

## 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>

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>



# 1 Executive Summary

- 2 ▪ Mobile devices provide access to workplace data and resources that are vital for organizations  
3 to accomplish their mission while providing employees the flexibility to perform their daily  
4 activities. Securing these devices is essential to the continuity of business operations.
- 5 ▪ While mobile devices can increase organizations' efficiency and employee productivity, they can  
6 also leave sensitive data vulnerable. Addressing such vulnerabilities requires mobile device  
7 management tools to help secure access to the network and resources. These tools are different  
8 from those required to secure the typical computer workstation.
- 9 ▪ To address the challenge of securing mobile devices while managing risks, the National  
10 Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and  
11 Technology (NIST) built a laboratory environment to explore how various mobile security  
12 technologies can be integrated within an enterprise's network.
- 13 ▪ This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-  
14 based, commercially available products to help meet their mobile device security and privacy  
15 needs.

## 16 **CHALLENGE**

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

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

## 28 **SOLUTION**

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

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

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

40 This guide provides:

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

47 The NCCoE sought existing technologies that provided the following capabilities:

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

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

56 While the NCCoE used a suite of commercial products to address this challenge, this guide does not  
57 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your  
58 organization's information security experts should identify the products that will best integrate with  
59 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that  
60 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
61 implementing parts of a solution.

## 62 **BENEFITS**

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

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

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

## 78     **SHARE YOUR FEEDBACK**

79 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  
80 you read the guide. If you adopt this solution for your own organization, please share your experience  
81 and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our  
82 solution, so we encourage organizations to share lessons learned and best practices for transforming the  
83 processes associated with implementing this guide.

85 To provide comments or to learn more by arranging a demonstration of this example implementation,  
86 contact the NCCoE at [mobile-nccoe@nist.gov](mailto:mobile-nccoe@nist.gov).

---

## 87     **TECHNOLOGY PARTNERS/COLLABORATORS**

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



93

94 Certain commercial entities, equipment, products, or materials may be identified by name or company  
95 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an  
96 experimental procedure or concept adequately. Such identification is not intended to imply special  
97 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it  
98 intended to imply that the entities, equipment, products, or materials are necessarily the best available  
99 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>



## 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 1800-21B 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](mailto: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](mailto:nccoe@nist.gov)

## 1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 17 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 27 **ABSTRACT**

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

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

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

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

## 40 **KEYWORDS**

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

## 43 **ACKNOWLEDGMENTS**

44 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 Gogoiel    | 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 |

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

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

## 49 **Contents**

|    |  |           |
|----|--|-----------|
| 50 | <b>1 Summary.....</b>  | <b>1</b>  |
| 51 | 1.1 Challenge.....   | 2         |
| 52 | 1.2 Solution.....  | 2         |
| 53 | 1.2.1 Standards and Guidance .....   | 3         |
| 54 | 1.3 Benefits.....  | 5         |
| 55 | <b>2 How to Use This Guide .....</b>   | <b>5</b>  |
| 56 | 2.1 Typographic Conventions.....   | 7         |
| 57 | <b>3 Approach.....</b>   | <b>7</b>  |
| 58 | 3.1 Audience.....  | 8         |
| 59 | 3.2 Scope .....  | 8         |
| 60 | 3.2.1 Orvilia Development .....  | 9         |
| 61 | 3.3 Assumptions .....  | 10        |
| 62 | 3.3.1 Systems Engineering .....  | 11        |
| 63 | 3.4 Risk Assessment .....  | 11        |
| 64 | 3.4.1 Risk Assessment of the Fictional Organization Orvilia Development..... | 13        |
| 65 | 3.4.2 Development of Threat Event Descriptions.....                          | 14        |
| 66 | 3.4.3 Identification of Vulnerabilities and Predisposing Conditions.....     | 22        |
| 67 | 3.4.4 Summary of Risk Assessment Findings .....                              | 22        |
| 68 | 3.4.5 Privacy Risk Assessment .....  | 24        |
| 69 | 3.5 Preliminary Solution Goals .....   | 26        |
| 70 | 3.5.1 Current Architecture.....  | 26        |
| 71 | 3.5.2 Preliminary Security Goals .....                                       | 28        |
| 72 | 3.6 Technologies.....  | 29        |
| 73 | 3.6.1 Architecture Components.....   | 29        |
| 74 | <b>4 Architecture .....</b>  | <b>34</b> |
| 75 | 4.1 Architecture Description .....   | 35        |
| 76 | 4.1.1 Enterprise Integration.....  | 36        |

|     |  |           |
|-----|--|-----------|
| 77  | 4.1.2 Mobile Component Integration .....   | 37        |
| 78  | 4.2 Enterprise Security Architecture Privacy Data Map.....   | 42        |
| 79  | 4.3 Security Control Map.....  | 43        |
| 80  | <b>5 Security Characteristic Analysis .....</b>  | <b>43</b> |
| 81  | 5.1 Assumptions and Limitations .....  | 43        |
| 82  | 5.2 Build Testing .....  | 43        |
| 83  | 5.2.1 Threat Event 1 —Unauthorized Access to Sensitive Information via a Malicious or<br>84              Privacy-Intrusive Application .....   | 44        |
| 85  | 5.2.2 Threat Event 2 —Theft of Credentials Through an SMS or Email Phishing Campaign   | 44        |
| 86  | 5.2.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages  |           |
| 87  | 45   |           |
| 88  | 5.2.4 Threat Event 4 —Confidentiality and Integrity Loss due to Exploitation of Known<br>89              Vulnerability in the OS or Firmware .....   | 46        |
| 90  | 5.2.5 Threat Event 5 —Violation of Privacy via Misuse of Device Sensors.....   | 46        |
| 91  | 5.2.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network<br>92              Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles, or<br>93              Certificates ..... | 47        |
| 94  | 5.2.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on<br>95              Unencrypted Device Communications .....  | 48        |
| 96  | 5.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-<br>97              Forced device Unlock Code.....  | 49        |
| 98  | 5.2.9 Threat Event 9—Unauthorized Access to Backend Services via authentication or<br>99              credential Storage Vulnerabilities in Internally Developed Applications .....                                    | 50        |
| 100 | 5.2.10 Threat Event 10 —Unauthorized Access of Enterprise Resources from an Unmanaged<br>101              and Potentially Compromised Device.....  | 50        |
| 102 | 5.2.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device .....  | 50        |
| 103 | 5.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its<br>104              Unauthorized Storage in Non-Organizationally Managed Services.....  | 51        |
| 105 | 5.3 Scenarios and Findings .....   | 52        |
| 106 | 5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings.....  | 53        |
| 107 | 5.3.2 Threat Event Scenarios and Findings .....  | 53        |
| 108 | 5.3.3 Data Action Scenarios and Findings .....   | 55        |
| 109 | <b>6 Conclusion.....</b>   | <b>56</b> |

|     |  |            |
|-----|--|------------|
| 110 | <b>7 Future Build Considerations .....</b>   | <b>57</b>  |
| 111 | <b>Appendix A List of Acronyms .....</b>   | <b>58</b>  |
| 112 | <b>Appendix B Glossary .....</b>   | <b>60</b>  |
| 113 | <b>Appendix C References.....</b>  | <b>66</b>  |
| 114 | <b>Appendix D Android, Apple, and Samsung Knox Mobile Enrollment.....</b>  | <b>78</b>  |
| 115 | D.1 Android Devices.....   | 78         |
| 116 | D.2 iOS Devices .....  | 78         |
| 117 | D.3 Samsung Knox Devices .....   | 78         |
| 118 | <b>Appendix E Risk Assessment .....</b>  | <b>79</b>  |
| 119 | E.1 Risk Assessment .....  | 79         |
| 120 | <b>Appendix F Privacy Risk Assessment .....</b>  | <b>101</b> |
| 121 | F.1 Data Action 1: Blocking Access and Wiping Devices .....  | 103        |
| 122 | F.2 Data Action 2: Employee Monitoring.....  | 104        |
| 123 | F.3 Data Action 3: Data Sharing Across Parties.....  | 105        |
| 124 | F.4 Mitigations Applicable Across Various Data Actions .....   | 107        |
| 125 | <b>Appendix G Threat Event Test Information .....</b>  | <b>108</b> |
| 126 | G.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or<br>Privacy-Intrusive Application.....   | 108        |
| 127 | G.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or Email<br>Phishing Campaign .....  | 108        |
| 128 | G.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages<br>.....   | 109        |
| 129 | G.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known<br>Vulnerability in the Operating System or Firmware .....  | 114        |
| 130 | G.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors.....  | 116        |
| 131 | G.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network<br>Communications via Installation of Malicious EMM/Mobile Device Management,<br>Network, Virtual Private Network (VPN) Profiles, or Certificates..... | 116        |

|     |   |            |
|-----|---|------------|
| 138 | G.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping on Unencrypted Device Communications.....                               | 121        |
| 140 | G.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-Forced Device Unlock Code.....   | 122        |
| 142 | G.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications..... | 123        |
| 144 | G.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an Unmanaged and Potentially Compromised Device .....                                   | 124        |
| 146 | G.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device .....   | 125        |
| 147 | G.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its Unauthorized Storage in Non-Organizationally Managed Services.....             | 126        |
| 149 | <b>Appendix H Example Security Control Map .....</b>  | <b>127</b> |

## 150 **List of Figures**

|     |   |     |
|-----|---|-----|
| 151 | <b>Figure 3-1 Risk Management Approach.....</b>   | 10  |
| 152 | <b>Figure 3-2 Risk Assessment Process .....</b>   | 12  |
| 153 | <b>Figure 3-3 NIST 800-30 Generic Risk Model .....</b>  | 13  |
| 154 | <b>Figure 3-4 Orvilia’s Mobile Deployment Before Security Enhancements.....</b>                       | 27  |
| 155 | <b>Figure 3-5 Orvilia’s Preliminary Security Goals .....</b>  | 28  |
| 156 | <b>Figure 4-1 Example Solution Architecture .....</b>   | 35  |
| 157 | <b>Figure 4-2 Example Solution Gateway Architecture .....</b>   | 37  |
| 158 | <b>Figure 4-3 Example Solution VPN Architecture.....</b>  | 40  |
| 159 | <b>Figure 4-4 NIST Privacy Risk Assessment Methodology Data Map for Orvilia’s Enterprise Security</b> |     |
| 160 | <b>Architecture.....</b>  | 42  |
| 161 | <b>Figure E-1 Risk Assessment Process .....</b>   | 80  |
| 162 | <b>Figure E-2 NIST 800-30 Generic Risk Model .....</b>  | 83  |
| 163 | <b>Figure F-1 PRAM Data Map for Orvilia’s Enterprise Security Architecture.....</b>                   | 102 |
| 164 | <b>Figure G-1 Setting a Custom Risk Level in Appthority .....</b>                                     | 108 |
| 165 | <b>Figure G-2 PAN-DB Blocked Website.....</b>   | 109 |
| 166 | <b>Figure G-3 Lock Screen and Security.....</b>   | 110 |
| 167 | <b>Figure G-4 Phishing Email on Android .....</b>   | 110 |
| 168 | <b>Figure G-5 Phishing Email on iOS .....</b>   | 111 |
| 169 | <b>Figure G-6 Untrusted Developer Warning .....</b>   | 111 |
| 170 | <b>Figure G-7 Application Signing Certificates.....</b>   | 112 |
| 171 | <b>Figure G-8 Restriction Setting Modification Screen.....</b>  | 113 |
| 172 | <b>Figure G-9 Unable to Trust Developer.....</b>  | 113 |
| 173 | <b>Figure G-10 Unknown Sources Detection .....</b>  | 114 |
| 174 | <b>Figure G-11 Vulnerability Identification .....</b>   | 115 |
| 175 | <b>Figure G-12 Patch Level Display .....</b>  | 115 |
| 176 | <b>Figure G-13 Kryptowire Analysis Report.....</b>  | 116 |
| 177 | <b>Figure G-14 Configuration Profile Example.....</b>   | 117 |

|     |   |     |
|-----|---|-----|
| 178 | <a href="#">Figure G-15 Configuration Profile Phishing Email</a>          | 118 |
| 179 | <a href="#">Figure G-16 Root Certificate Authority Enablement Warning</a> | 118 |
| 180 | <a href="#">Figure G-17 Reversed Web Page</a>                             | 119 |
| 181 | <a href="#">Figure G-18 Certificate Phishing Email</a>                    | 120 |
| 182 | <a href="#">Figure G-19 Reversed Web Page</a>                             | 120 |
| 183 | <a href="#">Figure G-20 Network Attack Detected</a>                       | 121 |
| 184 | <a href="#">Figure G-21 Unencrypted Data Transfer</a>                     | 122 |
| 185 | <a href="#">Figure G-22 Lock Screen Disabled Detection Notice</a>         | 123 |
| 186 | <a href="#">Figure G-23 Hard-Coded Credentials</a>                        | 124 |
| 187 | <a href="#">Figure G-24 No Certificates Found on Android</a>              | 125 |
| 188 | <a href="#">Figure G-25 No Certificates Found on iOS</a>                  | 125 |
| 189 | <a href="#">Figure G-26 Android Device Wipe Warning</a>                   | 126 |
| 190 | <a href="#">Figure G-27 Disallowing Screenshots and Screen Recording</a>  | 126 |

**191 List of Tables**

|     |   |            |
|-----|---|------------|
| 192 | <b>Table 3-1 Threat Event Mapping to the Mobile Threat Catalogue .....</b>                  | <b>14</b>  |
| 193 | <b>Table 3-2 Identify Vulnerabilities and Predisposing Conditions .....</b>                 | <b>22</b>  |
| 194 | <b>Table 3-3 Summary of Risk Assessment Findings .....</b>                                  | <b>22</b>  |
| 195 | <b>Table 4-1 Commercially Available Products Used .....</b>                                 | <b>34</b>  |
| 196 | <b>Table 5-1 Threat Event Scenarios and Findings Summary.....</b>                           | <b>53</b>  |
| 197 | <b>Table 5-2 Data Action Scenarios and Findings Summary.....</b>                            | <b>55</b>  |
| 198 | <b>Table E-1 Threat Sources of Concern.....</b>   | <b>87</b>  |
| 199 | <b>Table E-2 Threat Sources Qualitative Scale.....</b>                                      | <b>88</b>  |
| 200 | <b>Table E-3 Identify Vulnerabilities and Predisposing Conditions .....</b>                 | <b>92</b>  |
| 201 | <b>Table E-4 Likelihood of Threat Events of Concern .....</b>                               | <b>94</b>  |
| 202 | <b>Table E-5 Potential Adverse Impacts.....</b>   | <b>95</b>  |
| 203 | <b>Table E-6 Summary of Risk Assessment Findings .....</b>                                  | <b>98</b>  |
| 204 | <b>Table H-1 Example Solution’s Cybersecurity Standards and Best Practices Mapping.....</b> | <b>128</b> |

## 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

238 the basis for a custom solution that realizes the security and privacy characteristics that best support its  
239 unique mobile device usage scenario.

## 240 **1.1 Challenge**

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

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

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

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

## 257 **1.2 Solution**

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

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

270 This guide provides:

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

276 The NCCoE sought existing technologies that provided the following capabilities:

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

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

### 285 1.2.1 Standards and Guidance

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

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

- 302       ■ NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD)*  
303            *Security* [16]
- 304       ■ NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the*  
305            *Enterprise* [17]
- 306       ■ NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [18]
- 307       ■ NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and*  
308            *Organizations* [19]
- 309       ■ NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce*  
310            *Framework* [20]
- 311       ■ Center for Internet Security [21]
- 312       ■ Executive Office of the President, *Bring Your Own Device Toolkit* [22]
- 313       ■ Federal Chief Information Officers (CIO) Council and Department of Homeland Security (DHS)  
314            *Mobile Security Reference Architecture, Version 1.0* [23]
- 315       ■ Digital Services Advisory Group and Federal Chief Information Officers Council, *Government Use*  
316            *of Mobile Technology Barriers, Opportunities, and Gap Analysis* [24]
- 317       ■ International Organization for Standardization (ISO), International Electrotechnical Commission  
318            (IEC) 27001:2013, *Information technology—Security techniques—Information security*  
319            *management systems—Requirements* [25]
- 320       ■ Mobile Computing Decision Example Case Study [26]
- 321       ■ Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center  
322            (ATARC), *Mobility Strategy Development Guidelines Working Group Document* [27]
- 323       ■ MSCT ATARC, *Mobile Threat Protection App Vetting and App Security Working Group Document*  
324            [28]
- 325       ■ MSCT, *Device Procurement and Management Guidance* [29]
- 326       ■ MSCT, *Mobile Device Management (MDM)*, *MDM Working Group Document* [30]
- 327       ■ MSCT, *Mobile Services Roadmap, MSCT Strategic Approach* [31]
- 328       ■ NIAP U.S. Government Approved Protection Profile—*Extended Package for Mobile Device*  
329            *Management Agents Version 3.0* [32]
- 330       ■ NIAP U.S. Government Approved Protection Profile—*Protection Profile for Mobile Device*  
331            *Fundamentals Version 3.1* [33]
- 332       ■ NIAP U.S. Government Approved Protection Profile—*Protection Profile for Mobile Device*  
333            *Management Version 3.0* [34]
- 334       ■ NIAP Product Compliant List [35]

- 335       ■ United States Office of Management and Budget (OMB), Category Management Policy 16-3:  
336           Improving the Acquisition and Management of Common Information Technology: Mobile  
337           Devices and Services [36]  
338       ■ The United States Government Configuration Baseline (USGCB) [37]  
339       ■ United State Department of Homeland Security (DHS) Study on Mobile Device Security [38]  
340 Note that Defense Federal Acquisition Regulation Supplement regulations are out of scope for this  
341 effort.

### 342     **1.3 Benefits**

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

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

## 356     **2 How to Use This Guide**

357 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides  
358 users with the information they need to replicate how to improve mobile device security with on-  
359 premises mobile device management solutions. This reference design is modular and can be deployed in  
360 whole or in part.

361 This guide contains three volumes:

- 362       ■ NIST SP 1800-21A: *Executive Summary*  
363       ■ NIST SP 1800-21B: *Approach, Architecture, and Security Characteristics* – what we built and why  
364           (**you are here**)

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

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

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

- 369       ■ challenges that enterprises face in securing mobile devices from threats that are distinct from  
370 traditional desktop platforms
- 371       ■ example solution built at the NCCoE
- 372       ■ benefits of adopting the example solution

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

- 376       ■ [Section 3.4](#), Risk Assessment, provides a description of the risk analysis we performed
- 377       ■ [Section 4.3](#), Security Control Map, maps the security characteristics of this example solution to  
378 cybersecurity standards and best practices

379 You might share the *Executive Summary, NIST SP 1800-21A*, with your leadership team members to help  
380 them understand the importance of adopting standards-based solutions to improve mobile device  
381 security with on-premises mobile device management solutions.

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

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

397 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a  
398 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and

399 success stories will improve subsequent versions of this guide. Please contribute your thoughts to  
 400 [mobile-nccoe@nist.gov.](mailto:mobile-nccoe@nist.gov)

## 401 **2.1 Typographic Conventions**

402 The following table presents typographic conventions used in this volume.

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

## 403 **3 Approach**

404 The NIST build team surveyed reports of mobile device security trends and openly invited the mobile  
 405 device security community—including vendors, researchers, administrators, and users—to engage in a  
 406 discussion about pressing cybersecurity challenges. The community expressed two significant messages.  
 407 First, administrators experienced confusion about which policies and standards—out of myriad  
 408 sources—should be implemented. Second, mobile device users were frustrated by the degrees to which  
 409 enterprises have control over their mobile devices and maintain visibility into their personal activity.

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

### 414 **3.1 Audience**

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

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

### 424 **3.2 Scope**

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

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

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

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

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

443    **3.2.1 Orvilia Development**

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

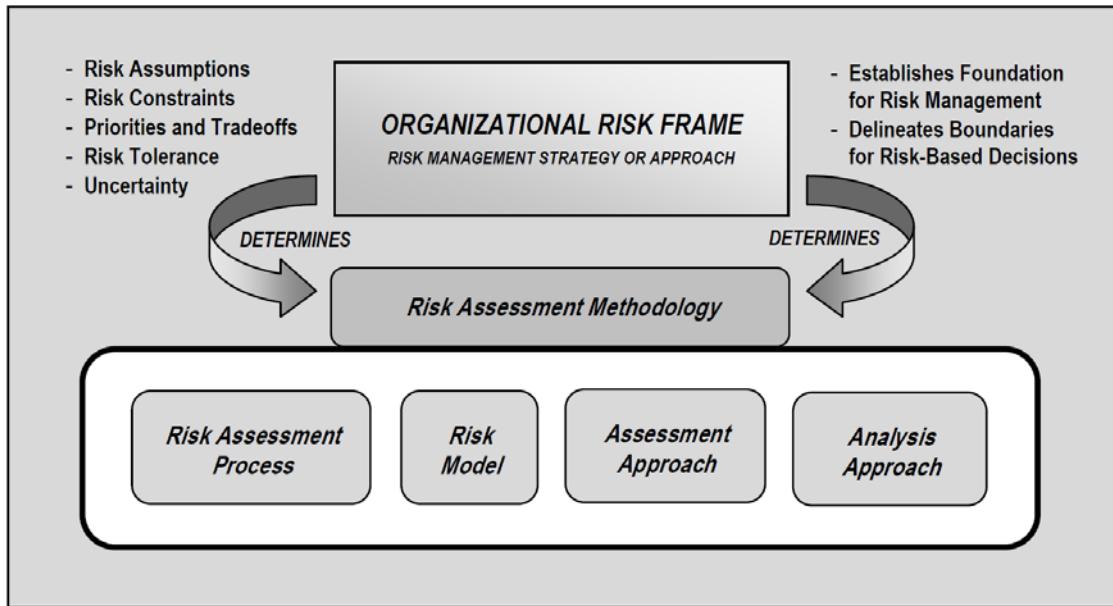
450    Orvilia has a simple deployment of on-premises IT resources. It hosts its own Microsoft Active Directory  
451    domain, Microsoft Exchange email server, and web-based resources for employees, such as timekeeping  
452    and travel support. All enterprise resources can be directly accessed by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

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

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

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

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

477 **Figure 3-1 Risk Management Approach**

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

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

### 487 **3.3 Assumptions**

488 This project is guided by the following assumptions:

- 489     ■ 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.
- 491     ■ An organization has access to the skills and resources required to implement a mobile device  
       security solution.
- 493     ■ 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

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

- 501 ▪ Organizations have either already invested or are willing to invest in the security of mobile  
502 devices used within their organization and of their IT systems more broadly. As such, we assume  
503 they either have the technology in place to support this implementation or have access to the  
504 off-the shelf information security technology used in this build, which we assume will perform as  
505 described by the respective product vendor.
- 506 ▪ Organizations have familiarized themselves with existing standards and any associated  
507 guidelines (e.g., NIST Cybersecurity Framework [5], NIST SP 800-124 Revision 1 [17], NIST SP  
508 1800-4 [8]) relevant to implementation of the solution proposed in this practice guide. We also  
509 assume that any existing technology to be used in the proposed solution has been implemented  
510 in a manner consistent with these standards.
- 511 ▪ Organizations have instituted relevant mobile device security policies and that these will be  
512 updated based on implementation of this solution.

### 513 3.3.1 Systems Engineering

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

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

### 524 3.4 Risk Assessment

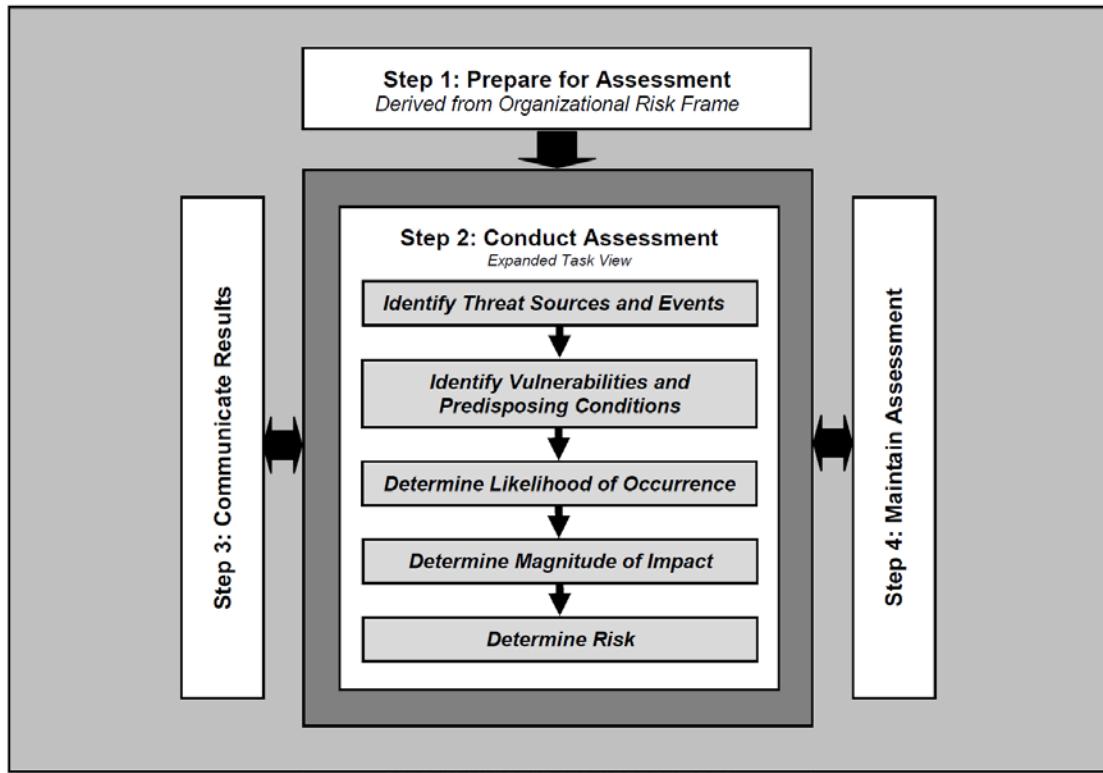
525 NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [9], states that risk is “a measure of  
526 the extent to which an entity is threatened by a potential circumstance or event, and typically a function  
527 of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of  
528 occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and  
529 prioritizing risks to organizational operations (including mission, functions, image, reputation),  
530 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of

531 an information system. Part of risk management incorporates threat and vulnerability analyses, and  
 532 considers mitigations provided by security controls planned or in place.”

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

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

544 **Figure 3-2 Risk Assessment Process**



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

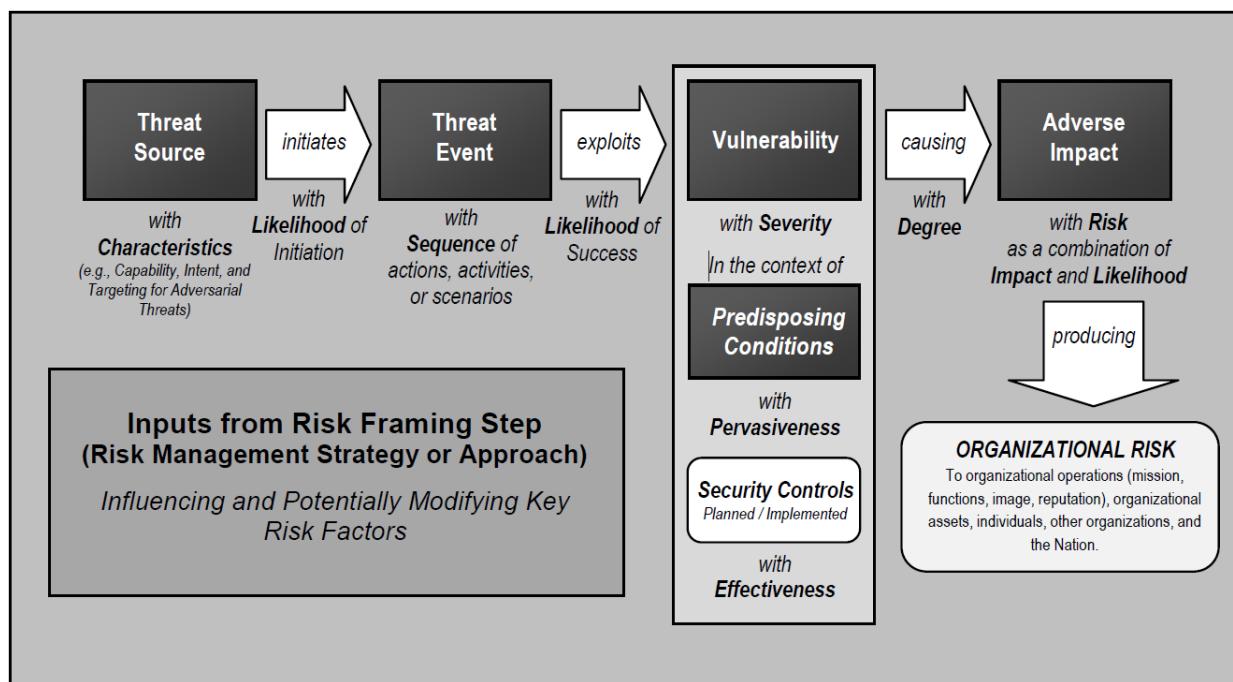
### 547 3.4.1 Risk Assessment of the Fictional Organization Orvilia Development

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

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

- 554     ■ threat sources
- 555     ■ threat events
- 556     ■ vulnerabilities
- 557     ■ predisposing conditions
- 558     ■ security controls
- 559     ■ adverse impacts
- 560     ■ organizational risks

561 **Figure 3-3 NIST 800-30 Generic Risk Model**



562    **3.4.2 Development of Threat Event Descriptions**

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

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

575    **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  |

576    **3.4.2.1 Threat Event 1—Unauthorized Access to Sensitive Information via a Malicious or**  
577    **Privacy-Intrusive Application**

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

585    Risk Assessment Analysis:

586    Overall Likelihood: Very High

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

592    Level of Impact: High

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

596    **3.4.2.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or**  
597    **Email Phishing Campaign**

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

604    Risk Assessment Analysis:

605    Overall Likelihood: Very High

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

607    Level of Impact: High

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

611     **3.4.2.3 Threat Event 3—Malicious Applications Installed via Uniform Resource Locators  
612         (URLs) in SMS or Email Messages**

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

622     Risk Assessment Analysis:

623     Overall Likelihood: High

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

629     Level of Impact: High

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

633     **3.4.2.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known  
634         Vulnerability in the OS or Firmware**

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

642    Risk Assessment Analysis:

643    Overall Likelihood: High

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

647    Level of Impact: High

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

#### 652    *3.4.2.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors*

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

661    Risk Assessment Analysis:

662    Overall Likelihood: Very High

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

667    Level of Impact: High

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

670     3.4.2.6 *Threat Event 6—Compromise of the Integrity of the Device or Its Network*  
671       *Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles,*  
672       *or Certificates*

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

684     Risk Assessment Analysis:

685     Overall Likelihood: Moderate

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

688     Level of Impact: Very High

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

691     3.4.2.7 *Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping*  
692       *on Unencrypted Device Communications*

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

701     Additionally, visibility into network layer traffic enables a malicious actor to conduct side-channel  
702     attacks against its encrypted messages, which can still result in a loss of confidentiality. Further,

703 eavesdropping on unencrypted messages during a handshake to establish an encrypted session with  
704 another host or endpoint may facilitate attacks that ultimately compromise security of the session.

705 Risk Assessment Analysis:

706 Overall Likelihood: High

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

710 Level of Impact: High

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

714 *3.4.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-  
715 Forced Device Unlock Code*

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

725 Risk Assessment Analysis:

726 Overall Likelihood: High

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

730 Level of Impact: High

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

734     3.4.2.9 *Threat Event 9—Unauthorized Access to Backend Services via Authentication or*  
735       *Credential Storage Vulnerabilities in Internally Developed Applications*

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

741     Risk Assessment Analysis:

742     Overall Likelihood: Very High

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

746     Level of Impact: High

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

749     3.4.2.10 *Threat Event 10—Unauthorized Access of Enterprise Resources from an*  
750       *Unmanaged and Potentially Compromised Device*

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

759     Risk Assessment Analysis:

760     Overall Likelihood: Very High

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

762     Level of Impact: High

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

766    *3.4.2.11 Threat Event 11—Loss of Organizational Data Due to a Lost or Stolen Device*

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

770    Risk Assessment Analysis:

771    Overall Likelihood: Very High

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

774    Level of Impact: High

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

777    *3.4.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data Due to Its  
778       Unauthorized Storage in Non-Organizationally Managed Services*

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

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

788    Risk Assessment Analysis:

789    Overall Likelihood: High

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

792    Level of Impact: High

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

795    **3.4.3 Identification of Vulnerabilities and Predisposing Conditions**

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

801    **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     |

802    **3.4.4 Summary of Risk Assessment Findings**

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

805    **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 |

- 806   **Note 1:** Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST Special  
 807   Publication 800-30 Revision 1 [9].
- 808   **Note 2:** The risk rating itself is derived from both the overall likelihood and level of impact using Table I-  
 809   2 of Appendix I in NIST Special Publication 800-30 Revision 1 [9]. Because these scales are not true  
 810   interval scales, the combined overall risk ratings from Table I-2 do not always reflect a strict  
 811   mathematical average of these two variables. This is demonstrated in the table above where levels of  
 812   moderate weigh more heavily than other ratings.
- 813   **Note 3:** Ratings of risk relate to the probability and level of adverse effect on organizational operations,  
 814   organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1,  
 815   adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low),  
 816   serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic effects (i.e.,  
 817   very high).
- 818   

### 3.4.5 Privacy Risk Assessment
- 819   This section describes the privacy risk assessment conducted on Orvilia's enterprise security  
 820   architecture. To perform the privacy risk assessment, the NIST Privacy Risk Assessment Methodology  
 821   (PRAM) was used. The PRAM is a tool for analyzing, assessing, and prioritizing privacy risks to help  
 822   organizations determine how to respond and select appropriate solutions. The PRAM can also serve as a  
 823   useful communication tool to convey privacy risks within an organization. A blank version of the PRAM is  
 824   available for download on NIST's website [43].
- 825   The PRAM uses the privacy risk model and privacy engineering objectives described in NIST Internal  
 826   Report (NISTIR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*  
 827   [44], to analyze for problematic data actions. Data actions are any system operations that process PII.  
 828   Processing can include collection, retention, logging, analysis, generation, transformation or merging,

829 disclosure, transfer, and disposal of PII. A problematic data action is one that could cause an adverse  
830 effect for individuals. The PRAM activities identified the following potential problems for individuals.

831 ***3.4.5.1 Potential Problems for Individuals***

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

- 834     ■ blocking access and wiping devices  
835     ■ employee monitoring  
836     ■ data sharing across parties

837 ***3.4.5.1.1 Data Action 1: Blocking Access and Wiping Devices***

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

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

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

851 ***3.4.5.1.2 Data Action 2: Employee Monitoring***

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

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

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

- 861       ■ develop organization policies and techniques regarding disposal of PII

862       **3.4.5.1.3 Data Action 3: Data Sharing Across Parties**

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

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

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

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

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

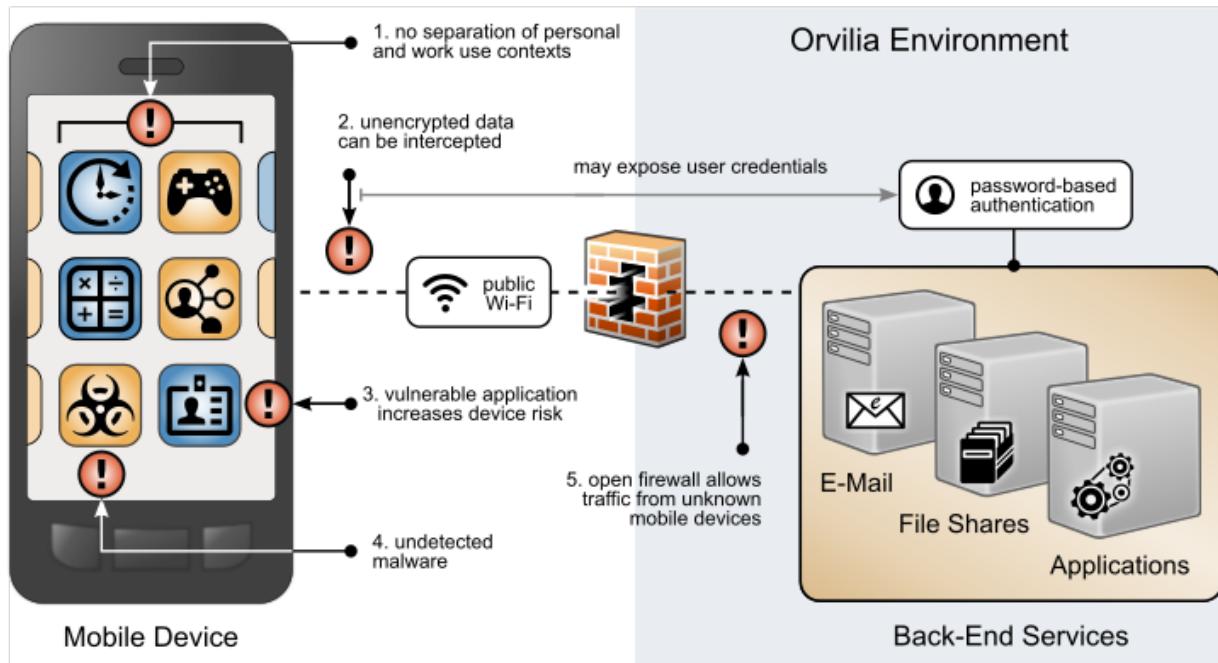
878       **3.5 Preliminary Solution Goals**

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

884       **3.5.1 Current Architecture**

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

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



890

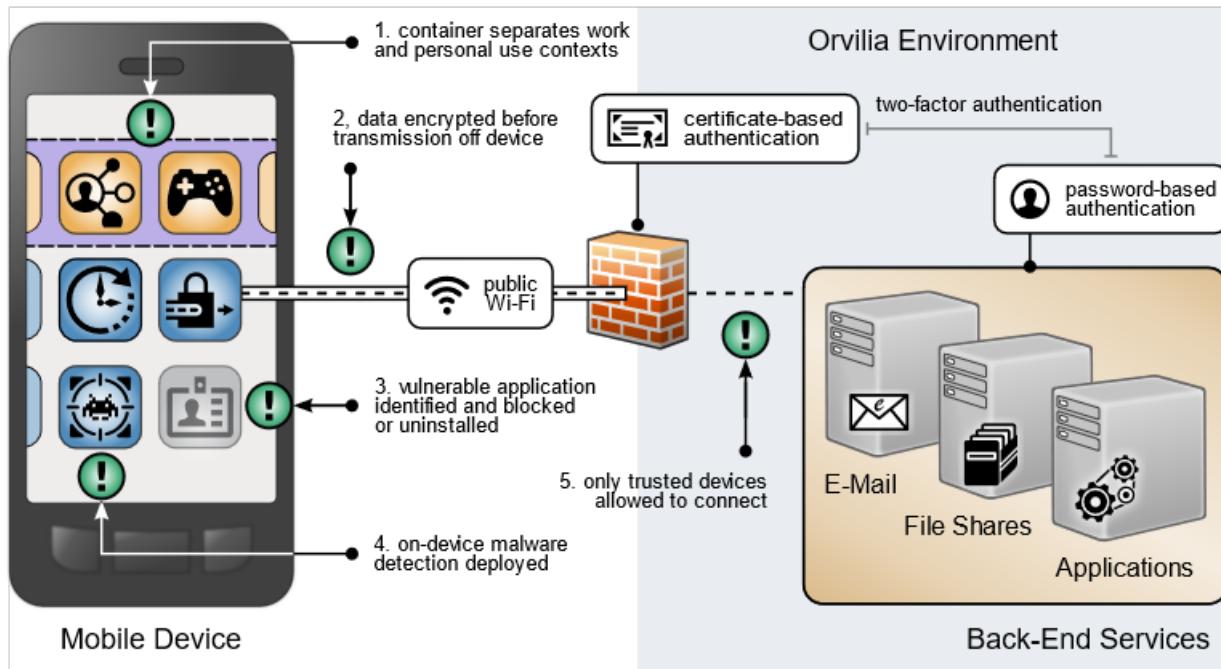
891 The following issues are highlighted in Figure 3-4 with a red exclamation mark:

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.

904    **3.5.2 Preliminary Security Goals**

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

907    **Figure 3-5 Orvilia's Preliminary Security Goals**



908    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.

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

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

## 926      **3.6 Technologies**

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

### 934      **3.6.1 Architecture Components**

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

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

#### 945      ***3.6.1.1 Trusted Execution Environment***

946      A trusted execution environment (TEE) is “a tamper-resistant processing environment that runs on a  
947      separation kernel. It guarantees the authenticity of the executed code, the integrity of the runtime  
948      states (e.g., central processing unit registers, memory and sensitive I/O), and the confidentiality of its  
949      code, data and runtime states stored on a persistent memory. In addition, it shall be able to provide  
950      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.

984 **3.6.1.3 Virtual Private Network**

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

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

998 NIAP's *Extended Package for VPN Gateways* [48], in combination with the internationally and  
999 collaboratively developed *Protection Profile for Network Devices* [49], describes important capabilities  
1000 and security requirements to expect from VPN gateways.

1001 **3.6.1.4 Mobile Application Vetting Service**

1002 Mobile application vetting services use a variety of static, dynamic, and behavioral techniques to  
1003 determine if an application demonstrates any behaviors that pose a security or privacy risk. The risk may  
1004 be to a device owner or user, to parties that own data on the device, or to external systems to which the  
1005 application connects. The set of detected behaviors is often aggregated to generate a singular score that  
1006 estimates the level of risk (or conversely, trustworthiness) attributed to an application. Clients can often  
1007 adjust the values associated with given behaviors (e.g., hard-coded cryptographic keys) to tailor the  
1008 score for their unique risk posture. Those scores may be further aggregated to present a score that  
1009 represents the overall risk or trustworthiness posed by the set of applications currently installed on a  
1010 given device.

1011 Mobile applications, malicious or benign, have high potential to negatively impact both security and user  
1012 privacy. A malicious application can contain code intended to exploit vulnerabilities present in  
1013 potentially any targeted hardware, firmware, or software on the device. Alternatively, or in conjunction  
1014 with exploit code, a malicious application may misuse any device, personal, or behavioral data to which  
1015 it has been explicitly or implicitly granted access, such as contacts, clipboard data, or location services.  
1016 Benign applications may still present vulnerabilities or weaknesses that malicious applications can  
1017 exploit to gain unauthorized access to its data or functionality. Further, benign applications may place  
1018 user privacy at risk by collecting more information than is necessary for the application to deliver  
1019 functionality desired by the user.

1020 While not specific to applications, some services may include device-based risks (e.g., lack of disk  
1021 encryption or vulnerable OS version) in their analysis to provide a more comprehensive assessment of  
1022 the risk or trustworthiness presented by a device when running an application or service.

1023 NIAP does not provide a Protection Profile for application vetting services themselves. However, NIAP's  
1024 *Protection Profile for Application Software* [50] describes security requirements to be expected from  
1025 mobile applications. Many mobile application vetting vendors provide capabilities to automate  
1026 evaluation of applications against NIAP's requirements.

#### 1027 *3.6.1.5 Mobile Threat Defense*

1028 MTD generally takes the form of an application that is installed on the device, which provides the widest  
1029 and most timely access to information about what activity is taking place. Ideally, the MTD solution will  
1030 be able to detect unwanted activity and properly inform the user so they can act to prevent or limit the  
1031 harm an attacker could cause. Additionally, MTD solutions may integrate with EMM solutions to  
1032 leverage the EMM agent's on-device capabilities, such as blocking a malicious application from being  
1033 launched until the user can remove it.

1034 MTD products typically analyze device-based threats, application-based threats, and network-based  
1035 threats. Device-based threats include outdated operating system versions and insecure configuration  
1036 settings. Application-based threats include the issues discussed above regarding the mobile application  
1037 vetting service, though sometimes without the same breadth or depth found in services dedicated to  
1038 application vetting. Network-based threats include use of unencrypted or public Wi-Fi networks and  
1039 attacks such as active attempts to intercept and decrypt network traffic.

#### 1040 *3.6.1.6 Mobile Threat Intelligence*

1041 In this guide, we describe mobile threat intelligence as actionable information that mobile  
1042 administrators can use to make changes to their security configuration to improve their posture relative  
1043 to recent discoveries. Intelligence data include malicious URLs, IP addresses, domain names, and  
1044 application names or package/bundle IDs, as well as malware signatures or vulnerabilities in  
1045 applications, mobile devices, device platform services, or mobile security products. This list is not all-  
1046 encompassing, as any recent information that could inform rapid changes to enable an enterprise to  
1047 better secure a mobile deployment against novel or newly enhanced threats is equally applicable to the  
1048 term. This capability may be found in various other types of technology, such as MTD and other network  
1049 analysis tools.

#### 1050 *3.6.1.7 Native Mobile OS Capabilities*

1051 Native mobile OS capabilities are available without the use of additional security features. They are  
1052 included as part of the mobile device's core capabilities. The following mobile OS capabilities can be  
1053 found in mobile devices, particularly smartphones.

## 1054    3.6.1.7.1 Secure Boot

1055 Secure boot is a general term that refers to a system architecture designed to prevent and detect any  
1056 unauthorized modification to the boot process. A system that successfully completes a secure boot has  
1057 loaded its start-up sequence information into a trusted operating system. A common mechanism is for  
1058 the first program executed (a boot loader) to be immutable (stored on read-only memory or  
1059 implemented strictly in hardware). Further, the integrity of mutable code is cryptographically verified  
1060 prior to execution by either immutable or verified code. This process establishes a chain of trust that can  
1061 be traced back to immutable, implicitly trustworthy code. Use of an integrated TEE as part of a secure  
1062 boot process is preferable to an implementation that uses software alone [51].

## 1063    3.6.1.7.2 Device Attestation

1064 This is an extension of the secure boot process that involves the operating system (or more commonly,  
1065 an integrated TEE) providing cryptographically verifiable proof that it has a known and trusted identity  
1066 and is in a trustworthy state, which means all software running on the device is free from unauthorized  
1067 modification.

1068 Device attestation requires cryptographic operations using an immutable private key that can be verified  
1069 by a trusted third party, which is typically the original equipment manufacturer of the TEE (e.g.,  
1070 Qualcomm or Samsung) or device platform vendor (e.g., Google, Apple, or Microsoft). Proof of  
1071 possession of a valid key establishes the integrity of the first link in a chain of trust that preserves the  
1072 integrity of all other pieces of data used in the attestation. It will include unique device identifiers,  
1073 metadata, and the results of integrity checks on mutable software, and possibly metrics from the boot  
1074 or attestation process itself [51].

## 1075    3.6.1.7.3 Device Management and MDM API

1076 Mobile operating systems and platform-integrated firmware (e.g., Samsung Knox) provide a number of  
1077 built-in security features that are generally active by default. Examples include disk and file-level  
1078 encryption, verification of digital signatures for installed software and updates, a device unlock code,  
1079 remote device lock, and automatic device wipe following a series of failed device unlock attempts. Some  
1080 of these features are directly configurable by the user via a built-in application or through a service  
1081 provided by the device platform vendor (e.g., Google, Apple, or Microsoft).

1082 Additionally, mobile operating systems expose an API to MDM products that allow an organization that  
1083 manages a device to have greater control over these and many more settings that might not be directly  
1084 accessible to the device user. Management APIs allow enterprises using integrated EMM or MDM  
1085 products to manage devices more effectively and efficiently than they could by using the built-in  
1086 application alone.

## 1087 4 Architecture

1088 This example solution consists of the six mobile security technologies described in [Section 3.6](#): trusted  
 1089 execution environment, enterprise mobility management, virtual private network, mobile application  
 1090 vetting service, mobile threat defense, and mobile threat intelligence. Table 4-1, Commercially Available  
 1091 Products Used, identifies the commercially available products used in this example solution and how  
 1092 they aligned with the six mobile security technologies.

1093 **Table 4-1 Commercially Available Products Used**

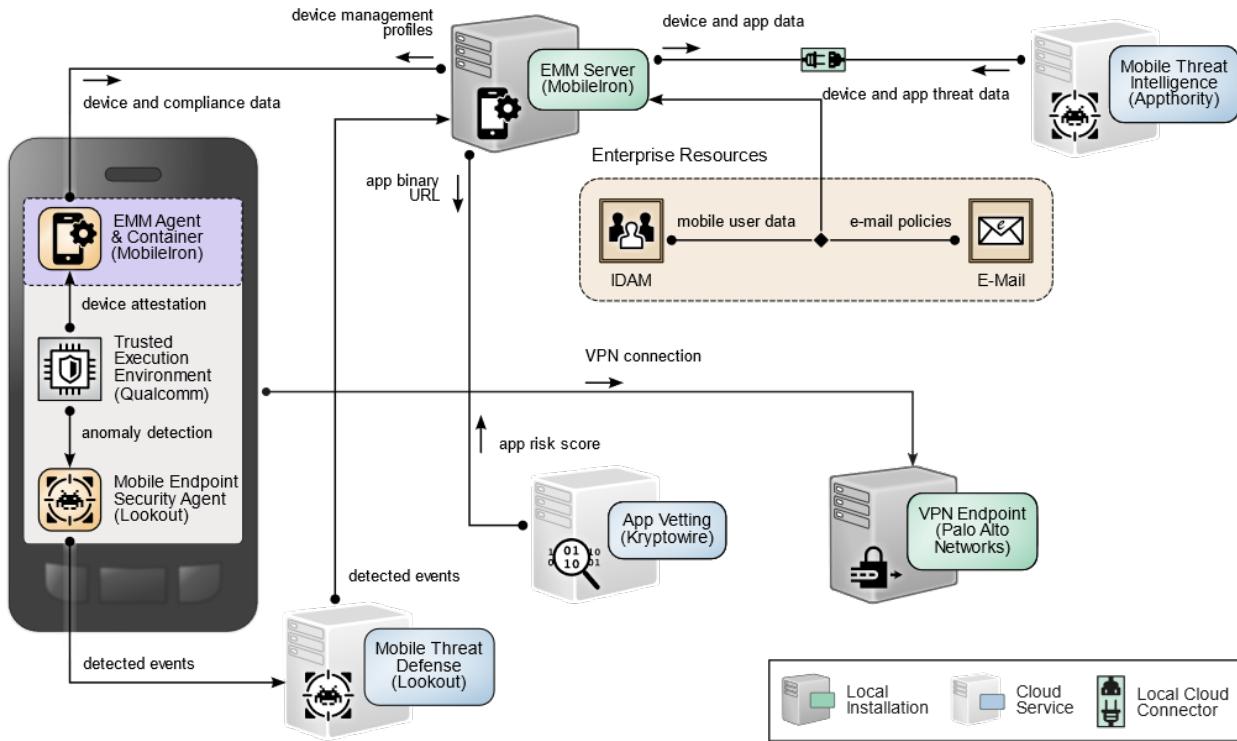
| Commercially Available Product   | Mobile Security Technology         |
|--|------------------------------------|
| Appthority Cloud Service   | Mobile threat intelligence         |
| Kryptowire Cloud Service   | Mobile application vetting service |
| Lookout Cloud Service/Lookout Agent Version 5.10.0.142 (iOS), 5.9.0.420 (Android)                | Mobile threat defense              |
| MobileIron Core Version 9.7.0.1<br>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      |

1094 These components are further integrated with broader on-premises security mechanisms and a VPN  
 1095 gateway as shown in Figure 4-1. This integrated solution provides a broad range of capabilities to help  
 1096 securely provision and manage devices, protect against and detect device compromise, and help provide  
 1097 security-enhanced access to enterprise resources by only authorized mobile users and devices.

1098 Organizations exploring the use of on-premises EMM technology should be aware they will be  
 1099 responsible for installing and configuring the on-premises instances of the EMM technology. This will  
 1100 include the software licenses that must be paid for directly by the organization for any underlying  
 1101 platforms or components. Pre-built software images and containers may be available that can help ease  
 1102 installation and configuration work. As a recommended best practice, if prebuilt containers and images  
 1103 are used, it is recommended that they be checked for common software vulnerabilities.

1104 On-premises mobile device management solutions offer the benefit that enterprise data resides within  
 1105 the organization. Allowed devices may still send and receive information from the mobile device  
 1106 solution that they are authorized to obtain. Organizations that are interested can explore monitoring  
 1107 data flows from the EMM to other devices. Additionally, on-premises mobile device management  
 1108 solutions provide the organization with the capability to maintain physical security of the EMM.

1109 **Figure 4-1 Example Solution Architecture**



## 1110 **4.1 Architecture Description**

1111 The NCCoE worked with industry subject matter experts to develop an open, standards-based,  
 1112 commercially available architecture that addresses the risks identified during the risk assessment  
 1113 process in [Section 3.4](#).

1114 Where possible, the architecture uses components that are present on NIAP's Product Compliant List  
 1115 [35], meaning the product has been successfully evaluated against a NIAP-approved Protection Profile  
 1116 [50]. NIAP collaborates with a broad community, including industry, government, and international  
 1117 partners, to publish technology-specific security requirements and tests in the form of Protection  
 1118 Profiles. The requirements and tests in these Protection Profiles are intended to ensure that evaluated  
 1119 products address identified security threats.

1120 The example solution architecture supports its desired security characteristics as a result of the  
1121 following integrations.

#### 1122 **4.1.1 Enterprise Integration**

1123 This example solution extends central identity and access management to mobile devices via an  
1124 integration between both MobileIron Core and Palo Alto Networks GlobalProtect with Microsoft Active  
1125 Directory Domain Services (ADDS). The integrity of identification and authentication by mobile devices  
1126 to the enterprise is further enhanced by using device certificates issued by local Microsoft Active  
1127 Directory Certificate Services (ADCS).

1128 By integrating with Active Directory (AD), MobileIron Core allows administrators to authorize select  
1129 groups of users to register a mobile device, limiting mobile access to only those users who require it.  
1130 Additionally, different security policies, device configurations, and authorized applications can be  
1131 deployed to different AD groups, allowing administrators to centrally manage distinct mobile use cases.  
1132 MobileIron Core queries AD using the lightweight directory access protocol.

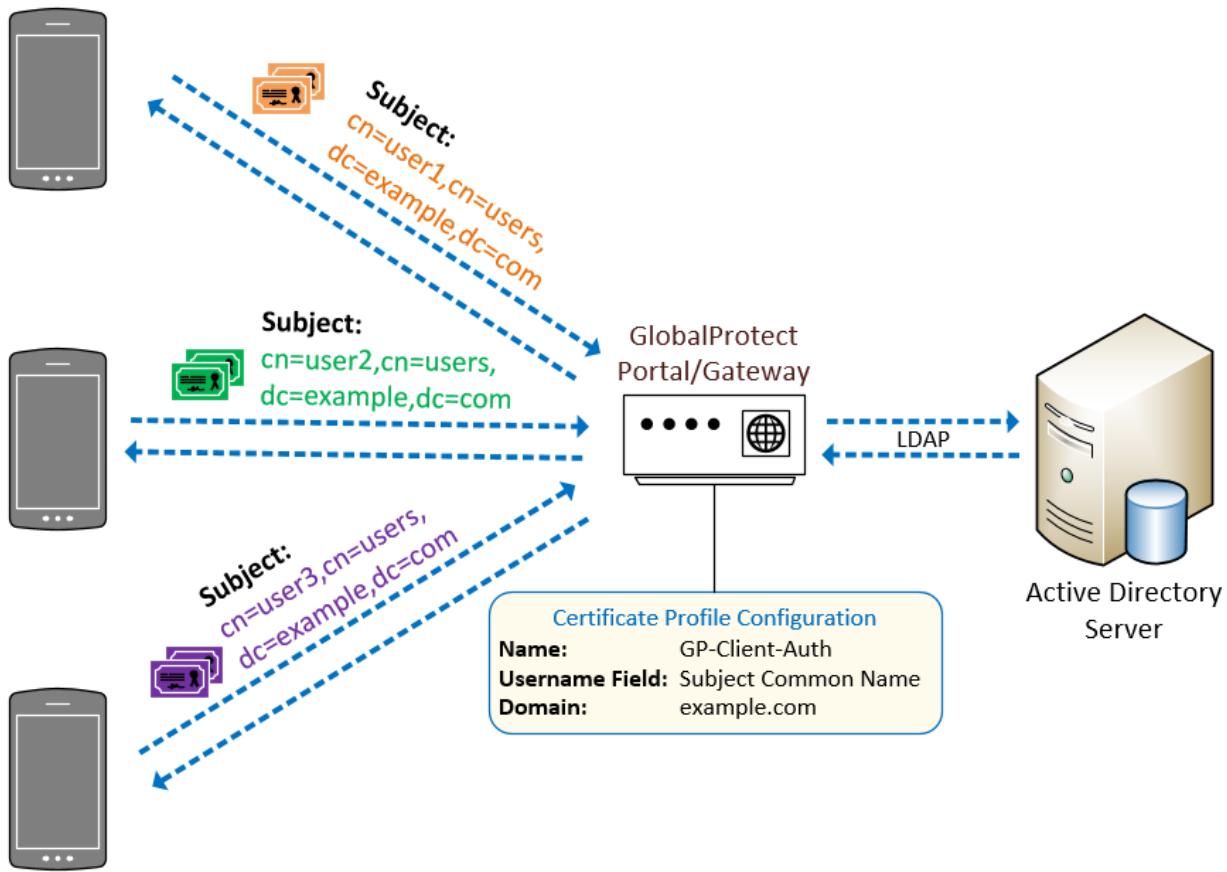
1133 Through its integration with ADCS, MobileIron Core automatically configures devices to obtain locally  
1134 managed device certificates by using the Simple Certificate Enrollment Protocol (SCEP). Our example  
1135 solution mitigates the potential of remote exploitation of SCEP by restricting certificate enrollment to  
1136 mobile devices that are connected to a dedicated enterprise-managed Wi-Fi network that allows devices  
1137 to access only MobileIron Core and the Network Device Enrollment Service server. Further, this example  
1138 solution uses a dynamic SCEP scheme, in which MobileIron Core supplies a registered mobile device  
1139 with a onetime password to include in its SCEP request, thus helping prevent unknown and untrusted  
1140 devices that gain unauthorized access to the dedicated Wi-Fi network from obtaining a trusted device  
1141 certificate.

1142 The example solution's chosen certificate enrollment configuration includes the mobile user's User  
1143 Principal Name (UPN) in the device certificate's Subject Alternative Name field, which the Palo Alto  
1144 Networks GlobalProtect VPN gateway uses to perform identity verification and enforce access control  
1145 for the unique combination of mobile user and device.

1146 MobileIron Core-registered devices also utilize the device certificate indirectly to enhance the security of  
1147 remote connections to the enterprise in two ways. First, communication with MobileIron Core (which  
1148 must be accessible from the internet in the demilitarized zone) is secured using two-way Transport Layer  
1149 Security (TLS). This protects MobileIron Core from establishing secure connections with untrusted  
1150 mobile devices. Second, the device certificate is used in the GlobalProtect VPN configuration, which  
1151 restricts access to the VPN to only trusted devices. Further, GlobalProtect uses the device user's UPN to  
1152 grant appropriate access to enterprise resources based on the device user's UPN through its integration  
1153 with ADDS.

1154 As shown in Figure 4-2 [52], devices present the certificates to the VPN and EMM authentication  
 1155 services after the certificate have been successfully issued. The GlobalProtect VPN authenticates the  
 1156 device user by mapping the common name field in the client certificate to an account stored in the local  
 1157 ADDS. On successful authentication, the GlobalProtect application prompts the user to authenticate  
 1158 using a second factor—their Active Directory domain password. Once this is verified, GlobalProtect  
 1159 establishes a tunnel with the gateway and is assigned an IP address from the IP pool in the gateway's  
 1160 tunnel configuration.

1161 **Figure 4-2 Example Solution Gateway Architecture**



#### 1162 **4.1.2 Mobile Component Integration**

1163 This section describes how the various mobile technology components integrate with one another. The  
 1164 majority of these components integrate with the EMM, MobileIron. MobileIron supports the integration  
 1165 of third-party cloud services through a defined API. MobileIron Core authenticates external systems by  
 1166 using basic authentication, so TLS protects the confidentiality of API account credentials and

1167 MobileIron's responses to clients' RESTful calls. MobileIron API client accounts for Kryptowire, Lookout  
1168 Mobile Endpoint Security, and Appthority Mobile Threat Protection (MTP) are each assigned  
1169 administrative roles that grant the minimum set of permissions necessary to achieve integration [53],  
1170 [54].

#### 1171 *4.1.2.1 Appthority–MobileIron*

1172 The Appthority application reputation service provides an integration with MobileIron Core systems  
1173 through implementation of connector software provided by Appthority. The connector provides the  
1174 code that exercises the APIs provided by MobileIron Core and the Appthority cloud service. In this  
1175 integration, an API user was created within the MobileIron Core system and assigned specific roles  
1176 required for successful operation of the application vetting service. Automatic syncing between the  
1177 Appthority service and MobileIron Core system can occur on a configurable basis. Specifically, the  
1178 application and device inventory data are synced between the two systems. In this integration, syncing  
1179 occurs every hour, but this value should be adjusted to fit the needs of the organization.

1180 In this example solution, the integration provides the primary security benefit of compliance  
1181 enforcement and remediation escalation. In the initial step of the process, the application inventory is  
1182 gathered from the MobileIron Core system, and each application is assigned a threat measurement  
1183 score. If an application is installed on a device that is not compliant with the configured policy,  
1184 Appthority MTP communicates with the MobileIron Core system to identify those devices, which  
1185 triggers MobileIron compliance enforcement actions.

#### 1186 *4.1.2.2 Lookout–MobileIron*

1187 The Lookout mobile threat defense service provides integration with MobileIron Core systems through  
1188 implementation of connector software provided by Lookout. The connector provides the code that  
1189 exercises the APIs provided by MobileIron Core and the Lookout cloud service. This integration allows  
1190 Lookout to retrieve device details as well as application inventory information and to apply labels to  
1191 devices as necessary.

1192 Following analysis, Lookout uses the API to apply specific labels to devices to categorize them based on  
1193 risk posture, which is calculated based on the severity of issues detected on the device. MobileIron can  
1194 then automatically respond to application of specific labels based on built-in compliance actions. This  
1195 allows administrators to configure exactly how MobileIron will respond to devices in the following  
1196 categories:

- 1197     ■ Pending—Lookout not yet activated
- 1198     ■ Secured—Lookout active
- 1199     ■ Threats Present—Lookout has detected threats
- 1200     ■ Deactivated—Lookout has been deactivated

- 1201       ■ Low Risk—devices with a low risk score in Lookout  
1202       ■ Moderate Risk—devices with a moderate risk score in Lookout  
1203       ■ High Risk—devices with a high-risk score in Lookout

1204 ***4.1.2.3 Kryptowire—MobileIron***

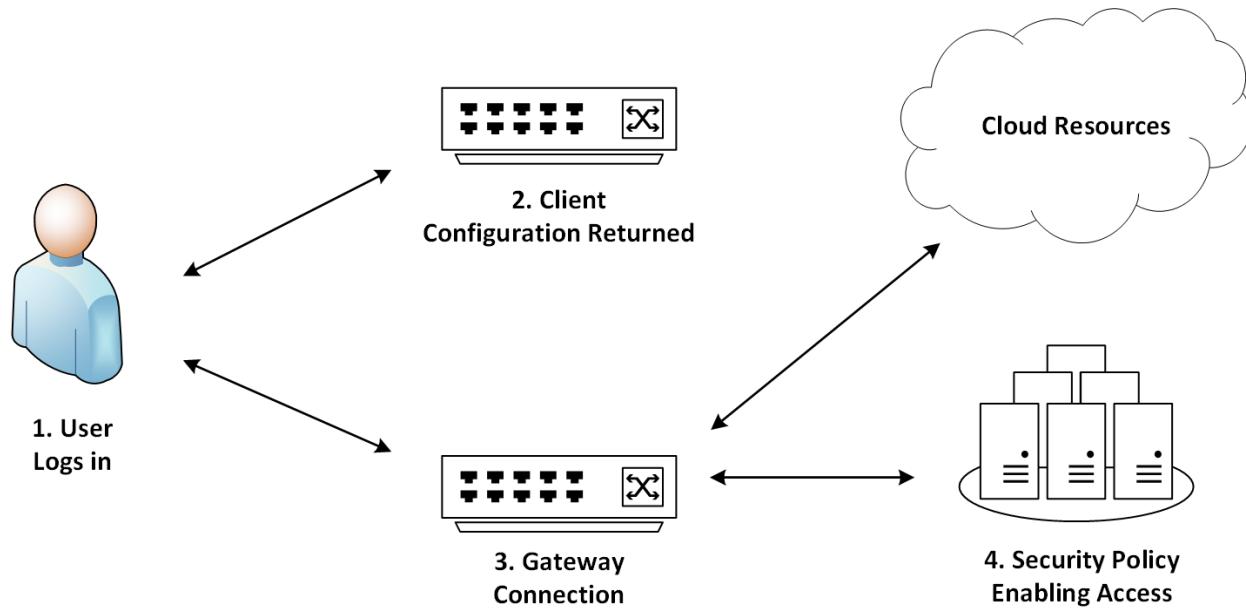
1205 Kryptowire obtains device details, such as device platform, OS version, and the universally unique  
1206 identifiers assigned to each registered device by MobileIron Core to enable clear identification of a  
1207 particular device across systems. Kryptowire obtains the inventory of applications from all of the devices  
1208 enrolled in MobileIron. Kryptowire performs static, dynamic, and behavioral binary code analysis on  
1209 mobile applications against government (NIAP) and industry (The Open Web Application Security  
1210 Project, or OWASP) [55] standards. Kryptowire provides both a detailed security analysis, provides  
1211 pass/fail evidence down to the line of code, and provides a summary weighted risk score for each  
1212 application. Mobile application administrators can use these detailed reports to inform decisions on  
1213 which applications are trusted and compliant with enterprise security and privacy policies and which are  
1214 restricted for enterprise or personal use.

1215 ***4.1.2.4 Palo Alto Networks—MobileIron***

1216 Palo Alto Networks' GlobalProtect VPN is used to secure remote connections from mobile devices.  
1217 MobileIron Core offers specific configuration options for the GlobalProtect client available on Android  
1218 and iOS that facilitates secure deployment of VPN clients and enablement of VPN access using  
1219 certificate-based authentication to the GlobalProtect gateway. Details of the certificate enrollment  
1220 process are provided in Section 4.1.1.

1221 The VPN architecture used in this example solution is composed of two components of the Palo Alto  
1222 Networks next-generation firewall—a GlobalProtect portal and a GlobalProtect gateway. The portal  
1223 provides the management functions for VPN infrastructure. Every endpoint that participates in the  
1224 GlobalProtect network receives configuration information from the portal, including information about  
1225 available gateways as well as any client certificates that may be required to connect to the GlobalProtect  
1226 gateway(s). The gateway provides security enforcement for traffic from GlobalProtect applications. It is  
1227 configured to provide access to specific enterprise resources only to mobile device users after a  
1228 successful authentication and authorization decision.

1229 The VPN tunnel negotiation between the VPN endpoint/mobile device and the VPN gateway is  
1230 presented in Figure 4-3 [56]. It demonstrates a user logging into the system (1), the portal returning the  
1231 client configuration (2), the agent automatically connecting to the gateway and establishing a VPN  
1232 tunnel (3), and the gateway's security policy enabling access to internal and external applications (4).

1233 **Figure 4-3 Example Solution VPN Architecture**

1234 For our example solution, we chose to enforce an always-on VPN configuration. This configuration  
 1235 causes registered devices to establish a VPN connection to the GlobalProtect gateway whenever they  
 1236 have network connectivity—this occurs over cellular or Wi-Fi and is persistent across device reboot. This  
 1237 configuration affords devices with the greatest degree of protection, as additional Palo Alto Networks  
 1238 services can be extended to GlobalProtect. This example solution uses URL filtering, which blocks mobile  
 1239 devices from accessing blacklisted internet domains or any domain that Palo Alto Networks associates  
 1240 with active exploits (e.g., phishing campaigns, watering hole attacks, botnet command and control). NIST  
 1241 SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and BYOD Security* [11], describes  
 1242 the most common VPN options used for remote workers.

#### 1243 **4.1.2.4.1 FIPS Compliance**

1244 Any sensitive information passing over the internet, wireless networks, and other untrusted networks  
 1245 should have its confidentiality and integrity preserved through cryptography [11]. While federal  
 1246 agencies are required to use cryptographic algorithms that are NIST-approved and contained in Federal  
 1247 Information Processing Standards (FIPS)-validated modules, adoption of these standards is available to  
 1248 private and commercial organizations [57]. This example solution uses these best practices to the extent  
 1249 possible in the following ways:

- 1250     ■ *FIPS-CC mode* in the GlobalProtect VPN appliance is enabled, which requires TLS 1.1 (or above)  
     1251       and limits the public key use to FIPS-approved algorithms. This example solution's  
     1252       implementation uses the highest version of TLS available, with TLS 1.2 being the minimum

1253           acceptable version. A full list of security functions can be found on the Palo Alto Networks FIPS-  
1254           CC Security Functions documentation site [58].

- 1255        ▪ As described in Section 4.1.1, dynamic SCEP challenges are enabled.

1256 To align our example solution with guidance in NIST SP 800-52 Revision 1. *Guidelines for the Selection,*  
1257 *Configuration, and Use of Transport Layer Security (TLS) Implementations* [12], this example solution  
1258 implements the following configuration:

- 1259        ▪ The GlobalProtect portal and gateway restrict the list of cipher suites available to the client  
1260           application by using a TLS service profile. The minimum version of TLS is set to 1.2 as  
1261           recommended by NIST SP 800-52.  
1262        ▪ The GlobalProtect portal and gateway server certificates use 2048-bit RSA key modulus signed  
1263           with *sha256WithRSAEncryption* algorithm.

#### 1264 *4.1.2.5 iOS and Android EMM Integration*

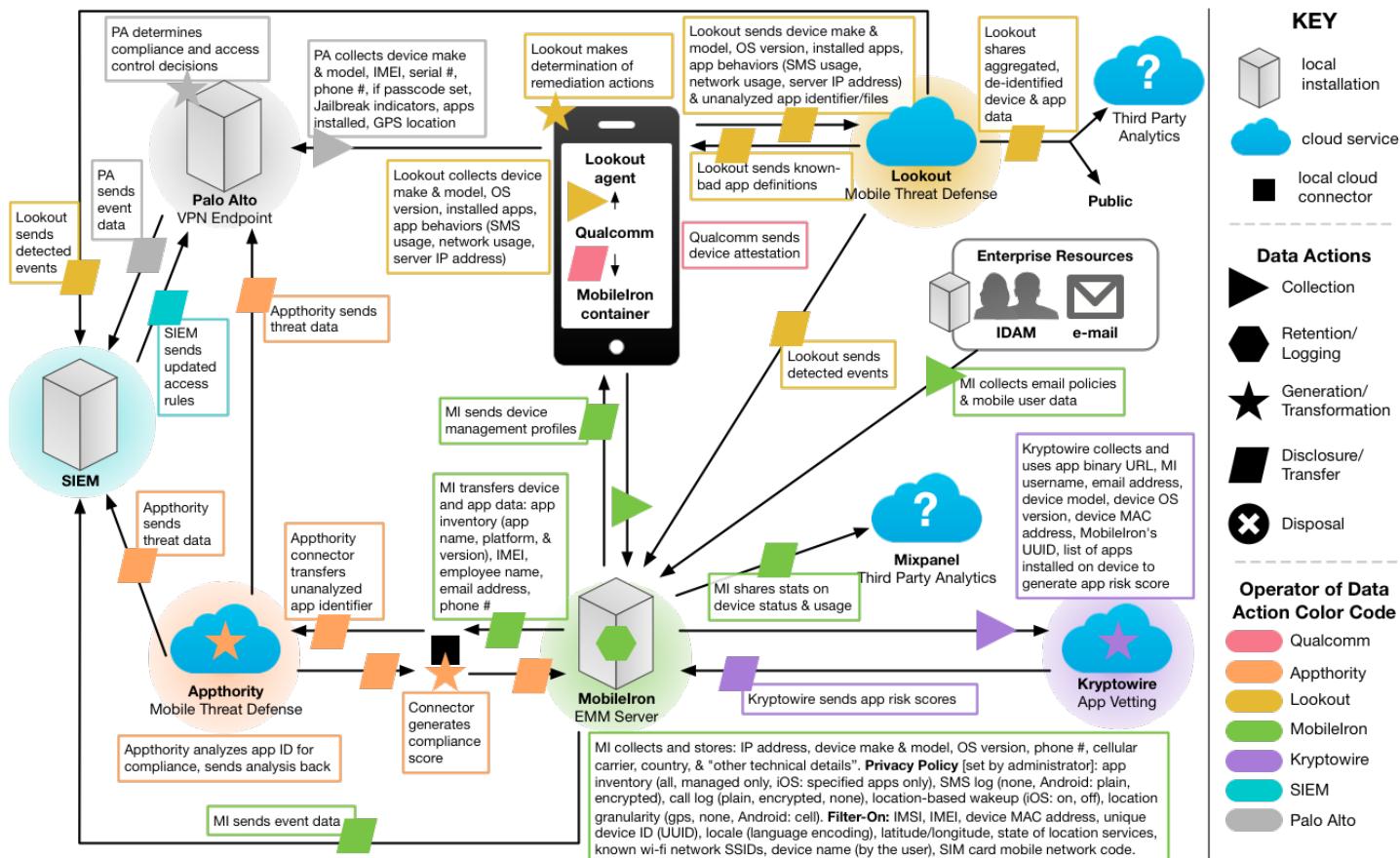
1265 iOS and Android-based devices both integrate directly with EMM solutions, providing enterprise-level  
1266 management of security controls based on policy. iOS devices are managed by configuration profiles.  
1267 Configuration profiles can force security policies such as VPN usage, enterprise Kerberos support, and  
1268 access to cloud services. iOS further incorporates a set of additional security controls in what is termed  
1269 *supervised mode*, which denotes a corporately owned device. Typically, organizations choose to use the  
1270 Device Enrollment Program [59] for large-scale deployments of iOS devices in *supervised mode* due to  
1271 the reduction of labor involved in manually configuring each device. However, due to the small number  
1272 of devices in our reference design, we have configured *supervised mode* using the Apple Configurator 2  
1273 tool [60]. A full description of iOS capabilities can be found in the iOS Security Guide [61].

1274 Similarly, Android-based devices offer security controls that an EMM can leverage for enterprise  
1275 deployments. The Android Enterprise program by Google is available on devices with Android 5.0  
1276 (Lollipop) and higher. An EMM deploys a device policy controller [62] as part of its on-device agent that  
1277 controls local device policies and system applications on devices. Android Enterprise supports COPE and  
1278 BYOD deployment scenarios through work-managed [63] and work-profile [64] device solutions. In  
1279 work-managed mode, the device is corporately owned, and the entire device is managed by the  
1280 enterprise, whereas work profiles can be added to personally owned devices. A newer mode introduced  
1281 in Android 8.0 supports a combination of work-managed and work profiles on the same device [65]. In  
1282 this scenario, the device is corporately owned, in that device level controls such as device wipe and reset  
1283 to factory default settings are available. A work profile is also created to keep enterprise applications  
1284 and data separate from any personal data. This scenario allows for some flexibility of the device owner  
1285 to permit personal use of the device while retaining device controls and is the chosen deployment of  
1286 this reference implementation.

## 1287 4.2 Enterprise Security Architecture Privacy Data Map

1288 Orvilia performed a privacy analysis using both the information gathered in the initial PRAM effort and the identified mobile security  
 1289 technologies included in the revised architecture. The output from the PRAM activities, including data flows between the components, along  
 1290 with their on-premises or cloud-based location, resulted in the information contained in Figure 4-4. For additional information on the PRAM  
 1291 activities, see the Privacy Risk Assessment Appendix.

1292 Figure 4-4 NIST Privacy Risk Assessment Methodology Data Map for Orvilia's Enterprise Security Architecture



1293 **4.3 Security Control Map**

1294 Using the developed risk information as input, the security characteristics of the solution were  
1295 identified. A security control map was developed documenting the example solution's capabilities with  
1296 applicable Subcategories from the NIST Cybersecurity Framework Version 1.1 [5]; NIST SP 800-53  
1297 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [13];  
1298 International Organization for Standardization (ISO), International Electrotechnical Commission (IEC)  
1299 27001:2013, *Information technology—Security techniques—Information security management systems –*  
1300 *Requirements* [25]; the Center for Internet Security's Control set [21] Version 6; and NIST SP 800-181,  
1301 *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [20].

1302 The security control map identifies the security characteristic standards mapping for the products as  
1303 they were used in the example solution. The products may be capable of additional capabilities not used  
1304 in this example solution. For that reason, it is recommended the mapping not be used as a reference for  
1305 all of the security capabilities these products may be able to address. The security control map can be  
1306 found in Table H-1.

1307 **5 Security Characteristic Analysis**

1308 The purpose of the security characteristic analysis is to understand the extent to which the project  
1309 meets its objective of demonstrating how to increase the security of mobile devices within an enterprise  
1310 by deploying EMM, MTD, MTI, application vetting, secure boot/image authentication, and VPN services.

1311 **5.1 Assumptions and Limitations**

1312 The security characteristic analysis has the following limitations:

- 1313     ▪ It is neither a comprehensive test of all security components nor a red-team exercise.  
1314     ▪ It cannot identify all weaknesses.  
1315     ▪ It does not include the lab infrastructure. It is assumed those systems are hardened. Testing  
1316       these devices would reveal only weaknesses in implementation that would not be relevant to  
1317       those adopting this reference architecture.

1318 **5.2 Build Testing**

1319 Functional testing was used to confirm the example solution's capabilities. We use the test activities to  
1320 demonstrate Orvilia's susceptibility to the threat before implementing the architecture detailed in this  
1321 practice guide. We use the test activities again after implementing the architecture to demonstrate that  
1322 the threats have been appropriately addressed.

