

NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security:

Bring Your Own Device (BYOD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz
Jason Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

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

November 2022

SECOND DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security: Bring Your Own Device (BYOD)

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B);
Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)*

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkowitz

*Applied Cybersecurity Division
Information Technology Laboratory*

Jason Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

*The MITRE Corporation
McLean, VA*

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

SECOND DRAFT

November 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Mobile Device Security:

Bring Your Own Device (BYOD)

Volume A:
Executive Summary

Kaitlin Boeckl

Nakia Grayson

Gema Howell

Naomi Lefkovitz

Applied Cybersecurity Division
Information Technology Laboratory

Jason Ajmo

Milissa McGinnis*

Kenneth F. Sandlin

Oksana Slivina

Julie Snyder

Paul Ward

The MITRE Corporation
McLean, VA

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

November 2022

SECOND DRAFT

This publication is available free of charge from

<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



1 Executive Summary

2 Many organizations provide employees the flexibility to use their personal mobile devices to perform
3 work-related activities. An ineffectively secured personal mobile device could expose an organization or
4 employee to data loss or a privacy compromise. Ensuring that an organization's data is protected when
5 it is accessed from personal devices poses unique challenges and threats.

6 Allowing employees to use their personal mobile devices for work-related activities is commonly known
7 as a bring your own device (BYOD) deployment. A BYOD deployment offers a convenient way to
8 remotely access organizational resources, while avoiding the alternative of carrying both a work phone
9 and personal phone. This NIST Cybersecurity Practice Guide demonstrates how organizations can use
10 standards-based, commercially available products to help meet their BYOD security and privacy needs.

11 CHALLENGE

12 BYOD devices can be used interchangeably for
13 work and personal purposes throughout the
14 day. While flexible and convenient, BYOD can
15 introduce challenges to an enterprise. These
16 challenges can include additional
17 responsibilities and complexity for information
18 technology (IT) departments caused by
19 supporting many types of personal mobile
20 devices used by the employees, enterprise
21 security threats arising from unprotected
22 personal devices, as well as challenges
23 protecting the privacy of employees and their
24 personal data stored on their mobile devices.

An ineffectively secured personal mobile device could expose an organization or employee to data loss or a privacy compromise.

25 SOLUTION

26 The National Cybersecurity Center of Excellence (NCCoE) collaborated with the mobile community and
27 cybersecurity technology providers to build a simulated BYOD environment. Using commercially
28 available products, the example solution's technologies and methodologies can enhance the security
29 posture of the adopting organization and help protect employee privacy and organizational information
30 assets.

This practice guide can help your organization:

- **protect data** from being accessed by unauthorized persons when a device is stolen or misplaced
- **reduce risk to employees** through enhanced privacy protections
- **improve the security of mobile devices and applications** by deploying mobile device technologies
- **reduce risks to organizational data** by separating personal and work-related information from each other

- **enhance visibility** into mobile device health to facilitate identification of device and data compromise, and permit efficient user notification
- **leverage industry best practices** to enhance mobile device security and privacy
- **engage stakeholders** to develop an enterprise-wide policy to inform management and employees of acceptable practices

31 The example solution uses technologies and security capabilities (shown below) from our project
 32 collaborators. The technologies used in the solution support security and privacy standards and
 33 guidelines including the NIST Cybersecurity Framework and NIST Privacy Framework, among others.
 34 Both iOS and Android devices are supported by this guide’s example solution.

Collaborator	Security Capability or Component
	Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance
	Application Vetting to determine if an application demonstrates behaviors that could pose a security or privacy risk
	Firewall and Virtual Private Network that controls network traffic and provides encrypted communication channels between mobile devices and other hosts
	Trusted Execution Environment that helps protect mobile devices from computer code with integrity issues
	Mobile Threat Defense detects unwanted activity and informs the device owner and BYOD administrators to prevent or limit harm that an attacker could cause

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

41 HOW TO USE THIS GUIDE

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

43 **Business decision makers, including chief information security and technology officers** can use this
44 part of the guide, *NIST SP 1800-22a: Executive Summary*, to understand the impetus for the guide, the
45 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could
46 benefit your organization.

47 **Technology, security, and privacy program managers** who are concerned with how to identify,
48 understand, assess, and mitigate risk can use the following:

- 49 ▪ *NIST SP 1800-22b: Approach, Architecture, and Security Characteristics*, which describes what
50 we built and why, the risk analysis performed, and the security/privacy control mappings.
- 51 ▪ *NIST SP 1800-22 Supplement: Example Scenario: Putting Guidance into Practice*, which provides
52 an example of a fictional company using this practice guide and other NIST guidance to
53 implement a BYOD deployment with their security and privacy requirements.

54 **IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-22c: How-*
55 *To Guides*, which provides specific product installation, configuration, and integration instructions for
56 building the example implementation, allowing you to replicate all or parts of this project.

57 SHARE YOUR FEEDBACK

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

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

66

67 COLLABORATORS

68 Collaborators participating in this project submitted their capabilities in response to an open call in the
69 Federal Register for all sources of relevant security capabilities from academia and industry (vendors
70 and integrators). Those respondents with relevant capabilities or product components signed a
71 Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to
72 build this example solution.

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

Mobile Device Security:

Bring Your Own Device (BYOD)

Volume B:
Approach, Architecture, and Security Characteristics

Kaitlin Boeckl

Nakia Grayson

Gema Howell

Naomi Lefkowitz

Applied Cybersecurity Division
Information Technology Laboratory

Jason Ajmo

Milissa McGinnis*

Kenneth F. Sandlin

Oksana Slivina

Julie Snyder

Paul Ward

The MITRE Corporation
McLean, VA

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

November 2022

SECOND DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



1 **DISCLAIMER**

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

8 While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk
9 through outreach and application of standards and best practices, it is the stakeholder’s responsibility to
10 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise,
11 and the impact should the threat be realized before adopting cybersecurity measures such as this
12 recommendation.

13 National Institute of Standards and Technology Special Publication 1800-22B Natl. Inst. Stand. Technol.
14 Spec. Publ. 1800-22B, 92 pages, (November 2022), CODEN: NSPUE2

15 **FEEDBACK**

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

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

19 Public comment period: November 29, 2022 through January 13, 2023

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

21 National Cybersecurity Center of Excellence
22 National Institute of Standards and Technology
23 100 Bureau Drive
24 Mailstop 2002
25 Gaithersburg, MD 20899
26 Email: nccoe@nist.gov

27 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

43 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

53 **ABSTRACT**

54 Bring Your Own Device (BYOD) refers to the practice of performing work-related activities on personally
55 owned devices. This practice guide provides an example solution demonstrating how to enhance
56 security and privacy in Android and iOS smartphone BYOD deployments.

57 Incorporating BYOD capabilities into an organization can provide greater flexibility in how employees
58 work and increase the opportunities and methods available to access organizational resources. For some
59 organizations, the combination of traditional in-office processes with mobile device technologies
60 enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-
61 first approach in which their employees communicate and collaborate primarily using their mobile
62 devices.

63 However, some of the features that make BYOD mobile devices increasingly flexible and functional also
 64 present unique security and privacy challenges to both work organizations and device owners. The
 65 unique nature of these challenges is driven by the diverse range of devices available that vary in type,
 66 age, operating system (OS), and the level of risk posed.

67 Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks to organizations.
 68 Solutions that are designed to secure corporate devices and on-premise data do not provide an effective
 69 cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the unique risks
 70 that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new privacy risks to
 71 employees by providing their employer a degree of access to their personal devices, thereby opening up
 72 the possibility of observation and control that would not otherwise exist.

73 To help organizations benefit from BYOD’s flexibility while protecting themselves from many of its
 74 critical security and privacy challenges, this Practice Guide provides an example solution using
 75 standards-based, commercially available products and step-by-step implementation guidance.

76 **KEYWORDS**

77 *Bring your own device; BYOD; mobile device management; mobile device security.*

78 **ACKNOWLEDGMENTS**

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

Name	Organization
Donna Dodson*	NIST
Joshua M. Franklin*	NIST
Jeff Greene	NIST
Natalia Martin	NIST
William Newhouse	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST
Chris Brown	The MITRE Corporation
Nancy Correll*	The MITRE Corporation

Name	Organization
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston*	The MITRE Corporation
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Erin Wheeler*	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward	IBM
Cesare Coscia	IBM
Chris Gogoel	Kryptowire (now known as Quokka)
Tom Karygiannis	Kryptowire (now known as Quokka)
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Mikel Draghici*	Zimperium

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

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

Technology Partner/Collaborator	Build Involvement
IBM	Mobile Device Management
Kryptowire (now known as Quokka)	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

85 **DOCUMENT CONVENTIONS**

86 The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the
 87 publication and from which no deviation is permitted. The terms “should” and “should not” indicate that
 88 among several possibilities, one is recommended as particularly suitable without mentioning or
 89 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in
 90 the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms
 91 “may” and “need not” indicate a course of action permissible within the limits of the publication. The
 92 terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

93 **CALL FOR PATENT CLAIMS**

94 This public review includes a call for information on essential patent claims (claims whose use would be
 95 required for compliance with the guidance or requirements in this Information Technology Laboratory
 96 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
 97 or by reference to another publication. This call also includes disclosure, where known, of the existence
 98 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
 99 unexpired U.S. or foreign patents.

100 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-
 101 ten or electronic form, either:

- 102 a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
- 103 currently intend holding any essential patent claim(s); or

104 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
105 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
106 publication either:

- 107 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
- 108 or
- 109 2. without compensation and under reasonable terms and conditions that are demonstrably free
- 110 of any unfair discrimination.

111 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
112 behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-
113 sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that
114 the transferee will similarly include appropriate provisions in the event of future transfers with the goal
115 of binding each successor-in-interest.

116 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
117 whether such provisions are included in the relevant transfer documents.

118 Such statements should be addressed to: mobile-nccoe@nist.gov.

119 **CONTENTS**

120 **1 Summary 1**

121 1.1 Challenge 1

122 1.2 Solution..... 3

123 1.2.1 Standards and Guidance 4

124 1.3 Benefits..... 4

125 **2 How to Use This Guide 4**

126 2.1 Typographic Conventions..... 6

127 **3 Approach 7**

128 3.1 Audience..... 7

129 3.2 Scope 8

130 3.3 Assumptions 8

131 3.4 Risk Assessment 9

132 **4 Architecture..... 10**

133 4.1 Common BYOD Risks and Potential Goals to Remediate Those Risks 11

134 4.1.1 Threat Events 11

135 4.1.2 Privacy Risks 11

136 4.1.3 Security and Privacy Goals 12

137 4.2 Example Scenario: Putting Guidance into Practice 13

138 4.3 Technologies that Support the Security and Privacy Goals of the Example Solution . 14

139 4.3.1 Trusted Execution Environment 14

140 4.3.2 Enterprise Mobility Management..... 14

141 4.3.3 Virtual Private Network 15

142 4.3.4 Mobile Application Vetting Service..... 16

143 4.3.5 Mobile Threat Defense 17

144 4.3.6 Mobile Operating System Capabilities..... 17

145 4.4 Architecture Description 19

146 4.5 Enterprise Integration of the Employees’ Personally Owned Mobile Devices 21

147 4.5.1 Microsoft Active Directory Integration 22

148 4.5.2 Mobile Device Enrollment 23

149 4.6 Mobile Components Integration 23

150 4.6.1 Zimperium–MaaS360..... 24

151 4.6.2 Kryptowire–MaaS360 25

152 4.6.3 Palo Alto Networks–MaaS360 25

153 4.6.4 iOS and Android MDM Integration 26

154 4.7 Privacy Settings: Mobile Device Data Processing..... 26

155 4.7.1 EMM: MaaS360..... 26

156 4.7.2 MTD: Zimperium 28

157 4.7.3 Application Vetting: Kryptowire 29

158 4.7.4 VPN: Palo Alto Networks 30

159 **5 Security and Privacy Analysis 30**

160 5.1 Analysis Assumptions and Limitations 30

161 5.2 Build Testing 30

162 5.3 Scenarios and Findings 31

163 5.3.1 Cybersecurity Framework, Privacy Framework, and NICE Framework Work Roles

164 Mappings 31

165 5.3.2 Threat Events and Findings..... 31

166 5.3.3 Privacy Risk Findings 33

167 5.4 Security and Privacy Control Mappings 34

168 **6 Example Scenario: Putting Guidance into Practice 34**

169 **7 Conclusion 35**

170 **8 Future Build Considerations 37**

171 **Appendix A List of Acronyms 38**

172 **Appendix B Glossary 40**

173 **Appendix C References 42**

174 **Appendix D Standards and Guidance 48**

175 **Appendix E Example Security Subcategory and Control Map..... 50**

176 **Appendix F Example Privacy Subcategory and Control Map 70**

177 **List of Figures**

178 **Figure 3-1 Cybersecurity and Privacy Risk Relationship 10**

179 **Figure 4-1 Security and Privacy Goals 12**

180 **Figure 4-2 iOS App Transport Security 19**

181 **Figure 4-3 Example Solution Architecture..... 20**

182 **Figure 4-4 Mobile Device Application Management and Benefits 22**

183 **Figure 4-5 Example Solution VPN Authentication Architecture 23**

184 **Figure 4-6 Data Collected by Example Solution Mobile Device Management 27**

185 **Figure 4-7 Example Solution Mobile Device Management Privacy Settings..... 28**

186 **Figure 7-1 Example Solution Architecture..... 36**

187 **List of Tables**

188 **Table 4-1 Examples of BYOD Deployment Threats 11**

189 **Table 4-2 Commercially Available Products Used 24**

190 **Table 5-1 Threat Events and Findings Summary 32**

191 **Table 5-2 Summary of Privacy Risks and Findings 33**

192 **Table E-1 Example Solution’s Cybersecurity Standards and Best Practices Mapping 50**

193 **Table F-1 Example Solution’s Privacy Standards and Best Practices Mapping 70**

194 **1 Summary**

195 This section familiarizes the reader with

- 196 ▪ Bring Your Own Device (BYOD) concepts
- 197 ▪ Challenges, solutions, and benefits related to BYOD deployments

198 BYOD refers to the practice of performing work-related activities on personally owned devices. This
199 practice guide provides an example solution demonstrating how to enhance security and privacy in
200 Android and iOS mobile phone BYOD deployments.

201 Incorporating BYOD capabilities in an organization can provide greater flexibility in how employees work
202 and can increase the opportunities and methods available to access organizational resources. For some
203 organizations, the combination of in-office processes with mobile device technologies enables portable
204 communication approaches and adaptive workflows. Other organizations may adopt a mobile-first
205 approach in which their employees communicate and collaborate primarily using their mobile devices.

206 Extending mobile device use by enabling BYOD capabilities in the enterprise can introduce new
207 information technology (IT) risks to organizations. Solutions that are designed to help secure corporate
208 devices and the data located on those corporate devices do not always provide an effective
209 cybersecurity solution for BYOD.

210 Deploying effective solutions can be challenging due to the unique risks that BYOD deployments impose.
211 Some of the features that make personal mobile devices increasingly flexible and functional also present
212 unique security and privacy challenges to both employers and device owners.

213 Additionally, enabling BYOD capabilities can introduce new privacy risks to employees by providing their
214 employer a degree of access to their personal devices, opening the possibility of mobile device
215 observation and control that would not otherwise exist.

216 This practice guide helps organizations deploy BYOD capabilities by providing an example solution that
217 helps address BYOD challenges, solutions, and benefits. In this practice guide, the term mobile phone is
218 used to describe an Apple iOS or Google Android mobile telephone device. Additionally, this practice
219 guide's scope for BYOD does not include deployment of laptops or devices similar to laptops.

220 **1.1 Challenge**

221 Many organizations now authorize employees to use their personal mobile devices to perform work-
222 related activities. This provides employees with increased flexibility to access organizational information
223 resources. However, BYOD architectures can also introduce vulnerabilities in the enterprise's IT
224 infrastructure because personally owned mobile devices are typically unmanaged and may lack mobile
225 device security and privacy protections. Unmanaged devices are at greater risk of unauthorized access
226 to sensitive information, tracking, email phishing, eavesdropping, misuse of device sensors, or
227 compromise of organizational data due to lost devices to name but a few risks.

228 BYOD deployment challenges can include:

229 **Supporting a broad ecosystem of mobile devices**

- 230 ▪ with diverse technologies that rapidly evolve and vary in manufacturer, operating system (OS),
231 and age of the device
- 232 ▪ where each device has unique security and privacy requirements and capabilities
- 233 ▪ whose variety can present interoperability issues that might affect organizational integration

234 **Reducing organizational risk and threats to the enterprise’s sensitive information**

- 235 ▪ posed by applications that may not usually be installed on devices issued by an organization
- 236 ▪ that result from lost, stolen, or sold mobile devices that still contain or have access to
237 organizational data
- 238 ▪ created by a user who shares their personally owned device with friends and family members
239 when that personally owned device may also be used for work activities
- 240 ▪ due to personally owned mobile devices being taken to places that increase the risk of loss of
241 control for the device
- 242 ▪ that result from malicious applications compromising the device and subsequently the data to
243 which the device has access
- 244 ▪ produced by network-based attacks that can traverse a device’s always-on connection to the
245 internet
- 246 ▪ caused by phishing attempts that try to collect user credentials or entice a user to install
247 malicious software
- 248 ▪ that results from the increased value of employees’ mobile devices due to enterprise data being
249 present

250 **Protecting the privacy of employees**

- 251 ▪ by helping to keep their personal photos, documents, location, and other data private and
252 inaccessible to others (including the organization)
- 253 ▪ by helping to ensure separation between their work and personal data while simultaneously
254 meeting the organization’s objectives for business functions, usability, security, and employee
255 privacy
- 256 ▪ by providing them with concise and understandable information about what data is collected
257 and what actions are allowed and disallowed on their devices

258 **Clearly communicating BYOD concepts**

- 259 ▪ among an organization’s IT team so it can develop the architecture to address BYOD’s unique
260 security and privacy concerns while using a repeatable, standardized, and clearly communicated
261 risk framework language
- 262 ▪ to organizational leadership and employees to obtain support and providing transparency in
263 deploying BYOD
- 264 ▪ related to mobile device security technologies so that the organization can consistently plan for
265 and implement the protection capabilities of their security tools

266 Given these challenges, it can be complex to manage the security and privacy aspects of personally
267 owned mobile devices that access organizational information assets. This document provides an
268 example solution to help organizations address these challenges.

269 1.2 Solution

270 To help organizations benefit from BYOD's flexibility while protecting themselves from many of its
271 critical security and privacy challenges, this National Institute of Standards and Technology (NIST)
272 Cybersecurity Practice Guide provides an example solution using standards-based, commercially
273 available products and step-by-step implementation guidance.

274 In our lab at the National Cybersecurity Center of Excellence (NCCoE), engineers built an environment
275 that contains an example solution for managing the security and privacy of BYOD deployments. In this
276 guide, we show how an enterprise can leverage the concepts presented in this example solution to
277 implement enterprise mobility management (EMM), mobile threat defense (MTD), application vetting, a
278 trusted execution environment (TEE) supporting secure boot/image authentication, and virtual private
279 network (VPN) services to support a BYOD solution.

280 We configured these technologies to protect organizational assets and employee privacy and provide
281 methodologies to enhance the data protection posture of the adopting organization. The standards and
282 best practices on which this example solution is based help ensure the confidentiality, integrity, and
283 availability of enterprise data on BYOD Android and iOS mobile phones as well as the predictability,
284 manageability, and disassociability of employee's data.

285 **The example solution in this practice guide helps:**

- 286 ▪ detect and protect against installing mobile malware, phishing attempts, and network-based
287 attacks
- 288 ▪ enforce passcode usage
- 289 ▪ protect organizational data by enabling selective device wipe capability of organizational data
290 and applications
- 291 ▪ protect against organizational data loss by restricting an employee's ability to copy and paste,
292 perform a screen capture, or store organizational data in unapproved locations
- 293 ▪ organizations understand BYOD risks and remediate threats (e.g., risks from jailbroken or rooted
294 devices)
- 295 ▪ provide users with access to protected business resources (e.g., SharePoint, knowledge base,
296 internal wikis, application data)
- 297 ▪ support executed code authenticity, runtime state integrity, and persistent memory data
298 confidentiality
- 299 ▪ protect data from eavesdropping while traversing a network
- 300 ▪ vet the security of mobile applications used for work-related activities
- 301 ▪ organizations implement settings to protect employee privacy
- 302 ▪ an organization deploy its own BYOD solution by providing a series of how-to guides—step-by-
303 step instructions covering the initial setup (installation or provisioning) and configuration for

304 each component of the architecture—to help security and privacy engineers rapidly deploy and
305 evaluate a mobile device solution in their test environment

306 Commercial, standards-based products such as the ones used in this practice guide are readily available
307 and interoperable with existing IT infrastructure and investments. Organizations can use this guidance in
308 whole or in part to help understand and mitigate common BYOD security and privacy challenges.

309 1.2.1 Standards and Guidance

310 This guide leverages many standards and guidance, including the NIST *Framework for Improving Critical*
311 *Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1], the *NIST Privacy Framework: A*
312 *Tool For Improving Privacy Through Enterprise Risk Management*, Version 1.0 (Privacy Framework) [2],
313 NIST Special Publication (SP) 800-181 *National Initiative for Cybersecurity Education (NICE) Cybersecurity*
314 *Workforce Framework (2017)* [3], the NIST Risk Management Framework [4], and the NIST Mobile
315 Threat Catalogue [5]. For additional information, see [Appendix D](#), Standards and Guidance.

316 1.3 Benefits

317 Carrying two mobile devices, one for work and one for personal use, introduces inconveniences and
318 disadvantages that some organizations and employees are looking to avoid. Recognizing that BYOD is
319 being adopted, the NCCoE worked to provide organizations with guidance for improving the security and
320 privacy of these solutions.

321 **For organizations, the potential benefits of this example solution include:**

- 322 ▪ enhanced protection against both malicious applications and loss of data if a device is stolen or
323 misplaced
- 324 ▪ reduced adverse effects if a device is compromised
- 325 ▪ visibility for system administrators into mobile security compliance, enabling automated
326 identification and notification of a compromised device
- 327 ▪ a vendor-agnostic, modular architecture based on technology roles
- 328 ▪ demonstrated enhanced security options for mobile access to organizational resources such as
329 intranet, email, contacts, and calendar

330 **For employees, the potential benefits of this example solution include:**

- 331 ▪ safeguards to help protect their privacy
- 332 ▪ better protected personal devices by screening work applications for malicious capability before
333 installing them
- 334 ▪ enhanced understanding about how their personal device will integrate with their organization
335 through a standardized BYOD deployment

336 2 How to Use This Guide

337 This section familiarizes the reader with:

- 338 ▪ this practice guide’s content

- 339 ▪ the suggested audience for each volume
- 340 ▪ typographic conventions used in this volume

341 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides
342 users with the information they need to replicate this BYOD example solution. This reference design is
343 modular and can be deployed in whole or in part.

344 This guide contains four volumes:

- 345 ▪ NIST SP 1800-22A: *Executive Summary* – high-level overview of the challenge, example solution,
346 and benefits of the practice guide
- 347 ▪ NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
348 **(you are here)**
- 349 ▪ NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how
350 organizations can implement this example solution’s guidance
- 351 ▪ NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution

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

353 **Business decision makers, including chief security, privacy, and technology officers** will be interested in
354 the *Executive Summary, NIST SP 1800-22A*, which describes the following topics:

- 355 ▪ challenges that enterprises face in securing BYOD deployments
- 356 ▪ example solution built at the NCCoE
- 357 ▪ benefits of adopting the example solution

358 **Technology, security, or privacy program managers** who are concerned with how to identify,
359 understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-22B*, which
360 describes what we did and why. The following sections will be of particular interest:

- 361 ▪ [Appendix E](#), Example Security Subcategory and Control Map, maps the security characteristics of
362 this example solution to cybersecurity standards and best practices.
- 363 ▪ [Appendix F](#), Example Privacy Subcategory and Control Map, describes how the privacy control
364 map identifies the privacy characteristic standards mapping for the products as they were used
365 in the example solution.

366 You might share the *Executive Summary, NIST SP 1800-22A*, with your leadership team members to help
367 them understand the importance of adopting standards-based BYOD deployments.

368 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.
369 You can use the how-to portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build
370 created in our lab. The how-to portion of the guide provides specific product installation, configuration,
371 and integration instructions for implementing the example solution. We do not re-create the product
372 manufacturers’ documentation, which is generally widely available. Rather, we show how we
373 incorporated the products together in our environment to create an example solution.

374 This guide assumes that IT professionals have experience implementing security products within the
375 enterprise. While we have used a suite of commercial products to address this challenge, this guide does

376 not endorse these particular products. Your organization can adopt this solution or one that adheres to
377 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
378 parts of this guide’s example solution for BYOD security management. Your organization’s security
379 experts should identify the products that will effectively address the BYOD risks identified for your
380 organization and best integrate with your existing tools and IT system infrastructure. We hope that you
381 will seek products that are congruent with applicable standards and best practices. [Section 4.3](#),
382 Technologies that Support the Security and Privacy Goals of the Example Solution, lists the products we
383 used and maps them to the cybersecurity controls provided by this reference solution.

384 **For those who would like to see how the example solution can be implemented**, this practice guide
385 contains an example scenario about a fictional company called Great Seneca Accounting. The example
386 scenario shows how BYOD objectives can align with an organization’s priority security and privacy
387 capabilities through NIST risk management standards, guidance, and tools. It is provided in this practice
388 guide’s supplement, *Example Scenario: Putting Guidance into Practice*.

- 389 ▪ Appendix F of the Supplement describes the risk analysis we performed, using an example
390 scenario.
- 391 ▪ Appendix G of the Supplement describes how to conduct a privacy risk assessment and use it to
392 improve mobile device architectures, using an example scenario.

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

397 Acronyms used in figures can be found in [Appendix A](#), List of Acronyms.

398 **2.1 Typographic Conventions**

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

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

400 3 Approach

401 This section familiarizes the reader with:

- 402 ▪ this guide's intended audience, scope, and assumptions
- 403 ▪ mobile device security and privacy risk assessments

404 To identify the cybersecurity challenges associated with deploying a BYOD solution, the team surveyed
 405 reports of mobile device security trends and invited the mobile device security community to engage in
 406 a discussion about pressing cybersecurity challenges.

407 Two broad and significant themes emerged from this research:

- 408 ▪ Administrators wanted to better understand what policies and standards should be
 409 implemented.
- 410 ▪ Employees were concerned about the degree to which enterprises have control over their
 411 personally owned mobile devices and potential visibility into the personal activity that takes
 412 place on them.

413 The team addressed these two challenges by reviewing the primary standards, best practices, and
 414 guidelines contained within [Appendix D](#), Standards and Guidance.

415 3.1 Audience

416 This practice guide is intended for organizations that want to adopt a BYOD architecture that enables
 417 use of personal mobile phones and tablets. The target audience is executives, security managers, privacy
 418 managers, engineers, administrators, and others who are responsible for acquiring, implementing,
 419 communicating with users about, or maintaining mobile enterprise technology. This technology can

420 include centralized device management, secure device/application security contexts, application vetting,
421 and endpoint protection systems.

422 This document will interest system architects already managing mobile device deployments and those
423 looking to integrate a BYOD architecture into existing organizational wireless systems. It assumes that
424 readers have a basic understanding of mobile device technologies and enterprise security and privacy
425 principles. Please refer to [Section 2](#) for how different audiences can effectively use this guide.

426 **3.2 Scope**

427 The scope of this build includes managing iOS or Android mobile phones and tablets deployed in a BYOD
428 configuration with cloud-based EMM. We excluded laptops and mobile devices with minimal computing
429 capability, including feature phones and wearables. We also do not address classified systems, devices,
430 data, and applications within this publication.

431 While this document is primarily about mobile device security for BYOD implementations, BYOD
432 introduces privacy risk to the organization and its employees who participate in the BYOD program.
433 Therefore, the NCCoE found addressing privacy risk to be a necessary part of developing the BYOD
434 architecture. The scope of privacy in this build is limited to those employees who use their devices as
435 part of their organization's BYOD solution. The build does not explicitly address privacy considerations of
436 other individuals whose information is processed by the organization through an employee's personal
437 device.

438 We intend for the example solution proposed in this practice guide to be broadly applicable to
439 enterprises, including both the public and private sectors.

440 **3.3 Assumptions**

441 This project is guided by the following assumptions:

- 442 ▪ The example solution was developed in a lab environment. While the environment is based on a
443 typical organization's IT enterprise, the example solution does not reflect the complexity of a
444 production environment.
- 445 ▪ The organization has access to the skills and resources required to implement a mobile device
446 security and privacy solution.
- 447 ▪ The example security and privacy control mappings provided as part of this practice guide are
448 focused on mobile device needs, and do not include general control mappings that would also
449 typically be used in an enterprise. Those general control mappings that do not specifically apply
450 to this guide's mobile device security example solution are outside the scope of this guide's
451 example solution.
- 452 ▪ Because the organizational environment in which this build could be implemented represents a
453 greater level of complexity than is captured in the current guide, we assume that organizations
454 will first examine the implications for their current environment before implementing any part
455 of the proposed example solution.
- 456 ▪ The organization has either already invested or is willing to invest in the security of mobile
457 devices used within it and in the privacy of participating employees, and in the organization's IT
458 systems more broadly. As such, we assume that the organization either has the technology in

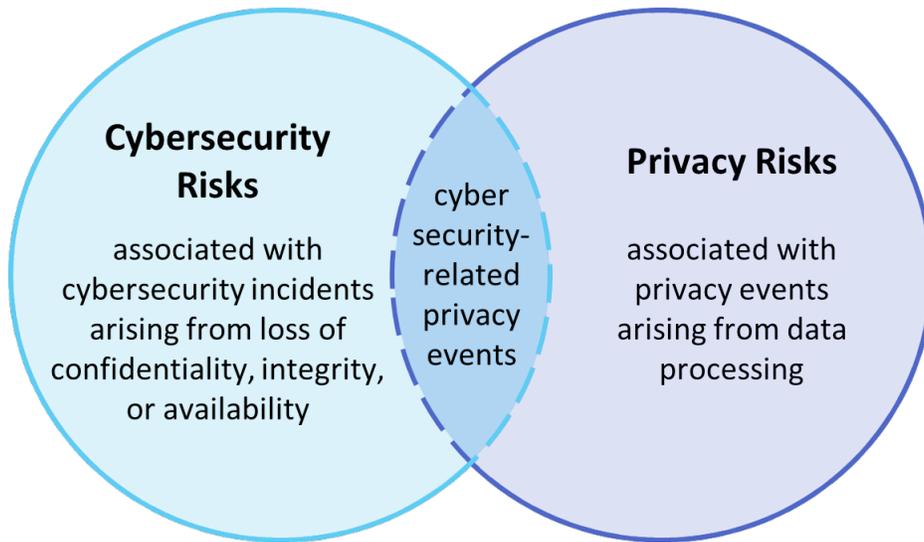
- 459 place to support this implementation or has access to the off-the-shelf technology used in this
460 build, which we assume will perform as described by the respective product vendor.
- 461 ▪ The organization has familiarized itself with existing standards and any associated guidelines
462 (e.g., NIST Cybersecurity Framework [1]; *NIST Privacy Framework* [2]; NIST SP 800-124 Revision 2
463 (Draft), *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]; NIST SP
464 1800-4 *Mobile Device Security: Cloud and Hybrid Builds* [7]) relevant to implementation of the
465 example solution proposed in this practice guide. We also assume that any existing technology
466 used in the example solution has been implemented in a manner consistent with these
467 standards.
 - 468 ▪ The organization has instituted relevant mobile device security and privacy policies, and these
469 will be updated based on implementation of this example solution.
 - 470 ▪ The organization will provide guidance and training to its employees regarding BYOD usage and
471 how to report device loss or suspected security issues in which their devices are involved. This
472 guidance will be periodically reviewed and updated, and employees will be regularly trained on
473 BYOD usage.

474 3.4 Risk Assessment

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

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

488 We identified the security and privacy risks for this BYOD example solution by examining the
489 relationship of risk between cybersecurity and privacy. Cybersecurity and privacy are two distinct risk
490 areas, though the two intersect in significant ways. As noted in Section 1.2.1 of the *NIST Privacy
491 Framework* [2], having a general understanding of the different origins of cybersecurity and privacy risks
492 is important for determining the most effective solutions to address the risks. Figure 3-1 illustrates this
493 relationship, showing that some privacy risks arise from cybersecurity risks, and some are unrelated to
494 cybersecurity risks. Allowing an unauthorized device to connect to the organization’s network through
495 its BYOD implementation is an example of a security risk that may not impact privacy.

496 **Figure 3-1 Cybersecurity and Privacy Risk Relationship**

497 The security capabilities in this build help address some of the privacy risks that arise for employees.
 498 This build also uses the *NIST Privacy Framework* [2] and Privacy Risk Assessment Methodology (PRAM)
 499 [8] to identify and address privacy risks that are beyond the scope of security risks. Regardless of
 500 whether cybersecurity and privacy are situated in the same part of the organization or in different parts,
 501 the two capabilities must work closely together to address BYOD risks.

502 A risk assessment can include additional analysis areas. For more information on the example solutions:

- 503 ▪ **Security and privacy threats, and goals to remediate those threats**, see [Section 4.1](#)
- 504 ▪ **Vulnerabilities** that influenced the reference architecture, see Appendix Section F-5 of the
 505 Supplement
- 506 ▪ **Risks** that influenced the architecture development, see Appendix Section F-6 of the
 507 Supplement
- 508 ▪ **Security Control Mapping** to cybersecurity and privacy standards and best practices, see
 509 [Appendix E](#) and [Appendix F](#)

510 **4 Architecture**

511 This section helps familiarize the reader with:

- 512 ▪ threats to BYOD architectures
- 513 ▪ example solution goals to remediate threats to BYOD architectures
- 514 ▪ how organizations might leverage the *Example Scenario: Putting Guidance into Practice*
 515 supplement of this practice guide to implement their mobile device solution
- 516 ▪ technologies to support the example solution goals
- 517 ▪ the example solution's architecture
- 518 ▪ how the example solution's products were integrated
- 519 ▪ mobile device data collection

520 4.1 Common BYOD Risks and Potential Goals to Remediate Those Risks

521 This section contains examples of common security and privacy concerns in BYOD architectures. We
 522 provide a list of architecture goals to address those challenges. Once completed, the example solution's
 523 architecture provides organizations with a security and privacy-enhanced design that can be leveraged
 524 for their mobile devices. The example solution's challenges and goals are highlighted below, followed by
 525 the architecture that supports those goals.

526 4.1.1 Threat Events

527 Leveraging a system life cycle approach [9], this build considered threats relating to BYOD deployments.
 528 Information from the Open Web Application Security Project Mobile Top 10 [10], which provides a
 529 consolidated list of mobile application risks, and information from the NIST Mobile Threat Catalogue [5],
 530 which examines the mobile information system threats in the broader mobile ecosystem were used to
 531 develop applicable threats. Table 4-1 gives each threat an identifier for the purposes of this build, a
 532 description of each threat event (TE), and the related NIST Mobile Threat Catalogue Threat identifiers
 533 (IDs).

534 We limited inclusion of TEs to those that we generally expected to have a high likelihood of occurrence
 535 and high potential for adverse impact. Organizations applying this build should evaluate the NIST Mobile
 536 Threat Catalogue for additional threats that may be relevant to their architecture. For an example of
 537 how to determine the risk from these threats, see Appendix F in the Supplement.

538 **Table 4-1 Examples of BYOD Deployment Threats**

Threat Event ID	Threat Event Description	NIST Mobile Threat Catalogue Threat ID
TE-1	privacy-intrusive applications	APP-2, APP-12
TE-2	account credential theft through phishing	AUT-9
TE-3	outdated phones	APP-4, APP-26, STA-0, STA-9, STA-16
TE-4	sensitive data transmissions	APP-0, CEL-18, LPN-2
TE-5	brute-force attacks to unlock a phone	AUT-2, AUT-4
TE-6	application credential storage vulnerability	APP-9, AUT-0
TE-7	unmanaged device protection	EMM-5
TE-8	lost or stolen data protection	PHY-0
TE-9	protecting enterprise data from being inadvertently backed up to a cloud service	EMM-9

539 4.1.2 Privacy Risks

540 In addition to the TEs just discussed, this practice guide's example solution also considers and helps
 541 mitigate privacy risks that can apply to BYOD deployments.

542 Privacy risks for individuals can present themselves through problematic data actions. The NIST Privacy
 543 Framework defines a problematic data action as “a data action that could cause an adverse effect for
 544 individuals” [2].

545 **4.1.2.1 Privacy Risk Examples and Mitigation Methodologies**

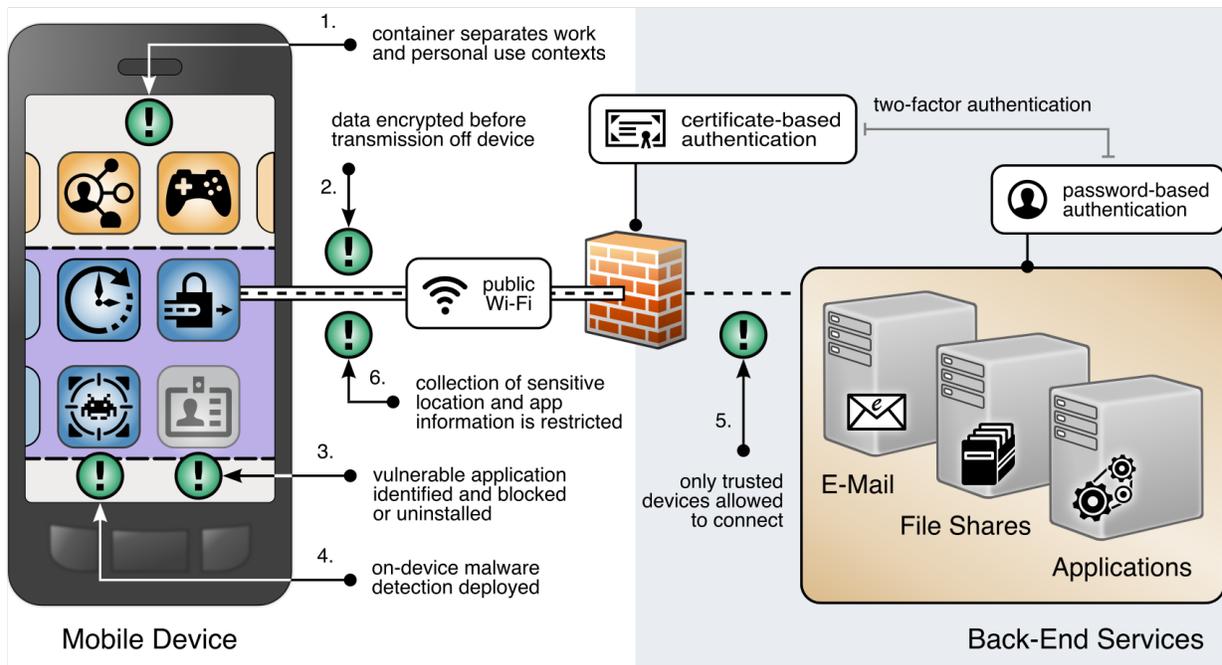
546 The example solution contained in this guide identifies and helps to mitigate some common privacy risks
 547 that a BYOD deployment may encounter. The privacy risks and their accompanying problematic data
 548 actions were identified using NIST-developed methodologies.

549 The NIST PRAM [8] and accompanying Catalog of Problematic Data Actions and Problems [11] are
 550 standardized methodologies for identifying privacy challenges that were used to conduct our privacy risk
 551 analysis. This publication provides the results of our privacy risk analysis for a fictional organization as an
 552 exemplar for the reader’s use, as well as suggested privacy architecture enhancements. See Appendix G
 553 of the Supplement for an example of how the privacy risks for this practice guide’s BYOD deployment
 554 example solution were developed. The following section, 4.1.3, outlines the security and privacy goals of
 555 this publication’s example solution architecture.

556 **4.1.3 Security and Privacy Goals**

557 To address the challenges stated in the previous sections, the architecture for this build addresses the
 558 high-level security and privacy goals illustrated in Figure 4-1.

559 **Figure 4-1 Security and Privacy Goals**



560 The following goals were highlighted above in [Figure 4-1](#) Security and Privacy Goals, with a green
561 exclamation mark:

- 562 1. **Separate organization and personal information.** BYOD deployments can place organizational
563 data at risk by allowing it to travel outside internal networks and systems when it is accessed on
564 a personal device. BYOD deployments can also place personal data at risk by capturing
565 information from employee devices. To help mitigate this, organizational and personal
566 information can be separated by restricting data flow between organizationally managed and
567 unmanaged applications. The goals include helping to prevent sensitive data from crossing
568 between work and personal contexts.
- 569 2. **Encrypt data in transit.** Devices deployed in BYOD scenarios can leverage nonsecure networks,
570 putting data at risk of interception. To help mitigate this, mobile devices can connect to the
571 organization over a VPN or similar solution to encrypt all data before it is transmitted from the
572 device, protecting otherwise unencrypted data from interception. A user would not be able to
573 access the organization's resources without an active VPN connection and required certificates.
- 574 3. **Identify vulnerable applications.** Employees may install a wide range of applications on their
575 personally owned devices, some of which may have security weaknesses. When vulnerable
576 personal applications are identified, an organization can remove the employee's work profile or
577 configuration file from the device rather than uninstalling the employee's personal applications.
- 578 4. **Prevent or detect malware.** On personally owned devices without restriction policies in place,
579 users may obtain applications outside official application stores, increasing the risk of installing
580 malware in disguise. To help protect from this risk, an organization could deploy malware
581 detection to devices to identify malicious applications within the work profile or managed
582 applications and facilitate remediation. Additionally, security features that are built-in to the OS
583 could aid in preventing or detecting the installation of malware.
- 584 5. **Trusted device access.** Because mobile devices can connect from unknown locations, an
585 organization can provision mobile devices with a security certificate that allows identifying and
586 authenticating them at the connection point, which combines with user credentials to create
587 two-factor authentication from mobile devices. An employee would not be able to access the
588 organization's resources without the required certificates.
- 589 6. **Restrict information collection.** Depending on how devices are enrolled, mobile device
590 management tools can sometimes track application inventory and location information,
591 including physical address, geographic coordinates, location history, internet protocol (IP)
592 address, and service set identifier (SSID). These capabilities may reveal sensitive information
593 about employees, such as frequently visited locations or habits. Device management tools can
594 be configured to exclude application and location information. Excluding the collection of
595 information further protects employee privacy when device and application data is shared
596 outside the organization for monitoring and analytics.

597 4.2 Example Scenario: Putting Guidance into Practice

598 The example solution's high-level goals underscore the need to use a thorough risk assessment process
599 for organizations implementing mobile device security capabilities. To learn more about how your
600 organization might implement this example solution, reference the *Example Scenario: Putting Guidance*
601 *into Practice* supplement of this practice guide. The supplement provides an example approach for

602 developing and deploying a BYOD architecture that directly addresses the mobile device TEs and
603 problematic data actions discussed in this guide.

604 The supplement shows how a fictional organization used the guidance in NIST’s Cybersecurity
605 Framework [1], Privacy Framework [2], RMF [9], and PRAM [8] to identify and address their BYOD
606 security and privacy goals.

607 **4.3 Technologies that Support the Security and Privacy Goals of the** 608 **Example Solution**

609 This section describes the mobile-specific technology components used within this example solution.
610 These technologies were selected to address the security goals, TEs, and problematic data actions
611 identified in [Section 4.1](#). This section provides a brief description of each technology and discusses the
612 security and privacy capabilities that each component provides.

613 The technology components in this section are combined into a cohesive enterprise architecture to help
614 address BYOD security threats and problematic data actions and provide security-enhanced access to
615 enterprise resources from mobile devices. The technologies described in this section provide protection
616 for enterprise resources accessed by BYOD users.

617 **4.3.1 Trusted Execution Environment**

618 A TEE is “a controlled and separated environment outside the high-level operating system that is
619 designed to allow trusted execution of code and to protect against viruses, Trojans, and root kits.” [12].
620 By providing a controlled and separated environment, the TEE helps enable applications and features
621 that can provide enhanced security and privacy functionality.

622 **4.3.2 Enterprise Mobility Management**

623 Organizations use EMM solutions to secure the mobile devices of users who are authorized to access
624 organizational resources. Such solutions generally have two main components. The first is a backend
625 service that mobile administrators use to manage the policies, configurations, and security actions
626 applied to enrolled mobile devices. The second is an on-device agent, usually in the form of a mobile
627 application, that integrates between the mobile OS and the solution’s backend service. Both iOS and
628 Android also support a bulk EMM enrollment use case (Apple Business Manager for iOS devices and
629 Android Enterprise Enrollment for Android devices), which we do not discuss in this document.

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

637 EMM solutions commonly include any of the following capabilities: mobile application management,
638 mobile content management, and implementations of or integrations with device- or mobile-OS-specific

639 user profile solutions, such as Android Enterprise or iOS User Enrollment. These capabilities can be used
640 in the following ways in a BYOD deployment:

- 641 ▪ Mobile application management can be used to manage the installation and usage of an
642 organization’s applications based on their trustworthiness and work relevance.
- 643 ▪ Mobile content management can control how managed applications access and use
644 organizational data.
- 645 ▪ The EMM works with operating system data separation and isolation capabilities that can
646 strengthen the separation between a user’s personal and professional usage of the device.
- 647 ▪ Also, EMM solutions often have integrations with a diverse set of additional tools and security
648 technologies that enhance their capabilities.

649 For further reading on this topic, NIST SP 800-124 Revision 2 (Draft), *Guidelines for Managing the*
650 *Security of Mobile Devices in the Enterprise* [6] provides additional information on mobile device
651 management with EMM solutions. The National Information Assurance Partnership’s (NIAP’s) *Protection*
652 *Profile for Mobile Device Management Servers and Extended Package for Mobile Device Management*
653 *Agents* [13] describes important capabilities and security requirements to look for in EMM systems.

654 EMMs can help BYOD deployments improve the security posture of the organization by providing a
655 baseline of controls to limit attack vectors and help protect enterprise information that is on a
656 personally owned device. EMMs can also provide an additional layer of separation between enterprise
657 data and personal data on a mobile device.

658 EMMs may also provide mobile application wrapping functionality. The wrapping process encapsulates
659 enterprise-developed applications in a vendor-created wrapper that intercepts application programming
660 interface (API) calls and provides additional layers of security. Wrapping is useful in many different
661 scenarios, for example, to force an application’s traffic to go through the corporate VPN. Wrapping
662 typically occurs when applications are uploaded to the EMM’s app store for distribution to enrolled
663 devices [14].

664 4.3.3 Virtual Private Network

665 A VPN gateway increases the security of remote connections from authorized mobile devices to an
666 organization’s internal network. A VPN is a virtual network, built on top of existing physical networks,
667 that can provide a secure communication channel for data and system control information transmitted
668 between networks. VPNs are used most often to protect communications carried over public networks
669 from eavesdropping and interception. A VPN can provide several types of data protection, including
670 confidentiality, integrity, authentication of data origin, replay protection, and access control that help
671 reduce the risks of transmitting data between network components.

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

678 NIAP's *Module for Virtual Private Network (VPN) Gateways 1.0* [15], in combination with *Protection*
679 *Profile for Network Devices* [16], describes important capabilities and security requirements to expect
680 from VPN gateways.

681 In a BYOD deployment, an enterprise can also leverage a per-application or full enterprise profile VPN to
682 provide a secure connection over the VPN tunnel strictly when using enterprise applications on the
683 mobile device. Personal applications on the device would not be allowed to use the VPN, ensuring the
684 enterprise only has visibility into enterprise traffic. This is especially important to BYOD deployments,
685 whose devices may connect over a wide variety of wireless networks. It also provides a layer of privacy
686 protection for employees by preventing personal mobile device traffic from being routed through the
687 enterprise.

688 4.3.4 Mobile Application Vetting Service

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

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

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

709 While NIAP does not provide a protection profile for application vetting services, their *Protection Profile*
710 *for Application Software* [17] describes security requirements to be expected from mobile applications.
711 Many mobile application vetting vendors provide capabilities to automate evaluation of applications
712 against NIAP's requirements.

713 Application vetting services help improve the security and privacy posture of the mobile devices by as-
714 ssuming the risk of the applications that may be installed on a personally owned device. Depending on
715 the deployment strategy, the application vetting service may analyze all installed applications, enter-
716 prise-only applications, or no applications.

717 4.3.5 Mobile Threat Defense

718 MTD generally takes the form of an application that is installed on the device that provides information
719 about the device's threat posture based on risks, security, and activity on the device. This is also known
720 as endpoint protection. Ideally, the MTD solution will be able to detect unwanted activity and properly
721 inform the user and BYOD administrators so they can act to prevent or limit the harm that an attacker
722 could cause. Additionally, MTD solutions may integrate with EMM solutions to leverage the MTD agent's
723 greater on-device management controls and enforcement capabilities, such as blocking a malicious
724 application from being launched until the user can remove it.

725 While detecting threats, MTD products typically analyze device-, application-, and network-based
726 threats. Device-based threats include outdated OS versions, insecure configurations, elevation of
727 privileges, unauthorized device profiles, and compromised devices. Application-based threat detection
728 can provide similar functionality to that of dedicated application vetting services. However, application-
729 based threat detection may not provide the same level of detail in its analysis as dedicated application
730 vetting services. Network-based threats include use of unencrypted and/or public Wi-Fi networks and
731 attacks such as active attempts to intercept and decrypt network traffic.

732 Because BYOD mobile phones can have a wide variety of installed applications and usage scenarios,
733 MTD profile helps improve the security and privacy posture by providing an agent-based capability to
734 detect unwanted activity within the work profile.

735 To further enhance device protection and analytic capabilities, MTD services may offer additional
736 integrations with 3rd party threat intelligence services such as MITRE ATT&CK for Mobile or VirusTotal.
737 These services could aid in enriching the data acquired from devices, providing more contextual and
738 technical information on the discovered threats. Then, the enriched data could be forwarded to other
739 services for additional analysis or triage, such as a Security Information and Event Management service.

740 4.3.6 Mobile Operating System Capabilities

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

744 4.3.6.1 Secure Boot

745 Secure boot is a general term that refers to a system architecture that is designed to prevent and detect
746 any unauthorized modification to the boot process. A system that successfully completes a secure boot
747 has loaded its start-up sequence information into a trusted OS. A common mechanism is for the first
748 program executed (a boot loader) to be immutable (stored on read-only memory or implemented
749 strictly in hardware). Further, the integrity of mutable code is cryptographically verified by either
750 immutable or verified code prior to execution. This process establishes a chain of trust that can be
751 traced back to immutable, implicitly trustworthy code.

752 4.3.6.2 Device Attestation

753 Device attestation is an extension of the secure boot process that involves the OS (or more commonly,
754 an integrated TEE and/or Hardware Security Model) providing cryptographically verifiable proof that it

755 has a known and trusted identity and is in a trustworthy state. This means that all software running on
756 the device is free from unauthorized modification.

757 Device attestation requires cryptographic operations using an immutable private key that can be verified
758 by a trusted third party, which is typically the original equipment manufacturer of the TEE or device
759 platform vendor. Proof of possession of a valid key establishes the integrity of the first link in a chain of
760 trust that preserves the integrity of all other pieces of data used in the attestation. It will include unique
761 device identifiers, metadata, the results of integrity checks on mutable software, and possibly metrics
762 from the boot or attestation process itself [18].

