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
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward
The MITRE Corporation
McLean, VA

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

November 2022

SECOND DRAFT

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

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in this document 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 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 NCCoE address goals of improving the 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 cyber security measures such as this recommendation.

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

FEEDBACK

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

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

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

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

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: 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.

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 iOS smartphone BYOD deployments.

Incorporating BYOD capabilities into an organization can provide greater flexibility in how employees work and 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 work organizations and device owners. The unique nature of these challenges is driven by the diverse range of devices available that vary in type, age, operating system (OS), and the level of risk posed.

Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks to organizations. 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 many of its 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
Jeff Greene	NIST
Natalia Martin	NIST
William Newhouse	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST

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

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

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.

CALL FOR PATENT CLAIMS

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

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

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

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

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

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

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

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

Contents

171 # List of Figures

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 4.1.4, Conduct a 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 3.7, Technologies, 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.

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.

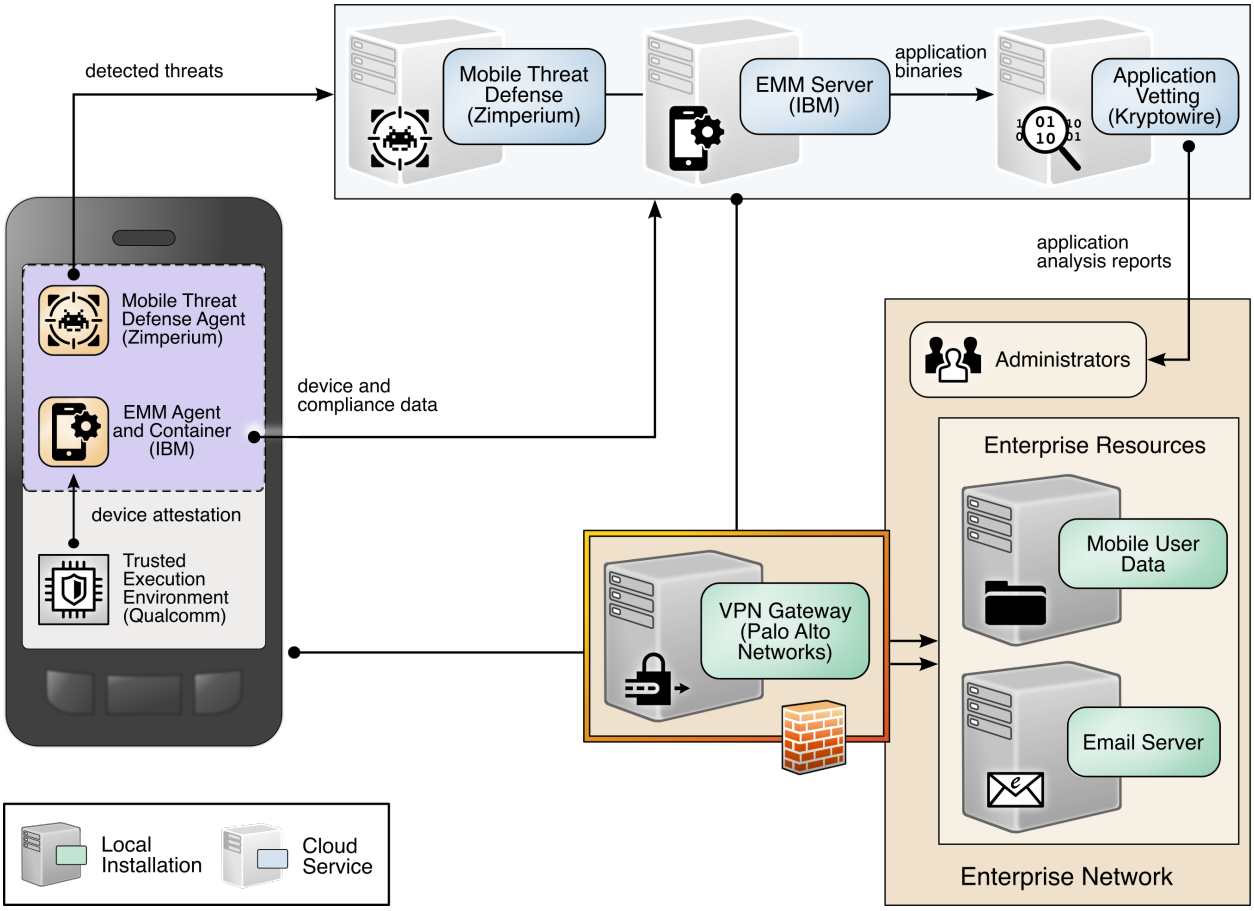
Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide.*
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`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

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

1.4 Logical Architecture Summary

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

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



325 # 2 Product Installation Guides

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

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

331 ## 2.1 Network Device Enrollment Services Server

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

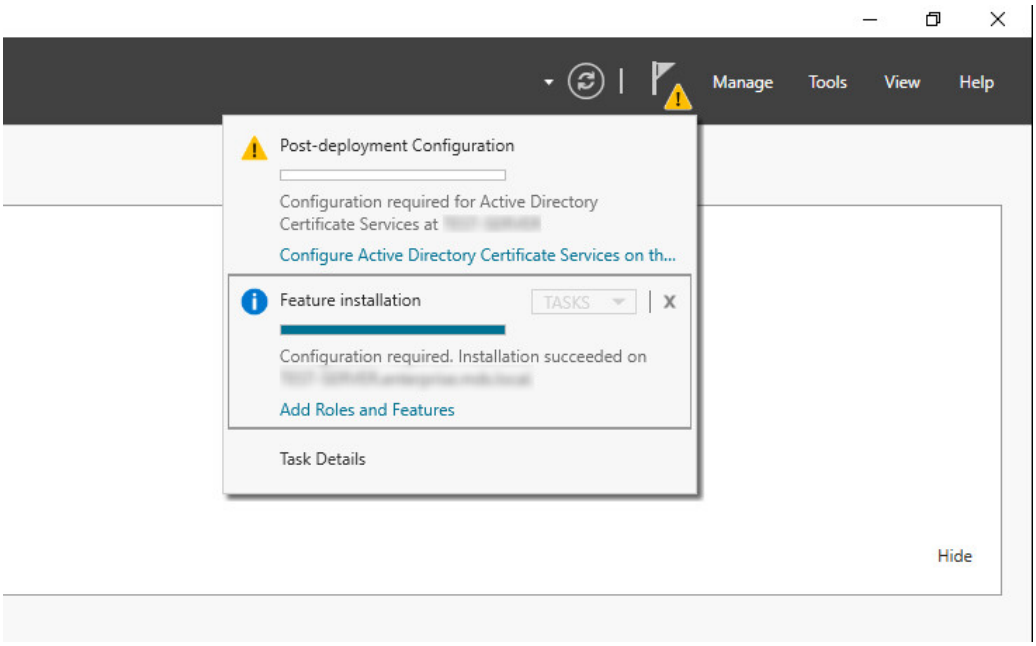
that a basic AD and certificate authority (CA) are in place, containing a root and subordinate CA, and that their certificates have been exported.

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

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



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

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

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

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

356 a. On the active directory server, open **Active Directory Users and Computers.**

357 b. Click **Users** and create a new user for the service. For this example, it will be named
358 NDES. Be sure the password never expires.

359 c. On the NDES server, open **Edit local users and groups**.

360 d. Click **Groups.** Right-click **IIS_IUSRS,** click **Add to Group,** and click **Add**.

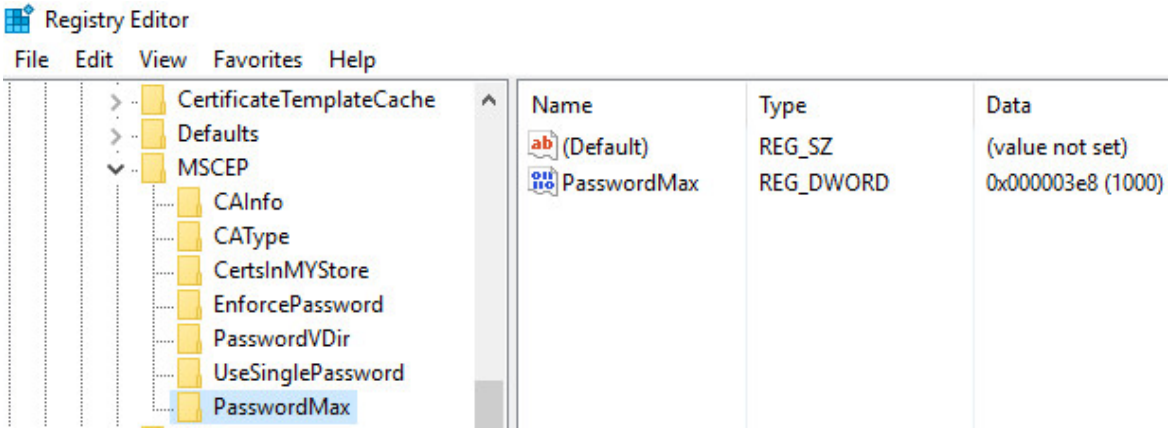
361 e. Search for the service account name—in this case, NDES. Click **Check Names,** then click
362 **OK** if no errors were displayed.

363 f. Click **Apply** and click **OK**.

364 g. Close all windows except the NDES configuration window.

12. Click **Select** next to the box and enter the service account credentials. Click **Next**.
13. 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**.
14. Click **Next** three times.
15. Click **Configure.**
16. On the SUB-CA, open the Certification Authority application.
17. Expand the SUB-CA node, right-click on **Certificate Templates,** and click **Manage**.
18. Right-click on **IPSec (Offline Request)** and click **Duplicate Template**.
19. Under the **General** tab, set the template display name to **NDES**.
20. Under the **Security** tab, click **Add**.
21. Select the previously configured NDES service account.
22. Click **OK**. Ensure the NDES service account is highlighted, and check **Read** and **Enroll**.
23. Click **Apply**.
24. In the Certification Authority program, right-click on **Certificate Templates,** and select **New > Certificate Template to Issue**.
25. Select the NDES template created in step 24.
26. Click **OK.**
27. On the NDES server, open the Registry Editor (`regedit`).
28. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography`.
29. Select the `MSCEP` key and update all entries besides (Default) to be **NDES**.
30. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP`.
31. Right-click on **MSCEP** and select **New > Key**. Name it **PasswordMax**.
32. Right-click on the newly created key and select **New > DWORD (32-bit) Value.**
33. 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.

392 **Figure 2-2 PasswordMax Registry Configuration**



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

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

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

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

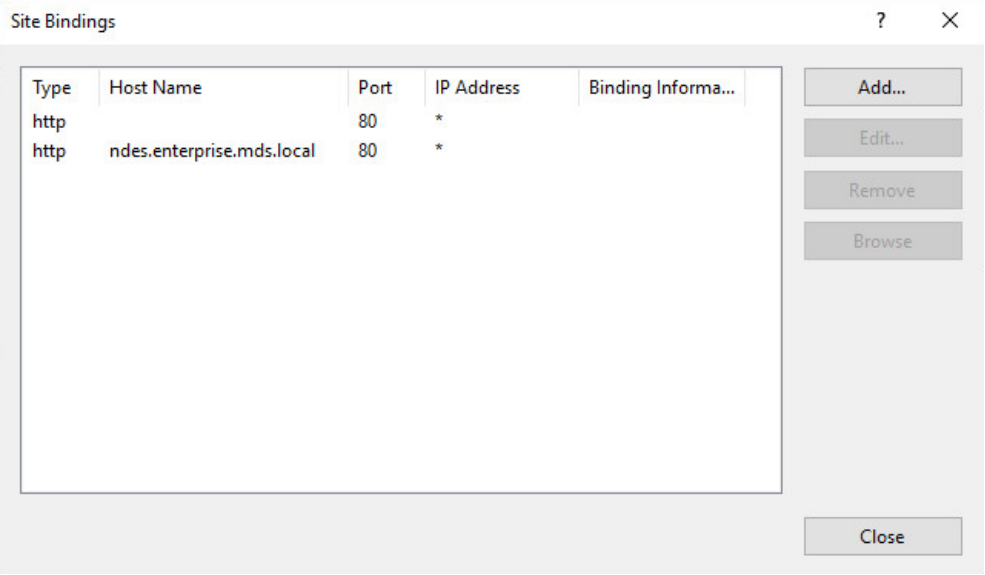
402 37. On the right, click **Bindings…**

403 38. Click **Add.**

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

406 40. Click **OK**.

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



408

409 41. Click **Close** and close the IIS Manager.

