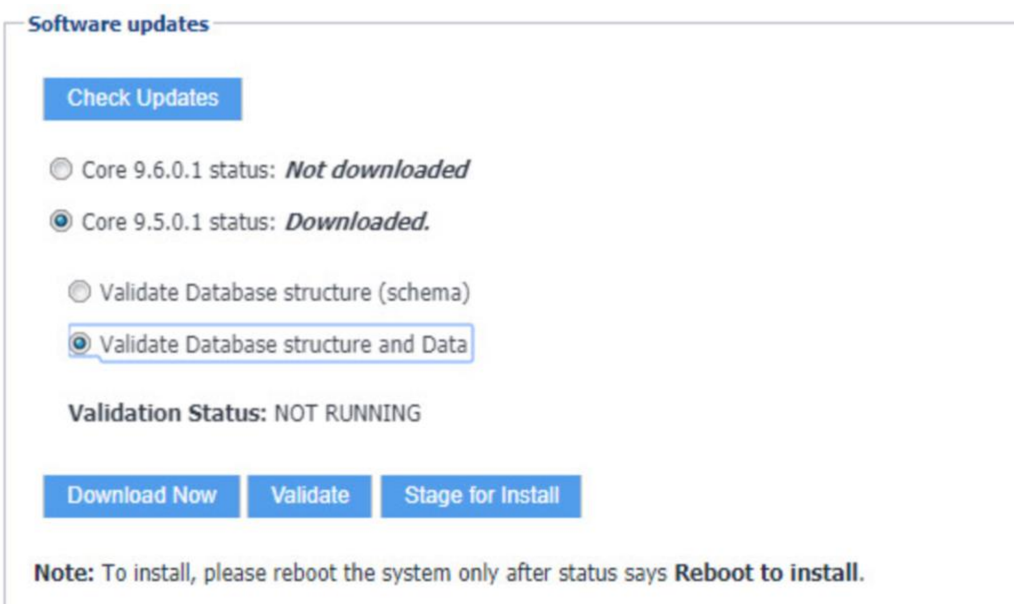
5. In the **Download Software** dialogue, select **OK.**

Figure 2-3 MobileIron Download Status



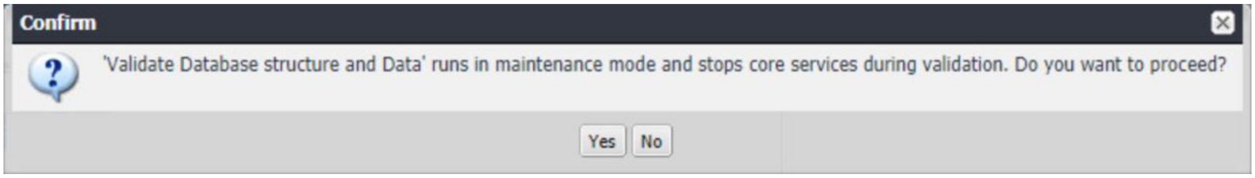
6. In the **Software updates** section:
    a. Select the **Core 9.5.0.1 status: Downloaded** option.
    b. Select the **Validate Database Structure and Data** option.
    c. Select **Validate.**

Figure 2-4 Validating Database Data



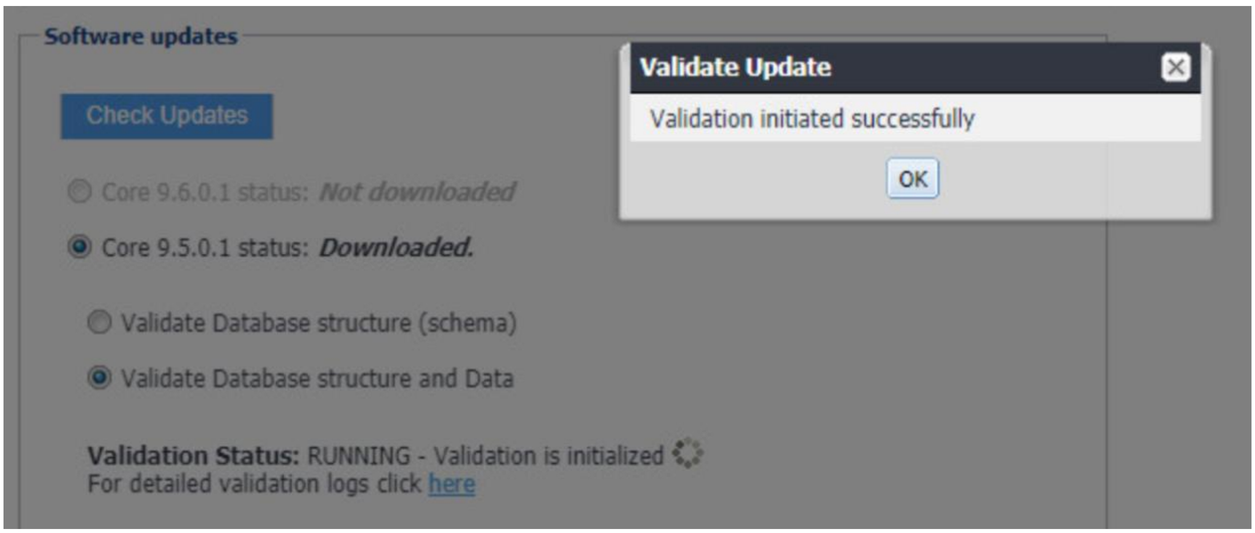
7. In the **Confirm** dialogue, select **Yes** to validate database structure and data.

Figure 2-5 Validating Database Data Confirmation



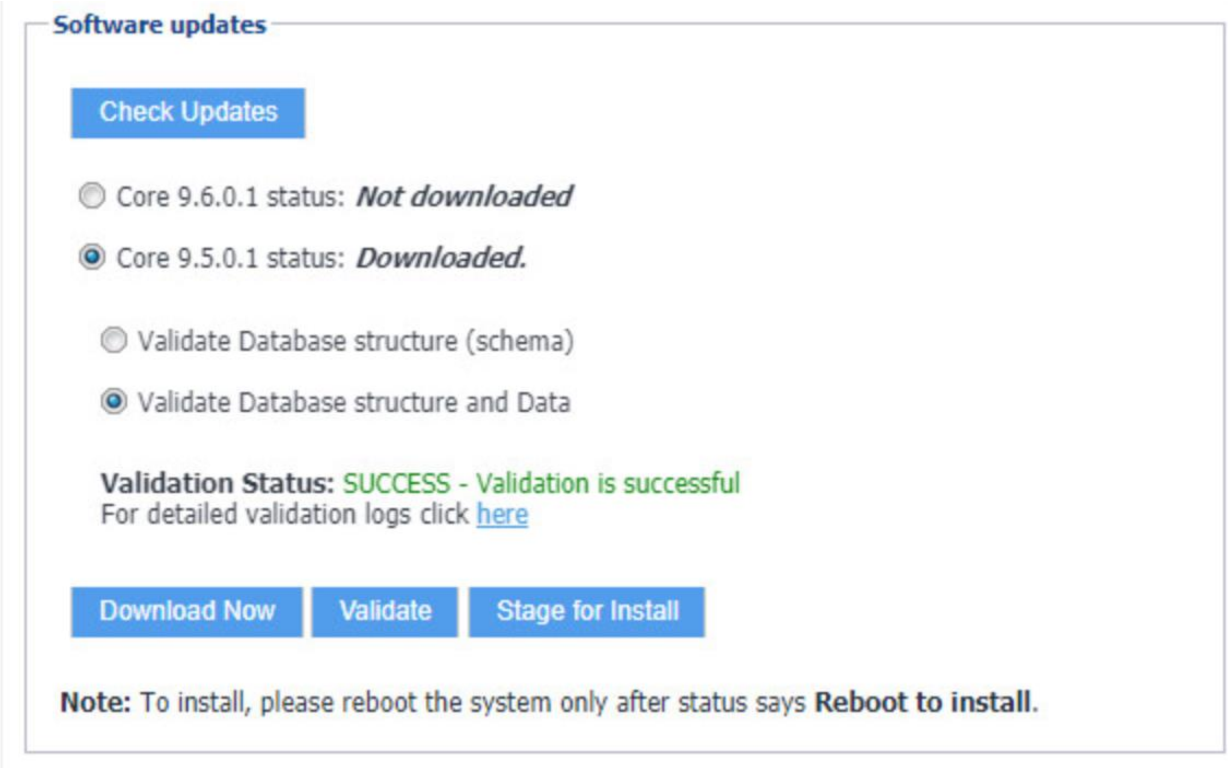
8. In the **Validate Update** dialogue, select **OK.**

Figure 2-6 Database Data Validation Initiation Confirmation



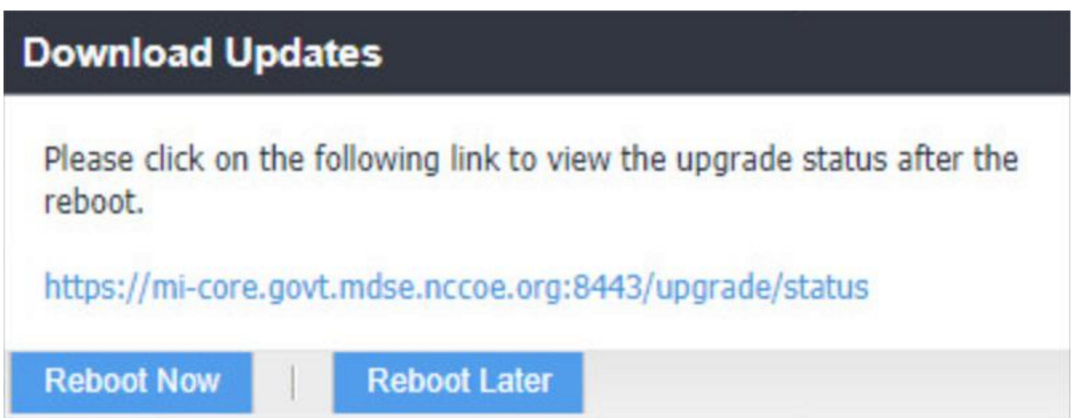
9. In the **Software updates** section, select **Stage for Install;** the **Download Updates** dialogue will appear.

Figure 2-7 Database Data Validation Status



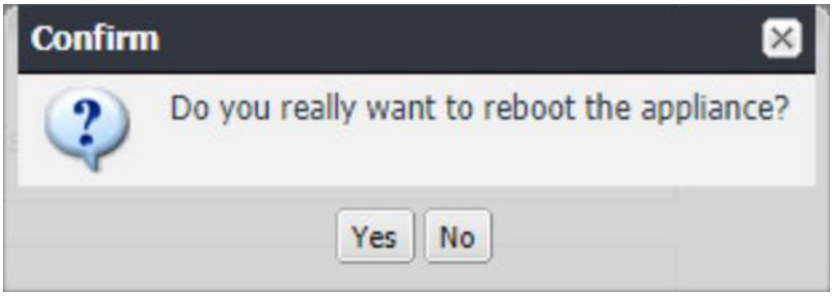
10. In the **Download Updates** dialogue, select **Reboot Now;** a series of dialogues will appear.

Figure 2-8 Software Updates Reboot Prompt



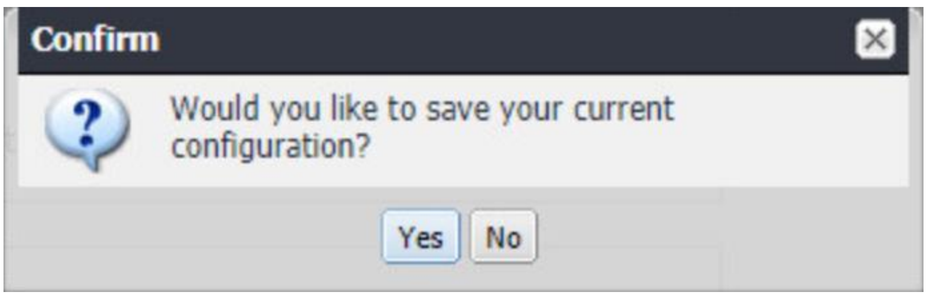
11. In the **Confirm** dialogues:
    a. Select **Yes** to confirm reboot of the appliance.

Figure 2-9 Software Update Reboot Confirmation



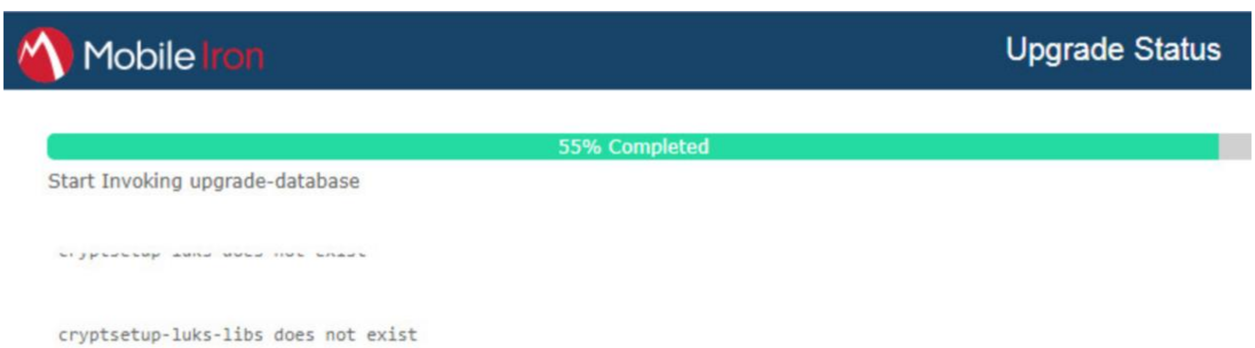
b. Select **Yes** to confirm saving the current configuration.

Figure 2-10 Reboot Configuration Save Prompt



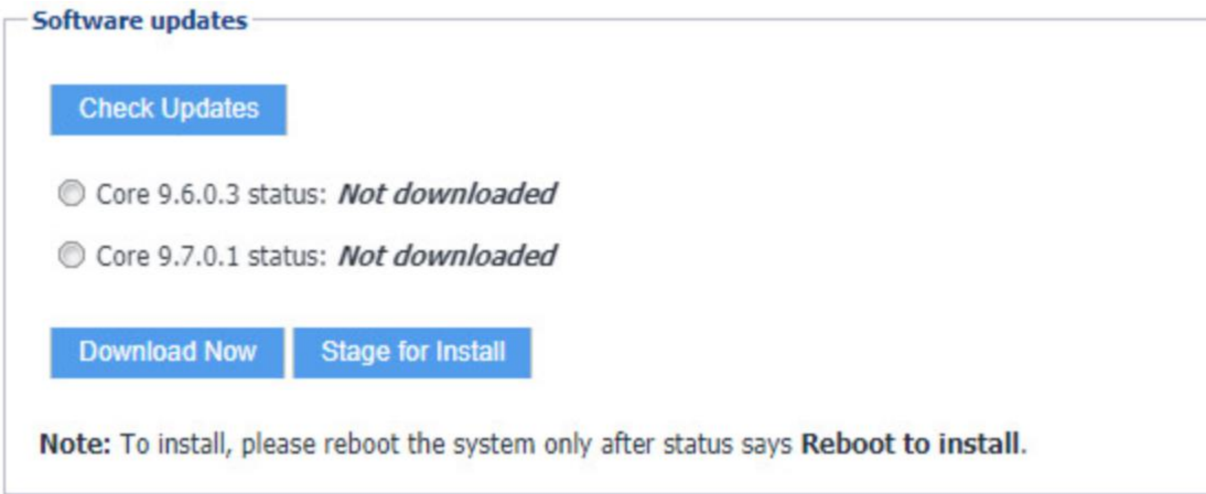
12. The Upgrade Status website hosted by Core will automatically open.

Figure 2-11 Upgrade Status



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



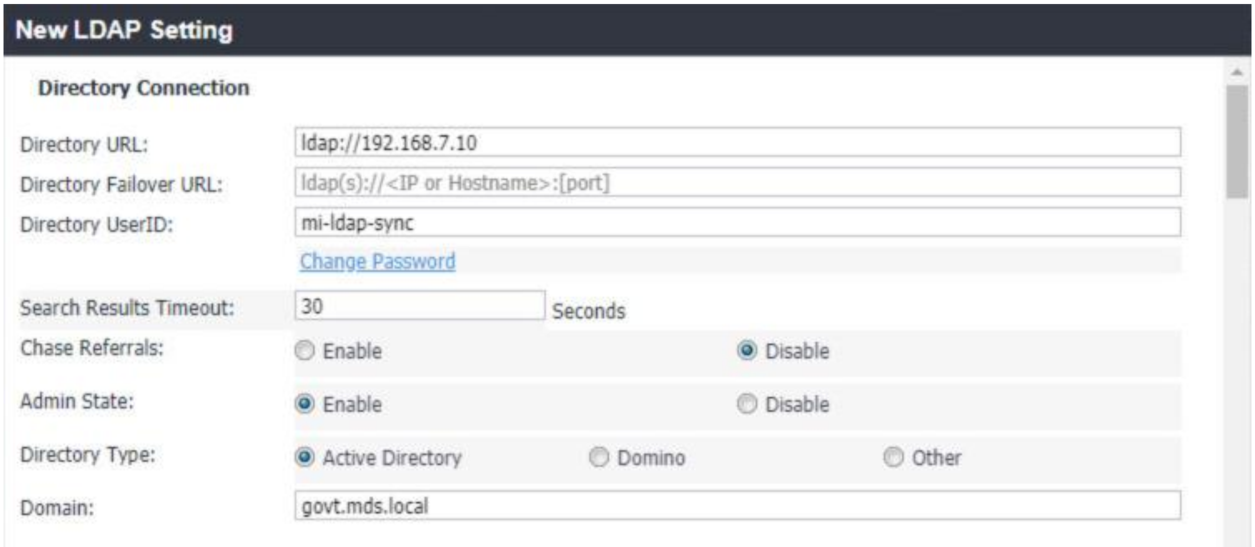
14. Repeat **Steps 4b** through **11** above, replacing 9.5.0.1 with **9.7.0.1** during **Steps 4b** and **6;** this will complete the upgrade path from MobileIron Core 9.5.0.0 to 9.7.0.1.

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:

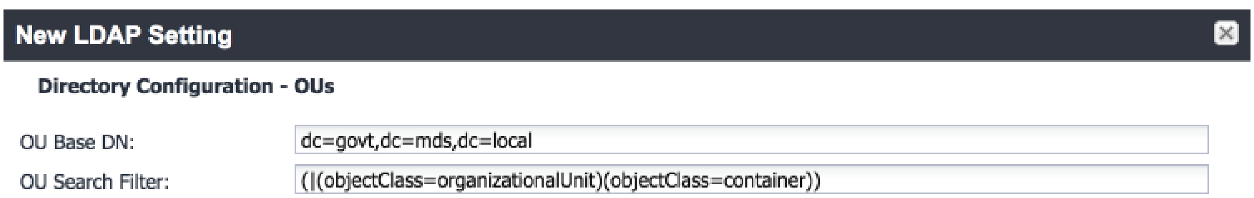
1. From Step 4 in the MobileIron guide, in the **New LDAP Server** dialogue:
   a. Directory Connection:

Figure 2-13 LDAP Settings



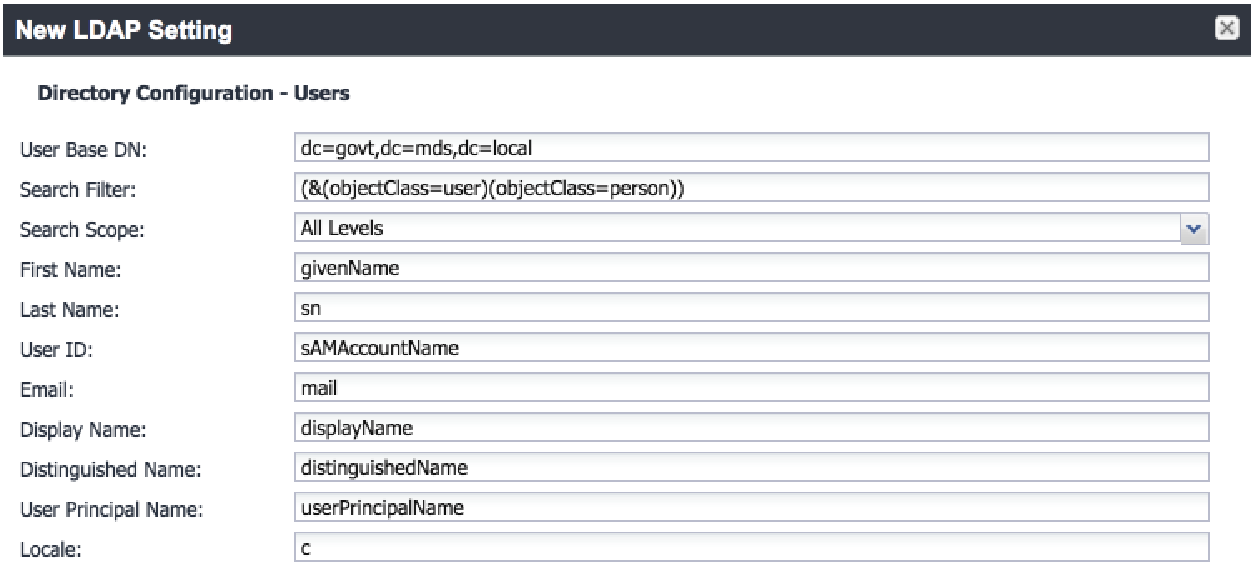
b. Directory Configuration—OUs:

Figure 2-14 LDAP OUs



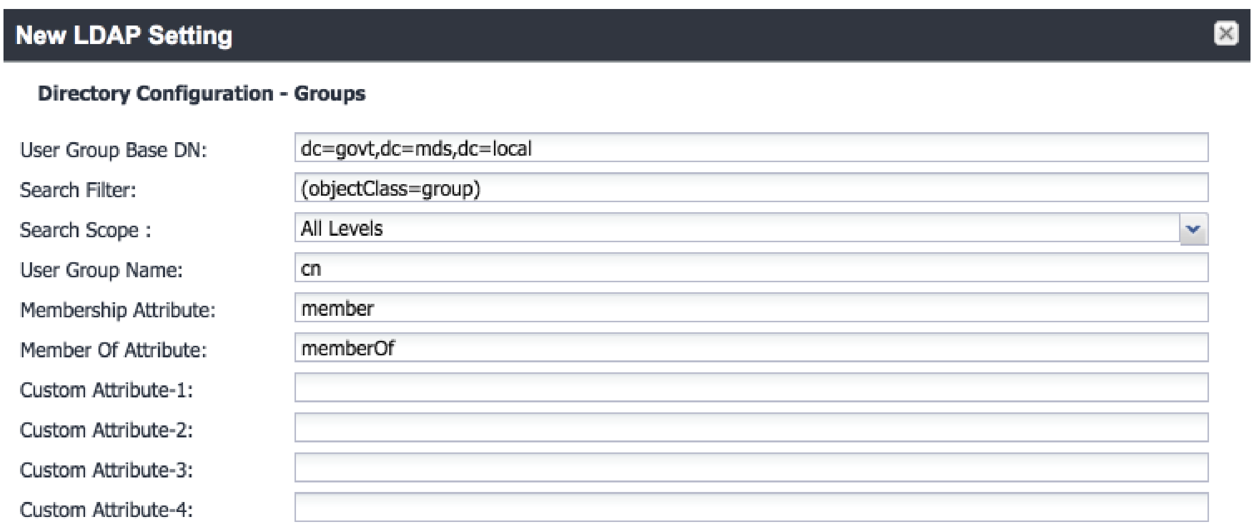
c. Directory Configuration—Users:

Figure 2-15 LDAP User Configuration



d. Directory Configuration—Groups:

Figure 2-16 LDAP Group Configuration



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.

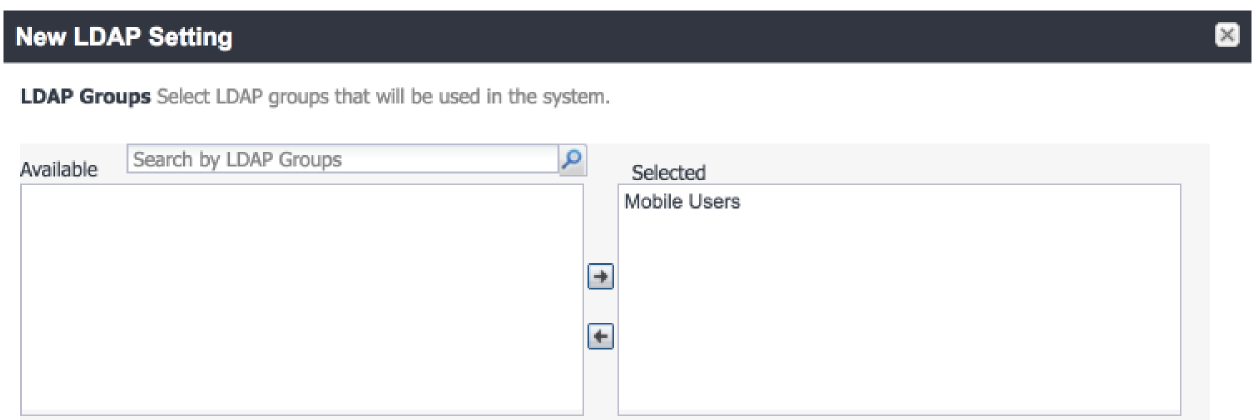
      2) Select the **right-arrow** button; the Mobile Users list item should move to the **Selected** list box.

   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.

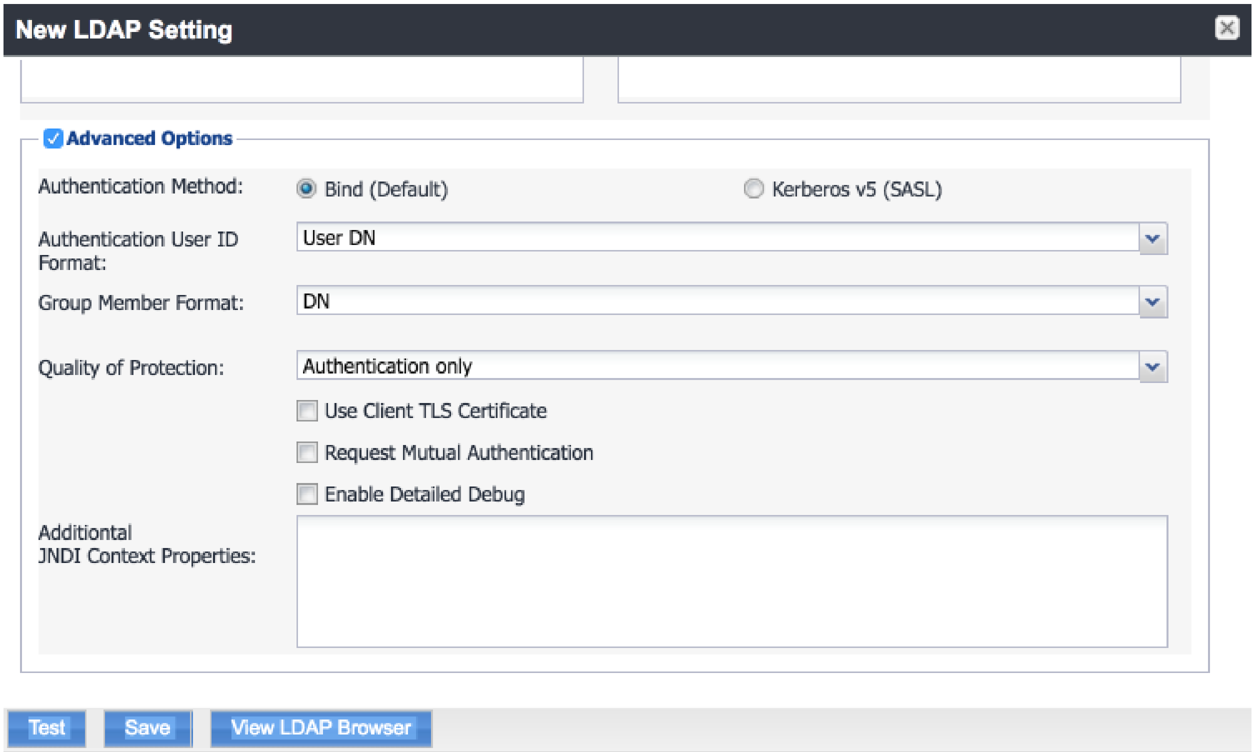
Figure 2-17 Selected LDAP Group



f. Custom Settings: Custom settings were not specified.

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

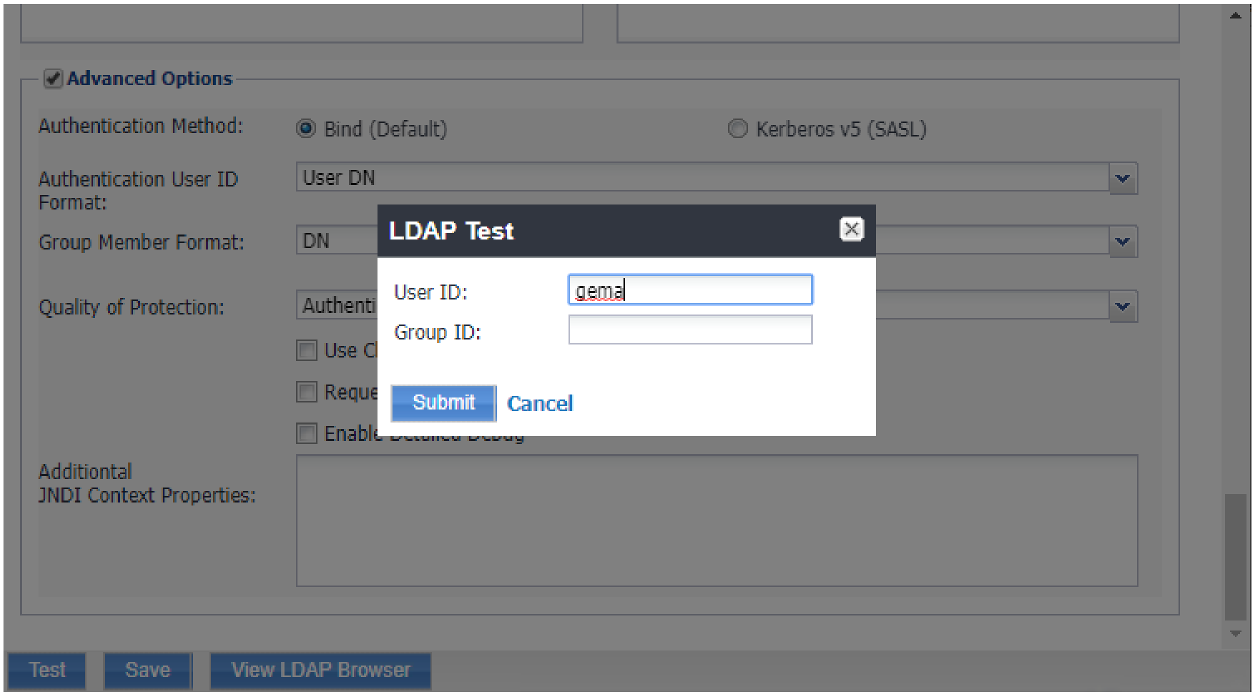
Figure 2-18 LDAP Advanced Options



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.

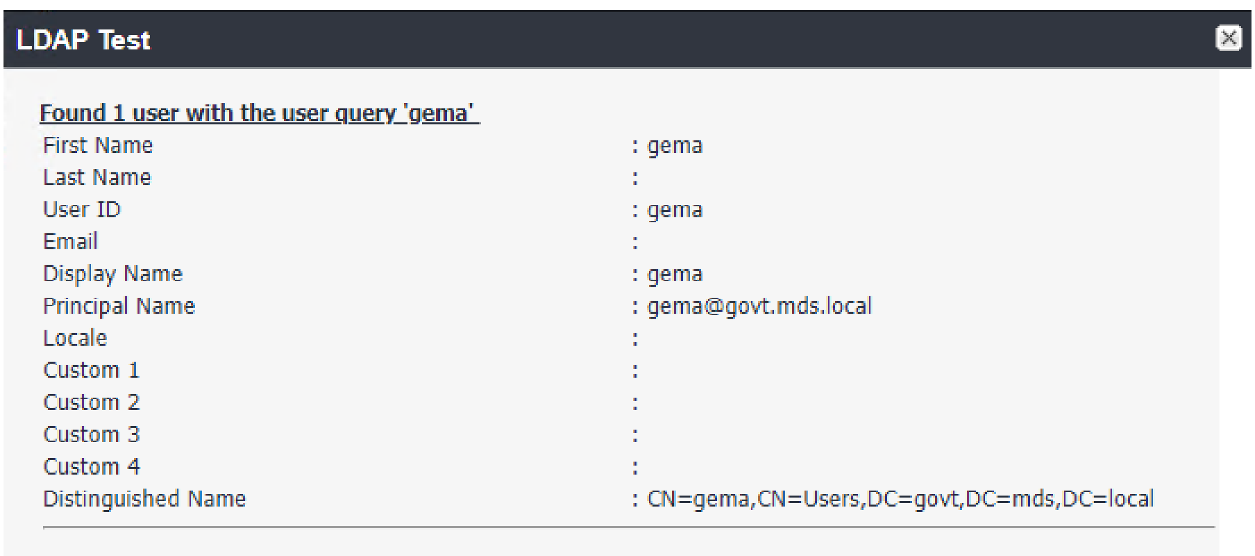
2. From **Steps 19** through **21** from the MobileIron guide, we tested that MobileIron can successfully query LDAP for Derived Personal Identity Verification Credential (DPC) Users.
    a. In the **New LDAP Setting** dialogue, click the **Test** button to open the **LDAP Test** dialogue.
    b. In 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



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

Figure 2-20 LDAP Test Result

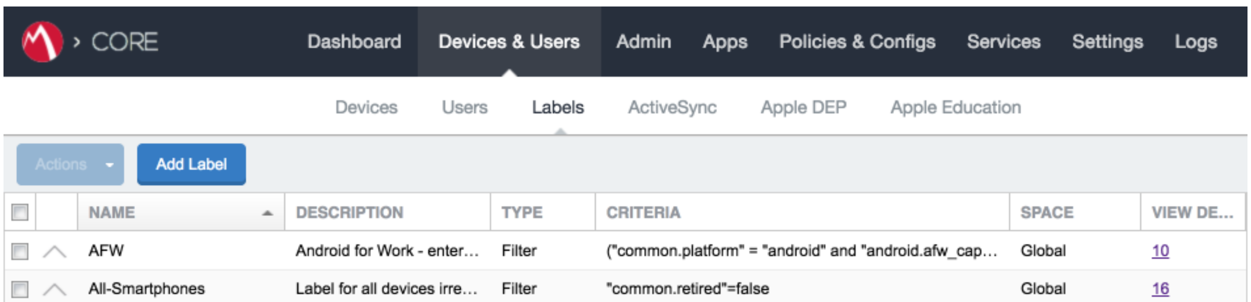


2.4.5 Create a Mobile Users Label

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.

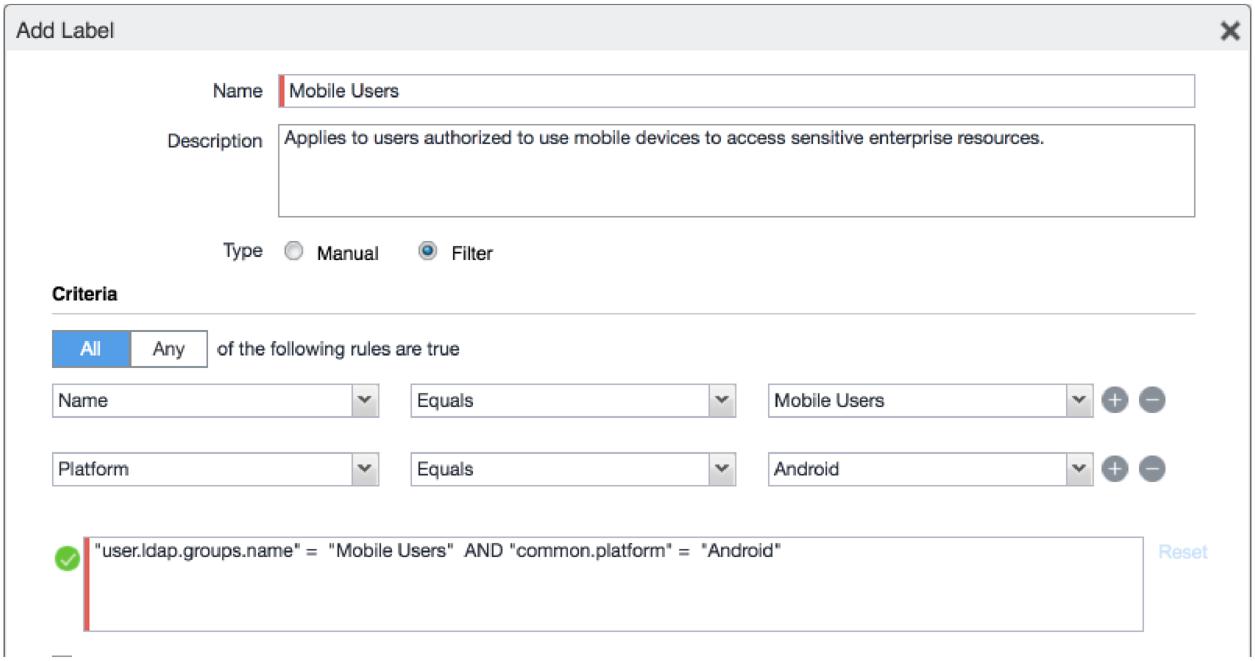
1. In the **MobileIron Core Admin Portal,** navigate to **Devices & Users > Labels.**
2. Select **Add Label.**

Figure 2-21 MobileIron Device Labels



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.**

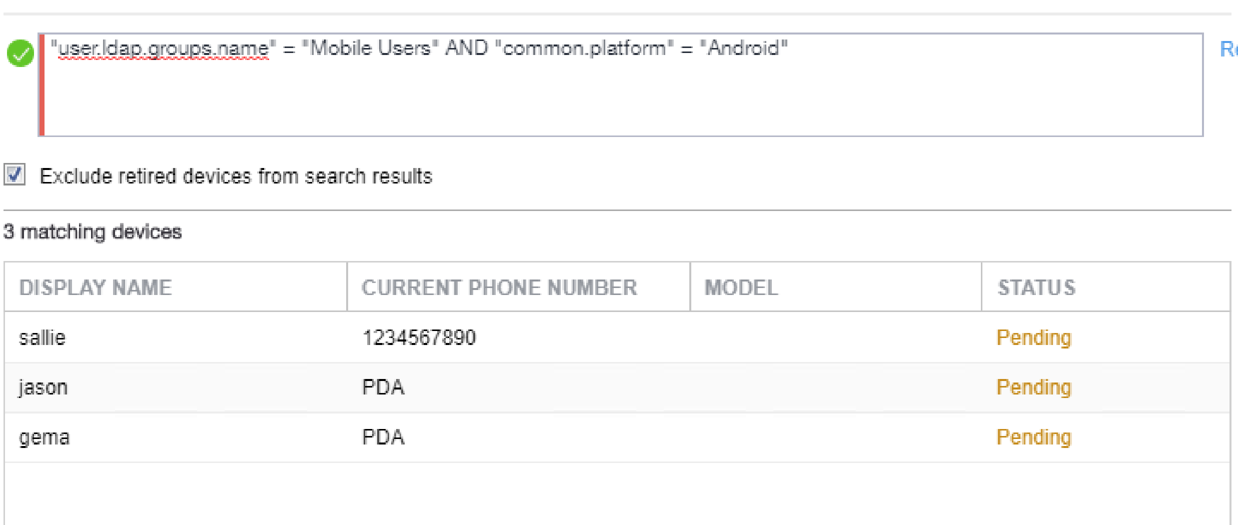
Figure 2-22 Adding a Device Label



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

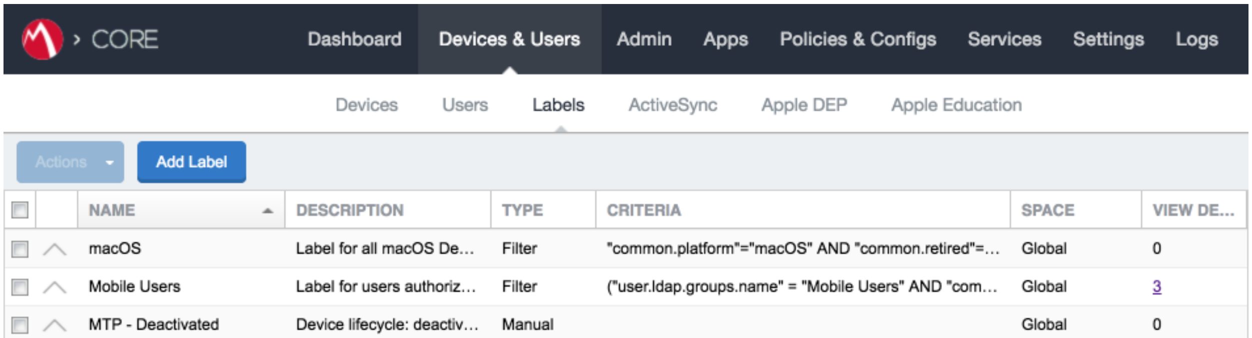
e. Select **Save.**

Figure 2-23 Device Label Matches



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

Figure 2-24 MobileIron Label List



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.

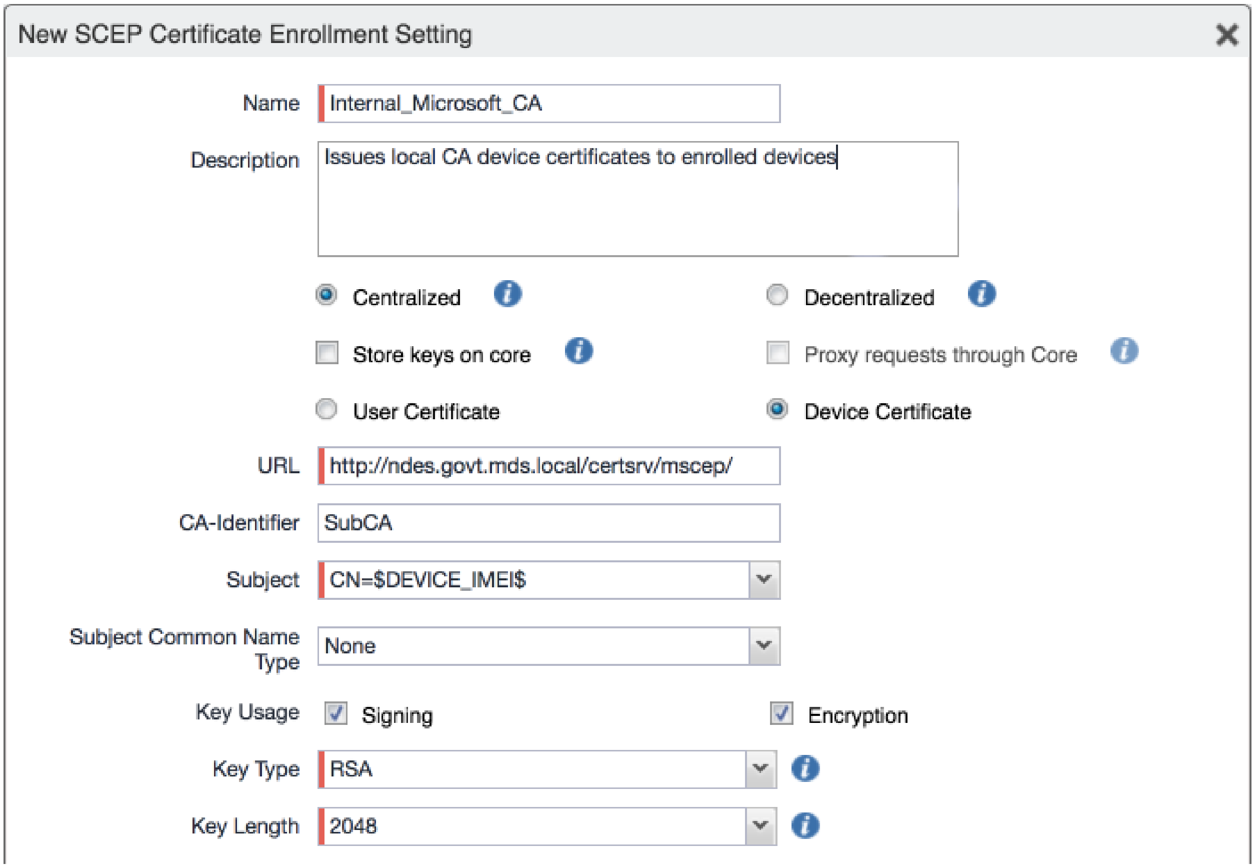
2.5.1 MobileIron Configuration

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



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:

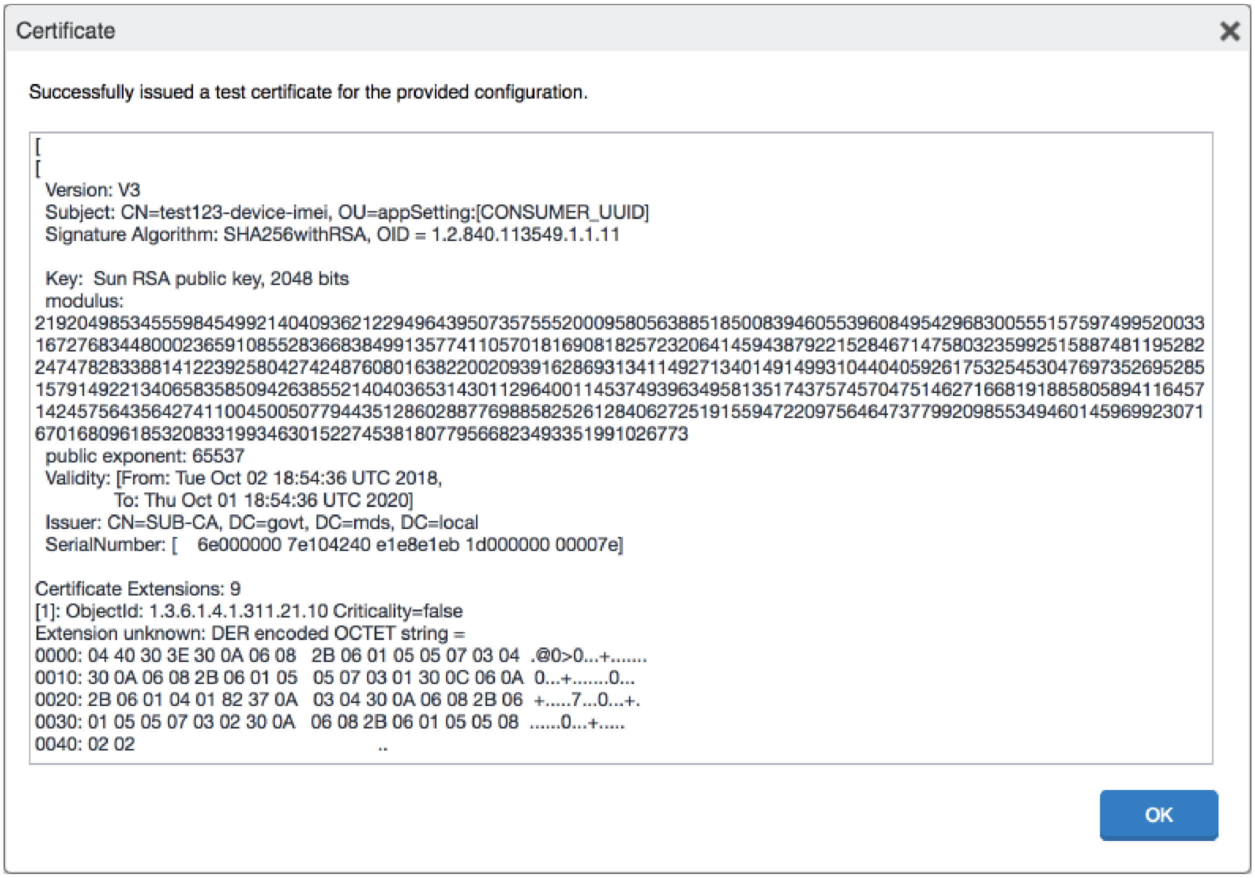
   i. For the **Type** drop-down menu, select **NT Principal Name.**

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

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

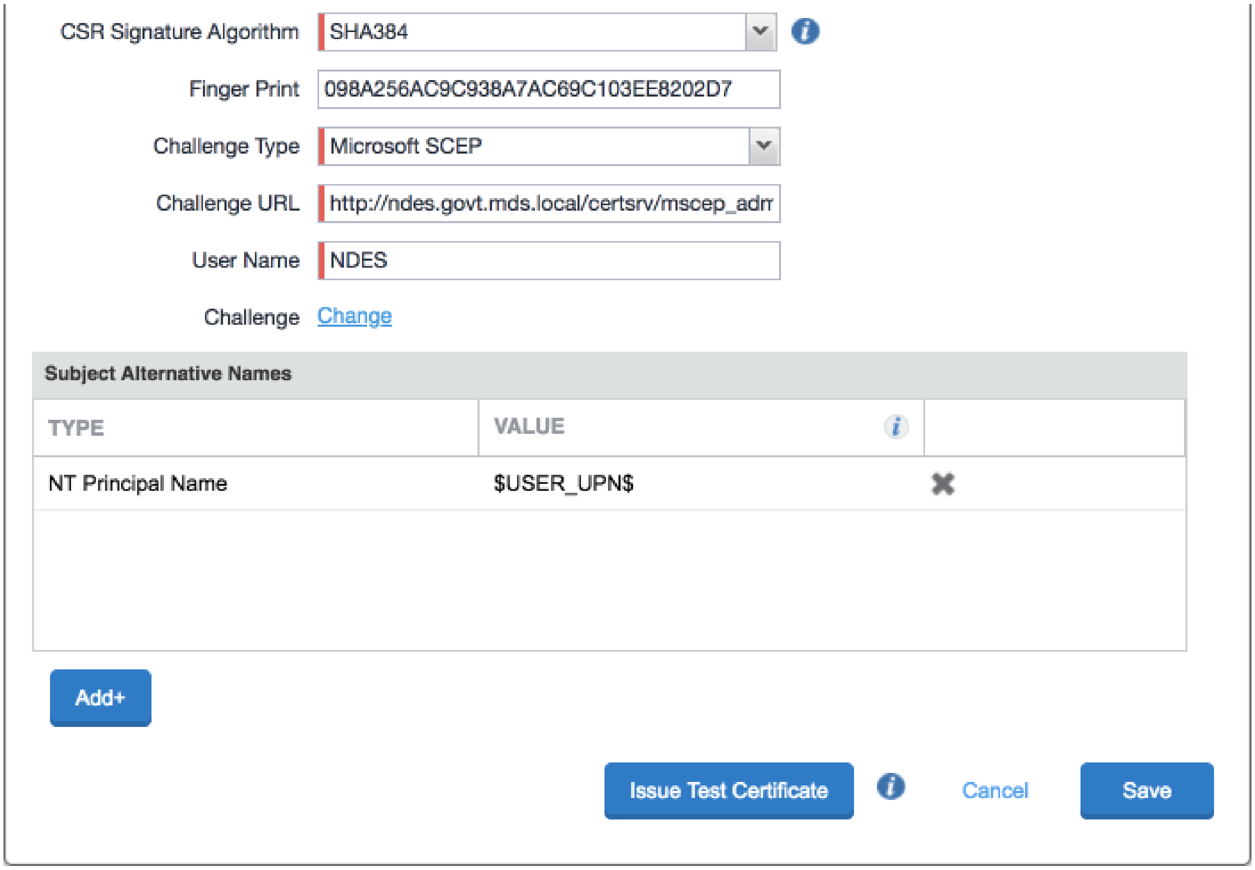
k. In the **Certificate** dialogue, select **OK.**

Figure 2-26 Test SCEP Certificate



4. Select **Save.**

Figure 2-27 Test SCEP Certificate Configuration



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.