763 *4.3.6.3 Mobile Device Management Application Programming Interfaces*

764 Mobile OS and platform-integrated firmware can provide a number of built-in security features that are
765 generally active by default. Examples of how management APIs can enhance device security include
766 verification of digital signatures for installed software and updates, requiring a device unlock code,
767 initiating remote device lock actions, and requiring automatic device wipe following a series of failed
768 device unlock attempts. The user can directly configure some of these features via a built-in application
769 or through a service provided by the device platform vendor [19].

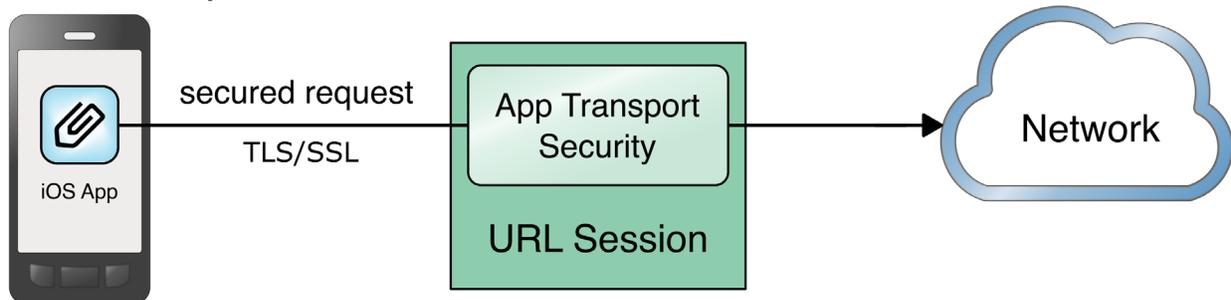
770 Additionally, mobile operating systems expose an API to MDM products that allow an organization that
771 manages a device to have greater control over these and many more settings that might not be directly
772 accessible to the device user. Management APIs allow enterprises using integrated EMM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

775 *4.3.6.4 iOS App Transport Security*

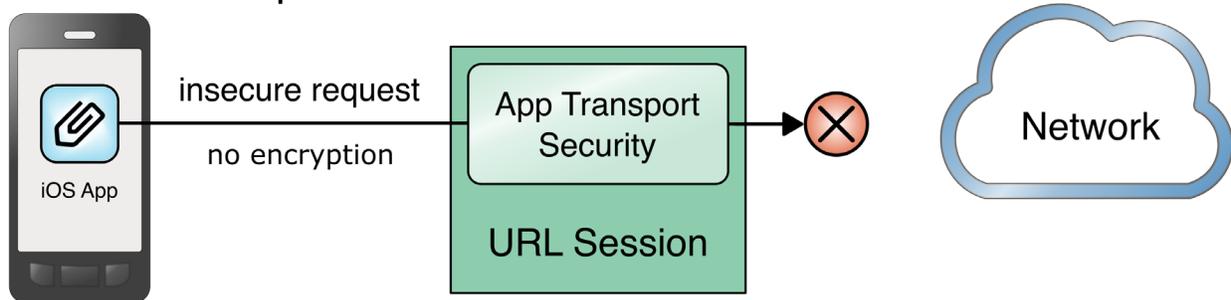
776 App Transport Security (ATS) is a networking security feature on Apple iOS devices that increases data
777 integrity and privacy for applications and extensions [20], [21]. ATS requires that the network
778 connections made by applications are secured through the Transport Layer Security protocol, which
779 uses reliable cipher suites and certificates. In addition, ATS blocks any connection that does not meet
780 minimum security requirements. For applications linked to iOS 9.0 and later, ATS is enabled by default.
781 Figure 4-2 shows how ATS compliant and noncompliant applications function. As demonstrated in the
782 figure, secured application requests are allowed, and insecure requests are blocked.

783 Figure 4-2 iOS App Transport Security

ATS Compliant Scenario



ATS Noncompliant Scenario



784 4.3.6.5 Android Network Security Configuration

785 With data privacy becoming even more important, Google released mobile OS enhancements to protect
 786 data that traverses Android devices and endpoints [22], [23]. The Android Network Security
 787 Configuration prevents applications from transmitting sensitive data unintentionally in unencrypted
 788 cleartext. By default, `cleartextTrafficPermitted` is set to `false`. Through the Android Network
 789 Security Configuration feature, developers can designate what certification authorities are trusted and
 790 pin specific certificates to ensure secure communications and issue certificates.

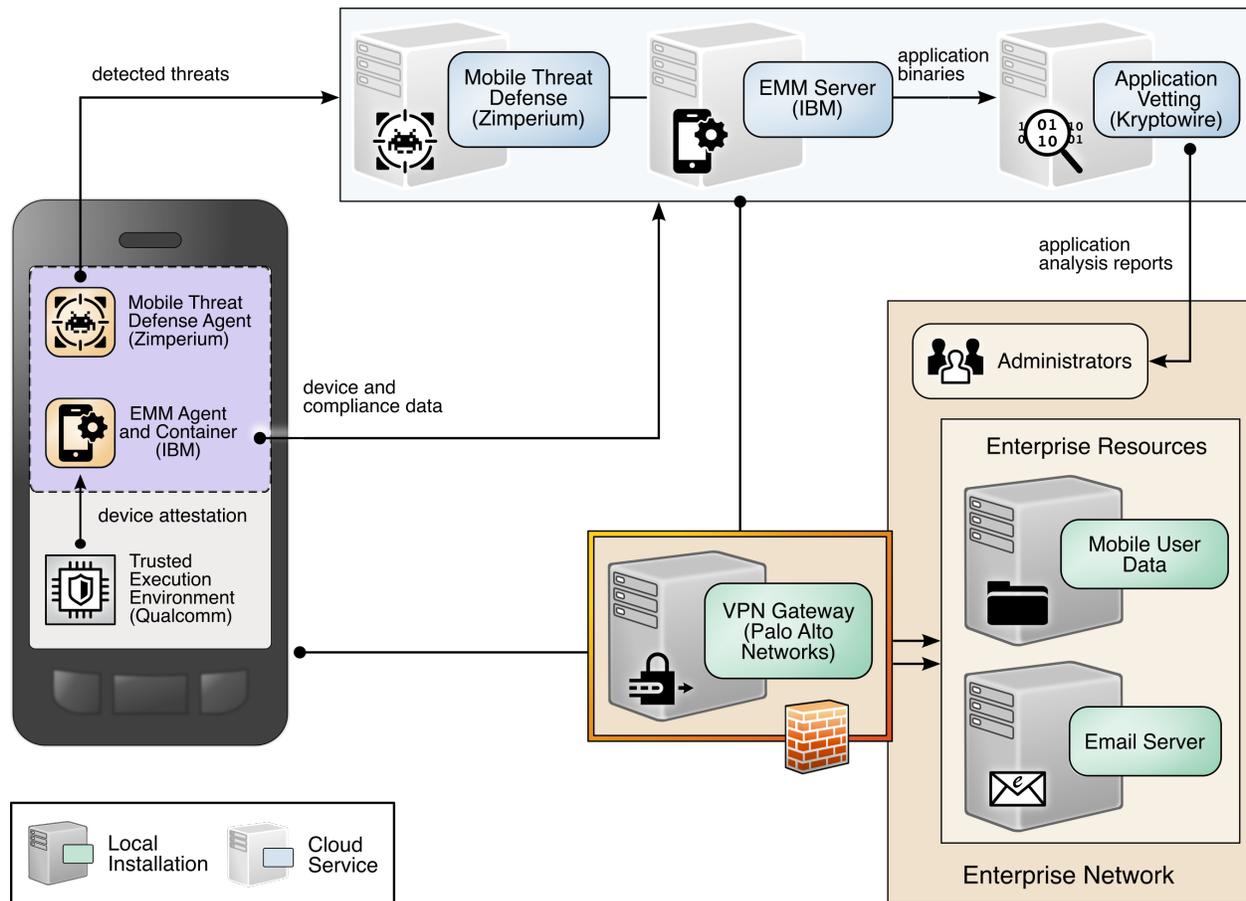
791 4.3.6.6 Application Sandboxing

792 Both Android and iOS impose sandboxing restrictions on applications running on the device. These
 793 security and privacy controls help isolate applications into their own runtime environments. The
 794 sandboxing restrictions then help prevent applications from accessing other applications' data or data
 795 on the underlying operating system not exposed by official APIs.

796 4.4 Architecture Description

797 The example solution architecture consists of the security technologies described in Section 4.3. The
 798 security technologies are further integrated with broader enterprise security mechanisms and a VPN
 799 gateway as shown in Figure 4-3. This example solution provides a broad range of capabilities to securely
 800 provision and manage devices, protect against, and detect device compromise, and provide secure
 801 access to enterprise resources to only authorized mobile users and devices.

802 Figure 4-3 Example Solution Architecture



803 The NCCoE worked with industry experts to develop an open, standards-based architecture using
 804 commercially available products to address the threats and problematic data actions identified in
 805 [Section 4.1](#).

806 Where possible, the architecture uses components that are present on the NIAP Product Compliant List,
 807 meaning that the product has been successfully evaluated against a NIAP-approved protection profile.
 808 The NIAP collaborates with a broad community, including industry, government, and international
 809 partners, to publish technology-specific security requirements and tests in the form of protection
 810 profiles. The requirements and tests in these protection profiles are intended to ensure that evaluated
 811 products address identified security threats and provide risk mitigation measures.

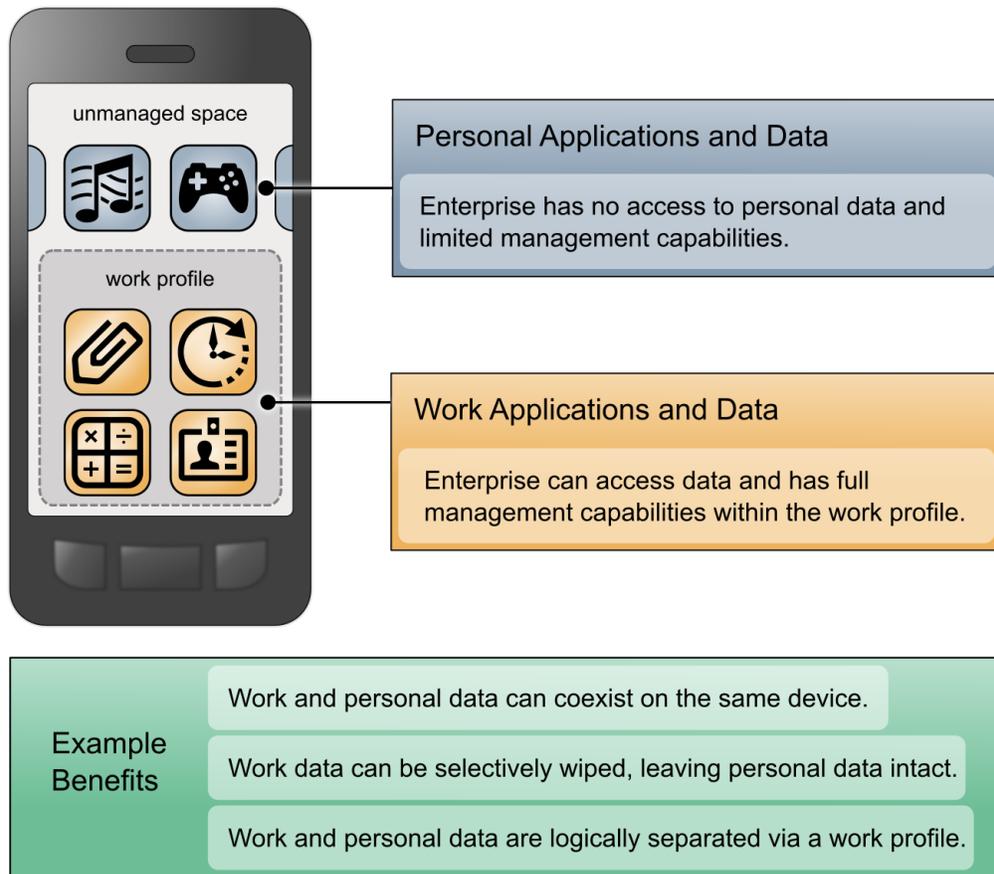
812 The security and privacy characteristics of the architecture result from many of the capability
 813 integrations outlined in [Section 4.5](#).

814 4.5 Enterprise Integration of the Employees' Personally Owned Mobile 815 Devices

816 One key benefit of BYOD solutions for employees is the ability to access both work and personal data on
817 the same device. While the technical approaches differ between iOS and Android devices, both
818 operating systems offer the following types of features for managing the coexistence of work and
819 personal data on devices [24], [25]:

- 820 ▪ enterprise and personal application data isolation
- 821 ▪ restriction of application installation from unofficial sources
- 822 ▪ selective wiping to remove enterprise data and preserve personal data
- 823 ▪ device passcode requirement enforcement
- 824 ▪ enterprise application configuration control
- 825 ▪ identity and certificate authority certificate support

826 Illustrating this concept, Figure 4-4 shows enterprise integration for managed and unmanaged
827 applications on mobile devices. To protect sensitive work data and employee privacy, work applications
828 can be separated into a work profile, with data access restricted between the personal and work
829 container profile applications.

830 **Figure 4-4 Mobile Device Application Management and Benefits**831 **4.5.1 Microsoft Active Directory Integration**

832 The example solution is integrated with Microsoft Active Directory (AD), which provides both enterprise
 833 identity management and certificate enrollment services via public key infrastructure. International
 834 Business Machines (IBM) MaaS360 connects directly to the domain controller and the Network Device
 835 Enrollment Service (NDES) servers via an IBM Cloud Extender installed on the local intranet, while
 836 GlobalProtect connects to the domain controller via the Palo Alto Networks firewall's Lightweight
 837 Directory Access Protocol service route.

838 By integrating directly with the AD infrastructure, administrators can configure MaaS360 to accept
 839 enrollment requests based on user groups in AD. GlobalProtect can inherit these roles and enforce
 840 access control protocols to restrict/deny permissions to the VPN. The AD integration is also used within
 841 MaaS360 to provide policy-based access to the MaaS360 administration console.

842 The Certificate Integration module within the MaaS360 Cloud Extender allows user certificates to be
 843 installed on the user's devices when enrolling with MaaS360. These certificates are then validated in
 844 GlobalProtect during the VPN authentication sequence, along with the user's corporate username and
 845 password. The Cloud Extender requests these certificates from the NDES server by using the Simple
 846 Certificate Enrollment Protocol.

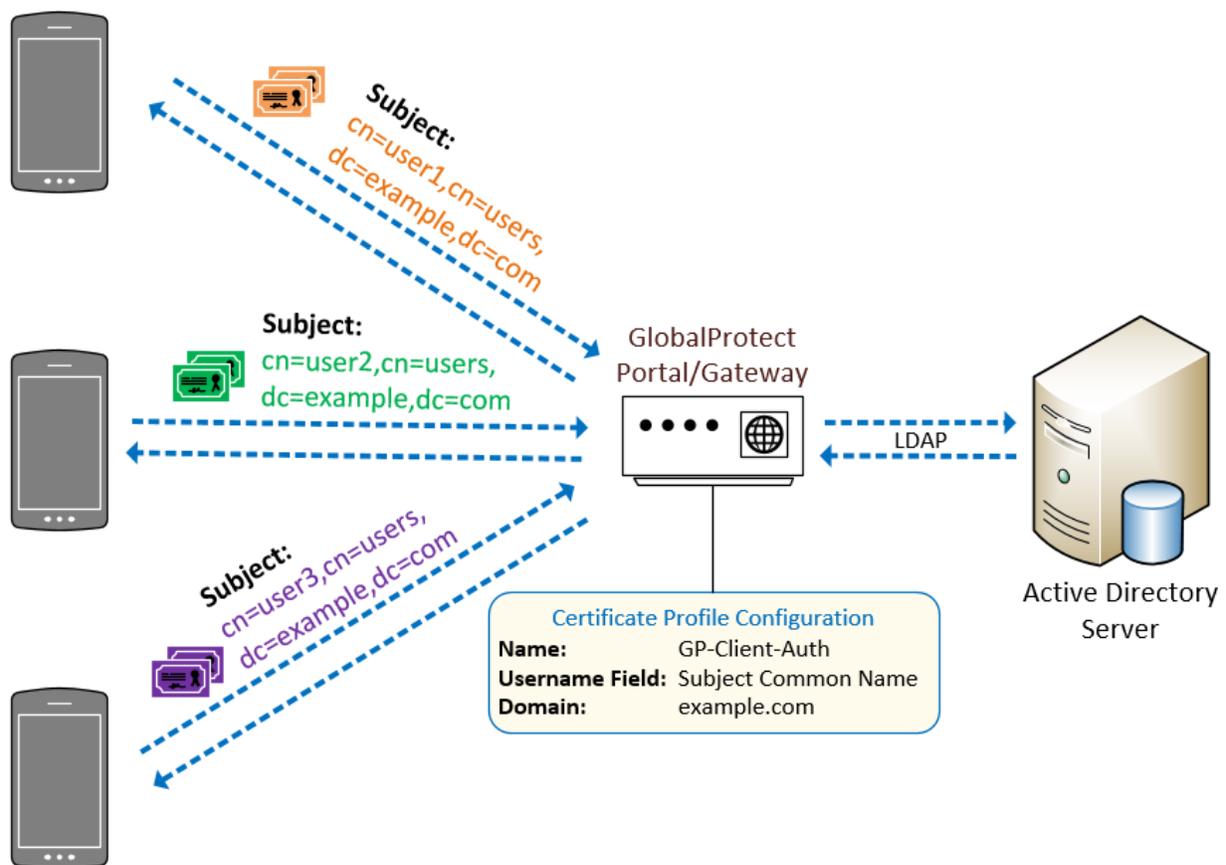
847 4.5.2 Mobile Device Enrollment

848 The example solution shown in Figure 4-5 mitigates the potential for SCEP to be remotely exploited by
 849 restricting certificate enrollment to mobile devices that are connected to a dedicated enterprise-
 850 managed Wi-Fi network. The uniform resource locator (URL) of the NDES server is resolvable only on
 851 this managed Wi-Fi network.

852 Furthermore, the NDES server is configured to require a dynamic challenge with each request. The Cloud
 853 Extender does this by including a one-time password with each request. This helps prevent unknown
 854 devices from requesting certificates. These certificates can then be used to prove identity when
 855 authenticating with the GlobalProtect VPN.

856 The certificate template includes the user's username and email address. This allows the GlobalProtect
 857 gateway to enforce access control and identity verification.

858 Figure 4-5 Example Solution VPN Authentication Architecture



859 4.6 Mobile Components Integration

860 IBM MaaS360 supports integration of third-party applications and cloud services via a representational
 861 state transfer (REST) API [26]. External services are authenticated via access tokens, obtained through
 862 MaaS360 support. Zimperium and Kryptowire used the REST API [27].

863 Table 4-2 identifies the commercially available products used in this example solution and how they
 864 align with the mobile security technologies. For additional information, Appendices G and H contain a
 865 mapping of these technologies to the cybersecurity and privacy standards and best practices that each
 866 product provides in the example solution.

867 **Table 4-2 Commercially Available Products Used**

Commercially Available Product	Mobile Security Technology
IBM MaaS360 Mobile Device Management (SaaS) Version 10.82 IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android) IBM MaaS360 Cloud Extender Cloud Extender Modules: Certificate Integration Module Version 2.96.000 Cloud Extender Base Module Version 2.96.000 Cloud Extender Basic Module Device Version 2.96.000 MaaS360 Configuration Utility Module Version 2.96.200 Mobile Device Management Module Version 2.31.020 User Authentication Module Version 2.96.200	mobile device management
Kryptowire Cloud Service	application vetting
Palo Alto Networks PA-VM-100 Version 9.0.1 Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android)	firewall virtual private network
Qualcomm (Version is mobile device dependent)	trusted execution environment
Zimperium Defense Suite Zimperium Console Version vGA-4.23.1 Zimperium zIPS Agent Version 4.9.2 (Android and iOS)	mobile threat defense
Apple iOS Version 13 Google Android Version 10	mobile device operating system

868 4.6.1 Zimperium–MaaS360

869 Through the MaaS360 REST API, Zimperium can retrieve various device attributes such as device name,
 870 model, OS, OS version, and the owner’s email address. It then continuously monitors the device’s risk
 871 posture through the Zimperium Intrusion Prevention System (zIPS) application and reports any changes
 872 in the posture to MaaS360. This enables MaaS360 administrators to apply different device policies and
 873 enforcement actions based on the risk posture of a device.

874 When a device is enrolled with MaaS360, the zIPS application is automatically installed and configured in
875 the work profile on the device. When the user first launches the zIPS application from within the work
876 profile, it will automatically enroll the device in Zimperium’s MTD service. zIPS will then continuously
877 monitor the device for threats, and any detected threats will be reported to Zimperium. Zimperium can
878 then report to MaaS360 if any changes in risk posture occurred.

879 MaaS360 can respond to the following risk posture levels, as assigned by Zimperium:

- 880 ▪ low
- 881 ▪ normal
- 882 ▪ elevated
- 883 ▪ critical

884 4.6.2 Kryptowire—MaaS360

885 Through the MaaS360 REST API, Kryptowire can retrieve a list of enrolled devices, device metadata (such
886 as device ID, enterprise username, and device name), and the inventory of enterprise applications
887 installed on those devices. This allows Kryptowire to automatically analyze all new applications installed
888 on enrolled devices, ensuring that the risk posture of the devices, and therefore the enterprise, stays at
889 an acceptable level.

890 Kryptowire also has configurable threat scores for various factors, such as requested permissions and
891 hardcoded encryption keys.

892 The threat scores can be configured to one of four levels:

- 893 ▪ low
- 894 ▪ medium
- 895 ▪ high
- 896 ▪ critical

897 The administrator can configure a threat score alert threshold and an email address to receive alerts
898 when an application’s threat score is at or above the threshold. The administrator can then take
899 appropriate action on the device in MaaS360.

900 Further, Kryptowire can provide information about applications including the latest version, when it was
901 last seen, when tracking began, and the number of versions that have been seen.

902 4.6.3 Palo Alto Networks—MaaS360

903 Palo Alto Networks GlobalProtect VPN secures remote connections from mobile devices. MaaS360
904 offers specific configuration options for the GlobalProtect client, using certificate-based authentication
905 to the GlobalProtect gateway and available for Android and iOS, that facilitate deployment of VPN
906 clients and enabled VPN access. [Section 4.5](#) presents details of the certificate enrollment process.

907 Two components of the Palo Alto Networks next-generation firewall compose the VPN architecture used
908 in this example solution—a GlobalProtect portal and a GlobalProtect gateway. The portal provides the

909 management functions for the VPN infrastructure. Every endpoint that participates in the GlobalProtect
910 network receives configuration information from the portal, including information about available
911 gateways as well as any client certificates that may be required to connect to the GlobalProtect
912 gateway(s). A GlobalProtect gateway provides security enforcement for network traffic. The
913 GlobalProtect gateway in this example solution is configured to provide mobile device users with access
914 to specific enterprise resources from the secure contexts after a successful authentication and
915 authorization decision.

916 The VPN tunnel negotiation between the VPN endpoint/mobile device context and the VPN gateway has
917 four steps: (1) The portal provides the client configuration, (2) a user logs into the system, (3) the agent
918 automatically connects to the gateway and establishes a VPN tunnel, and (4) the security policy on the
919 gateway enables access to internal and external applications.

920 For this example solution, a per-application VPN configuration is enforced on iOS and an always-on work
921 profile VPN configuration on Android. This configuration forces the device to automatically establish a
922 VPN connection to the GlobalProtect gateway whenever an application in the predefined list of
923 applications runs on the device or when an application in the work profile is launched.

924 4.6.4 iOS and Android MDM Integration

925 Both iOS and Android integrate directly with MaaS360. iOS devices are enrolled into MaaS360 using
926 User Enrollment, which is Apple's BYOD solution. User Enrollment creates a second persona on the
927 device, which places the work data on a separate encrypted partition on the device. User Enrollment
928 also requires managed user IDs, which are created in Apple Business Manager. This allows the
929 enterprise to associate the work data with the managed Apple ID, while the user associates their
930 personal data with their personal Apple ID.

931 Android devices are managed by Android Enterprise, which provides controls for both the device itself
932 and the work profile. The work profile is a separated, isolated, and encrypted environment based on an
933 SELinux user profile that stores all the enterprise applications and data, ensuring separation from
934 personal applications and data.

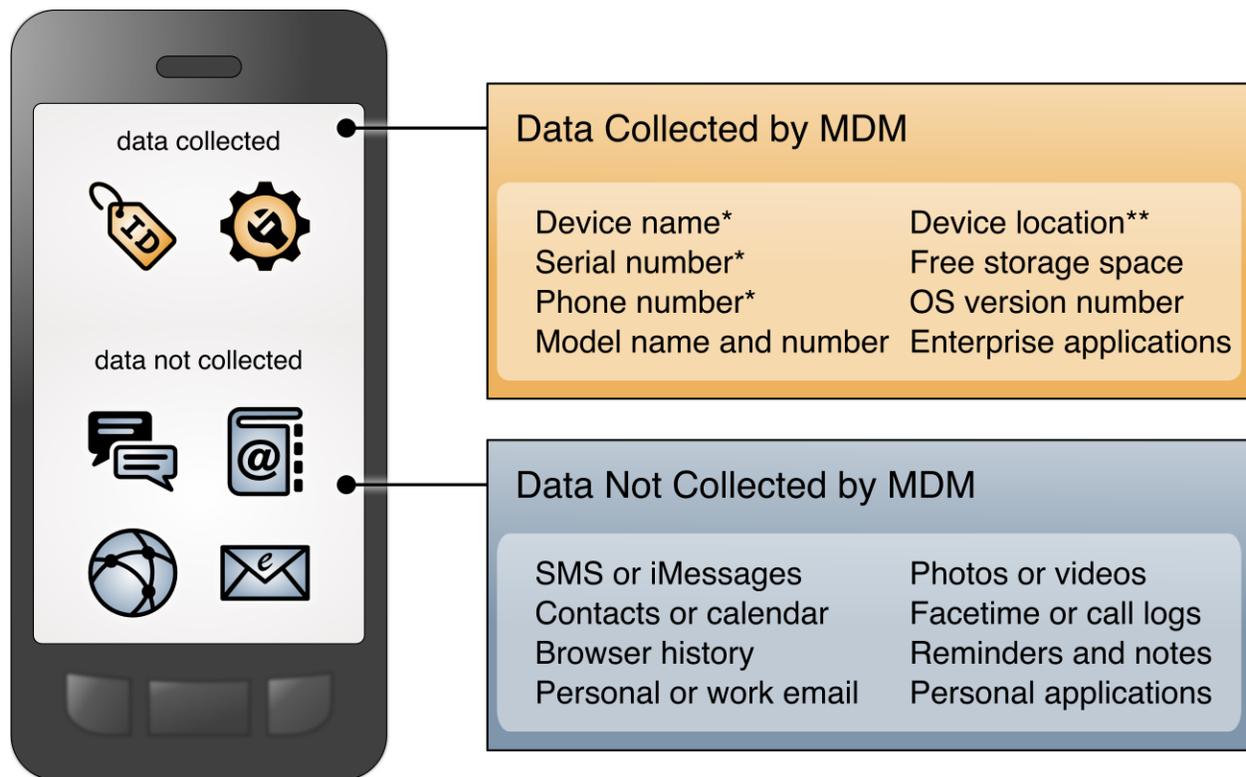
935 4.7 Privacy Settings: Mobile Device Data Processing

936 This section takes a look at components within the example architecture and the type of information an
937 enterprise may access from an employee's personal mobile device through those components.
938 Understanding the type of data an enterprise has access to can be helpful when understanding any
939 privacy implications.

940 4.7.1 EMM: MaaS360

941 When a personal mobile phone is connected to an EMM system, some data is collected and visible to
942 the enterprise. While additional data can be collected (depending on how devices are enrolled), our
943 example solution collects only the data shown in Figure 4-6 to help protect employee privacy. This
944 information is provided by MaaS360 to Kryptowire's application vetting capability. Kryptowire then uses
945 the MaaS360-supplied information to determine application security characteristics. IBM provides
946 documentation with more details on the information that MaaS360 collects and processes [28].

947 Figure 4-6 Data Collected by Example Solution Mobile Device Management



*: Android only
 **: With user consent

948 As shown in Figure 4-7, administrators can restrict collection of location and/or application inventory
 949 information. When an administrator restricts location collection, the administrator cannot see any
 950 location information about devices. Similarly, when an administrator restricts application inventory
 951 information, MaaS360 will only collect applications that are distributed through the enterprise and,
 952 therefore, will not transmit any personal applications to third-party application-vetting services. Both
 953 privacy controls can be applied to specific device groups—for example, location collection can be
 954 disabled for personally owned devices. These privacy controls typically only apply to devices that are
 955 enrolled as fully managed devices. Devices enrolled using Android Enterprise (work profile mode) or
 956 Apple User Enrollment have controls in place that prevent the EMM from accessing application
 957 inventory and location collection regardless of privacy control configuration.

958 **Figure 4-7 Example Solution Mobile Device Management Privacy Settings**

IBM MaaS360 | With Watson

Search for Devices, Users, Apps or Docs

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

➤ **Restrict Location Information**
Restrict administrators from collecting location indicators such as Physical Address, Geographical Coordinates & History, IP Address and SSID.

Select Applicable Ownership Types Corporate owned Employee owned
 Unknown

Select Applicable Group

➤ **Restrict App Inventory Information**
Restrict administrators from collecting personal App information. Apps distributed via the enterprise app catalog or part of corporate security policy will continue to be tracked.
NOTE: In case of Windows Desktops or Laptops, it is not possible to clearly distinguish corporate packages of type .msi or .exe from personal packages. Hence, windows packages will always be treated as personal apps and their information will not be collected when this setting is enabled.

Select Applicable Ownership Types Corporate owned Employee owned
 Unknown

Select Applicable Group

959 **4.7.2 MTD: Zimperium**

960 Zimperium provides configurable settings for what data is collected. In the list below, the top-level
 961 bullets can be disabled. Sub-bullets follow the enabled or disabled setting of the top-level. Zimperium
 962 also provides preset templates that can be utilized, including High, Medium, Low, and GDPR. When
 963 using the Custom template type, the enterprise can configure exactly what data is collected. Data
 964 collected can include:

- 965 ▪ device location (configurable granularity: street, city, county, none)
- 966 ▪ device operating system
- 967 ▪ device model
- 968 ▪ device IP address
- 969 ▪ device running processes (Android only)
- 970 ▪ network connection details
 - 971 ○ SSID
 - 972 ○ BSSID
 - 973 ○ external IP address
 - 974 ○ gateway IP
 - 975 ○ gateway MAC
 - 976 ○ nearby Wi-Fi networks
 - 977 ○ ARP table

- 978 ○ routing table
- 979 ▪ carrier information
- 980 ▪ attacker IP & MAC
- 981 ▪ risky or unapproved sites
- 982 ▪ phishing protection risky URLs
- 983 ▪ application forensics
- 984 ▪ application binaries (Android only)
- 985 ▪ application inventory (Android only)

986 zIPS also collects some information that cannot be disabled. These items include:

- 987 ▪ device root/jailbreak status
- 988 ▪ USB debug mode status (Android only)
- 989 ▪ developer mode status (Android only)
- 990 ▪ 3rd party app store presence (Android only)
- 991 ▪ mobile OS-specific vulnerability status (e.g., Stagefright)
- 992 ▪ device encryption status (Android only)
- 993 ▪ device protection status
- 994 ▪ screen lock status

995 zIPS must collect certain data items to properly communicate with the zConsole. These items include:

- 996 ▪ user credentials (email address, Zimperium-specific password)
- 997 ▪ mobile network operator
- 998 ▪ mobile network country code
- 999 ▪ device operating system
- 1000 ▪ device push token
- 1001 ▪ hash of local z9 database
- 1002 ▪ time and name of threat detection when a threat occurs

1003 4.7.3 Application Vetting: Kryptowire

1004 Kryptowire collects certain pieces of device information through the MaaS360 REST API for analytics and
1005 application association purposes. The data collected includes:

- 1006 ▪ MDM device ID
- 1007 ▪ MDM device name
- 1008 ▪ MDM username
- 1009 ▪ last MDM sync date
- 1010 ▪ MDM enrollment data

- 1011 ▪ enterprise and non-app store installed applications

1012 4.7.4 VPN: Palo Alto Networks

1013 The Palo Alto Networks VPN uses information about the device as it establishes VPN connections. The
1014 data collected by the VPN includes information about:

- 1015 ▪ device name
- 1016 ▪ logon domain
- 1017 ▪ operating system
- 1018 ▪ app version
- 1019 ▪ mobile device network information to which the device is connected
- 1020 ▪ device root/jailbreak status

1021 5 Security and Privacy Analysis

1022 This section familiarizes the reader with:

- 1023 ▪ the example solution’s assumptions and limitations
- 1024 ▪ results of the example solution’s laboratory testing
- 1025 ▪ scenarios and findings that show the security and privacy characteristics addressed by the
1026 reference design
- 1027 ▪ the security and privacy control capabilities of the example solution

1028 The purpose of the security and privacy characteristics evaluation is to understand the extent to which
1029 the project meets its objectives of demonstrating capabilities for securing mobile devices within an
1030 enterprise by deploying EMM, MTD, application vetting, secure boot/image authentication, and VPN
1031 services while also protecting the privacy of employees participating in the BYOD implementation.

1032 5.1 Analysis Assumptions and Limitations

1033 The security and privacy characteristics analysis has the following limitations:

- 1034 ▪ It is neither a comprehensive test of all security and privacy components nor a red-team
1035 exercise.
- 1036 ▪ It does not identify all weaknesses.
- 1037 ▪ It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these
1038 devices would reveal only weaknesses in implementation that would not be relevant to those
1039 adopting this reference architecture.

1040 5.2 Build Testing

1041 Test activities are provided to show how the example architecture addresses each TE and problematic
1042 data action. The NIST SP 1800-22 Supplement, *Example Scenario: Putting Guidance into Practice*,
1043 provides insights into how an organization may determine its susceptibility to the threat before

1044 implementing the architecture detailed in this practice guide. Also, NIST SP 1800-22 Volume C, Appendix
1045 D shows the test activities that were used to demonstrate how this practice guide's example solution
1046 addresses TEs and privacy risks.

1047 5.3 Scenarios and Findings

1048 One aspect of the security evaluation involved assessing how well the reference design addresses the
1049 security characteristics that it was intended to support. The Cybersecurity Framework and Privacy
1050 Framework Subcategories were used to provide structure to the security assessment by consulting the
1051 specific sections of each standard that are cited in reference to a subcategory. Using these subcategories
1052 as a basis for organizing the analysis, allowed systematic consideration of how well the reference design
1053 supports the intended security and privacy characteristics.

1054 This section of the publication provides findings for the security and privacy characteristics that the ex-
1055 ample solution was intended to support. These topics are described in the following subsections:

- 1056 ▪ development of the Cybersecurity Framework and NICE Framework mappings
- 1057 ▪ development of the Privacy Framework mappings
- 1058 ▪ TEs related to security and example solution architecture mitigations
- 1059 ▪ problematic data actions related to privacy and potential mitigations that organizations could
1060 employ

1061 An example scenario that demonstrates how an organization may use NIST SP 1800-22 and other NIST
1062 tools to implement a BYOD use case is discussed more in the NIST SP 1800-22 Supplement, *Example*
1063 *Scenario: Putting Guidance into Practice* of this practice guide.

1064 5.3.1 Cybersecurity Framework, Privacy Framework, and NICE Framework Work 1065 Roles Mappings

1066 As we installed, configured, and used the products in the architecture, we determined and documented
1067 the example solution's functions and their corresponding Cybersecurity Framework Subcategories, along
1068 with other guidance alignment.

1069 This mapping will help users of this practice guide communicate with their organization's stakeholders
1070 regarding the security controls that the practice guide recommends for helping mitigate BYOD threats,
1071 and the workforce capabilities that the example solution will require.

1072 The products, frameworks, security controls, and workforce mappings are in [Appendix E](#) (Cybersecurity
1073 Framework) and [Appendix H](#) (Privacy Framework).

1074 Developing profiles utilizing frameworks such as the Cybersecurity and Privacy Frameworks can help
1075 with identifying whether or not an organization is meeting their security and privacy expectations.

1076 5.3.2 Threat Events and Findings

1077 As part of the findings, the TEs were mitigated in the example solution architecture using the concepts
1078 and technology shown in Table 5-1. Each TE was matched with functions that helped mitigate the risks
1079 posed by the TE.

1080 Note: The TEE provided tamper-resistant processing environment capabilities that helped mitigate
 1081 mobile device runtime and memory threats in the example solution. We do not show the Qualcomm
 1082 TEE capability in the table because it is built into the phones used in this build.

1083 **Table 5-1 Threat Events and Findings Summary**

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 1: unauthorized access to sensitive information via a malicious or privacy-intrusive application	OS-level controls provide data separation between corporate and personal data.	EMM
Threat Event 2: theft of credentials through a short message service or email phishing campaign	Utilized PAN-DB and URL filtering to block known malicious websites.	Firewall
Threat Event 3: confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	Alerted the user that their OS is non-compliant.	EMM MTD
Threat Event 4: loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	Application vetting reports indicated if an application sent data without proper encryption.	Application vetting
Threat Event 5: compromise of device integrity via observed, inferred, or brute-forced device unlock code	The EMM enforces a required passcode. GlobalProtect requires periodic re-authentication.	EMM VPN
Threat Event 6: 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.	Application vetting
Threat Event 7: unauthorized access of enterprise resources from an unmanaged and potentially compromised device	Devices that were not enrolled in the EMM system were not able to connect to the corporate VPN.	VPN
Threat Event 8: loss of organizational data due to a lost or stolen device	Enforced passcode policies and device-wipe capabilities protected enterprise data.	EMM

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 9: 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

1084 The technologies in Table 5-1 are mapped to cybersecurity and privacy control mappings in [Appendix E](#)
 1085 and [Appendix F](#).

1086 **5.3.3 Privacy Risk Findings**

1087 The risk analysis found that three data actions in the build were potential privacy risks for individuals.
 1088 We identified potential technical mitigations that an organization could use to lessen their impact, as
 1089 shown below in Table 5-2. Organizations may also need to supplement these technical mitigations with
 1090 supporting policies and procedures.

1091 **Table 5-2 Summary of Privacy Risks and Findings**

Privacy Risk (for Employees)	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
Privacy Risk 1: Employee unable to access personal data or enterprise services or personal data is lost due to IT administrator performing device wipe or blocking access to device applications. This privacy risk is related to the Unwarranted Restriction Problematic Data Action.	<p>In the event of a security issue, employee access to enterprise resources can be prevented by removing the device from EMM control or restricting device access to organizational systems instead of wiping the device.</p> <p>The EMM enables selective wiping of only corporate resources from the device.</p> <p>To further protect the employee’s privacy, the ability to perform selective device information wipe activities can be limited to a small number of IT administrative staff.</p>	EMM
Privacy Risk 2: Employee personal activities and data disproportionately monitored and surveilled due	The example solution restricts staff access to system capabilities that permit	EMM

Privacy Risk (for Employees)	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
to use of information collected for operational purposes such as cybersecurity. This privacy risk is related to the Surveillance Problematic Data Action.	reviewing data about employees and their devices. Additionally, the example solution limits or disables collection of specific data elements (e.g., location data).	
Privacy Risk 3: Details about an employee are collected, transmitted and revealed to third party service providers. This privacy risk is related to the Unanticipated Revelation Problematic Data Action.	The example solution: <ul style="list-style-type: none"> • De-identifies personal and device data when it is not required to meet processing objectives. • Encrypts data transmitted between parties. • Limits or disables access to data. • Limits or disables the collection of specific data elements. 	EMM

1092 **5.4 Security and Privacy Control Mappings**

1093 The security and privacy capabilities of the example solution were identified, and example security and
1094 privacy control maps were developed to show these in a standardized methodology.

1095 The control maps show the security and privacy characteristics for the products used in the example
1096 solution.

1097 The security control map can be found in [Appendix E](#). The privacy control map is in [Appendix F](#).

1098 **6 Example Scenario: Putting Guidance into Practice**

1099 To demonstrate how an organization may use NIST SP 1800-22 and other NIST tools to implement a
1100 BYOD use case, the NCCoE created the *Example Scenario: Putting Guidance into Practice* supplement for
1101 this practice guide.

1102 This example scenario shows how a fictional, small-to-mid-size organization (Great Seneca Accounting)
1103 can successfully navigate common enterprise BYOD security challenges.

1104 In the narrative example, Great Seneca Accounting completes a security risk assessment by using the
1105 guidance in NIST SP 800-30 [29] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to
1106 the organization. The company then uses the NIST PRAM [8] to perform a privacy risk assessment.
1107 Appendix F and Appendix G of the Supplement describe these risk assessments in more detail. These risk
1108 assessments produce two significant conclusions:

- 1109 1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic
1110 data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the
1111 controls discussed in the example solution are relevant to their environment.
- 1112 2. The organization determines that it has a high-impact system, based on the impact guidance in
1113 NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
1114 [30], and needs to implement more controls beyond those identified in NIST SP 1800-22 to
1115 support the additional system components in its own solution (e.g., underlying OS, the data
1116 center where the equipment will reside).

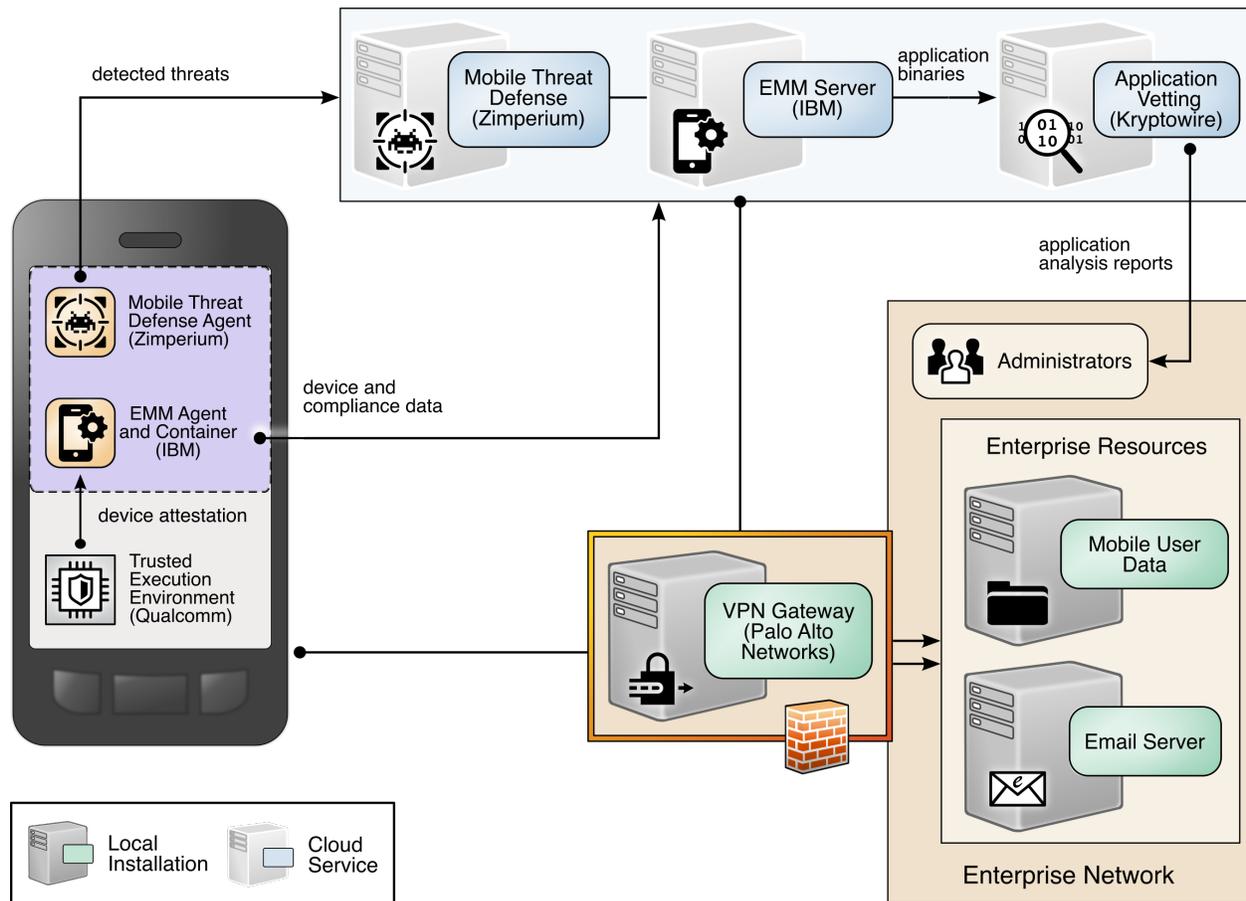
1117 As part of their review of NIST FIPS 200, Great Seneca Accounting selects security and privacy controls
1118 from NIST SP 800-53 [31] for their BYOD architecture implementation. They then tailor the control
1119 baselines based on the needs identified through the priority subcategories in its cybersecurity and
1120 privacy Target Profiles.

1121 A detailed description of the implementation process that the fictional organization Great Seneca
1122 Accounting followed is provided in the NIST SP 1800-22 *Example Scenario: Putting Guidance into*
1123 *Practice* supplement of this practice guide.

1124 7 Conclusion

1125 This practice guide provides an explanation of mobile device security and privacy concepts and an
1126 example solution for organizations implementing a BYOD deployment. As shown in Figure 7-1, this
1127 example solution applied multiple mobile device security technologies. These included a cloud-based
1128 EMM solution integrated with cloud- and agent-based mobile security technologies to help deploy a set
1129 of security and privacy capabilities that support the example solution.

1130 Figure 7-1 Example Solution Architecture



1131 Our fictional Great Seneca Accounting organization example scenario contained in the *Example*
 1132 *Scenario: Putting Guidance into Practice* supplement of this practice guide illustrates how the concepts
 1133 and architecture from this guide may be applied by an organization. Great Seneca started with an IT
 1134 infrastructure that lacked mobile device security architecture concepts. Great Seneca then employed
 1135 multiple NIST cybersecurity and privacy risk management tools to understand the gaps in its
 1136 architecture and the methods available today to enhance the security and privacy of its BYOD
 1137 deployment.

1138 This practice guide also includes in Volume C a series of how-to guides—step-by-step instructions
 1139 covering the initial setup (installation or provisioning) and configuration for each component of the
 1140 architecture—to help security engineers rapidly deploy and evaluate our example solution in their test
 1141 environment.

1142 The example solution uses standards-based, commercially available products that can be used by an
 1143 organization interested in deploying a BYOD solution. The example solution provides recommendations
 1144 for enhancing the security and privacy infrastructure by integrating on-premises and cloud-hosted
 1145 mobile security technologies. This practice guide provides an example solution that an organization may
 1146 use in whole or in part as the basis for creating a custom solution that best supports their unique needs.

1147 **8 Future Build Considerations**

1148 For a future build, the team is considering a virtual mobile infrastructure (VMI) or unified endpoint
1149 management (UEM) solution.

1150 The VMI deployment could include installing an application on a device at enrollment time, which would
1151 grant access to a virtual phone contained within the corporate infrastructure. The virtual phone would
1152 then contain the corporate-supplied applications that an employee would require for performing
1153 standard mobile work tasks. The thin client deployment limits the storage of organizational data on the
1154 device and helps ensure that access to the organization's data uses security-enhancing capabilities.

1155 UEM would entail managing a user's mobile device ecosystem, potentially including laptops, mobile
1156 phones, and internet of things devices (e.g., smart watches and Bluetooth headsets).

1157 **Appendix A List of Acronyms**

AD	Active Directory
API	Application Programming Interface
ATS	App Transport Security
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COPE	Corporate-Owned Personally-Enabled
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile Device Management
MTD	Mobile Threat Defense
NCCoE	National Cybersecurity Center of Excellence
NDES	Network Device Enrollment Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PII	Personally Identifiable Information
REST	Representational State Transfer
RMF	Risk Management Framework
SCEP	Simple Certificate Enrollment Protocol
SP	Special Publication
TE	Threat Event
TEE	Trusted Execution Environment
TLS	Transport Layer Security
UEM	Unified Endpoint Management
URL	Uniform Resource Locator

VPN

Virtual Private Network

Appendix B Glossary

Access Management	Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [32].
Availability	Ensure that users can access resources through remote access whenever needed [33].
Bring Your Own Device (BYOD)	A non-organization-controlled telework client device [33].
Confidentiality	Ensure that remote access communications and stored user data cannot be read by unauthorized parties [33].
Data Actions	System operations that process PII [34].
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [34].
Eavesdropping	An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant [35] (definition located under eavesdropping attack).
Firewall	Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [36].
Integrity	Detect any intentional or unintentional changes to remote access communications that occur in transit [33].
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [34].
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for

synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [31].

Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [37] (adapted from Government Accountability Office Report 08-536).
Predictability	Enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by a system [34].
Privacy Event	The occurrence or potential occurrence of problematic data actions [2].
Problematic Data Action	A data action that could cause an adverse effect for individuals [2].
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [29].
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [29].

1159 Appendix C References

- 1160 [1] National Institute of Standards and Technology (NIST). *NIST Framework for Improving Critical*
1161 *Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework). Apr. 16, 2018. [Online].
1162 Available: <https://www.nist.gov/cyberframework>.
- 1163 [2] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk*
1164 *Management*, Version 1.0 (Privacy Framework). Jan. 16, 2020. [Online]. Available:
1165 <https://www.nist.gov/privacy-framework>.
- 1166 [3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity*
1167 *Workforce Framework*, NIST Special Publication (SP) 800-181 (2017 version), NIST, Gaithersburg,
1168 Md., Aug. 2017. Available: <https://csrc.nist.gov/publications/detail/sp/800-181/final>.
- 1169 [4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available:
1170 [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview).
- 1171 [5] NIST. Mobile Threat Catalogue. [Online]. Available: [https://pages.nist.gov/mobile-threat-](https://pages.nist.gov/mobile-threat-catalogue/)
1172 [catalogue/](https://pages.nist.gov/mobile-threat-catalogue/).
- 1173 [6] J. Franklin et al., *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST
1174 SP 800-124 Revision 2 (Draft), NIST, Gaithersburg, Md., Mar. 2020. Available:
1175 <https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft>.
- 1176 [7] J. Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds*, NIST SP 1800-4, NIST,
1177 Gaithersburg, Md., Feb. 21, 2019. Available <https://doi.org/10.6028/NIST.SP.1800-4>.
- 1178 [8] NIST. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available:
1179 <https://www.nist.gov/privacy-framework/nist-pram>.
- 1180 [9] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A*
1181 *System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, NIST,
1182 Gaithersburg, Md., Dec. 2018. Available: [https://csrc.nist.gov/publications/detail/sp/800-](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)
1183 [37/rev-2/final](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final).
- 1184 [10] Open Web Application Security Project (OWASP). “OWASP Mobile Top 10,.” [Online]. Available:
1185 <https://owasp.org/www-project-mobile-top-10/>.
- 1186 [11] NIST. Privacy Engineering Program: Privacy Risk Assessment Methodology, Catalog of
1187 Problematic Data Actions and Problems. [Online]. Available: [https://www.nist.gov/itl/applied-](https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources)
1188 [cybersecurity/privacy-engineering/resources](https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources).
- 1189 [12] Qualcomm. “Mobile Security Solutions.” [Online]. Available:
1190 <https://www.qualcomm.com/products/features/mobile-security-solutions>.

