Mobile Device Security:

Bring Your Own Device (BYOD)

Volume C: How-To Guides

Kaitlin Boeckl Nakia Grayson Gema Howell Naomi Lefkovitz

Applied Cybersecurity Division Information Technology Laboratory

Jason G. 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.

March 2021

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 National Institute of Standards and Technology Special Publication 1800-22B Natl. Inst. Stand. Technol.
- 8 Spec. Publ. 1800-22C, 61 pages, (March 2021), CODEN: NSPUE2

9 FEEDBACK

- 10 You can improve this guide by contributing feedback. As you review and adopt this solution for your
- 11 own organization, we ask you and your colleagues to share your experience and advice with us.
- 12 Comments on this publication may be submitted to: <u>mobile-nccoe@nist.gov</u>.
- 13 Public comment period: March 18, 2021 through May 03, 2021
- 14 All comments are subject to release under the Freedom of Information Act (FOIA).

15	National Cybersecurity Center of Excellence
16	National Institute of Standards and Technology
17	100 Bureau Drive
18	Mailstop 2002
19	Gaithersburg, MD 20899
20	Email: <u>nccoe@nist.gov</u>

21 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

36 NIST CYBERSECURITY PRACTICE GUIDES

- 37 NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity
- 38 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
- 39 adoption of standards-based approaches to cybersecurity. They show members of the information
- 40 security community how to implement example solutions that help them align with relevant standards
- 41 and best practices, and provide users with the materials lists, configuration files, and other information
- 42 they need to implement a similar approach.
- 43 The documents in this series describe example implementations of cybersecurity practices that
- 44 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- 45 or mandatory practices, nor do they carry statutory authority.

46 **ABSTRACT**

- 47 Bring Your Own Device (BYOD) refers to the practice of performing work-related activities on personally
- 48 owned devices. This practice guide provides an example solution demonstrating how to enhance
- 49 security and privacy in Android and Apple smartphone BYOD deployments.
- 50 Incorporating BYOD capabilities into an organization can provide greater flexibility in how employees
- 51 work and increase the opportunities and methods available to access organizational resources. For some
- 52 organizations, the combination of traditional in-office processes with mobile device technologies
- 53 enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-

first approach in which their employees communicate and collaborate primarily using their mobiledevices.

- 56 However, some of the features that make BYOD mobile devices increasingly flexible and functional also
- 57 present unique security and privacy challenges to both work organizations and device owners. The
- 58 unique nature of these challenges is driven by the diverse range of devices available that vary in type,
- age, operating system (OS), and the level of risk posed.
- 60 Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks to organizations.
- 61 Solutions that are designed to secure corporate devices and on-premises data do not provide an
- 62 effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the
- 63 unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new
- 64 privacy risks to employees by providing their employer a degree of access to their personal devices,
- opening up the possibility of observation and control that would not otherwise exist.
- 66 To help organizations benefit from BYOD's flexibility while protecting themselves from many of its
- 67 critical security and privacy challenges, this Practice Guide provides an example solution using
- 68 standards-based, commercially available products and step-by-step implementation guidance.

69 **KEYWORDS**

70 Bring your own device; BYOD; mobile device management; mobile device security.

71 ACKNOWLEDGMENTS

72 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

Name	Organization
Kevin Stine	NIST
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
Karri Meldorf	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
Tom Karygiannis	Kryptowire
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks

Name	Organization
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Mikel Draghici	Zimperium

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

- 74 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
- response to a notice in the Federal Register. Respondents with relevant capabilities or product
- components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
- 77 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
<u>Kryptowire</u>	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

78 **DOCUMENT CONVENTIONS**

- 79 The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the
- 80 publication and from which no deviation is permitted. The terms "should" and "should not" indicate that
- 81 among several possibilities, one is recommended as particularly suitable without mentioning or
- 82 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in
- 83 the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms

"may" and "need not" indicate a course of action permissible within the limits of the publication. The
 terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

86 CALL FOR PATENT CLAIMS

87 This public review includes a call for information on essential patent claims (claims whose use would be

88 required for compliance with the guidance or requirements in this Information Technology Laboratory

89 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication

90 or by reference to another publication. This call also includes disclosure, where known, of the existence

of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant

- 92 unexpired U.S. or foreign patents.
- ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-ten or electronic form, either:
- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
 currently intend holding any essential patent claim(s); or
- b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
- to utilize the license for the purpose of complying with the guidance or requirements in this ITL draftpublication either:
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
 or
- without compensation and under reasonable terms and conditions that are demonstrably free
 of any unfair discrimination.
- 104 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
- behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-
- sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that
- 107 the transferee will similarly include appropriate provisions in the event of future transfers with the goal
- 108 of binding each successor-in-interest.
- 109 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of 110 whether such provisions are included in the relevant transfer documents.
- 111 Such statements should be addressed to: mobile-nccoe@nist.gov

112 Contents

113	1	Intr	oduct	ion	.1
114		1.1	Practio	e Guide Structure	1
115		1.2	Build (Dverview	2
116		1.3	Турод	raphic Conventions	3
117		1.4	Logica	Architecture Summary	3
118	2	Pro	duct l	nstallation Guides	.4
119		2.1	Netwo	rk Device Enrollment Services Server	4
120			2.1.1	Certificate Authority (CA) Configuration	5
121			2.1.2	NDES Configuration	5
122		2.2	Intern	ational Business Machines MaaS360	9
123			2.2.1	Cloud Extender	9
124			2.2.2	Android Enterprise Configuration	.16
125			2.2.3	iOS APNs Certificate Configuration	.17
126			2.2.4	Android Configuration	.17
127			2.2.5	iOS Configuration	.20
128		2.3	Zimpe	rium	22
129			2.3.1	Zimperium and MaaS360 Integration	.22
130			2.3.2	Automatic Device Activation	.24
131			2.3.3	Enforce Application Compliance	.25
132			2.3.4	MaaS360 Risk Posture Alerts	.26
133		2.4	Palo A	lto Networks Virtual Firewall	27
134			2.4.1	Network Configuration	.27
135			2.4.2	Demilitarized Zone Configuration	.30
136			2.4.3	Firewall Configuration	.31
137			2.4.4	Certificate Configuration	.32
138			2.4.5	Website Filtering Configuration	.33
139			2.4.6	User Authentication Configuration	.39
140			2.4.7	VPN Configuration	.43

141		2.4.8	Enable Automatic Application and Threat Updates	54
142	2.5	Krypto	owire	. 56
143	2	2.5.1	Kryptowire and MaaS360 Integration	56
144	Appendi	хA	List of Acronyms	58
145	Appendi	хB	Glossary	60
146	Appendi	x C	References	61

147 List of Figures

148	Figure 1-1 High-Level Build Architecture4
149	Figure 2-1 Post-Deployment Configuration
150	Figure 2-2 PasswordMax Registry Configuration8
151	Figure 2-3 NDES Domain Bindings9
152	Figure 2-4 Cloud Extender Architecture
153	Figure 2-5 Old Cloud Extender Interface11
154	Figure 2-6 Cloud Extender Service Account Details
155	Figure 2-7 Administrator Settings
156	Figure 2-8 Administrator Configuration Options14
157	Figure 2-9 Cloud Extender SCEP Configuration
158	Figure 2-10 Cloud Extender Certificate Properties
159	Figure 2-11 Enterprise Binding Settings Confirmation17
160	Figure 2-12 Android GlobalProtect Application Compliance20
161	Figure 2-13 Zimperium MaaS360 Integration Configuration23
162	Figure 2-14 Zimperium zIPS iOS Configuration
163	Figure 2-15 Zimperium zIPS Android Configuration
164	Figure 2-16 Add Alert Button
165	Figure 2-17 Zimperium Risk Posture Alert Configuration27
166	Figure 2-18 DNS Proxy Object Configuration

167	Figure 2-19 Original Packet Network Address Translation Configuration
168	Figure 2-20 Certificate Profile
169	Figure 2-21 Custom URL Category
170	Figure 2-22 URL Filtering Profile
171	Figure 2-23 URL Filtering Security Policy
172	Figure 2-24 Generating the Root CA
173	Figure 2-25 Blocked Website Notification
174	Figure 2-26 Service Route Configuration
175	Figure 2-27 LDAP Server Profile
176	Figure 2-28 LDAP Group Mapping
177	Figure 2-29 LDAP User Authentication Profile
178	Figure 2-30 Configured Tunnel Interfaces43
179	Figure 2-31 SSL VPN Tunnel Interface Configuration
180	Figure 2-32 GlobalProtect iOS Authentication Profile
181	Figure 2-33 LDAP Authentication Group Configuration
182	Figure 2-34 VPN Zone Configuration
183	Figure 2-35 GlobalProtect Portal General Configuration
184	Figure 2-36 GlobalProtect Portal Authentication Configuration
185	Figure 2-37 GlobalProtect Portal Agent Authentication Configuration
186	Figure 2-38 GlobalProtect Portal Agent Configuration
187	Figure 2-39 Captive Portal Configuration
188	Figure 2-40 GlobalProtect Portal
189	Figure 2-41 Downloaded Threats and Applications
190	Figure 2-42 Schedule Time Hyperlink55
191	Figure 2-43 Application and Threats Update Schedule

192 **1 Introduction**

- 193 The following volumes of this guide show information technology (IT) professionals and security
- engineers how we implemented this example solution. We cover all of the products employed in this
- 195 reference design. We do not re-create the product manufacturers' documentation, which is presumed
- to be widely available. Rather, these volumes show how we incorporated the products together in our
- 197 environment.
- 198 Note: These are not comprehensive tutorials. There are many possible service and security configurations
 199 for these products that are out of scope for this reference design.