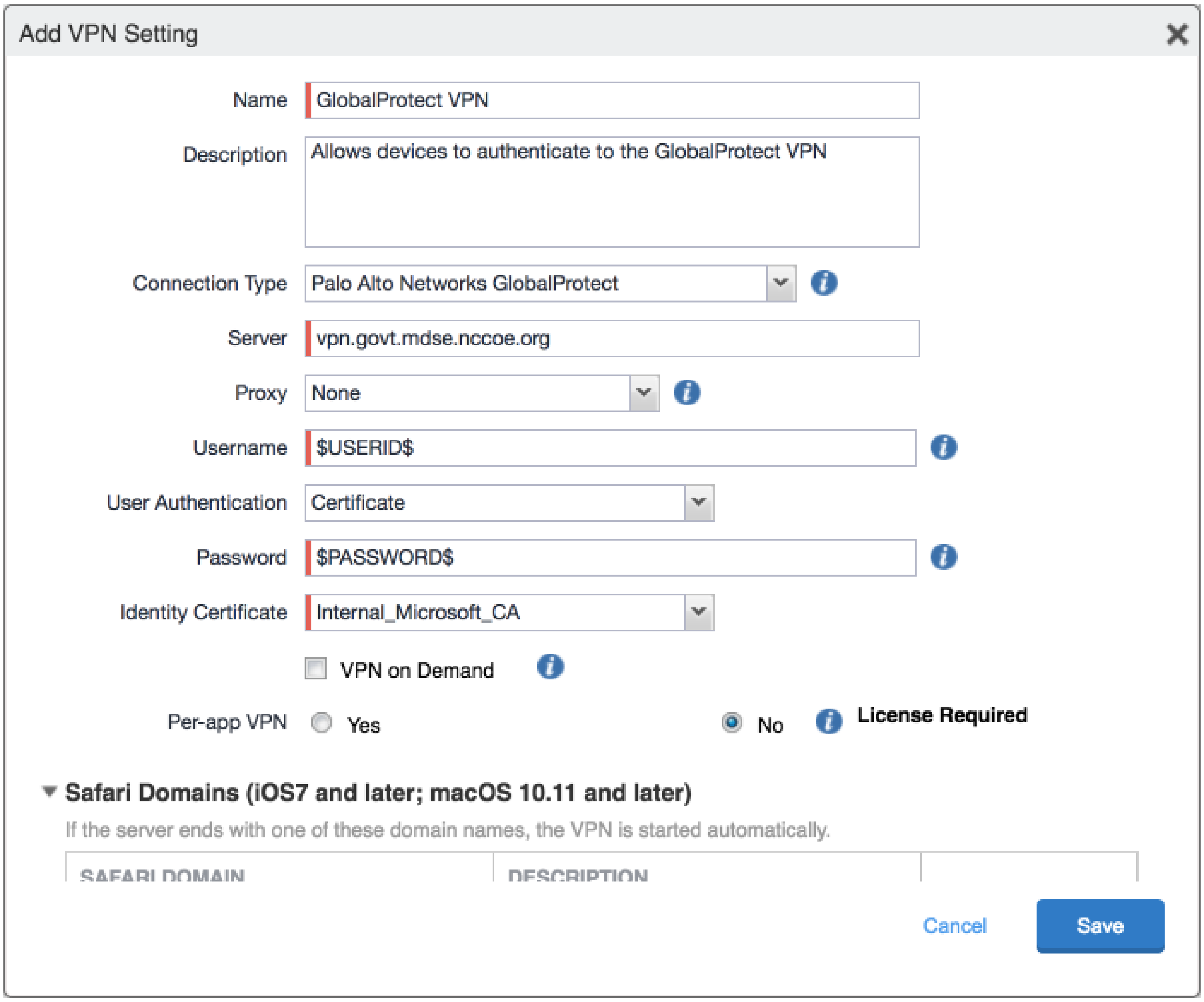
1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.
2. Select **Add New > VPN**; the **Add VPN Setting** dialogue will appear.
3. In the **Add VPN Setting** dialogue:
    a. In the **Name** field, enter a unique name to identify this VPN setting.
    b. In the **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



2.5.2 Basic Palo Alto Networks Configuration

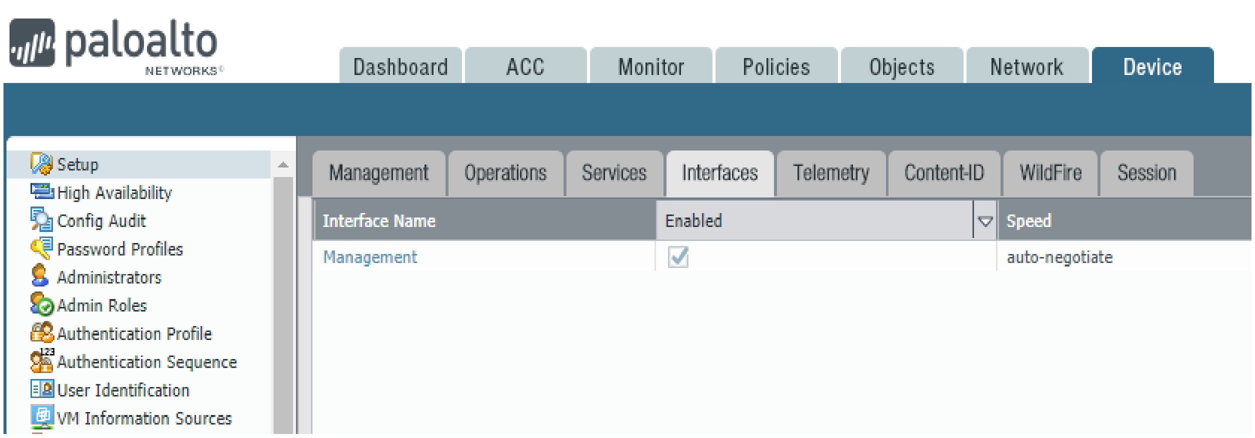
During basic configuration, internet protocol (IP) addresses are assigned to the management interface, domain name system (DNS), and network time protocol (NTP). The management interface allows the administrator to configure and implement security rules through this interface.

2.5.2.1 Configure Management Interface

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

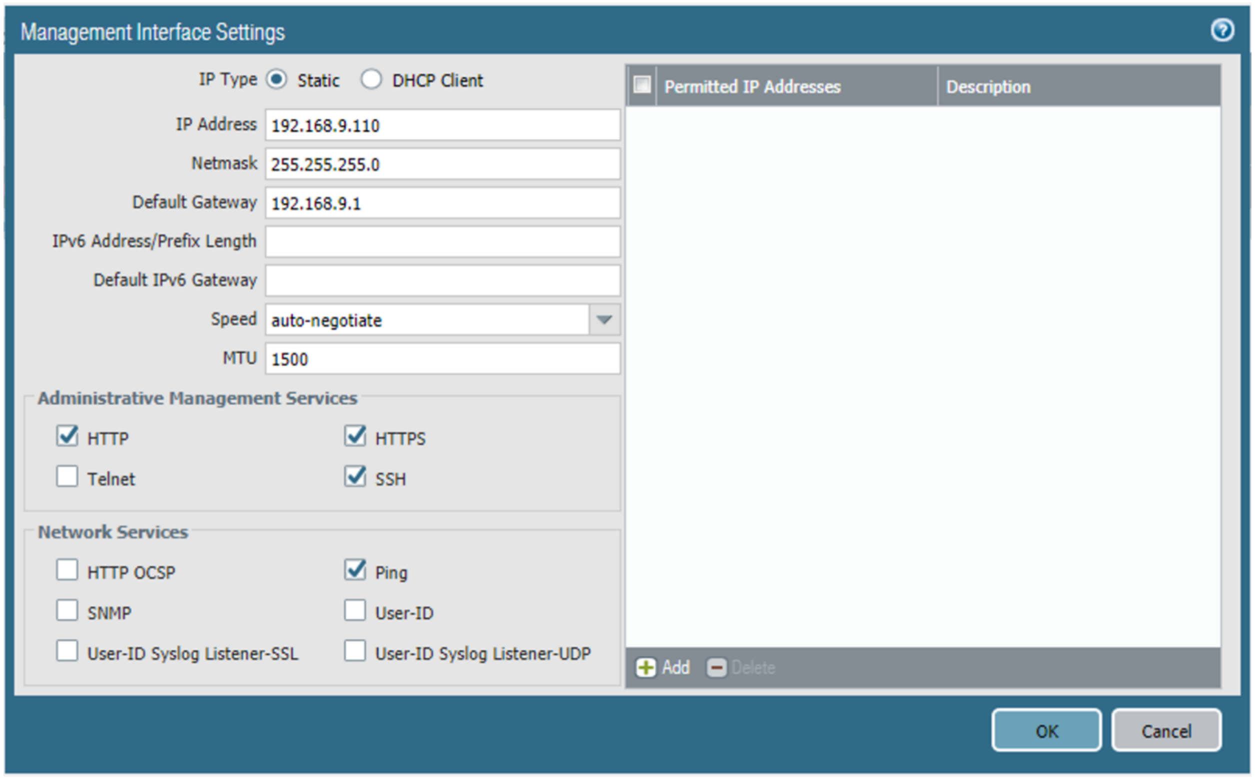
1. In the Palo Alto Networks portal, navigate to **Device > Setup > Interfaces.**
2. On the Interfaces tab, enable the **Management** option; the Management Interface Setting page will open.

Figure 2-29 Palo Alto Networks Management Interface Enabled



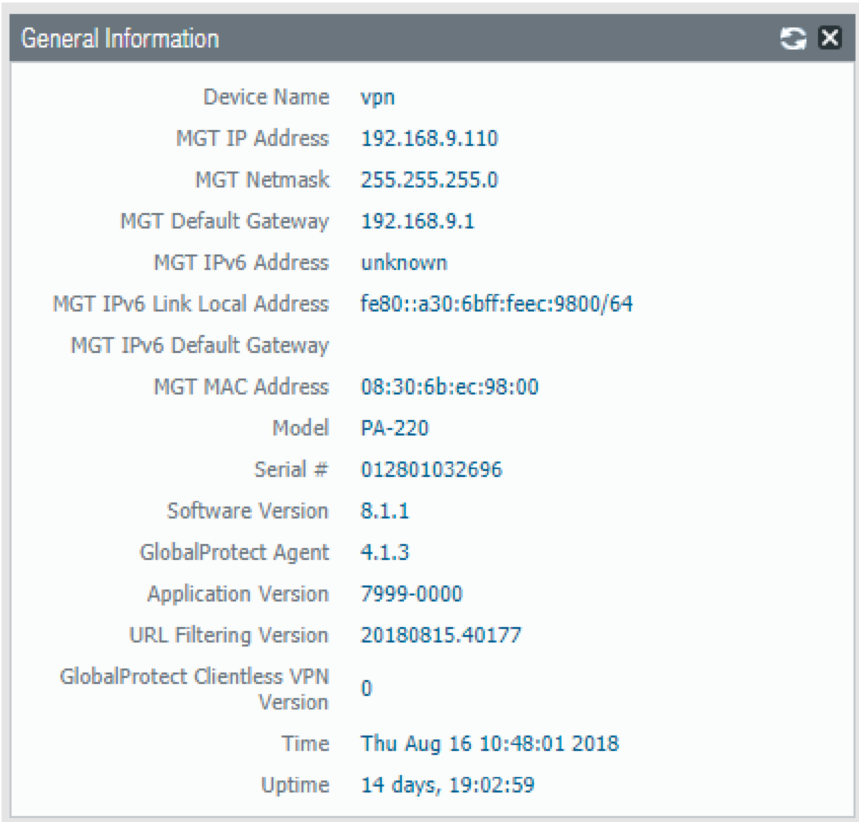
3. On the Management Interface Setting screen:
   a. In the **IP Address** field, enter the IP address for the Palo Alto Networks appliance.
   b. In the **Netmask** field, enter the netmask for the network.
   c. In the **Default Gateway** field, enter the IP address of the router that provides the 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



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

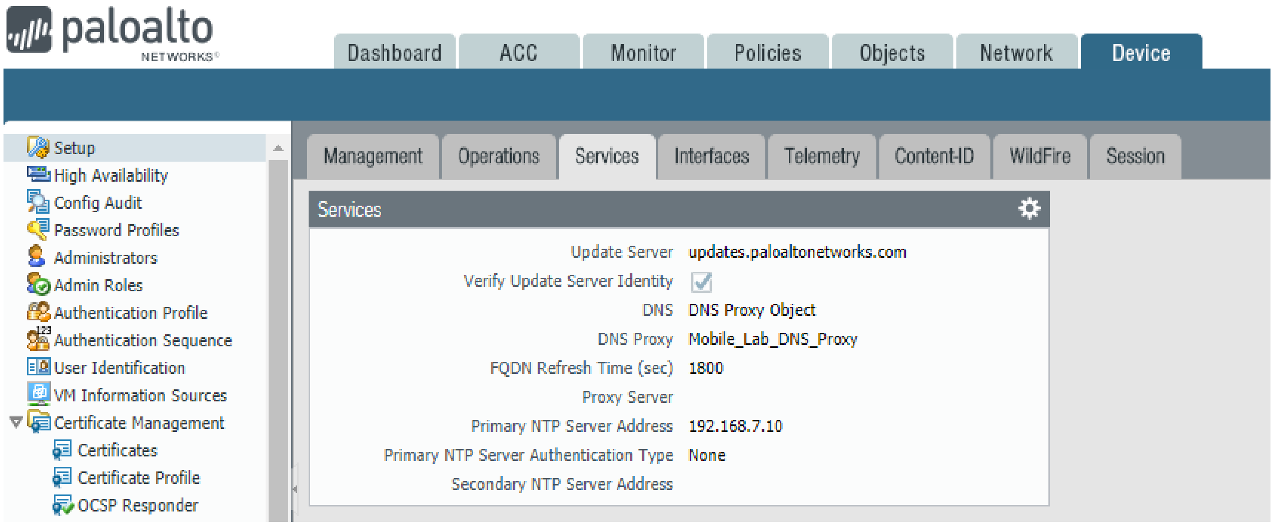
Figure 2-31 Palo Alto Networks Firewall General Information



2.5.2.2 Configure DNS and NTP

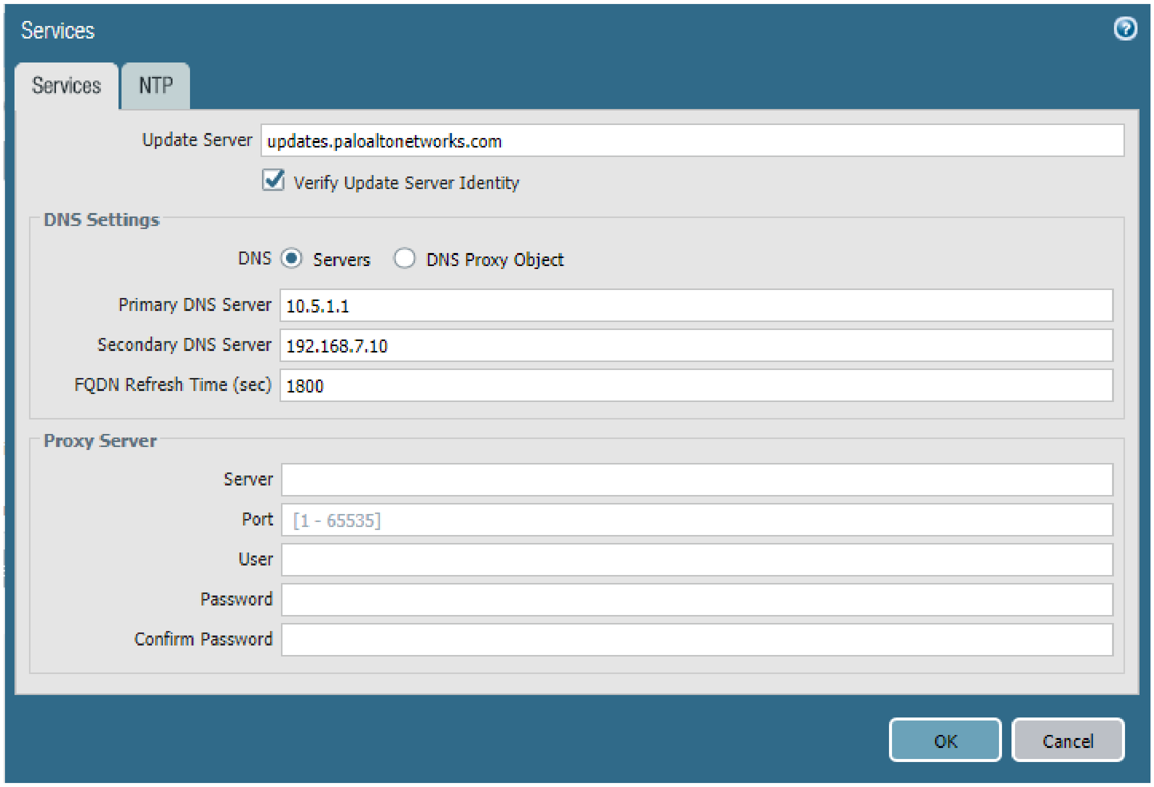
1. In the **Palo Alto Networks Portal**, navigate to **Device > Setup > Services.**
2. In the **Services** tab, select the settings icon.

Figure 2-32 Palo Alto Networks Services Configuration



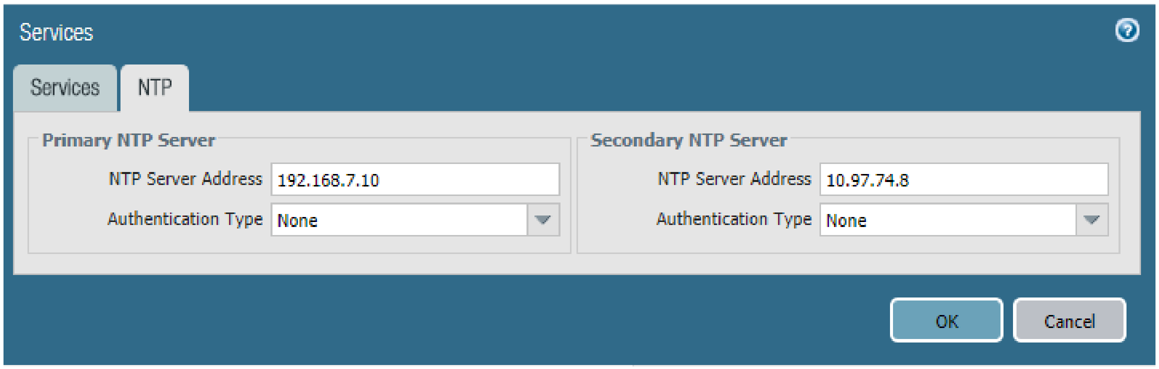
3. On the Services > Services tab:
    a. For the **Primary DNS Server** field, enter the primary DNS server IP address.
    b. For the **Secondary DNS Server** field, enter the secondary DNS server IP address, if applicable.
4. Select the **NTP** tab.

Figure 2-33 DNS Configuration



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



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

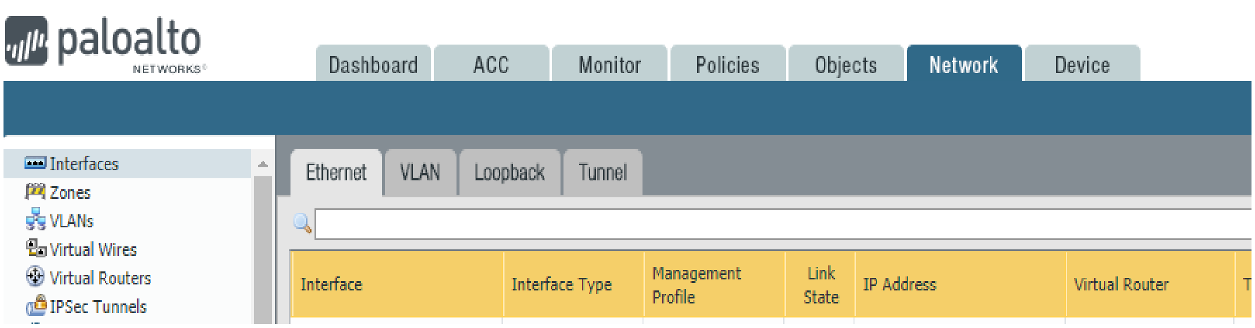
Our example implementation uses three interfaces:

- 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:

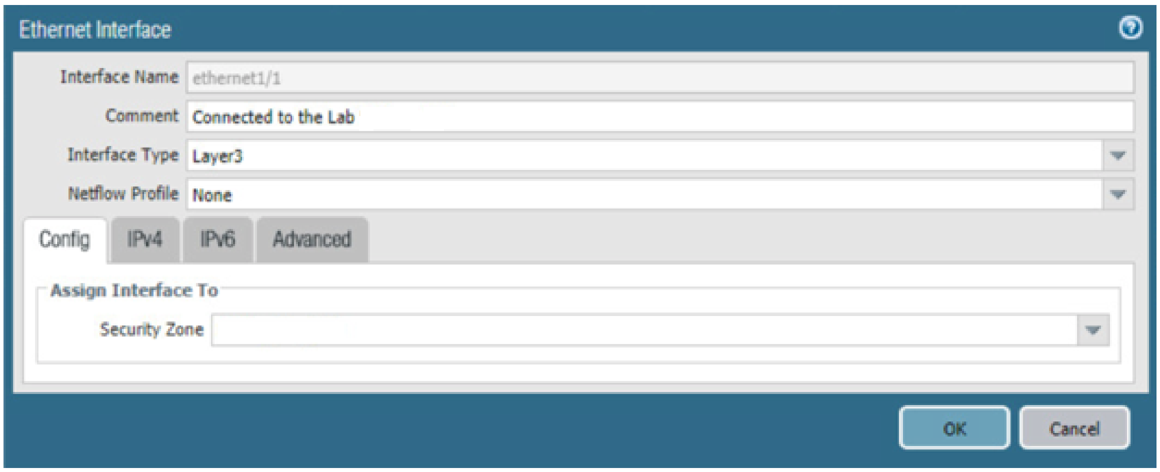
1. Navigate to **Palo Alto Networks Portal > Network > Ethernet > Interfaces > Ethernet.**

Figure 2-35 Ethernet Interfaces



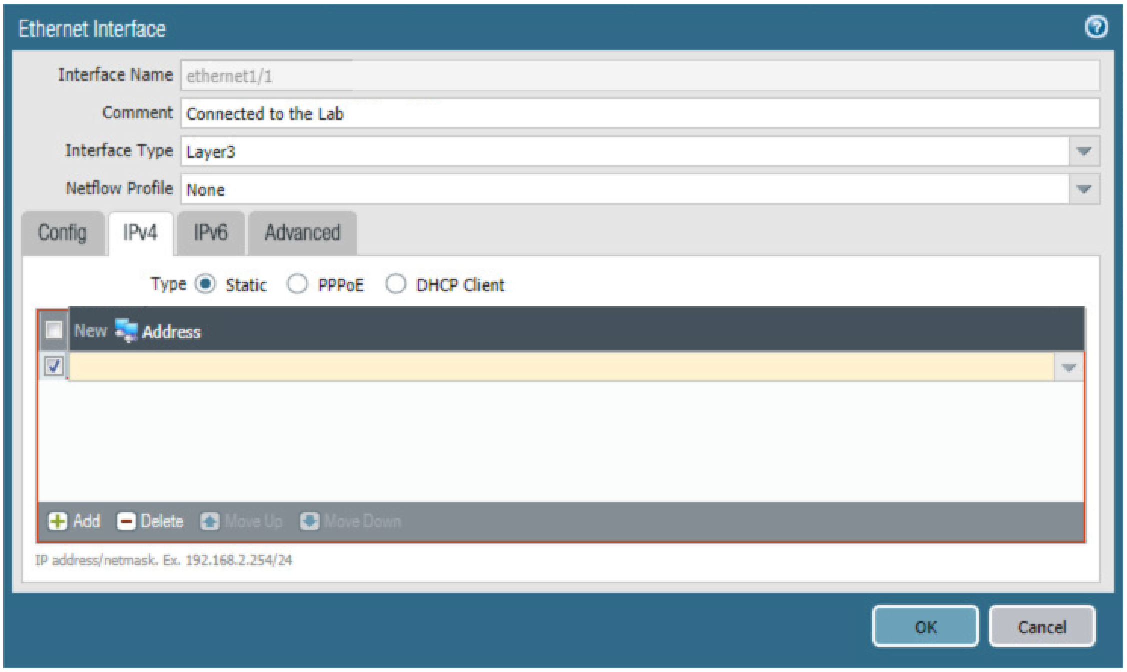
2. In the **Ethernet** tab, select the name of the interface to configure; the Ethernet Interface dialogue will appear.
3. In the **Ethernet Interface** dialogue:
    a. In the **Comment** field, enter a description for this interface.
    b. For the **Interface Type** drop-down menu, select **Layer3.**

Figure 2-36 Ethernet Interface Configuration



    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



iii. In the **Address** dialogue:

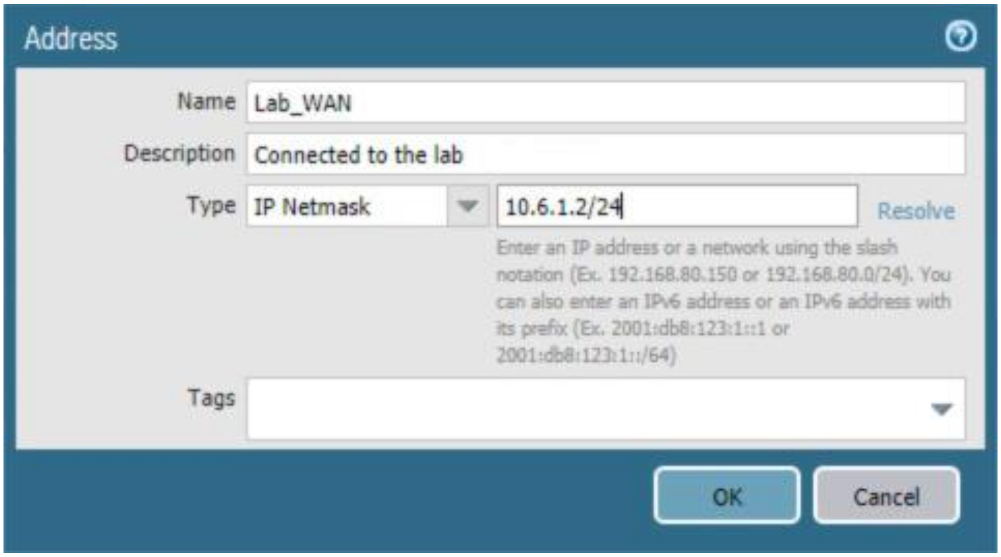
1) For the **Name** field, enter a unique name to identify this address.

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.

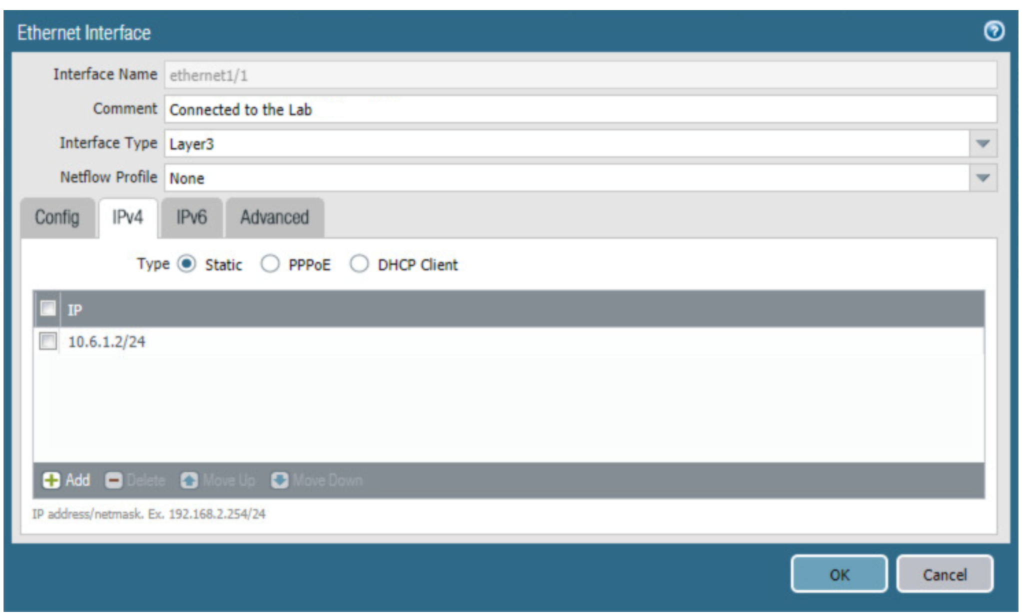
4) Select **OK.**

Figure 2-38 WAN Interface IP Address Configuration



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



4. Select **OK.**

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

2.5.3.2 Create Security Zones

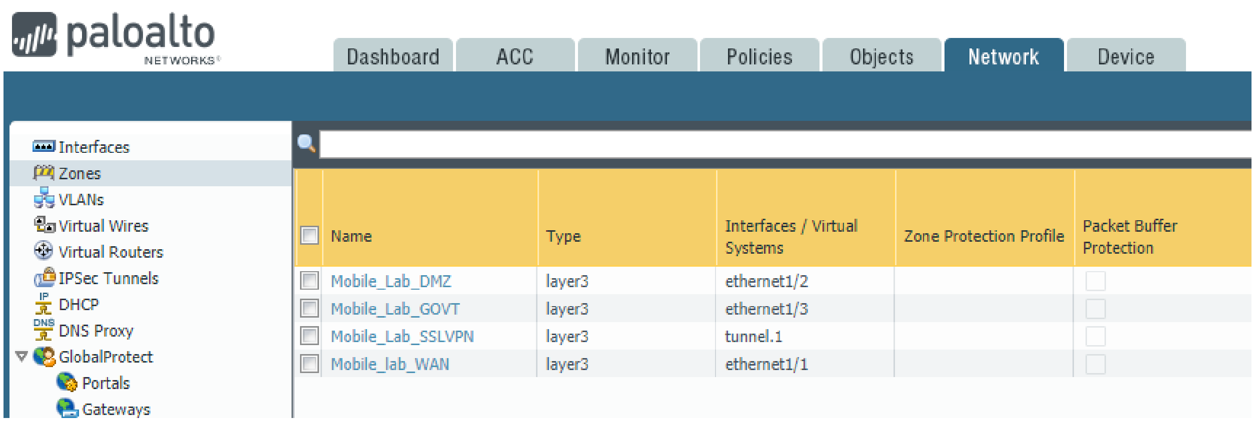
The PA Security Zone is a collection of single or multiple interfaces that have the same security rules. For this setup, four different zones have been configured:

- *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.**

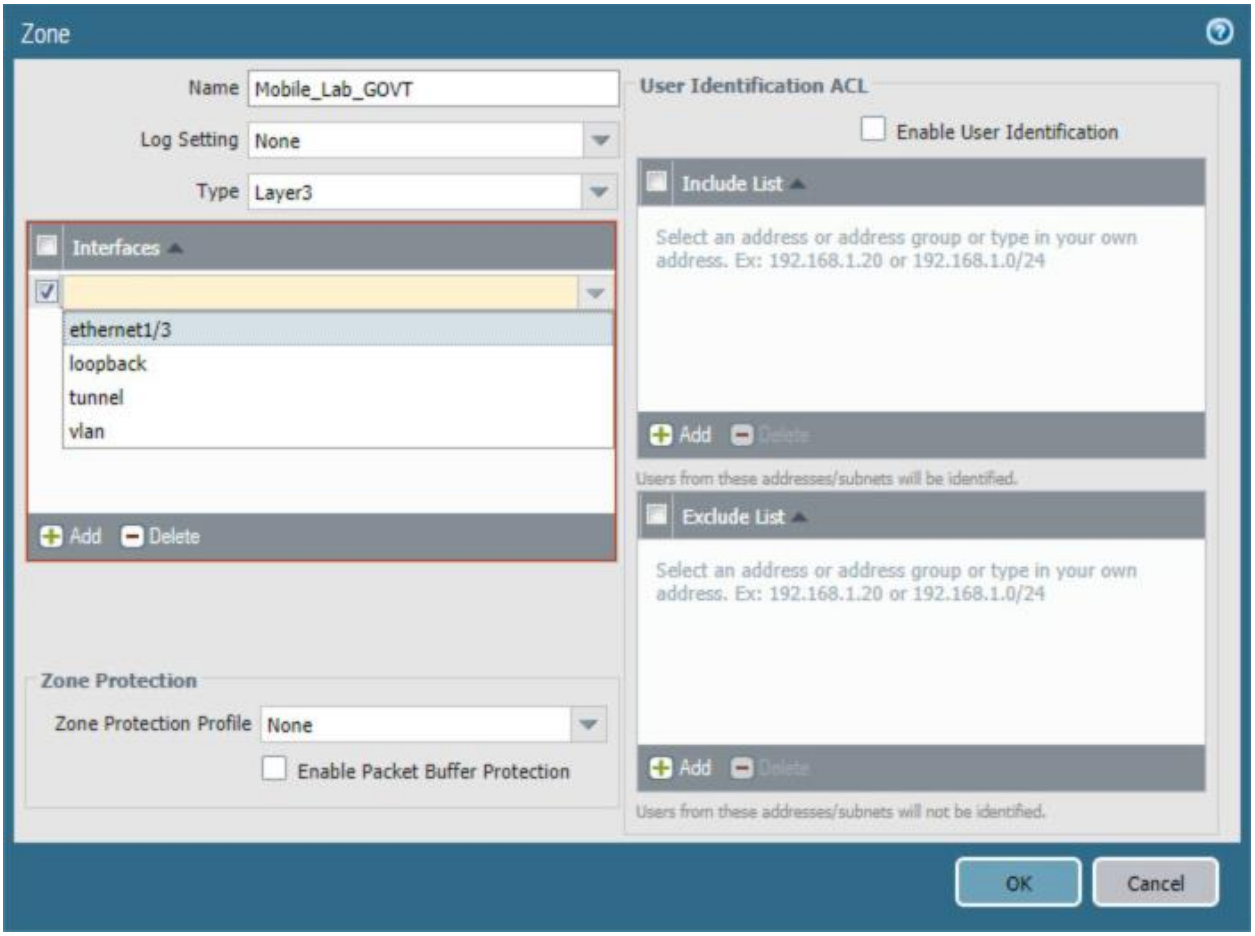
Figure 2-40 Security Zone List



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



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

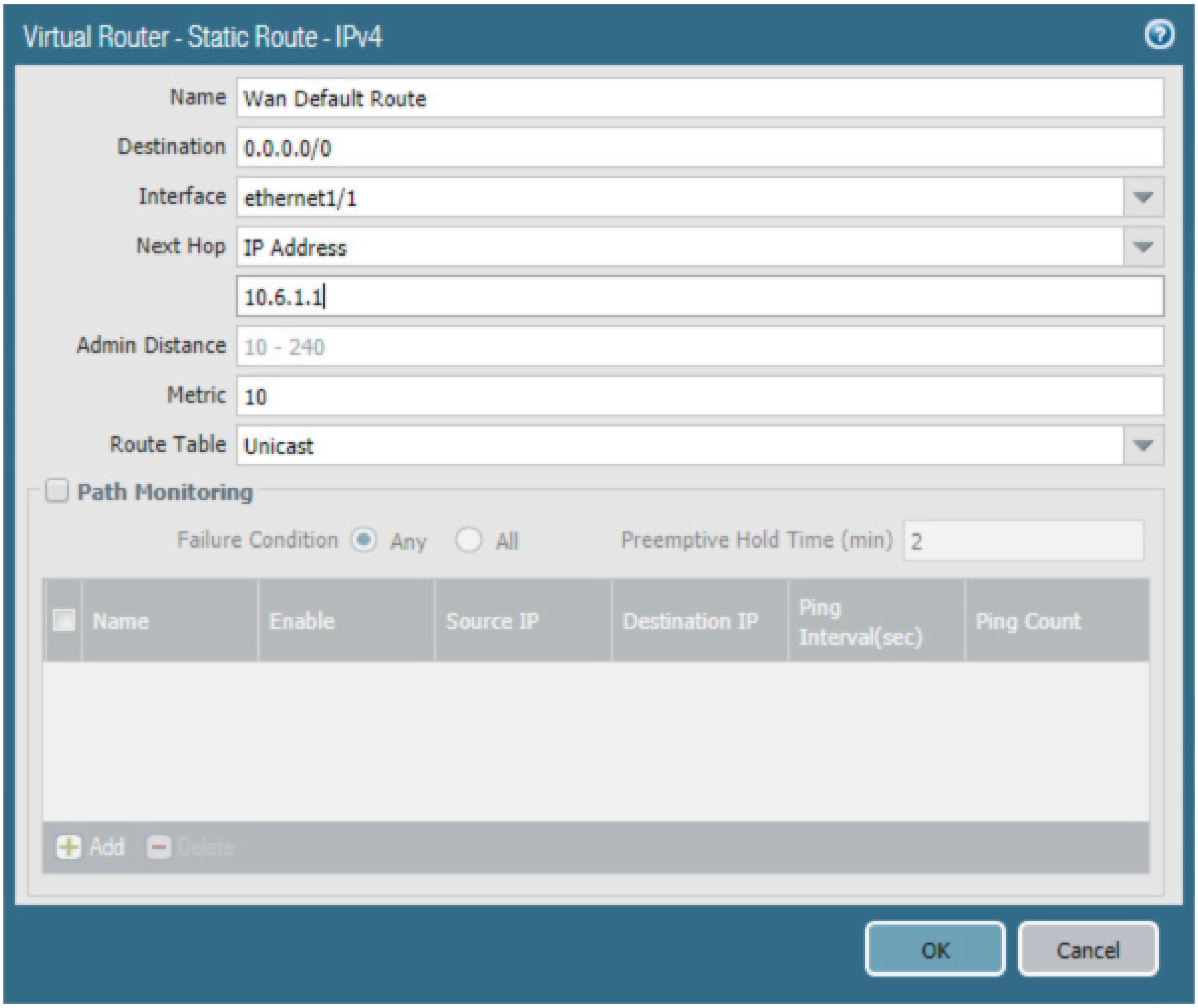
2.5.4 Configure Router

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.

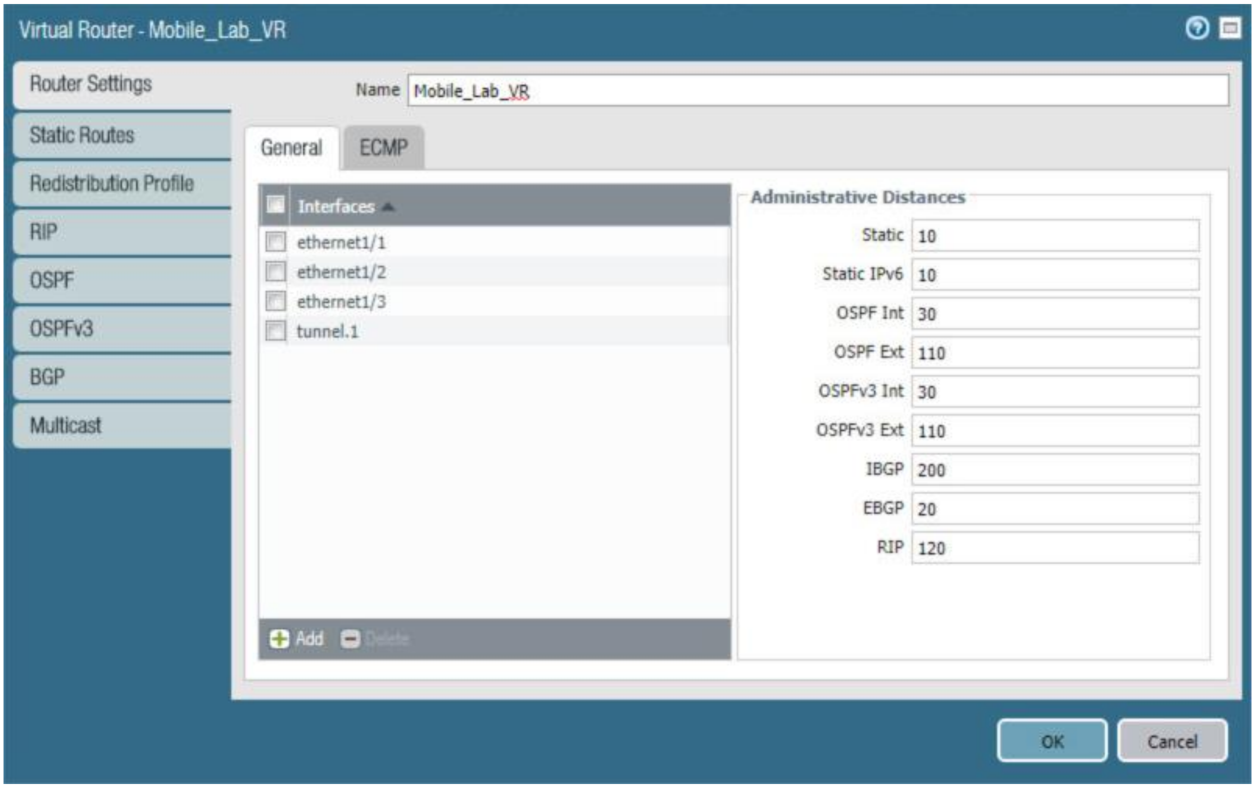
3. In the **Virtual Router** form, on the **Router Settings** tab:
    a. For the **Name** field, enter a unique name to identify this router.
    b. On the **Router Settings > General** tab:
        i. Under the **Interfaces** list box, select **Add;** a new list item will appear.
        ii. In the 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**



702 6. Select **OK.**

Figure 2-43 Virtual Router General Settings

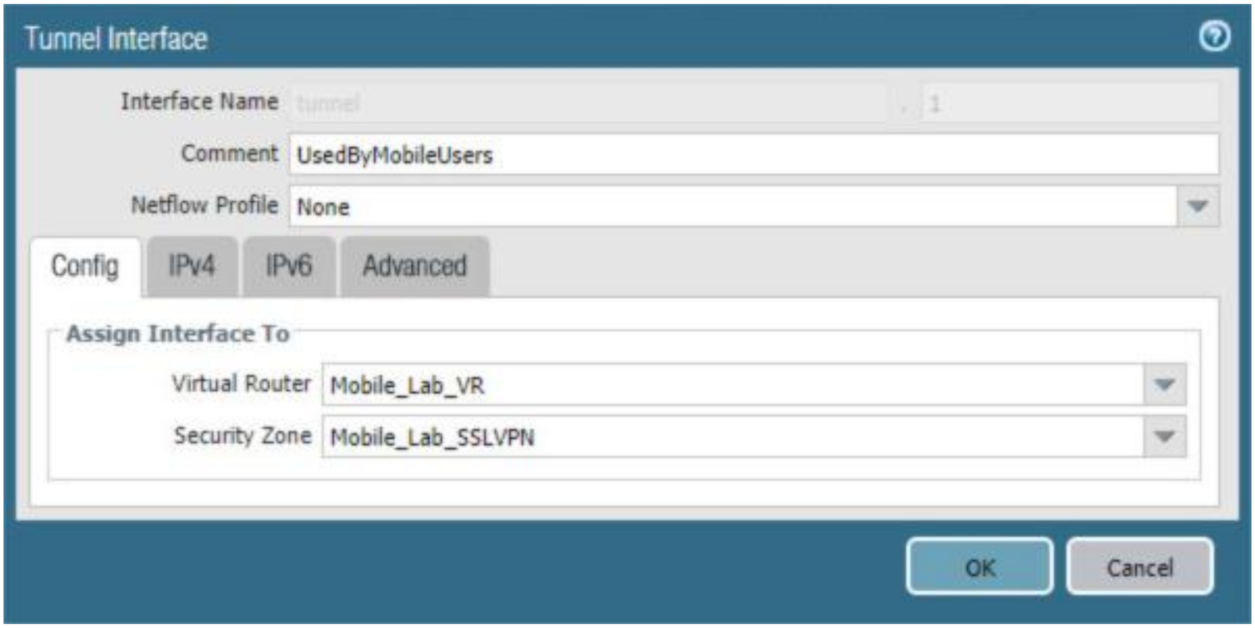


2.5.5 Configure Tunnel Interface

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



2.5.6 Configure Applications and Security Policies

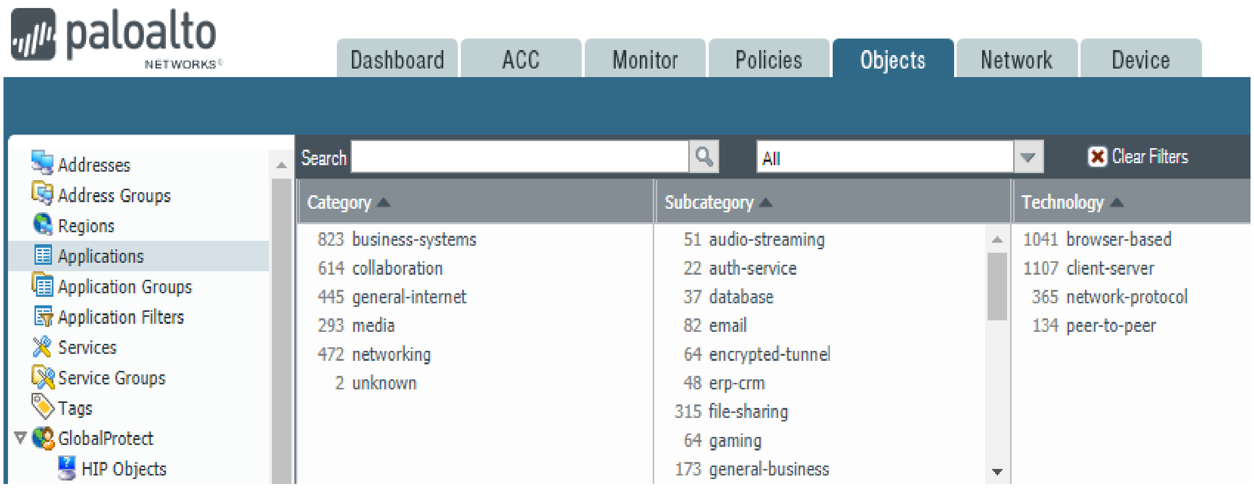
Security policies work similarly to firewall rules; they block or allow traffic between defined zones identified by a source, destination, and application(s) (contextually, Palo Alto Networks' objects define network protocols and ports). Palo Alto Networks has built-in applications for a large number 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:

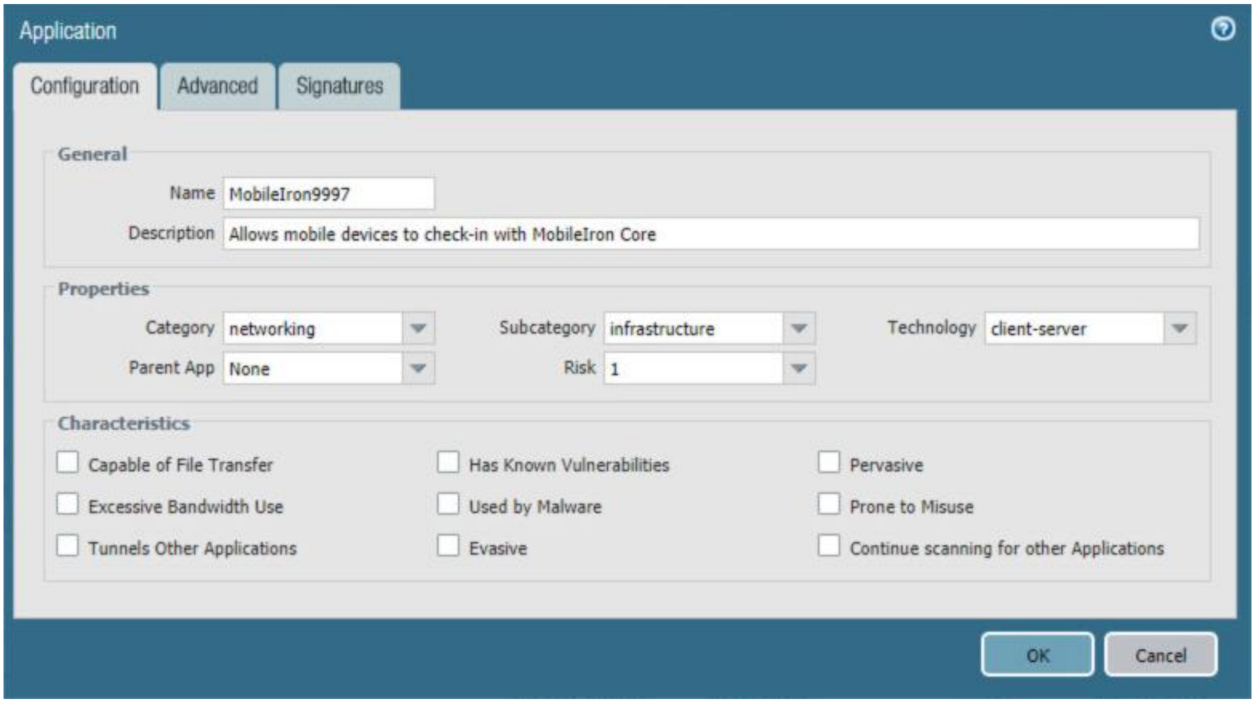
1. In the **Palo Alto Networks Portal,** navigate to **Objects > Applications.**

Figure 2-45 Application Categories



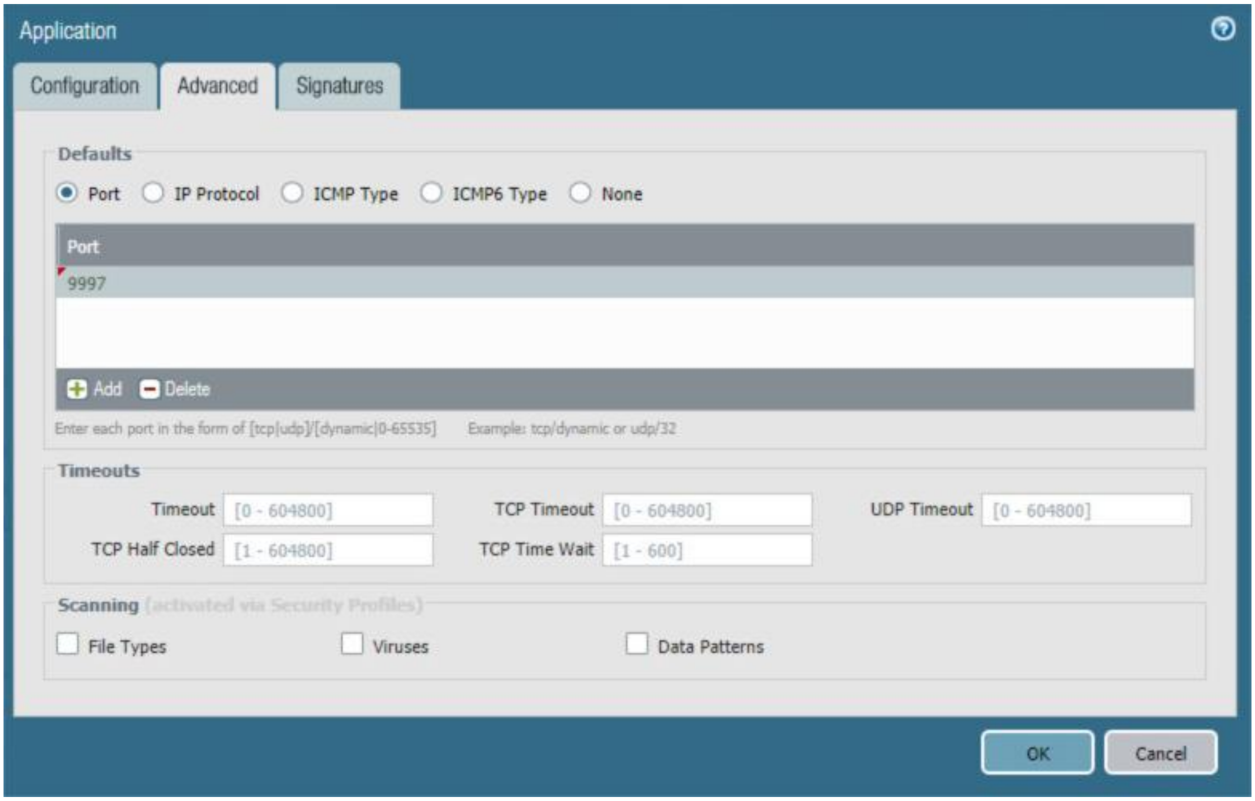
2. On the **Applications** screen:
3. Select **Add;** the Application form will open.
4. On the **Application > Configuration** screen:
    a. In the **General > Name** field, provide a unique name to identify this application.
    b. In the **General > Description** field, enter a meaningful description 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



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



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

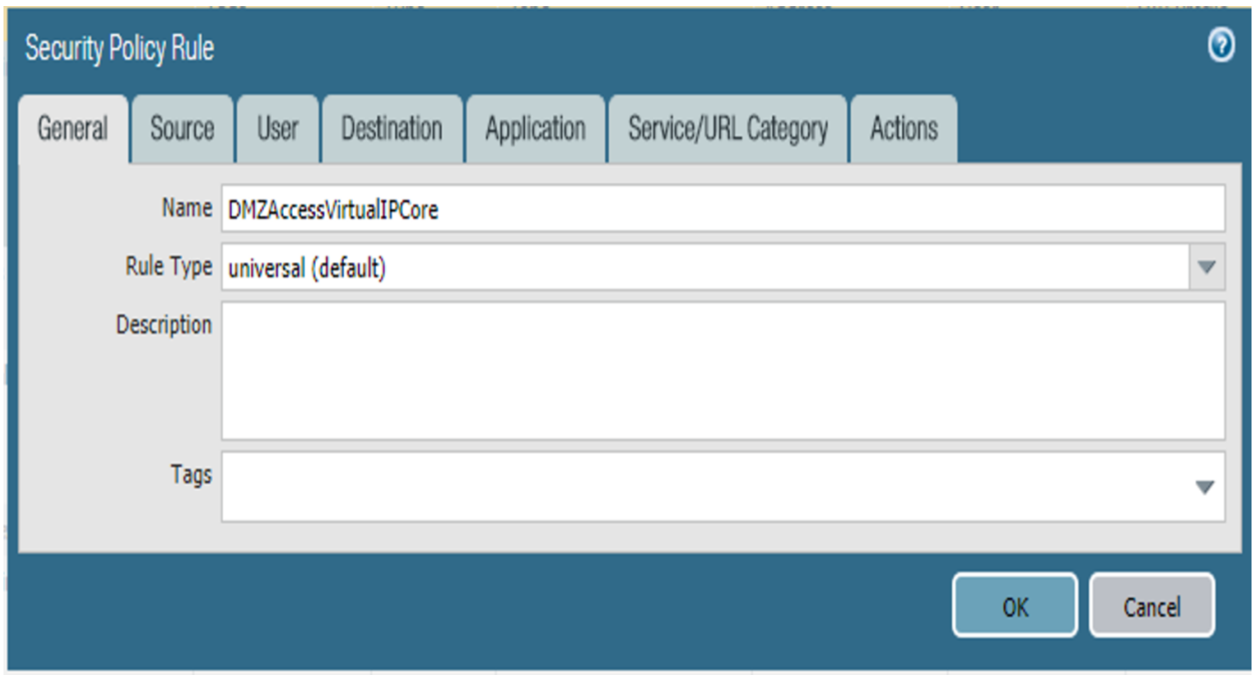
Security policies allow or explicitly deny communication within, between, or (externally) to or from Palo Alto Networks zones. For this sample implementation, several security policies were created to support communication by other components of the architecture. The first subsection covers the steps 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

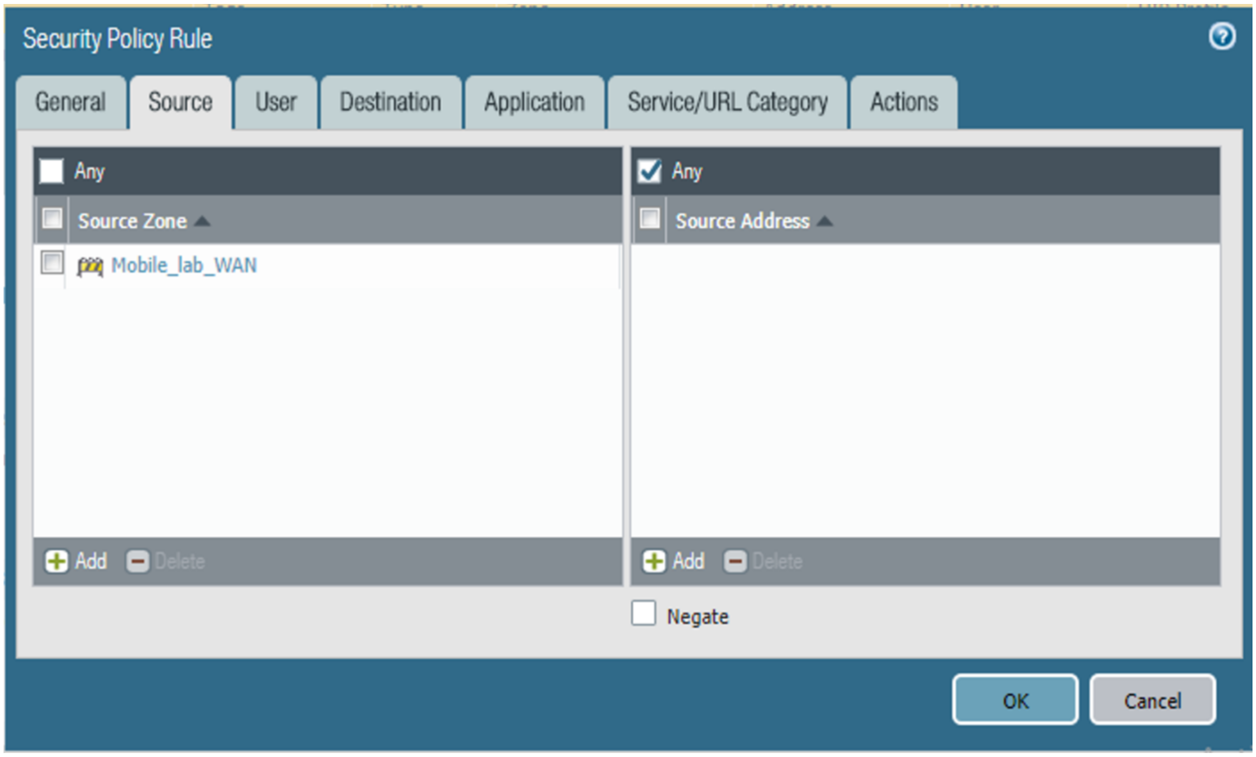


4. Select the **Source** tab.
5. On the **Source** tab:
    a. If the security rule applies to a specific source zone:
        i. Under the **Source Zone** list box, select **Add;** a new entry will appear in the list box.
        ii. For the new list item, select the source zone for this rule.
    b.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



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.

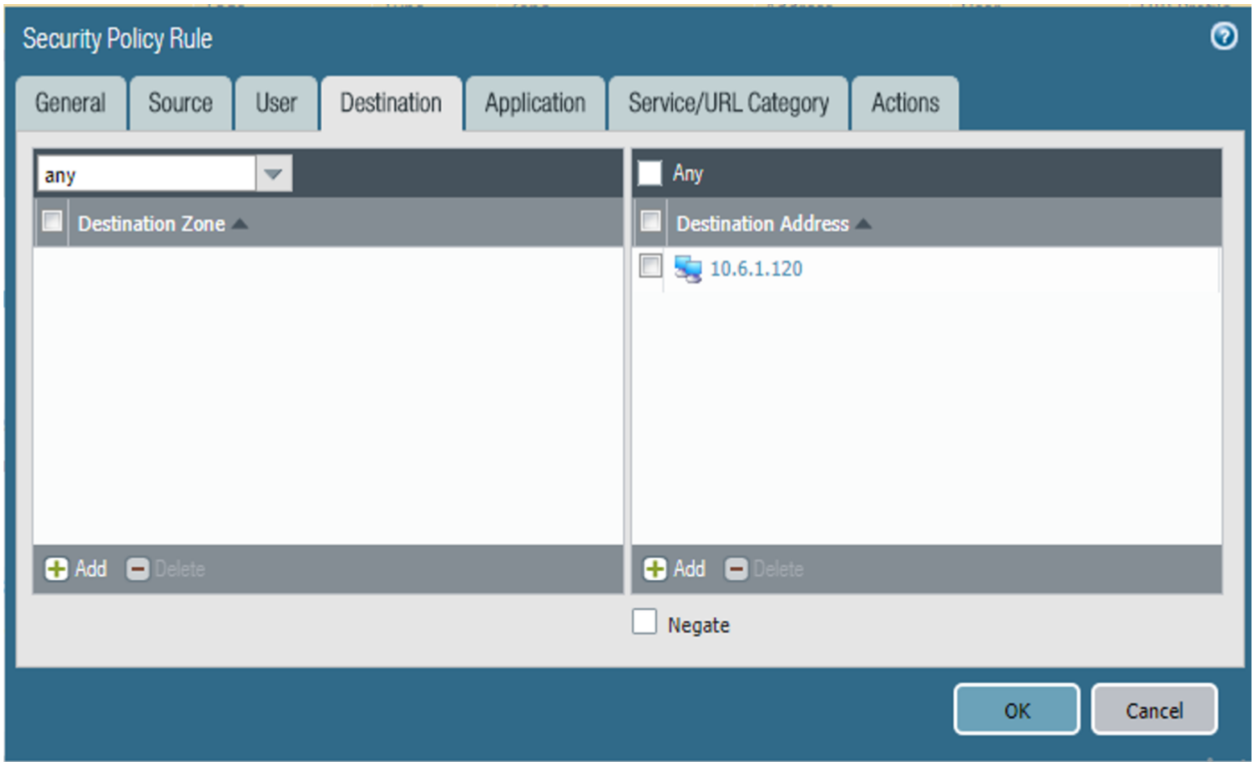
      ii. For the new **Source Zone** list item, select the destination zone for this rule.

   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.

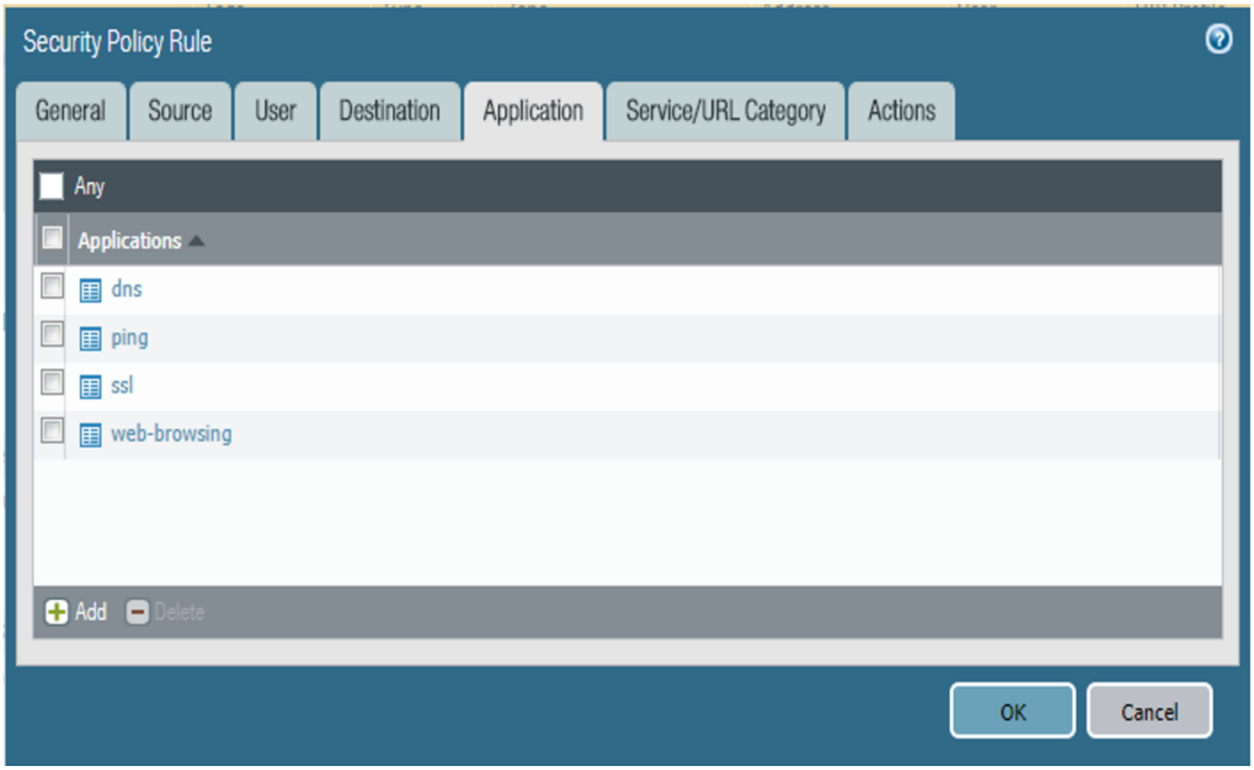
      ii. For the new list item, select the destination address for this rule.

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



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).

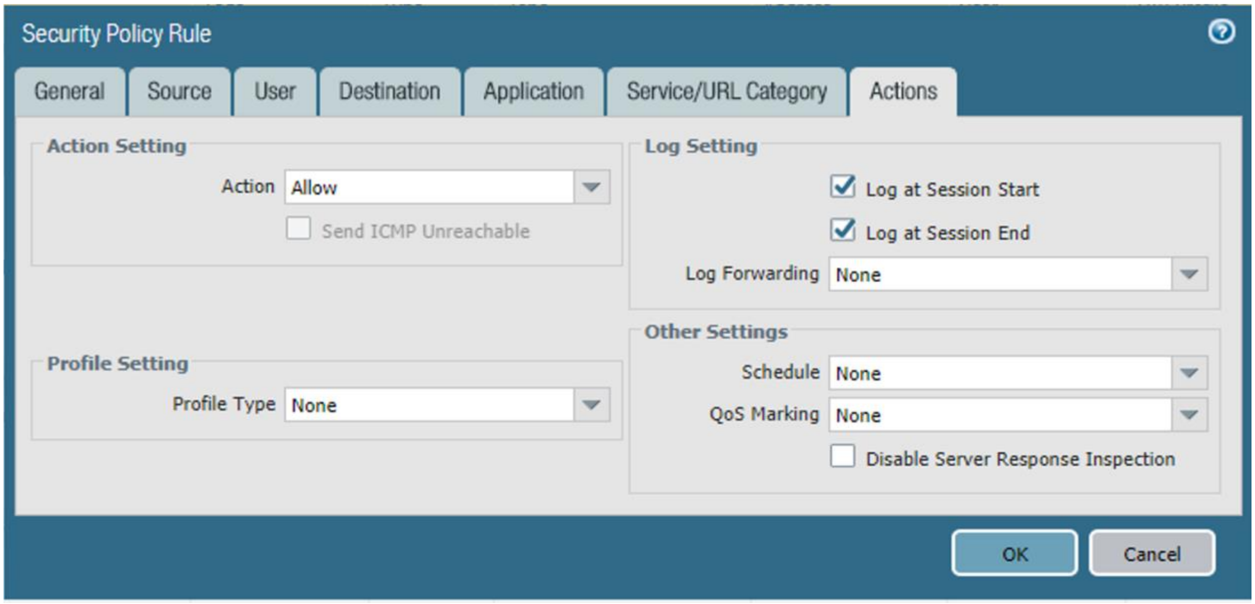
797 **Figure 2-51 DMZ Access to MobileIron Security Rule Application Protocol Configuration**



798 10. Select the **Actions** tab.

799 11. On the **Actions** tab: Unless explicitly blocking traffic permitted by a more permissive
800 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



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
AppthorityConnectorAccessToMI-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

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

Table 2-3 Implemented Security Policies

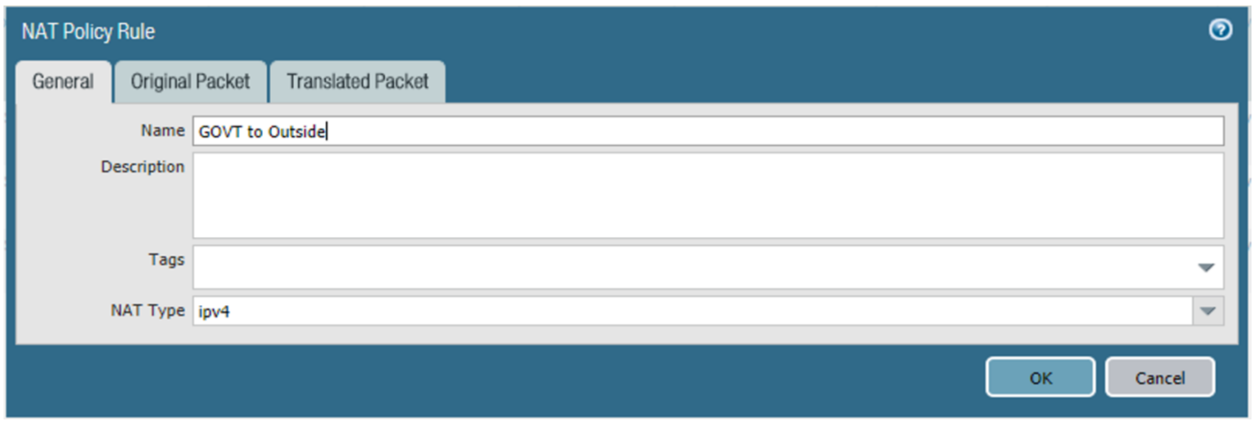
Name	Application	Service	Action	Profile	Options
DMZAccessVirtualIPCore	dns;ping;ssl;web-browsing	any	allow	none	none
CoretoAppleSrvs	any	any	allow	none	none
AdminAccessToMI	AdminAccessMI; ssh;ssl	any	allow	none	none
AppthorityConnectorAccessToMI-Core	AdminAccessMI; ssl;web-browsing	any	allow	none	none
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

2.5.7 Network Address Translation (NAT)

To allow communication with external networks over the internet, the appliance also needs to be 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



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.**

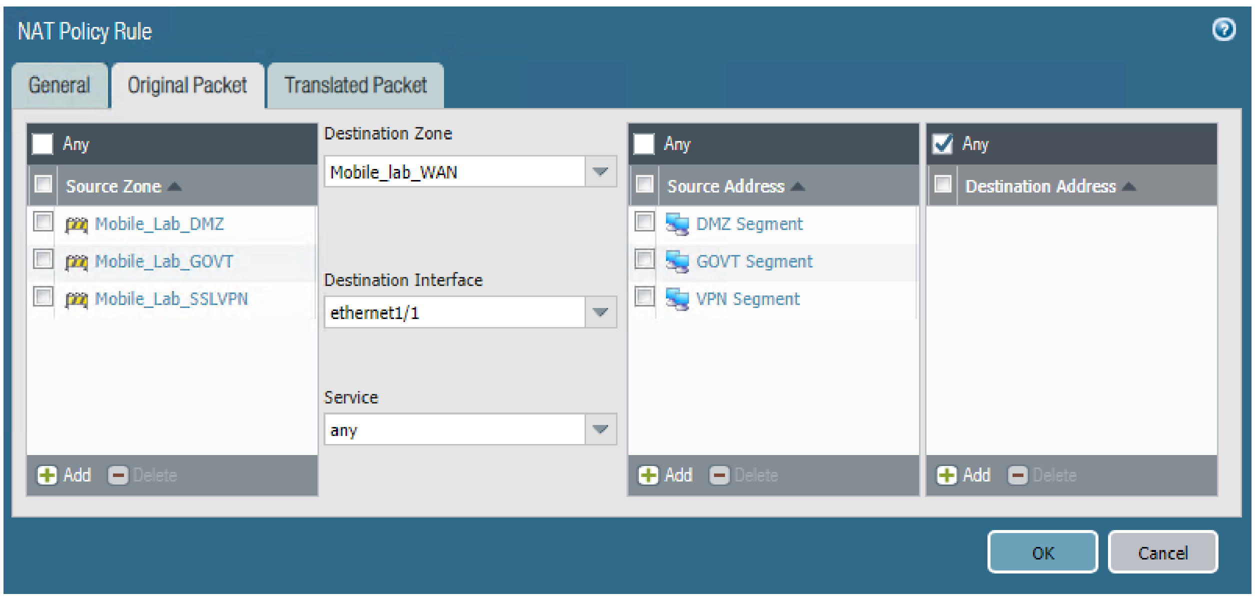
g. Under the **Source Address** list box, select **Add;** a new Source Address list item will appear.

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



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

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

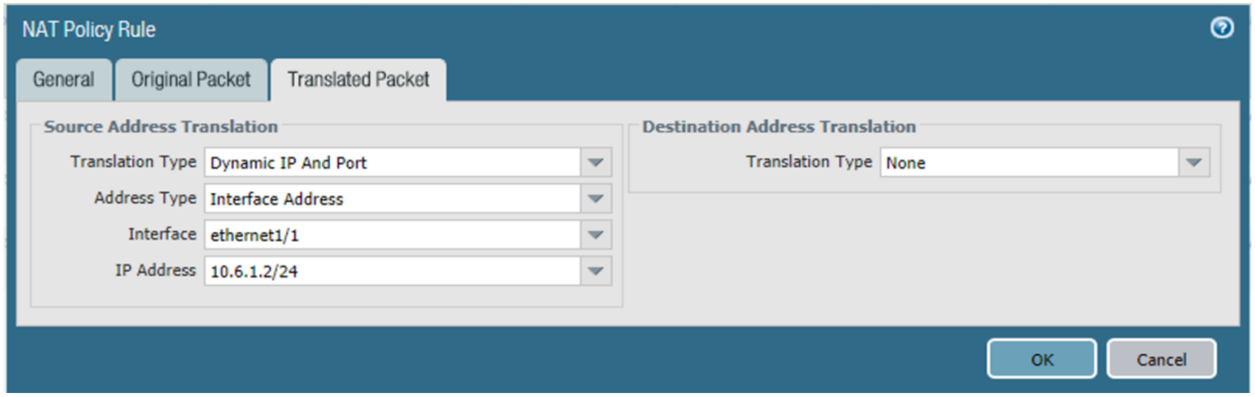
a. For the **Translation Type** drop-down menu, select **Dynamic IP and Port.**

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



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.

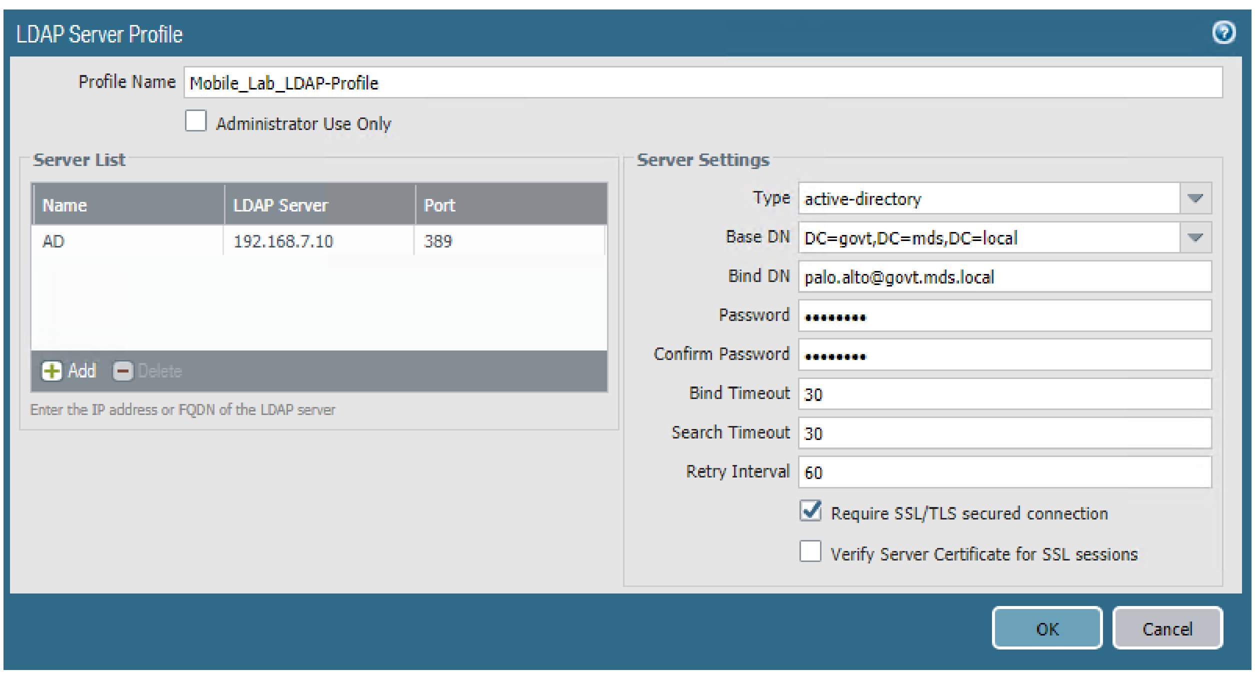
        iii. In the **Bind DN** field, enter the Active Directory domain user account that will authenticate to LDAP to perform queries.

        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.**

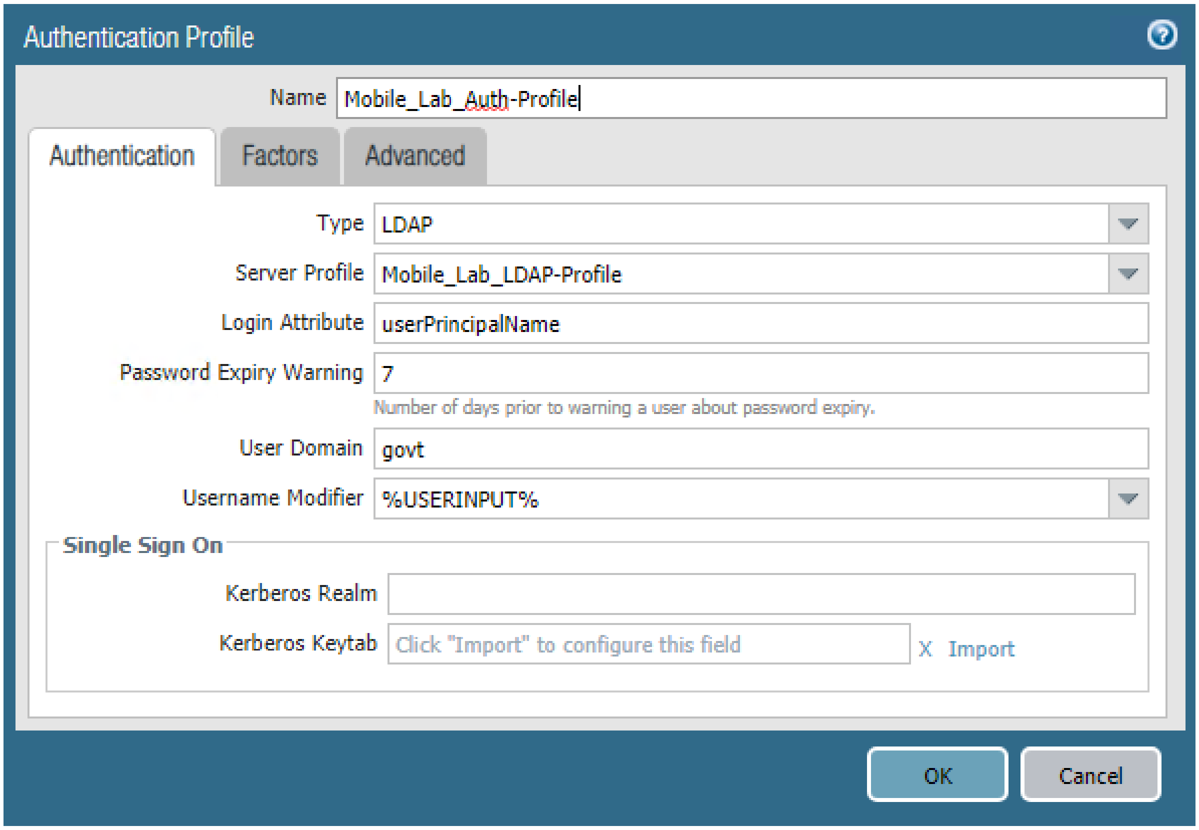
Figure 2-56 LDAP Profile



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



c. Select the **Advanced** tab.

d. On the **Advanced** tab:

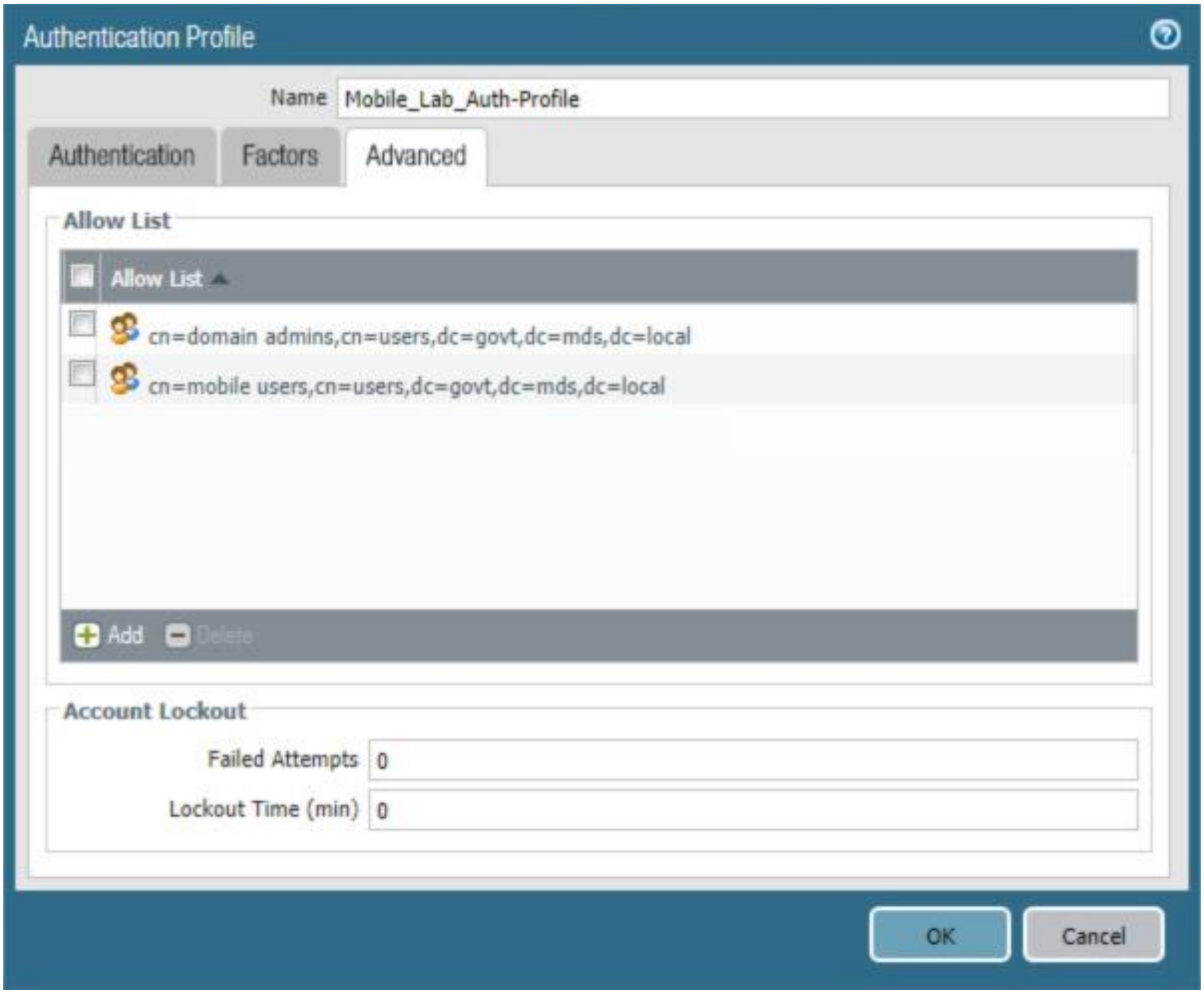
   i. Under the **Allow List** box, select **Add;** this will create a new list item.

   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



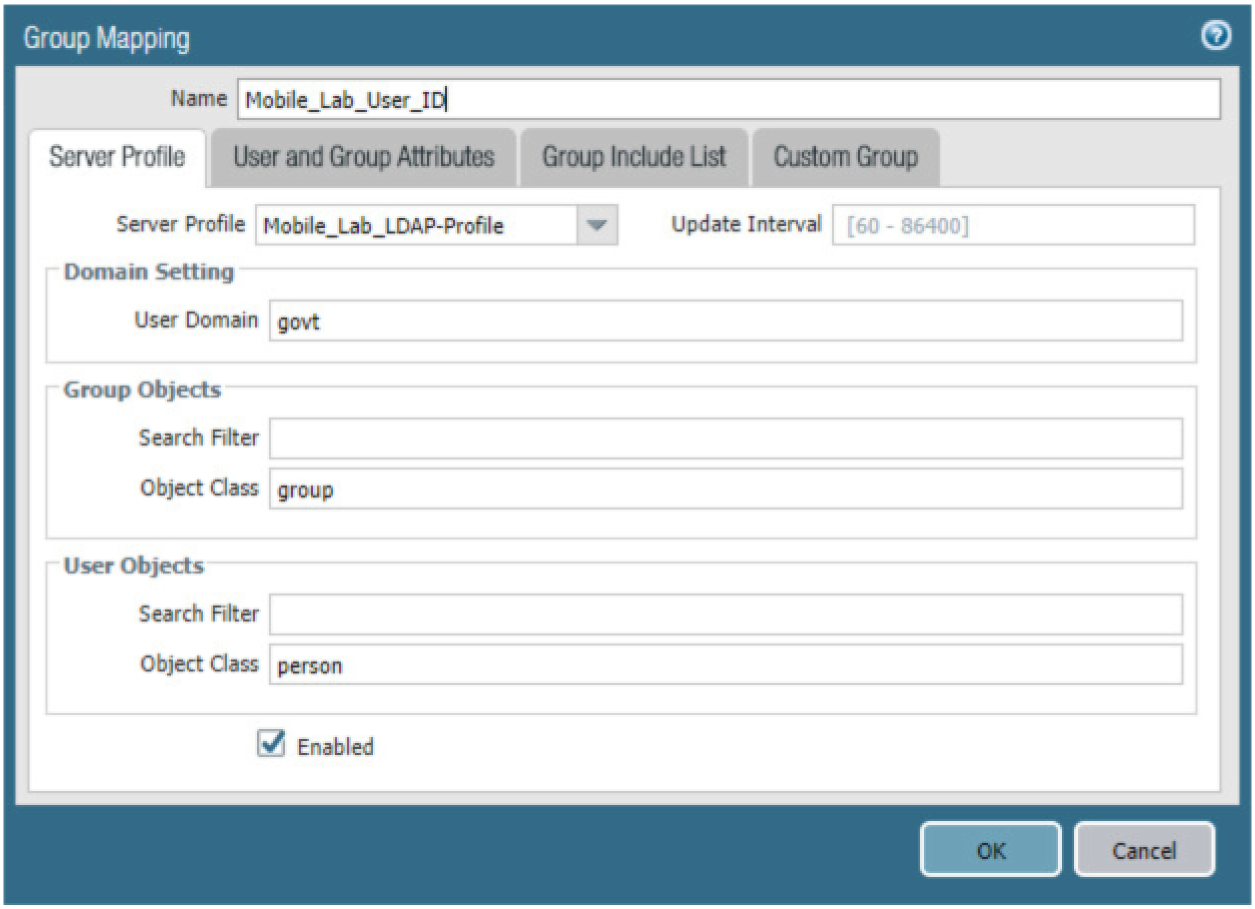
2.5.8.3 Configure User Identification

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



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

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

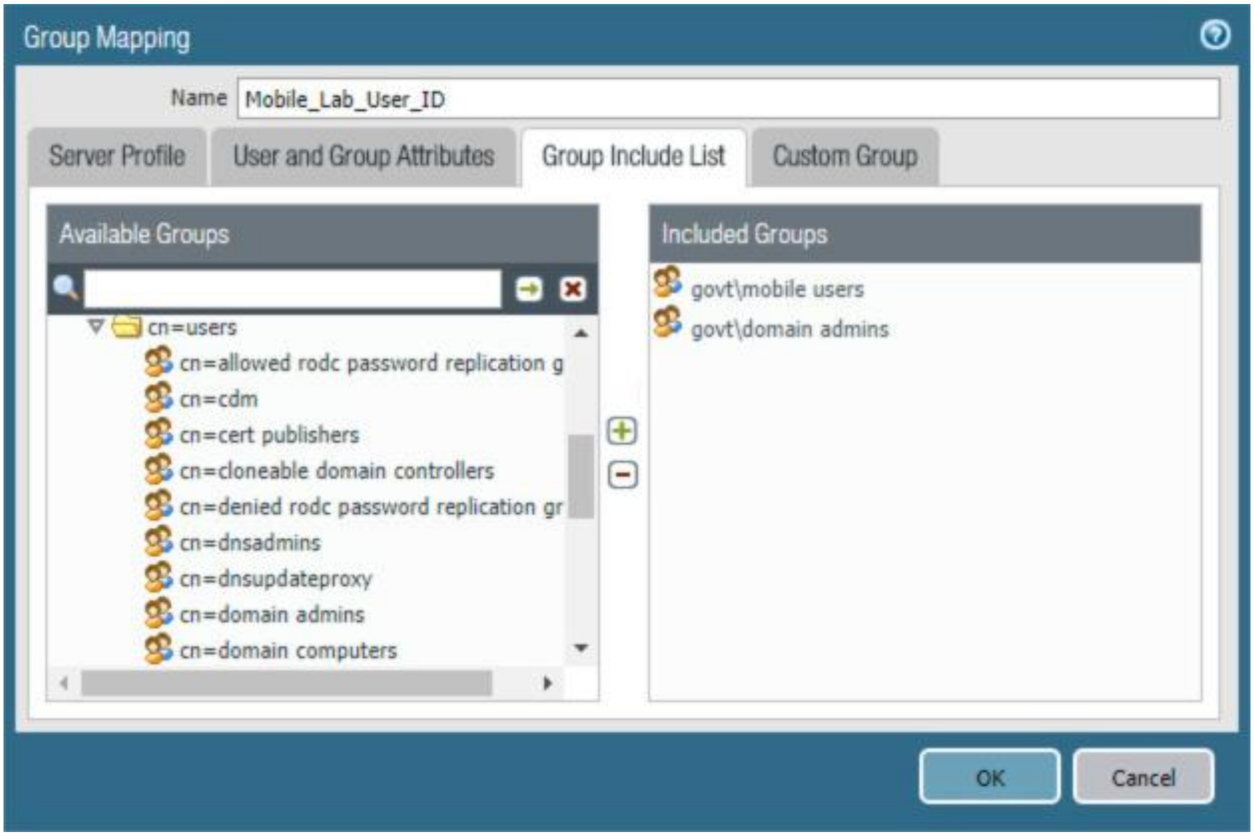
i. In the **Available Groups** list box, expand the Active Directory domain to reveal configured user groups.

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

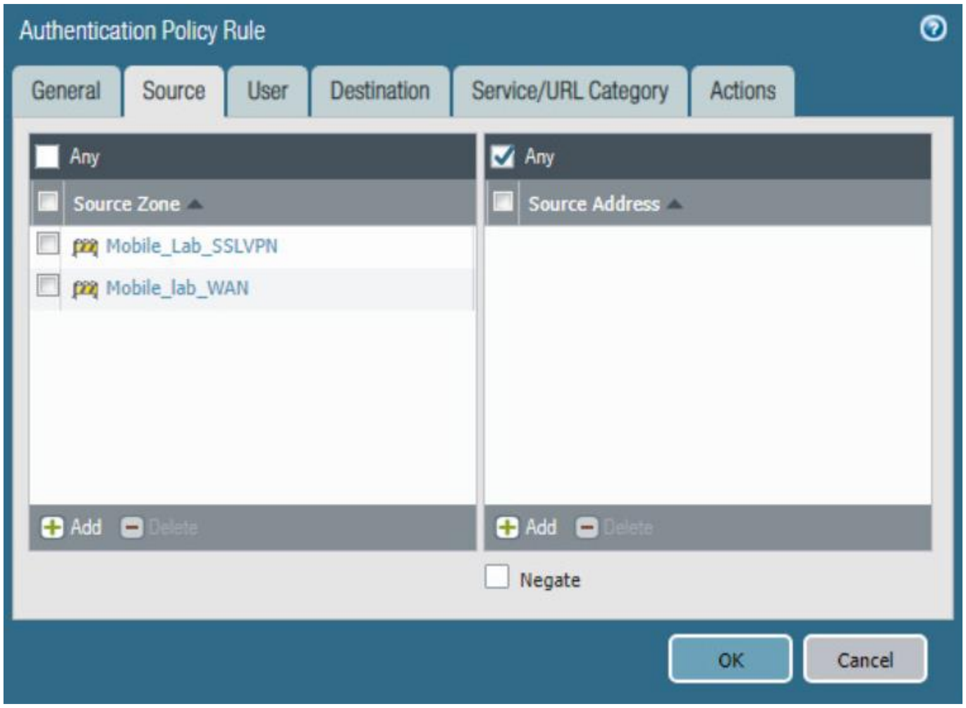


5. Select **OK.**

2.5.8.4 Configure Authentication Policy Rule

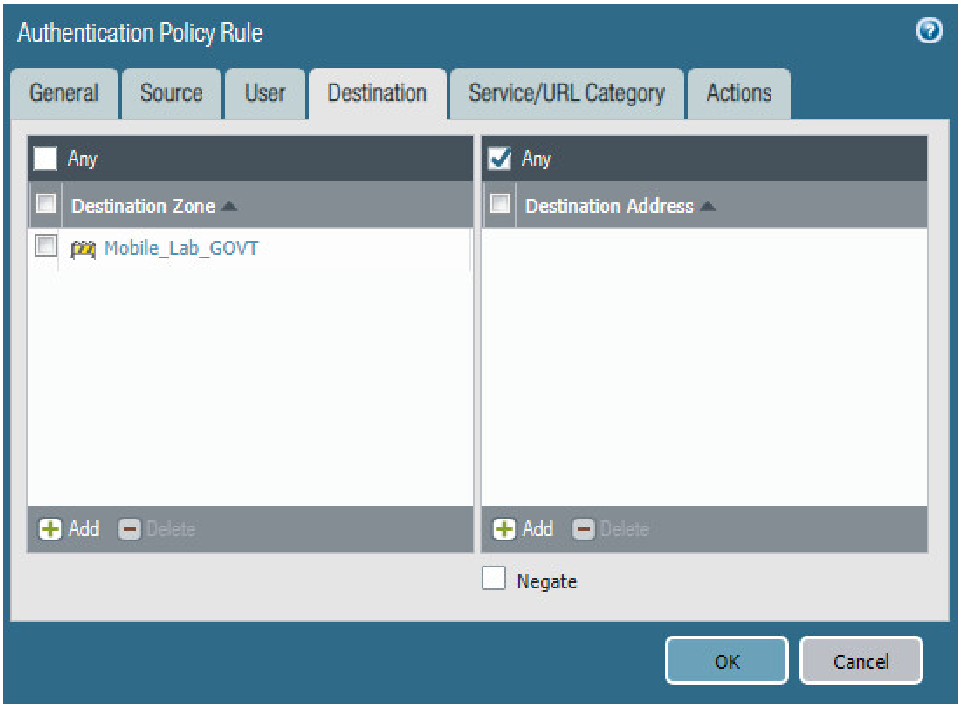
1. Navigate to **Policies** > **Authentication.**
2. Click **Add.**
3. Give the policy a name. In this implementation, **Mobile_Lab_Auth_Rule** was used.
4. Click **Source.**
5. Under Source Zone, click **Add.** Select the **SSL VPN** zone.
6. Under Source Zone, click **Add.** Select the **WAN** zone.

Figure 2-61 Authentication Policy Source Zones



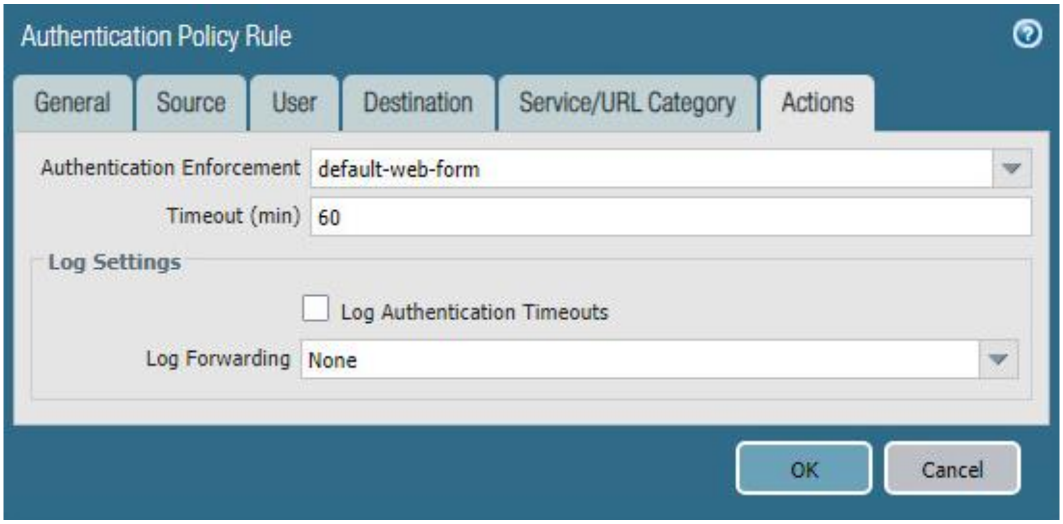
7. Click **Destination.**
8. Under Destination Zone, click **Add.**
9. Select the **LAN** zone.

