

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 Updates	58
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.

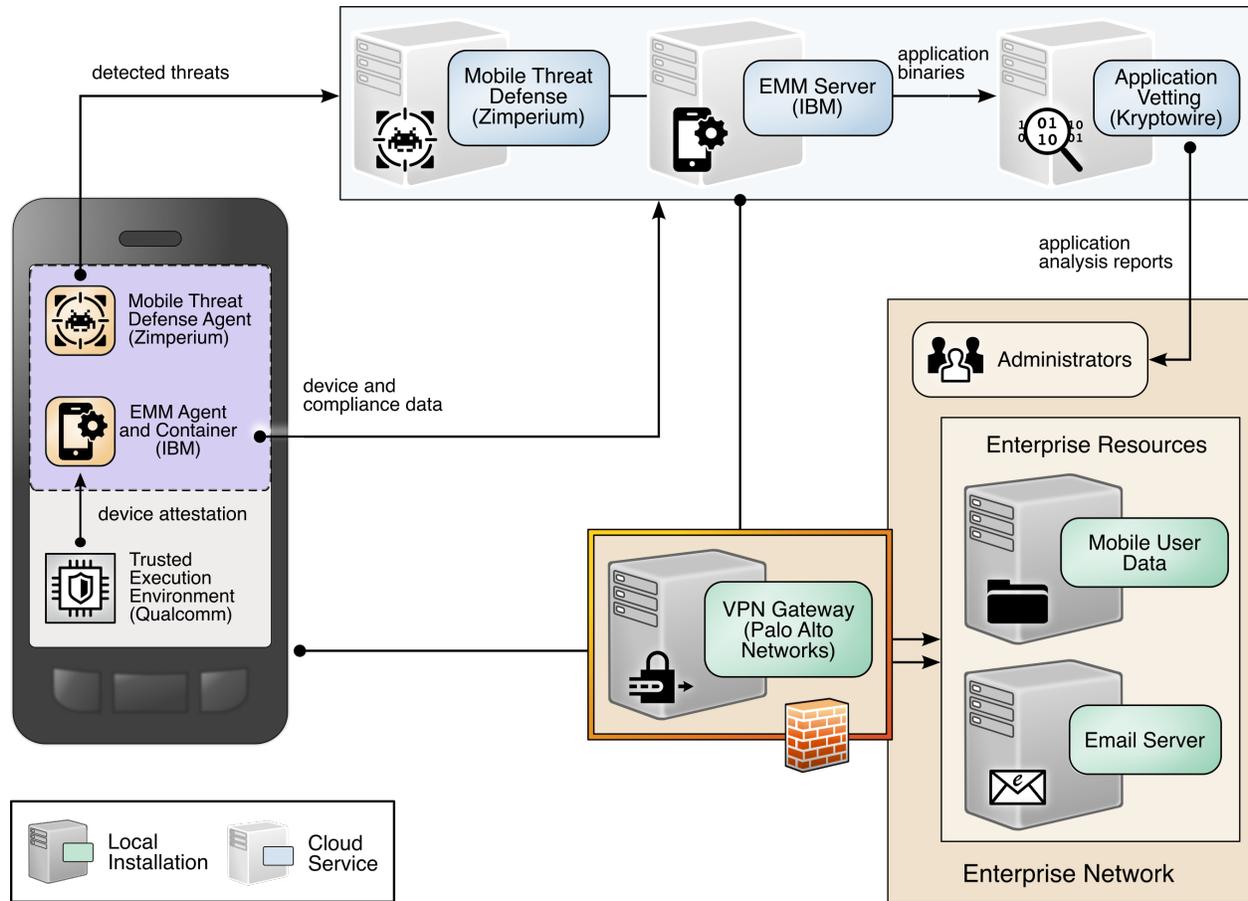
Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
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**

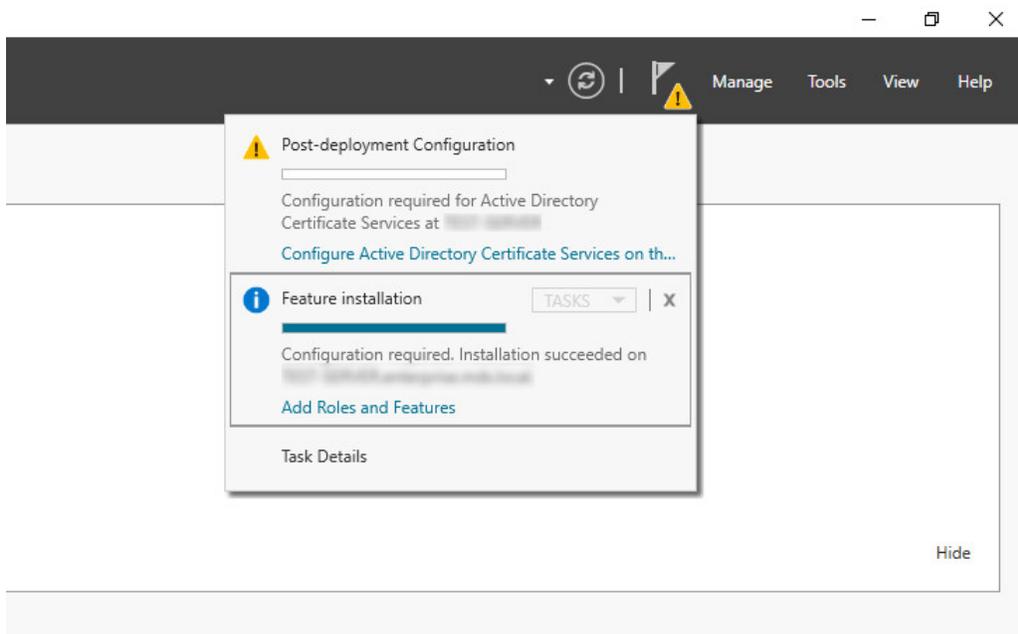
332 A Network Device Enrollment Service (NDES)/Simple Certificate Enrollment Protocol (SCEP) server was
 333 used to issue client certificates to new devices that were enrolled by using MaaS360. This guide assumes

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.

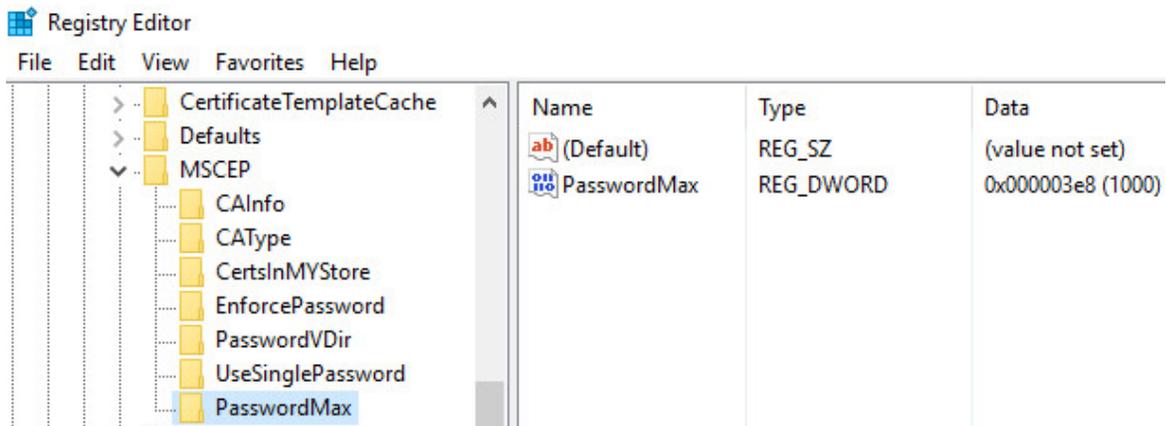
354 10. Check **Network Device Enrollment Service**. Click **Next**.

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**.

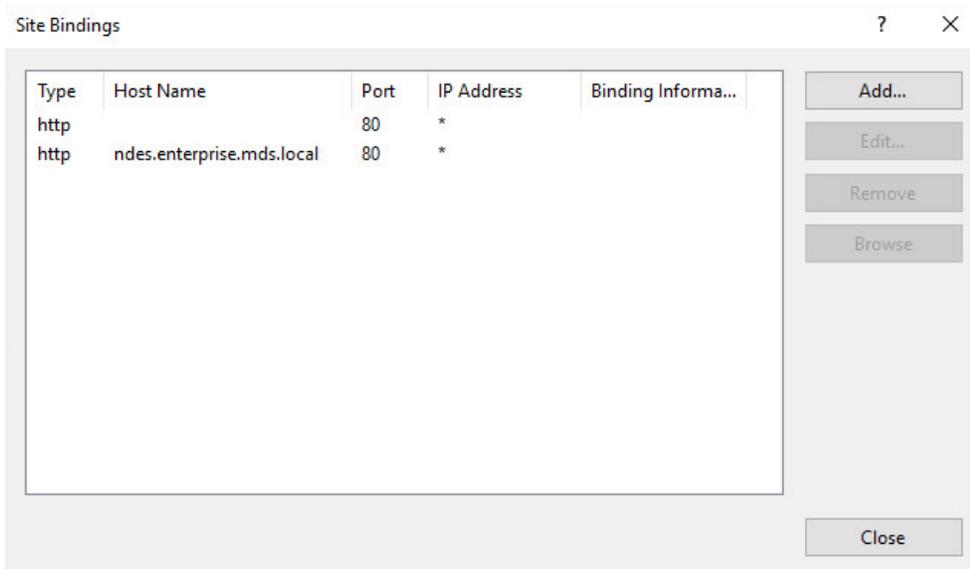
401 36. On the left, expand **NDES > Sites**, and select **Default Web Site**.

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

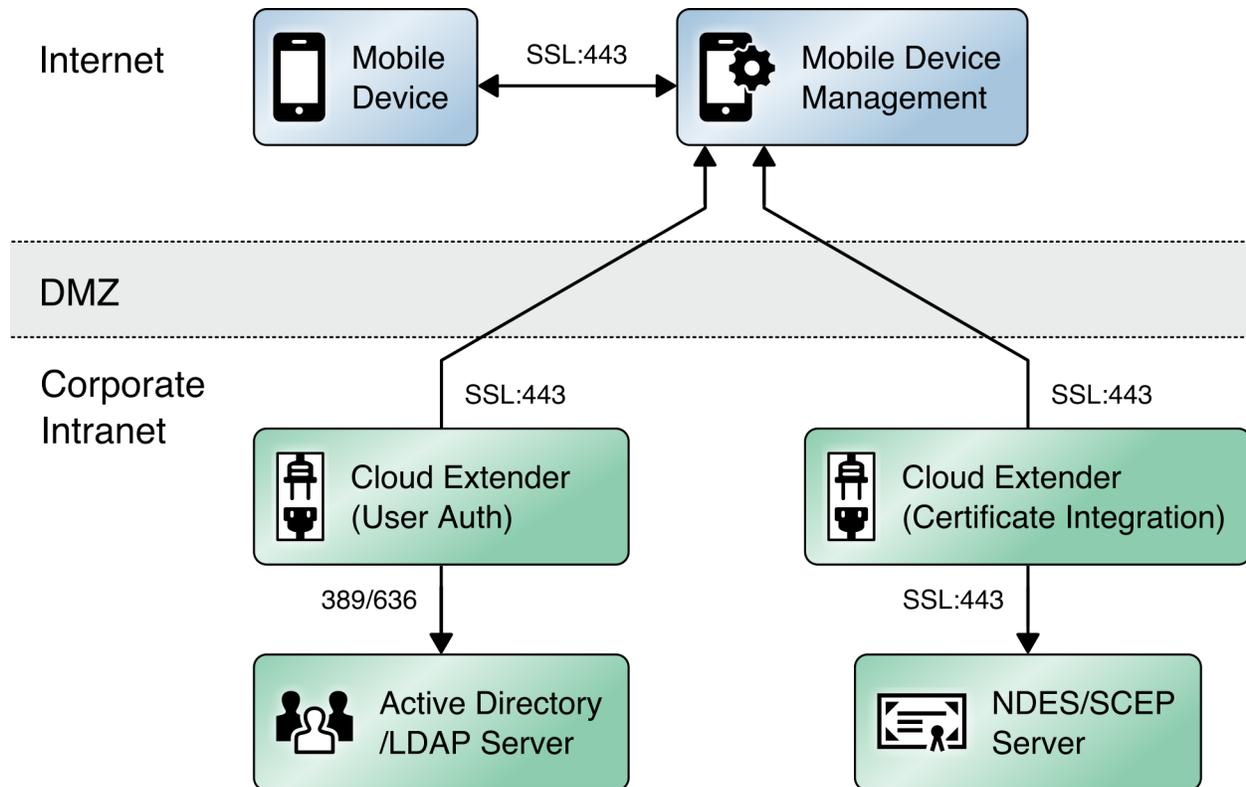
412 International Business Machines (IBM) contributed an instance of MaaS360
 413 (<https://www.ibm.com/products/maas360/unified-endpoint-management>) to deploy as the mobile
 414 device management (MDM) solution.