- 1191 [13] National Information Assurance Partnership (NIAP). U.S. Government Approved Protection
1192 Profile—Extended Package for Mobile Device Management Agents Version 3.0. Nov. 21, 2016.
1193 [Online]. Available: https://www.niap-ccevs.org/MMO/PP/ep_mdm_agent_v3.0.pdf.
- 1194 [14] International Business Machines (IBM). About enterprise app wrapping. Aug. 09, 2022 last
1195 updated. [Online]. Available: [https://www.ibm.com/docs/en/maas360?topic=overview-about-](https://www.ibm.com/docs/en/maas360?topic=overview-about-enterprise-app-wrapping)
1196 [enterprise-app-wrapping](https://www.ibm.com/docs/en/maas360?topic=overview-about-enterprise-app-wrapping).
- 1197 [15] NIAP. U.S. Government Approved Protection Profile—Module for Virtual Private Network (VPN)
1198 Gateways 1.1. July 01, 2020. [Online]. Available: [https://www.niap-](https://www.niap-ccevs.org/Profile/Info.cfm?PPID=449&id=449)
1199 [ccevs.org/Profile/Info.cfm?PPID=449&id=449](https://www.niap-ccevs.org/Profile/Info.cfm?PPID=449&id=449).
- 1200 [16] NIAP. U.S. Government Approved Protection Profile—collaborative Protection Profile for
1201 Network Devices Version 2.2e. Mar. 27, 2020. Available: [https://www.niap-](https://www.niap-ccevs.org/Profile/Info.cfm?PPID=447&id=447)
1202 [ccevs.org/Profile/Info.cfm?PPID=447&id=447](https://www.niap-ccevs.org/Profile/Info.cfm?PPID=447&id=447).
- 1203 [17] NIAP. Approved Protection Profiles. [Online]. Available: [https://www.niap-](https://www.niap-ccevs.org/Profile/PP.cfm)
1204 [ccevs.org/Profile/PP.cfm](https://www.niap-ccevs.org/Profile/PP.cfm).
- 1205 [18] Qualcomm. “Qualcomm Secure Boot and Image Authentication Technical Overview.” [Online].
1206 Available: [https://www.qualcomm.com/media/documents/files/secure-boot-and-image-](https://www.qualcomm.com/media/documents/files/secure-boot-and-image-authentication-technical-overview-v1-0.pdf)
1207 [authentication-technical-overview-v1-0.pdf](https://www.qualcomm.com/media/documents/files/secure-boot-and-image-authentication-technical-overview-v1-0.pdf).
- 1208 [19] Google Android. Android Management API. [Online]. Available:
1209 <https://developers.google.com/android/management>.
- 1210 [20] Apple Inc. “Preventing Insecure Network Connections.” [Online]. Available:
1211 [https://developer.apple.com/documentation/security/preventing_insecure_network_connectio](https://developer.apple.com/documentation/security/preventing_insecure_network_connections)
1212 [ns](https://developer.apple.com/documentation/security/preventing_insecure_network_connections).
- 1213 [21] Apple Inc. " Identifying the Source of Blocked Connections," [Online]. Available:
1214 [https://developer.apple.com/documentation/security/preventing_insecure_network_connectio](https://developer.apple.com/documentation/security/preventing_insecure_network_connections/identifying_the_source_of_blocked_connections)
1215 [ns/identifying_the_source_of_blocked_connections](https://developer.apple.com/documentation/security/preventing_insecure_network_connections/identifying_the_source_of_blocked_connections).
- 1216 [22] Android.com. “Network security configuration.” Dec. 27, 2019. [Online]. Available:
1217 <https://developer.android.com/training/articles/security-config>.
- 1218 [23] NowSecure.com. “A Security Analyst’s Guide to Network Security Configuration in Android P.”
1219 [Online]. Available: [https://www.nowsecure.com/blog/2018/08/15/a-security-analysts-guide-](https://www.nowsecure.com/blog/2018/08/15/a-security-analysts-guide-to-network-security-configuration-in-android-p/)
1220 [to-network-security-configuration-in-android-p/](https://www.nowsecure.com/blog/2018/08/15/a-security-analysts-guide-to-network-security-configuration-in-android-p/).

- 1221 [24] Apple Inc. "Overview: Managing Devices & Corporate Data on iOS." July 2018. [Online].
1222 Available:
1223 [https://www.apple.com/business/docs/resources/Managing_Devices_and_Corporate_Data_on](https://www.apple.com/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf)
1224 [iOS.pdf](https://www.apple.com/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf).
- 1225 [25] Google Android. "Build Android management solutions for enterprises." [Online]. Available:
1226 <https://developers.google.com/android/work>.
- 1227 [26] International Business Machines (IBM). "Web Services." [Online]. Available:
1228 <https://www.ibm.com/docs/en/maas360?topic=web-services>.
- 1229 [27] IBM. "IBM Community Public Wikis." [Online]. Available:
1230 [https://www.ibm.com/developerworks/community/wikis/home?lang=en-](https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usage)
1231 [us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usa](https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usage)
1232 [ge](https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usage).
- 1233 [28] IBM. "MaaS360 Data Privacy Information." [Online]. Available:
1234 <https://www.ibm.com/support/pages/maas360-data-privacy-information>.
- 1235 [29] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-
1236 30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available:
1237 <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>.
- 1238 [30] NIST. *Minimum Security Requirements for Federal Information and Information Systems*, Federal
1239 Information Processing Standards Publication (FIPS) 200, Mar. 2006. Available:
1240 <https://csrc.nist.gov/publications/detail/fips/200/final>.
- 1241 [31] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems*
1242 *and Organizations*, NIST SP 800-53, NIST, Gaithersburg, Md., Jan. 2015. Available:
1243 <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>.
- 1244 [32] IDManagement.gov. "Federal Identity, Credential, and Access Management Architecture."
1245 [Online]. Available: <https://arch.idmanagement.gov/services/access/>.
- 1246 [33] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own*
1247 *Device (BYOD) Security*, NIST SP 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available:
1248 <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>.
- 1249 [34] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal*
1250 *Systems*, NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available:
1251 <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.
- 1252 [35] P. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017.
1253 Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.

- 1254 [36] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Revision 2,
1255 NIST, Gaithersburg, Md., May 2015. Available:
1256 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.
- 1257 [37] E. McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information*
1258 *(PII)*, NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available:
1259 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.
- 1260 [38] J. Franklin et al., *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*, NIST SP
1261 1800-21, NIST, Gaithersburg, Md., July 22, 2019. Available:
1262 <https://csrc.nist.gov/News/2019/NIST-Releases-Draft-SP-1800-21-for-Comment>.
- 1263 [39] NIST, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS)*
1264 *Implementations*, NIST SP 800-52 Revision 2, August 2019. [Online]. Available:
1265 <https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final>.
- 1266 [40] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations (Final*
1267 *Public Draft)*, NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available:
1268 <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.
- 1269 [41] S. Frankel et al., *Guide to SSL VPNs*, NIST SP 800-113, NIST, Gaithersburg, Md., July 2008.
1270 Available: <https://csrc.nist.gov/publications/detail/sp/800-113/final>.
- 1271 [42] M. Souppaya and K. Scarfone, *User's Guide to Telework and Bring Your Own Device (BYOD)*
1272 *Security*, NIST SP 800-114 Revision 1, NIST, Gaithersburg, Md., July 2016. Available:
1273 <https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final>.
- 1274 [43] M. Ogata et al., *Vetting the Security of Mobile Applications*, NIST SP 800-163 Revision 1, NIST,
1275 Gaithersburg, Md., Apr. 2019. Available:
1276 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf>.
- 1277 [44] NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems*, NIST SP 800-171
1278 Revision 2, February 2020. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>.
- 1280 [45] Center for Internet Security. Center for Internet Security home page. [Online]. Available:
1281 <https://www.cisecurity.org/>.
- 1282 [46] Executive Office of the President, "Bring Your Own Device: A Toolkit to Support Federal Agencies
1283 Implementing Bring Your Own Device (BYOD) Programs," Aug. 23, 2012. Available:
1284 <https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device>.

- 1285 [47] Federal CIO Council and Department of Homeland Security. *Mobile Security Reference*
1286 *Architecture Version 1.0*. May 23, 2013. [Online]. Available:
1287 [https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf)
1288 [Reference-Architecture.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf).
- 1289 [48] Digital Services Advisory Group and Federal Chief Information Officers Council. *Government Use*
1290 *of Mobile Technology Barriers, Opportunities, and Gap Analysis*,. Dec. 2012. [Online]. Available:
1291 [https://s3.amazonaws.com/sitesusa/wp-](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf)
1292 [content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf)
1293 [_and_Gaps.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf).
- 1294 [49] International Organization for Standardization. “ISO/IEC 27001:2013 Information technology —
1295 Security techniques — Information security management systems — Requirements.” Oct. 2013.
1296 [Online]. Available: <https://www.iso.org/standard/54534.html>.
- 1297 [50] “Mobile Computing Decision.” [Online]. Available: [https://s3.amazonaws.com/sitesusa/wp-](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf)
1298 [content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf).
- 1299 [51] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center
1300 (ATARC). “Mobile Threat Protection App Vetting and App Security, Working Group Document.”
1301 July 2017. [Online]. Available: [https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-](https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12996/Mobile_Threat_Protection_Deliverable.pdf)
1302 [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).
- 1303 [52] Mobile Services Category Team (MSCT). “Device Procurement and Management Guidance.”
1304 Nov. 2016. [Online]. Available: [https://hallways.cap.gsa.gov/app/#/gateway/information-](https://hallways.cap.gsa.gov/app/#/gateway/information-technology/4485/mobile-device-procurement-and-management-guidance)
1305 [technology/4485/mobile-device-procurement-and-management-guidance](https://hallways.cap.gsa.gov/app/#/gateway/information-technology/4485/mobile-device-procurement-and-management-guidance).
- 1306 [53] Mobile Services Category Team (MSCT). “Mobile Device Management (MDM), MDM Working
1307 Group Document.” Aug. 2017. [Online]. Available: [https://s3.amazonaws.com/sitesusa/wp-](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf)
1308 [content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf).
- 1309 [54] Mobile Services Category Team (MSCT). “Mobile Services Roadmap (MSCT Strategic Approach).”
1310 Sept. 23, 2016. [Online]. Available: [https://atarc.org/project/mobile-services-roadmap-msct-](https://atarc.org/project/mobile-services-roadmap-msct-strategic-approach/)
1311 [strategic-approach/](https://atarc.org/project/mobile-services-roadmap-msct-strategic-approach/).
- 1312 [55] NIAP. U.S. Government Approved Protection Profile—Extended Package for Mobile Device
1313 Management Agents Version 2.0. Dec. 31, 2014. [Online]. Available: [https://www.niap-](https://www.niap-ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf)
1314 [ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf](https://www.niap-ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf).
- 1315 [56] NIAP. Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version
1316 3.1,. June 16, 2017. [Online]. Available: [https://www.niap-](https://www.niap-ccevs.org/Profile/Info.cfm?PPID=417&id=417)
1317 [ccevs.org/Profile/Info.cfm?PPID=417&id=417](https://www.niap-ccevs.org/Profile/Info.cfm?PPID=417&id=417).

- 1318 [57] NIAP. Approved Protection Profiles—Protection Profile for Mobile Device Management Version
1319 4.0. Apr. 25, 2019. [Online]. Available: [https://www.niap-
ccevs.org/Profile/Info.cfm?PPID=428&id=428](https://www.niap-
1320 ccevs.org/Profile/Info.cfm?PPID=428&id=428).
- 1321 [58] NIAP. Product Compliant List. [Online]. Available: <https://www.niap-ccevs.org/Product/>.
- 1322 [59] Office of Management and Budget, Category Management Policy 16-3: Improving the
1323 Acquisition and Management of Common Information Technology: Mobile Devices and Services,
1324 Aug. 4, 2016. Available:
1325 https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_20.pdf
1326 [f](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_20.pdf)
- 1327 [60] NIST. United States Government Configuration Baseline (in development). [Online]. Available:
1328 <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>.
- 1329 [61] Department of Homeland Security (DHS). “DHS S&T Study on Mobile Device Security.” Apr.
1330 2017. [Online]. Available: <https://www.dhs.gov/publication/csd-mobile-device-security-study>.
- 1331 [62] NIST, NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the*
1332 *Cybersecurity Framework*, Mar. 2020. [Online]. Available:
1333 <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf>.
- 1334 [63] NIST Privacy Framework and Cybersecurity Framework to NIST Special Publication 800-53,
1335 Revision 5 Crosswalk. [Online]. Available: [https://www.nist.gov/privacy-framework/nist-privacy-
framework-and-cybersecurity-framework-nist-special-publication-800-53](https://www.nist.gov/privacy-framework/nist-privacy-
1336 framework-and-cybersecurity-framework-nist-special-publication-800-53).

1337 Appendix D Standards and Guidance

- 1338 ▪ National Institute of Standards and Technology (NIST) *Framework for Improving Critical*
1339 *Infrastructure Cybersecurity* (Cybersecurity Framework) Version 1.1 [1]
- 1340 ▪ *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,*
1341 Version 1.0 (Privacy Framework) [2]
- 1342 ▪ NIST Mobile Threat Catalogue [5]
- 1343 ▪ NIST Risk Management Framework [4]
- 1344 ▪ NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [7]
- 1345 ▪ NIST SP 1800-21, *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* [38]
- 1346 ▪ NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [29]
- 1347 ▪ NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and*
1348 *Organizations: A System Life Cycle Approach for Security and Privacy* [9]
- 1349 ▪ NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own*
1350 *Device (BYOD) Security* [33]
- 1351 ▪ NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport*
1352 *Layer Security (TLS) Implementations* [39]
- 1353 ▪ NIST SP 800-53 Revision 4 (Final), *Security and Privacy Controls for Information Systems and*
1354 *Organizations* [31]
- 1355 ▪ NIST SP 800-53 Revision 5 (Final), *Security and Privacy Controls for Information Systems and*
1356 *Organizations* [40]
- 1357 ▪ NIST SP 800-63-3, *Digital Identity Guidelines* [35]
- 1358 ▪ NIST SP 800-113, *Guide to SSL VPNs* [41]
- 1359 ▪ NIST SP 800-114 Revision 1, *User’s Guide to Telework and Bring Your Own Device (BYOD)*
1360 *Security* [42]
- 1361 ▪ NIST SP 800-124 Revision 2 (Draft), *Guidelines for Managing the Security of Mobile Devices in the*
1362 *Enterprise* [6]
- 1363 ▪ NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [43]
- 1364 ▪ NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal*
1365 *Systems and Organizations* [44]
- 1366 ▪ NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce*
1367 *Framework (2017)* [3]
- 1368 ▪ NIST Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security*
1369 *Requirements for Federal Information and Information Systems* [30]

- 1370 ▪ NIST Privacy Risk Assessment Methodology [8]
- 1371 ▪ Center for Internet Security [45]
- 1372 ▪ Executive Office of the President, Bring Your Own Device toolkit [46]
- 1373 ▪ Federal Chief Information Officers Council and Department of Homeland Security *Mobile*
- 1374 *Security Reference Architecture, Version 1.0* [47]
- 1375 ▪ Digital Services Advisory Group and Federal Chief Information Officers Council, *Government Use*
- 1376 *of Mobile Technology Barriers, Opportunities, and Gap Analysis* [48]
- 1377 ▪ International Organization for Standardization (ISO), International Electrotechnical Commission
- 1378 (IEC) 27001:2013, “Information technology – Security techniques – Information security
- 1379 management systems – Requirements” [49]
- 1380 ▪ Mobile Computing Decision example case study [50]
- 1381 ▪ MSCT ATARC, “Mobile Threat Protection App Vetting and App Security,” Working Group
- 1382 Document [51]
- 1383 ▪ MSCT, “Device Procurement and Management Guidance” [52]
- 1384 ▪ MSCT, “Mobile Device Management (MDM),” MDM Working Group Document [53]
- 1385 ▪ MSCT, “Mobile Services Roadmap, MSCT Strategic Approach” [54]
- 1386 ▪ National Information Assurance Partnership (NIAP), U.S. Government Approved Protection
- 1387 Profile—Extended Package for Mobile Device Management Agents Version 2.0 [55]
- 1388 ▪ NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version
- 1389 3.1 [56]
- 1390 ▪ NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Management Version
- 1391 4.0 [57]
- 1392 ▪ NIAP, Product Compliant List [58]
- 1393 ▪ Office of Management and Budget, *Category Management Policy 16-3: Improving the*
- 1394 *Acquisition and Management of Common Information Technology: Mobile Devices and Services*
- 1395 [59]
- 1396 ▪ United States Government Configuration Baseline [60]
- 1397 ▪ Department of Homeland Security (DHS), “DHS S&T Study on Mobile Device Security” [61]
- 1398 ▪ NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the*
- 1399 *Cybersecurity Framework* [62]

1400 **Appendix E Example Security Subcategory and Control Map**

1401 Using the developed risk information as input, the security characteristics of the example solution were identified. A security control map was
 1402 developed documenting the example solution’s capabilities with applicable Subcategories from the National Institute of Standards and
 1403 Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1]; NIST Special
 1404 Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* [40]; International Organization for
 1405 Standardization (ISO); International Electrotechnical Commission (IEC) 27001:2013 *Information technology – Security techniques – Information
 1406 security management systems – Requirements* [49]; the Center for Internet Security’s (CIS) control set Version 6 [45]; and NIST SP 800-181,
 1407 *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

1408 Table E-1’s example security control map identifies the security characteristic standards mapping for the products as they were used in the
 1409 example solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended
 1410 that the mapping not be used as a reference for all of the security capabilities these products may be able to address.

1411 **Table E-1 Example Solution’s Cybersecurity Standards and Best Practices Mapping**

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Mobile Threat Defense						
Kryptowire Cloud Service	Application Vetting	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8: Security Assessment and Authorization RA-3, RA-5: Risk Assessment SA-4: Acquisition Process	A.12.6.1: Control of technical vulnerabilities A.18.2.3: Technical Compliance Review	CSC 4: Continuous Vulnerability Assessment and Remediation	SP-RSK-002: Security Control Assessor SP-ARC-002: Security Architect OM-ANA-001: Systems Security Analyst

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			<p>SI-7: Software, Firmware, and Information Integrity</p>			
		<p>ID.RA-3: Threats, both internal and external, are identified and documented.</p>	<p>RA-3: Risk Assessment</p> <p>SI-7: Software, Firmware, and Information Integrity</p> <p>PM-12, PM-16: Insider Threat Program</p>	<p>6.1.2: Information risk assessment process</p>	<p>CSC 4: Continuous Vulnerability Assessment and Remediation</p>	<p>SP-RSK-002: Security Control Assessor</p> <p>OM-ANA-001: Systems Security Analyst</p> <p>OV-SPP-001: Cyber Workforce Developer and Manager</p> <p>OV-TEA-001: Cyber Instructional Curriculum Developer</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
						<p>PR-VAM-001: Vulnerability Assessment Analyst</p> <p>PR-VAM-001: Vulnerability Assessment Analyst</p>
		<p>DE.CM-4: Malicious code is detected.</p>	<p>SI-7: Software, Firmware, and Information Integrity</p>	<p>A.12.2.1: Controls Against Malware</p>	<p>CSC 4: Continuous Vulnerability Assessment and Remediation</p> <p>CSC 7: Email and Web Browser Protections</p> <p>CSC 8: Malware Defenses</p> <p>CSC 12: Boundary Defense</p>	<p>PR-CIR-001: Cyber Defense Incident Responder</p> <p>PR-CDA-001: Cyber Defense Analyst</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		DE.CM-5: Unauthorized mobile code is detected.	SC-18: Mobile Code SI-7: Software, Firmware, and Information Integrity	A.12.5.1: Installation of Software on Operational Systems A.12.6.2: Restrictions on Software Installation	CSC 7: Email and Web Browser Protections CSC 8: Malware Defenses	PR-CDA-001: Cyber Defense Analyst SP-DEV-002: Secure Software Assessor
Zimperium Console version vGA-4.23.1	Cloud service that complements the zIPS Agent	ID.AM-1: Physical devices and systems within the organization are inventoried.	CM-8: Information System Component Inventory PM-5: Information System Inventory	A.8.1.1: Inventory of Assets A.8.1.2: Ownership of Assets	CSC 1: Inventory of Authorized and Unauthorized Devices	OM-STS-001: Technical Support Specialist OM-NET-001: Network Operations Specialist OM-ADM-001: System Administrator

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
<p>zIPS agent Version 4.9.2 (iOS), 4.9.2 (Android)</p>	<p>Endpoint security for mobile device threats</p>	<p>ID.AM-2: Software platforms and applications within the organization are inventoried.</p>	<p>CM-8: Information System Component Inventory</p> <p>PM-5: Information System Inventory</p>	<p>A.8.1.1: Inventory of Assets</p> <p>A.8.1.2: Ownership of Assets</p> <p>A.12.5.1: Installation of Software on Operational Systems</p>	<p>CSC 2: Inventory of Authorized and Unauthorized Software</p>	<p>SP-DEV-002: Secure Software Assessor</p> <p>SP-DEV-001: Software Developer</p> <p>SP-TRD-001: Research and Development Specialist</p>
		<p>DE.CM-8: Vulnerability scans are performed.</p>	<p>RA-5: Vulnerability Monitoring and Scanning</p>	<p>A.12.6.1: Management of technical vulnerabilities</p>	<p>CSC 4: Continuous Vulnerability Assessment and Remediation</p> <p>CSC 20: Penetration Tests and Red Team Exercises</p>	<p>PR-VAM-001: Vulnerability Assessment Analyst</p> <p>PR-INF-001: Cyber Defense Infrastructure Support Specialist</p> <p>PR-CDA-001: Cyber Defense Analyst</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		<p>DE.AE-5: Incident alert thresholds are established.</p>	<p>IR-4: Incident Handling</p> <p>IR-5: Incident Monitoring</p> <p>IR-8: Incident Response Plan</p>	<p>A.16.1.4: Assessment of and decision on information security events</p>	<p>CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs</p> <p>CSC 19: Incident Response and Management</p>	<p>PR-CIR-001: Cyber Defense Incident Responder</p> <p>AN-TWA-001: Threat/Warning Analyst</p>
		<p>DE.CM-5: Unauthorized mobile code is detected.</p>	<p>SC-18: Mobile Code</p> <p>SI-7: Software, Firmware, and Information Integrity</p>	<p>A.12.5.1: Installation of Software on Operational Systems</p> <p>A.12.6.2: Restrictions on Software Installation</p>	<p>CSC 7: Email and Web Browser Protections</p> <p>CSC 8: Malware Defenses</p>	<p>PR-CDA-001: Cyber Defense Analyst</p> <p>SP-DEV-002: Secure Software Assessor</p>
Enterprise Mobility Management						
<p>IBM MaaS360 Mobile Device Management (SaaS) Version 10.73</p>	<p>Enforces organizational mobile endpoint security policy</p>	<p>ID.AM-1: Physical devices and systems within the organization are inventoried.</p>	<p>CM-8: System Component Inventory</p> <p>PM-5: System Inventory</p>	<p>A.8.1.1: Inventory of Assets</p> <p>A.8.1.2: Ownership of Assets</p>	<p>CSC 1: Inventory of Authorized and Unauthorized Devices</p>	<p>OM-STS-001: Technical Support Specialist</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
						<p>OM-NET-001: Network Operations Specialist</p> <p>OM-ADM-001: System Administrator</p>
		<p>ID.AM-2: Software platforms and applications within the organization are inventoried.</p>	<p>CM-8: System Component Inventory</p> <p>PM-5: System Inventory</p>	<p>A.8.1.1: Inventory of Assets</p> <p>A.8.1.2: Ownership of Assets</p> <p>A.12.5.1: Installation of Software on Operational Systems</p>	<p>CSC 2: Inventory of Authorized and Unauthorized Software</p>	<p>SP-DEV-002: Secure Software Assessor</p> <p>SP-DEV-001: Software Developer</p> <p>SP-TRD-001: Research and Development Specialist</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		<p>PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.</p>	<p>AC-3: Access Enforcement</p> <p>IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11: Identification and Authentication Family</p>	<p>A.9.2.1: User Registration and De-Registration</p> <p>A.9.2.2: User Access Provisioning</p> <p>A.9.2.3: Management of Privileged Access Rights</p> <p>A.9.2.4: Management of Secret Authentication Information of Users</p> <p>A.9.2.6: Removal or Adjustment of Access Rights</p> <p>A.9.3.1: Use of Secret Authentication Information</p>	<p>CSC 1: Inventory of Authorized and Unauthorized Devices</p> <p>CSC 5: Controlled Use of Administrative Privileges</p> <p>CSC 15: Wireless Access Control</p> <p>CSC 16: Account Monitoring and Control</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>OM-ADM-001: System Administrator</p> <p>OV-MGT-002: Communications Security (COMSEC) Manager</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
				<p>A.9.4.2: Secure logon Procedures</p> <p>A.9.4.3: Password Management System</p>		

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		<p>PR.AC-3: Remote access is managed.</p>	<p>AC-1: Access Control Policy and Procedures</p> <p>AC-17: Remote Access</p> <p>AC-19: Access Control for Mobile Devices</p> <p>AC-20: Use of External Systems</p> <p>SC-15: Collaborative Computing Devices and Applications</p>	<p>A.6.2.1: Mobile Device Policy</p> <p>A.6.2.2: Teleworking</p> <p>A.11.2.6: Security of equipment and assets off premises</p> <p>A.13.1.1: Network Controls</p> <p>A.13.2.1: Information Transfer Policies and Procedures</p>	<p>CSC 12: Boundary Defense</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>OV-MGT-002: Communications Security (COMSEC) Manager</p>
		<p>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.</p>	<p>AC-1, AC-3: Access Control Policy and Procedures</p> <p>IA-2, IA-4, IA-5: Identification</p>	<p>A.7.1.1: Screening</p> <p>A.9.2.1: User Registration and De-Registration</p>	<p>CSC 16: Account Monitoring and Control</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>OV-MGT-002: Communications Security</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			and Authentica- tion PE-2: Physical Access Authori- zations			(COMSEC) Man- ager
		PR.IP-1: A baseline configuration of in- formation technol- ogy/industrial con- trol systems is cre- ated and main- tained, incorporat- ing security princi- ples (e.g., concept of least function- ality).	CM-8: System Component In- ventory SA-10: Devel- oper Configura- tion Manage- ment	A.12.1.2: Change Management A.12.5.1: Installa- tion of Software on Operational Systems A.12.6.2: Re- strictions on Soft- ware Installation A.14.2.2: System Change Control Procedures A.14.2.3: Tech- nical Review of Applications After Operating Plat- form Changes	CSC 3: Secure Configurations for Hardware and Software on Mobile De- vices, Laptops, Workstations, and Servers CSC 9: Limita- tion and Con- trol of Network Ports, Proto- cols, and Ser- vices CSC 11: Secure Configurations for Network Devices such as	SP-ARC-002: Security Archi- tect OV-SPP-002: Cyber Policy and Strategy Planner SP-SYS-001: Information Sys- tems Security Developer OM-ADM-001: System Adminis- trator

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
				<p>A.14.2.4: Restrictions on Changes to Software Packages</p>	<p>Firewalls, Routers, and Switches</p>	<p>PR-VAM-001: Vulnerability Assessment Analyst</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
<p>IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)</p>	<p>Endpoint software that complements IBM MaaS360 Mobile Device Management console—provides root/jail-break detection and other functions</p>	<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p>SC-16: Transmission of Security and Privacy Attributes</p> <p>SI-7: Software, Firmware, and Information Integrity</p>	<p>A.12.2.1: Controls Against Malware</p> <p>A.12.5.1: Installation of Software on Operational Systems</p> <p>A.14.1.2: Securing Application Services on Public Networks</p> <p>A.14.1.3: Protecting Application Services Transactions</p> <p>A.14.2.4: Restrictions on Changes to Software Packages</p>	<p>CSC 2: Inventory of Authorized and Unauthorized Software</p> <p>CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>SP-ARC-001: Enterprise Architect</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Trusted Execution Environment						
Qualcomm (version is mobile device dependent)	Secure boot and image integrity	PR.DS-1: Data-at-rest is protected.	SC-28: Protection of Information at Rest	A.8.2.3: Handling of Assets	CSC 13: Data Protection CSC 14: Controlled Access Based on the Need to Know	OV-SPP-002: Cyber Policy and Strategy Planner PR-INF-001: Cyber Defense Infrastructure Support Specialist OV-LGA-002: Privacy Officer/Privacy Compliance Manager OV-MGT-002: Communications Security (COMSEC) Manager

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p>SA-10(1): Developer Configuration Management</p> <p>SI-7: Software, Firmware, and Information Integrity</p>	<p>A.12.2.1: Controls Against Malware</p> <p>A.12.5.1: Installation of Software on Operational Systems</p> <p>A.14.1.2: Securing Application Services on Public Networks</p> <p>A.14.1.3: Protecting Application Services Transactions</p> <p>A.14.2.4: Restrictions on Changes to Software Packages</p>	<p>CSC 2: Inventory of Authorized and Unauthorized Software</p> <p>CSC 3: Secure Configurations for Hardware and Software on Mobile</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>PR-CDA-001: Cyber Defense Analyst</p> <p>SP-ARC-001: Enterprise Architect</p>
		<p>PR.DS-8: Integrity checking mechanisms are used to</p>	<p>SA-10: Developer Configuration Management</p>	<p>A.11.2.4: Equipment maintenance</p>	<p>Not applicable</p>	<p>OM-ADM-001: System Administrator</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		verify hardware integrity.	SI-7: Software, Firmware, and Information Integrity			SP-ARC-001: Enterprise Architect
		DE.CM-4: Malicious code is detected.	SC-35: External Malicious Code Identification SI-7: Software, Firmware, and Information Integrity	A.12.2.1: Controls Against Malware	CSC 4: Continuous Vulnerability Assessment and Remediation CSC 7: Email and Web Browser Protections CSC 8: Malware Defenses CSC 12: Boundary Defense	PR-CDA-001: Cyber Defense Analyst PR-INF-001: Cyber Defense Infrastructure Support Specialist
Virtual Private Network						
Palo Alto Networks PA-220	Enforces network security policy for remote devices	PR.AC-3: Remote access is managed.	AC-1, AC-3: Access Control Policy and Procedures	A.6.2.1: Mobile Device Policy A.6.2.2: Teleworking	CSC 12: Boundary Defense	OV-SPP-002: Cyber Policy and Strategy Planner

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			<p>AC-19: Access Control for Mobile Devices</p>	<p>A.11.2.6: Security of equipment and assets off-premises</p> <p>A.13.1.1: Network Controls</p> <p>A.13.2.1: Information Transfer Policies and Procedures</p>		<p>OV-MGT-002: Communications Security (COMSEC) Manager</p>
		<p>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).</p>	<p>AC-3: Access Enforcement</p> <p>SC-7: Boundary Protection</p>	<p>A.13.1.1: Network Controls</p> <p>A.13.1.3: Segregation in Networks</p> <p>A.13.2.1: Information Transfer Policies and Procedures</p> <p>A.14.1.2: Securing Application</p>	<p>CSC 9: Limitation and Control of Network Ports, Protocols, and Services</p> <p>CSC 14: Controlled Access Based on the Need to Know</p>	<p>PR-CDA-001: Cyber Defense Analyst</p> <p>OM-ADM-001: System Administrator</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
				<p>Services on Public Networks</p> <p>A.14.1.3: Protecting Application Services Transactions</p>	<p>CSC 15: Wireless Access Control</p> <p>CSC 18: Application Software Security</p>	
		<p>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.</p>	<p>AC-3: Access Enforcement</p> <p>IA-2, IA-4, IA-5, IA-8: Identification and Authentication (Organizational Users)</p> <p>PE-2: Physical Access Authorizations</p> <p>PS-3: Personnel Screening</p>	<p>A.7.1.1: Screening</p> <p>A.9.2.1: User Registration and De-Registration</p>	<p>CSC 16: Account Monitoring and Control</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>OV-MGT-002: Communications Security (COMSEC) Manager</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		<p>PR.DS-2: Data-in-transit is protected.</p>	<p>AC-17(2): Protection of Confidentiality and Integrity Using Encryption</p> <p>SC-8: Transmission Confidentiality and Integrity</p>	<p>A.8.2.3: Handling of Assets</p> <p>A.13.1.1: Network Controls</p> <p>A.13.2.1: Information Transfer Policies and Procedures</p> <p>A.13.2.3: Electronic Messaging</p> <p>A.14.1.2: Securing Application Services on Public Networks</p> <p>A.14.1.3: Protecting Application Services Transactions</p>	<p>CSC 13: Data Protection</p> <p>CSC 14: Controlled Access Based on the Need to Know</p>	<p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>OV-MGT-002: Communications Security (COMSEC) Manager</p> <p>OV-LGA-002: Privacy Officer/Privacy Compliance Manager</p>
		<p>PR.PT-4: Communications and control networks are protected.</p>	<p>AC-3, AC-4, AC-17, AC-18: Access Control Family</p>	<p>A.13.1.1: Network Controls</p>	<p>CSC 8: Malware Defenses</p>	<p>PR-INF-001: Cyber Defense Infrastructure</p>

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			<p>CP-2: Contingency Plan</p> <p>SC-7, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-38, SC-39, SC-40, SC-41, SC-43: System and Communications Protection Family</p>	<p>A.13.2.1: Information Transfer Policies and Procedures</p> <p>A.14.1.3: Protecting Application Services Transactions</p>	<p>CSC 12: Boundary Defense</p> <p>CSC 15: Wireless Access Control</p>	<p>Support Specialist</p> <p>OV-SPP-002: Cyber Policy and Strategy Planner</p> <p>PR-CDA-001: Cyber Defense Analyst</p>

1412 **Appendix F Example Privacy Subcategory and Control Map**

1413 Using the developed privacy information as input, we identified the privacy characteristics of the example solution. We developed a privacy
 1414 control map documenting the example solution’s capabilities with applicable Functions, Categories, and Subcategories from the National
 1415 Institute of Standards and Technology (NIST) Privacy Framework [2]; and NIST SP 800-53 Revision 5 [40]; and NIST SP 800-181, *National Initiative*
 1416 *for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version) [3].*

1417 The table that follows maps component functions in the build to the related Subcategories in the NIST Privacy Framework as well as to controls
 1418 in the NIST SP 800-53, Revision 5 controls catalog. Each column maps independently to the build component’s functions and, given the specific
 1419 capabilities of this mobile device security solution, may differ from other NIST-provided mappings for the Privacy Framework and SP 800-53
 1420 revision. For example, build functions may provide additional capabilities beyond what is contemplated by a Privacy Framework Subcategory or
 1421 that are implemented by additional controls beyond those that NIST identified as an informative reference for the Subcategory.

1422 Table F-1’s example privacy control map identifies the privacy characteristic mapping for the products as they were used in the example
 1423 solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended that the
 1424 mapping not be used as a reference for all the privacy capabilities these products may be able to address. The comprehensive mapping of the
 1425 NIST Privacy Framework to NIST SP 800-53, Revision 5 controls can be found on the NIST Privacy Framework Resource Repository website, in the
 1426 event an organization’s mobile device security solution is different to determine other controls that are appropriate for their environment [64].

1427 **Table F-1 Example Solution’s Privacy Standards and Best Practices Mapping**

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
IBM MaaS360	MaaS360 can be used to capture an inventory of the types and number of devices deployed and shows the administrators what data is collected from each enrolled device.	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	CM-12: Information Location CM-13: Data Action Mapping	OV-LGA-002: Privacy Officer/Privacy Compliance Manager OV-TEA-001: Cyber Instructional Curriculum Developer

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			<p>PM-5(1): System Inventory Inventory of Personally Identifiable Information</p> <p>PT-3: Personally Identifiable Information Processing Purposes</p> <p>RA-3: Risk Assessment</p> <p>RA-8: Privacy Impact Assessment</p>	
	<p>Administrators can view data elements in the administration portal. Users can see collected data within the MaaS360 application on their device. Data can be edited and deleted from within the administration console.</p>	<p>CT.DM-P1: Data elements can be accessed for review.</p>	<p>AC-2: Account Management</p> <p>AC-3: Access Enforcement</p> <p>AC-3(14): Access Enforcement Individual Access</p> <p>PM-21: Accounting of Disclosures</p>	<p>OM-DTA-002: Data Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<p>CT.DM-P3: Data elements can be accessed for alteration.</p>	<p>AC-2: Account Management</p> <p>AC-3: Access Enforcement</p> <p>AC-3(14): Access Enforcement Individual Access</p> <p>PM-21: Accounting of Disclosures</p> <p>SI-18: Personally Identifiable Information Quality Operations</p>	<p>OM-DTA-002: Data Analyst</p>
		<p>CT.DM-P4: Data elements can be accessed for deletion.</p>	<p>AC-2: Account Management</p> <p>AC-3: Access Enforcement</p> <p>SI-18: Personally Identifiable Information Quality Operations</p>	<p>OM-DTA-002: Data Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<p>CT.DM-P5: Data are destroyed according to policy.</p>	<p>MP-6: Media Sanitization</p> <p>SA-8(33): Security and Privacy Engineering Principles Minimization</p> <p>SI-18: Personally Identifiable Information Quality Operations</p> <p>SR-12: Component Disposal</p>	<p>OM-DTA-002: Data Analyst</p>
		<p>CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.</p>	<p>CM-6: Configuration Settings</p> <p>SA-8(33): Minimization</p> <p>SC-42(5): Collection Minimization</p> <p>SI-12(1): Information Management and Retention Limit Personally Identifiable Information Elements</p>	<p>OV-LGA-002: Privacy Officer/Privacy Compliance Manager</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	Devices may be backed up to the cloud.	PR.PO-P3: Backups of information are conducted, maintained, and tested.	CP-4: Contingency Plan Testing CP-6: Alternate Storage Site CP-9: System Backup	OM-ADM-001: System Administrator
	Devices are issued identity certificates via on-premises certificate infrastructure.	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	IA-2: Identification and Authentication (Organizational Users) IA-3: Device Identification and Authentication IA-4: Identifier Management IA-4(4): Identifier Management Identifier User Status	SP-ARC-002: Security Architect PR-CDA-001: Cyber Defense Analyst
	MaaS360 enforces a device personal identification number for access.	PR.AC-P2: Physical access to data and devices is managed.	PE-2: Physical Access Authorizations PE-3: Physical Access Control PE-3(1): System Access	OM-DTA-001: Database Administrator OM-DTA-002: Data Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			<p>PE-4: Access Control for Transmission</p> <p>PE-5: Access Control for Output Devices</p> <p>PE-6: Monitoring Physical Access</p> <p>PE-18: Location of System Components</p> <p>PE-20: Asset Monitoring and Tracking</p>	
		<p>PR.DS-P1: Data-at-rest are protected.</p>	<p>MP-2: Media Access</p> <p>MP-4: Media Storage</p> <p>PM-5(1): System Inventory Inventory of Personally Identifiable Information</p> <p>SC-28: Protection of Information at Rest</p>	<p>OM-DTA-001: Database Administrator</p> <p>OM-DTA-002: Data Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	Data flowing between the device and MaaS360 is encrypted with Transport Layer Security.	PR.DS-P2: Data-in-transit are protected.	PM-5(1): System Inventory Inventory of Personally Identifiable Information SC-8: Transmission Confidentiality and Integrity	PR-CIR-001: Cyber Defense Incident Responder
	Restrictions are used that prevent data flow between enterprise and personal applications.	PR.DS-P5: Protections against data leaks are implemented.	PM-5(1): System Inventory Inventory of Personally Identifiable Information AC-4: Information Flow Enforcement	PR-CIR-001: Cyber Defense Incident Responder
	Devices that are jailbroken or otherwise modified beyond original equipment manufacturer status can be detected.	PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	PM-22: Personally Identifiable Information Quality Management SI-7: Software, Firmware, and Information Integrity SI-18: Personally Identifiable Information Quality Operations	OM-DTA-002: Data Analyst OM-ANA-001: Systems Security Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
<p>Zimperium</p>	<p>Zimperium checks the device for unauthorized modifications.</p>	<p>PR.DS-P1: Data-at-rest are protected.</p>	<p>PM-5(1): System Inventory Inventory of Personally Identifiable Information</p> <p>SC-28: Protection of Information at Rest</p>	<p>SP-ARC-002: Security Architect</p> <p>PR-CDA-001: Cyber Defense Analyst</p>
		<p>PR.DS-P2: Data-in-transit are protected.</p>	<p>PM-5(1): System Inventory Inventory of Personally Identifiable Information</p> <p>SC-8: Transmission Confidentiality and Integrity</p> <p>SC-11: Trusted Path</p>	<p>OM-DTA-002: Data Analyst</p> <p>OM-ANA-001: Systems Security Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<p>PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p>PM-22: Personally Identifiable Information Quality Management</p> <p>SC-16: Transmission of Security Attributes</p> <p>SI-7: Boundary Protection</p> <p>SI-10: Network Disconnect</p> <p>SI-18: Personally Identifiable Information Quality Operations</p>	<p>OM-DTA-002: Data Analyst</p> <p>OM-ANA-001: Systems Security Analyst</p>
<p>Kryptowire (now known as Quokka)</p>	<p>Kryptowire can identify applications that do not use best practices, such as lack of encryption or hardcoded credentials.</p>	<p>CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests</p>	<p>AC-8: System Use Notification</p>	<p>SP-ARC-002: Security Architect</p> <p>PR-CDA-001: Cyber Defense Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		are established and in place.		
		CM.AW-P3: System/product/ service design enables data processing visibility.	PL-8: Security and Privacy Architecture PM-5(1): System Inventory Inventory of Personally Identifiable Information	SP-ARC-002: Security Architect PR-CDA-001: Cyber Defense Analyst
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/ disclosure.	AC-16: Security and Privacy Attributes SC-16: Transmission of Security Attributes	SP-ARC-002: Security Architect PR-CDA-001: Cyber Defense Analyst
		PR.DS-P1: Data-at-rest are protected.	PM-5(1): System Inventory Inventory of Personally Identifiable Information SC-28: Protection of Information at Rest	SP-ARC-002: Security Architect PR-CDA-001: Cyber Defense Analyst
		PR.DS-P2: Data-in-transit are protected.	PM-5(1): System Inventory Inventory of Personally Identifiable Information	SP-ARC-002: Security Architect PR-CDA-001: Cyber Defense Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			<p>SC-8: Transmission Confidentiality and Integrity</p> <p>SC-11: Trusted Path</p>	
<p>Palo Alto Networks PA-220</p>	<p>Provides firewall and virtual private network capabilities.</p>	<p>PR.DS-P2: Data-in-transit are protected.</p>	<p>PM-5(1): System Inventory Inventory of Personally Identifiable Information</p> <p>SC-8: Transmission Confidentiality and Integrity</p> <p>SC-11: Trusted Path</p>	<p>SP-ARC-002: Security Architect</p> <p>PR-CDA-001: Cyber Defense Analyst</p>
		<p>PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</p>	<p>AC-2: Account Management</p> <p>AC-3: Access Enforcement</p> <p>AC-5: Separation of Duties</p> <p>AC-6: Least Privilege</p> <p>AC-24: Access Control Decisions</p>	<p>SP-ARC-002: Security Architect</p> <p>PR-CDA-001: Cyber Defense Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<p>PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).</p>	<p>AC-4: Information Flow Enforcement</p> <p>AC-10: Access Control</p> <p>SC-7: Boundary Protection</p> <p>SC-10: Network Disconnect</p>	<p>OM-DTA-002: Data Analyst</p> <p>OM-ANA-001: Systems Security Analyst</p>
		<p>PR.PT-P3: Communications and control networks are protected.</p>	<p>AC-12: Session Termination</p> <p>AC-17: Remote Access</p> <p>AC-18: Wireless Access</p> <p>SC-5: Denial of Service Protection</p> <p>SC-7: Boundary Protection</p> <p>SC-10: Network Disconnect</p> <p>SC-11: Trusted Path</p>	<p>OV-LGA-002: Privacy Officer/Privacy Compliance Manager</p> <p>PR-CDA-001: Cyber Defense Analyst</p>

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			<p>SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)</p> <p>SC-23: Session Authenticity</p>	
<p>Qualcomm</p>	<p>The trusted execution environment provides data confidentiality and integrity.</p>	<p>PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p>PM-22: Personally Identifiable Information Quality Management</p> <p>SC-16: Transmission of Security and Privacy Attributes</p> <p>SI-7: Software, Firmware, and Information Integrity</p> <p>SI-10: Information Input Validation</p> <p>SI-18: Personally Identifiable Information Quality Operations</p>	<p>PR-INF-001: Cyber Defense Infrastructure Support Specialist</p> <p>OM-ANA-001: Systems Security Analyst</p>

Mobile Device Security: Bring Your Own Device (BYOD)

Supplement:

Example Scenario: Putting Guidance into Practice

Kaitlin Boeckl

Nakia Grayson

Gema Howell

Naomi Lefkowitz

Applied Cybersecurity Division

Information Technology Laboratory

Jason Ajmo

Milissa McGinnis*

Kenneth F. Sandlin

Oksana Slivina

Julie Snyder

Paul Ward

The MITRE Corporation

McLean, VA

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

November 2022

SECOND DRAFT

This publication is available free of charge from

<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



1 **1 Applying This Build: Example Scenario**

2 An example scenario about a fictional company named Great Seneca Accounting illustrates how
3 organizations can use this practice guide's example solution. The example shows how Bring Your Own
4 Device (BYOD) objectives can align with a fictional organization's security and privacy priorities using risk
5 management standards, guidance, and tools.

6 To demonstrate how an organization may use this National Institute of Standards and Technology (NIST)
7 Special Publication (SP) and other NIST tools to implement a BYOD use case, the National Cybersecurity
8 Center of Excellence created an example scenario that centers around a fictional, small-to-mid-size
9 organization called Great Seneca Accounting. This scenario exemplifies the issues that an organization
10 may face when addressing common enterprise BYOD security challenges.

11 **1.1 Standards and Guidance Used in this Example Scenario**

12 In addition to the Executive Summary contained in Volume A, and the architecture description in
13 Volume B, this practice guide also includes a series of how-to instructions in Volume C. The how-to
14 instructions in Volume C provide step-by-step instructions covering the initial setup (installation or
15 provisioning) and configuration for each component of the architecture. These step-by-step instructions
16 can help security engineers rapidly deploy and evaluate the example solution in their test environment.

17 The example solution uses standards-based, commercially available products that can be used by an
18 organization interested in deploying a BYOD solution. The example solution provides recommendations
19 for enhancing the security and privacy infrastructure by integrating on-premises and cloud-hosted
20 mobile security technologies. This practice guide provides an example solution that an organization may
21 use in whole or in part as the basis for creating a custom solution that best supports their unique needs.

22 The fictional Great Seneca Accounting organization illustrates how this guide may be applied by an
23 organization, starting with a mobile device infrastructure that lacked mobile device security architecture
24 concepts. Great Seneca employed multiple NIST cybersecurity and privacy risk management tools to
25 understand the gaps in its architecture and methods to enhance security of its systems and privacy for
26 its employees.

27 This example scenario provides useful context for using the following NIST Frameworks and other
28 relevant tools to help mitigate some of the security and privacy challenges that organizations may
29 encounter when deploying BYOD capabilities:

- 30 • NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity
31 Framework) [\[1\]](#)
- 32 • the NIST *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*,
33 Version 1.0 (Privacy Framework) [\[2\]](#)
- 34 • NIST Special Publication (SP) 800-181 *National Initiative for Cybersecurity Education (NICE)*
35 *Cybersecurity Workforce Framework* [\[3\]](#)
- 36 • NIST Risk Management Framework [\[4\]](#)

- NIST Mobile Threat Catalogue [\[5\]](#)

For additional information, see Volume B’s Appendix D.

2 About Great Seneca Accounting

In the example scenario, Great Seneca Accounting is a fictional accounting firm that grew from a single office location into a larger firm with a regional presence. Great Seneca Accounting performs accounting functions related to capturing, communicating, processing, transmitting, and analyzing financial data and accounting services for its customers.

When the firm was first created, most of its employees worked from the Great Seneca Accounting office, with minimal use of mobile devices. They were able to do this without actively embracing mobile device usage because most of the employees worked at their desks at the company’s single location.

Over the years, the Great Seneca Accounting company grew from a local company, where all of its employees performed work at their desks by using desktop computers provided by the organization, into a regional firm with employees who work remotely and who support regional customers.

Now, many of the employees spend part of their week traveling and working from customer or other remote locations. This has prompted the organization to specify, as a strategic priority, the need to support employees to work remotely, while both traveling and working from a customer location. As such, the company wants to embrace BYOD solutions to support its remote work.

[Figure 2-1](#) shows an overview of the typical work environments for a Great Seneca Accounting employee. Many employees work remotely while using their own mobile phones and tablets to perform both work and personal activities throughout the day.

Figure 2-1 Great Seneca Accounting’s Work Environments



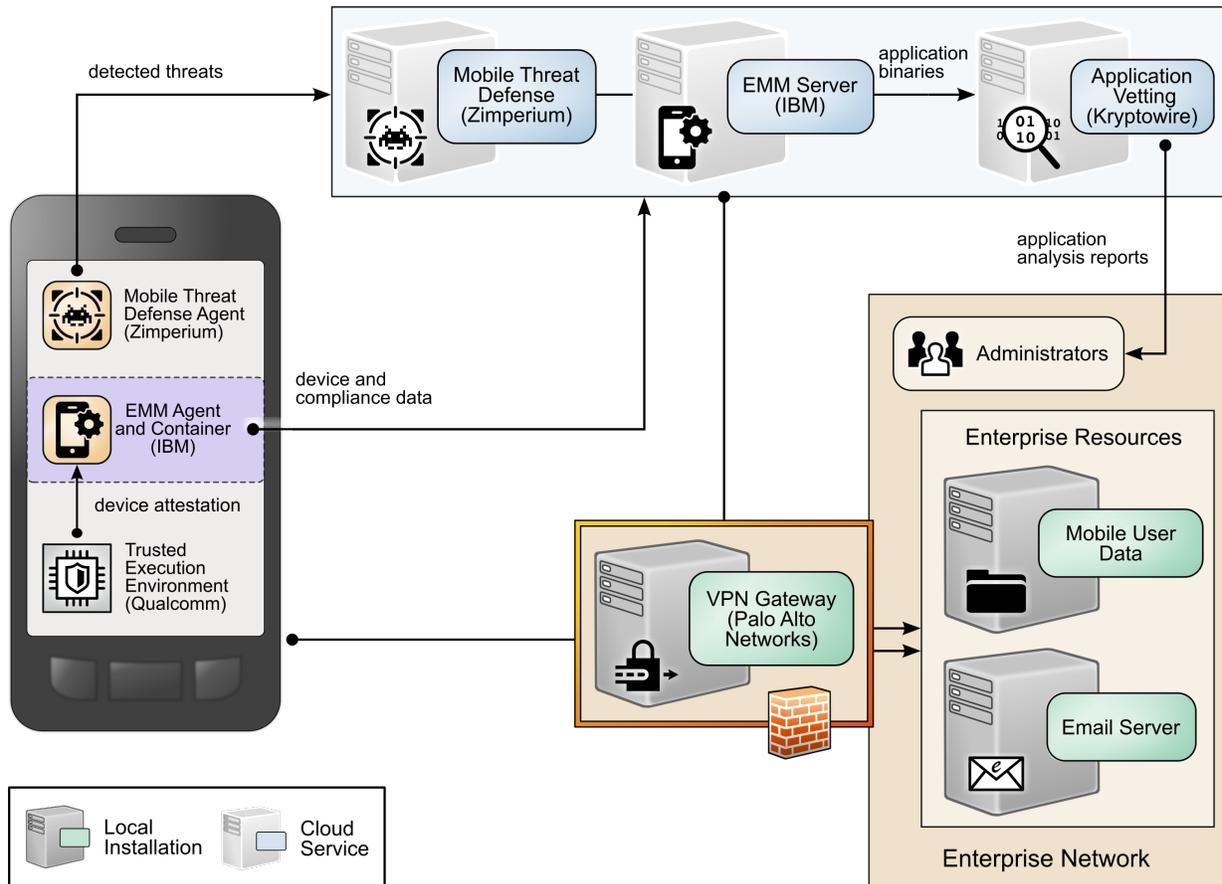
58 Great Seneca Accounting’s corporate management initiated a complete review of all policies,
59 procedures, and technology relating to its mobile deployment to ensure that the company is well
60 protected against attacks involving personal mobile devices. This includes mitigating risks against its
61 devices, custom applications, and corporate infrastructure supporting mobile services. Management
62 identified NIST’s Risk Management Framework (RMF) [\[4\]](#) and Privacy Risk Assessment Methodology
63 (PRAM) [\[6\]](#) as useful tools for supporting this analysis. The company developed Cybersecurity
64 Framework and Privacy Framework Target Profiles to guide Great Seneca Accounting’s decision-making
65 because the Target Profiles link Great Seneca Accounting’s mission and business priorities with
66 supporting cybersecurity and privacy activities.