200 1.1 Practice Guide Structure

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

- 205 This guide contains four volumes:
- 206 NIST SP 1800-22A: Executive Summary
- 207 NIST SP 1800-22B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* how
 organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* instructions for building the example solution (you are here)
- 212
- 213 Depending on your role in your organization, you might use this guide in different ways:

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

- 216 challenges that enterprises face in managing the security of BYOD deployments
- 217 the example solution built at the NCCoE
- 218 benefits of adopting the example solution

219 Technology or security program managers who are concerned with how to identify, understand, assess,

- and mitigate risk will be interested in *NIST SP 1800-22B*, which describes what we did and why. The
- 221 following sections will be of particular interest:
- Section 4.1.4, Conduct a Risk Assessment, describes the risk analysis we performed.

- 223 224
- Appendix I, Example Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

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

IT professionals who want to implement an approach like this will find this whole practice guide useful.
You can use this How-To portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build

- 229 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
- and integration instructions for implementing the example solution. We do not recreate the product
- 231 manufacturers' documentation, which is generally widely available. Rather, we show how we
- incorporated the products together in our environment to create an example solution.
- 233 This guide assumes that IT professionals have experience implementing security products within the
- enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- not endorse these particular products. Your organization can adopt this solution or one that adheres to
- these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- parts of a BYOD solution. Your organization's security experts should identify the products that will best
- 238 integrate with your existing tools and IT system infrastructure. We hope that you will seek products that
- are congruent with applicable standards and best practices. Volume B, Section 3.7, Technologies, lists
- 240 the products that we used and maps them to the cybersecurity controls provided by this reference
- 241 solution.
- 242 For those who would like to see how the example solution can be implemented, this practice guide
- 243 contains an example scenario about a fictional company called Great Seneca Accounting. The example
- scenario shows how BYOD objectives can align with an organization's priority security and privacy
- 245 capabilities through NIST risk management standards, guidance, and tools. It is provided in this practice
- 246 guide's supplement, NIST SP 1800-22 *Example Scenario: Putting Guidance into Practice*.
- A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
- 248 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
- success stories will improve subsequent versions of this guide. Please contribute your thoughts to
- 250 <u>mobile-nccoe@nist.gov</u>.

251 **1.2 Build Overview**

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

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

261 **1.3 Typographic Conventions**

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

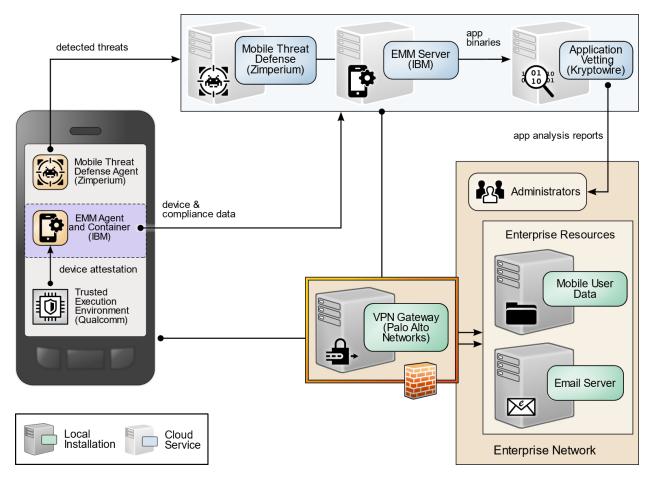
Typeface/Symbol	Meaning	Example
Italics	file names and path names;	For language use and style guidance,
	references to documents that	see the NCCoE Style Guide.
	are not hyperlinks; new	
	terms; and placeholders	
Bold	names of menus, options,	Choose File > Edit.
	command buttons, and fields	
Monospace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

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

1.4 Logical Architecture Summary

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

267 Figure 1-1 High-Level Build Architecture



268 2 Product Installation Guides

- This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.
- 271 This guide assumes that a basic active directory (AD) infrastructure has been configured. The domain
- 272 controller (DC) is used to authenticate users when enrolling devices as well as when connecting to the
- 273 virtual private network (VPN). In this implementation, the domain *enterprise.mds.local* was used.

274 2.1 Network Device Enrollment Services Server

- 275 A Network Device Enrollment Service (NDES)/Simple Certificate Enrollment Protocol (SCEP) server was
- used to issue client certificates to new devices that were enrolled by using MaaS360. This guide assumes
- 277 that a basic AD infrastructure is in place.

278 2.1.1 Certificate Authority (CA) Configuration

- 279 The guide followed for the build is linked below, followed by the specific configuration changes used.
- 280 Configuration guide: https://gallery.technet.microsoft.com/Windows-Server-2016-Active-165e88d1
- 281 Configuration changes that were made:
- The Root CA Name was changed to ROOT-CA.
- 283 The Issuing CA Name was changed to SUB-CA.
- The entry for DC=srv, DC=lab was replaced with DC=enterprise, DC=mds, DC=local at various points throughout the guide.

286 *2.1.1.1 Export Certificates*

This section assumes that a location exists that is accessible by all machines on the network, such as a
shared folder or network drive. Furthermore, this section assumes that configuration of the root and
subordinate CA has been completed.

- 290 1. Log in to the root CA.
- 291 2. Open the start menu, and search for *cmd*.
- 292 3. Right-click **Command Prompt**, and select **Run as administrator**.
- 293 4. Navigate to the shared storage location.
- 294 5. Run the command certutil -ca.cert root.cer.
- 295 6. The file named *root.cer* will now contain a base64-encoded copy of the root CA certificate.
- 296 7. Repeat steps 1–6 with the sub CA, replacing *root.cer* with *sub.cer*.
- 297 8. (optional) Disconnect and shut down the root CA.

298 2.1.2 NDES Configuration

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

- 301 1. From the Server Manager, select Manage > Add Roles and Features.
- 302 2. Click **Next** three times until **Server Roles** is highlighted.
- 303 3. Check the box next to Active Directory Certificate Services.
- 304 4. Click **Next** three times until **Role Services** is highlighted.

- 305 5. Uncheck **Certification Authority.** Check **Network Device Enrollment Service.**
- 306 6. Click **Add Features** on the pop-up.
- 307 7. Click **Next** three times.
- 308 8. Click Install.
- When installation completes, click the flag in the upper right-hand corner, and click Configure
 Active Directory Certificate Services.
- 311 Figure 2-1 Post-Deployment Configuration

Configuration required for Active Directory Certificate Services at	
Configure Active Directory Certificate Services on th Feature installation TASKS X	
Configuration required. Installation succeeded on	
Add Roles and Features	
Task Details	
	Configuration required. Installation succeeded on

312 10. Specify the credentials of a Domain Administrator. Click **Next.**

313 Note: The domain administrator credentials are required only to configure the NDES. Once the service is

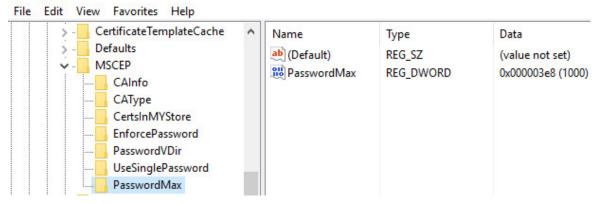
configured, the service is executed as the NDES service account, which does not require domain

- administrator permissions, created in step 12 below.
- 316 11. Check Network Device Enrollment Service. Click Next.
- 317 12. Configure an NDES service account by performing the following actions:
- a. On the active directory server, open Active Directory Users and Computers.
- 319b. Click **Users** and create a new user for the service. For this example, it will be named320NDES. Be sure the password never expires.

321	c. On the NDES server, open Edit local users and groups.
322	d. Click Groups. Right-click IIS_IUSRS, click Add to Group, and click Add.
323 324	 Search for the service account name—in this case, NDES. Click Check Names, and click OK if no errors were displayed.
325	f. Click Apply, and click OK .
326	g. Close all windows except the NDES configuration window.
327	13. Click Select next to the box, and enter the service account credentials. Click Next.
328 329 330	14. Because the NDES runs on its own server, we will target it at the SUB-CA. Select Computer name and click Select. Type in the computer name—in this case, SUB-CA. Click Check Names, and if no errors occurred, click OK.
331	15. Click Next three times.
332	16. Click Configure.
333	17. On the SUB-CA, open the Certification Authority application.
334	18. Expand the SUB-CA node, right-click on Certificate Templates, and click Manage .
335	19. Right-click on IPSec (Offline Request), and click Duplicate Template.
336	20. Under the General tab, set the template display name to NDES .
337	21. Under the Security tab, click Add.
338	22. Select the previously configured NDES service account.
339	23. Click OK . Ensure the NDES service account is highlighted, and check Read and Enroll .
340	24. Click Apply .
341 342	25. In the Certification Authority program, right-click on Certificate Templates, and select New > Certificate Template to Issue.
343	26. Select the NDES template created in step 24.
344	27. Click OK.
345	28. On the NDES server, open the Registry Editor (regedit).
346	29. Expand the following key: HKLM\SOFTWARE\Microsoft\Cryptography.
347	30. Select the MSCEP key and update all entries besides (Default) to be NDES .

- 348 31. Expand the following key: HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP.
- 349 32. Right-click on **MSCEP**, and select **New > Key**. Name it **PasswordMax**.
- 350 33. Right-click on the newly created key and select **New > DWORD (32-bit) Value.**
- 34. Name it **PasswordMax,** and give it a value of **0x00003e8.** This increases the NDES password
 cache to 1,000 entries instead of the default 5. This value can be further adjusted based on
 NDES demands.
- 354 Figure 2-2 PasswordMax Registry Configuration

📑 Registry Editor



- Note: The PasswordMax key governs the maximum number of NDES passwords that can reside in the cache. A password is cached when a valid certificate request is received, and it is removed from the cache when the password is used or when 60 minutes have elapsed, whichever occurs first. If the PasswordMax key is not present, the default value of 5 is used.
- In an elevated command prompt, execute %windir%\system32\inetsrv\appcmd set config
 /section:requestFiltering /requestLimits.maxQueryString:8192 to increase the maximum query string. This prevents requests longer than 2,048 bytes from being dropped.
- 362 2. Open the Internet Information Services (IIS) Manager.
- 363 3. On the left, expand NDES > Sites, and select Default Web Site.
- 364 4. On the right, click **Bindings...**
- 365 5. Click Add.
- 366 6. Below Host Name, enter the host name of the server. For this implementation, *ndes.enter-* 367 *prise.mds.local* was used.
- 368 7. Click **OK**.