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**

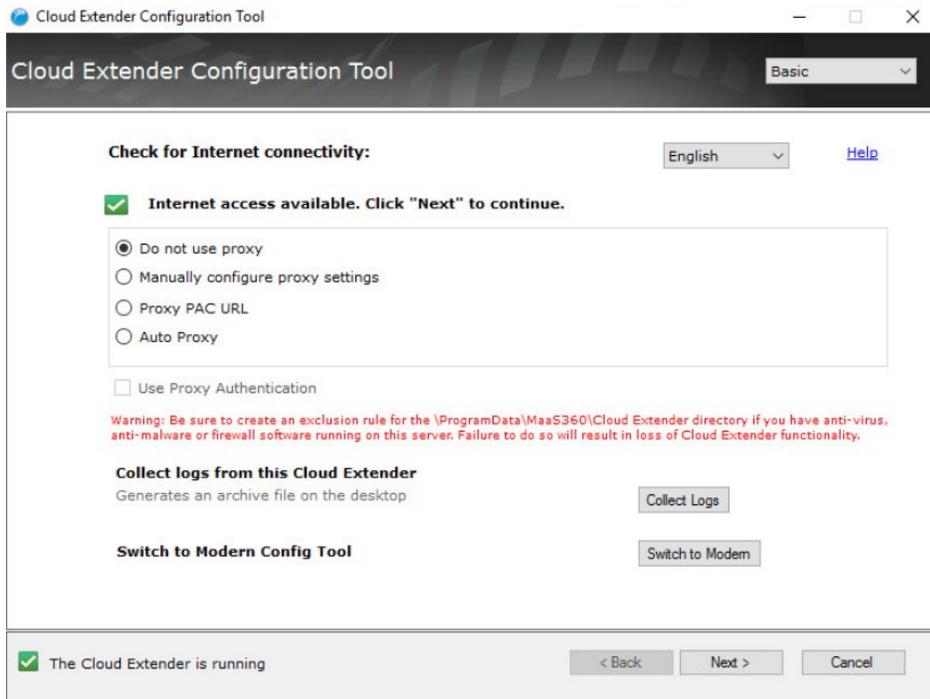
- 422 1. Log in to the MaaS360 web portal.
- 423 2. Click **Setup > Cloud Extender**.
- 424 3. Click the link that says **Click here to get your License Key**. The license key will be emailed to the
- 425 currently logged-in user's email address.
- 426 4. Click the link that says **Click here to download 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 ⓘ

2 Service Account ⓘ

3 Finish

Provide Service Account details

Service account should be:
 1. Domain User on Active Directory
 2. Local Administrator on this server

Username

Password

Domain

Enable Secure Authentication Mode

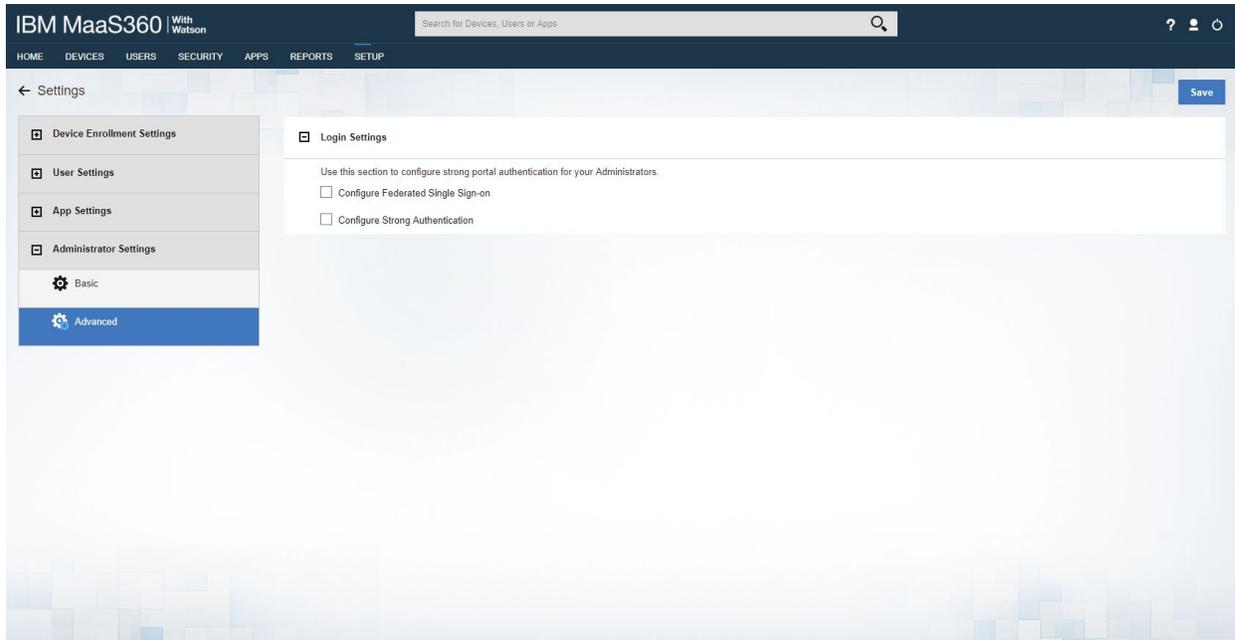
✔ The Cloud Extender is running

- 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

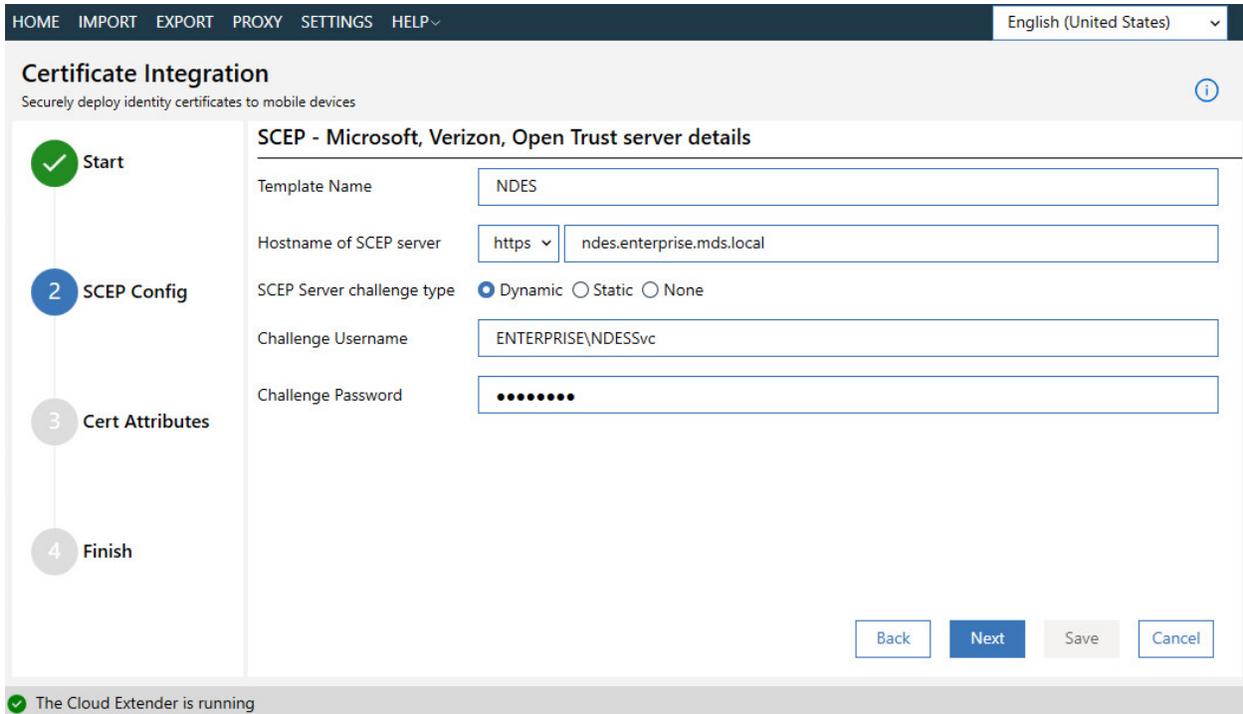
User Groups (Specify the Distinguished Name of the User Groups)

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) v

Certificate Integration

Securely deploy identity certificates to mobile devices ⓘ

Certificate Properties

Subject Name ⓘ /CN=%uname%/emailAddress=%email%

Subject Alternate Name None v

Cache certs on Cloud Extender

Location of Certificate Cache C:\CertCache

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.

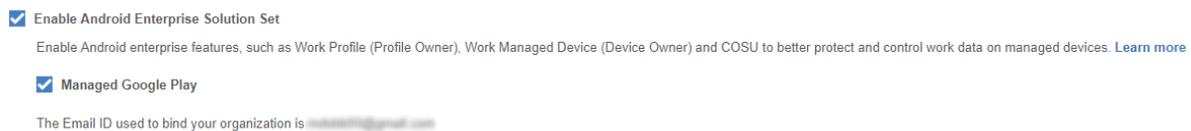
488 2.2.2 Android Enterprise Configuration

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

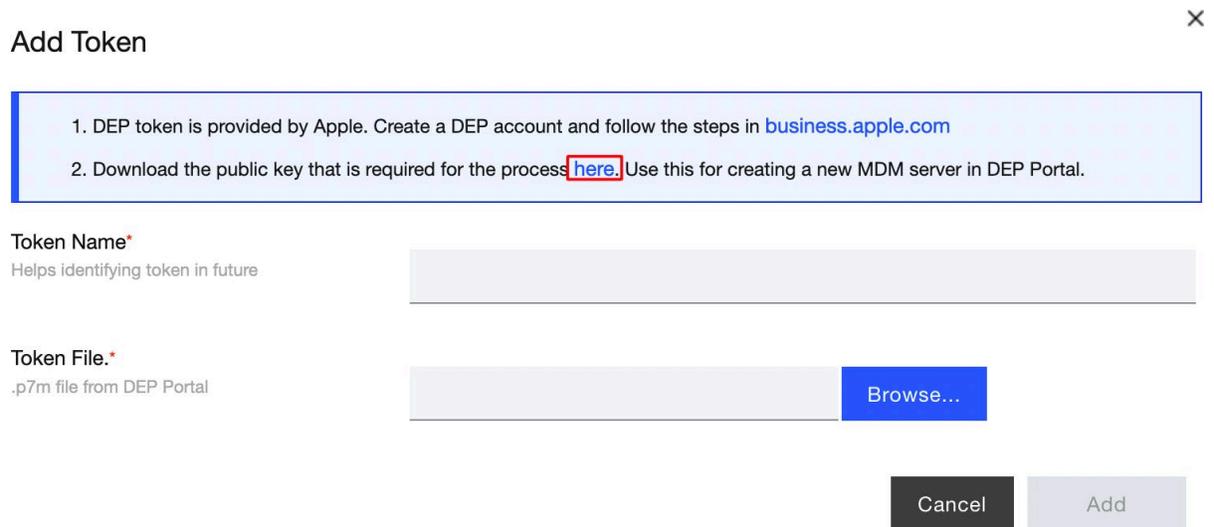
512 [IBM documentation](#).

