

# NIST SPECIAL PUBLICATION 1800-22C

---

## 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 Ajmo**  
**R. Eugene Craft**  
**Milissa McGinnis\***  
**Kenneth Sandlin**  
**Oksana Slivina**  
**Julie Snyder**  
**Paul Ward**

The MITRE Corporation  
McLean, VA

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

September 2023

FINAL

This publication is available free of charge from  
<https://doi.org/10.6028/NIST.SP.1800-22>



## DISCLAIMER

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

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

National Institute of Standards and Technology Special Publication 1800-22C Natl. Inst. Stand. Technol. Spec. Publ. 1800-22C, 99 pages, (September 2023), CODEN: NSPUE2

## FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at [mobile-nccoe@nist.gov](mailto:mobile-nccoe@nist.gov).

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

National Cybersecurity Center of Excellence  
National Institute of Standards and Technology  
100 Bureau Drive  
Mailstop 2002  
Gaithersburg, MD 20899  
Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework 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, Maryland.

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

This 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.

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- 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

## ABSTRACT

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

Incorporating BYOD deployments into an organization can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of traditional in-office processes with mobile device technologies 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 mobile devices.

However, some of the features that make BYOD mobile devices increasingly flexible and functional also present unique security and privacy challenges to both organizations and device owners. The unique nature of these challenges is driven by the differing risks posed by the type, age, operating system (OS), and other variances in mobile devices.

Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks. Solutions that are designed to secure corporate devices and on-premises data do not provide an effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new 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.

To help organizations benefit from BYOD's flexibility while protecting themselves from critical security and privacy challenges, this practice guide provides an example solution using standards-based, commercially available products and step-by-step implementation guidance.

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

Name	Organization
Donna Dodson*	NIST
Joshua M. Franklin*	NIST
Dylan Gilbert	NIST
Jeff Greene*	NIST
Natalia Martin	NIST

Name	Organization
William Newhouse	NIST
Cherilyn Pascoe	NIST
Murugiah Souppaya	NIST
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
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Jessica Walton	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 Lamoureux	Palo Alto Networks
Sean Morgan	Palo Alto Networks

Name	Organization
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Mikel Draghici*	Zimperium

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

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

Technology Partner/Collaborator	Build Involvement
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

## DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in 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.

## PATENT DISCLOSURE NOTICE

*NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.*

*As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.*

*No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.*

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Practice Guide Structure .....	1
1.2	Build Overview .....	2
1.3	Typographic Conventions .....	3
1.4	Logical Architecture Summary .....	3
<b>2</b>	<b>Product Installation Guides.....</b>	<b>4</b>
2.1	Network Device Enrollment Services Server .....	4
2.1.1	NDES Configuration .....	4
2.2	International Business Machines MaaS360 .....	8
2.2.1	Cloud Extender .....	8
2.2.2	Android Enterprise Configuration .....	15
2.2.3	iOS APNs Certificate Configuration .....	16
2.2.4	Apple User Enrollment (UE) Configuration .....	16
2.2.5	Android Configuration .....	18
2.2.6	iOS Configuration.....	20
2.3	Zimperium .....	23
2.3.1	Zimperium and MaaS360 Integration .....	23
2.3.2	Automatic Device Activation .....	24
2.3.3	Enforce Application Compliance .....	26
2.3.4	MaaS360 Risk Posture Alerts.....	27
2.4	Palo Alto Networks Virtual Firewall .....	28
2.4.1	Network Configuration .....	28
2.4.2	Demilitarized Zone Configuration .....	31
2.4.3	Firewall Configuration .....	31
2.4.4	Certificate Configuration .....	32
2.4.5	Website Filtering Configuration .....	33
2.4.6	User Authentication Configuration .....	39
2.4.7	VPN Configuration .....	43
2.4.8	Enable Automatic Application and Threat Updates .....	53
2.5	Kryptowire .....	55
2.5.1	Kryptowire and MaaS360 Integration .....	55
	<b>Appendix A List of Acronyms .....</b>	<b>56</b>



<b>Appendix B Glossary .....</b>	<b>58</b>
<b>Appendix C References .....</b>	<b>59</b>
<b>Appendix D Example Solution Lab Build Testing Details .....</b>	<b>60</b>
D.1 Threat Event 1 – Unauthorized Access to Sensitive Information Via a Malicious or Intrusive Application Practices .....	60
D.2 Threat Event 2 – Theft of Credentials Through a Short Message Service or Email Phishing Campaign .....	62
D.3 Threat Event 3 – Confidentiality and Integrity Loss Due to Exploitation of Known Vulnerability in the OS or Firmware .....	63
D.4 Threat Event 4 – Loss of Confidentiality of Sensitive Information Via Eavesdropping on Unencrypted Device Communications .....	65
D.5 Threat Event 5 – Compromise of Device Integrity Via Observed, Inferred, or Brute-Forced Device Unlock Code.....	66
D.6 Threat Event 6 – Unauthorized Access to Backend Services Via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications .....	68
D.7 Threat Event 7 – Unauthorized Access of Enterprise Resources From an Unmanaged and Potentially Compromised Device .....	69
D.8 Threat Event 8 – Loss of Organizational Data Due to a Lost or Stolen Device.....	72
D.9 Threat Event 9 – Loss of Confidentiality of Organizational Data Due to its Unauthorized Storage in Non-Organizationally Managed Services.....	74
D.10 Privacy Risk 1 – Wiping Activities on the Employee’s Device May Inadvertently Delete the Employee’s Personal Data .....	78
D.11 Privacy Risk 2 – Organizational Collection of Device Data May Subject Employees to Feeling or Being Surveilled.....	79
D.12 Privacy Risk 3 – Data Collection and Transmission Between Integrated Security Products May Expose Employee Data.....	81
D.13 Privacy Risk 4 – Employees Might Feel Compelled to Participate in Data Processing Practices Inconsistent with Expectations.....	83
D.14 Privacy Risk 5 – Unauthorized or Invasive Application Processing of Information Exposes Employee Data .....	85

## List of Figures

<b>Figure 1-1 High-Level Build Architecture .....</b>	<b>4</b>
<b>Figure 2-1 Post-Deployment Configuration .....</b>	<b>5</b>
<b>Figure 2-2 PasswordMax Registry Configuration .....</b>	<b>7</b>

Figure 2-3 NDES Domain Bindings.....	8
Figure 2-4 Cloud Extender Architecture.....	9
Figure 2-5 Old Cloud Extender Interface.....	10
Figure 2-6 Cloud Extender Service Account Details .....	11
Figure 2-7 Administrator Settings .....	12
Figure 2-8 Administrator Configuration Options .....	13
Figure 2-9 Cloud Extender SCEP Configuration .....	14
Figure 2-10 Cloud Extender Certificate Properties .....	14
Figure 2-11 Enterprise Binding Settings Confirmation.....	15
Figure 2-12 Where to Click to Download the Public Key.....	16
Figure 2-13 MDM configuration in Apple Business Manager .....	17
Figure 2-14 Creating the DEP token.....	17
Figure 2-15 VPP token in MaaS360 .....	18
Figure 2-16 iOS Enrollment Configuration .....	18
Figure 2-17 Android GlobalProtect Application Compliance.....	20
Figure 2-18 Zimperium MaaS360 Integration Configuration.....	24
Figure 2-19 Zimperium zIPS iOS Configuration.....	25
Figure 2-20 Zimperium zIPS Android Configuration .....	26
Figure 2-21 Add Alert Button .....	27
Figure 2-22 Zimperium Risk Posture Alert Configuration .....	28
Figure 2-23 DNS Proxy Object Configuration .....	29
Figure 2-24 Original Packet Network Address Translation Configuration .....	31
Figure 2-25 Certificate Profile .....	33
Figure 2-26 Custom URL Category.....	34
Figure 2-27 URL Filtering Profile.....	35
Figure 2-28 URL Filtering Security Policy .....	36
Figure 2-29 Generating the Root CA.....	37
Figure 2-30 Blocked Website Notification .....	39
Figure 2-31 Service Route Configuration .....	40
Figure 2-32 LDAP Server Profile .....	41
Figure 2-33 LDAP Group Mapping.....	42

Figure 2-34 LDAP User Authentication Profile .....	43
Figure 2-35 Configured Tunnel Interfaces.....	43
Figure 2-36 SSL VPN Tunnel Interface Configuration .....	44
Figure 2-37 GlobalProtect iOS Authentication Profile .....	45
Figure 2-38 LDAP Authentication Group Configuration .....	46
Figure 2-39 VPN Zone Configuration .....	47
Figure 2-40 GlobalProtect Portal General Configuration .....	48
Figure 2-41 GlobalProtect Portal Authentication Configuration .....	49
Figure 2-42 GlobalProtect Portal Agent Authentication Configuration .....	50
Figure 2-43 GlobalProtect Portal Agent Configuration .....	51
Figure 2-44 Captive Portal Configuration.....	52
Figure 2-45 GlobalProtect Portal.....	53
Figure 2-46 Downloaded Threats and Applications.....	53
Figure 2-47 Schedule Time Hyperlink .....	54
Figure 2-48 Application and Threats Update Schedule.....	54
Figure D-1 Contact Created in Work Profile.....	60
Figure D-2 Personal Profile Can't See Work Contacts .....	61
Figure D-3 Contact Created in Managed App.....	61
Figure D-4 Unmanaged App Can't See Managed Contacts .....	62
Figure D-5 Fictitious Phishing Webpage Blocked .....	63
Figure D-6 iOS MaaS360 OS Compliance Alert .....	64
Figure D-7 Zimperium Risk Detected .....	65
Figure D-8 Kryptowire Application Report.....	66
Figure D-9 Android Passcode Configuration .....	67
Figure D-10 iOS Passcode Configuration.....	67
Figure D-11 Zimperium Detecting Disabled Lock screen.....	68
Figure D-12 Application Report with Hardcoded Credentials .....	69
Figure D-13 Attempting to Access the VPN on an Unmanaged iOS Device .....	70
Figure D-14 Attempting to Access the VPN on an Unmanaged Android Device .....	71
Figure D-15 Attempting to Access the VPN on a Managed Android Device .....	72
Figure D-16 Selective Wiping a Device .....	73

Figure D-17 Selective Wipe Complete .....	73
Figure D-18 Corporate Data Removal Confirmation Notification on iOS .....	74
Figure D-19 Work Profile Removal Notification on Android .....	74
Figure D-20 iOS DLP Configuration Options .....	76
Figure D-21 Android DLP Configuration.....	77
Figure D-22 Attempting to Paste Text on iOS Between Unmanaged and Managed Apps.....	78
Figure D-23 Selective Wipe.....	79
Figure D-24 Application Inventory Information .....	80
Figure D-25 Location Information Restricted .....	80
Figure D-26 Non-Administrator Failed Portal Login.....	81
Figure D-27 Admin Login Settings .....	82
Figure D-28 Administrator Levels.....	82
Figure D-29 Mobile Device Information Collection Notification .....	84
Figure D-30 Mobile Device Information Collection Notification .....	85
Figure D-31 Privacy and Information Access of the Application.....	86
Figure D-32 Application Analysis.....	87

# 1 Introduction

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

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

## 1.1 Practice Guide Structure

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

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- 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**)

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:

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

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

- Section 3.4, Risk Assessment, describes the risk analysis we performed.
- Appendix E in Volume B, Example Security Subcategory and 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 created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a BYOD solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Volume B, Section 4.3, Technologies that Support the Security and Privacy Objectives of the Example Solution, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

**For those who would like to see how the example solution can be implemented**, this practice guide 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 capabilities through NIST risk management standards, guidance, and tools. It is provided in this practice 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 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to [mobile-nccoe@nist.gov](mailto:mobile-nccoe@nist.gov).

## 1.2 Build Overview

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 guide, we show how an enterprise can leverage this example solution's concepts to implement 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.

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

## 1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

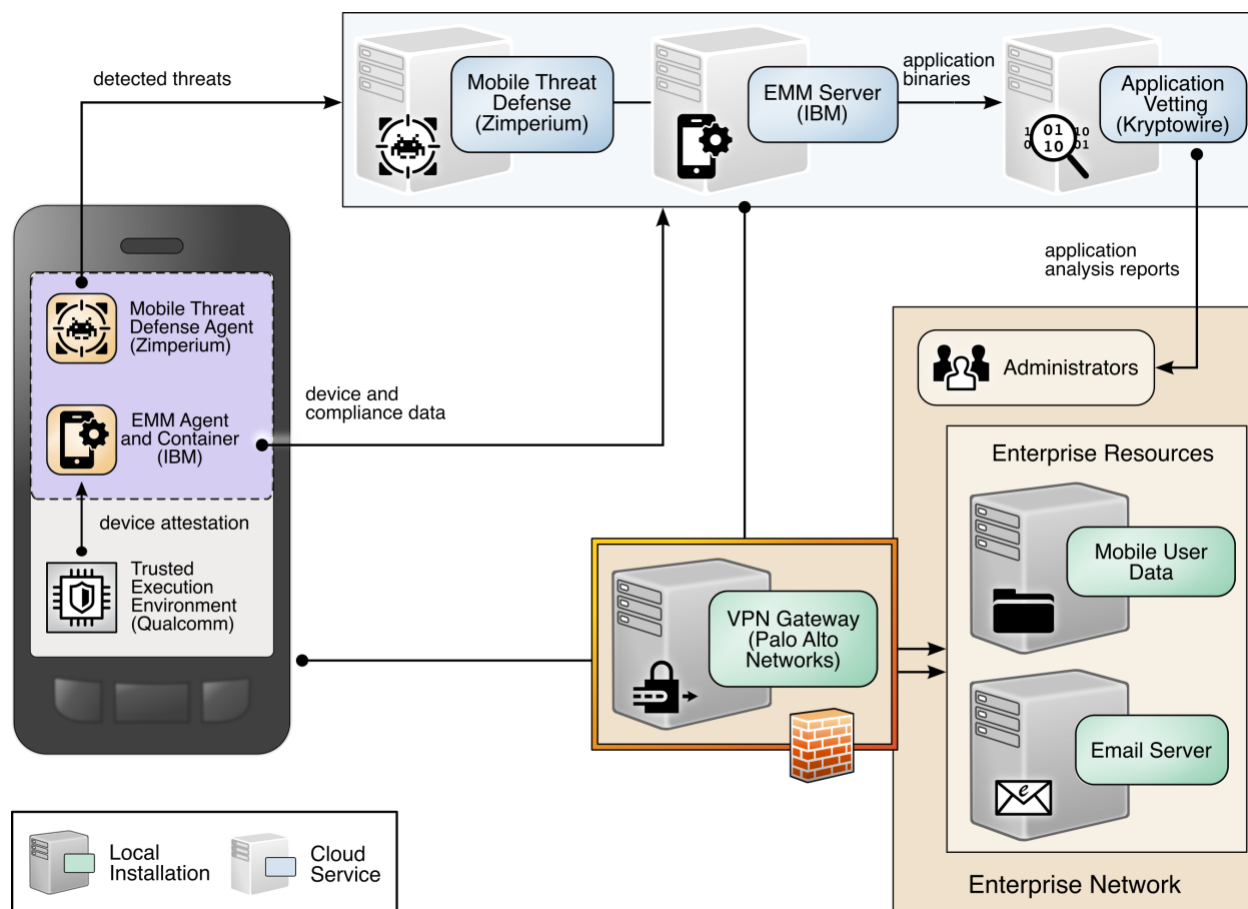
Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File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

Acronyms can be found in [Appendix A](#).

## 1.4 Logical Architecture Summary

[Figure 1-1](#) shows the components of the build architecture and how they interact on a high level.

Figure 1-1 High-Level Build Architecture



## 2 Product Installation Guides

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

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

### 2.1 Network Device Enrollment Services Server

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

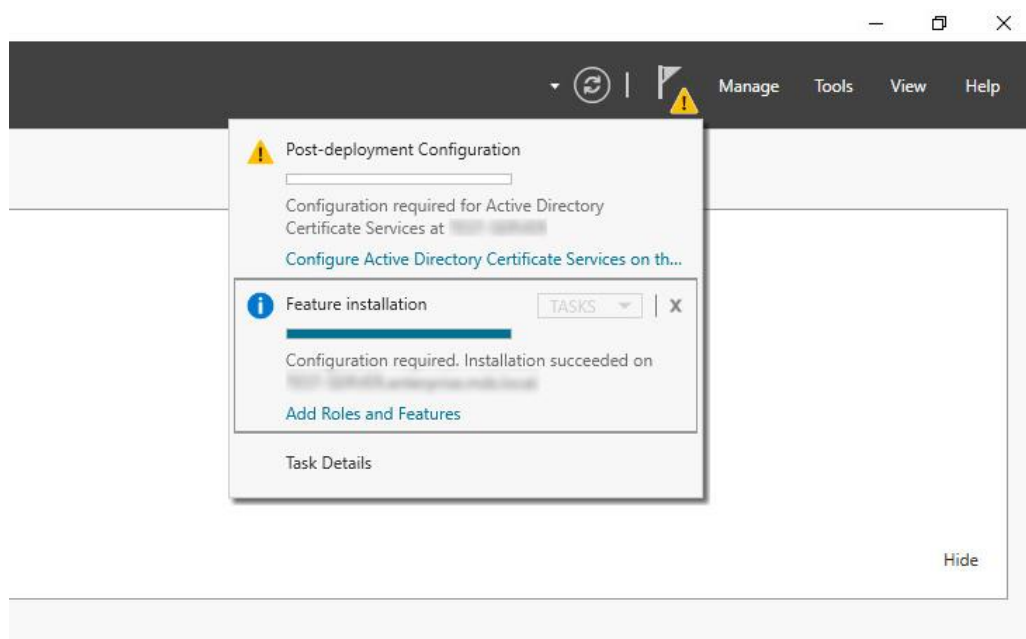
#### 2.1.1 NDES Configuration

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.