Figure 2-62 Authentication Policy Destination Zones



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



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

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

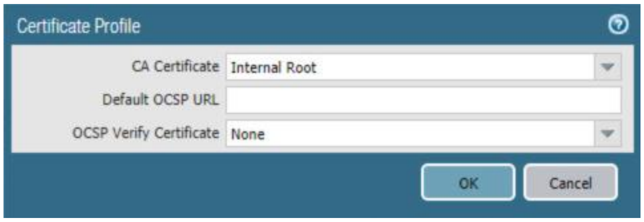
require certificate-based identification and authentication. This sample implementation uses certificates for the following systems:

- 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

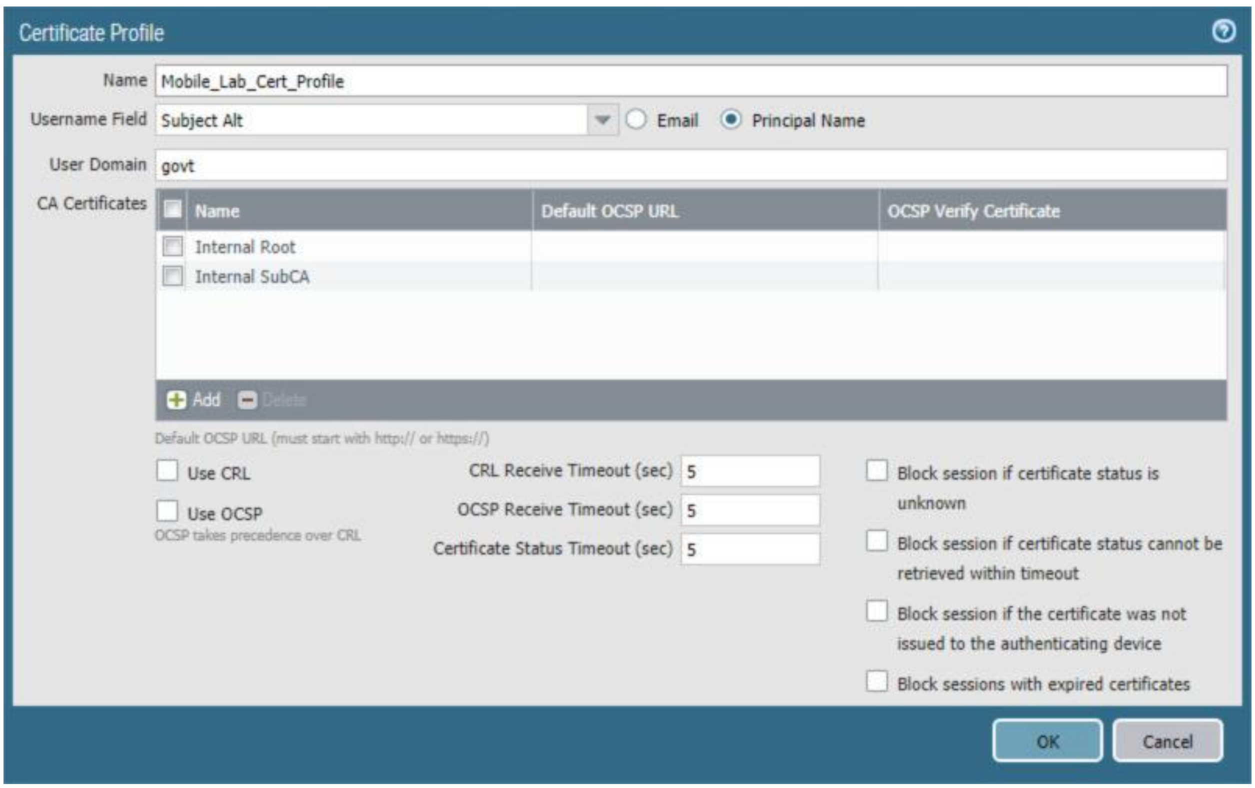
1. In the **Palo Alto Networks Portal,** navigate to **Device > Certificate Management > Certificate Profile.**
2. Under the details pane, select **Add;** the **Certificate Profile** form will open.
3. In the **Certificate Profile** form:
    a. In the **Name** field, enter a unique name to identify 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



4. Select **OK.**

Figure 2-66 Certificate Profile



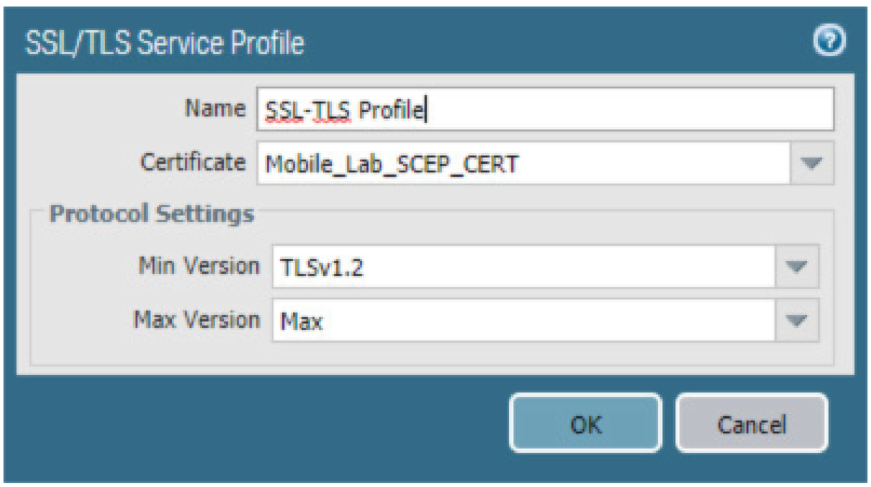
2.5.11 Configure SSL/TLS Service Profile

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

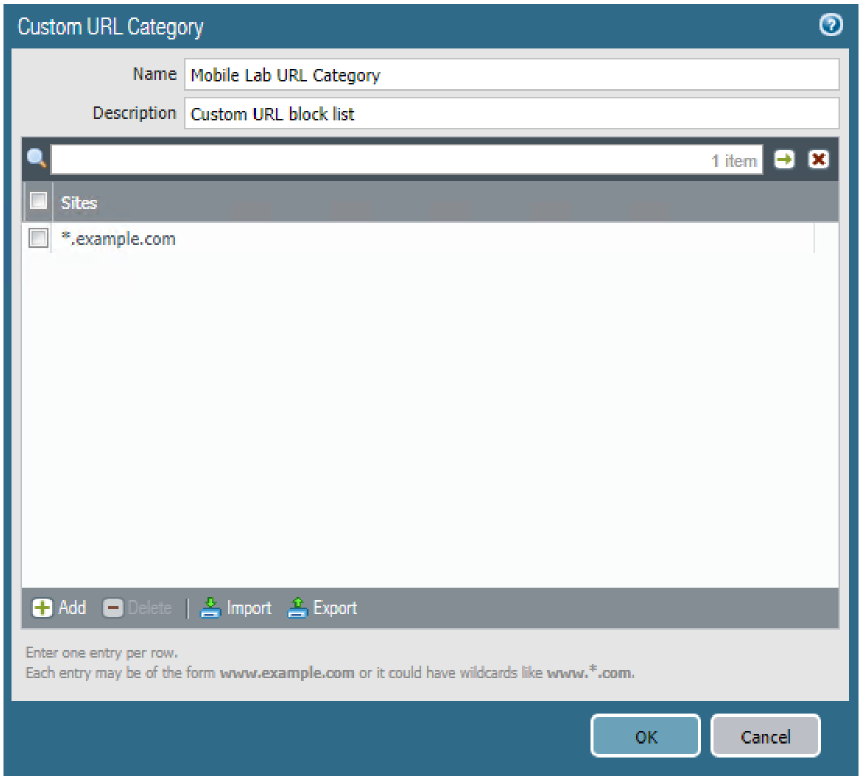


4. Repeat **Step 3** to add an identical SSL/TLS service profile for this appliance's server certificate issued through DigiCert.

2.5.12 URL Filtering Configuration

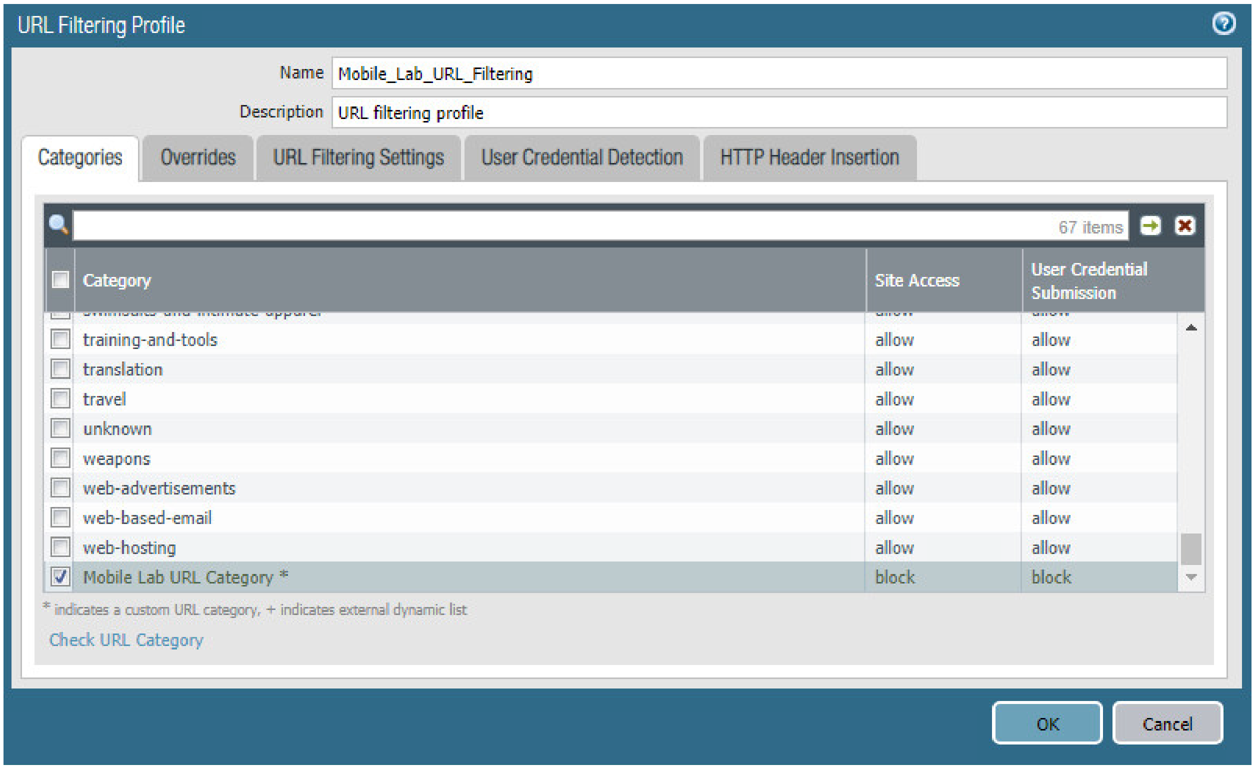
1. Navigate to **Objects > Custom Objects > URL Category.**
2. Click **Add.**
3. Give the category a name and description.
4. Add sites to be blocked. For this example, ***.example.com** was used.

Figure 2-68 Custom URL Category



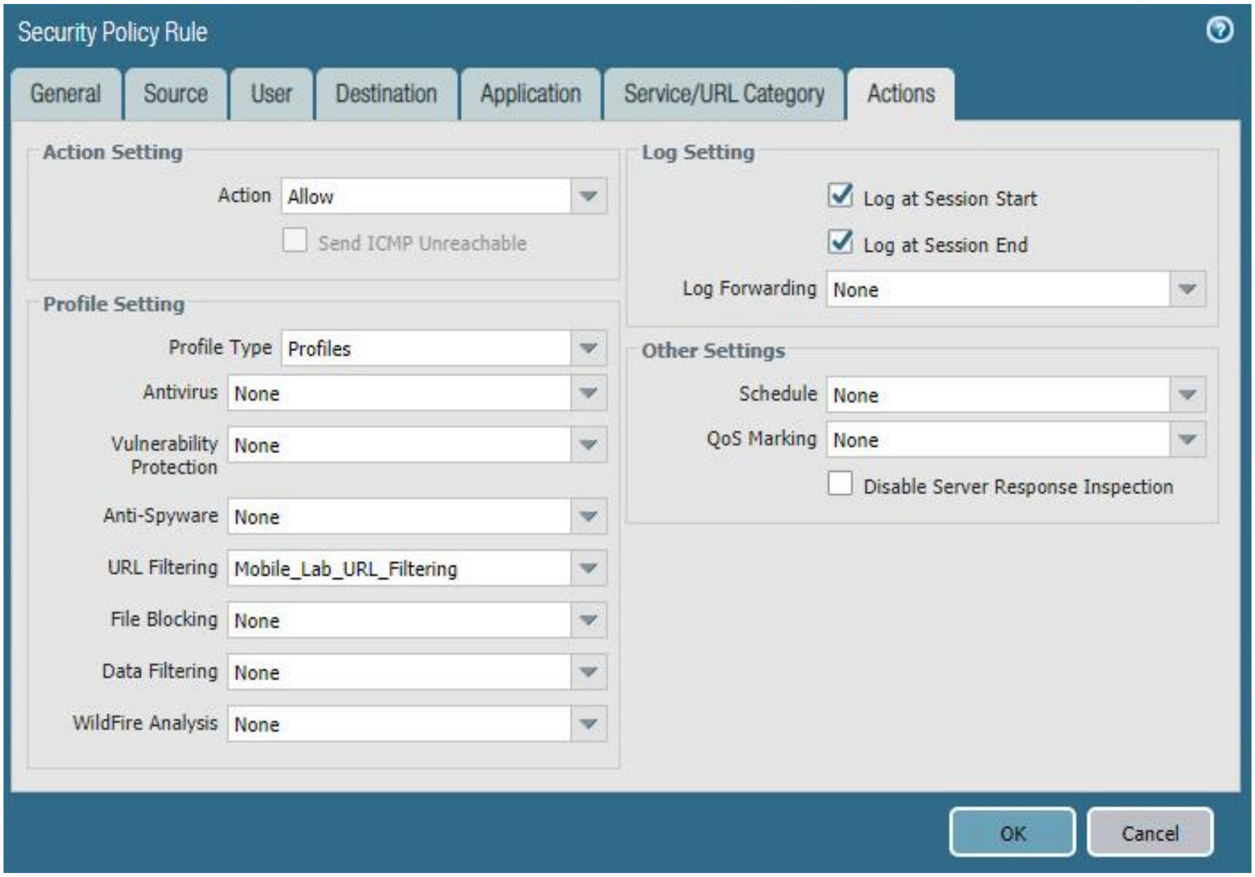
5. Click **OK.**
6. Navigate to **Objects > Security Profiles > URL Filtering.**
7. Check the box next to default and click **Clone.**
8. Select **default** from the window that appears.
9. Click **OK.**
10. Click the newly created profile, **default-1.**
11. Give the policy a meaningful name and description.
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



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



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.

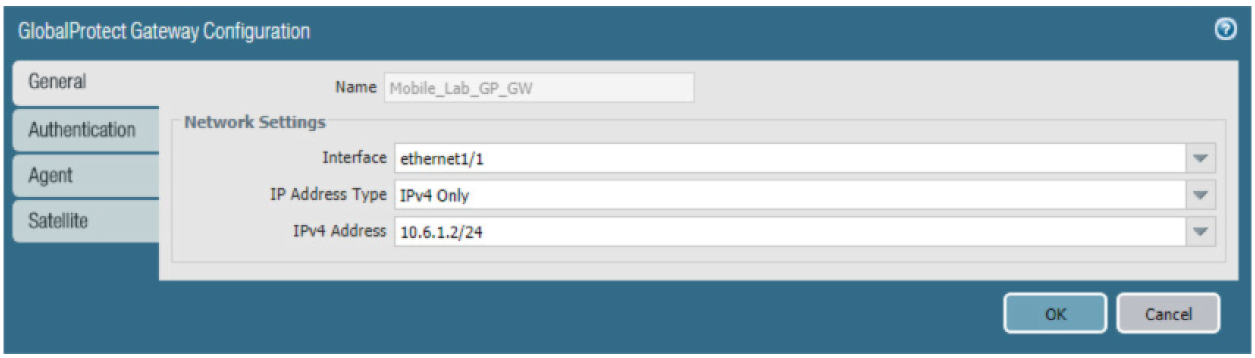
2.5.13.1 Configure GlobalProtect Gateway

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.

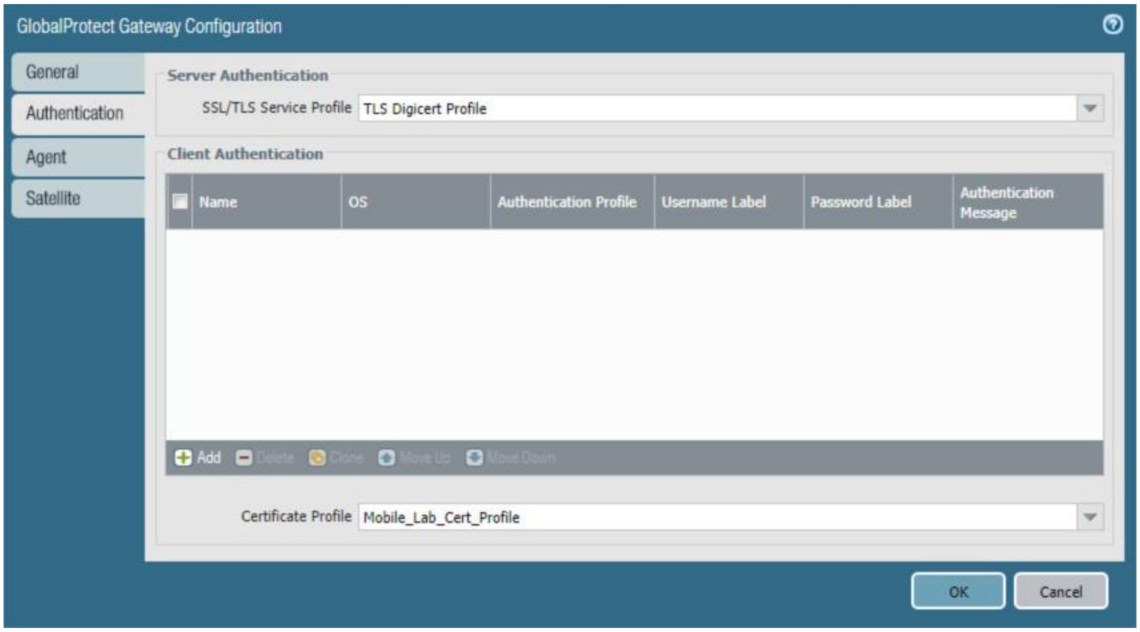
3. In the **GlobalProtect Gateway Configuration** form, on the **General** tab:
    a. In the **Name** field, enter a unique name to identify this GlobalProtect Gateway.
    b. Under **Network Settings**:
        i. In the **Interface** drop-down menu, select the physical interface connected to the subnet 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



    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



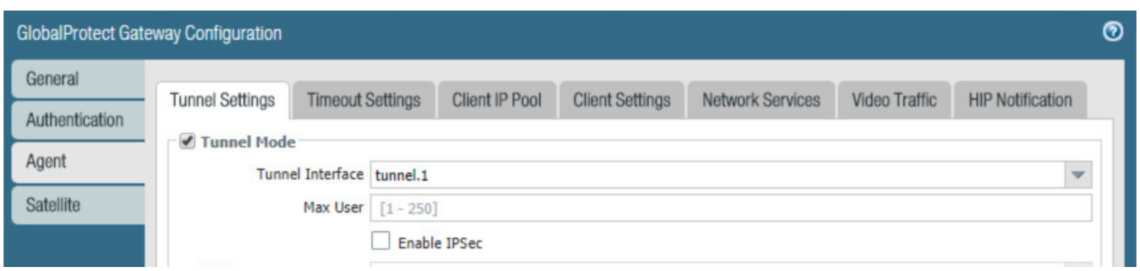
e. Select the **Agent** tab.

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



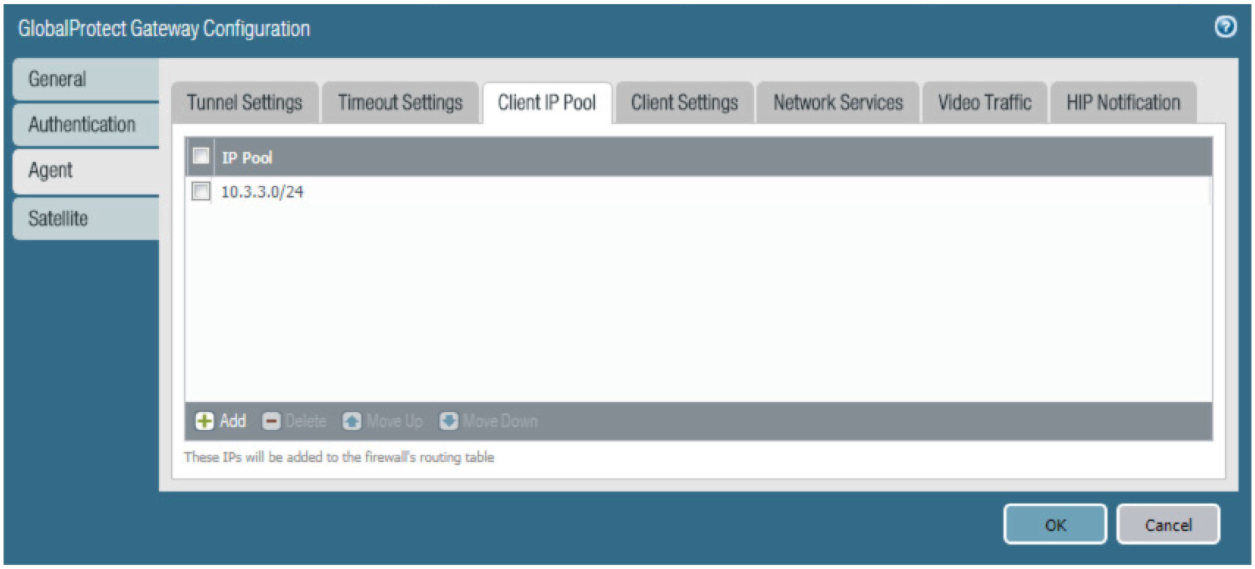
g. Select the **Agent > Client IP Pool** tab.

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

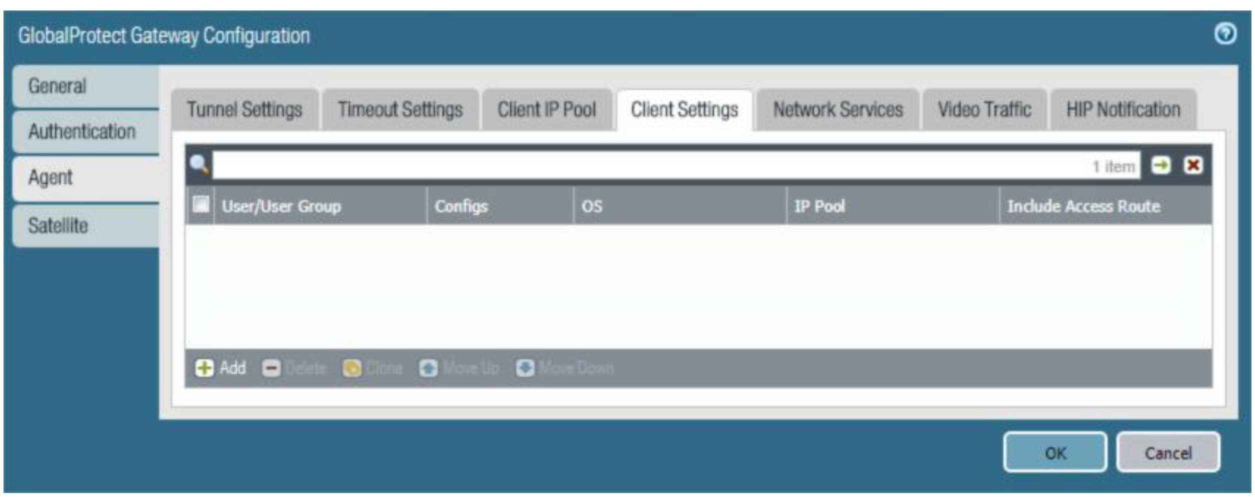


i. Select the **Agent > Client Settings** tab.

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

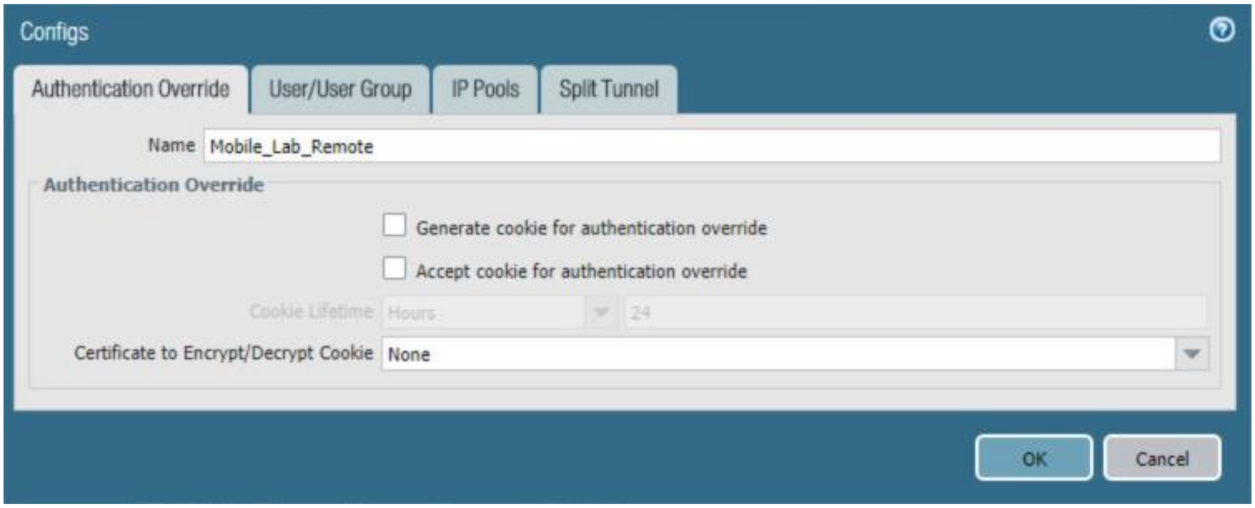
i. Under the **Client Settings** list box, select **Add;** the **Configs** form will open.

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



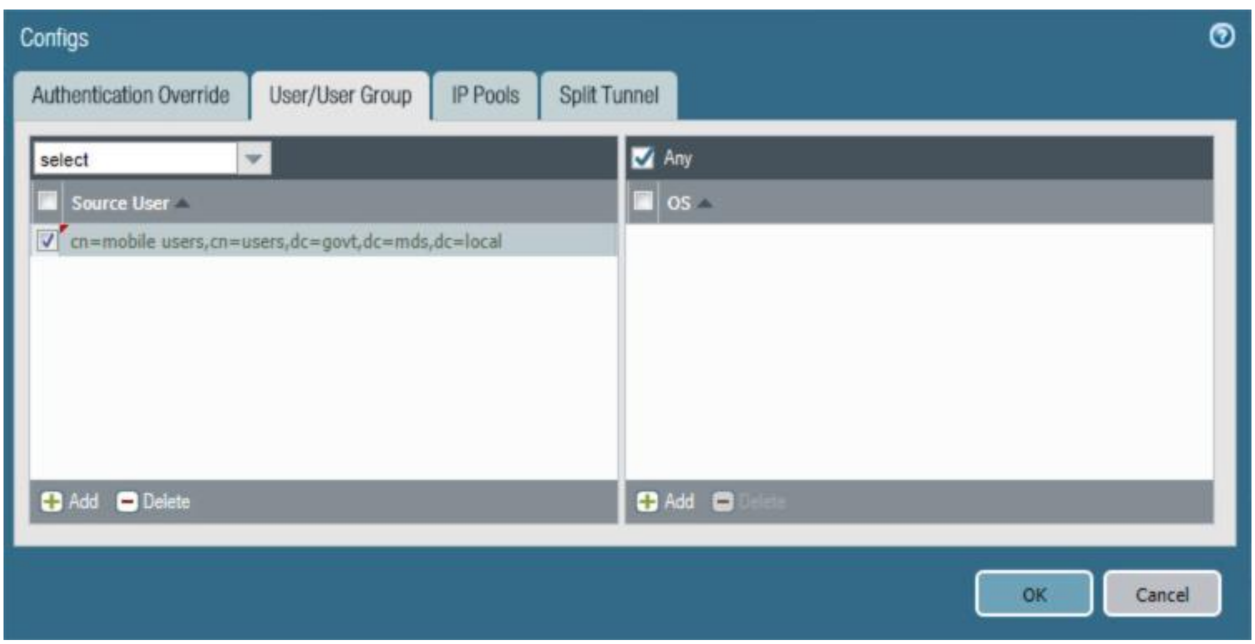
iii. Select the **User/User Group** tab.

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



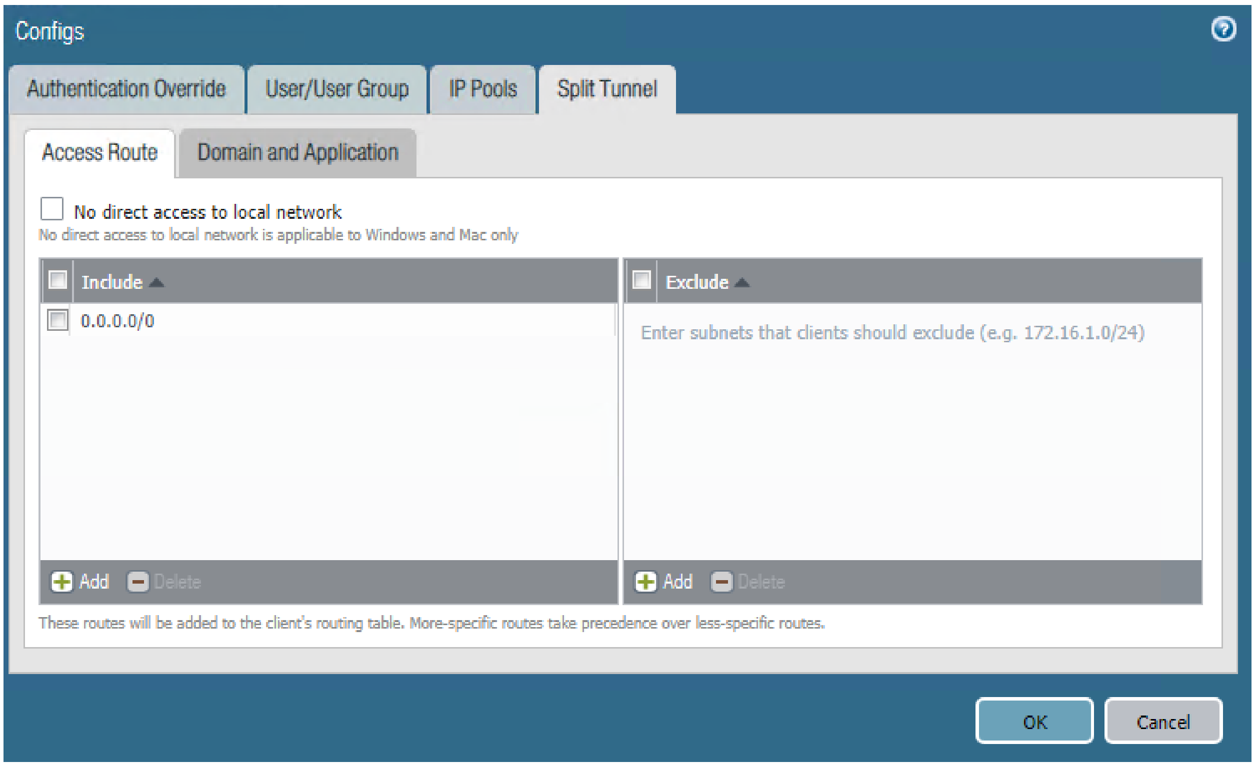
v. Select the **Split Tunnel** tab.

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



vii. Select **OK.**

k. Select **OK.**

2.5.13.2 Configure GlobalProtect Portal

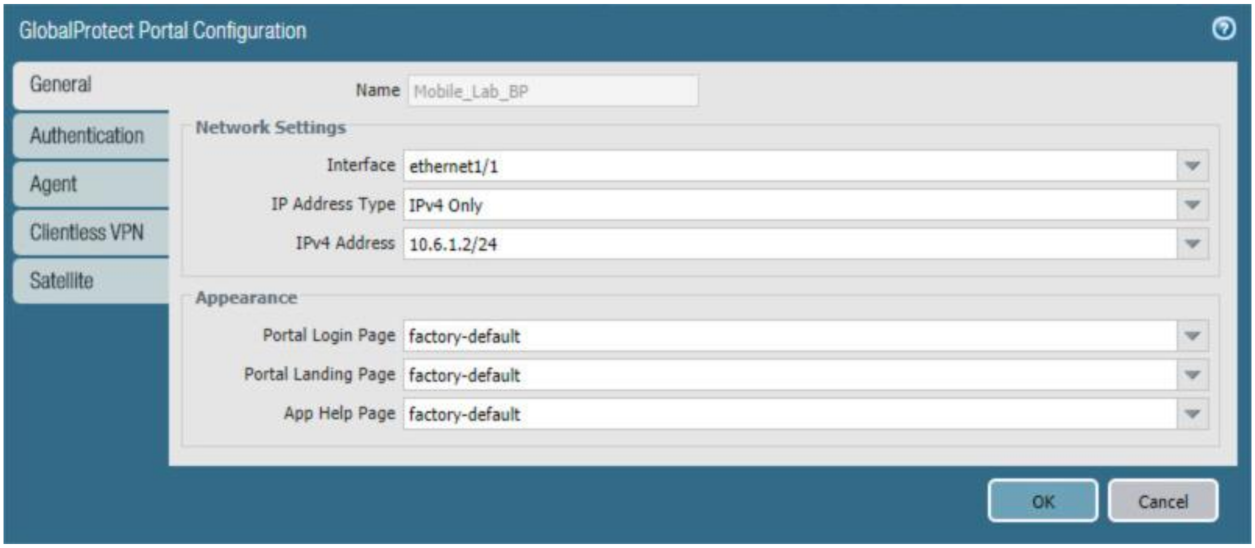
1. In the **Palo Alto Networks Portal**, navigate to **Network > GlobalProtect > Portal.**
2. Below the details pane, select **Add;** the **GlobalProtect Portal Configuration** form will open.
3. In the **GlobalProtect Portal Configuration** form, on the **General** tab:

   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



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.

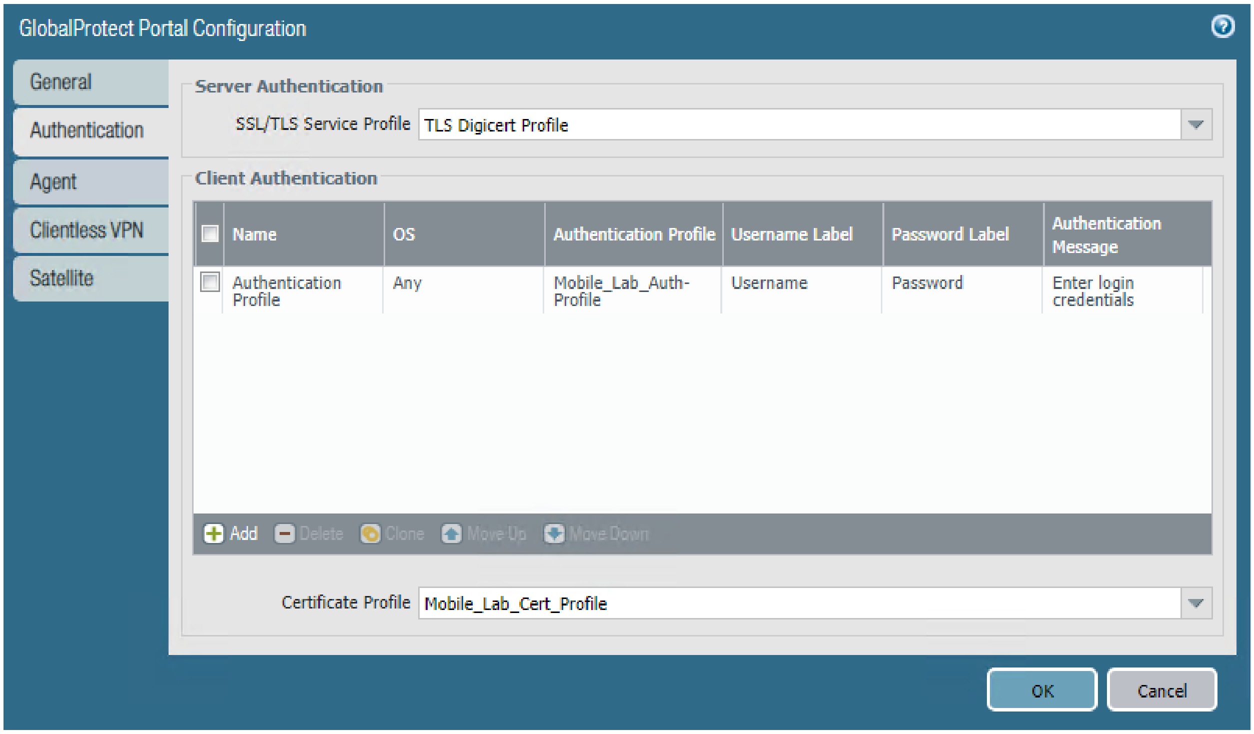
    c. Click **Add.**

    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



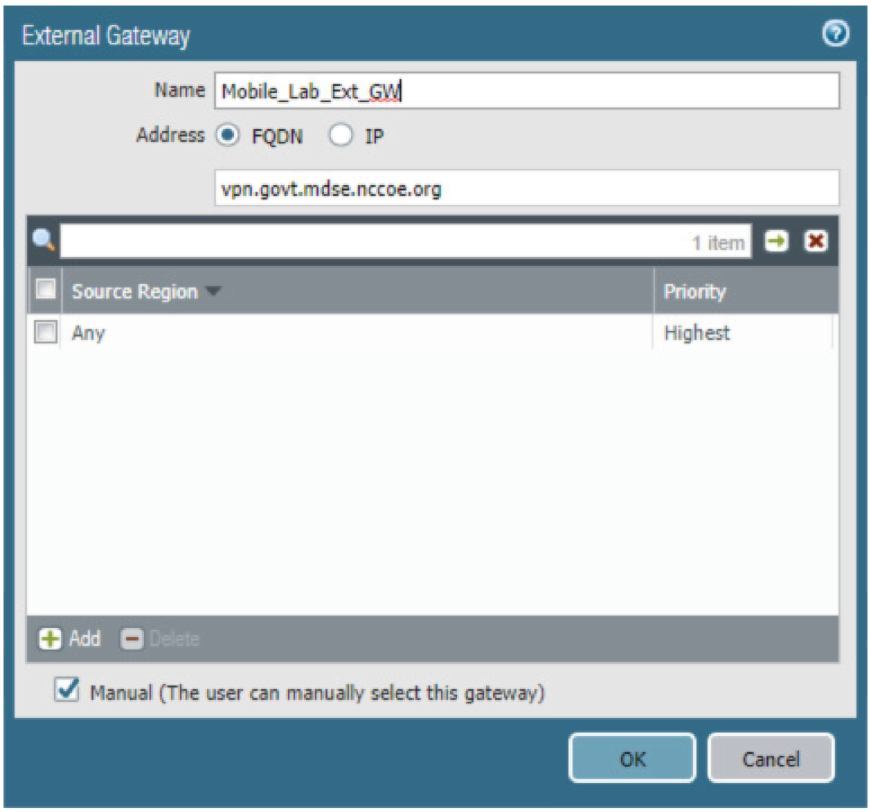
6. Select the **Agent** tab.
7. On the **Agent** tab:
   a. Below the **Agent** list box, select **Add;** the Configs form will open.
   b. In the **Configs** form:
      i. In the **Authentication** tab, below **Components that Require Dynamic Passwords,** check the box next to **Portal.**
      ii. 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



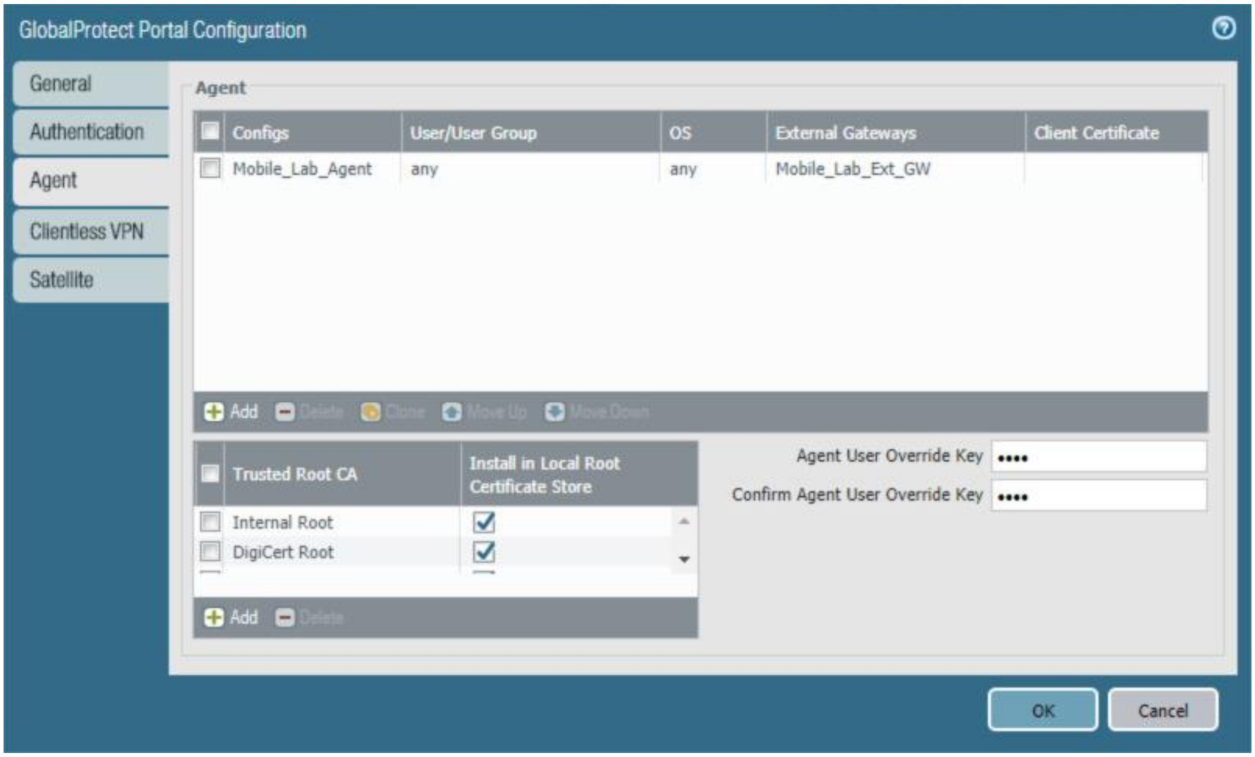
iv. Below the **Trusted Root CA** list box, select **Add;** a new list item will appear.

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



d. Select **OK.**

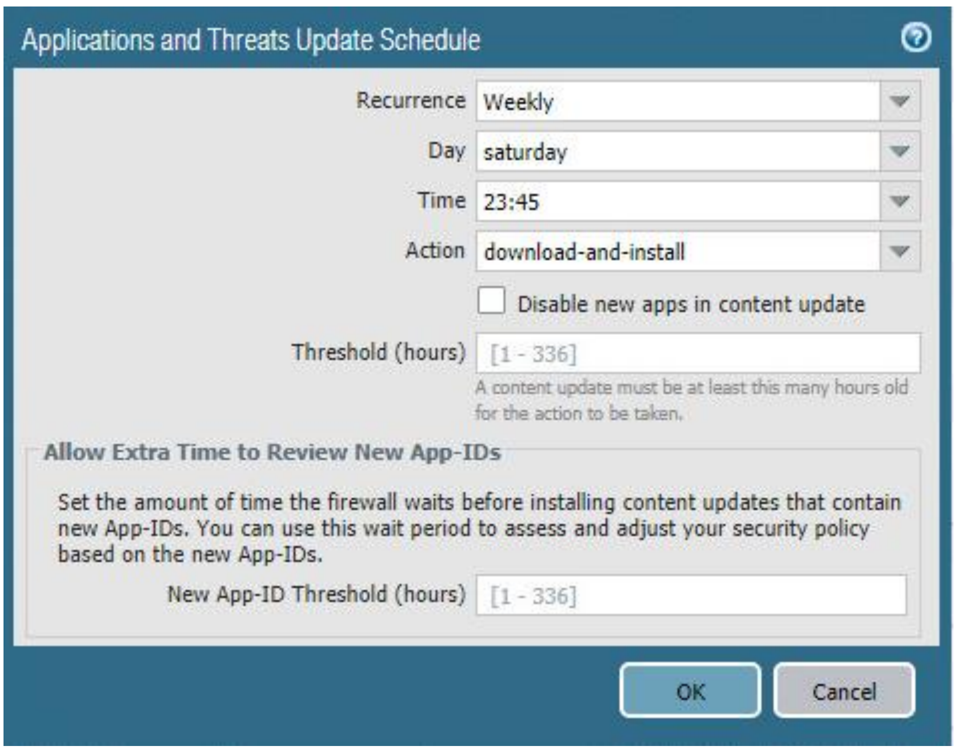
2.5.14 Configure Automatic Threat and Application Updates

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

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



12. Click **OK.**
13. Commit the changes.

2.6 Integration of Kryptowire EMM+S with MobileIron

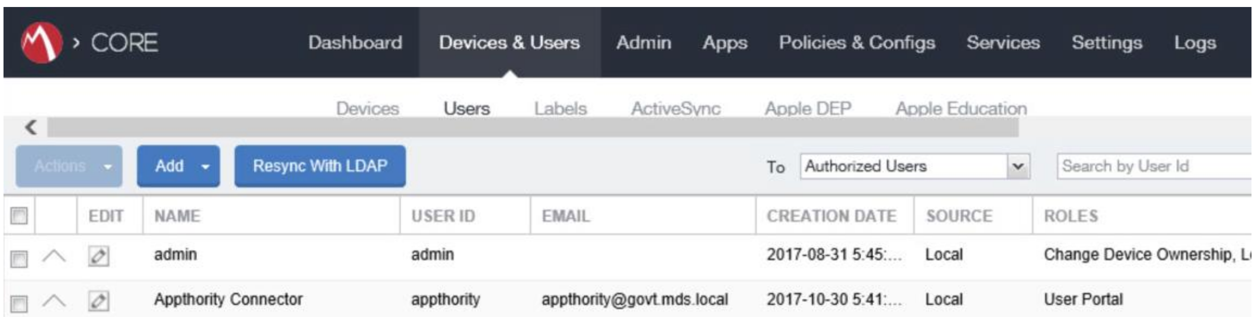
Kryptowire's application vetting service uses the MobileIron application programming interface (API) to regularly pull current device application inventory information from MobileIron Core. Updated analysis results are displayed in the Kryptowire portal.

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.

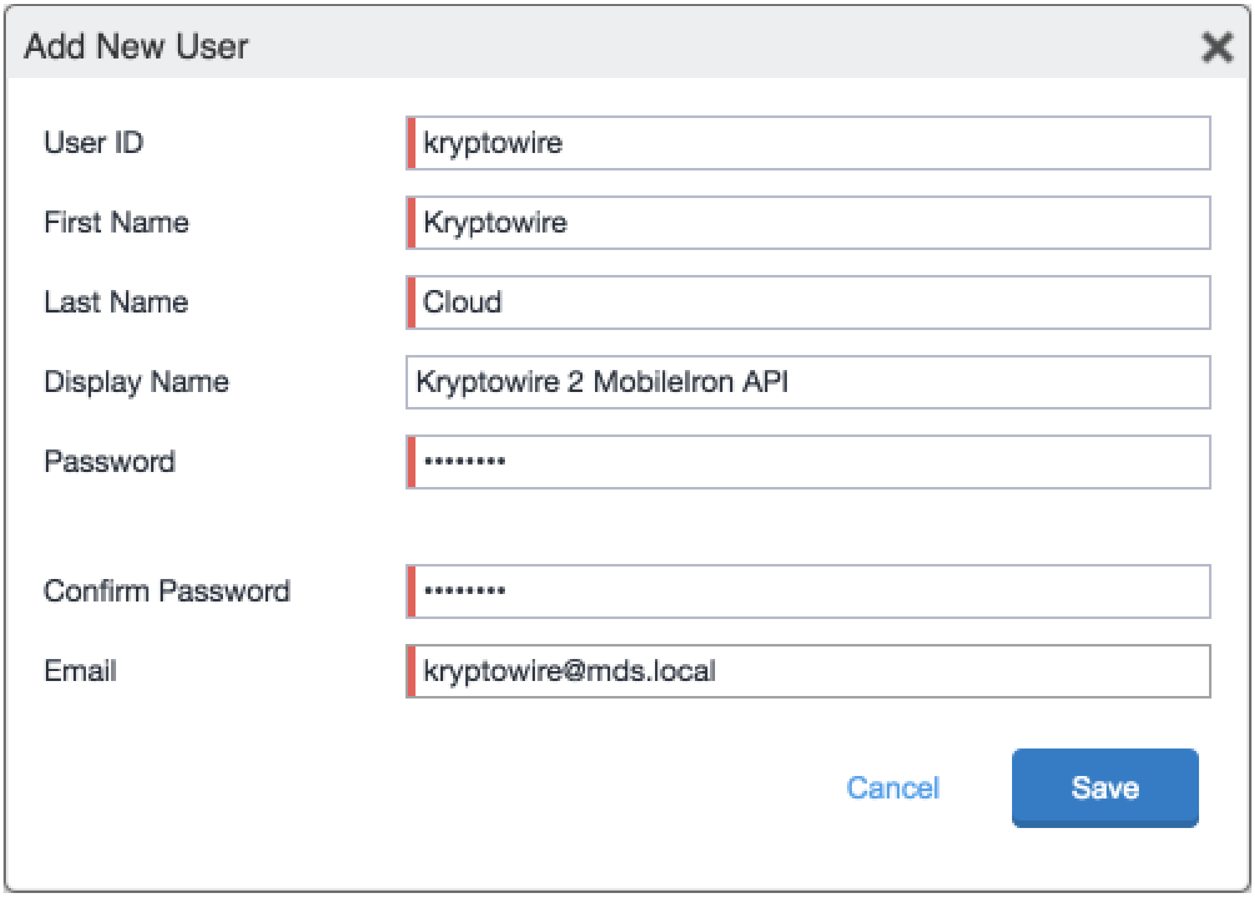
1. In the **MobileIron Admin Portal,** navigate to **Devices & Users > Users.**
2. On the **Users** page:
   a. Select **Add > Add Local User;** the Add New User dialogue will open.