1323    **5.2.1 Threat Event 1 —Unauthorized Access to Sensitive Information via a Malicious**  
1324    **or Privacy-Intrusive Application**

1325    **Summary:** Unauthorized access to sensitive information via a malicious or privacy-intrusive application  
1326    is tested. We tested this threat by placing a mock sensitive enterprise contact list and calendar entries  
1327    on devices, then attempted to install and use applications on the Apple App Store and Google Play Store  
1328    [66] that access and back up those entries. Ideally, the enterprise's security architecture would either  
1329    detect or prevent use of these applications, or it would block the applications from accessing enterprise-  
1330    controlled contact list and calendar entries.

1331    **Test Activity:**

1332    Install an iOS or Android application that accesses the contact and calendar entries and backs them up  
1333    to a cloud service. We have no reason to believe these applications are malicious. However, the  
1334    behavior of accessing and backing up enterprise-controlled data (contacts and calendar entries) without  
1335    authorization presents an activity that should be mitigated by this example solution's security  
1336    architecture.

1337    **Desired Outcome:** The enterprise's security architecture should identify the presence of the applications  
1338    and the fact that they access contact and calendar entries. The security architecture should block these  
1339    applications from installing, block them from running, or detect their presence and cause another  
1340    appropriate response to occur, such as blocking the mobile device from accessing enterprise resources  
1341    until the applications are removed.

1342    Alternatively, built-in device mechanisms such as Apple's managed applications functionality and  
1343    Google's Android enterprise work profile functionality could be used to separate the contact and  
1344    calendar entries associated with enterprise email accounts, so they can be accessed only by enterprise  
1345    applications (applications authorized and managed by the EMM), not applications manually installed by  
1346    the user. The user should not have the ability to manually provision their enterprise email account. The  
1347    account should be able to be provisioned only by the EMM, enabling enterprise controls on the  
1348    enterprise contact list and calendar data. However, in this practice guide build, we chose to make the  
1349    devices fully managed, not divided into separate enterprise and personal areas.

1350    **Observed Outcome:** Apptivity identified the presence of applications that have access to sensitive  
1351    data and updated the device labels in MobileIron Core.

1352    **5.2.2 Threat Event 2 —Theft of Credentials Through an SMS or Email Phishing**  
1353    **Campaign**

1354    **Summary:** A fictitious phishing event was created where protection against theft of credentials through  
1355    an SMS or email phishing campaign was tested.

1356    **Test Activity:**

- 1357     ▪ Establish a web page with a form that impersonates an enterprise login prompt.
- 1358     ▪ Send the web page's URL via SMS or email and attempt to collect and use enterprise login  
1359        credentials.
- 1360   **Desired Outcome:** The enterprise's security architecture should block the user from browsing to known  
1361        malicious websites. Additionally, the enterprise should use multifactor authentication or phishing-  
1362        resistant authentication methods, such as those based on public key cryptography, so that either there  
1363        is no password for a malicious actor to capture, or capturing the password is insufficient to obtain access  
1364        to enterprise resources.
- 1365   **Observed Outcome:** The example solution used Palo Alto Networks' next-generation firewall. The  
1366        firewall includes PAN-DB, a URL filtering service that automatically blocks known malicious URLs. The  
1367        URL filtering database is updated regularly to help protect users from malicious URLs. The next-  
1368        generation firewall blocked the attempt to visit the phishing site. However, if the malicious URL were  
1369        not present in PAN-DB, the user would be allowed to access the website.

### 1370    5.2.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email 1371        Messages

1372   **Summary:** Unauthorized applications, not present on the official Apple App Store or Google Play Store,  
1373        are installed via URL links in SMS, email messages, or third-party websites.

#### 1374   **Test Activity (Android):**

- 1375     ▪ Send an email to the user containing a link (<https://f-droid.org/Fdroid.apk>) to the F-Droid APK  
1376        (Android Application Package) file with a message urging the user to click on the link to install  
1377        the application.
- 1378     ▪ On the device, if not already enabled, attempt to enable the Unknown Sources toggle setting in  
1379        the device security settings to allow installing applications from sources other than the Google  
1380        Play Store.
- 1381     ▪ On the device, read the received email, click on the link, and attempt to install the F-Droid  
1382        application.
- 1383     ▪ Observe whether the F-Droid application could be successfully installed. If so, observe whether  
1384        the enterprise detected and responded to installation of the unauthorized application.

#### 1385   **Test Activity (iOS):**

- 1386     ▪ Send an email to the user containing a link to an iOS application available for installation from  
1387        the iosninja.io website, along with a message urging the user to click on the link to install the  
1388        application.
- 1389     ▪ On the device, read the received email, click on the link, and attempt to install the application.

1390       ■ On the device, attempt to explicitly trust the developer's signing certificate. Then attempt to run  
1391       the application.

1392       ■ Observe whether the application could run. If so, observe whether the enterprise detected and  
1393       responded to installation of the unauthorized application.

1394       **Desired Outcome:** The device does not allow the user to install the unauthorized application. If the  
1395       application is somehow installed, its presence should be detected, and an appropriate response should  
1396       occur, such as blocking the device from accessing enterprise resources until the application is removed.

1397       **Observed Outcome:** On iOS devices, Lookout detected that an application had been sideloaded, and it  
1398       applied a label to the device. MobileIron then quarantined the device until the threat was resolved.

1399       On iOS devices, MobileIron has a configuration option that prohibited the user from trusting the  
1400       developer certificate.

1401       On Android devices, MobileIron has a configuration option that prohibited the user from enabling  
1402       Unknown Sources on the device.

#### 1403       5.2.4 Threat Event 4 —Confidentiality and Integrity Loss due to Exploitation of 1404       Known Vulnerability in the OS or Firmware

1405       **Summary:** When malware successfully exploits a code execution vulnerability in the mobile OS or device  
1406       drivers, the delivered code generally executes with elevated privileges and issues commands in the  
1407       context of the root user or the OS kernel.

1408       **Test Activity:** Attempt to access enterprise resources from a mobile device with known vulnerabilities  
1409       (e.g., running an older, unpatched version of iOS or Android).

1410       **Desired Outcome:** The enterprise's security architecture should identify the presence of devices that are  
1411       running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be  
1412       possible, when warranted by the risks, to block devices from accessing enterprise resources until system  
1413       updates are installed.

1414       **Observed Outcome:** Lookout identified that devices were running outdated operating systems. This  
1415       information was communicated to MobileIron, which subsequently automatically quarantined the  
1416       devices until the operating system was updated.

#### 1417       5.2.5 Threat Event 5 —Violation of Privacy via Misuse of Device Sensors

1418       **Summary:** There is collection of location, camera, or microphone data by an application that has no  
1419       need to access this data.

1420 Note: Not all applications that have access to location, camera, or microphone data are malicious.  
1421 However, when an application is found to be collecting this information, additional vetting or testing  
1422 may be required to determine the intent of its use and to then determine if the application is malicious.

1423 **Test Activity:** Upload the application to Kryptowire; observe the output report.

1424 **Desired Outcome:** Output report identifies the use of location, camera, or microphone use by the  
1425 application.

1426 **Observed Outcome:** The Kryptowire report identified the use of location sensor, camera, or microphone  
1427 by the application.

## 1428 5.2.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network 1429 Communications via Installation of Malicious EMM/MDM, Network, VPN 1430 Profiles, or Certificates

1431 **Summary:** There is compromise of the integrity of the device or its network communications via  
1432 installation of malicious EMM/MDM, network, VPN profiles, or certificates using a man-in-the-middle  
1433 approach.

1434 **Test Activity:**

- 1435     ▪ Install mitmproxy (<https://mitmproxy.org/>) on a computer (we used a Mac) connected to the  
1436       same Wi-Fi network as the mobile devices.
- 1437     ▪ Install mitmproxy's CA certificate (stored at `~/.mitmproxy/mitmproxy-ca-cert.cer` on our Mac)  
1438       onto the mobile devices being tested. iOS- and Android-specific instructions are found below.
- 1439     ▪ Configure the computer as necessary to run mitmproxy in transparent mode, as described in  
1440       <https://docs.mitmproxy.org/stable/howto-transparent/>.
- 1441     ▪ To illustrate a malicious actor's ability to manipulate network traffic, we downloaded the  
1442       mitmproxy *internet\_in\_mirror* script from  
1443       [https://github.com/mitmproxy/mitmproxy/blob/master/examples/simple/internet\\_in\\_mirror.py](https://github.com/mitmproxy/mitmproxy/blob/master/examples/simple/internet_in_mirror.py). It performs a mirror reflection of the content of all websites.
- 1445     ▪ Run mitmproxy in transparent mode and using the *internet\_in\_mirror* script: `mitmproxy -mode  
1446       transparent -ssl-insecure -showhost -s internet_in_mirror.py`
- 1447     ▪ Rather than perform an intrusive attack such as address resolution protocol spoofing, we  
1448       manually configured each mobile device's Wi-Fi network settings to change the default  
1449       gateway's (sometimes referred to as router in the network settings) IP address to the  
1450       computer's IP address rather than the router's IP address. This configuration change forced all  
1451       the network traffic from each device through the computer.

1452 **Test Activity (Android):**

- 1453     ▪ Place mitmproxy's CA certificate as an attachment within an email message.
- 1454     ▪ Open the email message on the Android device and click on the attachment to attempt to install  
1455       the CA certificate.
- 1456     ▪ Modify the device's Wi-Fi network settings to manually change the default gateway's IP address  
1457       to the address of the computer running mitmproxy.
- 1458     ▪ Browse to a hypertext transfer protocol secure (https) website (e.g.,  
1459       <https://www.nccoe.nist.gov>), and observe whether the content has been reversed, illustrating  
1460       that the man-in-the-middle attack on a TLS-protected connection was successful.

1461 **Test Activity (iOS):**

- 1462     ▪ Use Apple Configurator 2 on a Mac, or another tool, to create an iOS configuration profile  
1463       containing mitmproxy's CA certificate. The configuration profile used in testing was named  
1464       Enterprise Access. The configuration profile was signed using a key associated with an Apple  
1465       free developer account certificate. The signature was optional (Configuration profiles do not  
1466       have to be signed).
- 1467     ▪ Send the configuration profile as an attachment within an email message.
- 1468     ▪ Open the email message and attempt to click on the attachment to install the configuration  
1469       profile. Attempt to follow the prompts to complete the profile installation.
- 1470     ▪ Attempt to enable the CA certificate in the iOS device's Certificate Trust Settings.

1471 **Desired Outcome:** The enterprise's security architecture should block installation of unauthorized  
1472 configuration profiles (iOS) or CA certificates (Android). Alternatively, the security architecture may  
1473 detect the presence of unauthorized configuration profiles or CA certificates and perform another  
1474 appropriate action, such as blocking the device from accessing enterprise resources until the  
1475 configuration profile or CA certificate is removed. The architecture should also detect attempted man-  
1476 in-the-middle attacks.

1477 **Observed Outcome:** Lookout detected a man-in-the-middle attack on both iOS and Android devices.  
1478 Lookout also detected the unknown configuration profile on iOS.

1479 **5.2.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via  
1480 Eavesdropping on Unencrypted Device Communications**

1481 **Summary:** Malicious actors can readily eavesdrop on communication over unencrypted, wireless  
1482 networks such as public Wi-Fi access points, which are commonly provided by coffee shops and hotels.  
1483 While a device is connected to such a network, a malicious actor would gain unauthorized access to any  
1484 data sent or received by the device for any session not already protected by encryption at either the  
1485 transport or application layers.

1486 **Test Activity:** Test if applications will attempt to establish an http or unencrypted connection.

1487   **Desired Outcome:** Be alerted when applications attempt to make an unencrypted connection or prevent  
1488   the application from being able to do so.

1489   Appthority can determine if applications will attempt to establish an http or unencrypted connection.

1490   iOS and Android also can require a secure connection for an application. (When it tries to connect to the  
1491   server if it is unencrypted, it will just drop the connection.)

1492   **Observed Outcome:** On both iOS and Android, Appthority detected a “sends data unencrypted” threat  
1493   for an application. Transferring data over unencrypted connections could result in the loss of  
1494   confidentiality of information being transmitted by that application.

#### 1495   5.2.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or 1496       Brute-Forced device Unlock Code

1497   **Summary:** A malicious actor may be able to obtain a user’s device unlock code by direct observation,  
1498   side-channel attacks, or brute-force attacks.

1499   **Test Activity:**

- 1500     ▪ Attempt to completely remove the device unlock code. Observe whether the attempt succeeds.
- 1501     ▪ Attempt to set the device unlock code to “1234,” a weak four-digit personal identification  
1502       number (PIN). Observe whether the attempt succeeds.
- 1503     ▪ Attempt to continuously unlock the device, confirming the device is factory reset after 10 failed  
1504       attempts.

1505   **Desired Outcome:** Policies set on the device by the EMM (MobileIron) should require a device unlock  
1506   code to be set, prevent the device unlock code from being removed, require a minimum complexity for  
1507   the device unlock code, and factory reset the device after 10 failed unlock attempts.

1508   Additionally, Lookout can identify and report devices that have the lock screen disabled.

1509   **Observed Outcome:** MobileIron applied a policy to the devices that enforced a mandatory PIN and  
1510   device wipe capability after 10 failed unlock attempts. Further, Lookout reports when the device has the  
1511   lock screen disabled. For both devices, all data was erased after 10 failed unlock attempts.

1512   The option to remove the unlock PIN/passcode had been disabled. Upon attempting to set the PIN to  
1513   something simple, such as a PIN with repetitious or consecutive characters, an error was displayed,  
1514   informing the user they cannot use the PIN they entered.

1515    5.2.9 Threat Event 9—Unauthorized Access to Backend Services via authentication  
1516       or credential Storage Vulnerabilities in Internally Developed Applications

1517    **Summary:** If a malicious actor gains unauthorized access to a mobile device, the attacker also has access  
1518       to the data and applications on that mobile device. The mobile device may contain an organization's in-  
1519       house applications and can subsequently gain access to sensitive data or backend services.

1520    **Test Activity:** Application was submitted to Appthority for analysis of credential weaknesses.

1521    **Desired Outcome:** Discover and report credential weaknesses.

1522    **Observed Outcome:** Appthority recognized within an application that it uses hard-coded credentials.  
1523       The application's use of hard-coded credentials could introduce vulnerabilities if the hard-coded  
1524       credentials were used for access to enterprise resources by unauthorized entities.

1525    5.2.10 Threat Event 10 —Unauthorized Access of Enterprise Resources from an  
1526       Unmanaged and Potentially Compromised Device

1527    **Summary:** An employee that accesses enterprise resources from an unmanaged mobile device may  
1528       expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do  
1529       not benefit from security mechanisms deployed by the organization such as mobile threat defense,  
1530       mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged  
1531       devices limit an organization's visibility into the state of a mobile device, including if the device is  
1532       compromised by an attacker.

1533    **Test Activity:** Attempt to directly access enterprise services, e.g., Exchange email server or corporate  
1534       VPN, on a mobile device that is not enrolled into the EMM system.

1535    **Desired Outcome:** Enterprise services should not be accessible from devices that are not enrolled into  
1536       the EMM system. Otherwise, the enterprise is not able to effectively manage devices to prevent threats.

1537    **Observed Outcome:** Devices that were not enrolled in MobileIron were unable to access enterprise  
1538       resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper  
1539       client certificates, only obtainable through enrolling in the EMM.

1540    5.2.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device

1541    **Summary:** Due to the nature of the small form factor of mobile devices, they are easy to misplace or be  
1542       stolen. A malicious actor who gains physical custody of a device with inadequate security controls may  
1543       be able to gain unauthorized access to sensitive data or resources accessible to the device.

1544    **Test Activity:** Attempt to download enterprise data onto a mobile device that is not enrolled into the  
1545       EMM system (may be performed in conjunction with TE-10). Attempt to remove (in conjunction with TE-  
1546       8) the device unlock code or demonstrate that the device does not have a device unlock code in place.

1547 Attempt to locate and wipe the device through the EMM console (it will fail if the device is not enrolled  
1548 in the EMM).

1549 **Desired Outcome:** It should be possible to locate or wipe EMM-enrolled devices in response to a report  
1550 that they have been lost or stolen. As demonstrated by TE-10, only EMM-enrolled devices should be  
1551 able to access enterprise resources. As demonstrated by TE-8, EMM-enrolled devices can be forced to  
1552 have a screen lock with a passcode of appropriate strength, which helps resist exploitation (including  
1553 loss of organizational data) if the device has been lost or stolen.

1554 Should the device be unreachable by the EMM (e.g., disconnected from all networking), EMM control  
1555 and corporate data will be removed after 10 failed unlock attempts.

1556 **Observed Outcome (Enrolled Devices):** Enrolled devices are protected. An enterprise policy requiring a  
1557 personal identification number/lock screen is present, and therefore the enterprise data on the device  
1558 could not be accessed. After 10 attempts to access the device, the device was wiped. Additionally, the  
1559 device was remotely wiped after it was reported as lost to enterprise mobile device service  
1560 management.

1561 **Observed Outcome (Unenrolled Devices):** As shown in Threat Event 10, only enrolled devices can access  
1562 enterprise services. When the device attempted to access enterprise data, no connection to the  
1563 enterprise services was available. Because the device cannot access the enterprise, enterprise  
1564 information would not be located on the device.

### 1565 5.2.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its 1566 Unauthorized Storage in Non-Organizationally Managed Services

1567 **Summary:** If employees violate data management policies by using unmanaged services to store  
1568 sensitive organizational data, this data will be placed outside organizational control, where the  
1569 organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who  
1570 compromise the unauthorized service account or any system hosting that account may gain  
1571 unauthorized access to the data.

1572 **Test Activity:** Connect to the enterprise VPN. Open an enterprise website or application. Attempt to  
1573 extract enterprise data by taking a screenshot, or copy/paste and send it via an unmanaged e-mail  
1574 account.

1575 **Desired Outcome:** Screenshots and other data-sharing actions will be prohibited by the EMM while  
1576 using managed applications.

1577 **Observed Outcome:** Through MobileIron restriction and lockdown policies, an administrator prevented  
1578 the following actions on devices:

1579 **Android**

- 1580       ■ copy/paste  
1581       ■ screen capture  
1582       ■ data transfer over near-field communication  
1583       ■ data transfer over Universal Serial Bus  
1584       ■ Bluetooth

1585 **iOS**

- 1586       ■ screen capture and recording (iOS 9+)  
1587       ■ AirDrop  
1588       ■ iCloud Backup  
1589       ■ iCloud Documents and data access  
1590       ■ managed applications storing data in iCloud  
1591       ■ data flow between managed and unmanaged applications  
1592       ■ hand-off

1593 These restrictions prohibited the user from executing common data leakage methods.

1594 **5.3 Scenarios and Findings**

1595 One aspect of our security evaluation involved assessing how well the reference design addresses the  
1596 security characteristics it was intended to support. The Cybersecurity Framework Subcategories were  
1597 used to provide structure to the security assessment by consulting the specific sections of each standard  
1598 that are cited in reference to a Subcategory. The cited sections provide validation points that the  
1599 example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a  
1600 basis for organizing our analysis allowed us to systematically consider how well the reference design  
1601 supports the intended security characteristics.

1602 This section provides the scenarios and findings for the security and privacy characteristics the example  
1603 solution was intended to support. They include:

- 1604       ■ development of the Cybersecurity Framework and NICE Framework mappings  
1605       ■ threat event scenarios and example solution architecture mitigations  
1606       ■ data action scenarios and potential mitigations that organizations could employ

1607 [5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings](#)

1608 While the example solution was being developed, the Cybersecurity Framework Subcategory mappings  
 1609 were developed into a table mapping for organizations implementing the example solution's  
 1610 capabilities.

1611 As the example solution's products were installed, configured, and used in the example solution  
 1612 architecture, the example solution's functions and their corresponding Cybersecurity Framework  
 1613 Subcategories, along with other guidance alignment, were determined and documented.

1614 This mapping became an important resource to the example solution contained in this practice guide  
 1615 because it provides the ability to communicate with the organization's stakeholders about the security  
 1616 controls that the example solution can help mitigate, and the workforce requirements that the example  
 1617 solution will require.

1618 The example solution's products, security control, and workforce mapping can be found in Table H-1.

1619 [5.3.2 Threat Event Scenarios and Findings](#)

1620 As part of the findings, the threat events were mitigated in the example solution architecture using the  
 1621 concepts and technology shown in Table 5-1. Each threat event was matched with functions that helped  
 1622 mitigate the risks posed by the threat event.

1623 Note: While not demonstrated in the table, TEE provided tamper-resistant processing environment  
 1624 capabilities that helped mitigate mobile device runtime and memory threats in the example solution.

1625 **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 |
|--|---|--|
| <b>Threat Event 1:</b> Unauthorized access to sensitive information via a malicious or privacy-intrusive application | Ensured administrators have insight into what corporate data applications can access. | MTI  |
| <b>Threat Event 2:</b> 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 |
|--|---|--|
| <b>Threat Event 3:</b> Malicious applications installed via URLs in SMS or email messages  | Disabled installing applications from unknown sources.  | EMM  |
| <b>Threat Event 4:</b> 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  |
| <b>Threat Event 5:</b> Violation of privacy via misuse of device sensors   | Application vetting reports indicated the sensors to which an application requested access.                           | MTI  |
| <b>Threat Event 6:</b> 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  |
| <b>Threat Event 7:</b> 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  |
| <b>Threat Event 8:</b> Compromise of device integrity via observed, inferred, or brute-forced device unlock code   | Enforced mandatory device wipe capabilities after 10 failed unlock attempts.  | EMM  |
| <b>Threat Event 9:</b> 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  |
| <b>Threat Event 10:</b> 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 |
|---|---|--|
| <b>Threat Event 11:</b> Loss of organizational data due to a lost or stolen device  | Enterprise data was protected by enforced passcode policies and device wipe capabilities. | EMM  |
| <b>Threat Event 12:</b> 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  |

1626    **5.3.3 Data Action Scenarios and Findings**

1627    The results of the PRAM found that three data actions were especially relevant to the build. Potential  
 1628    mitigations that could be used by an organization to lessen their impact were identified by the PRAM as  
 1629    shown below. Further details on the PRAM's findings can be found in Appendix F.

1630    **Table 5-2 Data Action Scenarios and Findings Summary**

| Data Action   | Data Action Description  | How the Data Action Could Be Mitigated   |
|---|--|--|
| <b>Data Action 1:</b><br>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. | <p>Block the device's access to enterprise resources until it is granted access permission again.</p> <p>Selectively wipe elements of the device without removing all data on the device. Within the example solution, this option is available for iOS devices.</p> <p>Advise employees to back up the personal data maintained on devices.</p> <p>Limit staff with the ability to perform wipes or block access.</p> |

| Data Action                                       | Data Action Description  | How the Data Action Could Be Mitigated  |
|---|--|---|
| <b>Data Action 2:</b><br>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. | <p>Limit staff with ability to review data about employees and their devices.</p> <p>Develop organizational policies and techniques to limit collection of specific data elements.</p> <p>Develop organizational policies and techniques regarding disposal of PII.</p>   |
| <b>Data Action 3:</b> 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.         | <p>Develop organizational policies and techniques for de-identification of data.</p> <p>Use encryption.</p> <p>Limit or disable access to data.</p> <p>Develop organizational policies and techniques to limit collection of specific data elements.</p> <p>Use contracts to limit third-party data processing.</p> |

## 1631 6 Conclusion

- 1632 This document provides an overview of the Risk Management Framework and the Privacy Risk  
 1633 Assessment Methodology, an explanation of mobile device security concepts, and an example solution  
 1634 for organizations implementing a COPE deployment.
- 1635 Our fictitious Orvilia Development organization started with a mobile device infrastructure that was  
 1636 lacking mobile device security architecture concepts. It employed a risk management and privacy  
 1637 methodology to understand the current gaps in its architecture and methods to enhance the security of  
 1638 its systems.
- 1639 After identifying the core threat events from the risk assessment, the appropriate mobile device security  
 1640 technologies were applied. These included an on-premises EMM solution integrated with cloud- and

1641 agent-based mobile security technologies to help deploy a set of security and privacy capabilities in  
1642 support of a usage scenario.

1643 The practice guide also includes in Volume C a series of How-To Guides—step-by-step instructions  
1644 covering the initial setup (installation or provisioning) and configuration for each component of the  
1645 architecture—to help security engineers rapidly deploy and evaluate our example solution in their test  
1646 environment.

1647 The example solution of our reference design uses standards-based, commercially available products. It  
1648 can be used directly by any organization with a COPE usage scenario by implementing a security  
1649 infrastructure that supports an integration of on-premises with cloud-hosted mobile security  
1650 technologies. The practice guide provides a reference design and example solution that an organization  
1651 may use in whole or in parts as the basis for a custom solution that realizes the security and privacy  
1652 characteristics that best support its unique mobile device usage scenario.

## 1653 **7 Future Build Considerations**

1654 A topic of interest for a future build is a BYOD scenario. This entails protecting corporate data on  
1655 personally owned devices that employees will use for work as well as personal activity. Another area of  
1656 interest is a thin client deployed to mobile devices. The thin client would allow the employee to access a  
1657 virtual device contained within the corporate infrastructure to access enterprise data and resources,  
1658 ensuring that no corporate data ever resides on the physical device.

1659 Further, examination of emerging 5G technologies as they relate to mobile device security is a new field  
1660 that presents a wide breadth of research opportunities.

**1661 Appendix A List of Acronyms**

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

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

1663 **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]

|   |  |
|---|--|
| <b>Cryptography</b>                         | 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]  |
| <b>Common Vulnerabilities and Exposures</b> | A dictionary of common names for publicly known information system vulnerabilities [72]  |
| <b>Data Action</b>                          | System operations that process PII [44]  |
| <b>Demilitarized Zone (DMZ)</b>             | A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks [73].  |
| <b>Disassociability</b>                     | Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [44]  |
| <b>Encryption</b>                           | The cryptographic transformation of data to produce ciphertext [68]  |
| <b>Enterprise Mobility Management</b>       | 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].   |
| <b>Identity Verification</b>                | 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]. |
| <b>Impact</b>                               | 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]   |

|                                       |  |
|---------------------------------------|--|
| <b>Key Logger</b>                     | 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]   |
| <b>Malware</b>                        | 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].  |
| <b>Man-in-the-Middle Attack</b>       | 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].  |
| <b>Mobile Device Management (MDM)</b> | 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].   |
| <b>Network Layer</b>                  | Layer of the TCP/IP protocol stack that is responsible for routing packets across networks [15]  |
| <b>Phishing</b>                       | 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]   |
| <b>Predisposing Conditions</b>        | 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] |

|   |   |
|---|---|
| <b>Privacy Risk Assessment Methodology (PRAM)</b> | 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].   |
| <b>Read-Only Memory</b>                           | ROM is a pre-recorded storage medium that can only be read from and not written to [76].  |
| <b>Red Team Exercise</b>                          | 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]  |
| <b>Replay Resistance</b>                          | 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]  |
| <b>Risk</b>                                       | 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]   |
| <b>Risk Assessment</b>                            | 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] |
| <b>Risk Management Framework</b>                  | 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].   |
| <b>Sandbox</b>                                    | 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].  |

|                                       |  |
|---------------------------------------|--|
| <b>Security Control</b>               | 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]  |
| <b>Side-Channel Attacks</b>           | 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].   |
| <b>Social Engineering</b>             | 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]   |
| <b>Threat</b>                         | 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] |
| <b>Threat Events</b>                  | An event or situation that has the potential for causing undesirable consequences or impact [9]  |
| <b>Threat Intelligence</b>            | Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes [78]   |
| <b>Threat Sources</b>                 | 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]   |
| <b>Transport Layer</b>                | Layer of the TCP/IP protocol stack that is responsible for reliable connection-oriented or connectionless end-to-end communications [15]   |
| <b>Transport Layer Security (TLS)</b> | 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].  |

|                                |   |
|--------------------------------|---|
| <b>Trusted Certificate</b>     | 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] |
| <b>Unmanaged Device</b>        | A device inside the assessment boundary that is either unauthorized or, if authorized, not assigned to a person to administer [80]  |
| <b>Virtual Private Network</b> | Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line [68]   |
| <b>Vulnerability</b>           | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [9]  |
| <b>Watering Hole</b>           | 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](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](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](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](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](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](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](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](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](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](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 Technology 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](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].

1665

1666

## 1667 **Appendix D Android, Apple, and Samsung Knox Mobile 1668 Enrollment**

1669 Device enrollment and management capabilities are available when deploying mobile devices in bulk.  
1670 Certain settings can be preloaded, and devices can ship preconfigured for enterprise management. iOS-,  
1671 Android-, and Samsung Knox-based devices integrate directly with Enterprise Mobility Management  
1672 (EMM) solutions, providing enterprise-level management of security controls based on policy.

### 1673 **D.1 Android Devices**

1674 For Android devices, zero-touch enrollment provides an option different from the manual setup of  
1675 Android devices. Android-based devices offer security controls that an EMM can leverage for enterprise  
1676 deployments. The Android Enterprise program by Google is available on devices with Android 5.0  
1677 (Lollipop) and higher. An EMM deploys a device policy controller as part of its on-device agent that  
1678 controls local device policies and system applications on devices. Android Enterprise supports corporate-  
1679 owned personally-enabled and bring your own device deployment scenarios through work-managed  
1680 and work-profile device solutions [82], [83].

### 1681 **D.2 iOS Devices**

1682 For iOS devices, Apple Configurator supports Volume Purchase and Device Enrollment Program  
1683 scenarios. Apple Business Manager provides a mobile device management solution to assist  
1684 organizations in deploying iOS devices. iOS devices are managed by configuration profiles. Configuration  
1685 profiles can force security policies such as virtual private network usage, enterprise Kerberos support,  
1686 and access to cloud services. iOS further incorporates a set of additional security controls in what is  
1687 termed supervised mode, which denotes a corporately owned device. Typically, organizations choose to  
1688 use the Device Enrollment Program for large-scale deployments of iOS devices in supervised mode due  
1689 to the reduction of labor involved in manually configuring each device. However, due to the small  
1690 number of devices in our reference design, we have configured supervised mode using the Apple  
1691 Configurator 2 tool. A more detailed description of iOS capabilities can be found in the iOS Security  
1692 Guide [84], [85].

### 1693 **D.3 Samsung Knox Devices**

1694 Samsung Knox Mobile Enrollment provides the ability to add Samsung devices to the enterprise without  
1695 manually enrolling each device. Samsung Knox Mobile Enrollment works on Samsung Galaxy devices  
1696 running Android Lollipop or higher. It allows remote provisioning of devices when they connect to Wi-Fi  
1697 or cellular networks. Samsung Knox Mobile Enrollment works with a number of EMM solutions,  
1698 including cloud-based options [86], [87], [88].

## 1700 **Appendix E Risk Assessment**

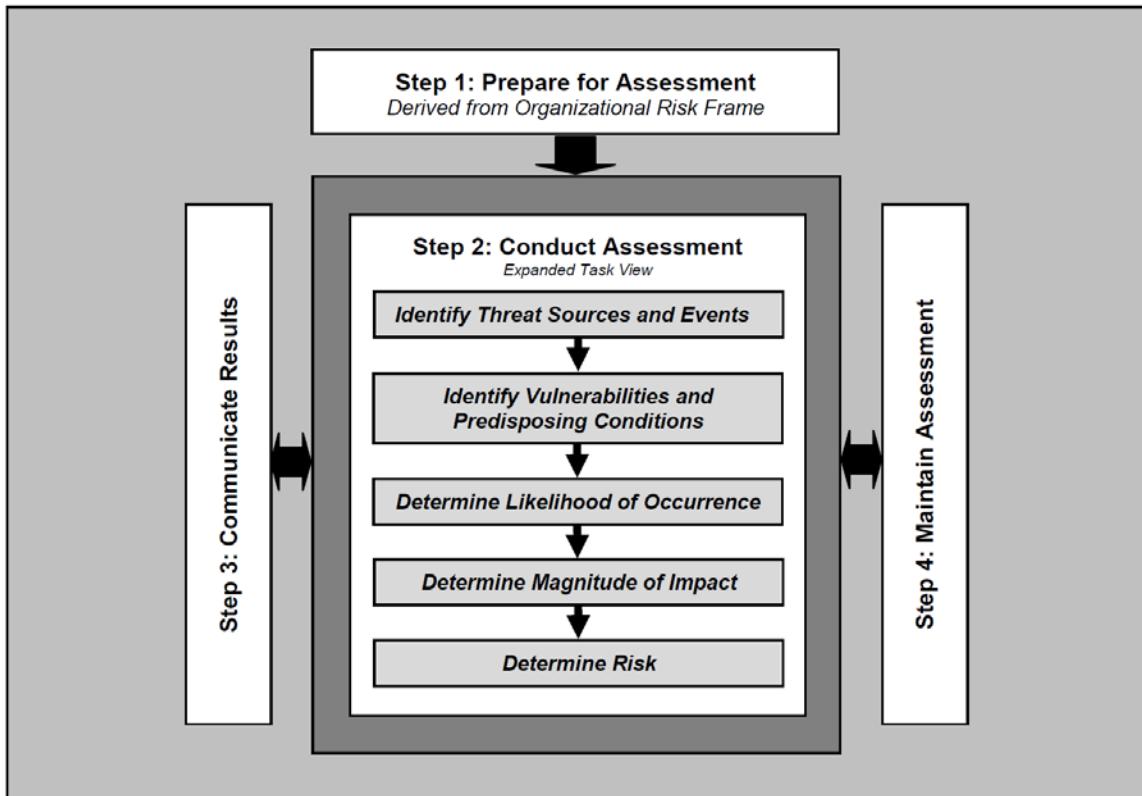
### 1701 **E.1 Risk Assessment**

1702 NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, [9] states that risk is “a measure of  
1703 the extent to which an entity is threatened by a potential circumstance or event, and typically a function  
1704 of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of  
1705 occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and  
1706 prioritizing risks to organizational operations (including mission, functions, image, reputation),  
1707 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of  
1708 an information system. Part of risk management incorporates threat and vulnerability analyses, and  
1709 considers mitigations provided by security controls planned or in place.”

1710 The NCCoE recommends that any discussion of risk management, particularly at the enterprise level,  
1711 begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for  
1712 Information Systems and Organizations*—material that is available to the public. The Risk Management  
1713 Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks,  
1714 from which we developed the project, the security characteristics of the build, and this guide.

1715 This section details the risk assessment undertaken to improve the mobile security posture of the  
1716 fictional organization Orvilia Development. Typically, a National Institute of Standards and Technology  
1717 (NIST) Special Publication (SP) 800-30 Revision 1-based risk assessment follows a four-step process as  
1718 shown in Figure E-1: Prepare for assessment, conduct assessment, communicate results, and maintain  
1719 assessment.

1720 Figure E-1 Risk Assessment Process



1721 To provide the most value in this exercise:

- 1722     ▪ We focused on the preparation, which established the context of the risk assessment.
- 1723     ▪ 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.
- 1725     ▪ 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.

1727 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.

### 1730     E.1.1 Task 1-1: Risk Assessment Purpose

1731     *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.*

1733 The purpose of the risk assessment of Orvilia Development was to identify and document new risks to  
1734 its mission resulting from addition of a mobility program.

1735 The results of the risk assessment informed decisions to Orvilia's mobility deployment that included:

- 1736     ▪ implementation of new security mechanisms  
1737     ▪ configuration changes to existing infrastructure  
1738     ▪ updates to security and appropriate-use policies relevant to their mobility program

### 1739 **E.1.2 Task 1-2: Risk Assessment Scope**

1740 *Identify the scope of the risk assessment in terms of organizational applicability, time frame supported,*  
1741 *and architectural/technology considerations.*

#### 1742 **Organizational Applicability:**

1743 The scope of this risk assessment was limited to systems impacted by inclusion of a mobility program; it  
1744 did not include existing information technology (IT) infrastructure to which no impact was anticipated.  
1745 With their original architecture, Orvilia deployed corporate-owned personally-enabled (COPE) devices.  
1746 Orvilia employees utilized mobile devices for local and remote work activities and limited personal  
1747 activities (e.g., phone calls, messaging, social applications, and personal emails).

1748 With Orvilia's new government contract, this risk assessment also evaluated Orvilia's mobile  
1749 deployment regarding its ability to access and store government data while meeting applicable  
1750 information security and privacy requirements.

1751 While not directly associated with risk assessment activities, Orvilia will be required to demonstrate  
1752 compliance with government standards and policies established to improve data security. Therefore,  
1753 Orvilia needed to determine how compliance with government policy and application of its standards  
1754 would best align with its strategy to identify, protect again, detect, respond to, and recover from threats  
1755 related to its mobility program.

#### 1756 **Time Frame Supported:**

1757 Because this was the first risk assessment performed by Orvilia, the process was more time-intensive  
1758 than it will be in future risk management cycles. Orvilia completed the initial risk assessment within six  
1759 months.

#### 1760 **Architectural and Technology Considerations:**

1761 This risk assessment was scoped to Orvilia's mobile deployment, which constitutes mobile devices used  
1762 to access Orvilia enterprise resources along with any backend IT components used to manage or provide  
1763 services to those mobile devices.

1764 The following provide an overview of the mobile deployment components involved in the original  
1765 (current) Orvilia architecture.

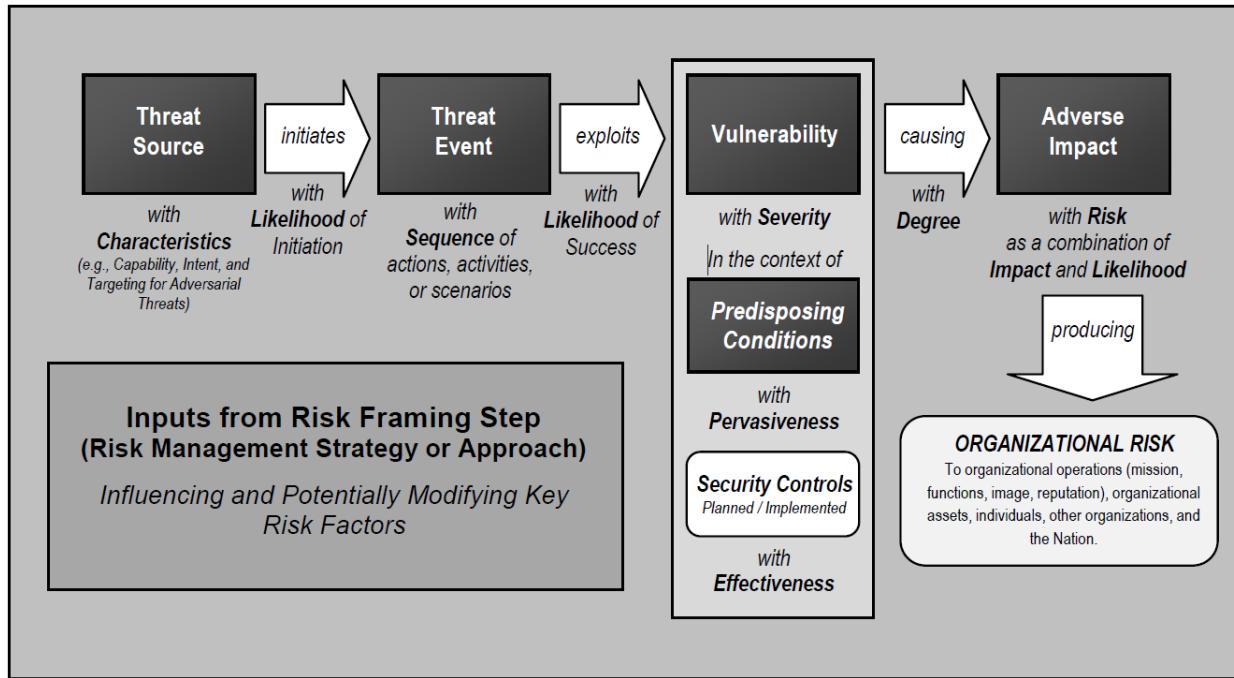
- 1766     ■ **Mobile Device:** A mobile device is a small form factor device with a rich operating system, at  
1767       least one wireless network interface, and the ability to run applications. These features are  
1768       considered essential for Orvilia to have portable and efficient access to enterprise data.
- 1769     ■ **Communication Networks and Data Transmission:** Mobile devices will establish connections to  
1770       the internet by using their cellular or Wi-Fi adapters. As connections may be made to unsecured  
1771       access points or may traverse untrusted networks, consideration will be given to the risks  
1772       associated with the security of those connections and the data transmitted over them.  
1773       Additionally, the organization will need to consider risks arising from permitting inbound  
1774       connections by mobile devices via the internet.
- 1775     ■ **Public Application Stores:** With a COPE deployment strategy, employees will have the option to  
1776       download any mobile application available from official platform application stores (e.g., Google  
1777       Play Store). While those platforms analyze applications for malicious behaviors, it is still possible  
1778       for such applications to exceed Orvilia's needs for user privacy or pose a risk to the devices or  
1779       data. Therefore, risks from such applications should be included in this assessment.
- 1780     ■ **Device and Operating System (OS) Vendor Infrastructure:** The hardware, firmware, and  
1781       software that compose each model of mobile device can vary, particularly those from different  
1782       manufacturers and vendors, which may incorporate technology that is exclusive to their  
1783       products. It will be important to select devices that demonstrate security mechanisms that align  
1784       with the organization's risk mitigation strategy. However, risks that are specific to given device  
1785       components (e.g., chipsets or driver versions) will be out of scope for this assessment.
- 1786     ■ **Enterprise Systems:** If a potentially compromised mobile device can connect to the enterprise, it  
1787       poses direct risks to any systems it can reach or data it can access. Such systems will reasonably  
1788       include on-premises mobile application stores, mobile management technologies, email servers,  
1789       file servers, and intranet web servers. Subsequent compromise of any of these systems may  
1790       cascade to others not directly reachable by the mobile device. Risks to all such systems by a  
1791       mobile device should be included in this assessment.

### 1792 E.1.3 Task 1-3: Risk Assessment Assumptions and Constraints

1793 *Identify the specific assumptions and constraints under which the risk assessment is conducted.*

1794 Risk assessment assumptions and constraints were developed using a NIST SP 800-30 Revision 1 Generic  
1795 Risk Model as shown in Figure E-2.

1796 Figure E-2 NIST 800-30 Generic Risk Model

1797 *E.1.3.1 Risk Assessment Assumptions*

1798 Some of the threats and their resulting risks and impacts span several levels. In cases where these risks  
 1799 and impacts have several possible levels, it was assumed that Orvilia would document these using a  
 1800 high-water mark methodology. This assumption of greatest risk then provided the basis for risk  
 1801 mitigation activities. For example, where the threat risk could pose a moderate, high, or very high  
 1802 outcome, the very high outcome was selected, and these very high risks were prioritized for mitigation.

1803 *E.1.3.2 Risk Assessment Constraints*

1804 Information regarding the following were used as input for the constraints for the risk assessment.

- 1805     ▪ threat sources
- 1806     ▪ threat events
- 1807     ▪ vulnerabilities and predisposing conditions
- 1808     ▪ likelihood
- 1809     ▪ impacts
- 1810     ▪ risk assessment and analysis approaches
- 1811     ▪ resources available for the assessment

- 1812        □ skills and expertise

1813 **Threat Sources**

1814 Orvilia's executives and managers identified two threat sources as possible concerns. Orvilia's technical  
1815 staff were provided security control mappings identified within this guide to help them understand the  
1816 additional security that the example solution could provide to Orvilia as they implemented the example  
1817 solution.

1818 Additionally, due to the cybersecurity-focused scope of the risk assessment, non-adversarial threat  
1819 sources (e.g., unintentional hardware, software, or system design and architecture shortcoming threats)  
1820 were not considered.

1821 As identified in Section E.1.6, Task 2-1: Identify and Characterize Threat Sources of Concern, the risk  
1822 assessment identified the following threat sources of concern:

- 1823        □ Orvilia's competitors  
1824        □ nation-state actors

1825 **Threat Events**

- 1826        □ Threat events were described at a high level and in general terms within the risk assessment.  
1827 Similar threat events were combined into a single, broader threat.
- 1828        □ Only those threat events that have been previously observed by an authoritative source were  
1829 considered (e.g., reported as already having occurred by other organizations), drawing primarily  
1830 from the NIST National Cybersecurity Center of Excellence Mobile Threat Catalogue [6].
- 1831        □ Threat events involving exploitation of vulnerabilities within the cellular network, including a  
1832 mobile device's cellular baseband, reasonably exceeded Orvilia's ability to directly identify and  
1833 mitigate them and were not further assessed.
- 1834        □ Threat events involving exploitation of vulnerabilities in low-level hardware, firmware, and  
1835 device controllers reasonably exceeded Orvilia's ability to directly identify and mitigate them  
1836 and were not further assessed.
- 1837        □ Threat events involving exploitation of vulnerabilities in the supply chain reasonably exceeded  
1838 Orvilia's ability to directly identify and mitigate them and were not further assessed.

1839 **Vulnerabilities and Predisposing Conditions**

- 1840        □ Mobile device vulnerabilities considered during this risk assessment included those in mobile  
1841 operating systems and mobile applications, including third-party software libraries.
- 1842        □ Vulnerabilities in commonly used noncellular network protocols such as Bluetooth and Wi-Fi  
1843 were considered.

- 1844       ■ Vulnerabilities related to a potential Enterprise Mobility Management (EMM) system were  
1845       considered.

- 1846       ■ Additional information and determinations were made via Appendix F of NIST SP 800-30  
1847       Revision 1.

1848       **Likelihood**

- 1849       ■ Likelihood determinations were made via Appendix G of NIST SP 800-30 Revision 1.

1850       Note: The rating of overall likelihood is derived from the Likelihood of Initiation and Likelihood that  
1851       Threat Events Result from Adverse Impacts using Table G-5 of Appendix G in NIST SP 800-30 Revision 1  
1852       [9]. Ratings of the latter two variables relied heavily on the subjective judgment of Orvilia employees.

1853       **Impacts**

- 1854       ■ Impact determinations were made via Appendix H of NIST SP 800-30 Revision 1.

1855       Note: Ratings of impact relied heavily on the subjective judgment of Orvilia employees.

1856       **Risk Assessment and Analysis Approaches**

- 1857       ■ This risk assessment focused on identifying an initial set of threats to Orvilia's mobile  
1858       deployment.
- 1859       ■ Approaches for describing threats and their impact were informed by the Adversarial Tactics,  
1860       Techniques, and Common Knowledge (ATT&CK) Framework [89].
- 1861       ■ The rating of Risk was derived from both the overall likelihood and level of impact using Table I-  
1862       2 of Appendix I in NIST SP 800-30 Revision 1 [9].

1863       **Resources Available for the Assessment**

- 1864       ■ Orvilia ensured the appropriate staff with the requisite expertise were available to conduct the  
1865       assessment within the time allotted.
- 1866       ■ Orvilia provided funding for the risk analysis staff.
- 1867       ■ Orvilia staff who conducted the risk assessment had the necessary information systems and  
1868       software.

1869       **Skills and Expertise**

- 1870       ■ Risk assessments were conducted by experts leveraging industry best practices and NIST risk  
1871       assessment frameworks.

1872       **E.1.4 Task 1-4: Risk Assessment Threat, Vulnerability, and Impact Sources**

1873       *Identify the sources of descriptive threat, vulnerability, and impact information to be used in the risk  
1874       assessment.*

1875 Orvilia used the following methods to identify mobile infrastructure threats, vulnerabilities, and impacts.

1876 *E.1.4.1 Sources of Threats*

1877 This risk assessment identified NIST's Mobile Threat Catalogue (MTC) [6], along with its associated NIST  
1878 Interagency Report 8144, *Assessing Threats to Mobile Devices & Infrastructure* [90], and MITRE's  
1879 ATT&CK Mobile Profile [91] as credible sources for threat information. Each entry in the MTC contains  
1880 several pieces of information: an identifier, a category, a high-level description, details on its origin,  
1881 exploit examples, Common Vulnerabilities and Exposures [92] examples, possible countermeasures, and  
1882 academic references.

1883 MITRE's ATT&CK is a curated knowledge base and model for cyber-adversary behavior. ATT&CK details  
1884 specific techniques that can be used by cyber adversaries. Each technique entry typically includes a  
1885 detailed technical description, mitigations, detection analytics, examples of use by malicious actors, and  
1886 references. The ATT&CK model organizes these techniques into high-level malicious actor tactical  
1887 objectives, referred to as tactics. A primary use case for ATT&CK is use by organizations to assess the  
1888 state of their cybersecurity defenses and prioritize deployment of defensive capabilities. The ATT&CK  
1889 Mobile Profile describes tactics and techniques specific to the mobile environment.

1890 Due to Orvilia's current use of cloud services, it identified the outputs of the Federal Risk and  
1891 Authorization Management Program [93] and associated NIST SP 800-53 security controls as being in  
1892 scope for this risk assessment.

1893 *E.1.4.2 Sources of Vulnerabilities*

1894 Vulnerabilities are commonly associated with mobile operating systems, device drivers, mobile  
1895 applications, and third-party libraries. However, vulnerabilities can be present in any level of the mobile  
1896 technology stack. For up-to-date information regarding vulnerabilities, this risk assessment identified  
1897 the National Vulnerability Database (NVD) [94] as a credible source of information. The NVD is the U.S.  
1898 government repository of standards-based vulnerability management data. Use of NVD was  
1899 supplemented by review of individual vendor vulnerability disclosures such as those published in the  
1900 Pixel/Nexus Security Bulletins [95] for Android, Apple security updates [96] for iOS, Managing Devices &  
1901 Corporate Data on iOS [97], and Android Security Updates [98] for Android-based Samsung devices.

1902 *E.1.4.3 Sources of Impacts*

1903 This risk assessment identified the scenario described in Section E.1.2 as the primary source of impact  
1904 determination information. The scenario identified the following systems as being critical to the  
1905 organization's mission:

- 1906
  - Microsoft Active Directory domain
  - Microsoft Exchange email server

- 1908        □ timekeeping web application  
 1909        □ travel support web application  
 1910        □ corporately owned mobile devices
- 1911 An example of a successful attack against a mobile device is one that could be used to glean the  
 1912 credentials for the travel support web application and use them to penetrate the application server.  
 1913 While Orvilia can absorb minimal downtime to the web application, the attacker could use this position  
 1914 to gain a foothold in the Orvilia infrastructure to laterally move to more critical systems in the  
 1915 environment, such as the email server. Compromise of the email server would have high impact,  
 1916 possibly causing serious harm to the organization.

### 1917 [E.1.5 Task 1-5: Risk Assessment Risk Model and Analytic Approach Identification](#)

1918 *Identify the risk model and analytic approach to be used in the risk assessment.*

1919 In this risk assessment, the analytic approach used qualitative (i.e., subjective) ratings of risk (i.e., very  
 1920 low, low, moderate, high, and very high). The approach was primarily threat oriented, as described in  
 1921 section E.1.6.

### 1922 [E.1.6 Task 2-1: Identify and Characterize Threat Sources of Concern](#)

1923 *Identify and characterize threat sources of concern, including capability, intent, and targeting  
 1924 characteristics for adversarial threats and range of effects for non-adversarial threats.*

1925 Orvilia examined NIST SP 800-30 Revision 1's Table D-2: Taxonomy of Threat Sources [9] and identified  
 1926 the following threat sources of concern:

1927 **Table E-1 Threat Sources of Concern**

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

1928 Orvilia produced the following table as output of Task 2-1 to provide relevant inputs to the risk tables. It  
 1929 identifies the threat sources identified in NIST SP 800-30 Revision 1 with the associated risk rating of

1930 capability, intent, and targeting score (using the previously mentioned five-point scale: very low, low,  
 1931 moderate, high, and very high).

1932 Orvilia's assessment found that all threat events could be initiated by both threat sources  
 1933 (Organization/Competitor and Nation-State).

1934 Capability refers to the level of expertise of the malicious actor. Intent refers to the malicious actor's  
 1935 goal. Targeting refers to the reconnaissance and selection methods performed by the malicious actor.

#### 1936 **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 |

#### 1937 **E.1.7 Task 2-2: Identify Potential Threat Events**

1938 *Identify potential threat events, relevance of the events, and the threat sources that could initiate the*  
 1939 *events.*

1940 The threat events used for the example solution are described below. These threat events describe how  
 1941 the mobile devices in Orvilia might be compromised by malicious activities. All of the threat events map  
 1942 to both threat sources identified in Section E.1.6.

1943 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  
 1944 analyzed the sources of mobile threats identified in Task 1-4. Using this process, Orvilia leadership  
 1945 identified the following threat events.

##### 1946 **E.1.7.1 Threat Event 1—Unauthorized Access to sensitive Information via a Malicious or** 1947 **Privacy-Intrusive Application**

1948 A mobile application can attempt to collect and exfiltrate any information to which it has been granted  
 1949 access. This includes any information generated during use of the application (e.g., user input), user-  
 1950 granted permissions (e.g., contacts, calendar, call logs, camera roll), and general device data available to  
 1951 any application (e.g., International Mobile Equipment Identity, device make and model, serial number).  
 1952 Further, if a malicious application exploits a vulnerability in other applications, the OS, or device

1953 firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or  
1954 otherwise accessible through the device.

1955 *E.1.7.2 Threat Event 2—Theft of credentials Through an SMS or Email Phishing Campaign*

1956 Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate  
1957 ones and entice users to authenticate to them by distributing phishing messages over short message  
1958 service (SMS) or email. Effective use of social engineering techniques such as impersonating an authority  
1959 figure or creating a sense of urgency may compel users to forgo scrutiny of the message and proceed to  
1960 authenticate to the fraudulent website; it then captures and stores the user’s credentials before  
1961 (usually) forwarding them to the legitimate website to allay suspicion.

1962 *E.1.7.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email  
1963 Messages*

1964 Malicious actors may send users SMS or email messages that contain a uniform resource locator (URL)  
1965 where a malicious application is hosted. Generally, such messages are crafted using social engineering  
1966 techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby  
1967 increasing the likelihood they access the URL by using their mobile device. If the URL is accessed, the  
1968 device will attempt to download and install the application. Effective use of social engineering by the  
1969 attacker will further compel an otherwise suspicious user to grant any trust required by the developer  
1970 and all permissions requested by the application. Granting the former facilitates installation of other  
1971 malicious applications by the same developer, and granting the latter increases the potential for the  
1972 application to do direct harm.

1973 *E.1.7.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation of Known  
1974 Vulnerability in the OS or Firmware*

1975 When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers,  
1976 the delivered code generally executes with elevated privileges and issues commands in the context of  
1977 the root user or the OS kernel. This may be enough for some to accomplish their goal, but advanced  
1978 malicious actors will usually attempt to install additional malicious tools and to establish a persistent  
1979 presence. If successful, the attacker will be able to launch further attacks against the user, the device, or  
1980 any other systems to which the device connects. As a result, any data stored on, generated by, or  
1981 accessible to the device at that time—or in the future—may be compromised.

1982 *E.1.7.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors*

1983 Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera,  
1984 gyroscope, Global Positioning System receiver, and radios) can use them to conduct surveillance. It may  
1985 be directed at the user, as when tracking the device location, or it may be applied more generally, as  
1986 when recording any nearby sounds. Captured sensor data, such as a recording of an executive meeting,

1987 may be immediately useful to a malicious actor. Alternatively, the data may be analyzed in isolation or in  
1988 combination with other data to yield sensitive information. For example, audio recordings of on-device  
1989 or proximate activity can be used to probabilistically determine user inputs to touchscreens and  
1990 keyboards—essentially turning the device into a remote keylogger.

1991 *E.1.7.6 Threat Event 6—Compromise of the Integrity of the Device or Its Network  
1992 Communications via Installation of Malicious EMM/MDM, Network, VPN Profiles,  
1993 or Certificates*

1994 Malicious actors who successfully install an EMM/mobile device management (MDM), network, or  
1995 virtual private network (VPN) profile or certificate onto a device will gain a measure of additional control  
1996 over the device or its communications. Presence of an EMM/MDM profile will allow an attacker to  
1997 misuse existing OS application programming interfaces to send the device a wide variety of commands.  
1998 This may allow a malicious actor to obtain device information, install or restrict applications, or remotely  
1999 locate, lock, or wipe the device. Malicious network profiles may allow a malicious actor to automatically  
2000 compel the device to connect to access points under their control to achieve a man-in-the-middle attack  
2001 on all outbound connections. Alternatively, VPN profiles assist in the undetected exfiltration of sensitive  
2002 data by encrypting it, thus hiding it from network scanning tools. Additionally, malicious certificates may  
2003 allow the malicious actor to compel the device to automatically trust connections to malicious web  
2004 servers, wireless access points, or installation of applications under their control.

2005 *E.1.7.7 Threat Event 7—Loss of Confidentiality of Sensitive Information via Eavesdropping  
2006 on Unencrypted Device Communications*

2007 Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as  
2008 public Wi-Fi access points, which are commonly provided by coffee shops and hotels. While a device is  
2009 connected to such a network, an attacker would gain unauthorized access to any data sent or received  
2010 by the device for any session not already protected by encryption at either the transport or application  
2011 layers. Even if the transmitted data were encrypted, an attacker would be privy to the domains, internet  
2012 protocol addresses, and services (as indicated by port numbers) to which the device connects; such  
2013 information could be used in future watering hole attacks or man-in-the-middle attacks against the  
2014 device user. Additionally, visibility into network layer traffic enables a malicious actor to conduct side-  
2015 channel attacks against its encrypted messages, which can still result in a loss of confidentiality. Further,  
2016 eavesdropping on unencrypted messages during a handshake to establish an encrypted session with  
2017 another host or endpoint may facilitate attacks that ultimately compromise the security of the session.

2018 *E.1.7.8 Threat Event 8—Compromise of Device Integrity via Observed, Inferred, or Brute-  
2019 Forced Device Unlock Code*

2020 A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel  
2021 attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the

2022 device; only the third technique requires physical access. However, side-channel attacks that infer the  
2023 unlock code by detecting taps and swipes to the screen can be attempted by applications with access to  
2024 any peripherals that detect sound or motion (e.g., microphone, gyroscope, or accelerometer). Once the  
2025 device unlock code has been obtained, a malicious actor with physical access to the device will gain  
2026 immediate access to any data or functionality not already protected by additional access control  
2027 mechanisms. Additionally, if the user employs the device unlock code as a credential to any other  
2028 systems, the malicious actor may further gain unauthorized access to those systems.

2029 *E.1.7.9 Threat Event 9—Unauthorized Access to Backend Services via Authentication or*  
2030 *Credential Storage Vulnerabilities in Internally Developed Applications*

2031 If a malicious actor gains unauthorized access to a mobile device, the malicious actor also has access to  
2032 the data and applications on that mobile device. The mobile device may contain an organization's in-  
2033 house applications and can subsequently gain access to sensitive data or backend services. This could  
2034 result from weaknesses or vulnerabilities present in the authentication or credential storage  
2035 mechanisms implemented within an in-house application.

2036 *E.1.7.10 Threat Event 10—Unauthorized Access of Enterprise Resources from an*  
2037 *Unmanaged and Potentially Compromised Device*

2038 An employee who accesses enterprise resources from an unmanaged mobile device may expose the  
2039 enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit  
2040 from security mechanisms deployed by the organization such as mobile threat defense, mobile threat  
2041 intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an  
2042 organization's visibility into the state of a mobile device, including if the device is compromised by a  
2043 malicious actor. Therefore, users who violate security policies to gain unauthorized access to enterprise  
2044 resources from such devices risk providing malicious actors with access to sensitive organizational data,  
2045 services, and systems.

2046 *E.1.7.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen Device*

2047 Due to the nature of the small form factor of mobile devices, they are easy to misplace or be stolen. A  
2048 malicious actor who gains physical custody of a device with inadequate security controls may be able to  
2049 gain unauthorized access to sensitive data or resources accessible to the device.

2050 *E.1.7.12 Threat Event 12—Loss of Confidentiality of Organizational Data due to Its*  
2051 *Unauthorized Storage to Non-Organizationally Managed Services*

2052 If employees violate data management policies by using unmanaged services to store sensitive  
2053 organizational data, the data will be placed outside organizational control, where the organization can  
2054 no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the

2055 unauthorized service account or any system hosting that account may gain unauthorized access to the  
 2056 data.

2057 Further, storage of sensitive data in an unmanaged service may subject the user or the organization to  
 2058 prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate  
 2059 efforts by the organization to achieve remediation or recovery from any future losses, such as those  
 2060 resulting from the public disclosure of trade secrets.

### 2061 E.1.8 Task 2-3: Identify Vulnerabilities and Predisposing Conditions

2062 *Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of  
 2063 concern result in adverse impacts.*

2064 Drawing on the scenario described in Section 3.2.1 of NIST SP 800-30 Revision 1, there existed  
 2065 vulnerabilities and predisposing conditions that increased the likelihood that identified threat events  
 2066 would result in adverse impacts for Orvilia. Each vulnerability or predisposing condition is listed in the  
 2067 table below along with the corresponding threat events.

2068 The methodology used to rate the level of pervasiveness was qualitative (i.e., subjective) and used a  
 2069 five-point scale.

- 2070     ▪ Very High
- 2071     ▪ High
- 2072     ▪ Moderate
- 2073     ▪ Low
- 2074     ▪ Very Low

2075 **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     |

2076    **Note 1:** Ratings of the level of pervasiveness were based on the qualitative scale found in Table F-5 of  
 2077    Appendix F in NIST SP 800-30 Revision 1 [9].

2078    **Note 2:** Ratings of pervasiveness indicate that the vulnerabilities apply few (i.e., very low), some (i.e.,  
 2079    low), many (i.e., moderate), most (i.e., high), or all (i.e., very high) organizational missions/business  
 2080    functions and processes, or information systems.

### 2081    E.1.9 Task 2-4: Determine Likelihood of a Threat and the Likelihood of the Threat 2082       Having Adverse Impacts

2083    *Determine the likelihood that threat events of concern result in adverse impacts, considering (i) the  
 2084    characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing  
 2085    conditions identified; and (iii) the organizational susceptibility reflecting the  
 2086    safeguards/countermeasures planned or implemented to impede such events.*

2087    In the interest of brevity, the threat events of concern identified in Task 2-2 were limited to those  
 2088    presumed to have a foreseeably high likelihood of occurrence.

2089    The methodology used to identify the likelihood of threats of concern was qualitative (i.e., subjective)  
 2090    and used the following five-point scale.

- 2091         □ Very High
- 2092         □ High
- 2093         □ Moderate
- 2094         □ Low
- 2095         □ Very Low

2096 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               |

2097 **Note 1:** For the Likelihood of Threat Event Initiation, the ratings translate as follows: Moderate =  
 2098 malicious actor is somewhat likely to initiate; High = malicious actor is highly likely to initiate; Very high =  
 2099 malicious actor is almost certain to initiate.

2100 **Note 2:** For the Likelihood of Threat Event Resulting in Adverse Impacts, the ratings translate as follows:  
 2101 Moderate = if the threat is initiated, it is somewhat likely to have adverse impacts; High = if the threat is  
 2102 initiated, it is highly likely to have adverse impacts; Very high = if the threat is initiated, it is almost  
 2103 certain to have adverse impacts.

2104 **Note 3:** Overall likelihood was calculated based on the qualitative scale found in Table G-3 of Appendix  
 2105 G in NIST SP 800-30 Revision 1 [9]. It is derived from both the Likelihood of Threat Event Initiation and

2106 Likelihood of Threat Event Resulting in Adverse Impacts. Because these scales are not true interval  
 2107 scales, the combined overall ratings do not always reflect a strict mathematical average of the two  
 2108 ratings.

### 2109 E.1.10 Task 2-5: Determine the Extent of Adverse Impacts

2110 *Determine the adverse impacts from threat events of concern considering (i) the characteristics of the*  
 2111 *threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified;*  
 2112 *and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede*  
 2113 *such events.*

2114 Threat events with a high potential for adverse impacts were then identified in our specific scenario.

2115 The methodology used to determine the extent of adverse impacts was qualitative (i.e., subjective) and  
 2116 used the following five-point scale.

- 2117     ■ Very High
- 2118     ■ High
- 2119     ■ Moderate
- 2120     ■ Low
- 2121     ■ Very Low

2122 **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<br><br>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<br><br>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<br><br>Damage to or loss of information systems or networks<br><br>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<br><br>Damage to or loss of information systems or networks<br><br>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<br><br>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<br><br>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<br><br>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<br><br>Damage to or loss of information systems or networks<br><br>Damage to reputation (and hence future or potential trust relationships)<br><br>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<br><br>Damage to or loss of information systems or networks<br><br>Loss of personally identifiable information<br><br>Damage to reputation (and hence future or potential trust relationships) | High           |

2123   **Note 1:** Ratings of maximum impact were based on the qualitative scale found in Appendix H, Table H-3  
 2124   in NIST SP 800-30 Revision 1 [9].

2125   **Note 2:** Ratings of maximum impact indicate the threat event could be expected to have negligible (i.e.,  
 2126   very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), or multiple  
 2127   severe or catastrophic effects (i.e., very high).

2128   **Note 3:** For specific examples of types of impact, see Appendix H of NIST SP 800-30, Revision 1 [9].

2129    **E.1.11 Task 2-6: Determine Risk to Organization**

2130    *Determine the risk to the organization from threat events of concern considering (i) the impact that  
2131    would result from the events; and (ii) the likelihood of the events occurring.*

2132    In the interest of brevity, the threat events of concern identified in Task 2-2 were limited to those  
2133    presumed to have a foreseeably high likelihood of occurrence and high potential for adverse impact in  
2134    Orvilia's specific scenario.

2135    **Threat Source Characteristics**

2136    This table summarizes the risk assessment findings.

2137    The methodology used to identify risk to organization was qualitative (i.e., subjective) and used the  
2138    following five-point scale.

- 2139        □ Very High
- 2140        □ High
- 2141        □ Moderate
- 2142        □ Low
- 2143        □ Very Low

2144    **Table E-6 Summary of Risk Assessment Findings**

| Threat Event  | Vulnerabilities,<br>Predisposing<br>Conditions | Overall<br>Likelihood | Level of<br>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 |

2145      **Note 1:** Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST SP 800-30  
 2146      Revision 1 [9].

2147   **Note 2:** The risk rating itself is derived from both the overall likelihood and level of impact using Table I-  
2148 2 of Appendix I in NIST SP 800-30 Revision 1 [9]. Because these scales are not true interval scales, the  
2149 combined overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these  
2150 two variables. This is demonstrated in the table above in which levels of Moderate weigh more heavily  
2151 than other ratings.

2152   **Note 3:** Ratings of risk relate to the probability and level of adverse effect on organizational operations,  
2153 organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1,  
2154 adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low),  
2155 serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic effects (i.e.,  
2156 very high).

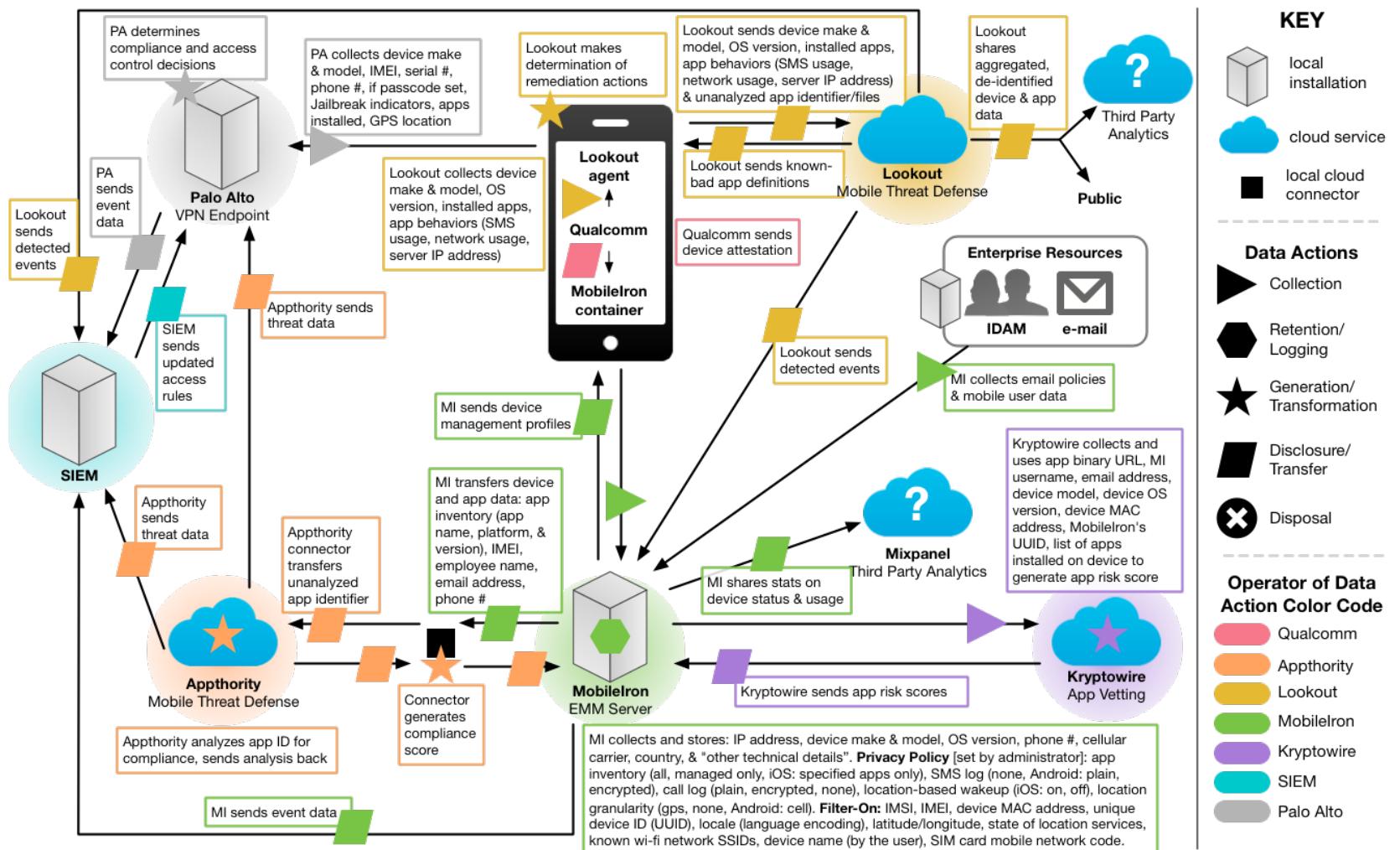
## 2157    **Appendix F    Privacy Risk Assessment**

2158 This section describes the privacy risk assessment conducted on Orvilia's enterprise security  
2159 architecture. To perform the privacy risk assessment, the National Institute of Standards and Technology  
2160 (NIST) Privacy Risk Assessment Methodology (PRAM) was used, a tool for analyzing, assessing, and  
2161 prioritizing privacy risks to help organizations determine how to respond and select appropriate  
2162 solutions. The PRAM can also serve as a useful communication tool to convey privacy risks within an  
2163 organization. A blank version of the PRAM is available for download on NIST's website [43].

2164 The PRAM uses the privacy risk model and privacy engineering objectives described in NIST Internal  
2165 Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [44], to  
2166 analyze potential problematic data actions. Data actions are any system operations that process  
2167 personally identifiable information (PII). Processing can include collection, retention, logging, analysis,  
2168 generation, transformation or merging, disclosure, transfer, and disposal of PII. A problematic data  
2169 action is one that could cause an adverse effect for individuals.

2170 The PRAM begins with framing the business objectives for the system, including the organizational  
2171 needs served, and framing organizational privacy governance, including identification of privacy-related  
2172 legal obligations and commitments to principles or other organizational policies. Next, create a data  
2173 map to illustrate the data actions performed by the system and the PII processed by the data actions.  
2174 These data actions, the PII being processed, and the contextual factors that describe the circumstances  
2175 surrounding the system's processing of PII serve as inputs to the risk analysis. Then, assess the  
2176 probability that a data action will become problematic for individuals, assess the secondary costs  
2177 absorbed by the organization from a data action creating a problem for individuals, and use likelihood  
2178 and impact calculations to determine the total estimated risk per data action. Finally, list potential  
2179 mitigating technical and policy controls for the identified risks. The output from the PRAM activities  
2180 resulted in the information contained in Figure F-1.

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



2182 As an output of the Orvilia PRAM, we identified three broad data actions with the potential to create  
2183 problems for individuals and relevant mitigations. Some mitigations listed under a particular data action  
2184 may provide privacy benefits to individuals beyond the scope of that data action. We also identified  
2185 overarching training and support controls that can help mitigate risks associated with all three of these  
2186 data actions.

2187 While a security information and event management (SIEM) capability was not used in the reference  
2188 implementation, SIEMs, as discussed here, can be extremely beneficial in understanding the privacy  
2189 implications of the mobile device security data being logged, aggregated, and stored.

## 2190 **F.1 Data Action 1: Blocking Access and Wiping Devices**

2191 Devices that might pose a risk to the organization’s security posture can be blocked from accessing  
2192 enterprise resources or wiped and reset to factory setting defaults. Options are outlined in the following  
2193 sections for how this might be accomplished.

### 2194 **F.1.1 Potential Problem for Individuals**

2195 In a corporate-owned personally-enabled or bring your own device environment, employees are likely to  
2196 use their devices for both personal and work-related purposes. Therefore, in a system that features the  
2197 capability to wipe a device entirely, there could be an issue of employees losing personal data—and  
2198 employees may not even expect this possibility. A hypothetical example would be that an Orvilia  
2199 employee stores pictures of their newborn child on their mobile device, but these photos are lost when  
2200 their device is wiped after anomalous activity is detected.

### 2201 **F.1.2 Mitigations**

#### 2202 **Block access instead of wiping devices.**

2203 As an alternative to wiping data entirely, devices can be blocked from accessing enterprise resources,  
2204 for example, until an unapproved application is removed. This temporary blocking of access helps  
2205 ensure an individual will not lose personal data through a full wipe of a device. Taking this approach may  
2206 help bring the system’s capabilities into alignment with employees’ expectations about what can  
2207 happen to their devices, especially if they are unaware that devices can be wiped by administrators—  
2208 providing for greater *predictability* in the system.

- 2209     ■ Related mitigation: If this approach is taken, remediation processes should also be established  
2210       and communicated to employees. It is important to have a clear remediation process in place to  
2211       help employees regain access to resources on their devices at the appropriate time. It is equally  
2212       important to clearly convey this remediation process to employees. A remediation process  
2213       provides greater manageability in the system supporting employees’ ability to access resources.  
2214       If well communicated to employees, this also provides greater predictability, as employees will  
2215       know the steps involved in regaining access.

2216 **Enable only selective wiping.**

2217 An alternative mitigation option for wiping is to specify the information to be wiped. Performing a  
2218 selective wipe is an option that only removes enterprise data from the device instead of being a full  
2219 factory reset. When configured this way, a wipe preserves employees' personal configurations,  
2220 applications, and data while removing only the corporate configurations, applications, and data. Within  
2221 the example solution, this option is available for iOS devices.

2222 **Advise employees to back up the personal data maintained on devices.**

2223 If device wiping remains an option for administrators, encourage employees to perform regular backups  
2224 of their personal data to ensure it remains accessible in case of a wipe.

2225 **Limit staff with the ability to perform wipes or block access.**

2226 Limit staff with the ability to perform a wipe to only those with that responsibility by using role-based  
2227 access controls. This can help decrease the chances of accidentally removing employee data or blocking  
2228 access to resources.

## 2229 **F.2 Data Action 2: Employee Monitoring**

2230 The assessed infrastructure offers Orvilia a number of security capabilities, including reliance on  
2231 comprehensive monitoring capabilities, as noted in Section 4, Architecture. A significant amount of data  
2232 relating to employees, their devices, and their activities is collected and analyzed by multiple parties.

### 2233 **F.2.1 Potential Problem for Individuals**

2234 Employees may not be aware that their interactions with the system are being monitored and may not  
2235 want this monitoring to occur. Collection and analysis of information might enable Orvilia or other  
2236 parties to craft a narrative about an employee based on their interactions with the system, which could  
2237 lead to a power imbalance between Orvilia and the employee and loss of trust in the employer if the  
2238 employee discovers unanticipated monitoring.

### 2239 **F.2.2 Mitigations**

2240 **Limit staff with ability to review data about employees and their devices.**

2241 This may be achieved using role-based access controls and by developing organizational policies to limit  
2242 how employee data can be used by staff with access to that data. Access can be limited to any  
2243 dashboard in the system containing data about employees and their devices but is most sensitive within  
2244 the mobile management dashboard, which is the hub for data about employees, their devices, and  
2245 threats. Minimizing access to sensitive information can enhance *disassociability* for employees using the  
2246 system.

2247 **Limit or disable collection of specific data elements.**

2248 Conduct a system-specific privacy risk assessment to determine what elements can be limited. Consider  
2249 the configuration options for intrusive device features, such as location services, application inventory  
2250 collection, and location-based wake-ups. When collecting application inventory data, ensure that  
2251 information is gathered only from applications installed from the organization's corporate application  
2252 store. While these administrative configurations may help provide for disassociability in the system,  
2253 there are also some opportunities for employees to limit the data collected.

2254 Organizations may allow their employees to manage certain aspects and configurations of their device.  
2255 For example, employees may be able to disable location services in their device OS to prevent collection  
2256 of location data. Each of these controls contributes to reducing the number of attributes collected  
2257 regarding employees and their mobile devices. This reduction of collected data limits administrators'  
2258 ability to associate information with specific individuals.

2259 **Dispose of PII.**

2260 Disposal of PII after an appropriate retention period can help reduce the risk of entities building profiles  
2261 of individuals. Disposal can also help bring the system's data processing into alignment with employees'  
2262 expectations and reduce the security risk associated with storing a large volume of PII. Disposal may be  
2263 particularly important for certain parties in the system that collect a larger volume of data or more  
2264 sensitive data. Disposal may be achieved using a combination of policy and technical controls. Parties in  
2265 the system may identify what happens to data, when, and how frequently.

### 2266 **F.3 Data Action 3: Data Sharing Across Parties**

2267 The infrastructure involves several parties that serve different purposes supporting Orvilia's security  
2268 objectives. As a result, there is a significant flow of data about individuals and their devices occurring  
2269 across various parties. This includes sharing device and application data publicly and with third-party  
2270 analytics services, and includes sharing device status and usage with third-party analytics.