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

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



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

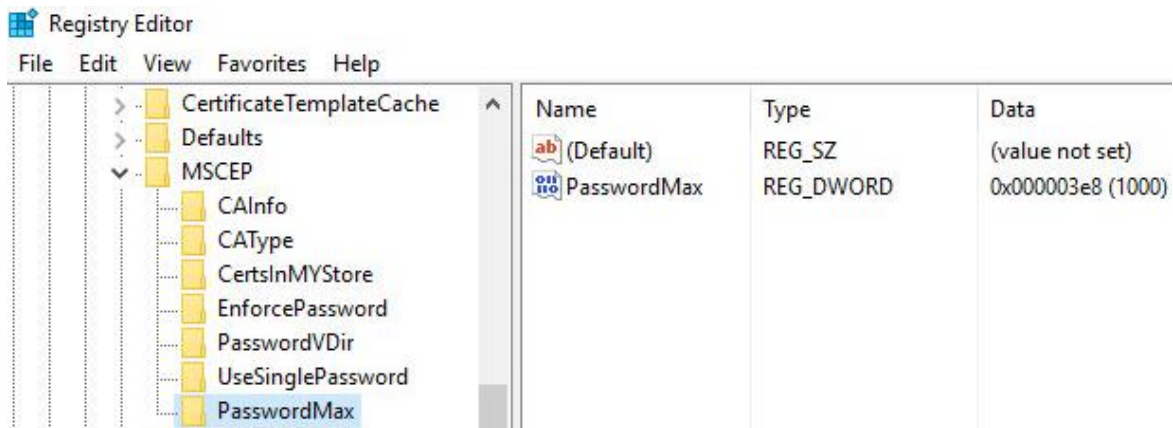
*Note: The domain administrator credentials are required only to configure the NDES. Once the service is configured, the service is executed as the NDES service account, which does not require domain administrator permissions, created in step 12 below.*

11. Check **Network Device Enrollment Service**. Click **Next**.
12. Configure an NDES service account by performing the following actions:
  - a. On the active directory server, open **Active Directory Users and Computers**.

- b. Click **Users** and create a new user for the service. For this example, it will be named NDES. Be sure the password never expires.
  - c. On the NDES server, open **Edit local users and groups**.
  - d. Click **Groups**. Right-click **IIS\_IUSRS**, click **Add to Group**, and click **Add**.
  - e. Search for the service account name—in this case, NDES. Click **Check Names**, then click **OK** if no errors were displayed.
  - f. Click **Apply** and click **OK**.
  - g. Close all windows except the NDES configuration window.
13. Click **Select** next to the box and enter the service account credentials. Click **Next**.
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**.
15. Click **Next** three times.
16. Click **Configure**.
17. On the SUB-CA, open the Certification Authority application.
18. Expand the SUB-CA node, right-click on **Certificate Templates**, and click **Manage**.
19. Right-click on **IPSec (Offline Request)** and click **Duplicate Template**.
20. Under the General tab, set the template display name to **NDES**.
21. Under the **Security** tab, click **Add**.
22. Select the previously configured NDES service account.
23. Click **OK**. Ensure the NDES service account is highlighted, and check **Read** and **Enroll**.
24. Click **Apply**.
25. In the Certification Authority program, right-click on **Certificate Templates**, and select **New > Certificate Template to Issue**.
26. Select the NDES template created in step 24.
27. Click **OK**.
28. On the NDES server, open the Registry Editor (`regedit`).
29. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography`.
30. Select the `MSCEP` key and update all entries besides (Default) to be **NDES**.
31. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP`.

32. Right-click on **MSCEP** and select **New > Key**. Name it **PasswordMax**.
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.

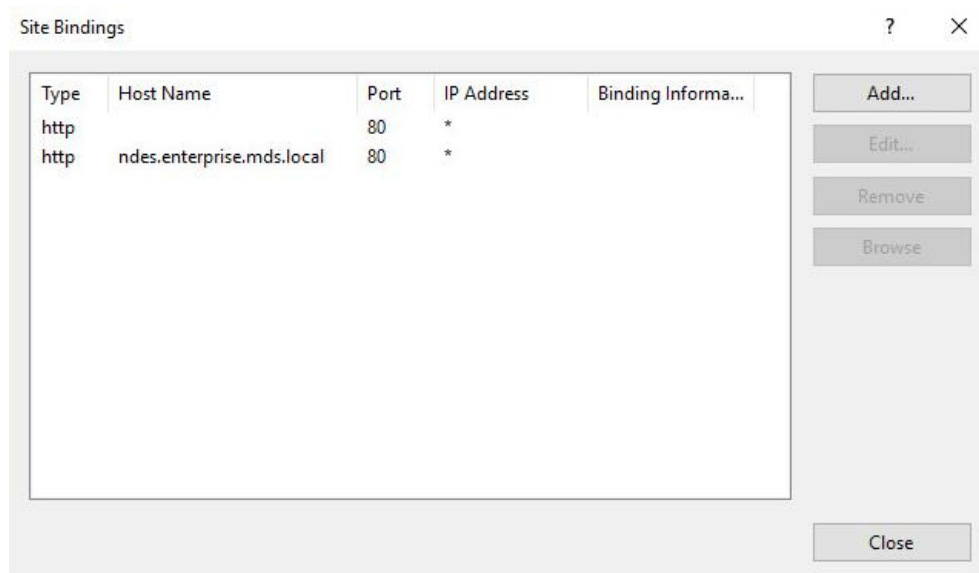
**Figure 2-2 PasswordMax Registry Configuration**



**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.

35. 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.
36. Open the **Internet Information Services (IIS) Manager**.
37. On the left, expand **NDES > Sites**, and select **Default Web Site**.
38. On the right, click **Bindings...**
39. Click **Add**.
40. Below **Host Name**, enter the host name of the server. For this implementation, *ndes.enterprise.mds.local* was used.
41. Click **OK**.

**Figure 2-3 NDES Domain Bindings**



42. Click **Close** and close the IIS Manager.

43. In an elevated command prompt, execute `iisreset`, or reboot the NDES server.

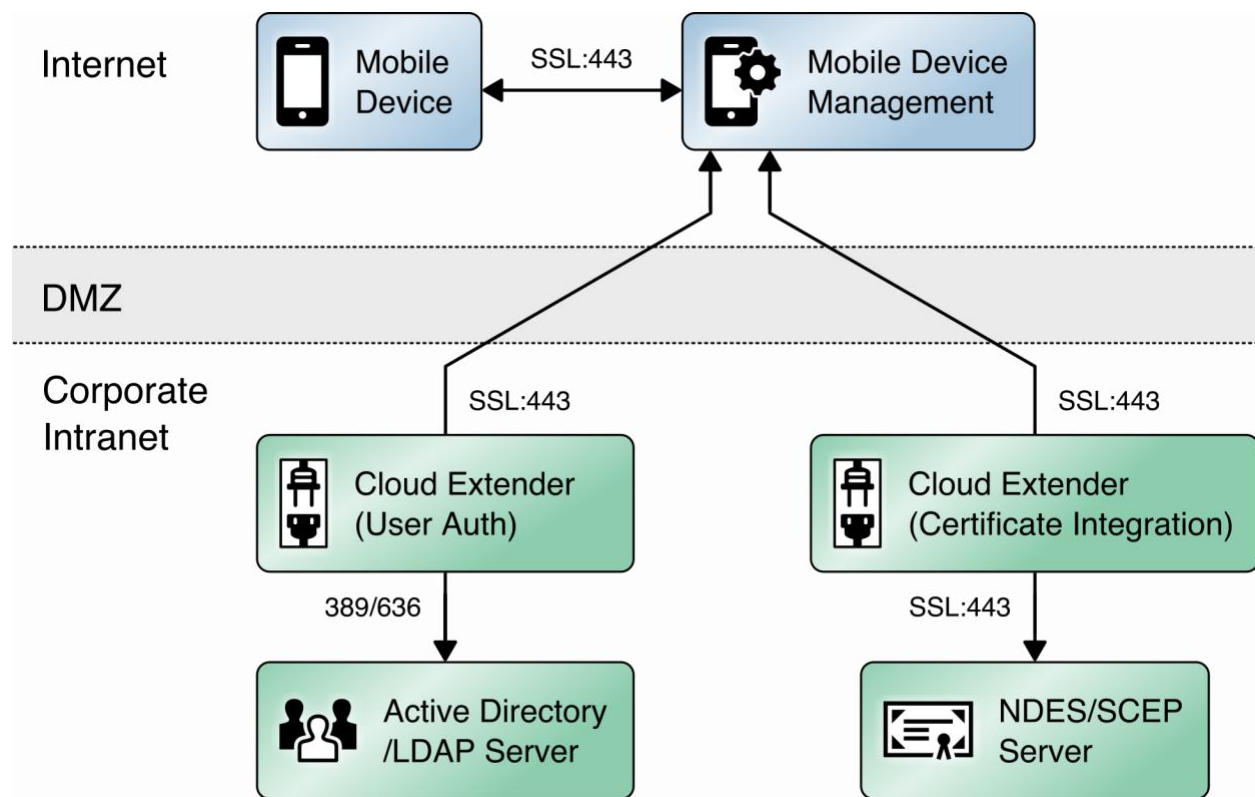
## 2.2 International Business Machines MaaS360

International Business Machines (IBM) contributed an instance of MaaS360 to deploy as the mobile device management (MDM) solution.

### 2.2.1 Cloud Extender

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 overview of how information flows between the web portal and the MaaS360 Cloud Extender.

Figure 2-4 Cloud Extender Architecture



#### 2.2.1.1 Cloud Extender Download

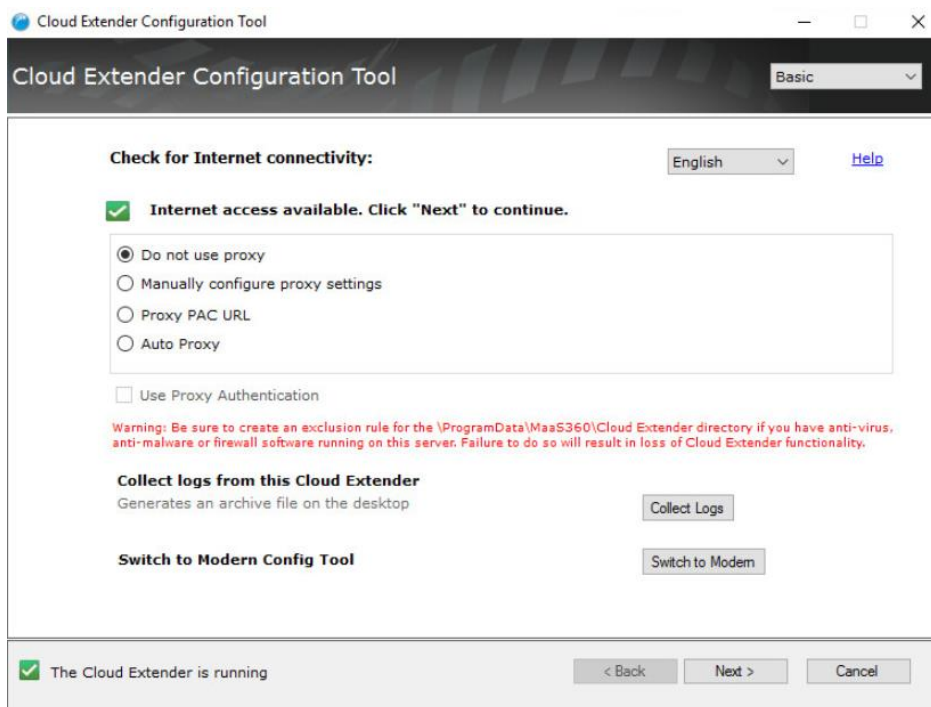
1. Log in to the MaaS360 web portal.
2. Click **Setup > Cloud Extender**.
3. Click the link that says **Click here to get your License Key**. The license key will be emailed to the currently logged-in user's email address.
4. Click the link that says **Click here to download the Cloud Extender**. Save the binary.
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.
6. Install **.NET 3.5 Features** in the **Server Manager** on the machine where the MaaS360 Cloud Extender will run.

#### 2.2.1.2 Cloud Extender Active Directory Configuration

1. On the target machine, run the installation binary.
2. Enter the license key when prompted.
3. Proceed through the setup until the Cloud Extender Configuration Utility opens.

4. If using the old cloud extender interface, click **Switch to Modern**.

Figure 2-5 Old Cloud Extender Interface



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

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

**2 Service Account**

#### Provide Service Account details

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

Username: MAAS360

Password: .....

Domain: enterprise.mds.local

☒ Enable Secure Authentication Mode

Back Next Save Cancel

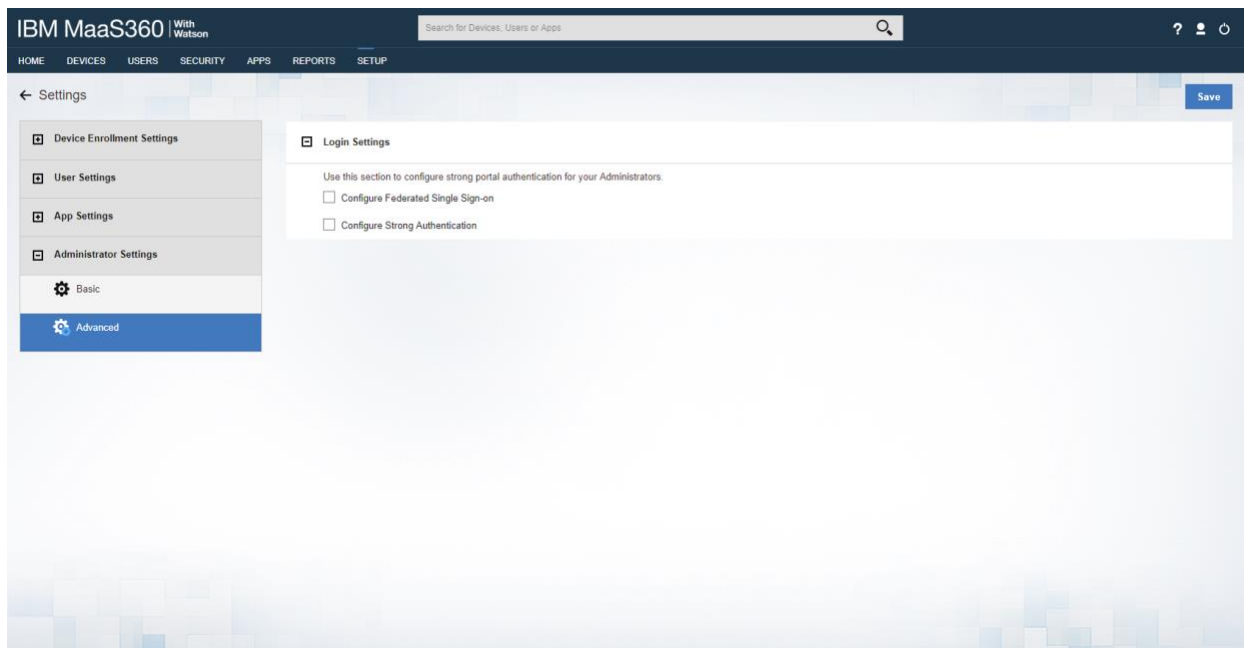
☒ The Cloud Extender is running

7. Click **Next**.
8. (optional) Use the next page to test the active directory integration.
9. Click **Save**.
10. In MaaS360, navigate to **Setup > Cloud Extender**. Ensure that configuration information is displayed, indicating that the MaaS360 Cloud Extender is running.

#### 2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration

1. Log in to the MaaS360 web portal as an administrator.
2. Go to **Setup > Settings**.
3. Expand **Administrator Settings** and click **Advanced**.

Figure 2-7 Administrator Settings




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



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----	⊕

11. Click **Save**.

#### 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).

1. Log in to the server running the MaaS360 Cloud Extender.
2. Launch the Cloud Extender Configuration Tool.
3. Toggle the button below Certificate Integration.
4. Click **Add New Template**.
5. Ensure **Microsoft CA** and **Device Identity Certificates** are selected.
6. Click **Next**.
7. Enter **NDES** for the Template Name and SCEP Default Template.
8. Enter the uniform resource locator (URL) of the NDES server next to **SCEP Server**.
9. Enter credentials of a user with enroll permissions on the template for **Challenge Username** and **Challenge Password**. For this demo implementation, we use the NDES service account.

Figure 2-9 Cloud Extender SCEP Configuration

The screenshot shows the 'Certificate Integration' page with the 'SCEP - Microsoft, Verizon, Open Trust server details' section. The left sidebar shows a progress bar with four steps: 'Start' (completed), 'SCEP Config' (current), 'Cert Attributes', and 'Finish'. The main content area contains the following fields:

- Template Name: NDES
- Hostname of SCEP server: https (dropdown) ndes.enterprise.mds.local
- SCEP Server challenge type: ☒ Dynamic ☐ Static ☐ None
- Challenge Username: ENTERPRISE\NDESSvc
- Challenge Password: (masked with dots)

At the bottom right are buttons for 'Back', 'Next', 'Save', and 'Cancel'. A status bar at the bottom indicates 'The Cloud Extender is running'.

10. Click **Next**.

11. (optional) Check the box next to **Cache certs on Cloud Extender** and specify a cache path on the machine.

Figure 2-10 Cloud Extender Certificate Properties

The screenshot shows the 'Certificate Integration' page with the 'Certificate Properties' section. The left sidebar shows a progress bar with four steps: 'Start' (completed), 'SCEP Config' (completed), 'Cert Attributes' (current), and 'Finish'. The main content area contains the following fields:

- Subject Name: /CN=%uname%/emailAddress=%email%
- Subject Alternate Name: None (dropdown)
- Cache certs on Cloud Extender: ☒
- Location of Certificate Cache: C:\CertCache (with a 'Browse' button)

At the bottom right are buttons for 'Back', 'Next', 'Save', and 'Cancel'. A status bar at the bottom indicates 'The Cloud Extender is running'.

12. Click **Next**.
13. (optional) Enter values for uname and email and generate a test certificate to test the configuration.
14. Click **Save**.