513 2.2.4 Apple User Enrollment (UE) Configuration

514 2.2.4.1 Apple Business Manager (ABM) Configuration

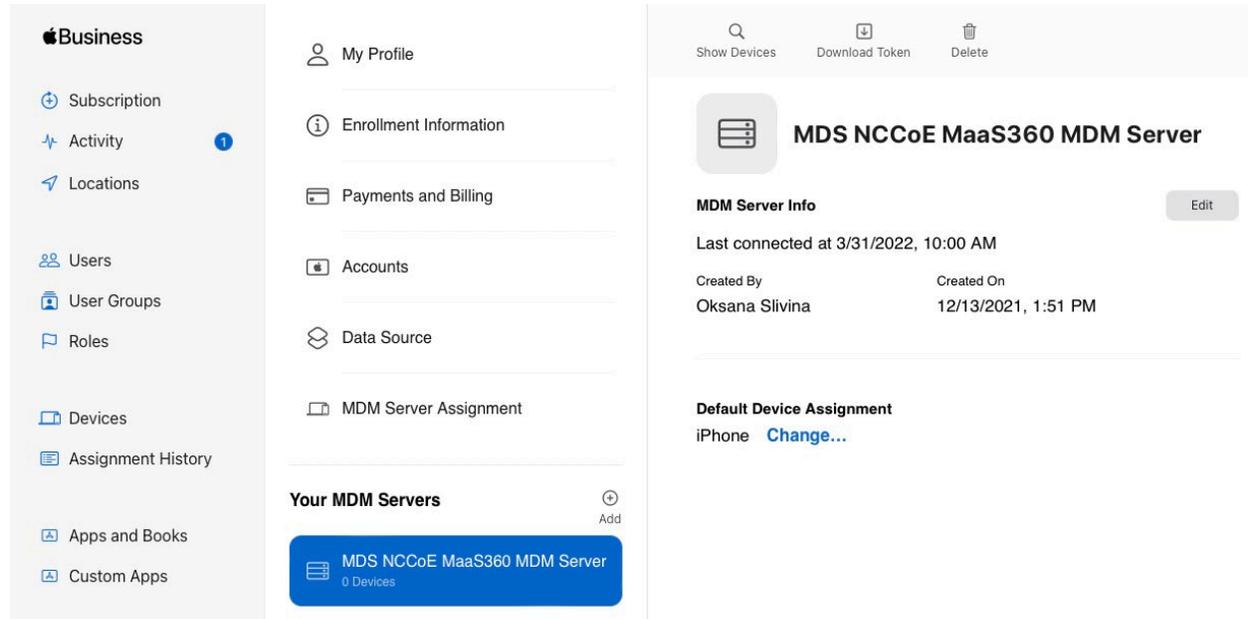
- 515 1. In MaaS360, navigate to **Setup > Settings > Enrollment Programs**, and click **Configure** next to *Apple*
- 516 *Device Enrollment Program*.
- 517 2. In the popup, click **Continue**.
- 518 3. Click **Tokens > Add Token**.
- 519 4. In the popup, give the token a name and click on the **here** 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.

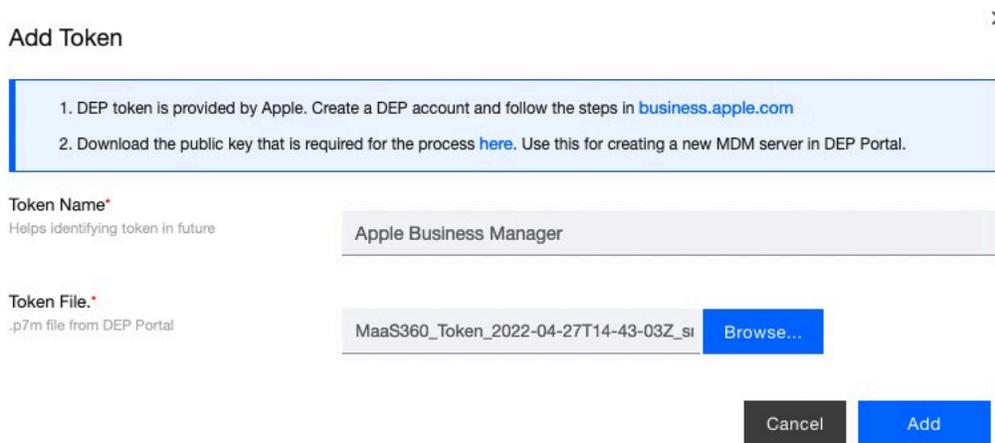
527 **Figure 2-13 MDM configuration in Apple Business Manager**



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**

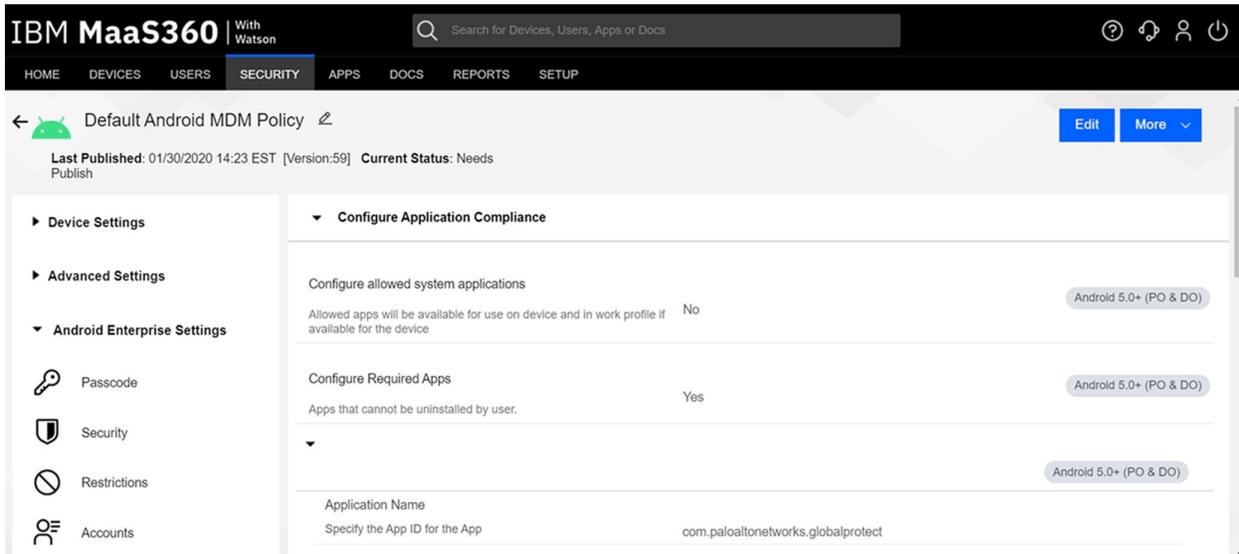
- 555 1. Navigate to **Security > Policies**.
- 556 2. Click the appropriate deployed Android policy.

- 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.

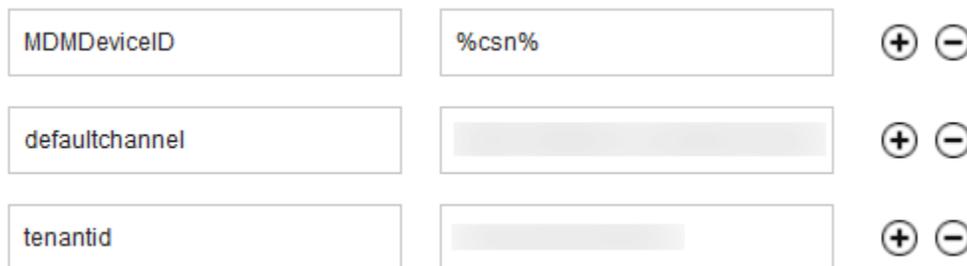
694 2.3.2 Automatic Device Activation

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

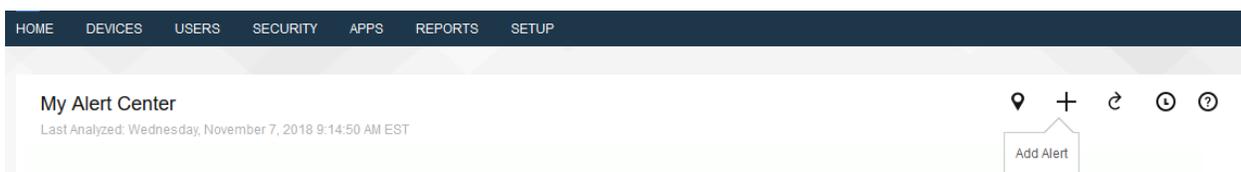
734 From the IBM MaaS360 web portal:

- 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 'Security'. The 'Advanced Search' section includes: 1. Search for: Active Devices (selected), Inactive Devices, All Devices; 2. With Device Type(s): Smartphones (checked), Tablets (checked); 3. Last Reported: Last 7 Days; 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 partially visible with 'Select Category', 'Select Attribute', 'Select Criteria', and 'Enter Text'.

- 761 8. Click **Update**.

762 2.4 Palo Alto Networks Virtual Firewall

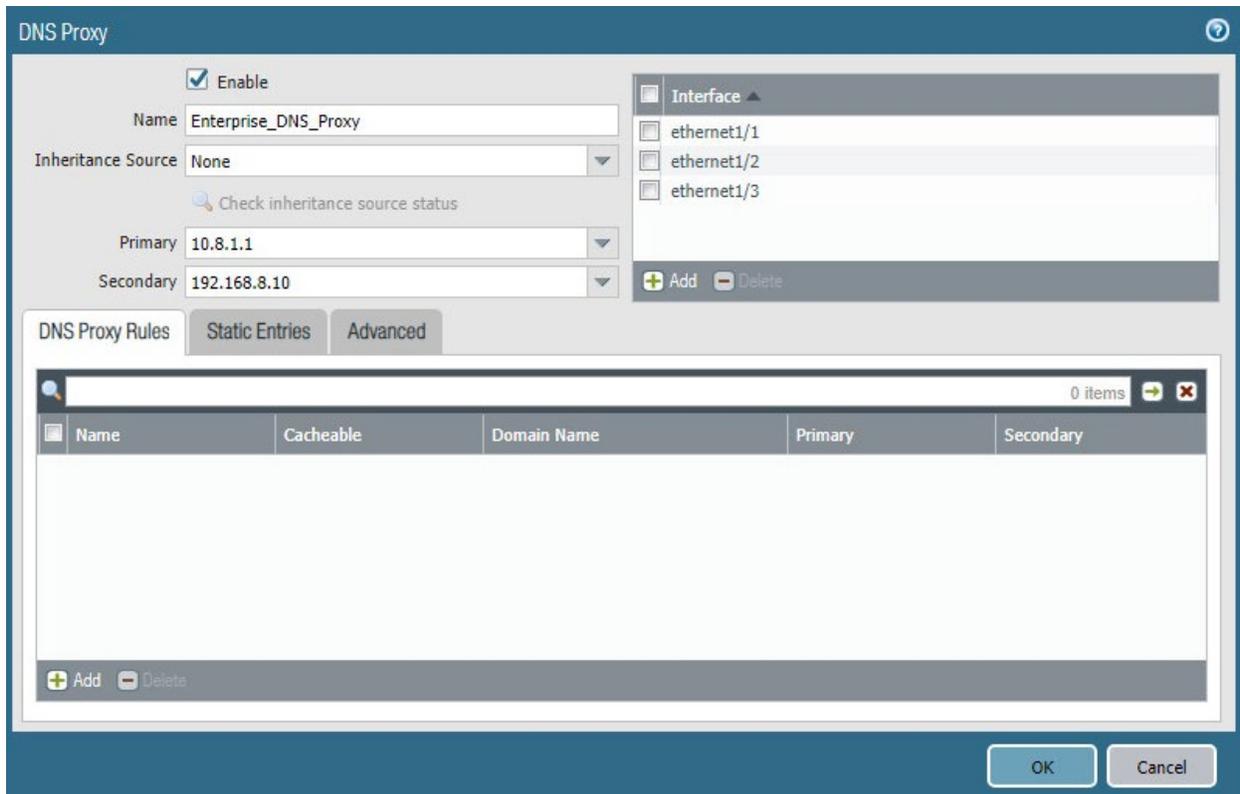
763 Palo Alto Networks contributed an instance of its VM-100 series firewall for use on the project.

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**.