369 Figure 2-3 NDES Domain Bindings

Туре	Host Name	Port	IP Address	Binding Informa	Add
http		80	*		Edit
http	ndes.enterprise.mds.local	80	*		EUIL
					Remove
					Browse

370

- 371 8. Click **Close**, and close the IIS Manager.
- 9. In an elevated command prompt, execute *isreset*, or reboot the NDES server.

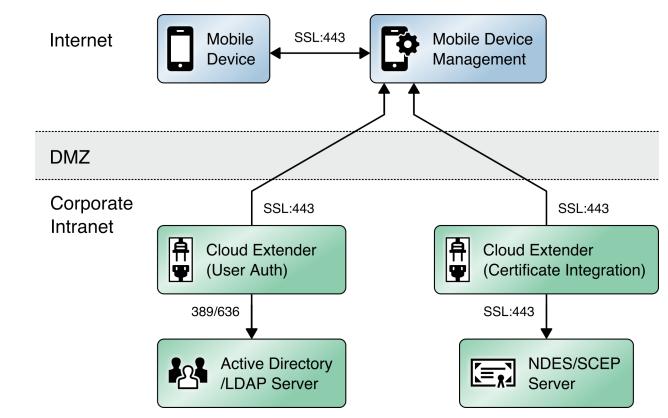
373 2.2 International Business Machines MaaS360

International Business Machines (IBM) contributed an instance of MaaS360 (<u>https://www.ibm.com/us-</u>
 <u>en/marketplace/unified-endpoint-management</u>) to deploy as the mobile device management (MDM)
 solution.

377 2.2.1 Cloud Extender

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

382 Figure 2-4 Cloud Extender Architecture



- 383 *2.2.1.1 Cloud Extender Download*
- 1. Log in to the MaaS360 web portal.
- 385 2. Click Setup > Cloud Extender.
- Click the link that says Click here to get your License Key. The license key will be emailed to the
 currently logged-in user's email address.
- 388 4. Click the link that says **Click here to download the Cloud Extender.** Save the binary.
- 389 5. Move the binary to a machine behind the corporate firewall that is always online. Recommenda 390 tion: Install it while logged in as a domain user on a machine that is not the domain controller.
- Install .NET 3.5 Features in the Server Manager on the machine where the MaaS360 Cloud Ex tender will run.
- *2.2.1.2 Cloud Extender Active Directory Configuration*
- 1. On the target machine, run the installation binary.

- 395 2. Enter the license key when prompted.
- 396 3. Proceed through the setup until the Cloud Extender Configuration Utility opens.
- 397 4. If using the old cloud extender interface, click **Switch to Modern.**
- 398 Figure 2-5 Old Cloud Extender Interface

	ck for Internet connectivity:	English v He
~	Internet access available. Click "Next" to co	ntinue.
۲	Do not use proxy	
0	Manually configure proxy settings	
0	Proxy PAC URL	
0	Auto Proxy	
	Use Proxy Authentication	
	ning: Be sure to create an exclusion rule for the \ProgramDa malware or firewall software running on this server. Failure	
Co	llect logs from this Cloud Extender	
Ge	nerates an archive file on the desktop	Collect Logs

- 399 5. Enable the toggle below User Authentication.
- 400 6. Create a new authentication profile by entering the username, password, and domain of the401 created service account.

402 Figure 2-6 Cloud Extender Service Account Details

HOME IMPORT EXPORT F	PROXY SETTIN	GS HELP∽	English (United States)	~
User Authentication		iry credentials		()
Start	Provide S	ervice Account details		0
Start		t should be: on Active Directory strator on this server		
	Username	MAAS360		
2 Service Account	Password	•••••		
	Domain	enterprise.mds.local		
	Enable Se	cure Authentication Mode		
Finish				
		Back Nex	kt Save Can	cel
The Cloud Extender is runni	ng			

- 403 7. Click **Next**.
- 404 8. (optional) Use the next page to test the active directory integration.
- 405 9. Click **Save**.
- In MaaS360, navigate to Setup > Cloud Extender. Ensure that configuration information is dis played, indicating that the MaaS360 Cloud Extender is running.
- 408 2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration
- 409 1. Log in to the MaaS360 web portal as an administrator.
- 410 2. Go to Setup > Settings.
- 411 3. Expand Administrator Settings, and click Advanced.

412 Figure 2-7 Administrator Settings

IBM MaaS360 With Watson	Search for Devices, Users or Apps	Q,	? 👤 🖒
HOME DEVICES USERS SECURITY APPS	REPORTS SETUP		
← Settings			Save
Device Enrollment Settings	Login Settings		
User Settings	Use this section to configure strong portal authentication for your Administrators. Configure Federated Single Sign-on		
App Settings	Configure Strong Authentication		
Administrator Settings			
Basic			
🏟 Advanced			

- 413 4. Select **Configure Federated Single Sign-on**.
- 414 5. Select Authenticate against Corporate User Directory.
- 415 6. Next to **Default Domain**, enter the active directory domain. In this implementation, *enter-* 416 *prise.mds.local* was used.
- 417 7. Check the box next to Allow existing Administrators to use portal credentials as well.
- 418 8. Check the box next to Automatically create new Administrator accounts and update roles
 419 based on user groups.
- 420 9. Under **User Groups**, enter the distinguished name of the group(s) that should be allowed to log
 421 in. In this implementation, CN=Domain Admins, CN=Users, DC=enterprise, DC=mds, DC=local
 422 was used.
- 423 10. Next to the box, select Administrator–Level 2. This allows domain admins to log in as MaaS360
 424 administrators.

425 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 ac User Groups (Specify the Distinguished Name		d on User Groups					
CN=Domain Admins,CN=Users,DC=enter	Administrator - Level 2	νΘ					
	Select Role	✓ ⊕					

- 426 11. Click **Save.**
- 427 2.2.1.4 Cloud Extender NDES Integration
- To properly generate device certificates, MaaS360 must be integrated with the on-premises public key infrastructure (PKI).
- 430 1. Log in to the server running the MaaS360 Cloud Extender.
- 431 2. Launch the Cloud Extender Configuration Tool.
- 432 3. Toggle the button below Certificate Integration.
- 433 4. Click Add New Template.
- 434 5. Ensure **Microsoft CA** and **Device Identity Certificates** are selected.
- 435 6. Click **Next.**
- 436 7. Enter **NDES** for the Template Name and SCEP Default Template.
- 437 8. Enter the uniform resource locator (URL) of the NDES server next to SCEP Server.
- 438 9. Enter credentials of a user with enroll permissions on the template for Challenge Username and
 439 Challenge Password. For this demo implementation, we use the NDES service account.

440 Figure 2-9 Cloud Extender SCEP Configuration

HOME IMPORT EXPORT F	PROXY SETTINGS HELP~		English (United States)	~
Certificate Integrati Securely deploy identity certificates				()
Start	SCEP - Microsoft, Veri	zon, Open Trust server details		
Start	Template Name	NDES		
	Hostname of SCEP server	https 🗸 ndes.enterprise.mds.local		
2 SCEP Config	SCEP Server challenge type	O Dynamic ○ Static ○ None		
Ť	Challenge Username	ENTERPRISE\NDESSvc		
3 Cert Attributes	Challenge Password	•••••		
4 Finish				
		Back Net	ct Save Can	cel
The Cloud Extender is running	ng			

- 441 10. Click **Next.**
- 442 11. (optional) Check the box next to Cache certs on Cloud Extender and specify a cache path on the443 machine.

444 Figure 2-10 Cloud Extender Certificate Properties

Home import export	PROXY SETTINGS HELP~			English (United States)	~
Certificate Integra Securely deploy identity certificat					()
Chart	Certificate Properties				
Start	Subject Name (i)	/CN=%uname%/emailAddress=%email%			
	Subject Alternate Name	None			~
SCEP Config	Cache certs on Cloud Extender				
	Location of Certificate Cache	C:\CertCache		Br	rowse
3 Cert Attributes					
4 Finish					
			Back Ne	xt Save Ca	incel
The Cloud Extender is run	nina				

445 12. Click **Next.**

- 446 13. (optional) Enter values for uname and email and generate a test certificate to test the configura-447 tion.
- 448 14. Click **Save.**
- 449 Note: If a file access message appears, delete the file, and re-save the file.

450 2.2.2 Android Enterprise Configuration

- 451 A Google account was used to provision Android Enterprise on the mobile devices. A managed domain
- 452 can be used, but in this use case it was not necessary. A managed domain is necessary only if the453 corporation already has data stored in Google's cloud.
- 454 1. Create a Google account if you do not have one you wish to bind with.
- 455 2. From the MaaS360 portal, navigate to **Setup > Services.**
- 456 3. Click Mobile Device Management.
- 457 4. Check the box next to **Enable Android Enterprise Solution Set.**
- 458 5. Enter your password, and click **Enable**.