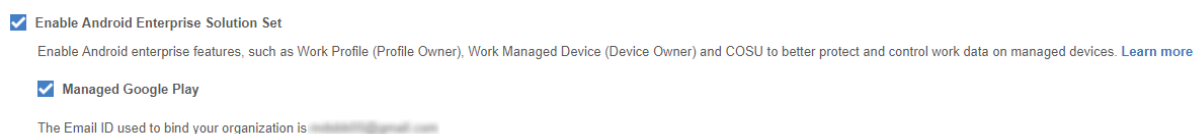
*Note: If a file access message appears, delete the file, and re-save the file.*

## 2.2.2 Android Enterprise Configuration

A Google account was used to provision Android Enterprise on the mobile devices. A managed domain can be used, but in this use case it was not necessary. A managed domain is necessary only if the corporation already has data stored in Google's cloud.

1. Create a Google account if you do not have one you wish to bind with.
2. From the MaaS360 portal, navigate to **Setup > Services**.
3. Click **Mobile Device Management**.
4. Check the box next to **Enable Android Enterprise Solution Set**.
5. Enter your password and click **Enable**.
6. Click **Mobile Device Management**.
7. Click the radio button next to **Enable via Managed Google Play Accounts (no G Suite)**.
8. Ensure all pop-up blockers are disabled. Click the link on the word **here**.
9. Enter your password and click **Enable**.
10. In the new page that opens, ensure you are signed into the Google account you wish to bind.
11. Click **Get started**.
12. Enter your business name and click **Next**.
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.
14. Click **Complete Registration**.
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.

**Figure 2-11 Enterprise Binding Settings Confirmation**



## 2.2.3 iOS APNs Certificate Configuration

For the iOS Apple Push Notification services (APNs) certificate configuration, the build team followed the [IBM documentation](#).

## 2.2.4 Apple User Enrollment (UE) Configuration

The following sections detail the configuration process for Apple User Enrollment, which enables BYOD on iOS devices.

### 2.2.4.1 Apple Business Manager (ABM) Configuration

1. In MaaS360, navigate to **Setup > Settings > Enrollment Programs**, and click **Configure** next to *Apple Device Enrollment Program*.
2. In the popup, click **Continue**.
3. Click **Tokens > Add Token**.
4. In the popup, give the token a name and click on the **here** link in step 2 of the popup to download the public key file.

Figure 2-12 Where to Click to Download the Public Key

Add Token

1. DEP token is provided by Apple. Create a DEP account and follow the steps in [business.apple.com](#)

2. Download the public key that is required for the process [here](#). Use this for creating a new MDM server in DEP Portal.

Token Name\*  
Helps identifying token in future

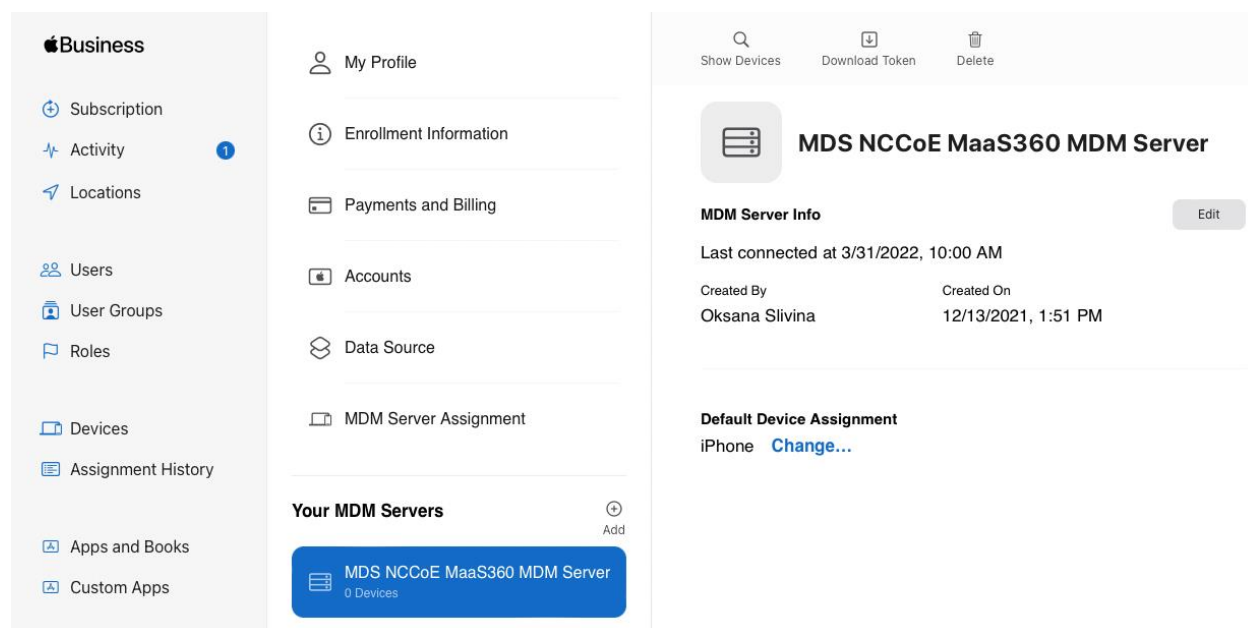
Token File.\*  
.p7m file from DEP Portal

Browse...

Cancel Add

5. In Apple Business Manager, sign in with an administrator account.
6. Click the user's name in the bottom left corner > **Settings**.
7. Click **Add** next to "Your MDM Servers" and enter a unique name for the server.
8. Upload the public key certificate file downloaded in step (4), then click **Save**.
9. Click **Download Token** to save the server token.

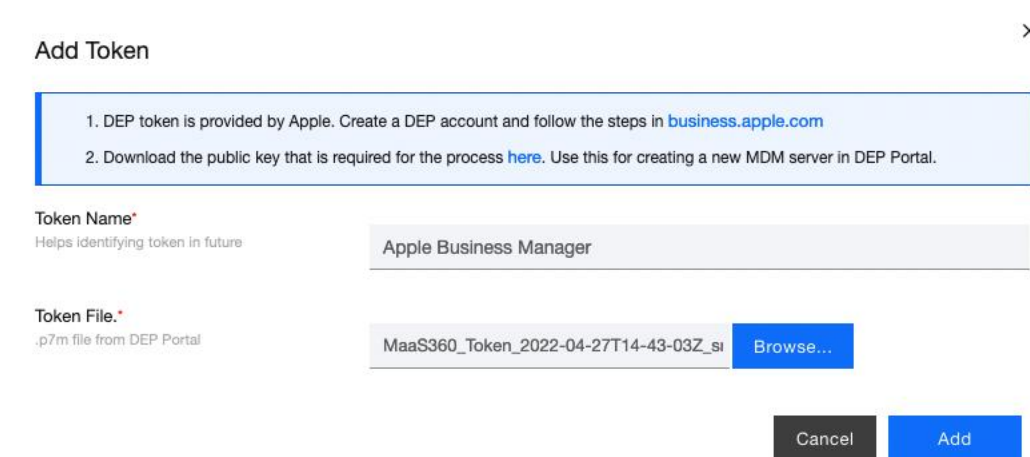
Figure 2-13 MDM configuration in Apple Business Manager



10. In MaaS360, click **Browse** and select the token downloaded in step (9).

11. Click **Add**.

Figure 2-14 Creating the DEP token



12. In Apple Business Manager, click the user's name in the bottom left corner and click **Payments and Billing**.

13. Under Server Tokens, click the token that corresponds to the Apple Business Manager tenant and save the token.

14. In MaaS360, navigate to **Apps > Catalogue**. Click **More > Apple VPP Licenses**.

15. Click **Add Token** and give the token a name. Click **Browse** and select the token file downloaded in step (13).

16. Click **Policies** and configure the VPP token policy based on organizational requirements.
17. Click **Distribution** and configure based on organizational requirements.
18. Click **Submit**.

**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 <a href="#">View</a> <a href="#">Update</a> <a href="#">Disable</a> <a href="#">More...</a>	0	United States	All Users		04/27/2022 13:15 EDT	04/26/2023 20:00 EDT	Active	NA
<div> <span> &lt;</span> <span>&lt;</span> <span>1</span> <span>&gt;</span> <span>&gt; </span> </div> <div> <a href="#">Jump To Page</a> </div> <div>             Displaying 1 - 1 of 1 Records   Show <span>25</span> Records           </div>								

### 2.2.4.2 MaaS360 Configuration

1. In the MaaS360 web portal, navigate to **Setup > Settings**.
2. Navigate to **Device Enrollment Settings > Advanced**.
3. Under *Advanced Management for Apple Devices > Select default enrollment mode for managing employee owned (BYOD) devices*, select the radio button next to **User enrollment mode**.
4. Scroll to the top of the page and click **Save**.

**Figure 2-16 iOS Enrollment Configuration**

☒ Select default enrollment mode for managing employee owned (BYOD) devices.

Applicable for self enrollment scenarios (URL: <https://m.dmv/...>)

☐ 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.

## 2.2.5 Android Configuration

The following sections detail the configuration policies applied to enrolled Android devices.

### 2.2.5.1 Policy Configuration

1. Navigate to **Security > Policies**.
2. Click the appropriate deployed Android policy.
3. Click **Edit**.
4. Navigate to **Android Enterprise Settings > Passcode**.
5. Check the box next to **Configure Passcode Policy**.
6. Configure the passcode settings based on corporate requirements.
7. Navigate to **Android Enterprise Settings > Restrictions**.
8. Check the box next to **Configure Restrictions**.

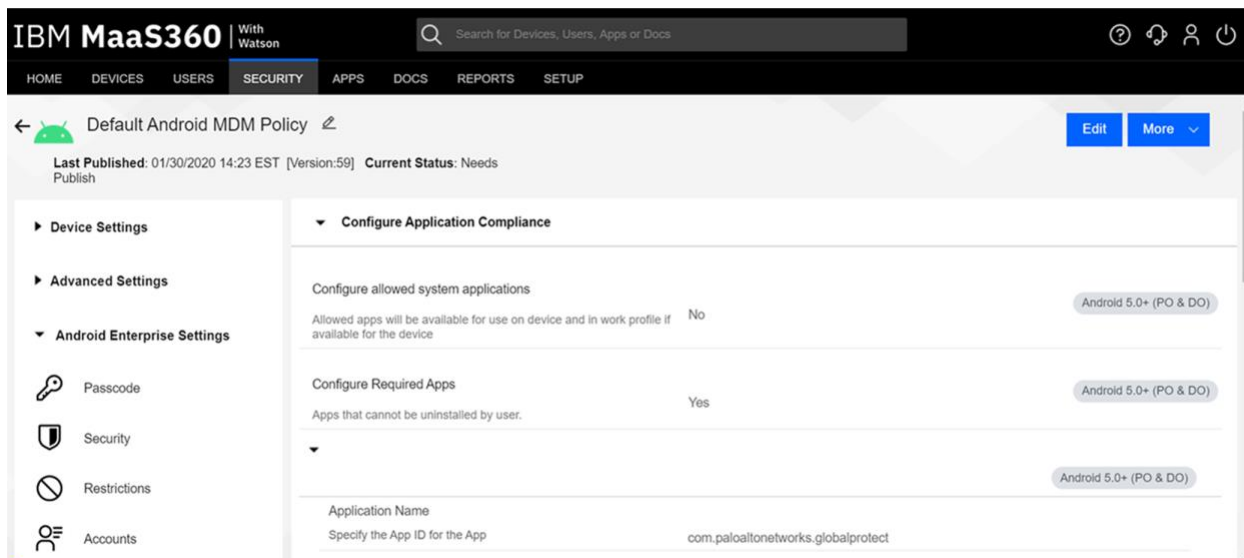
9. Configure restrictions based on corporate requirements.
10. Click **Save**.

#### 2.2.5.2 VPN Configuration

1. Navigate to **Security > Policies**.
2. Click the currently deployed Android device policy.
3. Click **Edit**.
4. Navigate to **Android Enterprise Settings > Certificates**.
5. Check the box next to **Configure CA Certificates**.
6. Click **Add New**.
7. Give the certificate a name, such as Internal Root.
8. Click **Browse** and navigate to the exported root CA certificate from earlier in the document.
9. Click **Save**.
10. Select **Internal Root** from the drop-down next to **CA Certificate**.
11. Click the + icon on the far right.
12. Repeat steps 6–10 with the internal sub-CA certificate.
13. Check the box next to **Configure Identity Certificates**.
14. From the drop-down next to Identity Certificate, select the profile that matches the name configured on the MaaS360 Cloud Extender—for this example, NDES.
15. Click **Save and Publish** and follow the prompts to publish the updated policy. Click **Apps**.
16. Click **Add > Android > Google Play App**.
17. Select the radio button next to **Add via Public Google Play Store**.
18. Search for **GlobalProtect**.
19. Select the matching result.
20. Click **I Agree** when prompted to accept the permissions.
21. Check the three boxes next to **Remove App on**.
22. Check the box next to **Instant Install**.
23. Select All Devices next to **Distribute to**.
24. Click **Add**.
25. Next to the newly added GlobalProtect application, select **More > Edit App Configurations**.

26. Click **Check for Settings**.
27. Next to **Portal**, enter the GlobalProtect portal address. In this implementation, *vpn.ent.mdse.nccoe.org* was used.
28. Next to **Username**, enter **%username%**.
29. Next to **Connection Method**, enter **user-logon**. *(Note: This will enable an always-on VPN connection for the work profile. The user will always see the VPN key icon, but it will apply only to applications contained within the work profile.)*
30. Click **Save** and follow the prompts to update the application configuration.
31. Navigate to **Security > Policies**.
32. Click the used Android policy.
33. Select **Android Enterprise Settings > App Compliance**.
34. Click **Edit**.
35. Click the + on the row below **Configure Required Apps**.
36. Enter the App Name, **GlobalProtect**.
37. Enter the App ID, **com.paloaltonetworks.globalprotect**.
38. Click **Save And Publish** and follow the prompts to publish the policy.

**Figure 2-17 Android GlobalProtect Application Compliance**



## 2.2.6 iOS Configuration

The following sections detail the configuration policies applied to enrolled iOS devices.



### 2.2.6.1 Policy Configuration

1. Navigate to **Security > Policies**.
2. Click the deployed iOS policy.
3. Click **Edit**.
4. Check the box next to **Configure Passcode Policy**.
5. Check the box next to **Enforce Passcode on Mobile Device**.
6. Configure the rest of the displayed options based on corporate requirements.
7. Click **Restrictions**.
8. Check the box next to **Configure Device Restrictions**.
9. Configure restrictions based on corporate requirements.
10. Click **Save**.

### 2.2.6.2 VPN Configuration

1. Click **Device Settings > VPN**.
2. Click **Edit**.
3. Next to **Configure for Type**, select **Custom SSL**.
4. Enter a name next to **VPN Connection Name**. In this sample implementation, **Great Seneca VPN** was used.
5. Next to **Identifier**, enter **com.paloaltonetworks.globalprotect.vpn**.
6. Next to **Host name of the VPN Server**, enter the URL of the VPN endpoint without http or https.
7. Next to **VPN User Account**, enter **%username%**.
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**.
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**.
14. In Apple Business Manager, click **Apps and Books**.
15. Search for *GlobalProtect*.

16. Select the non-legacy search result.
17. Select the business's location and enter the desired number of licenses (installations) and click **Get**.
18. In MaaS360, navigate to **Apps > Catalog**.
19. Navigate to **More > Apple VPP Licenses**.
20. In the VPP line, select **More > Sync**. Follow the confirmation pop-ups to confirm the sync with Apple Business Manager.
21. Navigate to **Apps > Catalog**.
22. Click **Add > iOS > iTunes App Store App**.
23. Search for **GlobalProtect**.
24. Select the non-Legacy version.
25. Click **Policies and Distribution**.
26. Check all three boxes next to **Remove App on**.
27. Select **All Devices** next to **Distribute to**.
28. Check the box next to **Instant Install**.
29. Click **Add**.
30. Navigate to **Security > Policies**.
31. Click the used iOS policy.
32. Click **Application Compliance**.
33. Click **Edit**.
34. Click the + next to the first row under **Configure Required Applications**.
35. Search for **GlobalProtect**.
36. Select the **non-Legacy** result.
37. Navigate to **Advanced Settings > Certificate Credentials**.
38. Check the box next to **Configure Credentials for Adding Certificates on the Device**.
39. Click **Add New**.
40. Give the certificate a name, such as Internal Root.
41. Click **Browse** and navigate to the exported root CA certificate from earlier in the document.
42. Click **Save**.

43. Select **Internal Root** from the drop-down next to **CA Certificate**.
44. Click the + icon on the far right.
45. Repeat steps 33–35 with the internal sub-CA certificate.
46. From the drop-down next to **Identity Certificate**, select the profile that matches the name configured on the MaaS360 Cloud Extender—for this example, **NDES**.
47. Click **Save And Publish** and follow the prompts to publish the policy.

## 2.3 Zimperium

Zimperium was used as a mobile threat defense service via a MaaS360 integration.

*Note: For Zimperium automatic enrollment to function properly, users **must** have an email address associated with their MaaS360 user account.*

### 2.3.1 Zimperium and MaaS360 Integration

This section assumes that IBM has provisioned an application programming interface (API) key for Zimperium within MaaS360.

1. Log in to the zConsole.
2. Navigate to **Manage > MDM**.
3. Select **Add MDM > MaaS360**.
4. Fill out the MDM URL, MDM username, MDM password, and API key.

*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>.*

5. Check the box next to **Sync users**.

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.

https://services.fiberlink.com/

**Username**  
Specify username for this MDM provider.

**Password**  
Specify password for this MDM provider.

\*\*\*\*\*

**MDM Name**  
Specify a unique name for this MDM provider.

IBM MaaS360

**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

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

### 2.3.2 Automatic Device Activation

*Note: This requires contacting Zimperium support to get required application configuration values.*

1. In Apple Business Manager, click **Apps and Books**.
2. Search for *Zimperium zIPS*.
3. Select the non-legacy search result.
4. Select the business's location and enter the desired number of licenses (installations) and click **Get**.

5. In MaaS360, navigate to **Apps > Catalog**.
6. Navigate to **More > Apple VPP Licenses**.
7. In the VPP line, select **More > Sync**. Follow the confirmation pop-ups to confirm the sync with Apple Business Manager.
8. Click **Apps** on the navigation bar.
9. Click **Add > iOS > iTunes App Store App**.
10. Search for **Zimperium zIPS**. Click the result that matches the name.
11. Click **Policies and Distribution**.
12. Check the three checkboxes next to **Remove App on**.
13. Next to **Distribute to**, select **All Devices**.
14. Click **Configuration**.
15. Set App Config Source to **Key/Value**.
16. The configuration requires three parameters: uuid, defaultchannel, and tenantid. uuid can be set to **%csn%**, but defaultchannel and tenantid must come from Zimperium support.