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

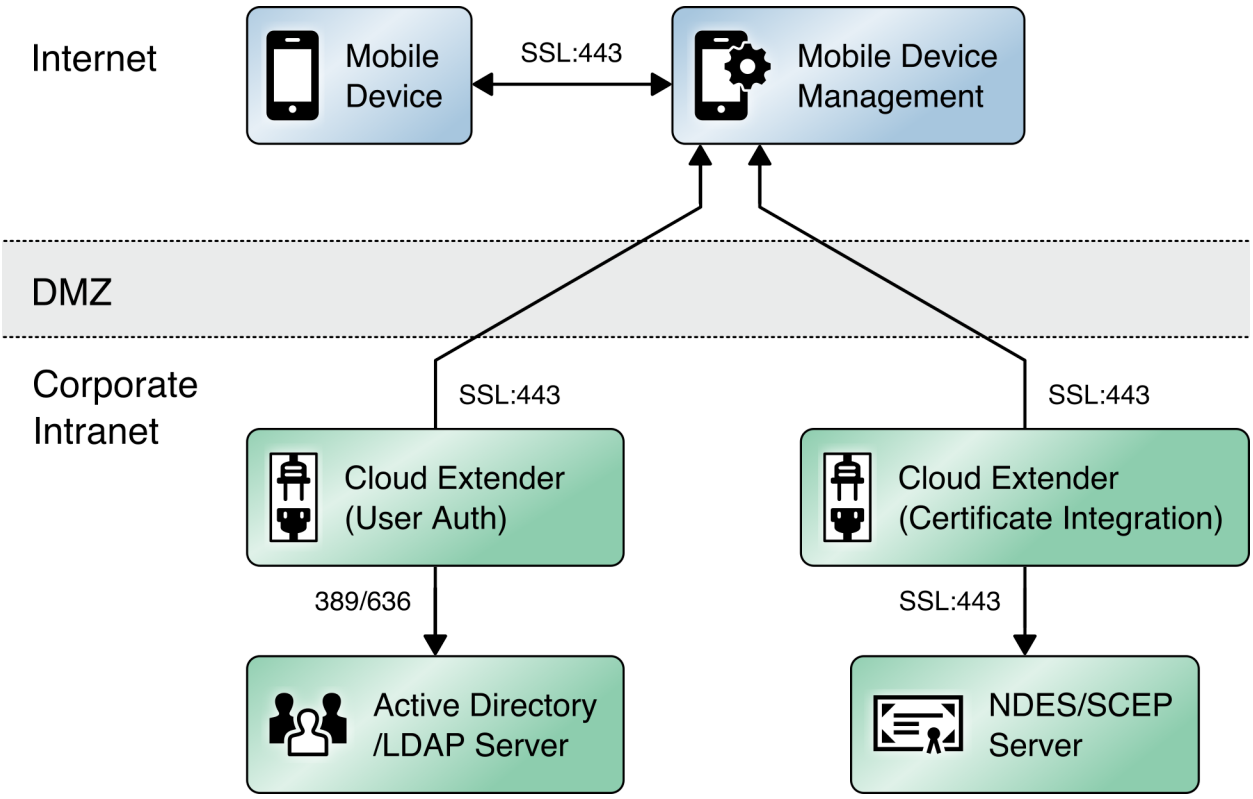
411 2.2 International Business Machines MaaS360

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

415 2.2.1 Cloud Extender

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

420 **Figure 2-4 Cloud Extender Architecture**



421 ### *2.2.1.1 Cloud Extender Download*

422 1. Log in to the MaaS360 web portal.

423 2. Click **Setup > Cloud Extender.**

424 3. Click the link that says **Click here to get your License Key.** The license key will be emailed to the
425 currently logged-in user's email address.

426 4. Click the link that says **Click here to download the Cloud Extender.** Save the binary.

427 5. Move the binary to a machine behind the corporate firewall that is always online. Recommenda-
428 tion: Install it while logged in as a domain user on a machine that is not the domain controller.

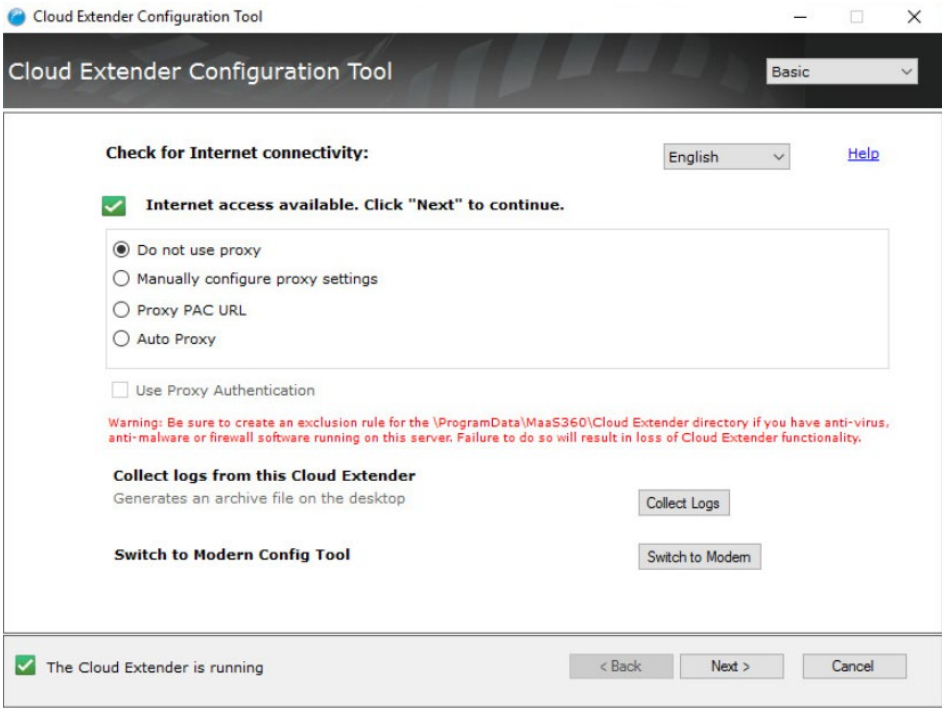
429 6. Install **.NET 3.5 Features** in the **Server Manager** on the machine where the MaaS360 Cloud Ex-
430 tender will run.

431 ### *2.2.1.2 Cloud Extender Active Directory Configuration*

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

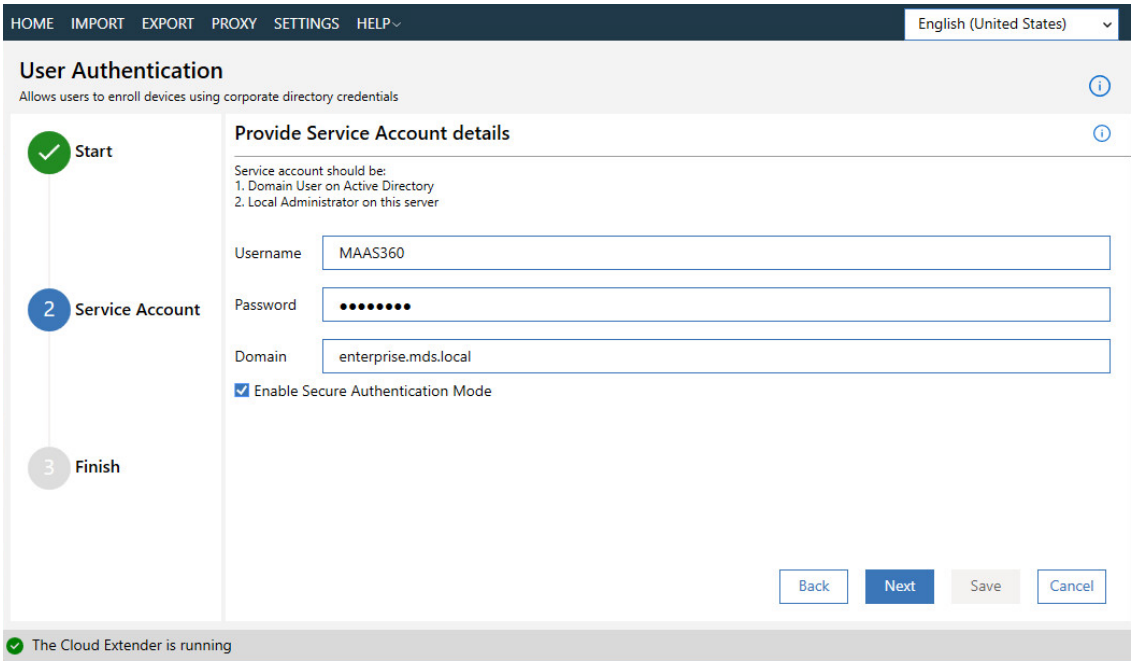
2. Enter the license key when prompted.
3. Proceed through the setup until the Cloud Extender Configuration Utility opens.
4. If using the old cloud extender interface, click **Switch to Modern.**

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.

440 **Figure 2-6 Cloud Extender Service Account Details**



441 7. Click **Next**.

442 8. (optional) Use the next page to test the active directory integration.

443 9. Click **Save**.

444 10. In MaaS360, navigate to **Setup > Cloud Extender.** Ensure that configuration information is dis-
445 played, indicating that the MaaS360 Cloud Extender is running.

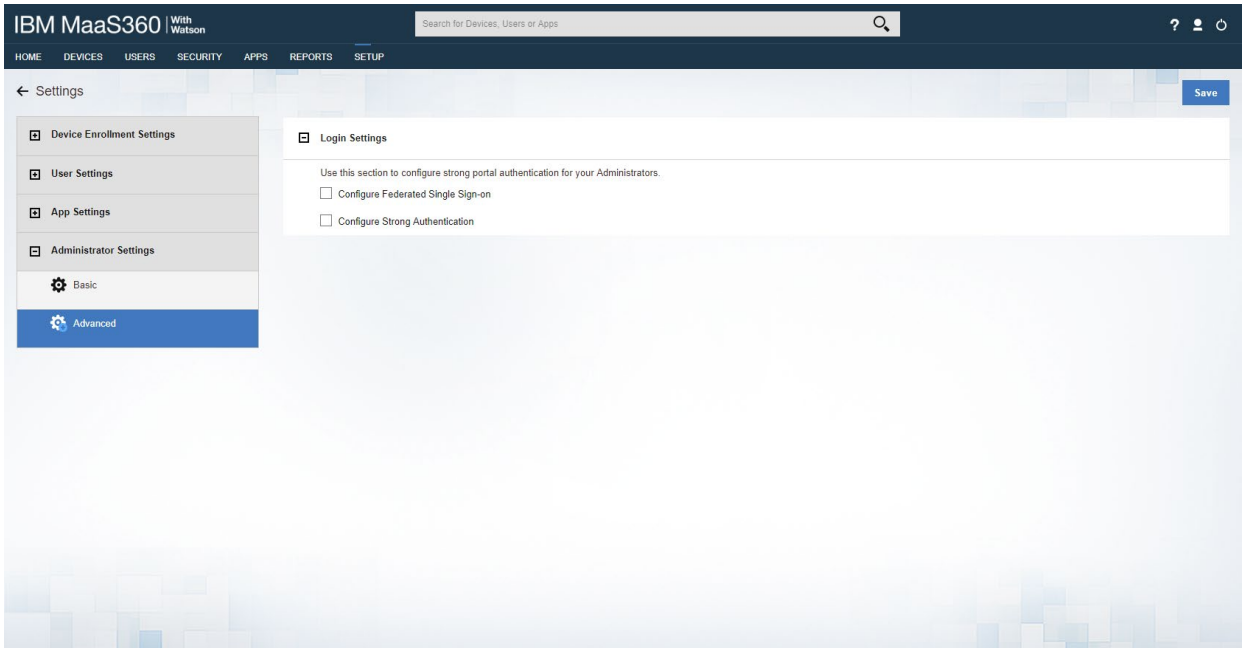
446 *2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration*

447 1. Log in to the MaaS360 web portal as an administrator.

448 2. Go to **Setup > Settings**.

449 3. Expand **Administrator Settings** and click **Advanced**.

450 **Figure 2-7 Administrator Settings**



451 4. Select **Configure Federated Single Sign-on**.

452 5. Select **Authenticate against Corporate User Directory**.

453 6. Next to **Default Domain,** enter the active directory domain. In this implementation, *enter-*
454 *prise.mds.local* was used.

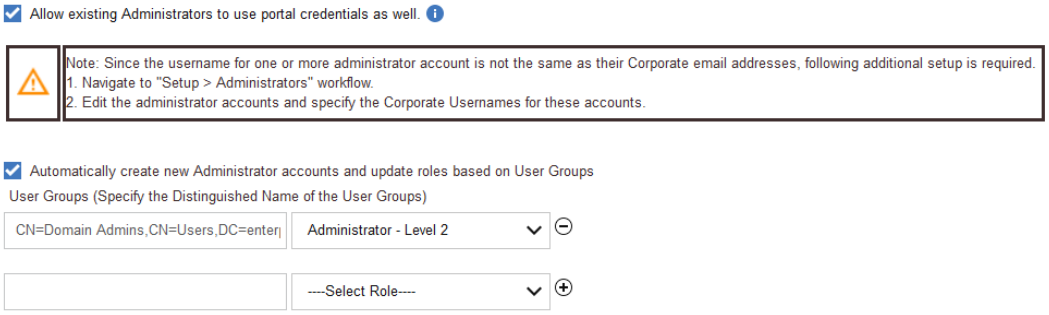
455 7. Check the box next to **Allow existing Administrators to use portal credentials as well**.

456 8. Check the box next to **Automatically create new Administrator accounts and update roles**
457 **based on user groups**.

458 9. Under **User Groups**, enter the distinguished name of the group(s) that should be allowed to log
459 in. In this implementation, CN=Domain Admins, CN=Users, DC=enterprise, DC=mds, DC=local
460 was used.

461 10. Next to the box, select **Administrator–Level 2.** This allows domain admins to log in as MaaS360
462 administrators.