67 Great Seneca Accounting identified the scope of their mobile solution to be both Android and Apple
68 personally owned mobile phones and tablets. While this example scenario intends to provide an
69 exemplar of organization guidance with a description of BYOD concepts and how to apply those
70 concepts, this example scenario should not suggest a limit on BYOD uses.

71 Great Seneca Accounting plans to use NIST SP 1800-22 (this practice guide) to inform its updated BYOD
72 architecture as well as NIST’s Mobile Threat Catalogue to identify threats to mobile deployment. These
73 NIST frameworks and tools used are described further in [Appendix E](#).

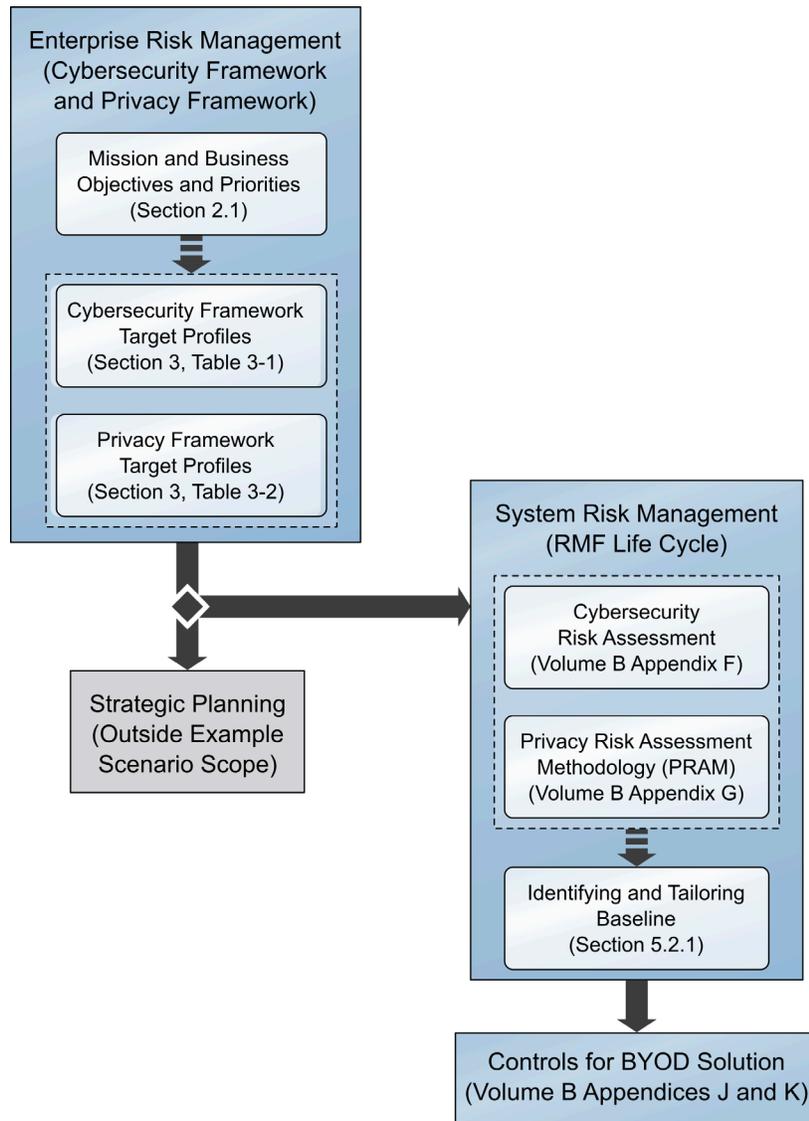
74 As shown in [Figure 2-2](#), this example solution applied multiple mobile device security technologies.
75 These included a cloud-based Enterprise Mobility Management solution integrated with cloud- and
76 agent-based mobile security technologies to help deploy a set of security and privacy capabilities that
77 support the example solution.

78 **Figure 2-2 Example Solution Architecture**



79 [Figure 2-3](#) shows the overall process that Great Seneca Accounting plans to follow. It highlights key
 80 activities from various NIST guidance documents related to security and privacy risk management, each
 81 of which is discussed in the sections identified in [Figure 2-3](#). Please note that this process is an
 82 abbreviated version of steps provided in NIST SP 800-37 Revision 2 [7], which shows how some available
 83 resources may be used by any organization.

84 **Figure 2-3 Great Seneca Accounting’s Security and Privacy Risk Management Steps**



85 **2.1 Great Seneca Accounting’s Business/Mission Objectives**

86 Great Seneca Accounting developed a mission statement and a set of supporting business/mission
 87 objectives to ensure that its activities align with its core purpose. The company has had the same
 88 mission since it was founded:

89 ***Mission Statement***

90 *Provide financial services with integrity and responsiveness*

91 While Great Seneca Accounting has a number of business/mission objectives, those below relate to its
92 interest in BYOD, listed in priority order:

- 93 1. Provide good data stewardship
- 94 2. Enable timely communication with clients
- 95 3. Provide innovative financial services
- 96 4. Enable workforce flexibility

97 3 Great Seneca Accounting's Target Profiles

98 Great Seneca Accounting used the NIST Cybersecurity Framework and NIST Privacy Framework as key
99 strategic planning tools to improve its security and privacy programs. It followed the processes outlined
100 in the frameworks, and as part of that effort, created two Target Profiles—one for cybersecurity and one
101 for privacy.

102 These Target Profiles describe the desired or aspirational state of Great Seneca Accounting by
103 identifying and prioritizing the cybersecurity and privacy activities and outcomes needed to support its
104 enterprise business/mission objectives. The Subcategories in each Framework Core articulate those
105 cybersecurity and privacy activities and outcomes.

106 **Note:** See [Appendix E](#) for a high-level description of the Cybersecurity Framework and Privacy
107 Framework.

108 To understand what Subcategories to prioritize implementing in each framework, Great Seneca
109 Accounting considered the importance of the Subcategories for accomplishing each business/mission
110 objective. The Target Profiles reflect that discussion by designating prioritized Subcategories as low,
111 moderate, or high.

112 Subcategory improvements important for BYOD deployment also became part of its Target Profiles
113 because Great Seneca Accounting was upgrading its existing information technology infrastructure as
114 part of its BYOD implementation.

115 The Cybersecurity Framework Target Profile in [Table 3-1](#) and the Privacy Framework Target Profile in
116 [Table 3-2](#) are included as examples of Great Seneca Accounting's identification of the business/mission
117 objectives that are relevant to their BYOD deployment.

118 Great Seneca Accounting chose to address the Subcategories that are prioritized as moderate and high
119 for multiple business/mission objectives in its Target Profiles for this year's BYOD deployment with plans
120 to address the low Subcategories in the future.

121 [Table 3-1](#) and [Table 3-2](#) include only those Subcategories that are prioritized as moderate or high for the
122 business/mission objectives. Any subcategory designated as low is included in [Table 3-1](#) and [Table 3-2](#)
123 only because it is high or moderate for another business/mission objective.

124 Great Seneca Accounting used the Target Profiles to help guide risk management decisions throughout
125 the organization's activities, including making decisions regarding budget allocation, technology design,

126 and staffing for its programs and technology deployments. Discussions for developing and using the
127 Target Profiles include stakeholders in various parts of the organization, such as business/mission
128 program owners, data stewards, cybersecurity practitioners, privacy practitioners, legal and compliance
129 experts, and technology experts.

130 **Note:** Low, moderate, and high designations indicate the level of relative importance among
131 Subcategories for Great Seneca to accomplish a business/mission objective.

132 Table 3-1 Great Seneca Accounting’s Cybersecurity Framework Target Profile

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
IDENTIFY	Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried.	moderate	moderate	moderate	low
		ID.AM-2: Software platforms and applications within the organization are inventoried.	moderate	moderate	moderate	low
	Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented.	moderate	moderate	moderate	moderate
		ID.RA-3: Threats, both internal and external, are identified and documented.	moderate	moderate	moderate	moderate
PROTECT	Identity Management and Access Control	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	moderate	high	moderate	high
		PR.AC-3: Remote access is managed.	moderate	high	high	high

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	moderate	high	high	high
	Data Security	PR.DS-1: Data-at-rest is protected.	high	moderate	moderate	high
		PR.DS-2: Data-in-transit is protected.	moderate	high	moderate	high
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	moderate	moderate	moderate	low
	Information Protection Processes and Procedures	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.	moderate	moderate	moderate	low

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
	Protective Technology	PR.PT-4: Communications and control networks are protected.	low	moderate	moderate	low
DETECT	Anomalies and Events	DE.AE-5: Incident alert thresholds are established.	high	high	high	high
	Security Continuous Monitoring	DE.CM-4: Malicious code is detected.	high	high	high	high
		DE.CM-5: Unauthorized mobile code is detected.	moderate	moderate	moderate	low
		DE.CM-8: Vulnerability scans are performed.	high	high	high	high

133 Table 3-2 Great Seneca Accounting’s Privacy Target Profile

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
IDENTIFY-P	Inventory and Mapping	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	high	high	high	high
GOVERN-P	Governance Policies, Processes, and Procedures	GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing, individuals’ prerogatives with respect to data processing) are established and communicated.	high	high	high	high
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	high	high	high	high
	Monitoring and Review	GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	high	high	high	high

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).	high	high	high	high
CONTROL-P	Data Management	CT.DM-P1: Data elements can be accessed for review.	high	moderate	high	moderate
		CT.DM-P3: Data elements can be accessed for alteration.	high	moderate	high	moderate
		CT.DM-P4: Data elements can be accessed for deletion.	high	moderate	high	moderate
		CT.DM-P5: Data are destroyed according to policy.	high	moderate	high	moderate

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
	Disassociated Processing	CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	high	high	high	high
COMMUNICATE-P	Data Processing Awareness	CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	high	moderate	moderate	moderate
PROTECT-P	Data Protection Policies, Processes, and Procedures	PR.PO-P3: Backups of information are conducted, maintained, and tested.	high	moderate	high	moderate
		PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	moderate	high	moderate	high
	Identity Management,	PR.AC-P2: Physical access to data and devices is managed.	high	moderate	high	moderate

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
	Authentication, and Access Control	PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	high	moderate	high	moderate
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high
		PR.DS-P1: Data-at-rest are protected.	high	moderate	moderate	high
	Data Security	PR.DS-P2: Data-in-transit are protected.	moderate	high	moderate	high
		PR.DS-P5: Protections against data leaks are implemented.	high	moderate	high	moderate
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		PR.PT-P3: Communications and control networks are protected.	moderate	high	moderate	high

135 **4 Great Seneca Accounting Embraces BYOD**

136 Great Seneca Accounting now allows its staff to use their personal mobile devices to perform their daily
137 work duties on an as-needed basis. Accountants use the devices for various tasks including
138 communicating with client organizations and other employees, collecting confidential client information,
139 analyzing financial transactions, generating reports, accessing tax and payroll information, and creating
140 and reviewing comprehensive financial statements.

141 Great Seneca accountants work from many locations including their corporate office building, their
142 homes, their customers' offices, and other locations. In order to be able to work in all these locations,
143 they require the use of mobile devices to perform their job functions.

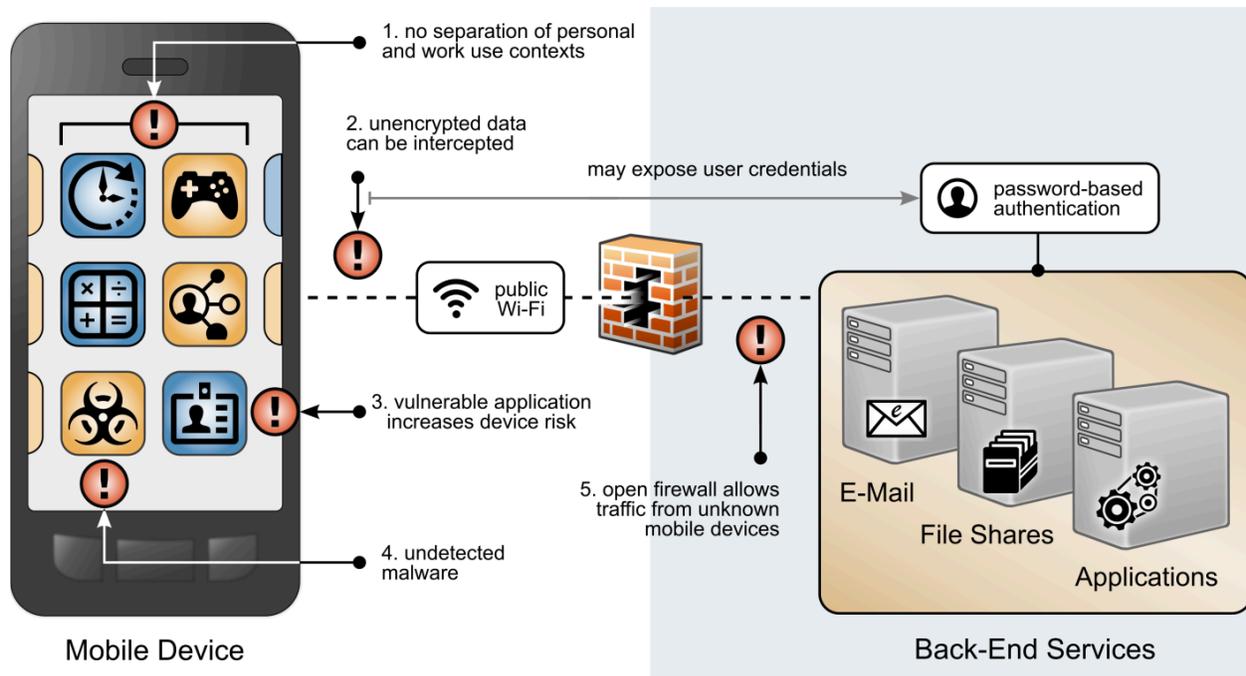
144 Great Seneca Accounting's current mobile infrastructure enables accountants to perform their job
145 duties by using their personally owned devices, despite minimal security installed and enforced on these
146 devices. Examples of security concerns with the use of personally owned devices are:

- 147 ▪ Employees can connect to any Wi-Fi network to perform work-related activities when they are
148 working on the road, including at a client's site.
- 149 ▪ Custom mobile applications being sideloaded onto devices that employees use.
- 150 ▪ The personally owned devices allow users to install applications on an as-needed basis without
151 separation of enterprise and personal data.

152 While not affecting Great Seneca Accounting, a string of well-publicized cybersecurity attacks was
153 recently reported in the news, and this prompted Great Seneca to review its mobile device security and
154 privacy deployment strategy. When making BYOD deployment decisions, Great Seneca Accounting plans
155 to prioritize implementing cybersecurity and privacy capabilities that would enable it to accomplish its
156 business/mission objectives (i.e., its reasons for deploying BYOD capabilities).

157 To do this, Great Seneca Accounting conducted a technical assessment of its current BYOD architecture
158 to help it understand ways to improve the confidentiality, integrity, availability, and privacy of data and
159 devices associated with its BYOD deployment. The company identified several vulnerabilities based on
160 its current mobile device deployment. [Figure 4-1](#) below presents a subset of those vulnerabilities.

161 **Figure 4-1 Great Seneca Accounting’s Current Mobile Deployment Architecture (Before Security and**
 162 **Privacy Enhancements)**



163 Figure 4-1 highlights the following vulnerabilities with a red exclamation mark:

- 164 1. BYOD deployments can place organizational and personal data, as well as employees’ privacy, at
 165 risk. Organizational and personal data can become commingled if either the same application is
 166 used in both contexts or if multiple applications access shared device resources (e.g., contacts or
 167 calendar) as applications for both personal and work usage are installed. This also puts
 168 employees’ privacy at risk, as the organization can have visibility into their personal life outside
 169 work.
- 170 2. BYOD deployments can leverage nonsecure networks. As employees use nonsecure Wi-Fi
 171 hotspots, mobile devices that are connecting to Great Seneca Accounting from those
 172 unencrypted networks place data transmitted prior to a secure connection at risk of discovery
 173 and eavesdropping, including passwords.
- 174 3. As employees install applications on their personally owned devices, the applications can have
 175 unidentified vulnerabilities or weaknesses that increase the risk of device compromise (e.g.,
 176 applications that access contacts may now have access to the organization’s client contact
 177 information). Further, legitimate, privacy-intrusive applications can legally collect data through
 178 terms and conditions and requested permissions.
- 179 4. On personally owned devices without restriction policies in place, employees may inadvertently
 180 download applications outside official application stores, which are malware in disguise.

181 5. Because personally owned mobile devices can connect from unknown locations, firewall rules
182 must allow inbound connections from unrecognized, potentially malicious Internet Protocol
183 addresses.

184 In addition to identifying the technical assets and the vulnerabilities, Great Seneca Accounting identified
185 the scope of the mobile solution (i.e., both Android and Apple personally owned mobile phones and
186 tablets) and the regulatory requirements or guidance that will apply to their deployment and solution
187 (e.g., encryption will be Federal Information Processing Standards [FIPS]-validated to protect sensitive
188 accounting information).

189 **5 Applying NIST Risk Management Methodologies to Great** 190 **Seneca Accounting's BYOD Architecture**

191 Sections 2 and 3 described Great Seneca Accounting, their business mission, and what security and
192 privacy areas they consider most important. Great Seneca created Target Profiles that mapped their
193 BYOD-related mission/business objectives and priorities with the Functions, Categories, and
194 Subcategories of both the Cybersecurity Framework and the Privacy Framework. Those Cybersecurity
195 Framework and Privacy Framework Target Profiles are provided in [Table 3-1](#) and [Table 3-2](#) in Section 3
196 of this document.

197 Now, the Target Profiles provided in Section 3 will demonstrate the role they play in identifying and
198 prioritizing the implementation of the security and privacy controls, as well as the capabilities that Great
199 Seneca would like to include in its new BYOD security and privacy-enhanced architecture.

200 **5.1 Using Great Seneca Accounting's Target Profiles**

201 The Cybersecurity Framework maps its Subcategories to Informative References. The Informative
202 References contained in the Framework Core provide examples of methods that Great Seneca can use
203 to achieve its desired outcomes. The Cybersecurity Framework's Subcategory and Informative
204 References mappings include NIST SP 800-53 controls.

205 An illustrative segment of the Cybersecurity Framework's Framework Core is shown in [Figure 5-1](#).
206 Highlighted in the green box is an example of how the Cybersecurity Framework provides a mapping of
207 Subcategories to Informative References.

208 **Figure 5-1 Cybersecurity Framework Subcategory to Informative Reference Mapping**

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9

209 To provide a starting point for Great Seneca’s mapping of their Cybersecurity Framework and Privacy
 210 Framework Target Profiles to the NIST SP 800-53 security and privacy controls and capabilities, Great
 211 Seneca leveraged the mapping provided in the Cybersecurity Framework. An example of the
 212 Cybersecurity Framework’s mapping is provided in [Figure 5-1](#).

213 See Volume B’s Appendices E and F for additional information on the security and privacy outcomes that
 214 this document’s example solution supports. Appendices E and F provide a mapping of this document’s
 215 example solution capabilities with the related Subcategories in the Cybersecurity Framework and
 216 Privacy Framework.

217 Volume B’s Appendix E provides the Cybersecurity Framework Subcategory mappings, and Volume B’s
 218 Appendix F provides the Privacy Framework Subcategory mappings. An excerpt of Volume B’s Appendix
 219 G is shown below in [Figure 5-2](#).

220 **Figure 5-2 Volume B Appendix E Example Solution Cybersecurity Framework Mapping Excerpt**

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles
Mobile Threat Defense						
Kryptowire Cloud Service	Application Vetting	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8: Security Assessment and Authorization RA-3, RA-5: Risk Assessment SA-4: Acquisition Process SI-7: Software, Firmware, and Information Integrity	A.12.6.1: Control of technical vulnerabilities A.18.2.3: Technical Compliance Review	CSC 4: Continuous Vulnerability Assessment and Remediation	SP-RSK-002: Security Control Assessor SP-ARC-002: Security Architect OM-ANA-001: Systems Security Analyst

221 **5.2 Great Seneca Uses the Target Profiles to Help Prioritize Security and**
 222 **Privacy Control Deployment**

223 Due to budget constraints, Great Seneca Accounting will focus on implementing the higher priority
 224 security and privacy controls that were identified in the organization’s two Target Profiles first. The
 225 company will then focus on implementing lower priority controls when more funding becomes available.
 226 This is accomplished by Great Seneca Accounting comparing the prioritized Subcategories contained in
 227 Section 3’s [Table 3-1](#) and [Table 3-2](#) with the outcomes that the example solution supports.

228 By comparing its Cybersecurity Framework Target Profile ([Table 3-1](#)) with the Subcategories supported
 229 by the example solution that are shown in Volume B’s Appendix F, Great Seneca Accounting determines
 230 that the example solution will help it achieve its desired Cybersecurity Framework Target Profile
 231 outcomes.

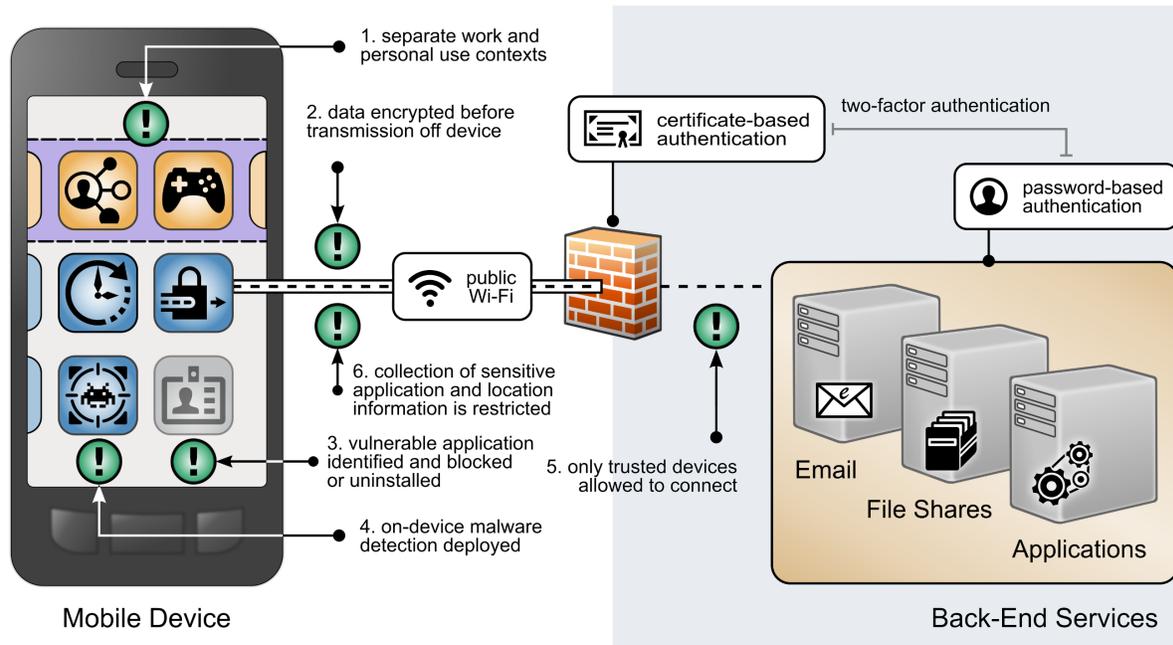
232 Great Seneca performs a similar comparison of the Privacy Framework Target Profile in [Table 3-2](#) with
 233 the Subcategories supported by the example solution that are shown in Volume B’s Appendix H. From
 234 that comparison of the example solution’s capabilities and Great Seneca’s privacy-related architecture
 235 goals, Great Seneca determines that the example solution provided in this practice guide will help it to
 236 achieve the privacy-related outcomes that were identified in [Table 3-2](#)’s Privacy Framework Target
 237 Profile.

238 **5.2.1 Identifying and Tailoring the Baseline Controls**

239 Now that Great Seneca Accounting understands how the Target Profiles will help prioritize the
 240 implementation of the high-level security and privacy goals shown in [Figure 5-3](#), they would like to look

241 more closely at the NIST SP 800-53 controls it will initially implement in its new BYOD architecture. This
 242 will help Great Seneca identify the capabilities it will deploy first to meet its architecture needs.

243 **Figure 5-3 Security and Privacy Goals**



244 Volume B’s Appendices E and F provide a list of the controls that the example solution implements,
 245 including how the controls in the example solution align to the Subcategories in both the Cybersecurity
 246 Framework and Privacy Framework. Because these controls only focus on the example solution, Great
 247 Seneca will need to implement additional controls that address the unique risks associated with its
 248 environment.

249 To help identify the specific controls Great Seneca Accounting will be implementing to support the new
 250 BYOD architecture, it uses the NIST RMF process to manage security and privacy risk for its systems. The
 251 organization decides to follow the RMF guidance in NIST SP 800-37 [7] to conduct security and privacy
 252 risk assessments as it continues preparing to design its new solution.

253 5.3 Great Seneca Accounting Performs a Risk Assessment

254 Great Seneca Accounting completes a security risk assessment by using the guidance in NIST SP 800-30
255 [\[8\]](#) and the Mobile Threat Catalogue [\[5\]](#) to identify cybersecurity threats to the organization. The
256 company then uses the NIST PRAM [\[6\]](#) to perform a privacy risk assessment. Appendices F and G in this
257 document describe these risk assessments in more detail. These risk assessments produce two
258 significant conclusions:

- 259 1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic
260 data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the
261 controls discussed in the example solution are relevant to their environment.
- 262 2. The organization determines that it has a high-impact system, based on the impact guidance in
263 NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
264 [\[9\]](#), and needs to implement more controls beyond those identified in NIST SP 1800-22 and its
265 Target Profiles to support the additional system components in its own solution (e.g., underlying
266 OS, the data center where the equipment will reside).

267 5.4 Great Seneca Accounting Tailors Their Security and Privacy Control 268 Baselines

269 As part of their review of NIST FIPS 200 [\[9\]](#), Great Seneca Accounting selects the high controls baseline in
270 NIST SP 800-53 [\[10\]](#) for their BYOD architecture implementation. They then tailor the control baselines
271 based on the needs identified through the priority Subcategories in its cybersecurity and privacy Target
272 Profiles.

273 Control baselines are tailored to meet their organization’s needs. NIST SP 800-53 [\[10\]](#) defines tailoring as
274 “The process by which security control baselines are modified by: (i) identifying and designating
275 common controls; (ii) applying scoping considerations on the applicability and implementation of
276 baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to
277 organization-defined security control parameters; (v) supplementing baselines with additional security
278 controls or control enhancements; and (vi) providing additional specification information for control
279 implementation.”

280 While not discussed in this example scenario, Great Seneca also plans to make tailoring decisions based
281 on other unique needs in its environment (e.g., legal, and regulatory requirements).

282 5.4.1 An Example Tailoring of the System and Communications Protection Security 283 Control Family

284 As Great Seneca Accounting reviews the System and Communications Protection (SC) control family in
285 NIST SP 800-53 [\[10\]](#), it notes there are opportunities for tailoring.

286 For example, the NIST SP 800-53 baseline includes control enhancements, whereas the Cybersecurity
287 Framework Informative References contain only base controls. Great Seneca Accounting decides to

288 implement the enhancements that are applicable to a high-impact system for the SC controls they have
 289 selected.

290 Using this decision as a guide, Great Seneca Accounting also makes the following tailoring decisions
 291 related to the NIST SP 800-53 SC control family:

- 292 ▪ NIST SP 800-53 provides recommendations regarding implementation priorities for controls. The
 293 implementation priorities of controls related to some Cybersecurity Framework Subcategories
 294 were adjusted to be higher or lower based on their alignment with Subcategory prioritization in
 295 the Target Profile.
- 296 ▪ For example, the implementation priority for Cybersecurity Framework Subcategory DE.CM-5
 297 was identified as having low or moderate importance for accomplishing all four BYOD-related
 298 Business/Mission Objectives. NIST SP 800-53 designates control SC-18, which supports the
 299 implementation of Cybersecurity Framework Subcategory DE.CM-5, as high priority. However,
 300 since Cybersecurity Framework Subcategory DE.CM-5 is moderate or low priority in this context,
 301 Great Seneca makes a tailoring decision to lower the implementation priority for the SC-18 NIST
 302 SP 800-53 control to moderate.
- 303 ○ DE.CM-5’s importance designations for accomplishing the BYOD-Related
 304 Business/Mission Objectives are highlighted in green in [Figure 5-4](#).

305 **Figure 5-4 Subcategory DE.CM-5 Mapping to BYOD-Related Business/Mission Objectives**

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable Workforce Flexibility	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
DETECT	Security Continuous Monitoring	DE.CM-5: Unauthorized mobile code is detected.	moderate	moderate	moderate	low

- 306 ▪ Conversely, just as the implementation priority for the NIST SP 800-53 control that supports
 307 implementation of Subcategory DC.CM-5 was lowered based on the Target Profile, the
 308 implementation priority for the NIST SP 800-53 controls that support implementation of
 309 Cybersecurity Framework Subcategory PR.AC-5 was raised. This is because Subcategory PR.AC-5
 310 was identified as having high importance for accomplishing all four BYOD-Related
 311 Business/Mission Objectives.
- 312 ○ The NIST SP 800-53 SC Family security control related to the Cybersecurity Framework
 313 Subcategory PR.AC-5 is SC-7. NIST SP 800-53 prioritizes control SC-7 as low. Since control
 314 SC-7 supports the implementation of a Cybersecurity Framework Subcategory that is
 315 designated as high priority in Great Seneca’s Target Profile (Cybersecurity Framework
 316 Subcategory PR.AC-5), Great Seneca makes a tailoring decision to increase the priority of
 317 NIST SP 800-53 control SC-7 to high.

- PR.AC-5’s high importance designation for accomplishing the BYOD-Related Business/Mission Objectives is highlighted in green in [Figure 5-5](#). All Subcategory prioritizations (including PR.AC-5’s shown below) can be found in [Table 3-1](#).

Figure 5-5 Subcategory PR.AC-5 Mapping to BYOD-Related Business/Mission Objectives

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable Workforce Flexibility	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
PROTECT	Identity Management and Access Control	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high

Great Seneca Accounting follows the same approach for the privacy controls in NIST SP 800-53, using the Privacy Framework Target Profile and controls identified through its PRAM analysis (for more information reference [Appendix G](#)).

Great Seneca Accounting will evaluate the security controls as they come up for review under its continuous monitoring program to determine whether there are enhancements to the implemented security controls that can be made over time.

In addition to identifying controls to select, the priorities articulated in Target Profiles will also help Great Seneca Accounting decide how to align financial resources for control implementations (e.g., buying a tool to automate a control as opposed to relying on policy and procedures alone). The Target Profiles will help Great Seneca identify how robustly to re-assess the efficacy of implemented controls before new system components or capabilities are enabled in a production environment. Great Seneca will also be able to use the Target Profiles to help evaluate the residual risks of the architecture in the context of Great Seneca Accounting’s business/mission objectives, and the frequency and depth of continued monitoring requirements over time.

Note: All the tailoring decisions discussed above are for example purposes only. An organization’s actual tailoring decision will be based upon their own unique business/mission objectives, risk assessment results, and organizational needs that may significantly vary from these examples.

339 **Appendix A List of Acronyms**

BYOD	Bring Your Own Device
FIPS	Federal Information Processing Standards
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
SP	Special Publication

340 **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 [11] .
Availability	Ensure that users can access resources through remote access whenever needed [12] .
Bring Your Own Device (BYOD)	A non-organization-controlled telework client device [12] .
Confidentiality	Ensure that remote access communications and stored user data cannot be read by unauthorized parties [12] .
Data Actions	System operations that process PII [13] .
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [13] .
Eavesdropping	An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant [14] (definition located under eavesdropping attack).
Firewall	Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [15] .
Integrity	Detect any intentional or unintentional changes to remote access communications that occur in transit [12] .
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [13] .
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for

synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [\[10\]](#).

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [\[16\]](#) (adapted from Government Accountability Office Report 08-536).

Problematic Data Action

A data action that could cause an adverse effect for individuals [\[2\]](#).

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [\[8\]](#).

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [\[8\]](#).

341 Appendix C References

- 342 [1] National Institute of Standards and Technology (NIST). *NIST Framework for Improving Critical*
343 *Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework). Apr. 16, 2018. [Online].
344 Available: <https://www.nist.gov/cyberframework>.
- 345 [2] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk*
346 *Management*, Version 1.0 (Privacy Framework). Jan. 16, 2020. [Online]. Available:
347 <https://www.nist.gov/privacy-framework>.
- 348 [3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity*
349 *Workforce Framework*, NIST Special Publication (SP) 800-181, NIST, Gaithersburg, Md., Aug.
350 2017. Available: <https://csrc.nist.gov/publications/detail/sp/800-181/final>.
- 351 [4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available:
352 [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview).
- 353 [5] NIST. Mobile Threat Catalogue. [Online]. Available: [https://pages.nist.gov/mobile-threat-](https://pages.nist.gov/mobile-threat-catalogue/)
354 [catalogue/](https://pages.nist.gov/mobile-threat-catalogue/).
- 355 [6] NIST. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available:
356 <https://www.nist.gov/privacy-framework/nist-pram>.
- 357 [7] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A*
358 *System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, NIST,
359 Gaithersburg, Md., Dec. 2018. Available: [https://csrc.nist.gov/publications/detail/sp/800-](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)
360 [37/rev-2/final](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final).
- 361 [8] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-
362 30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available:
363 <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>.
- 364 [9] NIST. *Minimum Security Requirements for Federal Information and Information Systems*, Federal
365 Information Processing Standards Publication (FIPS) 200, Mar. 2006. Available:
366 <https://csrc.nist.gov/publications/detail/fips/200/final>.
- 367 [10] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems*
368 *and Organizations*, NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available:
369 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.
- 370 [11] IDManagement.gov. "Federal Identity, Credential, and Access Management Architecture."
371 [Online]. Available: <https://arch.idmanagement.gov/services/access/>.

- 372 [12] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own*
373 *Device (BYOD) Security*, NIST SP 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available:
374 <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>.
- 375 [13] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal*
376 *Systems*, NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available:
377 <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.
- 378 [14] P. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017.
379 Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.
- 380 [15] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Revision 2,
381 NIST, Gaithersburg, Md., May 2015. Available:
382 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.
- 383 [16] E. McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information*
384 *(PII)*, NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available:
385 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.
- 386 [17] J. Franklin et al., *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*, NIST SP
387 1800-21, NIST, Gaithersburg, Md., July 22, 2019. Available:
388 <https://csrc.nist.gov/News/2019/NIST-Releases-Draft-SP-1800-21-for-Comment>.
- 389 [18] NIST, NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the*
390 *Cybersecurity Framework*, Mar. 2020. [Online]. Available:
391 <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf>.
- 392 [19] NIST. Risk Management Framework (RMF) Overview. [Online]. Available:
393 [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview).

394 **Appendix D A Note Regarding Great Seneca Accounting**

395 A description of a fictional organization, Great Seneca Accounting, was included in the National Institute
396 of Standards and Technology (NIST) Special Publication (SP) 1800-22 Mobile Device Security: Bring Your
397 Own Device (BYOD) Practice Guide.

398 This fictional organization demonstrates how a small-to-medium sized, regional organization imple-
399 mented the example solution in this practice guide to assess and protect their mobile-device-specific
400 security and privacy needs. It illustrates how organizations with office-based, remote-working, and trav-
401 elling personnel can be supported in their use of personally owned devices that enable their employees
402 to work while on the road, in the office, at customer locations, and at home.

403 **Figure D-1 Great Seneca Accounting’s Work Environments**



404 **Appendix E How Great Seneca Accounting Applied NIST Risk** 405 **Management Methodologies**

406 This practice guide contains an example scenario about a fictional organization called Great Seneca
407 Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be
408 in alignment with an organization’s security and privacy capabilities and objectives.

409 The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance,
410 and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this
411 practice guide.

412 This appendix provides a brief description of some of the key NIST tools referenced in the example
413 scenario supplement of this practice guide.

414 In this Appendix, Section E.1 provides descriptions of the risk frameworks and tools, along with a high-
415 level discussion of how Great Seneca Accounting applied each framework or tool in the example
416 scenario. Section E.2 describes how the *NIST Cybersecurity Framework* and *NIST Privacy Framework* can
417 be used to establish or improve cybersecurity and privacy programs.

418 **E.1 Overview of Risk Frameworks and Tools That Great Seneca Used**

419 Great Seneca used NIST frameworks and tools to identify common security and privacy risks related to
420 BYOD solutions and to guide approaches to how they were addressed in the architecture described in
421 [Section 4](#). Great Seneca used additional standards and guidance, listed in Appendix D of Volume B, to
422 complement these frameworks and tools when designing their BYOD architecture.

423 Both the Cybersecurity Framework and Privacy Framework include the concept of Framework Profiles,
424 which identify the organization’s existing activities (contained in a Current Profile) and articulate the
425 desired outcomes that support its mission and business objectives within its risk tolerance (that are
426 contained in the Target Profile). When considered together, Current and Target Profiles are useful tools
427 for identifying gaps and for strategic planning.

428 **E.1.1 Overview of the NIST Cybersecurity Framework**

429 **Description:** The NIST Cybersecurity Framework “is voluntary guidance, based on existing standards,
430 guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to
431 helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity
432 management communications amongst both internal and external organizational stakeholders.” [\[17\]](#)

433 **Application:** This guide refers to two of the main components of the Cybersecurity Framework: The
434 Framework Core and the Framework Profiles. As described in Section 2.1 of the Cybersecurity
435 Framework, the Framework Core provides a set of activities to achieve specific cybersecurity outcomes,

436 and reference examples of guidance to achieve those outcomes (e.g., controls found in NIST Special
437 Publication [SP] 800-53). Section 2.3 of the Cybersecurity Framework identifies Framework Profiles as
438 the alignment of the Functions, Categories, and Subcategories (i.e., the Framework Core) with the
439 business requirements, risk tolerance, and resources of the organization.

440 The Great Seneca Accounting example scenario assumed that the organization used the Cybersecurity
441 Framework Core and Framework Profiles, specifically the Target Profiles, to align cybersecurity
442 outcomes and activities with its overall business/mission objectives for the organization. In the case of
443 Great Seneca Accounting, its Cybersecurity Framework Target Profile helps program owners and system
444 architects understand business and mission-driven priorities and the types of cybersecurity capabilities
445 needed to achieve them. Great Seneca Accounting also used the NIST Interagency Report (NISTIR) 8170,
446 *The Cybersecurity Framework, Implementation Guidance for Federal Agencies* [18], for guidance in using
447 the NIST Cybersecurity Framework.

448 E.1.2 Overview of the NIST Privacy Framework

449 **Description:** The *NIST Privacy Framework* is a voluntary enterprise risk management tool intended to
450 help organizations identify and manage privacy risk and build beneficial systems, products, and services
451 while protecting individuals' privacy. It follows the structure of the Cybersecurity Framework to facilitate
452 using both frameworks together [2].

453 **Application:** This guide refers to two of the main components of the Privacy Framework: The Framework
454 Core and Framework Profiles. As described in Section 2.1 of the Privacy Framework, the Framework
455 Core provides an increasingly granular set of activities and outcomes that enable dialog about managing
456 privacy risk as well as resources to achieve those outcomes (e.g., guidance in NISTIR 8062, *An*
457 *Introduction to Privacy Engineering and Risk Management in Federal Systems* [13]). Section 2.2 of the
458 Privacy Framework identifies Framework Profiles as the selection of specific Functions, Categories, and
459 Subcategories from the core that an organization has prioritized to help it manage privacy risk.

460 Great Seneca Accounting used the Privacy Framework as a strategic planning tool for its privacy program
461 as well as its system, product, and service teams. The Great Seneca Accounting example scenario
462 assumed that the organization used the Privacy Framework Core and Framework Profiles, specifically
463 Target Profiles, to align privacy outcomes and activities with its overall business/mission objectives for
464 the organization. Its Privacy Framework Target Profile helped program owners and system architects to
465 understand business and mission-driven priorities and the types of privacy capabilities needed to
466 achieve them.

467 E.1.3 Overview of the NIST Risk Management Framework

468 **Description:** The NIST Risk Management Framework (RMF) “provides a process that integrates security
469 and risk management activities into the system development life cycle. The risk-based approach to
470 security control selection and specification considers effectiveness, efficiency, and constraints due to

471 applicable laws, directives, Executive Orders, policies, standards, or regulations” [19]. Two of the key
472 documents that describe the RMF are NIST SP 800-37 Revision 2, *Risk Management Framework for*
473 *Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; and NIST
474 SP 800-30, *Guide for Conducting Risk Assessments*.

475 **Application:** The RMF has seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and
476 Monitor. These steps provide a method for organizations to characterize the risk posture of their
477 information and systems and identify controls that are commensurate with the risks in the system’s
478 environment. They also support organizations with selecting beneficial implementation and assessment
479 approaches, reasoning through the process to understand residual risks, and monitoring the efficacy of
480 implemented controls over time.

481 The Great Seneca Accounting example solution touches on the risk assessment activities conducted
482 under the *Prepare* step, identifying the overall risk level of the BYOD system architecture in the
483 *Categorize* step, and, consistent with example approach 8 in NISTIR 8170, reasoning through the
484 controls that are necessary in the *Select* step. The influence of the priorities provided in Great Seneca
485 Accounting’s Cybersecurity Framework Target Profile is also briefly mentioned regarding making
486 decisions for how to apply controls during *Implement* (e.g., policy versus tools), how robustly to verify
487 and validate controls during *Assess* (e.g., document review versus “hands on the keyboard” system
488 testing), and the degree of evaluation required over time as part of the *Monitor* step.

489 E.1.4 Overview of the NIST Privacy Risk Assessment Methodology

490 **Description:** The NIST Privacy Risk Assessment Methodology (PRAM) is a tool for analyzing, assessing,
491 and prioritizing privacy risks to help organizations determine how to respond and select appropriate
492 solutions. A blank version of the PRAM is available for download on NIST’s website.

493 **Application:** The PRAM uses the privacy risk model and privacy engineering objectives described in
494 NISTIR 8062 to analyze for potential problematic data actions. Data actions are any system operations
495 that process data. Processing can include collection, retention, logging, analysis, generation,
496 transformation or merging, disclosure, transfer, and disposal of data. A problematic data action is one
497 that could cause an adverse effect, or problem, for individuals. The occurrence or potential occurrence
498 of problematic data actions is a privacy event. While there is a growing body of technical privacy
499 controls, including those found in NIST SP 800-53, applying the PRAM may result in identifying controls
500 that are not yet available in common standards. This makes it an especially useful tool for managing
501 risks that may otherwise go unaddressed.

502 The Great Seneca Accounting example solution assumed that a PRAM was used to identify problematic
503 data actions and mitigating controls for employees. The controls in this build include some technical
504 controls, such as controls that can be handled by security capabilities, as well as policy and procedure-
505 level controls that need to be implemented outside yet supported by the system.

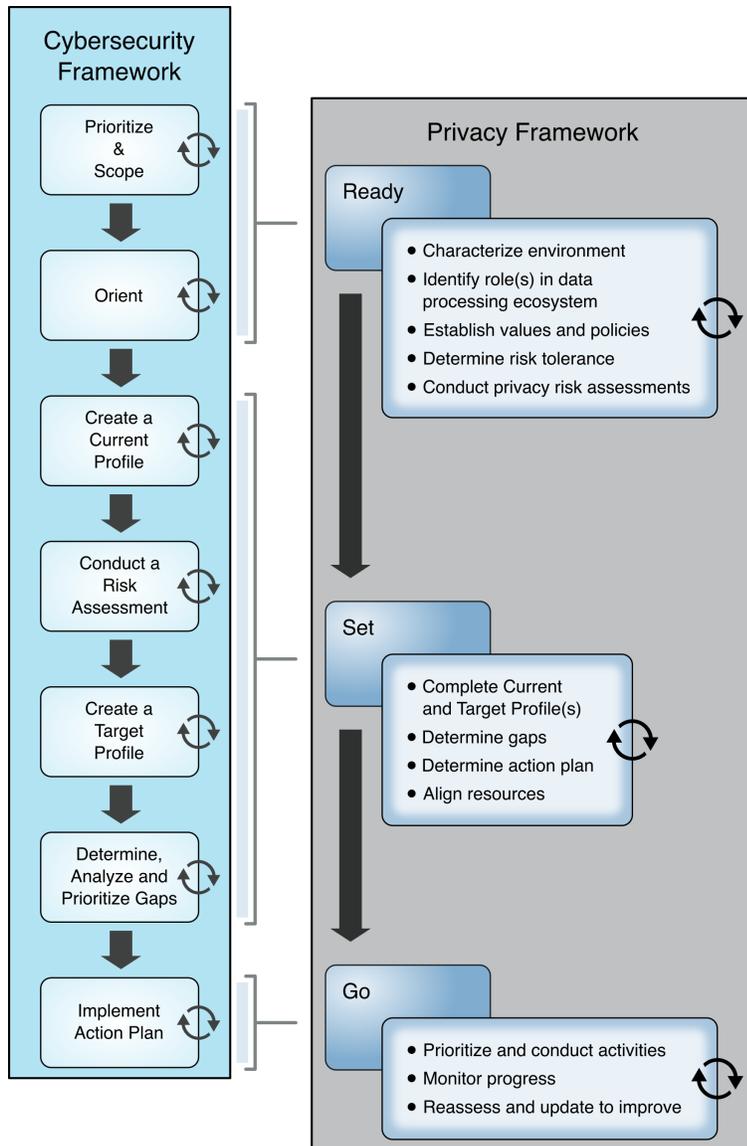
506 E.2 Using Frameworks to Establish or Improve Cybersecurity and Privacy 507 Programs

508 While their presentation differs, the NIST Cybersecurity Framework and NIST Privacy Framework also
509 both provide complementary guidance for establishing and improving cybersecurity and privacy
510 programs. The NIST Cybersecurity Framework's process for establishing or improving programs provides
511 seven steps that an organization could use iteratively and as necessary throughout the program's life
512 cycle to continually improve its cybersecurity posture:

- 513 ▪ Step 1: Prioritize and scope the organization's mission.
- 514 ▪ Step 2: Orient its cybersecurity program activities to focus efforts on applicable areas.
- 515 ▪ Step 3: Create a current profile of what security areas it currently supports.
- 516 ▪ Step 4: Conduct a risk assessment.
- 517 ▪ Step 5: Create a Target Profile of the security areas that the organization would like to improve
518 in the future.
- 519 ▪ Step 6: Determine, analyze, and prioritize cybersecurity gaps.
- 520 ▪ Step 7: Implement an action plan to close those gaps.

521 The *NIST Privacy Framework* includes the same types of activities for establishing and improving privacy
522 programs, described in a three-stage Ready, Set, Go model. Figure E-1 below shows a comparison of
523 these two approaches, demonstrating their close alignment.

524 **Figure E-1 Comparing Framework Processes to Establish or Improve Programs**



525 Both approaches are equally effective. Regardless of the approach selected, an organization begins with
 526 orienting around its business/mission objectives and high-level organizational priorities and carry out
 527 the remaining activities in a way that makes the most sense for the organization. The organization
 528 repeats these steps as necessary throughout the program’s life cycle to continually improve its risk
 529 posture.

530 **Appendix F How Great Seneca Accounting Used the NIST** 531 **Risk Management Framework**

532 This practice guide contains an example scenario about a fictional organization called Great Seneca
533 Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be
534 in alignment with an organization’s security and privacy capabilities and objectives.

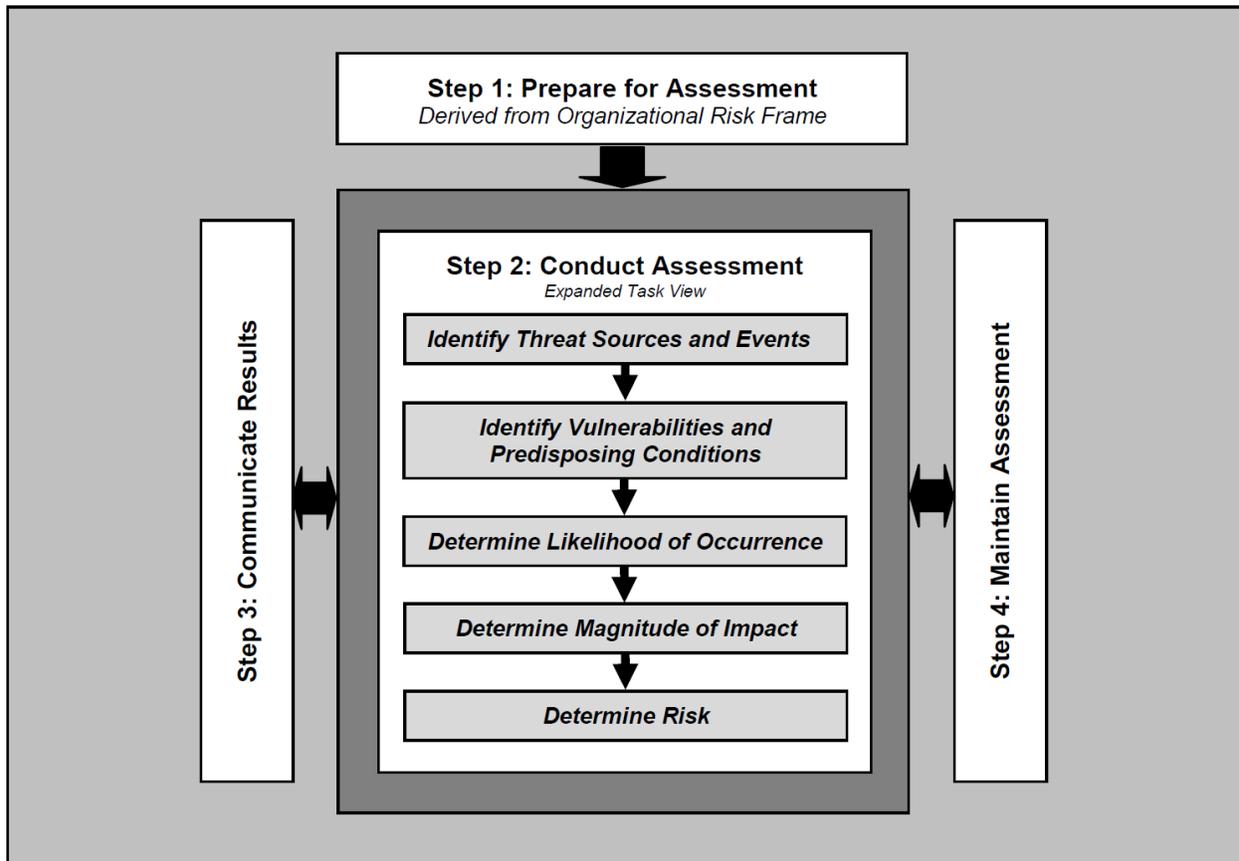
535 The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance,
536 and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this
537 practice guide.