#### 2271 **F.3.1 Potential Problems for Individuals**

2272 Data transmission about individuals and their devices among a variety of different parties could be  
2273 confusing for employees who might not know who has access to different information about them. If  
2274 administrators and co-workers know what colleague is conducting activity on his or her device that  
2275 triggers security alerts, it could cause employee embarrassment or emotional distress. This information  
2276 being revealed and associated with specific employees could also lead to stigmatization and even impact  
2277 Orvilia upper management in their decision-making regarding the employee. Further, clear text  
2278 transmissions could leave information vulnerable to attackers and the unanticipated release of  
2279 employee information.

2280 **F.3.2 Mitigations**

2281 **Use de-identification techniques.**

2282 De-identification of data helps decrease the chances that a third party is aggregating information  
2283 pertaining to one specific individual. While de-identification can help reduce privacy risk, there are  
2284 residual risks of reidentification. De-identification techniques may be applied to aggregated data before  
2285 sharing it with third-party analytics and publicly.

2286 **Use encryption.**

2287 Encryption decreases the chances of insecurity of information transmitted between parties.  
2288 Organizations should keep this in mind when considering how their enterprise data is transmitted and  
2289 stored. Mobile security systems share mobile device and application data with one another to optimize  
2290 efficiency and leverage data to perform security functions. This data may include application inventory  
2291 and employee name, email address, and phone number. Some systems offer multiple encryption  
2292 options that allow an organization to choose the encryption level necessary for the type of data that is  
2293 stored or transmitted.

2294 **Limit or disable access to data.**

2295 Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using  
2296 access controls to limit staff access to compliance information, especially when associated with  
2297 individuals, is important in preventing association of specific events with particular employees, which  
2298 could cause embarrassment. Some mobile security systems offer options for restricting the amount of  
2299 employee information that an administrator can access. These options may include hiding an  
2300 employee's username and email address from the administrator console. Mobile application  
2301 information may also include employee information. Organizations should consider how their mobile  
2302 security systems hide application names, application binary analysis details, network names service set  
2303 identifier, and network analysis details from administrators.

2304 **Limit or disable collection of specific data elements.**

2305 Conduct a system-specific privacy risk assessment to determine what elements can be limited.  
2306 Identifying the employee information collected and determining what data elements are stored assist in  
2307 assessing the privacy risk of mobile security systems. Organizations should consider the mobile security  
2308 system's ability to limit or reduce collection and storage of employee information, such as username,  
2309 email address, Global Positioning System location, and application data.

2310 **Use contracts to limit third-party data processing.**

2311 Establish contractual policies to limit data processing by third parties to only the processing that  
2312 facilitates delivery of security services, and no data processing beyond those explicit purposes.

## 2313 F.4 Mitigations Applicable Across Various Data Actions

2314 Several mitigations provide benefits to employees pertaining to all three data actions identified in the  
2315 privacy risk assessment. These training and support mitigations can help Orvilia appropriately inform  
2316 employees about the system and its data processing.

2317 **Mitigations:**

2318 **Provide training to employees about the system, parties involved, data processing, and administrative  
2319 actions that can be taken.**

2320 Training sessions can also highlight any privacy-preserving techniques used, such as for disclosures to  
2321 third parties. Training should include confirmation from employees that they understand the actions  
2322 that can be taken on their devices and the consequences—whether this involves blocking access or  
2323 wiping data. Employees may also be informed of data retention periods and when their data will be  
2324 disposed of. This can be more effective than simply sharing a privacy notice, which research has shown  
2325 that individuals are unlikely to read.

2326 **Provide ongoing notifications or reminders about system activity.**

2327 This can be achieved using push notifications, similar to those pictured in screenshots in Appendix G,  
2328 Threat Event 6, to help directly link administrative actions on devices to relevant threats and help  
2329 employees understand why an action is being taken. Notifications of changes to policies can help  
2330 increase system predictability by setting employee expectations appropriately with the way the system  
2331 processes data and the resulting actions.

2332 **Provide a support point of contact.**

2333 By providing employees with a point of contact in the organization who can respond to inquiries and  
2334 concerns regarding the system, employees can gain a better understanding of the system's processing of  
2335 their data, which enhances predictability.

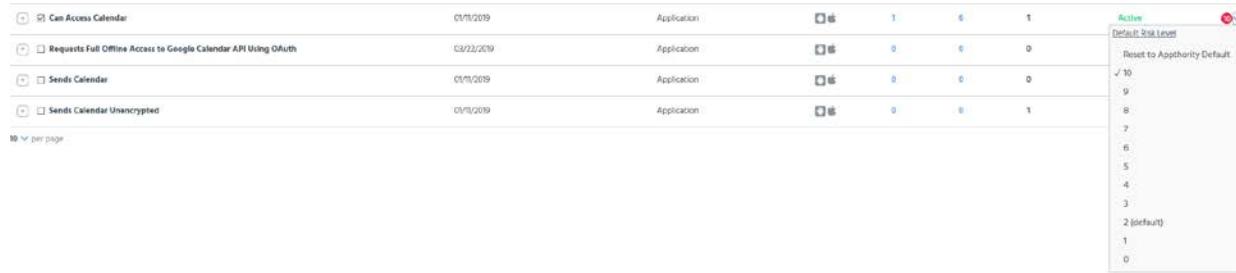
## 2336 **Appendix G Threat Event Test Information**

2337 Detailed information and screenshots for some of this practice guide's threat events and their testing  
 2338 results are provided below.

### 2339 **G.1 Threat Event 1—Unauthorized Access to Sensitive Information via a 2340 Malicious or Privacy-Intrusive Application**

2341 A part of Threat Event 1's testing conclusions is shown in the following screen capture, where the  
 2342 calendar access permission is being set to a risk score of 10. This allows MobileIron to automatically  
 2343 apply the mobile threat protection high-risk label to the device and quarantine the device until the  
 2344 privacy-intrusive application is removed.

2345 **Figure G-1 Setting a Custom Risk Level in Appthority**



The screenshot shows a table of permissions and a dropdown menu for setting a custom risk level. The table has columns for permission name, last modified date, type, and risk scores (0, 1, 6, 10). The dropdown menu is titled 'Active' and shows a list of risk levels from 0 to 10, with 10 selected. Other options include 'Default Risk Level', 'Reset to Appthority Default', and a red 'Cancel' button.

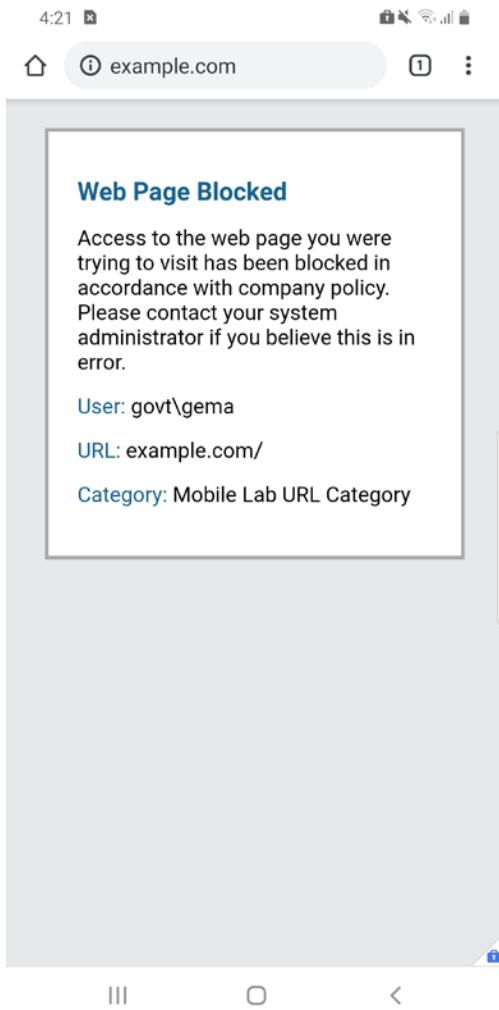
| Can Access Calendar   | 01/01/2019 | Application | 0 | 1 | 6 | 10 | Active                      |
|---|------------|-------------|---|---|---|----|-----------------------------|
| Requests Full Offline Access to Google Calendar API Using OAuth | 03/22/2019 | Application | 0 | 0 | 0 | 0  | Default Risk Level          |
| Sends Calendar  | 01/01/2019 | Application | 0 | 0 | 0 | 0  | Reset to Appthority Default |
| Sends Calendar Unencrypted                                      | 01/01/2019 | Application | 0 | 0 | 0 | 1  | 10                          |

10 per page

### 2346 **G.2 Threat Event 2—Theft of Credentials Through a Short Message Service (SMS) or Email Phishing Campaign**

2348 Threat Event 2's outcome is shown in the following screen capture, where PAN-DB is blocking a website  
 2349 manually added to the malicious uniform resource locator (URL) database.

2350 **Figure G-2 PAN-DB Blocked Website**

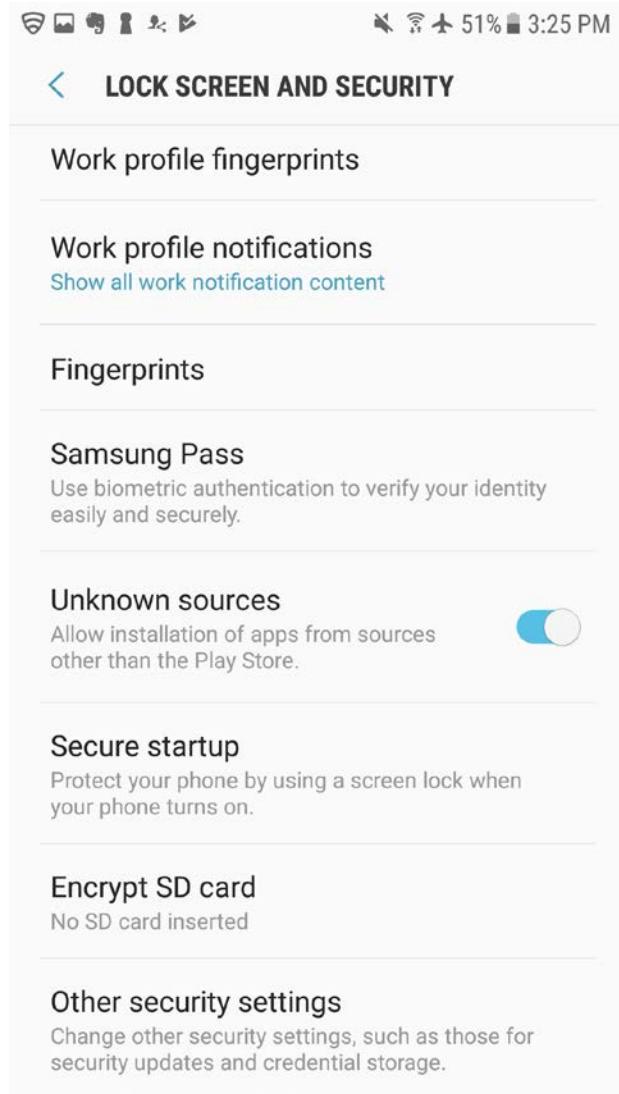
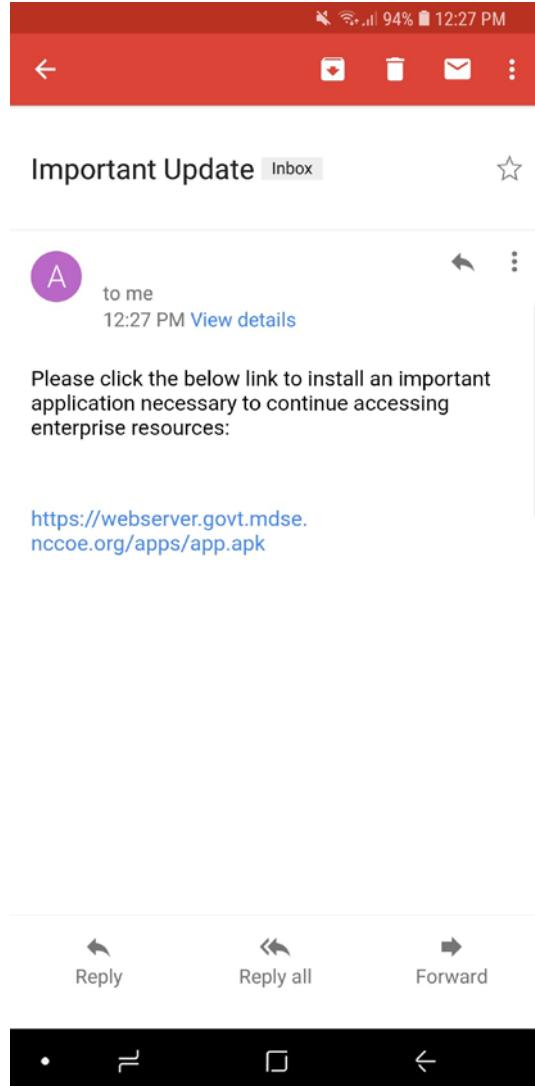


2351 **G.3 Threat Event 3—Malicious Applications Installed via URLs in SMS or Email Messages**

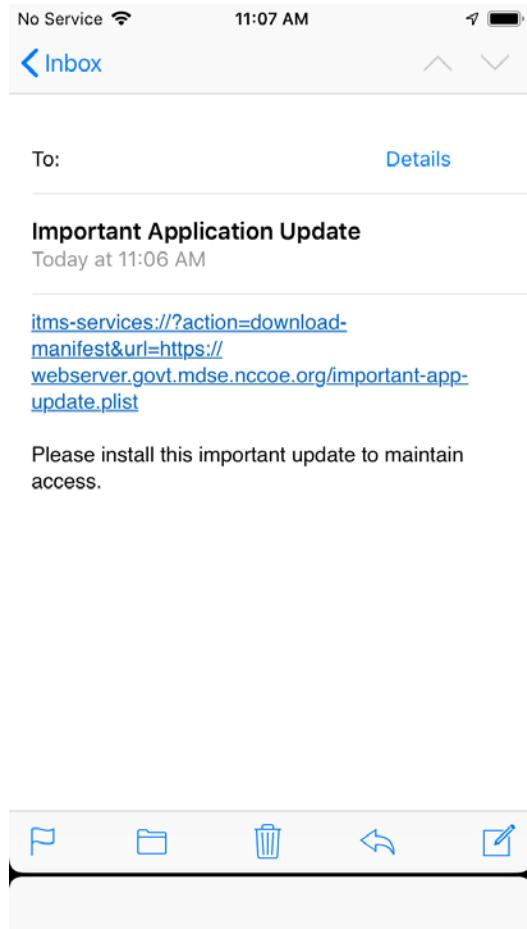
2352

2353 The following screenshots demonstrate enabling the Unknown Sources toggle and installing an application through a link in an email message.

2354

**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**

- 2357 After the application is installed, an untrusted developer notice appears as shown in Figure G-6 when  
 2358 the user attempts to launch the application.
- 2359 Figure G-7 shows Lookout's ability to detect application signing certificates that have been trusted on a  
 2360 device by the user to execute applications from sources other than Apple's App Store.

2361 **Figure G-7 Application Signing Certificates**

## Low Risk Configuration Issue

| ISSUE STATUS | RISK | ISSUE TYPE    | USER | DWELL TIME                 |
|--------------|------|---------------|------|----------------------------|
| Active       | Low  | Configuration | -    | Days H M S<br>123 21:23:12 |

DEVICE DETAILS  
iPhone X  
[View device >](#)

CLASSIFICATION  
Non-App Store Signer

FAMILY NAME  
iPhone Developer: MITRE (xxxxxxxxxx)

CLASSIFICATION DESCRIPTION  
This device has explicitly trusted a developer in a way that allows this developer to install any number of apps on this device without going through the standard Apple App Store or beta approval process. Apps installed this way may possibly be harmful. This device may also be testing an app under development. If you believe this developer does not pose a risk to your organization, you may allow it to be trusted.

Allow non-App Store signer

## Configuration Anomalies

| ANOMALY              | DESCRIPTION |
|----------------------|-------------|
| Non-App Store Signer | -           |

- 2362 The following screenshots depict an attempt to install and run the unauthorized demo application on an  
 2363 iOS device with the `allowEnterpriseAppTrust` policy restriction set to false by an Enterprise Mobility  
 2364 Management (EMM) system. The user is not able to trust the developer when the policy restriction is  
 2365 active, and hence the application will not run.

2366 Figure G-8 Restriction Setting Modification Screen

The screenshot shows a web-based administrative interface for configuration management. At the top, there's a navigation bar with links for Dashboard, Devices & Users, Admin, Apps, Policies & Configs (which is currently selected), Services, Settings, and Logs. Below the navigation is a sub-navigation bar with tabs for Configurations, Policies, ActiveSync Policies, Compliance Policies, and Compliance Actions. A search bar and filter options are also present. The main content area is titled 'Modify Restrictions Setting'. On the left, there's a sidebar with a list of configurations, one of which is 'Allow trusting new enterprise app authors (iOS 9.0 and later)'. This item is highlighted with a red box. To the right of the sidebar, there are several checkboxes with descriptions: 'Allow installing configuration profiles (supervised devices only)' (checked), 'Allow modifying account settings (supervised devices only)' (checked), 'Allow modifying Bluetooth settings (iOS 10.0 and later supervised devices only)' (checked), and 'Allow modifying cellular data app settings (supervised devices only)' (unchecked). At the bottom right of the main content area are 'Save' and 'Cancel' buttons.

2367 Figure G-9 Unable to Trust Developer

The screenshot shows an iPhone's Control Center with the time at 3:25 and battery level. Below it is a 'Device Management' screen. The text on the screen says: 'Apps from developer "iPhone Developer": are not trusted on this iPhone and will not run until the developer is trusted.' It also states 'Some restrictions are enforced by "NCCOE"' and lists 'APPS FROM DEVELOPER "IPHONE DEVELOPER":'. There is a single entry for 'Demo App' with a verified status.

2368 Android Device Testing

2369 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  
 2370 when the Unknown Sources setting has been enabled and can communicate this information to  
 2371 MobileIron to enable automated response actions, such as blocking device access to enterprise  
 2372 resources until the situation is resolved. However, even if Unknown Sources is disabled, it is possible  
 2373 that the setting was previously enabled and that unauthorized applications were installed at that time.

2375 Figure G-10 shows Lookout's ability to detect Android devices with Unknown Sources enabled.

2376 **Figure G-10 Unknown Sources Detection**

The screenshot shows the Lookout mobile device management interface. On the left is a dark sidebar with navigation links: Dashboard, Issues, Devices (selected), Apps, Policies, System, and Support. The main area displays information for a device named 'SM-G930V'. At the top right are 'DEACTIVATE' and 'DELETE' buttons. Below the device name are sections for 'STATUS' (Secured), 'USER' (empty field), 'DEVICE TYPE' (SM-G930V), 'MDM' (MobileIron), and 'CONNECTION' (Connected, 2 minutes ago). A large 'Issues' section below shows a table with columns for STATUS, ISSUE, and DETECTED. The table contains one row: 'Unknown Sources' is listed under 'ISSUE' and 'Allowed' under 'DETECTED'. Other rows in the table include 'Lock Screen' (Enabled), 'Developer Mode' (Enabled), and 'USB Debugging' (Enabled). A 'Configuration' section at the bottom lists these three settings.

| STATUS  | ISSUE           | DETECTED |
|---------|-----------------|----------|
| Enabled | Unknown Sources | Allowed  |
| Enabled |                 |          |
| Enabled |                 |          |

#### 2377 **G.4 Threat Event 4—Confidentiality and Integrity Loss due to Exploitation 2378 of Known Vulnerability in the Operating System or Firmware**

2379 Figure G-11 demonstrates Lookout's ability to identify known vulnerabilities to which unpatched iOS and  
2380 Android devices are susceptible. Figure G-12 shows the patch level of the device.

2381 Figure G-11 Vulnerability Identification

The screenshot shows the Lookout mobile security platform interface for iOS 11.2.1.0. The main header displays the device model and its release date (Dec 13, 2017). On the left, a sidebar menu includes Dashboard, Issues, Devices, Apps, Policies, System, and Support. A NIST - National Institute of Standards and Technology logo is visible at the bottom of the sidebar.

**Vulnerability summary**

| VULNERABILITY                     | CVE | SEVERITY |
|-----------------------------------|-----|----------|
| Critical severity vulnerabilities | 4   |          |
| High severity vulnerabilities     | 43  |          |
| Medium severity vulnerabilities   | 12  |          |
| Low severity vulnerabilities      | 1   |          |
| Unknown severity vulnerabilities  | 45  |          |

**Vulnerability details**

| CVE ID        | DESCRIPTION  | CVE SEVERITY |
|---------------|--|--------------|
| CVE-2018-4115 | A configuration profile may incorrectly remain in effect after removal in System Preferences | Critical     |
| CVE-2018-4110 | Cookies may unexpectedly persist in web app in Web App                                       | Critical     |
| CVE-2018-4148 | A remote attacker may be able to execute arbitrary code in Telephony                         | Critical     |
| CVE-2018-4124 | Processing a maliciously crafted string may lead to heap corruption in CoreText              | Critical     |

2382 Figure G-12 Patch Level Display

The screenshot shows the Lookout mobile security platform interface for the Android Security Patch Level 2017-08-01. The main header displays the patch level and its release date (Aug 7, 2017). The sidebar menu is identical to Figure G-11, including the NIST logo.

**Vulnerability summary**

| VULNERABILITY                     | CVE | SEVERITY |
|-----------------------------------|-----|----------|
| Critical severity vulnerabilities | 261 |          |
| High severity vulnerabilities     | 286 |          |
| Medium severity vulnerabilities   | 68  |          |
| Low severity vulnerabilities      | 1   |          |
| Unknown severity vulnerabilities  | 70  |          |

**Vulnerability details**

| CVE ID         | DESCRIPTION                              | CVE SEVERITY |
|----------------|--|--------------|
| CVE-2017-13208 | Remote code execution in System          | Critical     |
| CVE-2017-13179 | Remote code execution in Media framework | Critical     |
| CVE-2017-13177 | Remote code execution in Media framework | Critical     |
| CVE-2017-13178 | Remote code execution in Media framework | Critical     |
| CVE-2017-13160 | Remote code execution in System          | Critical     |

2383    **G.5 Threat Event 5—Violation of Privacy via Misuse of Device Sensors**

2384    The following screenshot depicts a Kryptowire application analysis report and the reported permissions  
2385    that this application was requesting.

2386    **Figure G-13 Kryptowire Analysis Report**

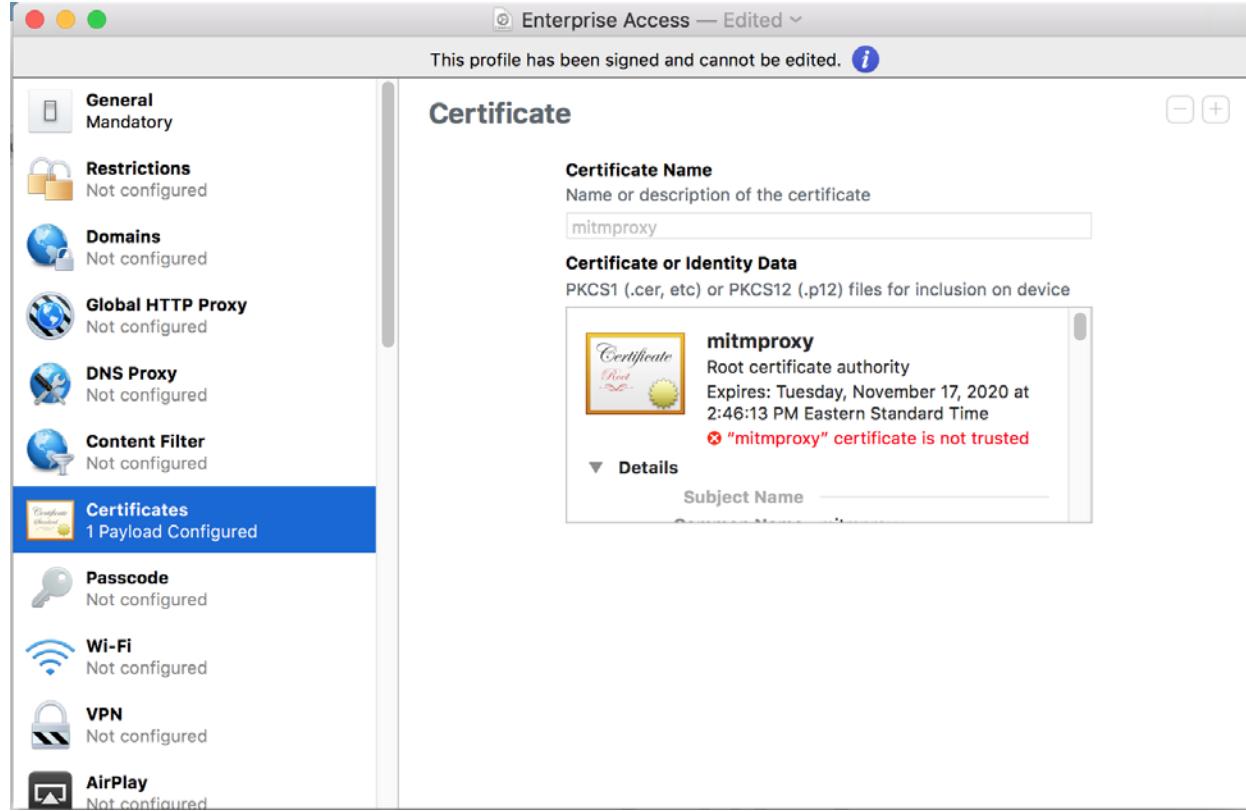
The figure shows a screenshot of the Kryptowire iOS Mobile Application Analysis report. At the top, it says "Automated Analysis Summary". Below that, there are three main sections: "Security", "Privacy & Information Access", and "Device Access".

- Security:**
  - ⚠️ No data at rest encryption
  - ⚠️ Does not use iOS provided encryption
  - ⚠️ No data in transit encryption
  - ✓ No hard coded credentials
  - ✓ No hard coded initialization vector (IV)
  - ✓ No external library loaded dynamically
  - ✓ No malware detected
- Privacy & Information Access:**
  - ⚠️ Gets information about the user
  - ⚠️ Integrates with an ad network
  - ⚠️ Accesses calendar
  - ⚠️ Has in app purchases
  - ✓ No cloud storage integration
  - ✓ No social network integration
  - ✓ Does not expose sensitive information
- Device Access:**
  - ⚠️ Can interactive with sending SMS/MMS messages
  - ⚠️ Accesses the Internet
  - ⚠️ Can access microphone
  - ⚠️ Accesses photos and/or videos
  - ⚠️ Accesses contacts/address book
  - ⚠️ Accesses location
  - ✓ Does not interact with email client
  - ✓ Does not access Bluetooth
  - ✓ Does not access camera

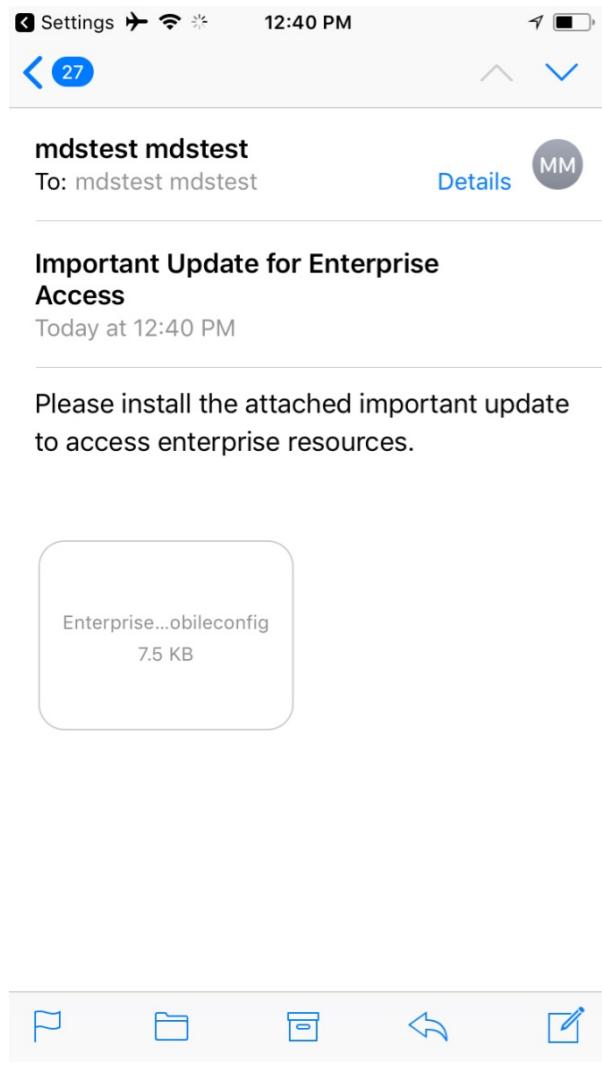
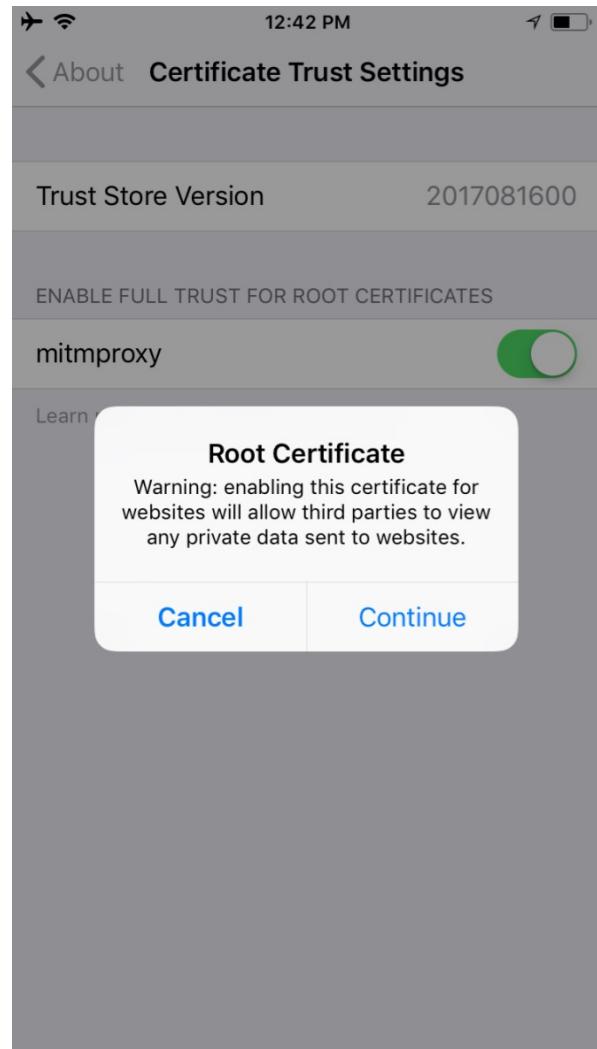
2387    **G.6 Threat Event 6—Compromise of the Integrity of the Device or Its  
2388    Network Communications via Installation of Malicious EMM/Mobile  
2389    Device Management, Network, Virtual Private Network (VPN) Profiles,  
2390    or Certificates**

2391    The configuration profile used for configuring and testing Threat Event 6 is shown in Figure G-14.

2392 Figure G-14 Configuration Profile Example

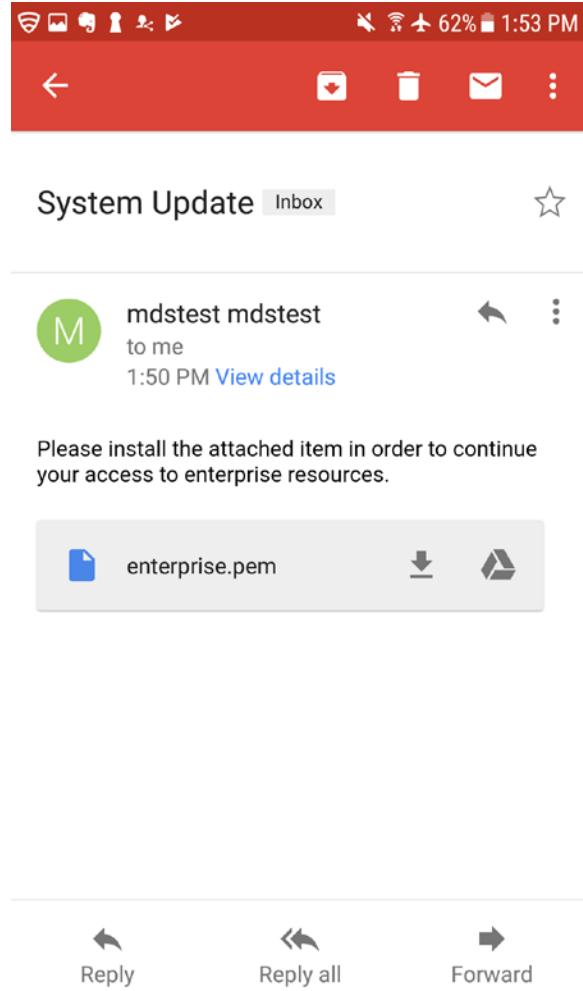


2393 Figure G-15 shows the email containing a malicious device configuration profile, and Figure G-16 shows  
2394 the warning displayed to the user when attempting to mark the malicious certificate as a trusted root.

**Figure G-15 Configuration Profile Phishing Email****Figure G-16 Root Certificate Authority Enablement Warning**

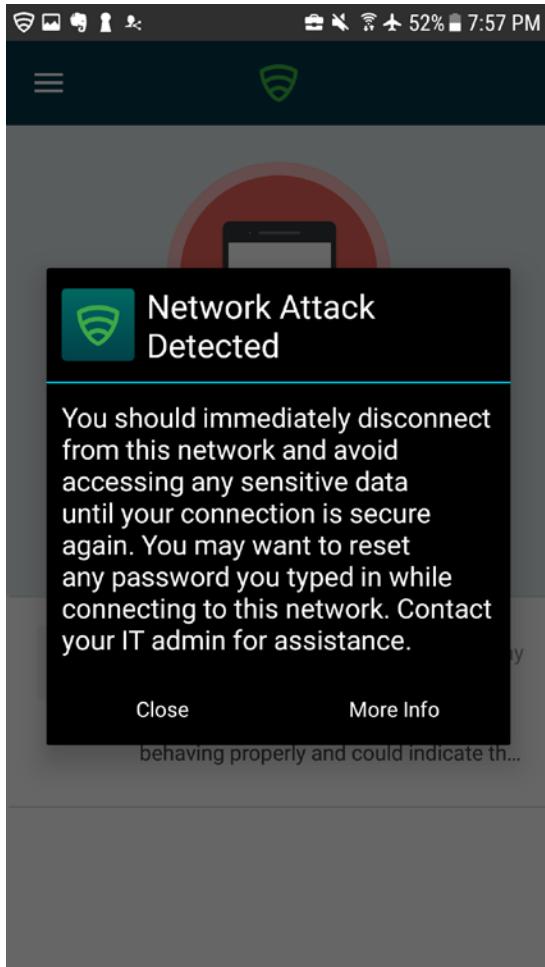
2395 **Figure G-17 Reversed Web Page**

- 2396 Browse to a hypertext transfer protocol secure (https) website from the mobile device and observe  
2397 whether the content has been reversed. Figure G-17 illustrates that the man-in-the-middle attack on a  
2398 Transport Layer Security-protected connection was successful.  
2399 The following screenshots demonstrate a man-in-the-middle attack on Android.

**Figure G-18 Certificate Phishing Email****Figure G-19 Reversed Web Page**

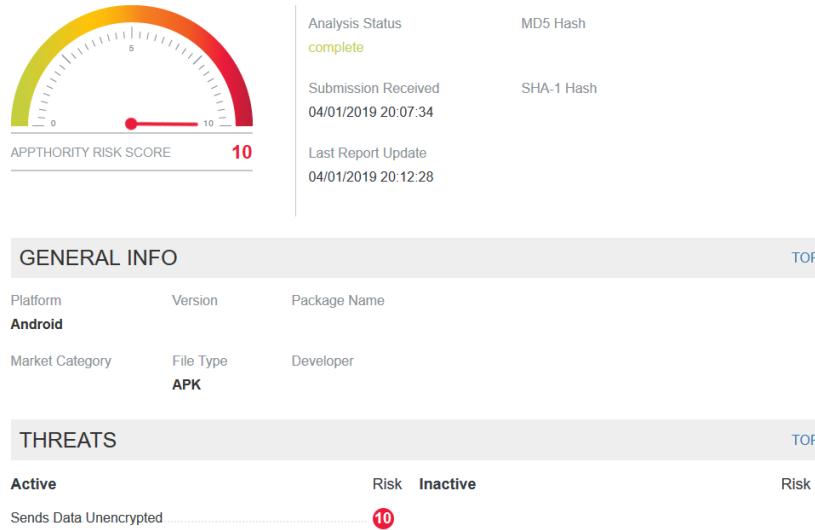
2400 Man-in-the-middle attack is detected by Lookout as shown in Figure G-20.

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.

2405 **Figure G-21 Unencrypted Data Transfer**

2406 **G.8 Threat Event 8—Compromise of Device Integrity via Observed,  
2407 Inferred, or Brute-Forced Device Unlock Code**

2408 MobileIron applies a policy to the devices to enforce a mandatory personal identification number and  
2409 device-wipe capability. Lookout reports devices that have the lock screen disabled.

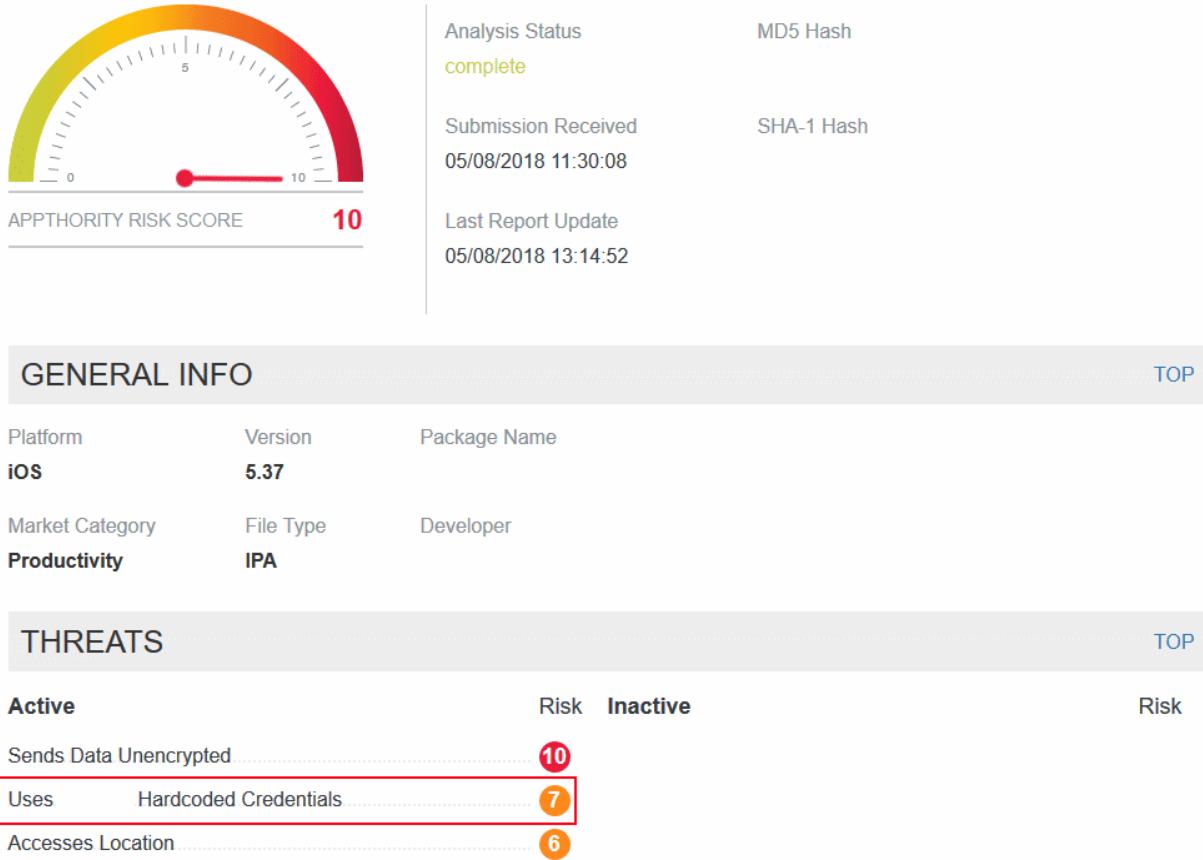
2410 Figure G-22 Lock Screen Disabled Detection Notice

The screenshot shows a web-based interface for the Lookout mobile device management application. The left sidebar has icons for Dashboard, Issues, Devices, Apps, and Policies. The main area is titled 'Configuration' and contains two sections: 'Lock Screen' and 'Device Encryption'. The 'Lock Screen' section is highlighted with a red border and shows 'Disabled'. The 'Device Encryption' section shows 'Disabled'. Below these are sections for 'Software', 'OS' (iOS), and 'OS Version' (11.2.1).

| Configuration     |          |
|-------------------|----------|
| Lock Screen       | Disabled |
| Device Encryption | Disabled |
| Software          |          |
| OS                | iOS      |
| OS Version        | 11.2.1   |

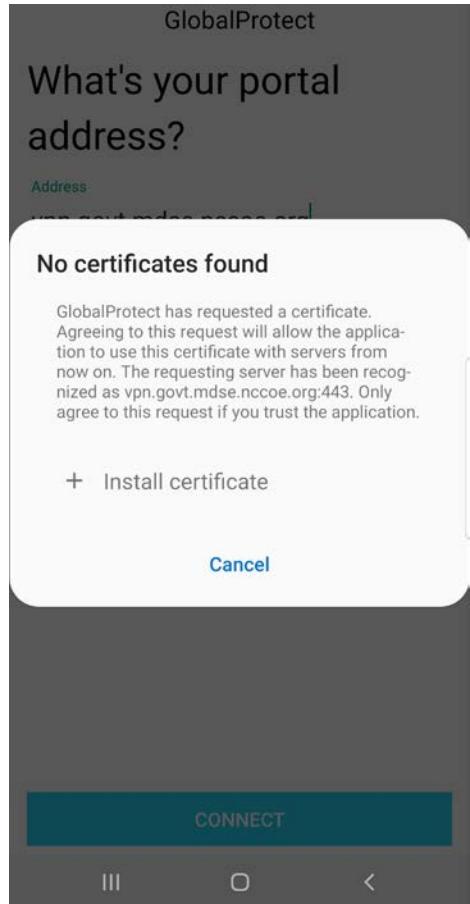
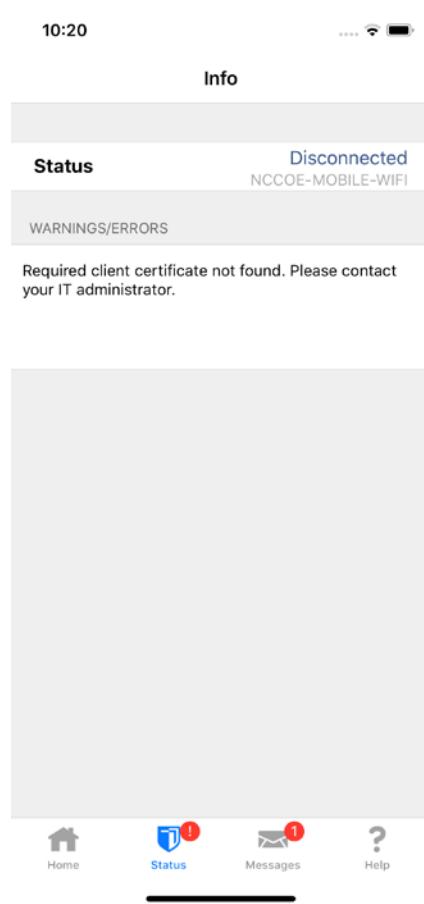
2411 **G.9 Threat Event 9—Unauthorized Access to Backend Services via  
2412       Authentication or Credential Storage Vulnerabilities in Internally  
2413       Developed Applications**

2414 As shown in Figure G-23, Appthority recognized that an application used hard-coded credentials. The  
2415 application's use of hard-coded credentials could introduce vulnerabilities if the hard-coded credentials  
2416 were used for access to enterprise resources by unauthorized entities or for unauthorized actions.

2417 **Figure G-23 Hard-Coded Credentials**

2418 **G.10 Threat Event 10—Unauthorized Access of Enterprise Resources from**  
 2419 **an Unmanaged and Potentially Compromised Device**

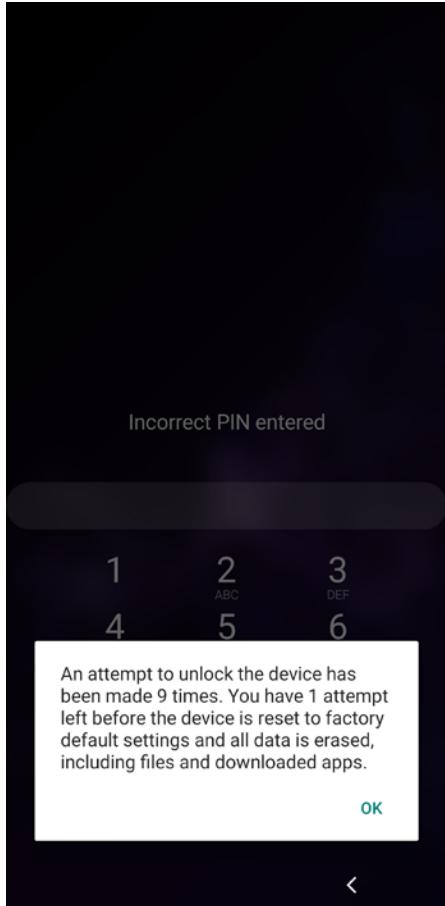
2420 The following two screenshots depict the inability to connect to the GlobalProtect VPN without the  
 2421 proper client certificates, obtainable only through enrolling the device in MobileIron.

**Figure G-24 No Certificates Found on Android****Figure G-25 No Certificates Found on iOS**

2422    **G.11 Threat Event 11—Loss of Organizational Data due to a Lost or Stolen  
2423    Device**

2424    This screenshot depicts the final warning before Android factory-resets the device. In the event the  
2425    device was stolen, all corporate data would be removed from the device after one more failed unlock  
2426    attempt, thwarting the malicious actor's goal.

2427 **Figure G-26 Android Device Wipe Warning**



2428 **G.12 Threat Event 12—Loss of Confidentiality of Organizational Data due  
2429 to Its Unauthorized Storage in Non-Organizationally Managed Services**

2430 The following screenshot shows one of the data loss prevention configuration options in MobileIron for  
2431 iOS.

2432 **Figure G-27 Disallowing Screenshots and Screen Recording**

2433  Allow screenshots and screen recording (iOS 9.0 and later)

## 2434    **Appendix H    Example Security Control Map**

2435    Table H-1 lists the technologies used in this project and provides a mapping among the generic  
2436    application term, the specific product used, the security control(s) the product provides, and a mapping  
2437    to the relevant National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181,  
2438    *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Work Roles*.  
2439    From left to right, the columns in the table describe:

- 2440        ▪ **Specific product used:** vendor product used by the example solution
- 2441        ▪ **How the component functions in the build:** capability the component provides in the example  
2442              solution. This is mapped to the general mobile technology component term.
- 2443        ▪ **Applicable Cybersecurity Framework Subcategories:** applicable Cybersecurity Framework  
2444              Subcategory(s) that the component is providing in the example solution
- 2445        ▪ **Applicable NIST controls:** the NIST SP 800-53 Revision 4 controls that the component provided  
2446              in the example solution
- 2447        ▪ **ISO/IEC 27001:2013:** International Organization for Standardization (ISO), International  
2448              Electrotechnical Commission (IEC) 27001:2013 mapping that the component provides in the  
2449              example solution
- 2450        ▪ **CIS 6:** Center for Internet Security (CIS) version 6 controls mapping that the component provides  
2451              in the example solution
- 2452        ▪ **NIST SP 800-181, NICE Framework Work Roles:** NICE Framework work role(s) that could be used  
2453              to manage this component's use in the example solution. This mapping provides information on  
2454              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  |
|------------------------------|--|--|--|---|---|--|
| <b>Mobile Threat Defense</b> |  |  |  |   |   |  |
| 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<br>Risk Assessment RA-3, RA-5<br>System and Services Acquisition SA-5, SA-11<br>System and Information Integrity SI-2, SI-4, SI-5 | A.12.6.1 Control of Technical vulnerabilities<br>A.18.2.3 Technical Compliance Review | CSC 4 Continuous Vulnerability Assessment and Remediation | SP-RSK-002 Security Control Assessor<br><br>SP-ARC-002 Security Architect<br><br>OM-ANA-001 Systems Security Analyst<br><br>PR-VAM-001 Vulnerability Assessment Analyst<br><br>PR-CDA-001 Cyber Defense Analyst<br><br>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<br>System and Information Integrity SI-5<br>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<br><br>PR-CDA-001 Cyber Defense Analyst<br><br>OV-SPP-001 Cyber Workforce Developer and Manager<br><br>OV-TEA-001 Cyber Instructional Curriculum Developer<br><br>AN-TWA-001 Threat/Warning Analyst<br><br>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<br>Information Systems Security Manager   |
|                       |  | DE.CM-4—<br>Malicious code is detected.                      | System and Information Integrity SI-3, SI-8                       | A.12.2.1<br>Controls Against Malware   | CSC 4<br>Continuous Vulnerability Assessment and Remediation<br>CSC 7 Email and Web Browser Protections<br>CSC 8 Malware Defenses<br>CSC 12 Boundary Defense | PR-VAM-001<br>Vulnerability Assessment Analyst<br><br>PR-CIR-001<br>Cyber Defense Incident Responder<br><br>PR-CDA-001<br>Cyber Defense Analyst<br><br>OM-NET-001<br>Network Operations Specialist |
|                       |  | DE.CM-5—<br>Unauthorized mobile code is detected.            | Mobile Code SC-18, SC-44<br>System and Information Integrity SI-4 | A.12.5.1<br>Installation of Software on Operational Systems<br>A.12.6.2<br>Restrictions on | CSC 7 Email and Web Browser Protections<br>CSC 8 Malware Defenses  | PR-CDA-001<br>Cyber Defense Analyst<br><br>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<br>Risk Assessment RA-3, RA-5<br>System and Services Acquisition SA-5, SA-11<br>System and Information Integrity SI-2, SI-4, SI-5 | A.12.6.1 Control of Technical vulnerabilities<br>A.18.2.3 Technical Compliance Review | CSC 4 Continuous Vulnerability Assessment and Remediation | SP-RSK-002 Security Control Assessor<br><br>SP-ARC-002 Security Architect<br><br>OM-ANA-001 Systems Security Analyst<br><br>PR-VAM-001 Vulnerability Assessment Analyst<br><br>PR-CDA-001 Cyber Defense Analyst<br><br>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<br>OM-ANA-001 Systems Security Analyst<br>OV-SPP-001 Cyber Workforce Developer and Manager<br>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<br>Threat/Warning Analyst<br>PR-VAM-001<br>Vulnerability Assessment Analyst<br>PR-CDA-001<br>Cyber Defense Analyst<br>OV-MGT-001<br>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<br>CSC 7 Email and Web Browser Protections<br>CSC 8 Malware Defenses<br>CSC 12 Boundary Defense |       | PR-CIR-001<br>Cyber Defense Incident Responder<br>PR-CDA-001<br>Cyber Defense Analyst<br>PR-VAM-001<br>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<br>Network Operations Specialist  |
|  |  | DE.CM-5—Unauthorized mobile code is detected.   | Mobile Code SC-18, SC-44<br>System and Information Integrity SI-4       | A.12.5.1 Installation of Software on Operational Systems<br>A.12.6.2 Restrictions on Software Installation                                  | CSC 7 Email and Web Browser Protections<br>CSC 8 Malware Defenses   | PR-CDA-001<br>Cyber Defense Analyst<br><br>OM-NET-001<br>Network Operations Specialist   |
| Lookout Cloud Service/<br>Lookout Agent Version 5.10.0.142 (iOS),<br>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<br>System and Communications Protection SC-7 | A.13.1.1 Network Controls<br>A.13.1.3 Segregation in Networks<br>A.13.2.1 Information Transfer Policies and Procedures<br>A.14.1.2 Securing | CSC 9 Imitation and Control of Network Ports, Protocols, and Services<br>CSC 14 Controlled Access Based on the Need to Know<br>CSC 15 Wireless Access Control | OM-ADM-001<br>System Administrator<br><br>OV-SPP-002<br>Cyber Policy and Strategy Planner<br><br>PR-CDA-001<br>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<br>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<br>Contingency Planning Policy and Procedures CP-8<br>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<br>A.13.1.3 Segregation in Networks<br>A.14.1.3 Protecting Application Services Transactions | CSC 8 Malware Defenses<br>CSC 12 Boundary Defense<br>CSC 15 Wireless Access Control              |                                      | OM-ADM-001 System Administrator<br><br>OV-SPP-002 Cyber Policy and Strategy Planner<br><br>OV-MGT-002 Communications Security (COMSEC) Manager<br><br>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<br>Cyber Defense Analyst<br><br>SP-ARC-002<br>Security Architect<br><br>OM-NET-001<br>Network Operations Specialist |
|                                       |  |  |   |                             |  | PR-CDA-001<br>Cyber Defense Analyst<br><br>OM-NET-001<br>Network Operations Specialist   |
| <b>Enterprise Mobility Management</b> |  |  |   |                             |  |  |
| 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<br>Technical Support Specialist<br><br>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  |
|-----------------------|--|--|---|--|--|--|
|                       |  | PR.AC-1—Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. | Information System Inventory<br>PM-5<br><br>Access Control<br>AC-1, AC-2<br>Identification and Authentication<br>IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 | A.8.1.2 Ownership of Assets<br><br>A.9.2.1 User Registration and De-Registration<br>A.9.2.2 User Access Provisioning<br>A.9.2.3 Management of Privileged Access Rights<br>A.9.2.4 Management of Secret Authentication Information of Users<br>A.9.2.6 Removal or Adjustment of Access Rights<br>A.9.3.1 Use of Secret Authentication Information | CSC 1 Inventory of Authorized and Unauthorized Devices<br>CSC 5 Controlled Use of Administrative Privileges<br>CSC 15 Wireless Access Control<br>CSC 16 Account Monitoring and Control | System Administrator<br><br>OV-SPP-002 Cyber Policy and Strategy Planner<br><br>OM-ADM-001 System Administrator<br><br>OV-MGT-002 Communications Security (COMSEC) Manager<br><br>OM-STS-001 Technical Support Specialist<br><br>OM-ANA-001 Systems Security Analyst<br><br>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<br>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<br>Identification and Authentication IA-1, IA-2, IA-4, IA-5, IA-8<br>Physical and Environmental Protection PE-2 | A.7.1.1 Screening<br>A.9.2.1 User Registration and De-Registration | CSC 16 Account Monitoring and Control                                  | OV-SPP-002<br>Cyber Policy and Strategy Planner<br><br>OV-MGT-002<br>Communications Security (COMSEC) Manager<br><br>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<br>System and Services Acquisition SA-10 | A.12.1.2 Change Management<br>A.12.5.1 Installation of Software on Operational Systems<br>A.12.6.2 Restrictions on Software Installation<br>A.14.2.2 System Change Control Procedures<br>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<br>CSC 9 Limitation and Control of Network Ports, Protocols, and Services<br>CSC 11 Secure Configurations for Network Devices Such as Firewalls, Routers, and Switches | SP-ARC-002 Security Architect<br>OV-SPP-002 Cyber Policy and Strategy Planner<br>SP-SYS-001 Information Systems Security Developer<br>OM-ADM-001 System Administrator<br>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<br>A.14.2.4 Restrictions on Changes to Software Packages |                    |       | OM-NET-001<br>Network Operations Specialist<br><br>OV-MGT-001<br>Information Systems Security Manager<br><br>OM-STS-001<br>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<br>System and Information Integrity SI-7 | A.12.2.1 Controls Against Malware<br>A.12.5.1 Installation of Software on Operational Systems<br>A.14.1.2 Securing Application Services on Public Networks<br>A.14.1.3 Protecting Application Services Transactions<br>A.14.2.4 Restrictions on Changes to Software Packages | CSC 2 Inventory of Authorized and Unauthorized Software<br>CSC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers | OV-SPP-002<br>Cyber Policy and Strategy Planner<br><br>SP-ARC-0001<br>Enterprise Architect<br><br>OV-MGT-001<br>Information Systems Security Manager<br><br>OM-ADM-001<br>System Administrator<br><br>OM-STS-001<br>Technical Support Specialist |
| <b>Trusted Execution Environment</b>                          |  |   |  |  |  |  |

| 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<br>System and Communications Protection SC-12, SC-28 | A.8.2.3<br>Handling of Assets | CSC 13 Data Protection<br>CSC 14 Controlled Access Based on the Need to Know | OV-SPP-002<br>Cyber Policy and Strategy Planner<br><br>PR-INF-001<br>Cyber Defense Infrastructure Support Specialist<br><br>OV-LGA-002<br>Privacy Officer/Privacy Compliance Manager<br><br>OV-MGT-002<br>COMSEC Manager<br><br>OM-NET-001<br>Network Operations Specialist<br><br>OM-ANA-001<br>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<br>System and Information Integrity SI-7 | A.12.2.1 Controls Against Malware<br>A.12.5.1 Installation of Software on Operational Systems<br>A.14.1.2 Securing Application Services on Public Networks<br>A.14.1.3 Protecting Application Services Transactions<br>A.14.2.4 Restrictions on Changes to Software Packages | CSC 2 Inventory of Authorized and Unauthorized Software<br>CSC 3 Secure Configurations for Hardware and Software on Mobile | OV-SPP-002<br>Cyber Policy and Strategy Planner<br><br>PR-CDA-001<br>Cyber Defense Analyst<br><br>SP-ARC-0001<br>Enterprise Architect<br><br>OV-MGT-001<br>Information Systems Security Manager<br><br>OM-STS-001<br>Technical Support Specialist<br><br>OM-ADM-001<br>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<br>System and Information Integrity SI-7 | A.11.2.4<br>Equipment Maintenance    | Not applicable  | OM-ADM-001<br>System Administrator<br><br>SP-ARC-0001<br>Enterprise Architect  |
|                       |  | DE.CM-4—Malicious code is detected.  | System and Information Integrity SI-3, SI-8                                       | A.12.2.1<br>Controls Against Malware | CSC 5 Controlled Use of Administrative Privileges<br>CSC 7 Email and Web Browser Protections<br>CSC 14 Controlled Access Based on the Need to Know<br>CSC 16 Account Monitoring and Control | PR-CDA-001<br>Cyber Defense Analyst<br><br>PR-INF-001<br>Cyber Defense Infrastructure Support Specialist<br><br>PR-VAM-001<br>Vulnerability Assessment Analyst<br><br>OM-NET-001<br>Network Operations Specialist<br><br>PR-CDA-001<br>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  |
|---------------------------------|--|--|--|---|-------------------------|--|
| <b>Virtual Private Network</b>  |  |  |  |   |                         |  |
| 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<br>System and Communications Protection SC-15 | A.6.2.1 Mobile Device Policy<br>A.6.2.2 Teleworking<br>A.11.2.6 Security of Equipment and Assets Off-Premises<br>A.13.1.1 Network Controls<br>A.13.2.1 Information Transfer Policies and Procedures | CSC 12 Boundary Defense | OV-SPP-002<br>Cyber Policy and Strategy Planner<br><br>OV-MGT-002<br>Communications Security (COMSEC) Manager<br><br>OM-NET-001<br>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<br>AC-4, AC-10<br>System and Communications Protection SC-7 | A.13.1.1 Network Controls<br>A.13.1.3 Segregation in Networks<br>A.13.2.1 Information Transfer Policies and Procedures<br>A.14.1.2 Securing Application Services on Public Networks<br>A.14.1.3 Protecting Application Services Transactions | CSC 9 Limitation and Control of Network Ports, Protocols, and Services<br>CSC 14 Controlled Access Based on the Need to Know<br>CSC 15 Wireless Access Control<br>CSC 18 Application Software Security | PR-CDA-001<br>Cyber Defense Analyst<br><br>OM-ADM-001<br>System Administrator<br><br>OM-NET-001<br>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<br>Identification and Authentication IA-1, IA-2, IA-4, IA-5, IA-8<br>Physical and Environmental Protection PE-2, PS-3 | A.7.1.1 Screening<br>A.9.2.1 User Registration and De-Registration  | CSC 16 Account Monitoring and Control  | OV-SPP-002 Cyber Policy and Strategy Planner<br><br>OV-MGT-002 Communications Security (COMSEC) Manager<br><br>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<br>A.13.1.1 Network Controls<br>A.13.2.1 Information Transfer Policies and Procedures<br>A.13.2.3 Electronic Messaging | CSC 13 Data Protection<br>CSC 14 Controlled Access Based on the Need to Know | OV-SPP-002 Cyber Policy and Strategy Planner<br><br>OV-MGT-002 Communications Security (COMSEC) Manager<br><br>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<br>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<br>Contingency Planning CP-8<br>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<br>A.13.2.1 Information Transfer Policies and Procedures<br>A.14.1.3 Protecting Application Services Transactions | CSC 8 Malware Defenses<br>CSC 12 Boundary Defense<br>CSC 15 Wireless Access Control                                |       | PR-INF-001 Cyber Defense Infrastructure Support Specialist<br>OV-SPP-002 Cyber Policy and Strategy Planner<br>PR-CDA-001 Cyber Defense Analyst<br>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>



## 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](mailto: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](mailto:nccoe@nist.gov)

## 1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 17 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 27 **ABSTRACT**

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

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

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

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

## 40 **KEYWORDS**

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

## 43 **ACKNOWLEDGMENTS**

44 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 Gogoiel    | 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 |

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

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

## 49 **Contents**

|    |   |          |
|----|---|----------|
| 50 | <b>1 Introduction .....</b>   | <b>1</b> |
| 51 | 1.1 Practice Guide Structure .....  | 1        |
| 52 | 1.2 Build Overview .....  | 2        |
| 53 | 1.3 Typographic Conventions.....  | 3        |
| 54 | 1.4 Logical Architecture Summary .....                                    | 3        |
| 55 | <b>2 Product Installation Guides.....</b>                                 | <b>4</b> |
| 56 | 2.1 Appthority Mobile Threat Detection.....                               | 4        |
| 57 | 2.2 Kryptowire EMM+S .....  | 5        |
| 58 | 2.3 Lookout Mobile Endpoint Security.....                                 | 5        |
| 59 | 2.4 MobileIron Core .....   | 5        |
| 60 | 2.4.1 Installation of MobileIron Core and Stand-Alone Sentry .....        | 5        |
| 61 | 2.4.2 General MobileIron Core Setup.....                                  | 5        |
| 62 | 2.4.3 Upgrade MobileIron Core.....  | 6        |
| 63 | 2.4.4 Integration with Microsoft Active Directory .....                   | 12       |
| 64 | 2.4.5 Create a Mobile Users Label.....                                    | 18       |
| 65 | 2.5 Integration of Palo Alto Networks GlobalProtect with MobileIron ..... | 20       |
| 66 | 2.5.1 MobileIron Configuration .....                                      | 20       |
| 67 | 2.5.2 Basic Palo Alto Networks Configuration .....                        | 24       |
| 68 | 2.5.3 Palo Alto Networks Interfaces and Zones Configuration .....         | 30       |
| 69 | 2.5.4 Configure Router .....  | 35       |
| 70 | 2.5.5 Configure Tunnel Interface.....                                     | 38       |
| 71 | 2.5.6 Configure Applications and Security Policies .....                  | 39       |
| 72 | 2.5.7 Network Address Translation (NAT) .....                             | 48       |
| 73 | 2.5.8 Configure SSL VPN .....   | 51       |
| 74 | 2.5.9 Import Certificates.....  | 60       |
| 75 | 2.5.10 Configure Certificate Profile .....                                | 62       |
| 76 | 2.5.11 Configure SSL/TLS Service Profile .....                            | 63       |
| 77 | 2.5.12 URL Filtering Configuration .....                                  | 64       |

|     |   |            |
|-----|---|------------|
| 78  | 2.5.13 GlobalProtect Gateway and Portal Configuration.....                    | 67         |
| 79  | 2.5.14 Configure Automatic Threat and Application Updates .....               | 76         |
| 80  | 2.6 Integration of Kryptowire EMM+S with MobileIron .....                     | 77         |
| 81  | 2.6.1 Add MobileIron API Account for Kryptowire.....                          | 78         |
| 82  | 2.6.2 Contact Kryptowire to Create Inbound Connection.....                    | 81         |
| 83  | 2.7 Integration of Lookout Mobile Endpoint Security with MobileIron .....     | 81         |
| 84  | 2.7.1 Add MobileIron API Account for Lookout .....                            | 81         |
| 85  | 2.7.2 Add MobileIron Labels for Lookout.....                                  | 85         |
| 86  | 2.7.3 Add Lookout for Work for Android to MobileIron App Catalog.....         | 87         |
| 87  | 2.7.4 Apply Labels to Lookout for Work for Android .....                      | 90         |
| 88  | 2.7.5 Add Lookout for Work app for iOS to MobileIron App Catalog .....        | 93         |
| 89  | 2.7.6 Add MDM Connector for MobileIron to Lookout MES .....                   | 104        |
| 90  | 2.7.7 Configure MobileIron Risk Response .....                                | 108        |
| 91  | 2.8 Integration of Appthority Mobile Threat Detection with MobileIron .....   | 115        |
| 92  | 2.8.1 Create MobileIron API Account for Appthority Connector .....            | 115        |
| 93  | 2.8.2 Deploy Appthority Connector Open Virtualization Appliance .....         | 118        |
| 94  | 2.8.3 Run the Enterprise Mobility Management Connector Deployment Script..... | 119        |
| 95  | 2.9 Registering Devices with MobileIron Core .....                            | 120        |
| 96  | 2.9.1 Supervising and Registering iOS Devices.....                            | 120        |
| 97  | 2.9.2 Activating Lookout for Work on iOS .....                                | 144        |
| 98  | 2.9.3 Provisioning Work-Managed Android Devices with a Work Profile .....     | 149        |
| 99  | <b>Appendix A List of Acronyms .....</b>                                      | <b>164</b> |
| 100 | <b>Appendix B Glossary.....</b>   | <b>166</b> |
| 101 | <b>Appendix C References .....</b>  | <b>168</b> |

## 102 **List of Figures**

|     |  |          |
|-----|--|----------|
| 103 | <b>Figure 1-1 Logical Architecture Summary .....</b>       | <b>4</b> |
| 104 | <b>Figure 2-1 MobileIron Repository Configuration.....</b> | <b>6</b> |
| 105 | <b>Figure 2-2 MobileIron Core Version .....</b>            | <b>7</b> |

|     |   |    |
|-----|---|----|
| 106 | <a href="#">Figure 2-3 MobileIron Download Status</a>                       | 8  |
| 107 | <a href="#">Figure 2-4 Validating Database Data</a>                         | 8  |
| 108 | <a href="#">Figure 2-5 Validating Database Data Confirmation</a>            | 9  |
| 109 | <a href="#">Figure 2-6 Database Data Validation Initiation Confirmation</a> | 9  |
| 110 | <a href="#">Figure 2-7 Database Data Validation Status</a>                  | 10 |
| 111 | <a href="#">Figure 2-8 Software Updates Reboot Prompt</a>                   | 10 |
| 112 | <a href="#">Figure 2-9 Software Update Reboot Confirmation</a>              | 11 |
| 113 | <a href="#">Figure 2-10 Reboot Configuration Save Prompt</a>                | 11 |
| 114 | <a href="#">Figure 2-11 Upgrade Status</a>                                  | 11 |
| 115 | <a href="#">Figure 2-12 Ability to Upgrade to 9.7.0.1</a>                   | 12 |
| 116 | <a href="#">Figure 2-13 LDAP Settings</a>                                   | 13 |
| 117 | <a href="#">Figure 2-14 LDAP OUs</a>  | 13 |
| 118 | <a href="#">Figure 2-15 LDAP User Configuration</a>                         | 14 |
| 119 | <a href="#">Figure 2-16 LDAP Group Configuration</a>                        | 14 |
| 120 | <a href="#">Figure 2-17 Selected LDAP Group</a>                             | 15 |
| 121 | <a href="#">Figure 2-18 LDAP Advanced Options</a>                           | 16 |
| 122 | <a href="#">Figure 2-19 Testing LDAP Configuration</a>                      | 17 |
| 123 | <a href="#">Figure 2-20 LDAP Test Result</a>                                | 17 |
| 124 | <a href="#">Figure 2-21 MobileIron Device Labels</a>                        | 18 |
| 125 | <a href="#">Figure 2-22 Adding a Device Label</a>                           | 19 |
| 126 | <a href="#">Figure 2-23 Device Label Matches</a>                            | 19 |
| 127 | <a href="#">Figure 2-24 MobileIron Label List</a>                           | 20 |
| 128 | <a href="#">Figure 2-25 MobileIron SCEP Configuration</a>                   | 21 |
| 129 | <a href="#">Figure 2-26 Test SCEP Certificate</a>                           | 22 |
| 130 | <a href="#">Figure 2-27 Test SCEP Certificate Configuration</a>             | 23 |
| 131 | <a href="#">Figure 2-28 MobileIron VPN Configuration</a>                    | 24 |
| 132 | <a href="#">Figure 2-29 Palo Alto Networks Management Interface Enabled</a> | 25 |
| 133 | <a href="#">Figure 2-30 Management Interface Configuration</a>              | 26 |

|     |   |    |
|-----|---|----|
| 134 | <a href="#">Figure 2-31 Palo Alto Networks Firewall General Information .....</a>                           | 27 |
| 135 | <a href="#">Figure 2-32 Palo Alto Networks Services Configuration .....</a>                                 | 28 |
| 136 | <a href="#">Figure 2-33 DNS Configuration.....</a>  | 29 |
| 137 | <a href="#">Figure 2-34 NTP Configuration.....</a>  | 30 |
| 138 | <a href="#">Figure 2-35 Ethernet Interfaces .....</a>   | 30 |
| 139 | <a href="#">Figure 2-36 Ethernet Interface Configuration .....</a>  | 31 |
| 140 | <a href="#">Figure 2-37 WAN Interface IPv4 Configuration .....</a>  | 32 |
| 141 | <a href="#">Figure 2-38 WAN Interface IP Address Configuration.....</a>                                     | 33 |
| 142 | <a href="#">Figure 2-39 Completed WAN Interface Configuration .....</a>                                     | 33 |
| 143 | <a href="#">Figure 2-40 Security Zone List .....</a>  | 34 |
| 144 | <a href="#">Figure 2-41 LAN Security Zone Configuration .....</a>   | 35 |
| 145 | <a href="#">Figure 2-42 Virtual Router Configuration .....</a>  | 37 |
| 146 | <a href="#">Figure 2-43 Virtual Router General Settings .....</a>   | 38 |
| 147 | <a href="#">Figure 2-44 SSL VPN Tunnel Interface.....</a>   | 39 |
| 148 | <a href="#">Figure 2-45 Application Categories .....</a>  | 40 |
| 149 | <a href="#">Figure 2-46 MobileIron Core Palo Alto Networks Application Configuration.....</a>               | 41 |
| 150 | <a href="#">Figure 2-47 MobileIron Application Port Configuration .....</a>                                 | 42 |
| 151 | <a href="#">Figure 2-48 DMZ Access to MobileIron Firewall Rule Configuration .....</a>                      | 43 |
| 152 | <a href="#">Figure 2-49 DMZ Access to MobileIron Security Rule Source Zone Configuration.....</a>           | 44 |
| 153 | <a href="#">Figure 2-50 DMZ Access to MobileIron Security Rule Destination Address Configuration.....</a>   | 45 |
| 154 | <a href="#">Figure 2-51 DMZ Access to MobileIron Security Rule Application Protocol Configuration .....</a> | 46 |
| 155 | <a href="#">Figure 2-52 DMZ Access to MobileIron Security Rule Action Configuration.....</a>                | 47 |
| 156 | <a href="#">Figure 2-53 Outbound NAT Rule .....</a>   | 49 |
| 157 | <a href="#">Figure 2-54 Outbound NAT Original Packet Configuration .....</a>                                | 50 |
| 158 | <a href="#">Figure 2-55 Outbound NAT Translated Packet Configuration .....</a>                              | 51 |
| 159 | <a href="#">Figure 2-56 LDAP Profile .....</a>  | 52 |
| 160 | <a href="#">Figure 2-57 Authentication Profile .....</a>  | 54 |
| 161 | <a href="#">Figure 2-58 Advanced Authentication Profile Settings .....</a>                                  | 55 |

|     |  |    |
|-----|--|----|
| 162 | <a href="#">Figure 2-59 LDAP Group Mapping</a>                           | 56 |
| 163 | <a href="#">Figure 2-60 LDAP Group Include List</a>                      | 57 |
| 164 | <a href="#">Figure 2-61 Authentication Policy Source Zones</a>           | 58 |
| 165 | <a href="#">Figure 2-62 Authentication Policy Destination Zones</a>      | 59 |
| 166 | <a href="#">Figure 2-63 Authentication Profile Actions</a>               | 60 |
| 167 | <a href="#">Figure 2-64 Import MobileIron Certificate</a>                | 61 |
| 168 | <a href="#">Figure 2-65 Internal Root Certificate Profile</a>            | 63 |
| 169 | <a href="#">Figure 2-66 Certificate Profile</a>                          | 63 |
| 170 | <a href="#">Figure 2-67 SSL/TLS Service Profile</a>                      | 64 |
| 171 | <a href="#">Figure 2-68 Custom URL Category</a>                          | 65 |
| 172 | <a href="#">Figure 2-69 URL Filtering Profile</a>                        | 66 |
| 173 | <a href="#">Figure 2-70 URL Filtering Security Policy</a>                | 67 |
| 174 | <a href="#">Figure 2-71 General GlobalProtect Gateway Configuration</a>  | 68 |
| 175 | <a href="#">Figure 2-72 GlobalProtect Authentication Configuration</a>   | 69 |
| 176 | <a href="#">Figure 2-73 GlobalProtect Tunnel Configuration</a>           | 69 |
| 177 | <a href="#">Figure 2-74 VPN Client IP Pool</a>                           | 70 |
| 178 | <a href="#">Figure 2-75 VPN Client Settings</a>                          | 70 |
| 179 | <a href="#">Figure 2-76 VPN Authentication Override Configuration</a>    | 71 |
| 180 | <a href="#">Figure 2-77 VPN User Group Configuration</a>                 | 71 |
| 181 | <a href="#">Figure 2-78 VPN Split Tunnel Configuration</a>               | 72 |
| 182 | <a href="#">Figure 2-79 GlobalProtect Portal Configuration</a>           | 73 |
| 183 | <a href="#">Figure 2-80 GlobalProtect Portal SSL/TLS Configuration</a>   | 74 |
| 184 | <a href="#">Figure 2-81 GlobalProtect External Gateway Configuration</a> | 75 |
| 185 | <a href="#">Figure 2-82 GlobalProtect Portal Agent Configuration</a>     | 76 |
| 186 | <a href="#">Figure 2-83 Schedule Link</a>                                | 77 |
| 187 | <a href="#">Figure 2-84 Threat Update Schedule</a>                       | 77 |
| 188 | <a href="#">Figure 2-85 MobileIron Users</a>                             | 78 |
| 189 | <a href="#">Figure 2-86 Kryptowire API User Configuration</a>            | 79 |

|     |   |     |
|-----|---|-----|
| 190 | <a href="#">Figure 2-87 MobileIron User List</a>                                  | 80  |
| 191 | <a href="#">Figure 2-88 Kryptowire API User Space Assignment</a>                  | 80  |
| 192 | <a href="#">Figure 2-89 Kryptowire Device List</a>                                | 81  |
| 193 | <a href="#">Figure 2-90 MobileIron User List</a>                                  | 82  |
| 194 | <a href="#">Figure 2-91 MobileIron Lookout User Configuration</a>                 | 83  |
| 195 | <a href="#">Figure 2-92 Lookout MobileIron Admin Account</a>                      | 84  |
| 196 | <a href="#">Figure 2-93 Lookout Account Space Assignment</a>                      | 84  |
| 197 | <a href="#">Figure 2-94 MobileIron Label List</a>                                 | 85  |
| 198 | <a href="#">Figure 2-95 MTP Low Risk Label Configuration</a>                      | 86  |
| 199 | <a href="#">Figure 2-96 MobileIron App Catalog</a>                                | 87  |
| 200 | <a href="#">Figure 2-97 Adding Lookout for Work to the MobileIron App Catalog</a> | 88  |
| 201 | <a href="#">Figure 2-98 Lookout for Work Application Configuration</a>            | 89  |
| 202 | <a href="#">Figure 2-99 Lookout for Work Application Configuration</a>            | 89  |
| 203 | <a href="#">Figure 2-100 Lookout for Work AFW Configuration</a>                   | 90  |
| 204 | <a href="#">Figure 2-101 Apply Lookout for Work to Android Devices</a>            | 91  |
| 205 | <a href="#">Figure 2-102 Apply To Labels Dialogue</a>                             | 92  |
| 206 | <a href="#">Figure 2-103 Lookout for Work with Applied Labels</a>                 | 93  |
| 207 | <a href="#">Figure 2-104 MobileIron App Catalog</a>                               | 93  |
| 208 | <a href="#">Figure 2-105 Lookout for Work Selected From iTunes</a>                | 94  |
| 209 | <a href="#">Figure 2-106 Lookout for Work App Configuration</a>                   | 95  |
| 210 | <a href="#">Figure 2-107 Lookout for Work App Configuration</a>                   | 96  |
| 211 | <a href="#">Figure 2-108 Lookout for Work Managed App Settings</a>                | 97  |
| 212 | <a href="#">Figure 2-109 App Catalog With Lookout for Work</a>                    | 97  |
| 213 | <a href="#">Figure 2-110 Lookout for Work Selected</a>                            | 98  |
| 214 | <a href="#">Figure 2-111 Apply To Labels Dialogue</a>                             | 99  |
| 215 | <a href="#">Figure 2-112 App Catalog With Lookout for Work</a>                    | 99  |
| 216 | <a href="#">Figure 2-113 Importing Managed Application Configuration</a>          | 101 |
| 217 | <a href="#">Figure 2-114 plist Import Configuration</a>                           | 102 |

|     |  |     |
|-----|--|-----|
| 218 | <a href="#">Figure 2-115 Lookout Configuration Selected .....</a>        | 102 |
| 219 | <a href="#">Figure 2-116 Apply To Label Dialogue .....</a>               | 103 |
| 220 | <a href="#">Figure 2-117 Lookout Configuration With Labels .....</a>     | 104 |
| 221 | <a href="#">Figure 2-118 Add Lookout Connector Display .....</a>         | 104 |
| 222 | <a href="#">Figure 2-119 Connector Settings .....</a>                    | 105 |
| 223 | <a href="#">Figure 2-120 Connector Enrollment Settings .....</a>         | 106 |
| 224 | <a href="#">Figure 2-121 Connector Sync Settings .....</a>               | 108 |
| 225 | <a href="#">Figure 2-122 MobileIron App Control Rule .....</a>           | 109 |
| 226 | <a href="#">Figure 2-123 MobileIron App Control Rule .....</a>           | 110 |
| 227 | <a href="#">Figure 2-124 MTP High Risk Compliance Action.....</a>        | 111 |
| 228 | <a href="#">Figure 2-125 Baseline Policy Selection .....</a>             | 112 |
| 229 | <a href="#">Figure 2-126 MTP High Risk Policy .....</a>                  | 112 |
| 230 | <a href="#">Figure 2-127 Security Policy Trigger .....</a>               | 113 |
| 231 | <a href="#">Figure 2-128 Policy List.....</a>                            | 114 |
| 232 | <a href="#">Figure 2-129 Apply To Label Dialogue .....</a>               | 115 |
| 233 | <a href="#">Figure 2-130 Appthority User Settings .....</a>              | 117 |
| 234 | <a href="#">Figure 2-131 Appthority Connector User.....</a>              | 118 |
| 235 | <a href="#">Figure 2-132 Appthority Connector Space Assignment .....</a> | 118 |
| 236 | <a href="#">Figure 2-133 Appthority Connector CLI Configuration.....</a> | 119 |
| 237 | <a href="#">Figure 2-134 Appthority EMM Connector Status .....</a>       | 120 |
| 238 | <a href="#">Figure 2-135 iOS Reset Screen .....</a>                      | 121 |
| 239 | <a href="#">Figure 2-136 Erase iPhone Confirmation .....</a>             | 122 |
| 240 | <a href="#">Figure 2-137 Erase iPhone Final Confirmation .....</a>       | 123 |
| 241 | <a href="#">Figure 2-138 Entering iOS Passcode .....</a>                 | 124 |
| 242 | <a href="#">Figure 2-139 iOS Trust Computer Confirmation .....</a>       | 125 |
| 243 | <a href="#">Figure 2-140 Entering Passcode to Trust Computer .....</a>   | 126 |
| 244 | <a href="#">Figure 2-141 Resetting iPhone in Configurator 2.....</a>     | 127 |
| 245 | <a href="#">Figure 2-142 Configurator 2 Erase Confirmation .....</a>     | 127 |

|     |  |     |
|-----|--|-----|
| 246 | <a href="#">Figure 2-143 Configurator 2 License Agreement .....</a>                          | 128 |
| 247 | <a href="#">Figure 2-144 Restoring iPhone .....</a>  | 128 |
| 248 | <a href="#">Figure 2-145 Prepare Option in Configuration 2 .....</a>                         | 129 |
| 249 | <a href="#">Figure 2-146 Device Preparation Options .....</a>                                | 130 |
| 250 | <a href="#">Figure 2-147 Preparation MDM Server Selection .....</a>                          | 131 |
| 251 | <a href="#">Figure 2-148 Signing into Apple Account .....</a>                                | 132 |
| 252 | <a href="#">Figure 2-149 Organization Assignment Dialogue .....</a>                          | 133 |
| 253 | <a href="#">Figure 2-150 Creating an Organization .....</a>                                  | 134 |
| 254 | <a href="#">Figure 2-151 Supervisory Identity Configuration .....</a>                        | 135 |
| 255 | <a href="#">Figure 2-152 Organization Selection.....</a>                                     | 136 |
| 256 | <a href="#">Figure 2-153 Supervising Identity Selection.....</a>                             | 136 |
| 257 | <a href="#">Figure 2-154 Selected Organization.....</a>                                      | 137 |
| 258 | <a href="#">Figure 2-155 Create an Organization Supervision Identity Configuration .....</a> | 138 |
| 259 | <a href="#">Figure 2-156 Setup Assistant Configuration.....</a>                              | 139 |
| 260 | <a href="#">Figure 2-157 Waiting for iPhone .....</a>  | 139 |
| 261 | <a href="#">Figure 2-158 MobileIron Registration Page .....</a>                              | 140 |
| 262 | <a href="#">Figure 2-159 Opening Settings Confirmation .....</a>                             | 141 |
| 263 | <a href="#">Figure 2-160 Profile Installation.....</a>                                       | 141 |
| 264 | <a href="#">Figure 2-161 Profile Installation.....</a>                                       | 142 |
| 265 | <a href="#">Figure 2-162 Profile Installation Warning .....</a>                              | 143 |
| 266 | <a href="#">Figure 2-163 Profile Installation Trust Confirmation .....</a>                   | 144 |
| 267 | <a href="#">Figure 2-164 Profile Installation Confirmation .....</a>                         | 144 |
| 268 | <a href="#">Figure 2-165 Lookout for Work Splash Screen .....</a>                            | 145 |
| 269 | <a href="#">Figure 2-166 Lookout for Work Permission Information .....</a>                   | 146 |
| 270 | <a href="#">Figure 2-167 Notifications Permissions Prompt .....</a>                          | 147 |
| 271 | <a href="#">Figure 2-168 Locations Permission Prompt.....</a>                                | 148 |
| 272 | <a href="#">Figure 2-169 Lookout for Work Home Screen .....</a>                              | 149 |
| 273 | <a href="#">Figure 2-170 MobileIron AFW Configuration .....</a>                              | 150 |

|     |   |     |
|-----|---|-----|
| 274 | <a href="#">Figure 2-171 AFW Configuration</a>                              | 151 |
| 275 | <a href="#">Figure 2-172 MobileIron Enrollment Process</a>                  | 152 |
| 276 | <a href="#">Figure 2-173 AFW Enrollment</a>                                 | 153 |
| 277 | <a href="#">Figure 2-174 MobileIron Installation</a>                        | 154 |
| 278 | <a href="#">Figure 2-175 Accepting AFW Terms and Conditions</a>             | 155 |
| 279 | <a href="#">Figure 2-176 MobileIron Privacy Information</a>                 | 156 |
| 280 | <a href="#">Figure 2-177 MobileIron Configuration Required Notification</a> | 157 |
| 281 | <a href="#">Figure 2-178 MobileIron Device Status</a>                       | 158 |
| 282 | <a href="#">Figure 2-179 AFW Configuration</a>                              | 159 |
| 283 | <a href="#">Figure 2-180 AFW Workspace Creation</a>                         | 160 |
| 284 | <a href="#">Figure 2-181 MobileIron Work Profile Lock Preferences</a>       | 161 |
| 285 | <a href="#">Figure 2-182 MobileIron Google Account Configuration</a>        | 162 |
| 286 | <a href="#">Figure 2-183 MobileIron Device Status</a>                       | 163 |

## 287 **List of Tables**

|     |   |    |
|-----|---|----|
| 288 | <a href="#">Table 1-1 Typographic Conventions</a>       | 3  |
| 289 | <a href="#">Table 2-1 Implemented Security Policies</a> | 47 |
| 290 | <a href="#">Table 2-2 Implemented Security Policies</a> | 48 |
| 291 | <a href="#">Table 2-3 Implemented Security Policies</a> | 48 |

## 292 1 Introduction

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

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

### 300 1.1 Practice Guide Structure

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

305 This guide contains three volumes:

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

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

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

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

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

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

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

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

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

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

## 344 1.2 Build Overview

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

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

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

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

### 361 **1.3 Typographic Conventions**

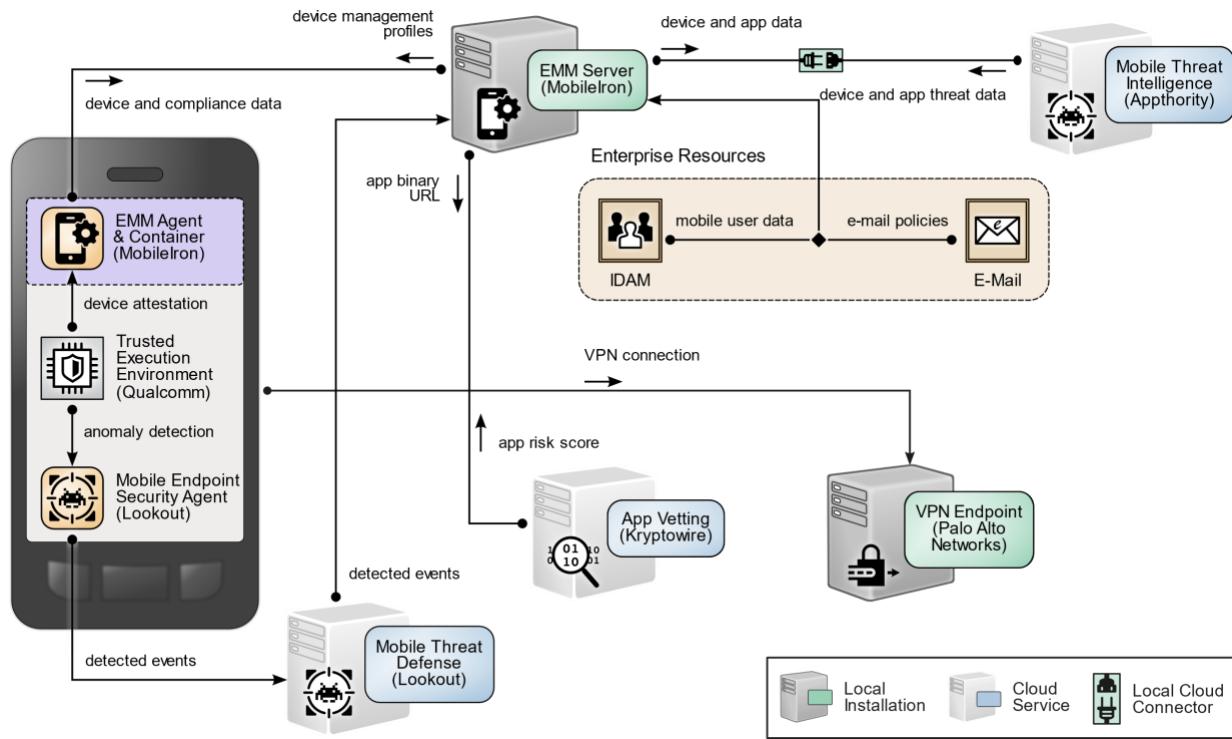
362 The following table presents typographic conventions used in this volume.