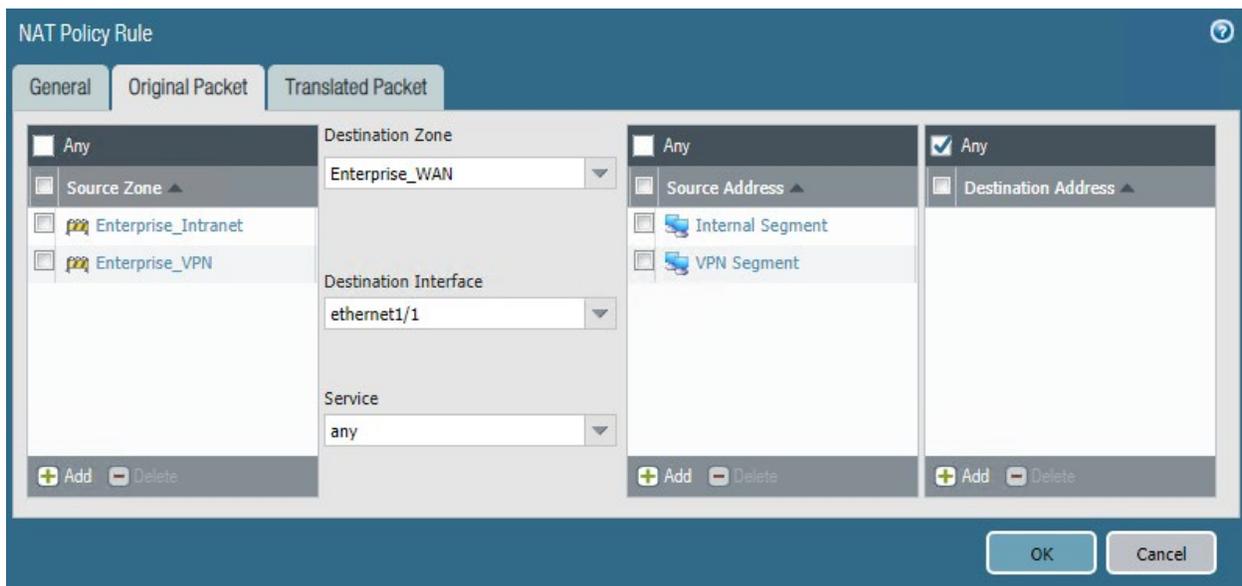
795 Figure 2-23 DNS Proxy Object Configuration



- 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

CA Certificates	Name	Default OCSF URL	OCSF Verify Certificate
<input type="checkbox"/>	Internal Root		
<input type="checkbox"/>	Internal Sub		

Use CRL CRL Receive Timeout (sec) 5
 Use OCSP OCSP Receive Timeout (sec) 5
OCSP takes precedence over CRL Certificate Status Timeout (sec) 5

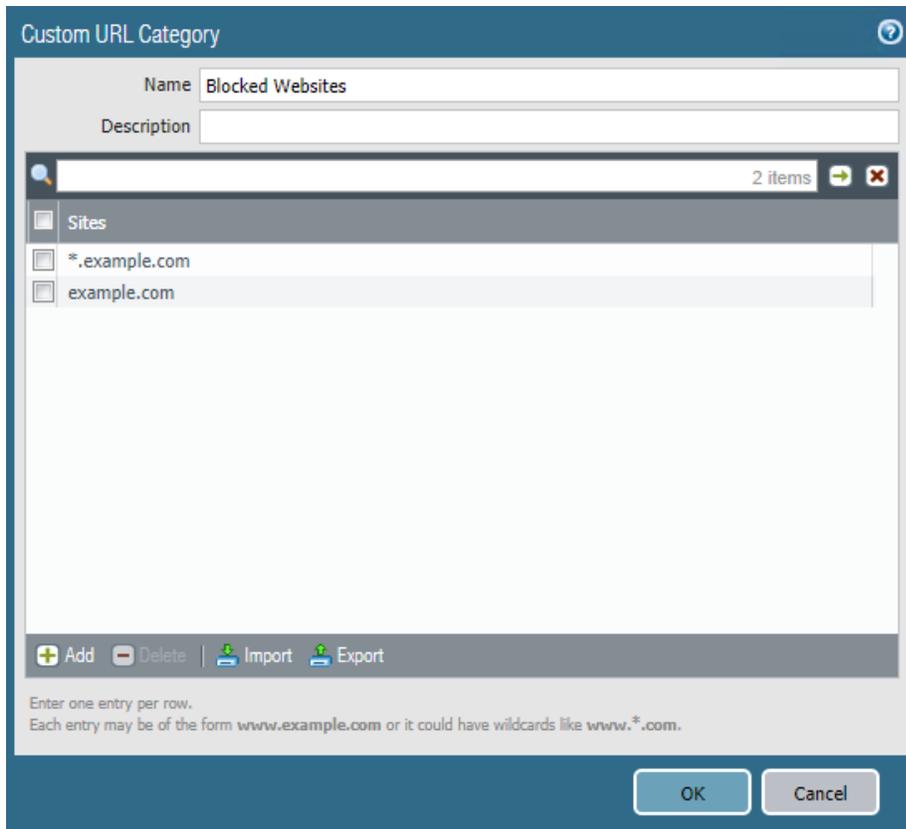
Block session if certificate status is unknown
 Block session if certificate status cannot be retrieved within timeout
 Block session if the certificate was not issued to the authenticating device
 Block sessions with expired certificates

OK Cancel

865 **2.4.5 Website Filtering Configuration**866 **2.4.5.1 Configure Basic Website Blocking**

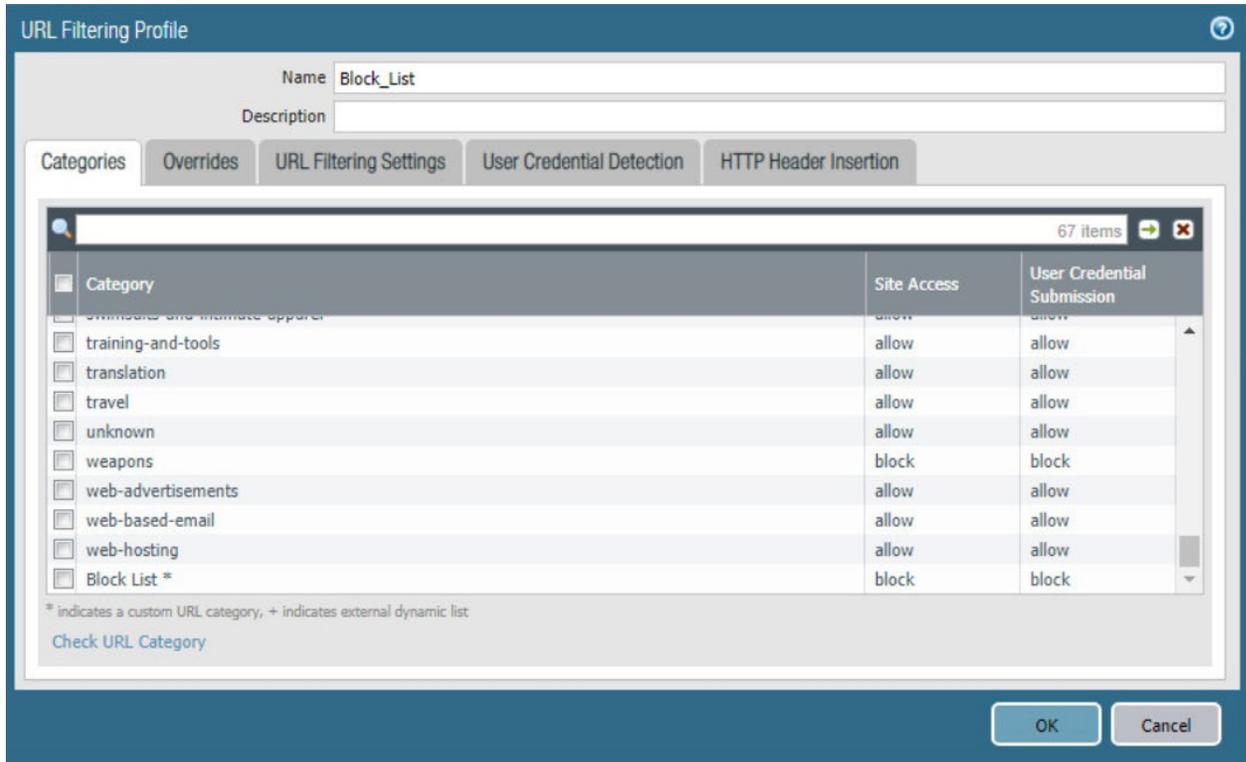
- 867 1. Navigate to **Objects > URL Category**.
- 868 2. Click **Add**.
- 869 3. Enter a name for the **URL Category**. Click **Add** on the bottom.
- 870 4. Add websites that should be blocked. Use the form **.example.com* for all subdomains and *example.com* for the root domain.
- 871

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' is set to 'Allow'. Under 'Profile Setting', 'URL Filtering' is set to 'Block_List'. Under 'Log Setting', 'Log Forwarding' is set to 'None'. Under 'Other Settings', 'Schedule' and 'QoS Marking' are set to 'None', and 'Disable Server Response Inspection' is unchecked. The window has 'OK' and 'Cancel' buttons 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.

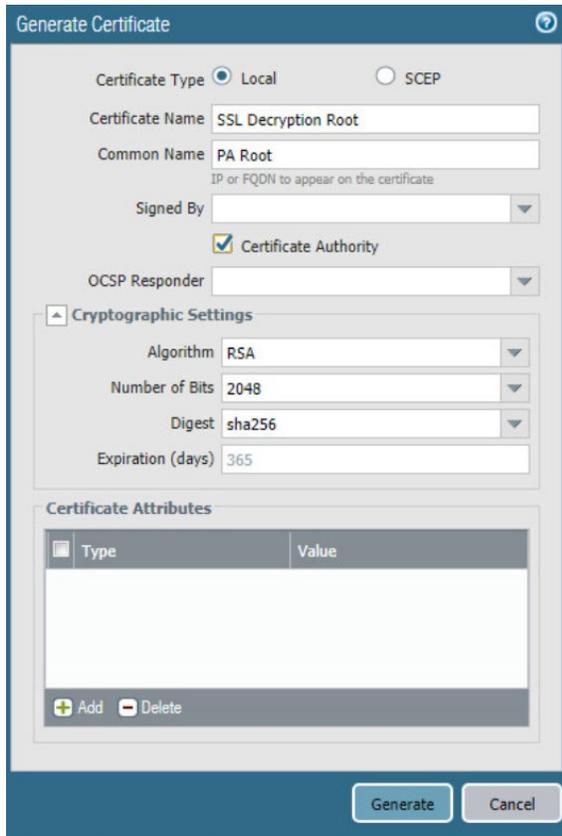
898 1. Navigate to **Device > Certificates**.

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.

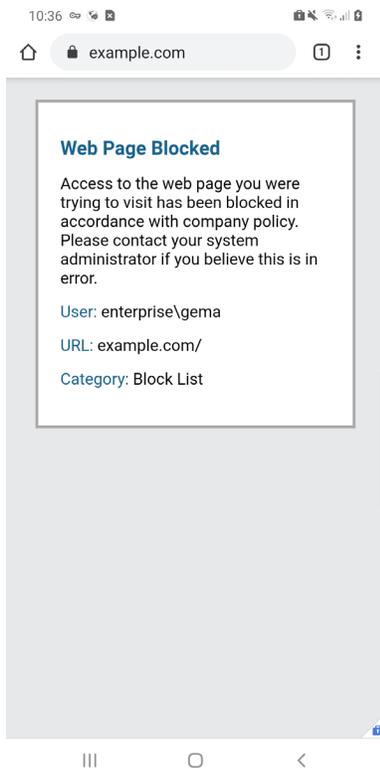
909 10. Check the box next to **Certificate Authority**.

910 11. Click **Generate**.