463 **Figure 2-8 Administrator Configuration Options**



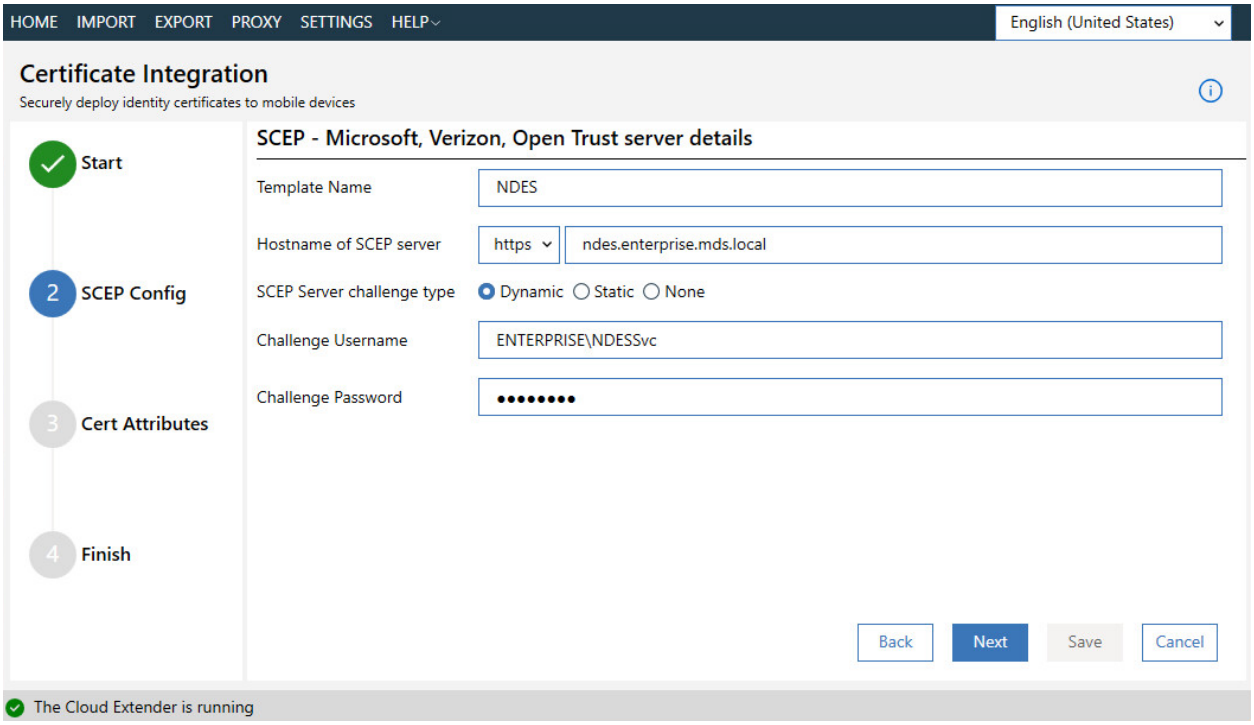
464 11. Click **Save.**

465 *2.2.1.4 Cloud Extender NDES Integration*

466 To properly generate device certificates, MaaS360 must be integrated with the on-premises public key
467 infrastructure (PKI).

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

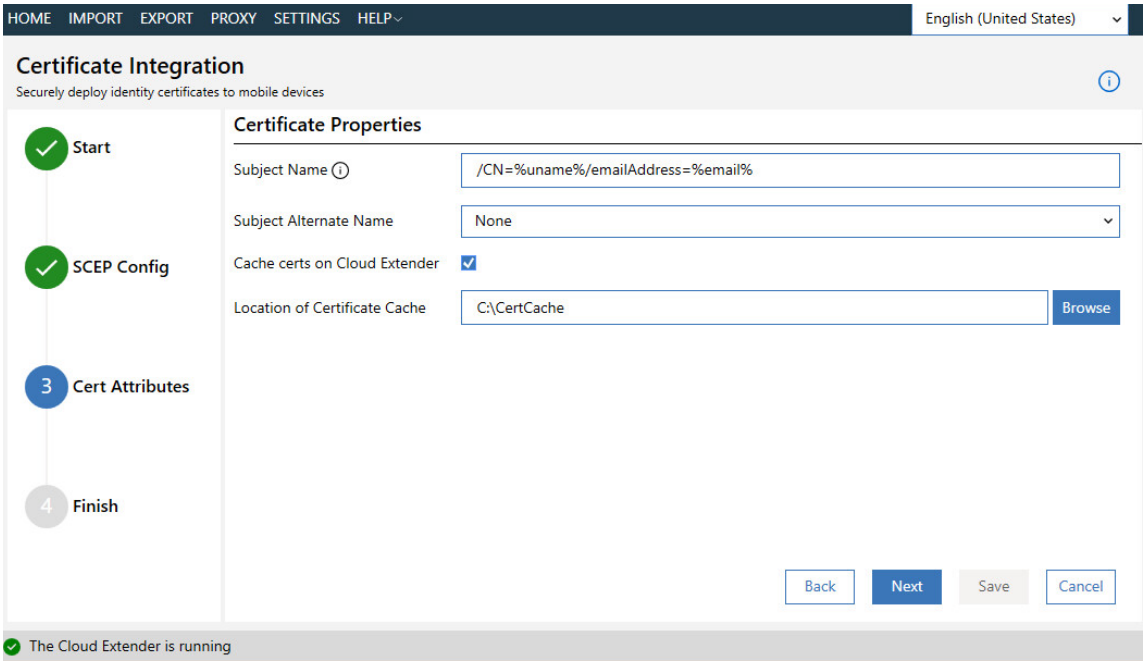
478 **Figure 2-9 Cloud Extender SCEP Configuration**



479 10. Click **Next.**

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

482 **Figure 2-10 Cloud Extender Certificate Properties**



483 12. Click **Next.**

484 13. (optional) Enter values for uname and email and generate a test certificate to test the configura-
485 tion.

486 14. Click **Save.**

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

488 2.2.2 Android Enterprise Configuration

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

492 1. Create a Google account if you do not have one you wish to bind with.

493 2. From the MaaS360 portal, navigate to **Setup > Services.**

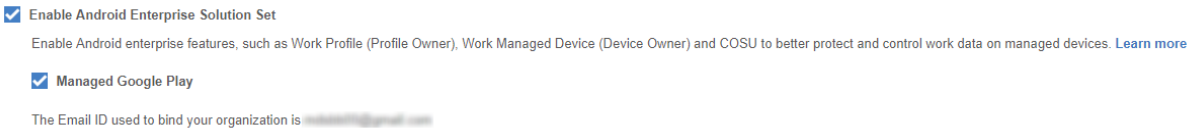
494 3. Click **Mobile Device Management.**

495 4. Check the box next to **Enable Android Enterprise Solution Set.**

496 5. Enter your password and click **Enable.**

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

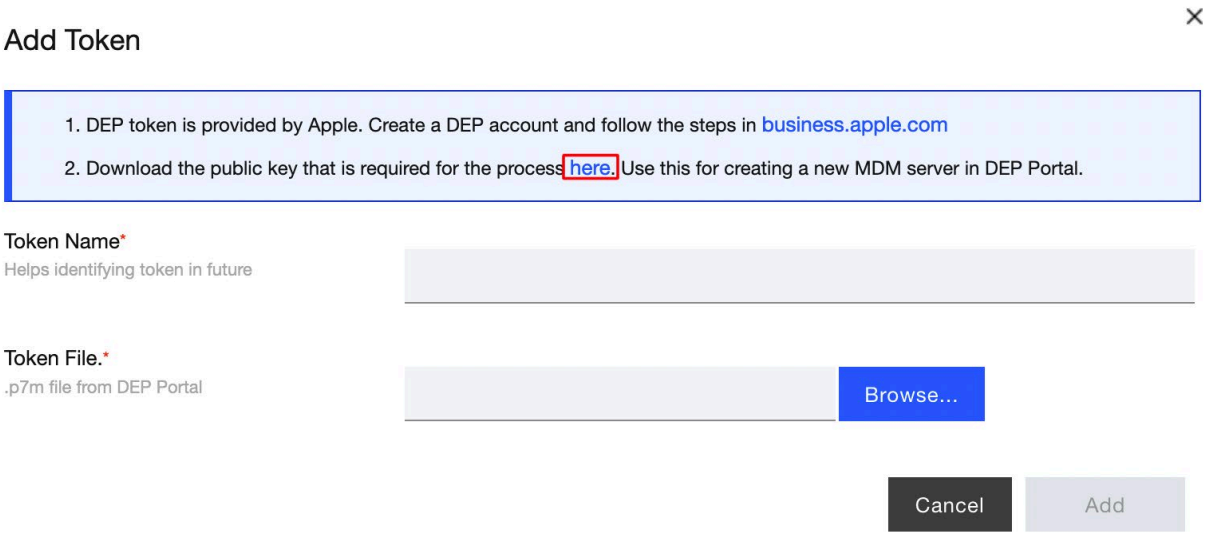
For the iOS Apple Push Notification services (APNs) certificate configuration, the build team followed the IBM documentation.

2.2.4 Apple User Enrollment (UE) Configuration

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.

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



522 5. In Apple Business Manager, sign in with an administrator account.

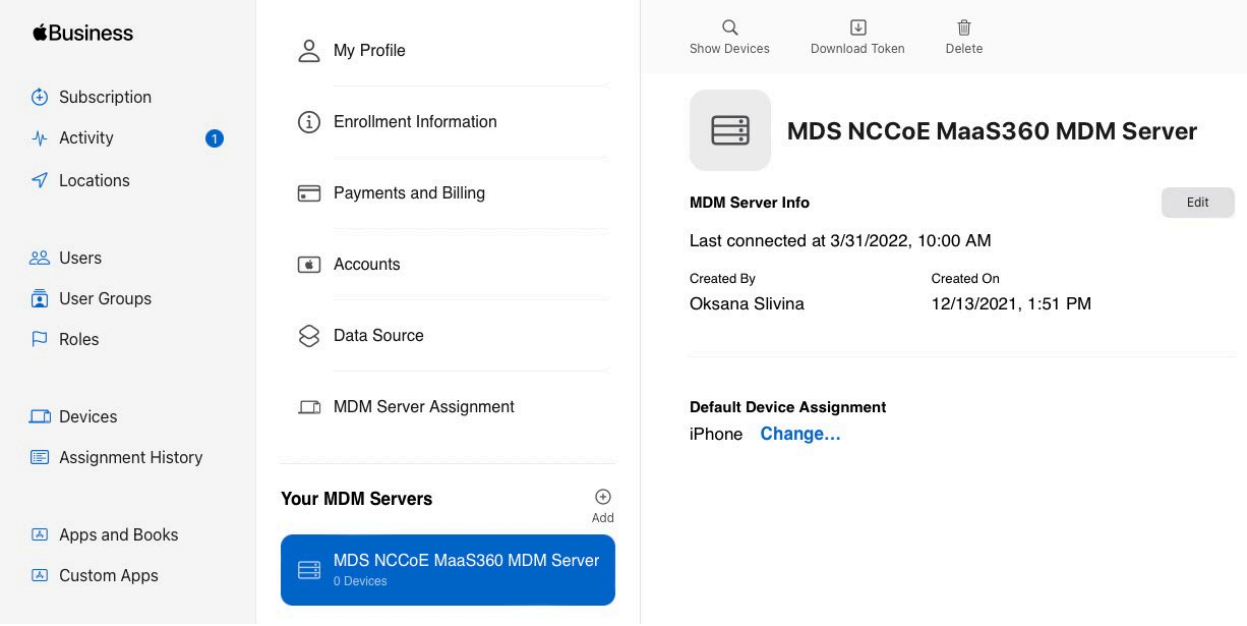
523 6. Click the user's name in the bottom left corner > **Settings**.

524 7. Click **Add** next to "Your MDM Servers" and enter a unique name for the server.

525 8. Upload the public key certificate file downloaded in step (4), then click **Save**.

526 9. Click **Download Token** to save the server token.

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

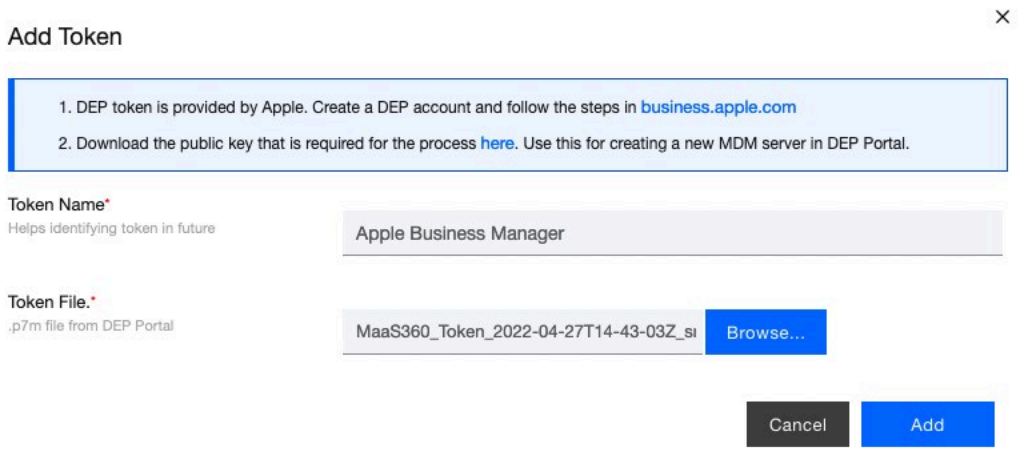


528

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

530 11. Click **Add**.