363 **Table 1-1 Typographic Conventions**

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

### 364 **1.4 Logical Architecture Summary**

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

367 **Figure 1-1 Logical Architecture Summary**

## 368 **2 Product Installation Guides**

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

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

### 376 **2.1 Appthority Mobile Threat Detection**

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

379 **2.2 Kryptowire EMM+S**

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

382 **2.3 Lookout Mobile Endpoint Security**

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

386 **2.4 MobileIron Core**

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

389 **2.4.1 Installation of MobileIron Core and Stand-Alone Sentry**

390 Follow the steps below to install MobileIron Core:

- 391 1. Obtain a copy of the *On-Premise Installation Guide for MobileIron Core, Sentry, and*  
392 *Enterprise Connector* from the MobileIron support portal.
- 393 2. Follow the MobileIron Core predeployment and installation steps in Chapter 1 of the *On-*  
394 *Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* for the  
395 version of MobileIron being deployed in your environment. In our lab implementation, we  
396 deployed MobileIron Core 9.5.0.0 as a Virtual Core running on VMware 6.0. Post-  
397 installation, we performed an upgrade to MobileIron Core 9.7.0.1 following guidance  
398 provided in *CoreConnectorReleaseNotes9701\_Rev12Apr2018*. Direct installations to  
399 MobileIron Core 9.7.0.1 will experience slightly different results, as some added features in  
400 this version are not used with earlier versions of configuration files.

401 **2.4.2 General MobileIron Core Setup**

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

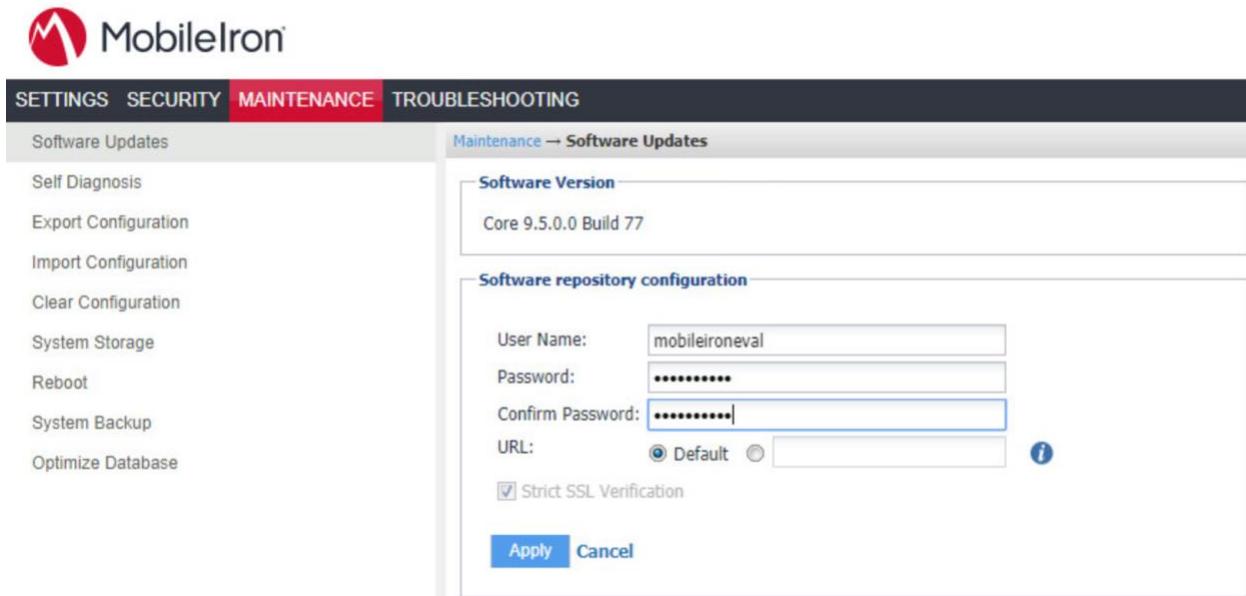
- 404 1. Obtain a copy of *MobileIron Core Device Management Guide for iOS Devices* from the  
405 MobileIron support portal.
- 406 2. Complete all instructions provided in Chapter 1, Setup Tasks.

#### 407    2.4.3 Upgrade MobileIron Core

408    The following steps were used to upgrade our instance of MobileIron Core from 9.5.0.0 to 9.7.0.1. Note  
 409    there was no direct upgrade path between these two versions; our selected upgrade path was 9.5.0.0 >  
 410    9.5.0.1 > 9.7.0.1.

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

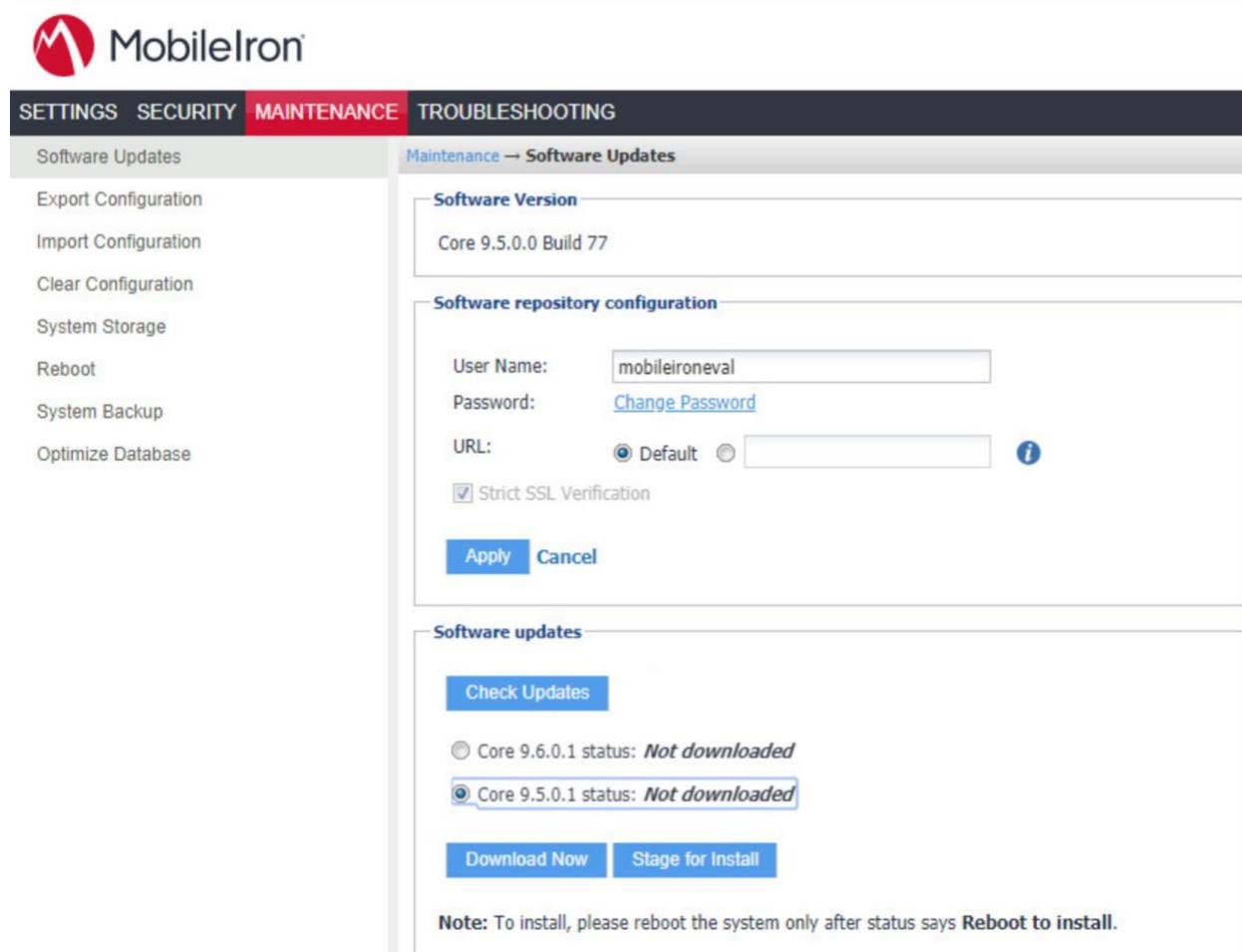
418    Figure 2-1 MobileIron Repository Configuration



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

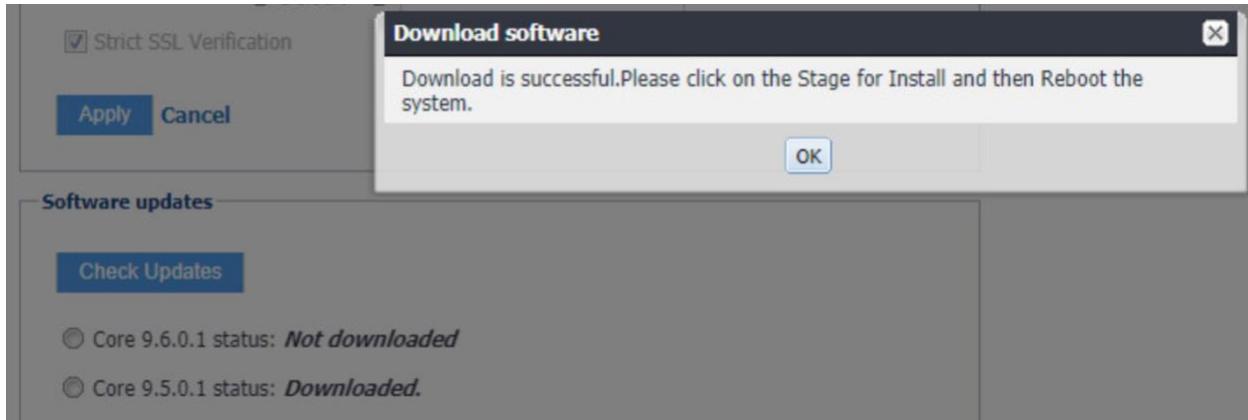
423 c. Select **Download Now**. After a delay, the Software Download dialogue will appear.

424 Figure 2-2 MobileIron Core Version



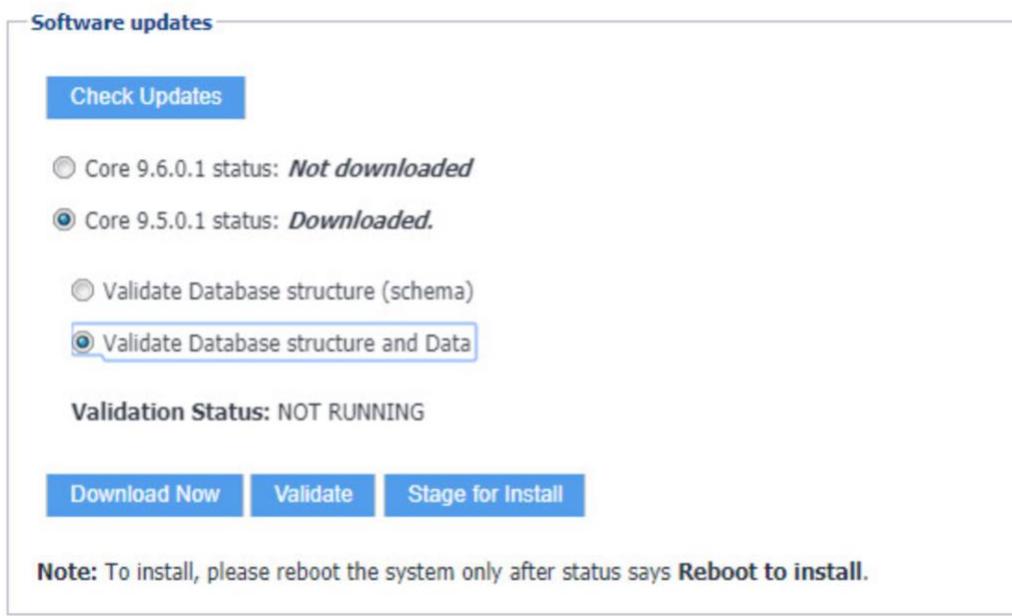
425 5. In the **Download Software** dialogue, select **OK**.

426 Figure 2-3 MobileIron Download Status

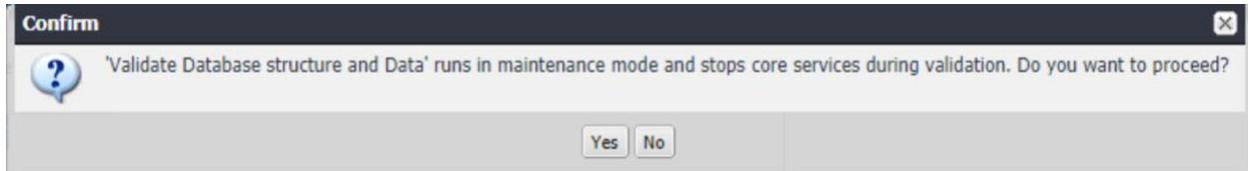
427 6. In the **Software updates** section:

- Select the **Core 9.5.0.1 status: Downloaded** option.
- Select the **Validate Database Structure and Data** option.
- Select **Validate**.

431 Figure 2-4 Validating Database Data

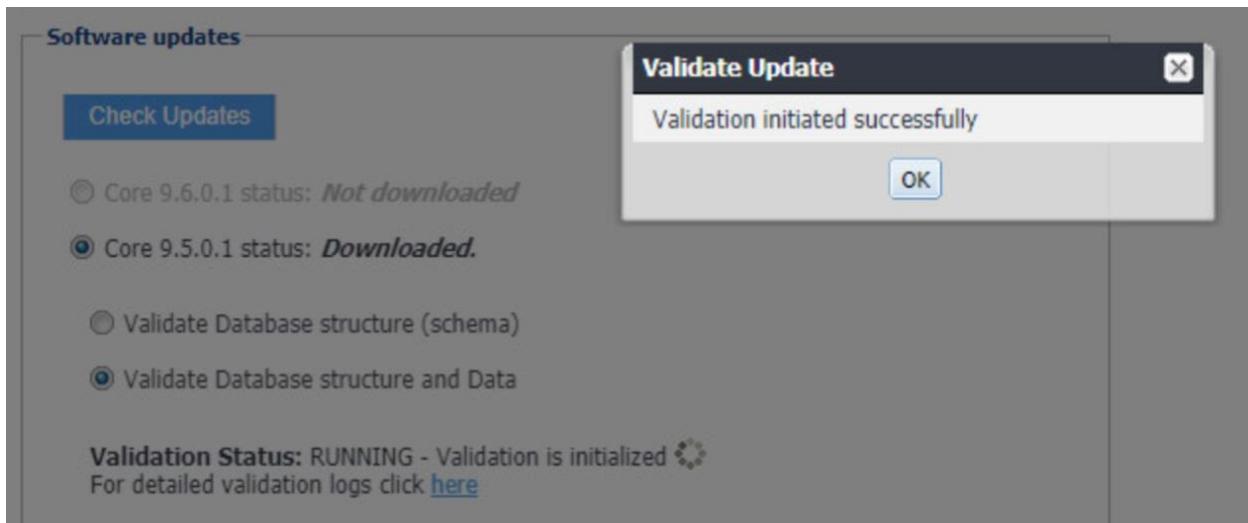
432 7. In the **Confirm** dialogue, select **Yes** to validate database structure and data.

433    **Figure 2-5 Validating Database Data Confirmation**



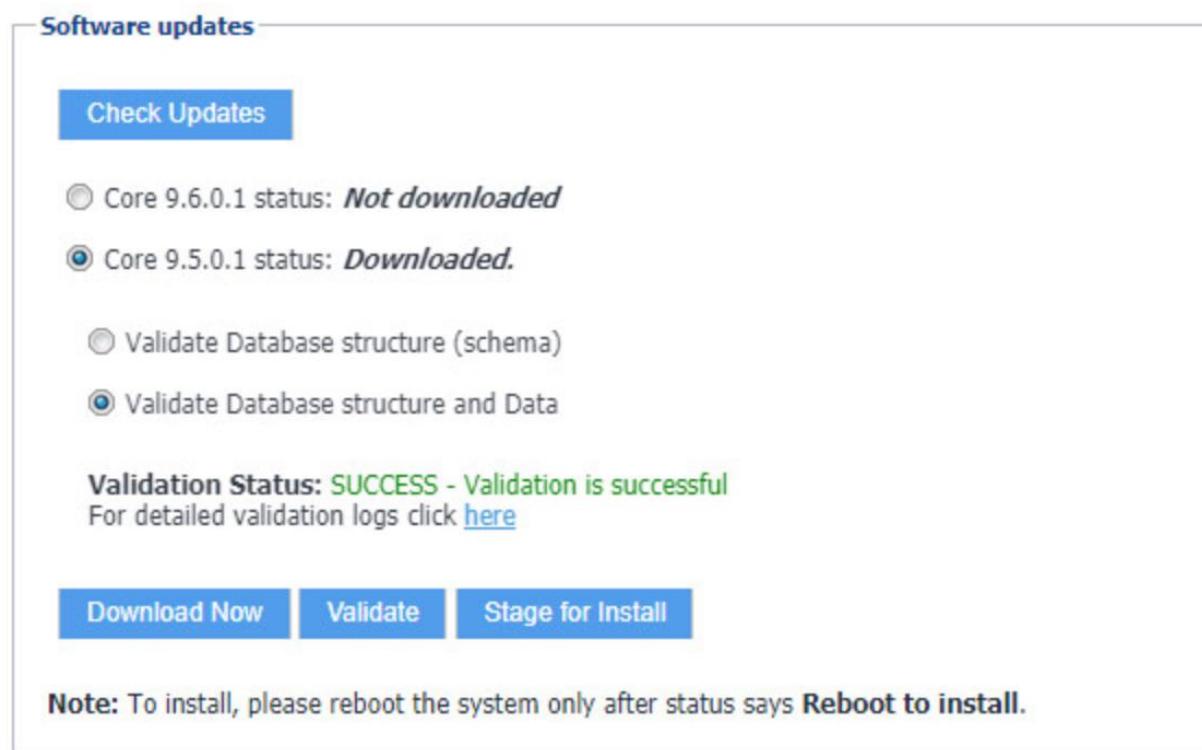
434    8. In the **Validate Update** dialogue, select **OK**.

435    **Figure 2-6 Database Data Validation Initiation Confirmation**

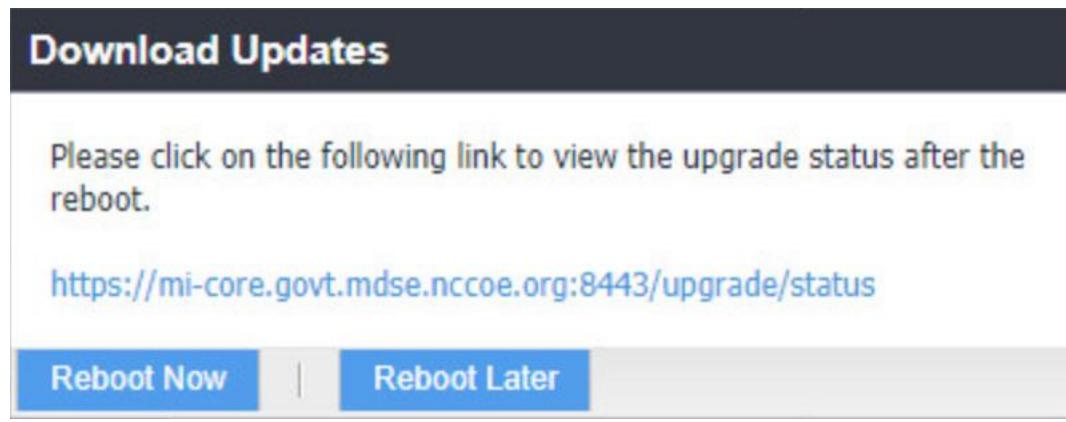


436    9. In the **Software updates** section, select **Stage for Install**; the **Download Updates** dialogue  
437    will appear.

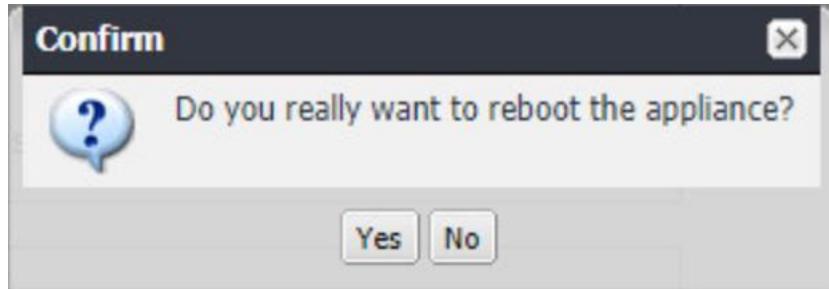
438 Figure 2-7 Database Data Validation Status

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

440 Figure 2-8 Software Updates Reboot Prompt

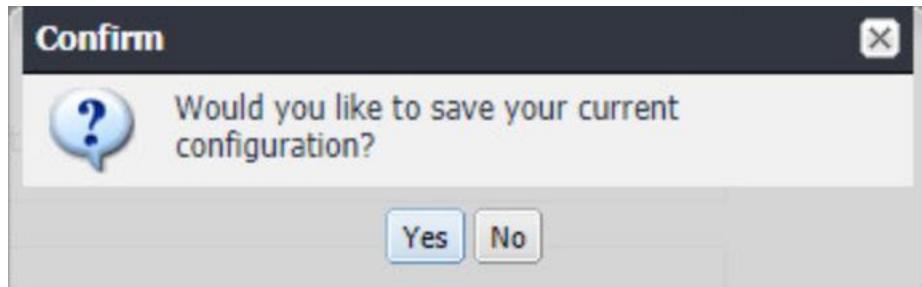
441 11. In the **Confirm** dialogues:442 a. Select **Yes** to confirm reboot of the appliance.

443 Figure 2-9 Software Update Reboot Confirmation



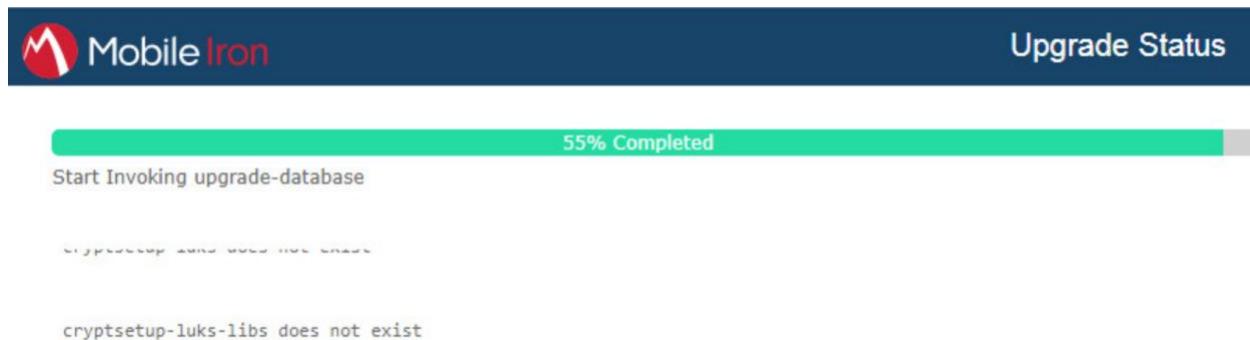
444 b. Select Yes to confirm saving the current configuration.

445 Figure 2-10 Reboot Configuration Save Prompt



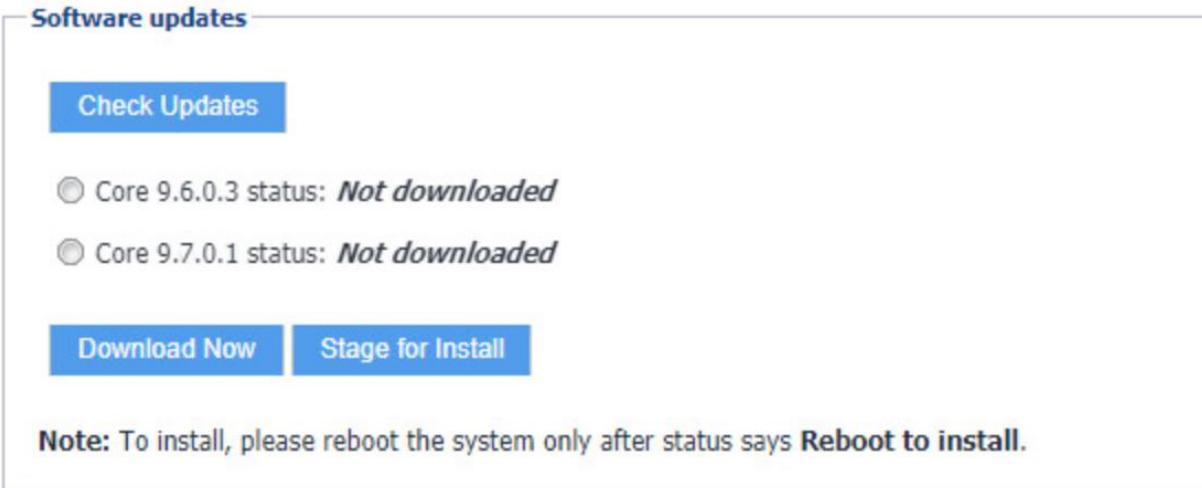
446 12. The Upgrade Status website hosted by Core will automatically open.

447 Figure 2-11 Upgrade Status



448 13. Once the upgrade is complete, **System Manager > Maintenance > Software Updates > Software Updates** now shows the capability to upgrade to 9.7.0.1.  
449

450    Figure 2-12 Ability to Upgrade to 9.7.0.1



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

#### 453    2.4.4 Integration with Microsoft Active Directory

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

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

461 Figure 2-13 LDAP Settings

New LDAP Setting

Directory Connection

|                         |  |
|-------------------------|--|
| Directory URL:          | ldap://192.168.7.10  |
| Directory Failover URL: | ldap(s)://<IP or Hostname>:[port]  |
| Directory UserID:       | mi-ldap-sync<br><a href="#">Change Password</a>  |
| Search Results Timeout: | 30 Seconds   |
| Chase Referrals:        | <input type="radio"/> Enable <input checked="" type="radio"/> Disable                                      |
| Admin State:            | <input checked="" type="radio"/> Enable <input type="radio"/> Disable                                      |
| Directory Type:         | <input checked="" type="radio"/> Active Directory <input type="radio"/> Domino <input type="radio"/> Other |
| Domain:                 | govt.mds.local   |

462 b. Directory Configuration—OUs:

463 Figure 2-14 LDAP OUs

New LDAP Setting

Directory Configuration - OUs

|                   |  |
|-------------------|--|
| OU Base DN:       | dc=govt,dc=mds,dc=local                                    |
| OU Search Filter: | ( (objectClass=organizationalUnit)(objectClass=container)) |

464 c. Directory Configuration—Users:

465 Figure 2-15 LDAP User Configuration

**New LDAP Setting**

**Directory Configuration - Users**

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

466 d. Directory Configuration—Groups:

467 Figure 2-16 LDAP Group Configuration

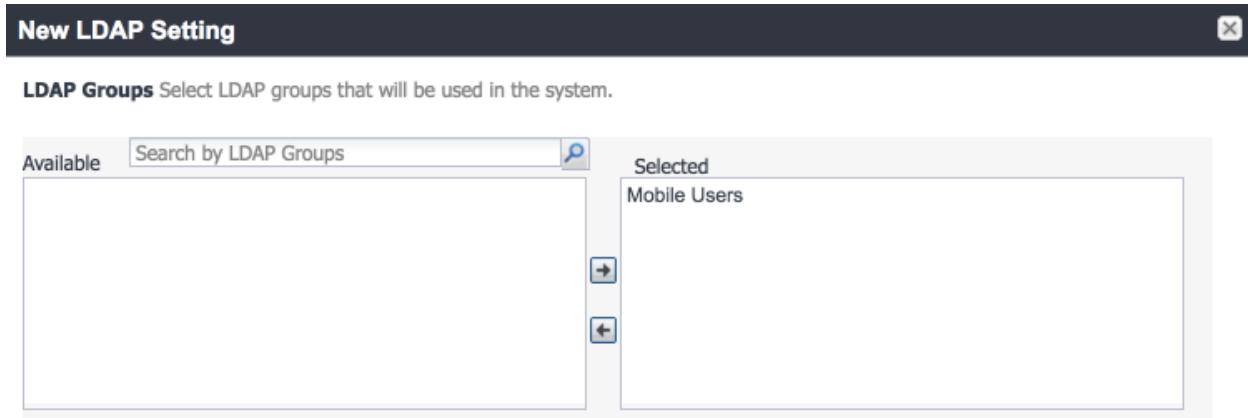
**New LDAP Setting**

**Directory Configuration - Groups**

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

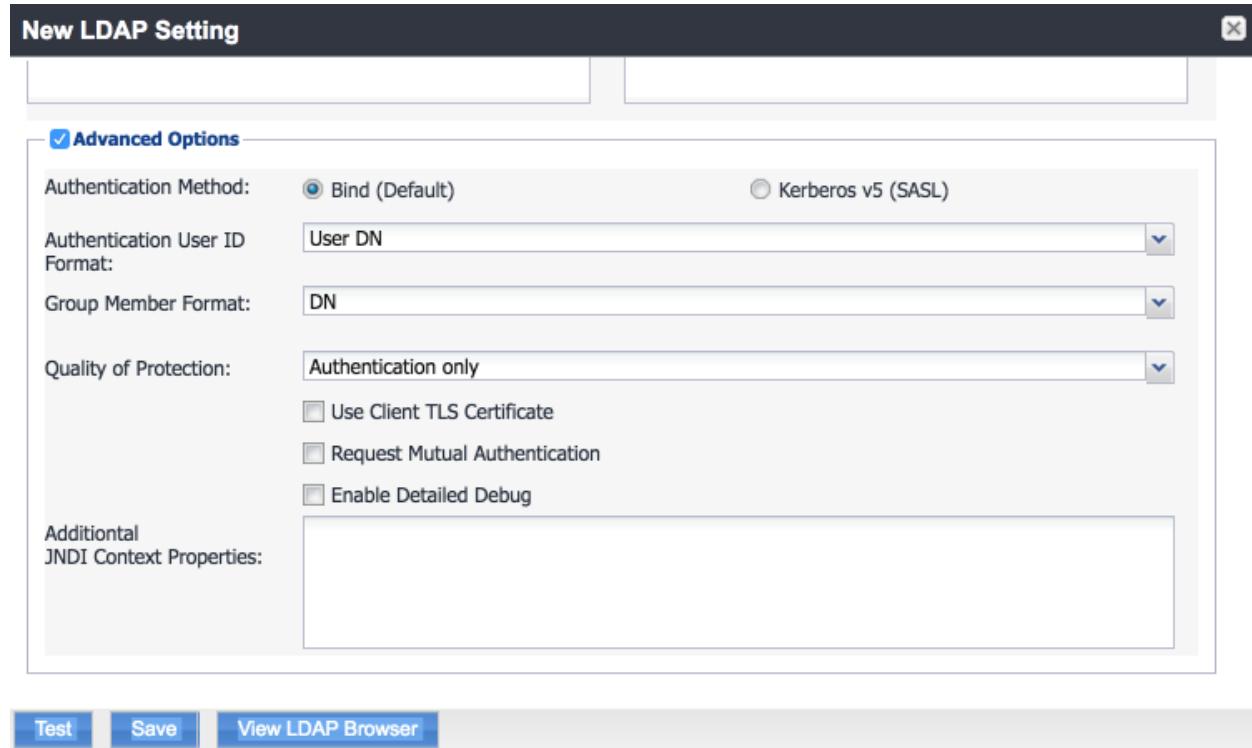
- 468                   e. LDAP Groups:
- 469                    i. As a preparatory step, we used Active Directory Users and Computers to create  
470                    a new security group for mobile-authorized users on the Domain Controller for  
471                    the *govt.mds.local* domain. In our example, this group is named **Mobile Users**.
- 472                    ii. In the search bar, enter the name of the LDAP group for mobile-authorized  
473                    users.
- 474                    iii. Select the **magnifying glass** button; the group name should be added to the  
475                    **Available** list.
- 476                    iv. In the **Available** list box:
- 477                      1) Select the **Mobile Users** list item.
- 478                      2) Select the **right-arrow** button; the Mobile Users list item should move to  
479                      the **Selected** list box.
- 480                    v. In the **Selected** list:
- 481                      1) Select the default **Users** group list item.
- 482                      2) Select the **left-arrow** button; the Users list item should move to the  
483                      **Available** list box.

484                  Figure 2-17 Selected LDAP Group



- 485                   f. Custom Settings: Custom settings were not specified.
- 486                   g. Advanced Options: Advanced options were configured as shown in Figure 2-18.

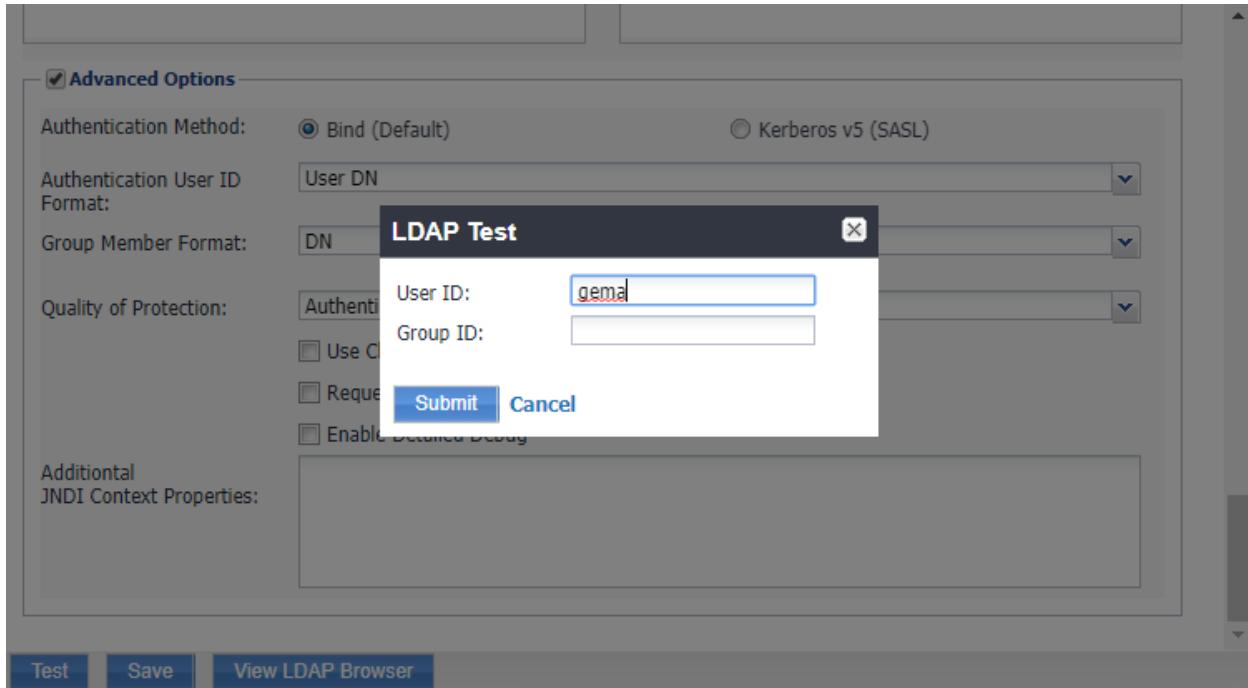
487 Figure 2-18 LDAP Advanced Options



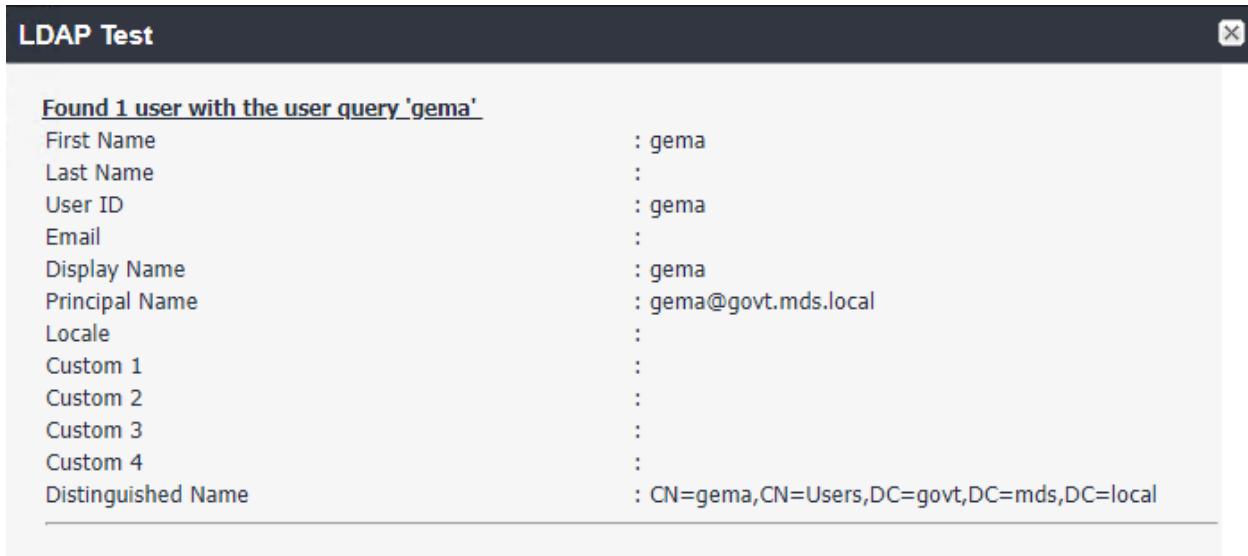
488 **Note:** In our lab environment, we did not enable stronger Quality of Protection or enable the Use of  
489 Client Transport Layer Security Certificate or Request Mutual Authentication features. However, we  
490 recommend that implementers consider using those additional mechanisms to secure communication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

- 492 2. From **Steps 19** through **21** from the MobileIron guide, we tested that MobileIron can  
493 successfully query LDAP for Derived Personal Identity Verification Credential (DPC) Users.
- 494 a. In the **New LDAP Setting** dialogue, click the **Test** button to open the **LDAP Test** dialogue.
- 495 b. In the **LDAP Test** dialogue, enter a **User ID** for a member of the DPC Users group, then  
496 click the **Submit** button. A member of the Mobile Users group in our environment is  
497 **gema**.

498 Figure 2-19 Testing LDAP Configuration

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

500 Figure 2-20 LDAP Test Result



501    **2.4.5 Create a Mobile Users Label**

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

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

508    **Figure 2-21 MobileIron Device Labels**

| NAME            | DESCRIPTION                   | TYPE   | CRITERIA   | SPACE  | VIEW DE...         |
|-----------------|-------------------------------|--------|--|--------|--------------------|
| AFW             | Android for Work - enter...   | Filter | {"common.platform" = "android" and "android.afw_cap..."} | Global | <a href="#">10</a> |
| All-Smartphones | Label for all devices irre... | Filter | "common.retired"=false                                   | Global | <a href="#">16</a> |

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

520 Figure 2-22 Adding a Device Label

Add Label

Name

Description

Type  Manual  Filter

**Criteria**

All  Any  of the following rules are true

|          |        |              |     |
|----------|--------|--------------|-----|
| Name     | Equals | Mobile Users | +/- |
| Platform | Equals | Android      | +/- |

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

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

522 e. Select **Save**.

523 Figure 2-23 Device Label Matches

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

Exclude retired devices from search results

3 matching devices

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

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

525 **Figure 2-24 MobileIron Label List**

|                          |                   | NAME                         | DESCRIPTION | TYPE  | CRITERIA | SPACE             | VIEW DE... |
|--------------------------|-------------------|------------------------------|-------------|---|----------|-------------------|------------|
| <input type="checkbox"/> | macOS             | Label for all macOS De...    | Filter      | "common.platform"="macOS" AND "common.retired"=...    | Global   | 0                 |            |
| <input type="checkbox"/> | Mobile Users      | Label for users authoriz...  | Filter      | ("user.ldap.groups.name" = "Mobile Users" AND "com... | Global   | <a href="#">3</a> |            |
| <input type="checkbox"/> | MTP - Deactivated | Device lifecycle: deactiv... | Manual      |   | Global   | 0                 |            |

526 

## 2.5 Integration of Palo Alto Networks GlobalProtect with MobileIron

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

531 

### 2.5.1 MobileIron Configuration

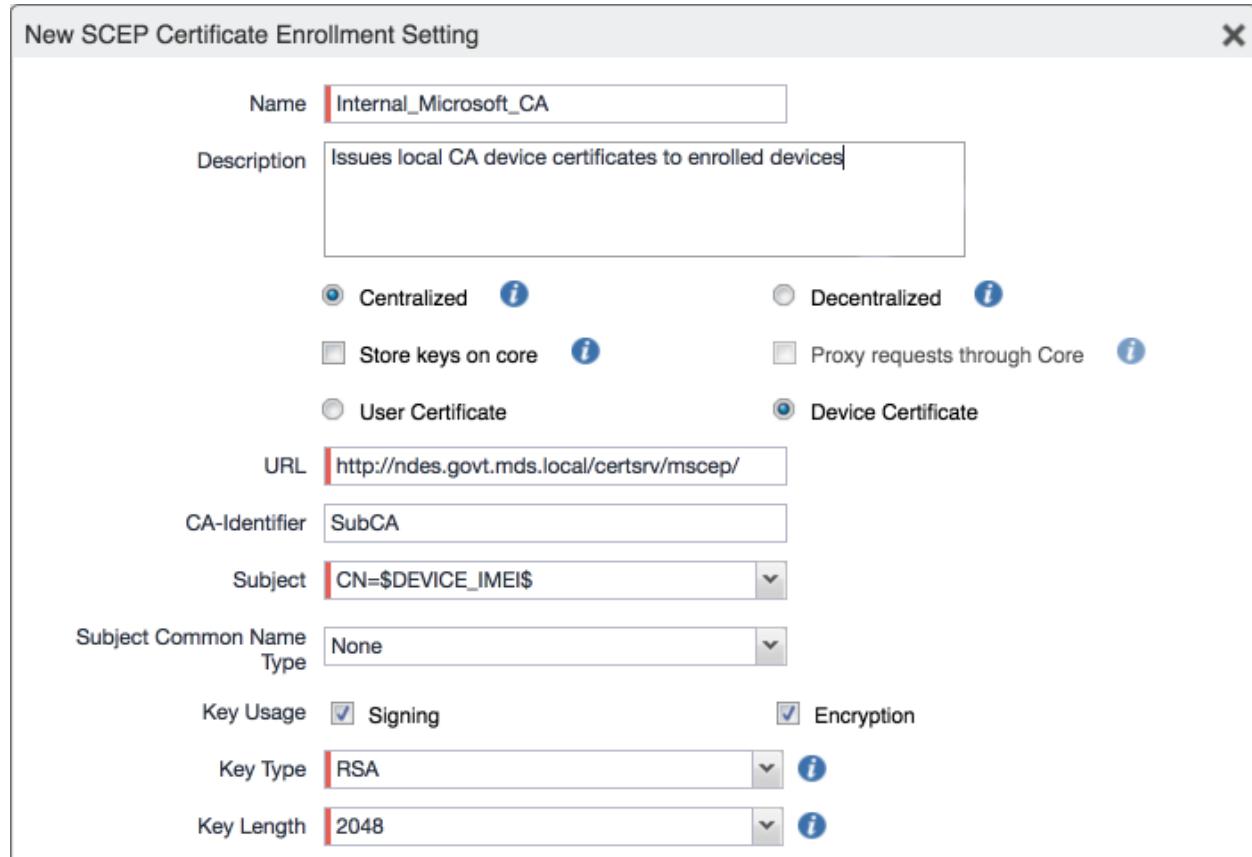
532 The following steps create the MobileIron Core configurations necessary to support integration with  
 533 Palo Alto GlobalProtect and Microsoft CA.

534 

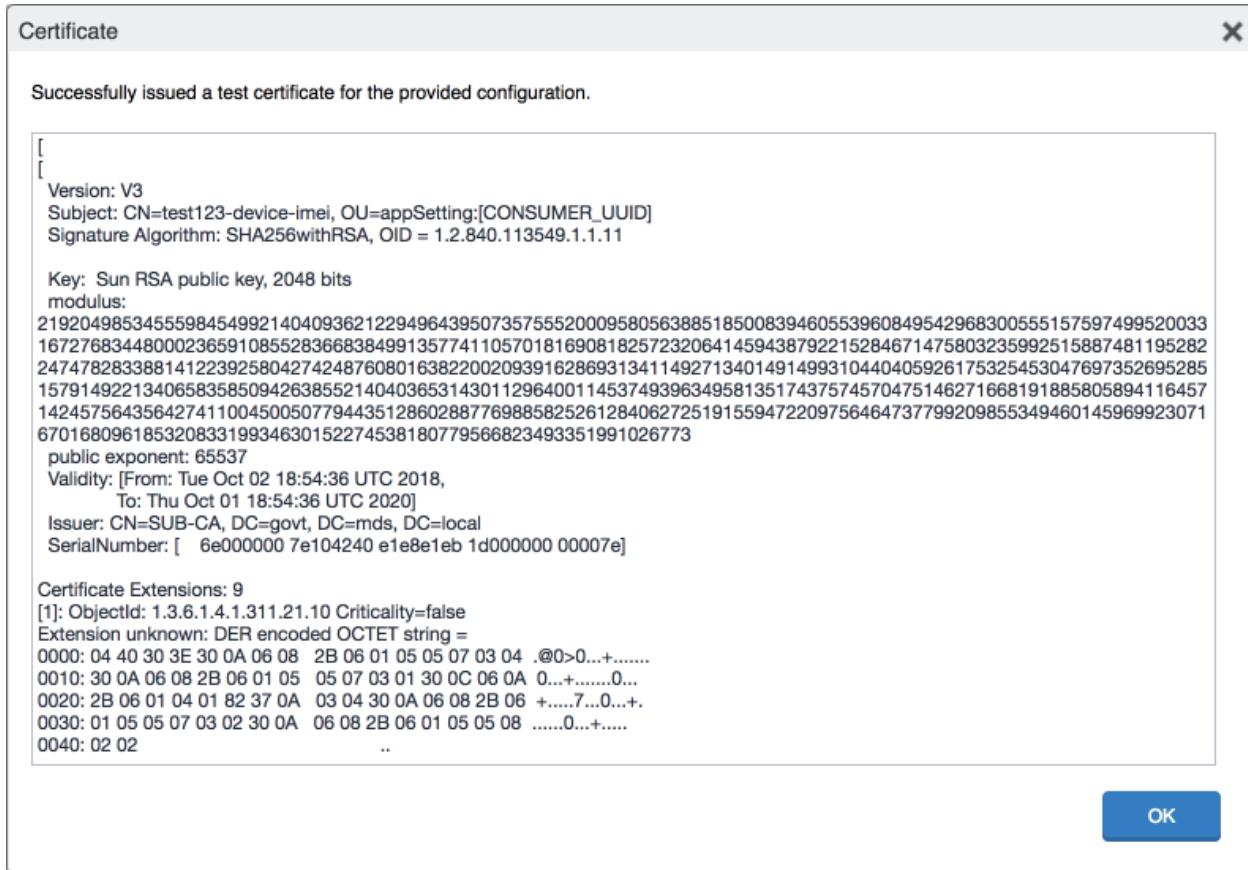
#### 2.5.1.1 *Create Simple Certificate Enrollment Protocol (SCEP) Configuration*

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

545 Figure 2-25 MobileIron SCEP Configuration



- 546 f. In the **Fingerprint** field, enter the fingerprint of the Microsoft CA that will issue the  
 547 device certificates.
- 548 g. For the **Challenge Type** drop-down menu, select **Microsoft SCEP**.
- 549 h. Below the **Subject Alternative Names** list box, select **Add**; a new list item will appear.
- 550 i. For the new list item:
- 551   i. For the **Type** drop-down menu, select **NT Principal Name**.
- 552   ii. For the **Value** drop-down menu, select **\$USER\_UPN\$**.
- 553 j. Select **Issue Test Certificate**; the **Certificate** dialogue should indicate success.
- 554 k. In the **Certificate** dialogue, select **OK**.

555 **Figure 2-26 Test SCEP Certificate**

556

4. Select **Save**.

557 **Figure 2-27 Test SCEP Certificate Configuration**

| Subject Alternative Names |              |   |
|---------------------------|--------------|---|
| TYPE                      | VALUE        | i |
| NT Principal Name         | \$USER_UPN\$ | X |

**Add+**

**Issue Test Certificate** **i** **Cancel** **Save**

558 **2.5.1.2 Create Palo Alto Networks GlobalProtect Configuration**

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

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

- 569           d. For the **User Authentication** drop-down menu, select **certificate**.
- 570           e. For the **Identity Certificate** drop-down menu, select the SCEP enrollment profile created  
571           in the previous section.
- 572           f. Select **Save**.

573 **Figure 2-28 MobileIron VPN Configuration**

| SAFARI DOMAIN | DESCRIPTION |
|---------------|-------------|
|               |             |

**Cancel** **Save**

## 574 [2.5.2 Basic Palo Alto Networks Configuration](#)

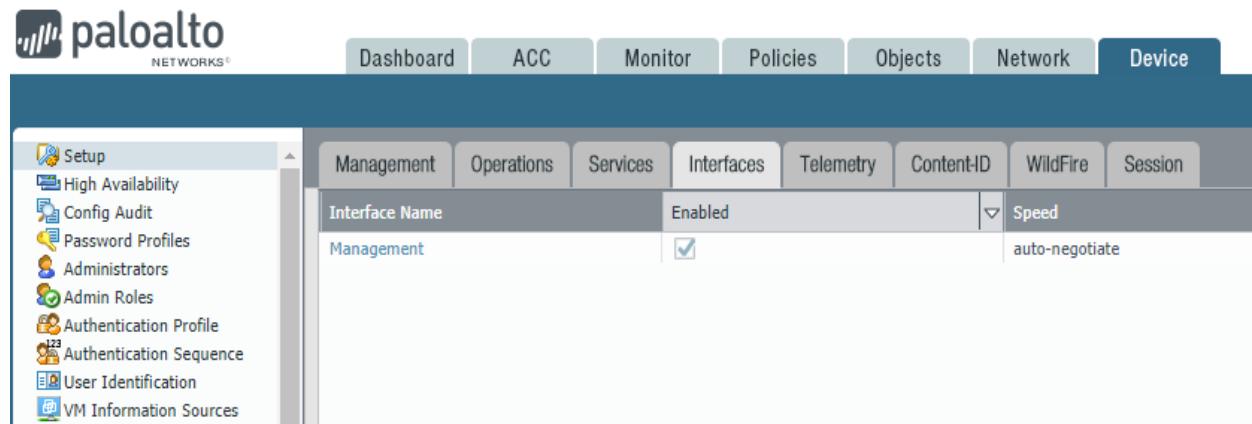
- 575 During basic configuration, internet protocol (IP) addresses are assigned to the management interface,  
576 domain name system (DNS), and network time protocol (NTP). The management interface allows the  
577 administrator to configure and implement security rules through this interface.

578    **2.5.2.1 Configure Management Interface**

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

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

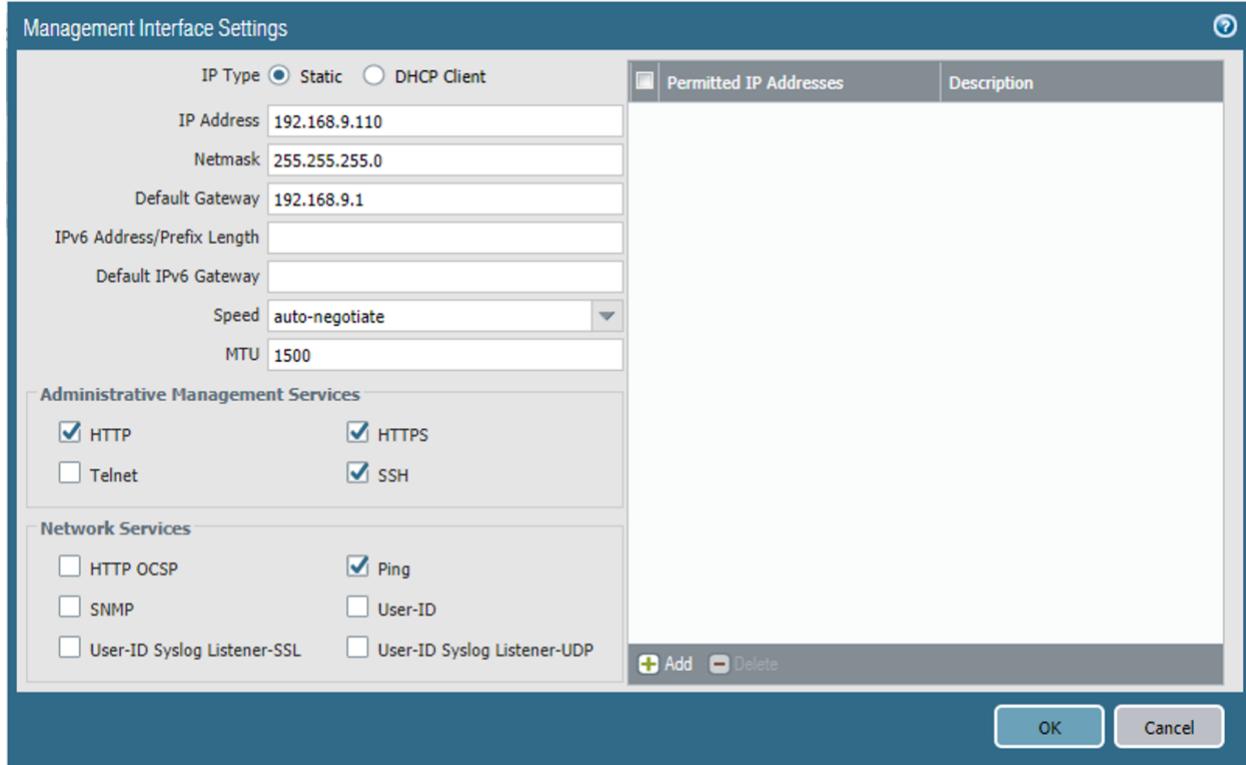
583    **Figure 2-29 Palo Alto Networks Management Interface Enabled**



| Interface Name | Enabled                             | Speed          |
|----------------|-------------------------------------|----------------|
| Management     | <input checked="" type="checkbox"/> | auto-negotiate |

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

593 Figure 2-30 Management Interface Configuration



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

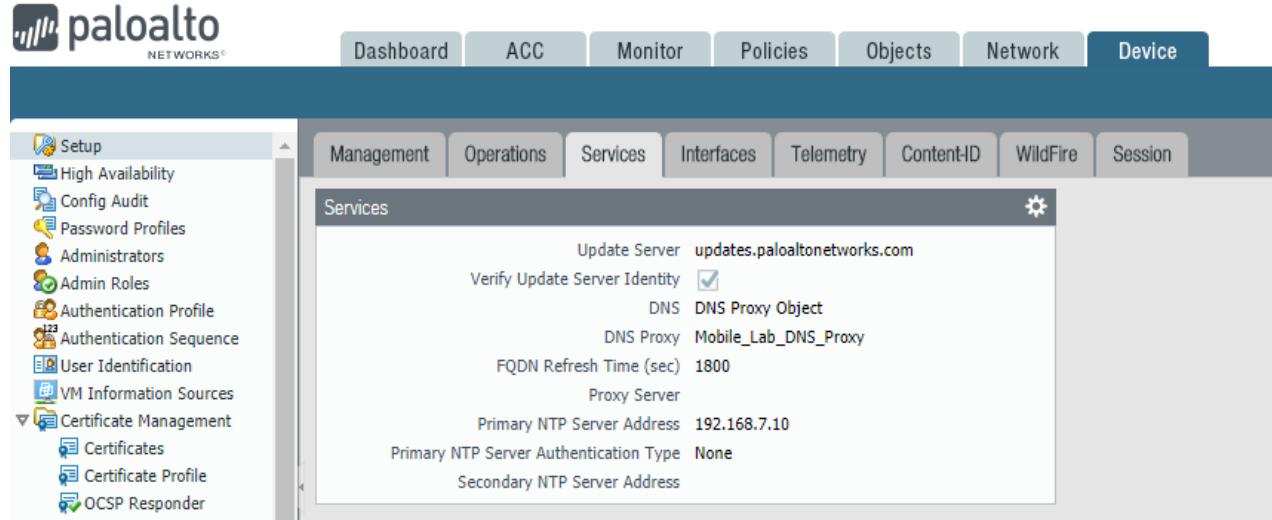
596 **Figure 2-31 Palo Alto Networks Firewall General Information**

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

597 **2.5.2.2 Configure DNS and NTP**

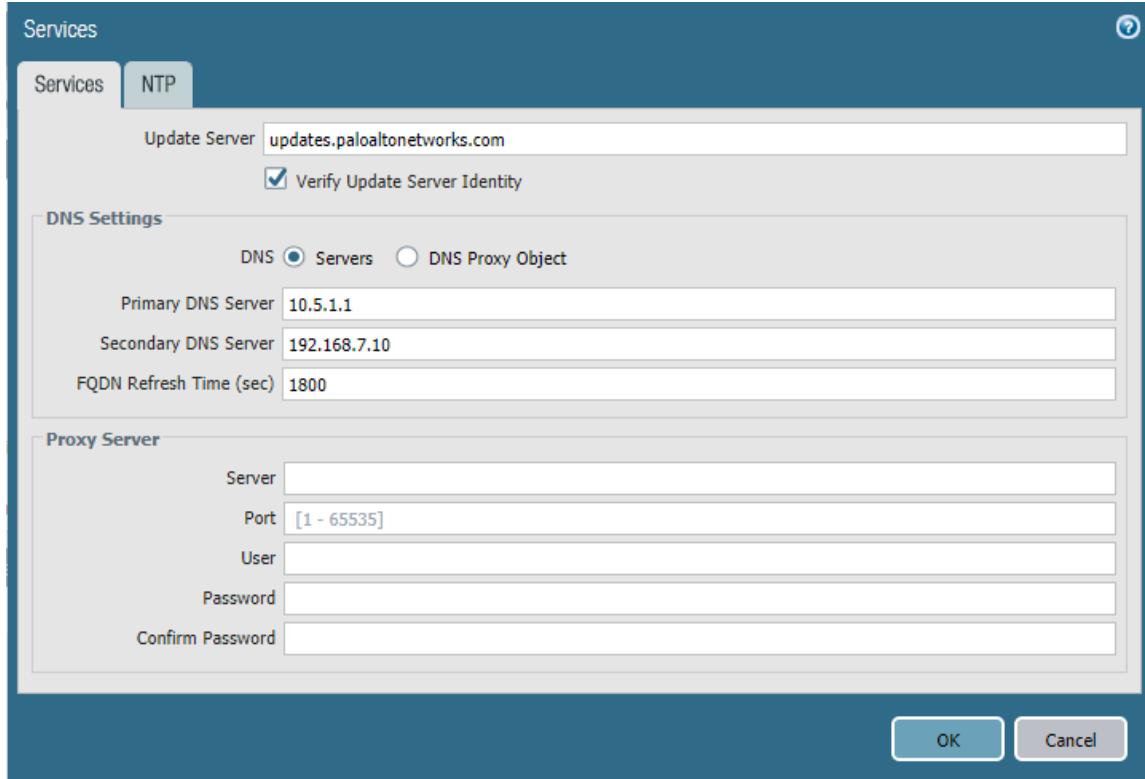
- 598     1. In the **Palo Alto Networks Portal**, navigate to **Device > Setup > Services**.
- 599     2. In the **Services** tab, select the settings icon.

600 Figure 2-32 Palo Alto Networks Services Configuration

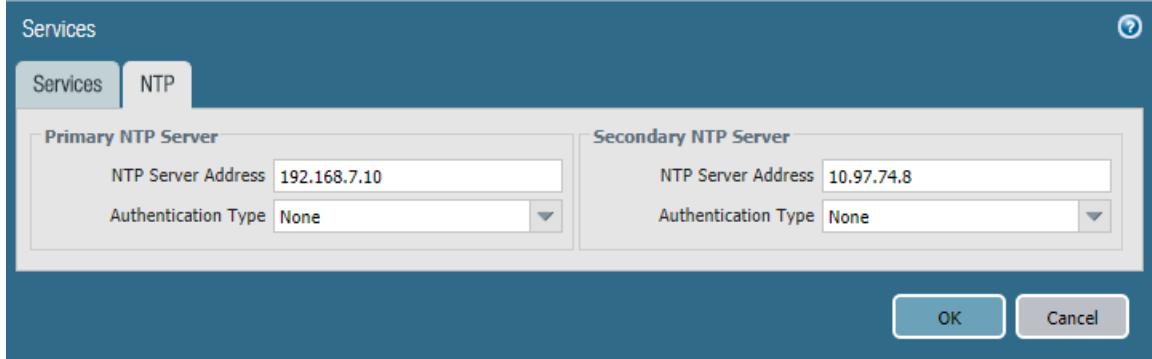


- 601        3. On the Services > Services tab:
- 602            a. For the **Primary DNS Server** field, enter the primary DNS server IP address.
- 603            b. For the **Secondary DNS Server** field, enter the secondary DNS server IP address, if applicable.
- 604
- 605        4. Select the **NTP** tab.

606      **Figure 2-33 DNS Configuration**



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

613 **Figure 2-34 NTP Configuration**614 **2.5.3 Palo Alto Networks Interfaces and Zones Configuration**

615 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.

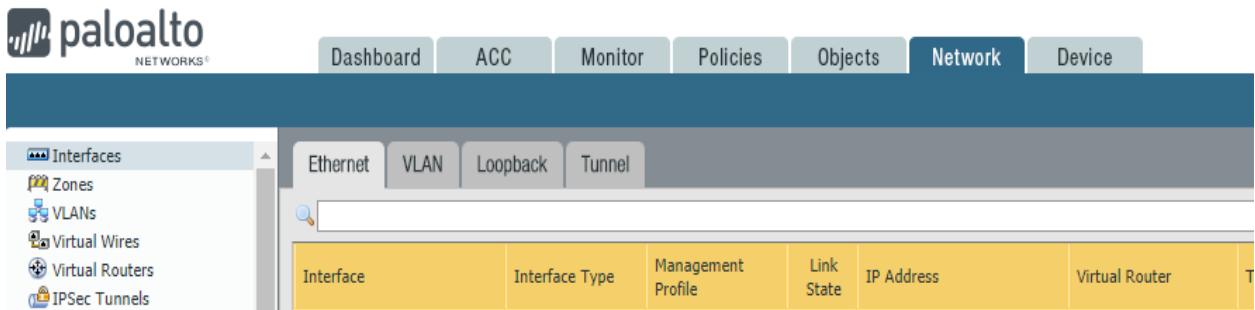
617 ***2.5.3.1 Create Ethernet Interfaces and Addresses***

618 Our example implementation uses three interfaces:

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

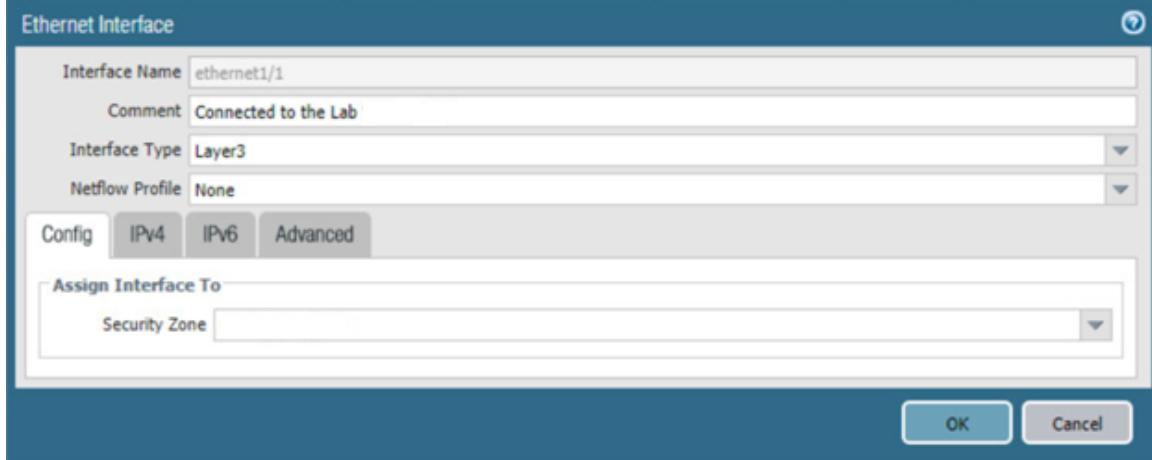
623 To create and configure Ethernet interfaces:

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

625 **Figure 2-35 Ethernet Interfaces**

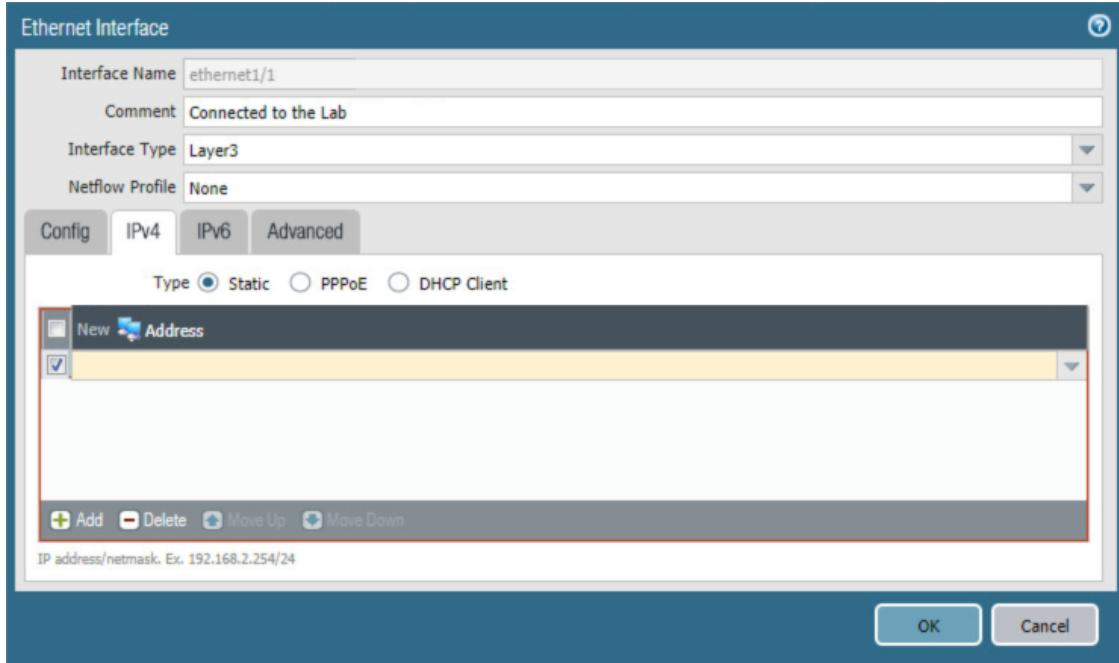
- 626           2. In the **Ethernet** tab, select the name of the interface to configure; the Ethernet Interface  
627           dialogue will appear.
- 628           3. In the **Ethernet Interface** dialogue:
- 629            a. In the **Comment** field, enter a description for this interface.
- 630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

631       Figure 2-36 Ethernet Interface Configuration



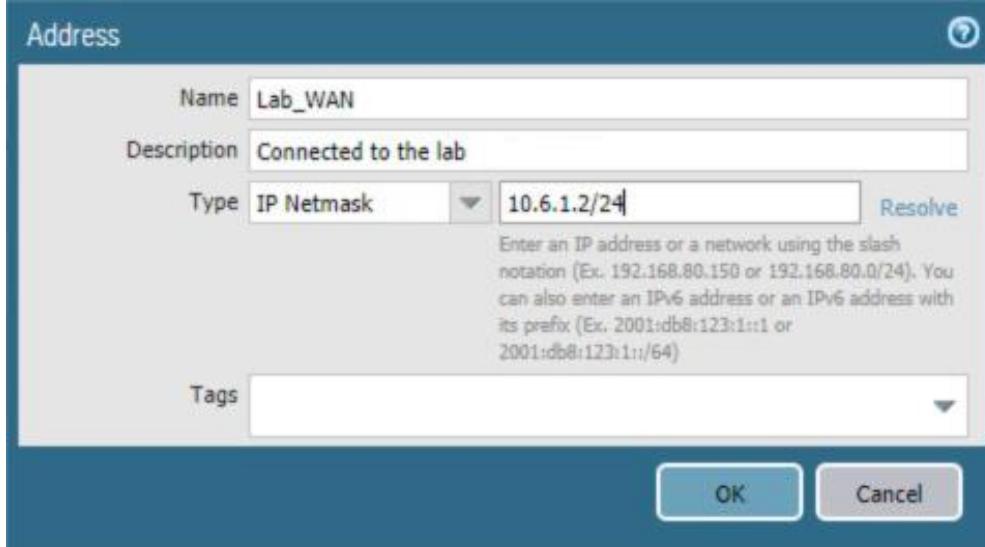
- 632           c. Select the **IPv4** tab.
- 633           d. On the **IPv4** tab:
- 634            i. In the **IP** list box, select **Add**; a blank list item will appear.
- 635            ii. In the blank list item, select **New Address**; the Address dialogue will appear.