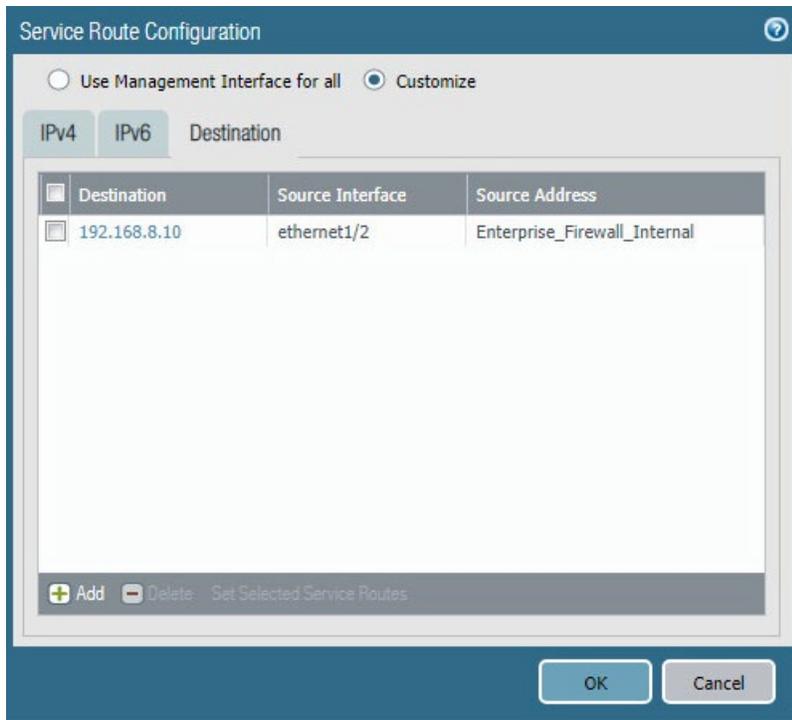
911 12. Click the newly created certificate.

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

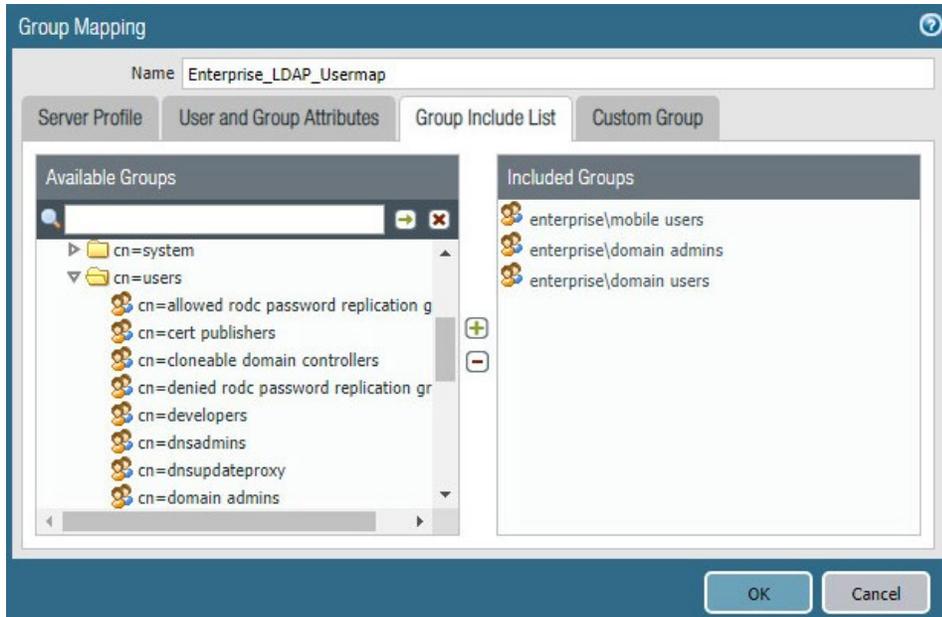
Retry Interval

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

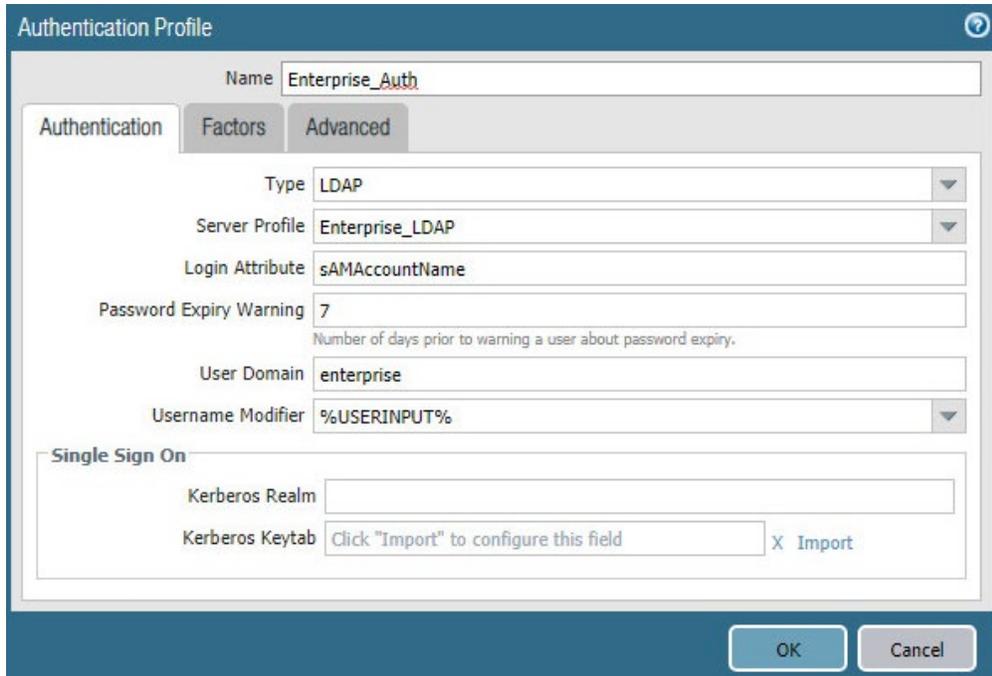
OK Cancel

- 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**

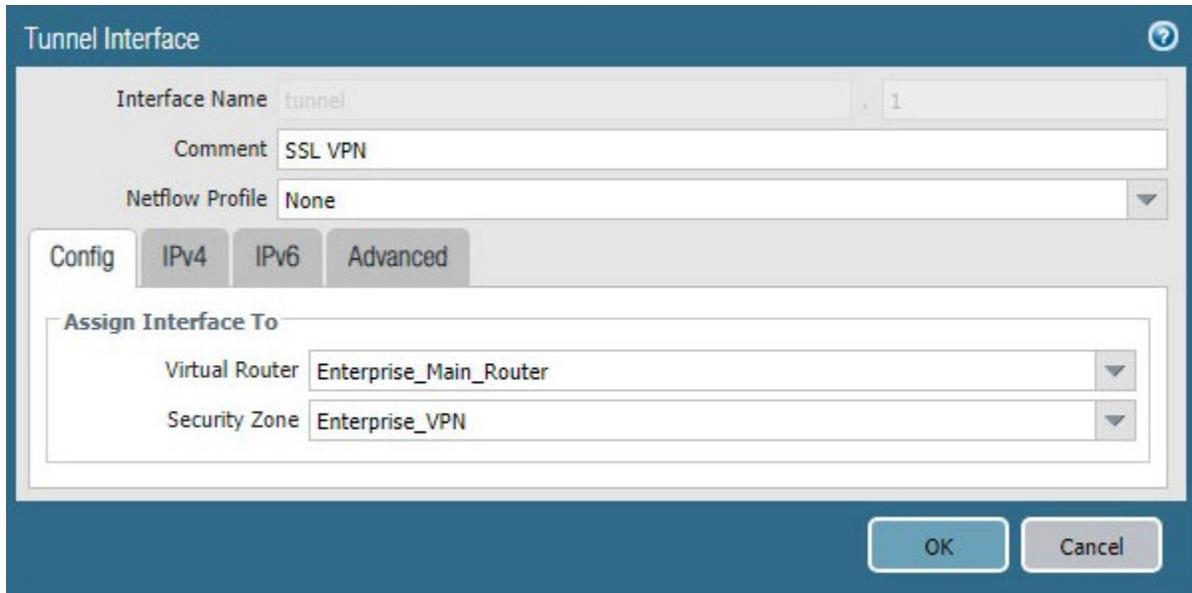
- 982 1. Navigate to **Network > Interfaces > Tunnel**.
- 983 2. Click **Add**.
- 984 3. Enter a tunnel number. Assign it to the main virtual router. Click **OK**.

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**



- 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

The screenshot shows a configuration window titled "Client Authentication". It contains the following fields and options:

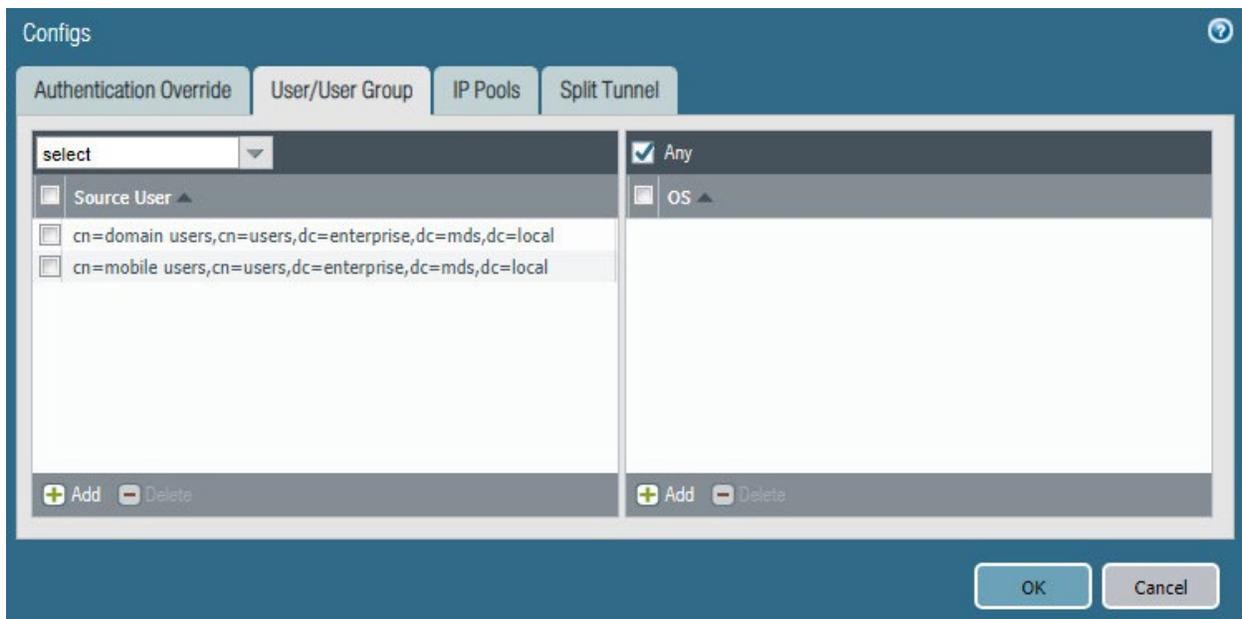
- Name:** iOS Auth
- OS:** iOS
- Authentication Profile:** Enterprise_Auth
- GlobalProtect App Login Screen:**
 - Username Label:** Username
 - Password Label:** Password
 - Authentication Message:** Enter login credentials
 - Authentication message can be up to 256 characters.
- Allow Authentication 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.

At the bottom right, there are "OK" and "Cancel" buttons.

- 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**

The screenshot shows the 'Zone' configuration window. The 'Name' field is 'Enterprise_VPN', 'Log Setting' is 'None', and 'Type' is 'Layer3'. Under 'Interfaces', 'tunnel.1' is listed. In the 'Zone Protection' section, the 'Zone Protection Profile' is 'None' and 'Enable Packet Buffer Protection' is unchecked. The 'User Identification ACL' section is expanded, showing 'Enable User Identification' checked. Below this are two lists: 'Include List' and 'Exclude List', both currently empty. Each list has a text prompt: 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24' and 'Add'/'Delete' buttons. The 'Include List' section is labeled 'Users from these addresses/subnets will be identified.' and the 'Exclude List' section is labeled 'Users from these addresses/subnets will not be identified.' At the bottom of the window are 'OK' and 'Cancel' buttons.