538 In the example scenario supplement of this practice guide, Great Seneca Accounting decided to use the
539 NIST Cybersecurity Framework, the *NIST Privacy Framework*, and the NIST Risk Management Framework
540 to help improve its mobile device architecture. The following material provides information about how
541 Great Seneca Accounting used the NIST Risk Management Framework to improve its BYOD deployment.

542 **F.1 Understanding the Risk Assessment Process**

543 This section provides information on the risk assessment process employed to improve the mobile
544 security posture of Great Seneca Accounting. Typically, a risk assessment based on NIST SP 800-30
545 Revision 1 follows a four-step process as shown in [Figure F-1](#): prepare for assessment, conduct
546 assessment, communicate results, and maintain assessment.

547 **Figure F-1 Risk Assessment Process**



548 **F.2 Risk Assessment of Great Seneca Accounting’s BYOD Program**

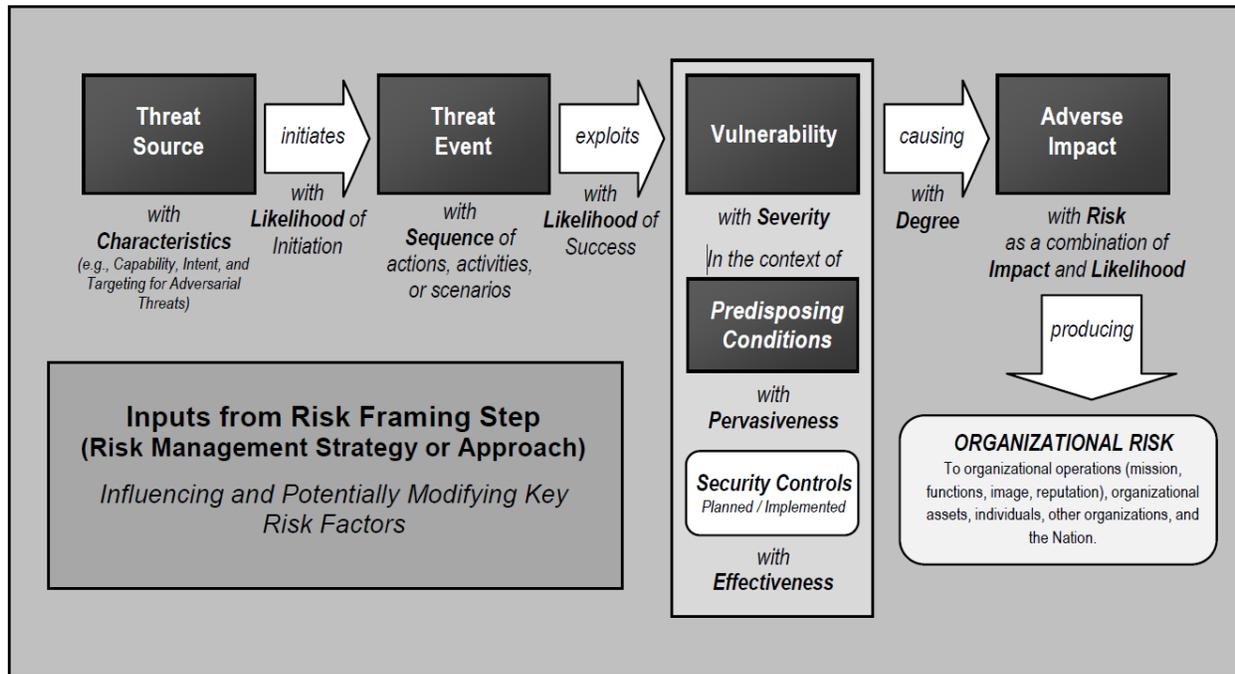
549 This risk assessment is scoped to Great Seneca Accounting’s mobile deployment, which includes the
 550 mobile devices used to access Great Seneca Accounting’s enterprise resources, along with any
 551 information technology components used to manage or provide services to those mobile devices.

552 Risk assessment assumptions and constraints were developed by using a NIST SP 800-30 Revision 1
 553 generic risk model as shown in [Figure F-2](#) to identify the following components of the risk assessment:

- 554 ▪ threat sources
- 555 ▪ threat events
- 556 ▪ vulnerabilities
- 557 ▪ predisposing conditions
- 558 ▪ security controls

- 559 ▪ adverse impacts
- 560 ▪ organizational risks

561 **Figure F-2 NIST SP 800-30 Generic Risk Model**



562 **F.3 Development of Threat Event Descriptions**

563 Great Seneca Accounting developed threat event tables based on NIST SP 800-30 Revision 1 and used
 564 those to help analyze the sources of mobile threats. Using this process, Great Seneca Accounting
 565 leadership identified the following potential mobile device threat events that are described in the
 566 following subsections.

567 **A note about selection of the threat events:**

568 This practice guide’s example solution helps protect organizations from the threat events shown in [Table](#)
 569 [F-1](#). A mapping of these threat events to the NIST Mobile Threat Catalogue is provided in [Table F-2](#).

570 **Table F-1 Great Seneca Accounting’s BYOD Deployment Threats**

Great Seneca Accounting’s Threat Event Identification Number	Threat Event Description
TE-1	privacy-intrusive applications
TE-2	account credential theft through phishing
TE-3	malicious applications
TE-4	outdated phones
TE-5	camera and microphone remote access
TE-6	sensitive data transmissions
TE-7	brute-force attacks to unlock a phone
TE-8	protection against weak password practices
TE-9	protection against unmanaged devices
TE-10	protection against lost or stolen data
TE-11	protecting data from being inadvertently backed up to a cloud service
TE-12	protection against sharing personal identification number (PIN) or password

571 Great Seneca Accounting’s 12 threat events and their mapping to the NIST Mobile Threat Catalogue [5]
 572 are shown in [Table F-2](#).

573 **Table F-2 Threat Event Mapping to the Mobile Threat Catalogue**

Great Seneca Accounting’s Threat Event Identification Number	NIST Mobile Threat Catalogue Threat ID
TE-1	APP-2, APP-12
TE-2	AUT-9
TE-3	APP-2, APP-5, APP-31, APP-40, APP-32, AUT-10
TE-4	APP-4, APP-26, STA-0, STA-9, STA-16
TE-5	APP-32, APP-36

Great Seneca Accounting’s Threat Event Identification Number	NIST Mobile Threat Catalogue Threat ID
TE-6	APP-0, CEL-18, LPN-2
TE-7	AUT-2, AUT-4
TE-8	APP-9, AUT-0
TE-9	EMM-5
TE-10	PHY-0
TE-11	EMM-9
TE-12	AUT-0, AUT-2, AUT-4, AUT-5

574 **F.4 Great Seneca Accounting’s Leadership and Technical Teams Discuss**
 575 **BYOD’s Potential Threats to Their Organization**

576 Great Seneca Accounting’s leadership team wanted to understand real-world examples of each threat
 577 event and what the risk was for each. Great Seneca Accounting’s leadership and technical teams then
 578 discussed those possible threats that BYOD could introduce to their organization.

579 The analysis performed by Great Seneca Accounting’s technical team included analyzing the likelihood
 580 of each threat, the level of impact, and the threat level that the BYOD deployment would pose. The
 581 following are leadership’s questions and the technical team’s responses regarding BYOD threats during
 582 that discussion using real-world examples. A goal of the example solution contained within this practice
 583 guide is to mitigate the impact of these threat events. Reference Table 5-1 in Volume B for a listing of
 584 the technology that addresses each of the following threat events.

585 **F.4.1 Threat Event 1**

586 **What happens if an employee installs risky applications?**

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

594 **Risk assessment analysis:**

595 Overall likelihood: very high

596 *Justification:* Employees have access to download any application at any time. If an employee requires
597 an application that provides a desired function, the employee can download that application from any
598 available source (trusted or untrusted) that provides a desired function. If an application performs an
599 employee’s desired function, the employee may download an application from an untrusted source
600 and/or disregard granted privacy permissions.

601 Level of impact: high

602 *Justification:* Employees may download an application from an untrusted source and/or disregard
603 granted privacy permissions. This poses a threat for sensitive corporate data, as some applications may
604 include features that could access corporate data, unbeknownst to the user.

605 **BYOD-specific threat:** In a BYOD scenario, users are still able to download and install applications at
606 their leisure. This capability allows users to unintentionally side-load or install a malicious application
607 that may harm the device or the enterprise information on the device.

608 **F.4.2 Threat Event 2**

609 **Can account information be stolen through phishing?**

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

616 **Risk assessment analysis:**

617 Overall likelihood: very high

618 *Justification:* Phishing campaigns are a very common threat that occurs almost every day.

619 Level of impact: high

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

623 **BYOD-specific threat:** The device-level controls applied to personal devices do not inhibit a user’s
624 activities. This allows the user to access personal/work messages and emails on their device that could

625 be susceptible to phishing attempts. If the proper controls are not applied to a user's enterprise
626 messages and email, successful phishing attempts could allow an attacker unauthorized access to
627 enterprise data.

628 F.4.3 Threat Event 3

629 **How much risk do malicious applications pose to Great Seneca Accounting?**

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

639 **Risk assessment analysis:**

640 Overall likelihood: high

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

646 Level of impact: high

647 *Justification:* Once a user installs a malicious side-loaded application, an adversary could gain full access
648 to a mobile device and, therefore, access to corporate data and credentials, without the user's
649 knowledge.

650 **BYOD-specific threat:** Like Threat Event 1, BYOD deployments may have fewer restrictions to avoid
651 preventing the user from performing desired personal functions. This increases the attack surface for
652 malicious actors to take advantage.

653 F.4.4 Threat Event 4

654 **What happens when outdated phones access Great Seneca Accounting's network?**

655 When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers,
656 the delivered code generally executes with elevated privileges and issues commands in the context of

657 the root user or the OS kernel. This may be enough for some malicious actors to accomplish their goal,
658 but those that are advanced will usually attempt to install additional malicious tools and to establish a
659 persistent presence. If successful, the attacker will be able to launch further attacks against the user, the
660 device, or any other systems to which the device connects. As a result, any data stored on, generated
661 by, or accessible to the device at that time—or in the future—may be compromised.

662 **Risk assessment analysis:**

663 Overall likelihood: high

664 *Justification:* Many public vulnerabilities specific to mobile devices have been seen over the years. In
665 these, users can jailbreak iOS devices and root Android devices to download third-party applications and
666 apply unique settings/configurations that the device would not typically be able to apply/access.

667 Level of impact: high

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

672 **BYOD-specific threat:** As with any device, personal devices are susceptible to device exploitation if not
673 properly used or updated.

674 **F.4.5 Threat Event 5**

675 **Can Great Seneca Accounting stop someone from turning on a camera or microphone?**

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

684 **Risk assessment analysis:**

685 Overall likelihood: very high

686 *Justification:* This has been seen on public application stores, with applications allegedly being used for
687 data-collection. As mentioned in Threat Event 1, unbeknownst to the user, a downloaded application
688 may be granted privacy-intrusive permissions that allow access to device sensors.

689 Level of impact: high

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

692 **BYOD-specific threat:** Applications commonly request access to these sensors. In a BYOD deployment,
693 the enterprise does not have control over what personal applications the user installs on their device.
694 These personal applications may access sensors on the device and eavesdrop on a user's enterprise-
695 related activities (e.g., calls and meetings).

696 F.4.6 Threat Event 6

697 **Is sensitive information protected when the data travels between the employee's mobile device and** 698 **Great Seneca Accounting's network?**

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

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

712 **Risk assessment analysis:**

713 Overall likelihood: moderate

714 *Justification:* Unlike installation of an application, installations of enterprise mobility management
715 (EMM)/mobile device management (MDM), network, virtual private network (VPN) profiles, and
716 certificates require additional effort and understanding from the user to properly implement.

717 Level of impact: very high

718 *Justification:* If malicious actor can install malicious configuration profiles or certificates, they would be
719 able to perform actions such as decrypting network traffic and possibly even control the device.

720 **BYOD-specific threat:** Like Threat Event 2, personal devices may not have the benefit of an always-on
721 device-wide VPN. This leaves application communications at the discretion of the developer.

722 F.4.7 Threat Event 7

723 **Is Great Seneca Accounting’s data protected from brute-force PIN attacks?**

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

733 **Risk assessment analysis:**

734 Overall likelihood: moderate

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

738 Level of impact: very high

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

742 **BYOD-specific threat:** Because BYODs are prone to travel (e.g., vacations, restaurants, and other
743 nonwork locations), the risk that the device’s passcode is obtained increases due to the heightened
744 exposure to threats in different environments.

745 F.4.8 Threat Event 8

746 **Can Great Seneca Accounting protect its data from weak password practices?**

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

752 **Risk assessment analysis:**

753 Overall likelihood: moderate

754 *Justification:* Often applications include hardcoded credentials for the default password of the admin
755 account. Default passwords are readily available online. The user might not change these passwords to
756 allow access and eliminate the need to remember a password.

757 Level of impact: high

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

760 **BYOD-specific threat:** The risk of hardcoded credentials residing in an application on the device is the
761 same for any mobile device deployment scenario.

762 **F.4.9 Threat Event 9**

763 **Can unmanaged devices connect to Great Seneca Accounting?**

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

772 **Risk assessment analysis:**

773 Overall likelihood: very high

774 *Justification:* This may occur accidentally when an employee attempts to access their email or other
775 corporate resources.

776 Level of impact: high

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

780 **BYOD-specific threat:** The risk of an unmanaged mobile device accessing the enterprise is the same for
781 any mobile deployment scenario.

782 **F.4.10 Threat Event 10**

783 **Can Great Seneca Accounting protect its data when a phone is lost or stolen?**

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

787 **Risk assessment analysis:**

788 Overall likelihood: very high

789 *Justification:* Mobile devices are small and can be misplaced. Enterprise devices may be lost or stolen at
790 the same frequency as personally owned devices.

791 Level of impact: high

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

794 **BYOD-specific threat:** Due to the heightened mobility of BYODs, they are more prone to being
795 accidentally lost or stolen.

796 **F.4.11 Threat Event 11**

797 **Can data be protected from unauthorized cloud services?**

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

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

807 **Risk assessment analysis:**

808 Overall likelihood: high

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

811 Level of impact: high

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

814 **BYOD-specific threat:** In a BYOD deployment, employees are more likely to have some backup or
815 automated cloud storage solution configured on their device, which may lead to unintentional backup of
816 enterprise data.

817 **F.4.12 Threat Event 12**

818 **Can Great Seneca Accounting protect its data from PIN or password sharing?**

819 Many individuals choose to share the PIN or password to unlock their personal device with family
820 members. This creates a scenario where a nonemployee can access the device, the work applications,
821 and therefore the work data.

822 **Risk assessment analysis:**

823 Overall likelihood: moderate

824 *Justification:* Even though employees are conditioned almost constantly to protect their work
825 passwords, personal device PINs and passwords are not always protected with that same level of
826 security. Anytime individuals share a password or PIN, there is increased risk that it might be exposed or
827 compromised.

828 Level of impact: very high

829 *Justification:* If a malicious actor can bypass a device lock and gain access to the device, they can
830 potentially access sensitive corporate data.

831 **BYOD-specific threat:** The passcode of an individual's personal mobile device is more likely to be shared
832 among family and/or friends to provide access to applications (e.g., games). Although sharing passcodes
833 may be convenient for personal reasons, this increases the risk of an unauthorized individual gaining
834 access to enterprise data through a personal device.

835 **F.5 Identification of Vulnerabilities and Predisposing Conditions**

836 In this section we identify vulnerabilities and predisposing conditions that increase the likelihood that
837 identified threat events will result in adverse impacts for Great Seneca Accounting. We list each
838 vulnerability or predisposing condition in [Table F-3](#), along with the corresponding threat events and
839 ratings of threat pervasiveness. More details on threat event ratings can be found in Appendix [Section](#)
840 [F.3](#).

841 **Table F-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-9, TE-10	very high
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their mobile devices.	TE-6	very high
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-10, TE-11, TE-12	very high

842 **F.6 Summary of Risk Assessment Findings**

843 [Table F-4](#) summarizes the risk assessment findings. More detail about the methodology used to rate
 844 overall likelihood, level of impact, and risk is in the Appendix [Section F.3](#).

845 **Table F-4 Summary of Risk Assessment Findings**

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	very high	high	high
TE-2: theft of credentials through an SMS or email phishing campaign	VULN-1	very high	high	high
TE-3: malicious applications installed via URLs in SMS or email messages	VULN-3	high	high	high

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
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: loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2, VULN-3	moderate	very high	high
TE-7: compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	moderate	very high	high
TE-8: unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	moderate	high	high
TE-9: unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1, VULN-3	very high	high	high
TE-10: loss of organizational data due to a lost or stolen device	VULN-1, VULN-3	very high	high	high
TE-11: loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	VULN-3	high	high	high
TE-12: unauthorized access to work applications via bypassed lock screen	VULN-3	moderate	very high	high

846 **Note 1:** Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST SP 800-30
847 Revision 1 [\[8\]](#).

848 **Note 2:** The risk rating is derived from both the overall likelihood and level of impact using Table I-2 of
849 Appendix I in NIST SP 800-30 Revision 1 [\[8\]](#). Because these are modified interval scales, the combined
850 overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two
851 variables. The table above demonstrates this where levels of moderate weigh more heavily than other
852 ratings.

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

891 the system’s capabilities into alignment with employees’ expectations about what can happen to their
892 devices, especially if they are unaware that devices can be wiped by administrators—providing greater
893 predictability in the system.

894 Related mitigation: If this mitigation approach is taken, the organization may also wish to consider
895 establishing and communicating these remediation processes to employees. It is important to have a
896 clear remediation process in place to help employees regain access to resources on their devices at the
897 appropriate time. It is also important to clearly convey this remediation process to employees. A
898 remediation process provides greater manageability in the system supporting employees’ ability to
899 access resources. If well-communicated to employees, this also provides greater predictability as
900 employees will know the steps to regain access.

901 **Enable only selective wiping of corporate resources on the device.**

902 An alternative mitigation option for wiping device data is to limit what can be wiped. International
903 Business Machines’ (IBM’s) MaaS360 can be configured to selectively wipe instead of performing a full
904 factory reset. When configured this way, a wipe preserves employees’ personal configurations,
905 applications, and data while removing only the corporate configurations, applications, and data.
906 However, on Android, a selective wipe will preserve restrictions imposed via policy on the device. To
907 fully remove MDM control, the Remove Work Profile action must be used.

908 **Advise employees to appropriately store and back up the personal data maintained on devices.**

909 If device wiping remains an option for administrators, encourage employees to perform regular backups
910 of their personal data to ensure it remains accessible in case of a wipe and to not store personal data
911 within the work container on their device.

912 **Restrict staff access to system capabilities that permit removing device access or performing wipes.**

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

916 **G.2 Privacy Risk 2: Organizational Collection of Device Data May Subject**
917 **Users to Feeling or Being Surveilled**

918 **Privacy Risk:** The assessed infrastructure offers Great Seneca Accounting and its employees a number of
919 security capabilities, including reliance on comprehensive monitoring capabilities, as noted in [Section 4](#),
920 Architecture. Multiple parties could collect and analyze a significant amount of data relating to employ-
921 ees, their devices, and their activities.

922

923 **Potential Problem for Individuals:** Employees may not be aware that the organization has the ability to
924 monitor their interactions with the system and may not want this monitoring to occur or understand the

925 way these interactions are being analyzed or used. If there is awareness, employees may feel compelled
926 to allow for monitoring to occur for the ability to use their mobile devices for corporate access.
927 Collection and analysis of information might enable Great Seneca Accounting or other parties to craft a
928 narrative about an employee based on the employee's interactions with the system, which could lead to
929 a power imbalance between Great Seneca Accounting and the employee and loss of trust in the
930 employer or loss of autonomy if the employee discovers monitoring that they did not anticipate or
931 expect. This privacy risk is related to the Surveillance Problematic Data Action.

932 **Mitigations:**

933 **Restrict staff access to system capabilities that permit reviewing data about employees and their**
934 **devices.**

935 This may be achieved using role-based access controls. Access can be limited to any dashboard in the
936 system containing data about employees and their devices but is most sensitive for the MaaS360
937 dashboard, which is the hub for data about employees, their devices, and threats. Minimizing access to
938 sensitive information can enhance disassociability for employees using the system.

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

940 Conduct a system-specific privacy risk assessment to determine what elements can be limited. In the
941 configuration of MaaS360, location services and application inventory collection may be disabled. iOS
942 devices can be configured in MaaS360 to collect only an inventory of applications that have been
943 installed through the corporate application store instead of all applications installed on the device.

944 While these administrative configurations may help provide disassociability in the system, there are also
945 some opportunities for employees to limit the data collected. Employees can choose to disable location
946 services in their device OS to prevent collection of location data. MaaS360 can also be configured to
947 provide employees with the ability to manage their own devices through the IBM User Portal.

948 Each of these controls contributes to limiting the number of attributes regarding employees and their
949 devices that is collected, which can impede administrators' ability to associate information with specific
950 individuals.

951 **Dispose of personally identifiable information (PII).**

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

958 **G.3 Privacy Risk 3: Data Collection and Transmission Between Integrated** 959 **Security Products May Expose User Data**

960 **Privacy Risk:** The infrastructure involves several parties that serve different purposes supporting Great
961 Seneca Accounting’s security objectives. As a result, device usage information could flow across various
962 parties.

963
964 **Potential Problems for Individuals:** This transmission among a variety of different parties could be
965 confusing for employees who might not know who has access to information about them. If
966 administrators and co-workers know which colleagues are conducting activity on their device that
967 triggers security alerts, employees could be embarrassed by its disclosure. Information being revealed
968 and associated with specific employees could also lead to stigmatization and even impact Great Seneca
969 Accounting upper management in its decision-making regarding the employee. Further, clear text
970 transmissions could leave information vulnerable to attackers and, therefore, to unanticipated release
971 of employee information. This privacy risk is related to the Unanticipated Revelation Problematic Data
972 Action.

973 **Mitigations:**

974 **De-identify personal and device data when that data is not necessary to meet processing objectives.**

975 De-identifying data helps decrease the chances that a third party is aggregating information pertaining
976 to one individual. While de-identification can help reduce privacy risk, there are residual risks of re-
977 identification.

978 **Encrypt data transmitted between parties.**

979 Encryption reduces the risk of compromise of information transmitted between parties. MaaS360
980 encrypts all communications over the internet with Transport Layer Security.

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

982 Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using
983 access controls to limit staff access to compliance information, especially when associated with
984 individuals, can be important in preventing association of specific events with specific employees.

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

986 Conduct a system-specific privacy risk assessment to determine what elements can be limited. MaaS360
987 can be configured to limit collection of application and location data. Further, instead of collecting a list
988 of all the applications installed on the device, MaaS360 can collect only the list of those applications that
989 were installed through the corporate application store (called “managed applications”). This would
990 prevent insight into the employees’ applications that employees downloaded for personal use.

991 Zimperium provides privacy policies that can be configured to collect or not collect data items when
992 certain events occur.

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

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

996 **G.4 Mitigations Applicable Across Various Privacy Risks**

997 Several mitigations benefit employees in all three privacy risks identified in the privacy risk assessment.
998 The following training and support mitigations can help Great Seneca Accounting appropriately inform
999 employees about the system and its data processing.

1000 **Mitigations:**

1001 **Train employees about the system, parties involved, data processing, and actions that administrators**
1002 **can take.**

1003 Training sessions can also highlight any privacy-preserving techniques used, such as for disclosures to
1004 third parties. Training should include confirmation from employees that they understand the actions
1005 that administrators can take on their devices and their consequences—whether this is blocking access or
1006 wiping data. Employees may also be informed of data retention periods and when their data will be
1007 deleted. This can be more effective than sharing a privacy notice, which research has shown, individuals
1008 are unlikely to read. Still, MaaS360 should also be configured to provide employees with access to a
1009 visual privacy policy, which describes what device information is collected and why, as well as what
1010 actions administrators can take on the device. This enables employees to make better informed
1011 decisions while using their devices, and it enhances predictability.

1012 **Provide ongoing notifications or reminders about system activity.**

1013 This can be achieved using notifications to help directly link administrative actions on devices to relevant
1014 threats and to also help employees understand why an action is being taken. MaaS360 also notifies
1015 employees when changes are made to the privacy policy or MDM profile settings. These notifications
1016 can help increase system predictability by setting employee expectations appropriately regarding the
1017 way the system processes data and the resulting actions.

1018 **Provide a support point of contact.**

1019 By providing employees with a point of contact in the organization who can respond to inquiries and
1020 concerns regarding the system, employees can better understand how the system processes their data,
1021 which enhances predictability.

1022 **G.5 Privacy References for Example Solution Technologies**

1023 Additional privacy information on the example solution’s technologies appears below.

1024 **Table G-1 Privacy References for the Example Solution Technologies**

Commercially Available Product	Mobile Security Technology	Product Privacy Information Location
<p>IBM MaaS360 Mobile Device Management (SaaS) Version 10.73</p> <p>IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)</p> <p>IBM MaaS360 Cloud Extender / Cloud Extender Modules</p>	<p>mobile device management</p>	<p>https://www.ibm.com/docs/en/search/privacy</p> <p>https://www.ibm.com/support/pages/node/571227</p> <p>https://www.ibm.com/support/knowledge-center/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_privacy.htm</p> <p>https://www.ibm.com/support/pages/maas360-data-privacy-information</p>
<p>Kryptowire Cloud Service</p>	<p>application vetting</p>	<p>https://www.kryptowire.com</p>
<p>Palo Alto Networks PA-VM-100 Version 9.0.1</p> <p>Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android)</p>	<p>virtual private network (VPN) and firewall/filtering</p>	<p>https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/host-information/about-host-information/what-data-does-the-globalprotect-app-collect-on-each-operating-system</p> <p>https://www.paloaltonetworks.com/resources/datasheets/url-filtering-privacy-datasheet</p>
<p>Qualcomm (Version is mobile device dependent)</p>	<p>trusted execution environment</p>	<p>https://www.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snap-dragon-mobile-platform.pdf</p>

Commercially Available Product	Mobile Security Technology	Product Privacy Information Location
Zimperium Defense Suite Zimperium Console Version vGA-4.23.1 Zimperium zIPS Agent Version 4.9.2 (Android and iOS)	mobile threat defense	https://www.zimperium.com/mobile-app-protection

Mobile Device Security:

Bring Your Own Device (BYOD)

Volume C:
How-To Guides

Kaitlin Boeckl

Nakia Grayson

Gema Howell

Naomi Lefkowitz

Applied Cybersecurity Division
Information Technology Laboratory

Jason Ajmo

Milissa McGinnis*

Kenneth F. Sandlin

Oksana Slivina

Julie Snyder

Paul Ward

The MITRE Corporation
McLean, VA

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

November 2022

SECOND DRAFT

This publication is available free of charge from

<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



1 **DISCLAIMER**

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

7 While NIST and NCCoE address goals of improving the management of cybersecurity and privacy risk
8 through outreach and application of standards and best practices, it is the stakeholder’s responsibility to
9 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise
10 and the impact should the threat be realized before adopting cyber security measures such as this
11 recommendation.

12 National Institute of Standards and Technology Special Publication 1800-22C Natl. Inst. Stand. Technol.
13 Spec. Publ. 1800-22C, 101 pages, (November 2022), CODEN: NSPUE2

14 **FEEDBACK**

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

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

18 Public comment period: November 29, 2022 through January 13, 2023

19 All comments are subject to release under the Freedom of Information Act (FOIA).

20 National Cybersecurity Center of Excellence
21 National Institute of Standards and Technology
22 100 Bureau Drive
23 Mailstop 2002
24 Gaithersburg, MD 20899
25 Email: nccoe@nist.gov

26 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

42 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

52 **ABSTRACT**

53 Bring Your Own Device (BYOD) refers to the practice of performing work-related activities on personally
54 owned devices. This practice guide provides an example solution demonstrating how to enhance
55 security and privacy in Android and iOS smartphone BYOD deployments.

56 Incorporating BYOD capabilities into an organization can provide greater flexibility in how employees
57 work and increase the opportunities and methods available to access organizational resources. For some
58 organizations, the combination of traditional in-office processes with mobile device technologies
59 enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-

60 first approach in which their employees communicate and collaborate primarily using their mobile
 61 devices.

62 However, some of the features that make BYOD mobile devices increasingly flexible and functional also
 63 present unique security and privacy challenges to both work organizations and device owners. The
 64 unique nature of these challenges is driven by the diverse range of devices available that vary in type,
 65 age, operating system (OS), and the level of risk posed.

66 Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks to organizations.
 67 Solutions that are designed to secure corporate devices and on-premises data do not provide an
 68 effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the
 69 unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new
 70 privacy risks to employees by providing their employer a degree of access to their personal devices,
 71 opening up the possibility of observation and control that would not otherwise exist.

72 To help organizations benefit from BYOD’s flexibility while protecting themselves from many of its
 73 critical security and privacy challenges, this Practice Guide provides an example solution using
 74 standards-based, commercially available products and step-by-step implementation guidance.

75 **KEYWORDS**

76 *Bring your own device; BYOD; mobile device management; mobile device security.*

77 **ACKNOWLEDGMENTS**

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

Name	Organization
Donna Dodson*	NIST
Joshua M. Franklin*	NIST
Jeff Greene	NIST
Natalia Martin	NIST
William Newhouse	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST

Name	Organization
Chris Brown	The MITRE Corporation
Nancy Correll*	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston*	The MITRE Corporation
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Erin Wheeler*	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward	IBM
Cesare Coscia	IBM
Chris Gogoel	Kryptowire (now known as Quokka)
Tom Karygiannis	Kryptowire (now known as Quokka)
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Mikel Draghici*	Zimperium

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

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

Technology Partner/Collaborator	Build Involvement
IBM	Mobile Device Management
Kryptowire (now known as Quokka)	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

84 **DOCUMENT CONVENTIONS**

85 The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the
 86 publication and from which no deviation is permitted. The terms “should” and “should not” indicate that
 87 among several possibilities, one is recommended as particularly suitable without mentioning or
 88 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in
 89 the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms
 90 “may” and “need not” indicate a course of action permissible within the limits of the publication. The
 91 terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

92 **CALL FOR PATENT CLAIMS**

93 This public review includes a call for information on essential patent claims (claims whose use would be
 94 required for compliance with the guidance or requirements in this Information Technology Laboratory
 95 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
 96 or by reference to another publication. This call also includes disclosure, where known, of the existence
 97 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
 98 unexpired U.S. or foreign patents.

99 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-
 100 ten or electronic form, either:

101 a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
102 currently intend holding any essential patent claim(s); or

103 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
104 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
105 publication either:

106 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
107 or

108 2. without compensation and under reasonable terms and conditions that are demonstrably free
109 of any unfair discrimination.

110 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
111 behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-
112 sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that
113 the transferee will similarly include appropriate provisions in the event of future transfers with the goal
114 of binding each successor-in-interest.

115 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
116 whether such provisions are included in the relevant transfer documents.

117 Such statements should be addressed to: mobile-nccoe@nist.gov.

118 **Contents**

119 **1 Introduction.....1**

120 1.1 Practice Guide Structure 1

121 1.2 Build Overview 2

122 1.3 Typographic Conventions..... 3

123 1.4 Logical Architecture Summary 3

124 **2 Product Installation Guides4**

125 2.1 Network Device Enrollment Services Server 4

126 2.1.1 NDES Configuration..... 5

127 2.2 International Business Machines MaaS360 9

128 2.2.1 Cloud Extender..... 9

129 2.2.2 Android Enterprise Configuration..... 16

130 2.2.3 iOS APNs Certificate Configuration 17

131 2.2.4 Apple User Enrollment (UE) Configuration 17

132 2.2.5 Android Configuration 20

133 2.2.6 iOS Configuration 23

134 2.3 Zimperium 26

135 2.3.1 Zimperium and MaaS360 Integration..... 26

136 2.3.2 Automatic Device Activation..... 27

137 2.3.3 Enforce Application Compliance..... 30

138 2.3.4 MaaS360 Risk Posture Alerts 30

139 2.4 Palo Alto Networks Virtual Firewall 31

140 2.4.1 Network Configuration 31

141 2.4.2 Demilitarized Zone Configuration..... 34

142 2.4.3 Firewall Configuration..... 35

143 2.4.4 Certificate Configuration..... 36

144 2.4.5 Website Filtering Configuration..... 37

145 2.4.6 User Authentication Configuration..... 43

146 2.4.7 VPN Configuration 47

147 2.4.8 Enable Automatic Application and Threat Updates58

148 2.5 Kryptowire 60

149 2.5.1 Kryptowire and MaaS360 Integration.....60

150 **Appendix A List of Acronyms..... 62**

151 **Appendix B Glossary 64**

152 **Appendix C References 65**

153 **Appendix D Example Solution Lab Build Testing Details..... 66**

154 D.1 Threat Event 1 66

155 D.2 Threat Event 2 68

156 D.3 Threat Event 3 69

157 D.4 Threat Event 4 70

158 D.5 Threat Event 5 71

159 D.6 Threat Event 6 73

160 D.7 Threat Event 7 74

161 D.8 Threat Event 8 76

162 D.9 Threat Event 9 78

163 D.10 Privacy Risk 1 – Wiping Activities on the User’s Device May Inadvertently Delete the
164 User’s Personal Data 82

165 D.11 Privacy Risk 2 – Organizational Collection of Device Data May Subject Users to Feeling
166 or Being Surveilled..... 83

167 D.12 Privacy Risk 3 - Mobile security services may not alert users to what information is
168 collected 85

169 D.13 Privacy Risk 4 – Data Collection and Transmission Between Integrated Security
170 Products May Expose User Data 87

171 **List of Figures**

172 **Figure 1-1 High-Level Build Architecture..... 4**

173 **Figure 2-1 Post-Deployment Configuration 6**

174	Figure 2-2 PasswordMax Registry Configuration	8
175	Figure 2-3 NDES Domain Bindings	9
176	Figure 2-4 Cloud Extender Architecture	10
177	Figure 2-5 Old Cloud Extender Interface	11
178	Figure 2-6 Cloud Extender Service Account Details	12
179	Figure 2-7 Administrator Settings.....	13
180	Figure 2-8 Administrator Configuration Options.....	14
181	Figure 2-9 Cloud Extender SCEP Configuration	15
182	Figure 2-10 Cloud Extender Certificate Properties	16
183	Figure 2-11 Enterprise Binding Settings Confirmation.....	17
184	Figure 2-12 Where to Click to Download the Public Key	18
185	Figure 2-13 MDM configuration in Apple Business Manager	19
186	Figure 2-14 Creating the DEP token	19
187	Figure 2-15 VPP token in MaaS360.....	20
188	Figure 2-16 iOS Enrollment Configuration	20
189	Figure 2-17 Android GlobalProtect Application Compliance	23
190	Figure 2-18 Zimperium MaaS360 Integration Configuration	27
191	Figure 2-19 Zimperium zIPS iOS Configuration.....	28
192	Figure 2-20 Zimperium zIPS Android Configuration	29
193	Figure 2-21 Add Alert Button	30
194	Figure 2-22 Zimperium Risk Posture Alert Configuration	31
195	Figure 2-23 DNS Proxy Object Configuration	33
196	Figure 2-24 Original Packet Network Address Translation Configuration	34
197	Figure 2-25 Certificate Profile.....	37
198	Figure 2-26 Custom URL Category	38
199	Figure 2-27 URL Filtering Profile	39
200	Figure 2-28 URL Filtering Security Policy.....	40
201	Figure 2-29 Generating the Root CA	41

202 **Figure 2-30 Blocked Website Notification**..... 43

203 **Figure 2-31 Service Route Configuration** 44

204 **Figure 2-32 LDAP Server Profile**..... 45

205 **Figure 2-33 LDAP Group Mapping** 46

206 **Figure 2-34 LDAP User Authentication Profile** 47

207 **Figure 2-35 Configured Tunnel Interfaces**..... 47

208 **Figure 2-36 SSL VPN Tunnel Interface Configuration**..... 48

209 **Figure 2-37 GlobalProtect iOS Authentication Profile** 50

210 **Figure 2-38 LDAP Authentication Group Configuration**..... 51

211 **Figure 2-39 VPN Zone Configuration**..... 52

212 **Figure 2-40 GlobalProtect Portal General Configuration** 53

213 **Figure 2-41 GlobalProtect Portal Authentication Configuration**..... 54

214 **Figure 2-42 GlobalProtect Portal Agent Authentication Configuration**..... 55

215 **Figure 2-43 GlobalProtect Portal Agent Configuration** 56

216 **Figure 2-44 Captive Portal Configuration**..... 57

217 **Figure 2-45 GlobalProtect Portal** 58

218 **Figure 2-46 Downloaded Threats and Applications**..... 59

219 **Figure 2-47 Schedule Time Hyperlink** 59

220 **Figure 2-48 Application and Threats Update Schedule**..... 60

221 **Figure 2-49 Contact Created in Work Profile**..... 67

222 **Figure 2-50 Personal Profile Can't See Work Contacts** 67

223 **Figure 2-51 Contact Created in Managed App** 67

224 **Figure 2-52 Unmanaged App Can't See Managed Contacts**..... 67

225 **Figure 2-53 Fictitious Phishing Webpage Blocked** 69

226 **Figure 2-54 iOS MaaS360 OS Compliance Alert**..... 70

227 **Figure 2-55 Zimperium Risk Detected**..... 70

228 **Figure 2-56 Kryptowire Application Report** 71

229 **Figure 2-57 Android Passcode Configuration** 72

230 **Figure 2-58 iOS Passcode Configuration 72**

231 **Figure 2-59 Zimperium Detecting Disabled Lockscreen 73**

232 **Figure 2-60 Application Report with Hardcoded Credentials 74**

233 **Figure 2-61 Attempting to Access the VPN on an Unmanaged iOS Device 75**

234 **Figure 2-62 Attempting to Access the VPN on an Unmanaged Android Device 75**

235 **Figure 2-63 Attempting to Access the VPN on a Managed Android Device 76**

236 **Figure 2-64 Selective Wiping a Device 77**

237 **Figure 2-65 Selective Wipe Complete 78**

238 **Figure 2-66 Corporate Data Removal Confirmation Notification on iOS 78**

239 **Figure 2-67 Work Profile Removal Notification on Android 78**

240 **Figure 2-68 iOS DLP Configuration Options 80**

241 **Figure 2-69 Android DLP Configuration 81**

242 **Figure 2-70 Attempting to Paste Text on iOS Between Unmanaged and Managed Apps 82**

243 **Figure 2-71 Selective Wipe 83**

244 **Figure 2-72 Application Inventory Information 84**

245 **Figure 2-73 Location Information Restricted 85**

246 **Figure 2-74 Mobile Device Information Collection Notification 86**

247 **Figure 2-75 Non-Administrator Failed Portal Login 88**

248 **Figure 2-76 - Admin Login Settings 89**

249 **Figure 2-77 - Administrator Levels 89**

250 1 Introduction

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

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

258 1.1 Practice Guide Structure

259 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a
260 standards-based reference design and provides users with the information they need to replicate
261 enhancing the security of bring your own device (BYOD) solutions. This reference design is modular and
262 can be deployed in whole or in part.

263 This guide contains four volumes:

- 264 ▪ NIST SP 1800-22A: *Executive Summary*
- 265 ▪ NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
- 266 ▪ NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how
267 organizations can implement this example solution's guidance
- 268 ▪ NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution (**you are**
269 **here**)

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

271 **Business decision makers, including chief security and technology officers**, will be interested in the
272 *Executive Summary, NIST SP 1800-22A*, which describes the following topics:

- 273 ▪ challenges that enterprises face in managing the security of BYOD deployments
- 274 ▪ the example solution built at the NCCoE
- 275 ▪ benefits of adopting the example solution

276 **Technology or security program managers** who are concerned with how to identify, understand, assess,
277 and mitigate risk will be interested in *NIST SP 1800-22B*, which describes what we did and why. The
278 following sections will be of particular interest:

- 279 ▪ Section 4.1.4, Conduct a Risk Assessment, describes the risk analysis we performed.

- 280 ▪ Appendix E in Volume B, Example Security Subcategory and Control Map, maps the security
281 characteristics of this example solution to cybersecurity standards and best practices.

282 You might share the *Executive Summary, NIST SP 1800-22A*, with your leadership team members to help
283 them understand the importance of adopting standards-based BYOD solutions.

284 **IT professionals** who want to implement an approach like this will find this whole practice guide useful.
285 You can use this How-To portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build
286 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
287 and integration instructions for implementing the example solution. We do not recreate the product
288 manufacturers' documentation, which is generally widely available. Rather, we show how we
289 incorporated the products together in our environment to create an example solution.

290 This guide assumes that IT professionals have experience implementing security products within the
291 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
292 not endorse these particular products. Your organization can adopt this solution or one that adheres to
293 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
294 parts of a BYOD solution. Your organization's security experts should identify the products that will best
295 integrate with your existing tools and IT system infrastructure. We hope that you will seek products that
296 are congruent with applicable standards and best practices. Volume B, Section 3.7, Technologies, lists
297 the products that we used and maps them to the cybersecurity controls provided by this reference
298 solution.

299 **For those who would like to see how the example solution can be implemented**, this practice guide
300 contains an example scenario about a fictional company called Great Seneca Accounting. The example
301 scenario shows how BYOD objectives can align with an organization's priority security and privacy
302 capabilities through NIST risk management standards, guidance, and tools. It is provided in this practice
303 guide's supplement, *NIST SP 1800-22 Example Scenario: Putting Guidance into Practice*.

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

308 1.2 Build Overview

309 In our lab at the National Cybersecurity Center of Excellence (NCCoE), NIST engineers built an
310 environment that contains an example solution for managing the security of BYOD deployments. In this
311 guide, we show how an enterprise can leverage this example solution's concepts to implement
312 Enterprise Mobility Management (EMM), mobile threat defense, application vetting, secure boot/image
313 authentication, and virtual private network (VPN) services in support of a BYOD solution.

314 These technologies were configured to protect organizational assets and end-user privacy, providing
 315 methodologies to enhance the data protection posture of the adopting organization. The standards,
 316 best practices, and certification programs that this example solution is based upon help ensure the
 317 confidentiality, integrity, and availability of enterprise data on mobile systems.

318 1.3 Typographic Conventions

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

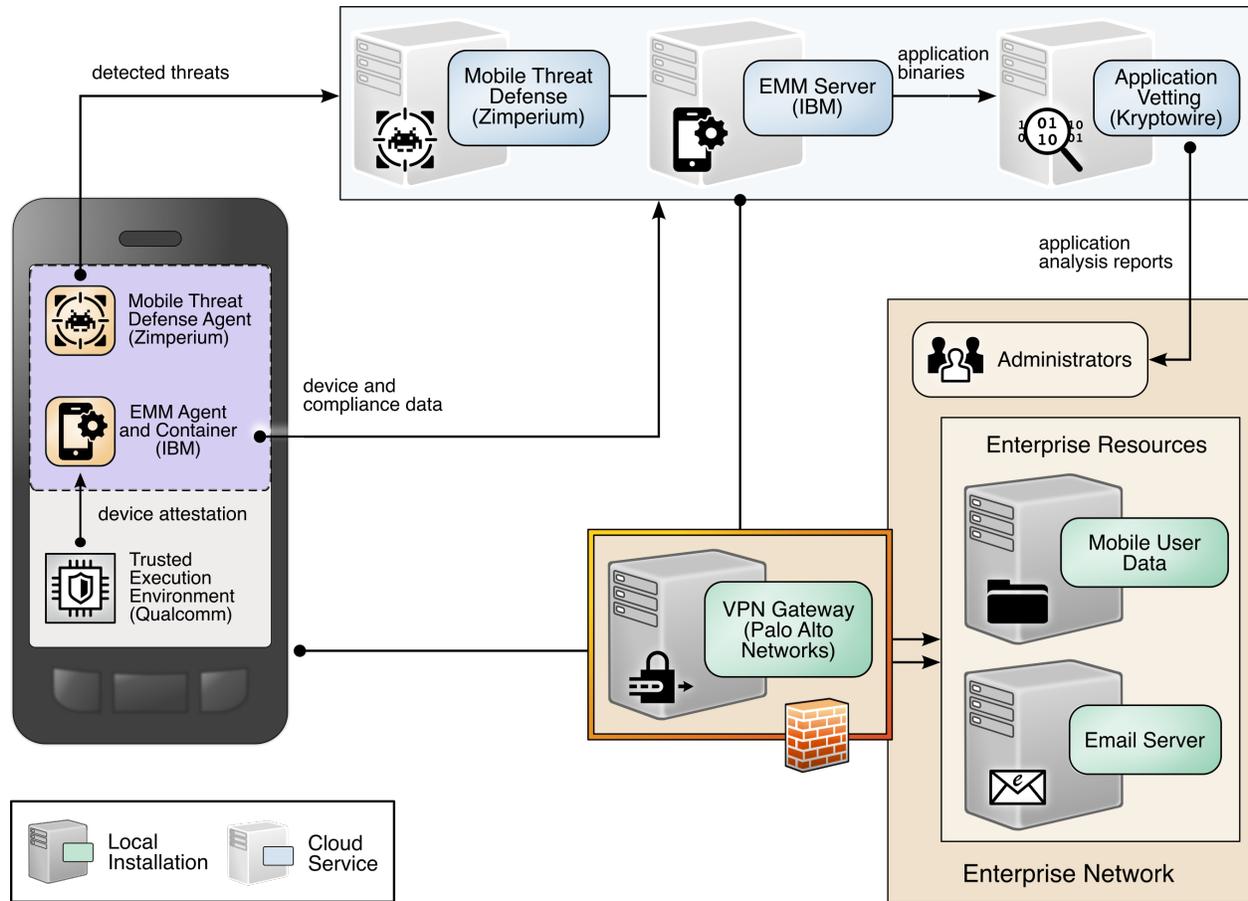
Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .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

320 Acronyms used in figures can be found in the Acronyms appendix.

321 1.4 Logical Architecture Summary

322 The graphic below shows the components of the build architecture and how they interact on a high
 323 level.

324 **Figure 1-1 High-Level Build Architecture**



325 **2 Product Installation Guides**

326 This section of the practice guide contains detailed instructions for installing and configuring all the
 327 products used to build an instance of the example solution.

328 This guide assumes that a basic active directory (AD) infrastructure has been configured. The domain
 329 controller (DC) is used to authenticate users when enrolling devices as well as when connecting to the
 330 virtual private network (VPN). In this implementation, the domain *enterprise.mds.local* was used.

331 **2.1 Network Device Enrollment Services Server**

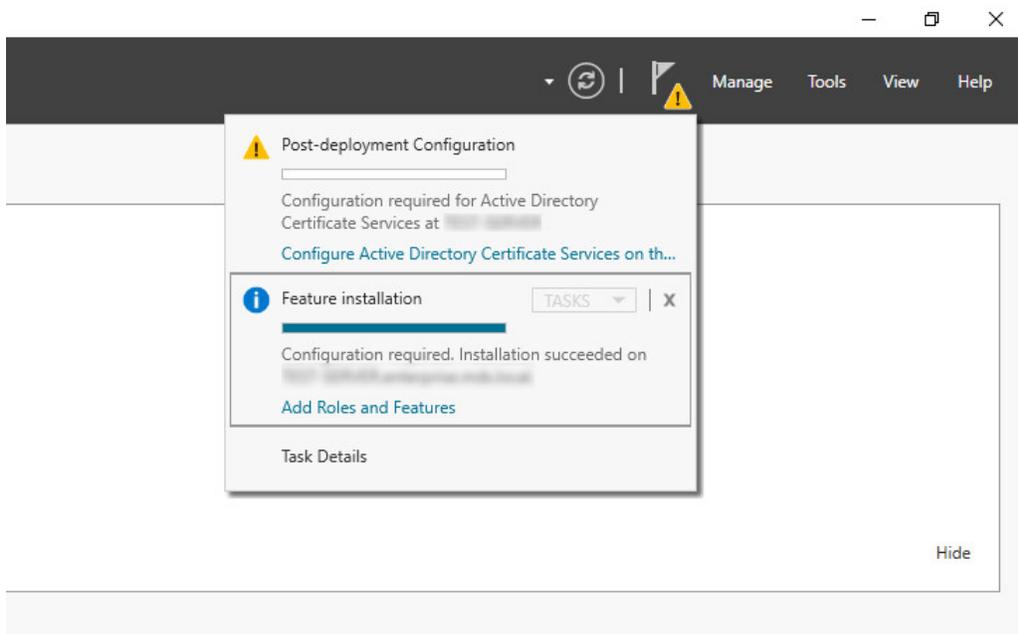
332 A Network Device Enrollment Service (NDES)/Simple Certificate Enrollment Protocol (SCEP) server was
 333 used to issue client certificates to new devices that were enrolled by using MaaS360. This guide assumes

334 that a basic AD and certificate authority (CA) are in place, containing a root and subordinate CA, and
335 that their certificates have been exported.

336 2.1.1 NDES Configuration

337 This section outlines configuration of an NDES that resides on its own server. Alternatively, the NDES can
338 be installed on the SUB-CA. This section assumes a new domain-attached Windows Server is running.

- 339 1. From the Server Manager, select **Manage > Add Roles and Features**.
- 340 1. Click **Next** three times until **Server Roles** is highlighted.
- 341 2. Check the box next to **Active Directory Certificate Services**.
- 342 3. Click **Next** three times until **Role Services** is highlighted.
- 343 4. Uncheck **Certification Authority**. Check **Network Device Enrollment Service**.
- 344 5. Click **Add Features** on the pop-up.
- 345 6. Click **Next** three times.
- 346 7. Click **Install**.
- 347 8. When installation completes, click the flag in the upper right-hand corner, and click **Configure**
348 **Active Directory Certificate Services**.

349 **Figure 2-1 Post-Deployment Configuration**

350 9. Specify the credentials of a Domain Administrator. Click **Next**.

351 Note: The domain administrator credentials are required only to configure the NDES. Once the service is
 352 configured, the service is executed as the NDES service account, which does not require domain
 353 administrator permissions, created in step 12 below.

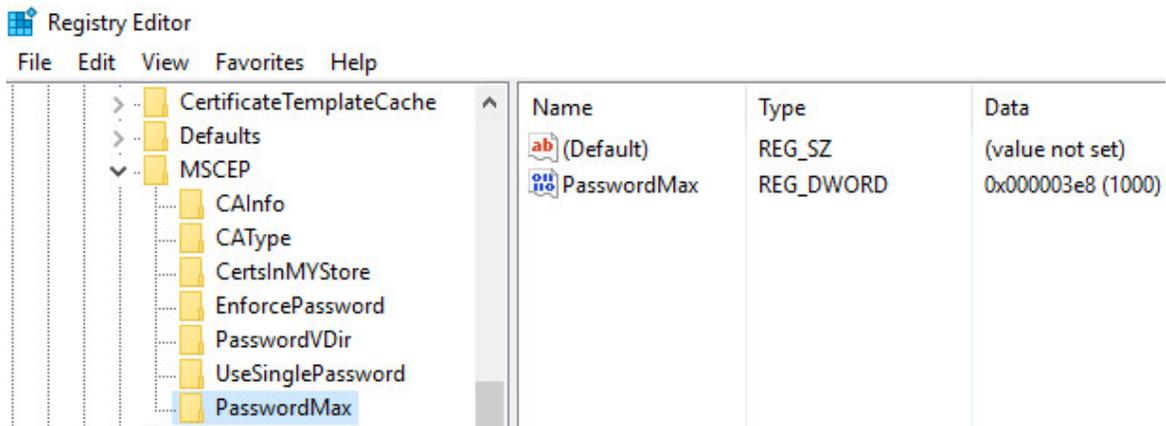
354 10. Check **Network Device Enrollment Service**. Click **Next**.