636    Figure 2-37 WAN Interface IPv4 Configuration

637                    iii. In the **Address** dialogue:

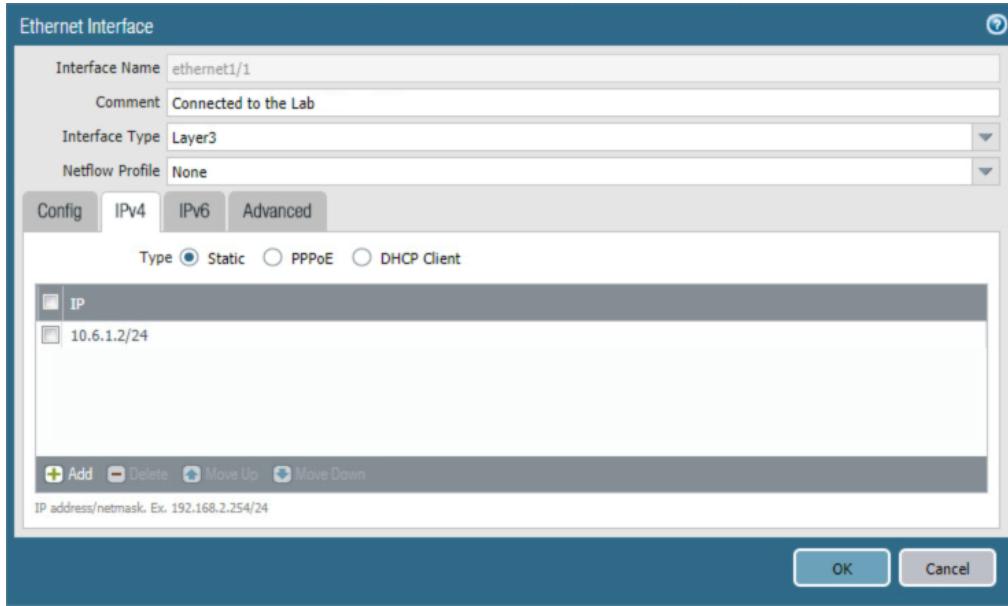
- 638                    1) For the **Name** field, enter a unique name to identify this address.
- 639                    2) For the **Description** field, enter a meaningful description of the purpose of  
640                    this address.
- 641                    3) In the unnamed field following the **Type** drop-down menu, enter the IPv4  
642                    address that this interface will use in **Classless Inter-Domain Routing**  
643                    notation. This example uses **10.6.1.2/24** for the WAN interface in our lab  
644                    environment.
- 645                    4) Select **OK**.

646 Figure 2-38 WAN Interface IP Address Configuration



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

649 Figure 2-39 Completed WAN Interface Configuration



650 4. Select **OK**.  
651 5. Repeat **Steps 2 and 3** for each of the additional Ethernet/Layer3 interfaces.

652    **2.5.3.2 Create Security Zones**

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

- 655
  - *Mobile\_Lab\_GOV*T: 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)

662    To configure each zone:

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

664    **Figure 2-40 Security Zone List**

| Name              | Type   | Interfaces / Virtual Systems | Zone Protection Profile | Packet Buffer Protection |
|-------------------|--------|------------------------------|-------------------------|--------------------------|
| Mobile_Lab_DMZ    | layer3 | ethernet1/2                  |                         | <input type="checkbox"/> |
| Mobile_Lab_GOV    | layer3 | ethernet1/3                  |                         | <input type="checkbox"/> |
| Mobile_Lab_SSLVPN | layer3 | tunnel.1                     |                         | <input type="checkbox"/> |
| Mobile_Lab_WAN    | layer3 | ethernet1/1                  |                         | <input type="checkbox"/> |

665       2. In the **Zones** pane, select **Add**; the Zones page will open.

666       3. On the **Zones** page:

667          a. For the **Name** field, provide a unique name for the zone.

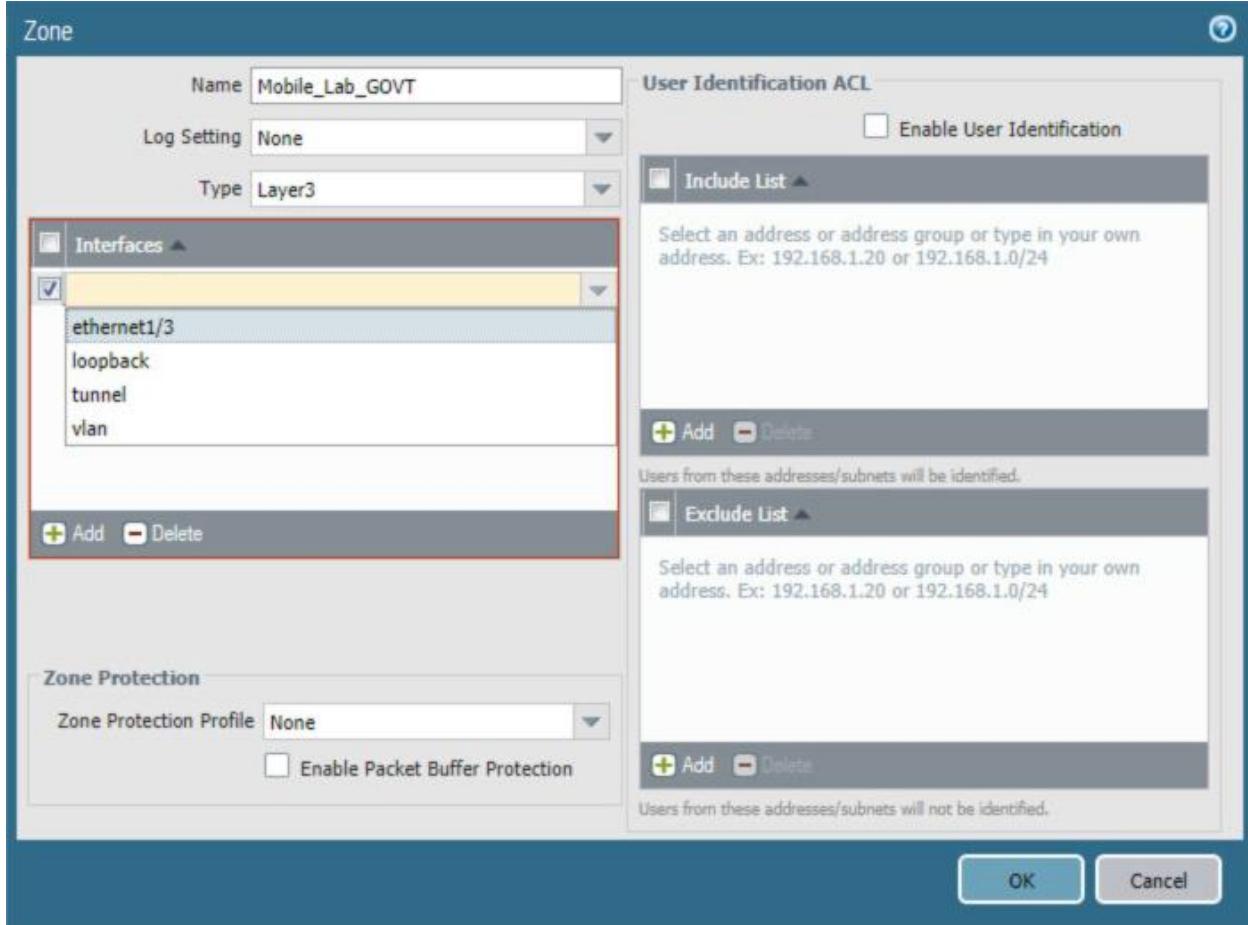
668          b. For the **Type** drop-down menu, select **Layer 3**.

669          c. Under **Interfaces**, select **Add**; a blank drop-down menu will appear.

670          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.

673 e. Select OK.

674 Figure 2-41 LAN Security Zone Configuration



675 f. Repeat Step b for each zone.

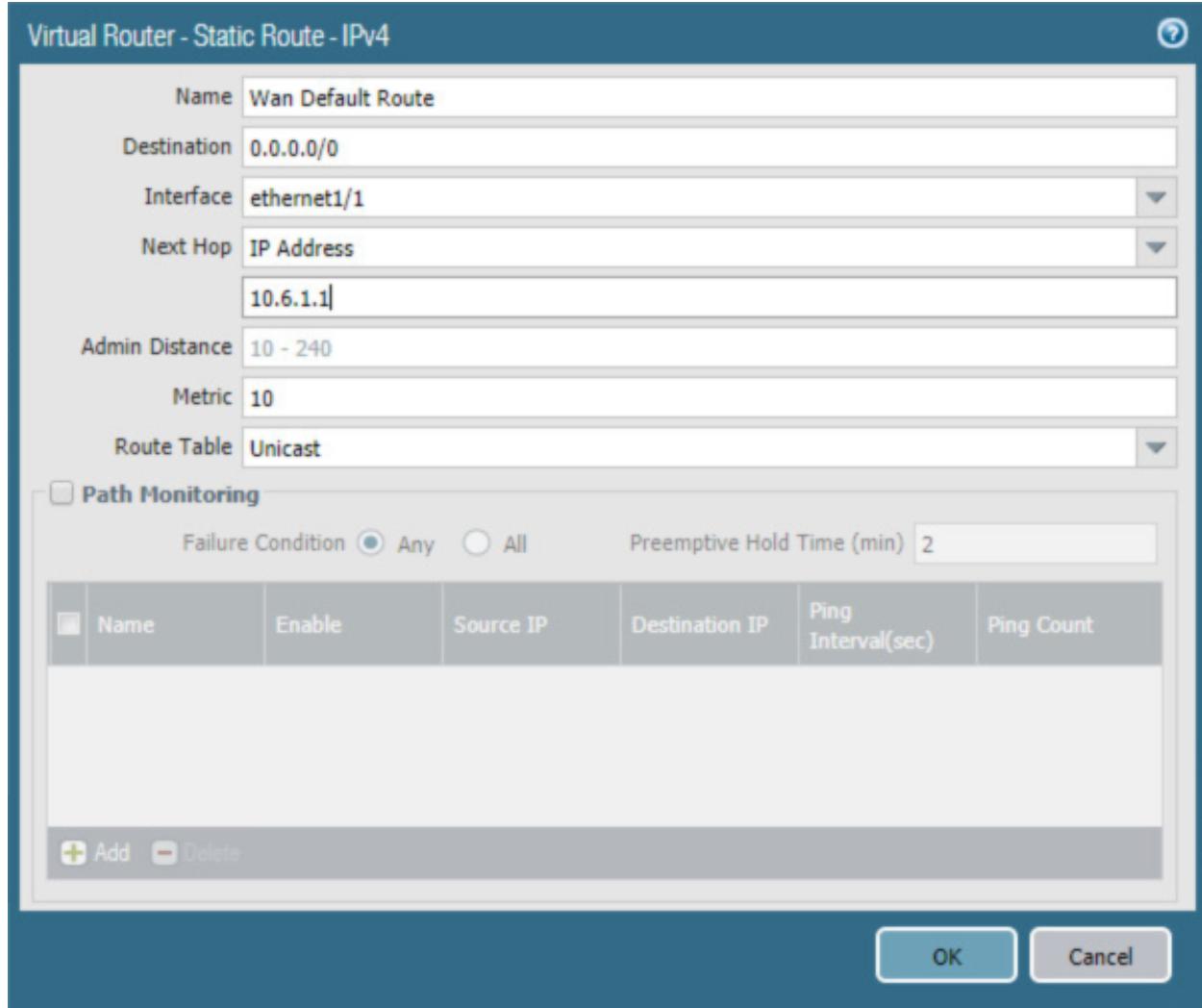
#### 2.5.4 Configure Router

676 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.

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

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

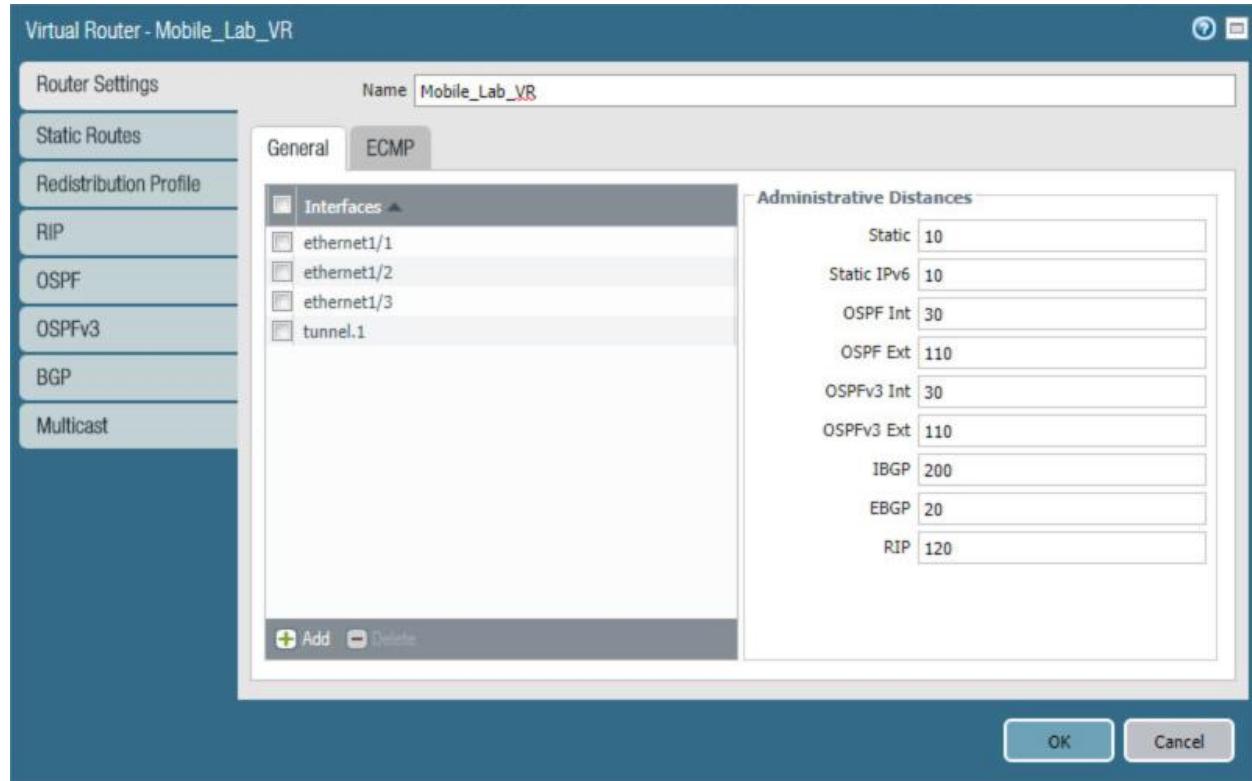
701 Figure 2-42 Virtual Router Configuration



702

6. Select **OK**.

703 Figure 2-43 Virtual Router General Settings



## 704 2.5.5 Configure Tunnel Interface

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

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

708 2. Below the details pane, select **Add**; the Tunnel Interface form will open.

709 3. In the **Tunnel Interface** form on the **Config** tab:

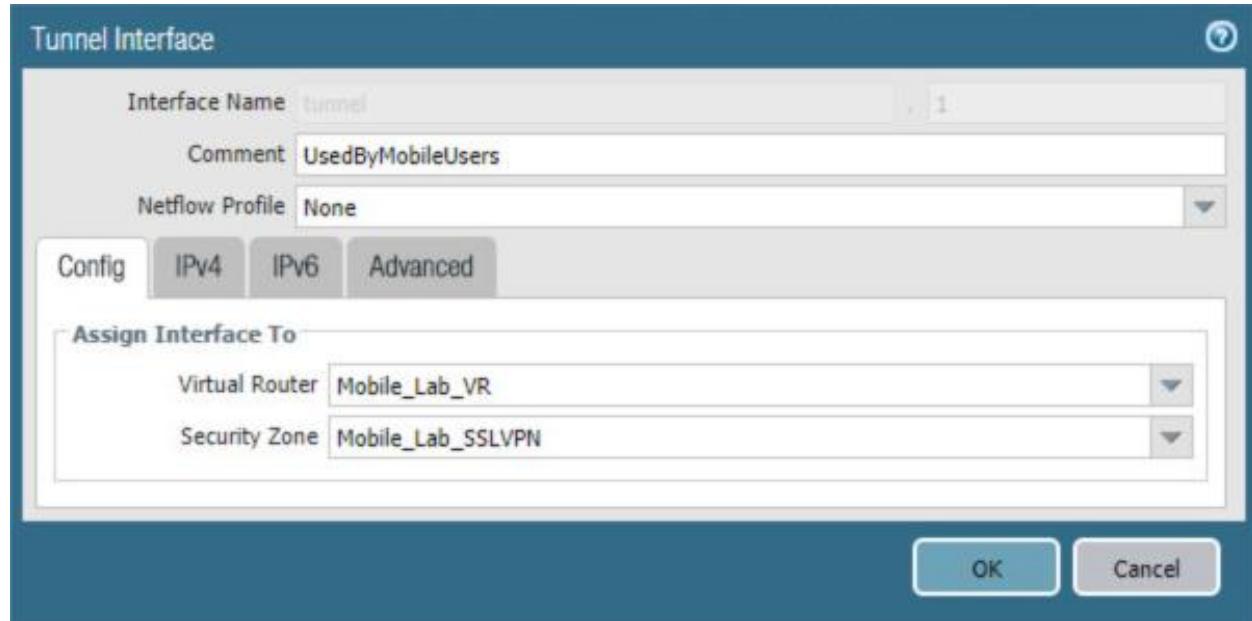
710 a. In the **Assign Interface To** section:

711 i. For the **Virtual Router** drop-down menu, select the virtual router created in the  
712 previous section.

713 ii. For the **Security Zone** drop-down menu, select the security zone created for the  
714 SSL VPN.

715 b. Select **OK**.

716 Figure 2-44 SSL VPN Tunnel Interface

717 

## 2.5.6 Configure Applications and Security Policies

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

723 

### 2.5.6.1 Configure Applications

724 The following steps will create an application:

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

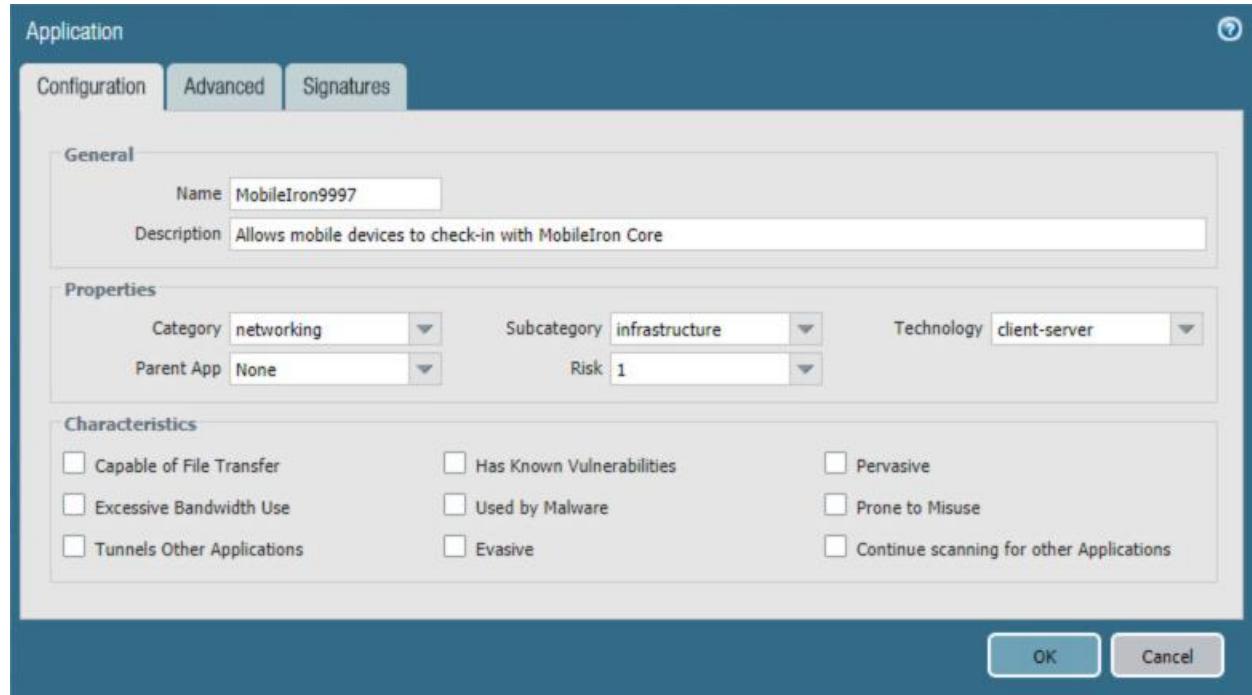
726 Figure 2-45 Application Categories



727

- 728        2. On the **Applications** screen:
- 729        3. Select **Add**; the Application form will open.
- 730        4. On the **Application > Configuration** screen:
  - 731            a. In the **General > Name** field, provide a unique name to identify this application.
  - 732            b. In the **General > Description** field, enter a meaningful description of its purpose.
  - 733            c. For the **Properties > Category** drop-down menu, select a category appropriate to your environment; our sample implementation uses **networking**.
  - 735            d. For the **Properties > Subcategory** drop-down menu, select a subcategory appropriate to your environment; our sample implementation uses **infrastructure**.
  - 737            e. For the **Properties > Technology** drop-down menu, select a technology appropriate to your environment; our sample implementation uses **client-server**.
- 739        5. Select the **Advanced** tab.

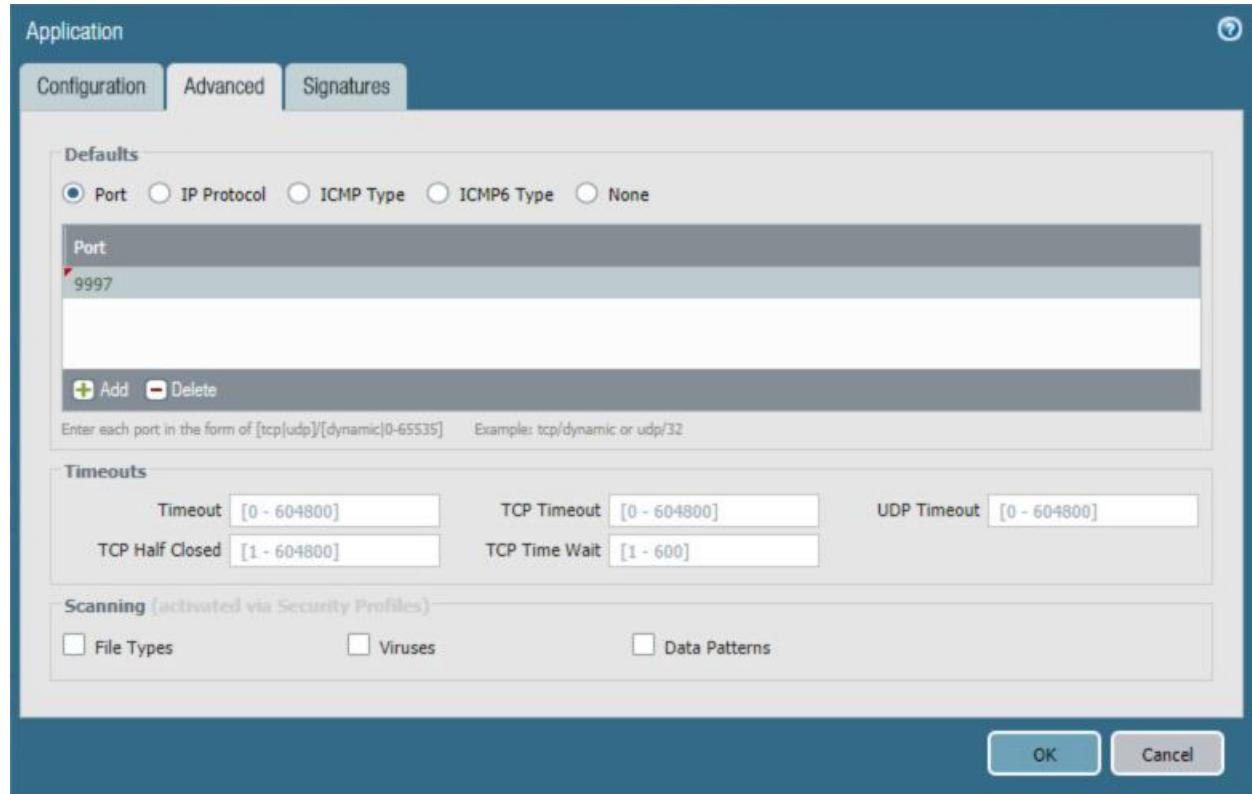
740 Figure 2-46 MobileIron Core Palo Alto Networks Application Configuration



741

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

748 Figure 2-47 MobileIron Application Port Configuration



749        8. Repeat **Steps 2 through 7** with the following modifications to create an application for  
 750        MobileIron Core system administration console:

- 751            a. **Configuration > General > Name is MobileIron8443.**  
 752            b. **Configuration > Default > Category is business-systems.**  
 753            c. **Configuration > Default > Subcategory is management.**  
 754            d. **Advanced > Defaults > Ports > entry\_1 is 8443.**

#### 755        2.5.6.2 *Configure Security Policies*

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

762    [2.5.6.2.1 Create Security Policies](#)

763    To create a security policy:

764        1. In the **Palo Alto Networks Portal**, navigate to **Policies > Security**.

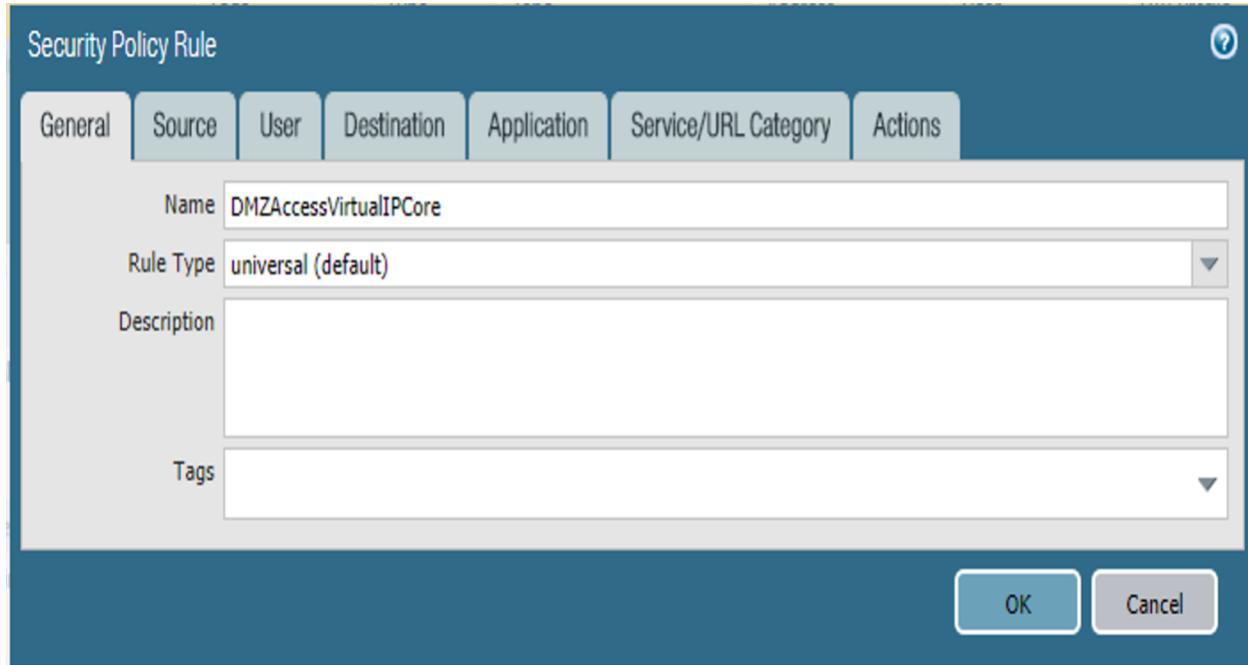
765        2. Select **Add**; the **Security Policy Rule** form will open.

766        3. In the **Security Policy Rule** form:

767            a. In the **Name** field, enter a unique name for this security rule.

768            b. For the **Rule Type** drop-down menu, select the scope of the rule.

769    **Figure 2-48 DMZ Access to MobileIron Firewall Rule Configuration**



770        4. Select the **Source** tab.

771        5. On the **Source** tab:

772            a. If the security rule applies to a specific source zone:

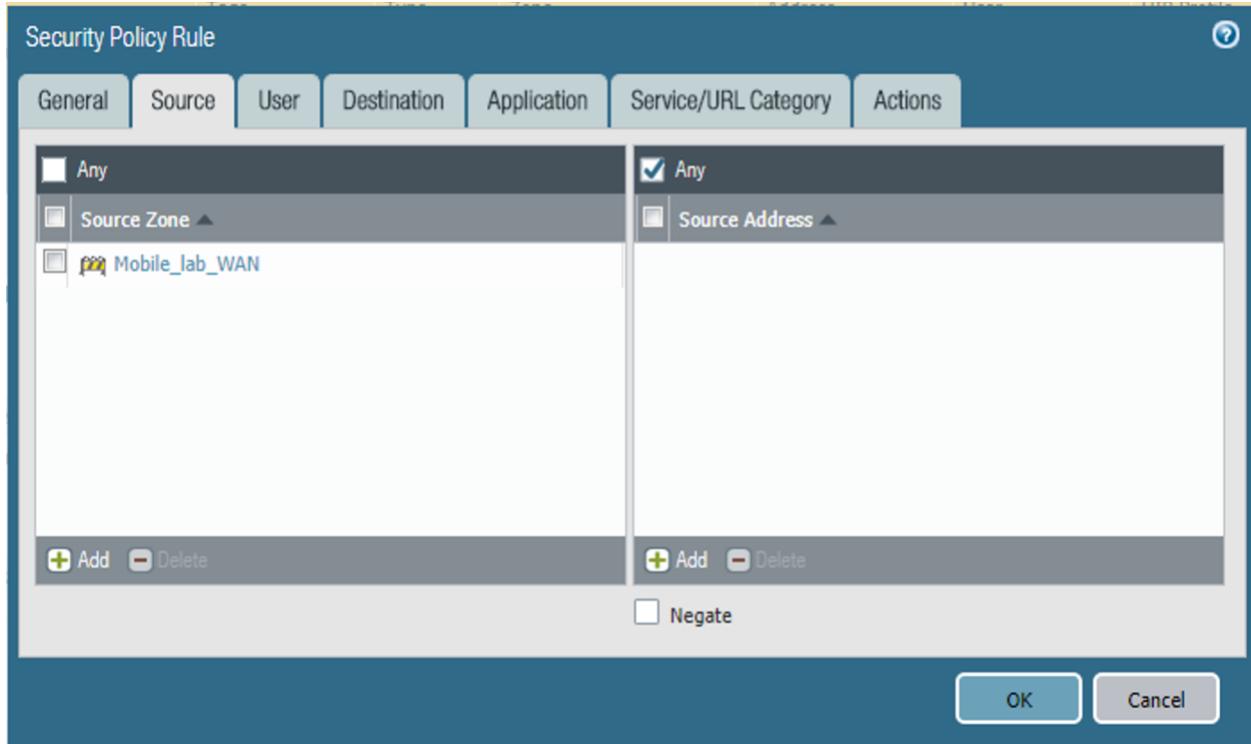
773                i. Under the **Source Zone** list box, select **Add**; a new entry will appear in the list box.

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

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

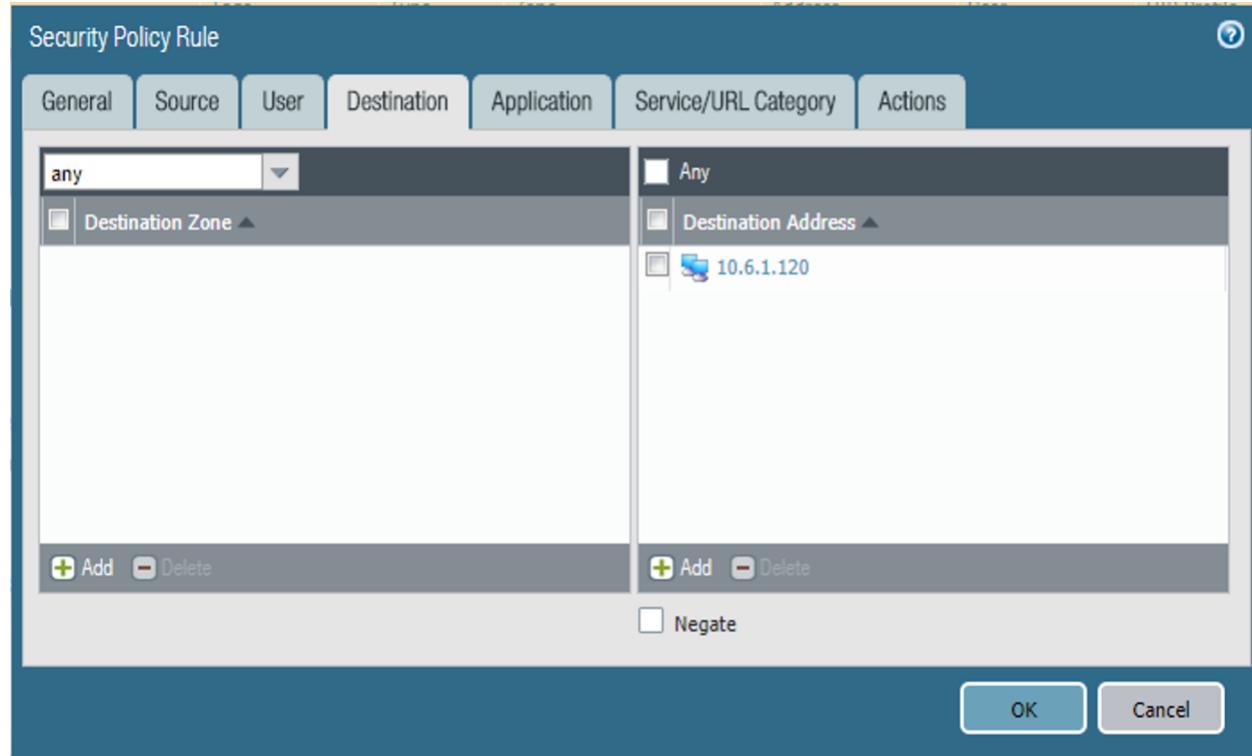
- 776                   i. Under the **Source Address** list box, select **Add**; a new list item will appear.  
777                   ii. For the new list item, select the source address for this rule.

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



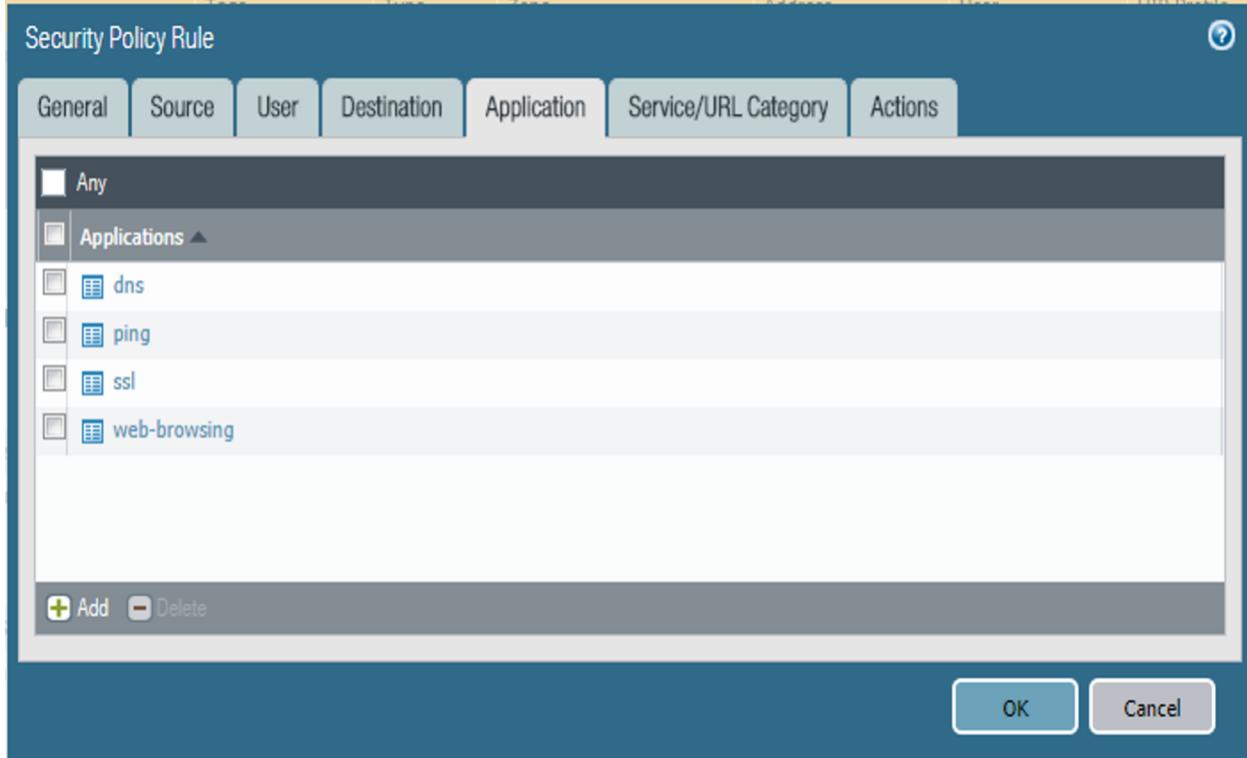
- 779                 6. Select the **Destination** tab.  
780                 7. On the **Destination** tab:  
781                 a. If the security rule applies to a specific destination zone:  
782                   i. Under the **Destination Zone** list box, select **Add**; a new destination list item will  
783                   appear.  
784                   ii. For the new **Source Zone** list item, select the destination zone for this rule.  
785                 b. If the rule applies to only specific destination IP addresses:  
786                   i. Under the **Destination Address** list box, select **Add**; a new list item will appear.  
787                   ii. For the new list item, select the destination address for this rule.

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

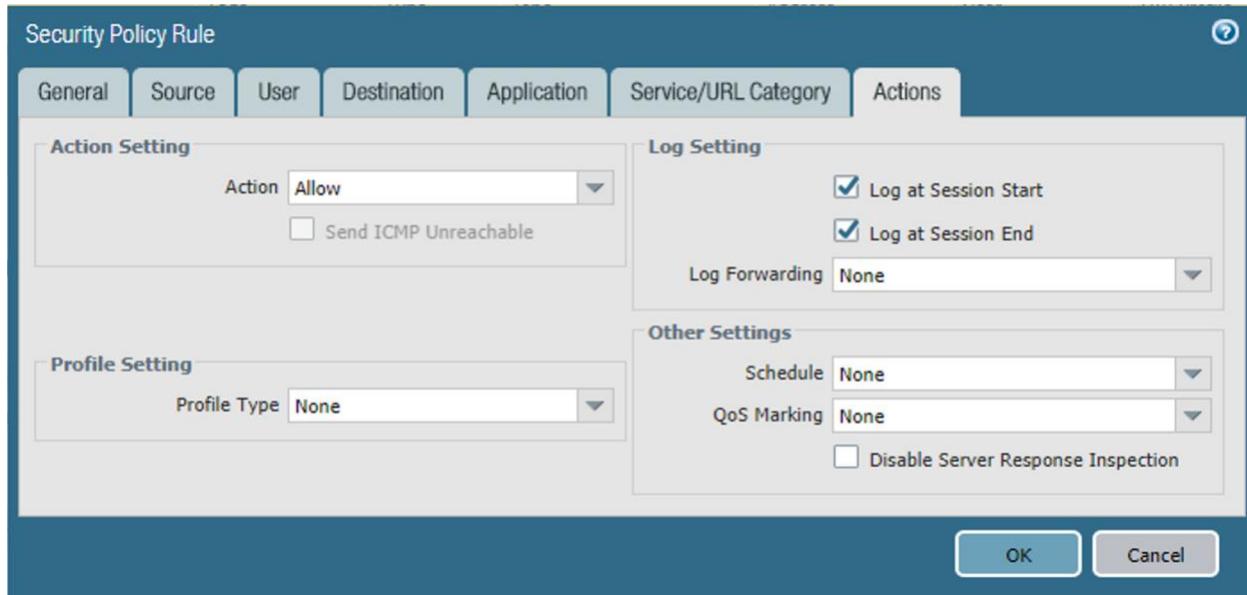
789 8. Select the **Application** tab.790 9. On the **Application** tab:

- 791 a. Under the **Applications** list box, select **Add**; a new list item will appear.
- 792 b. For the new **Applications** list item, select the application representing the protocol and  
793 port combination of the traffic to control.
- 794 c. Repeat **Steps 9a** and **9b** for each application involving the same source and destination  
795 that would also have its traffic allowed or explicitly blocked (if otherwise allowed by a  
796 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**.

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

802 12. Select **OK**.803 **2.5.6.2.2 Implemented Security Policies**

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

806 **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         |

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

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

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

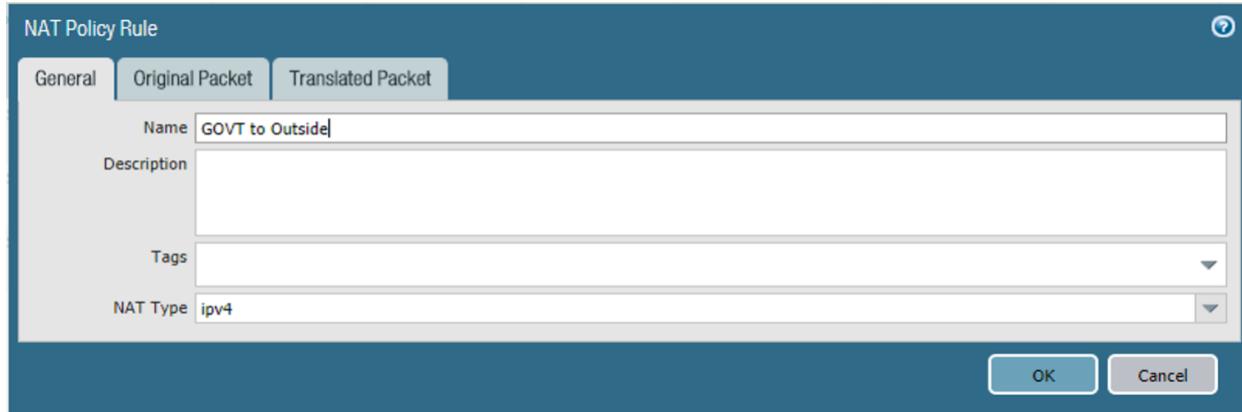
| Name                               | Application                     | Service             | Action | Profile | Options |
|------------------------------------|---------------------------------|---------------------|--------|---------|---------|
| DMZAccessVirtualIPCore             | dns;ping;ssl;web-browsing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

809 **2.5.7 Network Address Translation (NAT)**

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

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

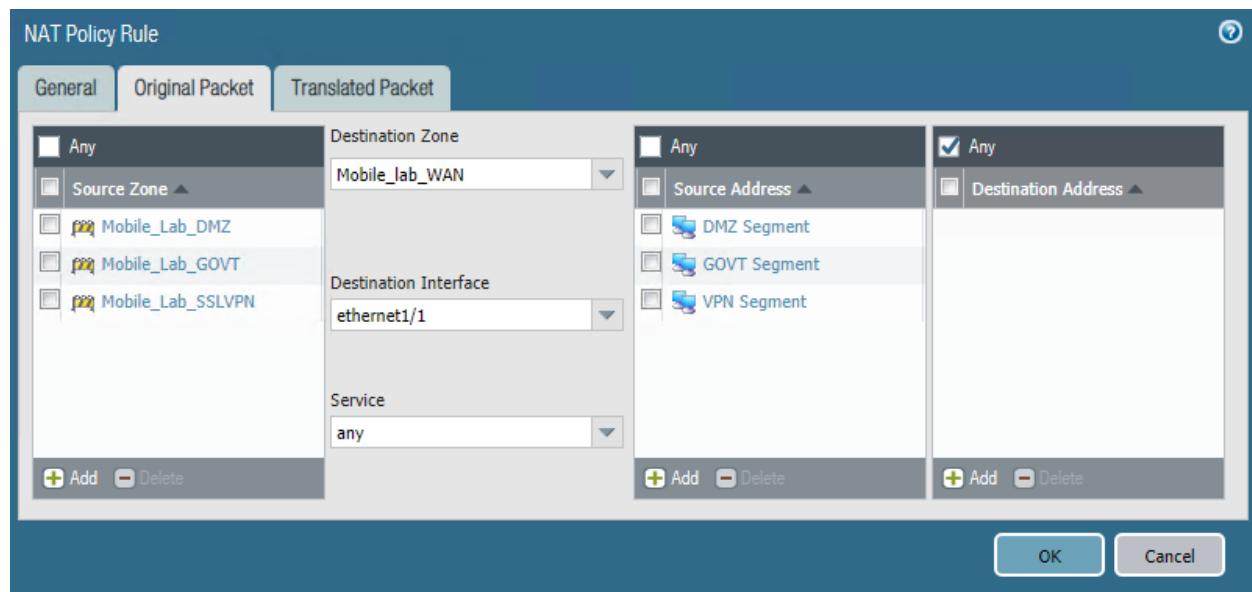
817 **Figure 2-53 Outbound NAT Rule**



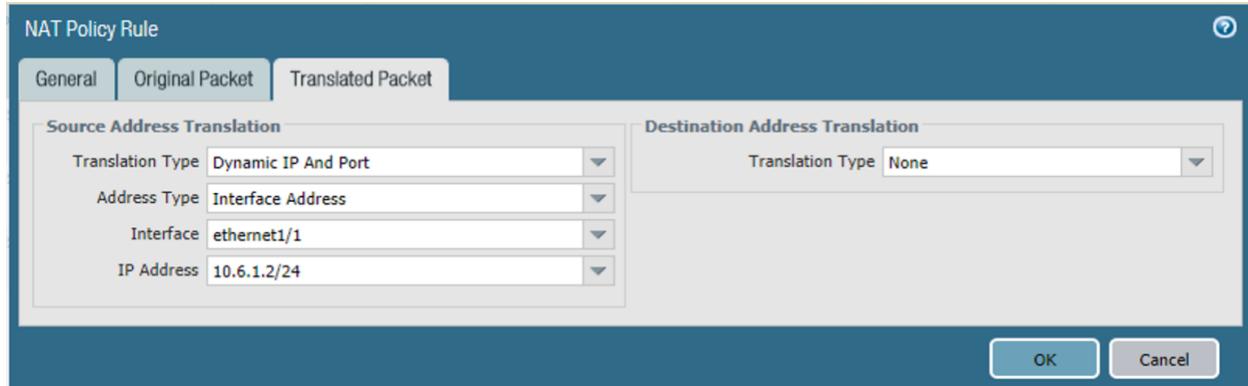
- 818           4. Select the **Original Packet** tab.  
819           5. On the **Original Packet** tab:  
820            a. Under the **Source Zone** list box, select **Add**; a new Source Zone list item will appear.  
821            b. For the new **Source Zone** list item, select the zone that represents your LAN subnet; in  
822            this sample implementation, that is **Mobile\_Lab\_GOVT**.  
823            c. Repeat **Steps 5a** and **5b** to add the zone that represents your DMZ; in this sample  
824            implementation, that is **Mobile\_Lab\_DMZ**.  
825            d. Repeat **Steps 5a** and **5b** to add the zone that represents your SSL VPN; in this sample  
826            implementation, that is **Mobile\_Lab\_SSLVPN**.  
827            e. For the **Destination Zone** drop-down menu, select the zone that represents the  
828            internet; in this sample implementation, that is **Mobile\_lab\_WAN**.  
829            f. For the **Destination Interface**, select the adapter that is physically connected to the  
830            same subnet as your internet gateway; in this sample implementation, that is  
831            **ethernet1/1**.

- 832 g. Under the **Source Address** list box, select **Add**; a new Source Address list item will  
833 appear.
- 834 h. For the new **Source Address** list item, select the address that represents the subnet (IP  
835 address range) for the LAN.
- 836 i. Repeat **Steps 5f** and **5g** to add the address representing the DMZ subnet.
- 837 j. Repeat **Steps 5f** and **5g** to add the address representing the SSL VPN subnet.

838 **Figure 2-54 Outbound NAT Original Packet Configuration**



- 839 6. Select the **Translated Packet** tab.
- 840 7. On the **Translated Packet** tab, under **Source Address Translation**:
- 841 a. For the **Translation Type** drop-down menu, select **Dynamic IP and Port**.
- 842 b. For the **Address Type** drop-down menu, select **Interface Address**.
- 843 c. For the **Interface** drop-down menu, select the same interface selected in **Step 5e**.
- 844 d. For the **IP Address** drop-down menu, select the IPv4 address on the same subnet as  
845 your internet gateway.
- 846

847 **Figure 2-55 Outbound NAT Translated Packet Configuration**

848

849       8. Select **OK**.

## 850 **2.5.8 Configure SSL VPN**

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

### 853 **2.5.8.1 Configure End-User Authentication**

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

#### 856 **2.5.8.1.1 Configured Server Profile**

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

859       1. In the **Palo Alto Networks Portal**, navigate to **Devices > Server Profiles > LDAP**.

860       2. Below the details pane, select **Add**; the **LDAP Server Profile** form will open.

861       3. In the **LDAP Server Profile** form:

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

863           b. Under the **Service List** box, select **Add**; a new **Server List** item will appear.

864           c. In the new **Service List** item:

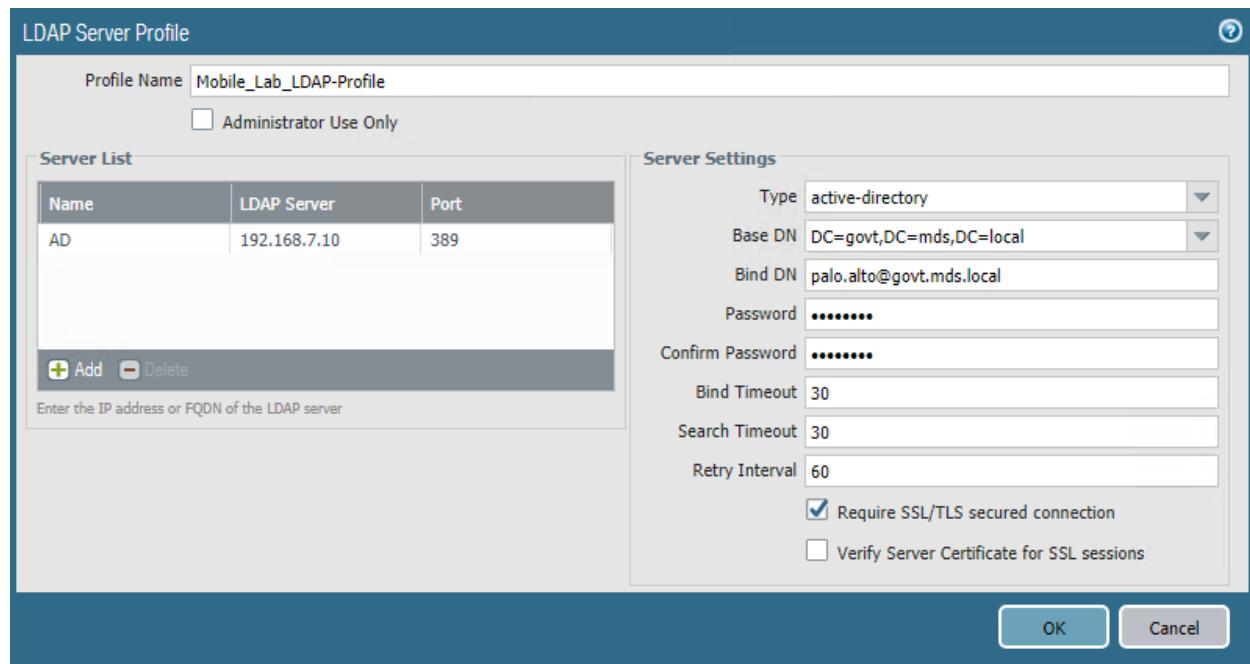
865              i. In the **Name** column, enter a name to identify the server.

866              ii. In the **LDAP Server** column, enter the IP address of the LDAP server.

- 867                   iii. The value in the **Port** column defaults to 389; change this if your LDAP server  
868                   communicates over a different port number.
- 869                   iv. Repeat **Steps 3ci** through **3ciii** for each LDAP server that you intend to use.
- 870                   d. Under **Server Settings**:
- 871                   i. In the **Type** drop-down menu, select **active-directory**.
- 872                   ii. In the **Base DN** drop-down menu, select the DN for your Active Directory domain  
873                   users who will use the SSL VPN.
- 874                   iii. In the **Bind DN** field, enter the Active Directory domain user account that will  
875                   authenticate to LDAP to perform queries.
- 876                   iv. In the **Password** field, enter the password for the Active Directory user account  
877                   specified in the previous step.
- 878                   v. In the **Confirm Password** field, reenter the password entered in the previous step.

879                  4. Select **OK**.

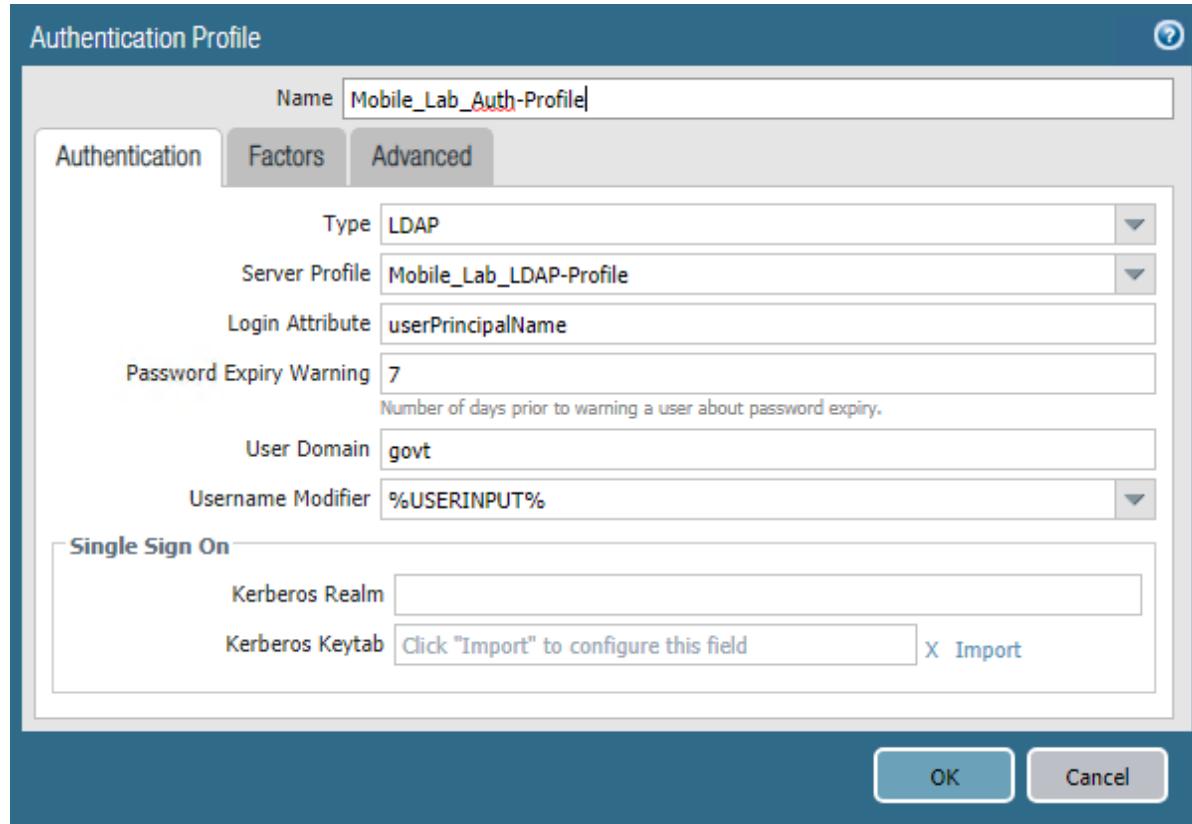
880 **Figure 2-56 LDAP Profile**



881    *2.5.8.2 Configure Authentication Profile*

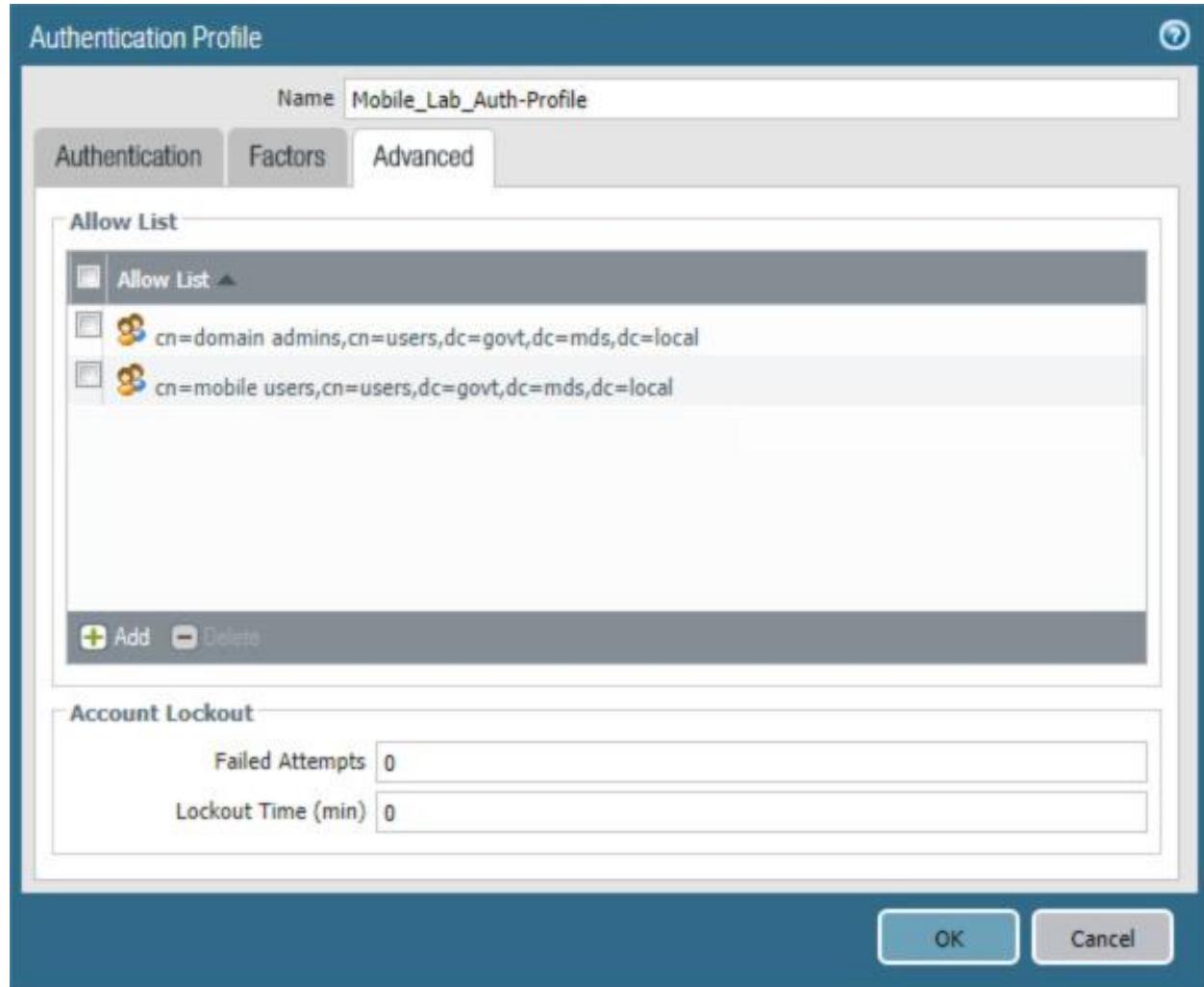
- 882        1. In the **Palo Alto Networks Portal**, navigate to **Device > Authentication Profile**.
- 883        2. Under the details pane, select **Add**; the **Authentication Profile** form will open.
- 884        3. In the **Authentication Profile** form:
  - 885            a. In the **Name** field,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

893    Figure 2-57 Authentication Profile



- 894            c. Select the **Advanced** tab.
- 895            d. On the **Advanced** tab:
- 896              i. Under the **Allow List** box, select **Add**; this will create a new list item.
- 897              ii. In the new list item, select the Active Directory group for your mobile users.
- 898              iii. Repeat **Steps 3di** and **3dii** for any additional groups that should authenticate to the SSL VPN.
- 899
- 900            e. Select **OK**.

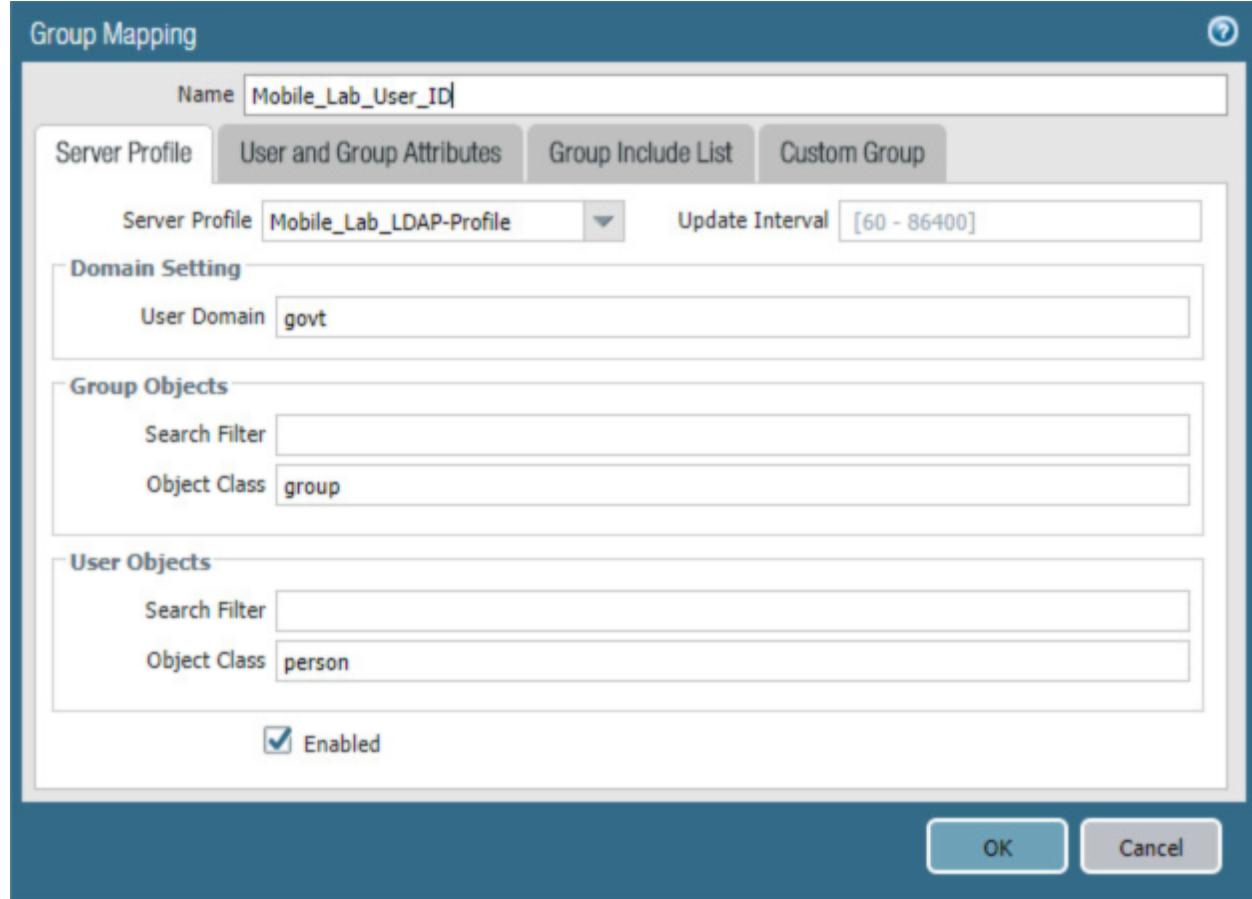
901 Figure 2-58 Advanced Authentication Profile Settings

902 *2.5.8.3 Configure User Identification*

- 903 1. In the **Palo Alto Networks Portal**, navigate to **Device & User Identification**.
- 904 2. In the details pane, select the **Group Mapping Settings** tab.
- 905 3. Below the details pane, select **Add** the **Group Mapping** form will open.
- 906 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:

- 909           i. For the **Server Profile** drop-down menu, select the LDAP Server Profile created  
910           previously.
- 911           ii. For **Domain Setting > User Domain**, enter the name of your Active Directory  
912           domain; this sample implementation uses **govt**.

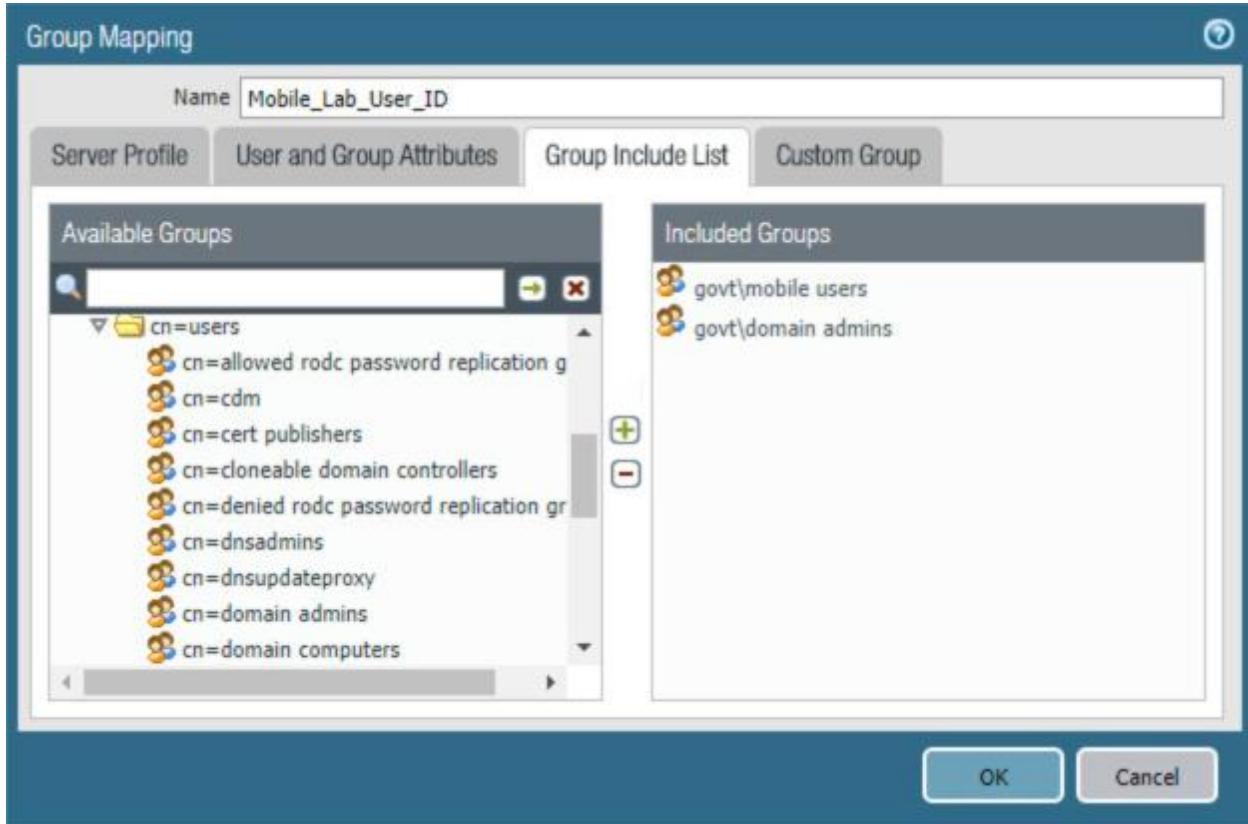
913     Figure 2-59 LDAP Group Mapping



- 914           c. Select the **Group Includes List** tab.
- 915           d. On the **Group Includes List** tab:
- 916           i. In the **Available Groups** list box, expand the Active Directory domain to reveal  
917           configured user groups.
- 918           ii. For each Active Directory group to be included in this User Identification  
919           configuration:
- 920               1) Select the **Active Directory** group.

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

922    Figure 2-60 LDAP Group Include List

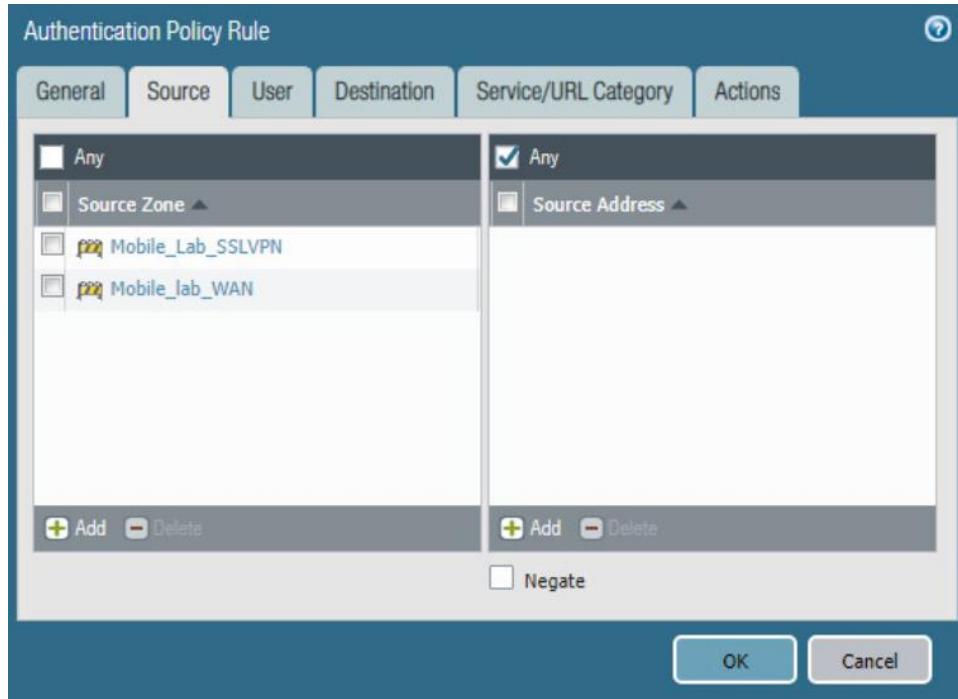


923                    5. Select **OK**.

#### 924    2.5.8.4    *Configure Authentication Policy Rule*

- 925                  1. Navigate to **Policies > Authentication**.
- 926                  2. Click **Add**.
- 927                  3. Give the policy a name. In this implementation, **Mobile\_Lab\_Auth\_Rule** was used.
- 928                  4. Click **Source**.
- 929                  5. Under Source Zone, click **Add**. Select the **SSL VPN** zone.
- 930                  6. Under Source Zone, click **Add**. Select the **WAN** zone.

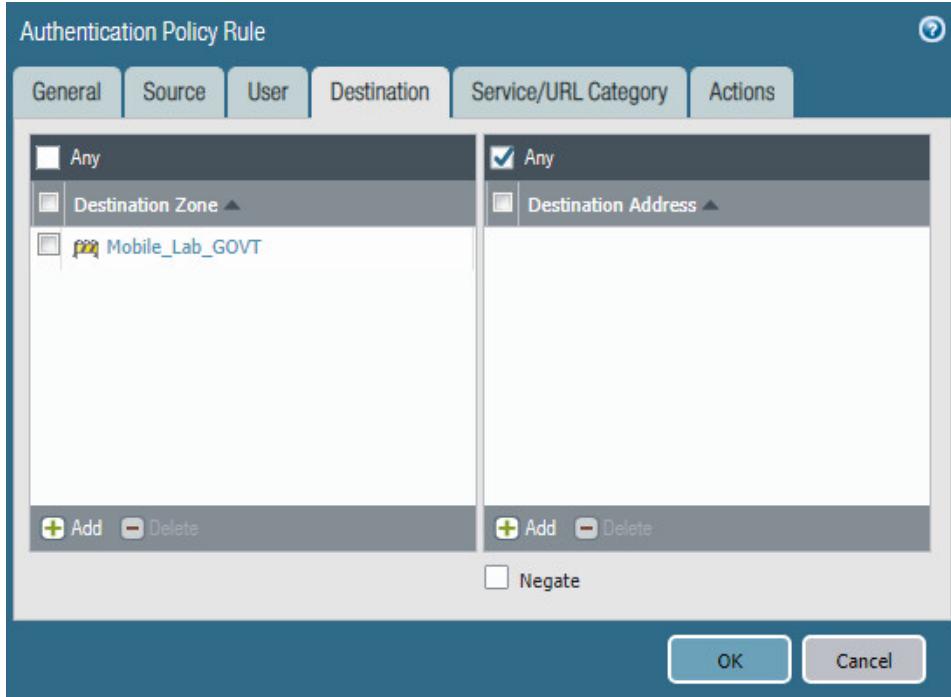
931 Figure 2-61 Authentication Policy Source Zones



932

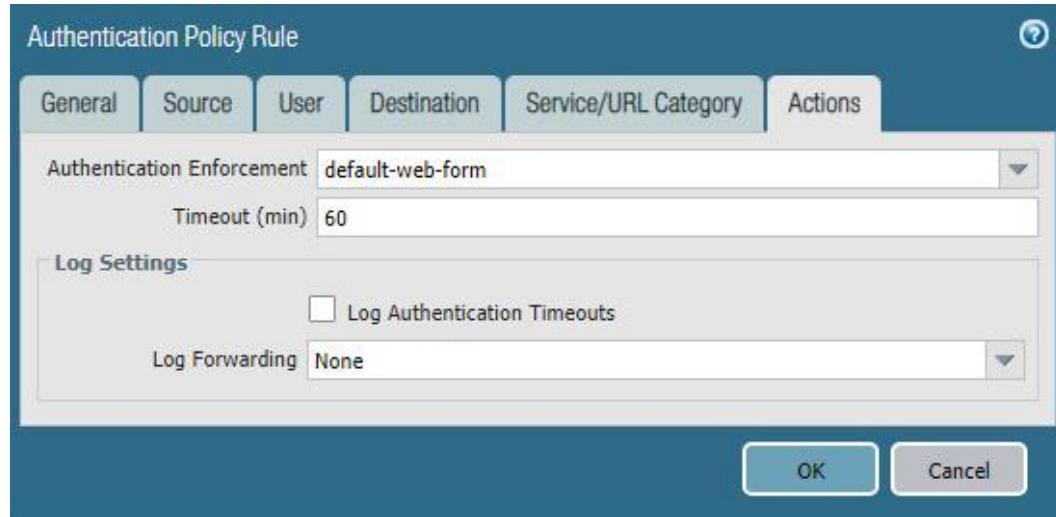
933 7. Click **Destination**.934 8. Under Destination Zone, click **Add**.935 9. Select the **LAN** zone.

936 Figure 2-62 Authentication Policy Destination Zones



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

945 Figure 2-63 Authentication Profile Actions

946 18. Click **OK** and commit the changes.947 

### 2.5.9 Import Certificates

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

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

- 952 1. In the **Palo Alto Networks Portal**, navigate to **Device > Certificate Management >**  
**Certificates**.
- 953 2. Under the details pane, select **Import**; the **Import Certificate** form will open.
- 954 3. In the **Import Certificate** form:
  - 955 a. For the **Certificate Type**, select **Local**.
  - 956 b. For the **Certificate Name** field, enter a unique name to identify this certificate.
  - 957 c. Next to the **Certificate File** field, Select **Browse...** to specify the full path to the file  
 containing the certificate.
  - 958 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.

- 964 e. If the certificate identifies the Palo Alto Networks appliance:
- 965 i. Enable the **Import private key** checkbox.
- 966 ii. Next to **Key File**, select **Browse...** to specify the full path to the file containing the  
967 private key for the uploaded certificate.
- 968 iii. For the **Passphrase** field, enter the pass phrase protecting the private key.
- 969 iv. For the **Confirm Passphrase** field, re-enter the pass phrase protecting the private  
970 key.