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 vertical menu 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

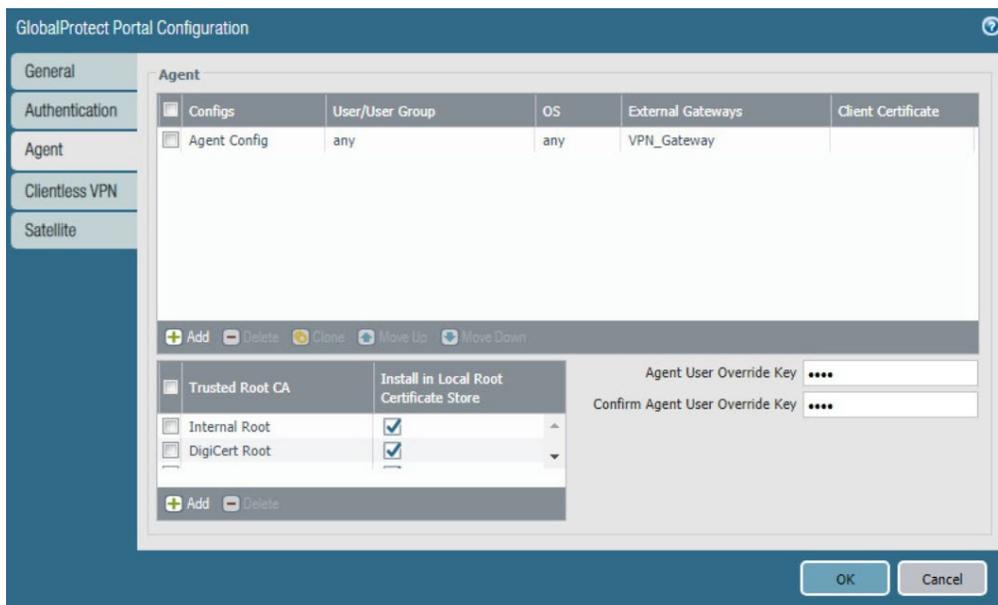
Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

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)

OK Cancel

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

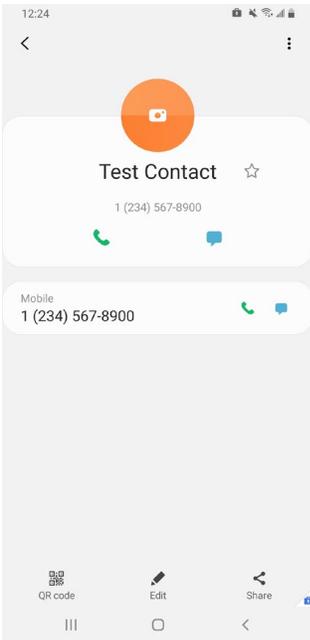


Figure 2-50 Personal Profile Can't See Work Contacts

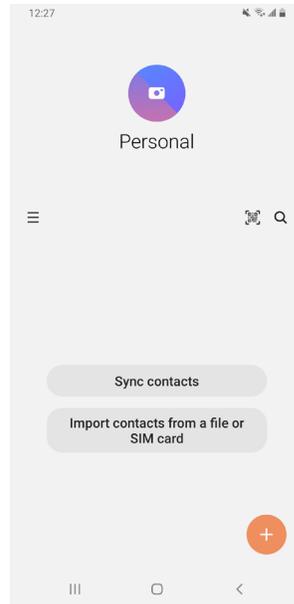


Figure 2-51 Contact Created in Managed App

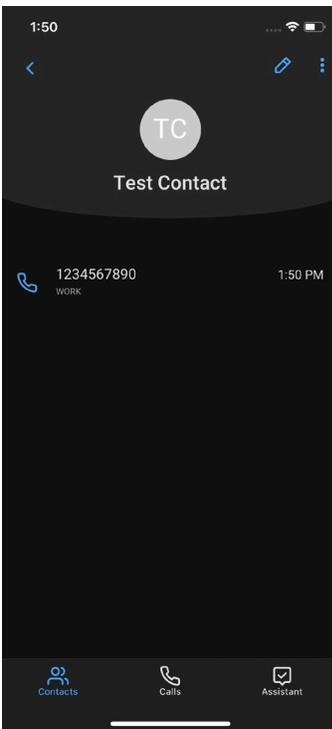
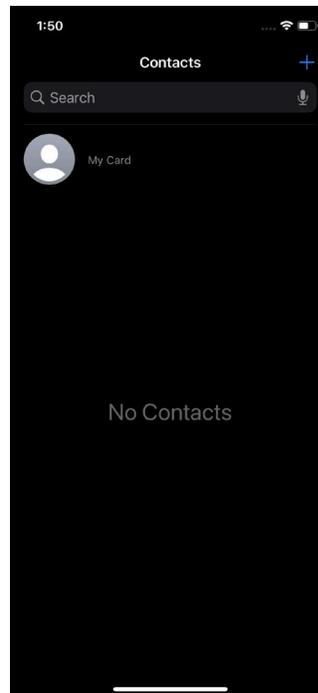


Figure 2-52 Unmanaged App Can't See Managed Contacts



1187 D.2 Threat Event 2

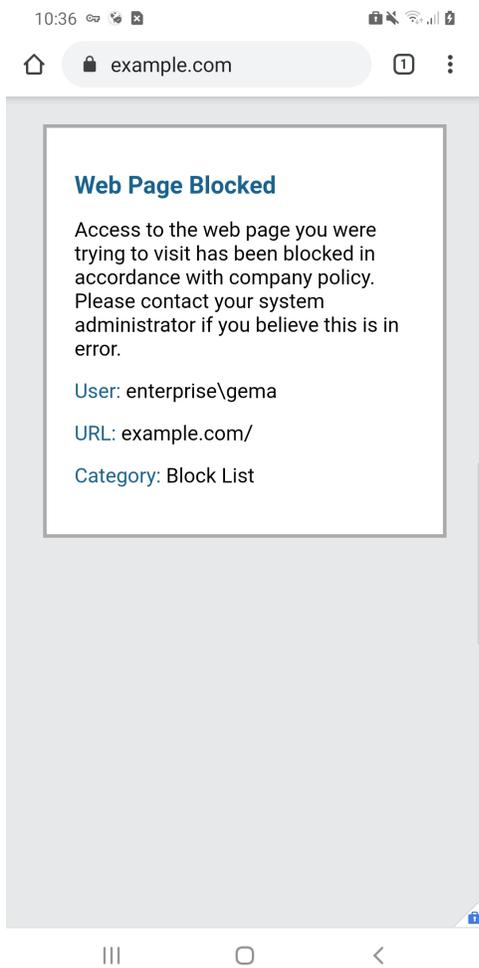
1188 **Summary:** A fictional phishing event was created to test protection against the theft of credentials
1189 through an email phishing campaign.

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).

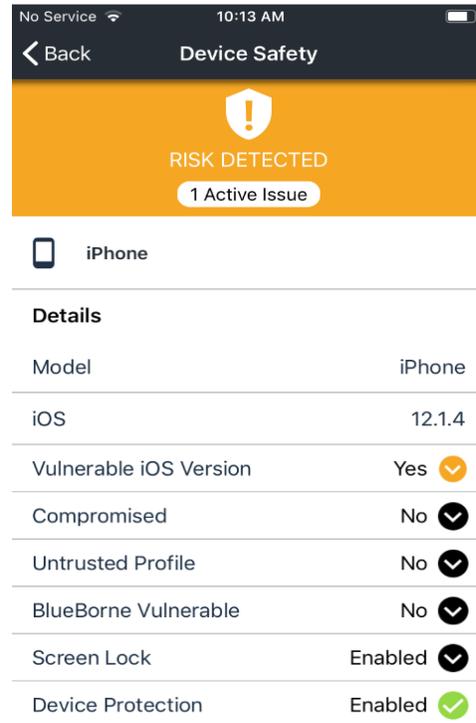
1214 **Desired Outcome:** The enterprise's security architecture should identify the presence of devices that are
1215 running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be
1216 possible, when warranted by the risks, to block devices from accessing enterprise 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

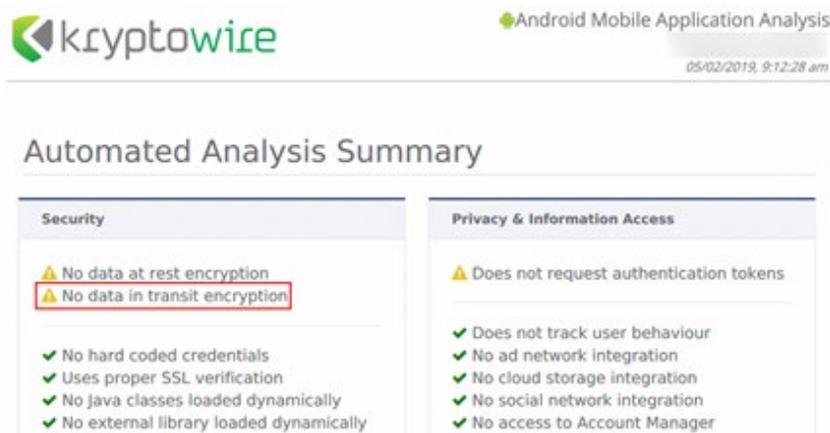
1225 **Summary:** Loss of confidentiality of sensitive information via eavesdropping on unencrypted device
 1226 communications.

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

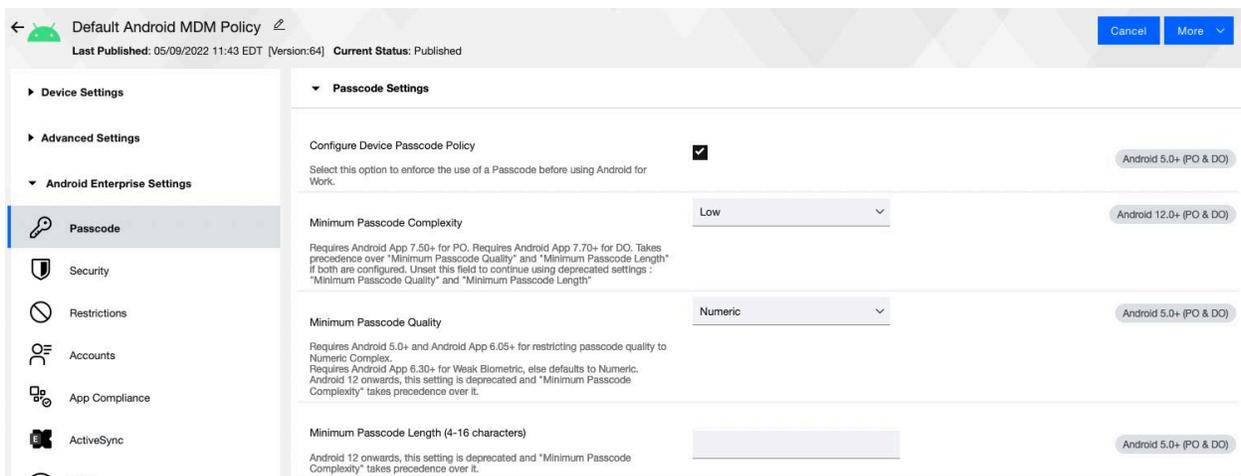
1250

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.

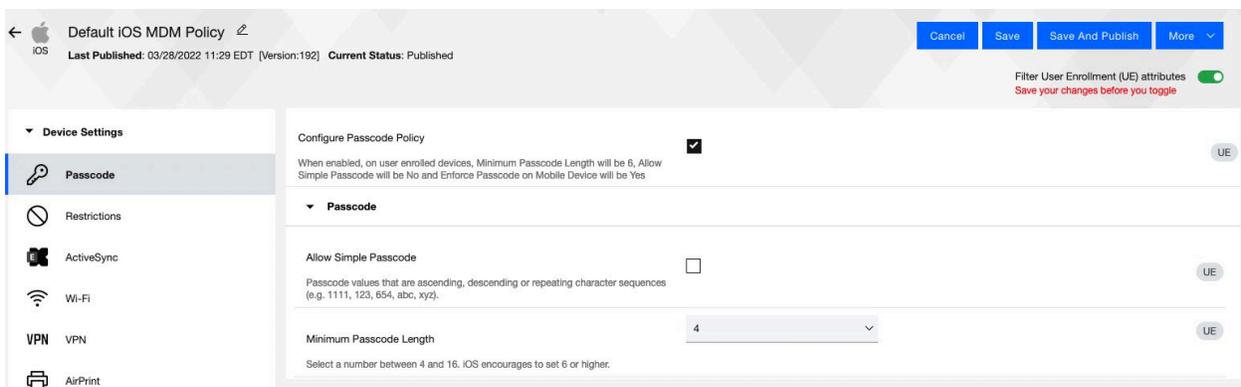
1254 Additionally, the MTD (Zimperium) can identify and report iOS devices with a disabled lock screen.