531 **Figure 2-14 Creating the DEP token**

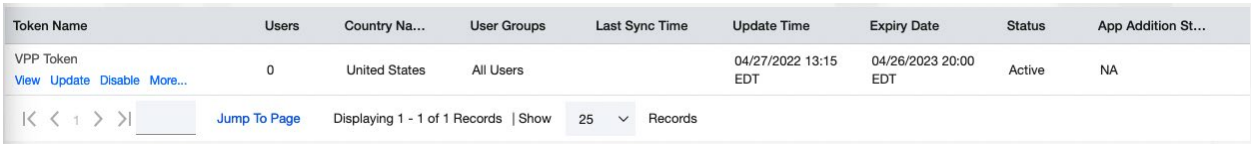


532

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

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



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

2.2.5 Android Configuration

2.2.5.1 Policy Configuration

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

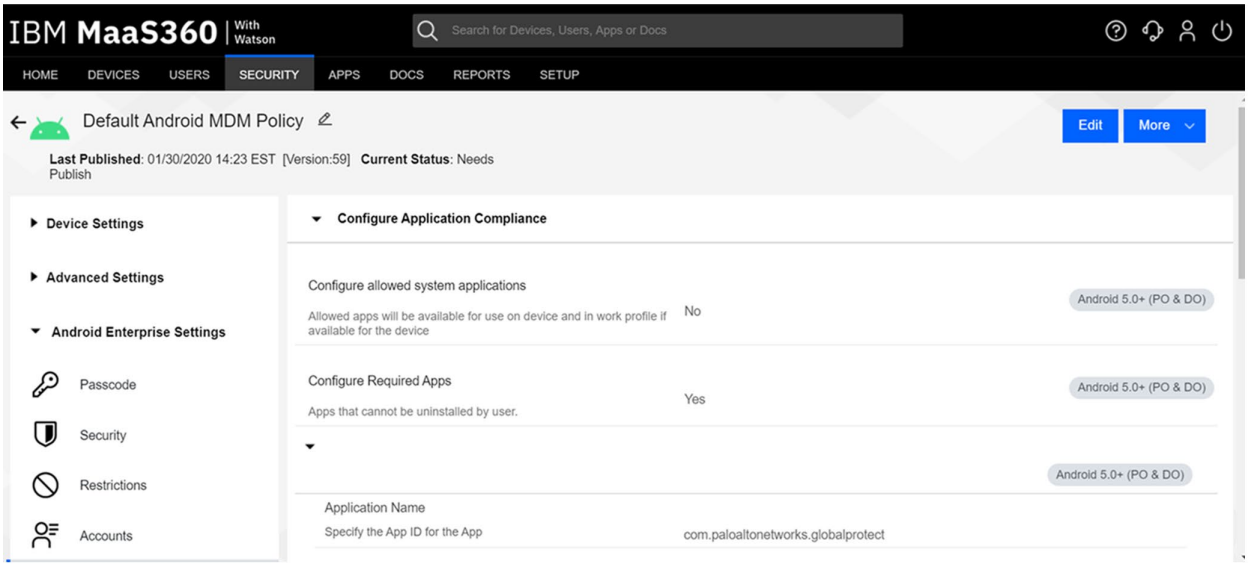
3. Click **Edit.**
4. Navigate to **Android Enterprise Settings > Passcode.**
5. Check the box next to **Configure Passcode Policy**.
6. Configure the passcode settings based on corporate requirements.
7. Navigate to **Android Enterprise Settings > Restrictions.**
8. Check the box next to **Configure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

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



609 ## 2.2.6 iOS Configuration

610 ### *2.2.6.1 Policy Configuration*

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

621 ### *2.2.6.2 VPN Configuration*

622 1. Click **Device Settings > VPN**.

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.

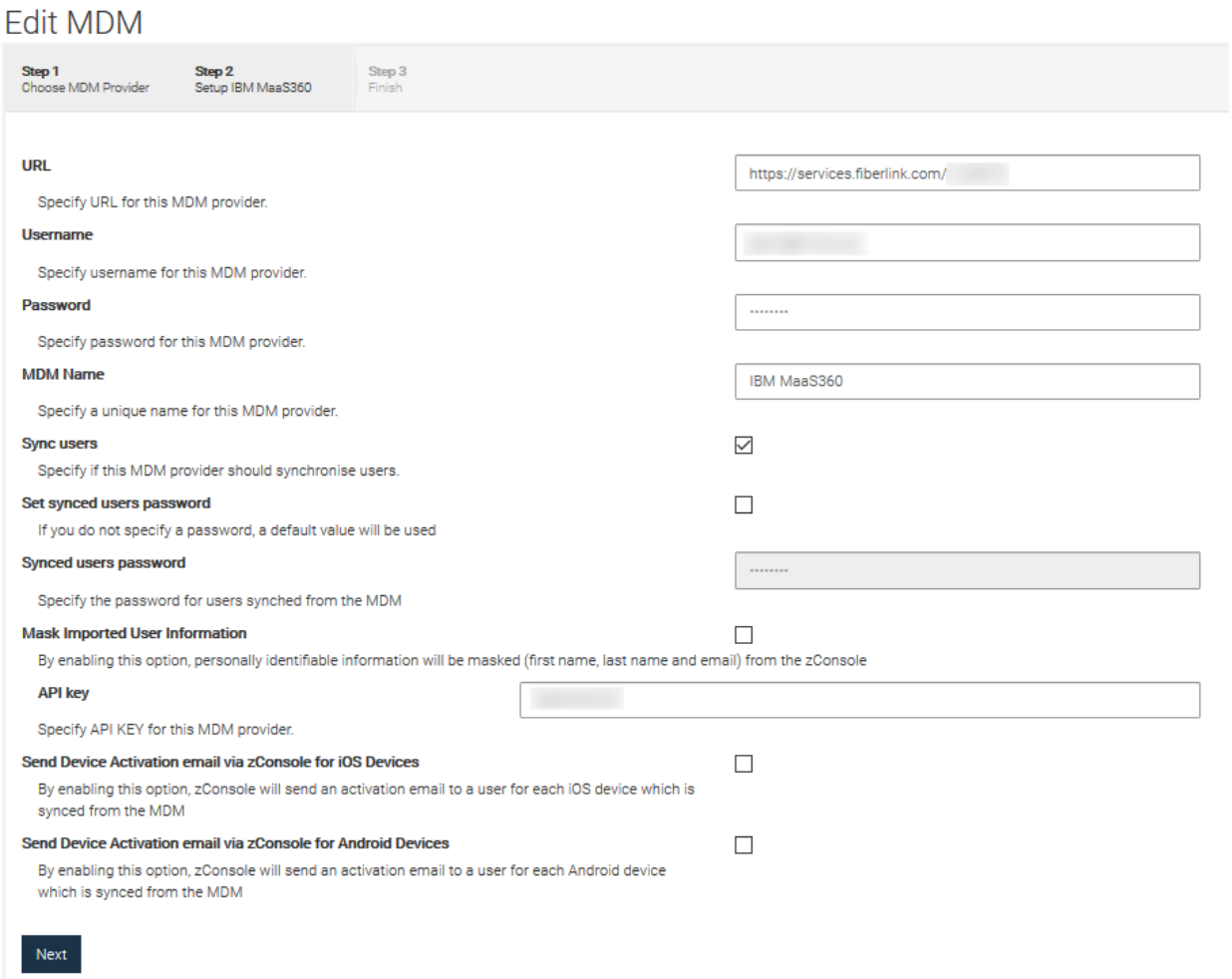
Note: For Zimperium automatic enrollment to function properly, users **must** have an email address associated with their MaaS360 user account.

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.
5. Note: For the MDM URL, append the account ID to the end. For example, if the account ID is 12345, the MDM URL would be https://services.fiberlink.com/12345.
6. Check the box next to **Sync users**.

689 **Figure 2-18 Zimperium MaaS360 Integration Configuration**



690 7. Click **Next**.

691 8. Select the MaaS360 groups to synchronize with Zimperium. In this case, **All Devices** was se-
692 lected**.**

693 9. Click **Finish**. Click **Sync Now** to synchronize all current MaaS360 users and devices.

694 2.3.2 Automatic Device Activation

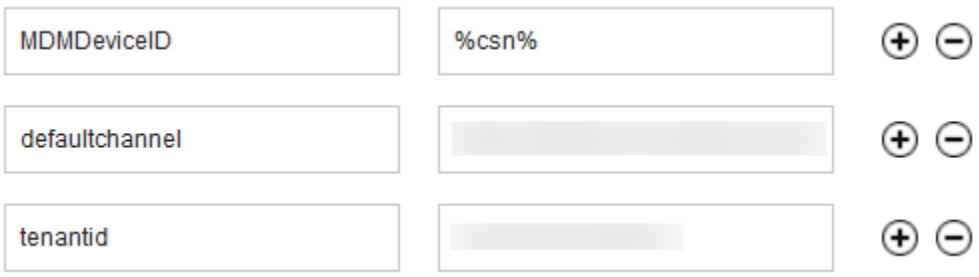
695 Note: This requires contacting Zimperium support to get required application configuration values.

696 1. In Apple Business Manager, click **Apps and Books**.

697 2. Search for *Zimperium zIPS*.

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.

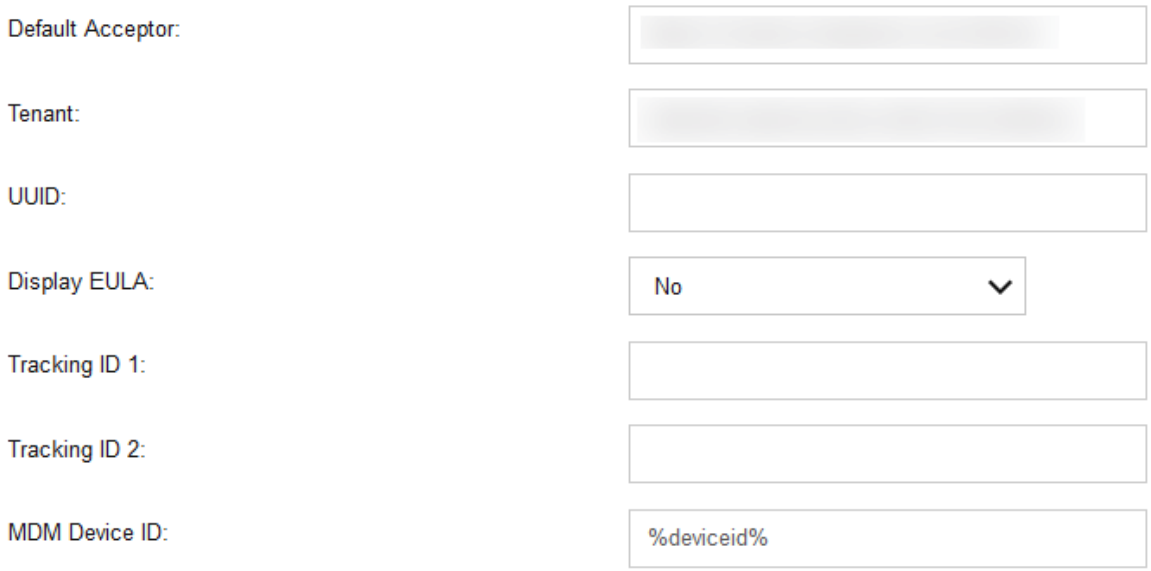
Figure 2-19 Zimperium zIPS iOS Configuration



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



32. Click **Add.**

2.3.3 Enforce Application Compliance

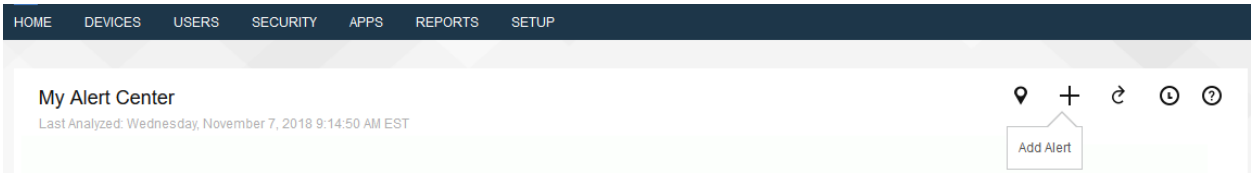
From the IBM MaaS360 web portal:

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.**

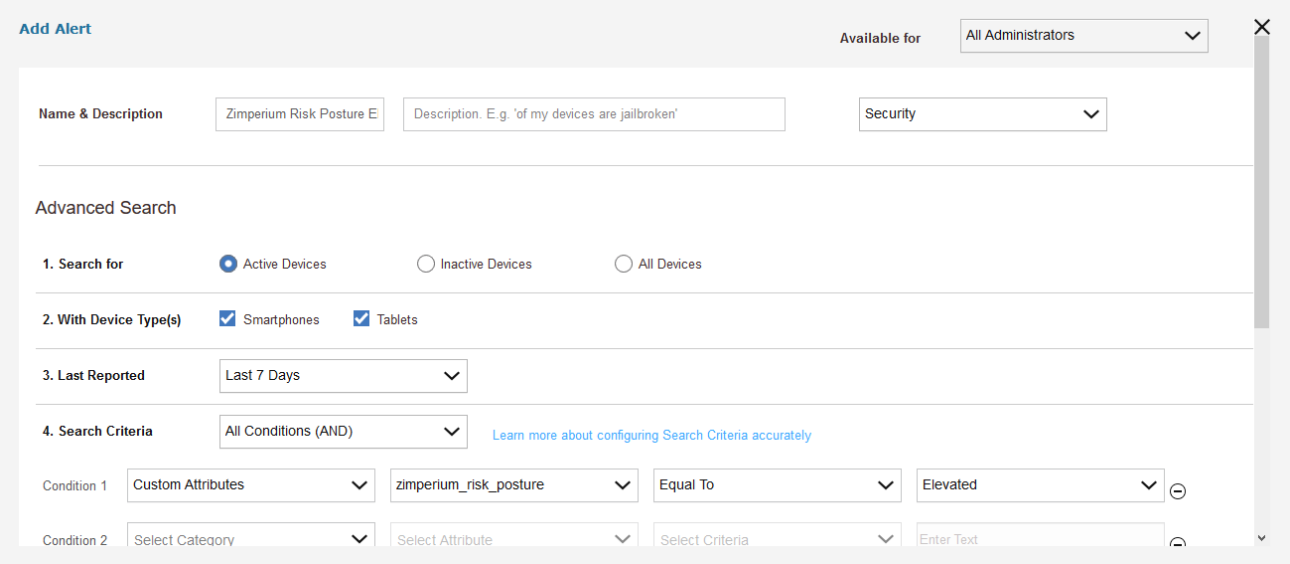
Figure 2-21 Add Alert Button



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

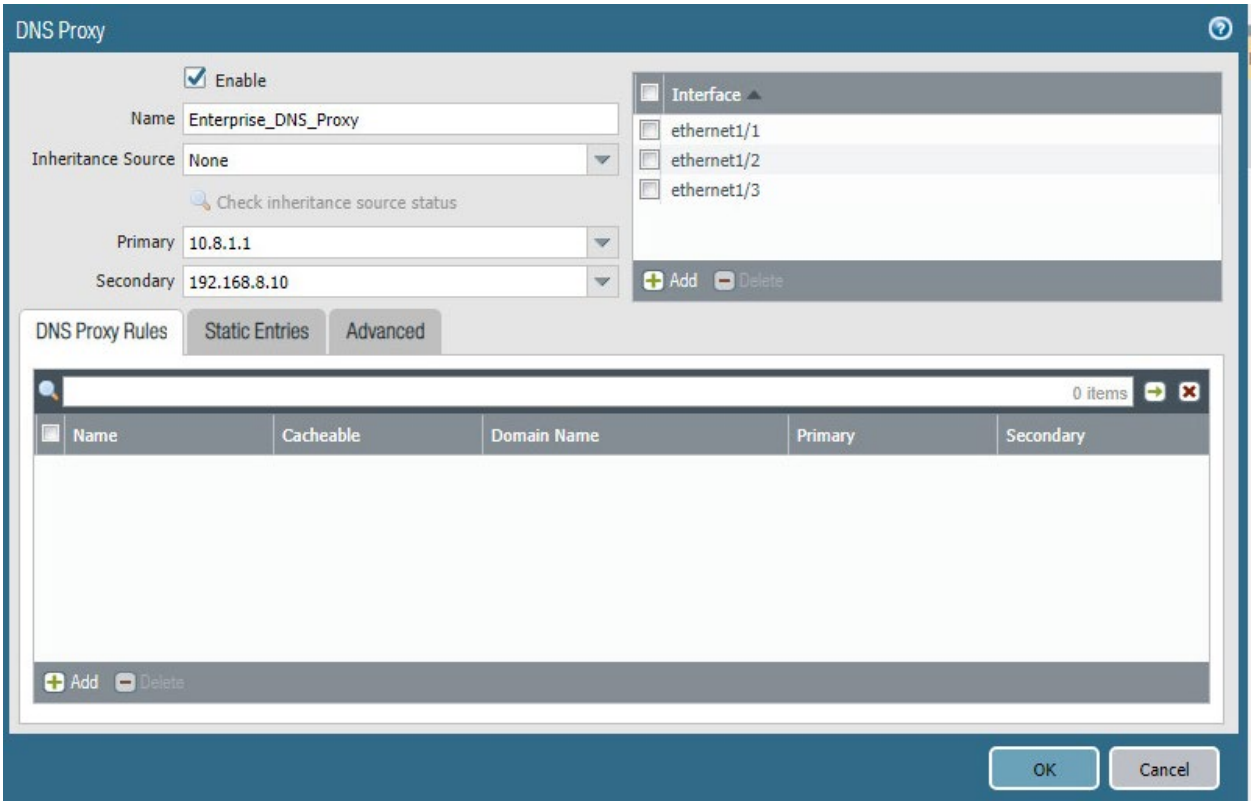
Palo Alto Networks contributed an instance of its VM-100 series firewall for use on the project.

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.**

795 **Figure 2-23 DNS Proxy Object Configuration**



796 22. Navigate to **Device > Services**.

797 23. Click the **gear** in the top-right corner of the Services panel.

798 24. Under **DNS settings,** click the radio button next to **DNS Proxy Object.** Select the created DNS
799 proxy object from the drop-down.

800 25. Click **OK** and commit the changes. This is where static DNS entries will be added in the future.

801 26. Navigate to **Objects > Addresses**.

802 27. For each device on the network, click **Add**. Give the device an appropriate name, enter an op-
803 tional description, and enter the IP address.

804 28. Click **OK**.

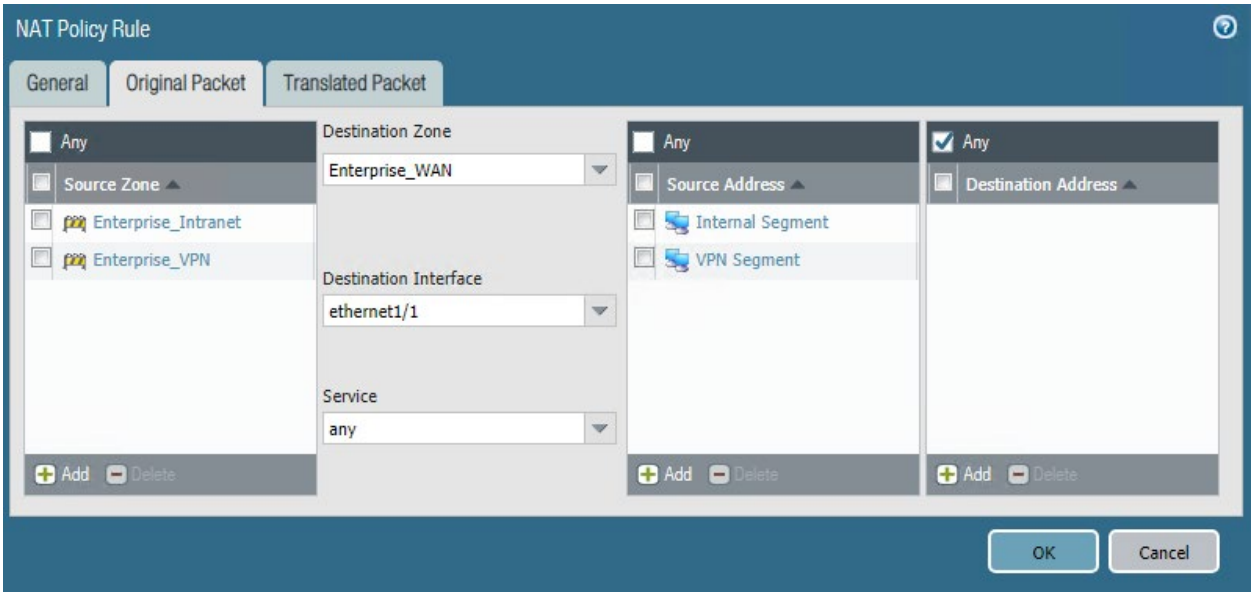
805 29. Once all devices are added, commit the changes.

806 30. Navigate to **Policies > NAT**.

807 31. Click **Add**.

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



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

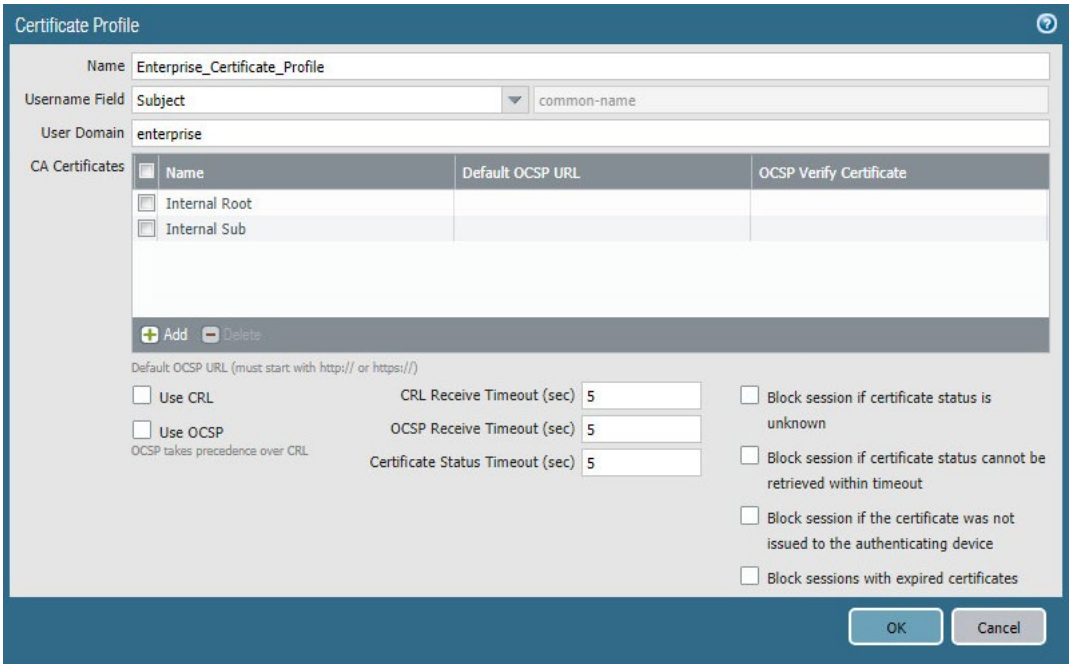
1. Navigate to **Policies > Security**.
2. Click **Add**.
3. Give the rule a meaningful name, such as Intranet Outbound.
4. Click **Source**. Click **Add** under **Source Zone** and set the source zone to be the internal network.
5. Click **Destination.** Click **Add** under **Destination Zone** and 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

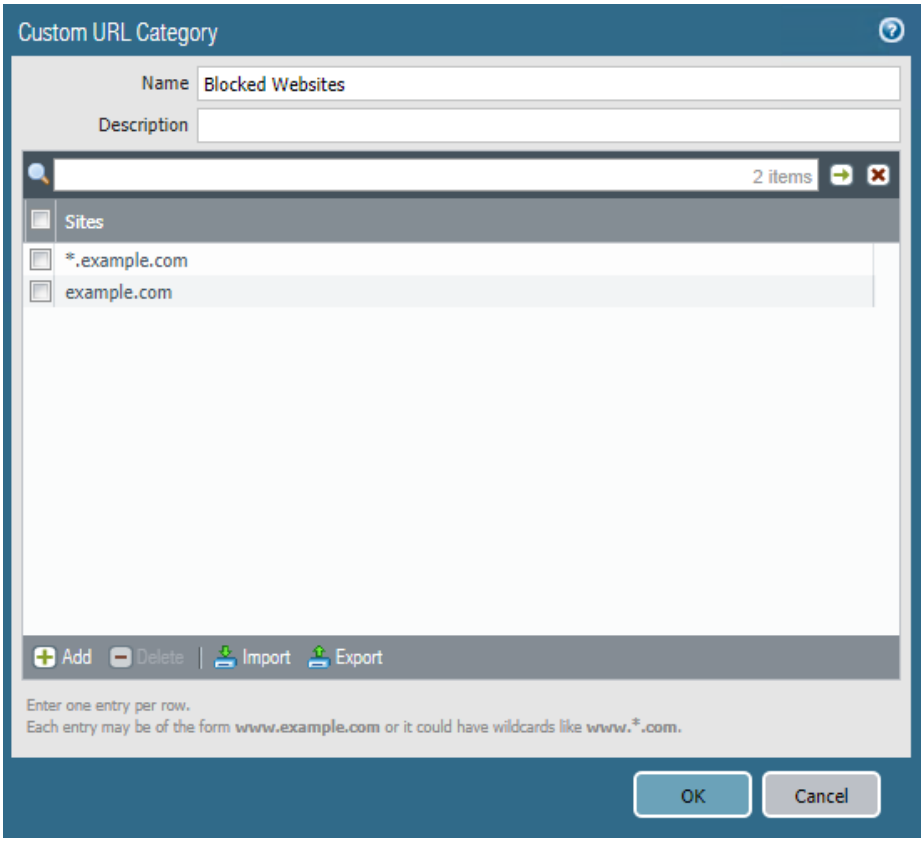


2.4.5 Website Filtering Configuration

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.

872 **Figure 2-26 Custom URL Category**



873 5. Click **OK**.

874 6. Navigate to **Objects > URL Filtering**.