Figure 2-19 Zimperium zIPS iOS Configuration

MDMDeviceID	%csn%	+ -
defaultchannel		+ -
tenantid		+ -

17. Click **Add**.
18. Click **Add > Android > Google Play App**.
19. Select the radio button next to **Add via Public Google Play Store**.
20. Search for **Zimperium Mobile IPS (zIPS)**.
21. Click the matching result.
22. Click **I Agree** when prompted to accept permissions.
23. Click **Policies and Distribution**.
24. Check all three boxes next to **Remove App on**.
25. Check **Instant Install**.

26. Select **All Devices** next to **Distribute to**.
27. Click **App Configurations**.
28. Check **Configure App Settings**.
29. Enter the values provided by Zimperium next to **Default Acceptor** and **Tenant**.
30. Next to **MDM Device ID**, insert **%deviceid%**.
31. Adjust any other configuration parameters as appropriate for your deployment scenario.

**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%"/>

32. Click **Add**.

### 2.3.3 Enforce Application Compliance

From the IBM MaaS360 web portal:

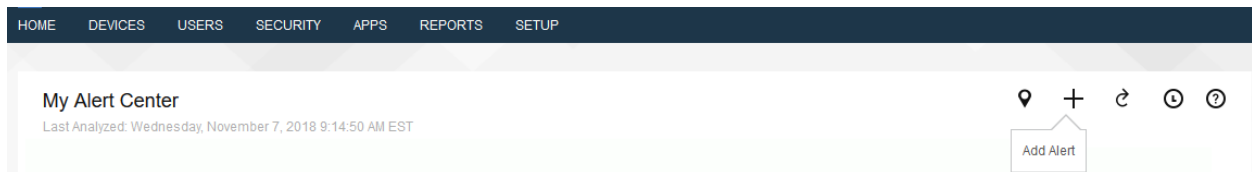
1. Navigate to **Security > Policies**.
2. Select the default Android policy.
3. Navigate to **Android Enterprise Settings > App Compliance**.
4. Click **Edit**.
5. Check the box next to **Configure Required Apps** if not checked already. If it is, click the + icon.
6. Enter **com.zimperium.zips** as the App ID.
7. Click **Save And Publish**. This will prevent the user from uninstalling zIPS once it is installed.
8. Navigate to **Security > Policies**.
9. Select the default iOS policy.

10. Click **Application Compliance**.
11. Click **Edit**.
12. Check the box next to **Configure Required Applications** if not checked already. If it is, click the **+** icon.
13. Enter **Zimperium zIPS** for the Application Name.
14. Click **Save And Publish** and follow the prompts to publish the policy.

### 2.3.4 MaaS360 Risk Posture Alerts

1. From the MaaS360 home screen, click the **+** button that says **Add Alert**.

Figure 2-21 Add Alert Button



2. Next to **Available for** select **All Administrators**.
3. For Name, enter **Zimperium Risk Posture Elevated**.
4. Under **Condition 1**, select **Custom Attributes** for the Category.
5. Select **zimperium\_risk\_posture** for Attribute.
6. Select **Equal To** for Criteria.
7. For Value, select **Elevated** for the count of risk posture elevated devices or **Critical** for risk posture critical devices.

Figure 2-22 Zimperium Risk Posture Alert Configuration

8. Click **Update**.

## 2.4 Palo Alto Networks Virtual Firewall

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

### 2.4.1 Network Configuration

1. 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).
2. Reboot the machine if cables were attached while running.
3. Navigate to **Network > Interfaces > Ethernet**.
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.
7. Once the appropriate interfaces are configured, commit the changes. The Link State icon should turn green for the configured interfaces. The commit dialogue will warn about unconfigured zones. That is an expected dialogue warning.
8. Navigate to **Network > Zones**.
9. Click **Add**. Give the zone an appropriate name, set the Type to **Layer3**, and assign it an interface.
10. Commit the changes.



11. Navigate to **Network > Virtual Routers**.
12. Click **Add**.
13. Give the router an appropriate name and add the internal and external interfaces.
14. Click **Static Routes > Add**. Give the static route an appropriate name, e.g., WAN. Set the destination to be **0.0.0.0/0**, 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.
15. (optional) Delete the default router by clicking the checkbox next to it and clicking **Delete** at the bottom of the page.
16. Commit the changes. The commit window should not display any more warnings.
17. Navigate to **Network > DNS Proxy**.
18. Click **Add**.
19. Give the proxy an appropriate name. Under **Primary**, enter the primary domain name system (DNS) IP address.
20. (optional) Enter the secondary DNS IP address.
21. Add the interfaces under **Interface**. Click **OK**.

Figure 2-23 DNS Proxy Object Configuration

**DNS Proxy**

☒ Enable

Name: Enterprise\_DNS\_Proxy

Inheritance Source: None

[Check inheritance source status](#)

Primary: 10.8.1.1

Secondary: 192.168.8.10

**Interface**

- ☐ ethernet1/1
- ☐ ethernet1/2
- ☐ ethernet1/3

[Add](#) [Delete](#)

**DNS Proxy Rules** | Static Entries | Advanced

Name	Cacheable	Domain Name	Primary	Secondary
0 items				

[Add](#) [Delete](#)

**OK** **Cancel**

22. Navigate to **Device > Services**.
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.
26. Navigate to **Objects > Addresses**.
27. For each device on the network, click **Add**. Give the device an appropriate name, enter an optional description, and enter the IP address.
28. Click **OK**.
29. Once all devices are added, commit the changes.
30. Navigate to **Policies > NAT**.
31. Click **Add**.
32. Give the network address translation rule a meaningful name, such as External Internet Access.
33. Click **Original Packet**.
34. Click **Add** and add the zone representing the intranet—in this case, **Enterprise\_Intranet**.
35. Repeat step 34 for the secure sockets layer (SSL) VPN zone.
36. Under **Source Address**, click **Add**.
37. Enter the subnet corresponding to the intranet segment.
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.

Figure 2-24 Original Packet Network Address Translation Configuration

The screenshot shows the 'NAT Policy Rule' configuration window with the 'Original Packet' tab selected. The window is divided into three main sections: 'Source Zone', 'Destination Zone', and 'Service'. The 'Source Zone' section has a list of zones with 'Any' selected. The 'Destination Zone' section has a dropdown menu with 'Enterprise\_WAN' selected. The 'Service' section has a dropdown menu with 'any' selected. The 'Translated Packet' tab is also visible, showing 'Source Address' and 'Destination Address' sections. The 'Source Address' section has a list of addresses with 'Any' selected. The 'Destination Address' section has a list of addresses with 'Any' selected. At the bottom of the window are 'OK' and 'Cancel' buttons.

## 2.4.2 Demilitarized Zone Configuration

1. Navigate to **Network > Interfaces**.
2. Click the interface that has the DMZ connection.
3. Add a comment, set the Interface Type to **Layer3**, and assign it to the virtual router created earlier.
4. Click **IPv4 > Add > New Address**. Assign it an IP block and give it a meaningful name. Click **OK**.
5. Navigate to **Network > Zones**.
6. Click **Add**. Give it a meaningful name, such as Enterprise\_DMZ.
7. Set the Type to **Layer3** and assign it the new interface that was configured—in this case, ethernet1/3.
8. Click **OK**.
9. Navigate to **Network > DNS Proxy**. Click **Add** under **Interface** and add the newly created interface. Click **OK**.
10. Commit the changes.
11. Navigate to **Network > Interfaces**, and the configured interfaces should be green.

## 2.4.3 Firewall Configuration

1. Navigate to **Policies > Security**.
2. Click **Add**.

3. Give the rule a meaningful name, such as Intranet Outbound.
4. Click **Source**. Click **Add** under **Source Zone** and set the source zone to be the internal network.
5. Click **Destination**. Click **Add** under **Destination Zone** and set the destination zone to be the WAN zone.
6. Click **Service/URL Category**. Under **Service**, click **Add**, and add **service-dns**. Do the same for service-http and service-https.
7. Click **OK**.
8. Click **Add**.
9. Click **Destination**. Add the IP address of the Simple Mail Transfer Protocol (SMTP) server.
10. Click **Application**. Click **Add**.
11. Search for **smtp**. Select it.
12. Click **OK**.
13. Commit the changes.
14. Internal hosts should now be able to communicate on the internet.

#### 2.4.4 Certificate Configuration

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

Figure 2-25 Certificate Profile

**Certificate Profile**

Name: Enterprise\_Certificate\_Profile

Username Field: Subject (dropdown) | common-name

User Domain: enterprise

Name	Default OSCP URL	OCSP Verify Certificate
<input type="checkbox"/> Internal Root		
<input type="checkbox"/> Internal Sub		

+ Add - Delete

Default OSCP URL (must start with http:// or https://)

☐ 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

## 2.4.5 Website Filtering Configuration

The following sections detail the configuration of website blocking on the Palo Alto firewall.

### 2.4.5.1 Configure Basic Website Blocking

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

Figure 2-26 Custom URL Category

Custom URL Category

Name: Blocked Websites

Description:

2 items

Sites
<input type="checkbox"/> *.example.com
<input type="checkbox"/> 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 Cancel

5. Click **OK**.
6. Navigate to **Objects > URL Filtering**.
7. Click **Add**.
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.

Figure 2-27 URL Filtering Profile

URL Filtering Profile

Name: Block\_List

Description:

Categories | Overrides | URL Filtering Settings | User Credential Detection | HTTP Header Insertion

67 items

Category	Site Access	User Credential Submission
<input type="checkbox"/> unknowns and intimate apparel	allow	allow
<input type="checkbox"/> training-and-tools	allow	allow
<input type="checkbox"/> translation	allow	allow
<input type="checkbox"/> travel	allow	allow
<input type="checkbox"/> unknown	allow	allow
<input type="checkbox"/> weapons	block	block
<input type="checkbox"/> web-advertisements	allow	allow
<input type="checkbox"/> web-based-email	allow	allow
<input type="checkbox"/> web-hosting	allow	allow
<input type="checkbox"/> Block List *	block	block

\* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

OK Cancel

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

Figure 2-28 URL Filtering Security Policy

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow' and 'Send ICMP Unreachable' unchecked. The 'Profile Setting' section lists various security features: 'Antivirus' (None), 'Vulnerability Protection' (None), 'Anti-Spyware' (None), 'URL Filtering' (Block\_List), 'File Blocking' (None), 'Data Filtering' (None), and 'WildFire Analysis' (None). The 'Log Setting' section has 'Log at Session Start' and 'Log at Session End' unchecked, and 'Log Forwarding' set to 'None'. The 'Other Settings' section has 'Schedule' (None), 'QoS Marking' (None), and 'Disable Server Response Inspection' unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

17. Click **OK**.
18. Repeat steps 13–17 for any policies that need the filtering profile applied.
19. Commit the changes.

#### 2.4.5.2 Configure SSL Website Blocking

*Note: This section is optional. [Section 2.4.5.1](#) 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.*

1. Navigate to **Device > Certificates**.
2. Click **Generate** on the bottom of the page.
3. Give the root certificate a name, such as SSL Decryption Root; and a common name (CN) such as PA Root.
4. Check the box next to **Certificate Authority**.



Figure 2-29 Generating the Root CA

The screenshot shows a 'Generate Certificate' window with the following fields and settings:

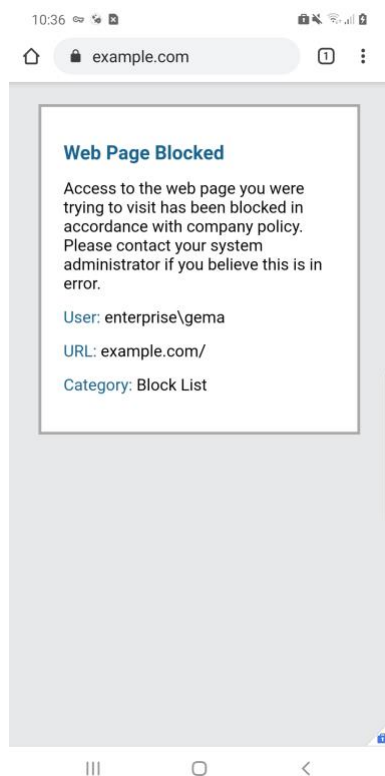
- Certificate Type:** Local (selected), SCEP
- Certificate Name:** SSL Decryption Root
- Common Name:** PA Root (with a note: IP or FQDN to appear on the certificate)
- Signed By:** (empty dropdown)
- Certificate Authority:** ☒ (checked)
- OCSP Responder:** (empty dropdown)
- Cryptographic Settings:**
  - Algorithm:** RSA
  - Number of Bits:** 2048
  - Digest:** sha256
  - Expiration (days):** 365
- Certificate Attributes:** A table with columns 'Type' and 'Value', currently empty, with 'Add' and 'Delete' buttons below it.

At the bottom are 'Generate' and 'Cancel' buttons.

5. Click **Generate**.
6. Click **Generate** at the bottom of the page.
7. Give the certificate a name, such as SSL Decryption Intermediate.
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.
10. Check the box next to **Certificate Authority**.
11. Click **Generate**.
12. Click the newly created certificate.
13. Check the boxes next to **Forward Trust Certificate** and **Forward Untrust Certificate**.
14. Click **OK**.
15. Navigate to **Policies > Decryption**.
16. Click **Add**.
17. Give the policy a name and description.

18. Click **Source**.
19. Under **Source Zone**, click **Add**.
20. Select the source zone(s) that matches the security policy that uses URL filtering. In this implementation, the Intranet and SSL VPN zones were selected.
21. Click **Destination**.
22. Under **Destination Zone**, click **Add**.
23. Select the destination zone that matches the security policy that uses URL filtering. Most likely it is the WAN zone.
24. Click **Service/URL Category**.
25. Under **URL Category**, click **Add**.
26. Select the created block list. This ensures that only sites matching the block list are decrypted.
27. Click **Options**.
28. Next to **Action**, select **Decrypt**.
29. Next to **Type**, select **SSL Forward Proxy**.
30. Next to **Decryption Profile**, select **None**.
31. Click **OK**.
32. Commit the changes.

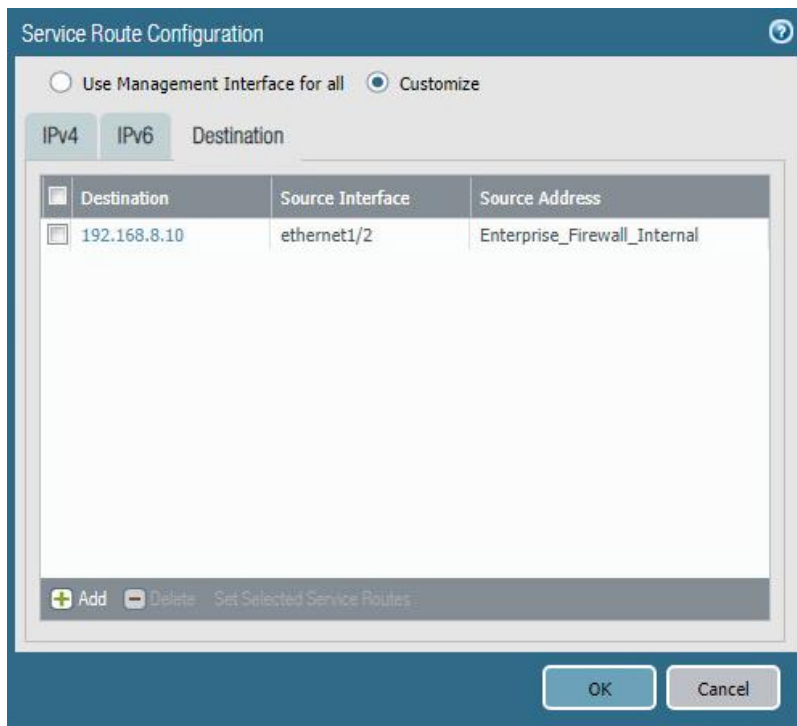
Figure 2-30 Blocked Website Notification



## 2.4.6 User Authentication Configuration

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

Figure 2-31 Service Route Configuration



8. Navigate to **Device > Server Profiles > LDAP**.
9. Click **Add**.
10. Give the profile a meaningful name, such as Enterprise\_LDAP\_Server.
11. Click **Add** in the server list. Enter the name for the server and the IP.
12. Under **Server Settings**, set the **Type** drop-down 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.*

14. Ensure that **Require SSL/TLS secured connection** is checked.
15. Click the **down arrow** next to **Base DN**. If the connection is successful, the Base DN (Distinguished Name) should display.
16. Click **OK**.

Figure 2-32 LDAP Server Profile

LDAP Server Profile

Profile Name: Enterprise\_LDAP

☐ Administrator Use Only

**Server List**

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: active-directory

Base DN: DC=enterprise,DC=mds,DC=local

Bind DN: palo-auth@enterprise.mds.local

Password: .....

Confirm Password: .....