459	6.	Click Mobile Device Management.
460	7.	Click the radio button next to Enable via Managed Google Play Accounts (no G Suite).
461	8.	Ensure all pop-up blockers are disabled. Click the link on the word here.
462	9.	Enter your password, and click Enable.
463	10	In the new page that opens, ensure you are signed into the Google account you wish to bind.
464	11.	Click Get started.
465	12	Enter your business name, and click Next.
466 467	13	If General Data Protection Regulation compliance is not required, scroll to the bottom, check the I agree box, and click Confirm. If compliance is required, fill out the requested information first.
468	14.	Click Complete Registration.
469 470	15	Confirm binding on the Setup page under Mobile Device Management. The settings should look like Figure 2-11, where the blurred-out portion is the Google email address used to bind.
471	Figure	2-11 Enterprise Binding Settings Confirmation
	Enable	Android Enterprise Solution Set Android enterprise features, such as Work Profile (Profile Owner), Work Managed Device (Device Owner) and COSU to better protect and control work data on managed devices. Learn more naged Google Play ail ID used to bind your organization is

- 472 2.2.3 iOS APNs Certificate Configuration
- For the iOS Apple Push Notification services (APNs) certificate configuration, the build team followed the
 IBM documentation.
- 475 2.2.4 Android Configuration
- 476 *2.2.4.1 Policy Configuration*
- 477 1. Navigate to Security > Policies.
- 478 2. Click the appropriate deployed Android policy.
- 479 3. Click **Edit.**
- 480 4. Navigate to Android Enterprise Settings > Passcode.
- 481 5. Check the box next to Configure Passcode Policy.

482	6.	Configure the passcode settings based on corporate requirements.
483	7.	Navigate to Android Enterprise Settings > Restrictions.
484	8.	Check the box next to Configure Restrictions.
485	9.	Configure restrictions based on corporate requirements.
486	10.	Click Save.
487	2.2.4.	2 VPN Configuration
488	1.	Navigate to Security > Policies.
489	2.	Click the currently deployed Android device policy.
490	3.	Click Edit.
491	4.	Navigate to Android Enterprise Settings > Certificates.
492	5.	Check the box next to Configure CA Certificates.
493	6.	Click Add New.
494	7.	Give the certificate a name, such as Internal Root.
495	8.	Click Browse , and navigate to the exported root CA certificate from earlier in the document.
496	9.	Click Save.
497	10.	Select Internal Root from the drop-down next to CA Certificate.
498	11.	Click the + icon on the far right.
499	12.	Repeat steps 6–10 with the internal sub CA certificate.
500	13.	Check the box next to Configure Identity Certificates.
501 502	14.	From the drop-down next to Identity Certificate , select the profile that matches the name con- figured on the MaaS360 Cloud Extender—for this example, NDES .
503	15.	Click Save and Publish, and follow the prompts to publish the updated policy. Click Apps.
504	16.	Click Add > Android > Google Play App.
505	17.	Select the radio button next to Add via Public Google Play Store.
506	18.	Search for GlobalProtect .

507 19. Select the matching result.

- 508 20. Click **I Agree** when prompted to accept the permissions.
- 509 21. Check the three boxes next to **Remove App on**.
- 510 22. Check the box next to **Instant Install**.
- 511 23. Select **All Devices** next to **Distribute to**.
- 512 24. Click **Add**.
- 513 25. Next to the newly added GlobalProtect application, select **More > Edit App Configurations.**
- 514 26. Click Check for Settings.
- 515 27. Next to **Portal**, enter the GlobalProtect portal address. In this implementation,
 516 *vpn.ent.mdse.nccoe.org* was used.
- 517 28. Next to **Username**, enter %username%.
- 518 29. Next to Connection Method, enter user-logon. (Note: This will enable an always-on VPN con519 nection for the work profile. The user will always see the VPN key icon, but it will apply only to
 520 applications contained within the work container.)
- 521 30. Click **Save**, and follow the prompts to update the application configuration.
- 522 31. Navigate to **Security > Policies**.
- 523 32. Click the used Android policy.
- 524 33. Select Android Enterprise Settings > App Compliance.
- 525 34. Click **Edit**.
- 526 35. Click the + on the row below **Configure Required Apps**.
- 527 36. Enter the App Name, **GlobalProtect**.
- 528 37. Enter the App ID, **com.paloaltonetworks.globalprotect**.
- 529 38. Click **Save And Publish**, and follow the prompts to publish the policy.

530 Figure 2-12 Android GlobalProtect Application Compliance

IBM MaaS360 With Watson	Q Search for Devices, Users, Apps or Docs		() A A ()
HOME DEVICES USERS SECURI	TY APPS DOCS REPORTS SETUP		
← Default Android MDM Pol	icy 🖉		Edit More 🗸
Last Published: 01/30/2020 14:23 EST Publish	[Version:59] Current Status: Needs		
Device Settings	Configure Application Compliance		
Advanced Settings	Configure allowed system applications Allowed apps will be available for use on device and in work profile if	No	Android 5.0+ (PO & DO)
 Android Enterprise Settings 	available for the device		
Passcode	Configure Required Apps Apps that cannot be uninstalled by user.	Yes	Android 5.0+ (PO & DO)
Security	•		
Restrictions			Android 5.0+ (PO & DO)
Accounts	Application Name Specify the App ID for the App	com.paloaltonetworks.globalprotect	

- 531 2.2.5 iOS Configuration
- 532 2.2.5.1 Policy Configuration
- 533 1. Navigate to **Security > Policies**.
- 534 2. Click the deployed iOS policy.
- 535 3. Click **Edit**.
- 536 4. Check the box next to **Configure Passcode Policy**.
- 537 5. Check the box next to **Enforce Passcode on Mobile Device**.
- 538 6. Configure the rest of the displayed options based on corporate requirements.
- 539 7. Click **Restrictions.**
- 540 8. Check the box next to **Configure Device Restrictions**.
- 541 9. Configure restrictions based on corporate requirements.
- 542 10. Click **Save**.
- 543 2.2.5.2 VPN Configuration
- 544 1. Click **Device Settings > VPN**.

	r	Click	Edit
545	Ζ.	CIICK	Euit.

- 546 3. Next to **Configure for Type,** select **Custom SSL**.
- 547 4. Enter a name next to VPN Connection Name. In this sample implementation, Great Seneca VPN
 548 was used.
- 549 5. Next to Identifier, enter com.paloaltonetworks.globalprotect.vpn.
- 550 6. Next to **Host name of the VPN Server,** enter the URL of the VPN endpoint without http or https.
- 551 7. Next to **VPN User Account,** enter **%username%.**
- 552 8. Next to User Authentication Type, select Certificate.
- 9. Next to Identity Certificate, select the name of the certificate profile created during the NDES
 configuration steps. In this sample implementation, NDES was used.
- 10. Next to Custom Data 1, enter allowPortalProfile=0
- 556 11. Next to Custom Data 2, enter fromAspen=1
- 12. Next to Apps to use this VPN, enter the application identifications (IDs) of applications to go
 through the VPN. This will be the applications deployed to the devices as work applications.
- 13. Next to **Provider Type**, select **Packet Tunnel**.
- 560 14. Click **Apps**.
- 561 15. Click Add > iOS > iTunes App Store App.
- 562 16. Search for **GlobalProtect**.
- 563 17. Select the **non-Legacy** version.
- 18. Click **Policies and Distribution**.
- 565 19. Check all three boxes next to **Remove App on**.
- 566 20. Select **All Devices** next to **Distribute to**.
- 567 21. Check the box next to **Instant Install.**
- 568 22. Click **Add**.
- 569 23. Navigate to **Security > Policies**.
- 570 24. Click the used iOS policy.
- 571 25. Click **Application Compliance**.

- 572 26. Click **Edit**.
- 573 27. Click the + next to the first row under **Configure Required Applications**.
- 574 28. Search for **GlobalProtect.**
- 575 29. Select the **non-Legacy** result.
- 576 30. Navigate to **Advanced Settings > Certificate Credentials**.
- 577 31. Check the box next to **Configure Credentials for Adding Certificates on the Device.**
- 578 32. Click Add New.
- 579 33. Give the certificate a name, such as Internal Root.
- 580 34. Click **Browse**, and navigate to the exported root CA certificate from earlier in the document.
- 581 35. Click **Save.**
- 582 36. Select Internal Root from the drop-down next to CA Certificate.
- 583 37. Click the + icon on the far right.
- 584 38. Repeat steps 33–35 with the internal sub CA certificate.
- 585 39. From the drop-down next to Identity Certificate, select the profile that matches the name con figured on the MaaS360 Cloud Extender—for this example, NDES.
- 587 40. Click **Save And Publish**, and follow the prompts to publish the policy.

588 2.3 Zimperium

- 589 Zimperium was used as a mobile threat defense service via a MaaS360 integration.
- 590 Note: For Zimperium automatic enrollment to function properly, users **must** have an email address
- associated with their MaaS360 user account.

592 2.3.1 Zimperium and MaaS360 Integration

- 593 This section assumes that IBM has provisioned an application programming interface (API) key for 594 Zimperium within MaaS360.
- 595 1. Log in to the zConsole.
- 596 2. Navigate to Manage > MDM.
- 597 3. Select **Add MDM > MaaS360**.

- 598 4. Fill out the MDM URL, MDM username, MDM password, and API key.
- 5. Note: For the MDM URL, append the account ID to the end. For example, if the account ID is 12345, the MDM URL would be https://services.fiberlink.com/12345.
- 601 6. Check the box next to **Sync users**.
- 602 Figure 2-13 Zimperium MaaS360 Integration Configuration

Edit MDM Step 2 Setup IBM MaaS360 Step 1 Choose MDM Provider Step 3 Finish URL https://services.fiberlink.com/ Specify URL for this MDM provider. Username Specify username for this MDM provider. Password Specify password for this MDM provider. MDM Name IBM MaaS360 Specify a unique name for this MDM provider. \checkmark 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 synched 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

- 603 7. Click **Next**.
- 8. Select the MaaS360 groups to synchronize with Zimperium. In this case, All Devices was selected.
- 606 9. Click **Finish**. Click **Sync Now** to synchronize all current MaaS360 users and devices.