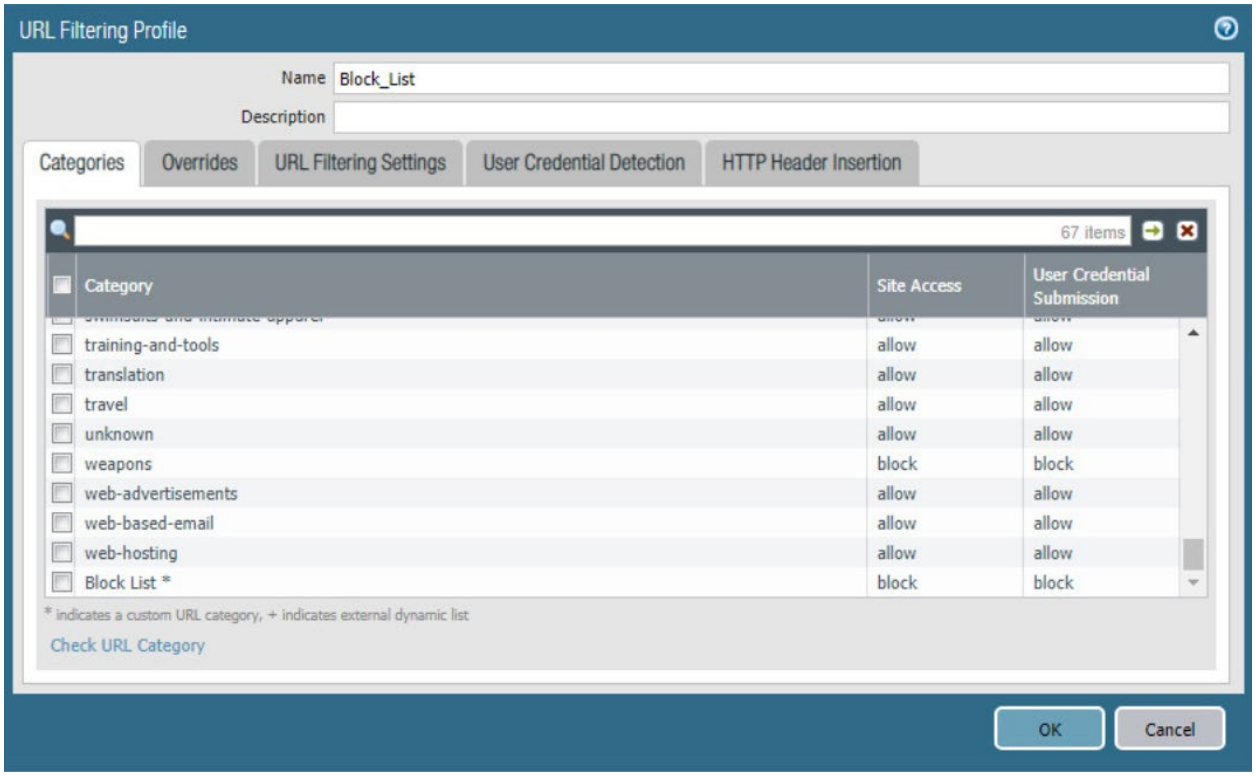
875 7. Click **Add**.

876 8. Give the filtering profile a name.

877 9. Scroll to the bottom of the categories table. The profile created in step 4 should be the last item
878 in the list, with an asterisk next to it. Click where it says **allow** and change the value to **block.**

879 10. Configure any additional categories to allow, alert, continue, block, or override.

880 **Figure 2-27 URL Filtering Profile**



881 11. Click **OK**.

882 12. Navigate to **Policies > Security**.

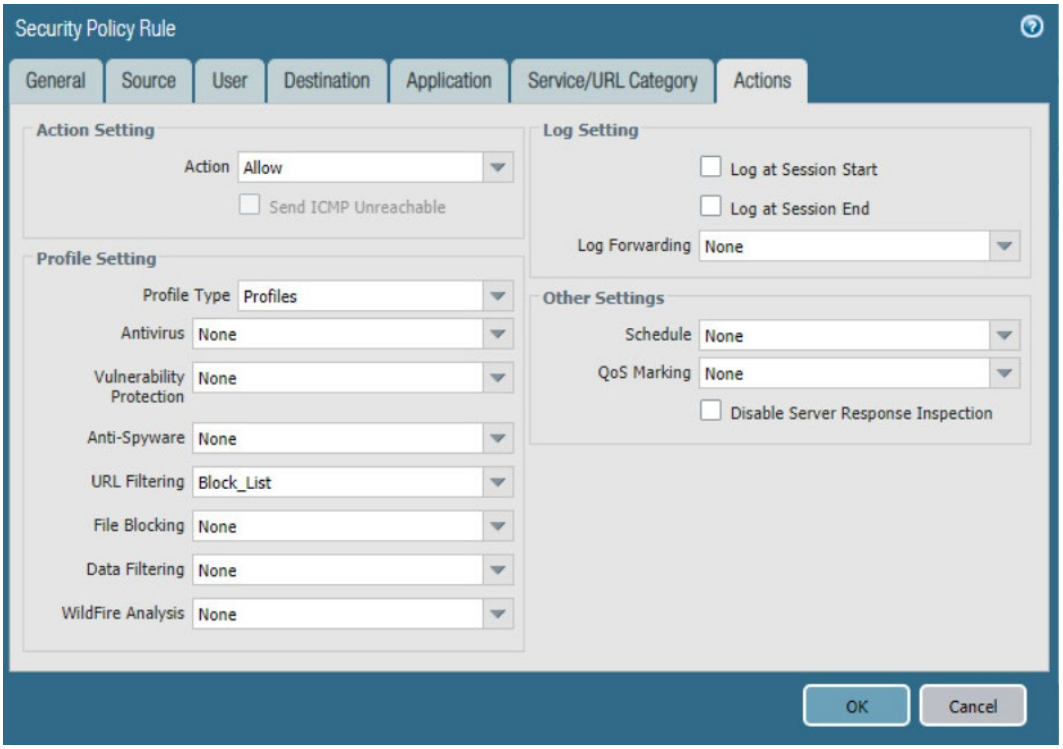
883 13. Select a policy to apply the URL filtering to.

884 14. Select **Actions**.

885 15. Next to **Profile Type,** select **Profiles**.

886 16. Next to **URL Filtering,** select the created URL filtering profile.

887 **Figure 2-28 URL Filtering Security Policy**



888 17. Click **OK.**

889 18. Repeat steps 13–17 for any policies which need the filtering profile applied.

890 19. Commit the changes.

891 *2.4.5.2 Configure SSL Website Blocking*

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

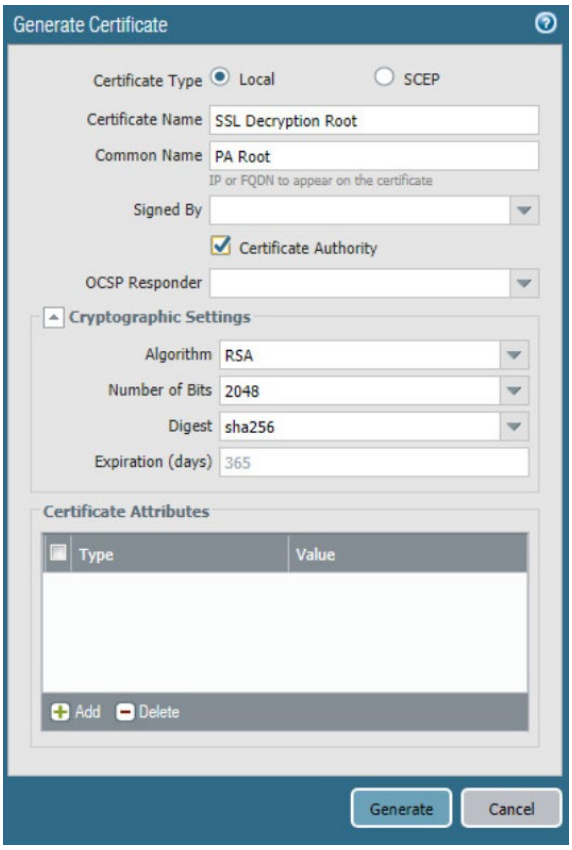
898 1. Navigate to **Device > Certificates**.

899 2. Click **Generate** on the bottom of the page.

900 3. Give the root certificate a name, such as SSL Decryption Root; and a common name (CN) such as
901 PA Root.

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

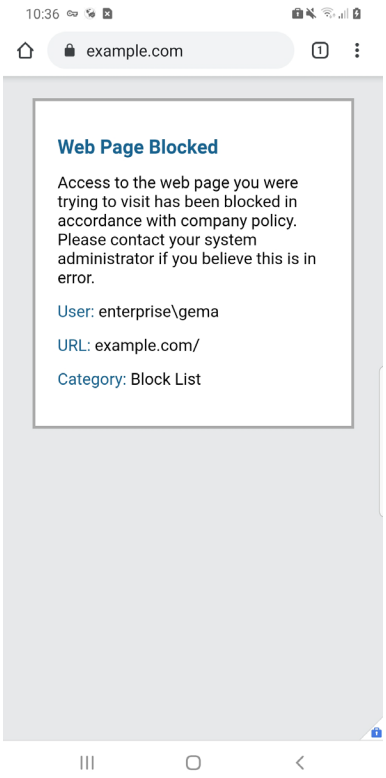
Figure 2-29 Generating the Root CA



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.

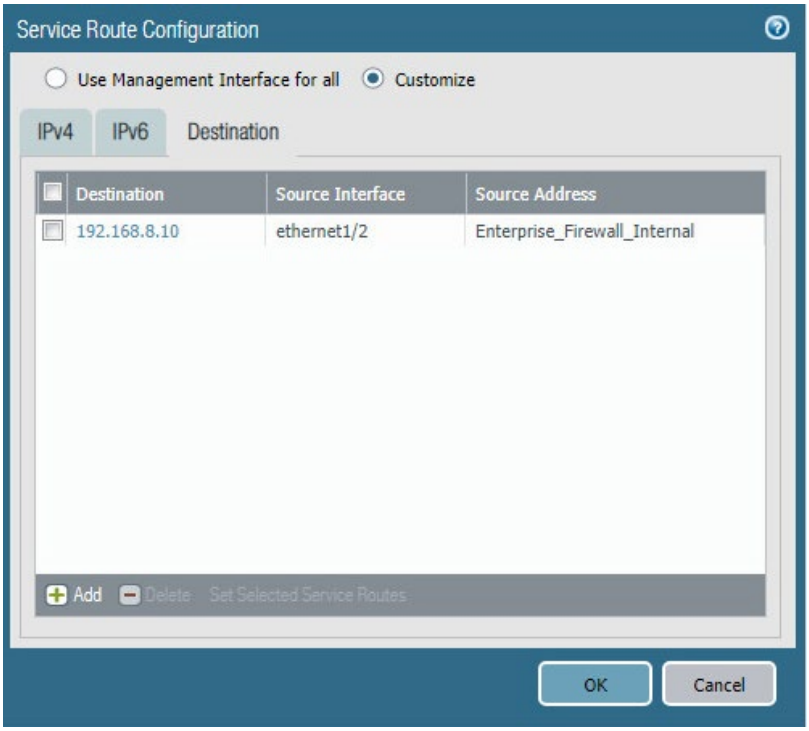
934 **Figure 2-30 Blocked Website Notification**



935 ## 2.4.6 User Authentication Configuration

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

943 **Figure 2-31 Service Route Configuration**



944 8. Navigate to **Device > Server Profiles > LDAP**.

945 9. Click **Add**.

946 10. Give the profile a meaningful name, such as Enterprise_LDAP_Server.

947 11. Click **Add** in the server list. Enter the name for the server and the IP.

948 12. Under **Server Settings,** set the **Type** drop-down to **active-directory**.

949 13. Enter the **Bind DN** and the password for the Bind DN.

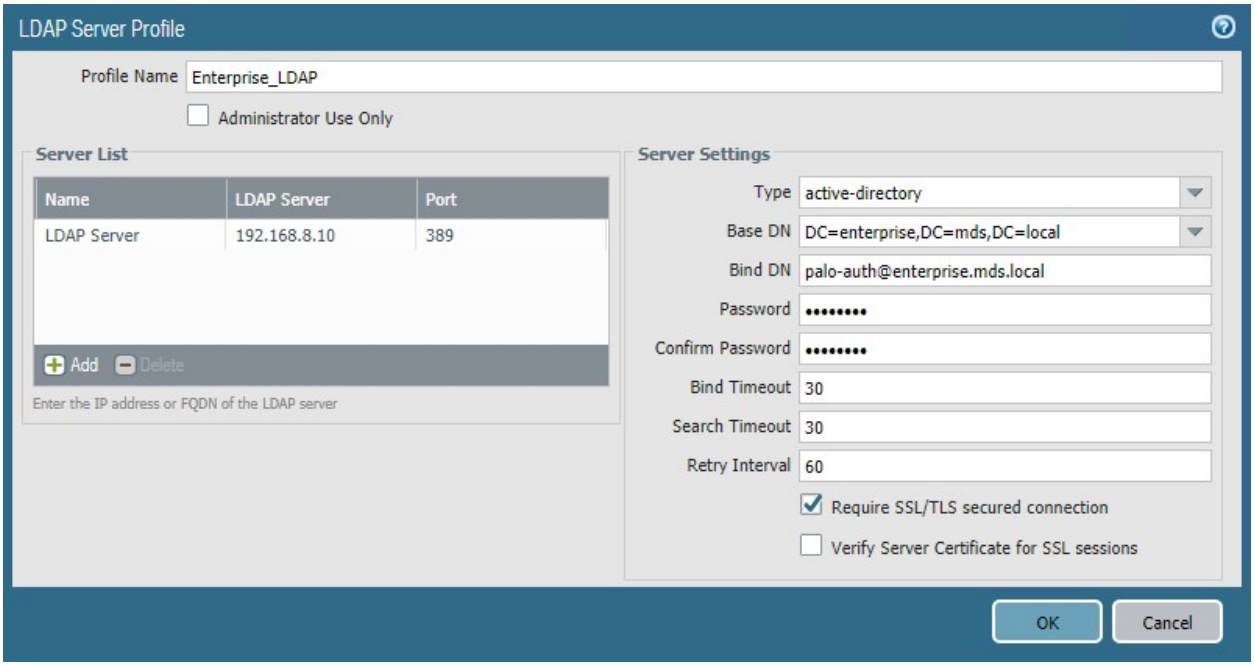
950 Note: In this implementation, a new user, palo-auth, was created in Active Directory. This user does not
951 require any special permissions or groups beyond the standard Domain Users group.

952 14. Ensure that **Require SSL/TLS secured connection** is checked.

953 15. Click the **down arrow** next to **Base DN**. If the connection is successful, the Base DN (Distin-
954 guished Name) should display.