Figure 2-85 MobileIron Users



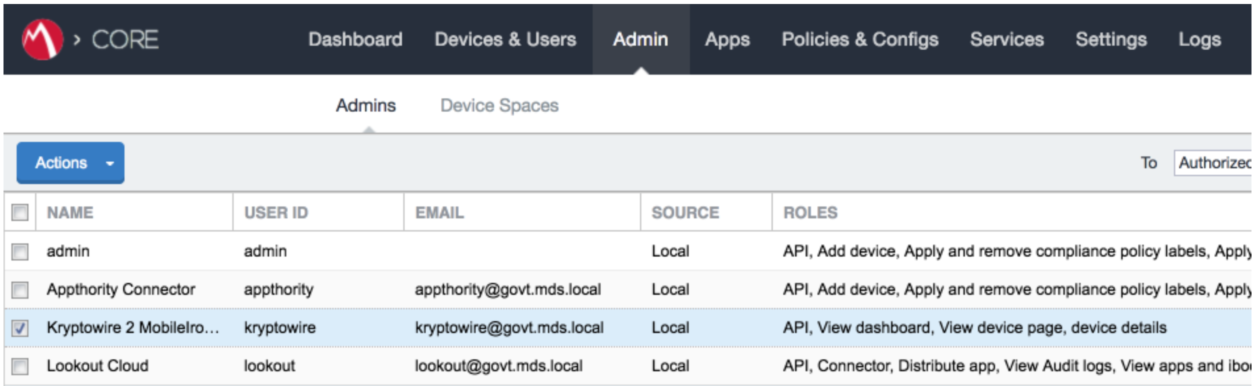
   b. In the **Add New User** dialogue:
      i. In the **User ID** field, enter the user identity that the Kryptowire cloud will authenticate under; our implementation uses a value of **kryptowire.**
      ii. In the **First Name** field, enter a generic first name for **Kryptowire**.
      iii. In the **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



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.

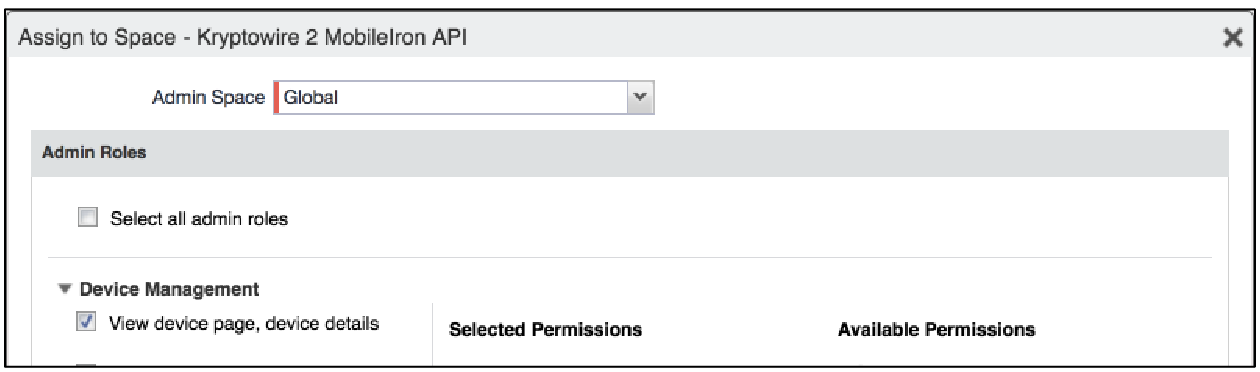
Figure 2-87 MobileIron User List



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



ii. Enable each of the following settings:

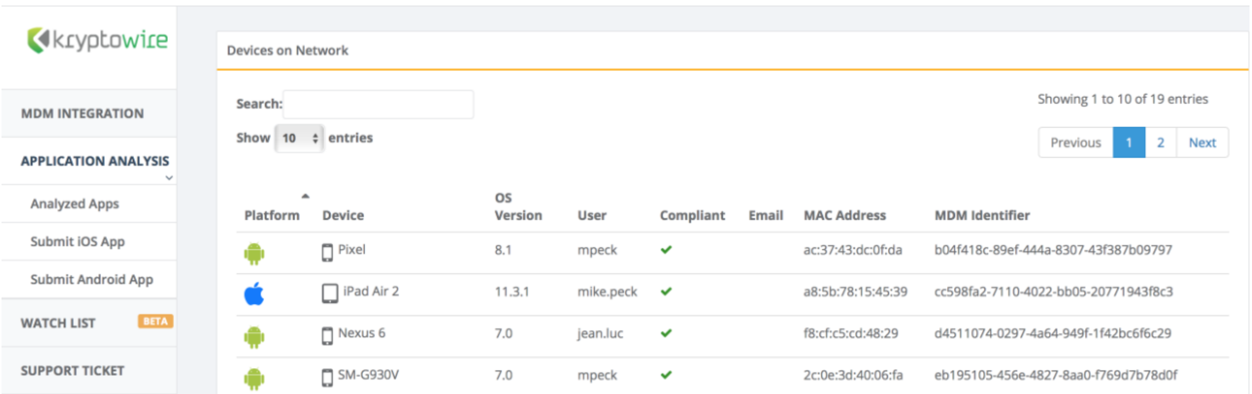
Admin Roles > Device Management > View device page, device details
Admin Roles > Device Management > View dashboard
Admin Roles > Privacy Control > View apps and ibooks in device details
Admin Roles > Privacy Control > View device IP and MAC address
Admin Roles > App Management > View app
Admin Roles > 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



2.7 Integration of Lookout Mobile Endpoint Security with MobileIron

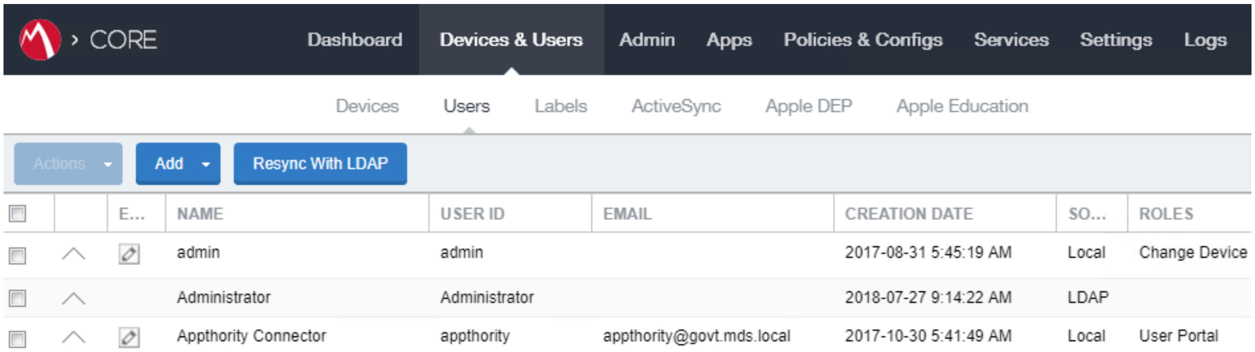
Lookout's Mobile Endpoint Security cloud service uses the MobileIron API to pull mobile device details and app inventory from MobileIron Core. Following analysis, Lookout uses the API to apply specific labels to devices to categorize them by the severity of any issues detected. MobileIron can be configured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



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.

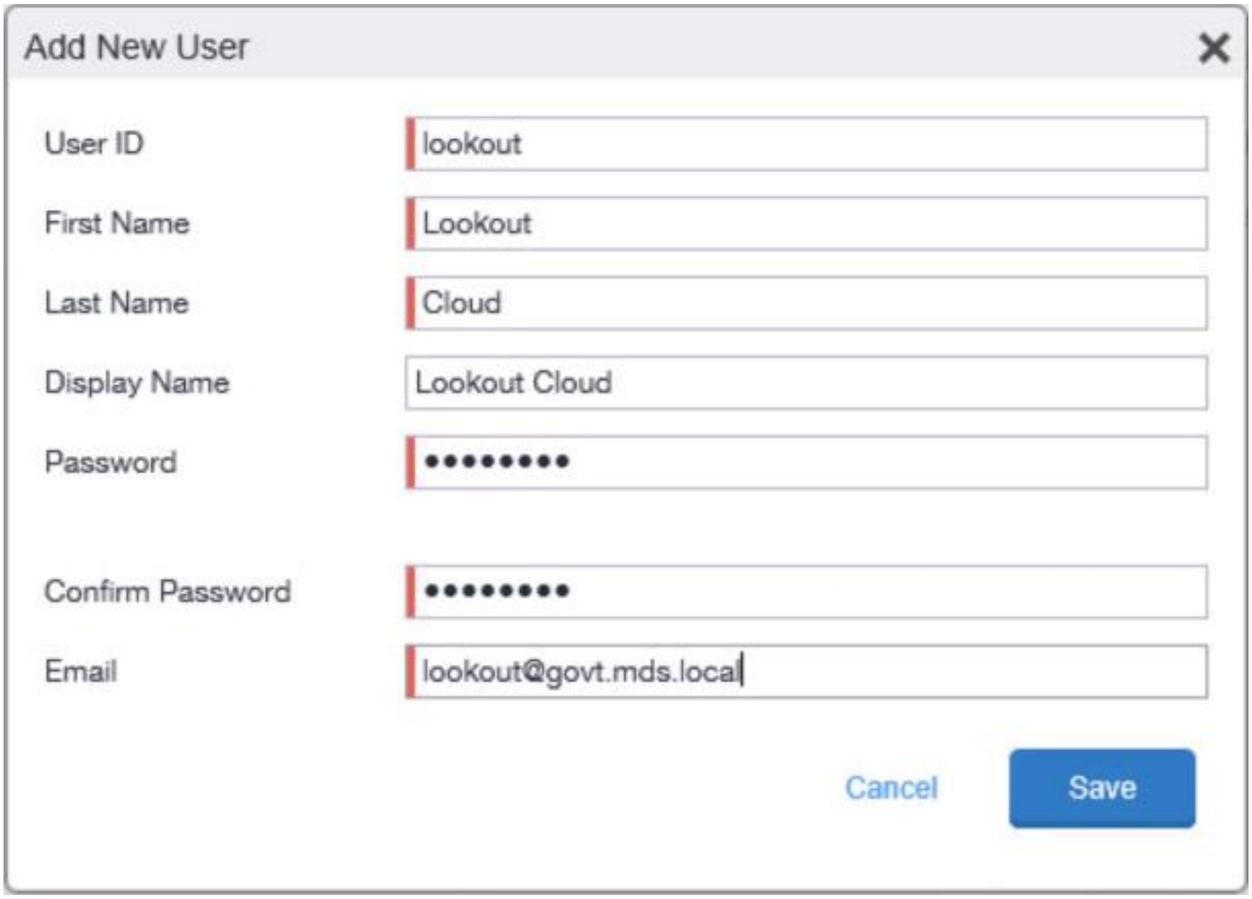
   v. In the **Password** field, provide the password the Lookout identity will use to authenticate to MobileIron.

   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.

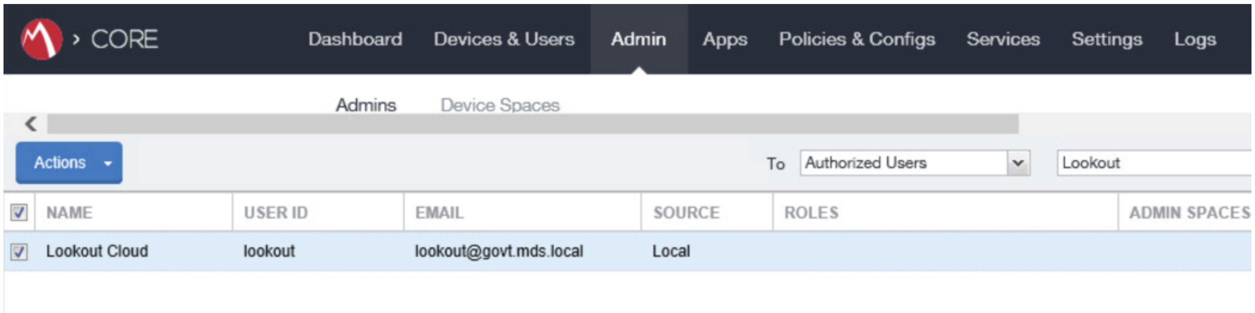
   viii. Select **Save**.

Figure 2-91 MobileIron Lookout User Configuration



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.

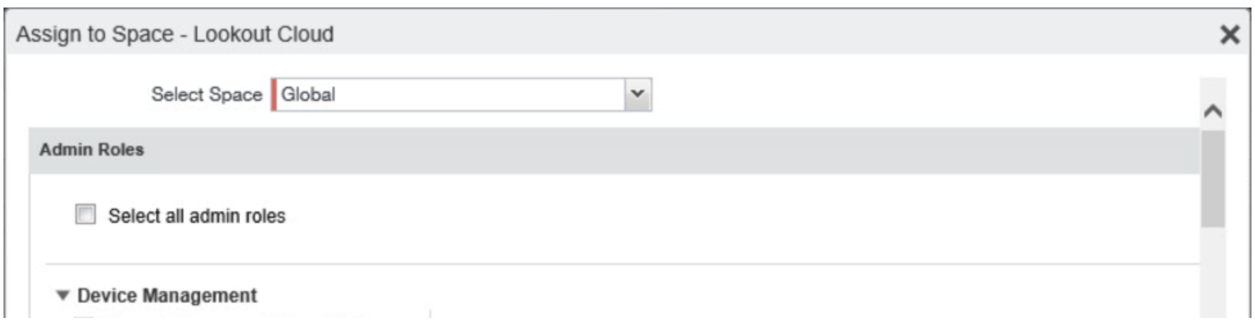
Figure 2-92 Lookout MobileIron Admin Account



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

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

Figure 2-93 Lookout Account Space Assignment



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

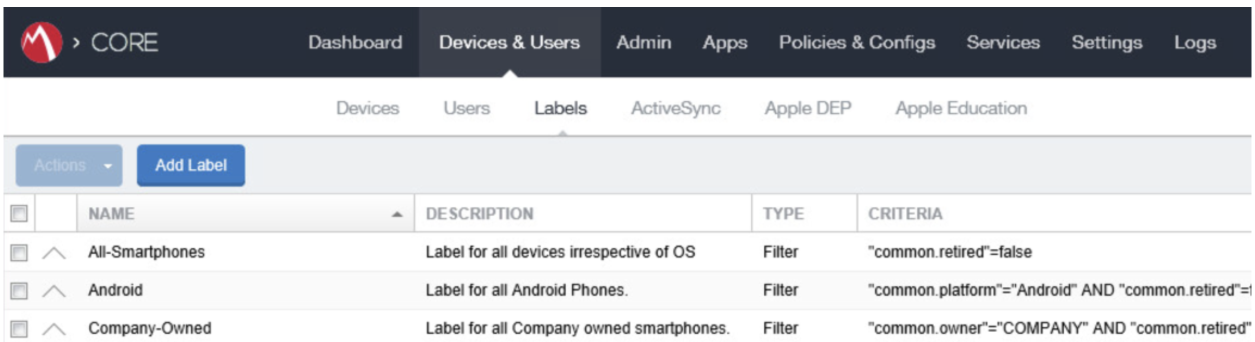
iii. Select **Save**.

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.

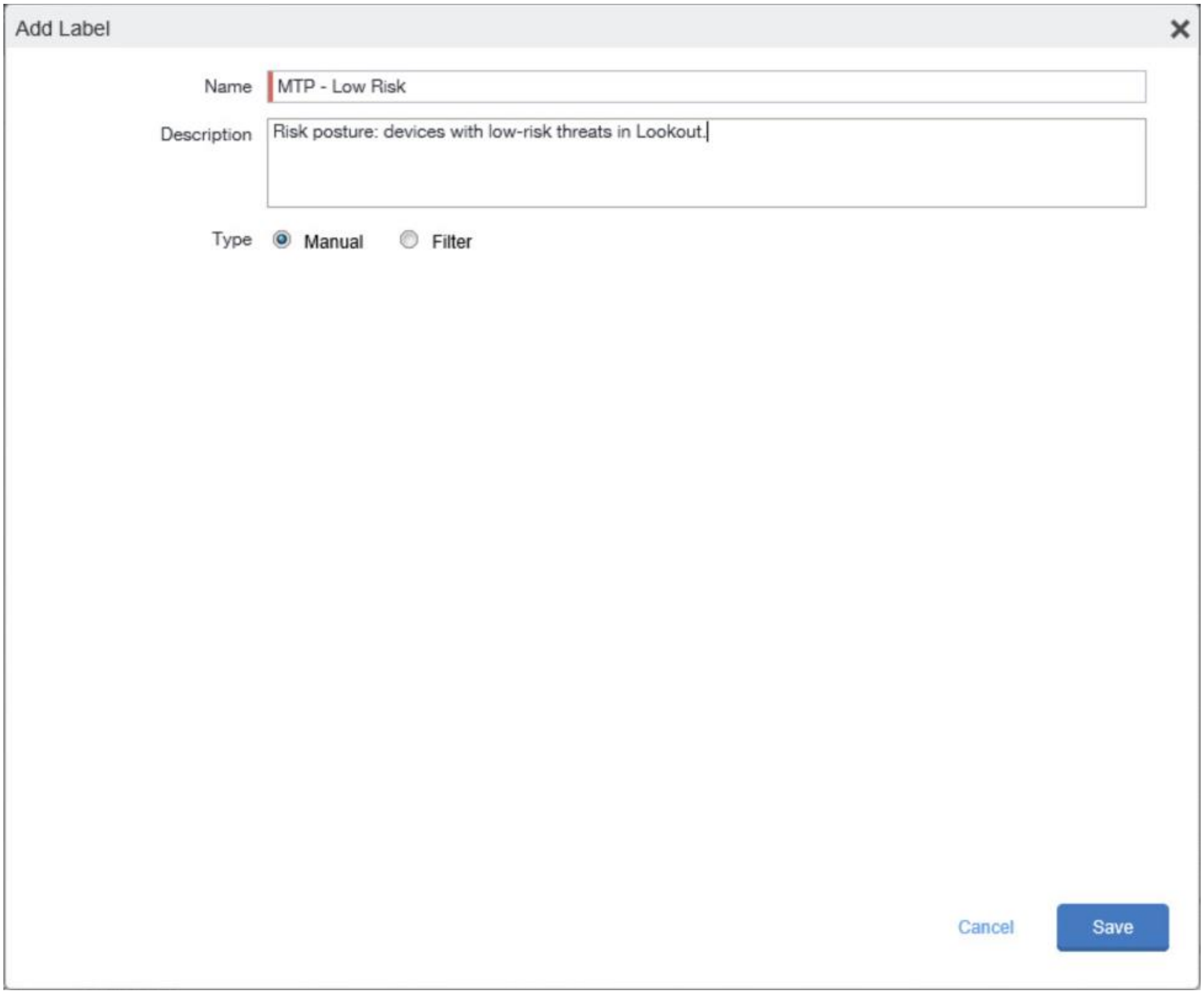
1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Labels**.
2. On the **Labels** page:
    a. Select **Add Label**; the **Add Label** dialogue will appear.

Figure 2-94 MobileIron Label List



    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**



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

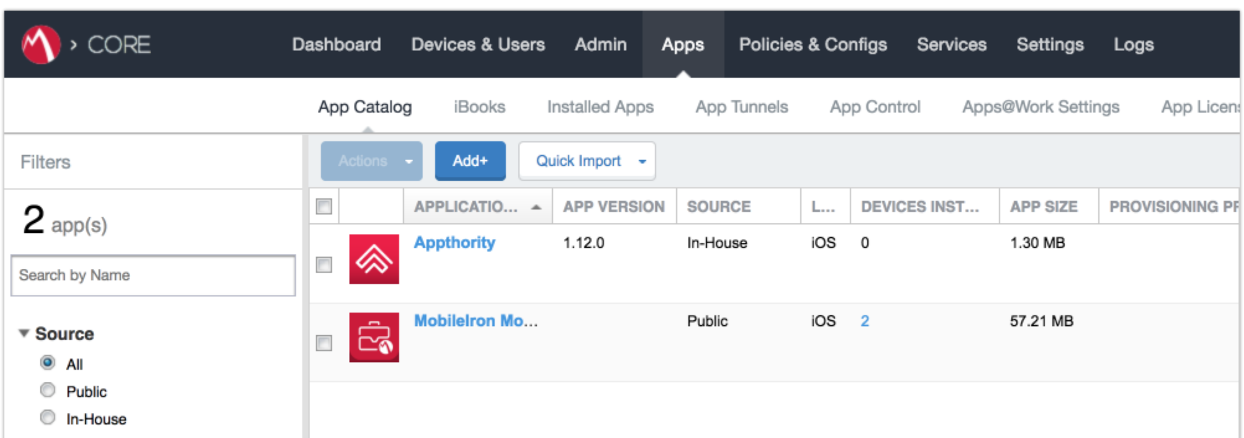
Note: Administrators can choose to alter the label names to something more appropriate for their environment.

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

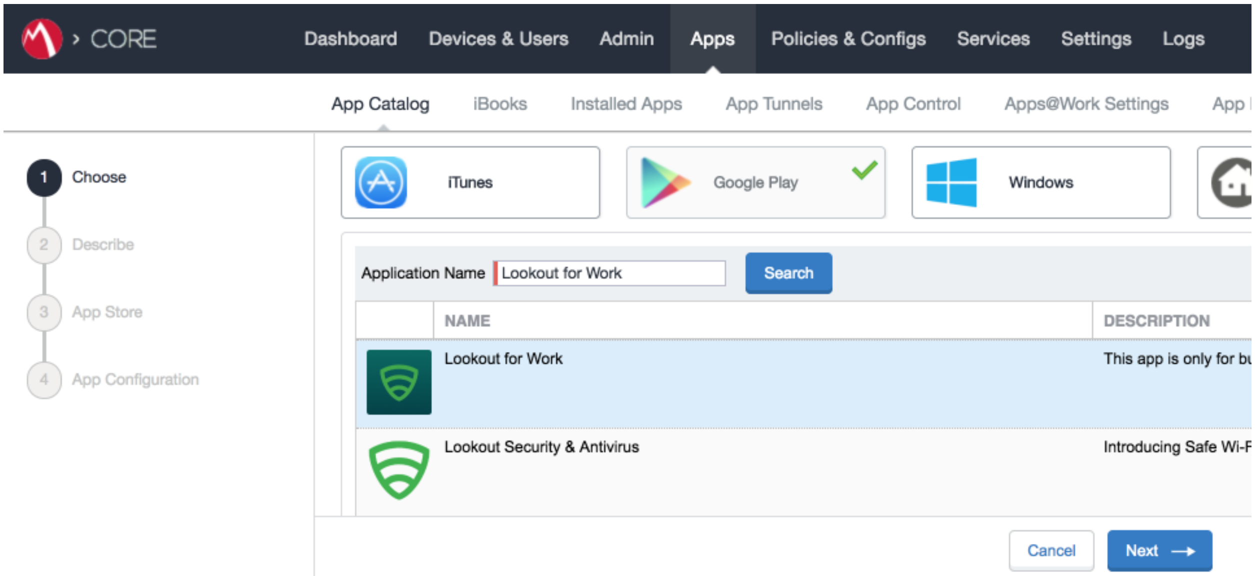


3. On the **App Catalog > Choose** page:
   a. Select **Google Play**; additional controls will be displayed.
   b. In the **Application Name** field, enter **Lookout for Work**.
   c. Select **Search**; search results will be displayed in the lower pane.

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

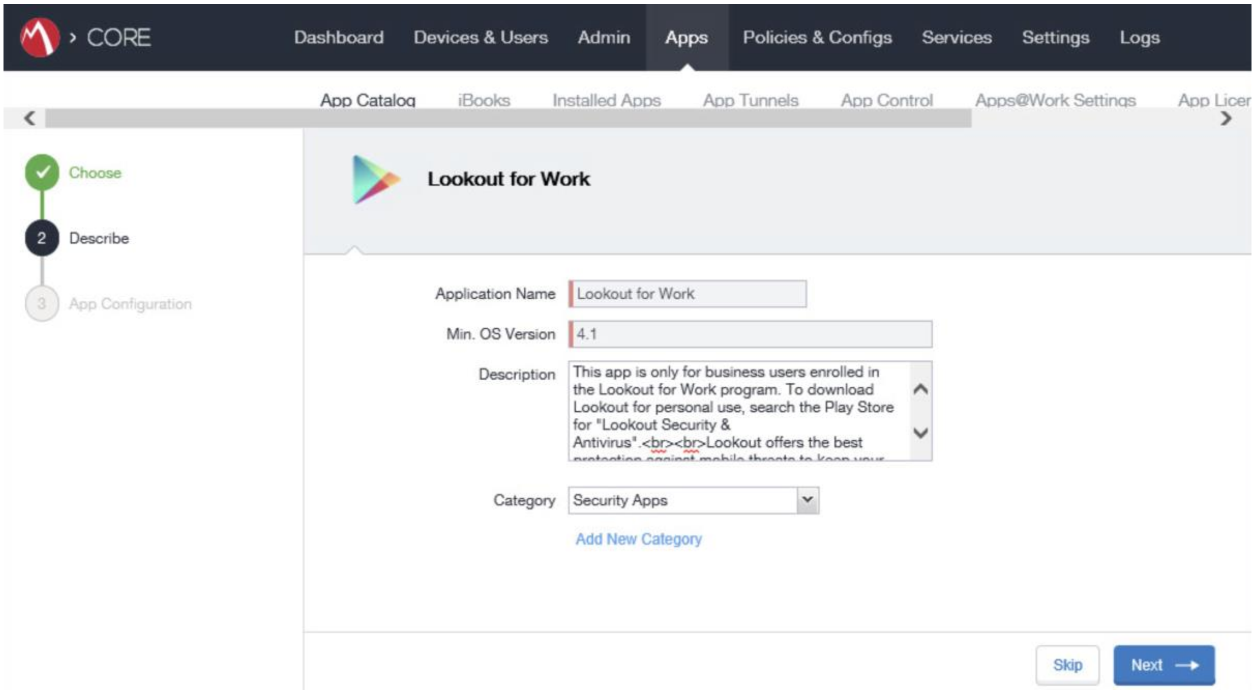


4. On the **App Catalog > Describe** page:

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

b. Select **Next.**

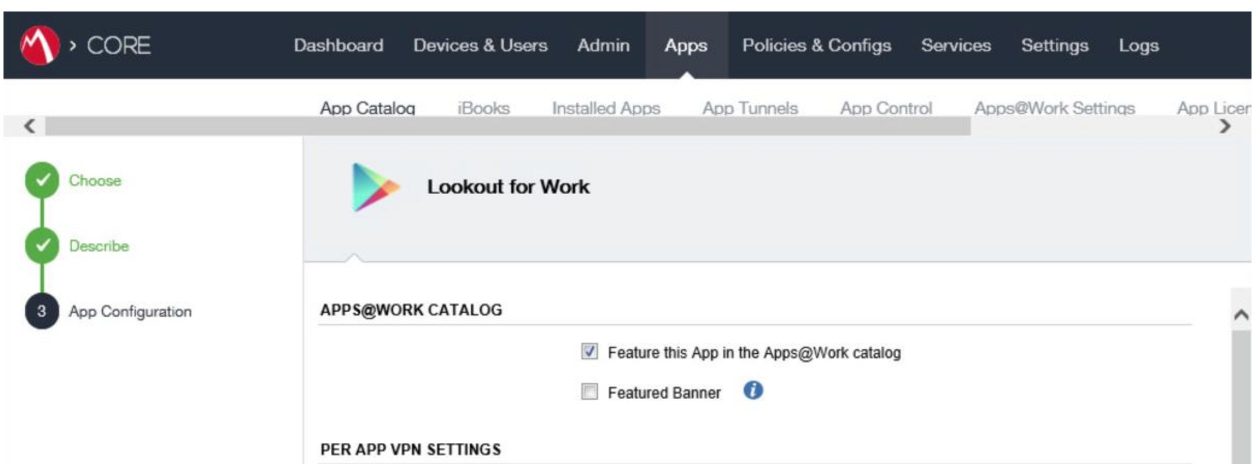
Figure 2-98 Lookout for Work Application Configuration



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



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

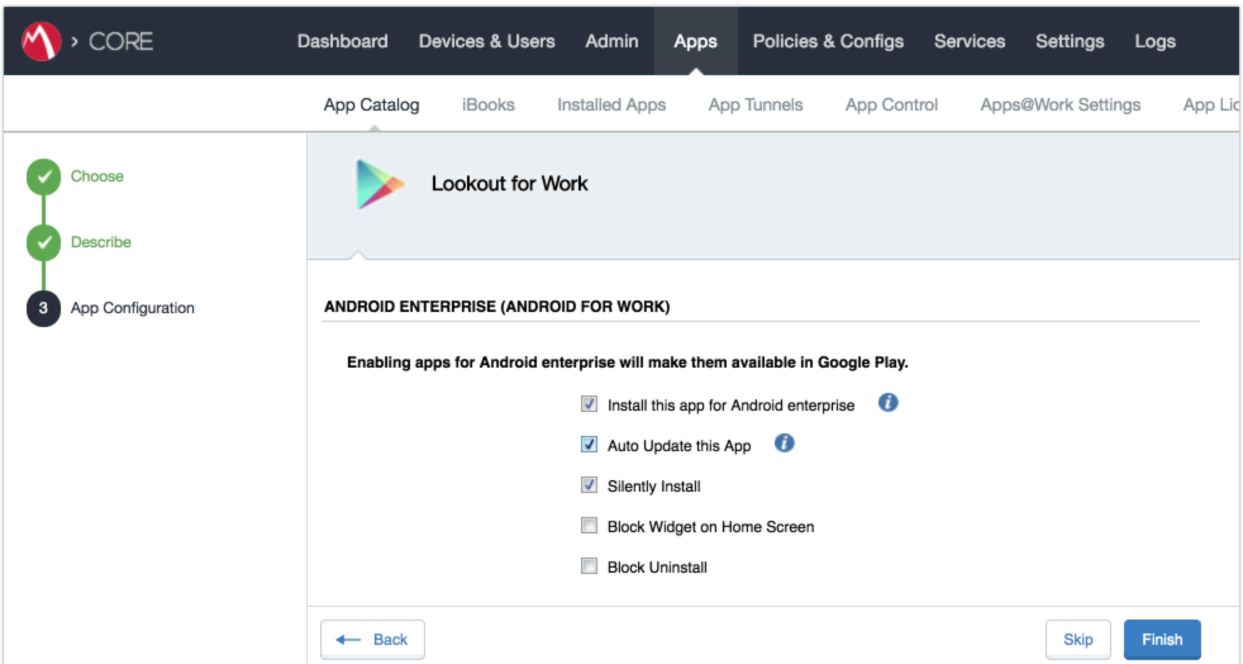
i. Enable **Install this app for Android enterprise**; additional controls will be made visible.

ii. Enable **Auto Update this App.**

iii. Ensure **Silently Install** is enabled.

c. Select **Finish.**

Figure 2-100 Lookout for Work AFW Configuration



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

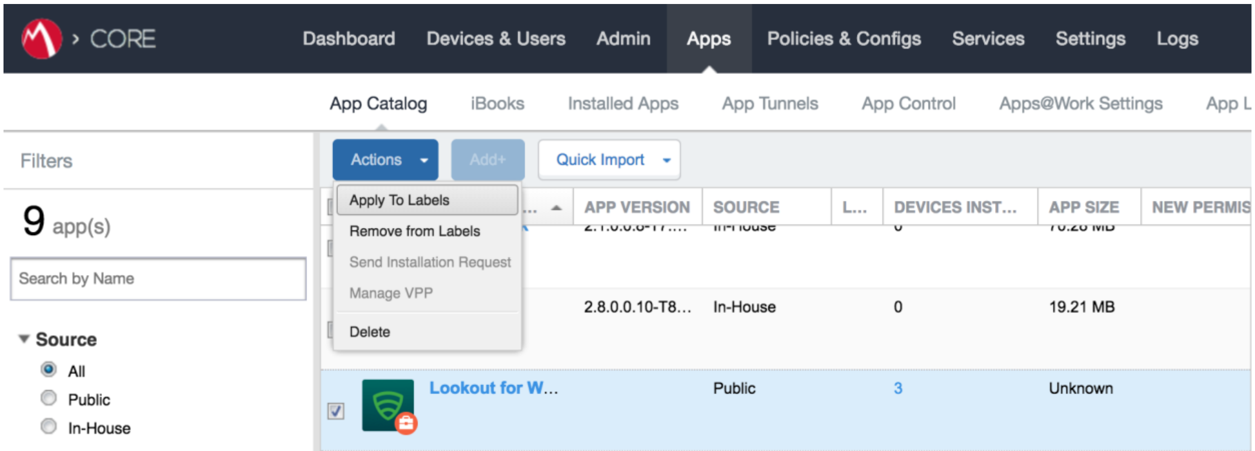
2.7.4 Apply Labels to Lookout for Work for Android

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

   a. Enable Lookout for Work.

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

1307 **Figure 2-101 Apply Lookout for Work to Android Devices**

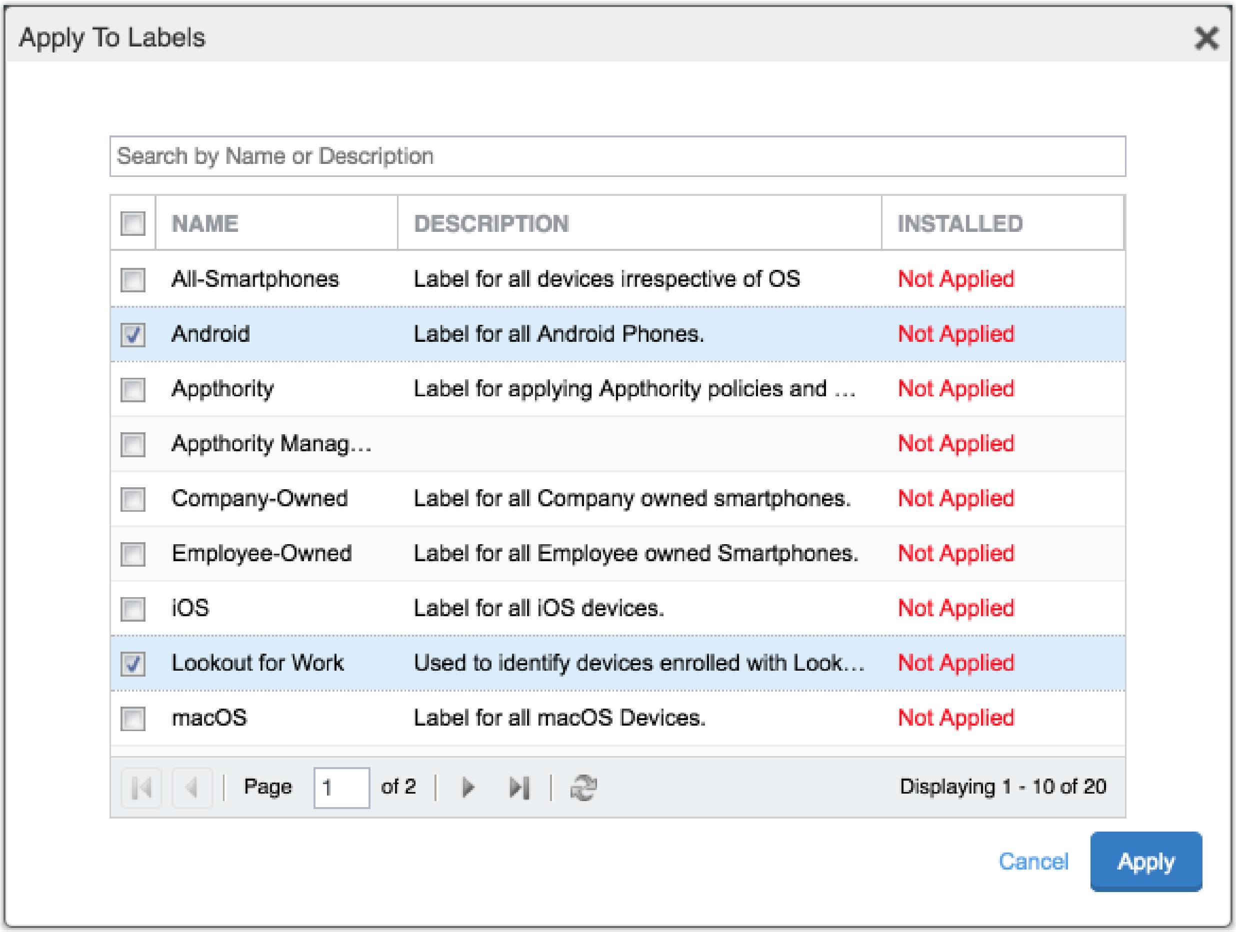


1308 c. In the **Apply To Labels** dialogue:

1309 i. Enable the **Lookout for Work** and **Android** labels, plus any other labels
1310 appropriate to your organization's mobile security policies.

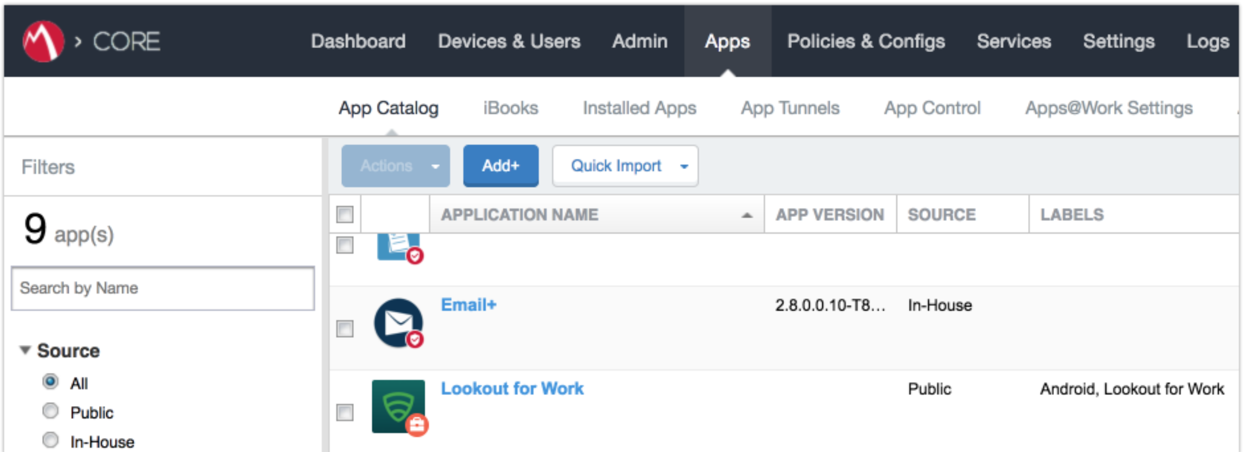
1311 ii. Select **Apply.**

Figure 2-102 Apply To Labels Dialogue



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

Figure 2-103 Lookout for Work with Applied Labels



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

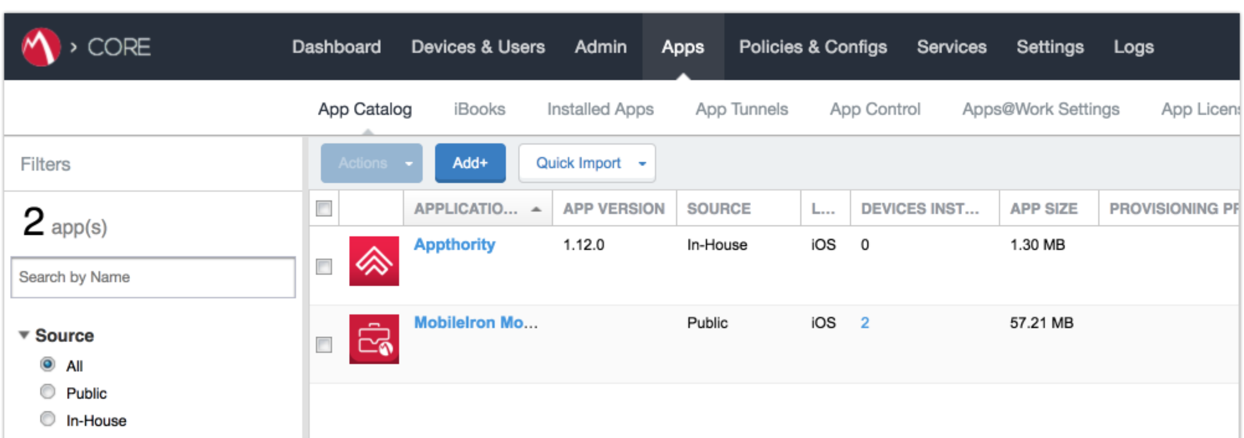
The following steps will add the Lookout for Work app for iOS to MobileIron, apply appropriate MobileIron labels, and create and upload a configuration file for one-touch activation of the app.

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



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

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

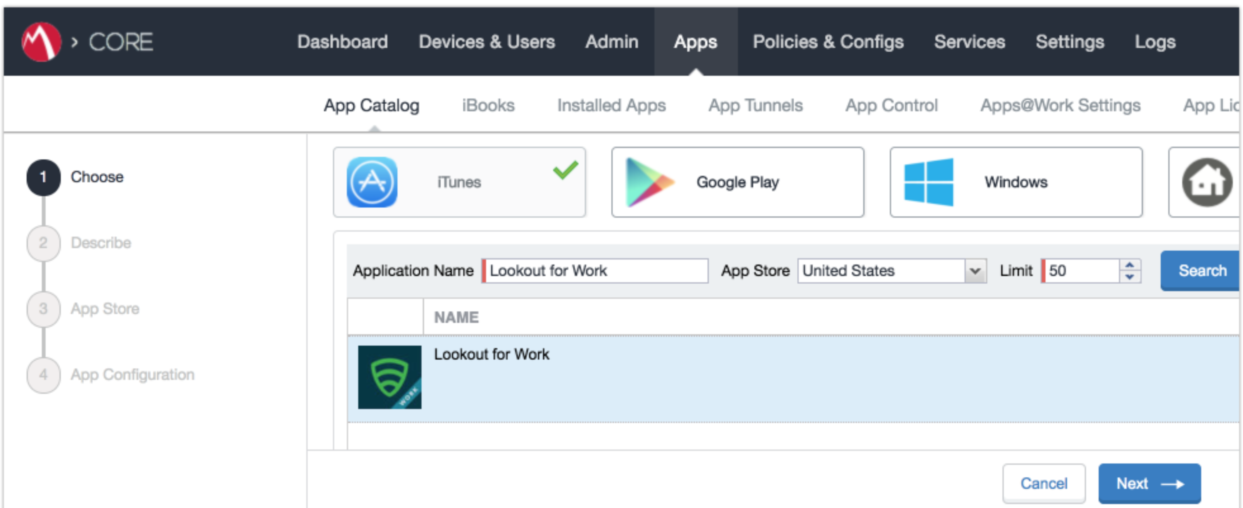
b. In the **Application Name** field, enter **Lookout for Work**.

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

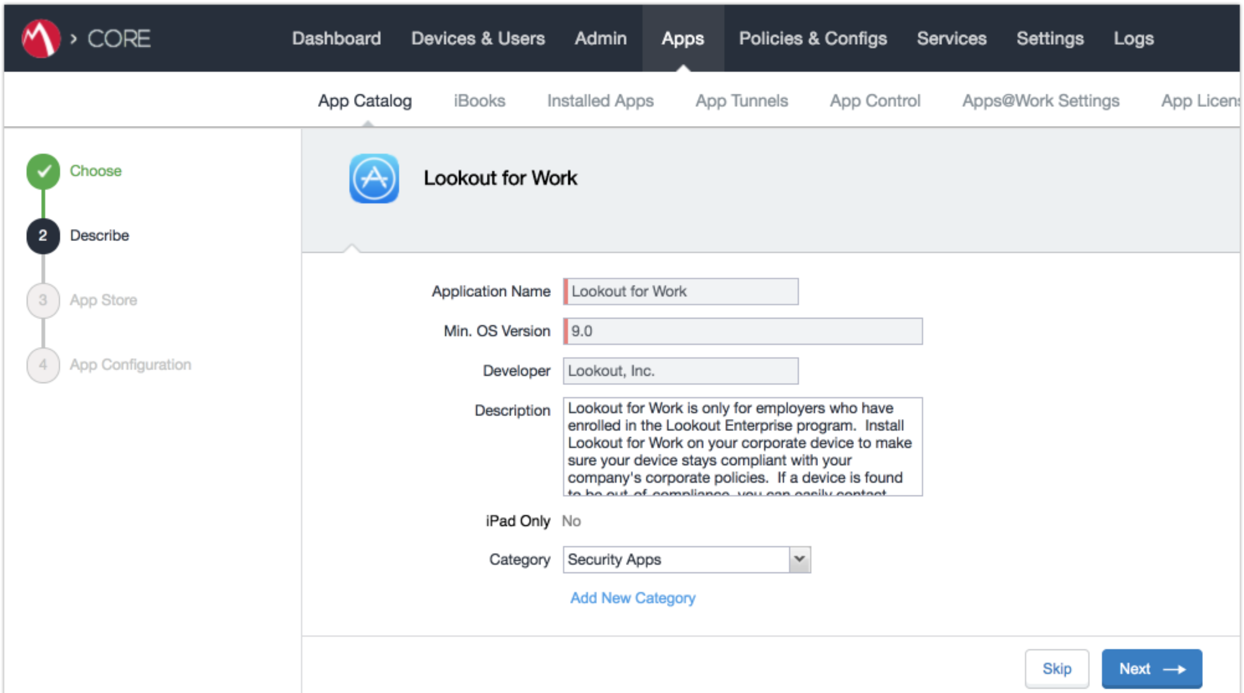


4. On the **App Catalog > Describe** page:

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

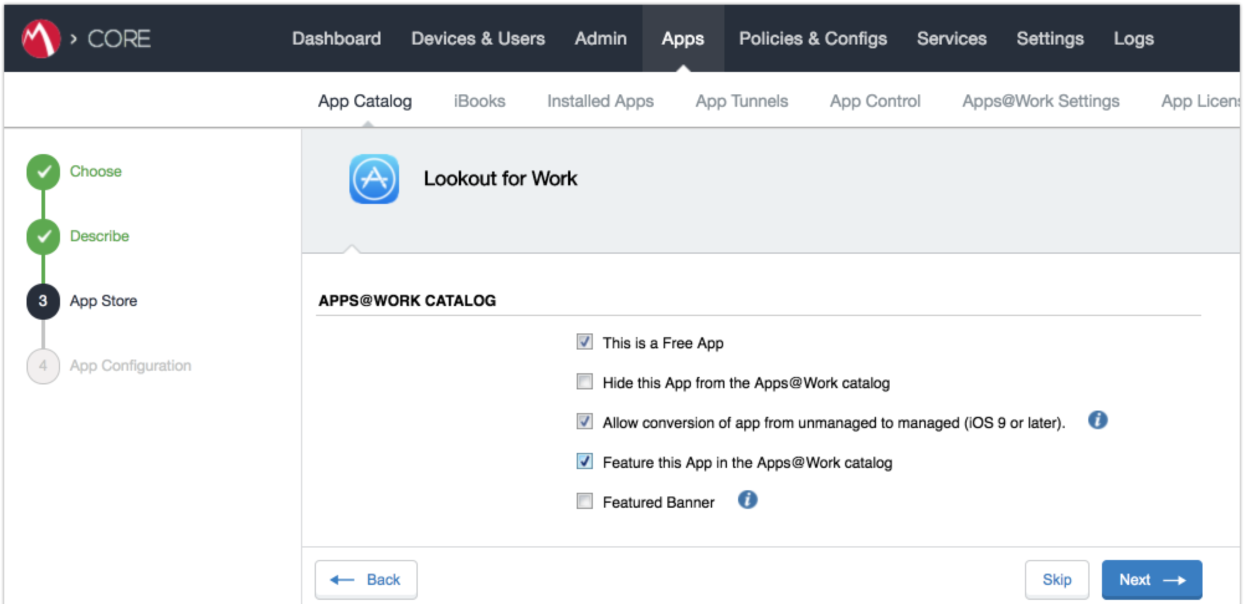
b. Select **Next**.