607 2.3.2 Automatic Device Activation

- Note: This requires contacting Zimperium support to get required application configuration values.
- 609 1. Log in to MaaS360.
- 610 2. Click **Apps** on the navigation bar.
- 611 3. Click Add > iOS > iTunes App Store App.
- 612 4. Search for **Zimperium zIPS.** Click the result that matches the name.
- 5. Click **Policies and Distribution**.
- 614 6. Check the three checkboxes next to **Remove App on**.
- 615 7. Next to **Distribute to,** select **All Devices**.
- 616 8. Click **Configuration.**
- 617 9. Set App Config Source to **Key/Value**.
- 61810. The configuration requires three parameters: uuid, defaultchannel, and tenantid. uuid can be619set to %csn%, but defaultchannel and tenantid must come from Zimperium support.
- 620 Figure 2-14 Zimperium zIPS iOS Configuration

MDMDeviceID	%csn%	⊕⊝
defaultchannel		⊕⊝
tenantid		۰.

- 621 11. Click **Add**.
- 622 12. Click Add > Android > Google Play App.
- 623 13. Select the radio button next to **Add via Public Google Play Store**.
- 624 14. Search for **Zimperium Mobile IPS** (zIPS).
- 625 15. Click the matching result.
- 626 16. Click I Agree when prompted to accept permissions.

- 627 17. Click **Policies and Distribution**.
- 628 18. Check all three boxes next to **Remove App on**.
- 629 19. Check Instant Install.
- 630 20. Select **All Devices** next to **Distribute to**.
- 631 21. Click **App Configurations**.
- 632 22. Check Configure App Settings.
- 633 23. Enter the values provided by Zimperium next to **Default Acceptor** and **Tenant**.
- 634 24. Next to **MDM Device ID**, insert **%deviceid%**.
- 635 25. Adjust any other configuration parameters as appropriate for your deployment scenario.
- 636 Figure 2-15 Zimperium zIPS Android Configuration

Default Acceptor:		
Tenant:		
UUID:		
Display EULA:	No	~
Tracking ID 1:		
Tracking ID 2:		
MDM Device ID:	%deviceid%	

637 26. Click Add.

638 2.3.3 Enforce Application Compliance

- 639 From the IBM MaaS360 web portal:
- 640 1. Navigate to Security > Policies.
- 641 2. Select the default Android policy.

642	3.	Navigate to Android Enterprise Settings > App Compliance.
643	4.	Click Edit.
644	5.	Check the box next to Configure Required Apps if not checked already. If it is, click the + icon.
645	6.	Enter com.zimperium.zips as the App ID.
646	7.	Click Save And Publish. This will prevent the user from uninstalling zIPS once it is installed.
647	8.	Navigate to Security > Policies.
648	9.	Select the default iOS policy.
649	10.	Click Application Compliance.
650	11.	Click Edit.
651 652	12.	Check the box next to Configure Required Applications if not checked already. If it is, click the + icon.
653	13.	Enter Zimperium zIPS for the Application Name.
654	14.	Click Save And Publish, and follow the prompts to publish the policy.
655	2.3.4	MaaS360 Risk Posture Alerts
656	1.	From the MaaS360 home screen, click the + button that says Add Alert.

657 Figure 2-16 Add Alert Button

658

HOME	DEVICES	USERS	SECURITY	APPS	REPORTS	SETUP						
· ·	Alert Cent Analyzed: Wedr		mber 7, 2018 9:1	14:50 AM ES	ŝT				+ I Alert	Ş	G	0
2	Next	to Ava	ailable fo	or. sel	ect All A	dministrators.						

- 659 3. For Name, enter **Zimperium Risk Posture Elevated**.
- 660 4. Under **Condition 1,** select **Custom Attributes** for Category.
- 661 5. Select **zimperium_risk_posture** for Attribute.
- 662 6. Select **Equal To** for Criteria.
- For Value, select Elevated for the count of risk posture elevated devices or Critical for risk posture critical devices.

dd Alert				Available for	All Administrators	~
Name & Description	Zimperium Risk Posture E	Description. E.g. 'of my device	es are jailbroken'	Security	~	
Advanced Search						
1. Search for	Active Devices	O Inactive Devices	O All Devices			
2. With Device Type(s)	🗹 Smartphones 🛛 🗹 Ta	iblets				
3. Last Reported	Last 7 Days	~				
3. Last Reported 4. Search Criteria	Last 7 Days All Conditions (AND)		ut configuring Search Criteria accurat	ely		
	All Conditions (AND)		ut configuring Search Criteria accurat		vated	∨ ⊝

665 Figure 2-17 Zimperium Risk Posture Alert Configuration

666 8. Click Update.

667 2.4 Palo Alto Networks Virtual Firewall

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

669 2.4.1 Network Configuration

- Ensure that all Ethernet cables are connected or assigned to the virtual machine and that the
 management web user interface is accessible. Setup will require four Ethernet connections: one
 for management, one for wide area network (WAN), one for local area network, and one for the
 demilitarized zone (DMZ).
- 674 2. Reboot the machine if cables were attached while running.
- 675 3. Navigate to **Network > Interfaces > Ethernet.**
- 676 4. Click **ethernet1/1**, and set the Interface Type to be **Layer3**.
- 5. Click **IPv4**, ensure that **Static** is selected under Type, and click **Add** to add a new static address.
- 6. If the appropriate address does not exist yet, click **New Address** at the bottom of the prompt.
- 679 7. Once the appropriate interfaces are configured, commit the changes. The Link State icon should
 680 turn green for the configured interfaces. The commit dialogue will warn about unconfigured
 681 zones. That is an expected dialogue warning.

682	8.	Navigate to Network > Zones.
683	9.	Click Add. Give the zone an appropriate name, set the Type to Layer3, and assign it an interface.
684	10.	Commit the changes.
685	11.	Navigate to Network > Virtual Routers.
686	12.	Click Add.
687	13.	Give the router an appropriate name, and add the internal and external interfaces.
688 689 690	14.	Click Static Routes > Add . Give the static route an appropriate name, e.g., WAN. Set the destina- tion to be 0.0.0/0 , set the interface to be the WAN interface, and set the next hop internet protocol (IP) address to be the upstream gateway's IP address.
691 692	15.	(optional) Delete the default router by clicking the checkbox next to it and clicking Delete at the bottom of the page.
693	16.	Commit the changes. The commit window should not display any more warnings.
694	17.	Navigate to Network > DNS Proxy.
695	18.	Click Add.
696 697	19.	Give the proxy an appropriate name. Under Primary, enter the primary domain name system (DNS) IP address.
698	20.	(optional) Enter the secondary DNS IP address.

699 21. Add the interfaces under Interface. Click OK.

	🗹 Enable				Interface 🔺			
Name	Enterprise_[DNS_Proxy			ethernet1/1			
Inheritance Source	None			-	ethernet1/2			
	Check in	nheritance source sta	atus		ethernet1/3			
Primary	10.8.1.1			•				
Secondary	192.168.8.1	.0		•	🕂 Add 📮 Delete	e		
DNS Proxy Rules	Static Ent	tries Advanced						
0.				_			0 item	
Name		Cacheable	Domain Nam	e		Primary	0 item Secondary	s 🔿 (
Name		Cacheable	Domain Nam	e		Primary		is 🔿 (
Name		Cacheable	Domain Nam	e		Primary		IS
Name		Cacheable	Domain Nam	e		Primary		IS 🔿 (
Add Delete		Cacheable	Domain Nam	e		Primary		s Đ (

700 Figure 2-18 DNS Proxy Object Configuration

- 701 22. Navigate to **Device > Services**.
- 702 23. Click the **gear** in the top-right corner of the Services panel.
- 24. Under DNS settings, click the radio button next to DNS Proxy Object. Select the created DNS
 proxy object from the drop-down.
- 25. Click **OK** and commit the changes. This is where static DNS entries will be added in the future.
- 706 26. Navigate to **Objects > Addresses**.
- For each device on the network, click Add. Give the device an appropriate name, enter an optional description, and enter the IP address.
- 709 28. Click **OK**.
- 710 29. Once all devices are added, commit the changes.
- 711 30. Navigate to **Policies > NAT**.
- 712 31. Click Add.

- 713 32. Give the network address translation rule a meaningful name, such as External Internet Access.
- 714 33. Click **Original Packet**.
- 715 34. Click **Add**, and add the zone representing the intranet—in this case, **Enterprise_Intranet**.
- 716 35. Repeat step 34 for the secure sockets layer (SSL) VPN zone.
- 717 36. Under **Source Address,** click **Add**.
- 718 37. Enter the subnet corresponding to the intranet segment.
- 719 38. Repeat step 37 for the SSL VPN segment.
- 39. Click Translated Packet. Set the translation type to Dynamic IP and Port. Set Address Type to be
 Interface Address. Set Interface to be the WAN interface, and set the IP address to be the WAN
 IP of the firewall.
- 40. Click **OK** and commit the changes.
- 724 Figure 2-19 Original Packet Network Address Translation Configuration

NAT Policy	Rule					0
General	Original Packet	Translated Packet				
🔲 Апу		Destination Zone		Any	🗹 Any	1
Source	e Zone 🔺	Enterprise_WAN	-	Source Address 🔺	Destination Address 🔺	H
🔲 🚧 En	terprise_Intranet			🗐 🔙 Internal Segment		11
🔲 🕬 En	terprise_VPN	Destination Interface		🕅 🔩 VPN Segment		
		ethernet1/1				
		Service				
		any	*			
🕂 Add 🌘	= Delete			🕂 Add 📮 Delete	🕂 Add 🛛 🚍 Delete	
					OK Cancel	

- 725 2.4.2 Demilitarized Zone Configuration
- 1. Navigate to **Network > Interfaces**.
- 727 2. Click the interface that has the DMZ connection.