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

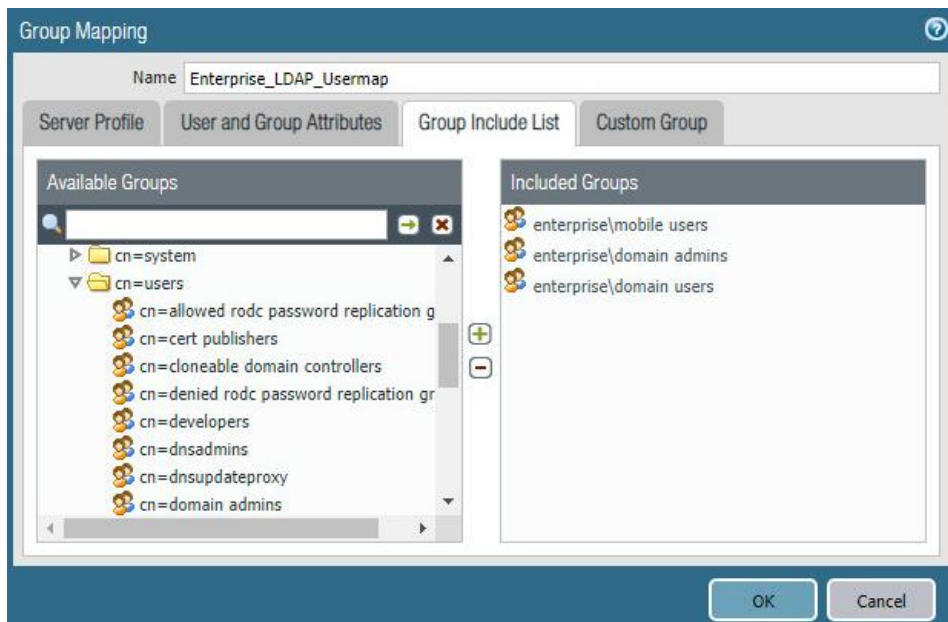
☒ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

OK Cancel

17. Navigate to **Device > User Identification > Group Mapping Settings**.
18. Click **Add**.
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.
21. Click **Group Include List**.
22. Expand the arrow next to the **base DN** and then again next to **cn=users**.
23. For each group that should be allowed to connect to the VPN, click the proper **entry** and then the **+ button**. In this example implementation, mobile users, domain users, and domain admins were used.

Figure 2-33 LDAP Group Mapping



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

Figure 2-34 LDAP User Authentication Profile

Authentication Profile

Name: Enterprise\_Auth

Authentication Factors Advanced

Type: LDAP

Server Profile: Enterprise\_LDAP

Login Attribute: sAMAccountName

Password Expiry Warning: 7  
Number of days prior to warning a user about password expiry.

User Domain: enterprise

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field X Import


OK Cancel

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

2.4.7 VPN Configuration

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

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

- 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.

Figure 2-36 SSL VPN Tunnel Interface Configuration

The screenshot shows the 'Tunnel Interface' configuration window. The 'Interface Name' is 'tunnel', the 'Comment' is 'SSL VPN', and the 'Netflow Profile' is 'None'. The 'Config' tab is selected, showing the 'Assign Interface To' section. The 'Virtual Router' is set to 'Enterprise\_Main\_Router' and the 'Security Zone' is set to 'Enterprise\_VPN'. The 'OK' and 'Cancel' buttons are at the bottom right.

7. Commit the changes.
8. Navigate to **Policies > Authentication**.
9. Click **Add**.
10. Give the policy a **descriptive name**. For this example, the rule was named VPN\_Auth.
11. Click **Source**.
12. Click **Add** and add the VPN and WAN zones.
13. Click **Destination**.
14. Check the **Any** box above **Destination Zone**.
15. Click **Service/URL Category**.
16. Click **Add** under **Service** and add **service-https**.
17. Click **Actions**.
18. Next to **Authentication Enforcement**, select **default-web-form**.
19. Click **OK**.

#### 2.4.7.1 Configure the GlobalProtect Gateway

1. Navigate to **Network > GlobalProtect > Gateways**.
2. Click **Add**.
3. Give the gateway a meaningful name. For this implementation, the name Enterprise\_VPN\_Gateway was used.



4. Under **Interface**, select the **WAN Ethernet interface**.
5. Ensure that **IPv4 Only** is selected next to **IP Address Type**.
6. Select the **WAN IP of the firewall** next to **IPv4 Address**. Ensure that end clients can resolve it.
7. Click **Authentication**.
8. Select the created **SSL/TLS service profile** next to **SSL/TLS Service Profile**.
9. Click **Add** under **Client Authentication**.
10. Give the object a meaningful name, such as iOS Auth.
11. Next to **OS**, select **iOS**.
12. Next to **Authentication Profile**, select the **created Authentication Profile**.
13. Next to **Allow Authentication with User Credentials OR Client Certificate**, select **Yes**.

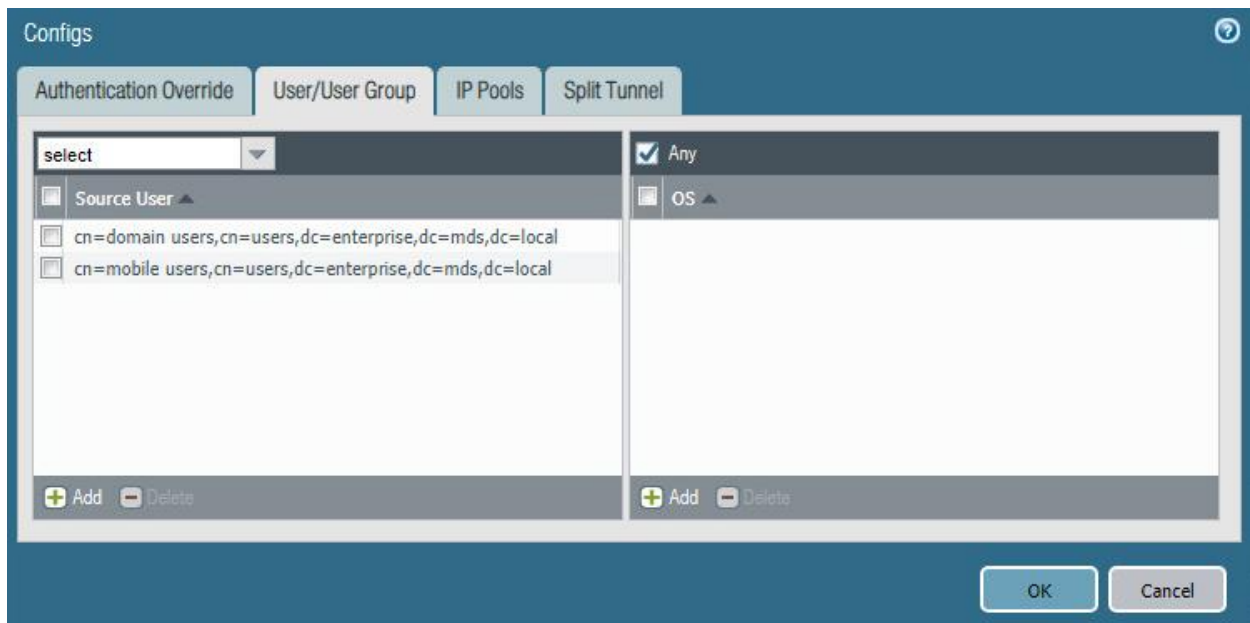
Figure 2-37 GlobalProtect iOS Authentication Profile

The screenshot shows the 'Client Authentication' configuration window for a GlobalProtect iOS Authentication Profile. The window has a title bar 'Client Authentication' with a help icon. The main content area is divided into sections. The first section contains three fields: 'Name' with the value 'iOS Auth', 'OS' with a dropdown menu showing 'iOS', and 'Authentication Profile' with a dropdown menu showing 'Enterprise\_Auth'. Below this is a section titled 'GlobalProtect App Login Screen' which contains three fields: 'Username Label' with the value 'Username', 'Password Label' with the value 'Password', and 'Authentication Message' with the value 'Enter login credentials'. A note below the message field states 'Authentication message can be up to 256 characters.' At the bottom of the main content area is a field for 'Allow Authentication with User Credentials OR Client Certificate' with a dropdown menu showing 'Yes (User Credentials OR Client Certificate Required)'. A note below this field states 'To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.' At the bottom right of the window are two buttons: 'OK' and 'Cancel'.

14. Click **OK**.
15. Click **Add** under **Client Authentication**.
16. Give the object a meaningful name, such as Android Auth.
17. Next to **OS**, select **Android**.
18. Next to **Authentication Profile**, select the **created Authentication Profile**.
19. Next to **Allow Authentication with User Credentials OR Client Certificate**, select **No**.
20. Click **Agent**.
21. Check the box next to **Tunnel Mode**.

22. Select the **created tunnel interface** next to **Tunnel Interface**.
23. Uncheck **Enable IPSec**.
24. Click **Timeout Settings**.
25. Set **Disconnect On Idle** to an organization defined time.
26. Click **Client IP Pool**.
27. Click **Add** and assign an IP subnet to the clients—in this case, **10.3.3.0/24**.
28. Click **Client Settings**.
29. Click **Add**.
30. Give the config a meaningful name, such as **Enterprise\_Remote\_Access**.
31. Click **User/User Group**.
32. Click **Add** under **Source User**.
33. Enter the **LDAP information** of the group allowed to use this rule. In this example, implementation, domain users, and mobile users were used.

**Figure 2-38 LDAP Authentication Group Configuration**



34. Click **Split Tunnel**.
35. Click **Add** under **Include**.
36. Enter **0.0.0.0/0** to enable full tunneling.
37. Click **OK**.

38. Click **Network Services**.
39. Set **Primary DNS** to be the internal domain controller/DNS server—in this case, **192.168.8.10**.
40. Click **OK**.
41. Navigate to **Network > Zones**.
42. Click the created **VPN zone**.
43. Check the box next to **Enable User Identification**.

**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. The 'Zone Protection' section shows 'Zone Protection Profile' as 'None' and 'Enable Packet Buffer Protection' as unchecked. The 'User Identification ACL' section has 'Enable User Identification' checked. It contains two lists: 'Include List' and 'Exclude List', both with instructions to 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24'. Each list has 'Add' and 'Delete' buttons. At the bottom are 'OK' and 'Cancel' buttons.

44. Click **OK**.
45. Commit the changes.

#### 2.4.7.2 Configure the GlobalProtect Portal

1. Navigate to **Network > GlobalProtect > Portals**.
2. Click **Add**.
3. Give the profile a meaningful name, such as **Enterprise\_VPN\_Portal**.

4. For Interface, assign it the firewall's **WAN interface**.
5. Set IP Address Type to **IPv4 Only**.
6. Set the IPv4 address to the firewall's **WAN address**.
7. Set all three appearance options to be **factory-default**.

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

GlobalProtect Portal Configuration

**General** | Authentication | Agent | Clientless VPN | Satellite

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

OK Cancel

8. Click **Authentication**.
9. Select the **created SSL/TLS service profile**.
10. Click **Add** under **Client Authentication**.
11. Give the profile a meaningful name, such as Enterprise\_Auth.
12. Select the created **authentication profile** next to **Authentication Profile**.
13. Click **OK**.

Figure 2-41 GlobalProtect Portal Authentication Configuration

The image shows the 'GlobalProtect Portal Configuration' window with the 'Agent' tab selected. The 'Server Authentication' section has 'SSL/TLS Service Profile' set to 'GlobalProtect\_Endpoint'. The 'Client Authentication' section contains a table with one entry: 'Enterprise\_Auth' for 'Any' OS, using 'Enterprise\_Auth' profile, with 'Username' and 'Password' labels, and the message 'Enter login credentials'. Below the table are buttons for 'Add', 'Delete', 'Clone', 'Move Up', and 'Move Down'. The 'Certificate Profile' is set to 'Enterprise\_Certificate\_Profile'. 'OK' and 'Cancel' buttons are at the bottom right.

	Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message
<input checked="" type="checkbox"/>	Enterprise_Auth	Any	Enterprise_Auth	Username	Password	Enter login credentials

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

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

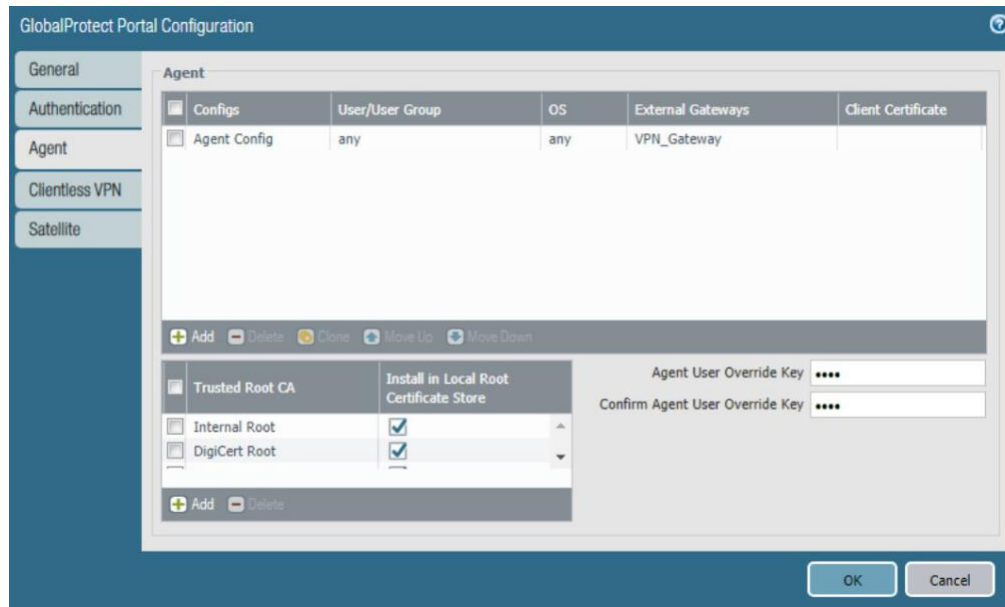
Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

OK Cancel

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

31. Click **Add** again. Select the **root certificate** used for SSL URL filtering, created in a previous section.
32. Check the box next to **Install in Local Root Certificate Store** for all three certificates.

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

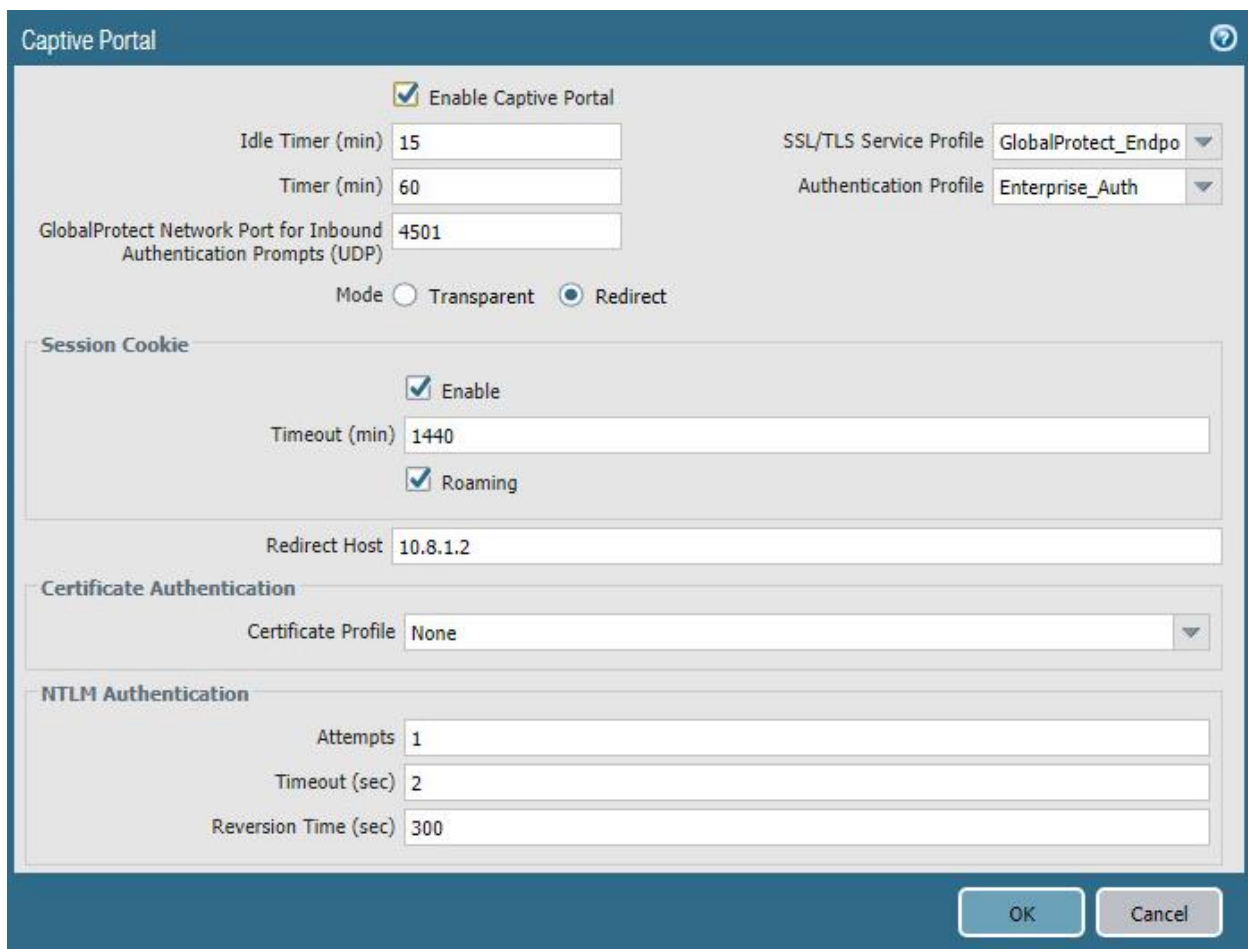


33. Click **OK**.

#### **2.4.7.3 Activate Captive Portal**

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

Figure 2-44 Captive Portal Configuration



The image shows a 'Captive Portal' configuration window. At the top, there's a title bar with a question mark icon. The main area is divided into several sections. The first section has a checkbox 'Enable Captive Portal' which is checked. Below it are three input fields: 'Idle Timer (min)' with value 15, 'Timer (min)' with value 60, and 'GlobalProtect Network Port for Inbound Authentication Prompts (UDP)' with value 4501. To the right of these are two dropdown menus: 'SSL/TLS Service Profile' set to 'GlobalProtect\_Endpo' and 'Authentication Profile' set to 'Enterprise\_Auth'. Below these is a 'Mode' section with two radio buttons: 'Transparent' and 'Redirect', with 'Redirect' being selected. The next section is 'Session Cookie', which has a checked 'Enable' checkbox, a 'Timeout (min)' field with value 1440, and a checked 'Roaming' checkbox. Below this is a 'Redirect Host' field with value 10.8.1.2. The 'Certificate Authentication' section has a 'Certificate Profile' dropdown set to 'None'. The 'NTLM Authentication' section has three input fields: 'Attempts' with value 1, 'Timeout (sec)' with value 2, and 'Reversion Time (sec)' with value 300. At the bottom right are 'OK' and 'Cancel' buttons.