Figure 2-106 Lookout for Work App Configuration



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



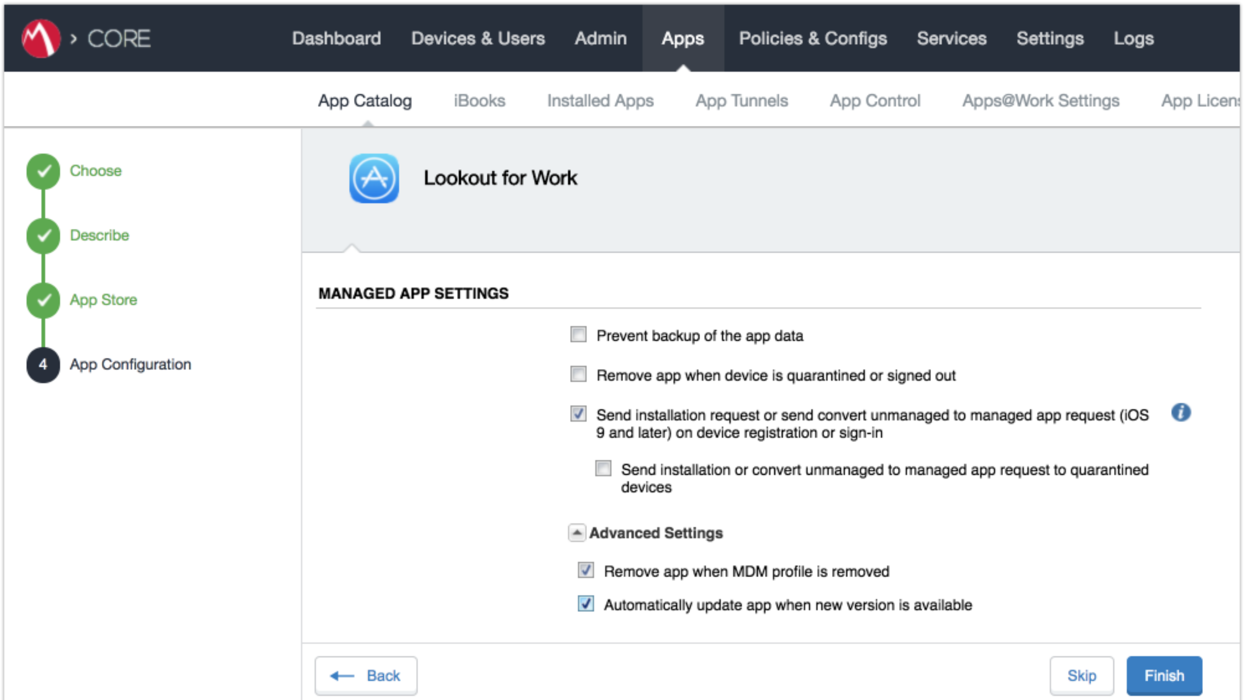
b. In the **App Catalog > App Configuration** section:

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.**

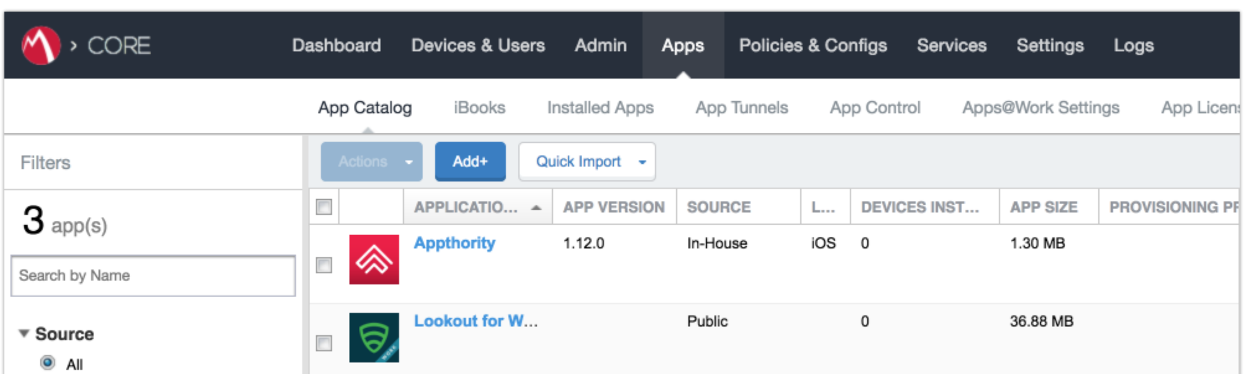
c. Select **Finish**.

Figure 2-108 Lookout for Work Managed App Settings



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

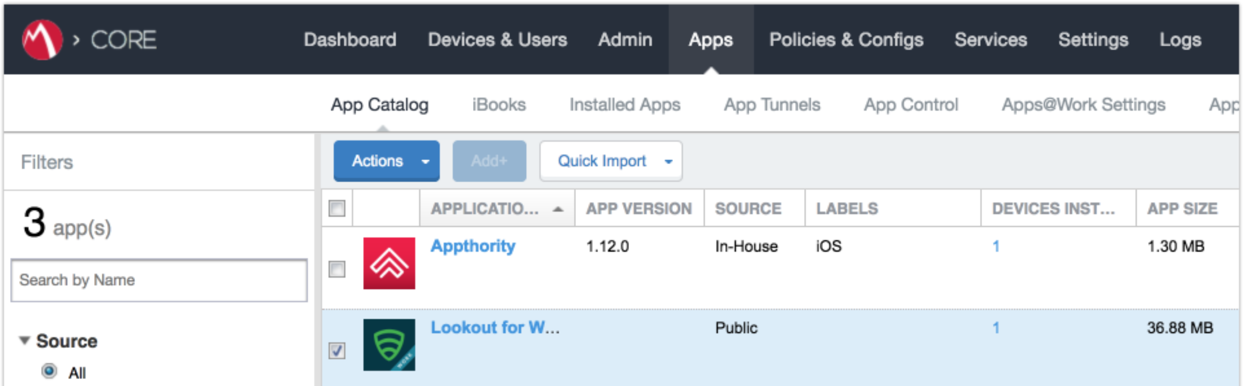


2.7.5.2 Apply MobileIron Labels to Lookout for Work App

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

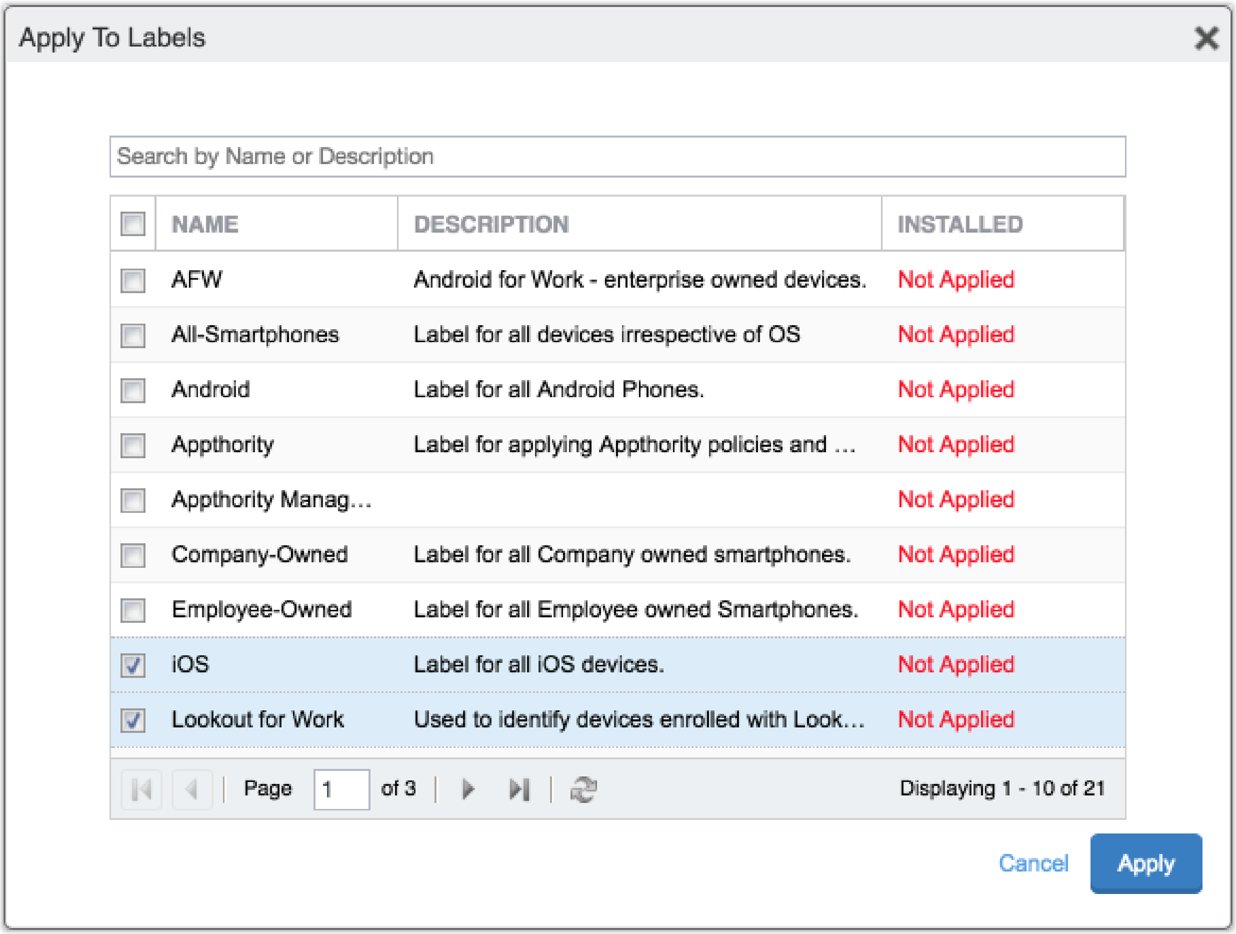


c. In the **Apply To Labels** dialogue:

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

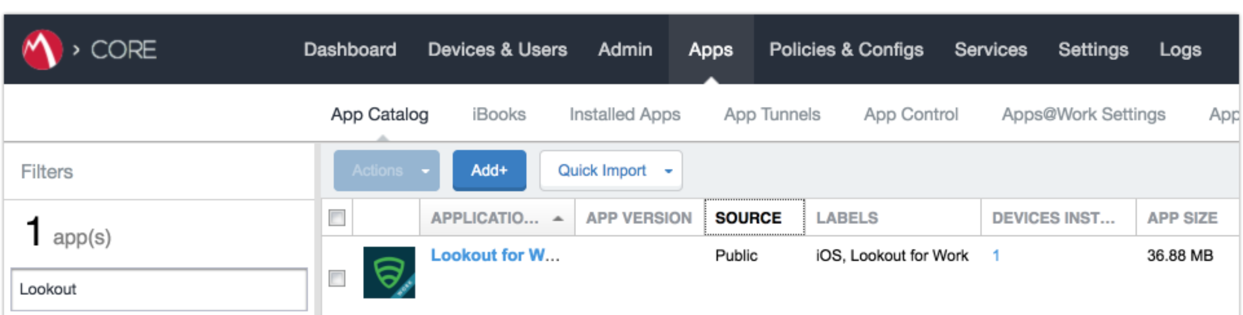
ii. Select **Apply.**

Figure 2-111 Apply To Labels Dialogue



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



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.

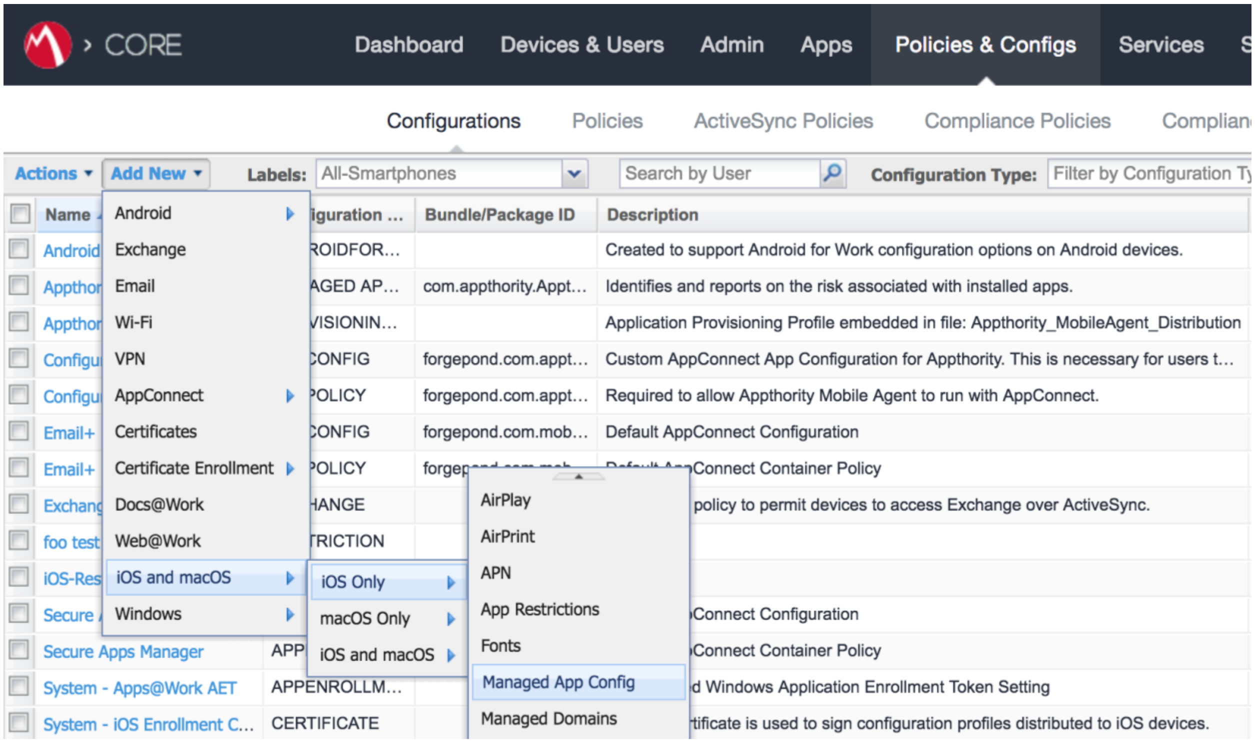
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"https://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>MDM</key>
    <string>MOBILEIRON</string>
    <key>DEVICE_UDID</key>
    <string>$DEVICE_UDID$</string>
    <key>EMAIL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

Figure 2-113 Importing Managed Application Configuration



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

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

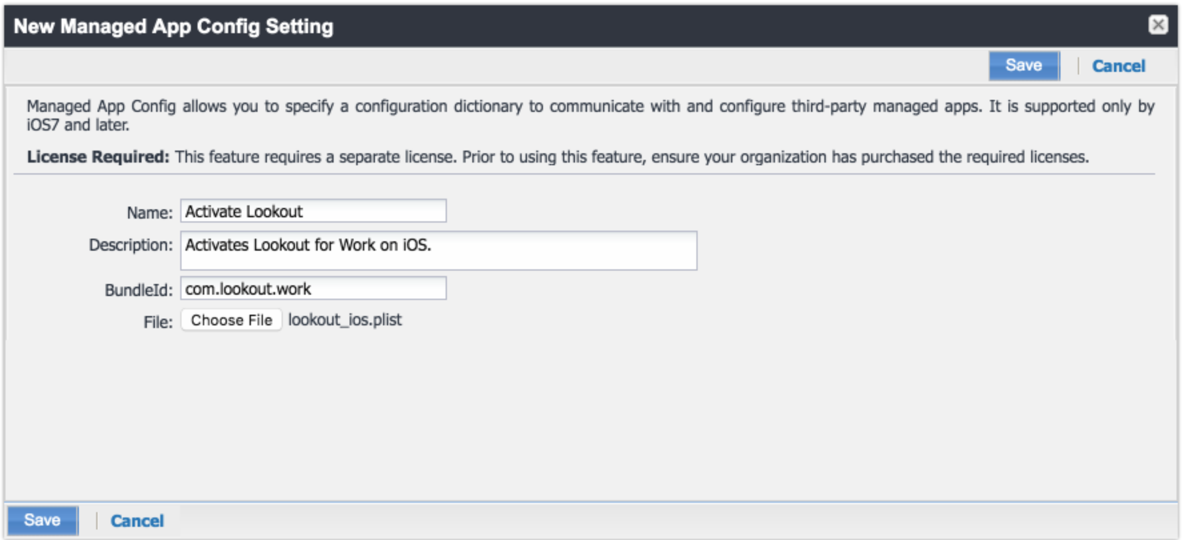
ii. In the **Description** field, provide the purpose for this configuration.

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

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

v. Select **Save.**

Figure 2-114 plist Import Configuration

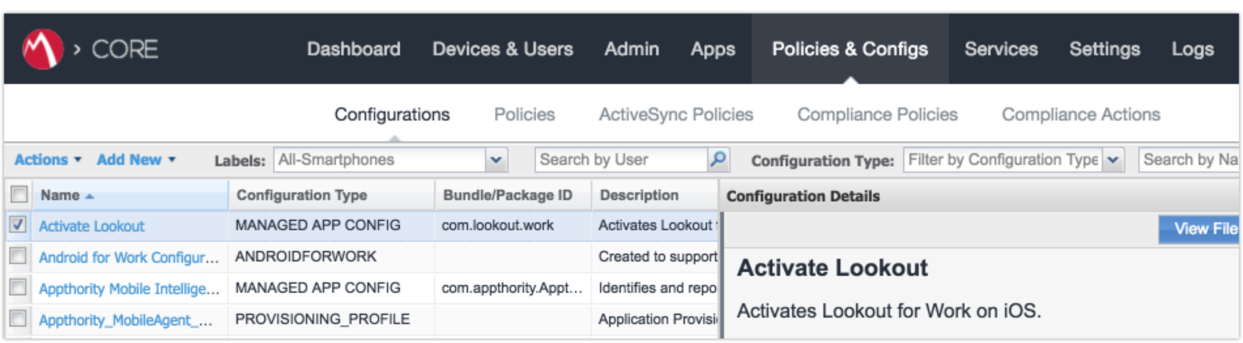


2.7.5.4 Apply Labels to Managed App Configuration for Lookout for Work

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

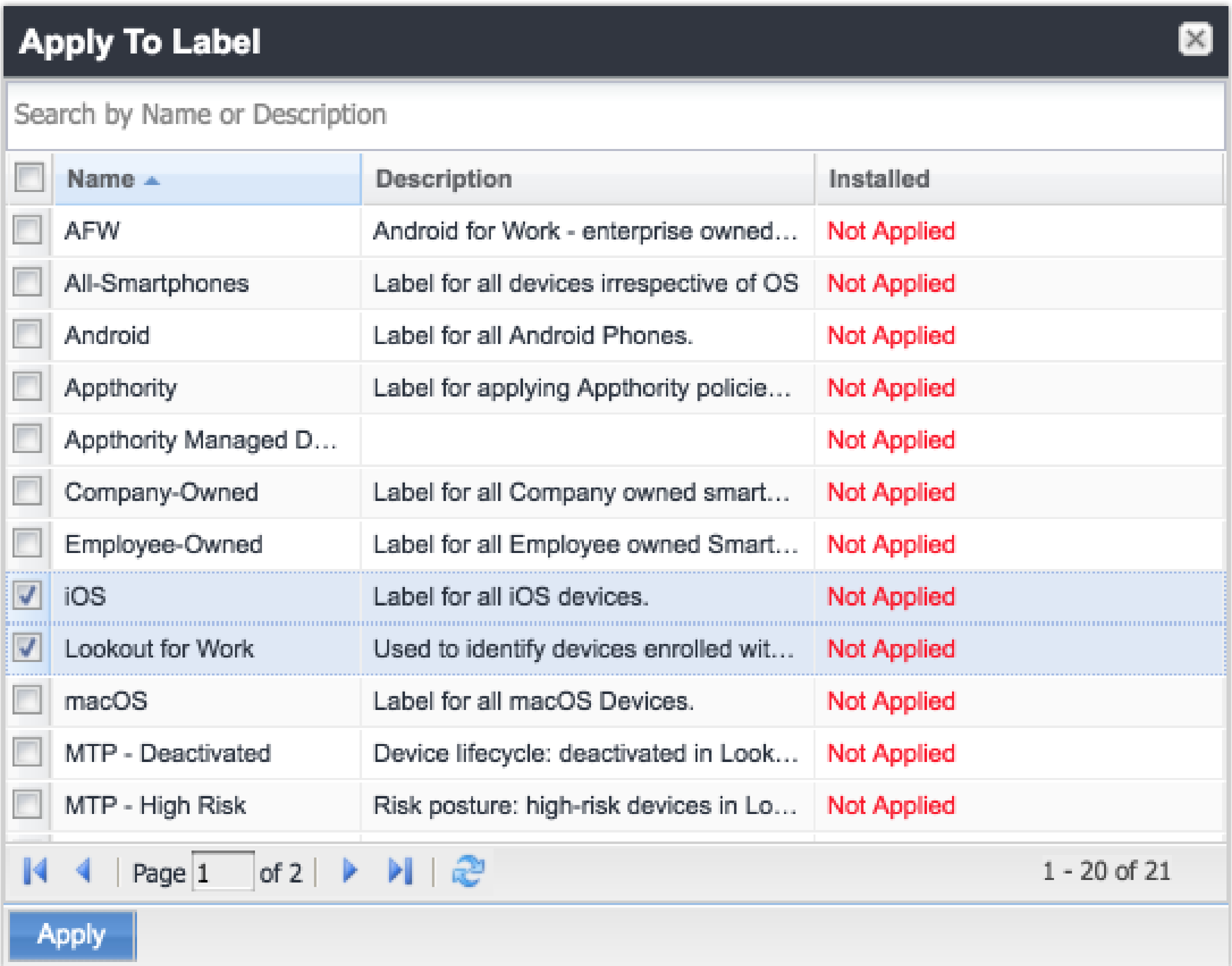


    c. In the **Apply To Label** dialogue:

i. Enable the iOS and Lookout for Work labels.

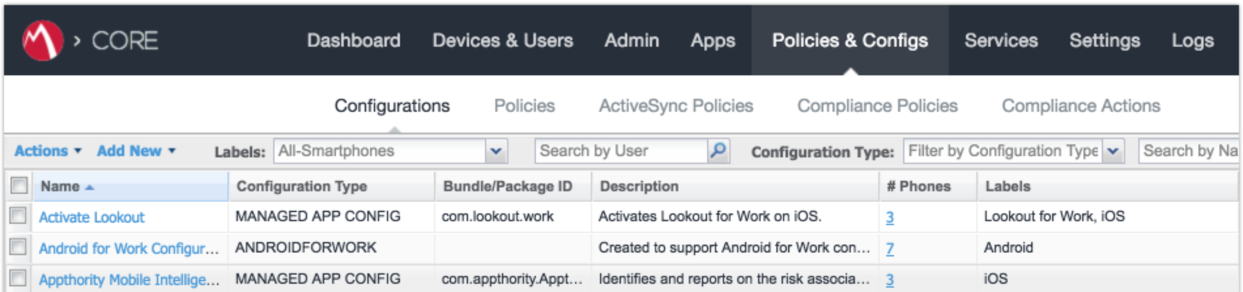
ii. Select **Apply.**

Figure 2-116 Apply To Label Dialogue



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

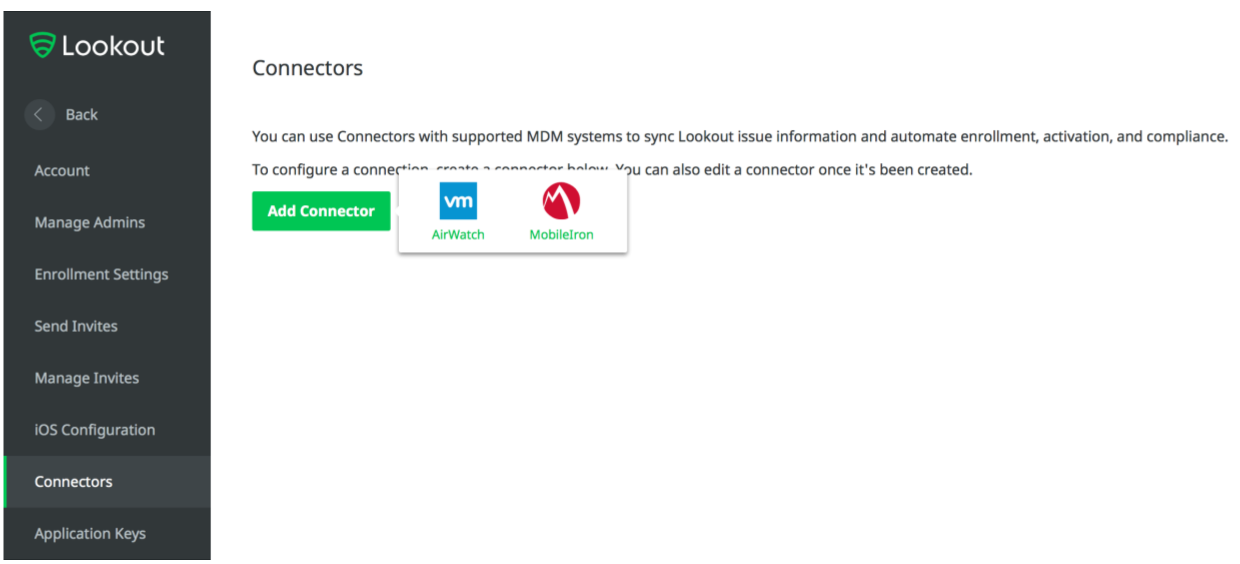


2.7.6 Add MDM Connector for MobileIron to Lookout MES

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



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

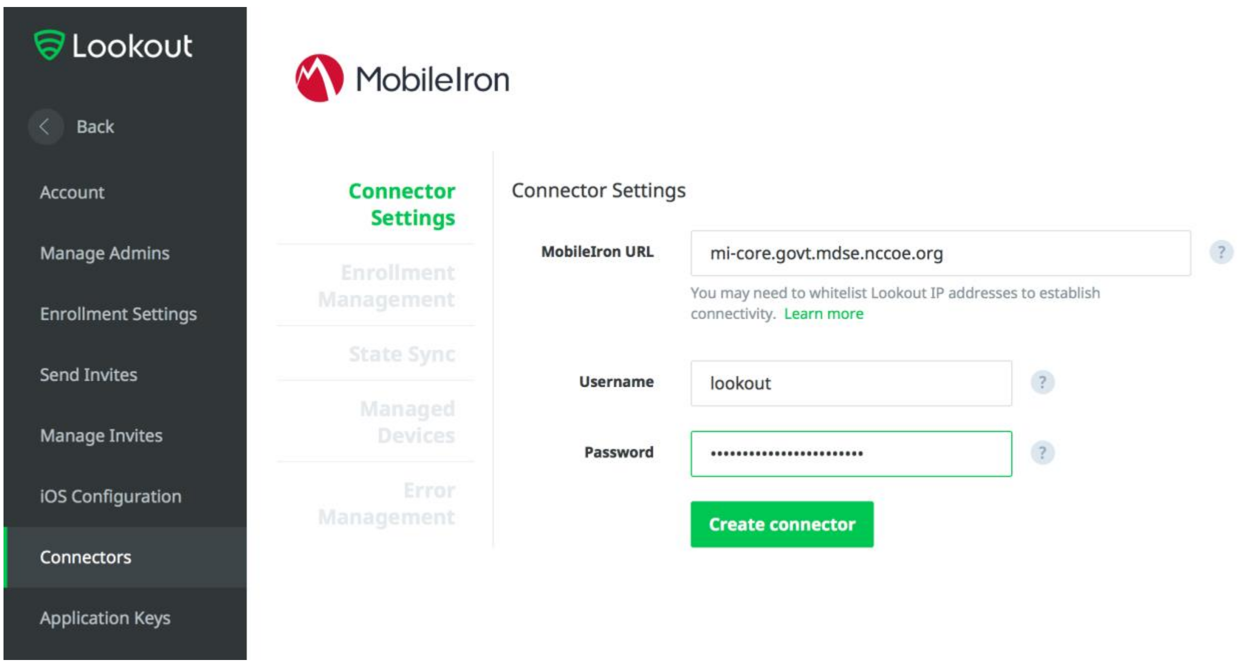
   i. For the **MobileIron URL** field, enter the FQDN for your instance of MobileIron. In our example implementation, the URL was **mi-core.govt.mdse.nccoe.org.**

   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



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

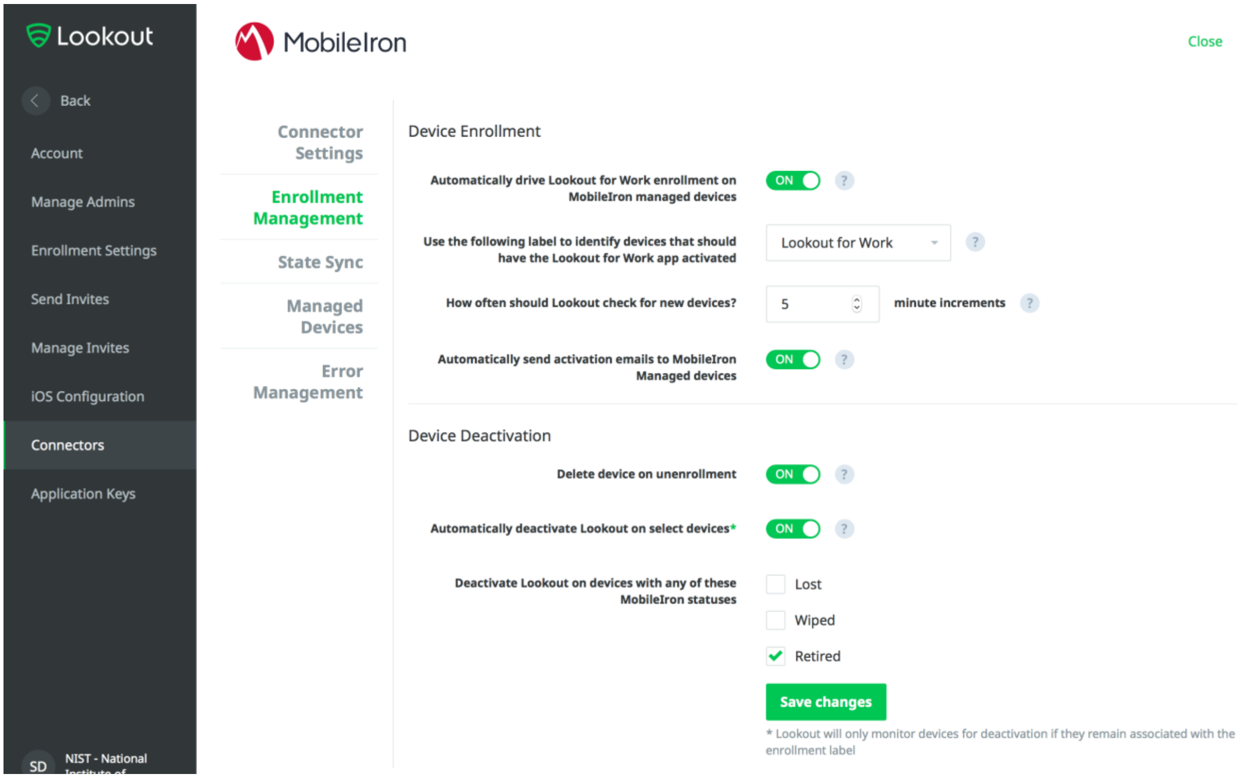
   i. Toggle **Device Enrollment > Automatically** drive Lookout for Work enrollment on MobileIron managed devices to **On.**

   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



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.

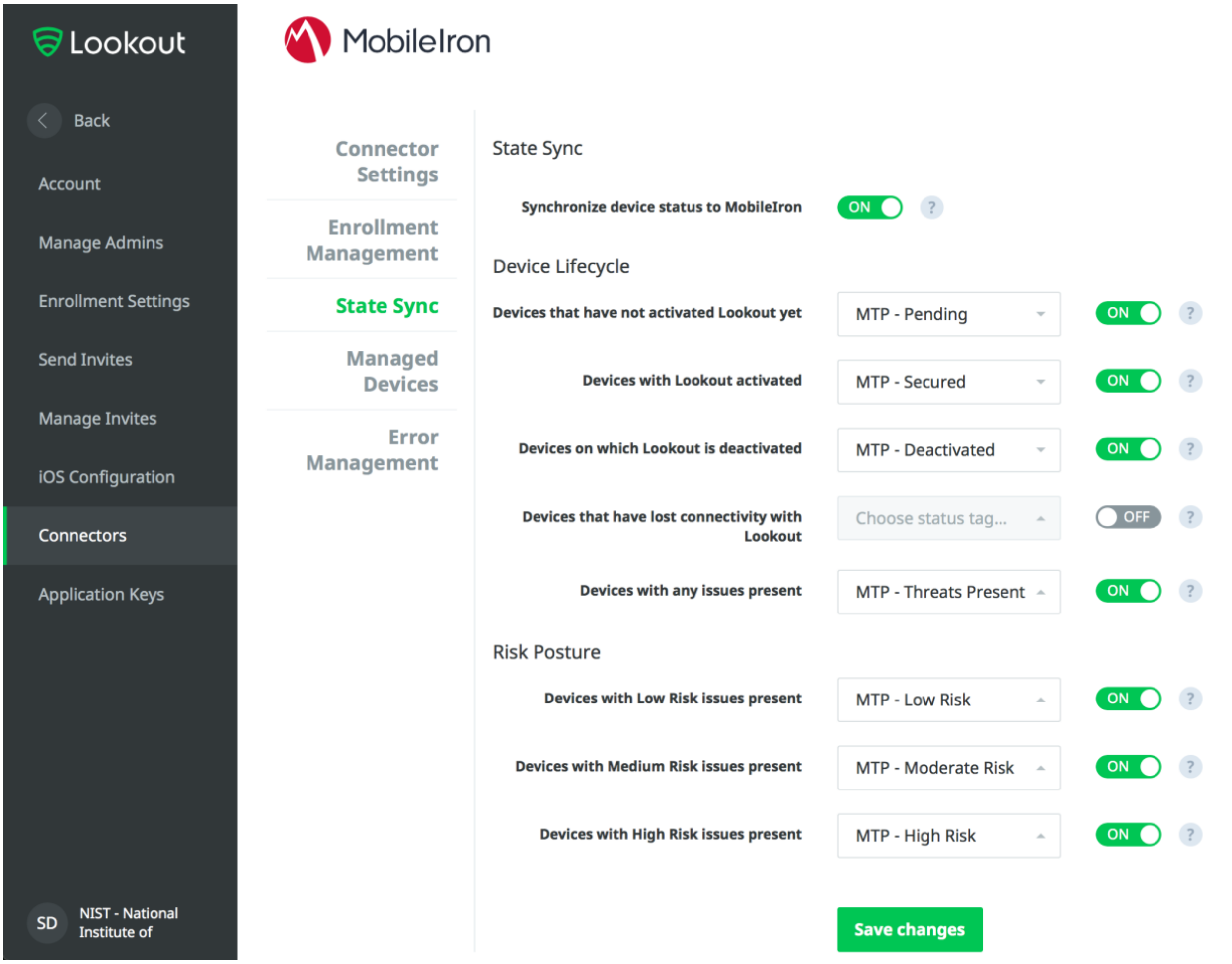
State	Purpose	Label Name
Devices that have not activated Lookout yet	Lifecycle management: devices with Lookout not yet activated	MTP - Pending

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



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.**

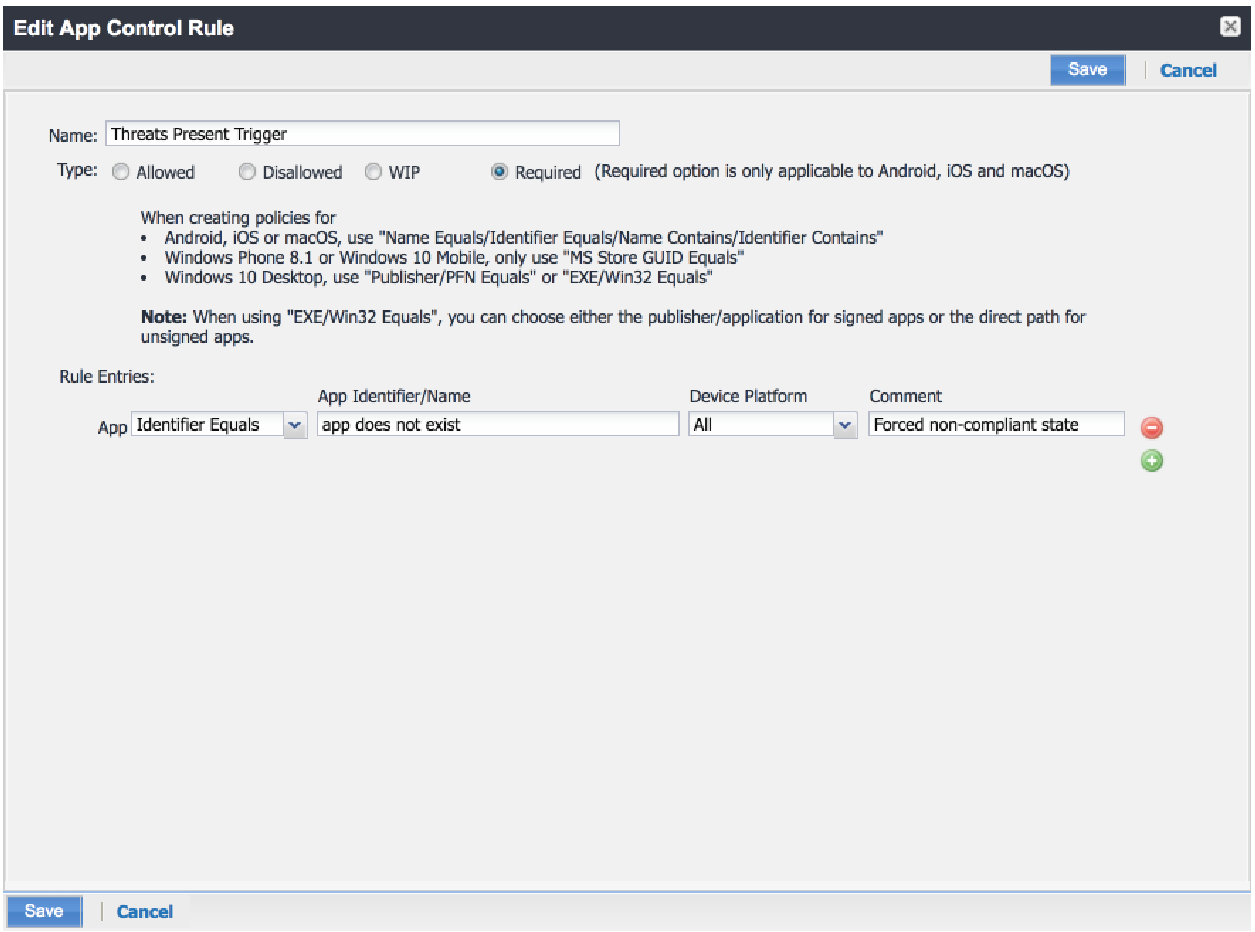
c. In the **App Identifier/Name** field enter **app does not exist.**

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

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

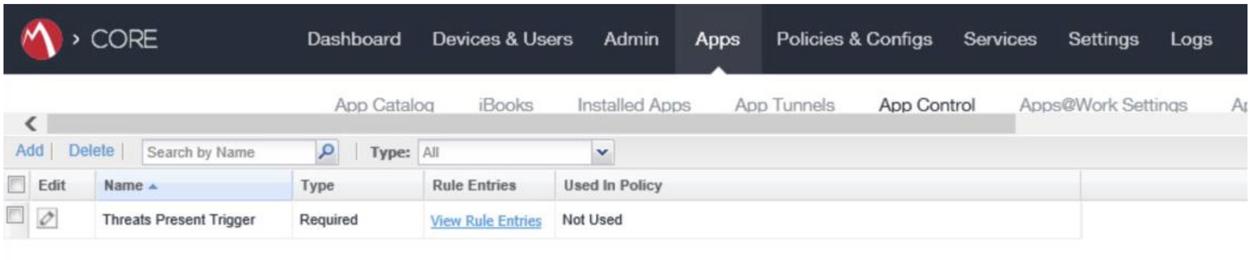
f. Select **Save.**

Figure 2-122 MobileIron App Control Rule



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

Figure 2-123 MobileIron App Control Rule

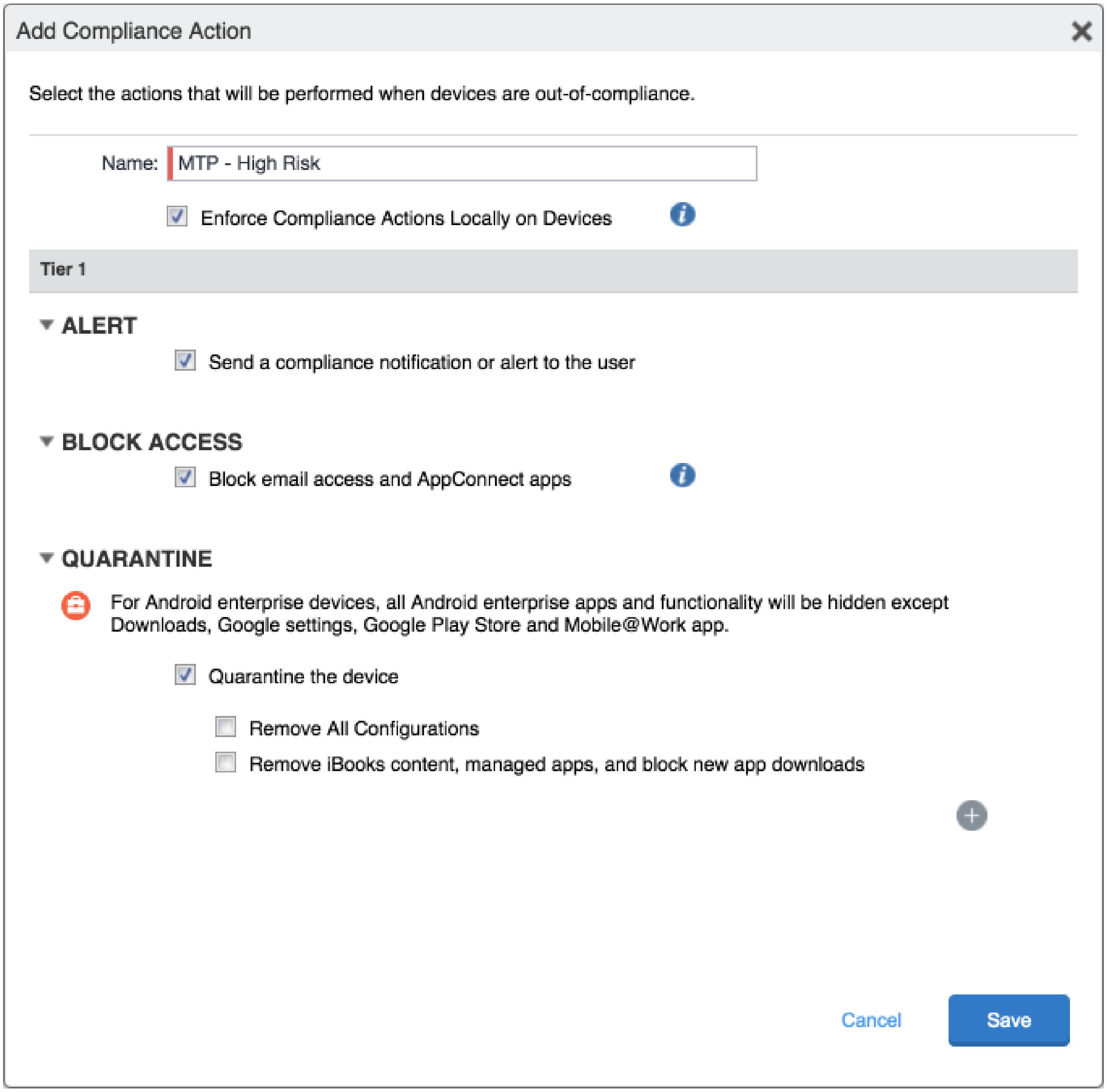


2.7.7.2 Add MobileIron Compliance Actions

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

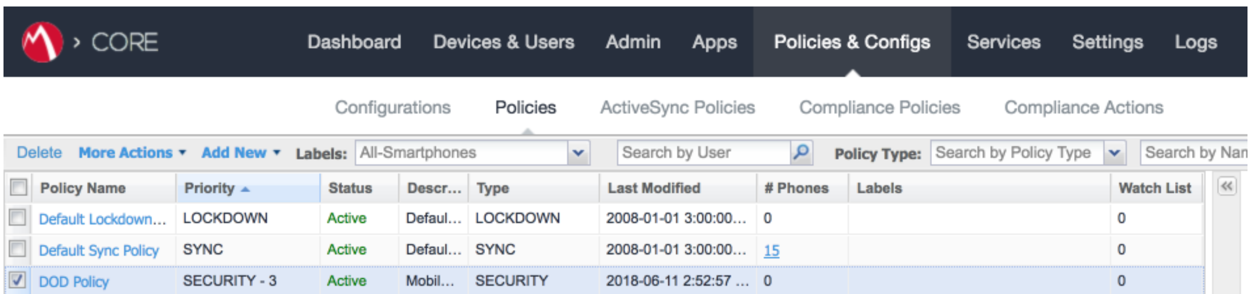


2.7.7.3 Create MobileIron Security Policy for Lookout MES

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



    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).