728 729	3.	Add a comment, set the Interface Type to Layer3, and assign it to the virtual router created ear- lier.
730	4.	Click IPv4 > Add > New Address. Assign it an IP block, and give it a meaningful name. Click OK.
731	5.	Navigate to Network > Zones.
732	6.	Click Add . Give it a meaningful name, such as Enterprise_DMZ.
733 734	7.	Set the Type to Layer3, and assign it the new interface that was configured—in this case, ether- net1/3.
735	8.	Click OK .
736 737	9.	Navigate to Network > DNS Proxy. Click Add under Interface , and add the newly created inter- face. Click OK.
738	10.	Commit the changes.
739	11.	Navigate to Network > Interfaces, and the configured interfaces should be green.
740	2.4.3	Firewall Configuration
741	1.	Navigate to Policies > Security .
742	2.	Click Add.
743	3.	Give the rule a meaningful name, such as Intranet Outbound.
744	4.	Click Source . Click Add under source zone, and set the source zone to be the internal network.
745 746	5.	Click Destination. Click Add under destination zone, and set the destination zone to be the WAN zone.
747 748	6.	Click Service/URL Category. Under Service , click Add , and add service-dns . Do the same for service-http and service-https.
749	7.	Click OK .
750	8.	Click Add.
751	9.	Click Destination. Add the IP address of the Simple Mail Transfer Protocol (SMTP) server.
752	10.	Click Application. Click Add.
753	11.	Search for smtp . Select it.
754	12.	Click OK .

- 755 13. Commit the changes.
- 14. Internal hosts should now be able to communicate on the internet.

757 2.4.4 Certificate Configuration

- 1. Navigate to **Device > Certificate Management > Certificate Profile**.
- 759 2. Click Add.
- 760 3. Give the profile a meaningful name, such as Enterprise_Certificate_Profile.
- 761 4. Select **Subject** under **Username Field**.
- 5. Select the radio button next to **Principal Name**.
- 763 6. Enter the domain under **User Domain**—in this case, enterprise.
- 764 7. Click Add under CA Certificates. Select the internal root CA certificate.
- 765 8. Click Add under CA Certificates. Select the internal sub CA certificate. (Note: The entire certifi 766 cate chain must be included in the certificate profile.)
- 767 9. Click **OK**.
- 768 10. Commit the changes.

769 Figure 2-20 Certificate Profile

Name	Interprise_Certificate_Profile							
sername Field	Subject	comm	on-name					
User Domain	enterprise							
CA Certificates	Name	Default OCSP URI	fault OCSP URL OCSP Verify Certificate					
	Internal Root							
	Internal Sub							
	Add Delete	::// or https://)	-					
		n// or https://) CRL Receive Timeout (sec)	5	Block session if certificate status is				
	Default OCSP URL (must start with http Use CRL Use OCSP			Block session if certificate status is unknown				
	Default OCSP URL (must start with http Use CRL	CRL Receive Timeout (sec)	5	unknown				
	Default OCSP URL (must start with http Use CRL Use OCSP	CRL Receive Timeout (sec) OCSP Receive Timeout (sec)	5	unknown Block session if certificate status cannot l				

- 770 2.4.5 Website Filtering Configuration
- 771 2.4.5.1 Configure Basic Website Blocking
- 1. Navigate to **Objects > URL Category**.
- 773 2. Click Add.
- 3. Enter a name for the URL Category. Click **Add** on the bottom.
- Add websites that should be blocked. Use the form **.example.com* for all subdomains and *ex- ample.com* for the root domain.

777 Figure 2-21 Custom URL Category

Custom URL Catego	©
Name	Blocked Websites
Description	
•	2 items 🗨 🗙
Sites	
*.example.com	
example.com	
🕂 Add 🗖 Delete	🔁 Import 🚊 Export
Enter one entry per row. Each entry may be of the	form www.example.com or it could have wildcards like www.*.com.
	OK

- 5. Click **OK**.
- 6. Navigate to **Objects > URL Filtering**.
- 780 7. Click Add.
- 781 8. Give the filtering profile a name.
- 9. Scroll to the bottom of the categories table. The profile created in step 4 should be the last item
 in the list, with an asterisk next to it. Click where it says **allow**, and change the value to **block**.
- 10. Configure any additional categories to allow, alert, continue, block, or override.

785 Figure 2-22 URL Filtering Profile

Name Block_List Description Categories Overrides URL Filtering Settings User Credential Detection HTTP Header Insertion	n		
	n		
ategories Overrides URL Filtering Settings User Credential Detection HTTP Header Insertio	n		
		67 items 🔿	×
	te Access	User Credential Submission	
	low	allow	-
translation all	low	allow	
Travel all	low	allow	
unknown all	low	allow	
weapons bl	ock	block	
web-advertisements all	low	allow	
web-based-email all	low	allow	
web-hosting all	low	allow	
Block List * bl	ock	block	-

- 786 11. Click **OK**.
- 787 12. Navigate to **Policies > Security**.
- 13. Select a policy to which to apply the URL filtering.
- 789 14. Select Actions.
- 790 15. Next to **Profile Type,** select **Profiles**.
- 791 16. Next to **URL Filtering,** select the created URL filtering profile.

792 Figure 2-23 URL Filtering Security Policy

General	Source	Use	er Destination	Application	Service/URL Category	Actions	
Action Se	-	Action	Allow	- -	Log Setting	Log at Session Sta	rt
			Send ICMP Unr			Log at Session End	
Profile Se	etting				Log Forwarding	None	
	Profile	Туре	Profiles	-	Other Settings		
	Antivirus	None		~	Schedule	None	
	Inerability	None		~	QoS Marking	None	
	Protection					Disable Server Res	ponse Inspection
Ant	ti-Spyware	None		~			
UR	L Filtering	Block	List	-			
Fil	e Blocking	None		-			
Dat	a Filtering	None		-			
WildFir	e Analysis	None		~			

- 793 17. Click **OK.**
- 18. Repeat steps 13–17 for any policies to which to apply the filtering profile.
- 795 19. Commit the changes.

796 2.4.5.2 Configure SSL Website Blocking

Note: This section is optional. Section <u>2.4.5.1</u> outlines how to configure basic URL filtering, which will
serve a URL blocked page for unencrypted (http [hypertext transfer protocol]) connections, and it will
send a transmission control protocol reset for encrypted (https [hypertext transfer protocol secure])
connections, which will show a default browser error page. This section outlines how to configure the
firewall so that it can serve the same error page for https connections as it does for http connections.
This is purely for user experience and has no impact on blocking functionality.

- 803 1. Navigate to **Device > Certificates**.
- 2. Click **Generate** on the bottom of the page.
- 805 3. Give the root certificate a name, such as SSL Decryption Root; and a common name (CN) such as
 806 PA Root.

4. Check the box next to **Certificate Authority**.

808 Figure 2-24 Generating the Root CA

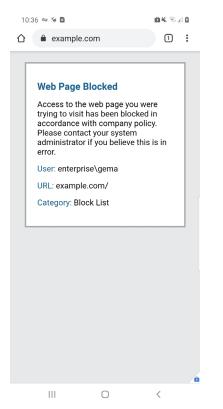


- 809 5. Click Generate.
- 810 6. Click **Generate** at the bottom of the page.
- 811 7. Give the certificate a name, such as SSL Decryption Intermediate.
- 812 8. Give the certificate a CN, such as PA Intermediate.
- 9. Next to **Signed By**, select the generated root CA. In this case, SSL Decryption Root was selected.
- 814 10. Check the box next to **Certificate Authority**.
- 815 11. Click **Generate**.
- 816 12. Click the newly created certificate.
- 13. Check the boxes next to **Forward Trust Certificate** and **Forward Untrust Certificate**.

818	14. Click OK .
819	15. Navigate to Policies > Decryption .
820	16. Click Add.
821	17. Give the policy a name and description.
822	18. Click Source.
823	19. Under Source Zone, click Add .
824 825	20. Select the source zone(s) that matches the security policy that uses URL filtering. In this imple- mentation, the Intranet and SSL VPN zones were selected.
826	21. Click Destination.
827	22. Under Destination Zone, click Add.
828 829	23. Select the destination zone that matches the security policy that uses URL filtering. Most likely it is the WAN zone.
830	24. Click Service/URL Category.
831	25. Under URL Category, click Add.
832	26. Select the created block list. This ensures that only sites matching the block list are decrypted.
833	27. Click Options .
834	28. Next to Action, select Decrypt.
835	29. Next to Type, select SSL Forward Proxy.
836	30. Next to Decryption Profile, select None.

- 837 31. Click **OK**.
- 838 32. Commit the changes.

839 Figure 2-25 Blocked Website Notification



- 840 2.4.6 User Authentication Configuration
- 1. Navigate to **Device > Setup > Services > Service Route Configuration**.
- 842 2. Click **Destination**.
- 843 3. Click Add.
- 844 4. Enter the IP address of the internal LDAP server for Destination.
- 5. Select the **internal network adapter** for Source Interface.
- 846 6. Select the **firewall's internal IP address** for Source Address.
- 847 7. Click **OK** twice, and commit the changes.