355 11. Configure an NDES service account by performing the following actions:

- 356 a. On the active directory server, open **Active Directory Users and Computers**.
- 357 b. Click **Users** and create a new user for the service. For this example, it will be named
 358 NDES. Be sure the password never expires.
- 359 c. On the NDES server, open **Edit local users and groups**.
- 360 d. Click **Groups**. Right-click **IIS_IUSRS**, click **Add to Group**, and click **Add**.
- 361 e. Search for the service account name—in this case, NDES. Click **Check Names**, then click
 362 **OK** if no errors were displayed.
- 363 f. Click **Apply** and click **OK**.
- 364 g. Close all windows except the NDES configuration window.

- 365 12. Click **Select** next to the box and enter the service account credentials. Click **Next**.
- 366 13. Because the NDES runs on its own server, we will target it at the SUB-CA. Select **Computer name**
367 and click **Select**. Type in the computer name—in this case, SUB-CA. Click **Check Names**, and if no
368 errors occurred, click **OK**.
- 369 14. Click **Next** three times.
- 370 15. Click **Configure**.
- 371 16. On the SUB-CA, open the Certification Authority application.
- 372 17. Expand the SUB-CA node, right-click on **Certificate Templates**, and click **Manage**.
- 373 18. Right-click on **IPSec (Offline Request)** and click **Duplicate Template**.
- 374 19. Under the **General** tab, set the template display name to **NDES**.
- 375 20. Under the **Security** tab, click **Add**.
- 376 21. Select the previously configured NDES service account.
- 377 22. Click **OK**. Ensure the NDES service account is highlighted, and check **Read** and **Enroll**.
- 378 23. Click **Apply**.
- 379 24. In the Certification Authority program, right-click on **Certificate Templates**, and select **New >**
380 **Certificate Template to Issue**.
- 381 25. Select the NDES template created in step 24.
- 382 26. Click **OK**.
- 383 27. On the NDES server, open the Registry Editor (`regedit`).
- 384 28. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography`.
- 385 29. Select the `MSCEP` key and update all entries besides (Default) to be **NDES**.
- 386 30. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP`.
- 387 31. Right-click on **MSCEP** and select **New > Key**. Name it **PasswordMax**.
- 388 32. Right-click on the newly created key and select **New > DWORD (32-bit) Value**.
- 389 33. Name it **PasswordMax** and give it a value of **0x00003e8**. This increases the NDES password
390 cache to 1,000 entries instead of the default 5. This value can be further adjusted based on
391 NDES demands.

392 Figure 2-2 PasswordMax Registry Configuration



393 **Note:** The **PasswordMax** key governs the maximum number of NDES passwords that can reside in the
 394 cache. A password is cached when a valid certificate request is received, and it is removed from the
 395 cache when the password is used or when 60 minutes have elapsed, whichever occurs first. If the
 396 **PasswordMax** key is not present, the default value of 5 is used.

397 34. In an elevated command prompt, execute `%windir%\system32\inetsrv\appcmd set config`
 398 `/section:requestFiltering /requestLimits.maxQueryString:8192` to increase the maxi-
 399 mum query string. This prevents requests longer than 2,048 bytes from being dropped.

400 35. Open the **Internet Information Services (IIS) Manager**.

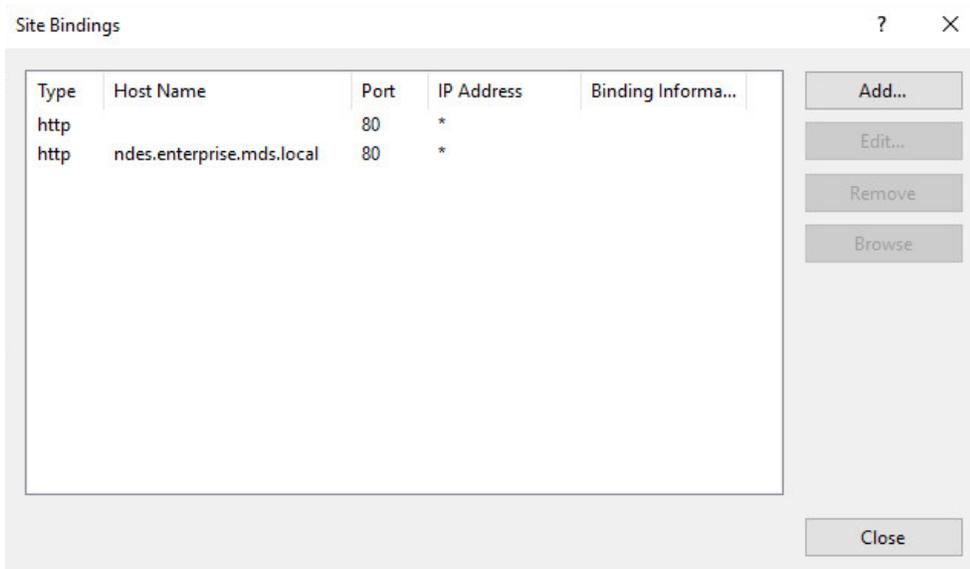
401 36. On the left, expand **NDES > Sites**, and select **Default Web Site**.

402 37. On the right, click **Bindings...**

403 38. Click **Add**.

404 39. Below **Host Name**, enter the host name of the server. For this implementation, *ndes.enter-*
 405 *prise.mds.local* was used.

406 40. Click **OK**.

407 **Figure 2-3 NDES Domain Bindings**

408

409 41. Click **Close** and close the IIS Manager.410 42. In an elevated command prompt, execute `iisreset`, or reboot the NDES server.411

2.2 International Business Machines MaaS360

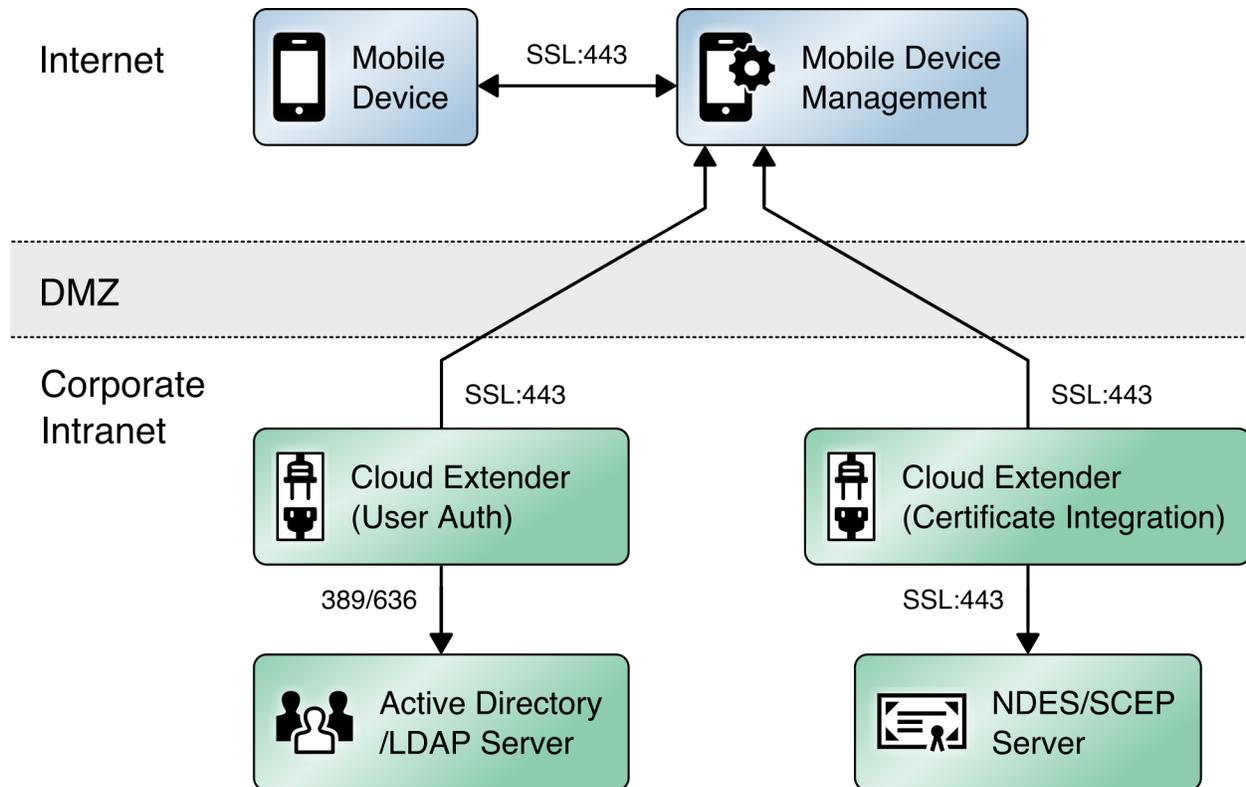
412 International Business Machines (IBM) contributed an instance of MaaS360
 413 (<https://www.ibm.com/products/maas360/unified-endpoint-management>) to deploy as the mobile
 414 device management (MDM) solution.

415

2.2.1 Cloud Extender

416 The IBM MaaS360 Cloud Extender is installed within the AD domain to provide AD and lightweight
 417 directory access protocol (LDAP) authentication methods for the MaaS360 web portal, as well as
 418 corporate VPN capabilities. The cloud extender architecture [1], as shown in [Figure 2-4](#), gives a visual
 419 overview of how information flows between the web portal and the MaaS360 Cloud Extender.

420 Figure 2-4 Cloud Extender Architecture

421 **2.2.1.1 Cloud Extender Download**

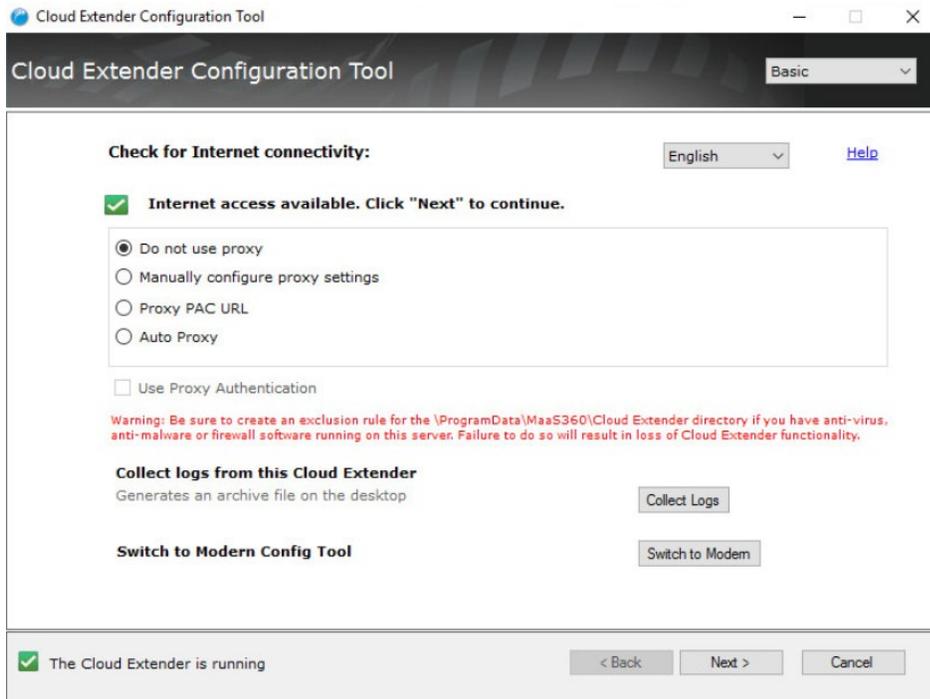
- 422 1. Log in to the MaaS360 web portal.
- 423 2. Click **Setup > Cloud Extender**.
- 424 3. Click the link that says **Click here to get your License Key**. The license key will be emailed to the
- 425 currently logged-in user's email address.
- 426 4. Click the link that says **Click here to download the Cloud Extender**. Save the binary.
- 427 5. Move the binary to a machine behind the corporate firewall that is always online. Recommendation: Install it while logged in as a domain user on a machine that is not the domain controller.
- 428
- 429 6. Install **.NET 3.5 Features** in the **Server Manager** on the machine where the MaaS360 Cloud Ex-
- 430 tender will run.

431 **2.2.1.2 Cloud Extender Active Directory Configuration**

- 432 1. On the target machine, run the installation binary.

- 433 2. Enter the license key when prompted.
- 434 3. Proceed through the setup until the Cloud Extender Configuration Utility opens.
- 435 4. If using the old cloud extender interface, click **Switch to Modern**.

436 **Figure 2-5 Old Cloud Extender Interface**



- 437 5. Enable the toggle below **User Authentication**.
- 438 6. Create a new authentication profile by entering the username, password, and domain of the
- 439 created service account.

440 Figure 2-6 Cloud Extender Service Account Details

HOME IMPORT EXPORT PROXY SETTINGS HELP

English (United States)

User Authentication

Allows users to enroll devices using corporate directory credentials

Start (Completed)

2 Service Account (Current)

3 Finish

Provide Service Account details

Service account should be:
 1. Domain User on Active Directory
 2. Local Administrator on this server

Username: MAAS360

Password: ●●●●●●

Domain: enterprise.mds.local

Enable Secure Authentication Mode

Back Next Save Cancel

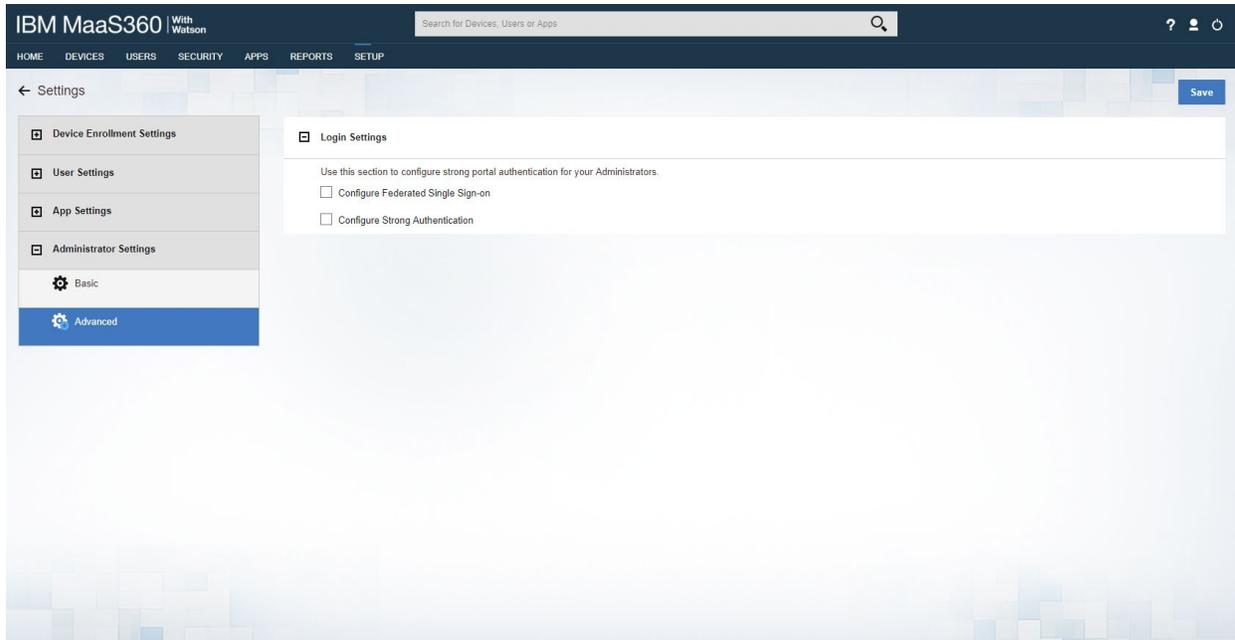
The Cloud Extender is running

- 441 7. Click **Next**.
- 442 8. (optional) Use the next page to test the active directory integration.
- 443 9. Click **Save**.
- 444 10. In MaaS360, navigate to **Setup > Cloud Extender**. Ensure that configuration information is displayed, indicating that the MaaS360 Cloud Extender is running.
- 445

446 *2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration*

- 447 1. Log in to the MaaS360 web portal as an administrator.
- 448 2. Go to **Setup > Settings**.
- 449 3. Expand **Administrator Settings** and click **Advanced**.

450 Figure 2-7 Administrator Settings



- 451 4. Select **Configure Federated Single Sign-on**.
- 452 5. Select **Authenticate against Corporate User Directory**.
- 453 6. Next to **Default Domain**, enter the active directory domain. In this implementation, *enterprise.mds.local* was used.
- 454
- 455 7. Check the box next to **Allow existing Administrators to use portal credentials as well**.
- 456 8. Check the box next to **Automatically create new Administrator accounts and update roles**
- 457 **based on user groups**.
- 458 9. Under **User Groups**, enter the distinguished name of the group(s) that should be allowed to log
- 459 in. In this implementation, CN=Domain Admins, CN=Users, DC=enterprise, DC=mds, DC=local
- 460 was used.
- 461 10. Next to the box, select **Administrator–Level 2**. This allows domain admins to log in as MaaS360
- 462 administrators.

463 **Figure 2-8 Administrator Configuration Options**

Allow existing Administrators to use portal credentials as well. ⓘ

 Note: Since the username for one or more administrator account is not the same as their Corporate email addresses, following additional setup is required.

1. Navigate to "Setup > Administrators" workflow.
2. Edit the administrator accounts and specify the Corporate Usernames for these accounts.

Automatically create new Administrator accounts and update roles based on User Groups

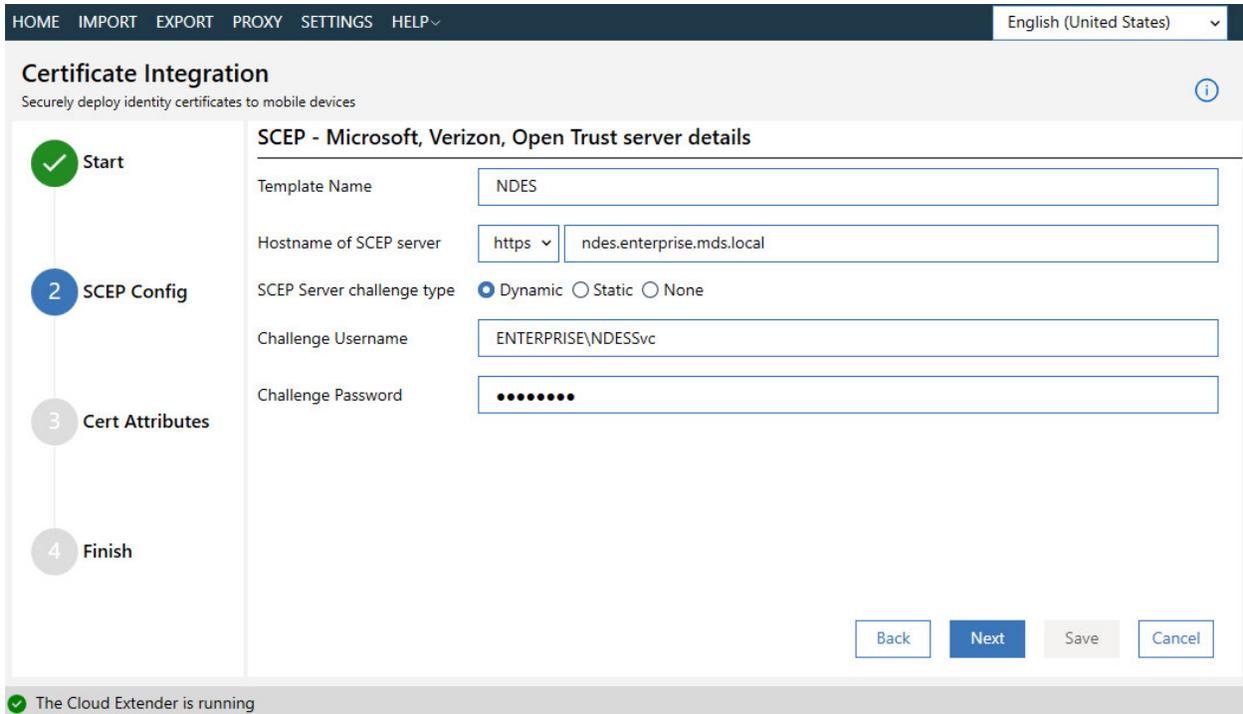
User Groups (Specify the Distinguished Name of the User Groups)

CN=Domain Admins,CN=Users,DC=enterj	Administrator - Level 2	⊖
	----Select Role----	⊕

464 11. Click **Save**.465 *2.2.1.4 Cloud Extender NDES Integration*466 To properly generate device certificates, MaaS360 must be integrated with the on-premises public key
467 infrastructure (PKI).

- 468 1. Log in to the server running the MaaS360 Cloud Extender.
- 469 2. Launch the Cloud Extender Configuration Tool.
- 470 3. Toggle the button below Certificate Integration.
- 471 4. Click **Add New Template**.
- 472 5. Ensure **Microsoft CA** and **Device Identity Certificates** are selected.
- 473 6. Click **Next**.
- 474 7. Enter **NDES** for the Template Name and SCEP Default Template.
- 475 8. Enter the uniform resource locator (URL) of the NDES server next to **SCEP Server**.
- 476 9. Enter credentials of a user with enroll permissions on the template for **Challenge Username** and
477 **Challenge Password**. For this demo implementation, we use the NDES service account.

478 Figure 2-9 Cloud Extender SCEP Configuration



479 10. Click **Next**.

480 11. (optional) Check the box next to **Cache certs on Cloud Extender** and specify a cache path on the
481 machine.

482 Figure 2-10 Cloud Extender Certificate Properties

HOME IMPORT EXPORT PROXY SETTINGS HELP ~ English (United States) ▾

Certificate Integration

Securely deploy identity certificates to mobile devices ⓘ

Certificate Properties

Subject Name ⓘ

Subject Alternate Name

Cache certs on Cloud Extender

Location of Certificate Cache

Back Next Save Cancel

✓ The Cloud Extender is running

483 12. Click **Next**.

484 13. (optional) Enter values for uname and email and generate a test certificate to test the configura-
485 tion.

486 14. Click **Save**.

487 Note: If a file access message appears, delete the file, and re-save the file.

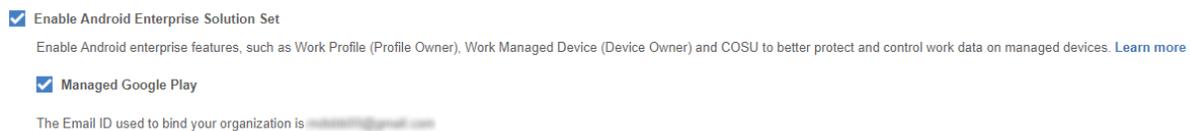
488 2.2.2 Android Enterprise Configuration

489 A Google account was used to provision Android Enterprise on the mobile devices. A managed domain
490 can be used, but in this use case it was not necessary. A managed domain is necessary only if the
491 corporation already has data stored in Google's cloud.

- 492 1. Create a Google account if you do not have one you wish to bind with.
- 493 2. From the MaaS360 portal, navigate to **Setup > Services**.
- 494 3. Click **Mobile Device Management**.
- 495 4. Check the box next to **Enable Android Enterprise Solution Set**.
- 496 5. Enter your password and click **Enable**.

- 497 6. Click **Mobile Device Management**.
- 498 7. Click the radio button next to **Enable via Managed Google Play Accounts (no G Suite)**.
- 499 8. Ensure all pop-up blockers are disabled. Click the link on the word **here**.
- 500 9. Enter your password and click **Enable**.
- 501 10. In the new page that opens, ensure you are signed into the Google account you wish to bind.
- 502 11. Click **Get started**.
- 503 12. Enter your business name and click **Next**.
- 504 13. If General Data Protection Regulation compliance is not required, scroll to the bottom, check the
- 505 **I agree** box, and click **Confirm**. If compliance is required, fill out the requested information first.
- 506 14. Click **Complete Registration**.
- 507 15. Confirm binding on the **Setup** page under **Mobile Device Management**. The settings should look
- 508 like Figure 2-11, where the blurred-out portion is the Google email address used to bind.

509 **Figure 2-11 Enterprise Binding Settings Confirmation**



510 2.2.3 iOS APNs Certificate Configuration

511 For the iOS Apple Push Notification services (APNs) certificate configuration, the build team followed the

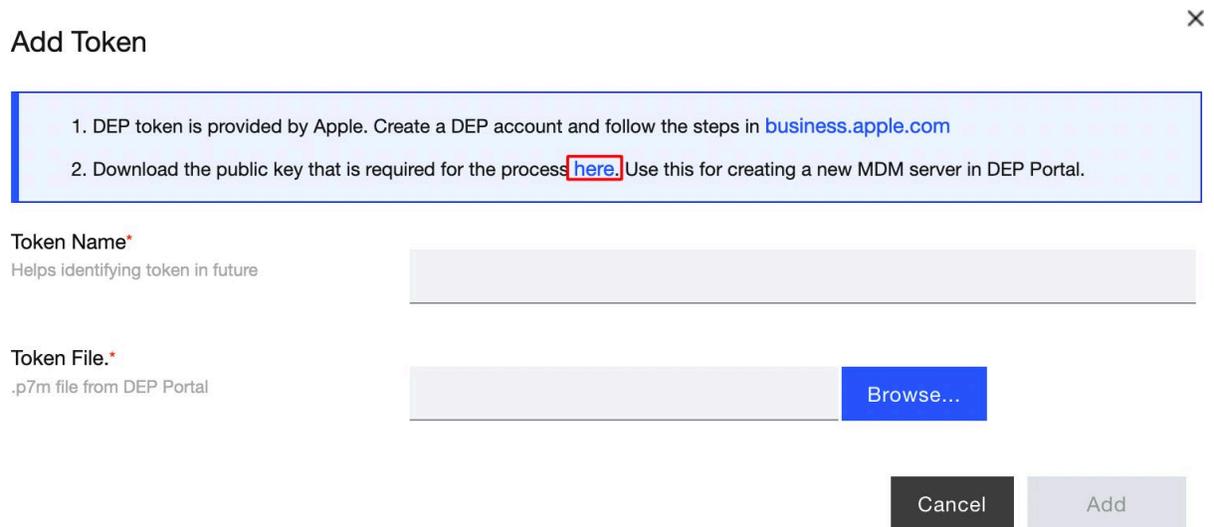
512 [IBM documentation](#).

513 2.2.4 Apple User Enrollment (UE) Configuration

514 2.2.4.1 Apple Business Manager (ABM) Configuration

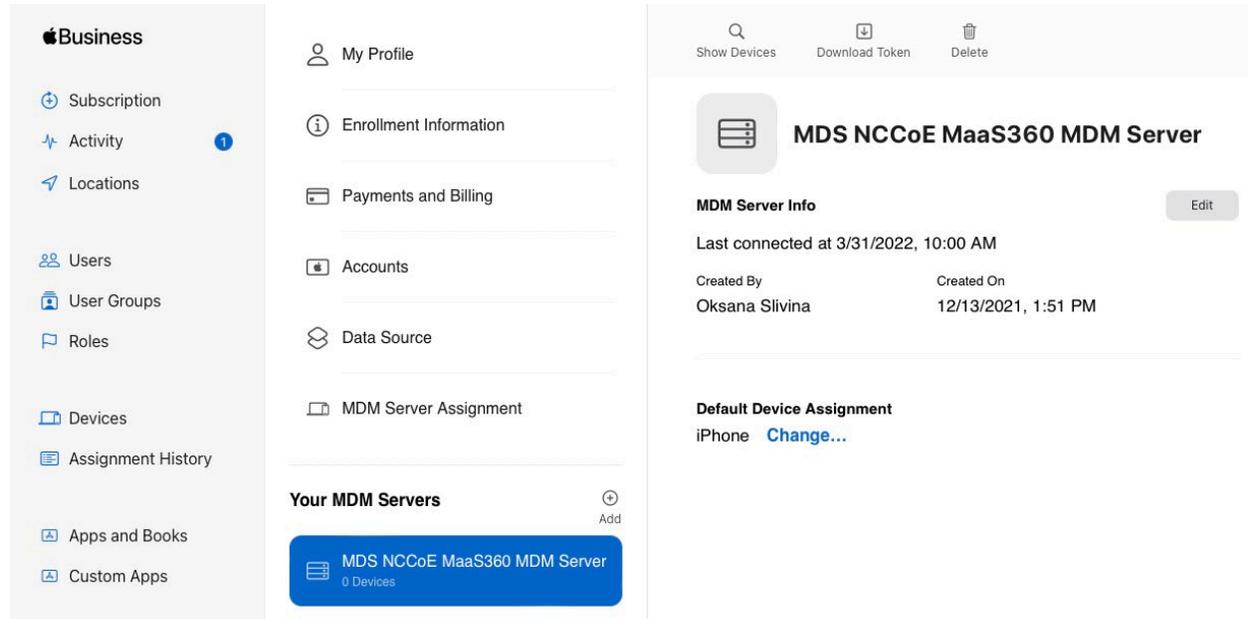
- 515 1. In MaaS360, navigate to **Setup > Settings > Enrollment Programs**, and click **Configure** next to *Apple*
- 516 *Device Enrollment Program*.
- 517 2. In the popup, click **Continue**.
- 518 3. Click **Tokens > Add Token**.
- 519 4. In the popup, give the token a name and click on the **here** link in step 2 of the popup to download the
- 520 public key file.

521 **Figure 2-12 Where to Click to Download the Public Key**



- 522 5. In Apple Business Manager, sign in with an administrator account.
- 523 6. Click the user’s name in the bottom left corner > **Settings**.
- 524 7. Click **Add** next to “Your MDM Servers” and enter a unique name for the server.
- 525 8. Upload the public key certificate file downloaded in step (4), then click **Save**.
- 526 9. Click **Download Token** to save the server token.

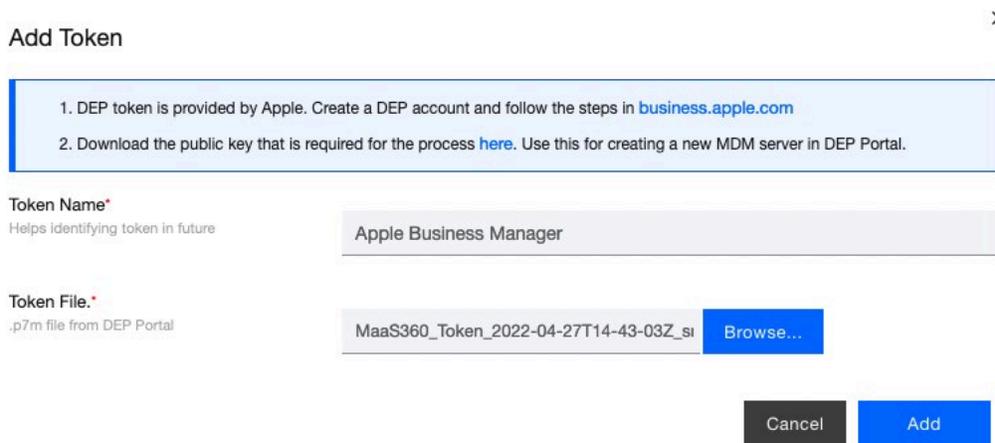
527 **Figure 2-13 MDM configuration in Apple Business Manager**



528
529 10. In MaaS360, click **Browse** and select the token downloaded in step (9).

530 11. Click **Add**.

531 **Figure 2-14 Creating the DEP token**



532
533 12. In Apple Business Manager, click the user’s name in the bottom left corner and click **Payments and**
534 **Billing**.

- 535 13. Under *Server Tokens*, click the token that corresponds to the Apple Business Manager tenant and save
 536 the token.
- 537 14. In MaaS360, navigate to **Apps > Catalogue**. Click **More > Apple VPP Licenses**.
- 538 15. Click **Add Token** and give the token a name. Click **Browse** and select the token file downloaded in step
 539 (13).
- 540 16. Click **Policies** and configure the VPP token policy based on organizational requirements.
- 541 17. Click **Distribution** and configure based on organizational requirements.
- 542 18. Click **Submit**.

543 **Figure 2-15 VPP token in MaaS360**

Token Name	Users	Country Na...	User Groups	Last Sync Time	Update Time	Expiry Date	Status	App Addition St...
VPP Token View Update Disable More...	0	United States	All Users		04/27/2022 13:15 EDT	04/26/2023 20:00 EDT	Active	NA

544 |< < 1 > >| [Jump To Page](#) Displaying 1 - 1 of 1 Records | Show 25 Records

545 **2.2.4.2 MaaS360 Configuration**

- 546 1. In the MaaS360 web portal, navigate to **Setup > Settings**.
- 547 2. Navigate to **Device Enrollment Settings > Advanced**.
- 548 3. Under *Advanced Management for Apple Devices > Select default enrollment mode for managing*
 549 *employee owned (BYOD) devices*, select the radio button next to **User enrollment mode**.
- 550 4. Scroll to the top of the page and click **Save**.

551 **Figure 2-16 iOS Enrollment Configuration**

Select default enrollment mode for managing employee owned (BYOD) devices.

Applicable for self enrollment scenarios (URL: <https://m.dm/...>)

Managed mode - Manage entire device. ⓘ

User enrollment mode - Manage only corporate resources. ⓘ

When user enrollment mode is selected, MaaS360 currently does not support macOS enrollment into MDM(Managed Mode) as employee owned devices. Alternatively, the macOS devices can be enrolled as corporate owned.

552

553 **2.2.5 Android Configuration**

554 **2.2.5.1 Policy Configuration**

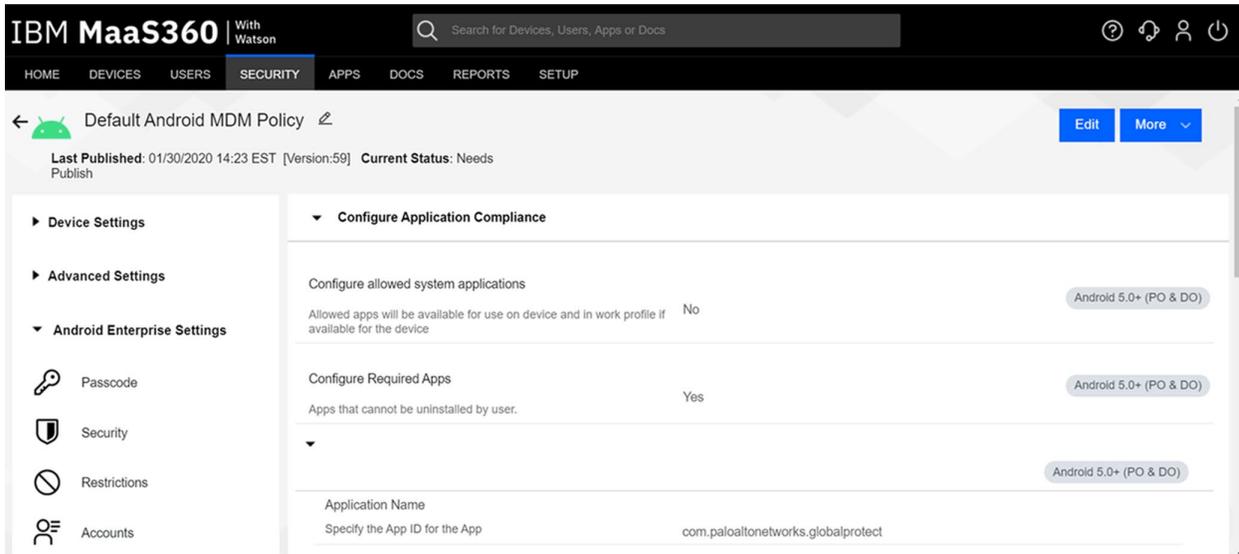
- 555 1. Navigate to **Security > Policies**.
- 556 2. Click the appropriate deployed Android policy.

- 557 3. Click **Edit**.
- 558 4. Navigate to **Android Enterprise Settings > Passcode**.
- 559 5. Check the box next to **Configure Passcode Policy**.
- 560 6. Configure the passcode settings based on corporate requirements.
- 561 7. Navigate to **Android Enterprise Settings > Restrictions**.
- 562 8. Check the box next to **Configure Restrictions**.
- 563 9. Configure restrictions based on corporate requirements.
- 564 10. Click **Save**.

565 *2.2.5.2 VPN Configuration*

- 566 1. Navigate to **Security > Policies**.
- 567 2. Click the currently deployed Android device policy.
- 568 3. Click **Edit**.
- 569 4. Navigate to **Android Enterprise Settings > Certificates**.
- 570 5. Check the box next to **Configure CA Certificates**.
- 571 6. Click **Add New**.
- 572 7. Give the certificate a name, such as Internal Root.
- 573 8. Click **Browse** and navigate to the exported root CA certificate from earlier in the document.
- 574 9. Click **Save**.
- 575 10. Select **Internal Root** from the drop-down next to **CA Certificate**.
- 576 11. Click the + icon on the far right.
- 577 12. Repeat steps 6–10 with the internal sub-CA certificate.
- 578 13. Check the box next to **Configure Identity Certificates**.
- 579 14. From the drop-down next to **Identity Certificate**, select the profile that matches the name con-
580 figured on the MaaS360 Cloud Extender—for this example, **NDES**.
- 581 15. Click **Save and Publish** and follow the prompts to publish the updated policy. Click **Apps**.
- 582 16. Click **Add > Android > Google Play App**.

- 583 17. Select the radio button next to **Add via Public Google Play Store**.
- 584 18. Search for **GlobalProtect**.
- 585 19. Select the matching result.
- 586 20. Click **I Agree** when prompted to accept the permissions.
- 587 21. Check the three boxes next to **Remove App on**.
- 588 22. Check the box next to **Instant Install**.
- 589 23. Select **All Devices** next to **Distribute to**.
- 590 24. Click **Add**.
- 591 25. Next to the newly added GlobalProtect application, select **More > Edit App Configurations**.
- 592 26. Click **Check for Settings**.
- 593 27. Next to **Portal**, enter the GlobalProtect portal address. In this implementation,
594 *vpn.ent.mdse.nccoe.org* was used.
- 595 28. Next to **Username**, enter **%username%**.
- 596 29. Next to **Connection Method**, enter **user-logon**. (Note: This will enable an always-on VPN con-
597 nection for the work profile. The user will always see the VPN key icon, but it will apply only to
598 applications contained within the work profile.)
- 599 30. Click **Save** and follow the prompts to update the application configuration.
- 600 31. Navigate to **Security > Policies**.
- 601 32. Click the used Android policy.
- 602 33. Select **Android Enterprise Settings > App Compliance**.
- 603 34. Click **Edit**.
- 604 35. Click the + on the row below **Configure Required Apps**.
- 605 36. Enter the App Name, **GlobalProtect**.
- 606 37. Enter the App ID, **com.paloaltonetworks.globalprotect**.
- 607 38. Click **Save And Publish** and follow the prompts to publish the policy.

608 **Figure 2-17 Android GlobalProtect Application Compliance**609 **2.2.6 iOS Configuration**610 **2.2.6.1 Policy Configuration**

- 611 1. Navigate to **Security > Policies**.
- 612 2. Click the deployed iOS policy.
- 613 3. Click **Edit**.
- 614 4. Check the box next to **Configure Passcode Policy**.
- 615 5. Check the box next to **Enforce Passcode on Mobile Device**.
- 616 6. Configure the rest of the displayed options based on corporate requirements.
- 617 7. Click **Restrictions**.
- 618 8. Check the box next to **Configure Device Restrictions**.
- 619 9. Configure restrictions based on corporate requirements.
- 620 10. Click **Save**.

621 **2.2.6.2 VPN Configuration**

- 622 1. Click **Device Settings > VPN**.

- 623 2. Click **Edit**.
- 624 3. Next to **Configure for Type**, select **Custom SSL**.
- 625 4. Enter a name next to **VPN Connection Name**. In this sample implementation, **Great Seneca VPN**
626 was used.
- 627 5. Next to **Identifier**, enter **com.paloaltonetworks.globalprotect.vpn**.
- 628 6. Next to **Host name of the VPN Server**, enter the URL of the VPN endpoint without http or https.
- 629 7. Next to **VPN User Account**, enter **%username%**.
- 630 8. Next to **User Authentication Type**, select **Certificate**.
- 631 9. Next to **Identity Certificate**, select the name of the certificate profile created during the NDES
632 configuration steps. In this sample implementation, **NDES** was used.
- 633 10. Next to **Custom Data 1**, enter **allowPortalProfile=0**
- 634 11. Next to **Custom Data 2**, enter **fromAspen=1**
- 635 12. Next to **Apps to use this VPN**, enter the application identifications (IDs) of applications to go
636 through the VPN. This will be the applications deployed to the devices as work applications.
- 637 13. Next to **Provider Type**, select **Packet Tunnel**.
- 638 14. In Apple Business Manager, click **Apps and Books**.
- 639 15. Search for *GlobalProtect*.
- 640 16. Select the non-legacy search result.
- 641 17. Select the business's location and enter the desired number of licenses (installations) and click
642 **Get**.
- 643 18. In MaaS360, navigate to **Apps > Catalog**.
- 644 19. Navigate to **More > Apple VPP Licenses**.
- 645 20. In the VPP line, select **More > Sync**. Follow the confirmation pop-ups to confirm the sync with
646 Apple Business Manager.
- 647 21. Navigate to **Apps > Catalog**.
- 648 22. Click **Add > iOS > iTunes App Store App**.
- 649 23. Search for **GlobalProtect**.

- 650 24. Select the non-Legacy version.
- 651 25. Click **Policies and Distribution**.
- 652 26. Check all three boxes next to **Remove App on**.
- 653 27. Select **All Devices** next to **Distribute to**.
- 654 28. Check the box next to **Instant Install**.
- 655 29. Click **Add**.
- 656 30. Navigate to **Security > Policies**.
- 657 31. Click the used iOS policy.
- 658 32. Click **Application Compliance**.
- 659 33. Click **Edit**.
- 660 34. Click the + next to the first row under **Configure Required Applications**.
- 661 35. Search for **GlobalProtect**.
- 662 36. Select the **non-Legacy** result.
- 663 37. Navigate to **Advanced Settings > Certificate Credentials**.
- 664 38. Check the box next to **Configure Credentials for Adding Certificates on the Device**.
- 665 39. Click **Add New**.
- 666 40. Give the certificate a name, such as Internal Root.
- 667 41. Click **Browse** and navigate to the exported root CA certificate from earlier in the document.
- 668 42. Click **Save**.
- 669 43. Select **Internal Root** from the drop-down next to **CA Certificate**.
- 670 44. Click the + icon on the far right.
- 671 45. Repeat steps 33–35 with the internal sub-CA certificate.
- 672 46. From the drop-down next to **Identity Certificate**, select the profile that matches the name con-
673 figured on the MaaS360 Cloud Extender—for this example, **NDES**.
- 674 47. Click **Save And Publish** and follow the prompts to publish the policy.

675 2.3 Zimperium

676 Zimperium was used as a mobile threat defense service via a MaaS360 integration.

677 Note: For Zimperium automatic enrollment to function properly, users **must** have an email address
678 associated with their MaaS360 user account.

679 2.3.1 Zimperium and MaaS360 Integration

680 This section assumes that IBM has provisioned an application programming interface (API) key for
681 Zimperium within MaaS360.

- 682 1. Log in to the zConsole.
- 683 2. Navigate to **Manage > MDM**.
- 684 3. Select **Add MDM > MaaS360**.
- 685 4. Fill out the MDM URL, MDM username, MDM password, and API key.
- 686 5. Note: For the MDM URL, append the account ID to the end. For example, if the account ID is
687 12345, the MDM URL would be <https://services.fiberlink.com/12345>.
- 688 6. Check the box next to **Sync users**.

689 Figure 2-18 Zimperium MaaS360 Integration Configuration

Edit MDM

Step 1 Choose MDM Provider Step 2 Setup IBM MaaS360 Step 3 Finish

URL
Specify URL for this MDM provider.

Username
Specify username for this MDM provider.

Password
Specify password for this MDM provider.

MDM Name
Specify a unique name for this MDM provider.

Sync users
Specify if this MDM provider should synchronise users.

Set synced users password
If you do not specify a password, a default value will be used

Synced users password
Specify the password for users synced from the MDM

Mask Imported User Information
By enabling this option, personally identifiable information will be masked (first name, last name and email) from the zConsole

API key
Specify API KEY for this MDM provider.

Send Device Activation email via zConsole for iOS Devices
By enabling this option, zConsole will send an activation email to a user for each iOS device which is synced from the MDM

Send Device Activation email via zConsole for Android Devices
By enabling this option, zConsole will send an activation email to a user for each Android device which is synced from the MDM

Next

- 690 7. Click **Next**.
- 691 8. Select the MaaS360 groups to synchronize with Zimperium. In this case, **All Devices** was se-
- 692 lected.
- 693 9. Click **Finish**. Click **Sync Now** to synchronize all current MaaS360 users and devices.

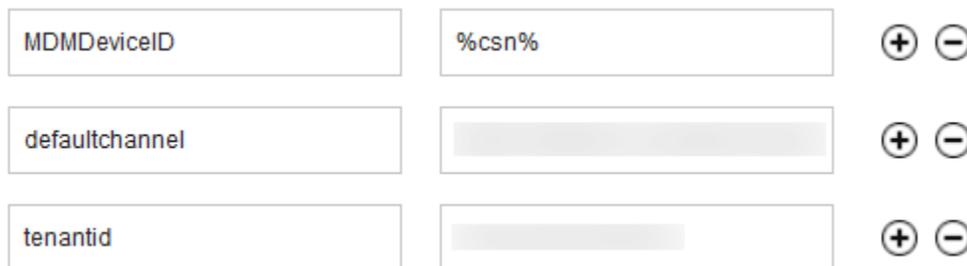
694 2.3.2 Automatic Device Activation

695 Note: This requires contacting Zimperium support to get required application configuration values.

- 696 1. In Apple Business Manager, click **Apps and Books**.
- 697 2. Search for *Zimperium zIPS*.

- 698 3. Select the non-legacy search result.
- 699 4. Select the business’s location and enter the desired number of licenses (installations) and click
700 **Get**.
- 701 5. In MaaS360, navigate to **Apps > Catalog**.
- 702 6. Navigate to **More > Apple VPP Licenses**.
- 703 7. In the VPP line, select **More > Sync**. Follow the confirmation pop-ups to confirm the sync with
704 Apple Business Manager.
- 705 8. Click **Apps** on the navigation bar.
- 706 9. Click **Add > iOS > iTunes App Store App**.
- 707 10. Search for **Zimperium zIPS**. Click the result that matches the name.
- 708 11. Click **Policies and Distribution**.
- 709 12. Check the three checkboxes next to **Remove App on**.
- 710 13. Next to **Distribute to**, select **All Devices**.
- 711 14. Click **Configuration**.
- 712 15. Set App Config Source to **Key/Value**.
- 713 16. The configuration requires three parameters: uuid, defaultchannel, and tenantid. uuid can be
714 set to **%csn%**, but defaultchannel and tenantid must come from Zimperium support.

715 **Figure 2-19 Zimperium zIPS iOS Configuration**



- 716 17. Click **Add**.
- 717 18. Click **Add > Android > Google Play App**.
- 718 19. Select the radio button next to **Add via Public Google Play Store**.

- 719 20. Search for **Zimperium Mobile IPS (zIPS)**.
- 720 21. Click the matching result.
- 721 22. Click **I Agree** when prompted to accept permissions.
- 722 23. Click **Policies and Distribution**.
- 723 24. Check all three boxes next to **Remove App on**.
- 724 25. Check **Instant Install**.
- 725 26. Select **All Devices** next to **Distribute to**.
- 726 27. Click **App Configurations**.
- 727 28. Check **Configure App Settings**.
- 728 29. Enter the values provided by Zimperium next to **Default Acceptor** and **Tenant**.
- 729 30. Next to **MDM Device ID**, insert **%deviceid%**.
- 730 31. Adjust any other configuration parameters as appropriate for your deployment scenario.

731 **Figure 2-20 Zimperium zIPS Android Configuration**

Default Acceptor:	<input type="text"/>
Tenant:	<input type="text"/>
UUID:	<input type="text"/>
Display EULA:	<input type="text" value="No"/> ▼
Tracking ID 1:	<input type="text"/>
Tracking ID 2:	<input type="text"/>
MDM Device ID:	<input type="text" value="%deviceid%"/>

- 732 32. Click **Add**.

733 2.3.3 Enforce Application Compliance

734 From the IBM MaaS360 web portal:

- 735 1. Navigate to **Security > Policies**.
- 736 2. Select the default Android policy.
- 737 3. Navigate to **Android Enterprise Settings > App Compliance**.
- 738 4. Click **Edit**.
- 739 5. Check the box next to **Configure Required Apps** if not checked already. If it is, click the + icon.
- 740 6. Enter **com.zimperium.zips** as the App ID.
- 741 7. Click **Save And Publish**. This will prevent the user from uninstalling zIPS once it is installed.
- 742 8. Navigate to **Security > Policies**.
- 743 9. Select the default iOS policy.
- 744 10. Click **Application Compliance**.
- 745 11. Click **Edit**.
- 746 12. Check the box next to **Configure Required Applications** if not checked already. If it is, click the +
- 747 icon.
- 748 13. Enter **Zimperium zIPS** for the Application Name.
- 749 14. Click **Save And Publish** and follow the prompts to publish the policy.

750 2.3.4 MaaS360 Risk Posture Alerts

- 751 1. From the MaaS360 home screen, click the + button that says **Add Alert**.

752 **Figure 2-21 Add Alert Button**



- 753 2. Next to **Available for** select **All Administrators**.
- 754 3. For Name, enter **Zimperium Risk Posture Elevated**.
- 755 4. Under **Condition 1**, select **Custom Attributes** for the Category.

- 756 5. Select **zimperium_risk_posture** for Attribute.
- 757 6. Select **Equal To** for Criteria.
- 758 7. For Value, select **Elevated** for the count of risk posture elevated devices or **Critical** for risk posture critical devices.
- 759

760 **Figure 2-22 Zimperium Risk Posture Alert Configuration**

The screenshot shows the 'Add Alert' configuration window. At the top right, it is set to be 'Available for' 'All Administrators'. The 'Name & Description' section contains the name 'Zimperium Risk Posture E', a description 'Description: E.g. 'of my devices are jailbroken'', and a category of 'Security'. The 'Advanced Search' section includes three radio buttons for '1. Search for' (Active Devices is selected), checkboxes for '2. With Device Type(s)' (Smartphones and Tablets are checked), a dropdown for '3. Last Reported' (Last 7 Days), and a dropdown for '4. Search Criteria' (All Conditions (AND)). Below this, 'Condition 1' is configured with 'Custom Attributes', 'zimperium_risk_posture', 'Equal To', and 'Elevated'. 'Condition 2' is currently empty with placeholder text: 'Select Category', 'Select Attribute', 'Select Criteria', and 'Enter Text'.

- 761 8. Click **Update**.

762 2.4 Palo Alto Networks Virtual Firewall

763 Palo Alto Networks contributed an instance of its VM-100 series firewall for use on the project.

764 2.4.1 Network Configuration

- 765 1. Ensure that all Ethernet cables are connected or assigned to the virtual machine and that the
- 766 management web user interface is accessible. Setup will require four Ethernet connections: one
- 767 for management, one for wide area network (WAN), one for local area network, and one for the
- 768 demilitarized zone (DMZ).
- 769 2. Reboot the machine if cables were attached while running.
- 770 3. Navigate to **Network > Interfaces > Ethernet**.
- 771 4. Click **ethernet1/1** and set the Interface Type to be **Layer3**.
- 772 5. Click **IPv4**, ensure that **Static** is selected under Type, and click **Add** to add a new static address.