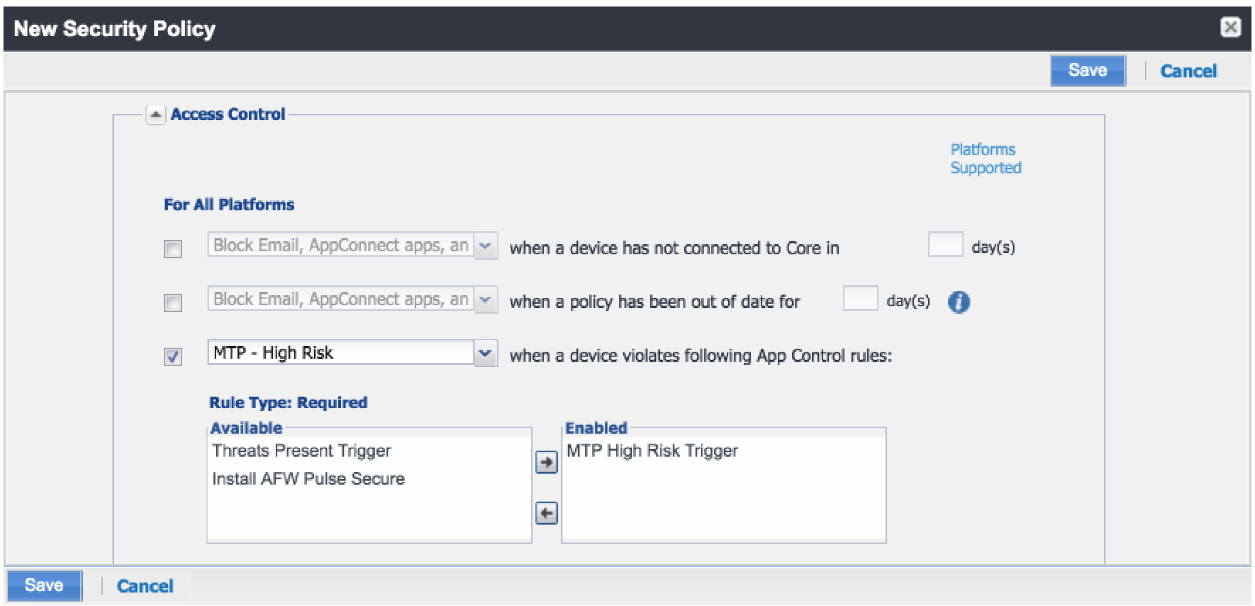
Figure 2-126 MTP High Risk Policy

        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

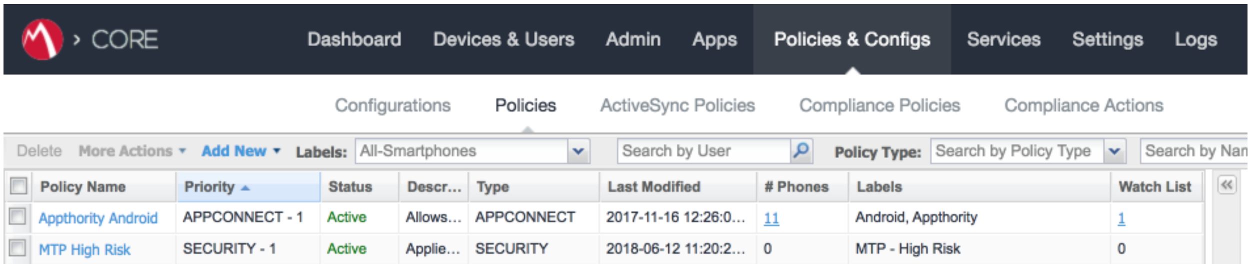


2.7.7.4 Apply Lookout MES Label to MobileIron Security Policy

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

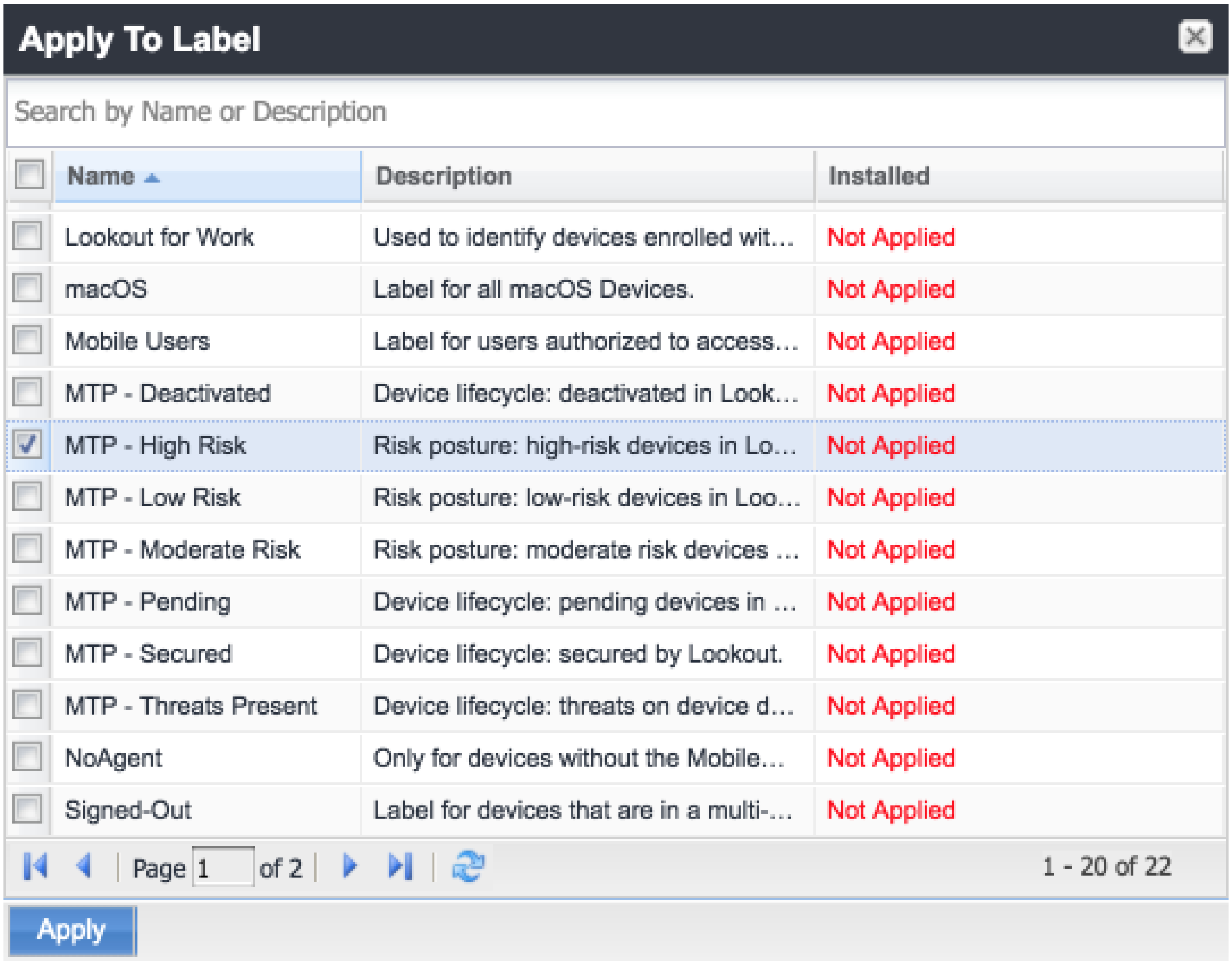


c. In the **Apply to Label** dialogue:

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

   ii. Select **Apply.**

Figure 2-129 Apply To Label Dialogue



2.8 Integration of Appthority Mobile Threat Detection with MobileIron

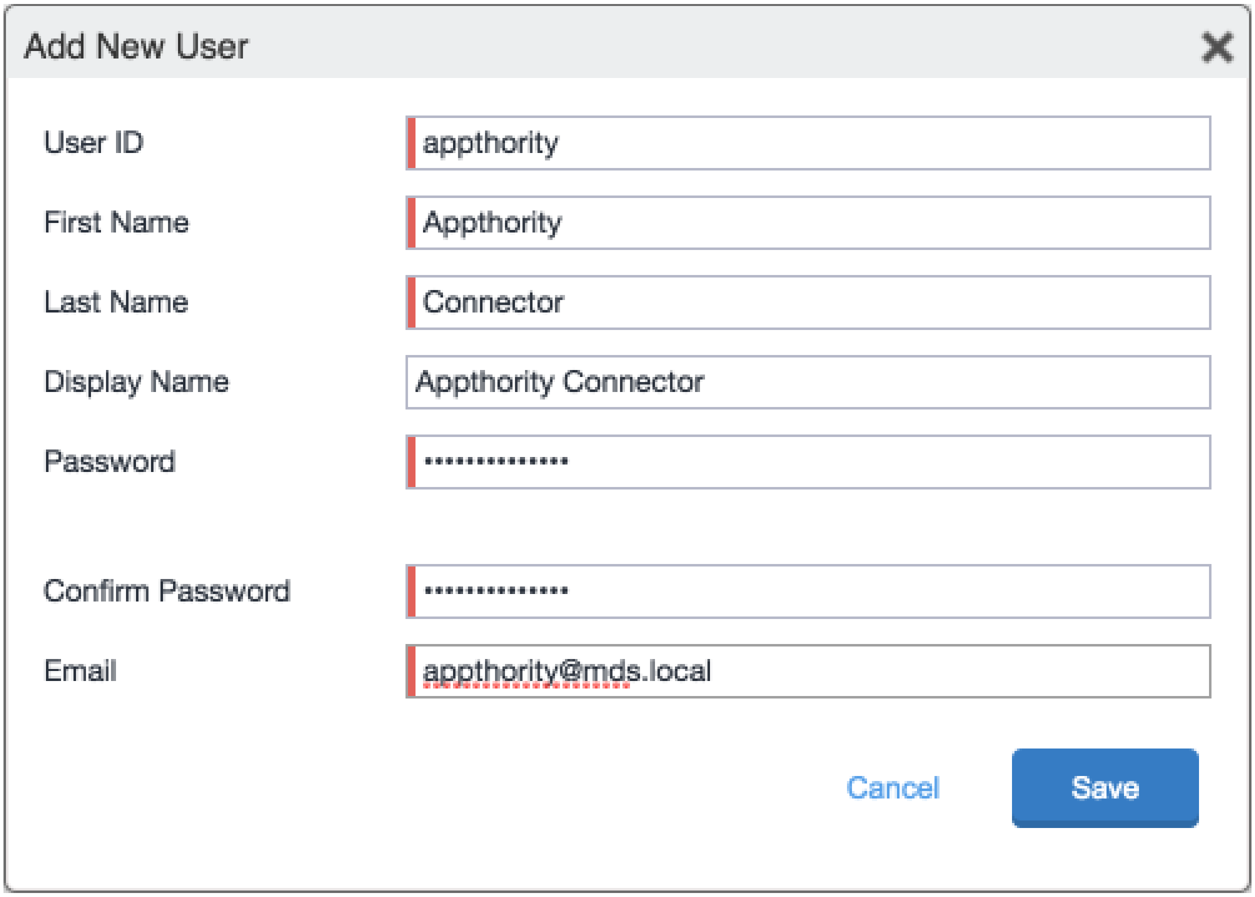
Appthority provides an on-premises connector for MobileIron that runs as a Docker container on RedHat Linux. The connector uses the MobileIron API to obtain information on managed devices and their installed apps, which is then synchronized with the cloud service instance to obtain app and device risk 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.

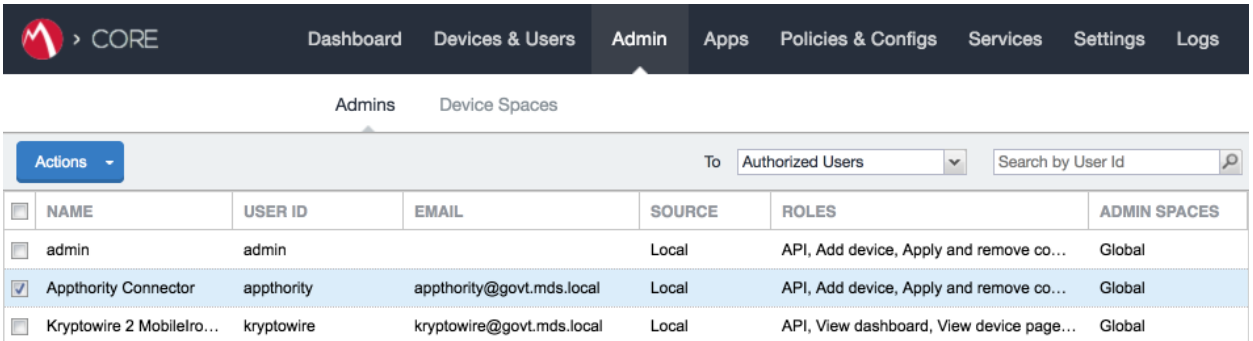
1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Users.**
2. On the **Users** page:
    a. Select **Add > Add Local User**; the **Add New User** dialogue will open.
    b. In the **Add New User** dialogue:
        i. In the **User ID** field, enter the **user identity** the Appthority 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 Apphority User Settings



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.

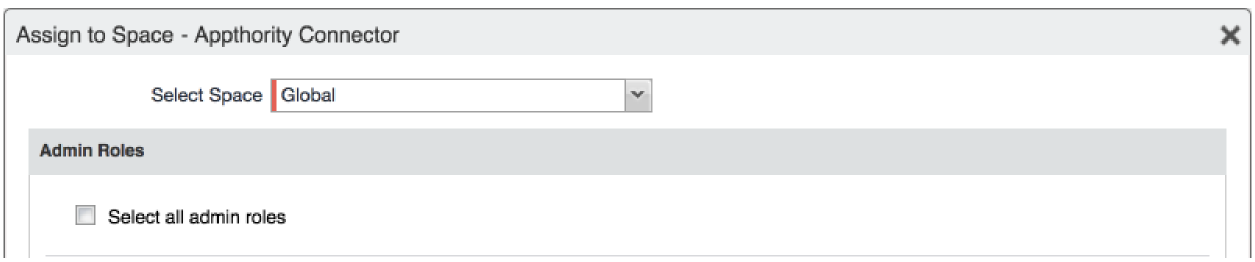
Figure 2-131 Apthority Connector User



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

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

Figure 2-132 Appthority Connector Space Assignment



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 Appthority Connector Open Virtualization Appliance

One deployment option for the Appthority 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 Appthority support portal: https://support.appthority.com/.

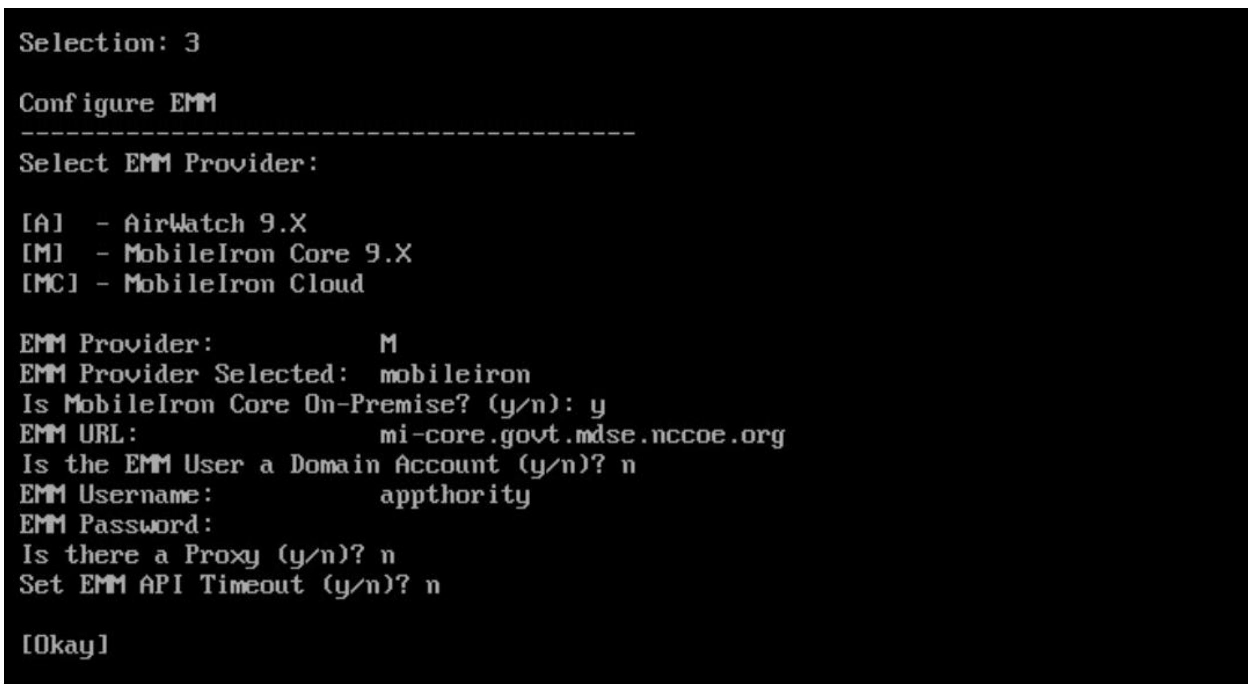
2.8.3 Run the Enterprise Mobility Management Connector Deployment Script

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. 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.