971 Figure 2-64 Import MobileIron Certificate



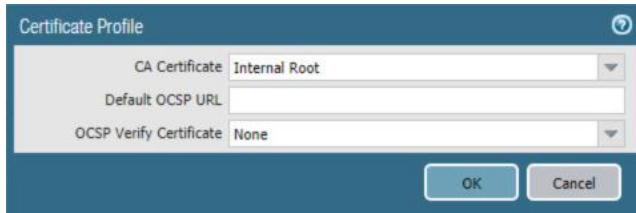
- 972 f. Select **OK**.
- 973 4. Repeat **Step 3** for each certificate to import into the Palo Alto Networks appliance. This will  
974 include all certificates that the appliance will use to identify itself or authenticate to remote  
975 systems, all certificates in the chain of trust for each such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

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

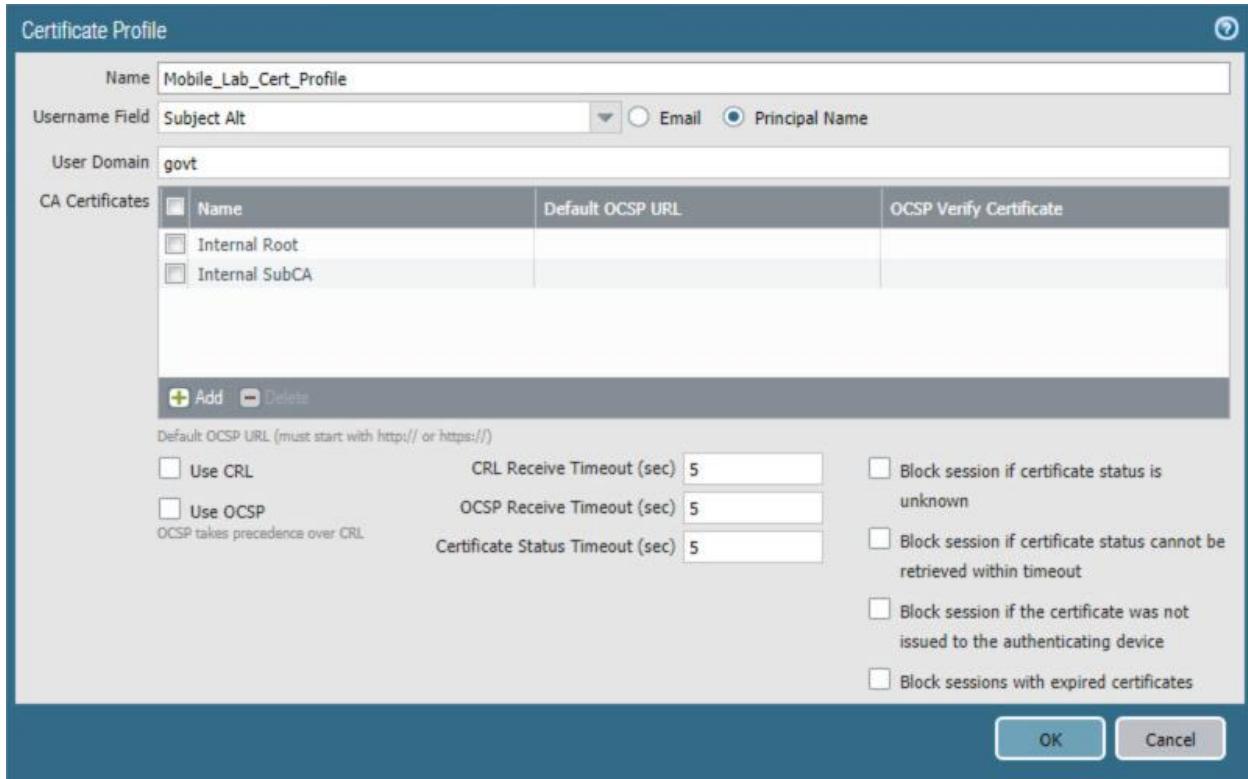
- 979        ▪ server certificate for this appliance issued by DigiCert
- 980        ▪ DigiCert root CA certificate
- 981        ▪ DigiCert subordinate CA certificate
- 982        ▪ Microsoft CA enterprise root certificate
- 983        ▪ Microsoft CA enterprise subordinate CA certificate

984        **2.5.10 Configure Certificate Profile**

- 985        1. In the **Palo Alto Networks Portal**, navigate to **Device > Certificate Management >**  
986            **Certificate Profile**.
- 987        2. Under the details pane, select **Add**; the **Certificate Profile** form will open.
- 988        3. In the **Certificate Profile** form:
  - 989            a. In the **Name** field, enter a unique name to identify this certificate profile.
  - 990            b. In the **Username Field** drop-down menu, select **Subject Alt**.
  - 991            c. Select the **Principal Name** option.
  - 992            d. In the **User Domain** field, enter the Active Directory domain name for your enterprise;  
993            this sample implementation uses **govt**.
  - 994            e. Under the **CA Certificate** list box, select **Add**; a secondary Certificate Profile form will  
995            appear.
  - 996            f. In the secondary **Certificate Profile** form, in the **CA Certificate** drop-down menu, select  
997            the Microsoft Active Directory Certificate Services root certificate uploaded in **Section**  
998            **2.5.6**.
  - 999            g. Select **OK**.
  - 1000          h. Repeat **Step 3f** for each intermediary certificate in the trust chain between the root  
1001            certificate and the subordinate CA certificate that issues certificates to mobile devices.
  - 1002          i. Select **OK**.

1003 **Figure 2-65 Internal Root Certificate Profile**

1004 4. Select OK.

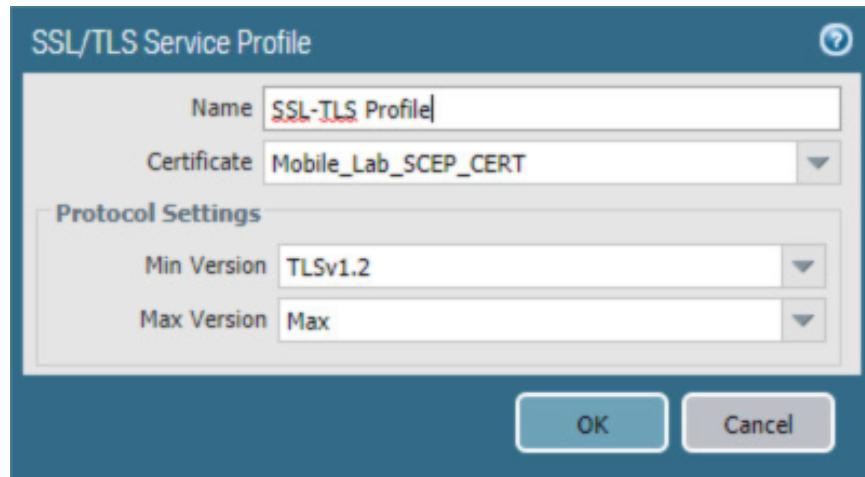
1005 **Figure 2-66 Certificate Profile**1006 **2.5.11 Configure SSL/TLS Service Profile**

1007 The following steps will configure the SSL/TLS profile, which determines what certificates to trust when  
 1008 mobile devices are connecting to the VPN and what certificate to use when establishing outbound  
 1009 SSL/TLS connections.

- 1010 1. In the **Palo Alto Networks Portal**, navigate to **Device > Certificate Management > SSL/TLS**  
 1011 **Service Profile**.

- 1012           2. Below the details pane, select **Add**; the **SSL/TLS Service Profile** form will open.
- 1013           3. In the **SSL/TLS Service Profile** form:
- 1014            a. In the **Name** field, enter a unique name to identify this service profile.
- 1015            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.
- 1016            c. For the **Min Version** drop-down menu, select **TLSv1.2**.
- 1017            d. Select **OK**.

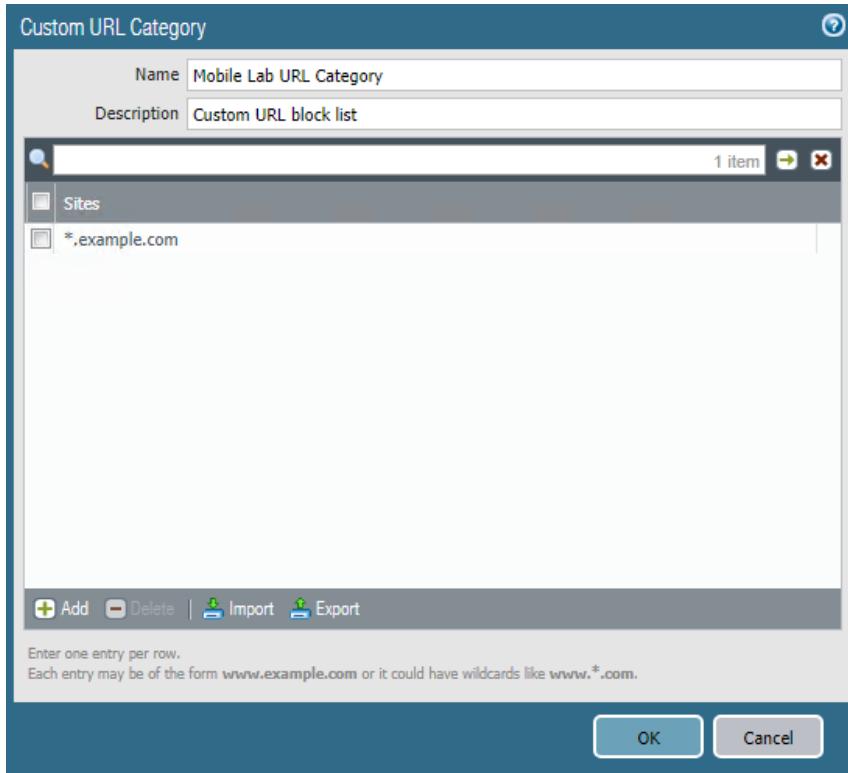
1020 **Figure 2-67 SSL/TLS Service Profile**



- 1021           4. Repeat **Step 3** to add an identical SSL/TLS service profile for this appliance's server  
1022           certificate issued through DigiCert.

### 1023 **2.5.12 URL Filtering Configuration**

- 1024        1. Navigate to **Objects > Custom Objects > URL Category**.
- 1025        2. Click **Add**.
- 1026        3. Give the category a name and description.
- 1027        4. Add sites to be blocked. For this example, \*.example.com was used.

1028 **Figure 2-68 Custom URL Category**

- 1029        5. Click **OK**.
- 1030        6. Navigate to **Objects > Security Profiles > URL Filtering**.
- 1031        7. Check the box next to default and click **Clone**.
- 1032        8. Select **default** from the window that appears.
- 1033        9. Click **OK**.
- 1034        10. Click the newly created profile, **default-1**.
- 1035        11. Give the policy a meaningful name and description.
- 1036        12. Scroll to the bottom of the list. The name of the created category will be last on the list.
- 1037        13. Click the option below **Site Access** and next to your created URL category.
- 1038        14. Set the Site Access option to **block**.

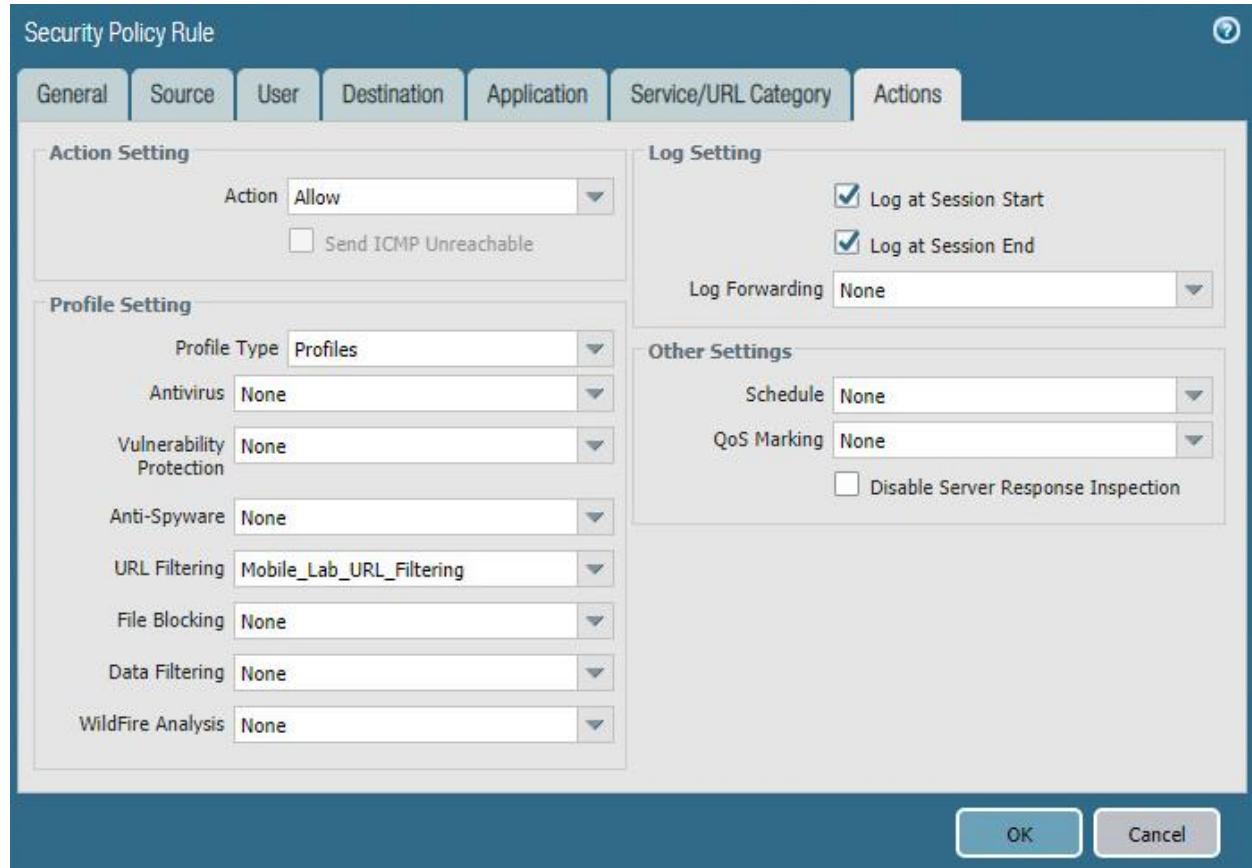
1039 **Figure 2-69 URL Filtering Profile**

| Category  | Site Access | User Credential Submission |
|---|-------------|----------------------------|
| adult-and-inappropriate-content                               | allow       | allow                      |
| training-and-tools  | allow       | allow                      |
| translation   | allow       | allow                      |
| travel  | allow       | allow                      |
| unknown   | allow       | allow                      |
| weapons   | allow       | allow                      |
| web-advertisements  | allow       | allow                      |
| web-based-email   | allow       | allow                      |
| web-hosting   | allow       | allow                      |
| <input checked="" type="checkbox"/> Mobile Lab URL Category * | block       | block                      |

\* indicates a custom URL category, + indicates external dynamic list  
Check URL Category

- 1040        15. Click **OK**.
- 1041        16. Navigate to **Policies > Security**.
- 1042        17. Click the default outbound policy for the internal network (not VPN).
- 1043        18. Click **Actions**.
- 1044        19. Next to Profile Type, select **Profiles**.
- 1045        20. Next to URL Filtering, select the newly created profile.
- 1046        21. Click **OK**.
- 1047        22. Repeat **Steps 18** through **21** for the SSL VPN outbound traffic.

1048 Figure 2-70 URL Filtering Security Policy



1049 23. Commit the changes.

### 2.5.13 GlobalProtect Gateway and Portal Configuration

1051 The SSL VPN configuration requires creation of both a GlobalProtect gateway and a GlobalProtect portal,  
 1052 the latter of which could be used to manage VPN connections across multiple gateways. In this sample  
 1053 implementation, only a single gateway and portal are configured.

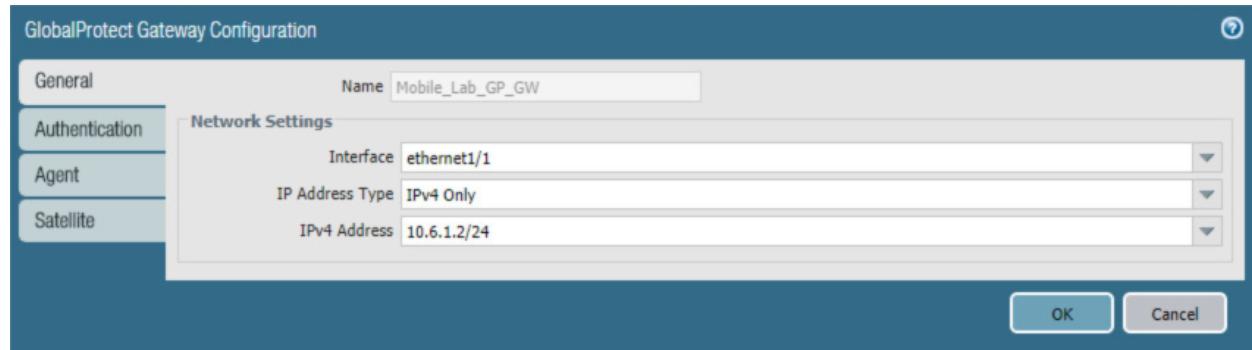
#### 2.5.13.1 Configure GlobalProtect Gateway

1055 The GlobalProtect gateway provides remote users with secure access to internal resources based on  
 1056 their Microsoft AD group. To configure the GlobalProtect gateway:

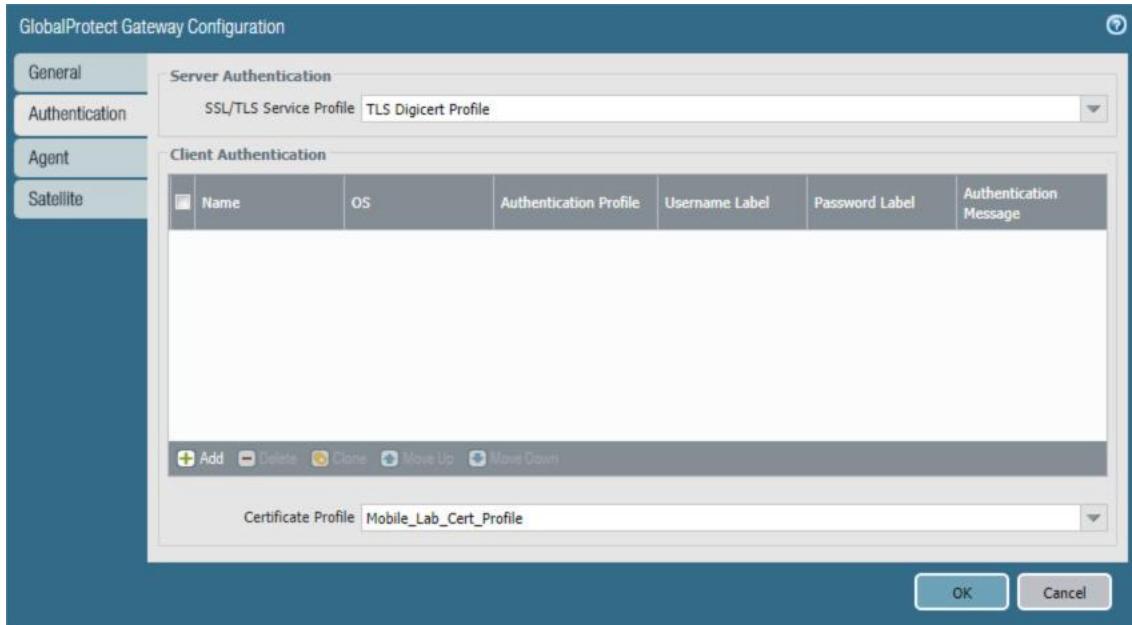
- 1057 1. In the **Palo Alto Networks Portal**, navigate to **Network > GlobalProtect > Gateways**.
- 1058 2. Below the details pane, select **Add**; the **GlobalProtect Gateway Configuration** form will  
 1059 open.

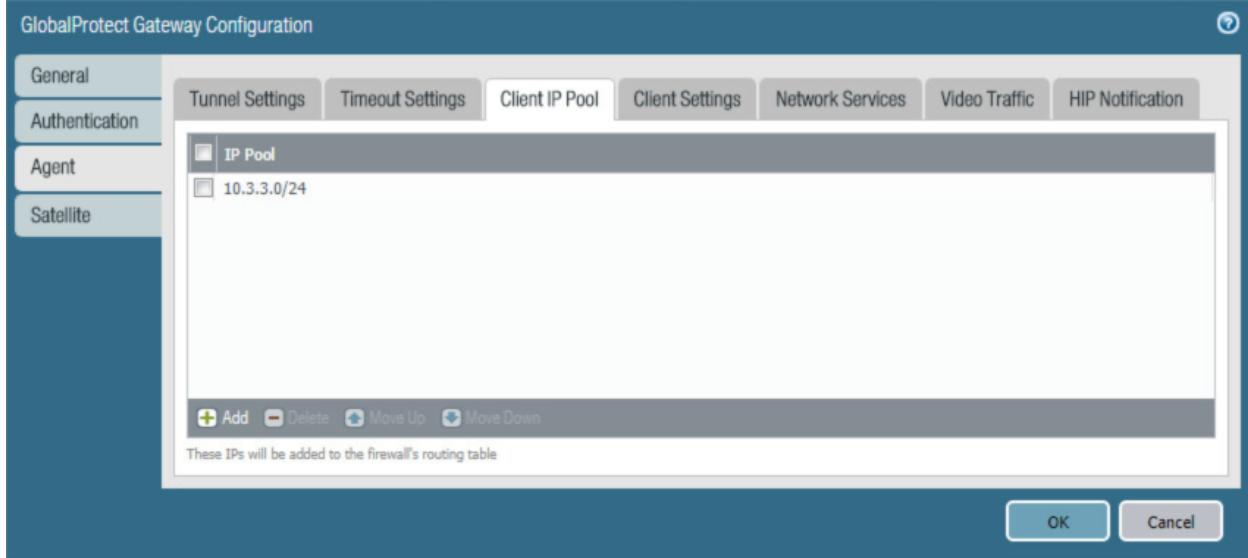
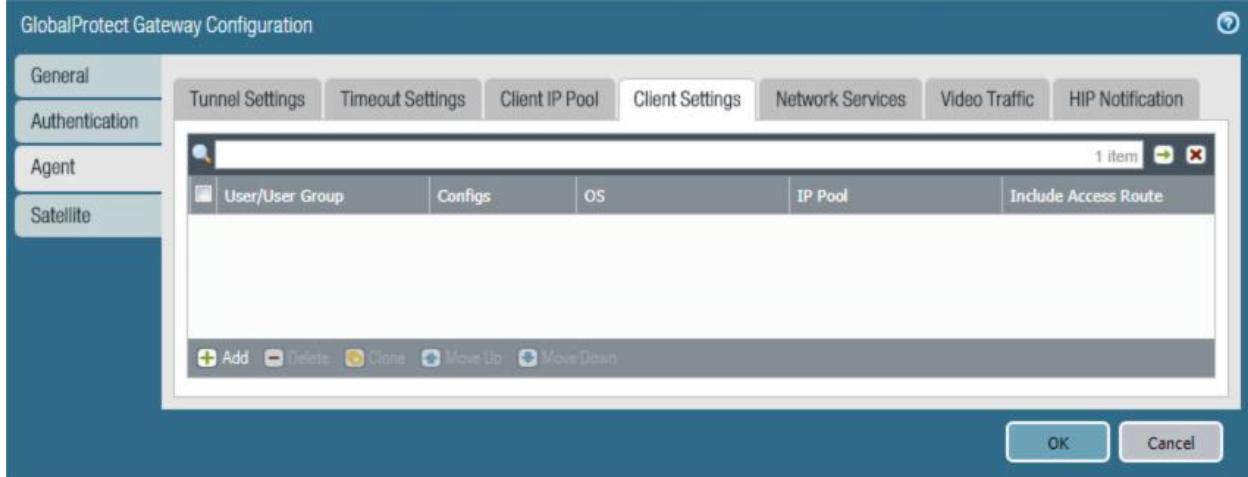
- 1060           3. In the **GlobalProtect Gateway Configuration** form, on the **General** tab:
- 1061            a. In the **Name** field, enter a unique name to identify this GlobalProtect Gateway.
- 1062            b. Under **Network Settings**:
- 1063              i. In the **Interface** drop-down menu, select the physical interface connected to the  
1064                 subnet on which the internet gateway device is located.
- 1065              ii. In the **IPv4 Address** drop-down menu, select the IP address associated with the  
1066                 physical interface specified in the previous step.

1067          Figure 2-71 General GlobalProtect Gateway Configuration

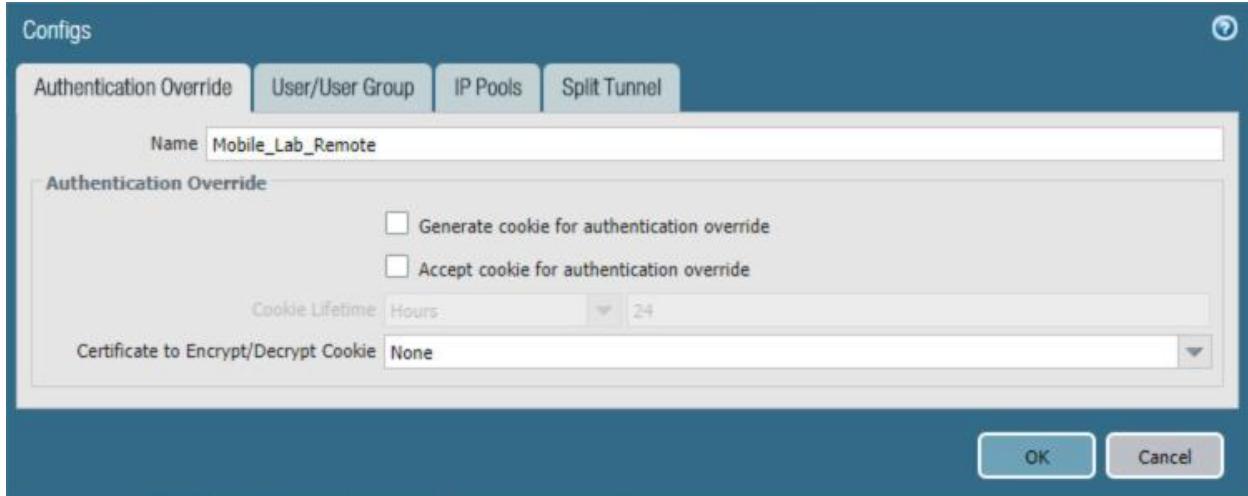


- 1068           c. Select the **Authentication** tab.
- 1069           d. In the **Authentication** tab:
- 1070              i. For the **Server Authentication > SSL/TLS Service Profile** drop-down menu, select  
1071                 the TLS/SSL profile associated with the publicly trusted server certificate for this  
1072                 appliance.
- 1073              ii. For the **Client Authentication > Certificate Profile** drop-down menu, select the  
1074                 client TLS/SSL profile associated with the internally trusted client certificates  
1075                 issued to mobile devices.

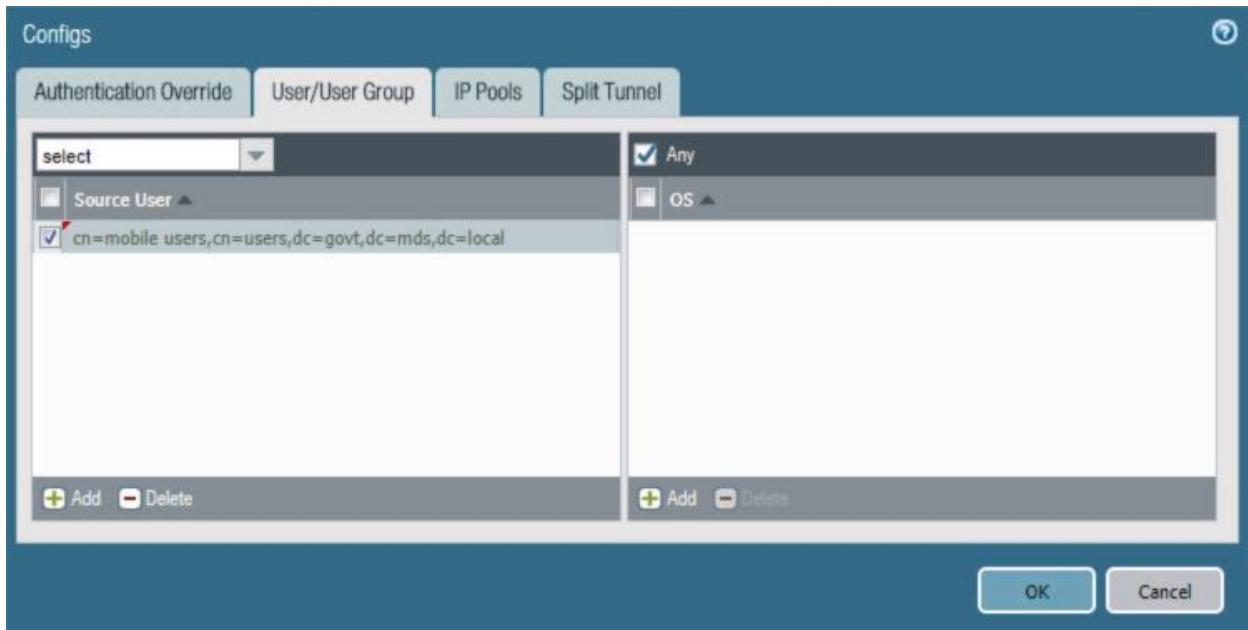
1076 **Figure 2-72 GlobalProtect Authentication Configuration**1077 e. Select the **Agent** tab.1078 f. On the **Agent > Tunnel Settings** tab:1079 i. Select the **Tunnel Mode** checkbox.1080 ii. Select the **Enable IPSec** checkbox to disable IPSec.1081 **Figure 2-73 GlobalProtect Tunnel Configuration**1082 g. Select the **Agent > Client IP Pool** tab.1083 h. On the **Agent > Client IP Pool** tab:1084 i. Below the **IP Pool** list box, select **Add**; a new list item will appear.1085 ii. For the new **IP Pool** list item, enter the network address for the IP address pool  
1086 from which connected devices will be allocated an IP address.

1087 **Figure 2-74 VPN Client IP Pool**1088 i. Select the **Agent > Client Settings** tab.1089 j. On the **Agent > Client Settings** tab:1090 i. Under the **Client Settings** list box, select **Add**; the **Configs** form will open.1091 **Figure 2-75 VPN Client Settings**1092 ii. In the **Configs** form on the **Authorization Override** tab, enter a unique name to  
1093 identify this client configuration.

1094 Figure 2-76 VPN Authentication Override Configuration

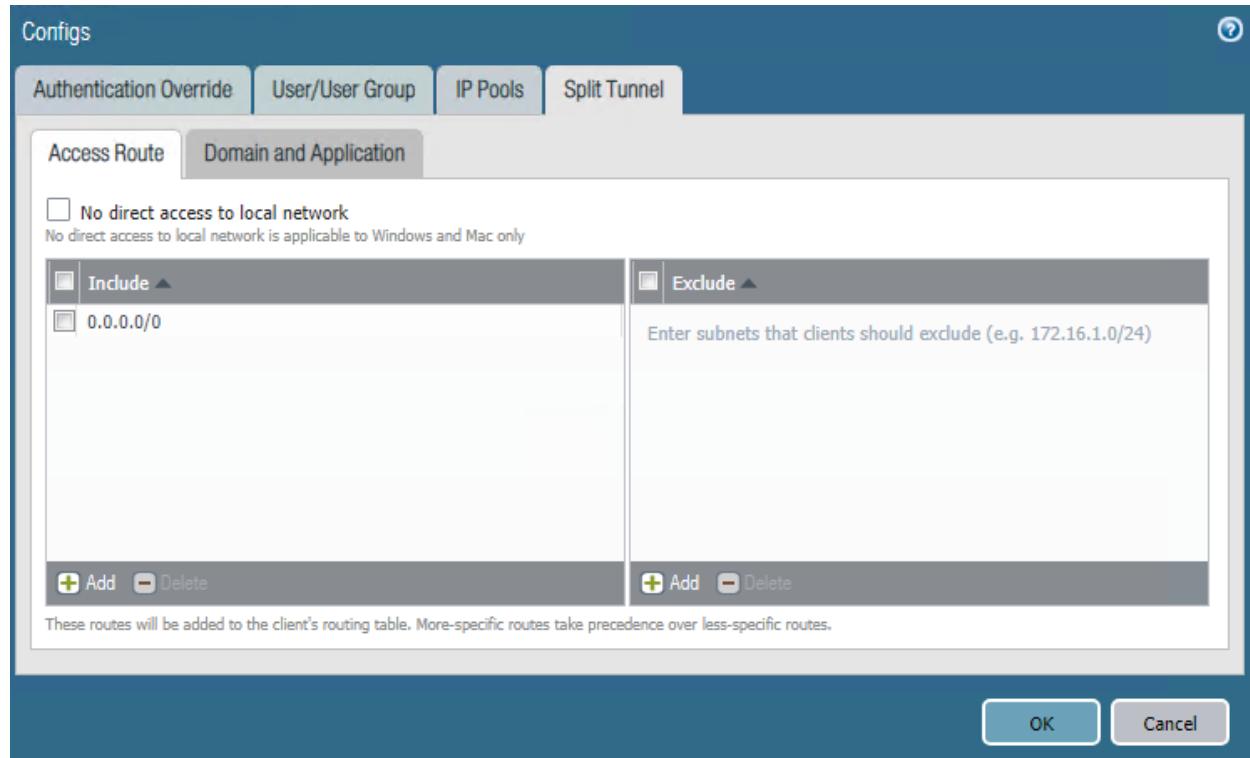
1095 iii. Select the **User/User Group** tab.1096 iv. On the **User/User Group** tab:1097 1) Below the **Source User** list box, select **Add**; a new list item will appear.1098 2) In the **Source User** list item, select the Microsoft AD user group to grant  
1099 access to internal resources through this GlobalProtect gateway.

1100 Figure 2-77 VPN User Group Configuration



- 1101                         v. Select the **Split Tunnel** tab.
- 1102                         vi. On the **Split Tunnel** tab, on the **Access Route** tab:
- 1103                             1) Under the **Include** list box, select **Add**; a new list item will appear.
- 1104                             2) In the new **Include** list item, enter **0.0.0.0/0**. This enforces full tunneling.

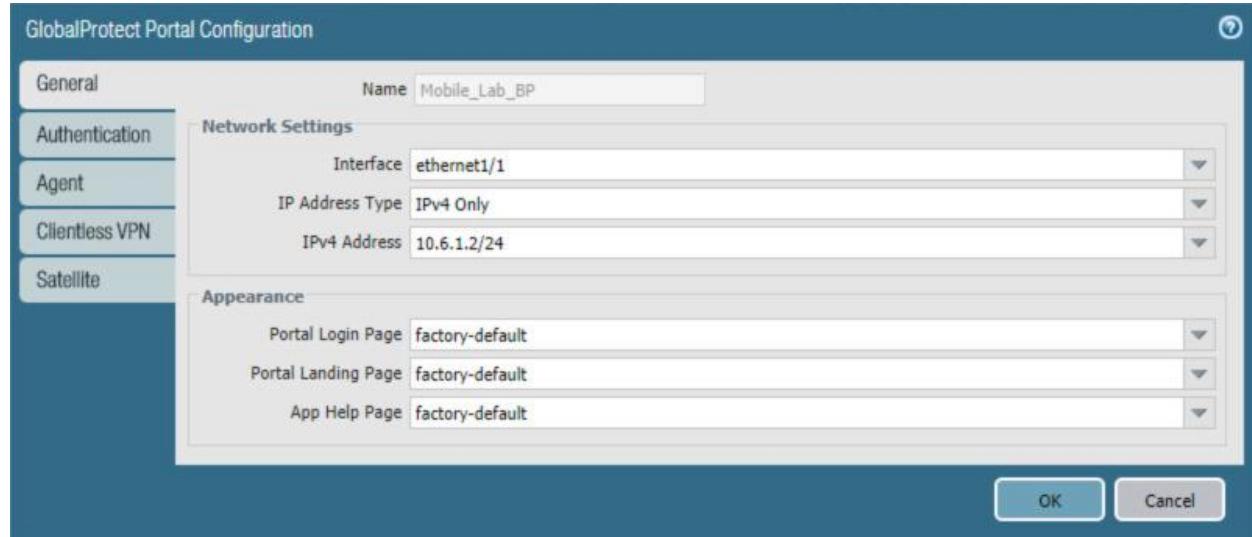
1105 **Figure 2-78 VPN Split Tunnel Configuration**



- 1106                         vii. Select **OK**.
- 1107                         k. Select **OK**.
- 1108 **2.5.13.2 Configure GlobalProtect Portal**
- 1109                         1. In the **Palo Alto Networks Portal**, navigate to **Network > GlobalProtect > Portal**.
- 1110                         2. Below the details pane, select **Add**; the **GlobalProtect Portal Configuration** form will open.
- 1111                         3. In the **GlobalProtect Portal Configuration** form, on the **General** tab:
- 1112                             a. In the **Name** field, enter a unique name to identify this GlobalProtect portal.

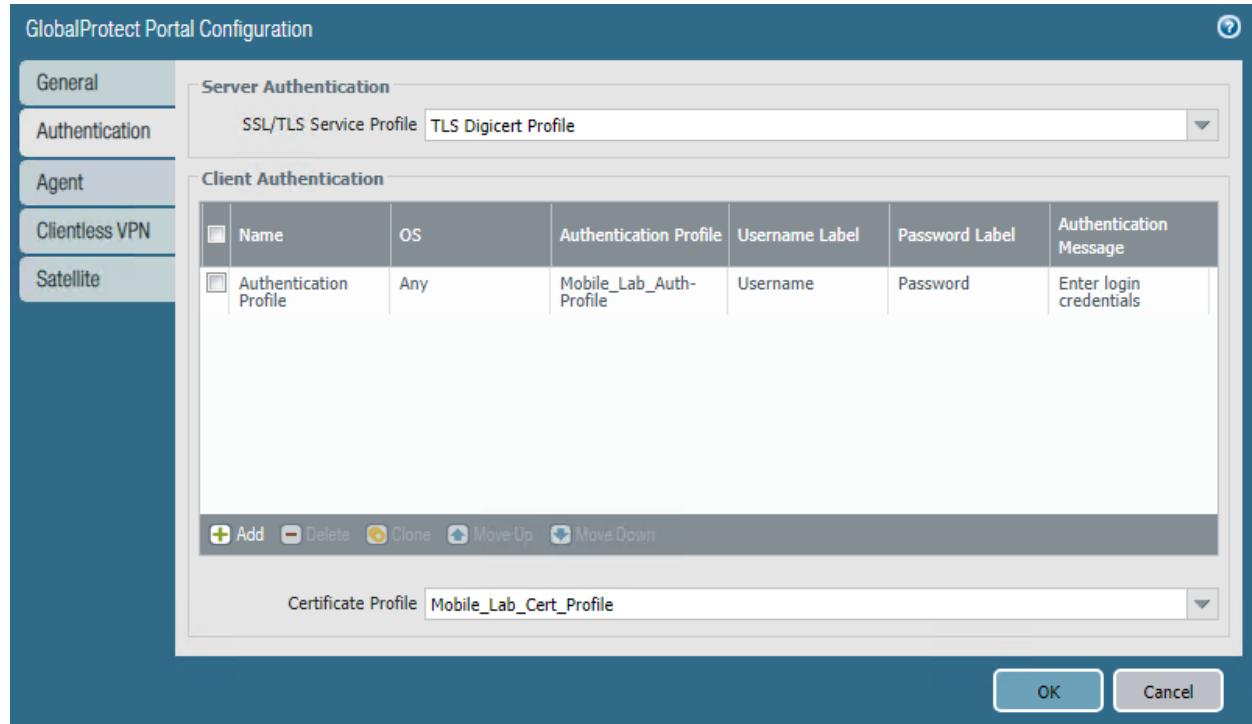
- 1113            b. In the **Interface** drop-down menu, select the physical interface connected to the subnet  
1114            on which the internet gateway device is located.
- 1115            c. In the **IP Address Type** drop-down menu, select **IPv4 Only**.

1116      **Figure 2-79 GlobalProtect Portal Configuration**



- 1117            4. Select the **Authentication** tab.
- 1118            5. In the **Authentication** tab:
- 1119            a. For the **Server Authentication > SSL/TLS Service Profile** drop-down menu, select the  
1120            SSL/TLS service profile based on your third-party server certificate.
- 1121            b. For the **Certificate Profile** drop-down menu, select the client TLS/SSL profile associated  
1122            with the internally trusted client certificates issued to mobile devices.
- 1123            c. Click **Add**.
- 1124            d. Enter a profile name. In this example implementation, Client Authentication was used.
- 1125            e. For the **Authentication Profile** drop-down menu, select the previously created  
1126            authentication profile.
- 1127            f. Click **OK**.

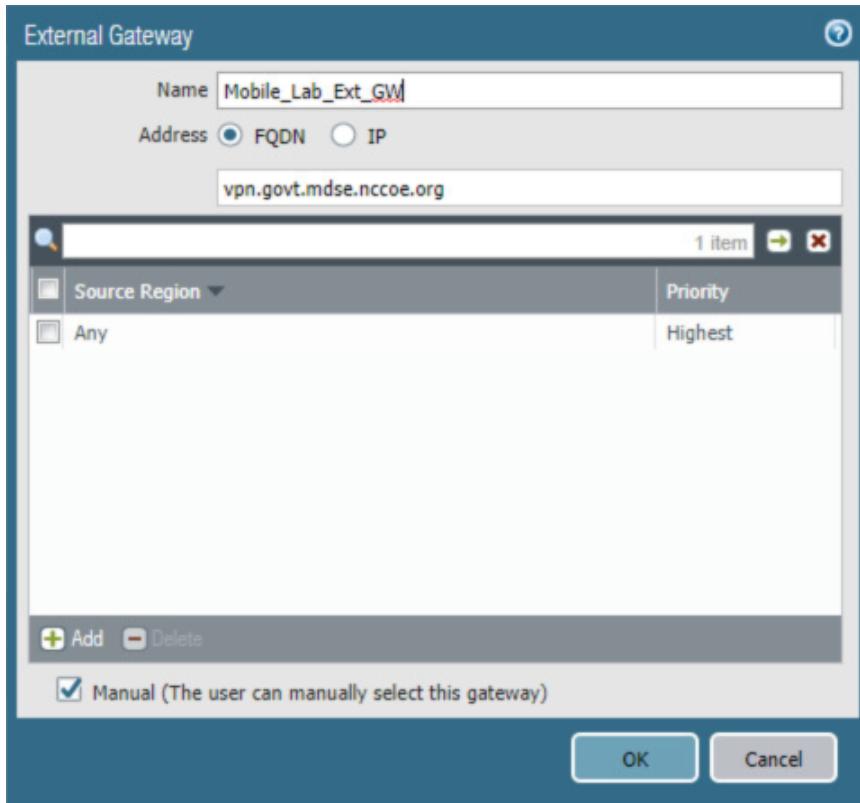
1128 Figure 2-80 GlobalProtect Portal SSL/TLS Configuration



- 1129        6. Select the **Agent** tab.
- 1130        7. On the **Agent** tab:
- Below the **Agent** list box, select **Add**; the **Configs** form will open.
  - In the **Configs** form:
    - In the **Authentication** tab, below **Components that Require Dynamic Passwords**, check the box next to **Portal**.
    - In the **External** tab, under the **External Gateways** list box select **Add**; the **External Gateway** form will open.
    - In the External Gateway form:
      - In the **Name** field, enter a unique name to identify this external gateway.
      - For the **Address** option, enter the FQDN for this appliance; in this sample implementation, the FQDN is **vpn.govt.mdse.nccoe.org**.
      - Below the **Source Region** list box, select **Add**; a new list item will appear.

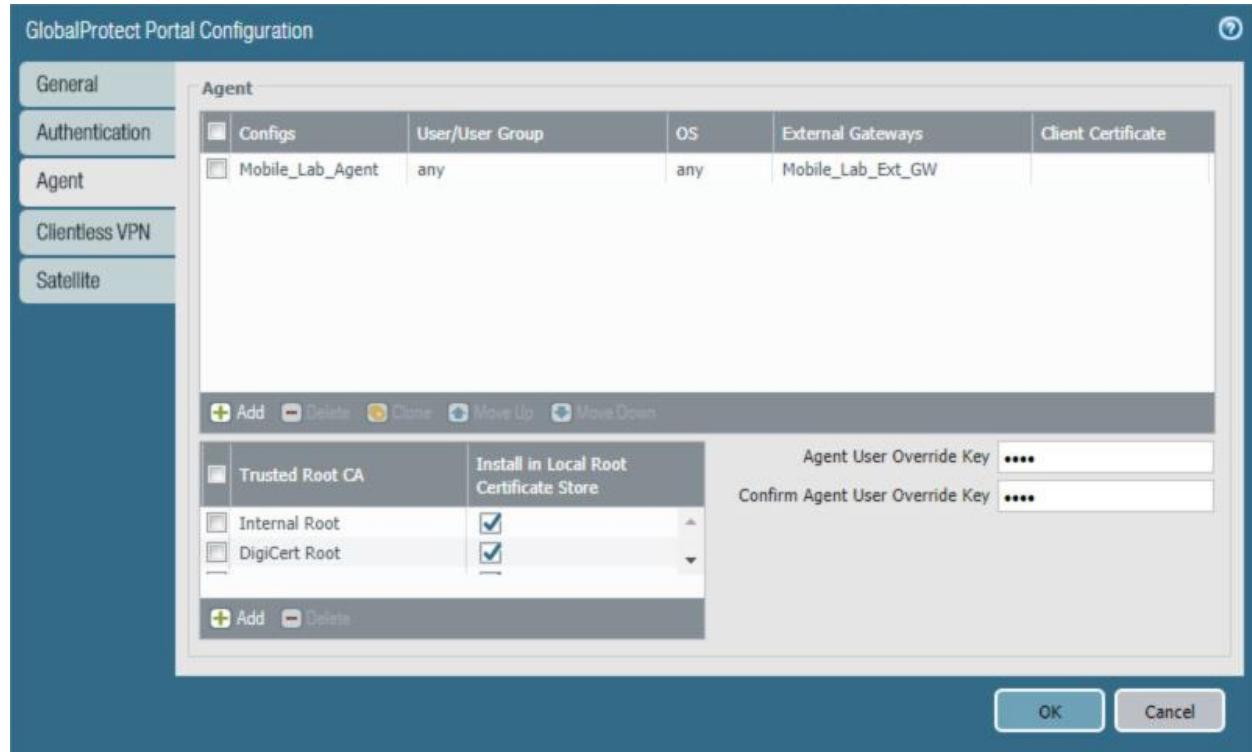
- 1142                   4) In the new **Source Region** list item, select **Any**.
- 1143                   5) Select the **Manual** checkbox.
- 1144                   6) Select **OK**.

1145   Figure 2-81 GlobalProtect External Gateway Configuration



- 1146                   iv. Below the **Trusted Root CA** list box, select **Add**; a new list item will appear.
- 1147                   v. In the new **Trusted Root CA** list item, select your internal CA root certificate.
- 1148                   vi. Repeat **Steps 7biii** and **7biv** to add each certificate in your internal or third-party  
1149                   certificate trust chains used when mobile devices contact the GlobalProtect  
1150                   portal.
- 1151                   c. Click **App**. Ensure that Connect Method is set to **User-logon (Always On)**.

1152 Figure 2-82 GlobalProtect Portal Agent Configuration

1153 d. Select **OK**.

## 1154 2.5.14 Configure Automatic Threat and Application Updates

- 1155 1. In the **PAN-OS portal**, navigate to **Device > Dynamic Updates**.
- 1156 2. Click **Check Now** at the bottom of the page.
- 1157 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.
- 1159 4. When the download completes, click **Done**.
- 1160 5. Click **Install** next to the downloaded update.
- 1161 6. Click **Continue Installation**.
- 1162 7. When installation completes, click **Close**.
- 1163 8. Next to Schedule, click the link with the date and time.

1164 Figure 2-83 Schedule Link

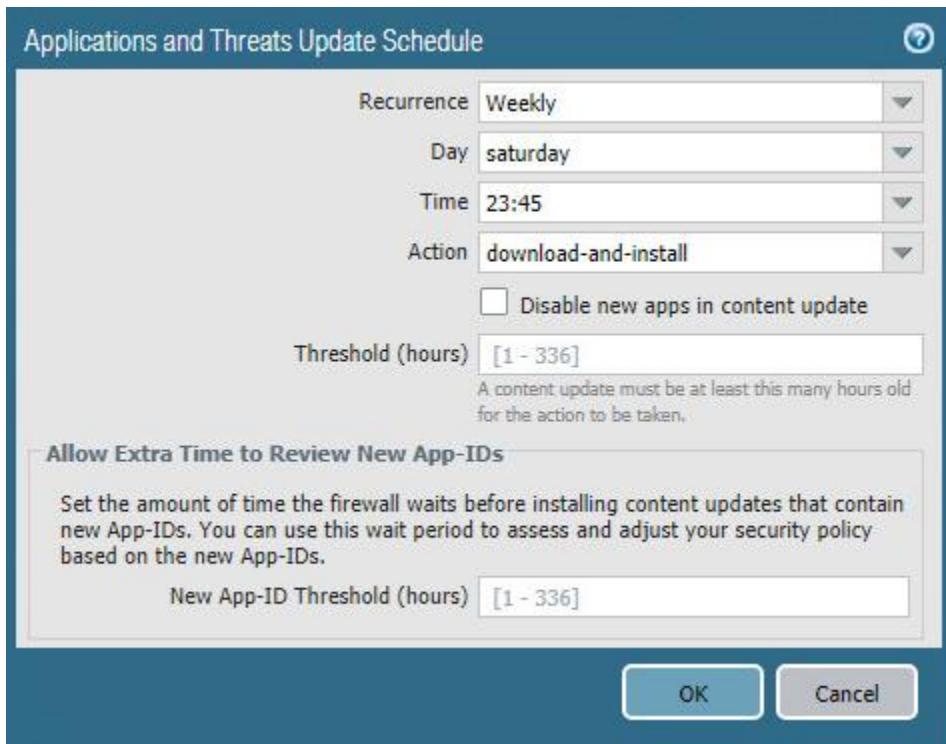
| Version ▲                  | File Name                             | Features   | Type |
|----------------------------|---------------------------------------|--|------|
| ▼ Applications and Threats | Last checked: 2018/11/29 12:25:15 EST | Schedule: Every Wednesday at 01:02 (Download only) |      |

1165 9. Select the desired recurrence. For this implementation, Weekly was used.

1166 10. Select the desired day and time. For this implementation, Saturday at 23:45 was used.

1167 11. Next to Action, select **download-and-install**.

1168 Figure 2-84 Threat Update Schedule



1169

1170 12. Click **OK**.

1171 13. Commit the changes.

1172 

## 2.6 Integration of Kryptowire EMM+S with MobileIron

1173 Kryptowire's application vetting service uses the MobileIron application programming interface (API) to  
1174 regularly pull current device application inventory information from MobileIron Core. Updated analysis  
1175 results are displayed in the Kryptowire portal.

1176    **2.6.1 Add MobileIron API Account for Kryptowire**

1177    The following steps will create an administrative account that will grant Kryptowire the specific  
 1178    permissions it requires within MobileIron.

- 1179        1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Users**.  
 1180        2. On the **Users** page:  
                 a. Select **Add > Add Local User**; the Add New User dialogue will open.

1182    **Figure 2-85 MobileIron Users**

| Actions                  | EDIT  | NAME                 | USER ID    | EMAIL                     | CREATION DATE       | SOURCE | ROLES                         |
|--------------------------|---|----------------------|------------|---------------------------|---------------------|--------|-------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> <input type="checkbox"/> | admin                | admin      |                           | 2017-08-31 5:45:... | Local  | Change Device Ownership, L... |
| <input type="checkbox"/> | <input type="checkbox"/> <input type="checkbox"/> | Appthority Connector | appthority | appthority@govt.mds.local | 2017-10-30 5:41:... | Local  | User Portal                   |

- 1183        b. In the **Add New User** dialogue:  
 1184            i. In the **User ID** field, enter the user identity that the Kryptowire cloud will  
                   authenticate under; our implementation uses a value of **kryptowire**.  
 1185            ii. In the **First Name** field, enter a generic first name for **Kryptowire**.  
 1186            iii. In the **Last Name** field, enter a generic last name for **Kryptowire**.  
 1187            iv. In the **Display Name** field, optionally enter a displayed name for this user  
                   account.  
 1188            v. In the **Password** field, provide the password that the **Kryptowire** identity will use  
                   to authenticate to MobileIron.  
 1189            vi. In the **Confirm Password** field, enter the same password as in the preceding step.  
 1190            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.  
 1191            viii. Select **Save**

1197 Figure 2-86 Kryptowire API User Configuration

Add New User X

|                  |                             |
|------------------|-----------------------------|
| User ID          | kryptowire                  |
| First Name       | Kryptowire                  |
| Last Name        | Cloud                       |
| Display Name     | Kryptowire 2 MobileIron API |
| Password         | .....                       |
| Confirm Password | .....                       |
| Email            | kryptowire@mds.local        |

[Cancel](#) Save

- 1198        3. In the **MobileIron Admin Portal**, navigate to **Admin > Admins**.
- 1199        4. On the **Admins** page:
- 1200            a. Enable the account you created for Kryptowire during **Step 2**.
- 1201            b. Select **Actions > Assign to Space**; this will open the Assign to Space dialogue for the Kryptowire account.
- 1202

1203 **Figure 2-87 MobileIron User List**

| Actions                             | NAME                      | USER ID    | EMAIL                     | SOURCE | ROLES  |
|-------------------------------------|---------------------------|------------|---------------------------|--------|--|
| <input type="checkbox"/>            | admin                     | admin      |                           | Local  | API, Add device, Apply and remove compliance policy labels, Apply  |
| <input type="checkbox"/>            | Appthority Connector      | apthority  | apthority@govt.mds.local  | Local  | API, Add device, Apply and remove compliance policy labels, Apply  |
| <input checked="" type="checkbox"/> | Kryptowire 2 MobileIro... | kryptowire | kryptowire@govt.mds.local | Local  | API, View dashboard, View device page, device details              |
| <input type="checkbox"/>            | Lookout Cloud             | lookout    | lookout@govt.mds.local    | Local  | API, Connector, Distribute app, View Audit logs, View apps and ibo |

1204

1205 c. In the **Assign to Space** dialogue:1206 i. In the **Select Space** drop-down menu, select **Global**.1207 **Figure 2-88 Kryptowire API User Space Assignment**

Assign to Space - Kryptowire 2 MobileIron API

Admin Space: Global

Admin Roles

Select all admin roles

Device Management

View device page, device details      Selected Permissions      Available Permissions

1208

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  |

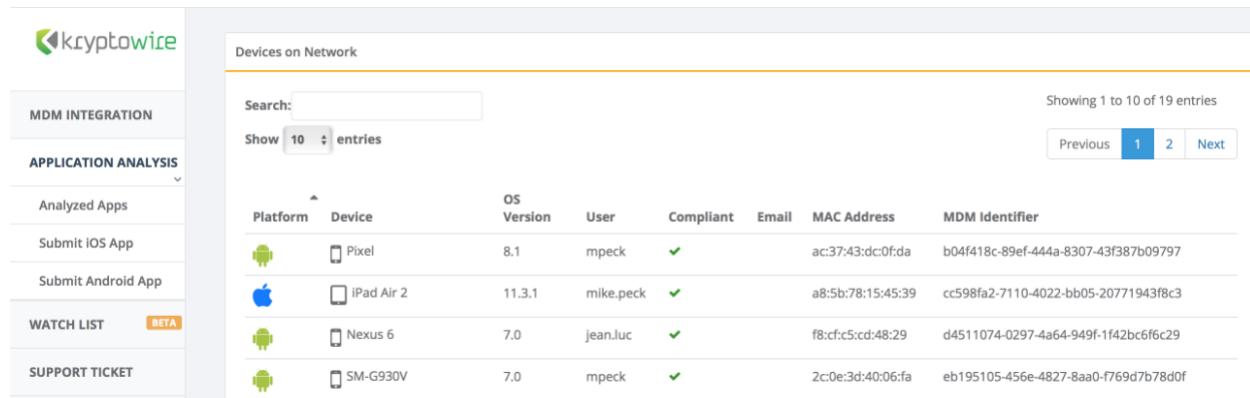
1209

iii. Select **Save**.

## 1210 2.6.2 Contact Kryptowire to Create Inbound Connection

1211 Once the MobileIron API account has been created, contact Kryptowire customer support to integrate  
 1212 your instance of MobileIron Core. Note that this will require creation of firewall rules that permit  
 1213 inbound connections from IP addresses designated by Kryptowire to MobileIron Core on port 443. Once  
 1214 the connection has been established, the Kryptowire portal will populate with information on devices  
 1215 registered with MobileIron. The EMM (Enterprise Mobility Management) ID presented by Kryptowire  
 1216 will be the same as the Universally Unique ID assigned to a device by MobileIron Core.

1217 **Figure 2-89 Kryptowire Device List**



The screenshot shows a web-based interface for managing devices. On the left, there's a sidebar with navigation links: MDM INTEGRATION, APPLICATION ANALYSIS (with sub-options Analyzed Apps, Submit iOS App, Submit Android App), WATCH LIST (BETA), and SUPPORT TICKET. The main area is titled "Devices on Network". It includes a search bar, a "Show 10 entries" dropdown, and a pagination control showing "Showing 1 to 10 of 19 entries" with buttons for Previous, 1, 2, and Next. A table lists four devices:

| Platform | Device     | OS Version | User      | Compliant | Email | MAC Address        | MDM Identifier                       |
|----------|------------|------------|-----------|-----------|-------|--------------------|--------------------------------------|
|          | Pixel      | 8.1        | mpeck     | ✓         |       | ac:37:43:d:c:0f:da | b04f418c-89ef-444a-8307-43f387b09797 |
|          | iPad Air 2 | 11.3.1     | mike.peck | ✓         |       | a8:5b:78:15:45:39  | cc598fa2-7110-4022-bb05-20771943f8c3 |
|          | Nexus 6    | 7.0        | jean.luc  | ✓         |       | f8:cfc5:cd:48:29   | d4511074-0297-4a64-949f-1f42bc6fc29  |
|          | SM-G930V   | 7.0        | mpeck     | ✓         |       | 2c:0e:3d:40:06:fa  | eb195105-456e-4827-8aa0-f769d7b78d0f |

## 1218 2.7 Integration of Lookout Mobile Endpoint Security with MobileIron

1219 Lookout’s Mobile Endpoint Security cloud service uses the MobileIron API to pull mobile device details  
 1220 and app inventory from MobileIron Core. Following analysis, Lookout uses the API to apply specific  
 1221 labels to devices to categorize them by the severity of any issues detected. MobileIron can be  
 1222 configured to automatically respond to the application of specific labels per built-in compliance actions.

### 1223 2.7.1 Add MobileIron API Account for Lookout

1224 The following steps will create an administrative account that will grant to Lookout the specific  
 1225 permissions it requires within MobileIron.

- 1226 1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Users**.
- 1227 2. On the **Users** page:
  - 1228 a. Select **Add > Add Local User**; the Add New User dialogue will open.

1229 **Figure 2-90 MobileIron User List**

| Actions                  | E...                     | NAME                 | USER ID       | EMAIL                     | CREATION DATE         | SO... | ROLES         |
|--------------------------|--------------------------|----------------------|---------------|---------------------------|-----------------------|-------|---------------|
| <input type="checkbox"/> | <input type="checkbox"/> | admin                | admin         |                           | 2017-08-31 5:45:19 AM | Local | Change Device |
| <input type="checkbox"/> | <input type="checkbox"/> | Administrator        | Administrator |                           | 2018-07-27 9:14:22 AM | LDAP  |               |
| <input type="checkbox"/> | <input type="checkbox"/> | Appthority Connector | appthority    | appthority@govt.mds.local | 2017-10-30 5:41:49 AM | Local | User Portal   |

1230 b. In the **Add New User** dialogue:

- 1231 i. In the **User ID** field, enter the user identity the Lookout cloud will authenticate under. Our implementation uses a value of **lookout**.
- 1232 ii. In the **First Name** field, enter a generic first name for **Lookout**.
- 1233 iii. In the **Last Name** field, enter a generic last name for **Lookout**.
- 1234 iv. In the **Display Name** field, optionally enter a displayed name for this user account.
- 1235 v. In the **Password** field, provide the password the Lookout identity will use to authenticate to MobileIron.
- 1236 vi. In the **Confirm Password** field, enter the same password as in the preceding step.
- 1237 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.
- 1238 viii. Select **Save**.

1244 Figure 2-91 MobileIron Lookout User Configuration

Add New User X

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

[Cancel](#) Save

- 1245        3. In the **MobileIron Admin Portal**, navigate to **Admin**.
- 1246        4. On the **Admin** page:
- 1247            a. Enable the account you created for Lookout during **Step 2**.
- 1248            b. Select **Actions > Assign to Space**; this will open the **Assign to Space** dialogue for the Lookout account.
- 1249

1250 **Figure 2-92 Lookout MobileIron Admin Account**

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

1251 c. In the **Assign to Space** dialogue:1252 i. In the **Select Space** drop-down menu, select **Global**.1253 **Figure 2-93 Lookout Account Space Assignment**

- Select all admin roles

▼ Device Management

- 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

1254 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  |

1255 iii. Select **Save**.

1256    **2.7.2 Add MobileIron Labels for Lookout**

1257    Lookout will dynamically apply MobileIron labels to protected devices to communicate information  
 1258    about their current state. The following steps will create a group of Lookout-specific labels.

1259        1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Labels**.

1260        2. On the **Labels** page:

1261            a. Select **Add Label**; the **Add Label** dialogue will appear.

1262    **Figure 2-94 MobileIron Label List**

| Actions                  | Name            | Description                              | Type   | Criteria   |
|--------------------------|-----------------|--|--------|--|
| <input type="checkbox"/> | All-Smartphones | Label for all devices irrespective of OS | Filter | "common.retired"=false                                 |
| <input type="checkbox"/> | Android         | Label for all Android Phones.            | Filter | "common.platform"="Android" AND "common.retired"=false |
| <input type="checkbox"/> | Company-Owned   | Label for all Company owned smartphones. | Filter | "common.owner"="COMPANY" AND "common.retired"=false    |

1263        b. In the **Add Label** dialogue:

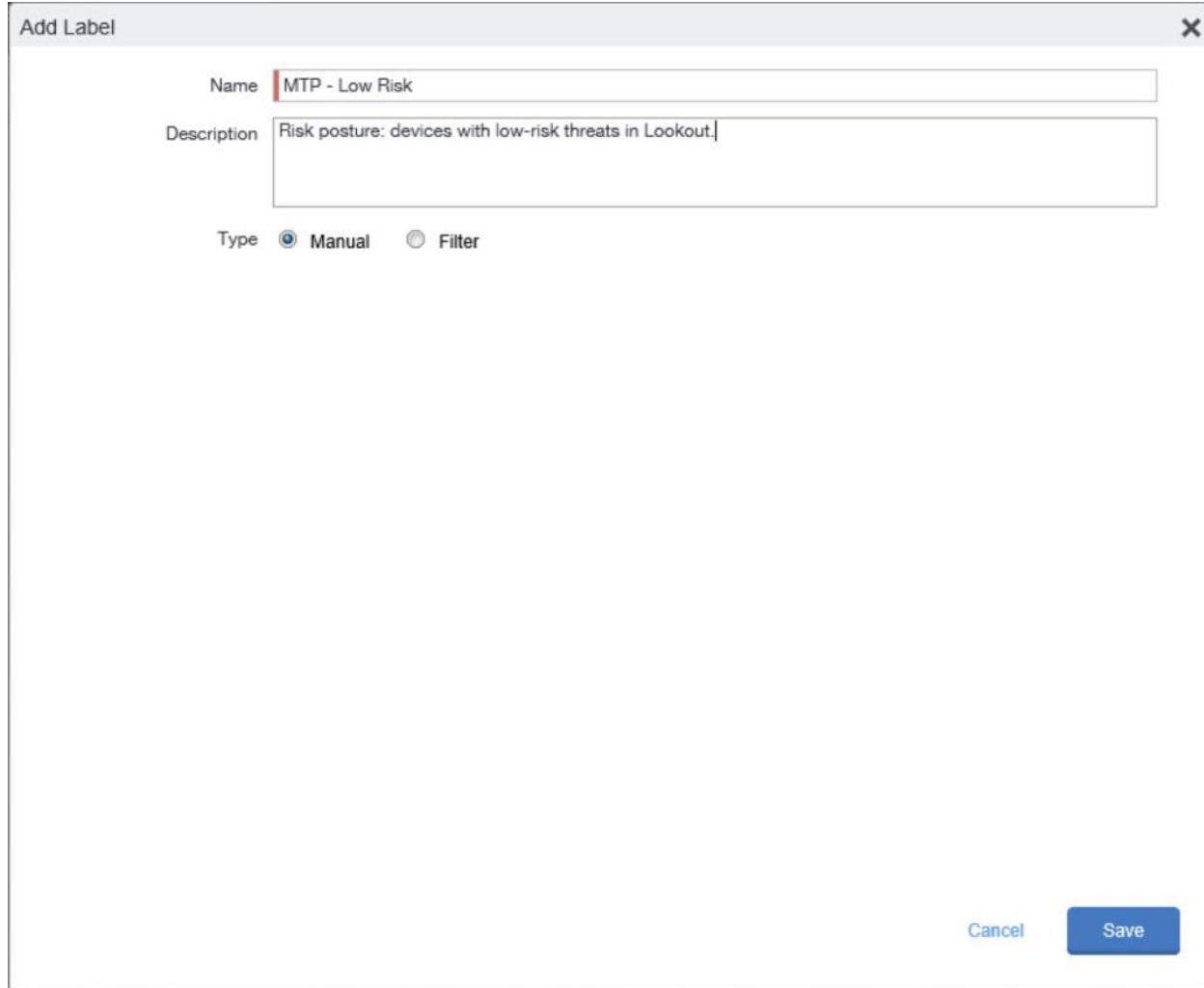
1264            i. In the **Name** field, enter the name of the label. Note: future steps will use the  
 1265              Label Names presented here but use of these names is optional.

1266            ii. In the **Description** field, enter a brief description for this label.

1267            iii. For the **Type** option, select **Manual**; this will hide all other form inputs.

1268            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     |

1270    **Note:** Administrators can choose to alter the label names to something more appropriate for their  
 1271    environment.

### 1272    2.7.3 Add Lookout for Work for Android to MobileIron App Catalog

1273    The following steps will add the Lookout for Work app for Android to MobileIron.

- 1274        1. In the **MobileIron Admin Portal**, navigate to **Apps > App Catalog**.
- 1275        2. On the **App Catalog** page, select **Add**; this will start the workflow to add a new app to the  
 1276        app catalog.

1277    **Figure 2-96 MobileIron App Catalog**

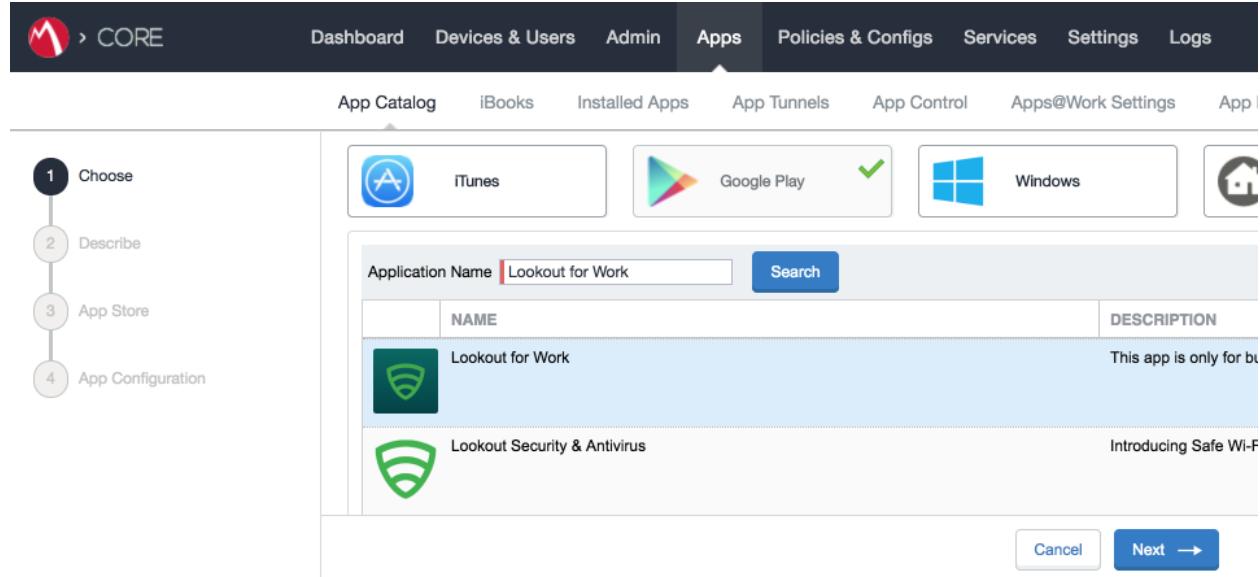
| Actions | APPICATION...    | APP VERSION | SOURCE   | L... | DEVICES INST... | APP SIZE | PROVISIONING PF |
|---------|------------------|-------------|----------|------|-----------------|----------|-----------------|
|         | Appthority       | 1.12.0      | In-House | iOS  | 0               |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

- 1278        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.

1282           d. In the list of search results, select the **Lookout for Work** app.

1283           e. Select **Next**.

1284 **Figure 2-97 Adding Lookout for Work to the MobileIron App Catalog**

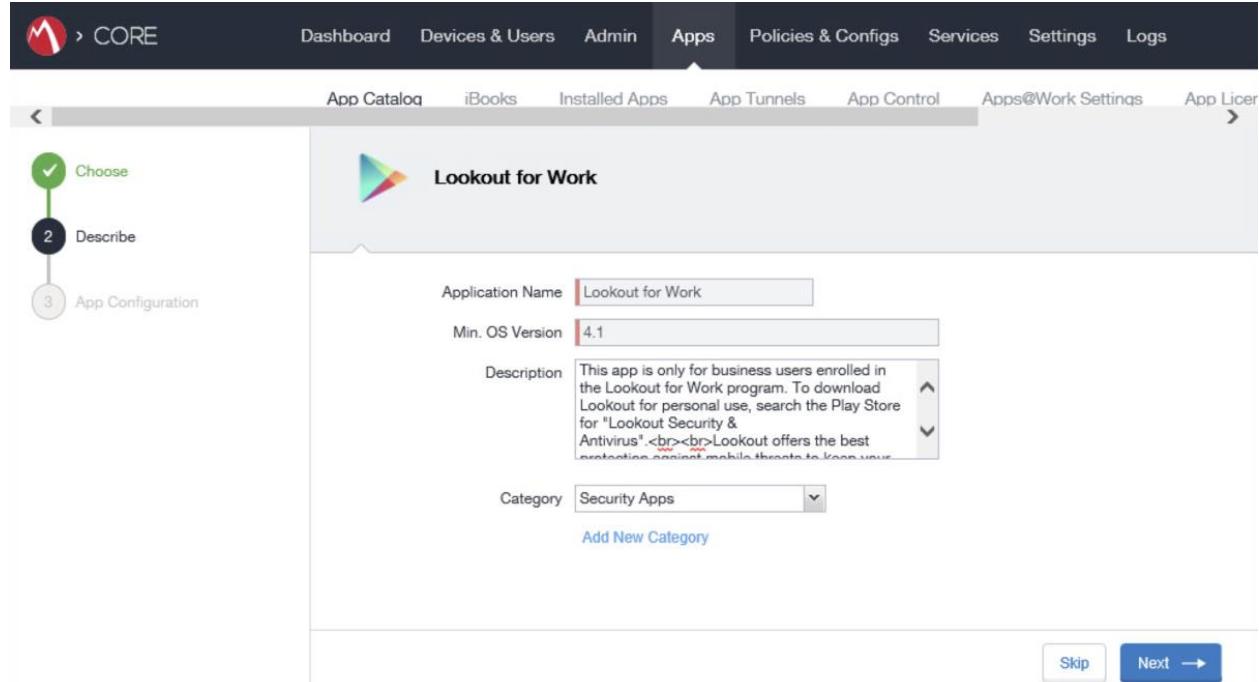


1285           4. On the **App Catalog > Describe** page:

1286           a. In **Category** drop-down menu, optionally assign the app to a category as appropriate to  
1287           your MobileIron deployment strategy.

1288           b. Select **Next**.

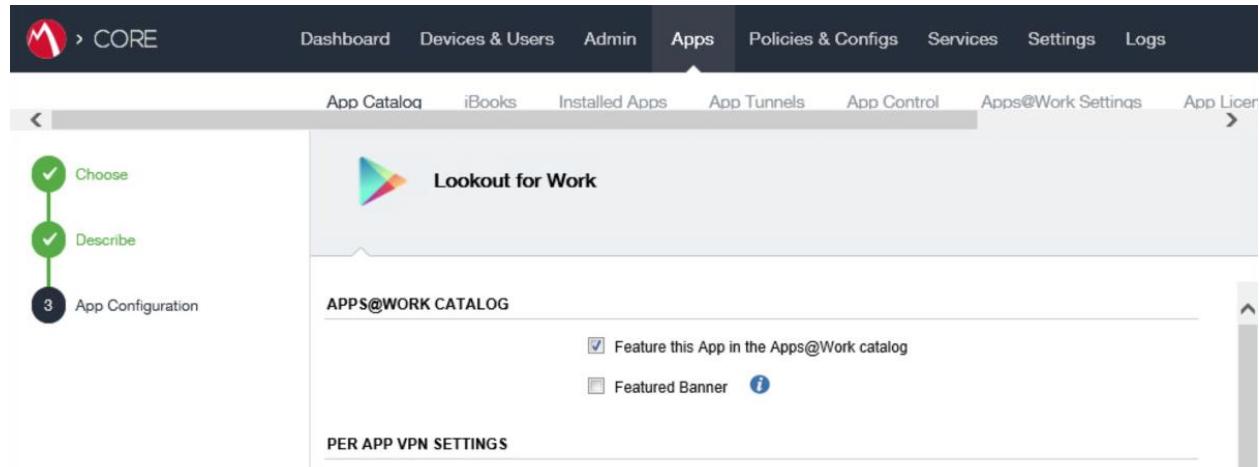
1289 Figure 2-98 Lookout for Work Application Configuration



1290 5. On the App Catalog &gt; App Configuration page:

- 1291 a. In the Apps@Work Catalog section, Enable Feature this App in the Apps@Work  
1292 catalog.

1293 Figure 2-99 Lookout for Work Application Configuration

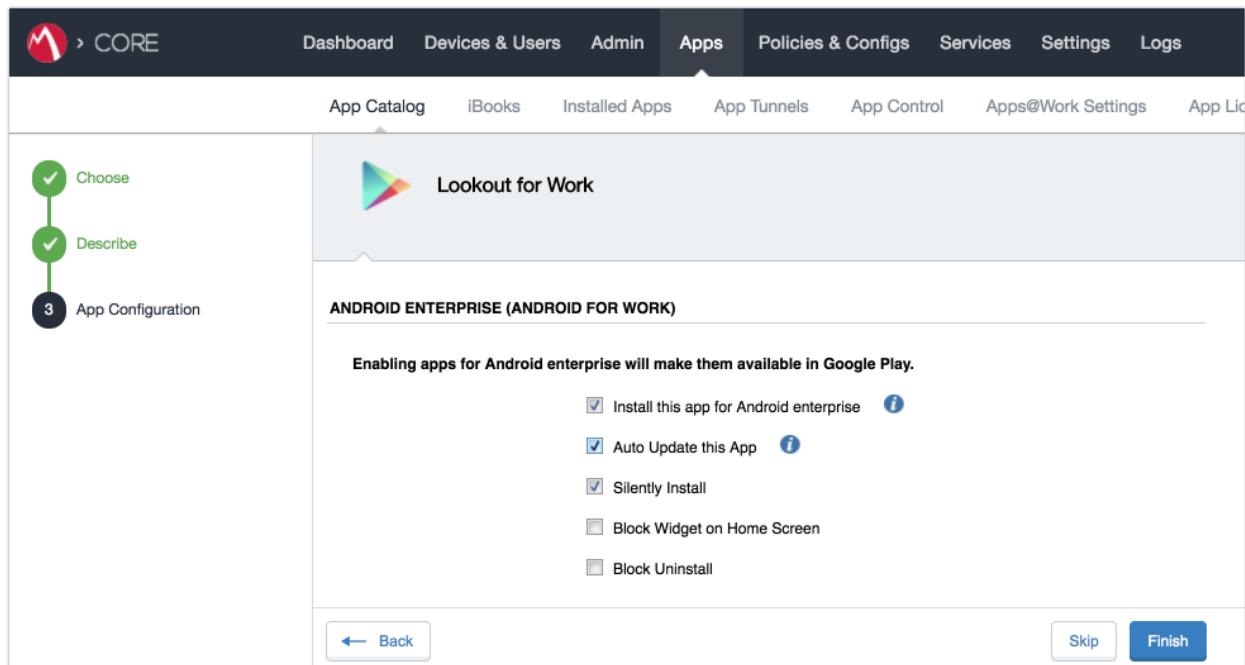


1294

- 1295 b. In the Android Enterprise (Android for Work [AFW]) section:

- 1296                   i. Enable **Install this app for Android enterprise**; additional controls will be made  
 1297                   visible.
- 1298                   ii. Enable **Auto Update this App**.
- 1299                   iii. Ensure **Silently Install** is enabled.
- 1300                   c. Select **Finish**.

1301 Figure 2-100 Lookout for Work AFW Configuration



- 1302                   6. The **Lookout for Work** app should now appear in the App Catalog with the AFW indicator.

#### 1303 2.7.4 Apply Labels to Lookout for Work for Android

- 1304                   1. On the **App Catalog** page:
- 1305                   a. Enable Lookout for Work.
- 1306                   b. Select **Actions > Apply To Labels**; the Apply To Labels dialogue will appear.