Captive Portal

☒ Enable Captive Portal

Idle Timer (min) 15

Timer (min) 60

GlobalProtect Network Port for Inbound Authentication Prompts (UDP) 4501

SSL/TLS Service Profile GlobalProtect\_Endpo

Authentication Profile Enterprise\_Auth

Mode ☐ Transparent ☒ Redirect

Session Cookie

☒ Enable

Timeout (min) 1440

☒ Roaming

Redirect Host 10.8.1.2

Certificate Authentication

Certificate Profile None

NTLM Authentication

Attempts 1

Timeout (sec) 2

Reversion Time (sec) 300

OK Cancel

6. Click **OK**.
7. Commit the changes.

#### 2.4.7.4 Activate the GlobalProtect Client

1. Navigate to **Device > GlobalProtect Client**.
2. Acknowledge pop up messages.
3. Click **Check Now** at the bottom of the page.
4. Click **Download** next to the **first release** that comes up. In this implementation, version 5.0.2atewas used.
5. Click **Activate** next to the **downloaded release**.
6. Navigate to the FQDN of the VPN. You should see the Palo Alto Networks logo and the GlobalProtect portal login prompt, potentially with a message indicating that a required certificate cannot be found. This is expected on desktops because there is nothing in place to seamlessly deploy client certificates.



Figure 2-45 GlobalProtect Portal



*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.*

2.4.8 Enable Automatic Application and Threat Updates

- 1. In the **PAN-OS portal**, navigate to **Device > Dynamic Updates**.
- 2. Install the latest updates.
  - 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.
  - c. When the download completes click **Close**.

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

- d. Click **Install** on the first row.

- e. Click **Continue Installation**, leaving the displayed box unchecked. Installation will take a few minutes.
  - f. When the installation completes click **Close**.
3. Enable automatic threat updates. (*Note: Automatic threat updates are performed in the background and do not require a reboot of the appliance.*)
  - a. At the top of the page, next to **Schedule**, click the hyperlink with the date and time, as shown in Figure 2-47.

**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)

- b. Select the **desired recurrence**. For this implementation, weekly was used.
  - c. Select the **desired day and time** for the update to occur. For this implementation, Saturday at 23:45 was used.
  - d. Next to **Action**, select **download-and-install**.

**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

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

## 2.5 Kryptowire

Kryptowire was used as an application vetting service via a custom active directory-integrated web application.

### 2.5.1 Kryptowire and MaaS360 Integration

1. Contact IBM support to provision API credentials for Kryptowire.
2. Contact Kryptowire support to enable the MaaS360 integration, including the MaaS360 API credentials.
3. 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**.
4. Set the **Threat Score Threshold** to the desired amount. In this sample implementation, 75 was used.
5. Enter an **email address** where email alerts should be delivered.
6. Click **Save Settings**. Kryptowire will now send an email to the email address configured in step 5 when an analyzed application is at or above the configured alert threshold.

## Appendix A List of Acronyms

<b>ABM</b>	Apple Business Manager
<b>AD</b>	Active Directory
<b>API</b>	Application Programming Interface
<b>APN</b>	Apple Push Notification
<b>BYOD</b>	Bring Your Own Device
<b>CA</b>	Certificate Authority
<b>CN</b>	Common Name
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>DC</b>	Domain Controller
<b>DMZ</b>	Demilitarized Zone
<b>DN</b>	Distinguished Name
<b>DNS</b>	Domain Name System
<b>EMM</b>	Enterprise Mobility Management
<b>FQDN</b>	Fully Qualified Domain Name
<b>HKEY</b>	Handle to Registry Key
<b>HKLM</b>	HKEY_LOCAL_MACHINE
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>IBM</b>	International Business Machines
<b>ID</b>	Identification
<b>IIS</b>	Internet Information Services
<b>IP</b>	Internet Protocol
<b>IPSec</b>	Internet Protocol Security
<b>IPv4</b>	Internet Protocol version 4
<b>IT</b>	Information Technology
<b>ITL</b>	Information Technology Laboratory
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MDM</b>	Mobile Device Management

<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NDES</b>	Network Device Enrollment Service
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>PII</b>	Personally Identifiable Information
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>SCEP</b>	Simple Certificate Enrollment Protocol
<b>SMTP</b>	Simple Mail Transport Protocol
<b>SP</b>	Special Publication
<b>SSID</b>	Service Set Identifier
<b>SSL</b>	Secure Sockets Layer
<b>TLS</b>	Transport Layer Security
<b>UE</b>	User Enrollment
<b>URL</b>	Uniform Resource Locator
<b>UUID</b>	Universally Unique Identifier
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide Area Network
<b>zIPS</b>	Zimperium Mobile IPS

## Appendix B Glossary

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

## Appendix C    References

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

## Appendix D Example Solution Lab Build Testing Details

This section shows the test activities performed to demonstrate how this practice guide's example solution that was built in the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) lab addresses the threat events and privacy risks defined from the risk assessment found in Volume B, Section 3.4.

### D.1 Threat Event 1 – Unauthorized Access to Sensitive Information Via a Malicious or Intrusive Application Practices

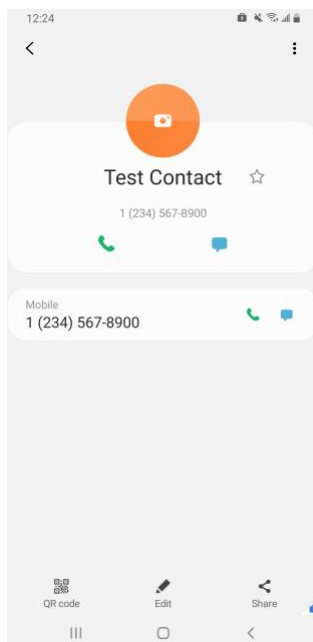
**Summary:** Unauthorized access to work information via a malicious or privacy-intrusive application.

**Test Activity:** Place mock enterprise contacts on devices, then attempt to install and use unmanaged applications that access and back up those entries.

**Desired Outcome:** Built-in device mechanisms such as Apple User Enrollment functionality and Google's Android Enterprise work profile functionality are used to separate the contact and calendar entries associated with enterprise email accounts so that they can only be accessed by enterprise applications (applications that the enterprise mobility management (EMM) authorizes and manages), not by applications manually installed by the user.

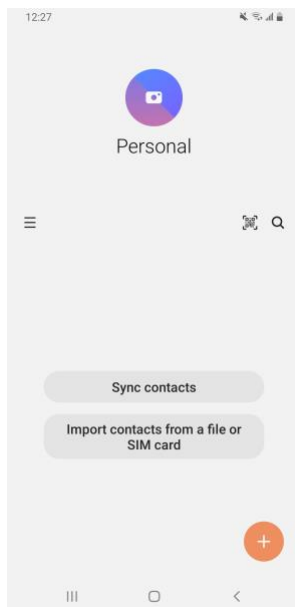
**Observed Outcome:** Since the test application was unmanaged, it was unable to access the enterprise contacts and calendar entries. This is due to Android Enterprise and Apple User Enrollment providing data separation and isolation capabilities between the personal and work profiles. The observed outcomes are shown in Figure D-1 and [Figure D-2](#), which show how a contact created in a work profile cannot be seen by a personal profile. In addition, [Figure D-3](#) and [Figure D-4](#) show how a contact created in a managed application cannot be seen by an unmanaged application.

**Figure D-1 Contact Created in Work Profile**





**Figure D-2 Personal Profile Can't See Work Contacts**



**Figure D-3 Contact Created in Managed App**

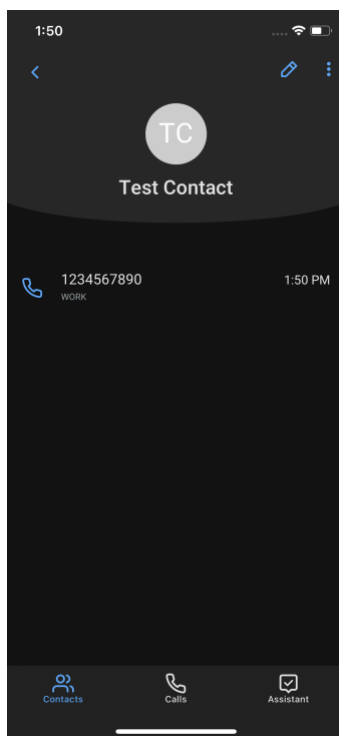
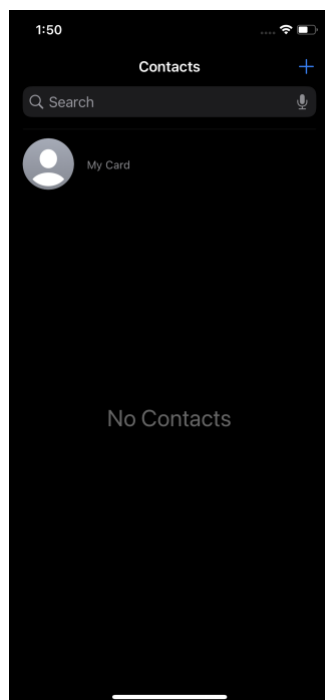


Figure D-4 Unmanaged App Can't See Managed Contacts



## D.2 Threat Event 2 – Theft of Credentials Through a Short Message Service or Email Phishing Campaign

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

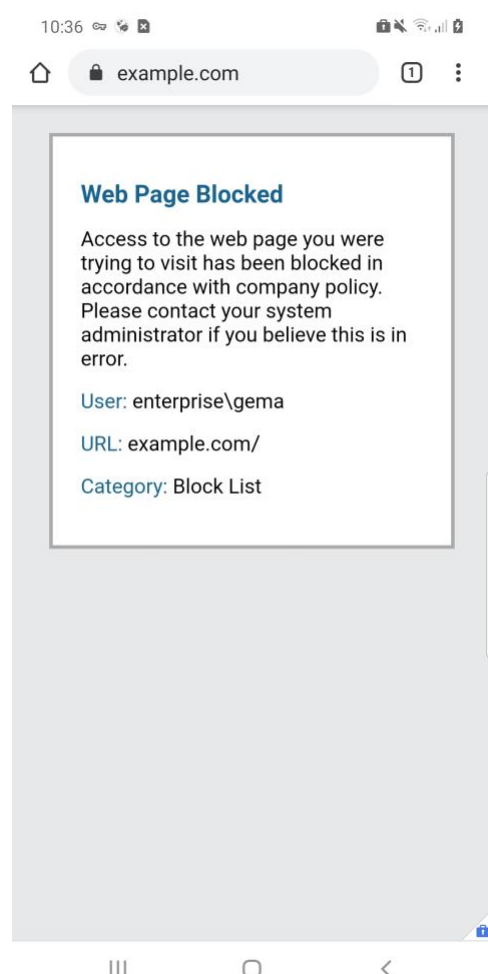
**Test Activity:**

- This threat event can be tested by establishing a web page with a form that impersonates an enterprise login prompt.
- The web page's uniform resource locator (URL) is then sent via email and there is an attempt to collect and use enterprise login credentials.

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

**Observed Outcome:** The example solution used Palo Alto Networks' next-generation firewall. The firewall includes PAN-DB, a URL filtering service that automatically blocks known malicious URLs. The URL filtering database is updated regularly to help protect users from malicious URLs. The next-generation firewall blocked the attempt to visit the phishing site when accessing it from within the work profile. However, if the malicious URL were not present in PAN-DB, or the URL was accessed in the personal profile of the device, the user would be allowed to access the website. Figure D-5 shows the observed outcome of the phishing webpage being blocked from within the work profile.

Figure D-5 Fictitious Phishing Webpage Blocked



### D.3 Threat Event 3 – Confidentiality and Integrity Loss Due to Exploitation of Known Vulnerability in the OS or Firmware

**Summary:** Confidentiality and integrity loss due to the exploitation of a known vulnerability in the operating system or firmware.

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

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

**Observed Outcome:** Zimperium was able to identify devices that were running an outdated version of iOS or Android, and it informed MaaS360 when a device was out of compliance. Once MaaS360 alerted the user, they had a pre-configured amount of time to remediate the risk before work data was

removed from the device, leaving the personal data unaffected. Figure D-6 and [Figure D-7](#) show the security architecture identifying the presence of outdated operating systems.

**Figure D-6 iOS MaaS360 OS Compliance Alert**

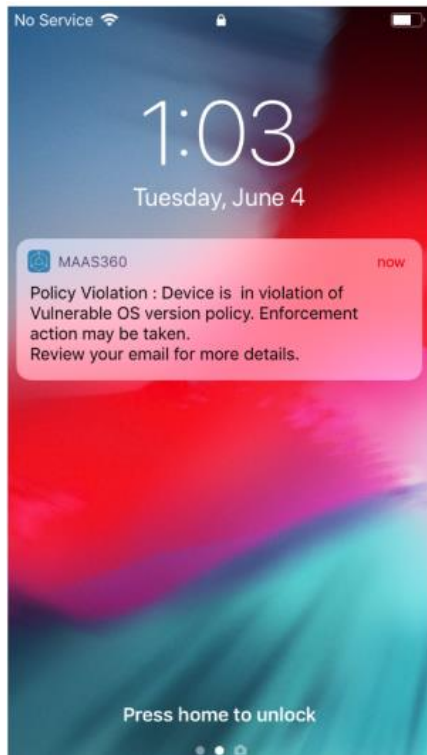
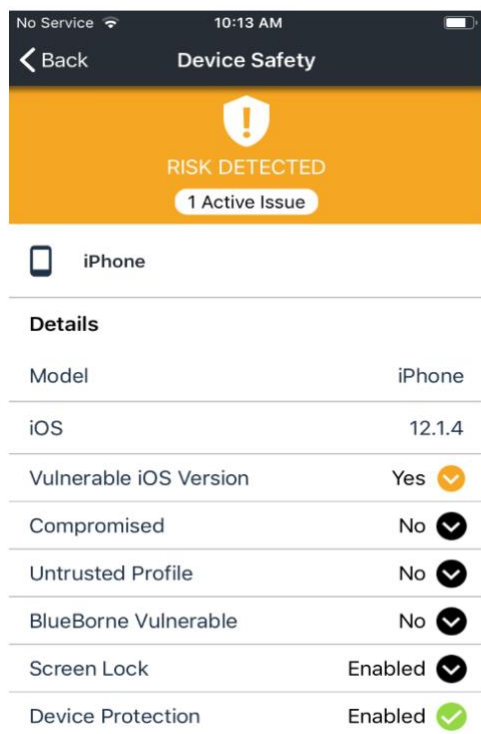


Figure D-7 Zimperium Risk Detected



## D.4 Threat Event 4 – Loss of Confidentiality of Sensitive Information Via Eavesdropping on Unencrypted Device Communications

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

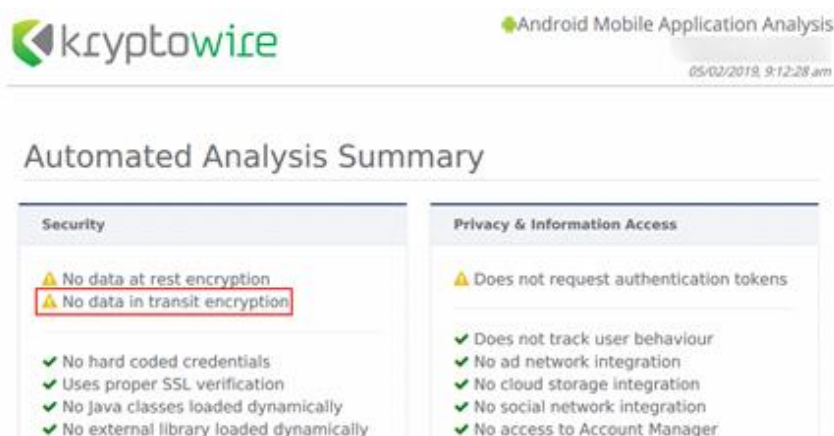
**Test Activity:** Test if applications will attempt to establish a hypertext transfer protocol or unencrypted connection.

### Desired Outcome:

- 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.

**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 D-8 shows the analysis summary finding of no in transit data encryption in use.

Figure D-8 Kryptowire Application Report



## D.5 Threat Event 5 – Compromise of Device Integrity Via Observed, Inferred, or Brute-Forced Device Unlock Code

**Summary:** Compromise of device integrity via observed, inferred, or brute-forced device unlock code.

**Test Activity:**

- Attempt to completely remove the device unlock code. Observe whether the attempt succeeds.
- Attempt to set the device unlock code to “1234,” a weak four-digit personal identification number (PIN). Observe whether the attempt succeeds.

**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 for the device unlock code. The VPN (GlobalProtect) should require periodic re-authentication with multi-factor authentication to prevent devices with a bypassed lock screen from accessing on-premises enterprise resources.

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

**Observed Outcome:** MaaS360 applies a policy to the devices to enforce a mandatory PIN, Zimperium reports devices with a disabled lock screen, and GlobalProtect requires periodic re-authentication using MFA. [Figure D-9](#) through [Figure D-11](#) show the passcode and lock screen configuration settings.

Figure D-9 Android Passcode Configuration

Default Android MDM Policy [🔗](#)  
 Last Published: 05/09/2022 11:43 EDT [Version:64] Current Status: Published Cancel More ▾

Device Settings

Advanced Settings

Android Enterprise Settings

**Passcode**

Security

Restrictions

Accounts

App Compliance

ActiveSync

Passcode Settings

Configure Device Passcode Policy ☒ Android 5.0+ (PO & DO)

Select this option to enforce the use of a Passcode before using Android for Work.

Minimum Passcode Complexity Low ▾ Android 12.0+ (PO & DO)

Requires Android App 7.50+ for PO. Requires Android App 7.70+ for DO. Takes precedence over "Minimum Passcode Quality" and "Minimum Passcode Length" if both are configured. Unset this field to continue using deprecated settings: "Minimum Passcode Quality" and "Minimum Passcode Length"

Minimum Passcode Quality Numeric ▾ Android 5.0+ (PO & DO)

Requires Android 5.0+ and Android App 6.05+ for restricting passcode quality to Numeric Complex. Requires Android App 6.30+ for Weak Biometric, else defaults to Numeric. Android 12 onwards, this setting is deprecated and "Minimum Passcode Complexity" takes precedence over it.