- 773 6. If the appropriate address does not exist yet, click **New Address** at the bottom of the prompt.
- 774 7. Once the appropriate interfaces are configured, commit the changes. The Link State icon should
775 turn green for the configured interfaces. The commit dialogue will warn about unconfigured
776 zones. That is an expected dialogue warning.
- 777 8. Navigate to **Network > Zones**.
- 778 9. Click **Add**. Give the zone an appropriate name, set the Type to **Layer3**, and assign it an interface.
- 779 10. Commit the changes.
- 780 11. Navigate to **Network > Virtual Routers**.
- 781 12. Click **Add**.
- 782 13. Give the router an appropriate name and add the internal and external interfaces.
- 783 14. Click **Static Routes > Add**. Give the static route an appropriate name, e.g., WAN. Set the destina-
784 tion to be **0.0.0.0/0**, set the interface to be the WAN interface, and set the next hop internet
785 protocol (IP) address to be the upstream gateway's IP address.
- 786 15. (optional) Delete the default router by clicking the checkbox next to it and clicking **Delete** at the
787 bottom of the page.
- 788 16. Commit the changes. The commit window should not display any more warnings.
- 789 17. Navigate to **Network > DNS Proxy**.
- 790 18. Click **Add**.
- 791 19. Give the proxy an appropriate name. Under **Primary**, enter the primary domain name system
792 (DNS) IP address.
- 793 20. (optional) Enter the secondary DNS IP address.
- 794 21. Add the interfaces under **Interface**. Click **OK**.

795 Figure 2-23 DNS Proxy Object Configuration

DNS Proxy

Enable

Name: Enterprise_DNS_Proxy

Inheritance Source: None

Primary: 10.8.1.1

Secondary: 192.168.8.10

Interface

- ethernet1/1
- ethernet1/2
- ethernet1/3

Static Entries

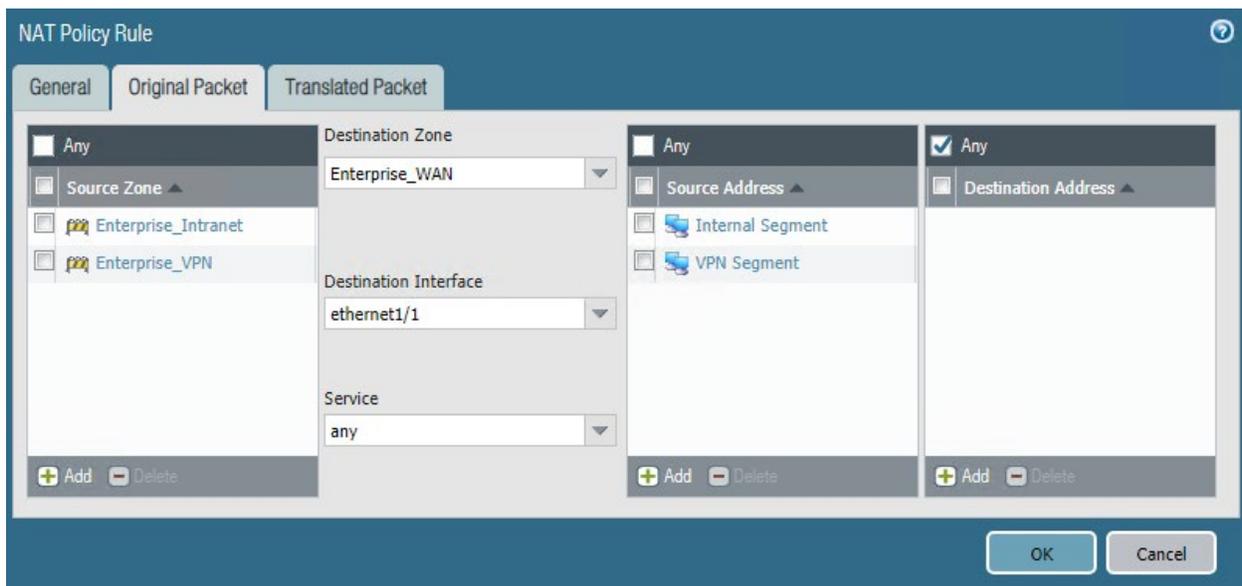
Name	Cacheable	Domain Name	Primary	Secondary
0 items				

OK Cancel

- 796 22. Navigate to **Device > Services**.
- 797 23. Click the **gear** in the top-right corner of the Services panel.
- 798 24. Under **DNS settings**, click the radio button next to **DNS Proxy Object**. Select the created DNS
- 799 proxy object from the drop-down.
- 800 25. Click **OK** and commit the changes. This is where static DNS entries will be added in the future.
- 801 26. Navigate to **Objects > Addresses**.
- 802 27. For each device on the network, click **Add**. Give the device an appropriate name, enter an op-
- 803 tional description, and enter the IP address.
- 804 28. Click **OK**.
- 805 29. Once all devices are added, commit the changes.
- 806 30. Navigate to **Policies > NAT**.
- 807 31. Click **Add**.

- 808 32. Give the network address translation rule a meaningful name, such as External Internet Access.
- 809 33. Click **Original Packet**.
- 810 34. Click **Add** and add the zone representing the intranet—in this case, **Enterprise_Intranet**.
- 811 35. Repeat step 34 for the secure sockets layer (SSL) VPN zone.
- 812 36. Under **Source Address**, click **Add**.
- 813 37. Enter the subnet corresponding to the intranet segment.
- 814 38. Repeat step 37 for the SSL VPN segment.
- 815 39. Click **Translated Packet**. Set the translation type to **Dynamic IP and Port**. Set Address Type to be
- 816 **Interface Address**. Set Interface to be the WAN interface and set the IP address to be the WAN
- 817 IP of the firewall.
- 818 40. Click **OK** and commit the changes.

819 **Figure 2-24 Original Packet Network Address Translation Configuration**



820 2.4.2 Demilitarized Zone Configuration

- 821 1. Navigate to **Network > Interfaces**.
- 822 2. Click the interface that has the DMZ connection.

- 823 3. Add a comment, set the Interface Type to **Layer3**, and assign it to the virtual router created ear-
824 lier.
- 825 4. Click **IPv4 > Add > New Address**. Assign it an IP block and give it a meaningful name. Click **OK**.
- 826 5. Navigate to **Network > Zones**.
- 827 6. Click **Add**. Give it a meaningful name, such as Enterprise_DMZ.
- 828 7. Set the Type to **Layer3** and assign it the new interface that was configured—in this case, ether-
829 net1/3.
- 830 8. Click **OK**.
- 831 9. Navigate to **Network > DNS Proxy**. Click **Add** under **Interface** and add the newly created inter-
832 face. Click **OK**.
- 833 10. Commit the changes.
- 834 11. Navigate to **Network > Interfaces**, and the configured interfaces should be green.

835 2.4.3 Firewall Configuration

- 836 1. Navigate to **Policies > Security**.
- 837 2. Click **Add**.
- 838 3. Give the rule a meaningful name, such as Intranet Outbound.
- 839 4. Click **Source**. Click **Add** under **Source Zone** and set the source zone to be the internal network.
- 840 5. Click **Destination**. Click **Add** under **Destination Zone** and set the destination zone to be the WAN
841 zone.
- 842 6. Click **Service/URL Category**. Under **Service**, click **Add**, and add **service-dns**. Do the same for ser-
843 vice-http and service-https.
- 844 7. Click **OK**.
- 845 8. Click **Add**.
- 846 9. Click **Destination**. Add the IP address of the Simple Mail Transfer Protocol (SMTP) server.
- 847 10. Click **Application**. Click **Add**.
- 848 11. Search for **smtp**. Select it.
- 849 12. Click **OK**.

850 13. Commit the changes.

851 14. Internal hosts should now be able to communicate on the internet.

852 2.4.4 Certificate Configuration

853 1. Navigate to **Device > Certificate Management > Certificate Profile**.

854 2. Click **Add**.

855 3. Give the profile a meaningful name, such as Enterprise_Certificate_Profile.

856 4. Select **Subject** under **Username Field**.

857 5. Select the radio button next to **Principal Name**.

858 6. Enter the domain under **User Domain**—in this case, enterprise.

859 7. Click **Add** under **CA Certificates**. Select the **internal root CA certificate**.

860 8. Click **Add** under **CA Certificates**. Select the **internal sub-CA certificate**. (Note: The entire certifi-
861 cate chain must be included in the certificate profile.)

862 9. Click **OK**.

863 10. Commit the changes.

864 **Figure 2-25 Certificate Profile**

Name: Enterprise_Certificate_Profile
 Username Field: Subject (dropdown) | common-name
 User Domain: enterprise

<input type="checkbox"/>	Name	Default OCSF URL	OCSF Verify Certificate
<input type="checkbox"/>	Internal Root		
<input type="checkbox"/>	Internal Sub		

Add Delete

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

Use CRL CRL Receive Timeout (sec) 5
 Use OCSP OCSF Receive Timeout (sec) 5
OCSF takes precedence over CRL Certificate Status Timeout (sec) 5

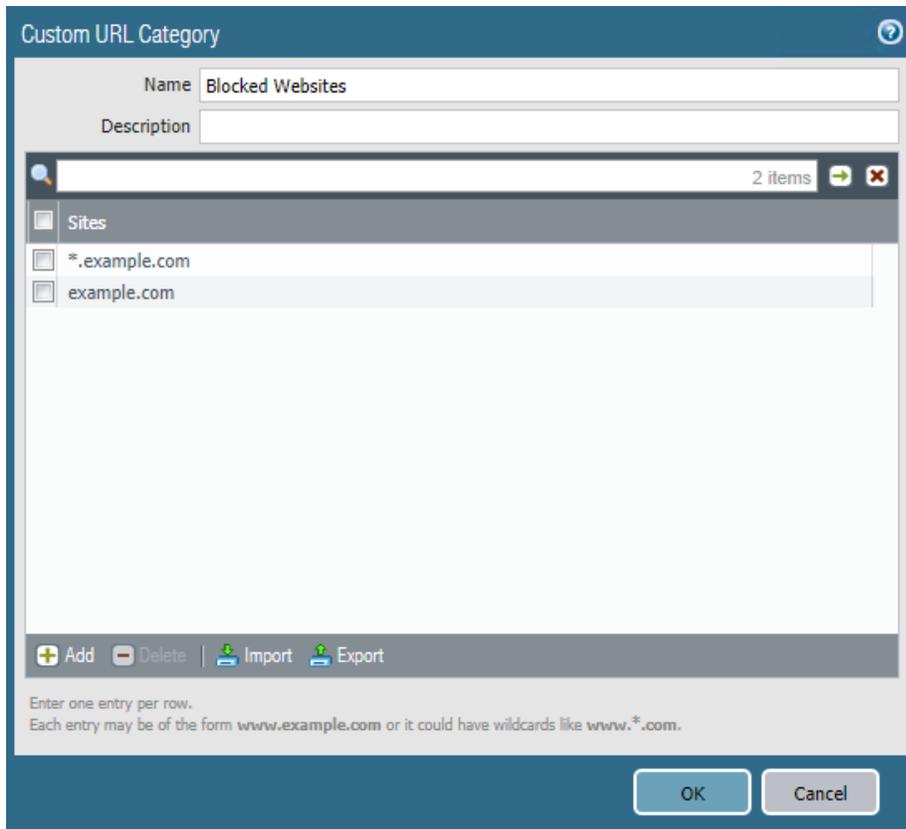
Block session if certificate status is unknown
 Block session if certificate status cannot be retrieved within timeout
 Block session if the certificate was not issued to the authenticating device
 Block sessions with expired certificates

OK Cancel

865 **2.4.5 Website Filtering Configuration**866 **2.4.5.1 Configure Basic Website Blocking**

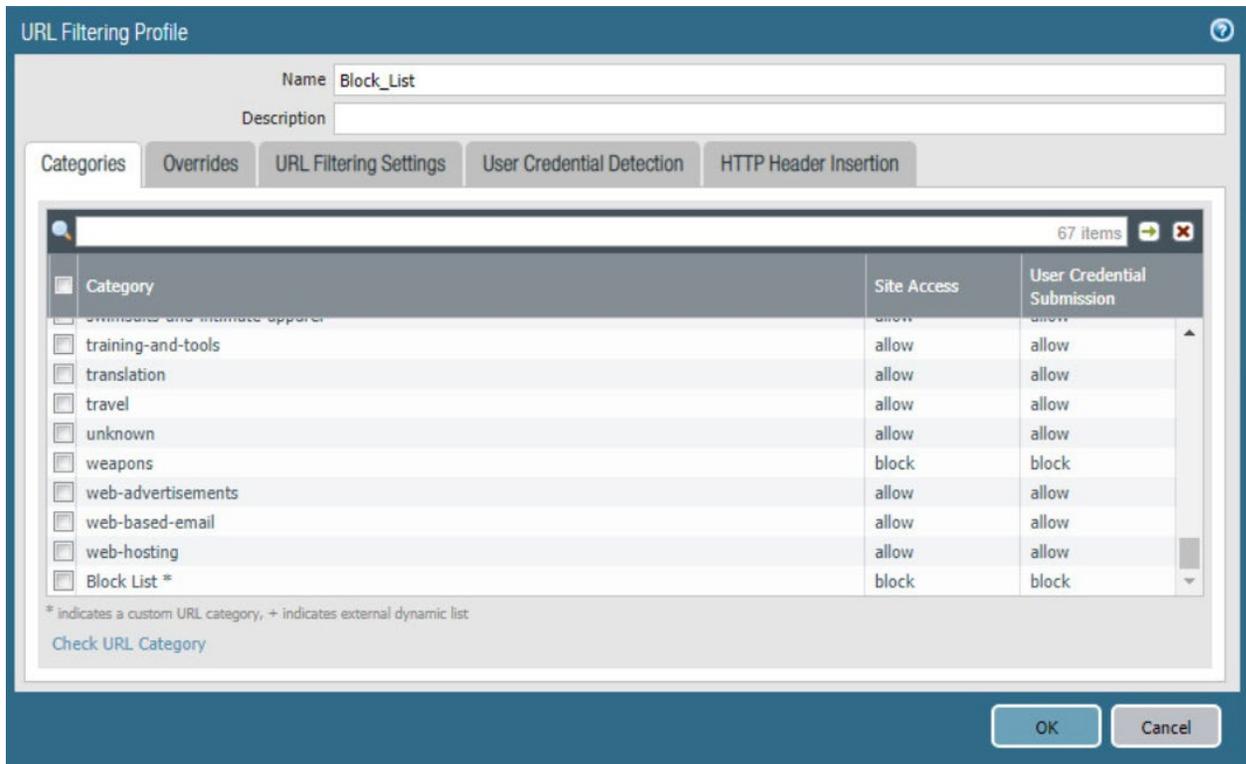
- 867 1. Navigate to **Objects > URL Category**.
- 868 2. Click **Add**.
- 869 3. Enter a name for the **URL Category**. Click **Add** on the bottom.
- 870 4. Add websites that should be blocked. Use the form **.example.com* for all subdomains and *example.com* for the root domain.
- 871

872 Figure 2-26 Custom URL Category



- 873 5. Click **OK**.
- 874 6. Navigate to **Objects > URL Filtering**.
- 875 7. Click **Add**.
- 876 8. Give the filtering profile a name.
- 877 9. Scroll to the bottom of the categories table. The profile created in step 4 should be the last item
878 in the list, with an asterisk next to it. Click where it says **allow** and change the value to **block**.
- 879 10. Configure any additional categories to allow, alert, continue, block, or override.

880 Figure 2-27 URL Filtering Profile



- 881 11. Click **OK**.
- 882 12. Navigate to **Policies > Security**.
- 883 13. Select a policy to apply the URL filtering to.
- 884 14. Select **Actions**.
- 885 15. Next to **Profile Type**, select **Profiles**.
- 886 16. Next to **URL Filtering**, select the created URL filtering profile.

887 **Figure 2-28 URL Filtering Security Policy**

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow' and 'Send ICMP Unreachable' unchecked. The 'Profile Setting' section has 'Profile Type' set to 'Profiles' and 'URL Filtering' set to 'Block_List'. The 'Log Setting' section has 'Log at Session Start' and 'Log at Session End' unchecked, and 'Log Forwarding' set to 'None'. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None', and 'Disable Server Response Inspection' unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

888 17. Click **OK**.

889 18. Repeat steps 13–17 for any policies which need the filtering profile applied.

890 19. Commit the changes.

891 *2.4.5.2 Configure SSL Website Blocking*

892 Note: This section is optional. [Section 2.4.5.1](#) outlines how to configure basic URL filtering, which will
 893 serve a URL blocked page for unencrypted (http [hypertext transfer protocol]) connections, and it will
 894 send a transmission control protocol reset for encrypted (https [hypertext transfer protocol secure])
 895 connections, which will show a default browser error page. This section outlines how to configure the
 896 firewall so that it can serve the same error page for https connections as it does for http connections.
 897 This is purely for user experience and has no impact on blocking functionality.

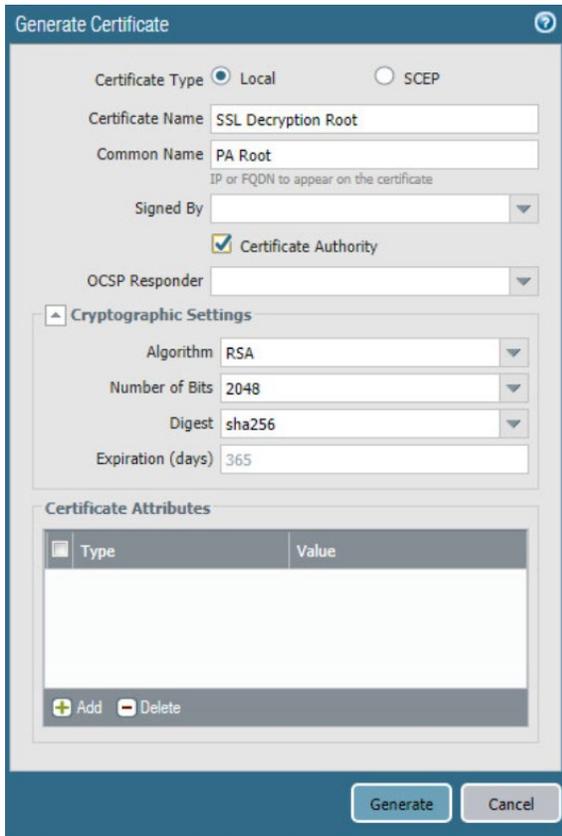
898 1. Navigate to **Device > Certificates**.

899 2. Click **Generate** on the bottom of the page.

900 3. Give the root certificate a name, such as SSL Decryption Root; and a common name (CN) such as
 901 PA Root.

902 4. Check the box next to **Certificate Authority**.

903 **Figure 2-29 Generating the Root CA**



904 5. Click **Generate**.

905 6. Click **Generate** at the bottom of the page.

906 7. Give the certificate a name, such as SSL Decryption Intermediate.

907 8. Give the certificate a CN, such as PA Intermediate.

908 9. Next to **Signed By**, select the generated root CA. In this case, SSL Decryption Root was selected.

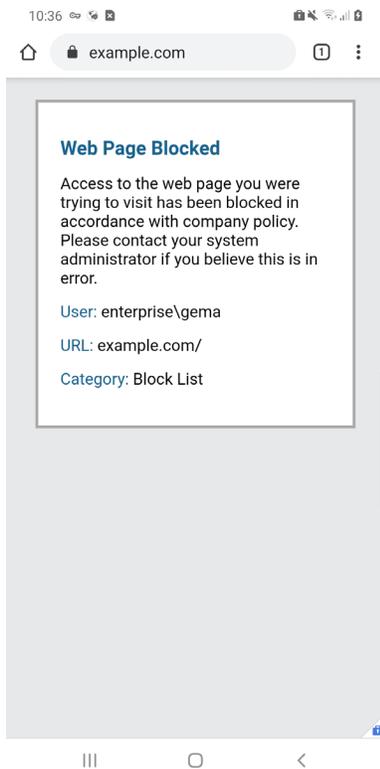
909 10. Check the box next to **Certificate Authority**.

910 11. Click **Generate**.

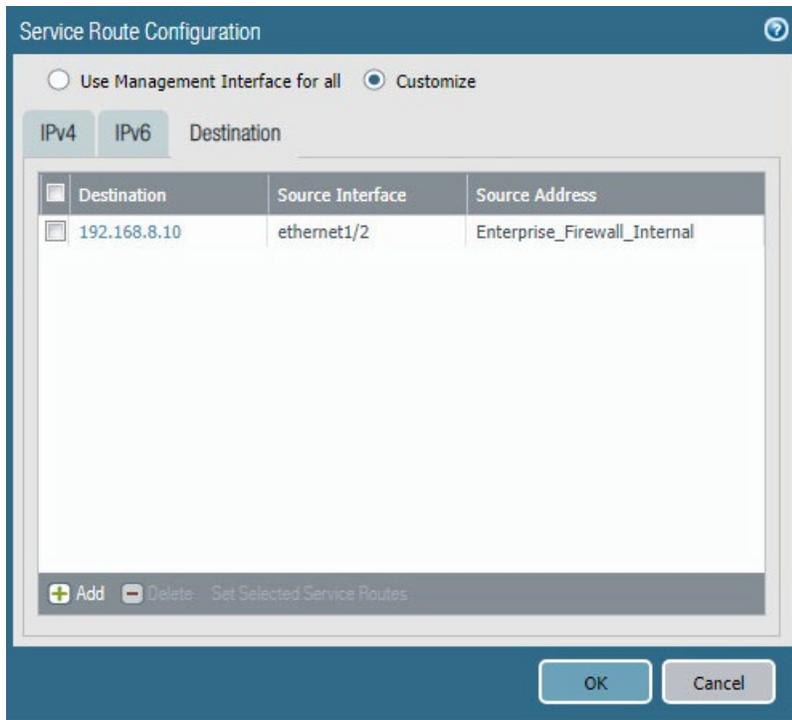
911 12. Click the newly created certificate.

912 13. Check the boxes next to **Forward Trust Certificate** and **Forward Untrust Certificate**.

- 913 14. Click **OK**.
- 914 15. Navigate to **Policies > Decryption**.
- 915 16. Click **Add**.
- 916 17. Give the policy a name and description.
- 917 18. Click **Source**.
- 918 19. Under **Source Zone**, click **Add**.
- 919 20. Select the source zone(s) that matches the security policy that uses URL filtering. In this imple-
920 mentation, the Intranet and SSL VPN zones were selected.
- 921 21. Click **Destination**.
- 922 22. Under **Destination Zone**, click **Add**.
- 923 23. Select the destination zone that matches the security policy that uses URL filtering. Most likely it
924 is the WAN zone.
- 925 24. Click **Service/URL Category**.
- 926 25. Under **URL Category**, click **Add**.
- 927 26. Select the created block list. This ensures that only sites matching the block list are decrypted.
- 928 27. Click **Options**.
- 929 28. Next to **Action**, select **Decrypt**.
- 930 29. Next to **Type**, select **SSL Forward Proxy**.
- 931 30. Next to **Decryption Profile**, select **None**.
- 932 31. Click **OK**.
- 933 32. Commit the changes.

934 **Figure 2-30 Blocked Website Notification**935 **2.4.6 User Authentication Configuration**

- 936 1. Navigate to **Device > Setup > Services > Service Route Configuration**.
- 937 2. Click **Destination**.
- 938 3. Click **Add**.
- 939 4. Enter the IP address of the internal LDAP server for Destination.
- 940 5. Select the **internal network adapter** for Source Interface.
- 941 6. Select the **firewall's internal IP address** for Source Address.
- 942 7. Click **OK** twice and commit the changes.

943 **Figure 2-31 Service Route Configuration**

- 944 8. Navigate to **Device > Server Profiles > LDAP**.
- 945 9. Click **Add**.
- 946 10. Give the profile a meaningful name, such as Enterprise_LDAP_Server.
- 947 11. Click **Add** in the server list. Enter the name for the server and the IP.
- 948 12. Under **Server Settings**, set the **Type** drop-down to **active-directory**.
- 949 13. Enter the **Bind DN** and the password for the Bind DN.

950 **Note:** In this implementation, a new user, palo-auth, was created in Active Directory. This user does not
 951 require any special permissions or groups beyond the standard Domain Users group.

- 952 14. Ensure that **Require SSL/TLS secured connection** is checked.
- 953 15. Click the **down arrow** next to **Base DN**. If the connection is successful, the Base DN (Distingu-
 954 guished Name) should display.
- 955 16. Click **OK**.

956 **Figure 2-32 LDAP Server Profile**

LDAP Server Profile

Profile Name

Administrator Use Only

Name	LDAP Server	Port
LDAP Server	192.168.8.10	389

+ Add - Delete

Enter the IP address or FQDN of the LDAP server

Server Settings

Type

Base DN

Bind DN

Password

Confirm Password

Bind Timeout

Search Timeout

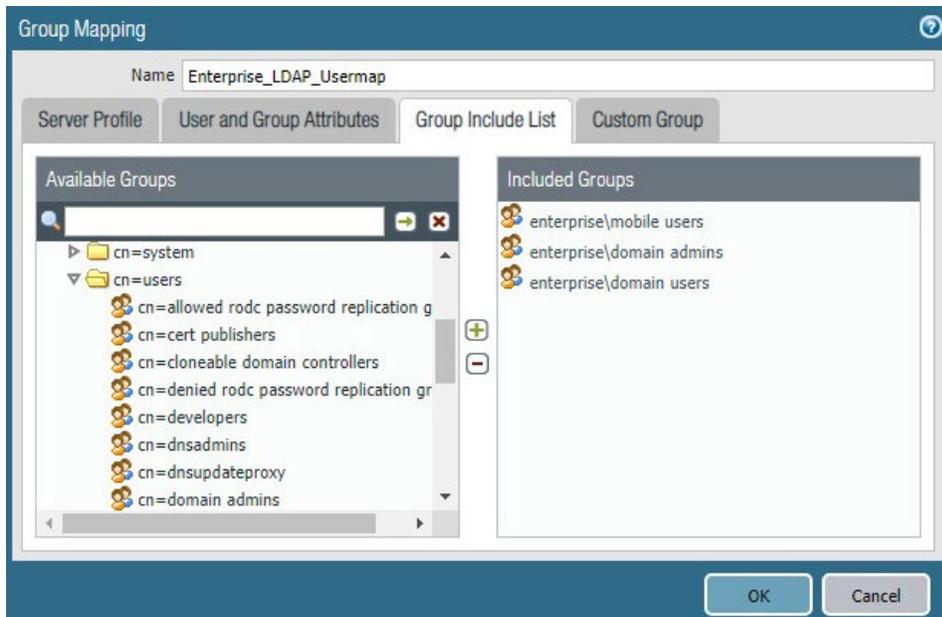
Retry Interval

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

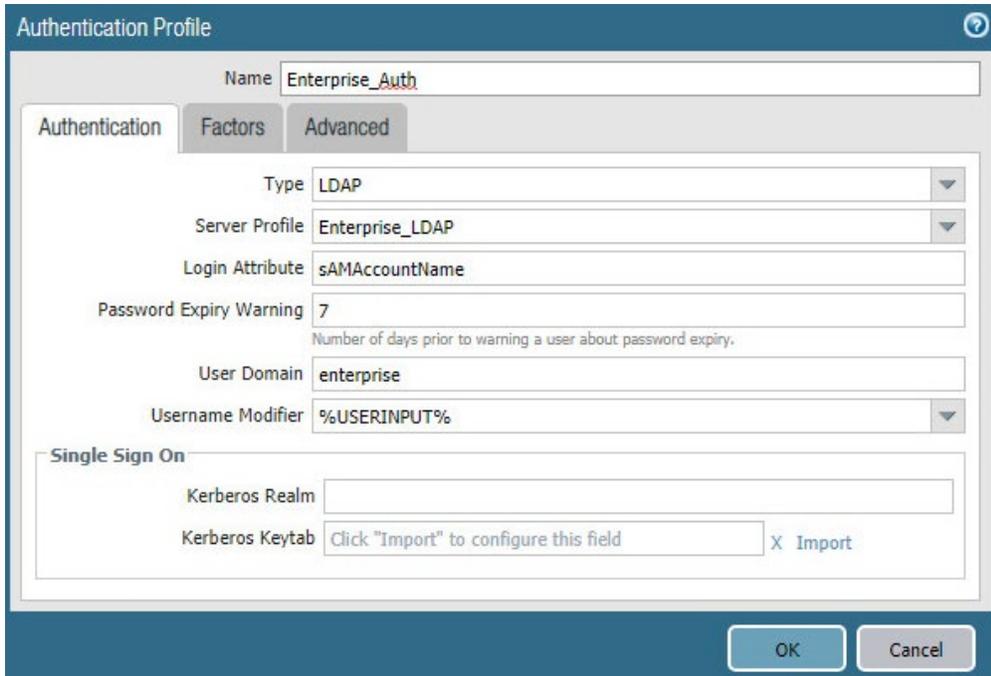
OK Cancel

- 957 17. Navigate to **Device > User Identification > Group Mapping Settings**.
- 958 18. Click **Add**.
- 959 19. Give the mapping a name, such as Enterprise_LDAP_Usermap.
- 960 20. Select the **server profile**, and enter the **user domain**—in this case, Enterprise.
- 961 21. Click **Group Include List**.
- 962 22. Expand the arrow next to the **base DN** and then again next to **cn=users**.
- 963 23. For each group that should be allowed to connect to the VPN, click the proper **entry** and then
- 964 the **+ button**. In this example implementation, mobile users, domain users, and domain admins
- 965 were used.

966 **Figure 2-33 LDAP Group Mapping**

- 967 24. Click **OK**.
- 968 25. Navigate to **Device > Authentication Profile**.
- 969 26. Click **Add**.
- 970 27. Give the profile a meaningful name, such as **Enterprise_Auth**.
- 971 28. For the Type, select **LDAP**.
- 972 29. Select the newly created LDAP profile next to **Server Profile**.
- 973 30. Set the Login Attribute to be **sAMAccountName**.
- 974 31. Set the User Domain to be the **LDAP domain name**—in this case, **enterprise**.

975 **Figure 2-34 LDAP User Authentication Profile**



- 976 32. Click on **Advanced**.
- 977 33. Click **Add**. Select **enterprise\domain users**.
- 978 34. Repeat step 33 for **mobile users** and **domain admins**.
- 979 35. Click **OK**.
- 980 36. Commit the changes.

981 **2.4.7 VPN Configuration**

- 982 1. Navigate to **Network > Interfaces > Tunnel**.
- 983 2. Click **Add**.
- 984 3. Enter a tunnel number. Assign it to the main virtual router. Click **OK**.

985 **Figure 2-35 Configured Tunnel Interfaces**

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	none	none		
tunnel.1		none	Enterprise_Main_Ro...	Enterprise_VPN		SSL VPN

- 986 4. Click the **newly created tunnel**.
- 987 5. Click the drop-down next to **Security Zone**. Select **New Zone**.
- 988 6. Give it a name and assign it to the newly created tunnel. Click **OK** twice.

989 **Figure 2-36 SSL VPN Tunnel Interface Configuration**

The screenshot shows a configuration window titled "Tunnel Interface". It has a header bar with a question mark icon. Below the header, there are three input fields: "Interface Name" with the value "tunnel", "Comment" with the value "SSL VPN", and "Netflow Profile" with a dropdown menu set to "None". Below these fields are four tabs: "Config", "IPv4", "IPv6", and "Advanced". The "Config" tab is selected. Underneath the tabs is a section titled "Assign Interface To" which contains two dropdown menus: "Virtual Router" set to "Enterprise_Main_Router" and "Security Zone" set to "Enterprise_VPN". At the bottom right of the window are two buttons: "OK" and "Cancel".

- 990 7. Commit the changes.
- 991 8. Navigate to **Policies > Authentication**.
- 992 9. Click **Add**.
- 993 10. Give the policy a **descriptive name**. For this example, the rule was named VPN_Auth.
- 994 11. Click **Source**.
- 995 12. Click **Add** and add the VPN and WAN zones.
- 996 13. Click **Destination**.
- 997 14. Check the **Any** box above **Destination Zone**.
- 998 15. Click **Service/URL Category**.
- 999 16. Click **Add** under **Service** and add **service-https**.
- 1000 17. Click **Actions**.

1001 18. Next to **Authentication Enforcement**, select **default-web-form**.

1002 19. Click **OK**.

1003 *2.4.7.1 Configure the GlobalProtect Gateway*

1004 1. Navigate to **Network > GlobalProtect > Gateways**.

1005 2. Click **Add**.

1006 3. Give the gateway a meaningful name. For this implementation, the name Enterprise_VPN_Gate-
1007 way was used.

1008 4. Under **Interface**, select the **WAN Ethernet interface**.

1009 5. Ensure that **IPv4 Only** is selected next to **IP Address Type**.

1010 6. Select the **WAN IP of the firewall** next to **IPv4 Address**. Ensure that end clients can resolve it.

1011 7. Click **Authentication**.

1012 8. Select the created **SSL/TLS service profile** next to **SSL/TLS Service Profile**.

1013 9. Click **Add** under **Client Authentication**.

1014 10. Give the object a meaningful name, such as iOS Auth.

1015 11. Next to **OS**, select **iOS**.

1016 12. Next to **Authentication Profile**, select the **created Authentication Profile**.

1017 13. Next to **Allow Authentication with User Credentials OR Client Certificate**, select **Yes**.

1018 **Figure 2-37 GlobalProtect iOS Authentication Profile**

Client Authentication

Name: iOS Auth

OS: iOS

Authentication Profile: Enterprise_Auth

GlobalProtect App Login Screen

Username Label: Username

Password Label: Password

Authentication Message: Enter login credentials

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate: Yes (User Credentials OR Client Certificate Required)

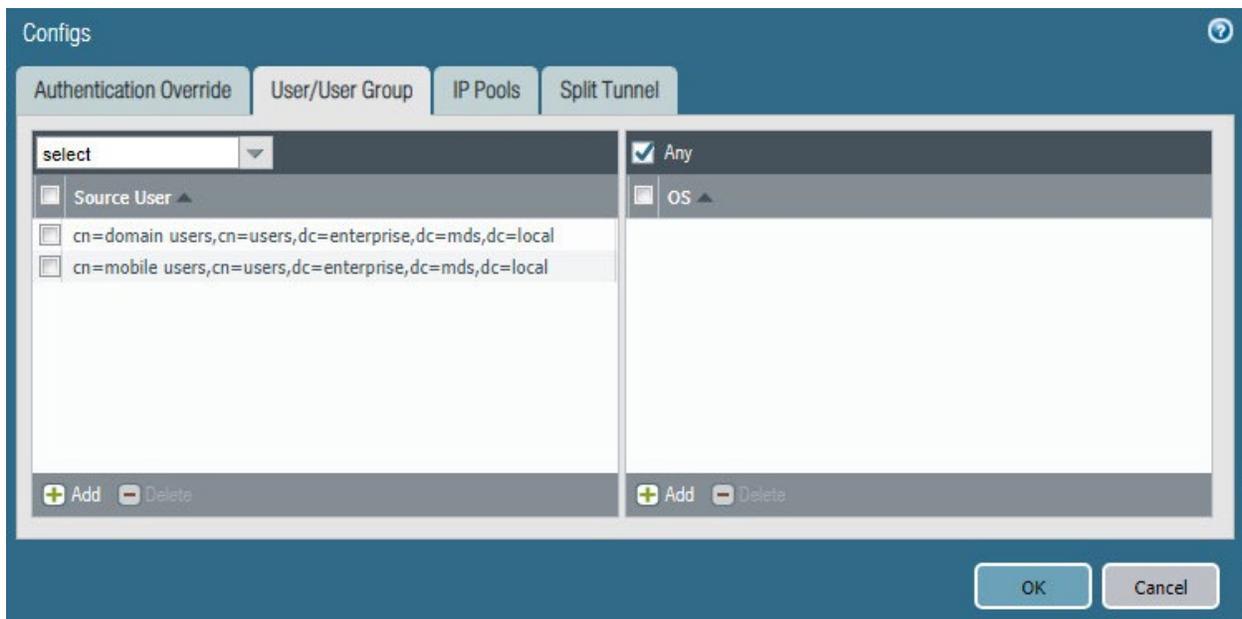
To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

OK Cancel

- 1019 14. Click **OK**.
- 1020 15. Click **Add** under **Client Authentication**.
- 1021 16. Give the object a meaningful name, such as Android Auth.
- 1022 17. Next to **OS**, select **Android**.
- 1023 18. Next to **Authentication Profile**, select the **created Authentication Profile**.
- 1024 19. Next to **Allow Authentication with User Credentials OR Client Certificate**, select **No**.
- 1025 20. Click **Agent**.
- 1026 21. Check the box next to **Tunnel Mode**.
- 1027 22. Select the **created tunnel interface** next to **Tunnel Interface**.
- 1028 23. Uncheck **Enable IPSec**.
- 1029 24. Click **Timeout Settings**.
- 1030 25. Set **Disconnect On Idle** to an organization defined time.
- 1031 26. Click **Client IP Pool**.
- 1032 27. Click **Add** and assign an IP subnet to the clients—in this case, **10.3.3.0/24**.
- 1033 28. Click **Client Settings**.

- 1034 29. Click **Add**.
- 1035 30. Give the config a meaningful name, such as Enterprise_Remote_Access.
- 1036 31. Click **User/User Group**.
- 1037 32. Click **Add** under **Source User**.
- 1038 33. Enter the **LDAP information** of the group allowed to use this rule. In this example, implementa-
- 1039 tion, domain users, and mobile users were used.

1040 **Figure 2-38 LDAP Authentication Group Configuration**



- 1041 34. Click **Split Tunnel**.
- 1042 35. Click **Add** under **Include**.
- 1043 36. Enter **0.0.0.0/0** to enable full tunneling.
- 1044 37. Click **OK**.
- 1045 38. Click **Network Services**.
- 1046 39. Set **Primary DNS** to be the internal domain controller/DNS server—in this case, **192.168.8.10**.
- 1047 40. Click **OK**.
- 1048 41. Navigate to **Network > Zones**.

1049 42. Click the created **VPN zone**.

1050 43. Check the box next to **Enable User Identification**.

1051 **Figure 2-39 VPN Zone Configuration**

1052 44. Click **OK**.

1053 45. Commit the changes.

1054 *2.4.7.2 Configure the GlobalProtect Portal*

1055 1. Navigate to **Network > GlobalProtect > Portals**.

1056 2. Click **Add**.

1057 3. Give the profile a meaningful name, such as Enterprise_VPN_Portal.

1058 4. For Interface, assign it the firewall's **WAN interface**.

- 1059 5. Set IP Address Type to **IPv4 Only**.
- 1060 6. Set the IPv4 address to the firewall's **WAN address**.
- 1061 7. Set all three appearance options to be **factory-default**.

1062 **Figure 2-40 GlobalProtect Portal General Configuration**

The screenshot shows the 'GlobalProtect Portal Configuration' dialog box. On the left, there is a sidebar with tabs: 'General', 'Authentication', 'Agent', 'Clientless VPN', and 'Satellite'. The 'General' tab is active. The main area contains the following fields:

- Name:** Enterprise_VPN_Portal
- Network Settings:**
 - Interface:** ethernet1/1
 - IP Address Type:** IPv4 Only
 - IPv4 Address:** Enterprise_Firewall_External
- Appearance:**
 - Portal Login Page:** factory-default
 - Portal Landing Page:** factory-default
 - App Help Page:** factory-default

At the bottom right, there are 'OK' and 'Cancel' buttons.

- 1063 8. Click **Authentication**.
- 1064 9. Select the **created SSL/TLS service profile**.
- 1065 10. Click **Add** under **Client Authentication**.
- 1066 11. Give the profile a meaningful name, such as Enterprise_Auth.
- 1067 12. Select the created **authentication profile** next to **Authentication Profile**.
- 1068 13. Click **OK**.

1069 Figure 2-41 GlobalProtect Portal Authentication Configuration

GlobalProtect Portal Configuration

General

Authentication

Agent

Clientless VPN

Satellite

Server Authentication

SSL/TLS Service Profile: GlobalProtect_Endpoint

Client Authentication

<input type="checkbox"/>	Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message
<input checked="" type="checkbox"/>	Enterprise_Auth	Any	Enterprise_Auth	Username	Password	Enter login credentials

+ Add - Delete 🔄 Clone ↕ Move Up ↕ Move Down

Certificate Profile: Enterprise_Certificate_Profile

OK Cancel

- 1070 14. Click **Agent** and click **Add** under **Agent**.
- 1071 15. Give the agent configuration a name.
- 1072 16. Ensure that the **Client Certificate** is set to **None**, and **Save User Credentials** is set to **No**.
- 1073 17. Check the box next to **External gateways-manual only**.

1074 Figure 2-42 GlobalProtect Portal Agent Authentication Configuration

Configs

Authentication User/User Group Internal External App Data Collection

Name Agent Config

Client Certificate None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials No

Authentication Override

Generate cookie for authentication override

Accept cookie for authentication override

Cookie Lifetime Hours 24

Certificate to Encrypt/Decrypt Cookie None

Components that Require Dynamic Passwords (Two-Factor Authentication)

Portal External gateways-manual only

Internal gateways-all External gateways-auto discovery

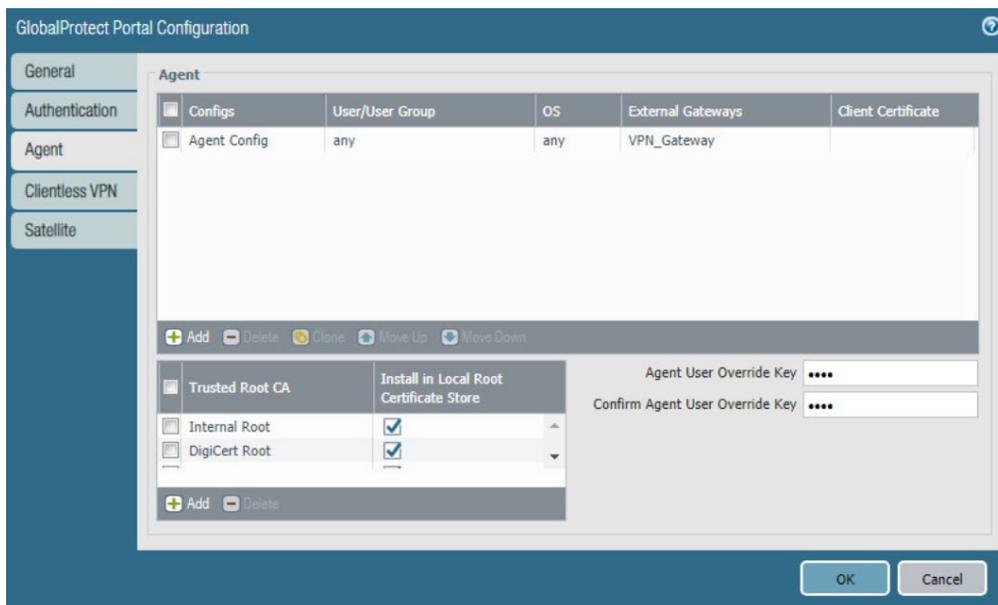
Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

OK Cancel

- 1075 18. Click **External**.
- 1076 19. Click **Add** under **External Gateways**.
- 1077 20. Give the gateway a name and enter the fully qualified domain name (FQDN) of the VPN end
1078 point.
- 1079 21. Click **Add** under **Source Region** and select **Any**.
- 1080 22. Check the box next to **Manual**.
- 1081 23. Click **OK**.
- 1082 24. Click **App**.
- 1083 25. Under **App Configurations > Connect Method**, select **On-demand**.
- 1084 26. Next to **Welcome Page**, select **factory-default**.
- 1085 27. Click **OK**.
- 1086 28. Click **Add** under **Trusted Root CA**.

- 1087 29. Select the **internal root certificate** used to generate device certificates.
- 1088 30. Click **Add** again. Select the **root certificate** used to create the VPN end-point SSL certificate. For
1089 this implementation, it is a DigiCert root certificate.
- 1090 31. Click **Add** again. Select the **root certificate** used for SSL URL filtering, created in a previous sec-
1091 tion.
- 1092 32. Check the box next to **Install in Local Root Certificate Store** for all three certificates.

1093 **Figure 2-43 GlobalProtect Portal Agent Configuration**



- 1094 33. Click **OK**.

1095 *2.4.7.3 Activate Captive Portal*

- 1096 1. Navigate to **Device > User Identification > Captive Portal Settings**.
- 1097 2. Click the **gear** icon on the top right of the Captive Portal box.
- 1098 3. Select the **created SSL/TLS service profile and authentication profile**.
- 1099 4. Click the radio button next to **Redirect**.
- 1100 5. Next to **Redirect Host**, enter the **IP address** of the firewall's WAN interface—in this case,
1101 **10.8.1.2**.

1102 Figure 2-44 Captive Portal Configuration

Captive Portal

Enable Captive Portal

Idle Timer (min)

Timer (min)

GlobalProtect Network Port for Inbound Authentication Prompts (UDP)

SSL/TLS Service Profile

Authentication Profile

Mode Transparent Redirect

Session Cookie

Enable

Timeout (min)

Roaming

Redirect Host

Certificate Authentication

Certificate Profile

NTLM Authentication

Attempts

Timeout (sec)

Reversion Time (sec)

1103 6. Click **OK**.

1104 7. Commit the changes.

1105 *2.4.7.4 Activate the GlobalProtect Client*1106 1. Navigate to **Device > GlobalProtect Client**.

1107 2. Acknowledge pop up messages.

1108 3. Click **Check Now** at the bottom of the page.1109 4. Click **Download** next to the **first release** that comes up. In this implementation, version 5.0.2ate-
1110 was used.1111 5. Click **Activate** next to the **downloaded release**.

- 1112 6. Navigate to the FQDN of the VPN. You should see the Palo Alto Networks logo and the Glob-
1113 alProtect portal login prompt, potentially with a message indicating that a required certificate
1114 cannot be found. This is expected on desktops because there is nothing in place to seamlessly
1115 deploy client certificates.

1116 **Figure 2-45 GlobalProtect Portal**



- 1117 Note: If you intend to use the GlobalProtect agent with a self-signed certificate (e.g., internal PKI), be
1118 sure to download the SSL certificate from the VPN website and install it in the trusted root CA store.

1119 2.4.8 Enable Automatic Application and Threat Updates

- 1120 1. In the **PAN-OS portal**, navigate to **Device > Dynamic Updates**.
- 1121 2. Install the latest updates.
- 1122 a. At the bottom of the page, click **Check Now**.

- 1123 b. Under **Applications and Threats**, click **Download** next to the last item in the list with the
- 1124 latest Release Date. This will take a few minutes.
- 1125 c. When the download completes, click **Close**.

1126 **Figure 2-46 Downloaded Threats and Applications**

Release Date	Downloaded	Currently Installed	Action	Documentation
2018/10/31 17:41:37 EDT	✓		Install Review Policies Review Apps	Release Notes

- 1127 d. Click **Install** on the first row.
- 1128 e. Click **Continue Installation**, leaving the displayed box unchecked. Installation will take a
- 1129 few minutes.
- 1130 f. When the installation completes, click **Close**.
- 1131 3. Enable automatic threat updates. (Note: Automatic threat updates are performed in the back-
- 1132 ground and do not require a reboot of the appliance.)
- 1133 a. At the top of the page, next to **Schedule**, click the hyperlink with the date and time, as
- 1134 shown in Figure 2-47.

1135 **Figure 2-47 Schedule Time Hyperlink**

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)

- 1136 b. Select the **desired recurrence**. For this implementation, weekly was used.
- 1137 c. Select the **desired day and time** for the update to occur. For this implementation, Satur-
- 1138 day at 23:45 was used.
- 1139 d. Next to **Action**, select **download-and-install**.

1140 Figure 2-48 Application and Threats Update Schedule

Applications and Threats Update Schedule

Recurrence: Weekly

Day: saturday

Time: 23:45

Action: download-and-install

Disable new apps in content update

Threshold (hours): [1 - 336]
A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs

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

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

OK Cancel

1141 e. Click **OK**.

1142 f. Commit the changes.

1143

2.5 Kryptowire

1144 Kryptowire was used as an application vetting service via a custom active directory-integrated web
 1145 application.

1146

2.5.1 Kryptowire and MaaS360 Integration

1147 1. Contact IBM support to provision API credentials for Kryptowire.

1148 2. Contact Kryptowire support to enable the MaaS360 integration, including the MaaS360 API cre-
 1149 dentials.1150 3. In the Kryptowire portal, click the **logged-in user's email address** in the upper right-hand corner
 1151 of the portal. Navigate to **Settings > Analysis**.1152 4. Set the **Threat Score Threshold** to the desired amount. In this sample implementation, 75 was
 1153 used.

- 1154 5. Enter an **email address** where email alerts should be delivered.
- 1155 6. Click **Save Settings**. Kryptowire will now send an email to the email address configured in step 5
- 1156 when an analyzed application is at or above the configured alert threshold.

1157 **Appendix A List of Acronyms**

AD	Active Directory
API	Application Programming Interface
CA	Certificate Authority
CN	Common Name
DC	Domain Controller
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HKEY	Handle to Registry Key
HKLM	HKEY_LOCAL_MACHINE
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machines
IIS	Internet Information Services
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MDSE	Mobile Device Security for Enterprise
NCCoE	National Cybersecurity Center of Excellence
NDES	Network Device Enrollment Service
NIST	National Institute of Standards and Technology

OU	Organizational Unit
PKI	Public Key Infrastructure
SCEP	Simple Certificate Enrollment Protocol
SP	Special Publication
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network

1158 **Appendix B** **Glossary**

Bring Your Own Device (BYOD) A non-organization-controlled telework client device. [\[2\]](#)

1159 **Appendix C** **References**

- 1160 [1] International Business Machines. "Cloud Extender architecture." [Online]. Available:
1161 https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/referenc
1162 [es/ce_architecture.htm](https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/referenc).
- 1163 [2] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own*
1164 *Device (BYOD) Security*, National Institute of Standards and Technology (NIST) Special Publication
1165 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available:
1166 <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>.

1167 **Appendix D Example Solution Lab Build Testing Details**

1168 This section shows the test activities performed to demonstrate how this practice guide's example
1169 solution that was built in the National Institute of Standards and Technology (NIST) National
1170 Cybersecurity Center of Excellence (NCCoE) lab addresses the threat events and privacy risks defined
1171 from the risk assessment found in Volume B section 3.4.

1172 **D.1 Threat Event 1**

1173 **Summary:** Unauthorized access to work information via a malicious or privacy-intrusive application.

1174 **Test Activity:** Place mock enterprise contacts on devices, then attempt to install and use unmanaged
1175 applications that access and back up those entries.

1176 **Desired Outcome:** Built-in device mechanisms such as Apple User Enrollment functionality and Google's
1177 Android Enterprise work profile functionality are used to separate the contact and calendar entries
1178 associated with enterprise email accounts so that they can only be accessed by enterprise applications
1179 (applications that the enterprise mobility management (EMM) authorizes and manages), not by
1180 applications manually installed by the user.

1181 **Observed Outcome:** Since the test application was unmanaged, it was unable to access the enterprise
1182 contacts and calendar entries. This is due to Android Enterprise and Apple User Enrollment providing
1183 data separation and isolation capabilities between the personal and work profiles. The observed
1184 outcomes are shown in Figures 2-49 and 2-50 which show how a contact created in a work profile
1185 cannot be seen by a personal profile. Also, Figures 2-51 and 2-52 show how a contact created in a
1186 managed application cannot be seen by an unmanaged application.