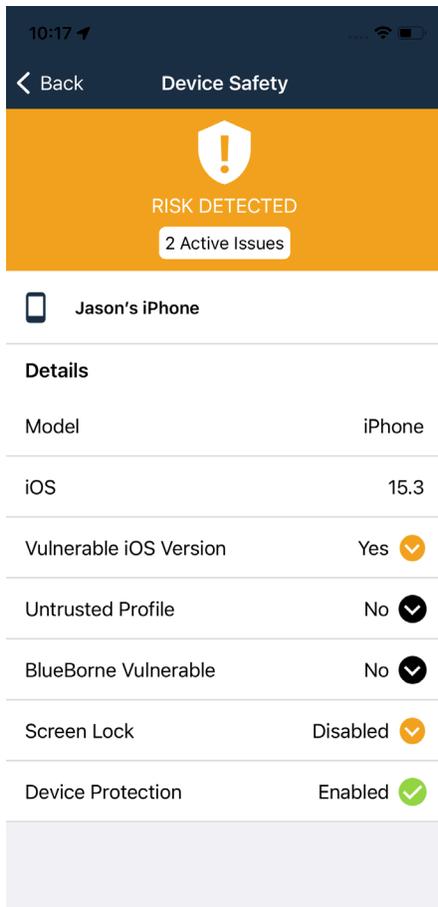
1255 **Observed Outcome:** MaaS360 applies a policy to the devices to enforce a mandatory PIN, Zimperium
 1256 reports devices with a disabled lock screen, and GlobalProtect requires periodic re-authentication using
 1257 MFA. Figures 2-57 through 2-59 show the passcode and lockscreen configuration settings.

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**

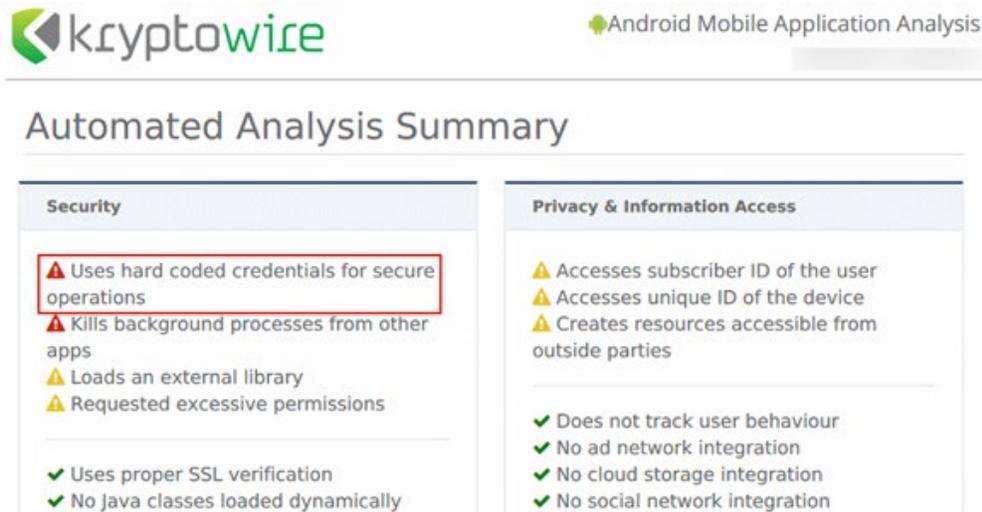
1262 **Summary:** Unauthorized access to backend services via authentication or credential storage
 1263 vulnerabilities in internally developed applications.

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

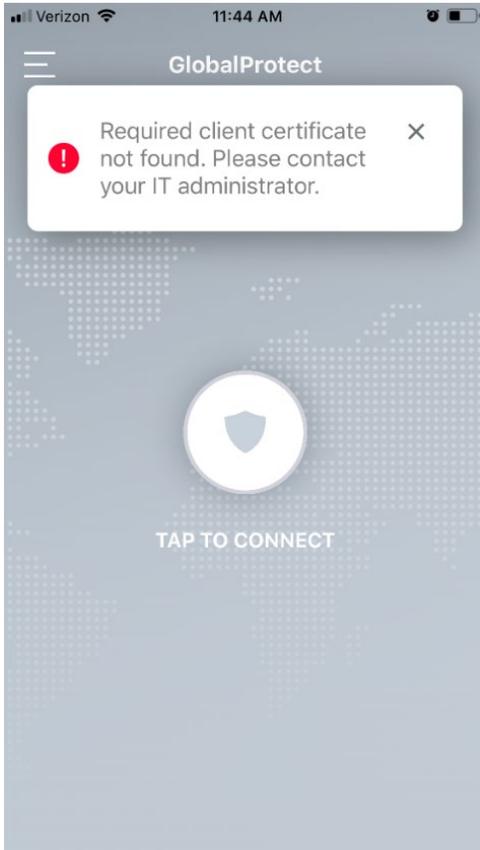
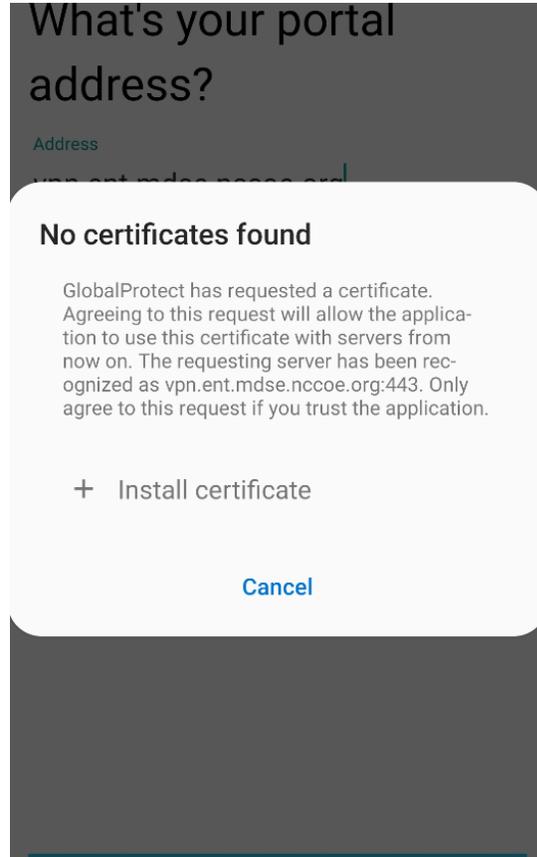
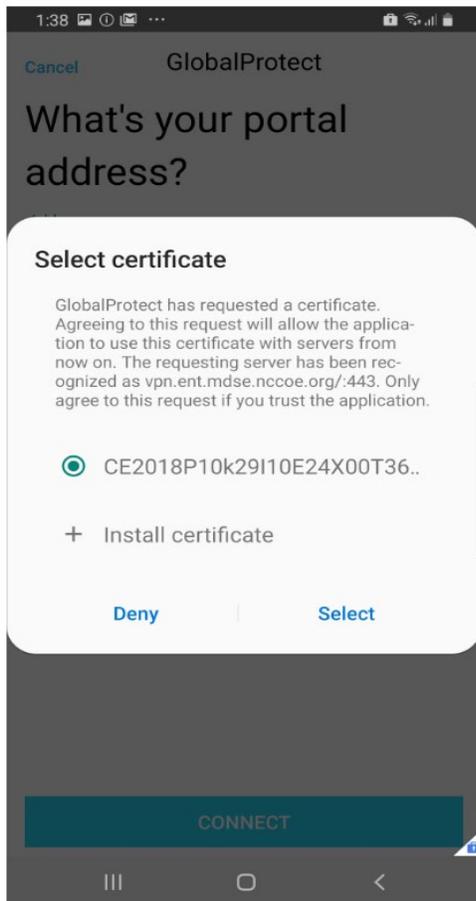


Figure 2-62 Attempting to Access the VPN on an Unmanaged Android Device



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

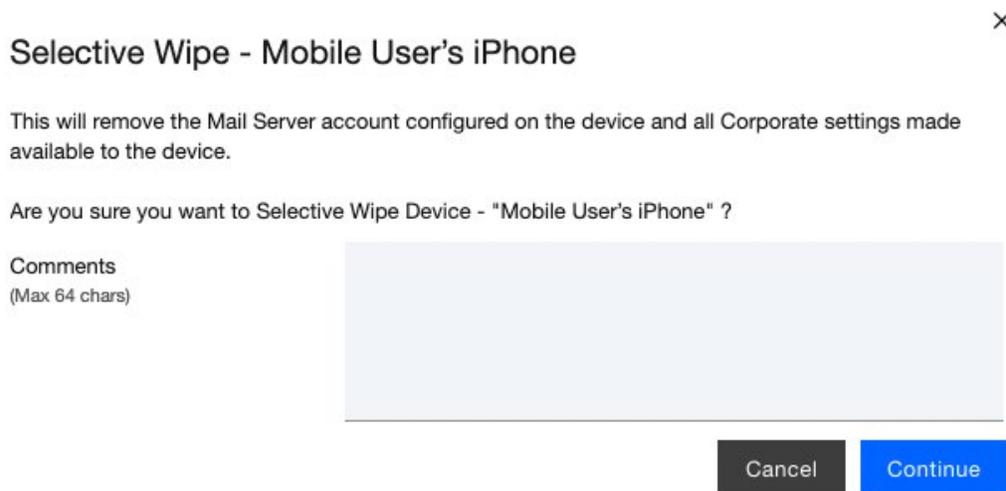
1293 screen lock with a passcode of appropriate strength, which helps resist exploitation (including loss of
1294 organizational data) if the device has been lost or stolen.

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

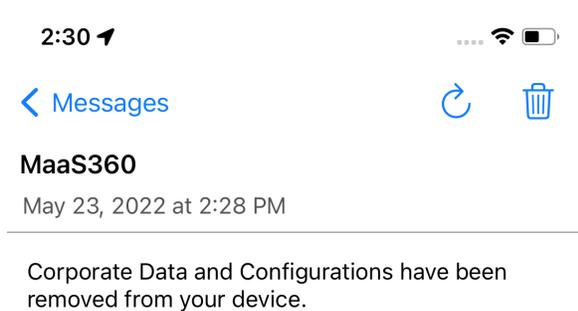
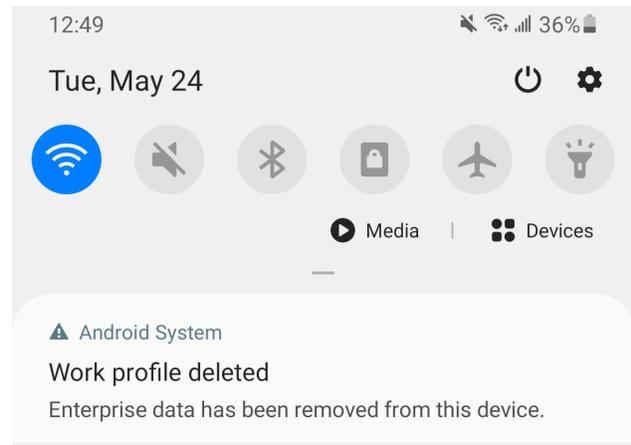


Figure 2-67 Work Profile Removal Notification on Android



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 categories and items:

- Device Settings**
 - Passcode
 - Restrictions** (selected)
 - ActiveSync
 - Wi-Fi
 - VPN
 - AirPrint
 - Accounts
- Advanced Settings**

The main content area is titled 'Configure Device Restrictions' and lists several settings:

- Unencrypted backups are restricted for all APNS managed devices.** (Yes) - UE
- Device Functionality**
 - Allow Open from Managed to Unmanaged apps** (No) - UE, iOS 7.0+
 - Allow Open from Unmanaged to Managed Apps** (No) - UE, iOS 7.0+
 - Allow AirDrop for Managed Apps** (Yes) - UE, iOS 9.0+
 - Allow Screen Capture** (Yes) - UE