Minimum Passcode Length (4-16 characters)  Android 5.0+ (PO & DO)

Android 12 onwards, this setting is deprecated and "Minimum Passcode Complexity" takes precedence over it.

Figure D-10 iOS Passcode Configuration

Default iOS MDM Policy [🔗](#)  
 Last Published: 03/28/2022 11:29 EDT [Version:192] Current Status: Published Cancel Save Save And Publish More ▾

Filter User Enrollment (UE) attributes ☒ Save your changes before you toggle

Device Settings

**Passcode**

Restrictions

ActiveSync

Wi-Fi

VPN

AirPrint

Configure Passcode Policy ☒ UE

When enabled, on user enrolled devices, Minimum Passcode Length will be 6, Allow Simple Passcode will be No and Enforce Passcode on Mobile Device will be Yes

Passcode

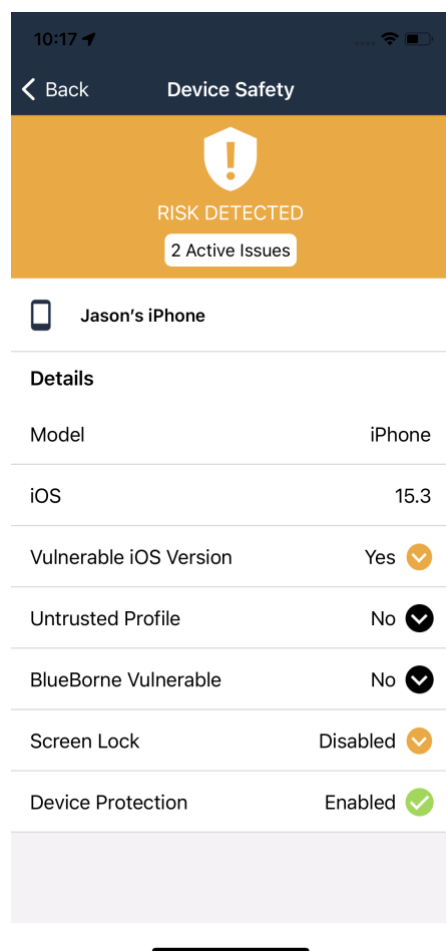
Allow Simple Passcode ☐ UE

Passcode values that are ascending, descending or repeating character sequences (e.g. 1111, 123, 654, abc, xyz).

Minimum Passcode Length 4 ▾ UE

Select a number between 4 and 16. iOS encourages to set 6 or higher.

Figure D-11 Zimperium Detecting Disabled Lock screen



## D.6 Threat Event 6 – Unauthorized Access to Backend Services Via Authentication or Credential Storage Vulnerabilities in Internally Developed Applications

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

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

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

**Observed Outcome:** Kryptowire recognized that the application uses hardcoded credentials. The application's use of hardcoded credentials could introduce vulnerabilities if unauthorized entities used the hardcoded credentials to access enterprise resources. Figure D-12 shows the discovery of hardcoded credentials.



Figure D-12 Application Report with Hardcoded Credentials



## D.7 Threat Event 7 – Unauthorized Access of Enterprise Resources From an Unmanaged and Potentially Compromised Device

**Summary:** Unauthorized access of enterprise resources from an unmanaged and potentially compromised device.

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

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

**Observed Outcome:** Devices that were not enrolled in MaaS360 were unable to access enterprise resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper client certificates—obtainable only through enrolling in the EMM. [Figure D-13](#) through [Figure D-15](#) show the desired outcome of the VPN gateway protecting the enterprise.

**Figure D-13 Attempting to Access the VPN on an Unmanaged iOS Device**

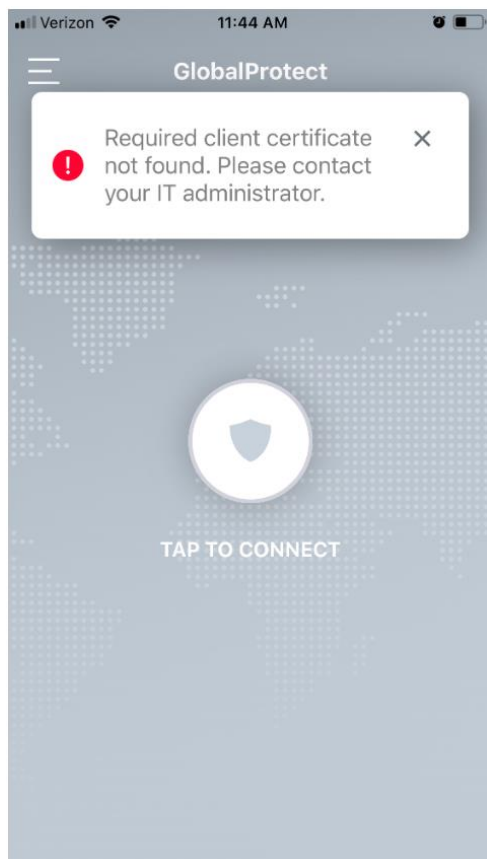


Figure D-14 Attempting to Access the VPN on an Unmanaged Android Device

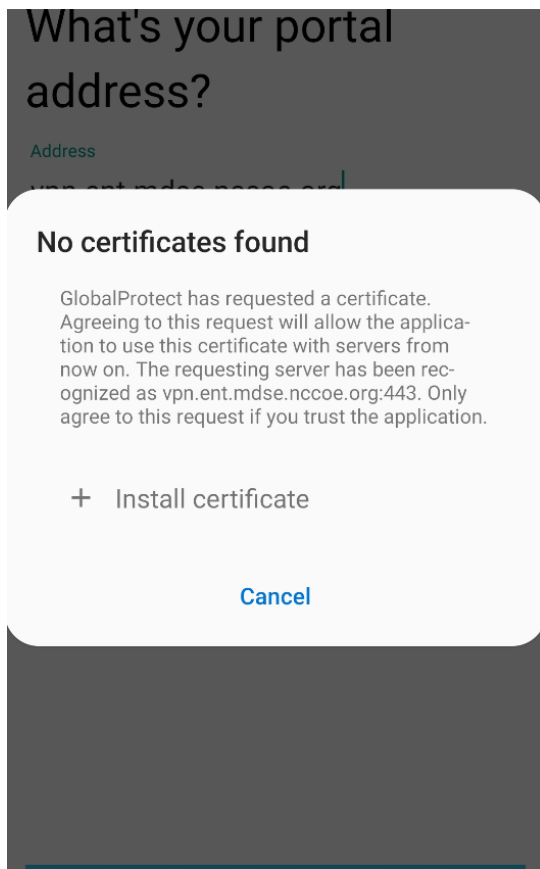
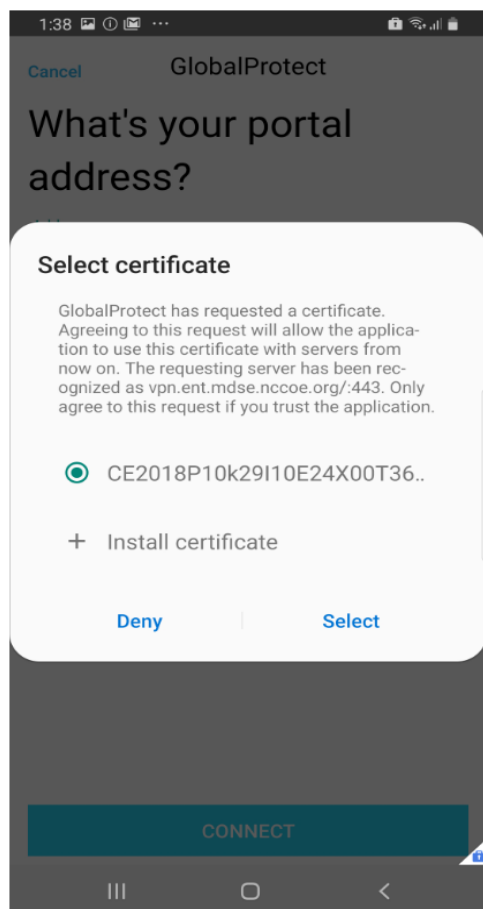


Figure D-15 Attempting to Access the VPN on a Managed Android Device



## D.8 Threat Event 8 – Loss of Organizational Data Due to a Lost or Stolen Device

**Summary:** Loss of organizational data due to a lost or stolen device.

**Test Activity:** Attempt to download enterprise data onto a mobile device that is not enrolled in the EMM system (may be performed in conjunction with TE-7). Attempt to remove (in conjunction with TE-5) the screen lock passcode or demonstrate that the device does not have a screen lock passcode in place. Attempt to locate and selectively wipe the device through the EMM console (will fail if the device is not enrolled in the EMM).

**Desired Outcome:** It should be possible to locate or wipe EMM enrolled devices in response to a report that they have been lost or stolen. As demonstrated by TE-7, only EMM enrolled devices should be able to access enterprise resources. As demonstrated by TE-5, EMM enrolled devices can be forced to have a screen lock with a passcode of appropriate strength, which helps resist exploitation (including loss of organizational data) if the device has been lost or stolen.

**Observed Outcome (Enrolled Devices):** Enrolled devices are protected. They have an enterprise policy requiring a PIN/lock screen, and therefore, the enterprise data on the device could not be accessed.

Additionally, the device could be remotely wiped after it was reported as lost to enterprise mobile device service management, ensuring no corporate data is left in the hands of attackers.

**Observed Outcome (Unenrolled Devices):** As shown in Threat Event 7, only enrolled devices could access enterprise resources. When the device attempted to access enterprise data, no connection to the enterprise services was available. Because the device cannot access the enterprise, the device would not contain enterprise information.

In both outcomes, both enrolled and unenrolled, it would be at the user’s discretion if they wanted to wipe all personal data as well. Because this is a Bring Your Own Device (BYOD) scenario, only corporate data (managed applications on iOS, and the work container on Android) would be deleted from a device if the device were lost or stolen. Figure D-16 through [Figure D-19](#) show the removal of only organization data using selective wipe features.

Figure D-16 Selective Wiping a Device

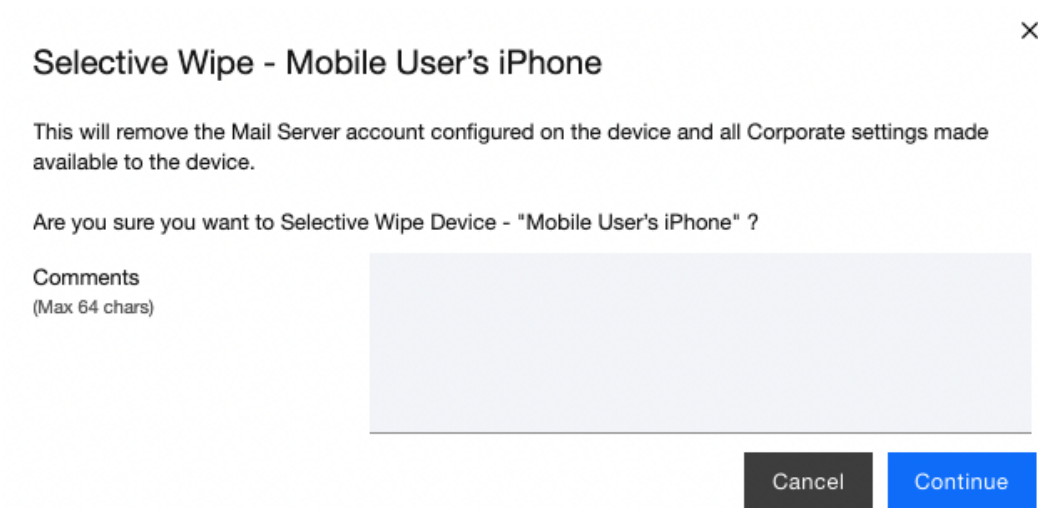


Figure D-18 Corporate Data Removal Confirmation Notification on iOS

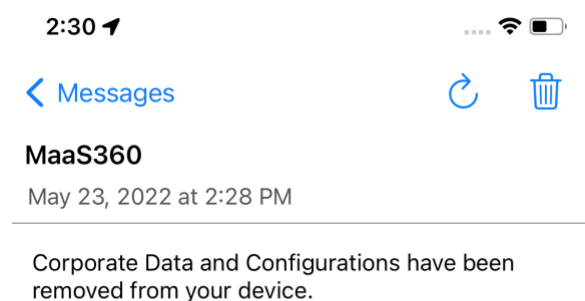
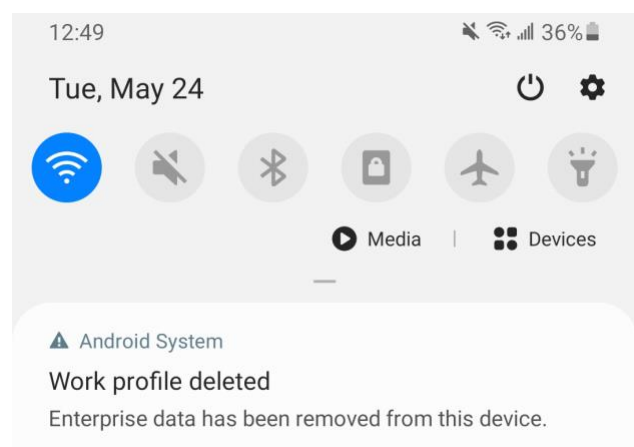


Figure D-19 Work Profile Removal Notification on Android



## D.9 Threat Event 9 – Loss of Confidentiality of Organizational Data Due to its Unauthorized Storage in Non-Organizationally Managed Services

**Summary:** Loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services.

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

**Desired Outcome:** The EMM will prohibit screenshots and other data-sharing actions while using managed applications.

**Observed Outcome:** As shown in [Figure D-20](#) through [Figure D-22](#), MaaS360 device policies prevented the following actions on BYOD managed phones:

- **Android**

- clipboard sharing
- screen capture
- share list
- backup to Google
- Secure Digital card write
- Universal Serial Bus storage
- video recording
- Bluetooth
- background data sync
- Android Beam
- Sbeam
- **iOS**
  - opening, writing, and saving from managed to unmanaged applications
  - AirDrop for managed applications
  - screen capture
  - AirPlay
  - iCloud backup
  - document, photo stream, and application sync
  - print
  - importing files

Figure D-20 iOS DLP Configuration Options

Default iOS MDM Policy

Last Published: 03/28/2022 11:29 EDT [Version:192]
 Current Status: Needs Publish

Edit More

Filter User Enrollment (UE) attributes ☒ Save your changes before you toggle

Device Settings

Passcode

**Restrictions**

ActiveSync

Wi-Fi

VPN

AirPrint

Accounts

Advanced Settings

Configure Device Restrictions

Unencrypted backups are restricted for all APNS managed devices. Yes

Select this option to configure restrictions on use of device features, application and content.

Device Functionality

Allow Open from Managed to Unmanaged apps

Allows Content to be opened from Managed to Unmanaged apps. Applies to Mail, Calendar events, Contacts and other types of content. No

Allow Open from Unmanaged to Managed Apps

Allows Content to be opened from Unmanaged to Managed apps. Applies to Mail, Calendar events, Contacts and other types of content. No

Allow AirDrop for Managed Apps

Allow AirDrop to be used with managed apps. Yes

Allow Screen Capture

Disable to prevent screenshots, and on iOS9 devices video capture. Yes



Figure D-21 Android DLP Configuration

Default Android MDM Policy [Edit](#)

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

To enable camera on device, camera app needs to be allowed in native app compliance apart from enabling this.

Yes

Android 5.0+ (PO & DO)

Allow camera on personal profile

Camera app also needs to be allowed in native app compliance apart from enabling this.

Yes

Android 11+ (WPCO)

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

Note: Disabling this feature would not allow DO enrollments on the device.

Yes

Android 5.1.1+ (PO & DO)

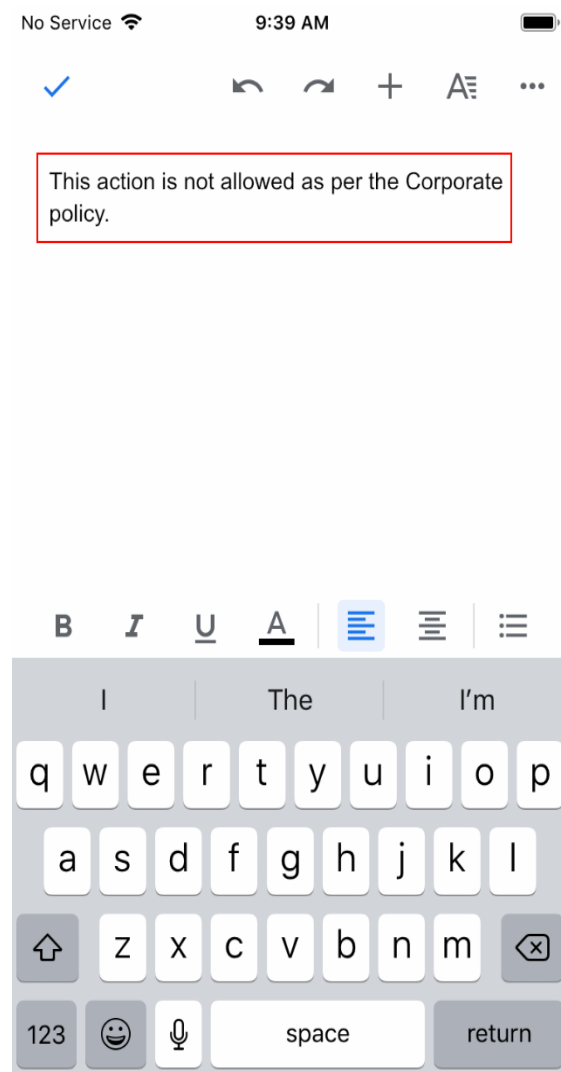
Allow sharing of locations

This policy controls location permission availability for apps. Keep this policy enabled if you are configuring WiFi policies, Trustee 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.