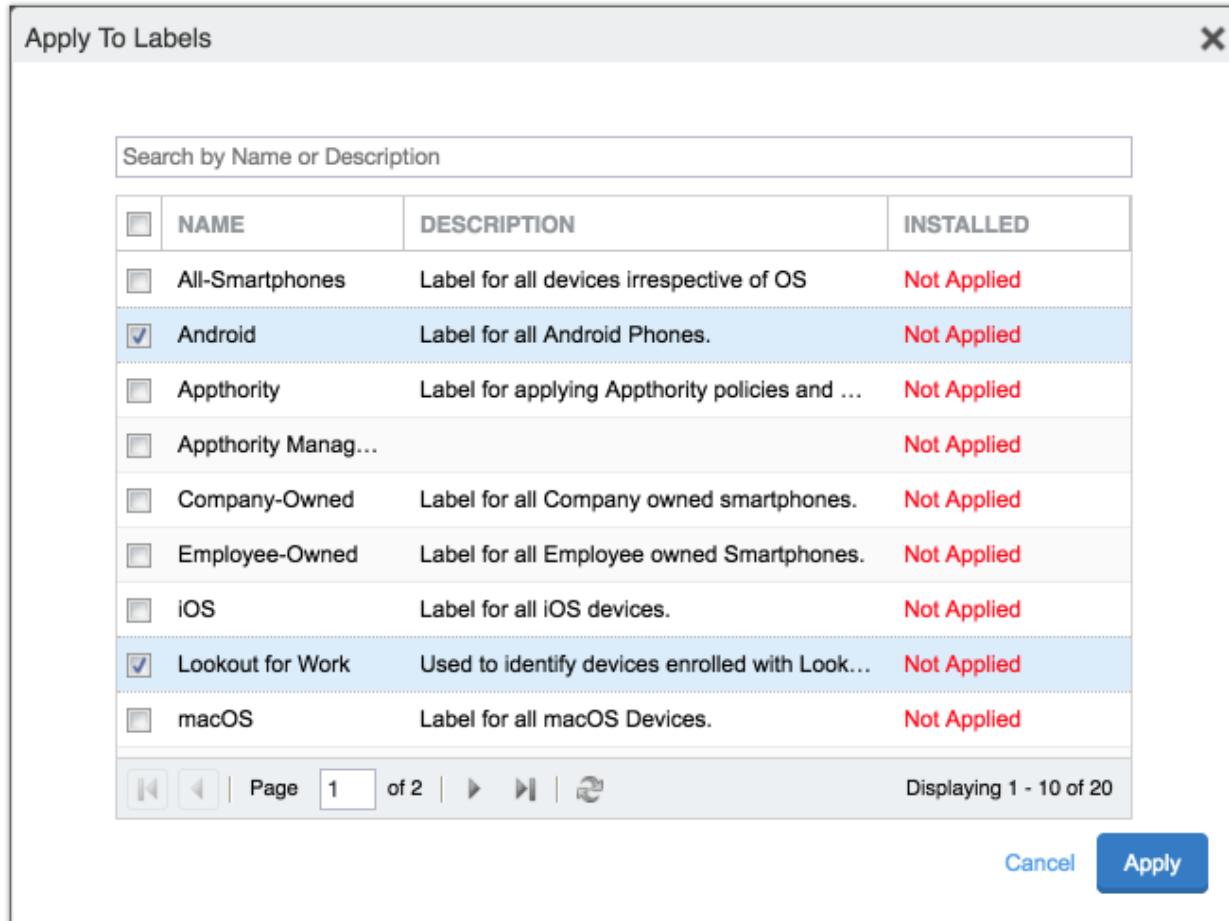
1307 **Figure 2-101 Apply Lookout for Work to Android Devices**

The screenshot shows the Core platform's 'App Catalog' section. A context menu is open over an app entry for 'Lookout for W...'. The menu is titled 'Actions' and includes options like 'Apply To Labels', 'Remove from Labels', 'Send Installation Request', 'Manage VPP', and 'Delete'. The 'Apply To Labels' option is currently selected. The main table below shows app details such as APP VERSION (2.8.0.0.10-T8...), SOURCE (In-House), DEVICES INSTALLED (0), APP SIZE (19.21 MB), and NEW PERMISSIONS (Unknown). The 'Lookout for W...' app row is highlighted.

| APP VERSION      | SOURCE   | DEVICES INST... | APP SIZE | NEW PERMIS... |
|------------------|----------|-----------------|----------|---------------|
| 2.8.0.0.10-T8... | In-House | 0               | 19.21 MB | Unknown       |

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**.

1312 Figure 2-102 Apply To Labels Dialogue



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

1315 Figure 2-103 Lookout for Work with Applied Labels

The screenshot shows the MobileIron Admin Portal interface. The top navigation bar includes links for Dashboard, Devices & Users, Admin, Apps (selected), Policies & Configs, Services, Settings, and Logs. Below the navigation is a sub-navigation bar with links for App Catalog, iBooks, Installed Apps, App Tunnels, App Control, and Apps@Work Settings. A 'Filters' section on the left shows 9 app(s) and a search bar. A 'Source' filter dropdown is set to 'All'. The main content area displays a table for the 'Lookout for Work' app. The table columns are APPLICATION NAME, APP VERSION, SOURCE, and LABELS. The app row shows 'Email+' as the application name, '2.8.0.0.10-T8...' as the app version, 'In-House' as the source, and 'Public' and 'Android, Lookout for Work' under the LABELS column.

| APPLICATION NAME        | APP VERSION      | SOURCE   | LABELS                    |
|-------------------------|------------------|----------|---------------------------|
| Email+                  | 2.8.0.0.10-T8... | In-House |                           |
| <b>Lookout for Work</b> |                  | Public   | Android, Lookout for Work |

## 1316 2.7.5 Add Lookout for Work app for iOS to MobileIron App Catalog

1317 The following steps will add the Lookout for Work app for iOS to MobileIron, apply appropriate  
1318 MobileIron labels, and create and upload a configuration file for one-touch activation of the app.

## 1319 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.

1323 Figure 2-104 MobileIron App Catalog

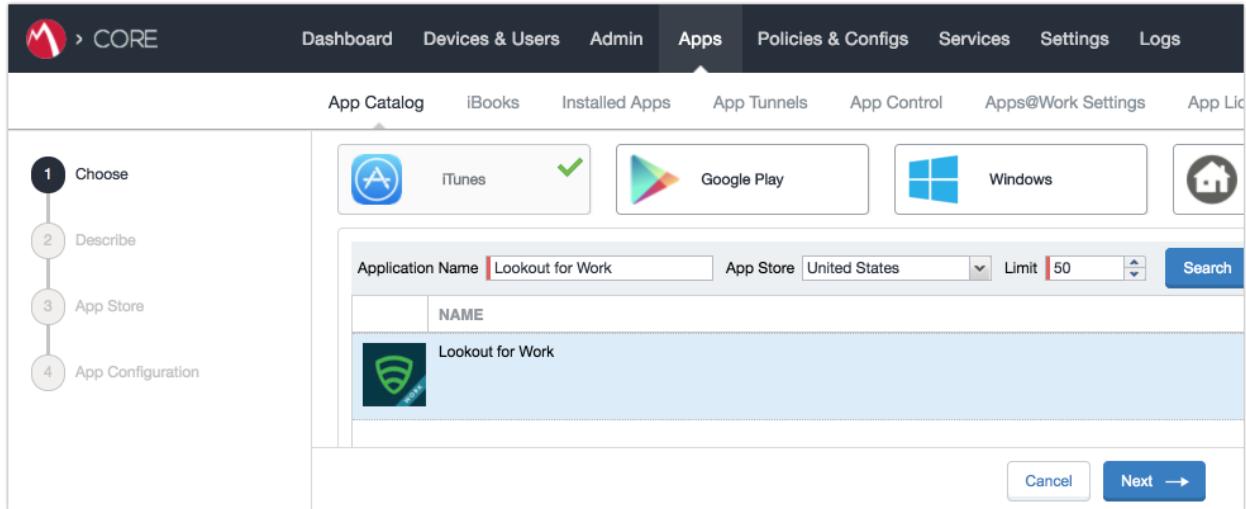
The screenshot shows the MobileIron Admin Portal interface, similar to Figure 2-103. The top navigation bar and sub-navigation bar are identical. The 'Filters' section on the left shows 2 app(s). The main content area displays a table for the app catalog. The table columns are APPLICATION NAME, APP VERSION, SOURCE, DEVICES INSTALLED, APP SIZE, and PROVISIONING PROFILE. Two apps are listed: 'Appthority' (version 1.12.0, In-House, 0 devices installed, 1.30 MB) and 'MobileIron Mo...' (version 2.0, Public, 2 devices installed, 57.21 MB).

| APPLICATION NAME | APP VERSION | SOURCE   | DEVICES INSTALLED | APP SIZE | PROVISIONING PROFILE |
|------------------|-------------|----------|-------------------|----------|----------------------|
| Appthority       | 1.12.0      | In-House | 0                 | 1.30 MB  |                      |
| MobileIron Mo... | 2.0         | Public   | 2                 | 57.21 MB |                      |

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

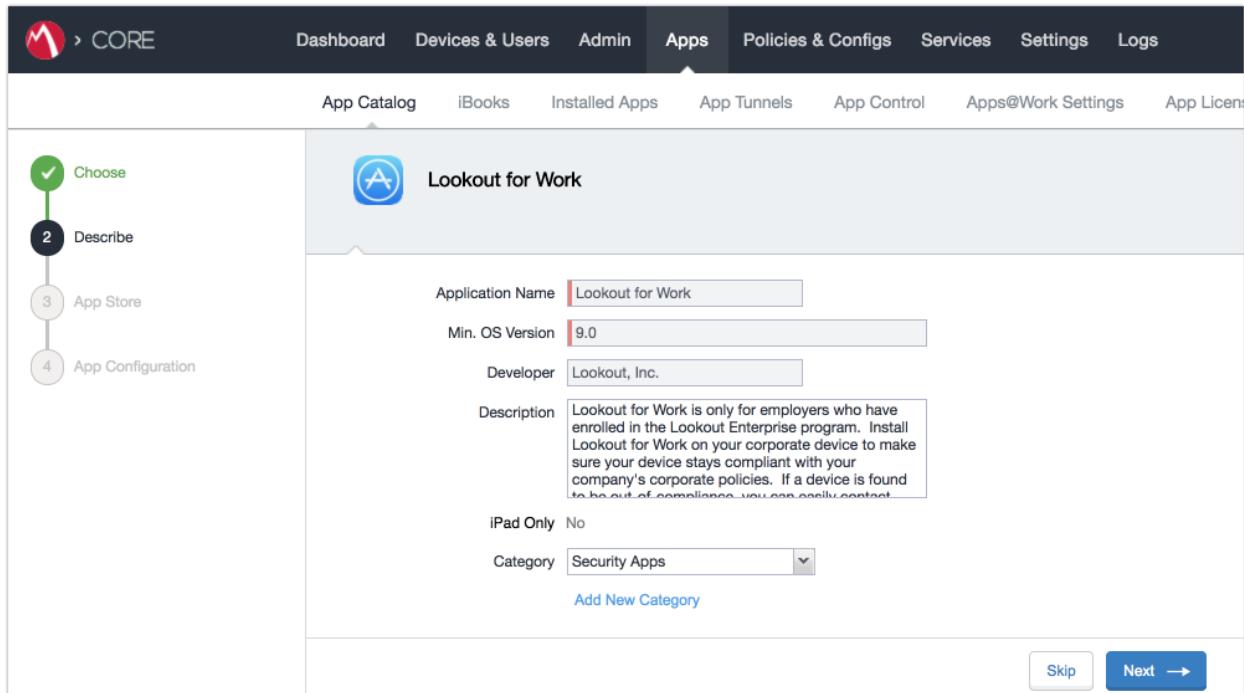
- 1325           a. Select **iTunes**; additional controls will be displayed.
- 1326           b. In the **Application Name** field, enter **Lookout for Work**.
- 1327           c. Select **Search**; search results will be displayed in the lower pane.
- 1328           d. In the list of search results, select the **Lookout for Work** app.
- 1329           e. Select **Next**.

1330   **Figure 2-105 Lookout for Work Selected From iTunes**

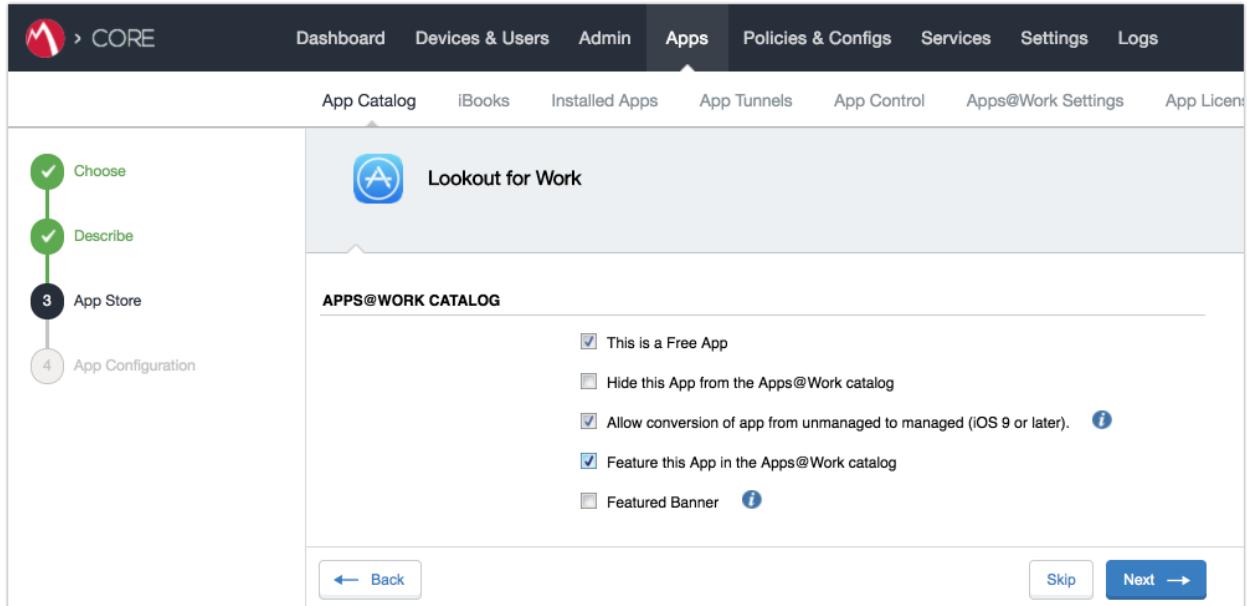


- 1331          4. On the **App Catalog > Describe** page:
- 1332           a. In **Category** drop-down menu, optionally assign the app to a category as appropriate to your MobileIron deployment strategy.
- 1334           b. Select **Next**.

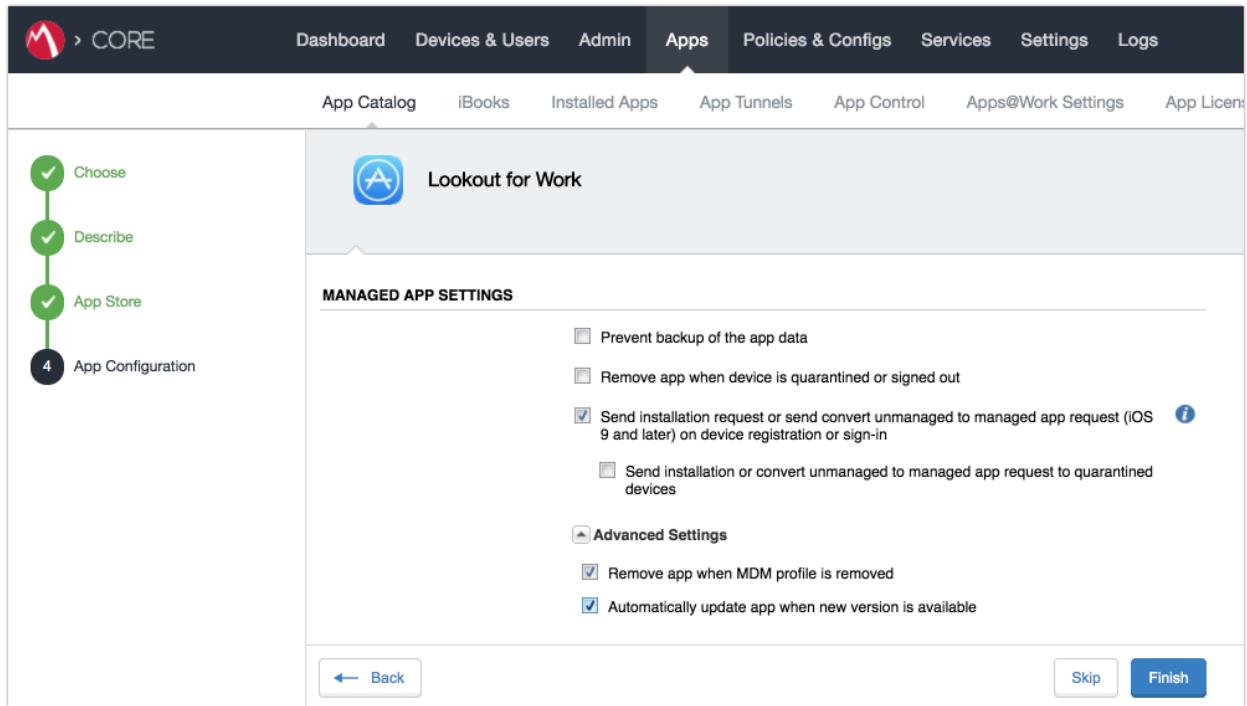
1335 Figure 2-106 Lookout for Work App Configuration

1336 5. On the **App Catalog > App Store** page:1337 a. In the **Apps@Work Catalog** section:1338 i. Enable **Allow conversion of app from unmanaged to managed (iOS 9 or later)**.1339 ii. Enable **Feature this App in the Apps@Work catalog**.1340 iii. Select **Next**.

1341 Figure 2-107 Lookout for Work App Configuration

1342 b. In the **App Catalog > App Configuration** section:1343 i. Enable **Send installation request or send convert unmanaged to managed app request (iOS 9 and later)** on device registration or sign-in.1344 ii. Enable **Advanced Settings > Automatically update app when new version is available.**1345 c. Select **Finish**.

1348 Figure 2-108 Lookout for Work Managed App Settings

1349 6. The **Lookout for Work** app should now appear in the App Catalog with AFW indicator.

1350 Figure 2-109 App Catalog With Lookout for Work

| App Catalog |         |                  |             |          |      |                 |          |                 |  |  |
|-------------|---------|------------------|-------------|----------|------|-----------------|----------|-----------------|--|--|
|             | ACTIONS | APPICATION...    | APP VERSION | SOURCE   | L... | DEVICES INST... | APP SIZE | PROVISIONING PF |  |  |
| 3 app(s)    | Add+    | Appthority       | 1.12.0      | In-House | iOS  | 0               | 1.30 MB  |                 |  |  |
|             |         | Lookout for W... |             | Public   |      | 0               | 36.88 MB |                 |  |  |

1351 [2.7.5.2 Apply MobileIron Labels to Lookout for Work App](#)1352 1. On the **App Catalog** page:

1353 a. Enable Lookout for Work.

1354 b. Select **Actions > Apply To Labels**; the Apply To Labels dialogue will appear.

1355 **Figure 2-110 Lookout for Work Selected**

The screenshot shows the CORE application management interface. The top navigation bar includes links for Dashboard, Devices & Users, Admin, Apps (which is the active tab), Policies & Configs, Services, Settings, and Logs. Below the navigation is a sub-menu with options for App Catalog, iBooks, Installed Apps, App Tunnels, App Control, Apps@Work Settings, and Apps. A 'Filters' section on the left shows '3 app(s)' and includes a search bar and a 'Source' dropdown set to 'All'. The main content area displays a table of apps. The first row, for 'Appthority', has its checkbox unchecked. The second row, for 'Lookout for W...', has its checkbox checked. The columns in the table are: APPICATION, APP VERSION, SOURCE, LABELS, DEVICES INST..., and APP SIZE. The 'Lookout for W...' row shows Public as the source, iOS as the label, 1 device installed, and a file size of 36.88 MB.

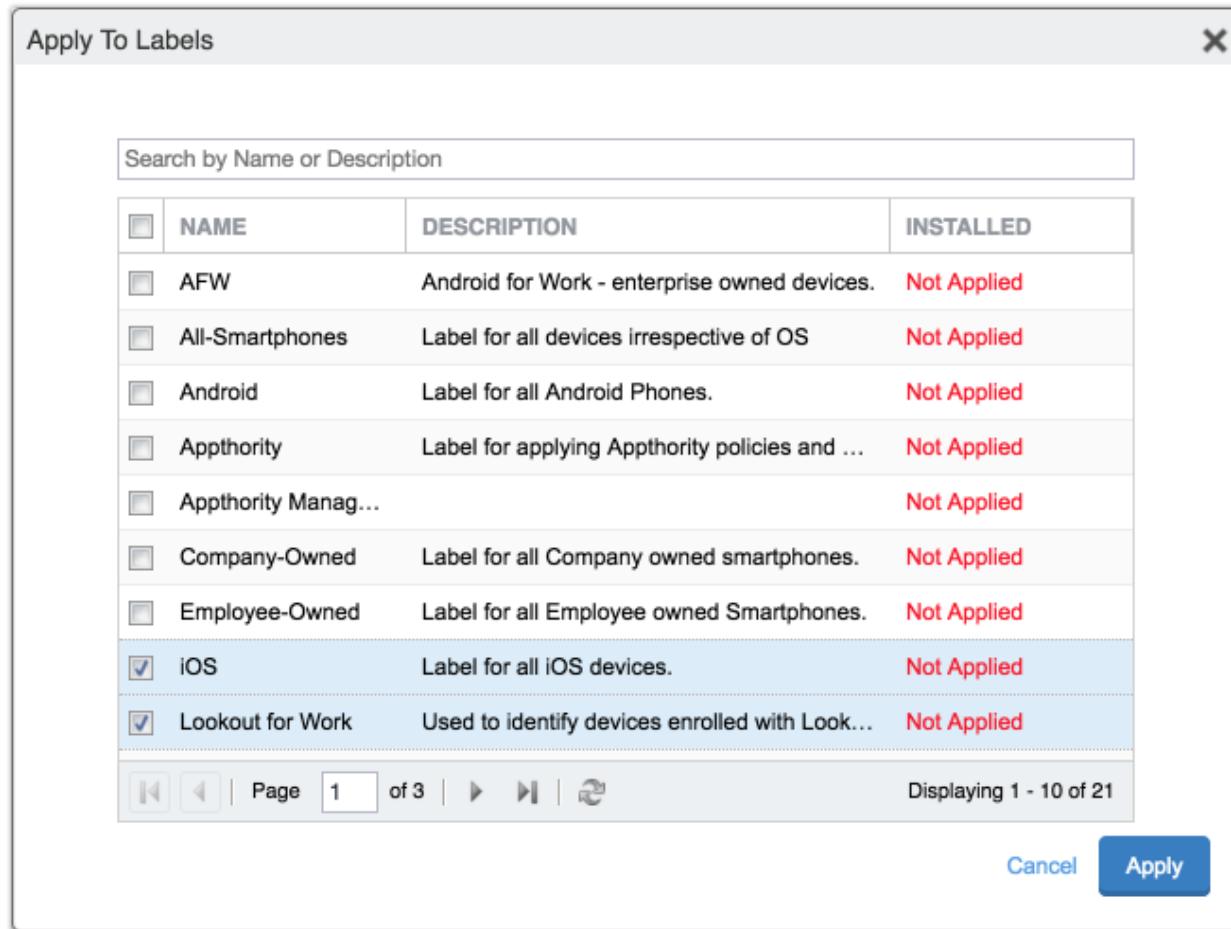
| APPICATION       | APP VERSION | SOURCE   | LABELS | DEVICES INST... | APP SIZE |
|------------------|-------------|----------|--------|-----------------|----------|
| Appthority       | 1.12.0      | In-House | iOS    | 1               | 1.30 MB  |
| Lookout for W... |             | Public   |   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

1356 c. In the **Apply To Labels** dialogue:

1357 i. Enable the **Lookout for Work** and **iOS** labels, plus any other labels appropriate to  
1358 your organization's mobile security policies.

1359 ii. Select **Apply**.

1360 Figure 2-111 Apply To Labels Dialogue



1361

- 1362 d. The **Lookout for Work** app should now appear with the Lookout for Work and iOS labels  
1363 applied.

1364 Figure 2-112 App Catalog With Lookout for Work

| APPICATION       | APP VERSION | SOURCE                | LABELS | DEVICES INST... | APP SIZE |
|------------------|-------------|-----------------------|--------|-----------------|----------|
| Lookout for W... | Public      | iOS, Lookout for Work | 1      | 36.88 MB        |          |

1365    **2.7.5.3 Create Managed App Configuration File for Lookout for Work**

1366    MobileIron can push a configuration file down to managed iOS devices to allow users easy activation of  
1367    Lookout for Work. The following steps will create and upload the necessary file.

- 1368        1. Using a **plain text** editor, create the following text file by **replacing the asterisks on line 13**  
1369            with your organization's Global Enrollment Code.

```
1370 <?xml version="1.0" encoding="UTF-8"?>
1371 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
1372 "https://www.apple.com/DTDs/PropertyList-1.0.dtd">
1373 <plist version="1.0">
1374   <dict>
1375     <key>MDM</key>
1376     <string>MOBILEIRON</string>
1377     <key>DEVICE_UDID</key>
1378     <string>$DEVICE_UDID$</string>
1379     <key>EMAIL</key>
1380     <string>$EMAIL$</string>
1381     <key>GLOBAL_ENROLLMENT_CODE</key>
1382     <string>*****</string>
1383   </dict>
1384 </plist>
```

- 1385        2. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.

- 1386        3. On the **Configurations** Page:

- 1387            a. Select **Add New > iOS and OS X > iOS Only > Managed App Config**; the New Managed  
1388              App Config Setting dialogue will open.

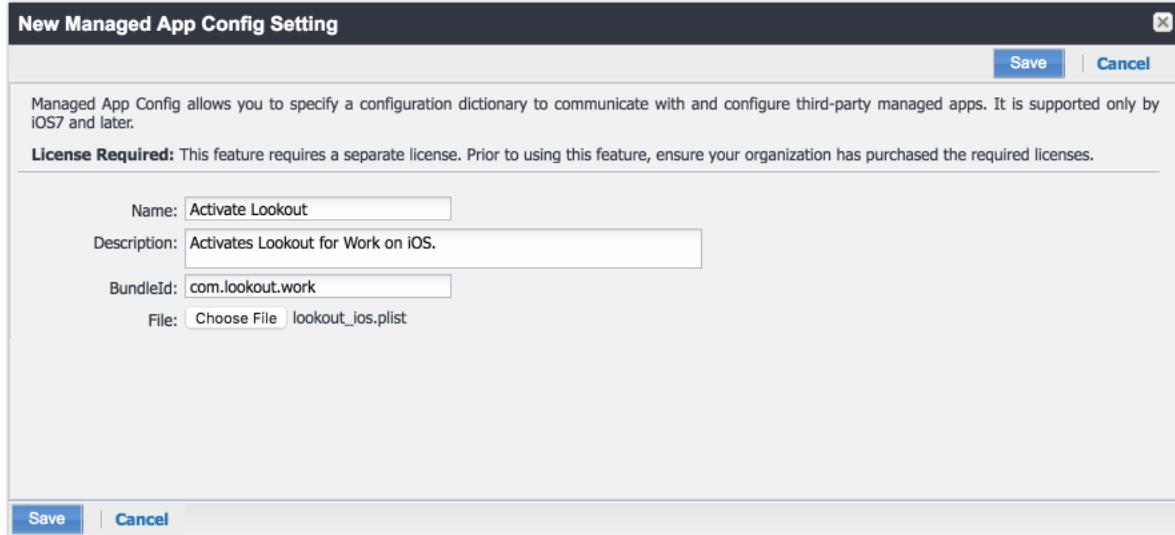
1389 Figure 2-113 Importing Managed Application Configuration

The screenshot shows the CORE application's 'Configurations' page. The 'Actions' column contains icons for each configuration entry. The 'Labels' dropdown is set to 'All-Smartphones'. The 'Configuration Type' dropdown is set to 'Filter by Configuration Type'. The table lists various configurations:

| Name                         | Type              | Bundle/Package ID      | Description  |
|------------------------------|-------------------|------------------------|--|
| Android                      | Configuration ... |                        | Created to support Android for Work configuration options on Android devices.                    |
| Exchange                     | ROIDFOR...        |                        |  |
| Email                        | AGED AP...        | com.appthority.Appt... | Identifies and reports on the risk associated with installed apps.                               |
| Wi-Fi                        | VISIONIN...       |                        |  |
| VPN                          | CONFIG            | forgepond.com.appt...  | Application Provisioning Profile embedded in file: Appthority_MobileAgent_Distribution           |
| AppConnect                   | POLICY            | forgepond.com.appt...  | Custom AppConnect App Configuration for Appthority. This is necessary for users t...             |
| Certificates                 | CONFIG            | forgepond.com.mob...   | Default AppConnect Configuration   |
| Certificate Enrollment       | POLICY            | forgepond.com.mobi...  | Default AppConnect Container Policy  |
| Docs@Work                    | CHANGE            |                        | policy to permit devices to access Exchange over ActiveSync.                                     |
| Web@Work                     | RESTRICTION       |                        |  |
| iOS and macOS                | iOS Only          |                        | AirPlay<br>AirPrint<br>APN<br>App Restrictions<br>Fonts<br>Managed App Config<br>Managed Domains |
| Windows                      | macOS Only        |                        |  |
| Secure Apps Manager          | APP               | iOS and macOS          |  |
| System - Apps@Work AET       | APPENROLLMENT     |                        |  |
| System - iOS Enrollment C... | CERTIFICATE       |                        |  |

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

- 1391 i. In the **Name** field, provide a name for this configuration; our implementation  
1392 used **Activate Lookout**.
- 1393 ii. In the **Description** field, provide the purpose for this configuration.
- 1394 iii. In the **BundleId** field, enter the bundle ID for Lookout at Work, which for our  
1395 version was **com.lookout.work**.
- 1396 iv. Select **Choose File...** to upload the plist file created during **Step 1**.
- 1397 v. Select **Save**.

1398 **Figure 2-114 plist Import Configuration**1399 **2.7.5.4 Apply Labels to Managed App Configuration for Lookout for Work**

1400 The following steps will apply the managed app configuration created in the previous section to labels.

1401 1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Configurations**.1402 2. On the **Configurations** page:1403 a. Enable the **Lookout Activation** managed app configuration created in the previous  
1404 section.1405 b. Select **Actions > Apply To Label**; the Apply To Label dialogue will open.1406 **Figure 2-115 Lookout Configuration Selected**

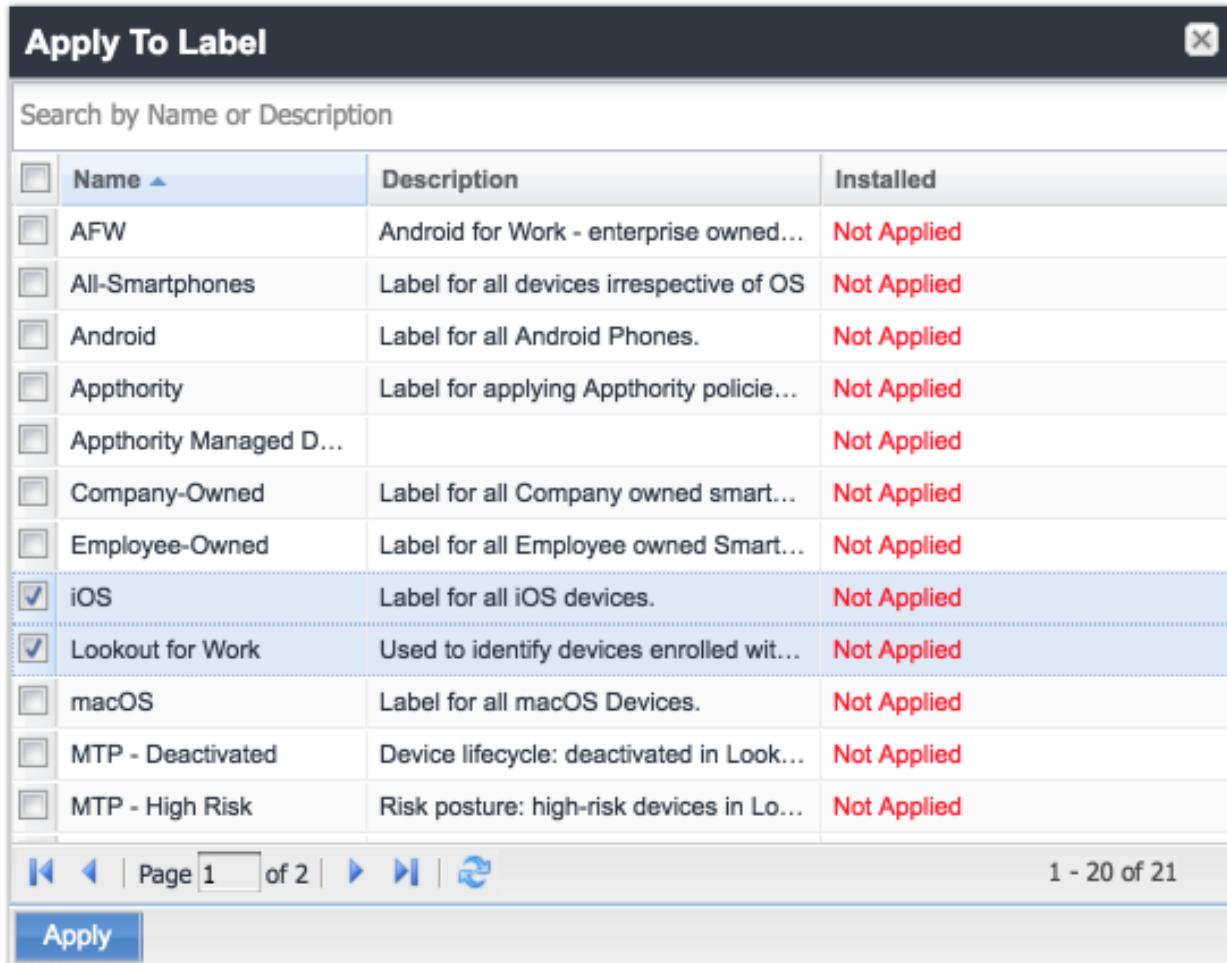
| CORE                     |                                |                                |                    |                      |                   | Dashboard              | Devices & Users | Admin                                     | Apps                  | Policies & Configs                               | Services     | Settings | Logs |  |
|--------------------------|--------------------------------|--------------------------------|--------------------|----------------------|-------------------|------------------------|-----------------|---|-----------------------|--|--------------|----------|------|--|
|                          |                                |                                |                    |                      |                   | Configurations         | Policies        | ActiveSync Policies                       | Compliance Policies   | Compliance Actions                               |              |          |      |  |
|                          |                                |                                |                    |                      |                   | Actions ▾              | Add New ▾       | Labels: All-Smartphones                   | Search by User        | Configuration Type: Filter by Configuration Type | Search by Na |          |      |  |
| <input type="checkbox"/> | Name ▾                         | Activate Lookout               | Configuration Type | MANAGED APP CONFIG   | Bundle/Package ID | com.lookout.work       | Description     | Activates Lookout for Work on iOS.        | Configuration Details | <a href="#">View File</a>                        |              |          |      |  |
| <input type="checkbox"/> | Android for Work Configur...   | Android for Work Configur...   | Configuration Type | ANDROIDFORWORK       | Bundle/Package ID |                        | Description     | Created to support Android for Work.      | Configuration Details |  |              |          |      |  |
| <input type="checkbox"/> | Appthority Mobile Intellige... | Appthority Mobile Intellige... | Configuration Type | MANAGED APP CONFIG   | Bundle/Package ID | com.appthority.Appt... | Description     | Identifies and repository for Appthority. | Configuration Details |  |              |          |      |  |
| <input type="checkbox"/> | Appthority_MobileAgent_...     | Appthority_MobileAgent_...     | Configuration Type | PROVISIONING_PROFILE | Bundle/Package ID |                        | Description     | Application Provisioning profile.         | Configuration Details |  |              |          |      |  |

1407 c. In the **Apply To Label** dialogue:

1408 i. Enable the iOS and Lookout for Work labels.

1409 ii. Select **Apply**.

1410 Figure 2-116 Apply To Label Dialogue



1411 d. The system should now reflect the **Lookout for iOS** and **iOS** labels have been applied to  
1412 the **Activate Lookout** configuration.

1413 **Figure 2-117 Lookout Configuration With Labels**

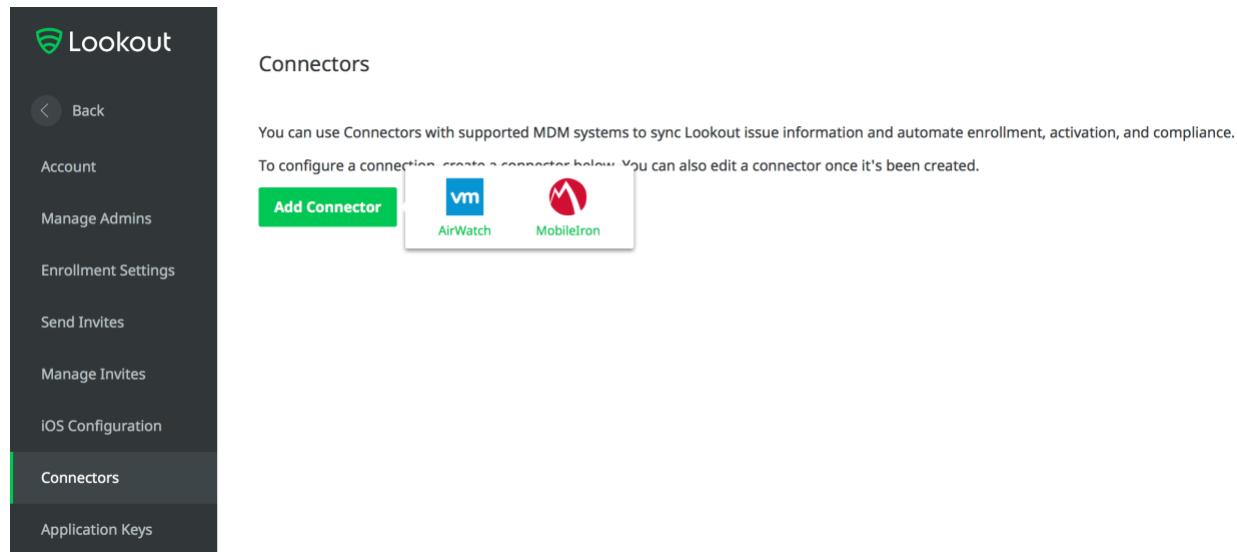
| Configurations           |                                |                         |                        |   |                              | Policies              | ActiveSync Policies | Compliance Policies | Compliance Actions |
|--------------------------|--------------------------------|-------------------------|------------------------|---|------------------------------|-----------------------|---------------------|---------------------|--------------------|
| Actions ▾ Add New ▾      |                                | Labels: All-Smartphones | Search by User         | Configuration Type:                           | Filter by Configuration Type | Search by Na          |                     |                     |                    |
| <input type="checkbox"/> | Name ▾                         | Configuration Type      | Bundle/Package ID      | Description                                   | # Phones                     | Labels                |                     |                     |                    |
| <input type="checkbox"/> | Activate Lookout               | MANAGED APP CONFIG      | com.lookout.work       | Activates Lookout for Work on iOS.            | 3                            | Lookout for Work, iOS |                     |                     |                    |
| <input type="checkbox"/> | Android for Work Configur...   | ANDROIDFORWORK          |                        | Created to support Android for Work con...    | 2                            | Android               |                     |                     |                    |
| <input type="checkbox"/> | Appthority Mobile Intellige... | MANAGED APP CONFIG      | com.appthority.Appt... | Identifies and reports on the risk associa... | 3                            | iOS                   |                     |                     |                    |

1414 

## 2.7.6 Add MDM Connector for MobileIron to Lookout MES

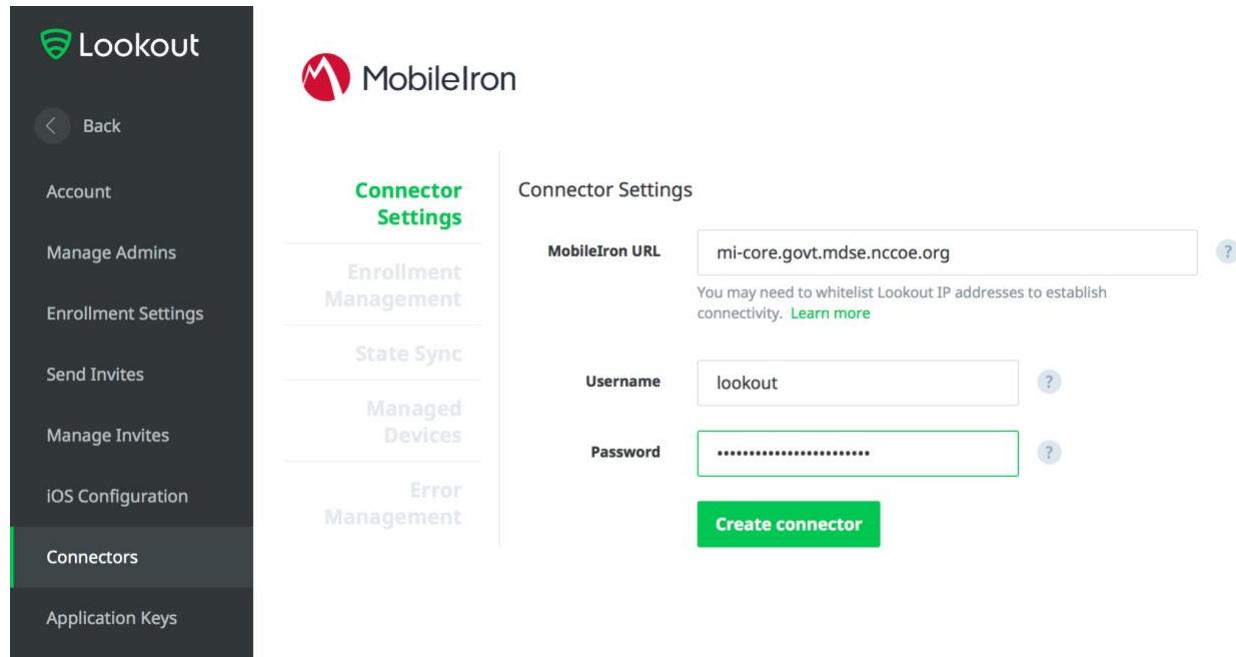
1415 The following instructions will connect Lookout with your MobileIron instance and associate Lookout  
1416 device states with the MobileIron labels created previously.

- 1417 1. Using the most-recent version of *MDM Service IP Whitelisting* available from the Lookout  
1418 support portal, configure your organization's firewalls to permit inbound connections from  
1419 the IP addresses provided on port 443 to your instance of MobileIron Core.
- 1420 2. In the **Lookout MES portal**, navigate to **Lookout > System > Connectors**.
- 1421 3. On the **Connectors** page:
- 1422 a. Select **Add Connector > MobileIron**; this will open a new form.

1423 **Figure 2-118 Add Lookout Connector Display**

- 1424            b. In the **Connector Settings** section of the form:
- 1425            i. For the **MobileIron URL** field, enter the FQDN for your instance of MobileIron. In  
1426            our example implementation, the URL was **mi-core.govt.mdse.nccoe.org**.
- 1427            ii. For the **Username** field, enter the User ID of the MobileIron admin account  
1428            created in 2.7.1. In our example implementation, the **User ID is lookout**.
- 1429            iii. For the **Password** field, enter the password associated with that MobileIron  
1430            admin account.
- 1431            iv. Select **Create Connector**; this will enable additional sections of the form.

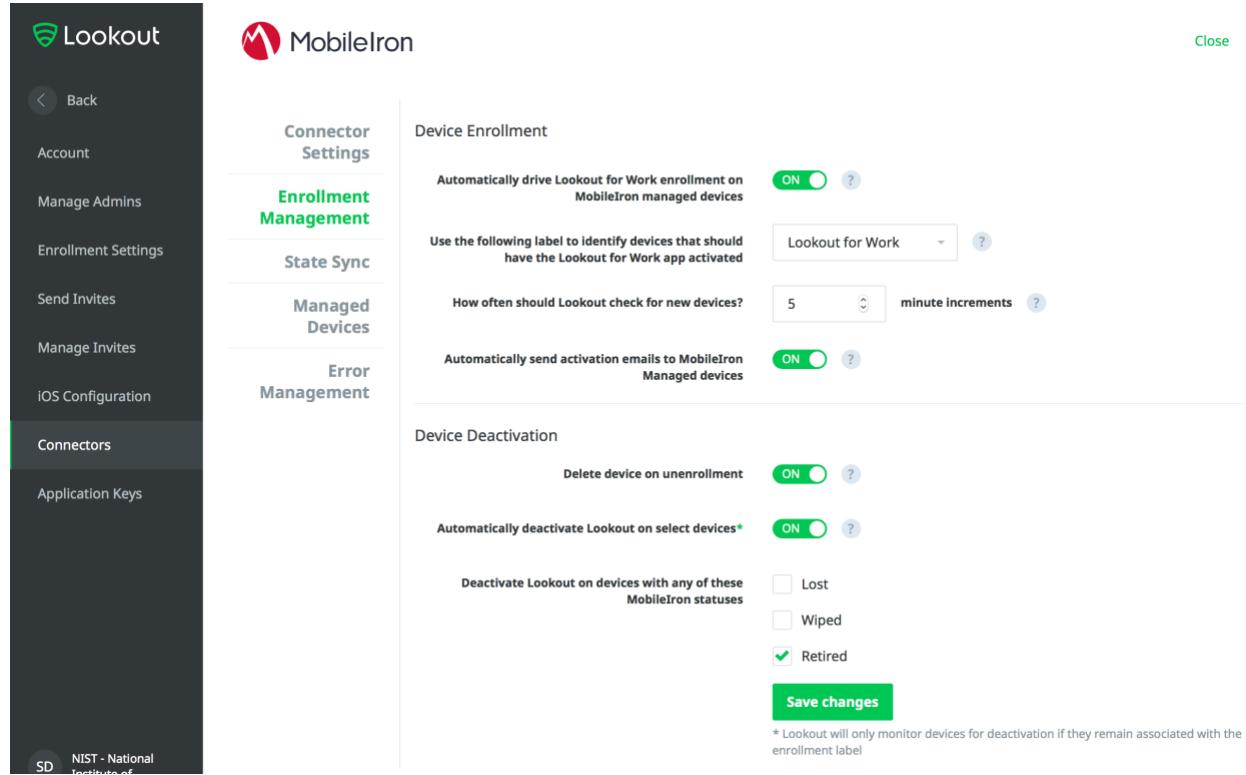
1432        **Figure 2-119 Connector Settings**



- 1433            c. In the **Enrollment Management** section of the form:
- 1434            i. Toggle **Device Enrollment > Automatically** drive Lookout for Work enrollment on  
1435            MobileIron managed devices to **On**.
- 1436            ii. For the **Device Enrollment > Use the following label to identify devices that**  
1437            **should have the Lookout for Work app activated** drop-down menu, select the  
1438            **Lookout for Work** label.
- 1439            iii. Toggle **Device Enrollment > Automatically send activation emails to MobileIron**  
1440            **managed devices** to **On**.

1441 iv. Select **Save Changes**.

1442 Figure 2-120 Connector Enrollment Settings



1443 d. In the **State Sync** section of the form:

1444 i. Toggle **State Sync > Synchronize Device Status to MobileIron** to **On**.

1445 ii. For each entry in the table below:

1446 1) Toggle the control to **On**.

1447 2) From the drop-down menu, select the **MobileIron Label** with the  
 1448 associated Purpose from the table in **Section 2.6.2 Add MobileIron Labels**  
 1449 **for Lookout**. We provide the Label Name we used for each Purpose in our  
 1450 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        |

1451     **Note:** Administrators can choose to alter the label names to something more appropriate for their  
 1452     environment.

1453                 iii. Select **Save Changes**.

1454 Figure 2-121 Connector Sync Settings

The screenshot shows two side-by-side mobile application interfaces. On the left is the Lookout app, with a dark theme. It has a navigation bar at the top with a back arrow and the word 'Lookout'. Below this is a vertical list of menu items: 'Account', 'Manage Admins', 'Enrollment Settings', 'Send Invites', 'Manage Invites', 'iOS Configuration', 'Connectors' (which is highlighted with a green bar), and 'Application Keys'. At the bottom left is a circular badge with 'SD' and 'NIST - National Institute of' text. On the right is the MobileIron Admin Portal, with a light theme. It features a header with the MobileIron logo. A sidebar on the left contains 'Connector Settings', 'Enrollment Management', 'State Sync' (which is highlighted in green), 'Managed Devices', and 'Error Management'. The main content area is titled 'State Sync' and includes a section for 'Device Lifecycle' with dropdowns for 'Devices that have not activated Lookout yet' (set to 'MTP - Pending'), 'Devices with Lookout activated' (set to 'MTP - Secured'), 'Devices on which Lookout is deactivated' (set to 'MTP - Deactivated'), and 'Devices that have lost connectivity with Lookout' (set to 'Choose status tag...'). It also includes sections for 'Risk Posture' with dropdowns for 'Devices with Low Risk issues present' (set to 'MTP - Low Risk'), 'Devices with Medium Risk issues present' (set to 'MTP - Moderate Risk'), and 'Devices with High Risk issues present' (set to 'MTP - High Risk'). At the bottom right of the main content area is a green 'Save changes' button.

## 1455 2.7.7 Configure MobileIron Risk Response

1456 The following steps will allow MobileIron to generate responses to various device states as assigned to  
 1457 devices by Lookout (e.g. MTP - High Risk).

## 1458 2.7.7.1 Add MobileIron App Control Rule

- 1459 1. In the **MobileIron Admin Portal**, navigate to **Apps > App Control**.
- 1460 2. Select **Add**; the Add App Control Rule dialogue will appear.
- 1461 3. In the **Add App Control Rule** dialogue:
  - a. In the **Name** field, enter **Threats Present Trigger**.

- 1463        b. Of the **Type** options, select **Required**.
- 1464        c. In the **App Identifier/Name** field enter **app does not exist**.
- 1465        d. In the **Device Platform** drop-down menu, select **All**.
- 1466        e. In the **Comment** field, optionally enter **Forces non-compliant state**.
- 1467        f. Select **Save**.

1468        Figure 2-122 MobileIron App Control Rule

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

- 1469        4. The new app control rule should now appear on the **Apps > App Control** page.

1470 **Figure 2-123 MobileIron App Control Rule**

The screenshot shows the MobileIron Admin Portal interface. The top navigation bar includes links for Dashboard, Devices & Users, Admin, Apps (selected), Policies & Configs, Services, Settings, and Logs. Below the navigation is a toolbar with Add, Delete, Search by Name, and a Type dropdown set to All. The main content area displays a table for App Control rules. The table has columns for Name, Type, Rule Entries, and Used in Policy. One row is visible, showing 'Threats Present Trigger' as the Name, 'Required' as the Type, and 'View Rule Entries' and 'Not Used' under the other columns.

1471 **2.7.7.2 Add MobileIron Compliance Actions**

1472 A Compliance Action defines what actions MobileIron will take when an App Control policy, like the one  
 1473 created in the previous section, is violated by a managed mobile device. The following steps will create  
 1474 and configure an example Compliance Action in response to the MTP - High Risk App Control rule. Note  
 1475 that a single Compliance Action can be associated with multiple App Control rules if the same response  
 1476 would be configured for each. Otherwise, a new Compliance Action should be created.

- 1477 1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Compliance Actions**.
- 1478 2. Select **Add**; the **Add Compliance Action** dialogue will open.
- 1479 3. In the **Add Compliance Action** dialogue:
  - 1480 a. In the **Name** field, add a description of the compliance action; we recommend indicating  
 1481 the kind of action taken. This example illustrates creating a compliance action that will  
 1482 be associated with the **MTP - High Risk** label.
  - 1483 b. Select the **Enforce Compliance Actions Locally on Devices** check box.
  - 1484 c. Select the **Send a compliance notification or alert to the user** check box.
  - 1485 d. Select the **Block email access and AppConnect apps** check box.
  - 1486 e. Select the **Quarantine the device** check box.
  - 1487 f. Deselect the **Remove All Configurations** check box.
  - 1488 g. Select **Save**.

1489 Figure 2-124 MTP High Risk Compliance Action

Add Compliance Action X

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

Name:  *i*

Enforce Compliance Actions Locally on Devices *i*

**Tier 1**

**▼ ALERT**

Send a compliance notification or alert to the user

**▼ BLOCK ACCESS**

Block email access and AppConnect apps *i*

**▼ QUARANTINE**

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

Quarantine the device

Remove All Configurations

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

+ Cancel Save

1490

1491 **2.7.7.3 Create MobileIron Security Policy for Lookout MES**

1492 In addition to potentially defining other controls, such as password requirements, a Security Policy can  
 1493 map a Compliance Action to an App Control rule, enabling MobileIron to execute the configured actions  
 1494 whenever a device that applies the policy violates the App Control rule. The following steps will create a

1495 new Security Policy for Lookout MES High Risk devices using an existing policy as a baseline from which  
 1496 to apply more stringent controls.

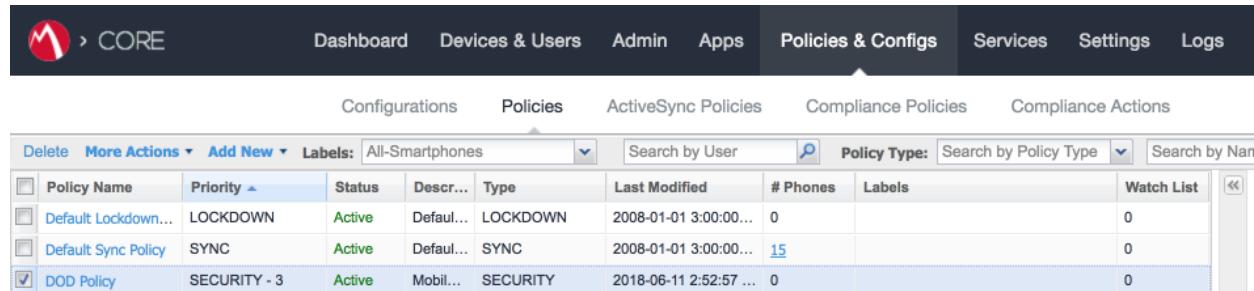
1497 1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Policies**.

1498 2. On the **Policies** page:

1499 a. Select the security policy to use as a baseline.

1500 b. Select **More Actions > Save As**; this will open the **New Security Policy** dialogue.

1501 **Figure 2-125 Baseline Policy Selection**



| Policies                            |                     |                |        |              |          |                        |          |                          |
|-------------------------------------|---------------------|----------------|--------|--------------|----------|------------------------|----------|--------------------------|
| Labels: All-Smartphones             |                     | Search by User |        | Policy Type: |          | Search by Policy Type  |          | Search by Name           |
| <input type="checkbox"/>            | Policy Name         | Priority ▲     | Status | Descri...    | Type     | Last Modified          | # Phones | Labels                   |
| <input type="checkbox"/>            | Default Lockdown... | LOCKDOWN       | Active | Defaul...    | LOCKDOWN | 2008-01-01 3:00:00...  | 0        | <input type="checkbox"/> |
| <input type="checkbox"/>            | Default Sync Policy | SYNC           | Active | Defaul...    | SYNC     | 2008-01-01 3:00:00...  | 15       | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | DOD Policy          | SECURITY - 3   | Active | Mobil...     | SECURITY | 2018-06-11 2:52:57 ... | 0        | <input type="checkbox"/> |

1502

1503 c. In the **New Security Policy** dialogue:

1504 i. In the **Name** field, rename the policy to **MTP - High Risk**.

1505 ii. In the **Priority** drop-down menu, select the security policy this policy will be  
 1506 prioritized in relation to; in this example, it is higher than the **MTP Medium Risk**  
 1507 policy. **Note:** for ease of setting priority, it is recommended to add new security  
 1508 policies in ascending order (lowest to highest priority).

1509 **Figure 2-126 MTP High Risk Policy**



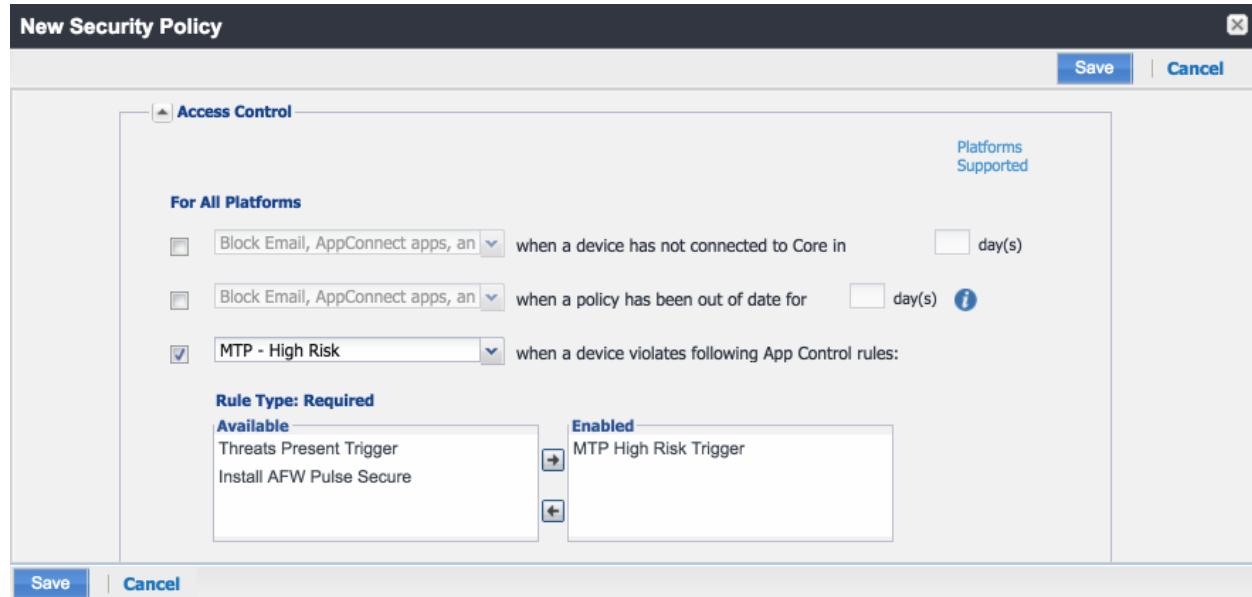
|              |   |
|--------------|---|
| Name:        | MTP High Risk   |
| Status:      | <input checked="" type="radio"/> Active <input type="radio"/> Inactive                            |
| Priority:    | <input checked="" type="radio"/> Higher than <input type="radio"/> Lower than MTP Medium Risk (2) |
| Description: | Applied to devices with MTP - High Risk label   |

1510

1511 iii. Under **Access Control > For All Platforms** section:

- 1512            1. For the **when a device violates the following app control rules** drop-down  
 1513            menu, select the **MTP - High Risk** compliance action.  
 1514            2. In the **Available** list of app control rules, highlight **MTP High Risk Trigger**.  
 1515            3. Select the **right arrow** to move MTP High Risk Trigger item into the **Enabled**  
 1516            **List**.  
 1517            iv. Select **Save**.

1518 **Figure 2-127 Security Policy Trigger**



1519

#### 2.7.7.4 Apply Lookout MES Label to MobileIron Security Policy

1520        1521 The following steps will apply the MTP - High Risk label to the security policy created in the previous  
 1522 section. As a result, once the Lookout cloud service applies the label to any device with a detected high-  
 1523 risk threat and such a device checks in with MobileIron, the security policy will automatically be applied  
 1524 to it (provided it is of higher priority than the policy currently applied). In turn that will cause the MTP  
 1525 High Risk Trigger App Control policy to be violated and the MTP - High Risk Compliance Action to be  
 1526 taken. Once Lookout detects that the threat has been resolved, the Lookout service will remove the  
 1527 MTP - High Risk label and on device check-in, MobileIron will then apply the next-lower-priority security  
 1528 policy.

- 1529            1. In the **MobileIron Admin Portal**, navigate to **Policies & Configs > Policies**.  
 1530            2. On the **Policies** page:  
 1531            a. Select the check box in the **MTP High Risk** security policy item.  
 1532            b. Select **More Actions > Apply to Label**; the Apply to Label dialogue will open.

1533 **Figure 2-128 Policy List**

| Policies  |                |                     |             |                                      |                       |                    |                     |            |
|---|----------------|---------------------|-------------|--------------------------------------|-----------------------|--------------------|---------------------|------------|
| Configurations  |                | ActiveSync Policies |             | Compliance Policies                  |                       | Compliance Actions |                     |            |
| Delete More Actions ▾ Add New ▾ Labels: All-Smartphones ▾ |                | Search by User      |             | Policy Type: Search by Policy Type ▾ |                       | Search by Name     |                     |            |
| Policy Name   | Priority ▾     | Status              | Description | Type                                 | Last Modified         | # Phones           | Labels              | Watch List |
| Appthority Android  | APPCONNECT - 1 | Active              | Allows...   | APPCONNECT                           | 2017-11-16 12:26:0... | 11                 | Android, Appthority | 1          |
| MTP High Risk   | SECURITY - 1   | Active              | Applies...  | SECURITY                             | 2018-06-12 11:20:2... | 0                  | MTP - High Risk     | 0          |

1534

1535 c. In the **Apply to Label** dialogue:1536 i. Select the check box for the **MTP - High Risk** item.1537 ii. Select **Apply**.

1538 Figure 2-129 Apply To Label Dialogue

| Apply To Label                      |                       |  |             |
|-------------------------------------|-----------------------|--|-------------|
| Search by Name or Description       |                       |  |             |
|                                     | Name ▾                | Description                              | Installed   |
| <input type="checkbox"/>            | Lookout for Work      | Used to identify devices enrolled wit... | Not Applied |
| <input type="checkbox"/>            | macOS                 | Label for all macOS Devices.             | Not Applied |
| <input type="checkbox"/>            | Mobile Users          | Label for users authorized to access...  | Not Applied |
| <input type="checkbox"/>            | MTP - Deactivated     | Device lifecycle: deactivated in Look... | Not Applied |
| <input checked="" type="checkbox"/> | MTP - High Risk       | Risk posture: high-risk devices in Lo... | Not Applied |
| <input type="checkbox"/>            | MTP - Low Risk        | Risk posture: low-risk devices in Loo... | Not Applied |
| <input type="checkbox"/>            | MTP - Moderate Risk   | Risk posture: moderate risk devices ...  | Not Applied |
| <input type="checkbox"/>            | MTP - Pending         | Device lifecycle: pending devices in ... | Not Applied |
| <input type="checkbox"/>            | MTP - Secured         | Device lifecycle: secured by Lookout.    | Not Applied |
| <input type="checkbox"/>            | MTP - Threats Present | Device lifecycle: threats on device d... | Not Applied |
| <input type="checkbox"/>            | NoAgent               | Only for devices without the Mobile...   | Not Applied |
| <input type="checkbox"/>            | Signed-Out            | Label for devices that are in a multi... | Not Applied |

⏪ ⏴ | Page 1 of 2 | ⏵ ⏹ | 🔍

1 - 20 of 22

Apply

1539

## 1540 2.8 Integration of Appthority Mobile Threat Detection with MobileIron

1541 Appthority provides an on-premises connector for MobileIron that runs as a Docker container on RedHat  
 1542 Linux. The connector uses the MobileIron API to obtain information on managed devices and their  
 1543 installed apps, which is then synchronized with the cloud service instance to obtain app and device risk  
 1544 scores, which are assigned to devices using custom attributes. The following sections provide the steps  
 1545 to create a MobileIron API account and deploy and configure the Appthority connector.

### 1546 2.8.1 Create MobileIron API Account for Appthority Connector

1547 The following steps will create an administrative account that will grant Appthority the specific  
 1548 permissions it requires within MobileIron.

- 1549           1. In the **MobileIron Admin Portal**, navigate to **Devices & Users > Users**.
- 1550           2. On the **Users** page:
- 1551            a. Select **Add > Add Local User**; the **Add New User** dialogue will open.
- 1552            b. In the **Add New User** dialogue:
- 1553              i. In the **User ID** field, enter the **user identity** the Appthority connector will  
1554                authenticate under. Our implementation uses a value of **Appthority**.
- 1555              ii. In the **First Name** field, enter a generic first name for **Appthority**.
- 1556              iii. In the **Last Name** field, enter a generic last name for **Appthority**.
- 1557              iv. In the **Display Name** field, optionally enter a displayed name for this user  
1558             account.
- 1559              v. In the **Password** field, provide the password the **Appthority** identity will use to  
1560             authenticate to MobileIron.
- 1561              vi. In the **Confirm Password** field, enter the same password as in the preceding step.
- 1562              vii. In the **Email** field, provide an email account for the **Appthority** identity; this  
1563             should be an account under the control of your organization.
- 1564              viii. Select **Save**.

1565 Figure 2-130 Appthority User Settings

Add New User X

|                  |                      |
|------------------|----------------------|
| User ID          | appthority           |
| First Name       | Appthority           |
| Last Name        | Connector            |
| Display Name     | Appthority Connector |
| Password         | .....                |
| Confirm Password | .....                |
| Email            | appthority@mds.local |

[Cancel](#) Save

1566

- 1567 1. In the **MobileIron Admin** Portal, navigate to **Admin**.
- 1568 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.

1572 **Figure 2-131 Appthority Connector User**

| Actions                             | NAME                       | USER ID    | EMAIL                     | SOURCE | ROLES                                    | ADMIN SPACES |
|-------------------------------------|----------------------------|------------|---------------------------|--------|--|--------------|
| <input type="checkbox"/>            | admin                      | admin      |                           | Local  | API, Add device, Apply and remove co...  | Global       |
| <input checked="" type="checkbox"/> | Appthority Connector       | appthority | appthority@govt.mds.local | Local  | API, Add device, Apply and remove co...  | Global       |
| <input type="checkbox"/>            | Kryptowire 2 Mobilelero... | kryptowire | kryptowire@govt.mds.local | Local  | API, View dashboard, View device page... | Global       |

1573

1574 c. In the **Assign to Space** dialogue:1575 i. In the **Select Space** drop-down menu, select **Global**.1576 **Figure 2-132 Appthority Connector Space Assignment**

Assign to Space - Appthority Connector

Select Space Global

Admin Roles

Select all admin roles

1577

1578 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  |

1579

iii. Select **Save**.1580 

## 2.8.2 Deploy Appthority Connector Open Virtualization Appliance

1581 One deployment option for the Appthority connector is a pre-built RedHat virtual machine distributed as  
 1582 an Open Virtualization Appliance (OVA). We imported the OVA into our virtual lab environment  
 1583 following guidance provided in *Connector On-Premises: Virtual Machine Setup* available from the  
 1584 Appthority support portal: <https://support.appthority.com/>.

1585    **2.8.3 Run the Enterprise Mobility Management Connector Deployment Script**

1586    Once the Appthority docker container is running, the setup script will configure it to use the MobileIron  
 1587    API account created previously. Detailed instructions on using the script are available on the Appthority  
 1588    support portal at [https://help-  
 1589    mtp.appthority.com/SetUp/EMM/EMM\\_Script/RunEMMDeployScript.html](https://help-mtp.appthority.com/SetUp/EMM/EMM_Script/RunEMMDeployScript.html). The first two steps ask for  
 1590    Appthority-supplied credentials necessary to verify your subscription and to link the connector with the  
 1591    correct instance of their cloud service. In the third step you will provide details to integrate with your  
 1592    on-premises instance of MobileIron core. Our results from completing the third step are shown below.  
 1593    1. **Obtain** a copy of *Run the EMM Connector Deployment Script* from the Appthority support  
 1594    portal at [https://help-  
 1595    mtp.appthority.com/SetUp/EMM/EMM\\_Script/RunEMMDeployScript.html](https://help-mtp.appthority.com/SetUp/EMM/EMM_Script/RunEMMDeployScript.html) (authentication  
 1596    to the portal is required).  
 1597    2. **Execute** the script. The third step in the script involves providing settings to enable the  
 1598    Appthority Connector to communicate with MobileIron Core. The results of our completion  
 1599    of that step are provided below as a reference.