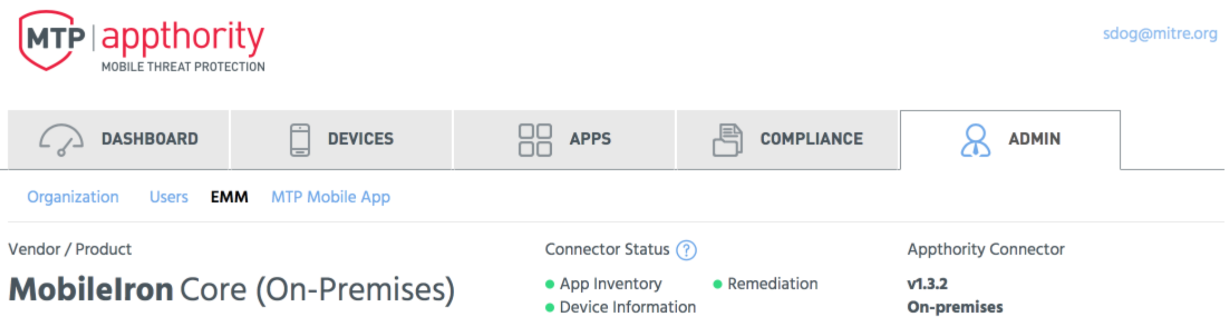
Figure 2-133 Appthority Connector CLI Configuration



```
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 Apptherity EMM Connector Status



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

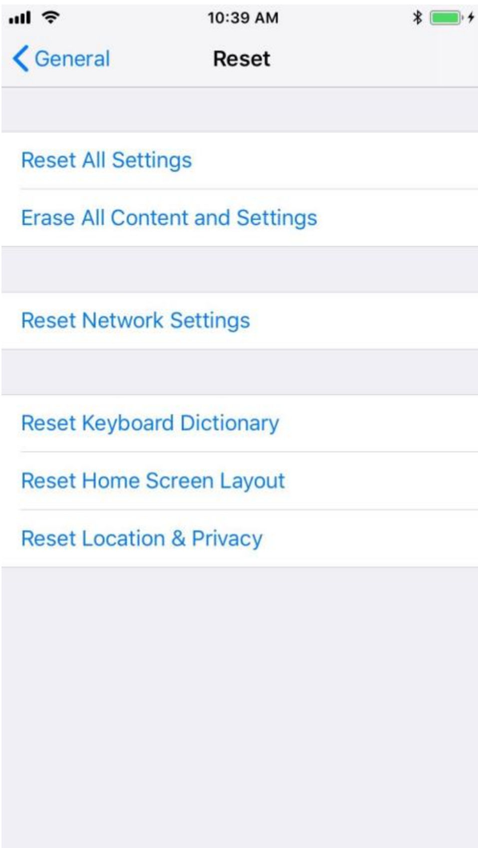
Before a device can be placed into Supervised Mode, it must be in a factory-reset state with the Activation Lock on the device removed. If Activation Lock is in-place, Configurator 2 will be unable to place the device into Supervised Mode.

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:

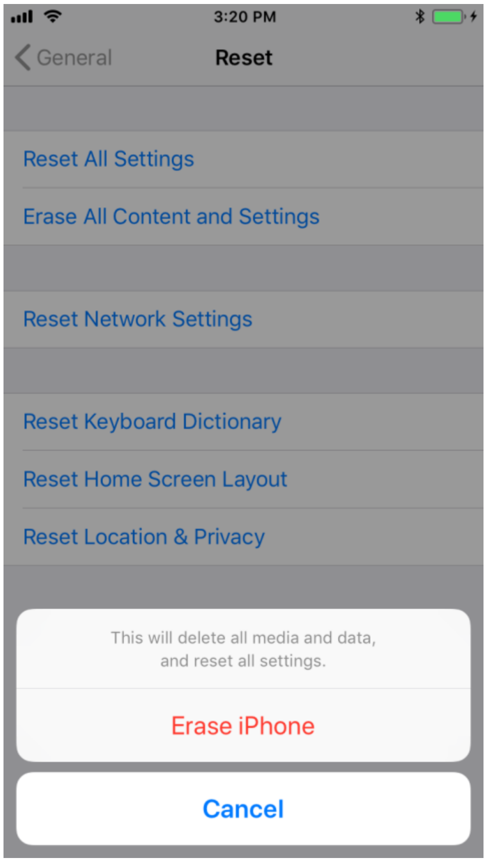
1. Navigate to **Settings > General > Reset.**
2. Select **Erase All Content and Settings.**

Figure 2-135 iOS Reset Screen



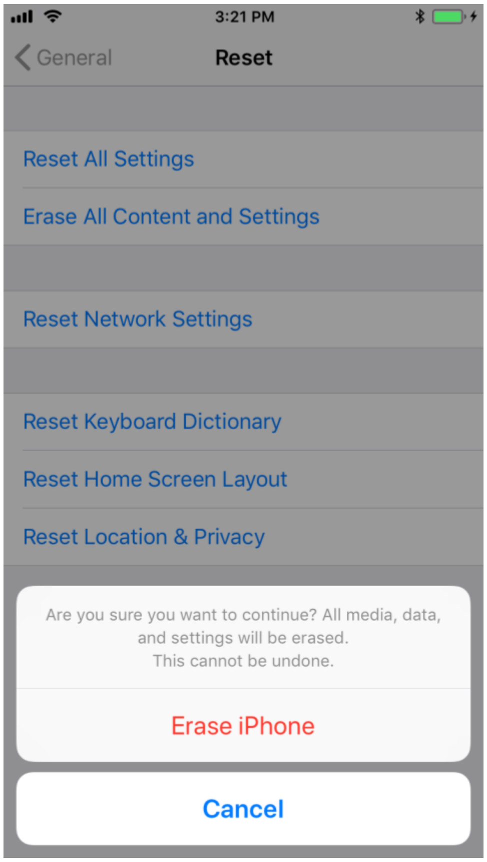
1. At the warning that this will delete all media and data and reset all settings, select **Erase iPhone.**

Figure 2-136 Erase iPhone Confirmation



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



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

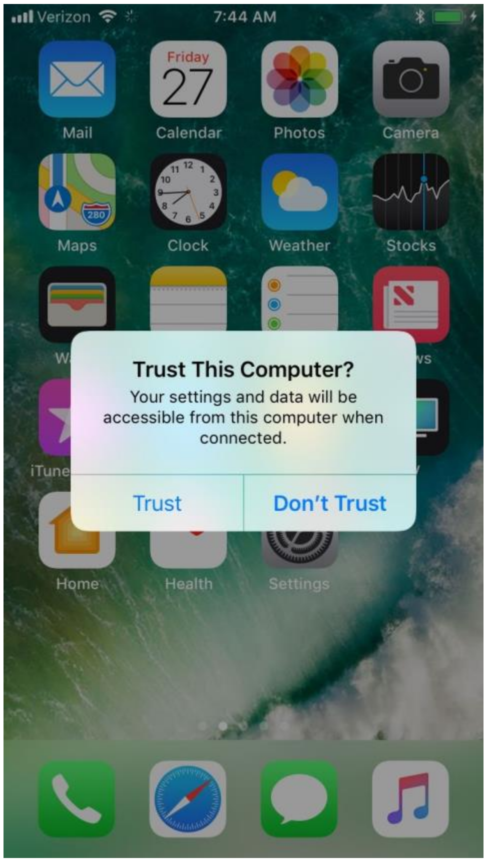
1. **Connect** the iOS device with the system running **Configurator 2** over **Universal Serial Bus (USB).**

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

Figure 2-138 Entering iOS Passcode

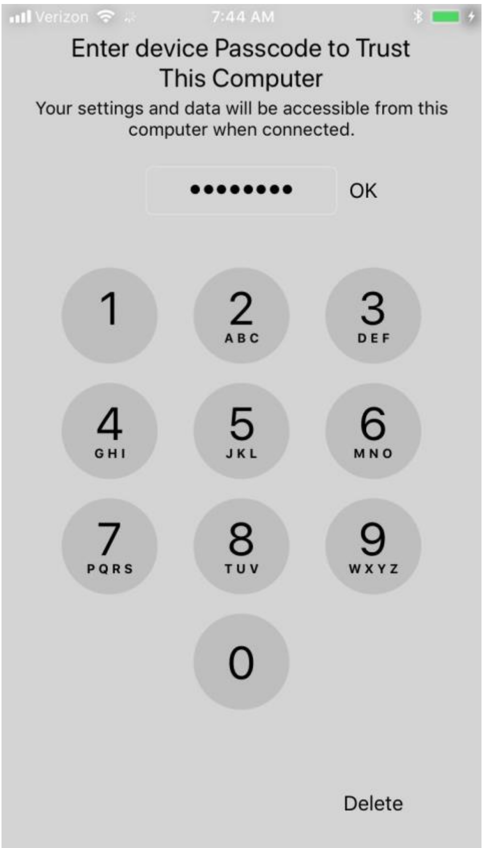
3. At the **Trust this Computer?** dialogue, select **Trust.** Note that this step, along with step that follows, is only encountered the first time a device is paired with a given system.

Figure 2-139 iOS Trust Computer Confirmation



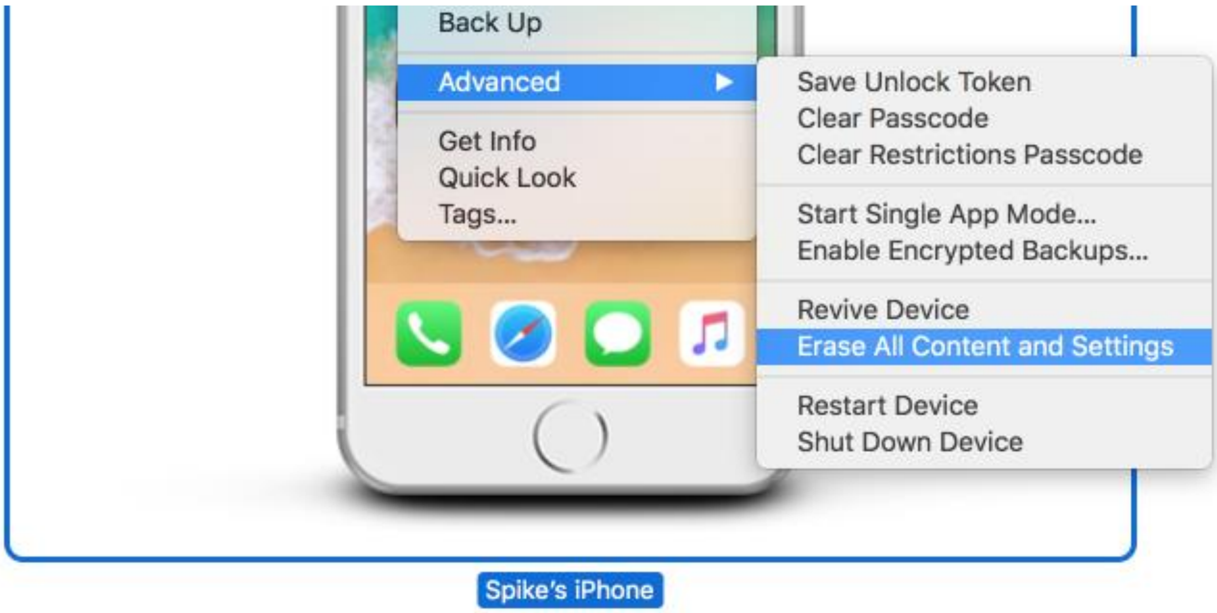
4. At the **Enter Device Passcode to Trust This Computer** screen:
    a. **Enter** the device unlock passcode.
    b. Select **OK**.

Figure 2-140 Entering Passcode to Trust Computer



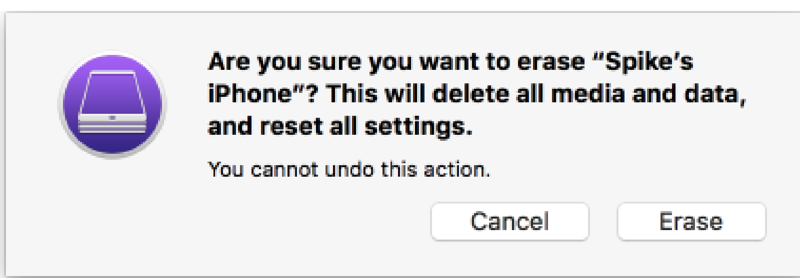
5. In **Configurator 2**, select the **representation** of the connected device.
6. From the **context** menu, select **Advanced > Erase All Content and Settings**.

Figure 2-141 Resetting iPhone in Configurator 2



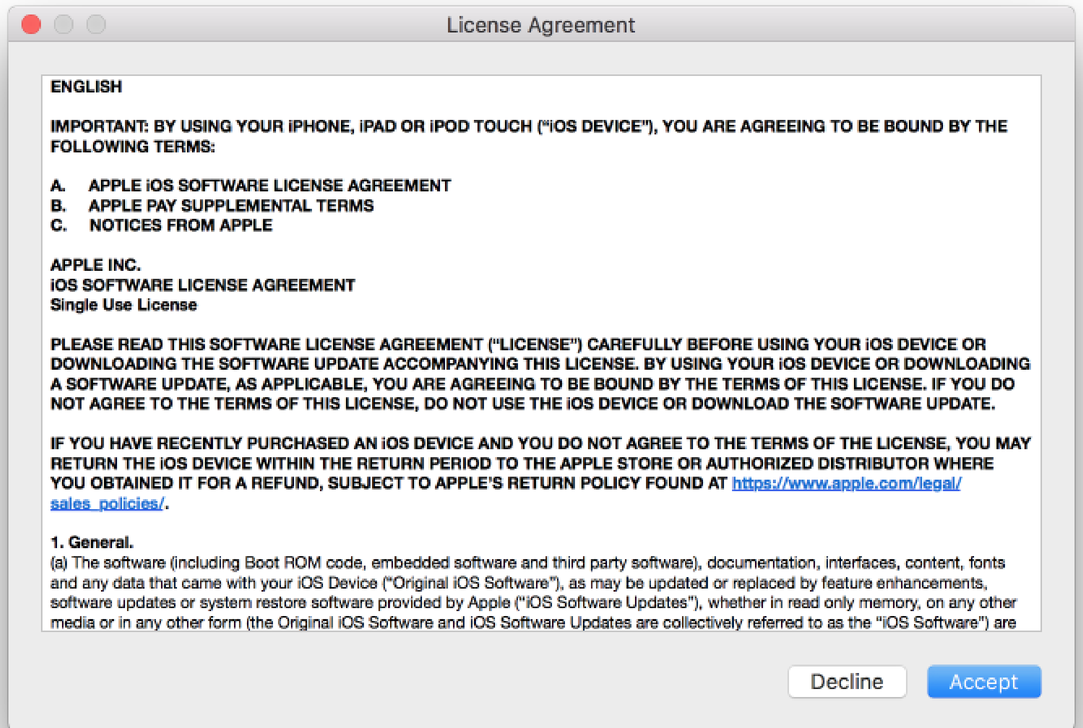
7. At the **Are you sure you want to erase "<device name>"?** dialogue, select **Erase.**

Figure 2-142 Configurator 2 Erase Confirmation



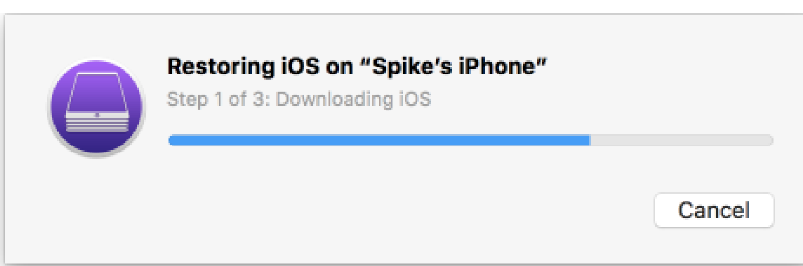
8. At the **License Agreement** screen:
    a. **Review** the license agreement.
    b. Select **Accept** to agree to the license and continue using the software**.**

Figure 2-143 Configurator 2 License Agreement



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

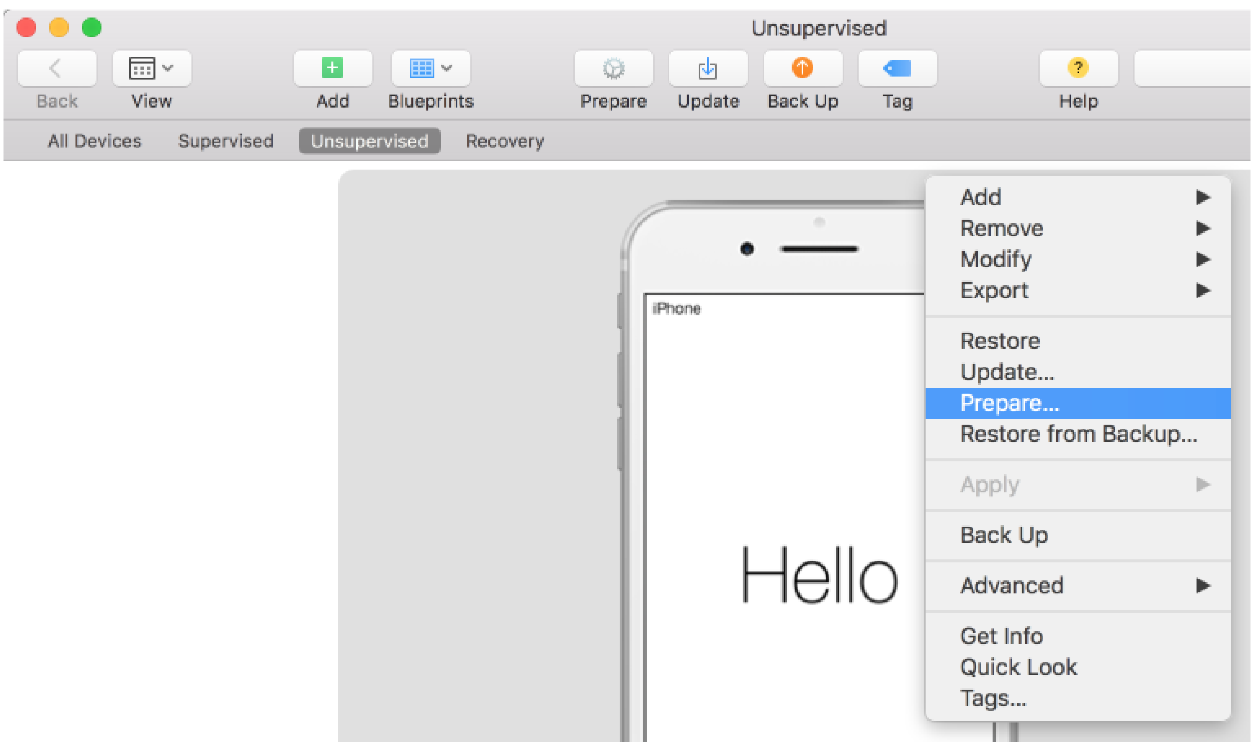


2.9.1.2 Placing an iOS Device into Supervised Mode

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:

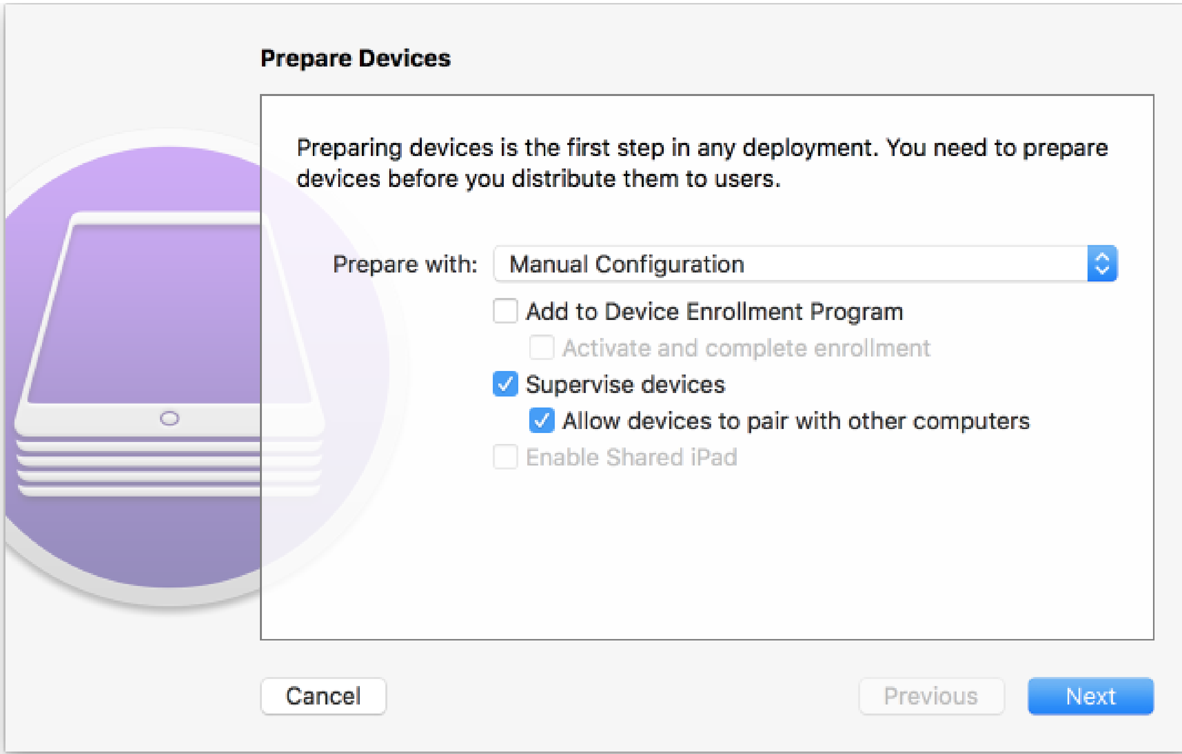
1. **Pair** the target iOS device with the system running Configurator 2 over USB.
2. Navigate to **Configurator 2 > Unsupervised**; a representation of the connected device should appear.
3. On the **All Devices** tab:
   a. **Select** the representation of the paired device.
   b. From the **context**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



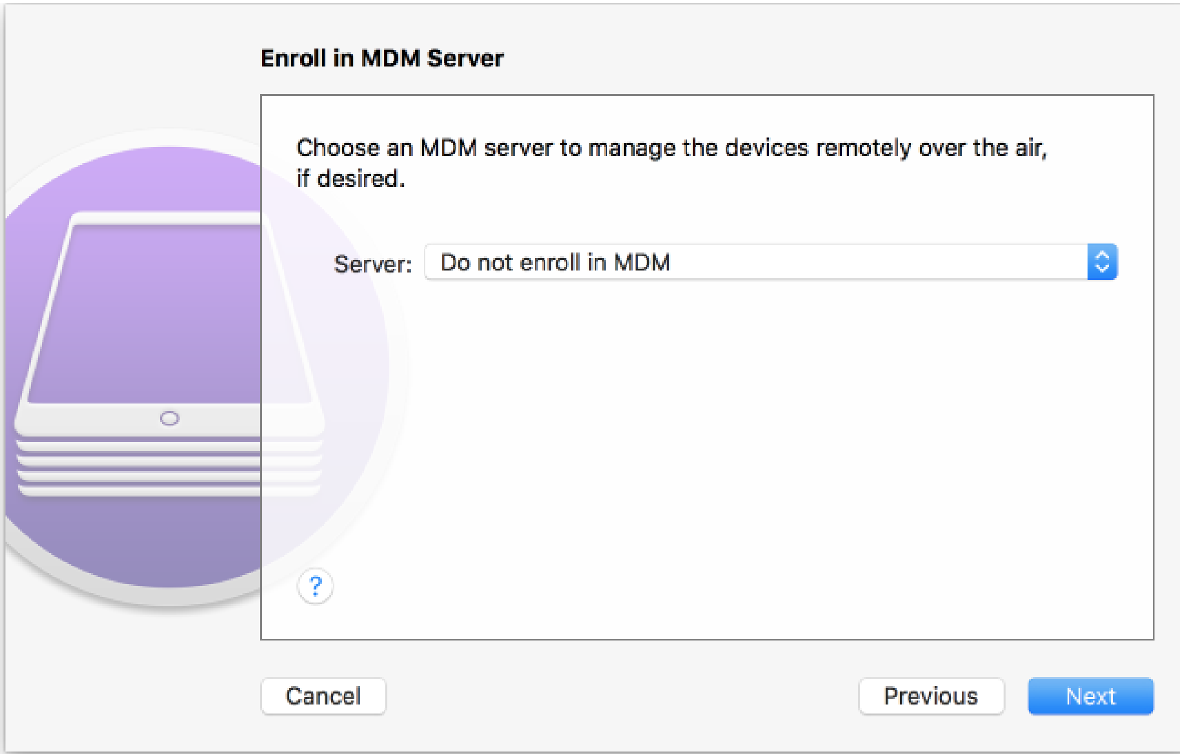
1694

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

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

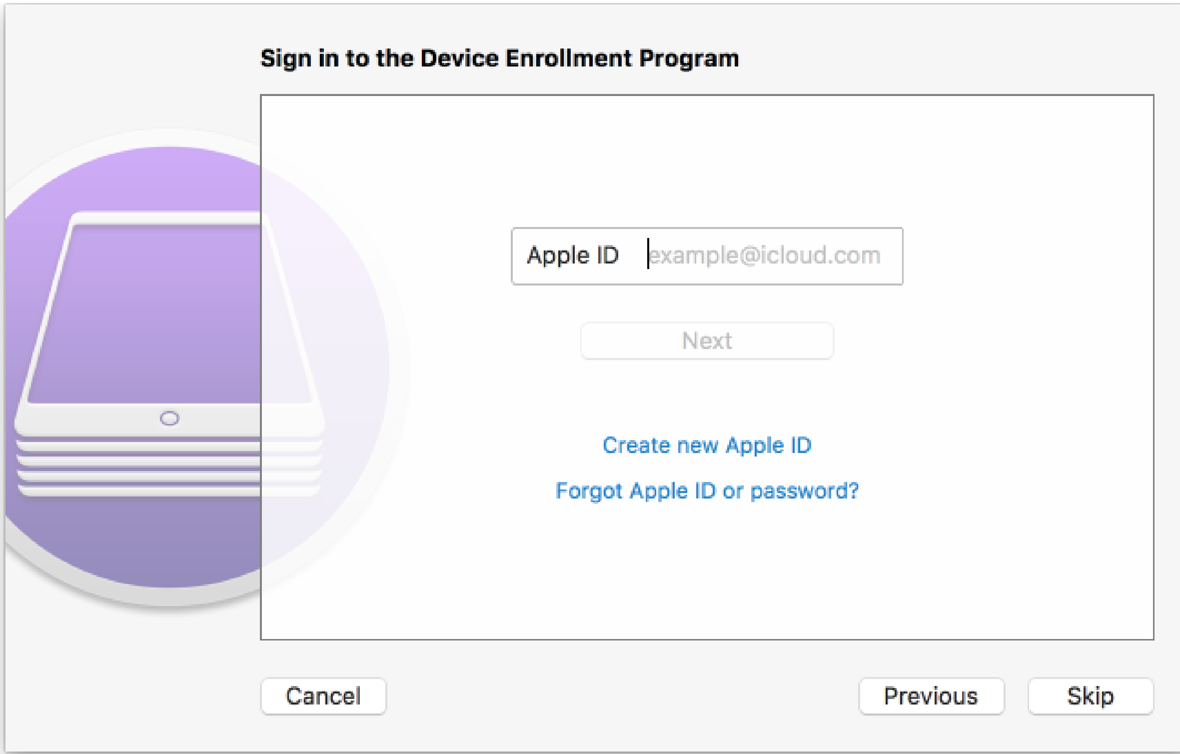
1697 b. Select **Next.**

Figure 2-147 Preparation MDM Server Selection



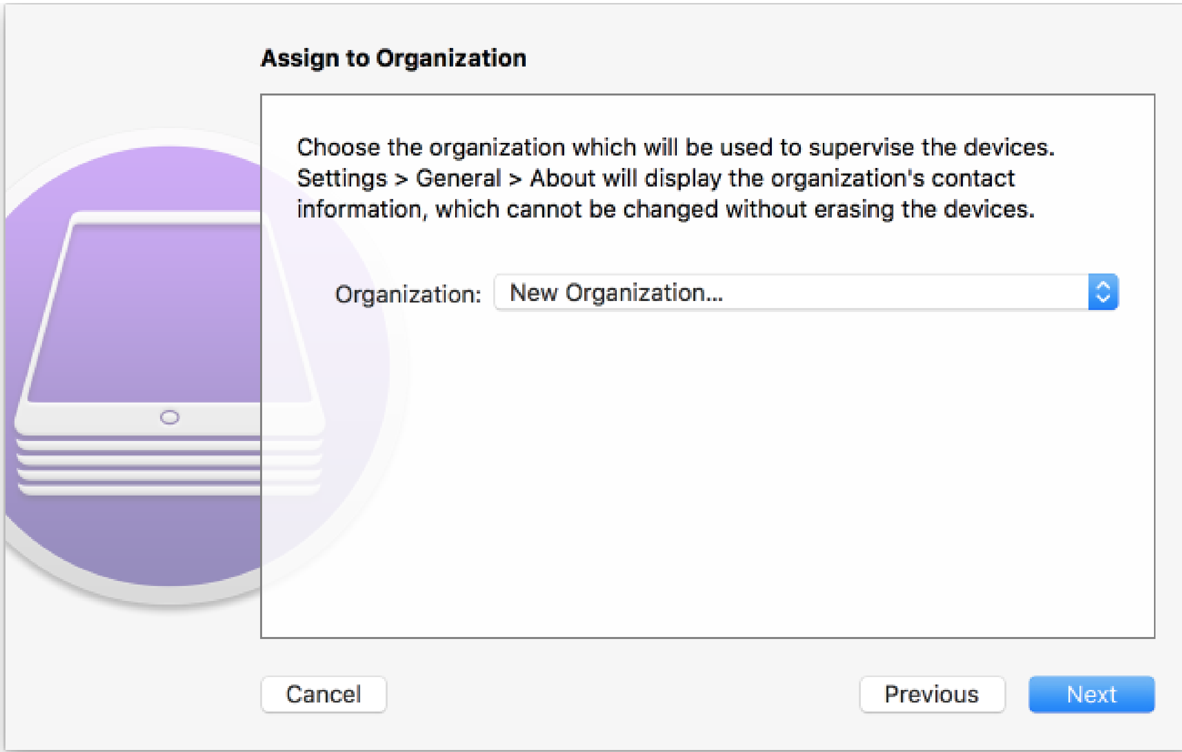
6. For the **Sign into the Device Enrollment Program** step, select **Skip.**

Figure 2-148 Signing into Apple Account



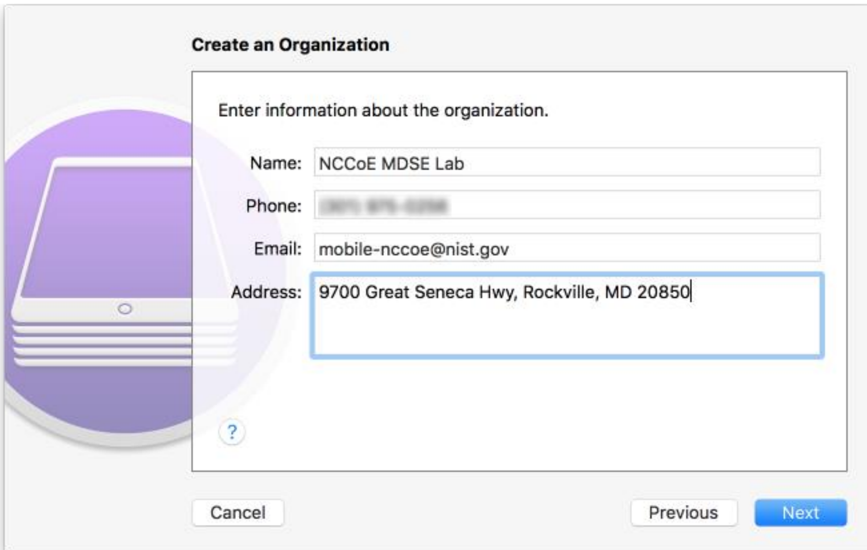
7. For the **Assign to Organization** step:
   a. If you have previously created your organization, select **Next** and continue with **Step 9.**
   b. If you have not created your organization, from the **Organization** drop-down menu, select **New Organization...**

Figure 2-149 Organization Assignment Dialogue



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



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.

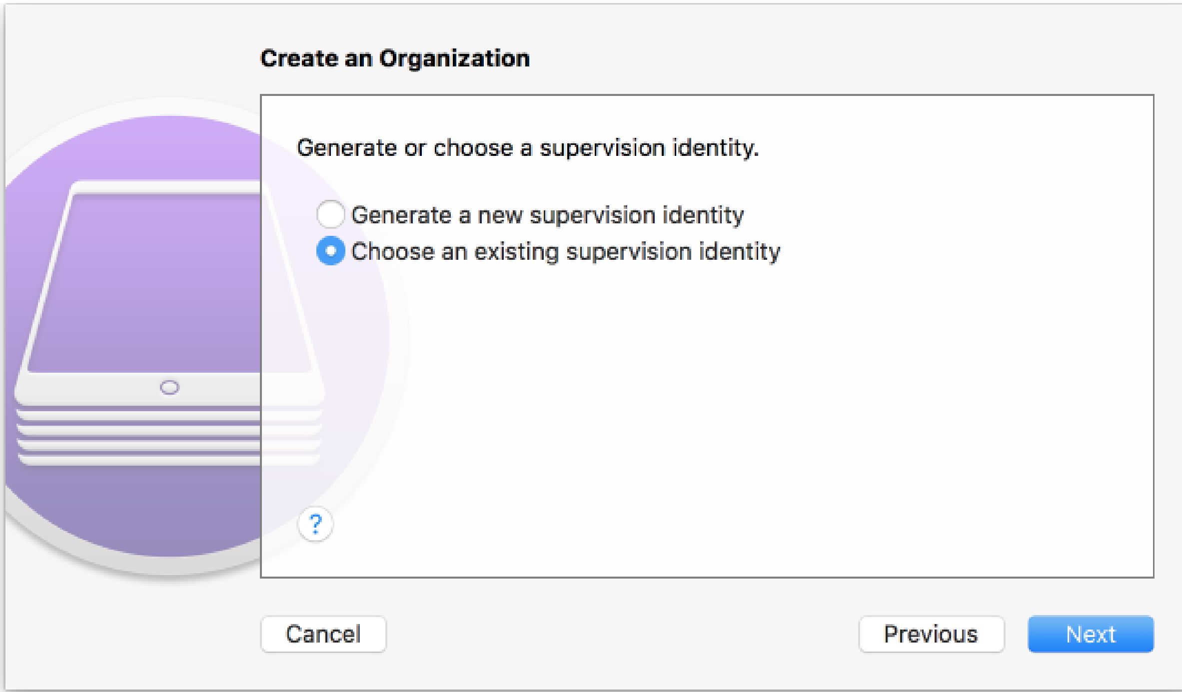
    b. Otherwise, continue with **Step 14**.

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.**

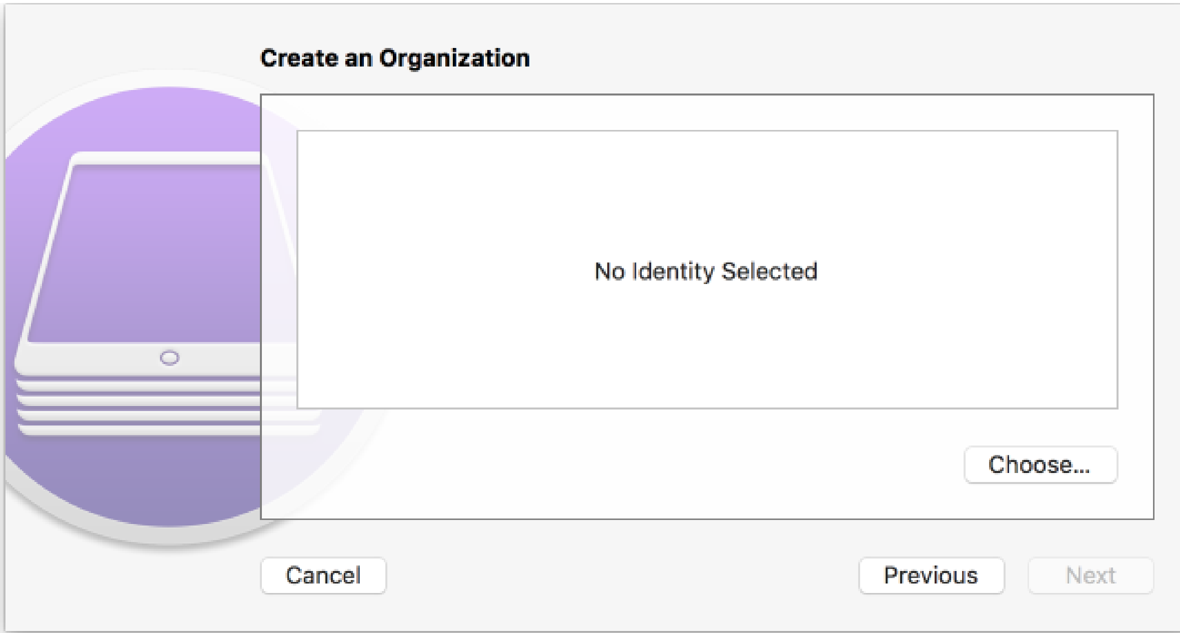
1726 **Figure 2-151 Supervisory Identity Configuration**



1727

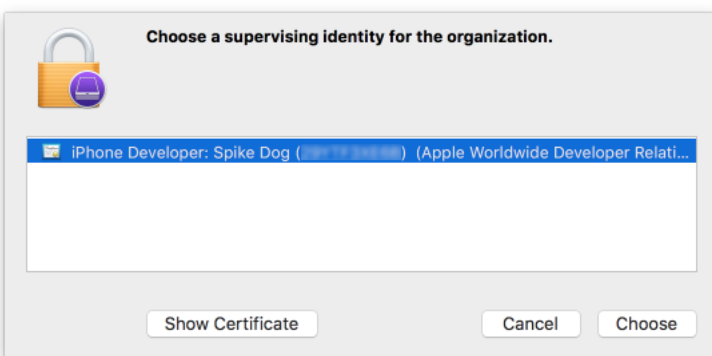
1728 11. Select **Choose...**

Figure 2-152 Organization Selection



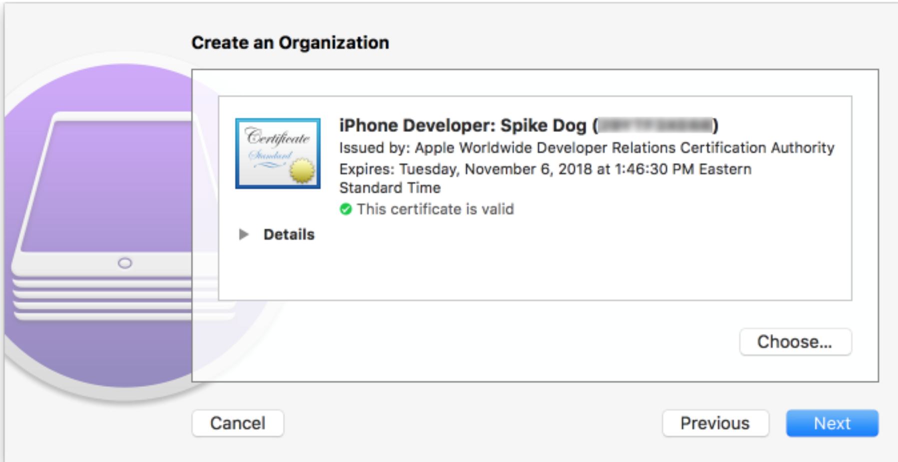
12. At the **Choose a supervising identity for the organization** dialogue:
    a. **Select** the digital certificate from the list of those available to the system.
    b. Select **Choose.**

Figure 2-153 Supervising Identity Selection



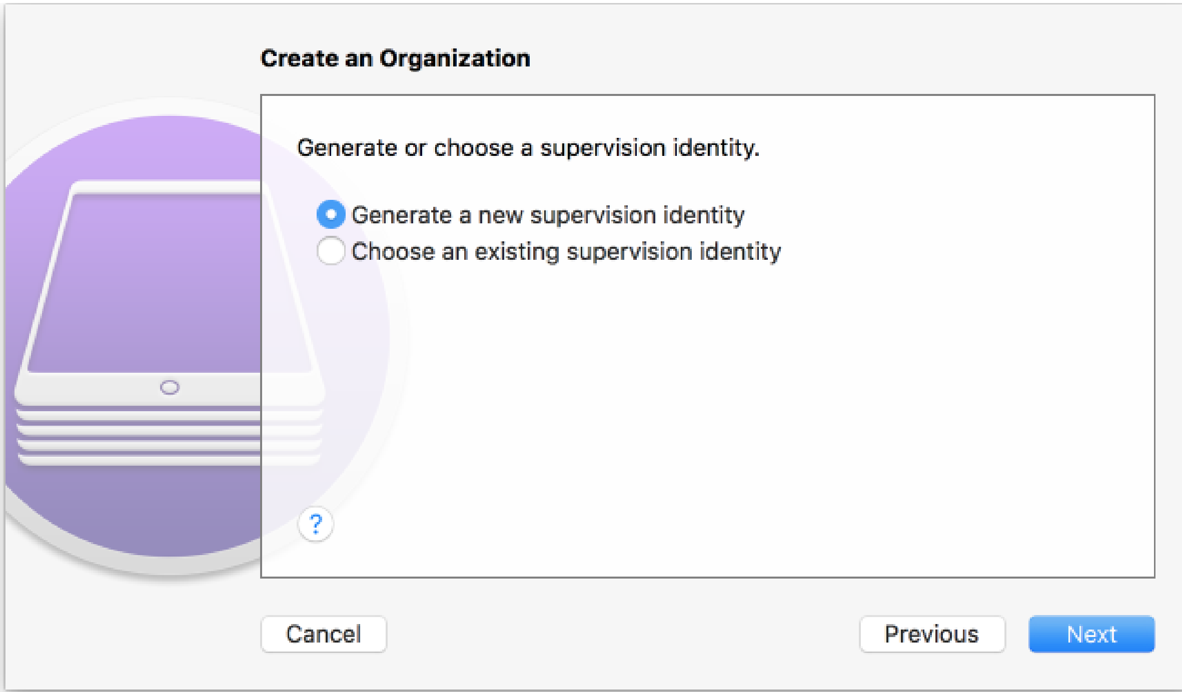
13. At the **Create an Organization** screen, select **Next.**

Figure 2-154 Selected Organization



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



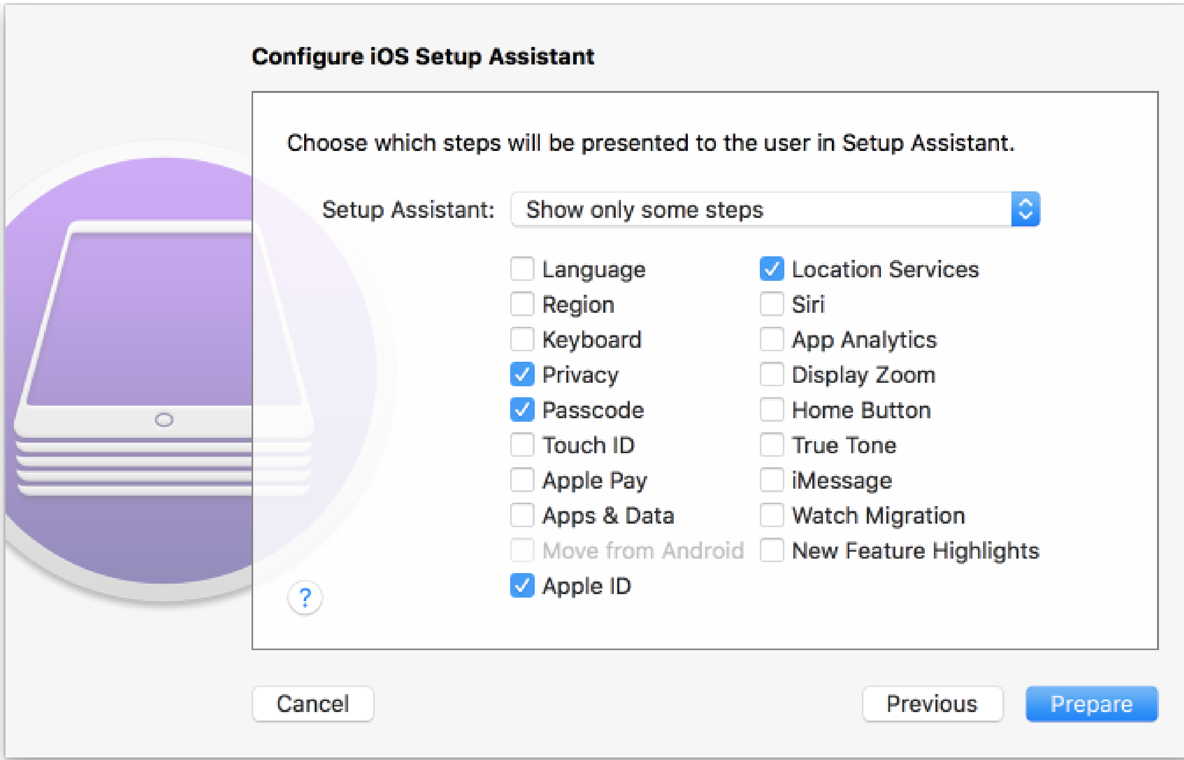
15. For the **Configure iOS Setup Assistant** step:

    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.

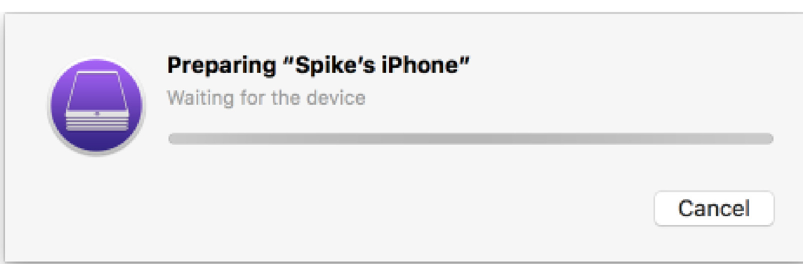
    c. Select **Prepare**.

Figure 2-156 Setup Assistant Configuration



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

Figure 2-157 Waiting for iPhone

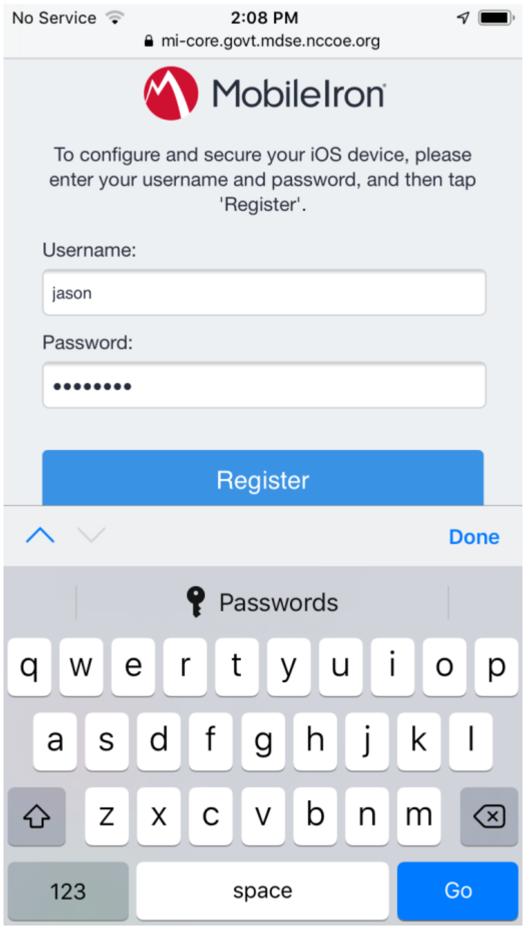


2.9.1.3 Registration with MobileIron Core

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.

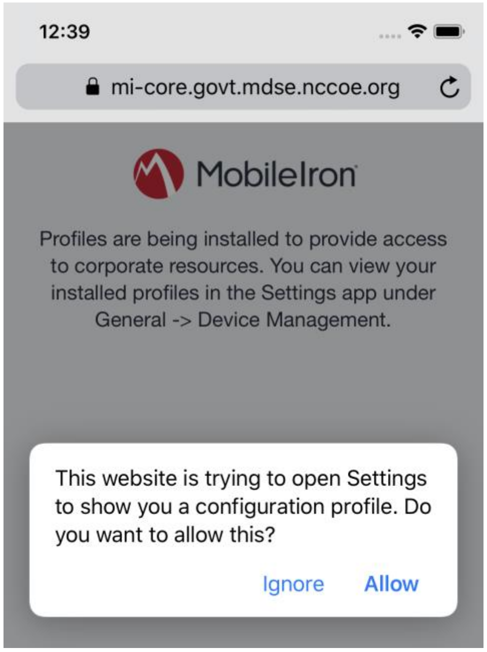
1. Using **Safari**, navigate to **MobileIron Core** page, substituting <FQDN> for that of your organization's instance of MobileIron Core. In our example implementation, the resulting URL is https://mi-core.govt.mdse.nccoe.org/go .

Figure 2-158 MobileIron Registration Page



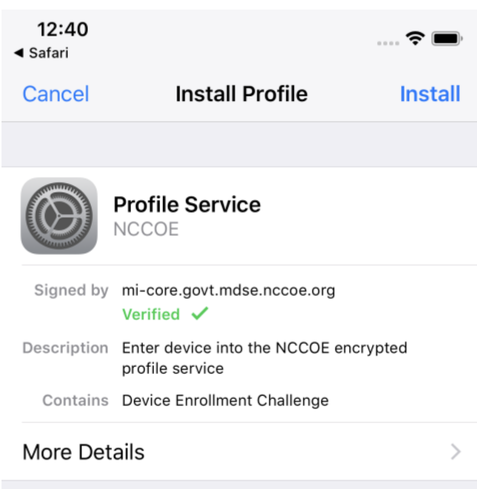
2. At the **warning** that the web site is trying to open **Settings** to show a configuration profile, select **Allow**; the **Settings** built-in app will open.

Figure 2-159 Opening Settings Confirmation



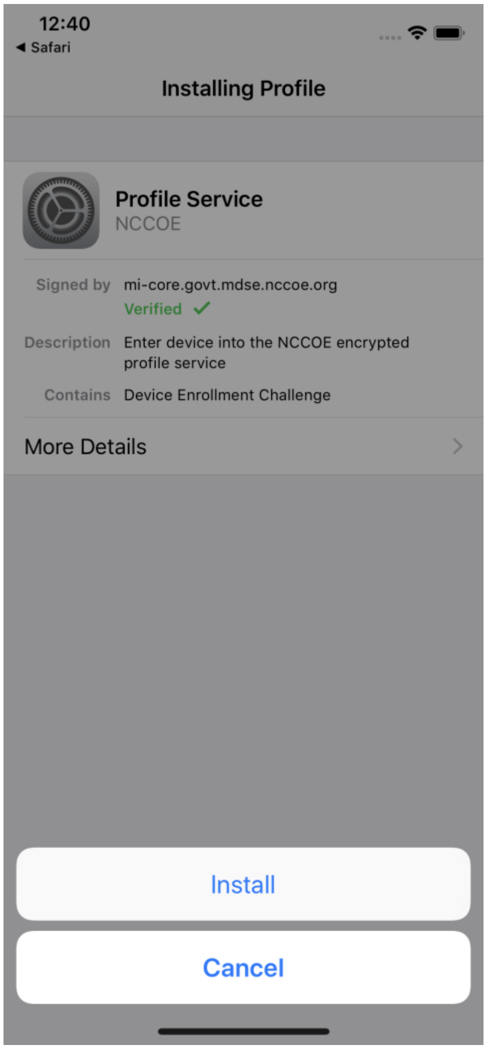
3. At the **Settings > Install Profile** screen:
   a. Verify the **Signed by** field indicates the server identity is **Verified.**
   b. Select **Install**.

Figure 2-160 Profile Installation



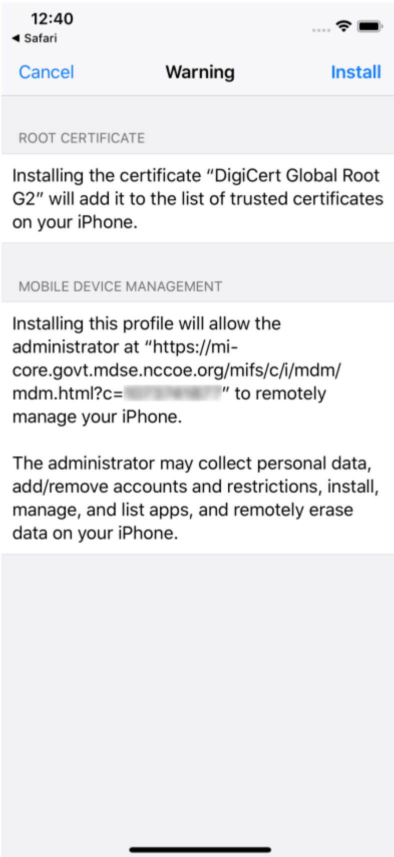
4. At the **Installing Profile** screen, select **Install**.

Figure 2-161 Profile Installation



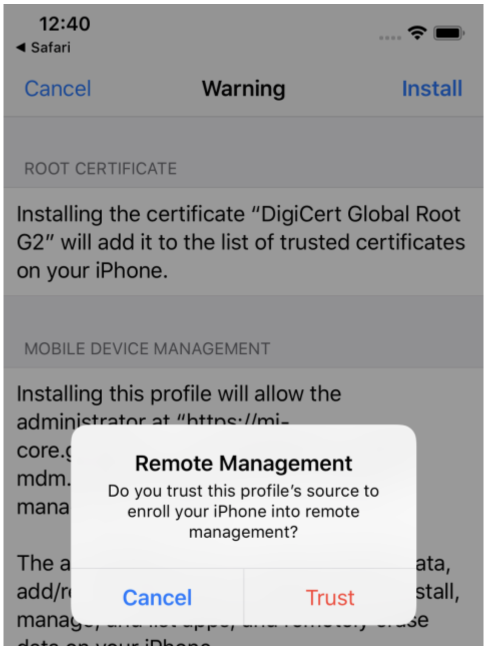
5. At the **Warning** screen:
    a. Verify that information under **Root Certificate** and **MDM** is consistent with information provided by your mobile device administrator.
    b. Select **Install**.

Figure 2-162 Profile Installation Warning



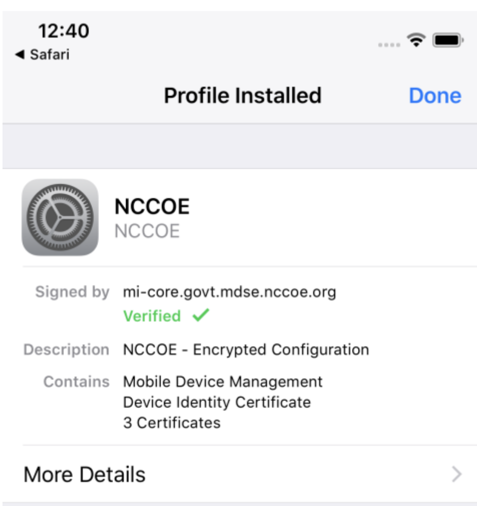
6. In the **Remote Management** dialogue, select **Trust.**

Figure 2-163 Profile Installation Trust Confirmation



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

Figure 2-164 Profile Installation Confirmation



2.9.2 Activating Lookout for Work on iOS

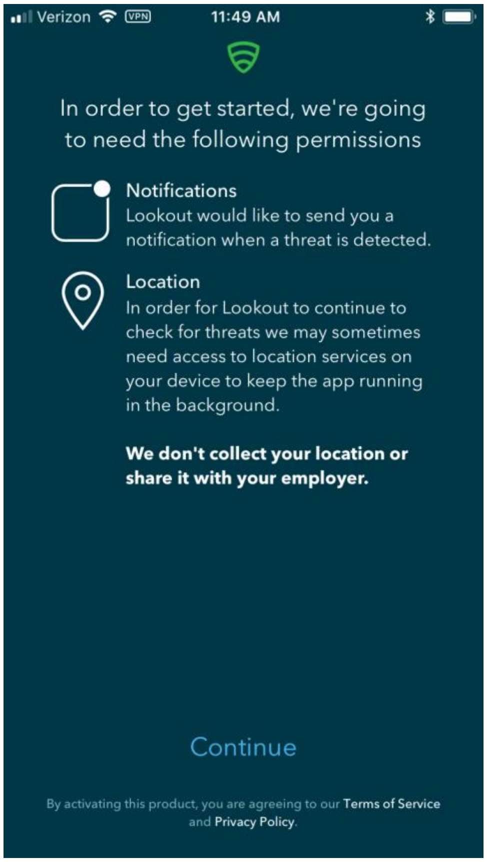
The configuration of the Lookout for Work (iOS) app in the MobileIron app catalog causes a configuration file to be included during automatic install. As a result, when a user first launches Lookout for Work, it should be activated without any user interaction. Additional action is required to grant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

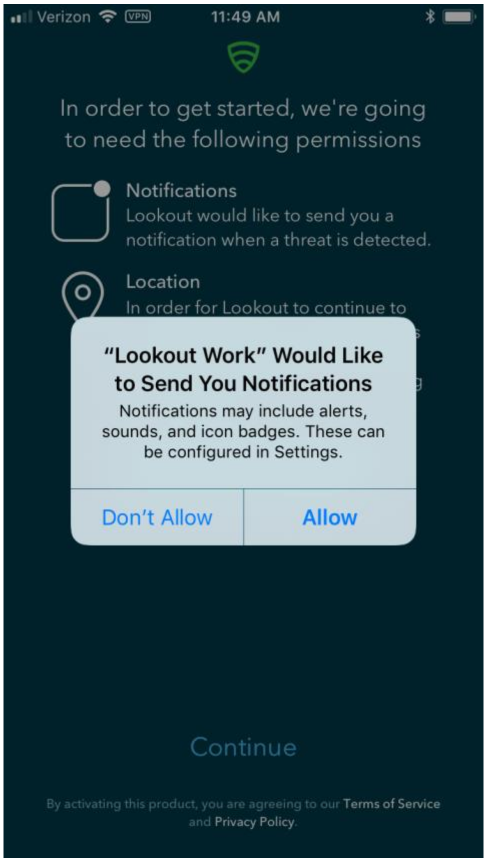
2. At the **welcome** screen, select **Continue.**

Figure 2-166 Lookout for Work Permission Information



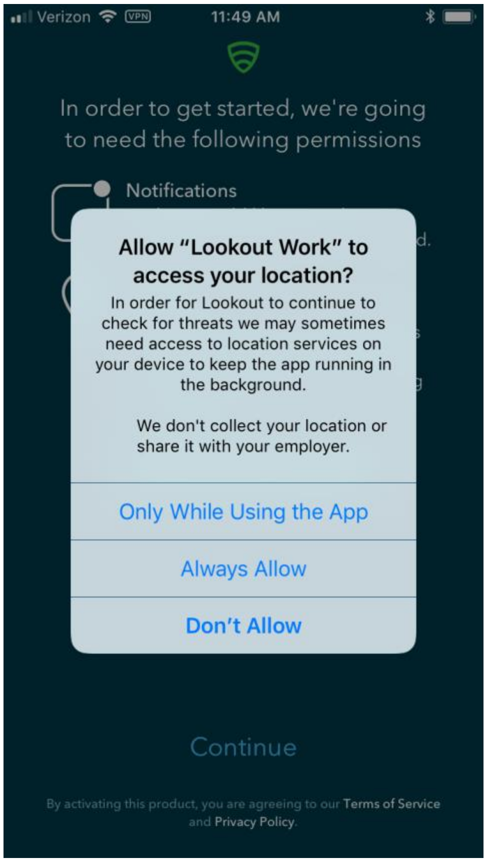
3. At the **"Lookout Work"** Would Like to Send You Notifications dialogue, select **Allow**.

Figure 2-167 Notifications Permissions Prompt



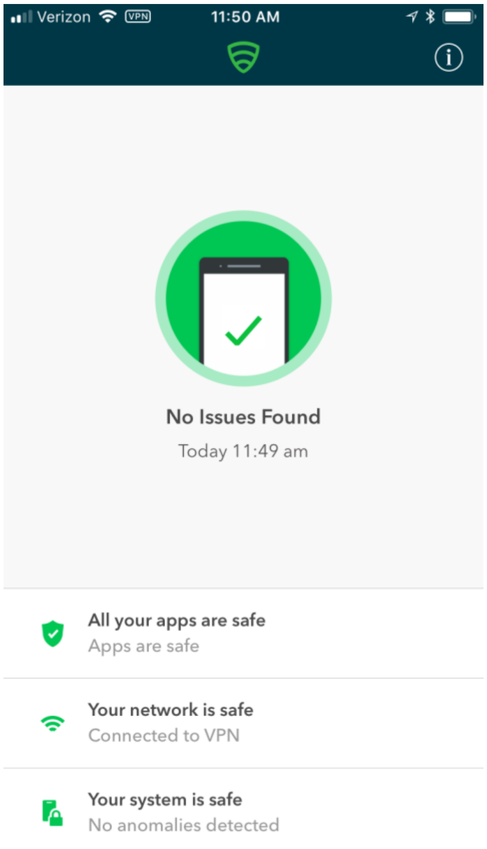
4. At the **Allow "Lookout Work" To Access Your Location?** dialogue, select **Always Allow**.

Figure 2-168 Locations Permission Prompt



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

Figure 2-169 Lookout for Work Home Screen



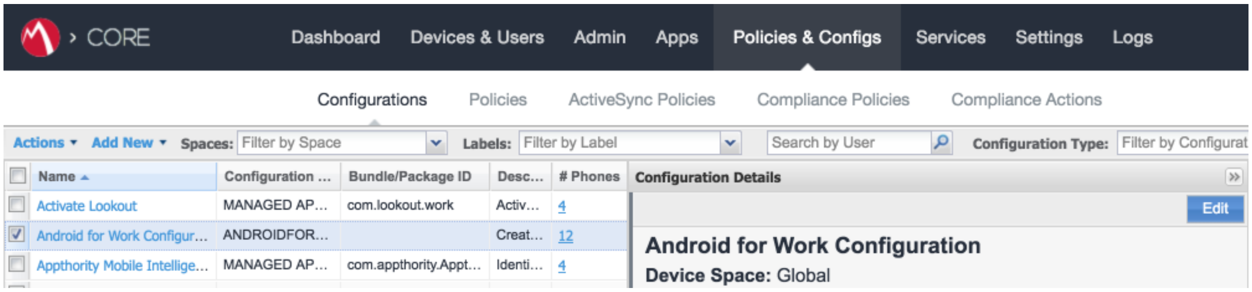
2.9.3 Provisioning Work-Managed Android Devices with a Work Profile

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

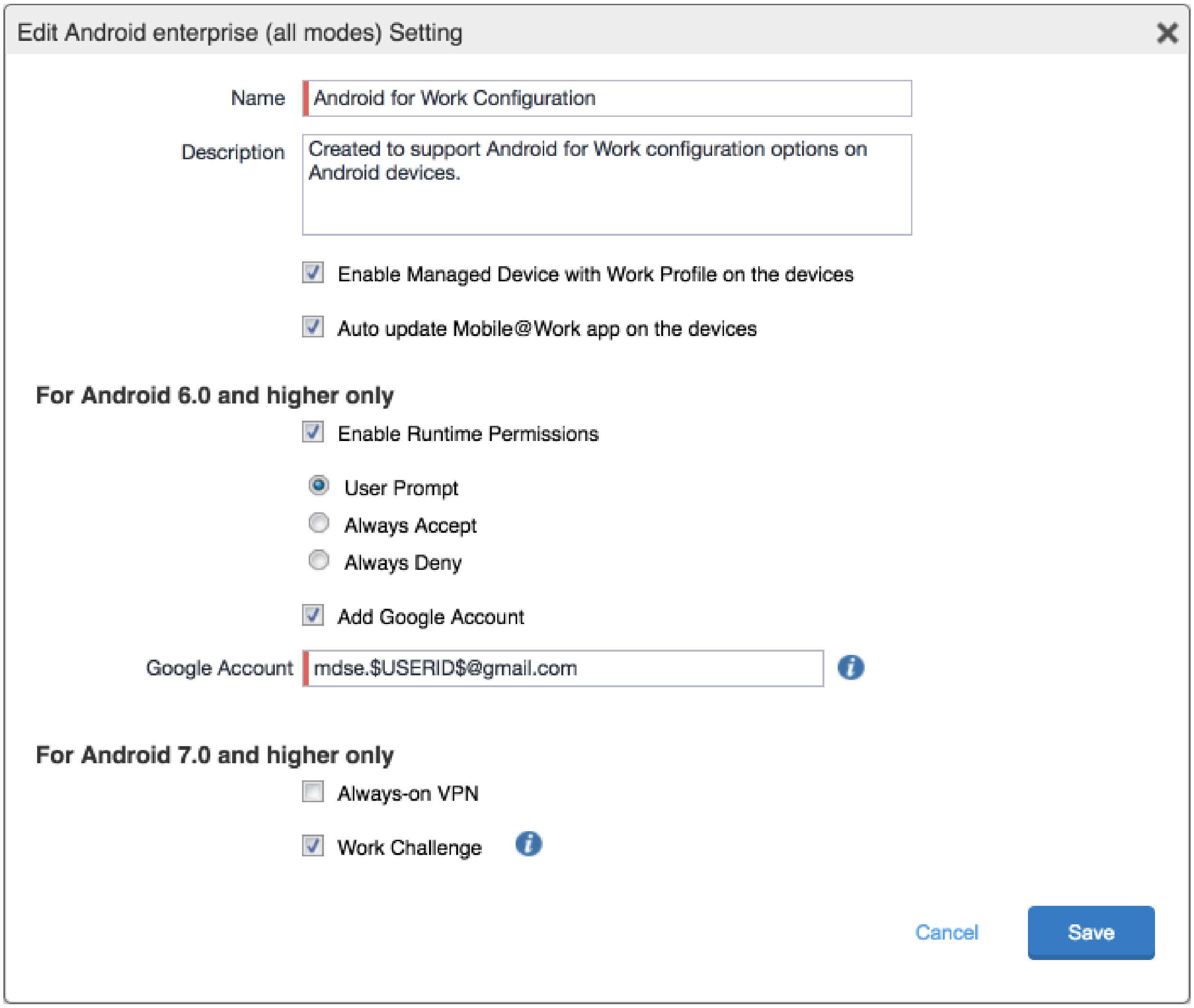
1. In the **MobileIron Admin** Portal, navigate to **Policies** > **Configs** > **Configurations**.
2. **Enable** the check box in the row for the **AFW** configuration.
3. In the **Configuration Details** pane, select **Edit**.

Figure 2-170 MobileIron AFW Configuration



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

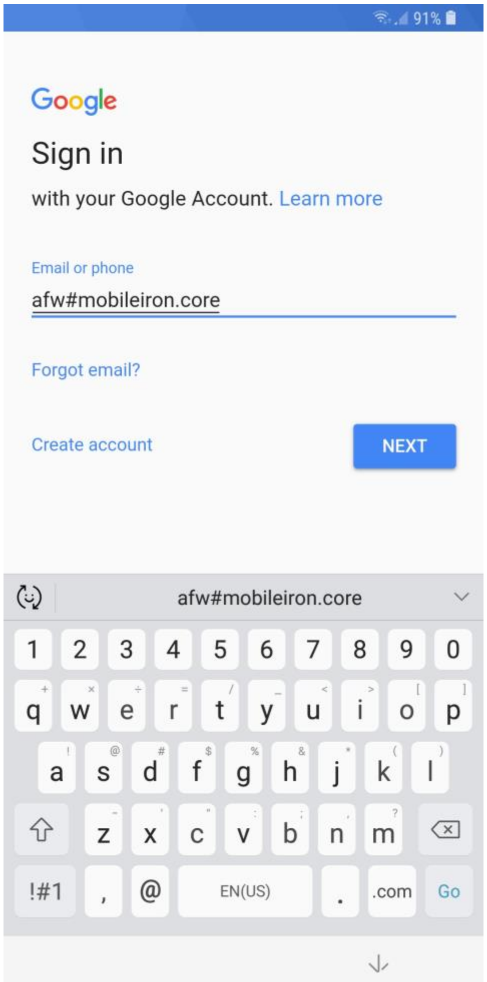


2.9.3.2 Registering Android Devices

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.

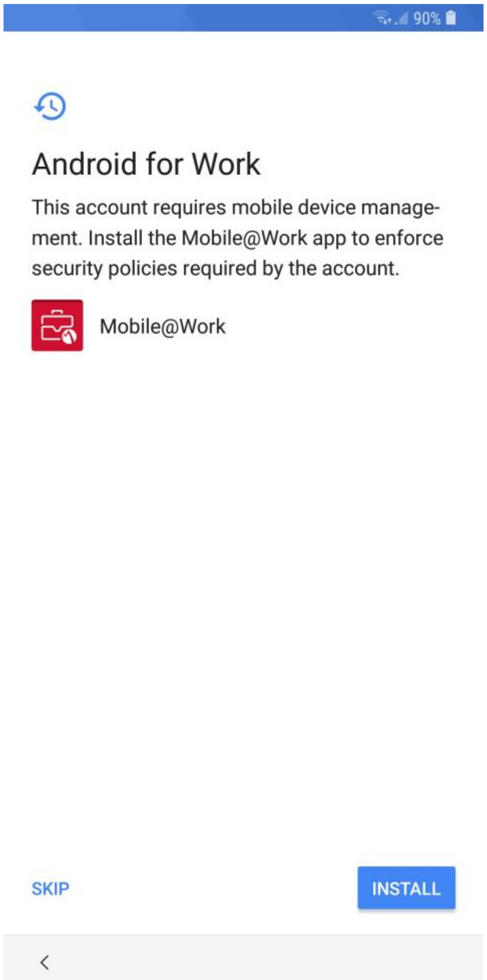
5. When prompted to **sign in** with your Google Account:
    a. In the **Email or phone field,** enter **afw#mobileiron.core**.
    b. Select **Next.**

Figure 2-172 MobileIron Enrollment Process



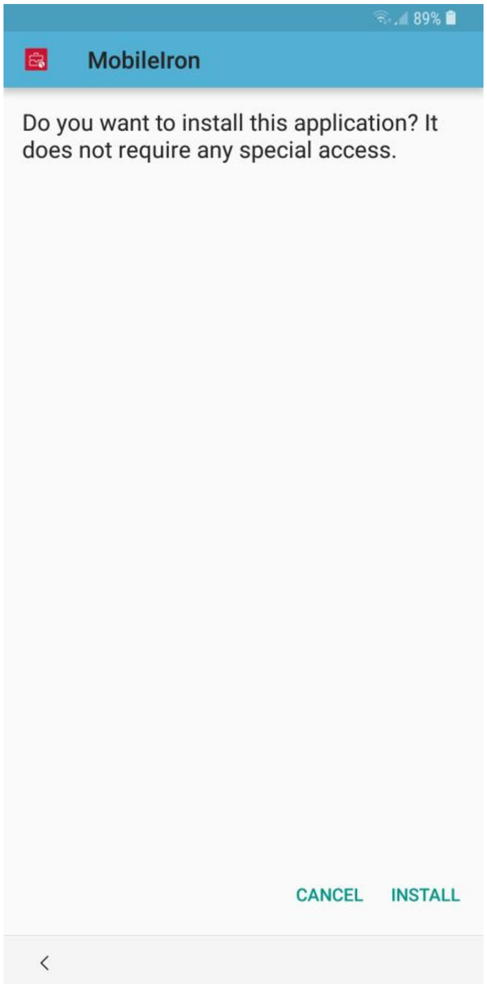
6. When **AFW** prompts you to install *Mobile@Work*, select **Install**; this will download the Mobile@Work client to the device.

Figure 2-173 AFW Enrollment



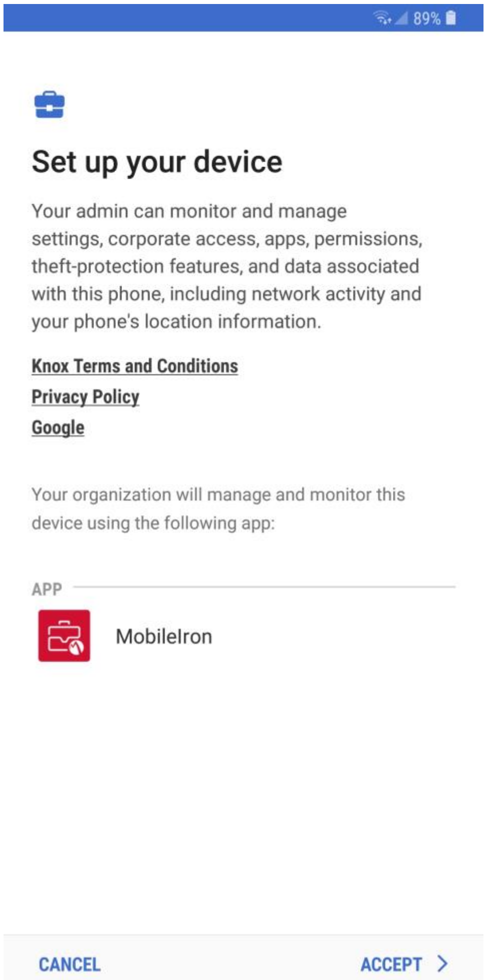
7. At the prompt to install MobileIron, select **Install.**

Figure 2-174 MobileIron Installation



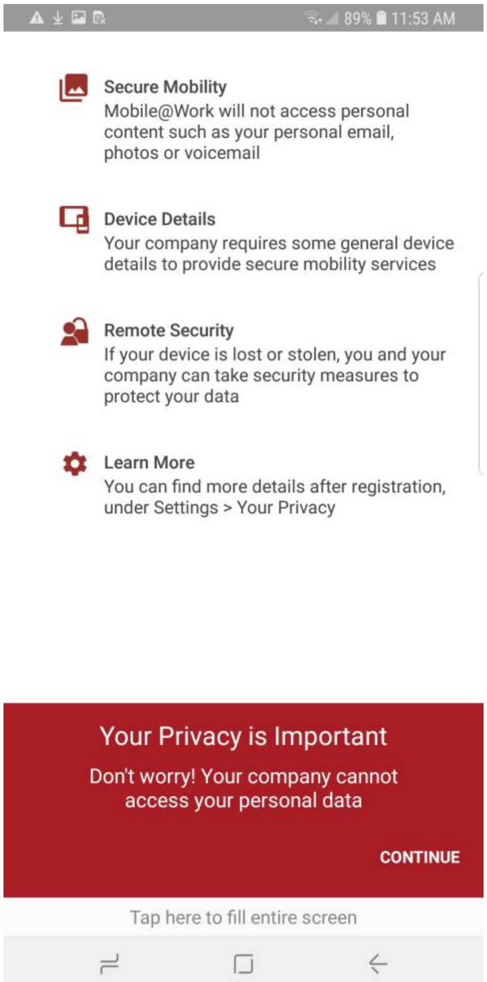
8. At the Set up your device screen, select **Accept**.

Figure 2-175 Accepting AFW Terms and Conditions



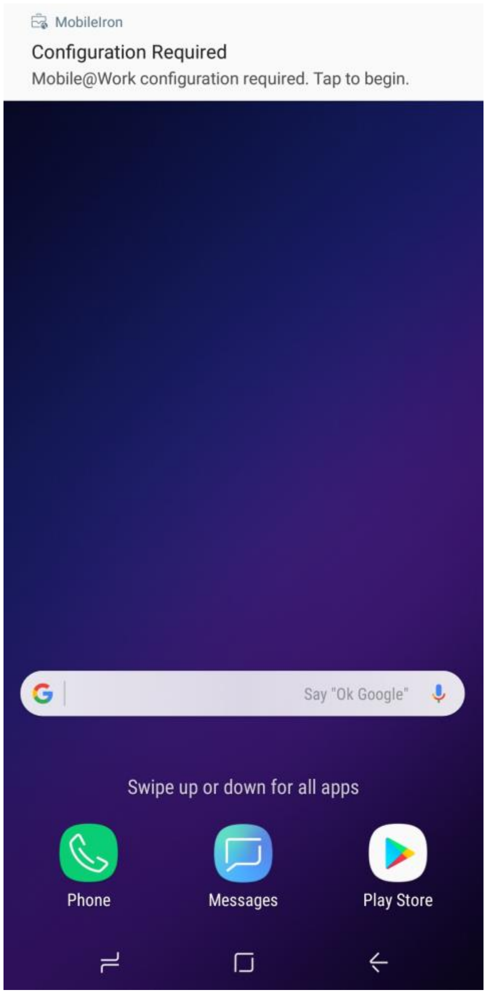
9. This screen notifies the user of the data that *Mobile@Work* collects and how it is used. When this information has been reviewed, select **Accept.** Mobile@Work will minimize and return to the operating system home screen.

Figure 2-176 MobileIron Privacy Information



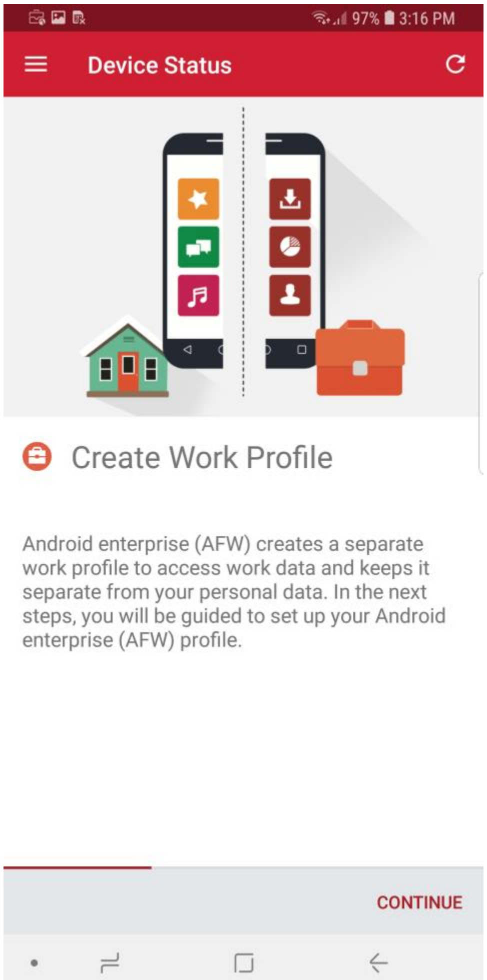
10. When MobileIron sends a **Configuration Required** notification, select the **notification.**

Figure 2-177 MobileIron Configuration Required Notification



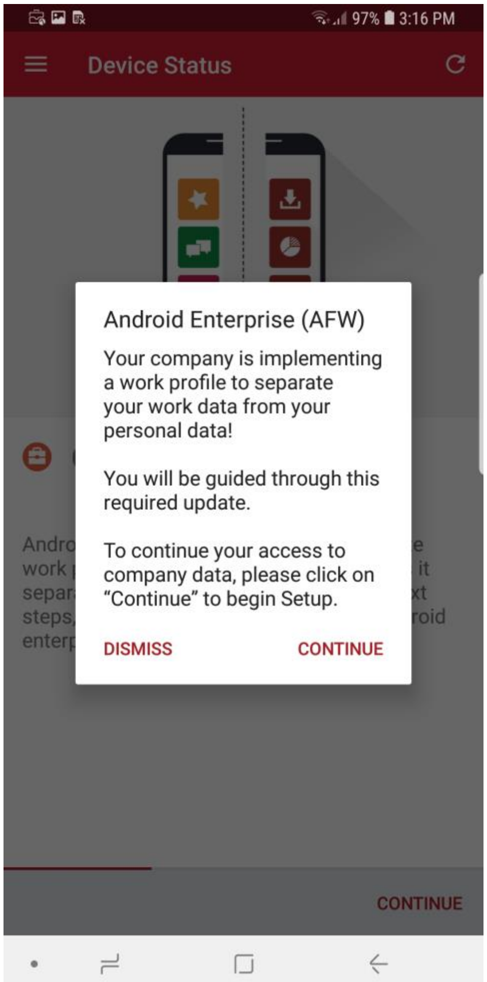
11. On the **Device Status** > **Create Work Profile** screen, select **Continue**.

Figure 2-178 MobileIron Device Status



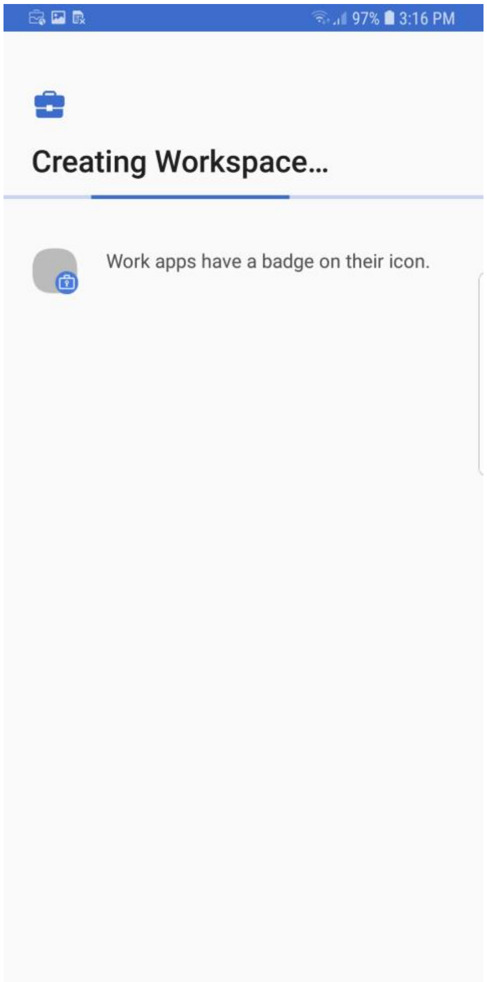
12. At the **AFW** prompt, select **Continue.**

Figure 2-179 AFW Configuration



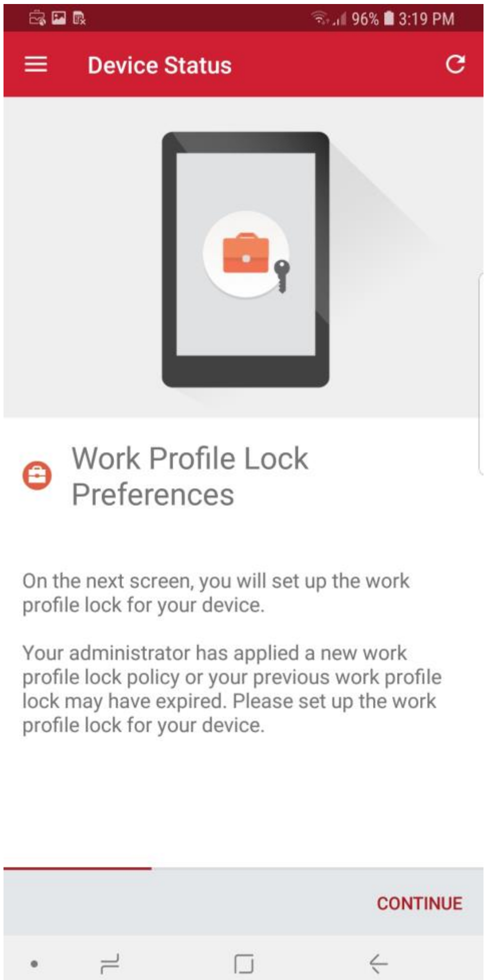
13. **AFW** will notify the user that it is creating the personal workspace. The next two screens repeat **Steps 7** and **8** as above.

Figure 2-180 AFW Workspace Creation



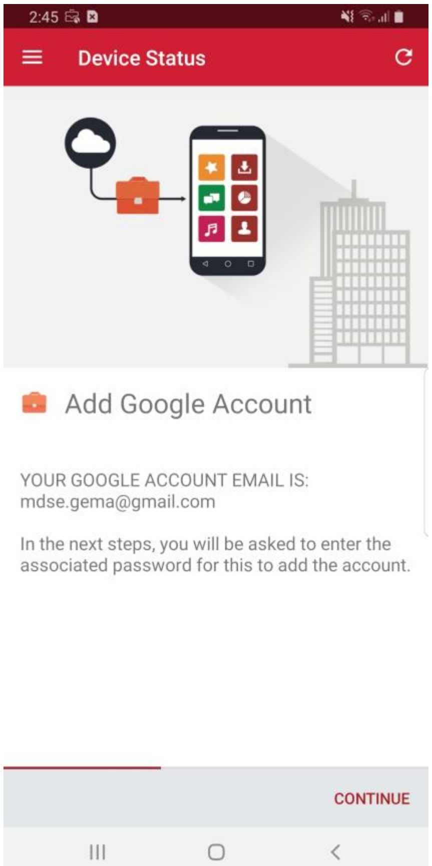
14. At the **Device Status** > **Work Profile Lock Preferences** screen, select **Continue.**

Figure 2-181 MobileIron Work Profile Lock Preferences



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.**

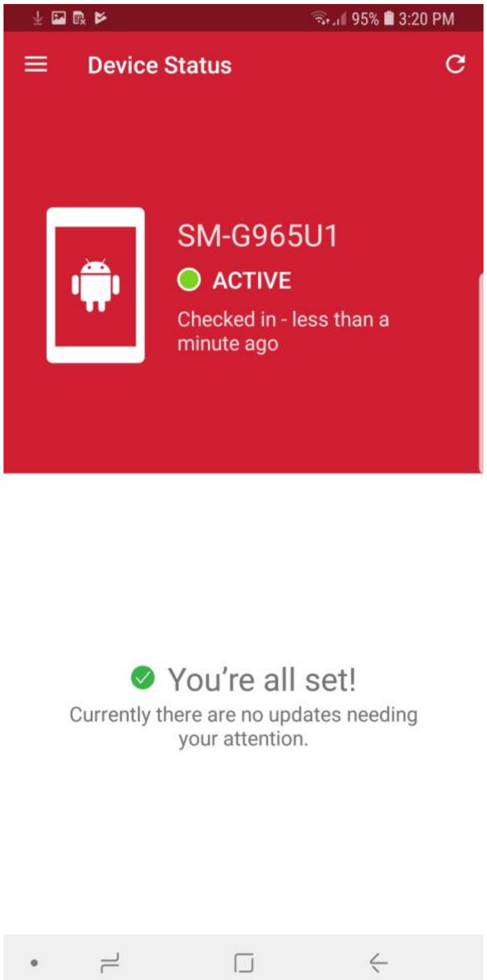
Figure 2-182 MobileIron Google Account Configuration



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.

Figure 2-183 MobileIron Device Status



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].