955 16. Click **OK.**

956 **Figure 2-32 LDAP Server Profile**



957 17. Navigate to **Device > User Identification > Group Mapping Settings**.

958 18. Click **Add**.

959 19. Give the mapping a name, such as Enterprise_LDAP_Usermap.

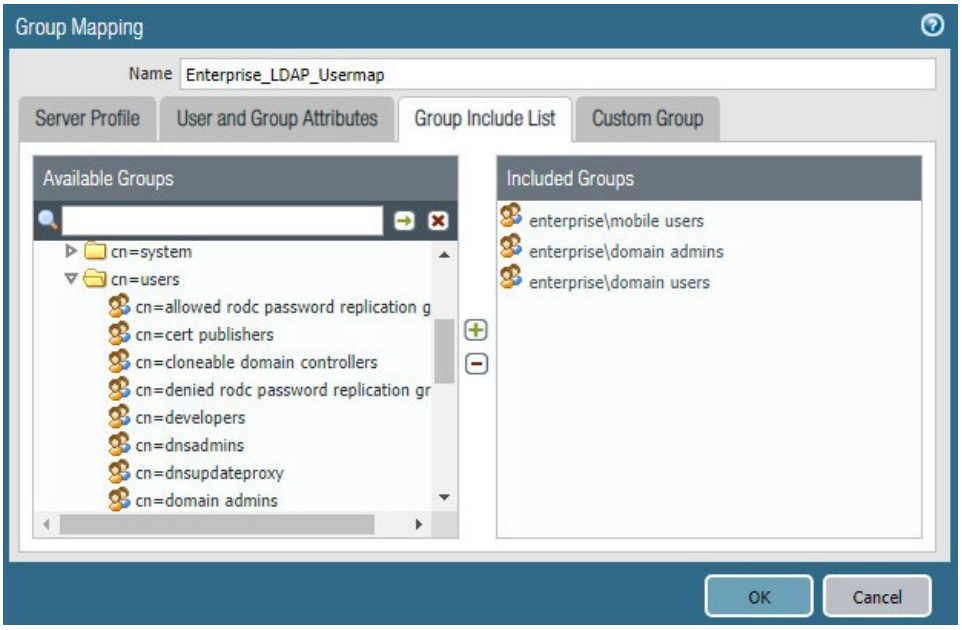
960 20. Select the **server profile,** and enter the **user domain—**in this case, Enterprise.

961 21. Click **Group Include List**.

962 22. Expand the arrow next to the **base DN** and then again next to **cn=users.**

963 23. For each group that should be allowed to connect to the VPN, click the proper **entry** and then
964 the **+ button.** In this example implementation, mobile users, domain users, and domain admins
965 were used.

966 **Figure 2-33 LDAP Group Mapping**



967 24. Click **OK**.

968 25. Navigate to **Device > Authentication Profile**.

969 26. Click **Add**.

970 27. Give the profile a meaningful name, such as Enterprise_Auth.

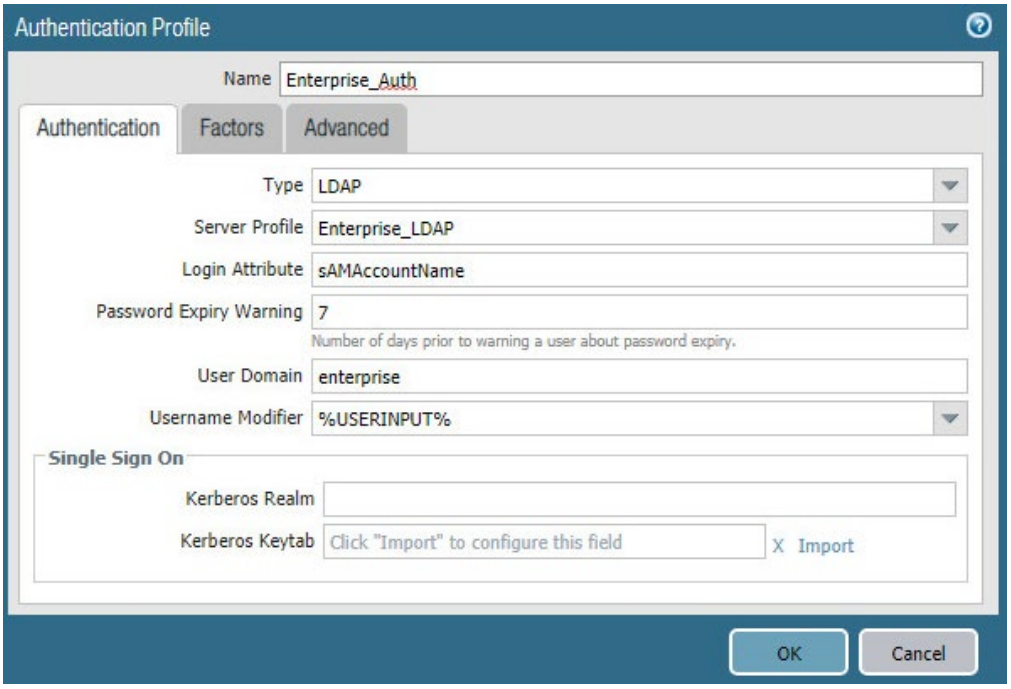
971 28. For the Type, select **LDAP**.

972 29. Select the newly created LDAP profile next to **Server Profile**.

973 30. Set the Login Attribute to be **sAMAcountName**.

974 31. Set the User Domain to be the **LDAP domain name**—in this case, **enterprise**.

975 **Figure 2-34 LDAP User Authentication Profile**



976 32. Click on **Advanced.**

977 33. Click **Add.** Select **enterprise\domain users.**

978 34. Repeat step 33 for **mobile users** and **domain admins.**

979 35. Click **OK.**

980 36. Commit the changes.

981 2.4.7 VPN Configuration

982 1. Navigate to **Network > Interfaces > Tunnel.**

983 2. Click **Add.**

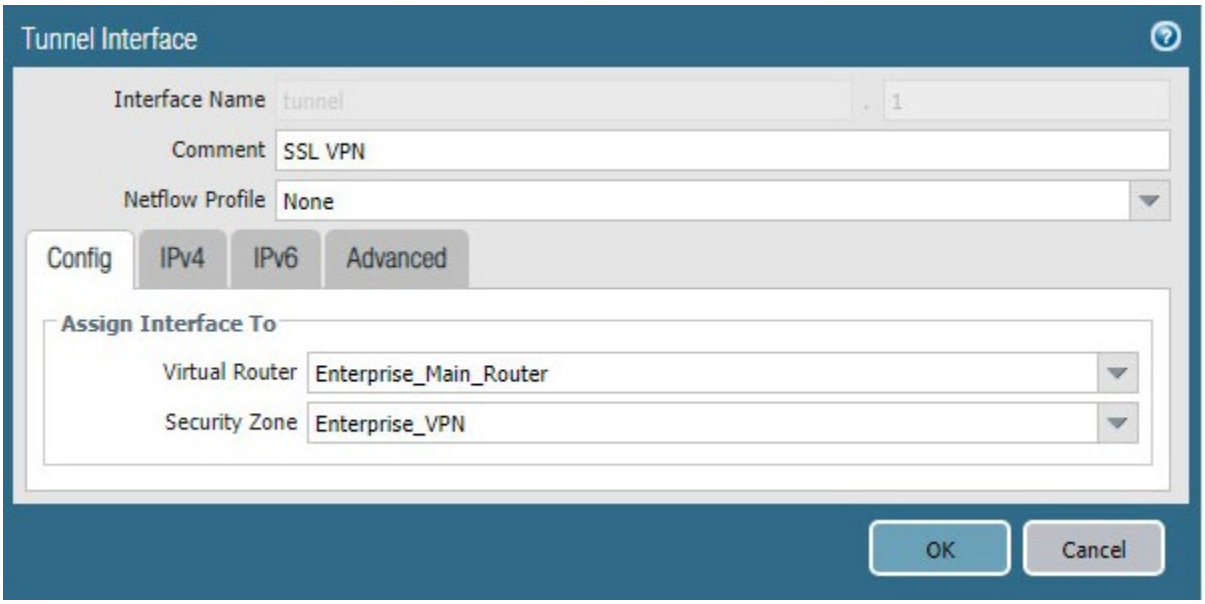
984 3. Enter a tunnel number. Assign it to the main virtual router. Click **OK.**

985 **Figure 2-35 Configured Tunnel Interfaces**

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

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



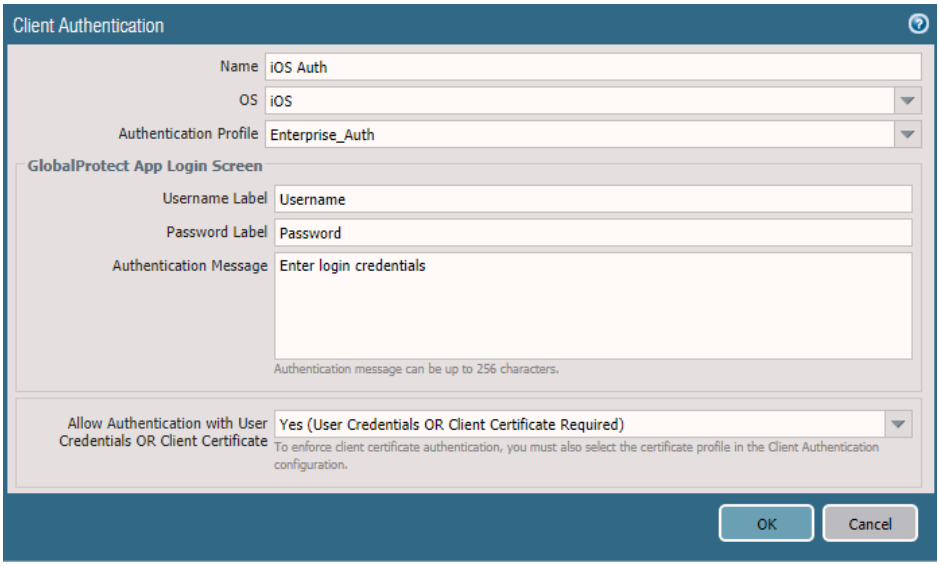
7. Commit the changes.
8. Navigate to **Policies > Authentication**.
9. Click **Add**.
10. Give the policy a **descriptive name**. For this example, the rule was named VPN_Auth.
11. Click **Source**.
12. Click **Add** and add the VPN and WAN zones.
13. Click **Destination**.
14. Check the **Any** box 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**.

1018 **Figure 2-37 GlobalProtect iOS Authentication Profile**



1019 14. Click **OK**.

1020 15. Click **Add** under **Client Authentication**.

1021 16. Give the object a meaningful name, such as Android Auth.

1022 17. Next to **OS,** select **Android**.

1023 18. Next to **Authentication Profile,** select the **created Authentication Profile**.

1024 19. Next to **Allow Authentication with User Credentials OR Client Certificate,** select **No**.

1025 20. Click **Agent**.

1026 21. Check the box next to **Tunnel Mode**.

1027 22. Select the **created tunnel interface** next to **Tunnel Interface**.

1028 23. Uncheck **Enable IPSec**.

1029 24. Click **Timeout Settings**.

1030 25. Set **Disconnect On Idle** to an organization defined time.

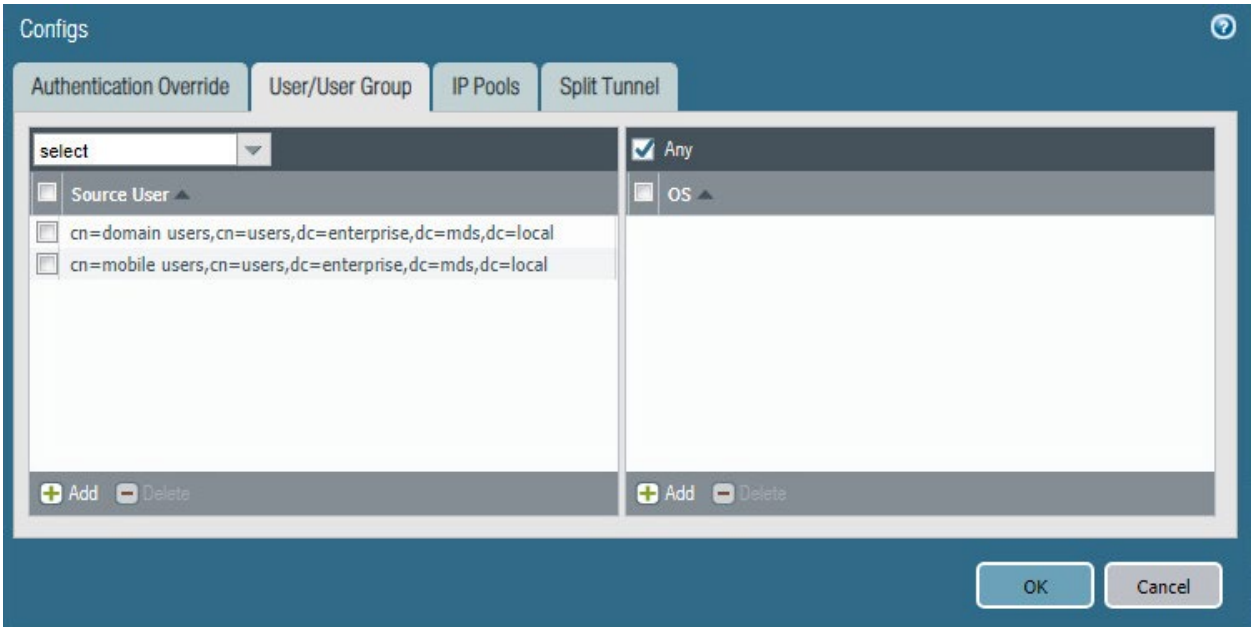
1031 26. Click **Client IP Pool**.