Yes

Android 5.0+ (PO & DO)

Figure D-22 Attempting to Paste Text on iOS Between Unmanaged and Managed Apps



## D.10 Privacy Risk 1 – Wiping Activities on the Employee’s Device May Inadvertently Delete the Employee’s Personal Data

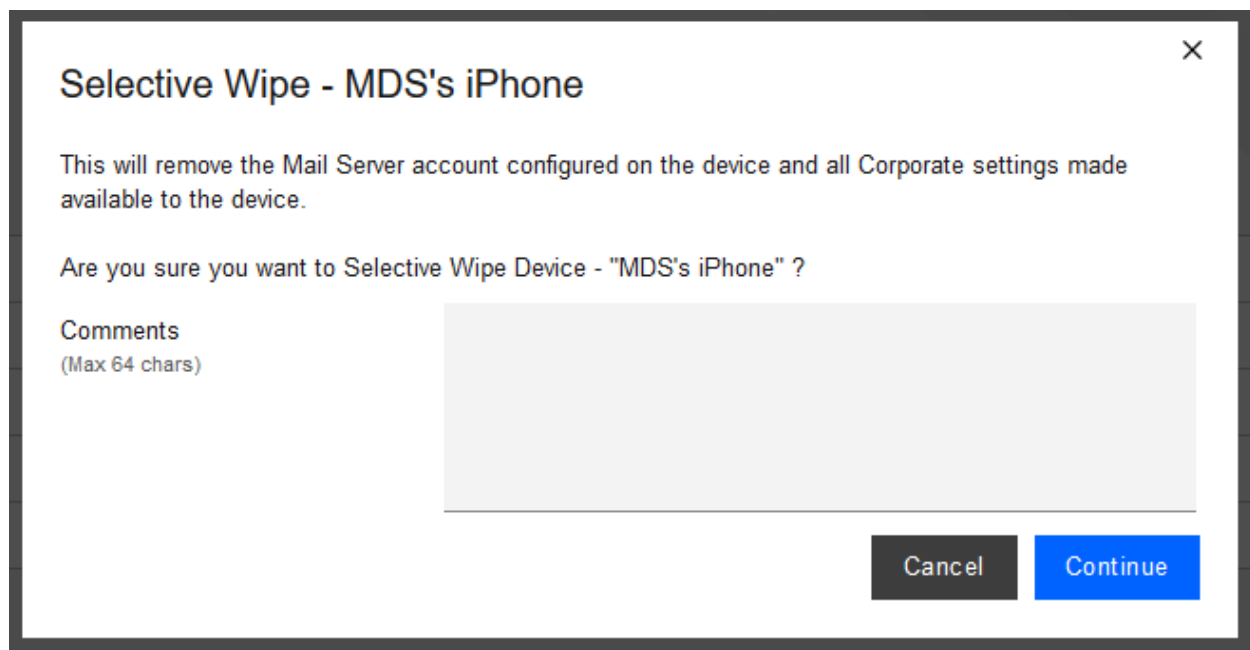
**Summary:** Personal data on the phone could be lost during a device wipe.

**Test Activity:** Selectively wipe a device using MaaS360; restrict staff access to only allow wiping of work profile data.

**Desired Outcome:** The user will no longer be able to access work applications and data on the device and retains all access to their personal applications and data. The restricted administrator accounts will only be able to remove work profile data.

**Observed Outcome:** Corporate data and applications are removed while personal data is untouched. The EMM console removes staff access to performing full device wiping. Figure D-23 shows initiation of a selective wipe. The selective wipe will remove the Mail Server account and all corporate settings available to the device.

Figure D-23 Selective Wipe



**Additional Potential Mitigations:**

- Notify users of use-policy regarding corporate applications.
- Disallow configuration of work applications by users where possible to prevent comingling of personal and work data.
- Restrict staff access to system capabilities that permit removing device access or performing wipes.

## D.11 Privacy Risk 2 – Organizational Collection of Device Data May Subject Employees to Feeling or Being Surveilled

**Summary:** The user may experience surveillance from the organization collecting device application and location data.

**Test Activity:** Disable location tracking and verify that applications outside of the organizationally controlled portions of the phone are not inventoried by the EMM.

**Desired Outcome:** Collection of application and location data is restricted by the EMM. The EMM does not collect an inventory of personal applications on the device and does not collect location information, including physical address, geographic coordinates and history, internet protocol (IP) address, and service set identifier (SSID).

**Observed Outcome:** When inspecting a device, location and application inventory information are not collected by an EMM, and application inventory information is not transmitted to Kryptowire. Collection of the installed personal apps is restricted by OS-level controls.

Figure D-24 shows inventory information for **installed** applications. When privacy restrictions are configured, only corporate application inventory information is collected. No personal applications are found in the EMM’s installed applications list.

Figure D-24 Application Inventory Information

←

MDS's iPhone

Apps Installed

Locate

Message

Buzz

More

▼ Apps Installed

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	<a href="#">Remove App</a>	<a href="#">Security Details</a>
MaaS360	com.fiberlink.ma as360forios	3.97.36	147.02	2.99	Installed by MDM	iTunes	Required	<a href="#">Remove App</a>	<a href="#">Security Details</a>
MaaS360 VPN	com.fiberlink.ma as360.maas360v pn	3.20.50	7.53	0.02	Installed by MDM	iTunes		<a href="#">Remove App</a>	<a href="#">Security Details</a>
zIPS	com.zimperium. zIPS.appstore	4.12.0	36.94	0.05	Installed by MDM	iTunes	Required	<a href="#">Remove App</a>	<a href="#">Security Details</a>

1

<

>

Jump To Page

Displaying 1 - 4 of 4 Records

CSV

Export

Figure D-25 shows that privacy settings have been enabled to restrict collection of location information.

Figure D-25 Location Information Restricted

IBM MaaS360

With Watson

Search for Devices, Users, Apps or Docs

HOME

DEVICES

USERS

SECURITY

APPS

DOCS

REPORTS

SETUP

Restrict Location Information

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

Select Applicable Ownership Types

☐ Corporate owned

☒ Employee owned

☐ Unknown

Select Applicable Group

All Devices

Restrict App Inventory Information

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

Select Applicable Ownership Types

☐ Corporate owned

☒ Employee owned

☐ Unknown

Select Applicable Group

All Devices

Additional Potential Mitigations:

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

- Limit or disable collection of specific data elements.
- Dispose of personally identifiable information (PII).

## D.12 Privacy Risk 3 – Data Collection and Transmission Between Integrated Security Products May Expose Employee Data

**Summary:** Access to monitoring data from the device is not restricted to administrators. Application and location data are shared with third parties that support monitoring, data analytics, and other functions for operating the BYOD solution.

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

**Desired Outcome:** System provides access controls to monitoring functions and logs. Data flow between the organization and third parties does not contain location information, including physical address, geographic coordinates and history, IP address, and SSID.

**Observed Outcome:** Domain administrators were allowed to log in, but non-administrator users were not.

Figure D-26 demonstrates how a non-administrator account will be prevented from logging into the MaaS360 portal.

Figure D-26 Non-Administrator Failed Portal Login

The screenshot shows the IBM MaaS360 login interface. At the top left is a back arrow. The title "Log into IBM MaaS360" is centered. Below the title, a red error message states: "The credentials entered were incorrect or this account is not provisioned. Contact your Administrator to request that your Login account be provisioned." The username "testuser" is entered in the blue text field. Below the username is a white password field with the placeholder text "Password". At the bottom is a large blue "Log In" button. Below the button is a blue link that says "Forgot Username or Password?".

Figure D-27 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

enterprise.mds.local

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)

CN=Domain Admins,CN=Users,DC=enterj

Administrator - Level 2

▼

⊖

----Select Role----

▼

⊕

Figure D-28 Administrator Levels

⋮ Administrator

⋮ Administrator - Level 2

⋮ API

⋮ Help Desk

⋮ Read-Only

⋮ Service Administrator

Potential Mitigations:

- De-identify personal and device data when such data is not necessary to meet processing objectives.
- Encrypt data transmitted between parties.
- Limit or disable access to data.

NIST SP 1800-22C: Mobile Device Security: Bring Your Own Device

82

- Limit or disable collection of specific data elements.
- Use policy controls such as contracts to limit third-party data processing.

### D.13 Privacy Risk 4 – Employees Might Feel Compelled to Participate in Data Processing Practices Inconsistent with Expectations

**Summary:** Users may not have knowledge of what information is collected and monitored by the organization.

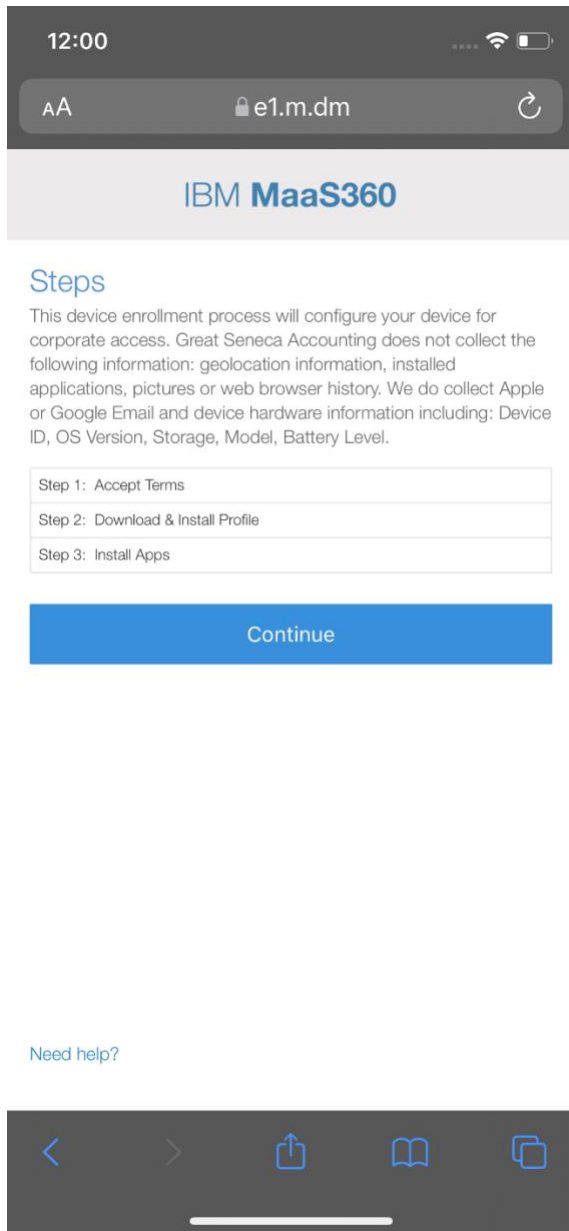
**Test Activity:** Test to ensure that MDM provides custom notification to users detailing collected device information.

**Desired Outcome:** MDM provides details of what information is collected during device enrollment.

**Observed Outcome:** Device data collection information is displayed to users.

[Figure D-29](#) demonstrates how users will be notified of what device information is collected by mobile security products during the device enrollment process.

**Figure D-29 Mobile Device Information Collection Notification**



**Additional Potential Mitigations:**

- Provide notification to the user.
- Train users on mobile-device collection policy.
- Provide a point of contact for user questions regarding organizational data collection and use policies.
- Train system administrators regarding the privacy requirements for operating the BYOD systems.



## D.14 Privacy Risk 5 – Unauthorized or Invasive Application Processing of Information Exposes Employee Data

**Summary:** The employee or organization installs third-party applications that access data on the device without fully understanding the nature of the applications data processing practices, creating opportunities for invasive or malicious activity or installation of malware. An application may over-collect information or conduct analysis that may result in embarrassment to the employee or create opportunities for surveillance that extend beyond the level of monitoring needed for an organization.

**Test Activity:** Log in to an Application Vetting solution to automatically analyze all new applications installed on enrolled devices, then run the reports to see threat details.

The administrator configures a threat score alert threshold and an email address to receive alerts when an application's threat score is at or above the threshold.

**Desired Outcome:** After application analysis the risk posture of the devices, and therefore, the enterprise stays at an acceptable level. If the work application did not pass the App Vetting process it should not be used by the enterprise.

**Observed Outcome:** App vetting solution recognized that the application exceeded the configured security threshold and over-collected personal information. The application's collection of contacts, calendars and device sensors could introduce vulnerabilities. Figure D-30 through [Figure D-32](#) demonstrate the app vetting findings.

Figure D-30 Mobile Device Information Collection Notification

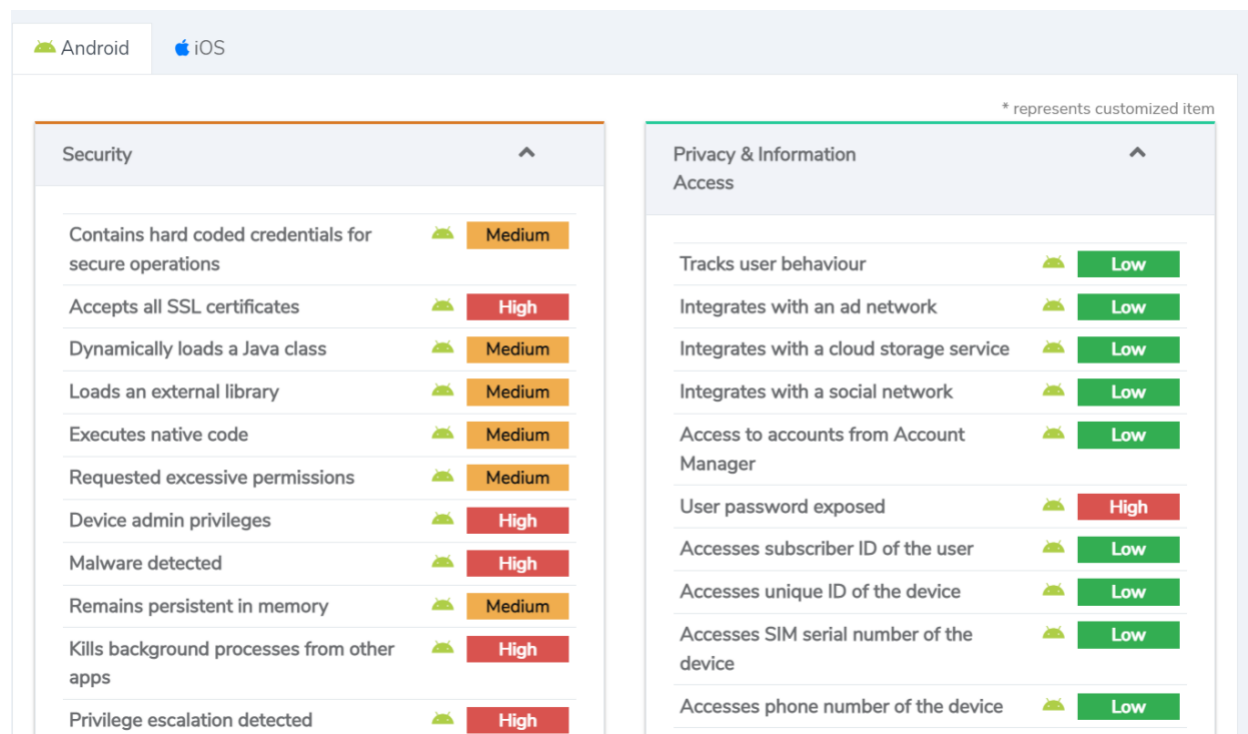


Figure D-31 Privacy and Information Access of the Application



















Privacy & Information Access		^
Tracks user behaviour		Low
Integrates with an ad network		Low
Integrates with a cloud storage service		Low
Integrates with a social network		Low
Access to accounts from Account Manager		Low
User password exposed		High
Accesses subscriber ID of the user		Low
Accesses unique ID of the device		Low
Accesses SIM serial number of the device		Low
Accesses phone number of the device		Low
Has in app purchases		Medium
Exposes sensitive information		High
Creates resources accessible from outside parties		Medium
Connection to foreign country		Medium
Exposes low risk sensitive information		Medium
App communicates with high risk locations		Critical
Accesses calendar		Low
Accesses contacts		Medium

Figure D-32 Application Analysis

Kryptowire EMM Portal

MDM INTEGRATION

APPLICATION ANALYSIS

Analyzed Apps

Submit iOS App

Submit Android App

WATCH LIST

SUPPORT TICKET

LOGOUT

BETA

Search:

Showing 1 to 10 of 1,053 entries

Show

10

entries

Previous

1

2

3













4

5

...

106

Next

App	Platform	Date Submitted	Threat Score	Security Issues	Reports
 <div>[REDACTED]</div> <div>Ver: 4.48.0</div>		2023-03-22 14:25:33			
 <div>[REDACTED]</div> <div>Ver: 1.0</div>		2018-12-05 14:46:18			
 <div>[REDACTED]</div> <div>Ver: 1.0</div>		2018-12-05 14:42:28	83.4	Application is debuggable, <? Loads code dynamically	<div><a href="#">PDF Report</a> <a href="#">NIAP HTML</a> <a href="#">JSON</a></div> <div><a href="#">HTML Rep</a> <a href="#">NIAP PDF</a></div>
 <div>[REDACTED]</div> <div>Ver: 53.1.7</div>		2018-10-24 00:37:01	60.2	Can access contacts, Can access the device's location, Can access microphone, Can access photos and videos, Can send with SMS messages, Can obtain user/device specific information, Has in app purchases, Integrates with ad network	<div><a href="#">PDF Report</a> <a href="#">NIAP HTML</a> <a href="#">JSON</a></div> <div><a href="#">HTML Rep</a> <a href="#">NIAP PDF</a></div>
 <div>[REDACTED]</div> <div>Ver: 1.0.15</div>		2018-10-24 00:36:59	75.1	Can access contacts, Can access the device's location, Can access microphone, Can access photos and videos, Can send with SMS messages, Has in app purchases, Integrates with social network, Exposes sensitive information	<div><a href="#">PDF Report</a> <a href="#">NIAP HTML</a> <a href="#">JSON</a></div> <div><a href="#">HTML Rep</a> <a href="#">NIAP PDF</a></div>

#### Additional Potential Mitigations:

- EMM leverages OS related separation between enterprise and personal data.
- Train users on safe practices for downloading files and installing applications of their devices.
- Scan downloaded applications for malware.
- Institute procedures for conducting a privacy risk assessment for applications installed by the organization.