Figure 2-49 Contact Created in Work Profile

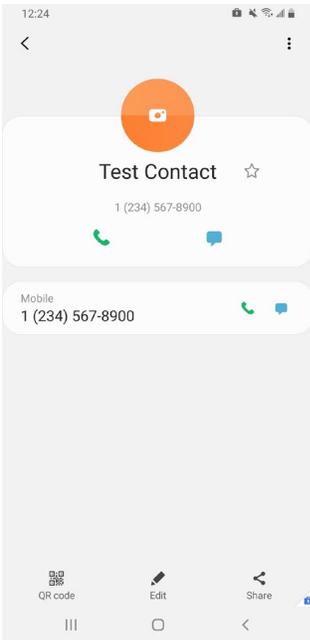


Figure 2-50 Personal Profile Can't See Work Contacts

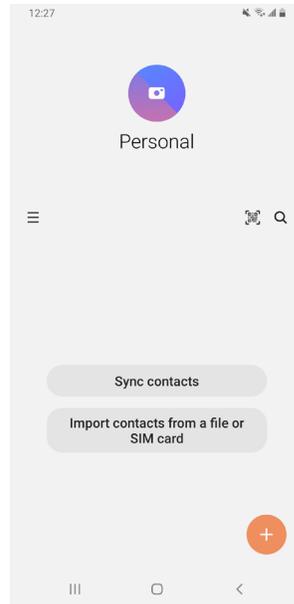


Figure 2-51 Contact Created in Managed App

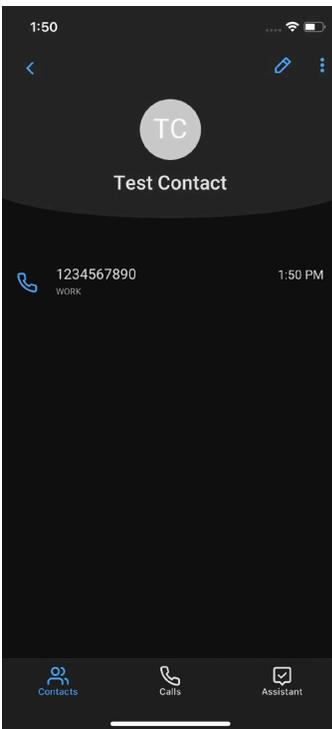
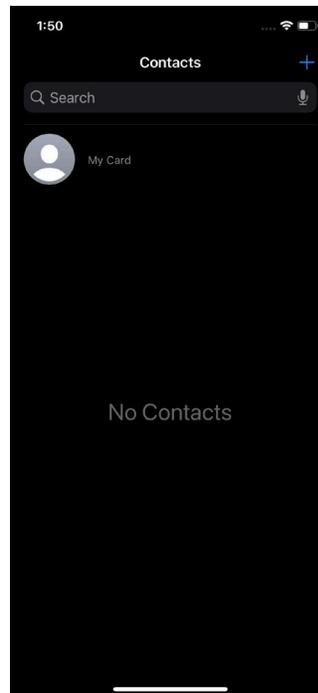


Figure 2-52 Unmanaged App Can't See Managed Contacts



1187 **D.2 Threat Event 2**

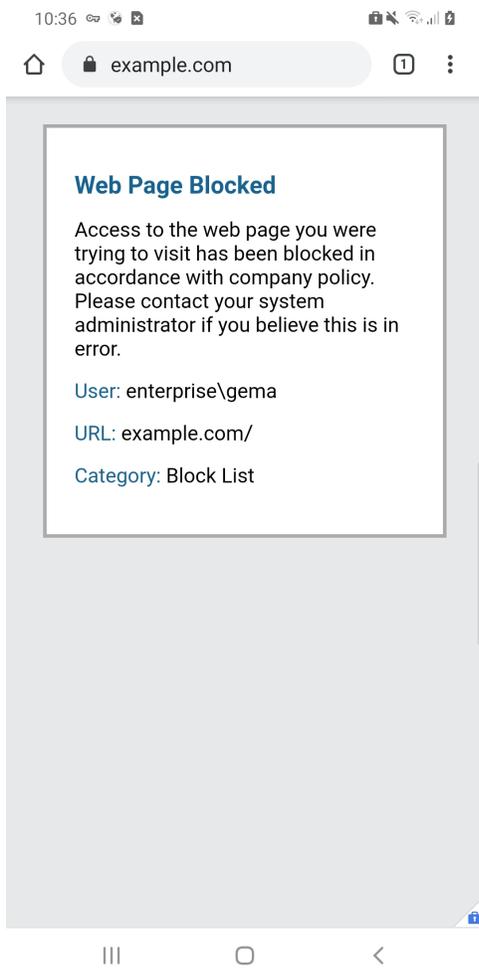
1188 **Summary:** A fictional phishing event was created to test protection against the theft of credentials
1189 through an email phishing campaign.

1190 **Test Activity:**

- 1191 ▪ This threat event can be tested by establishing a web page with a form that impersonates an
1192 enterprise login prompt.
- 1193 ▪ The web page's uniform resource locator (URL) is then sent via email and there is an attempt to
1194 collect and use enterprise login credentials.

1195 **Desired Outcome:** The enterprise's security architecture should block the user from browsing to known
1196 malicious websites. Additionally, the enterprise should require multifactor authentication or phishing-
1197 resistant authentication methods such as those based on public key cryptography so that either there is
1198 no password for a malicious actor to capture or capturing the password is insufficient to obtain access to
1199 enterprise resources.

1200 **Observed Outcome:** The example solution used Palo Alto Networks' next-generation firewall. The
1201 firewall includes PAN-DB, a URL filtering service that automatically blocks known malicious URLs. The
1202 URL filtering database is updated regularly to help protect users from malicious URLs. The next-
1203 generation firewall blocked the attempt to visit the phishing site when accessing it from within the work
1204 profile. However, if the malicious URL were not present in PAN-DB, or the URL was accessed in the
1205 personal profile of the device, the user would be allowed to access the website. Figure 2-53 shows the
1206 observed outcome of the phishing webpage being blocked from within the work profile.

1207 **Figure 2-53 Fictitious Phishing Webpage Blocked**

1208

1209 **D.3 Threat Event 3**

1210 **Summary:** Confidentiality and integrity loss due to the exploitation of a known vulnerability in the
1211 operating system or firmware.

1212 **Test Activity:** Attempt to access enterprise resources from a mobile device with known vulnerabilities
1213 (e.g., running an older, unpatched version of iOS or Android).

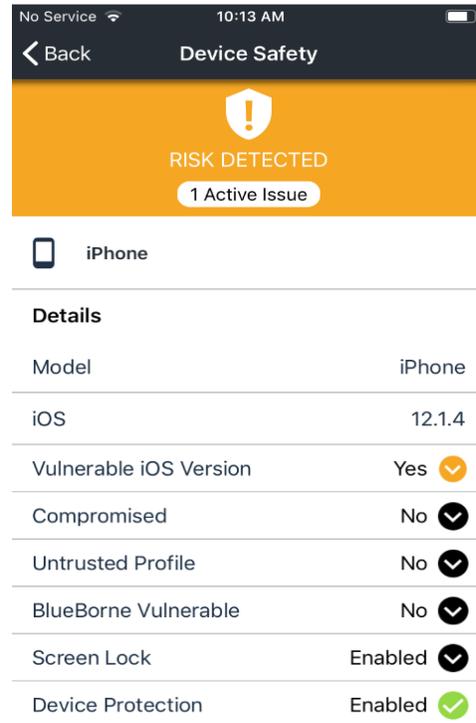
1214 **Desired Outcome:** The enterprise's security architecture should identify the presence of devices that are
1215 running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be
1216 possible, when warranted by the risks, to block devices from accessing enterprise resources until system
1217 updates are installed.

1218 **Observed Outcome:** Zimperium was able to identify devices that were running an outdated version of
 1219 iOS or Android, and it informed MaaS360 when a device was out of compliance. Once MaaS360 alerted
 1220 the user, they had a pre-configured amount of time to remediate the risk before work data was
 1221 removed from the device, leaving the personal data unaffected. Figure 2-54 and 2-55 shows the security
 1222 architecture identifying the presence of outdated operating systems.

Figure 2-54 iOS MaaS360 OS Compliance Alert



Figure 2-55 Zimperium Risk Detected



1223

1224 D.4 Threat Event 4

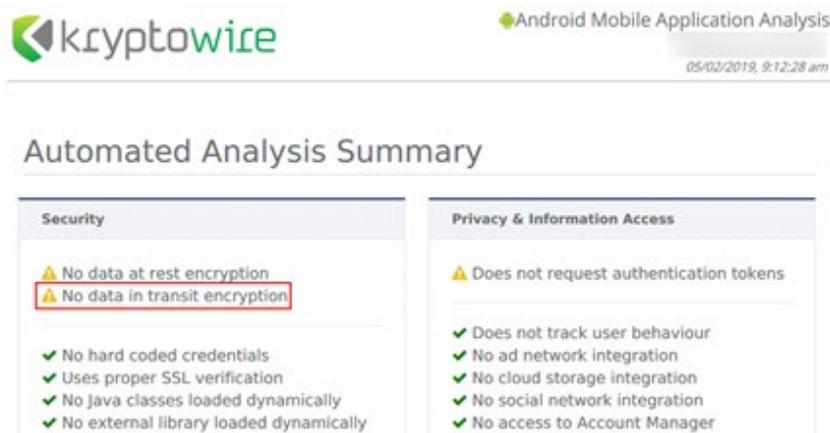
1225 **Summary:** Loss of confidentiality of sensitive information via eavesdropping on unencrypted device
 1226 communications.

1227 **Test Activity:** Test if applications will attempt to establish a hypertext transfer protocol or unencrypted
 1228 connection.

1229 **Desired Outcome:**

- 1230
- 1231
- 1232
- 1233
- 1234
- 1235
- 1236
- 1237
- Android: Because all work applications are inside a work profile, a profile-wide virtual private network (VPN) policy can be applied to mitigate this threat event; all communications, both encrypted and unencrypted, will be sent through the VPN tunnel. This will prevent eavesdropping on any communication originating from a work application.
 - iOS: Apply a per-application VPN policy that will send all data transmitted by managed applications through the VPN tunnel. This will prevent eavesdropping on any unencrypted communication originating from work applications.
 - Kryptowire can identify if an application attempts to establish an unencrypted connection.

1238 **Observed Outcome:** The Kryptowire report indicated that the application did not use in-transit data encryption. When the managed version of that application was launched, an SSL VPN connection was automatically established. Figure 2-56 shows the analysis summary finding of no in transit data encryption in use.

1242 **Figure 2-56 Kryptowire Application Report**1243 **D.5 Threat Event 5**

1244 **Summary:** Compromise of device integrity via observed, inferred, or brute-forced device unlock code.

1245 **Test Activity:**

- 1246
- 1247
- 1248
- Attempt to completely remove the device unlock code. Observe whether the attempt succeeds.
 - Attempt to set the device unlock code to “1234,” a weak four-digit personal identification number (PIN). Observe whether the attempt succeeds.

1249 **Desired Outcome:** Policies set on the device by the EMM (MaaS360) should require a device unlock code to be set, prevent the device unlock code from being removed, and require a minimum complexity

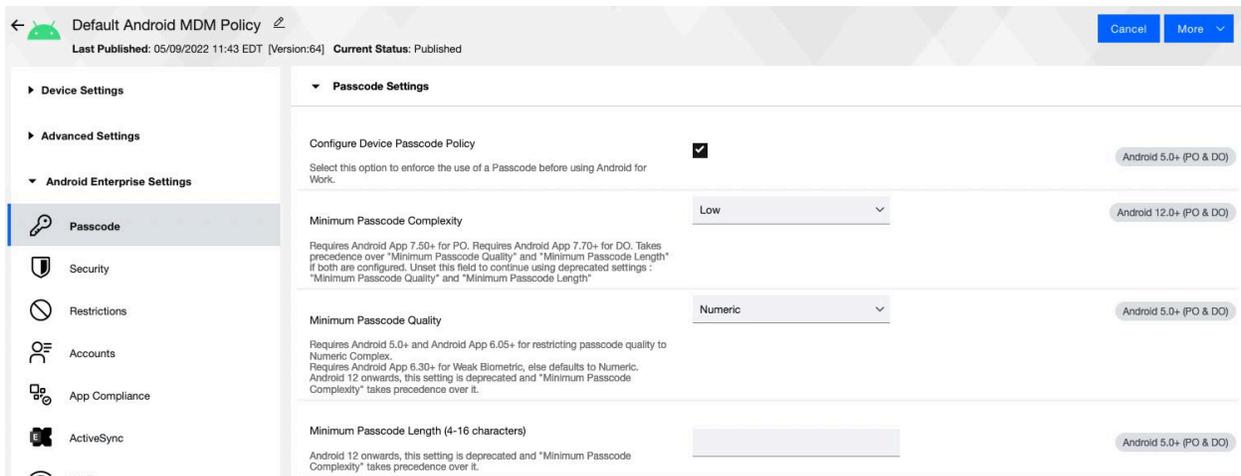
1250

1251 for the device unlock code. The VPN (GlobalProtect) should require periodic re-authentication with
 1252 multi-factor authentication to prevent devices with a bypassed lockscreen from accessing on-premises
 1253 enterprise resources.

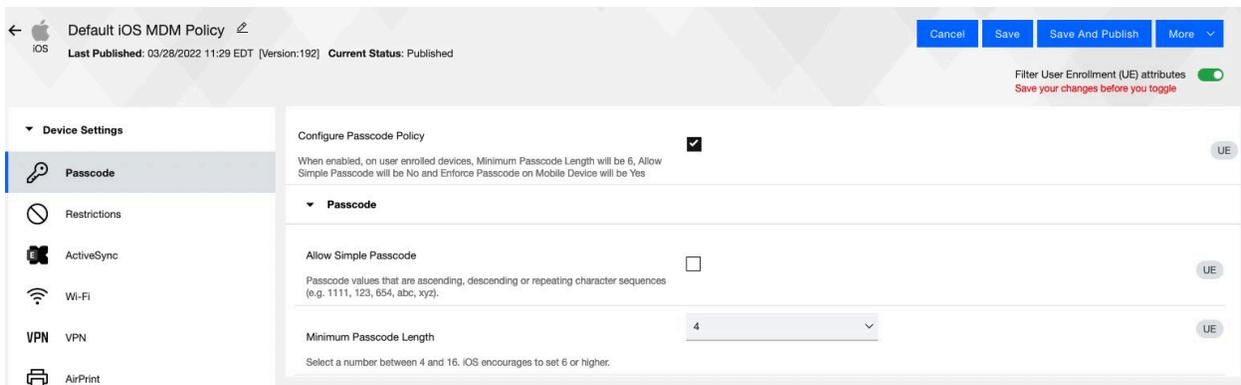
1254 Additionally, the MTD (Zimperium) can identify and report iOS devices with a disabled lock screen.

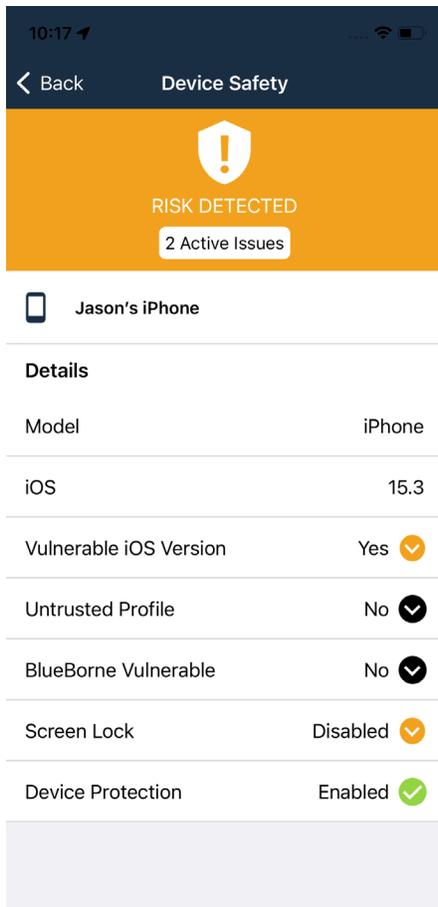
1255 **Observed Outcome:** MaaS360 applies a policy to the devices to enforce a mandatory PIN, Zimperium
 1256 reports devices with a disabled lock screen, and GlobalProtect requires periodic re-authentication using
 1257 MFA. Figures 2-57 through 2-59 show the passcode and lockscreen configuration settings.

1258 **Figure 2-57 Android Passcode Configuration**



1259 **Figure 2-58 iOS Passcode Configuration**



1260 **Figure 2-59 Zimperium Detecting Disabled Lockscreen**1261 **D.6 Threat Event 6**

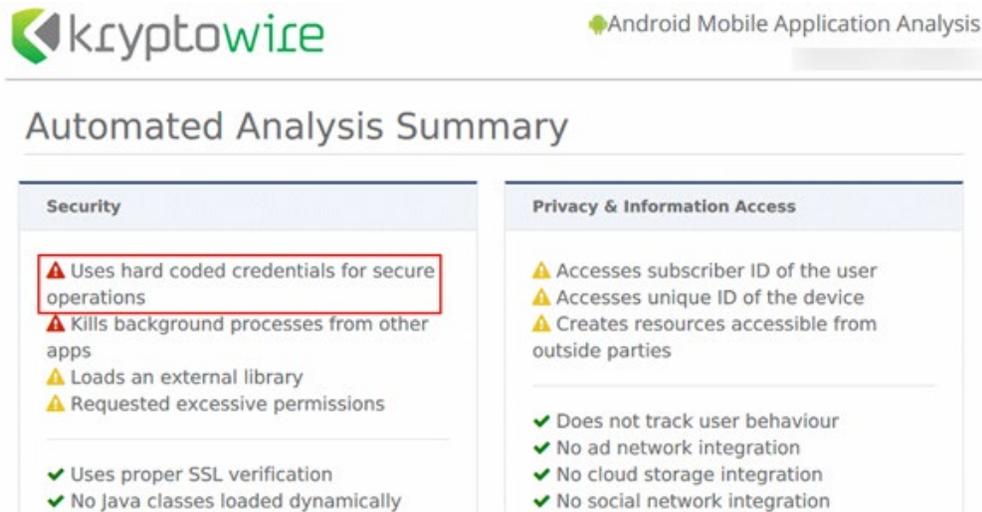
1262 **Summary:** Unauthorized access to backend services via authentication or credential storage
 1263 vulnerabilities in internally developed applications.

1264 **Test Activity:** Application was submitted to Kryptowire for analysis of credential weaknesses.

1265 **Desired Outcome:** Discover and report credential weaknesses.

1266 **Observed Outcome:** Kryptowire recognized that the application uses hardcoded credentials. The
 1267 application's use of hardcoded credentials could introduce vulnerabilities if unauthorized entities used
 1268 the hardcoded credentials to access enterprise resources. Figure 2-60 shows the discovery of hardcoded
 1269 credentials.

1270 Figure 2-60 Application Report with Hardcoded Credentials

1271 **D.7 Threat Event 7**

1272 **Summary:** Unauthorized access of enterprise resources from an unmanaged and potentially
 1273 compromised device.

1274 **Test Activity:** Attempt to directly access enterprise services, e.g., Exchange email server or corporate
 1275 VPN, on a mobile device that is not enrolled in the EMM system.

1276 **Desired Outcome:** Enterprise services should not be accessible from devices that are not enrolled in the
 1277 EMM system. Otherwise, the enterprise is not able to effectively manage devices to prevent threats.

1278 **Observed Outcome:** Devices that were not enrolled in MaaS360 were unable to access enterprise
 1279 resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper
 1280 client certificates—obtainable only through enrolling in the EMM. Figures 2-61 through 2-63 show the
 1281 desired outcome of the VPN gateway protecting the enterprise.

Figure 2-61 Attempting to Access the VPN on an Unmanaged iOS Device

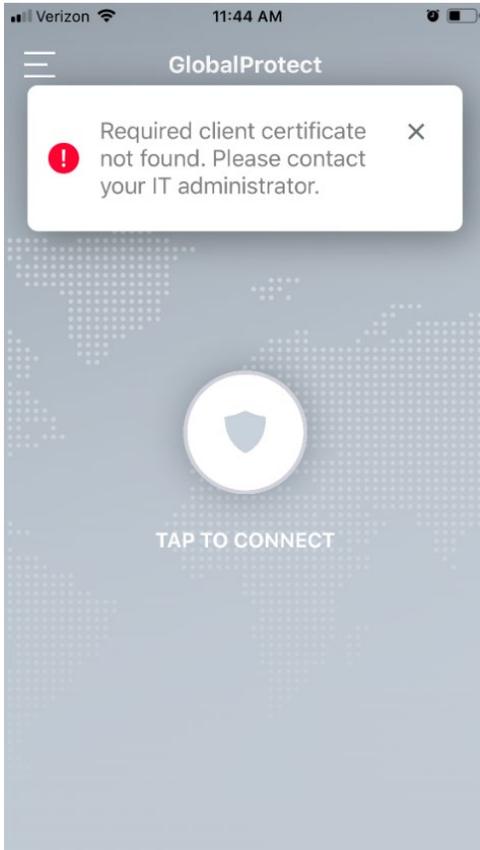
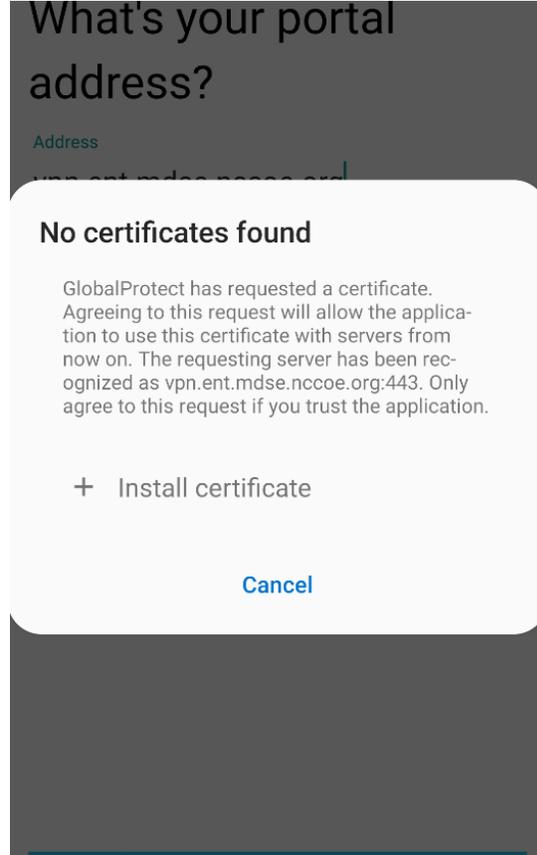
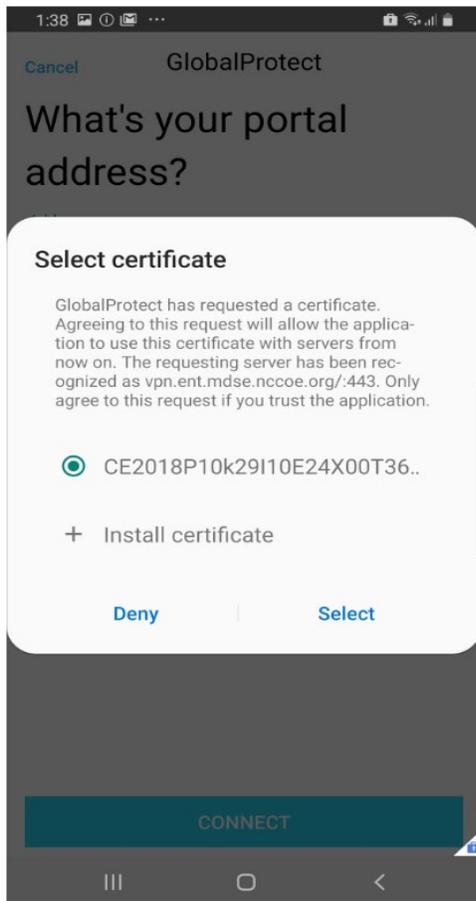


Figure 2-62 Attempting to Access the VPN on an Unmanaged Android Device



1282 Figure 2-63 Attempting to Access the VPN on a Managed Android Device

1283 **D.8 Threat Event 8**1284 **Summary:** Loss of organizational data due to a lost or stolen device.

1285 **Test Activity:** Attempt to download enterprise data onto a mobile device that is not enrolled in the
 1286 EMM system (may be performed in conjunction with TE-7). Attempt to remove (in conjunction with TE-
 1287 5) the screen lock passcode or demonstrate that the device does not have a screen lock passcode in
 1288 place. Attempt to locate and selectively wipe the device through the EMM console (will fail if the device
 1289 is not enrolled in the EMM).

1290 **Desired Outcome:** It should be possible to locate or wipe EMM enrolled devices in response to a report
 1291 that they have been lost or stolen. As demonstrated by TE-7, only EMM enrolled devices should be able
 1292 to access enterprise resources. As demonstrated by TE-5, EMM enrolled devices can be forced to have a

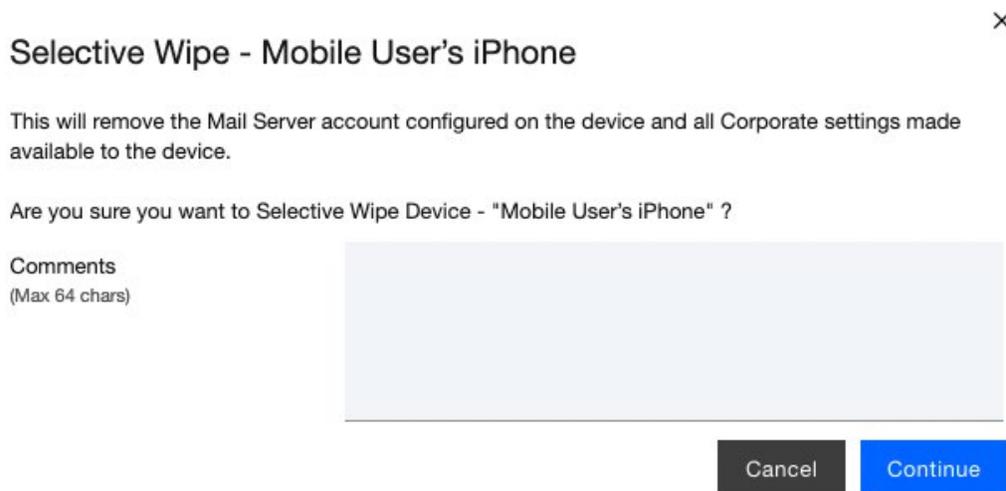
1293 screen lock with a passcode of appropriate strength, which helps resist exploitation (including loss of
1294 organizational data) if the device has been lost or stolen.

1295 **Observed Outcome (Enrolled Devices):** Enrolled devices are protected. They have an enterprise policy
1296 requiring a PIN/lock screen, and therefore, the enterprise data on the device could not be accessed.
1297 Additionally, the device could be remotely wiped after it was reported as lost to enterprise mobile
1298 device service management, ensuring no corporate data is left in the hands of attackers.

1299 **Observed Outcome (Unenrolled Devices):** As shown in Threat Event 7, only enrolled devices could
1300 access enterprise resources. When the device attempted to access enterprise data, no connection to the
1301 enterprise services was available. Because the device cannot access the enterprise, the device would not
1302 contain enterprise information.

1303 In both outcomes, both enrolled and unenrolled, it would be at the user's discretion if they wanted to
1304 wipe all personal data as well. Because this is a Bring Your Own Device (BYOD) scenario, only corporate
1305 data (managed applications on iOS, and the work container on Android) would be deleted from a device
1306 if the device were lost or stolen. Figures 2-64 through 2-67 show the removal of only organization data
1307 using selective wipe features.

1308 **Figure 2-64 Selective Wiping a Device**



1309 **Figure 2-65 Selective Wipe Complete**

Applied Policy	MDM: Default iOS MDM Policy (192) ● WorkPlace Persona: WorkPlace Persona Policy (9) ●
Jailbroken/Rooted	No ●
Selective Wipe Status	Completed (05/23/2022 14:28 EDT) ●
Passcode Status	MDM:Compliant ● WorkPlace: Enabled ●
Rules Compliance Status	In Compliance ●
Rule Set Name	Zimperium - Critical

Figure 2-66 Corporate Data Removal Confirmation Notification on iOS

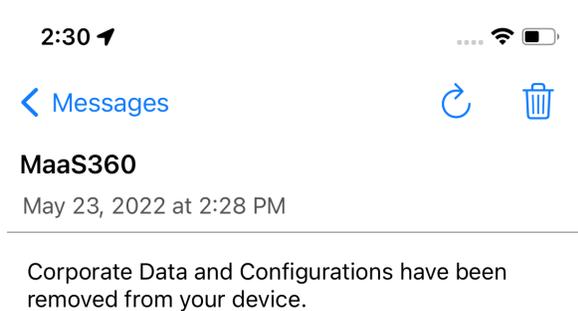
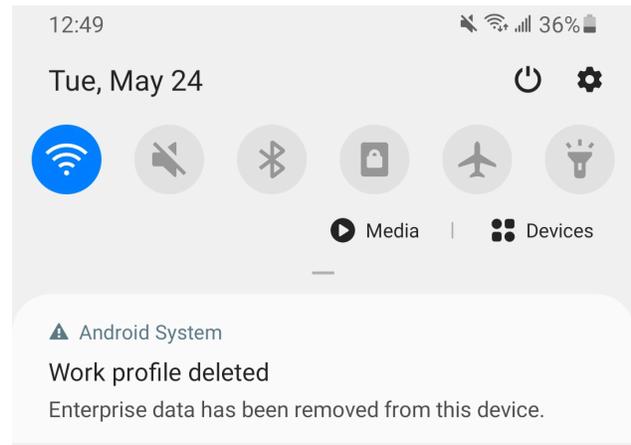


Figure 2-67 Work Profile Removal Notification on Android



1310 **D.9 Threat Event 9**

1311 **Summary:** Loss of confidentiality of organizational data due to its unauthorized storage in non-
1312 organizationally managed services.

1313 **Test Activity:** Connect to the enterprise VPN. Open an enterprise website or application. Attempt to
1314 extract enterprise data by taking a screenshot, or copy/paste and send it via an unmanaged email
1315 account.

1316 **Desired Outcome:** The EMM will prohibit screenshots and other data-sharing actions while using
1317 managed applications.

1318 **Observed Outcome:** As shown in [Figures 2-68](#) through [2-70](#), MaaS360 device policies prevented the
1319 following actions on BYOD managed phones:

1320 **Android**

- 1321 ▪ clipboard sharing
- 1322 ▪ screen capture
- 1323 ▪ share list
- 1324 ▪ backup to Google
- 1325 ▪ Secure Digital card write
- 1326 ▪ Universal Serial Bus storage
- 1327 ▪ video recording
- 1328 ▪ Bluetooth
- 1329 ▪ background data sync
- 1330 ▪ Android Beam
- 1331 ▪ Sbeam

1332 **iOS**

- 1333 ▪ opening, writing, and saving from managed to unmanaged applications
- 1334 ▪ AirDrop for managed applications
- 1335 ▪ screen capture
- 1336 ▪ AirPlay
- 1337 ▪ iCloud backup
- 1338 ▪ document, photo stream, and application sync
- 1339 ▪ print
- 1340 ▪ importing files

1341 Figure 2-68 iOS DLP Configuration Options

The screenshot displays the configuration interface for a Default iOS MDM Policy. At the top, it shows the policy name, last published date (03/28/2022 11:29 EDT), version (192), and current status (Needs Publish). There are 'Edit' and 'More' buttons, and a toggle for 'Filter User Enrollment (UE) attributes' which is currently turned on.

The left sidebar contains a navigation menu with the following items: Device Settings (expanded), Passcode, Restrictions (selected), ActiveSync, Wi-Fi, VPN, AirPrint, and Accounts. Under Device Settings, there is an 'Advanced Settings' section.

The main content area is titled 'Configure Device Restrictions' and lists several settings:

- Unencrypted backups are restricted for all APNS managed devices:** Set to Yes. A red warning message states: "Unencrypted backups are restricted for all APNS managed devices. Select this option to configure restrictions on use of device features, application and content." This setting is available for all UE.
- Device Functionality:**
 - Allow Open from Managed to Unmanaged apps:** Set to No. Description: "Allows Content to be opened from Managed to Unmanaged apps. Applies to Mail, Calendar events, Contacts and other types of content." Available for UE, iOS 7.0+.
 - Allow Open from Unmanaged to Managed Apps:** Set to No. Description: "Allows Content to be opened from Unmanaged to Managed apps. Applies to Mail, Calendar events, Contacts and other types of content." Available for UE, iOS 7.0+.
 - Allow AirDrop for Managed Apps:** Set to Yes. Description: "Allow AirDrop to be used with managed apps." Available for UE, iOS 9.0+.
 - Allow Screen Capture:** Set to Yes. Description: "Disable to prevent screenshots, and on iOS9 devices video capture." Available for UE.

1342 Figure 2-69 Android DLP Configuration

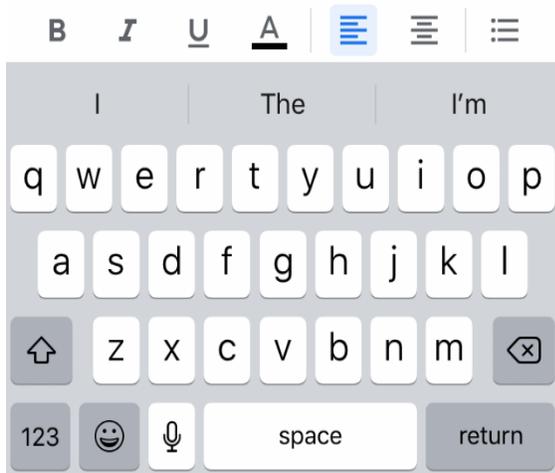
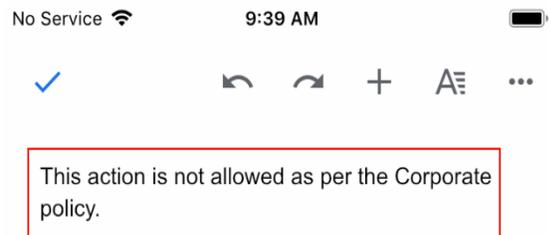
Default Android MDM Policy [↗](#)
Edit
More ▼

Last Published: 05/23/2022 10:19 EDT [Version:65]
Current Status: Published

- ▶ Device Settings
- ▶ Advanced Settings
- ▼ Android Enterprise Settings
- 🔑 Passcode
- 🛡 Security
- 🚫 **Restrictions**
- 👤 Accounts
- 📱 App Compliance
- 📧 ActiveSync
- 📶 Wi-Fi
- VPN VPN
- 📄 Certificates
- 🌐 Browser
- 📺 COSU (Kiosk mode)
- 🖼 Wallpapers
- 🔄 System Update Settings
- 📁 Profile Management

Configure Restrictions	Yes	
▼ Device Features		
Allow camera	Yes	Android 5.0+ (PO & DO)
To enable camera on device, camera app needs to be allowed in native app compliance apart from enabling this.		
Allow camera on personal profile	Yes	Android 11+ (WPCO)
Camera app also needs to be allowed in native app compliance apart from enabling this.		
Mute Master Volume	No	Android 5.0+ DO
Allow unmuting of microphone	Yes	Android 5.0+ (DO)
Allow volume adjustments	Yes	Android 5.0+ (DO)
Allow bluetooth configuration	Yes	Android 5.0+ (DO)
Allow outgoing beam	Yes	Android 5.1.1+ (PO & DO)
Note: Disabling this feature would not allow DO enrollments on the device.		
Allow sharing of locations	Yes	Android 5.0+ (PO & DO)
This policy controls location permission availability for apps. Keep this policy enabled if you are configuring WiFi policies, Trusteer policies or WiFi or Bluetooth settings within kiosk. Location permission is required for discovering list of configured networks, current connected network and discovering other bluetooth networks.		

1343 **Figure 2-70 Attempting to Paste Text on iOS Between Unmanaged and Managed Apps**



1344 **D.10 Privacy Risk 1 – Wiping Activities on the User’s Device May**
1345 **Inadvertently Delete the User’s Personal Data**

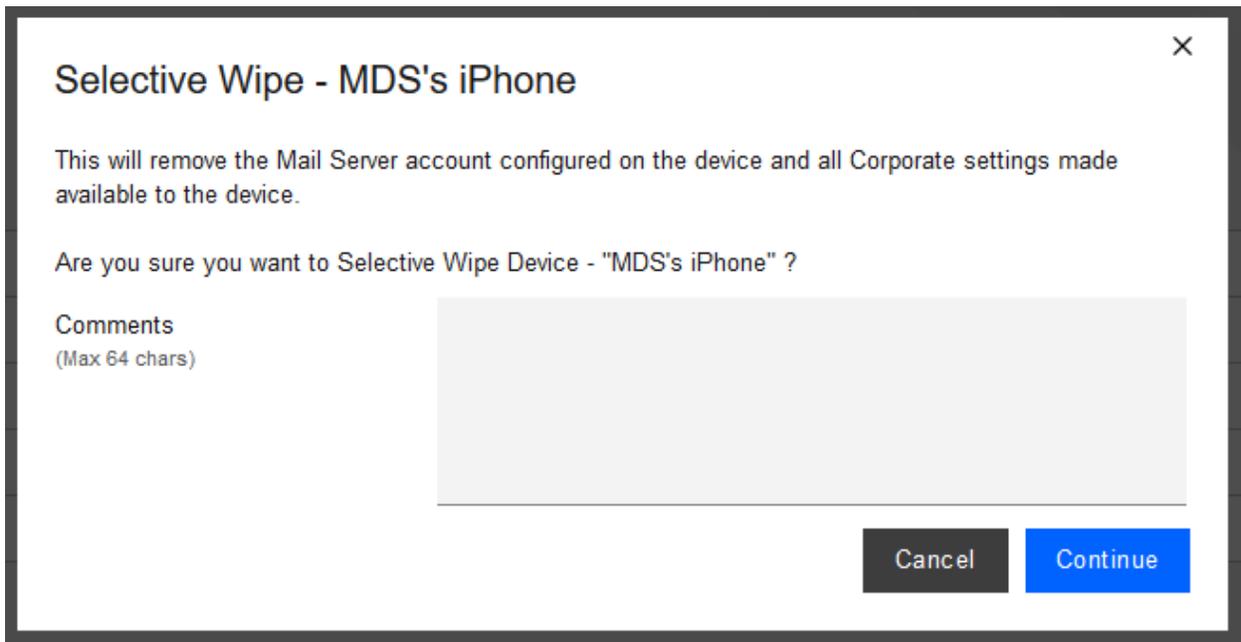
1346 **Summary:** Personal data that is comingled in the organizationally controlled portions of the phone could
1347 be lost during selective wipe of the device.

1348 **Test Activity:** Selectively wipe a device using MaaS360; restrict staff access to performing wiping of work
1349 profile data.

1350 **Desired Outcome:** The user will no longer be able to access work applications and data on the device
1351 and retains all access to their personal applications and data. The restricted administrator accounts will
1352 not be able to remove work profile data.

1353 **Observed Outcome:** Corporate data and applications are removed while personal data is untouched.
1354 The EMM console removes staff access to performing work profile wiping. Figure 2-71 shows initiation
1355 of a selective wipe. The selective wipe will remove the Mail Server account and all corporate settings
1356 available to the device.

1357 **Figure 2-71 Selective Wipe**



1358 **Additional Potential Mitigations:**

- 1359
- Notify users of use policy regarding corporate applications
 - Disallow configuration of work applications by users where possible to prevent comingling of personal and work data
 - Restrict staff access to system capabilities that permit removing device access or performing wipes.
- 1360
- 1361
- 1362
- 1363

1364 **D.11 Privacy Risk 2 – Organizational Collection of Device Data May**
1365 **Subject Users to Feeling or Being Surveilled**

1366 **Summary:** The user may experience surveillance from the organization collecting device application and
1367 location data.

1368 **Test Activity:** Disable location tracking and verify that applications outside of the organizationally
 1369 controlled portions of the phone are not inventoried by the EMM.

1370 **Desired Outcome:** Collection of application and location data is restricted by the EMM. The EMM does
 1371 not collect an inventory of personal applications on the device and does not collect location information,
 1372 including physical address, geographic coordinates and history, internet protocol (IP) address, and
 1373 service set identifier (SSID).

1374 **Observed Outcome:** When inspecting a device, location and application inventory information are not
 1375 collected by an EMM, and application inventory information is not transmitted to Kryptowire. Collection
 1376 of the installed personal apps are restricted by OS-level controls.

1377 Figure 2-72 shows inventory information for **installed** applications. When privacy restrictions are
 1378 configured, only corporate application inventory information is collected. No personal applications are
 1379 found in the EMM’s installed applications list.

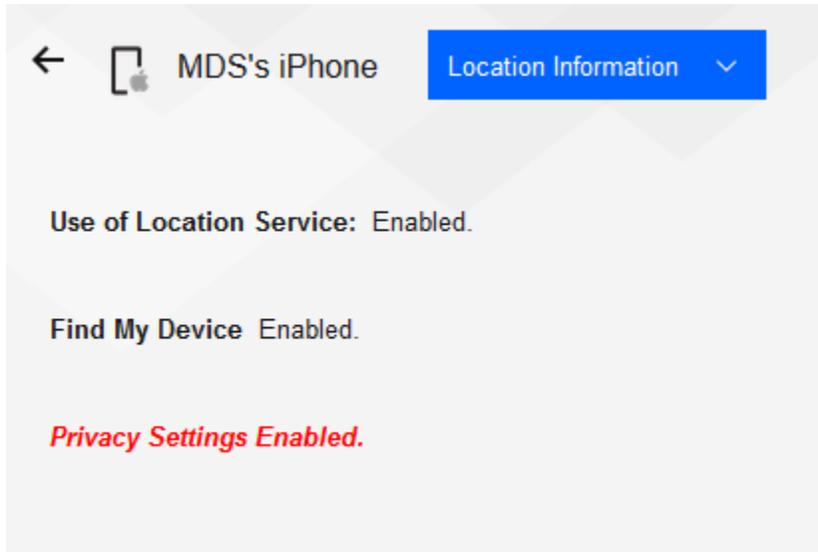
1380 **Figure 2-72 Application Inventory Information**

Application...	App ID	Full Version	Application...	Data Size (...)	Managed	App Source	Complianc...	Action	View Security...
GlobalProtect	com.paloaltonet works.globalprot ect.vpn	5.1.1	8.46	0.77	Installed by MDM	iTunes	Required	Remove App	Security Details
MaaS360	com.fiberlink.ma as360forios	3.97.36	147.02	2.99	Installed by MDM	iTunes	Required	Remove App	Security Details
MaaS360 VPN	com.fiberlink.ma as360.maas360v pn	3.20.50	7.53	0.02	Installed by MDM	iTunes	Required	Remove App	Security Details
zIPS	com.zimperium. zIPS.appstore	4.12.0	36.94	0.05	Installed by MDM	iTunes	Required	Remove App	Security Details

Navigation: < < 1 > > | Jump To Page | Displaying 1 - 4 of 4 Records | CSV | Export

1381 The following figure shows that privacy settings have been enabled to restrict collection of location
 1382 information.

1383 Figure 2-73 Location Information Restricted

1384 **Additional Potential Mitigations:**

- 1385
- 1386
- 1387
- 1388
- Restrict staff access to system capabilities that permit reviewing data about employees and their devices.
 - Limit or disable collection of specific data elements.
 - Dispose of personally identifiable information (PII).

1389 **D.12 Privacy Risk 3 - Mobile security services may not alert users to what**

1390 **information is collected**

1391 **Summary:** Users may not have knowledge of what information is collected and monitored by the

1392 organization.

1393 **Test Activity:** Test to ensure that MDM provides custom notification to users detailing collected device

1394 information.

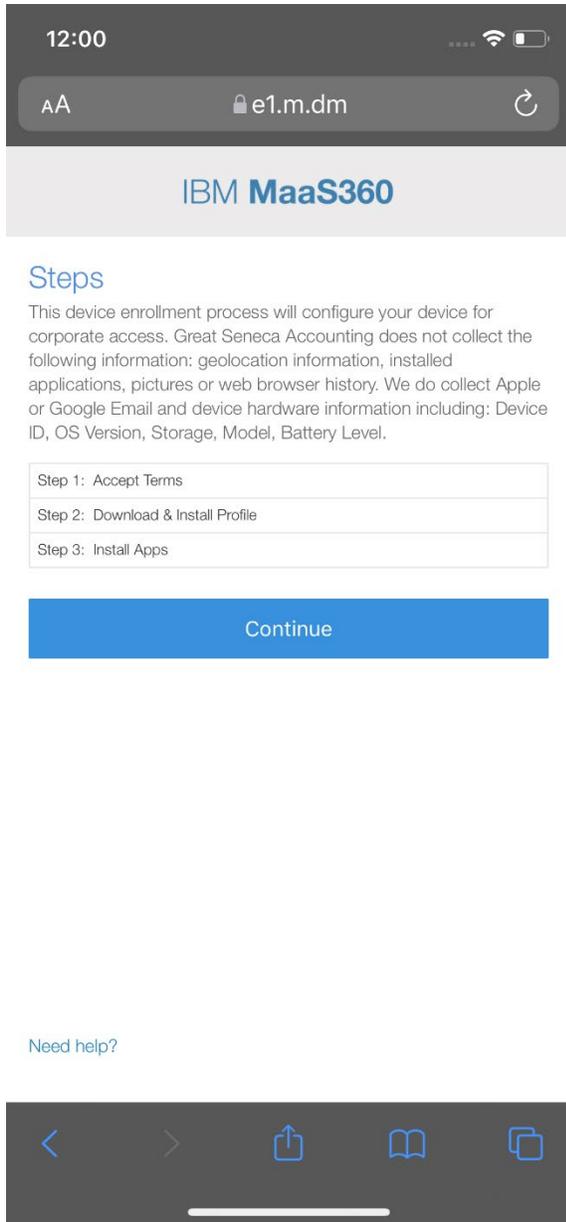
1395 **Desired Outcome:** MDM provides details of what information is collected during device enrollment.

1396 **Observed Outcome:** Device data collection information is displayed to users.

1397 [Figure 2-74](#) demonstrates how users will be notified of what device information is collected by mobile

1398 security products during the device enrollment process.

1399 **Figure 2-74 Mobile Device Information Collection Notification**



1400 **Additional Potential Mitigations:**

- 1401 • Provide notification to the user
- 1402 • Train users on mobile device collection policy
- 1403 • Provide a point of contact for user questions regarding organizational data collection and use
- 1404 policies

1405 **D.13 Privacy Risk 4 – Data Collection and Transmission Between**
1406 **Integrated Security Products May Expose User Data**

1407 **Summary:** Access to monitoring data from the device is not restricted to administrators. Application and
1408 location data are shared with third parties that support monitoring, data analytics, and other functions
1409 for operating the BYOD solution.

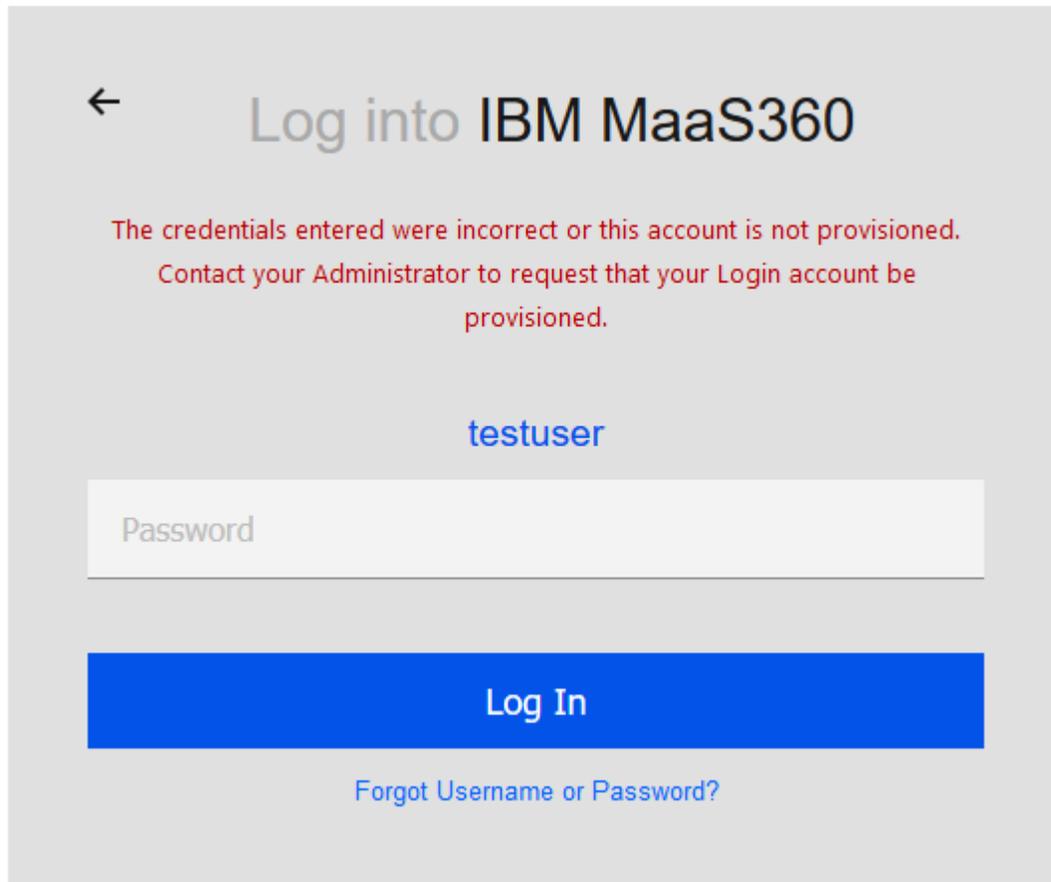
1410 **Test Activity:** Attempt to log in to the MaaS360 admin portal without domain administrator permissions.

1411 **Desired Outcome:** System provides access controls to monitoring functions and logs. Data flow between
1412 the organization and third parties does not contain location information, including physical address,
1413 geographic coordinates and history, IP address, and SSID.

1414 **Observed Outcome:** Domain administrators were allowed to log in, but non-administrator users were
1415 not.

1416 [Figure 2-75](#) demonstrates how a non-administrator account will be prevented from logging into the
1417 MaaS360 portal.

1418 Figure 2-75 Non-Administrator Failed Portal Login



1419 Figure 2-76 - Admin Login Settings

▼ Login Settings

Use this section to configure strong portal authentication for your Administrators.

Note: MaaS360 portal authentication mechanism will be used by default if Federated Single Sign-on is not used

Configure Federated Single Sign-on

- Use SAML for Single Sign-on
- Authenticate against Corporate User Directory

You will need to install Cloud Extender for this. For help with configuration refer to the [installation guide](#).

Default Domain

Custom login URL for your administrators: <https://m1.maas360.com/login?custID:>

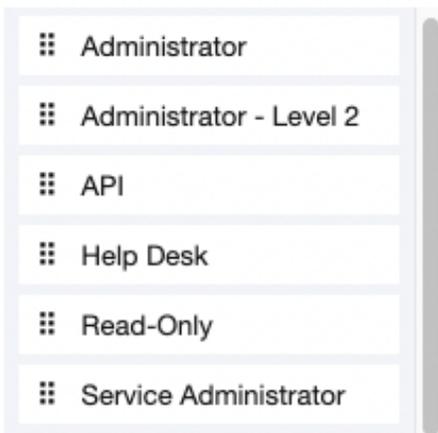
Automatically create new Administrator accounts and update roles based on User Groups

User Groups (Specify the Distinguished Name of the User Groups)

▼ ⊖

▼ ⊕

1420 Figure 2-77 - Administrator Levels



1421 **Potential Mitigations:**

- 1422 • De-identify personal and device data when such data is not necessary to meet processing
1423 objectives.
- 1424 • Encrypt data transmitted between parties.
- 1425 • Limit or disable access to data.
- 1426 • Limit or disable collection of specific data elements.
- 1427 • Use policy controls such as contracts to limit third-party data processing.