848 Figure 2-26 Service Route Configuration

Service Route Configurat	tion		0
	nterface for all) Oustonation	mize	
Destination	Source Interface	Source Address	
192.168.8.10	ethernet1/2	Enterprise_Firewall_Internal	
Add ■ Delete Se	t Selected Service Routes		
		OK Can	cel

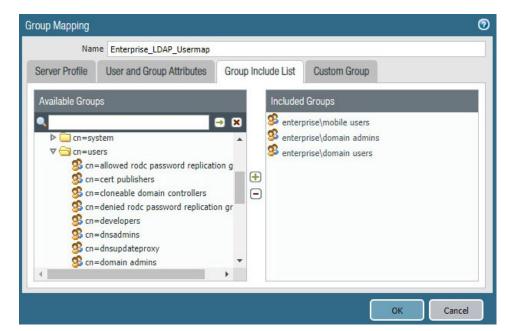
- 849 8. Navigate to **Device > Server Profiles > LDAP**.
- 850 9. Click Add.
- 10. Give the profile a meaningful name, such as Enterprise_LDAP_Server.
- 852 11. Click **Add** in the server list. Enter the name for the server and the IP.
- 12. Under **Server Settings**, set the Type to active-directory.
- 13. Enter the **Bind DN** and the password for the Bind DN.
- Note: In this implementation, a new user, palo-auth, was created in Active Directory. This user does not require any special permissions or groups beyond the standard Domain Users group.
- 857 14. Ensure that **Require SSL/TLS secured connection** is checked.
- 858 15. Click the **down arrow** next to **Base DN**. If the connection is successful, the Base DN (Distin-859 guished Name) should display.
- 860 16. Click **OK.**

861 Figure 2-27 LDAP Server Profile

LDAP Server Profile					0
Profile Name	Enterprise_LDAP				
	Administrator Use On	ly			
Server List			Server Settings		
Name	LDAP Server	Port	Туре	active-directory	-
LDAP Server	192.168.8.10	389	Base DN	DC=enterprise,DC=mds,DC=local	-
			Bind DN	palo-auth@enterprise.mds.local	
			Password	••••••	
🕂 Add 🛛 🖃 Delete			Confirm Password	••••••	
	FQDN of the LDAP server	_	Bind Timeout	30	
			Search Timeout	30	
			Retry Interval	60	
				Require SSL/TLS secured connection	
				Verify Server Certificate for SSL sessions	
				OK Can	cel

- 862 17. Navigate to **Device > User Identification > Group Mapping Settings**.
- 863 18. Click Add.
- 864 19. Give the mapping a name, such as Enterprise_LDAP_Usermap.
- 20. Select the **server profile**, and enter the **user domain**—in this case, Enterprise.
- 866 21. Click Group Include List.
- 22. Expand the arrow next to the **base DN** and then again next to **cn=users**.
- 868 23. For each group that should be allowed to connect to the VPN, click the proper entry and then
 869 the + button. In this example implementation, mobile users, domain users, and domain admins
 870 were used.

871 Figure 2-28 LDAP Group Mapping



- 872 24. Click **OK**.
- 873 25. Navigate to **Device > Authentication Profile**.
- 874 26. Click **Add**.
- 875 27. Give the profile a meaningful name, such as Enterprise_Auth.
- 876 28. For the Type, select LDAP.
- 29. Select the newly created LDAP profile next to **Server Profile**.
- 30. Set the Login Attribute to be **sAMAcountName**.
- 31. Set the User Domain to be the LDAP domain name—in this case, enterprise.

	Name E	nterprise_ <u>Auth</u>	
Authentication	Factors	Advanced	
	Тур	LDAP	
	Server Profile	Enterprise_LDAP	
	Login Attribut	sAMAccountName	
Password	Expiry Warning	1 7	
		Number of days prior to warning a user about password expiry.	
	User Domain	enterprise	
Use	rname Modifie	v %USERINPUT%	
Single Sign O	1		
	Kerberos Rea	m	
	Kerberos Keyt	Click "Import" to configure this field X Import	

880 Figure 2-29 LDAP User Authentication Profile

- 881 32. Click on Advanced.
- 33. Click Add. Select enterprise\domain users.
- 883 34. Repeat step 33 for **mobile users** and **domain admins.**
- 884 35. Click **OK.**
- 885 36. Commit the changes.

886 2.4.7 VPN Configuration

- 1. Navigate to **Network > Interfaces > Tunnel.**
- 888 2. Click Add.
- 889 3. Enter a tunnel number. Assign it to the main virtual router. Click **OK**.
- 890 Figure 2-30 Configured Tunnel Interfaces

	Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
	tunnel		none	none	none		
891	tunnel.1		none	Enterprise_Main_Ro	Enterprise_VPN	۹.	SSL VPN

- 892 4. Click the **newly created tunnel**.
- 5. Click the drop-down next to **Security Zone.** Select **New Zone**.
- 6. Give it a name, and assign it to the newly created tunnel. Click **OK** twice.
- 895 Figure 2-31 SSL VPN Tunnel Interface Configuration

Tunnel Int	erface			0
Ir	nterface Name	tunnel	. 1	
	Comment	SSL VPN		
1	Netflow Profile	None		
Config	IPv4 IP	6 Advanced		
Assign	Interface To			
	Virtual Rout	er Enterprise_Main_Router		
	Security Zo	ne Enterprise_VPN		-
			ОК	Cancel

- 896 7. Commit the changes.
- 897 8. Navigate to **Policies > Authentication**.
- 898 9. Click **Add**.
- 10. Give the policy a **descriptive name**. For this example, the rule was named VPN_Auth.
- 900 11. Click **Source**.
- 901 12. Click **Add**, and add the VPN and WAN zones.
- 902 13. Click **Destination**.
- 903 14. Check the **Any** box above **Destination Zone**.
- 904 15. Click Service/URL Category.
- 905 16. Click **Add** under **Service**, and add **service-https**.
- 906 17. Click **Actions**.

907	18	. Next to Authentication Enforcement, select default-web-form.
908	19	. Click OK .
909	2.4.7.	1 Configure the GlobalProtect Gateway
910	1.	Navigate to Network > GlobalProtect > Gateways.
911	2.	Click Add.
912 913	3.	Give the gateway a meaningful name. For this implementation, the name Enterprise_VPN_Gate- way was used.
914	4.	Under Interface, select the WAN Ethernet interface.
915	5.	Ensure that IPv4 Only is selected next to IP Address Type.
916	6.	Select the WAN IP of the firewall next to IPv4 Address. Ensure that end clients can resolve it.
917	7.	Click Authentication.
918	8.	Select the created SSL/TLS service profile next to SSL/TLS Service Profile.
919	9.	Click Add under Client Authentication.
920	10	. Give the object a meaningful name, such as iOS Auth.
921	11	. Next to OS, select iOS .
922	12	. Next to Authentication Profile, select the created Authentication Profile.

923 13. Next to Allow Authentication with User Credentials OR Client Certificate, select Yes.

Name	iOS Auth
OS	iOS
Authentication Profile	Enterprise_Auth
GlobalProtect App Login Screen	
Username Labe	Username
Password Labe	Password
Authentication Message	Enter login credentials
	Authentication message can be up to 256 characters.
Allow Authentication with Use 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.

924 Figure 2-32 GlobalProtect iOS Authentication Profile

- 925 14. Click **OK**.
- 926 15. Click Add under Client Authentication.
- 927 16. Give the object a meaningful name, such as Android Auth.
- 928 17. Next to **OS**, select Android.
- 929 18. Next to Authentication Profile, select the created Authentication Profile.
- 930 19. Next to Allow Authentication with User Credentials OR Client Certificate, select No.
- 931 20. Click **Agent**.
- 932 21. Check the box next to **Tunnel Mode**.
- 933 22. Select the **created tunnel interface** next to **Tunnel Interface**.
- 934 23. Uncheck Enable IPSec.
- 935 24. Click **Timeout Settings**.
- 936 25. Set **Disconnect On Idle** to an organization defined time.
- 937 26. Click Client IP Pool.
- 938 27. Click Add, and assign an IP subnet to the clients—in this case, 10.3.3.0/24.
- 939 28. Click **Client Settings**.

- 940 29. Click **Add**.
- 941 30. Give the config a meaningful name, such as Enterprise_Remote_Access.
- 942 31. Click User/User Group.
- 943 32. Click **Add** under **Source User**.
- 944 33. Enter the LDAP information of the group allowed to use this rule. In this example, implementa 945 tion, domain users, and mobile users were used.
- 946 Figure 2-33 LDAP Authentication Group Configuration

Configs	0
Authentication Override User/User Group IP Pools Split T	unnel
select	✓ Any
Source User	os 🔺
 cn=domain users,cn=users,dc=enterprise,dc=mds,dc=local cn=mobile users,cn=users,dc=enterprise,dc=mds,dc=local 	
🛨 Add 🛛 🖨 Delete	🖶 Add 🗨 Delete
	OK Cancel

- 947 34. Click **Split Tunnel**.
- 948 35. Click Add under Include.
- 949 36. Enter **0.0.0.0/0** to enable full tunneling.
- 950 37. Click **OK**.
- 951 38. Click Network Services.
- 952 39. Set **Primary DNS** to be the internal domain controller/DNS server—in this case, **192.168.8.10**.
- 953 40. Click **OK**.
- 954 41. Navigate to **Network > Zones**.

- 955 42. Click the created **VPN zone**.
- 956 43. Check the box next to **Enable User Identification**.
- 957 Figure 2-34 VPN Zone Configuration

Zone		0				
Name	Enterprise_VPN	User Identification ACL				
Log Setting	None	Enable User Identification				
Туре	Layer3	Include List 🔺				
■ Interfaces ▲ ■ tunnel.1		Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24				
		Add Delete Users from these addresses/subnets will be identified.				
🕂 Add 🖨 Delete		Exclude List Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24				
Zone Protection Zone Protection Profile	e None 💌					
	Enable Packet Buffer Protection	Add Delete Users from these addresses/subnets will not be identified.				
		OK Cancel				

- 958 44. Click **OK**.
- 959 45. Commit the changes.
- 960 *2.4.7.2 Configure the GlobalProtect Portal*
- 961 1. Navigate to **Network > GlobalProtect > Portals**.
- 962 2. Click Add.
- 963 3. Give the profile a meaningful name, such as Enterprise_VPN_Portal.
- 964 4. For Interface, assign it the firewall's **WAN interface.**

- 965 5. Set IP Address Type to **IPv4 Only**.
- 966 6. Set the IPv4 address to the firewall's **WAN address**.
- 967 7. Set all three appearance options to be **factory-default**.
- 968 Figure 2-35 GlobalProtect Portal General Configuration

GlobalProtect Por	tal Configuration		0
General	Name	Enterprise_VPN_Portal	
Authentication	Network Settings		
Agent	Interface	ethernet1/1	-
-	IP Address Type	IPv4 Only	-
Clientless VPN	IPv4 Address	Enterprise_Firewall_External	-
Satellite	Appearance		
	Portal Login Page	factory-default	-
	Portal Landing Page	factory-default	-
	App Help Page	factory-default	-
		OK Canc	al

- 969 8. Click Authentication.
- 970 9. Select the created SSL/TLS service profile.
- 971 10. Click Add under Client Authentication.
- 972 11. Give the profile a meaningful name, such as Enterprise_Auth.
- 973 12. Select the created **authentication profile** next to **Authentication Profile**.
- 974 13. Click **OK**.