1342 Figure 2-69 Android DLP Configuration

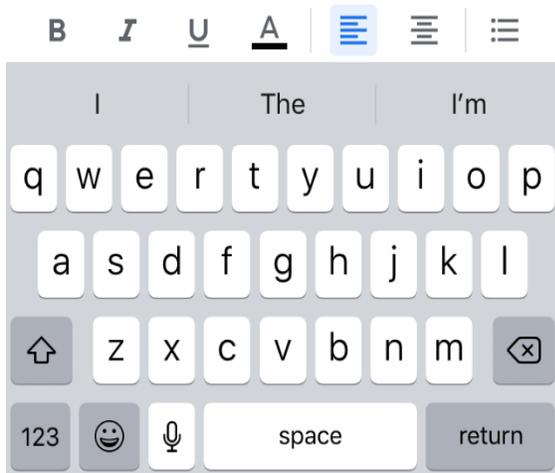
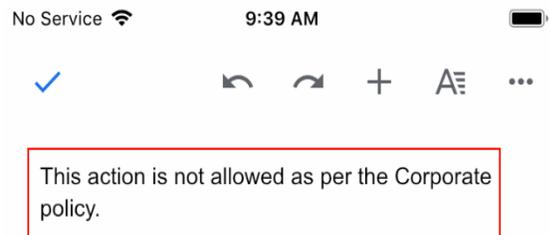
Default Android MDM Policy [↗](#)
Edit
More ▼

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**

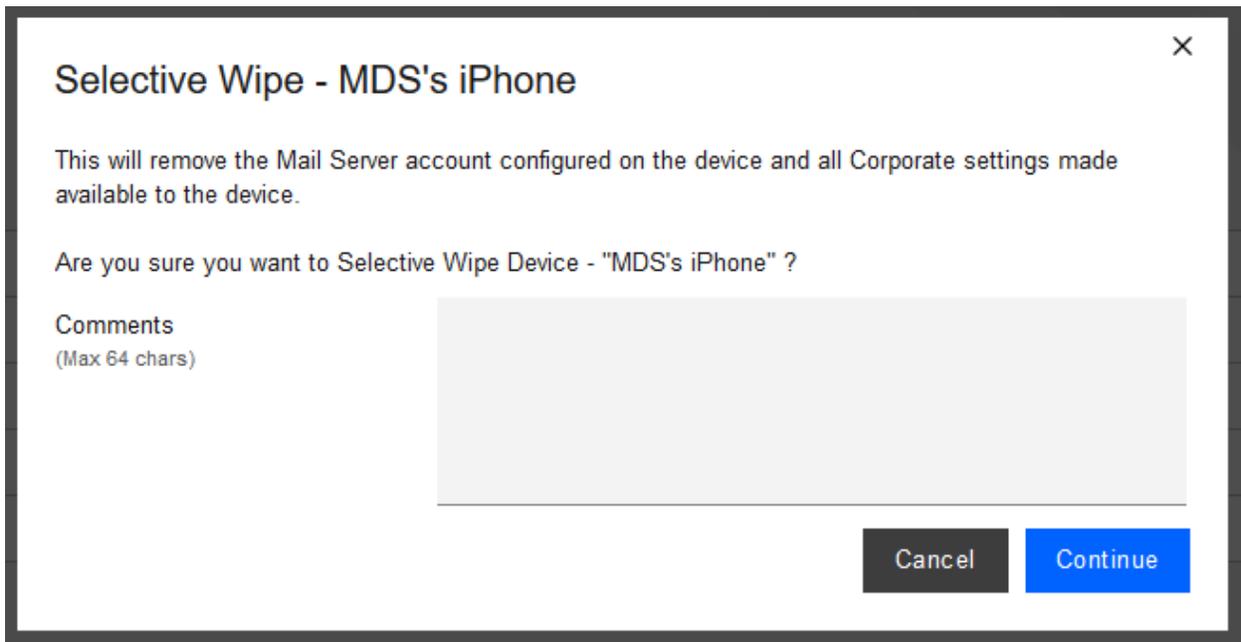
1346 **Summary:** Personal data that is comingled in the organizationally controlled portions of the phone could
1347 be lost during selective wipe of the device.

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
 - 1360 • Disallow configuration of work applications by users where possible to prevent comingling of
 - 1361 personal and work data
 - 1362 • Restrict staff access to system capabilities that permit removing device access or performing
 - 1363 wipes.

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.

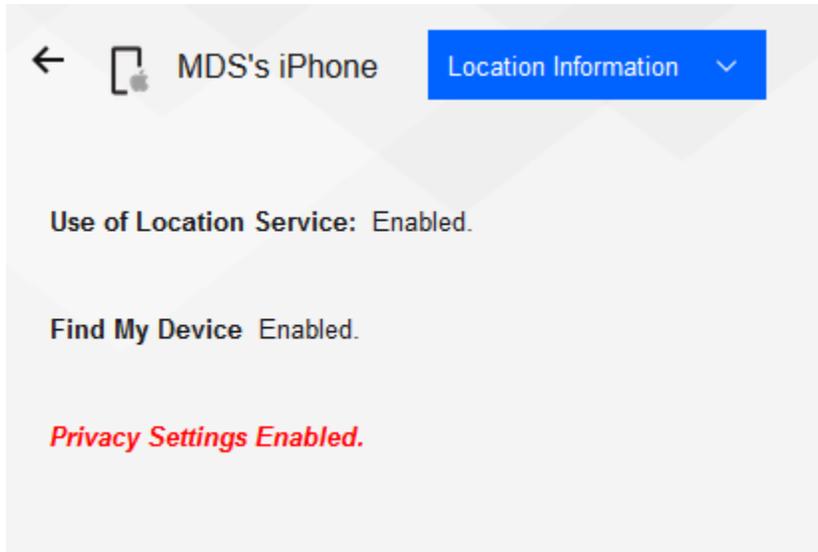
1380 **Figure 2-72 Application Inventory Information**

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 • Restrict staff access to system capabilities that permit reviewing data about employees and their
1386 devices.
- 1387 • Limit or disable collection of specific data elements.
- 1388 • 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.

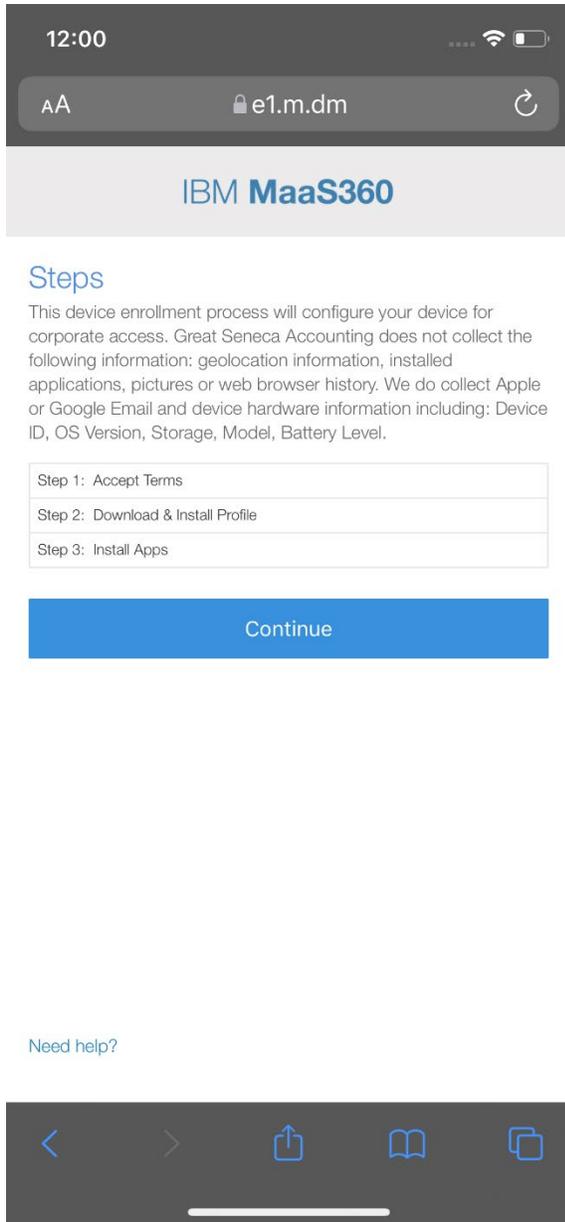
1393 **Test Activity:** Test to ensure that MDM provides custom notification to users detailing collected device
1394 information.

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.

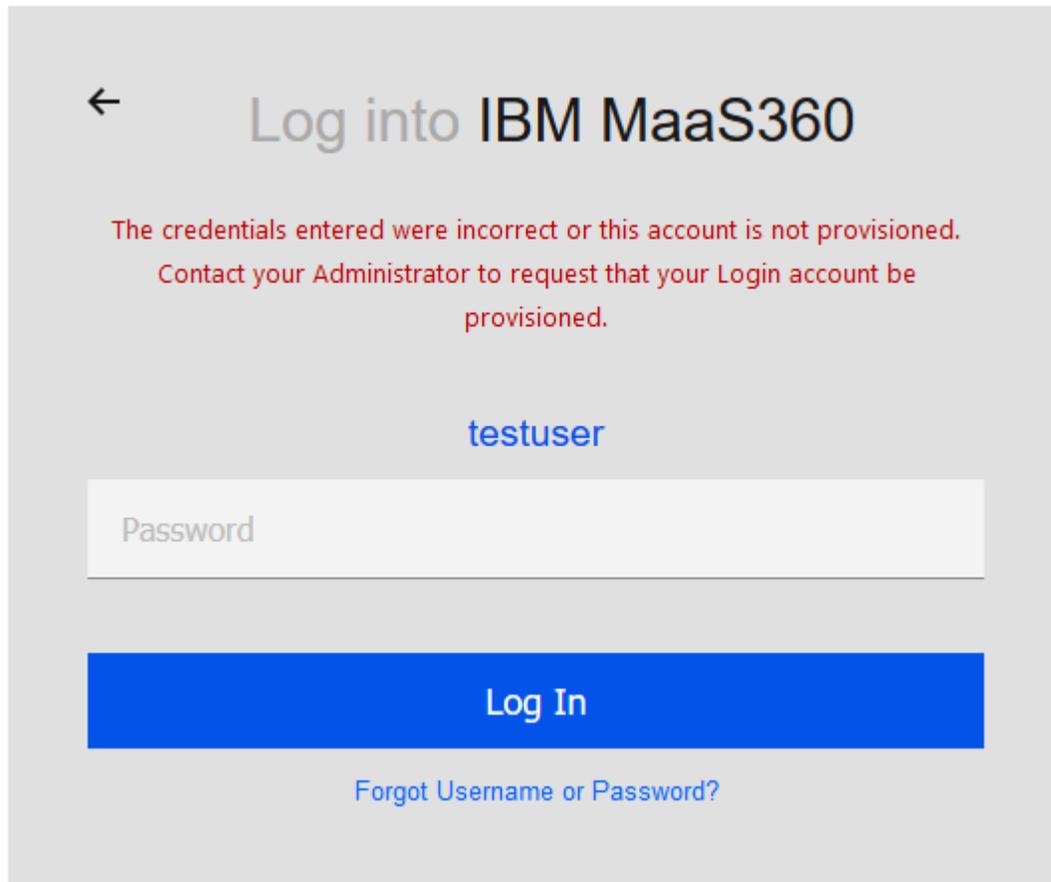
1410 **Test Activity:** Attempt to log in to the MaaS360 admin portal without domain administrator permissions.

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:>

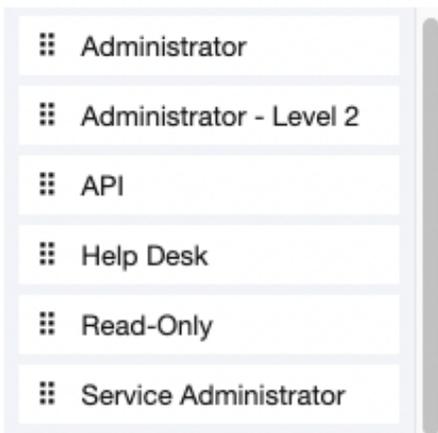
Automatically create new Administrator accounts and update roles based on User Groups

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.