1600    **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

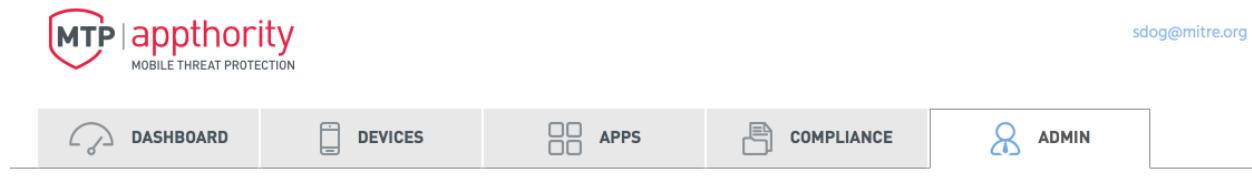
EMM Provider:      M
EMM Provider Selected: mobileiron
Is MobileIron Core On-Premise? (y/n): y
EMM URL:          mi-core.govt.mdse.nccoe.org
Is the EMM User a Domain Account (y/n)? n
EMM Username:     appthority
EMM Password:
Is there a Proxy (y/n)? n
Set EMM API Timeout (y/n)? n

[Okay]

```

1601
 1602
 1603    3. Once the script has been completed, verify successful synchronization with the Appthority  
 1604    cloud service by accessing the Appthority MTP portal and navigating to **Admin > EMM** and  
 1605    viewing items under **Connector Status**.

1606 Figure 2-134 Appthority EMM Connector Status



1607

1608 

## 2.9 Registering Devices with MobileIron Core

1609 In this scenario, the employee manages their own personal apps, data, and many device functions. The  
 1610 organization manages work-related apps and data, and has control over specific device functions, such  
 1611 as requiring a complex device unlock PIN or being able to remotely wipe a lost device. The mechanisms  
 1612 to achieve similar security characteristics between iOS and Android devices differ.

1613 

### 2.9.1 Supervising and Registering iOS Devices

1614 Many MDM-based security controls are only applicable to iOS devices that are running in Supervised  
 1615 Mode. The following steps outline how to place an iOS device into this mode, and then register with  
 1616 MobileIron Core.

1617 

#### 2.9.1.1 Resetting the iOS Device

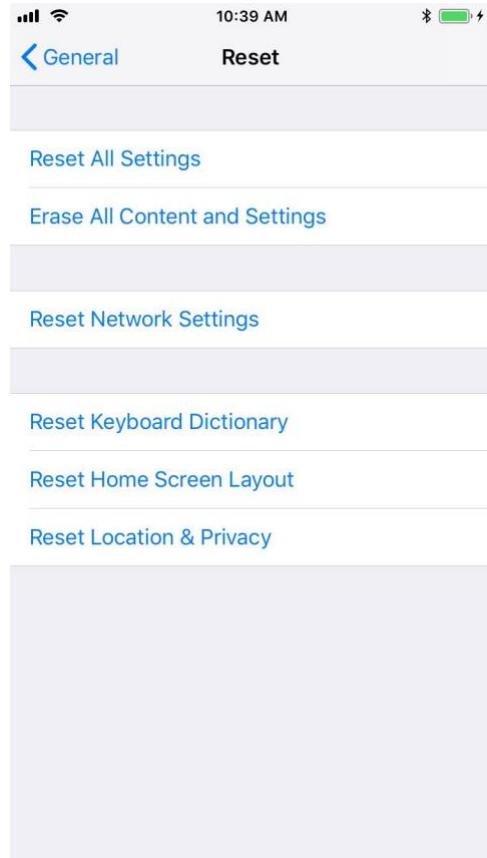
1618 Before a device can be placed into Supervised Mode, it must be in a factory-reset state with the  
 1619 Activation Lock on the device removed. If Activation Lock is in-place, Configurator 2 will be unable to  
 1620 place the device into Supervised Mode.

## 1621    2.9.1.1.1 Reset an Unsupervised Device Using Settings App

1622 If a device is not already in Supervised Mode, it is recommended to have the current device user  
1623 manually reset and activate the device to factory settings using the following steps:

1624    1. Navigate to **Settings > General > Reset**.

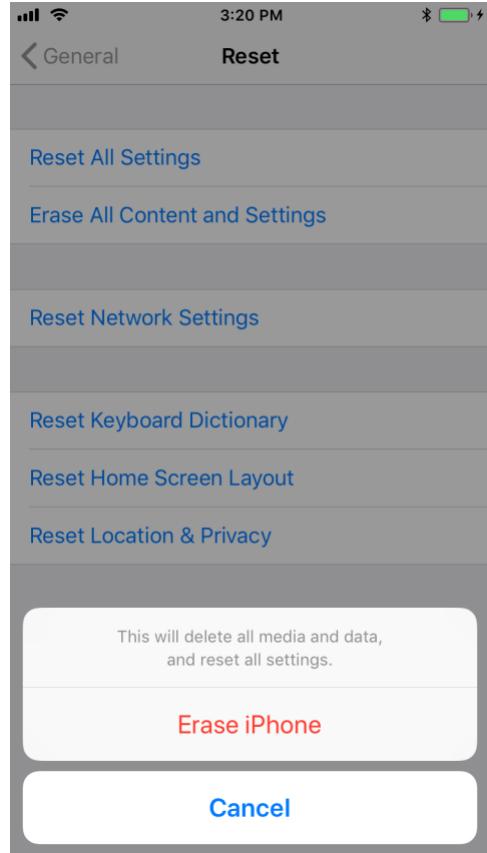
1625    2. Select **Erase All Content and Settings**.

1626    **Figure 2-135 iOS Reset Screen**

1627

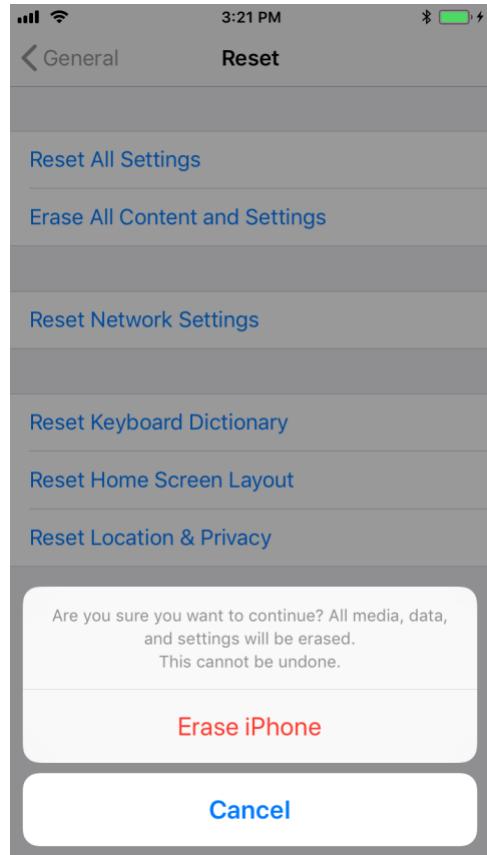
1628    1. At the warning that this will delete all media and data and reset all settings, select **Erase**  
1629       **iPhone**.

1630 **Figure 2-136 Erase iPhone Confirmation**



1631

- 1632 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.  
1633  
1634

1635 **Figure 2-137 Erase iPhone Final Confirmation**

1636

- 1637 1. Once the device displays the **Hello** screen, press the **Home key**.
- 1638 2. At the **Select Your Language** screen, select **English**.
- 1639 3. At the **Select Your Country or Region** screen, select **United States**.
- 1640 4. At the **Quick Start** screen select **Set up Manually**.
- 1641 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.
- 1645 6. **Stop** at the **Data & Privacy** screen. At this point, the device should be placed into **Supervised Mode** using **Configurator 2**.

## 1647    2.9.1.1.2 Reset a Supervised Device Using Configurator 2

1648        1. Connect the iOS device with the system running **Configurator 2** over Universal Serial Bus  
1649              (USB).1650        2. On the device at the **Enter Passcode** screen (if locked), enter the **device unlock passcode**.

1651    Figure 2-138 Entering iOS Passcode



1652

1653        3. At the **Trust this Computer?** dialogue, select **Trust**. Note that this step, along with step that  
1654              follows, is only encountered the first time a device is paired with a given system.

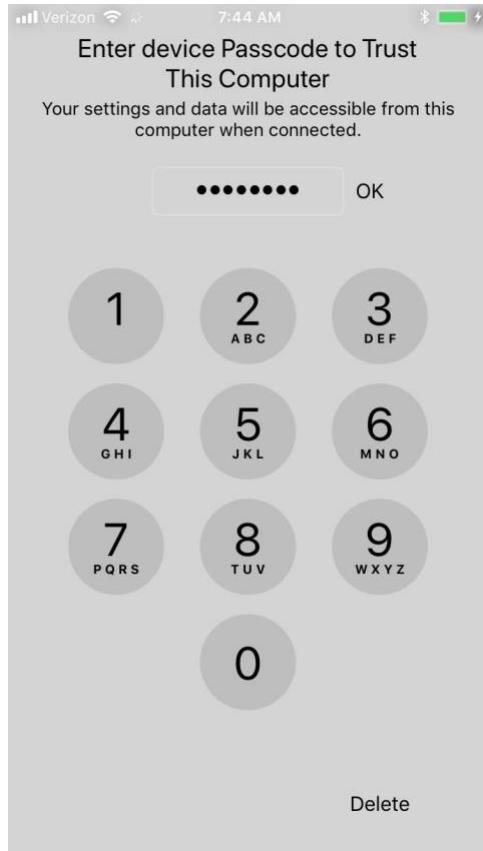
1655    **Figure 2-139 iOS Trust Computer Confirmation**



1656

- 1657    4. At the **Enter Device Passcode to Trust This Computer** screen:
- 1658        a. **Enter** the device unlock passcode.
- 1659        b. **Select OK.**

1660 Figure 2-140 Entering Passcode to Trust Computer

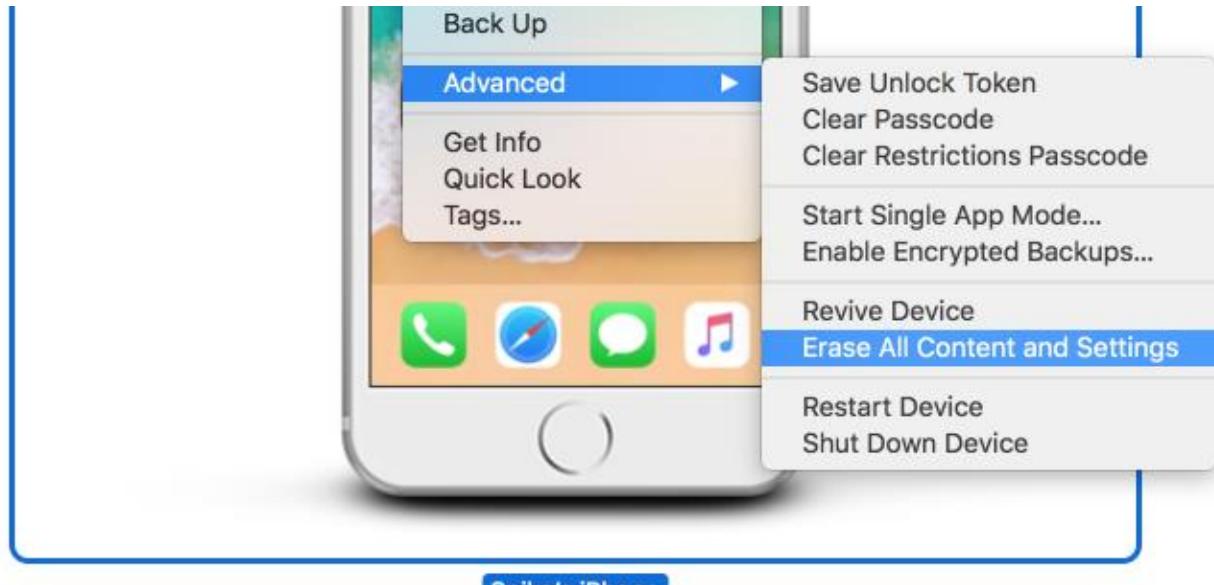


1661

1662        5. In **Configurator 2**, select the **representation** of the connected device.

1663        6. From the **context** menu, select **Advanced > Erase All Content and Settings**.

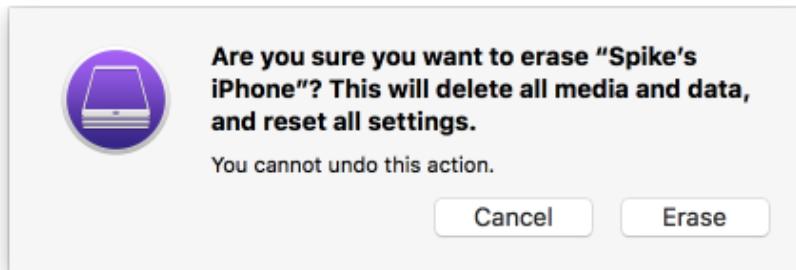
1664 Figure 2-141 Resetting iPhone in Configurator 2



1665

1666 7. At the **Are you sure you want to erase "<device name>"?** dialogue, select **Erase**.

1667 Figure 2-142 Configurator 2 Erase Confirmation



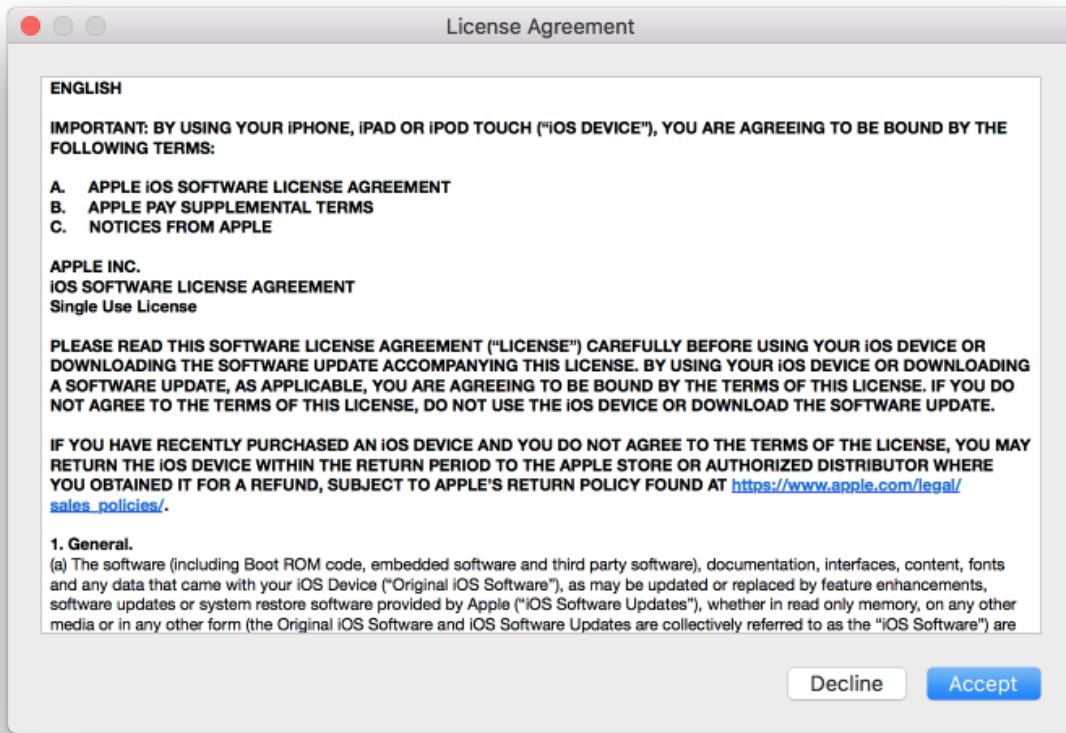
1668

1669 8. At the **License Agreement** screen:

1670 a. **Review** the license agreement.

1671 b. Select **Accept** to agree to the license and continue using the software.

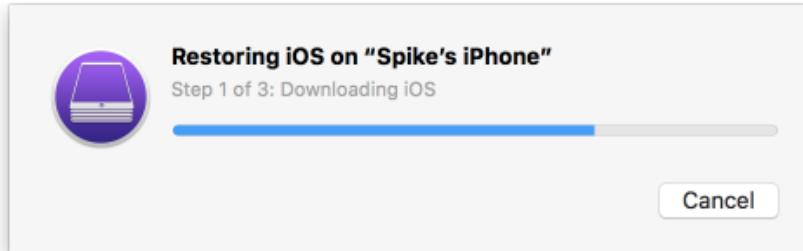
1672 Figure 2-143 Configurator 2 License Agreement



1673

- 1674        9. **Configurator 2** will take several minutes to restore the device to factory default settings.  
1675        **Configurator 2** will also activate the device following restoration.

1676 Figure 2-144 Restoring iPhone



1677

1678    **2.9.1.2 Placing an iOS Device into Supervised Mode**

1679    iOS devices that have been factory reset and subsequently activated (the Activation Lock has been  
1680    removed) can be placed into Supervised Mode using software available from Apple, Configurator 2, by  
1681    the following steps:

1682        1. **Pair** the target iOS device with the system running Configurator 2 over USB.

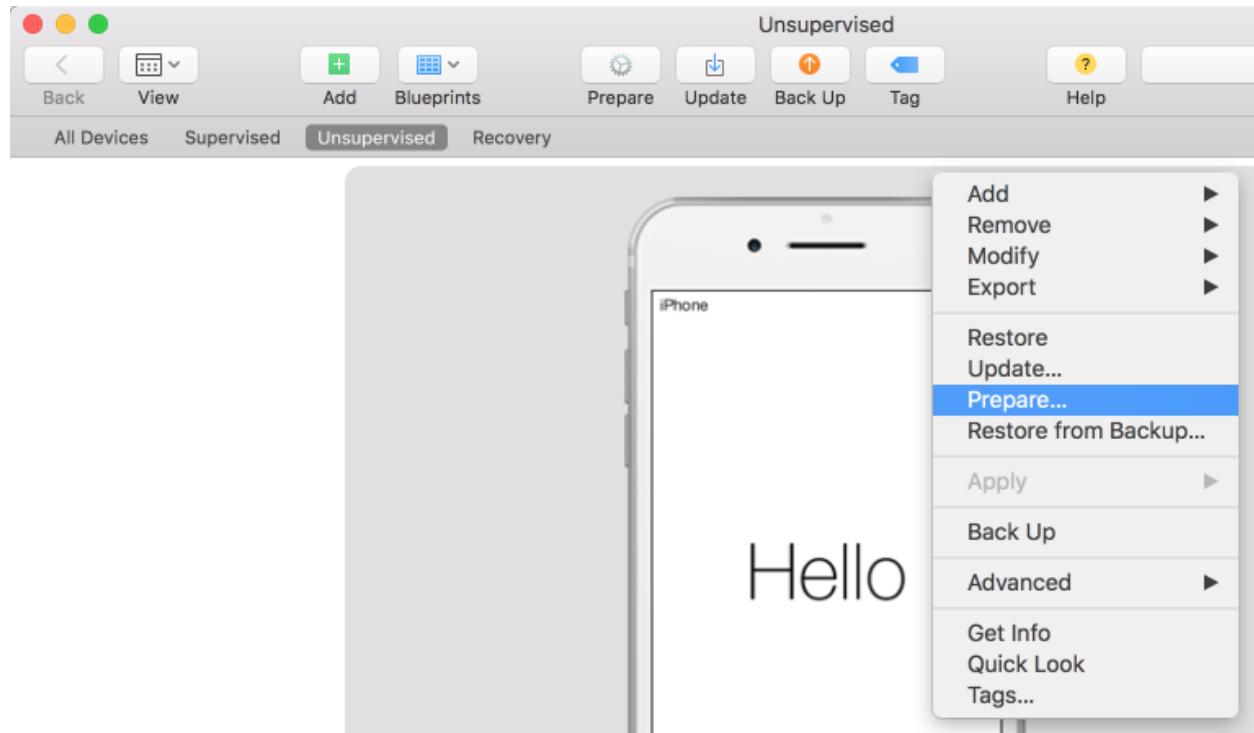
1683        2. Navigate to **Configurator 2 > Unsupervised**; a representation of the connected device  
1684        should appear.

1685        3. On the **All Devices** tab:

1686            a. **Select** the representation of the paired device.

1687            b. From the **context** menu, select **Prepare**; a wizard will open to guide the process.

1688    **Figure 2-145 Prepare Option in Configuration 2**



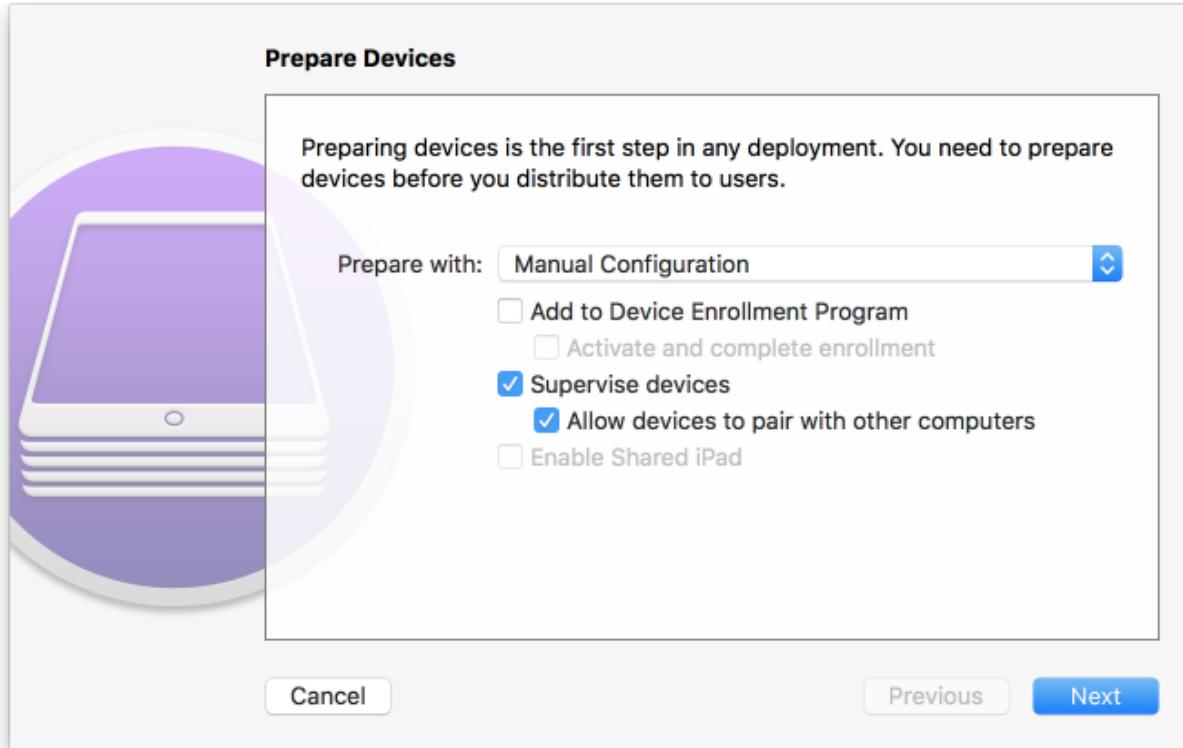
1689

1690        4. For the **Prepare Devices** step:

1691            a. **Enable** Supervise Devices.

1692            b. Select **Next**.

1693    Figure 2-146 Device Preparation Options



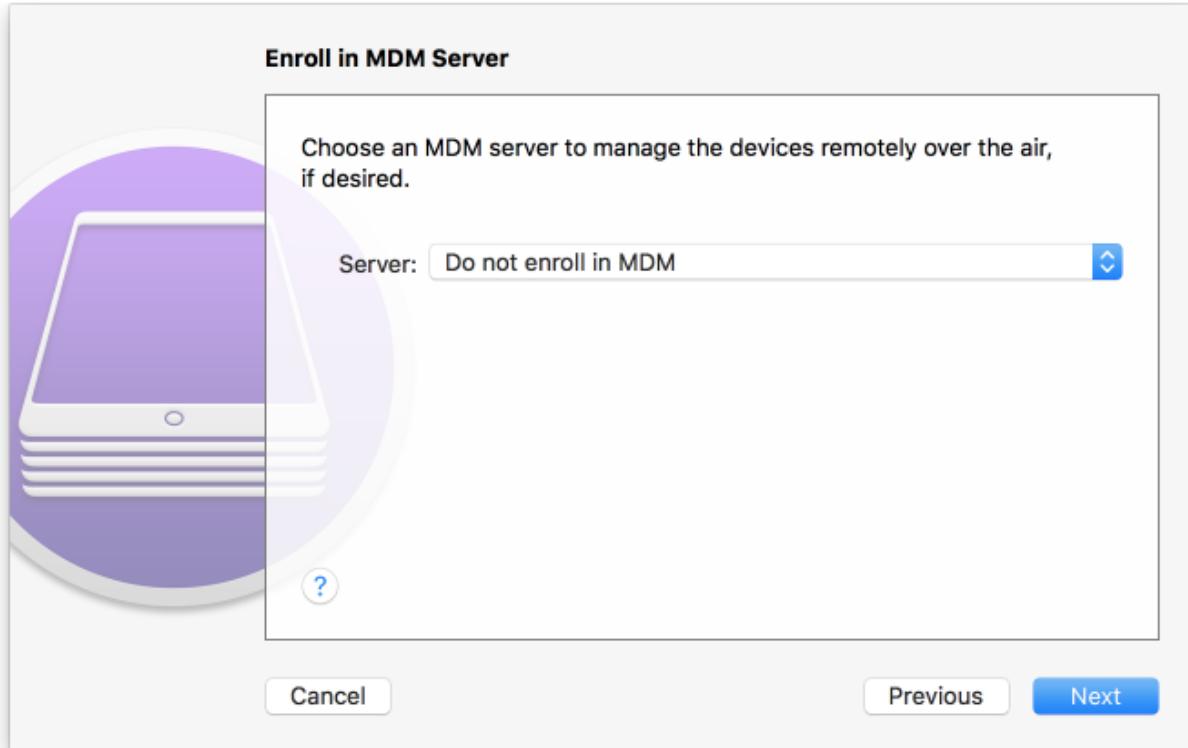
1694

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**.

1698    Figure 2-147 Preparation MDM Server Selection

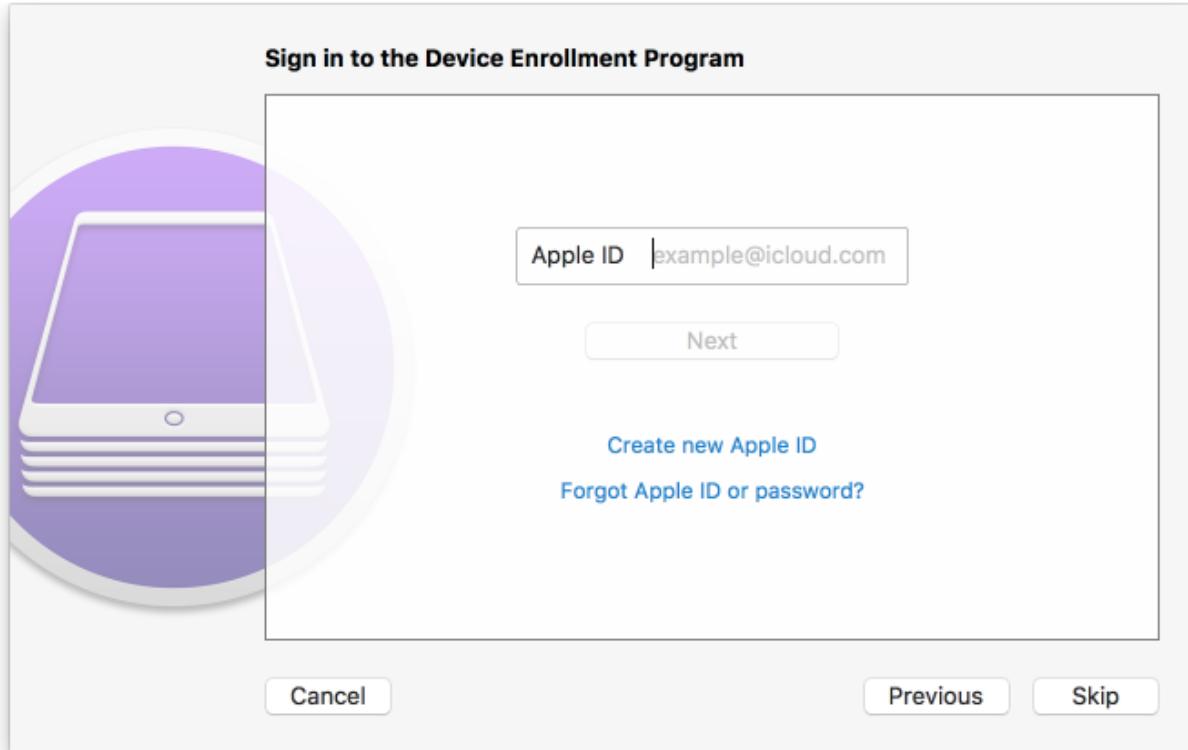


1699

1700

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

1701    Figure 2-148 Signing into Apple Account



1702

1703

7. For the **Assign to Organization** step:

1704

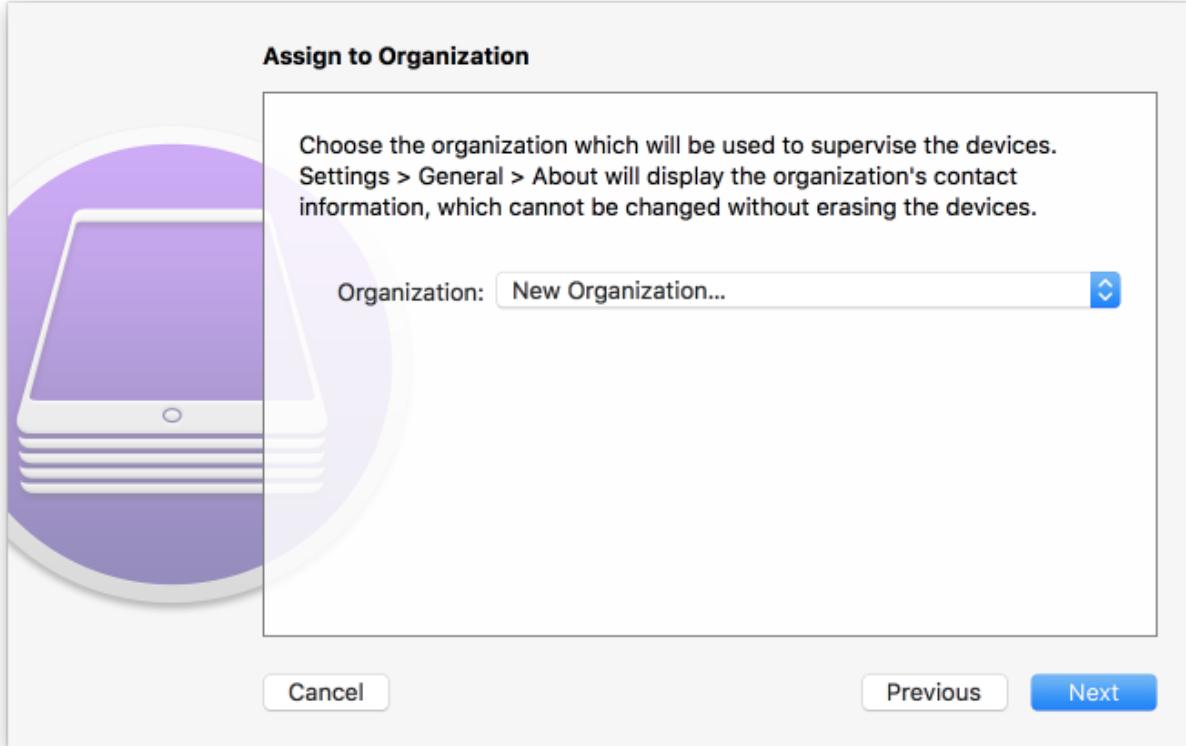
a. If you have previously created your organization, select **Next** and continue with **Step 9**.

1705

1706

b. If you have not created your organization, from the **Organization** drop-down menu, select **New Organization...**

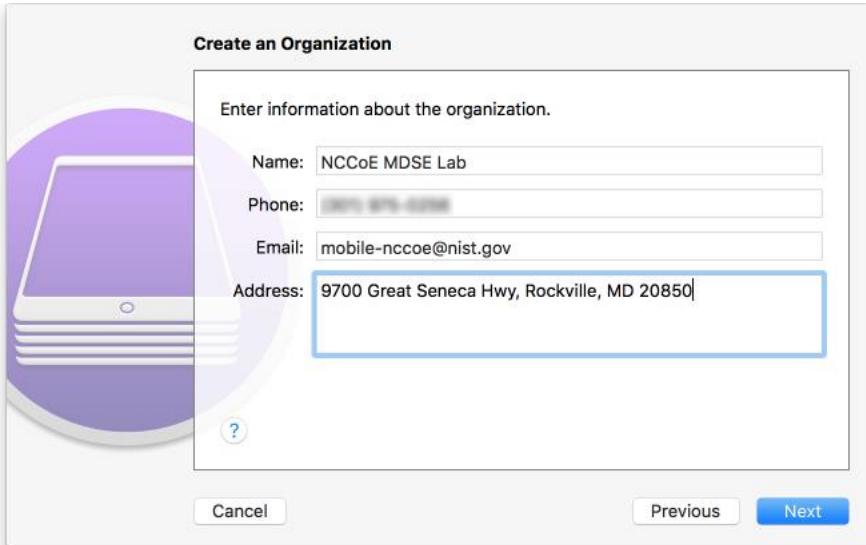
1707 Figure 2-149 Organization Assignment Dialogue



1708

- 1709 8. At the **Create an Organization** screen:
- 1710 a. In the **Name** field, enter the name of your organization.
- 1711 b. In the **Phone** field, enter an appropriate support number for your mobility program.
- 1712 c. In the **Email** field, enter an appropriate support email for your mobility program.
- 1713 d. In the **Address** field, enter the address for your organization.
- 1714 e. Select **Next**.

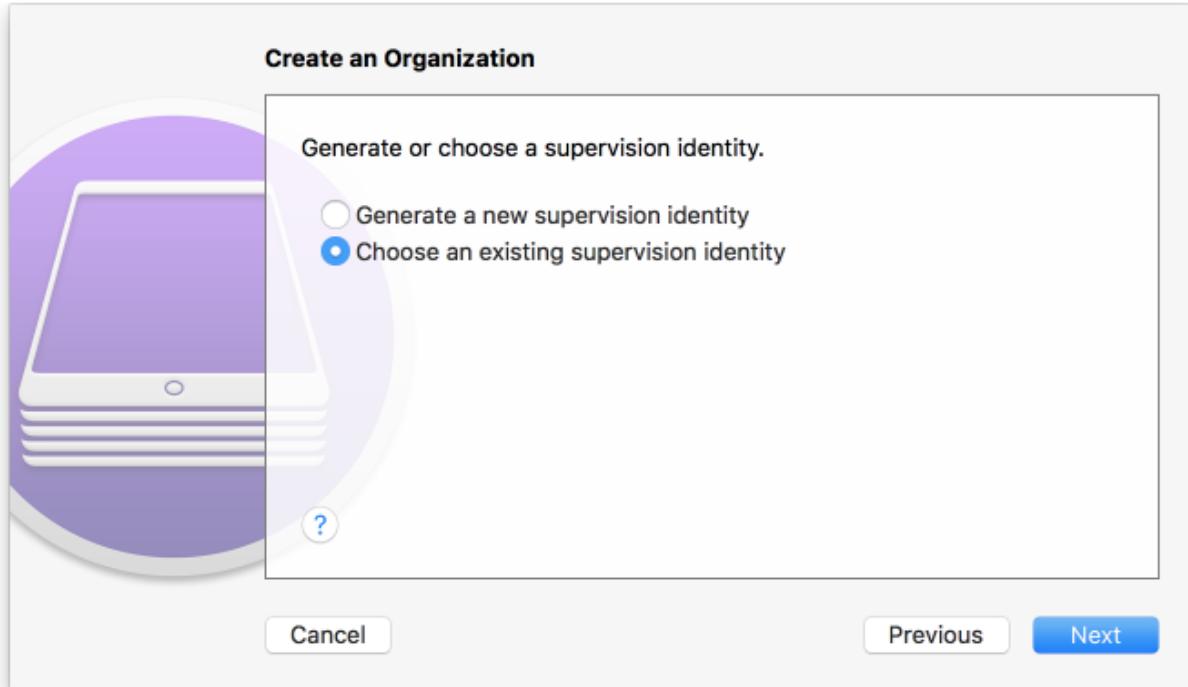
1715    Figure 2-150 Creating an Organization



1716

- 1717    9. If your organization has established a digital identity for placing devices into **Supervised**  
1718    **Mode:**
- 1719    a. Continue with **Step 10.** **Note:** that the same digital identity must be used for any given  
1720    device.
- 1721    b. Otherwise, continue with **Step 14.**
- 1722    10. In the **Create an Organization** screen:
- 1723    a. For the **Generate or choose a supervision identity** option, select **Choose an existing**  
1724    **supervision identity.**
- 1725    b. Select **Next.**

1726 Figure 2-151 Supervisory Identity Configuration

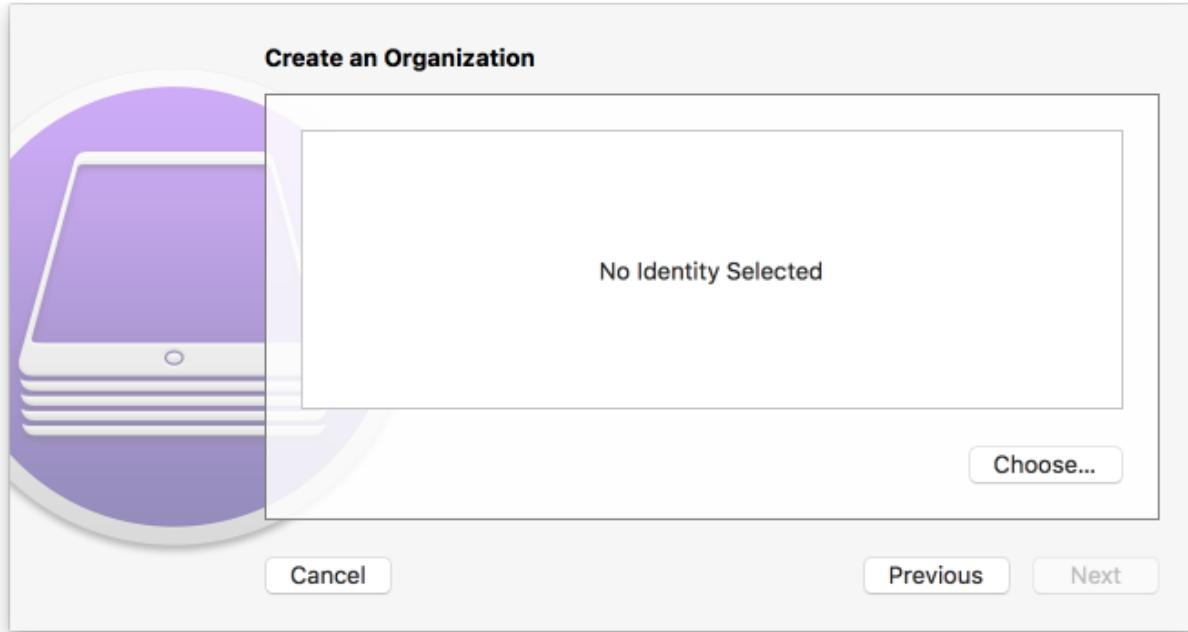


1727

1728

11. Select **Choose...**

1729    Figure 2-152 Organization Selection



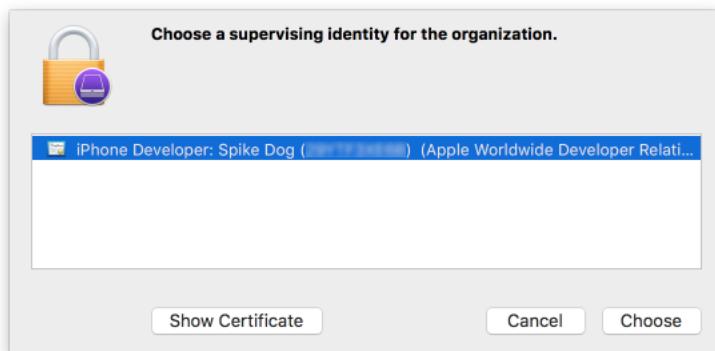
1730

1731        12. At the **Choose a supervising identity for the organization** dialogue:

1732            a. **Select** the digital certificate from the list of those available to the system.

1733            b. Select **Choose**.

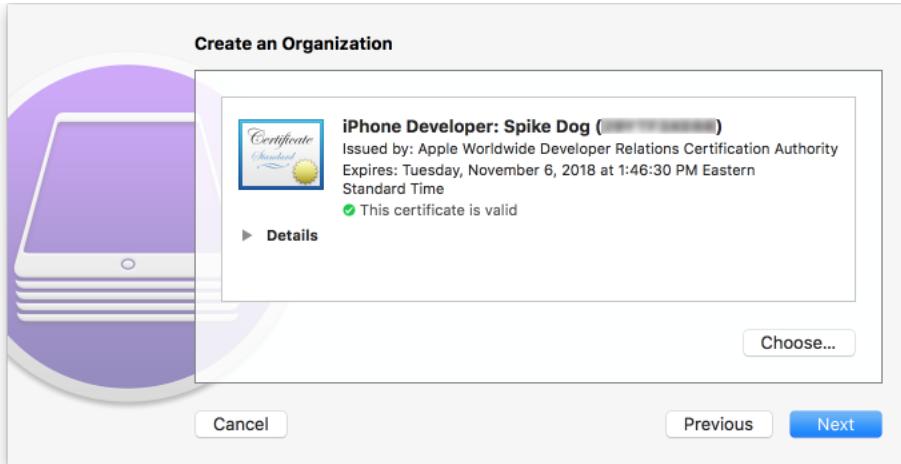
1734    Figure 2-153 Supervising Identity Selection



1735

1736        13. At the **Create an Organization** screen, select **Next**.

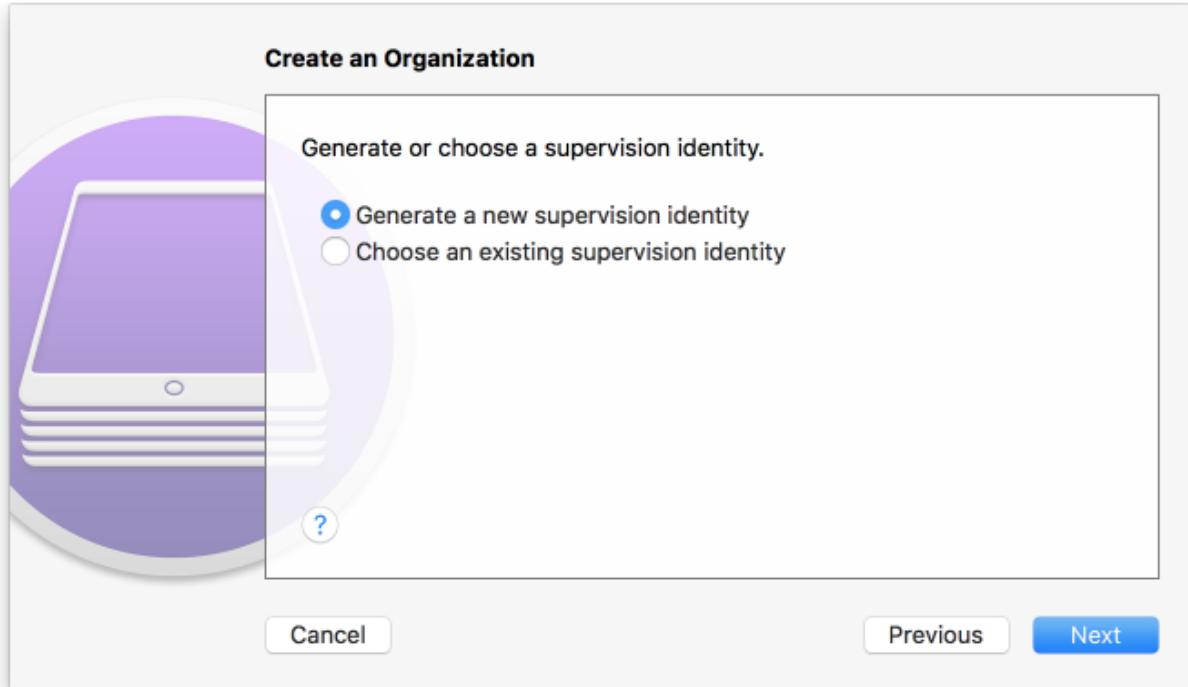
1737    Figure 2-154 Selected Organization



1738

- 1739    14. In the **Create an Organization** screen:
- 1740       a. For the **Generate or choose a supervision identity option**, select **Generate a new**  
1741               **supervision identity**.
- 1742       b. Select **Next**.

1743 Figure 2-155 Create an Organization Supervision Identity Configuration

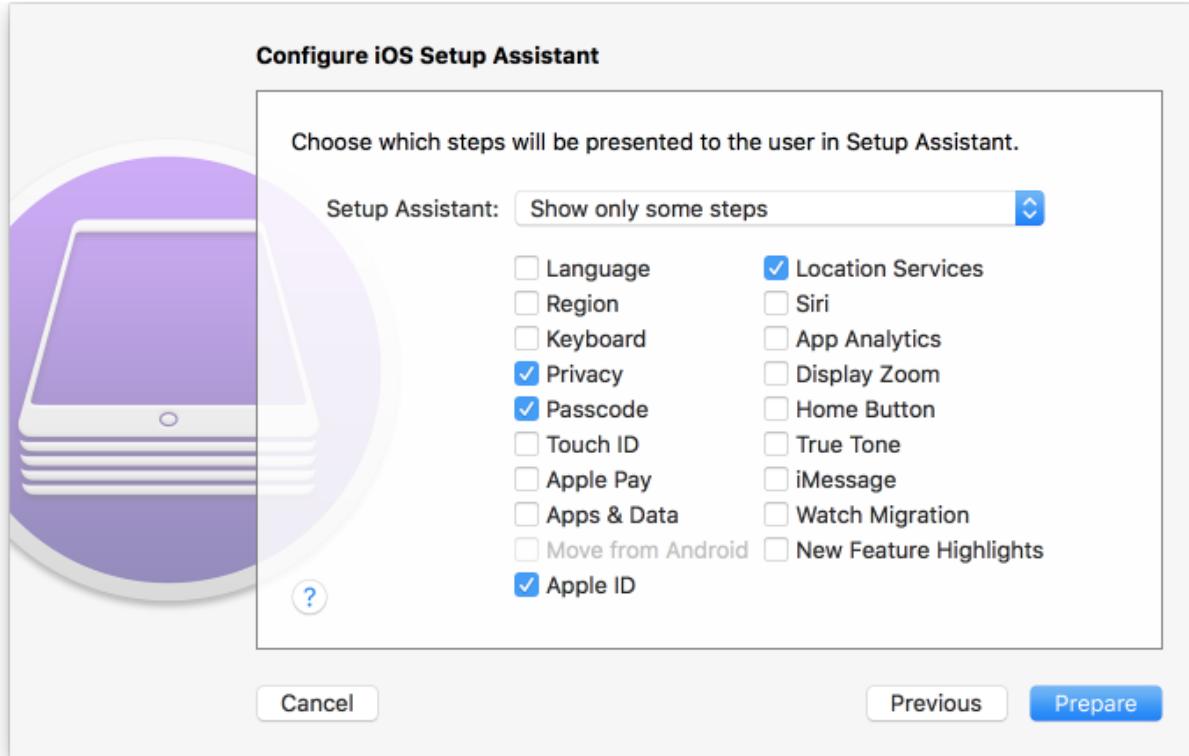


1744

1745 15. For the **Configure iOS Setup Assistant** step:

- 1746 a. Ensure the **Setup Assistant** drop-down menu shows **Show only some steps** selected;  
1747 additional options will appear.
- 1748 b. Enable each of the **Privacy**, **Passcode**, **Apple ID**, and **Location Services** check-boxes.
- 1749 c. Select **Prepare**.

1750 Figure 2-156 Setup Assistant Configuration

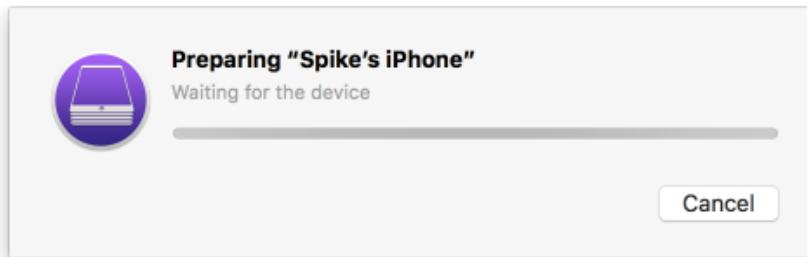


1751

1752        16. Configurator 2 will take several minutes to prepare the device and place it into **Supervised Mode**.

1753

1754 Figure 2-157 Waiting for iPhone



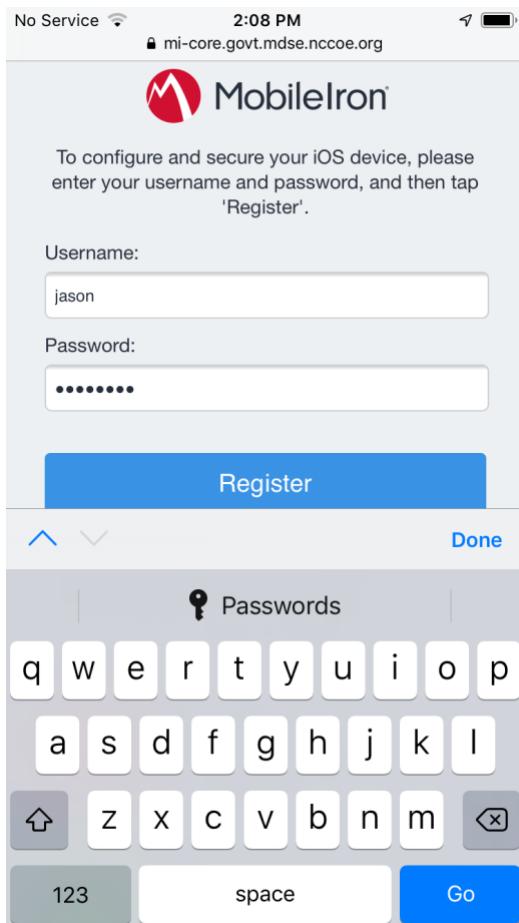
1755

### 2.9.1.3 Registration with MobileIron Core

1756 The following steps will register an iOS device in Supervised Mode with MobileIron Core, which uses a  
1757 web-based process rather than the *Mobile@Work* app.

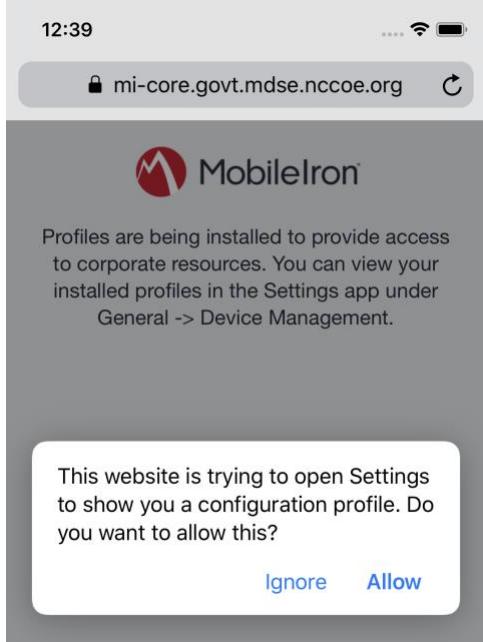
1759           1. Using **Safari**, navigate to **MobileIron Core** page, substituting <FQDN> for that of your  
1760           organization's instance of MobileIron Core. In our example implementation, the resulting  
1761           URL is <https://mi-core.govt.mdse.nccoe.org/go> .

1762 **Figure 2-158 MobileIron Registration Page**



1763  
1764           2. At the **warning** that the web site is trying to open **Settings** to show a configuration profile,  
1765           select **Allow**; the **Settings** built-in app will open.

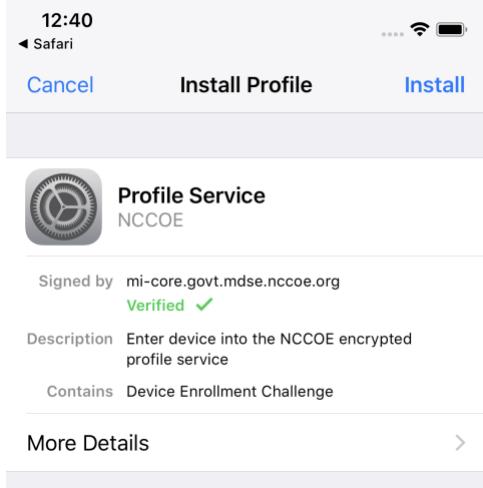
1766 Figure 2-159 Opening Settings Confirmation



1767

1768 3. At the **Settings > Install Profile** screen:1769 a. Verify the **Signed by** field indicates the server identity is **Verified**.1770 b. Select **Install**.

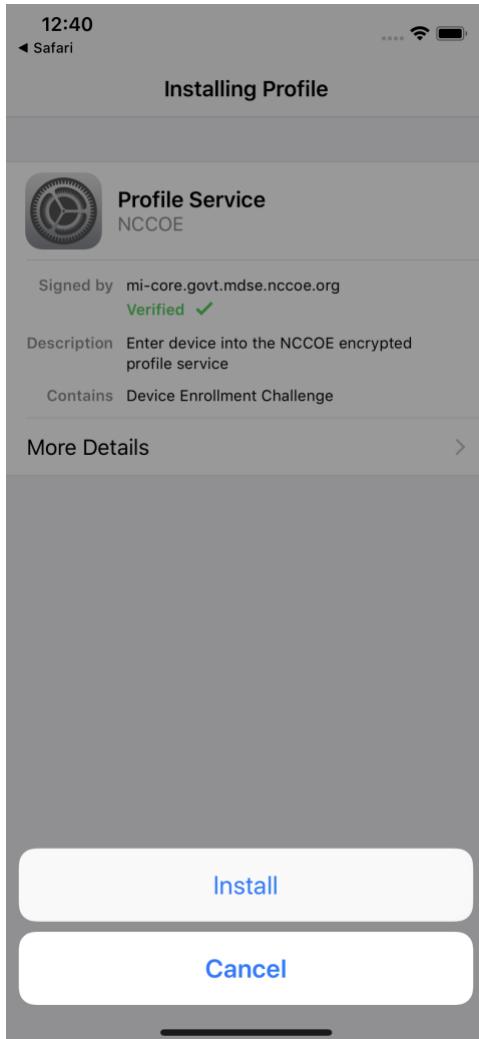
1771 Figure 2-160 Profile Installation



1772

1773 4. At the **Installing Profile** screen, select **Install**.

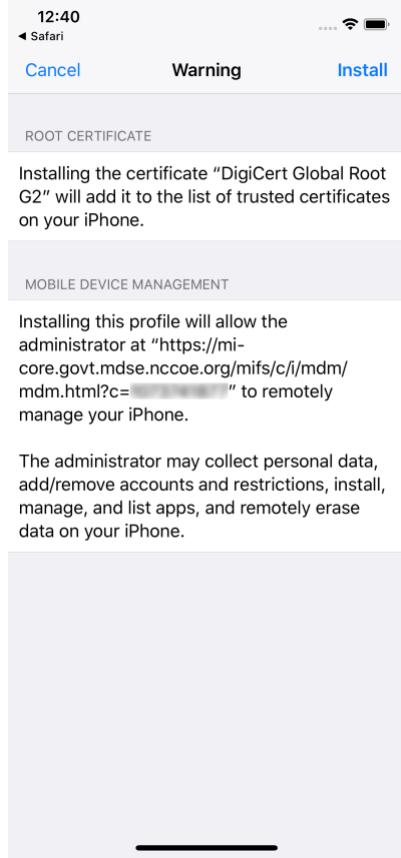
1774 **Figure 2-161 Profile Installation**



1775

1776        5. At the **Warning** screen:

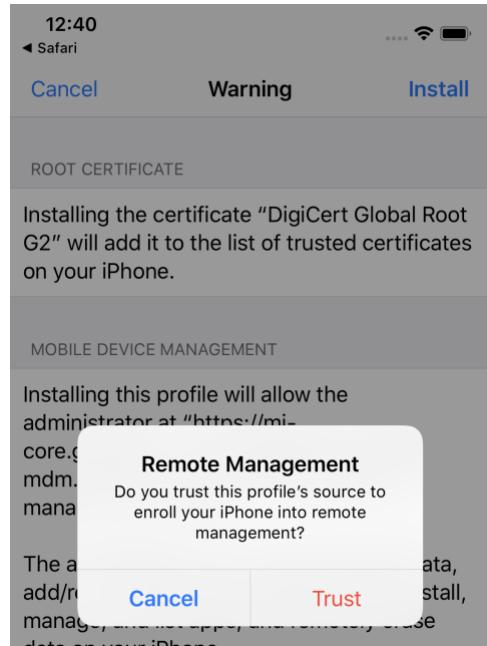
- 1777            a. Verify that information under **Root Certificate** and **MDM** is consistent with information  
1778            provided by your mobile device administrator.
- 1779            b. Select **Install**.

1780 **Figure 2-162 Profile Installation Warning**

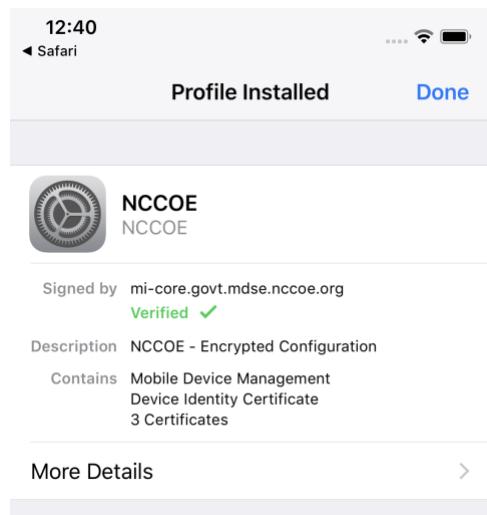
1781

1782

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

1783 **Figure 2-163 Profile Installation Trust Confirmation**

- 1784  
1785     7. At the **Profile Installed** screen, select **Done**. The device is now registered with MobileIron.

1786 **Figure 2-164 Profile Installation Confirmation**

- 1787  
1788 **2.9.2 Activating Lookout for Work on iOS**  
1789 The configuration of the Lookout for Work (iOS) app in the MobileIron app catalog causes a  
1790 configuration file to be included during automatic install. As a result, when a user first launches Lookout

1791 for Work, it should be activated without any user interaction. Additional action is required to grant  
1792 Lookout for Work the permissions necessary for it to provide optimal protection.

1793 1. Launch the **Lookout for Work** app; activation occurs silently at the **splash** screen.

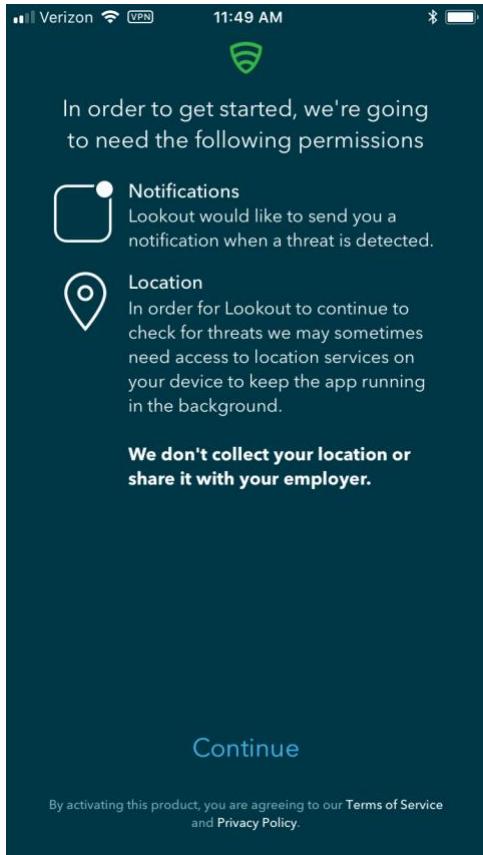
1794 **Figure 2-165 Lookout for Work Splash Screen**



1795

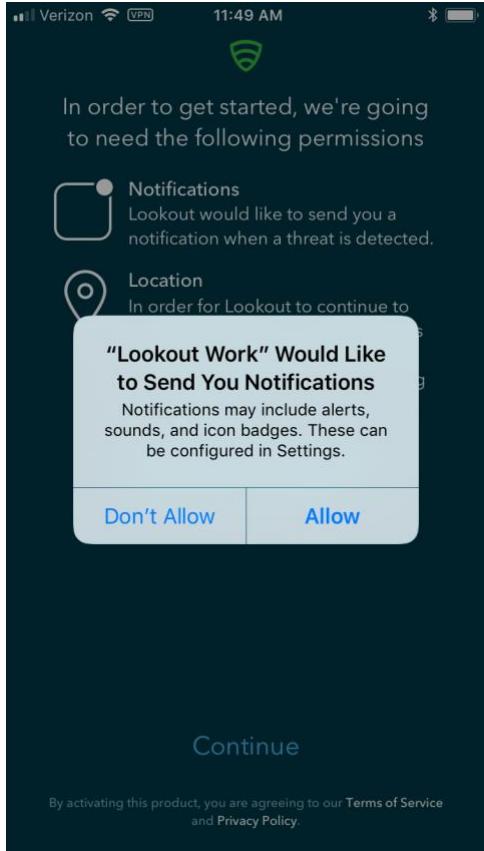
1796 2. At the **welcome** screen, select **Continue**.

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



1798

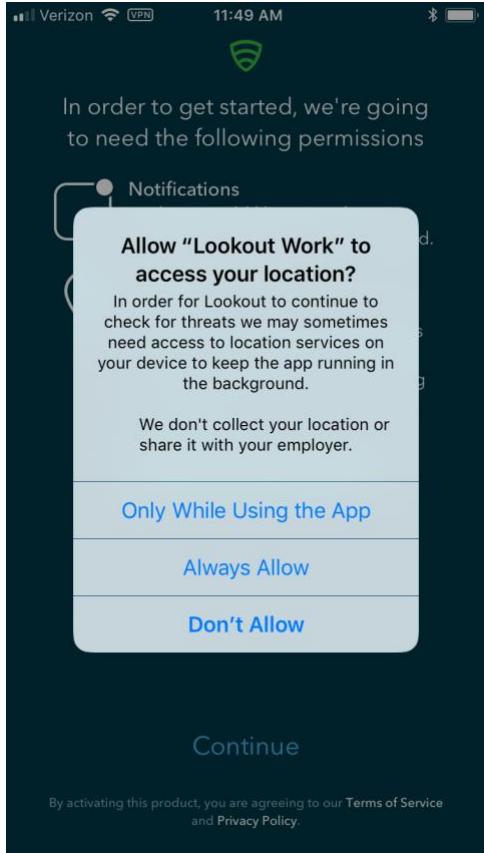
1799 3. At the "Lookout Work" Would Like to Send You Notifications dialogue, select **Allow**.

1800 **Figure 2-167 Notifications Permissions Prompt**

1801

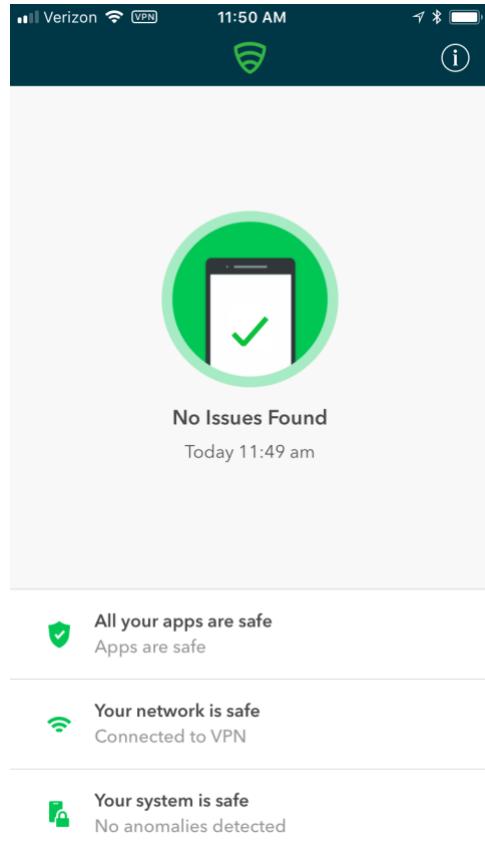
1802

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

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

1804

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

1807 **Figure 2-169 Lookout for Work Home Screen**

1808

### 2.9.3 Provisioning Work-Managed Android Devices with a Work Profile

1810 In this scenario, Android devices are deployed as work-managed with a work profile. Enabling this  
1811 feature for AFW-capable devices requires a change to the AFW configuration. It also requires that the  
1812 device user already has a personal Google account to provision the work profile; it is not created as part  
1813 of the workflow to register a device with MobileIron Core.

#### 2.9.3.1 Enable Work Profile on Work-Managed Devices

- 1815 1. In the **MobileIron Admin** Portal, navigate to **Policies > Configs > Configurations**.
- 1816 2. **Enable** the check box in the row for the **AFW** configuration.
- 1817 3. In the **Configuration Details** pane, select **Edit**.

1818    Figure 2-170 MobileIron AFW Configuration

| Name                                  | Configuration     | Bundle/Package ID      | Description | # Phones | Configuration Details |
|---------------------------------------|-------------------|------------------------|-------------|----------|-----------------------|
| Activate Lookout                      | MANAGED APPLIANCE | com.lookout.work       | Activ...    | 4        |                       |
| <b>Android for Work Configuration</b> | ANDROIDFOR...     |                        | Create...   | 12       | <b>Edit</b>           |
| Appthority Mobile Intelligence...     | MANAGED APPLIANCE | com.appthority.Appt... | Identifi... | 4        |                       |

**Android for Work Configuration**  
Device Space: Global

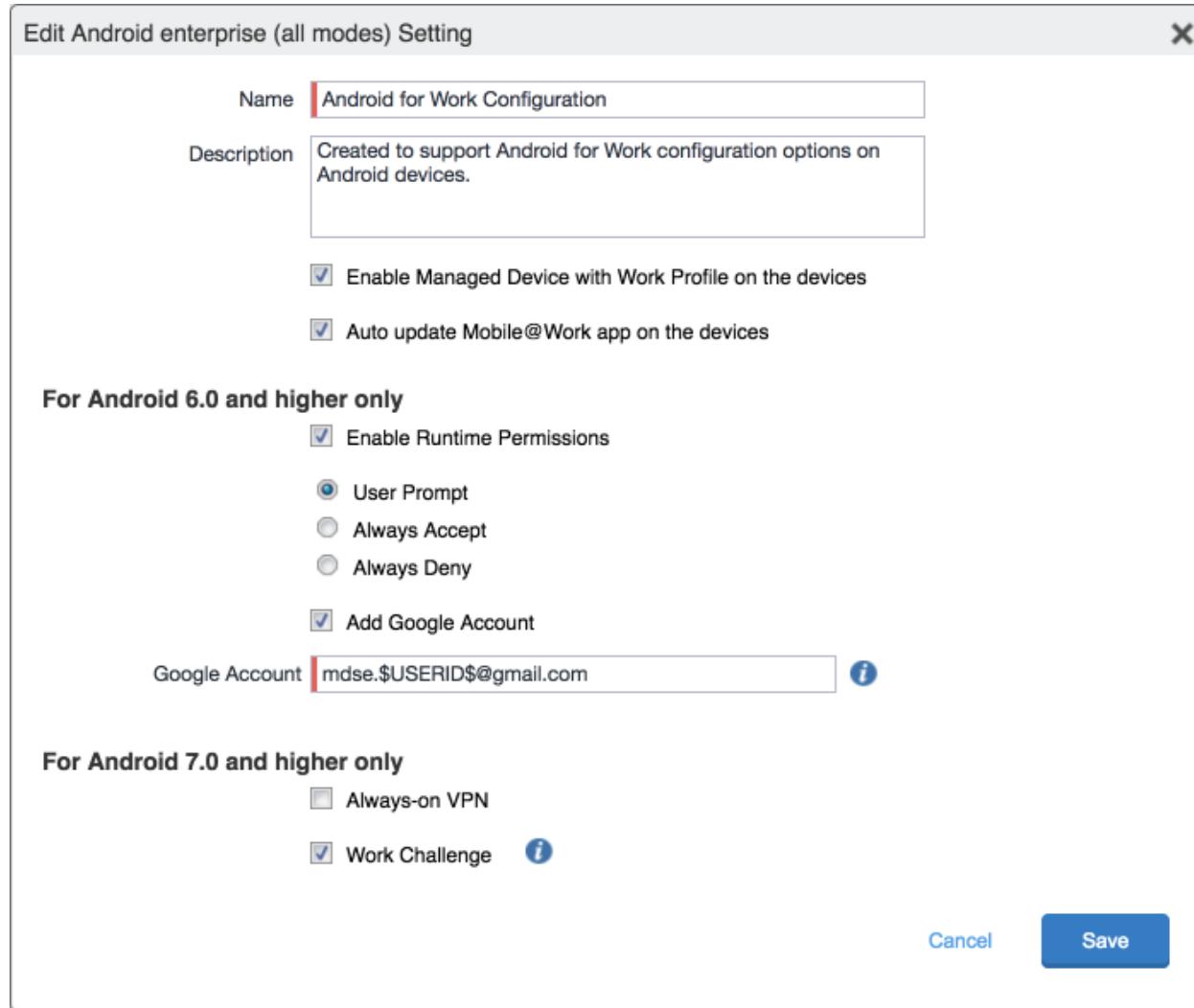
1819

1820    4. In the **Edit Android enterprise (all modes) Setting** dialogue:1821        a. Enable **Enable Managed Devices with Work Profile** on the devices.1822        b. Enable **Add Google account**.

1823        c. In the **Google Account** text box, provide a valid Google domain account. The example in  
 1824        our reference implementation will map a MobileIron user ID of gema to and email  
 1825        address of **mdse.gema@gmail.com**. See *MobileIron Core 9.4.0.0 Device Management*  
 1826        *Guide for AFW* for a list of variables to appropriately adapt this field to your existing  
 1827        identity management strategy.

1828        d. Select **Save**.

1829 Figure 2-171 AFW Configuration

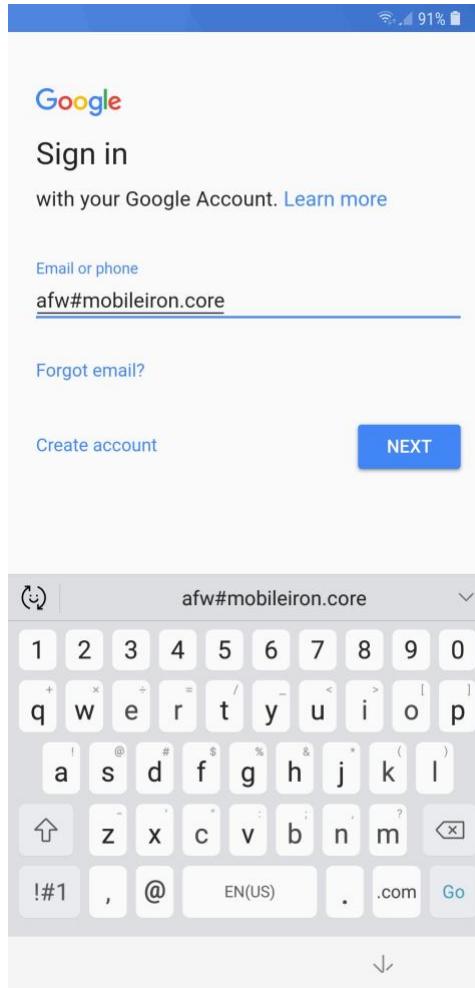


1830

1831 *2.9.3.2 Registering Android Devices*1832 The following steps can only be completed when working with an Android device that is still set to (or  
1833 has been reset to) factory default settings.1834 5. When prompted to **sign in** with your Google Account:

- 1835 a. In the **Email or phone field**, enter **afw#mobileiron.core**.
- 1836 b. Select **Next**.

1837    Figure 2-172 MobileIron Enrollment Process



1838

- 1839         6. When **AFW** prompts you to install *Mobile@Work*, select **Install**; this will download the  
1840         *Mobile@Work* client to the device.

1841    **Figure 2-173 AFW Enrollment**



## Android for Work

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



Mobile@Work

SKIP

INSTALL

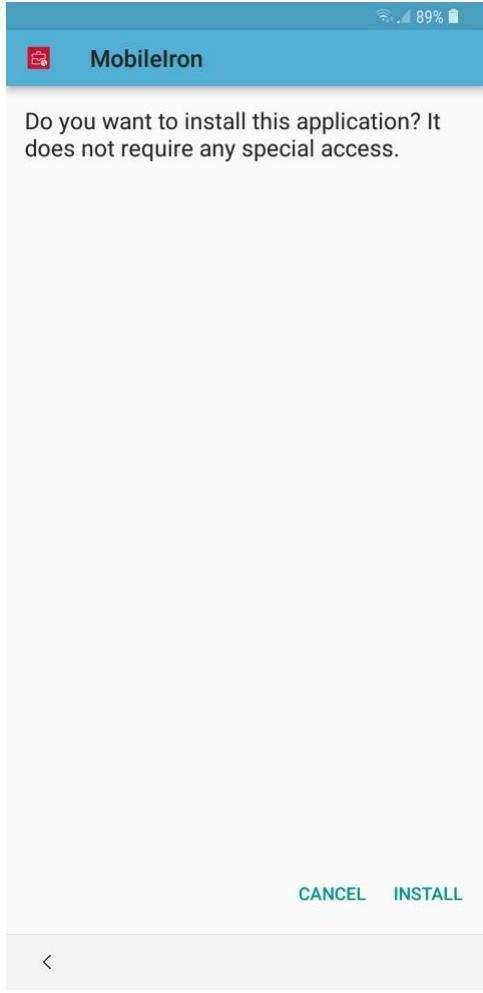
1842



1843

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

1844      **Figure 2-174 MobileIron Installation**



1845

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

1847 **Figure 2-175 Accepting AFW Terms and Conditions**

### Set up your device

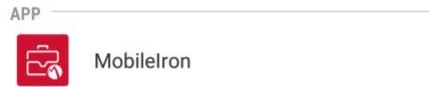
Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information.

[Knox Terms and Conditions](#)

[Privacy Policy](#)

[Google](#)

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



1848

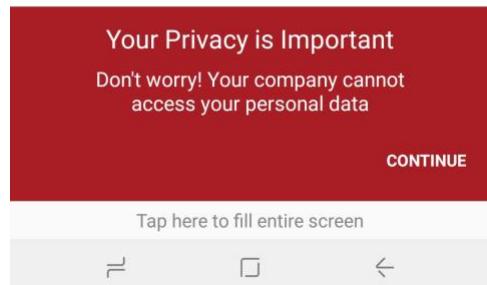
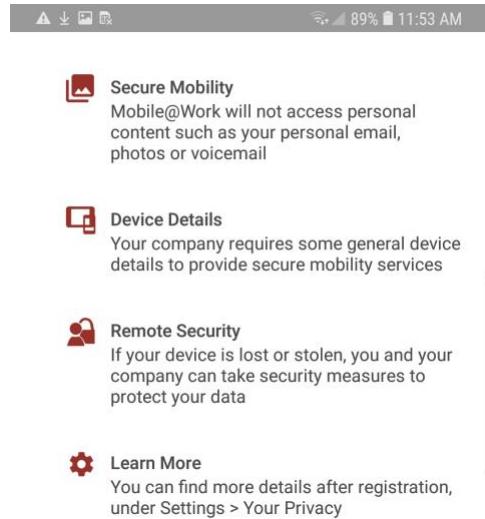


1849

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.

1850

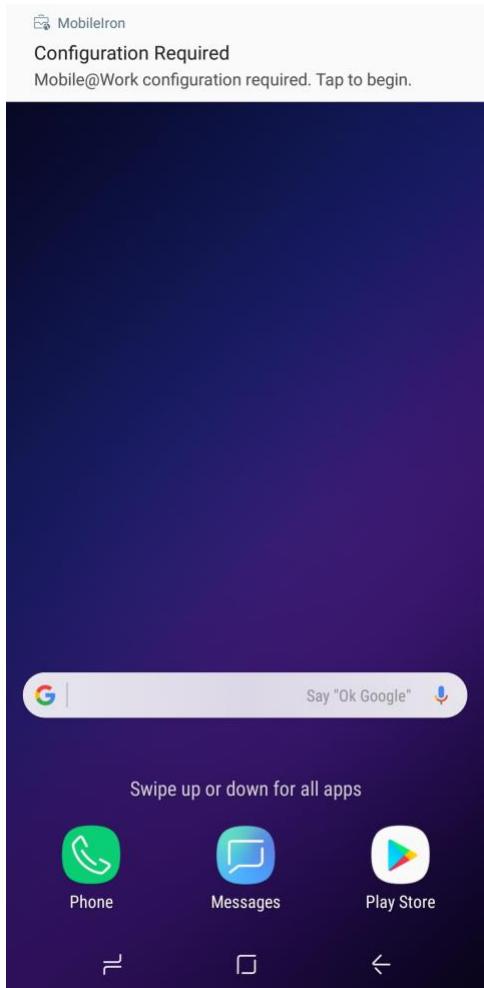
1851

1852 **Figure 2-176 MobileIron Privacy Information**

1853

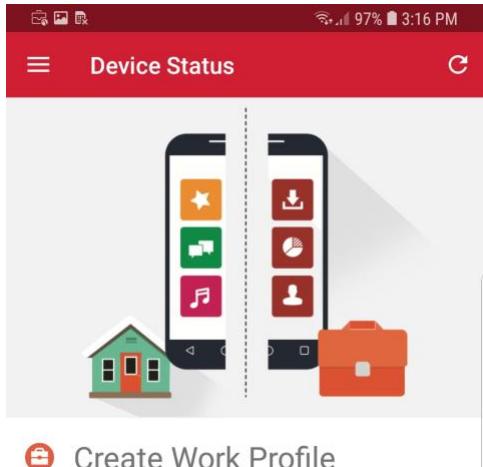
1854 10. When MobileIron sends a **Configuration Required** notification, select the **notification**.

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

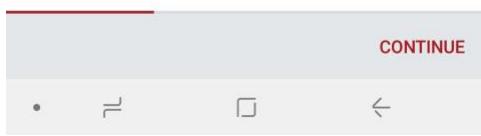


1856

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

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

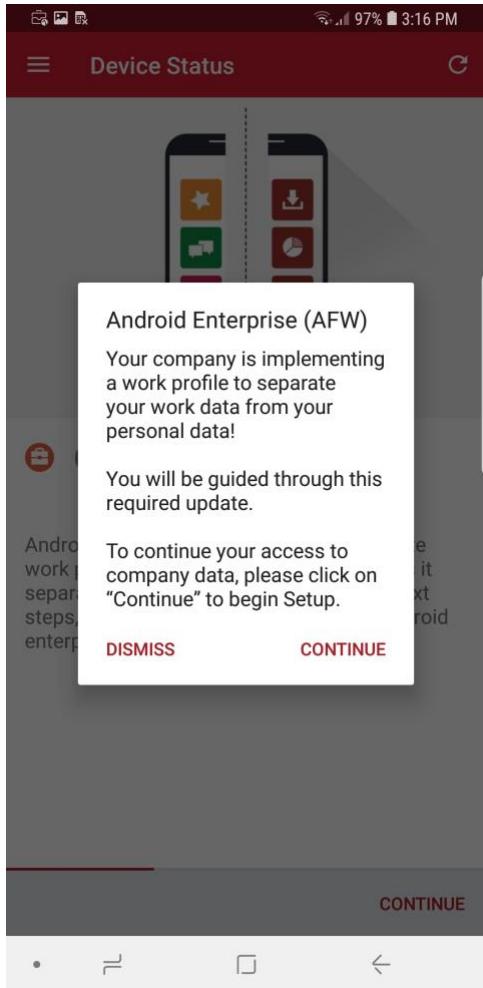
Android enterprise (AFW) creates a separate work profile to access work data and keeps it separate from your personal data. In the next steps, you will be guided to set up your Android enterprise (AFW) profile.



1859

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

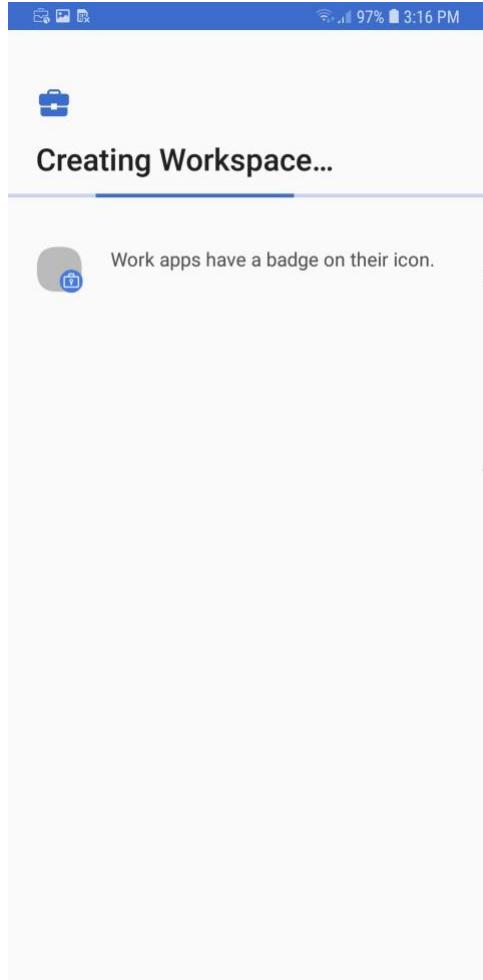
1861    **Figure 2-179 AFW Configuration**



1862

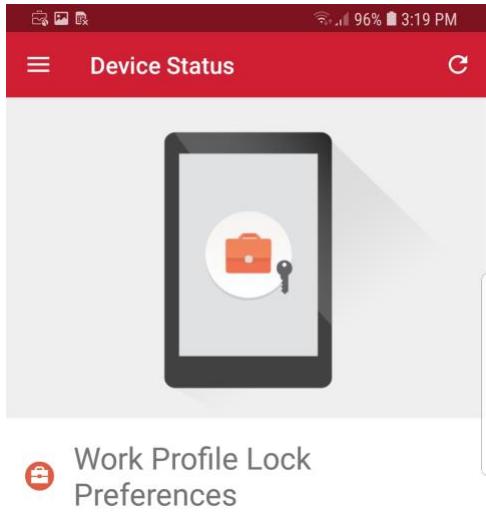
1863        13. AFW will notify the user that it is creating the personal workspace. The next two screens repeat **Steps 7** and **8** as above.  
1864

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



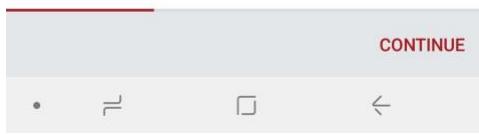
1866

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

1868 **Figure 2-181 MobileIron Work Profile Lock Preferences**

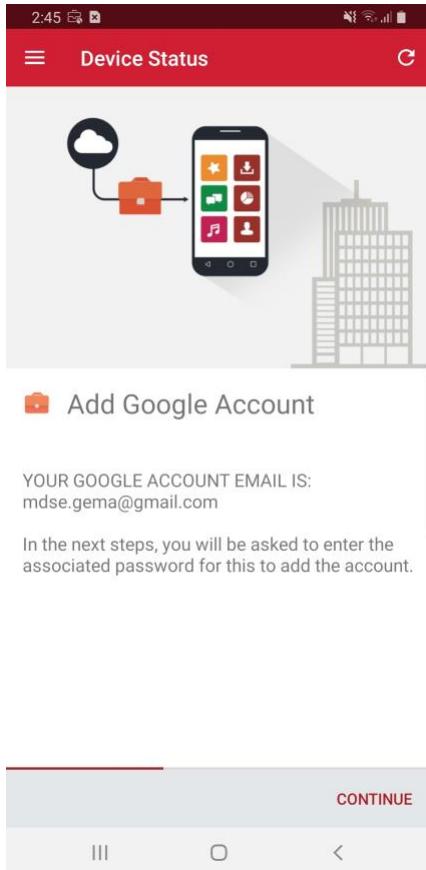
On the next screen, you will set up the work profile lock for your device.

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



1869

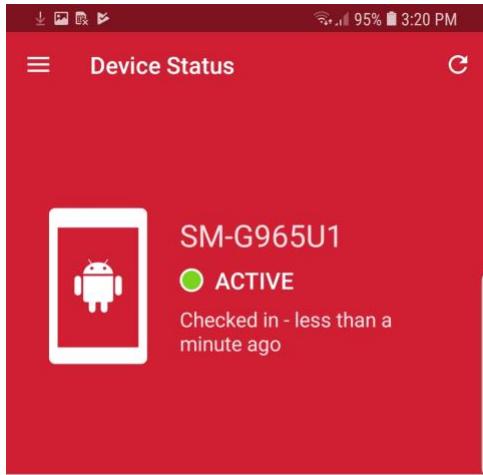
- 1870        15. The user will be prompted to create a passcode to protect the AFW container.  
1871        16. At the **Device Status > Add Google Account** screen, select **Continue**.

1872 **Figure 2-182 MobileIron Google Account Configuration**

1873

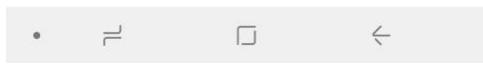
- 1874        17. The user will be prompted to authenticate to the same Google domain account mapped to  
1875           their MobileIron account based on the email address set in the AFW configuration in  
1876           MobileIron Core. In our example implementation, the mapped Google account is  
1877           **mdse.gema@gmail.com**.
- 1878        18. Once the *Mobile@Work* app has been provisioned with the user's account, the Device  
1879           Status screen should appear; the device has now successfully been provisioned into  
1880           MobileIron.

1881 Figure 2-183 MobileIron Device Status



✓ You're all set!  
Currently there are no updates needing  
your attention.

1882



## Appendix A List of Acronyms

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

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

## Appendix B    Glossary

|   |   |
|---|---|
| <b>Application Programming Interface (API)</b>      | 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]   |
| <b>App-Vetting Process</b>                          | 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]  |
| <b>Authenticate</b>                                 | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system [3]  |
| <b>Certificate</b>                                  | 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] |
| <b>Certificate Authority (CA)</b>                   | A trusted entity that issues and revokes public key certificates [5]  |
| <b>Demilitarized Zone (DMZ)</b>                     | 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]   |
| <b>Derived Personal Identity Verification (PIV)</b> | 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]  |
| <b>Hypertext Transfer Protocol (HTTP)</b>           | A standard method for communication between clients and Web servers [8]   |
| <b>Hypertext Transfer Protocol Secure (HTTPS)</b>   | HTTP transmitted over TLS [9]   |
| <b>Internet Protocol (IP) addresses</b>             | Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks [10]  |

|   |   |
|---|---|
| <b>Lightweight Directory Access Protocol (LDAP)</b> | 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]   |
| <b>Local Area Network (LAN)</b>                     | 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]   |
| <b>Mutual Authentication</b>                        | The process of both entities involved in a transaction verifying each other [13]  |
| <b>Passphrase</b>                                   | 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]  |
| <b>Personal Identity Verification (PIV)</b>         | 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] |
| <b>Risk Analysis</b>                                | 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]   |
| <b>Risk Assessment</b>                              | 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]   |
| <b>Root Certificate Authority (CA)</b>              | 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].