General	Server Authenticatio	n					
Authentication	SSL/TLS Service Profile GlobalProtect_Endpoint						
Agent	Client Authentication	1					
Clientless VPN	Name	os	Authentication Profile	Username Label	Password Label	Authentication Message	
Satellite		10.00					
	✓ Enterprise_Auth	Any	Enterprise_Auth	Username	Password	Enter login credentials	
	Add Delete			Username	Password	Enter login credentials	

975 Figure 2-36 GlobalProtect Portal Authentication Configuration

- 976 14. Click **Agent**, and click **Add** under **Agent**.
- 977 15. Give the agent configuration a name.
- 978 16. Ensure that the **Client Certificate** is set to **None**, and **Save User Credentials** is set to **No**.
- 979 17. Check the box next to **External gateways-manual only**.

Authentication	User/User Group	Internal	External	Арр	Data Collection	
	Name	Agent Cor	nfiq			
	Client Certificate	None			~	
		The selected	client certificate	including	ts private key will be instal	lled on client machines.
	Save User Credentials	No				
Authenticatio	n Override					
		Genera	te cookie for	authenti	cation override	
		Accept	cookie for au	thenticat	tion override	
	Cookie Lifetime	Hours			24	
Certificate to	Encrypt/Decrypt Cookie	None				
Components t	that Require Dynamic	Password	s (Two-Fac	tor Auth	entication)	
	Portal					External gateways-manual only
	Internal gatew	ays-all				External gateways-auto discovery
	hat will use dynamic password Is for each selected option.	s like one-tim	e password (OT	P) to authe	inticate users as opposed t	to using saved credentials. As a result, the user will always be prompte

980 Figure 2-37 GlobalProtect Portal Agent Authentication Configuration

- 981 18. Click External.
- 982 19. Click Add under External Gateways.
- 983 20. Give the gateway a name, and enter the fully qualified domain name (FQDN) of the VPN end984 point.
- 985 21. Click Add under Source Region, and select Any.
- 986 22. Check the box next to Manual.
- 987 23. Click **OK**.
- 988 24. Click **App**.
- 989 25. Under App Configurations > Connect Method, select On-demand.
- 990 26. Next to **Welcome Page**, select factory-default.
- 991 27. Click **OK**.
- 992 28. Click Add under Trusted Root CA.

- 993 29. Select the **internal root certificate** used to generate device certificates.
- 30. Click Add again. Select the root certificate used to create the VPN end-point SSL certificate. For
 this implementation, it is a DigiCert root certificate.
- 996 31. Click Add again. Select the root certificate used for SSL URL filtering, created in a previous sec 997 tion.
- 998 32. Check the box next to **Install in Local Root Certificate Store** for all three certificates.
- 999 Figure 2-38 GlobalProtect Portal Agent Configuration

neral	Agent				
thentication	Configs	User/User Group	os	External Gateways	Client Certificate
ent	Agent Config	any	any	VPN_Gateway	
entless VPN	1				
atellite	•				
ttointo					
temite					
atomito					
itemite					
	🕈 Add 🖨 Deiete 🍳	S Clane 🔹 Mave Up 🔹 Mave Dav	άī.		
atomito		Cline C More La C More Dan Install in Local Root	n.	Agent User Override Key	
	Add Delete 🕻		n.	Agent User Override Key Confirm Agent User Override Key	
		Install in Local Root	A		
Conne	Trusted Root CA	Install in Local Root Certificate Store			
LUHILU .	Trusted Root CA	Install in Local Root Certificate Store			
	Trusted Root CA	Install in Local Root Certificate Store			

- 1000 33. Click **OK.**
- 1001 2.4.7.3 Activate Captive Portal
- 1002 1. Navigate to **Device > User Identification > Captive Portal Settings**.
- 1003 2. Click the **gear** icon on the top right of the Captive Portal box.
- 1004 3. Select the created SSL/TLS service profile and authentication profile.
- 1005 4. Click the radio button next to **Redirect**.
- Next to Redirect Host, enter the IP address of the firewall's WAN interface—in this case,
 1007 10.8.1.2.

1008	Figure 2-39	Captive	Portal	Configuration
1000	I Iguic L 00	Captive	1 01 001	Comparation

Captive Portal			0
Idle Timer (min)	Enable Captive Portal	SSL/TLS Service Profile	GlobalProtect_Endpo 💌
Timer (min) GlobalProtect Network Port for Inbound Authentication Prompts (UDP)		Authentication Profile	Enterprise_Auth
Mode Session Cookie	 Transparent Redirect 		
Timeout (min)	Enable 1440		
Redirect Host	Roaming 10.8.1.2		
Certificate Authentication Certificate Profile	None		~
NTLM Authentication			
Attempts	1		
Timeout (sec)	2		
Reversion Time (sec)	300		
			OK Cancel

- 1009 6. Click **OK**.
- 1010 7. Commit the changes.
- 1011 2.4.7.4 Activate the GlobalProtect Client
- 1012 1. Navigate to **Device > GlobalProtect Client**.
- 1013 2. Acknowledge pop up messages.
- 1014 3. Click **Check Now** at the bottom of the page.
- Click **Download** next to the **first release** that comes up. In this implementation, version 5.0.2ate was used.
- 1017 5. Click **Activate** next to the **downloaded release**.

- 1018 6. Navigate to the FQDN of the VPN. You should see the Palo Alto Networks logo and the Glob-
- alProtect portal login prompt, potentially with a message indicating that a required certificate
- 1020 cannot be found. This is expected on desktops because there is nothing in place to seamlessly1021 deploy client certificates.
- 1022 Figure 2-40 GlobalProtect Portal

·////·	paloalto	
	NETWORKS [®]	
Glo	balProtect Portal	
Username		
Password		
	LOG IN	

- Note: If you intend to use the GlobalProtect agent with a self-signed certificate (e.g., internal PKI), be
 sure to download the SSL certificate from the VPN website and install it in the trusted root CA store.
- 1025 2.4.8 Enable Automatic Application and Threat Updates
- 1026 1. In the **PAN-OS portal**, navigate to **Device > Dynamic Updates**.
- 1027 2. Install the latest updates.
- 1028 a. At the bottom of the page, click **Check Now.**

- b. Under Applications and Threats, click Download next to the last item in the list with the
 latest Release Date. This will take a few minutes.
- 1031 c. When the download completes, click **Close.**
- 1032 Figure 2-41 Downloaded Threats and Applications

Release Date	Downloaded	Currently Installed	Action	Documentation
2018/10/31 17:41:37 EDT	Ŷ		Install Review Policies	Release Notes

- 1033 d. Click Install on the first row.
- 1034e. Click Continue Installation, leaving the displayed box unchecked. Installation will take a1035few minutes.
- 1036 f. When the installation completes, click **Close.**
- Enable automatic threat updates. (Note: Automatic threat updates are performed in the back ground and do not require a reboot of the appliance.)
- 1039a. At the top of the page, next to **Schedule,** click the hyperlink with the date and time, as1040shown in Figure 2-42.
- 1041 Figure 2-42 Schedule Time Hyperlink

	Version 🔺	File Name	Features	Туре
	▼ Applications and Thre	ats Last checked: 2018/11/29 12:25:15 EST	Schedule: Every Wednes	day at 01:02 (Download only)
1042	b. Select th	ne desired recurrence. For this implem	entation, weekly was	used.
1043 1044		Select the desired day and time for the update to occur. For this implementation, Satur- day at 23:45 was used.		
1045	d. Next to	Action, select download-and-install.		

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 hour for the action to be taken.	s old
Allow Extra Time to Review New App-I	Ds	
Set the amount of time the firewall waits b new App-IDs. You can use this wait period based on the new App-IDs.		
New App-ID Threshold (hours)	[1 - 336]	

1046 Figure 2-43 Application and Threats Update Schedule

- 1047
- e. Click **OK.**
- 1048 f. Commit the changes.

1049 **2.5 Kryptowire**

- 1050 Kryptowire was used as an application vetting service via a custom active directory-integrated web 1051 application.
- 1052 2.5.1 Kryptowire and MaaS360 Integration
- 1053 1. Contact IBM support to provision API credentials for Kryptowire.
- Contact Kryptowire support to enable the MaaS360 integration, including the MaaS360 API cre dentials.
- In the Kryptowire portal, click the logged-in user's email address in the upper right-hand corner
 of the portal. Navigate to Settings > Analysis.
- Set the Threat Score Threshold to the desired amount. In this sample implementation, 75 was
 used.

- 1060 5. Enter an **email address** where email alerts should be delivered.
- 1061
 6. Click Save Settings. Kryptowire will now send an email to the email address configured in step 5
 1062
 when an analyzed application is at or above the configured alert threshold.

1063 Appendix A List of Acronyms

AD	Active Directory
ΑΡΙ	Application Programming Interface
СА	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
НТТР	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
РКІ	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

1064 Appendix B Glossary

Bring Your Own Device A non-organization-controlled telework client device. [2] (BYOD)

1065 Appendix C References

- 1066 [1] International Business Machines. "Cloud Extender architecture." [Online]. Available:
 1067 <u>https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/referenc</u>
 1068 <u>es/ce_architecture.htm</u>.
- 1069 [2] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own*
- 1070 *Device (BYOD) Security,* National Institute of Standards and Technology (NIST) Special Publication 1071 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available:
- 1072 https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.