1032 27. Click **Add** and assign an IP subnet to the clients—in this case, **10.3.3.0/24**.

1033 28. Click **Client Settings**.

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.

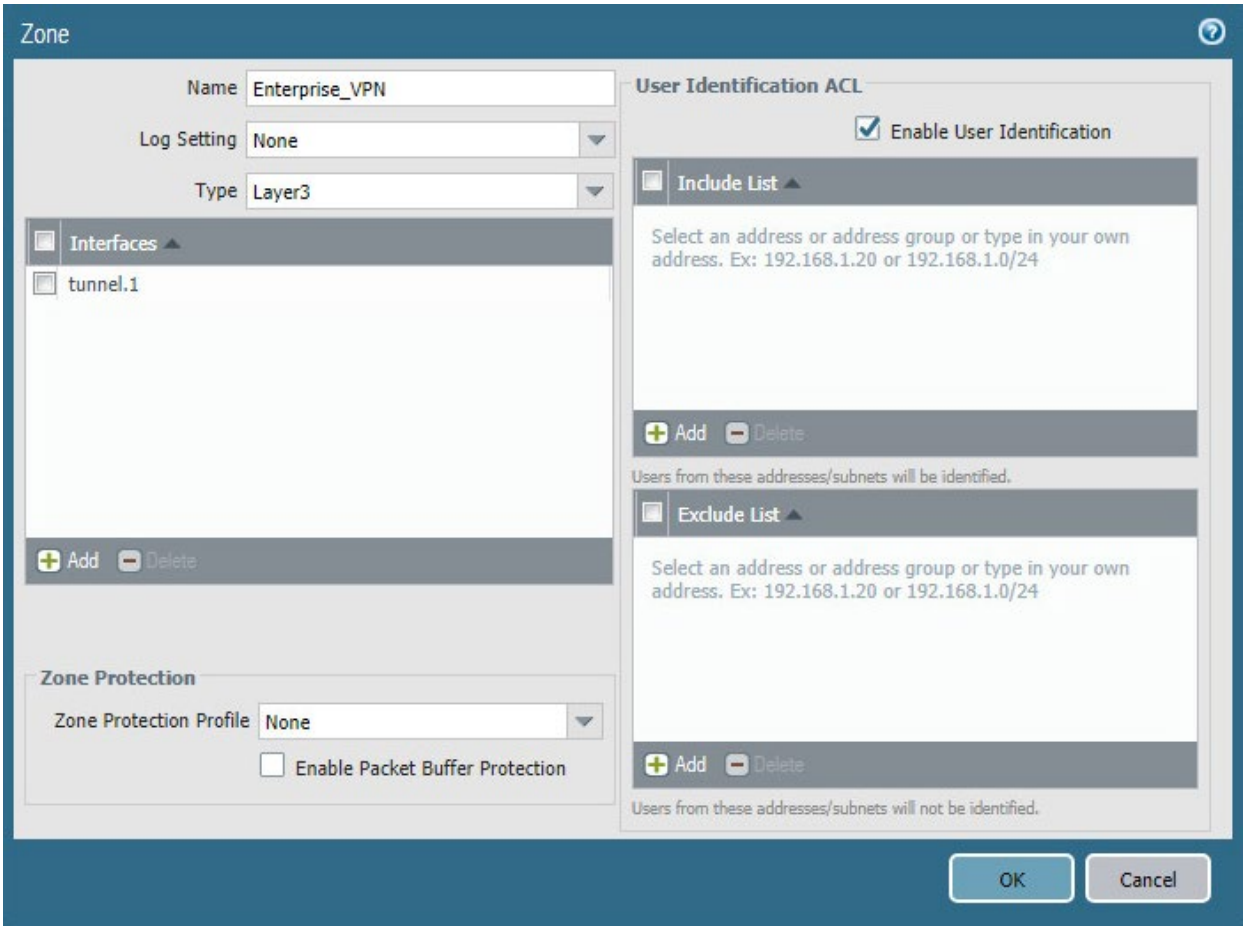
Figure 2-38 LDAP Authentication Group Configuration



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



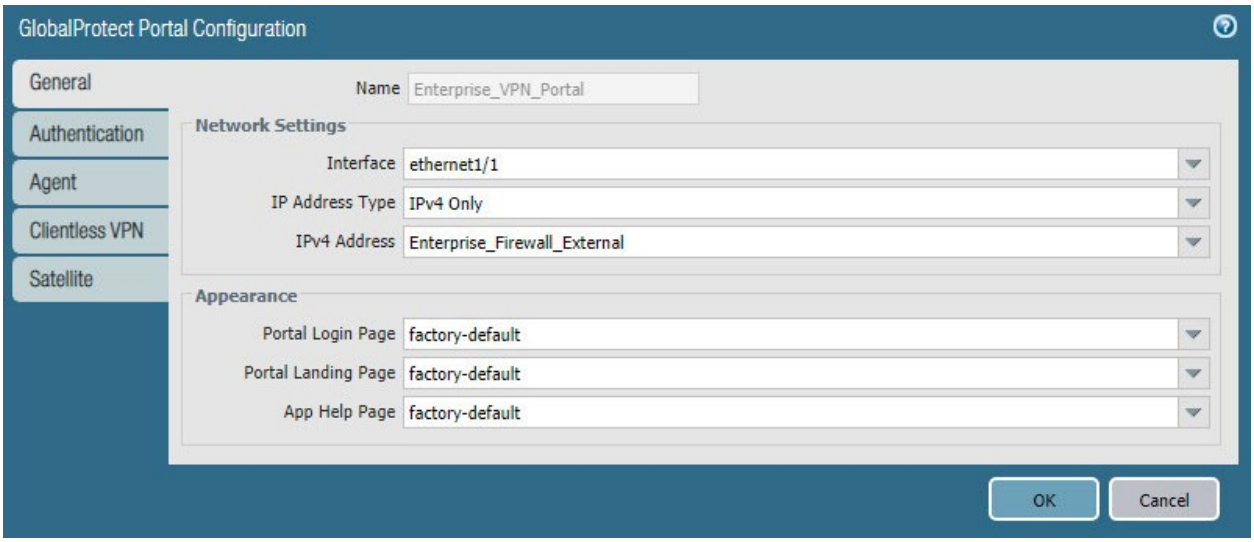
44. Click **OK**.
45. Commit the changes.

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.**

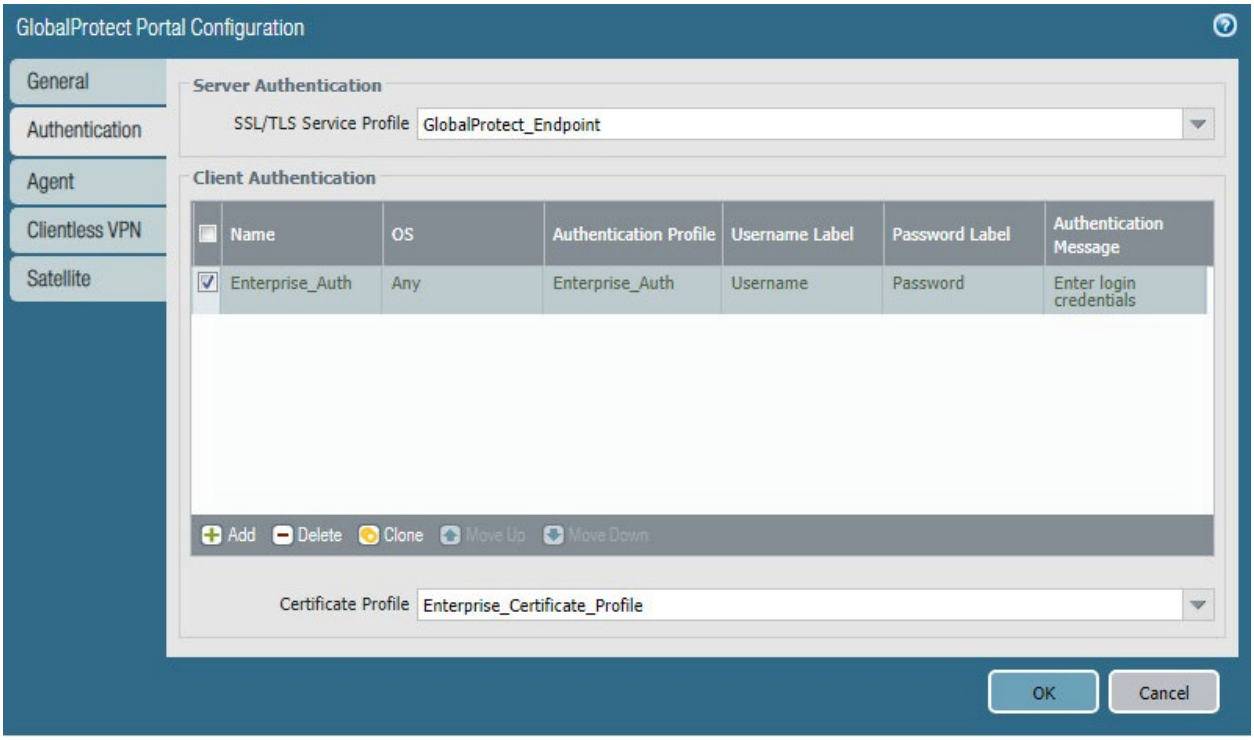
5. Set IP Address Type to **IPv4 Only**.
6. Set the IPv4 address to the firewall's **WAN address**.
7. Set all three appearance options to be **factory-default**.

Figure 2-40 GlobalProtect Portal General Configuration



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**.

1069 **Figure 2-41 GlobalProtect Portal Authentication Configuration**



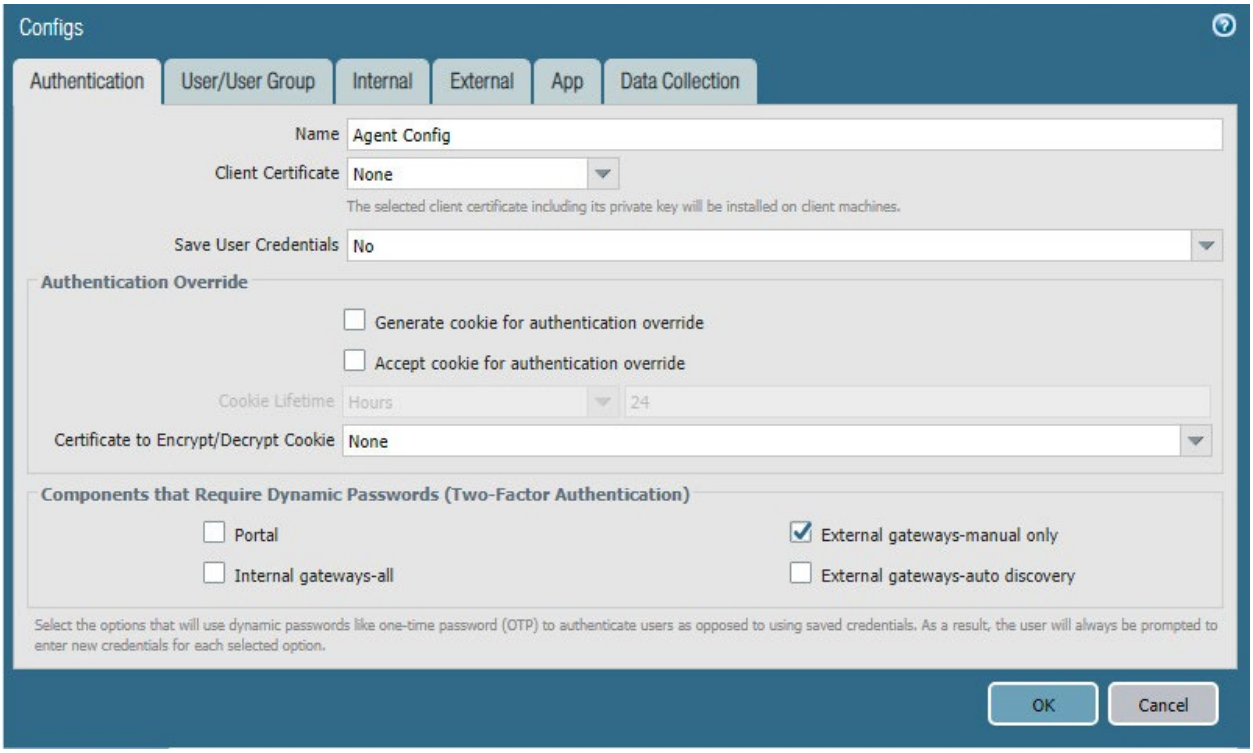
1070 14. Click **Agent** and click **Add** under **Agent**.

1071 15. Give the agent configuration a name.

1072 16. Ensure that the **Client Certificate** is set to **None**, and **Save User Credentials** is set to **No**.

1073 17. Check the box next to **External gateways-manual only**.

1074 **Figure 2-42 GlobalProtect Portal Agent Authentication Configuration**



1075 18. Click **External**.

1076 19. Click **Add** under **External Gateways**.

1077 20. Give the gateway a name and enter the fully qualified domain name (FQDN) of the VPN end
1078 point.

1079 21. Click **Add** under **Source Region** and select **Any**.

1080 22. Check the box next to **Manual**.

1081 23. Click **OK**.

1082 24. Click **App**.

1083 25. Under **App Configurations > Connect Method,** select **On-demand**.

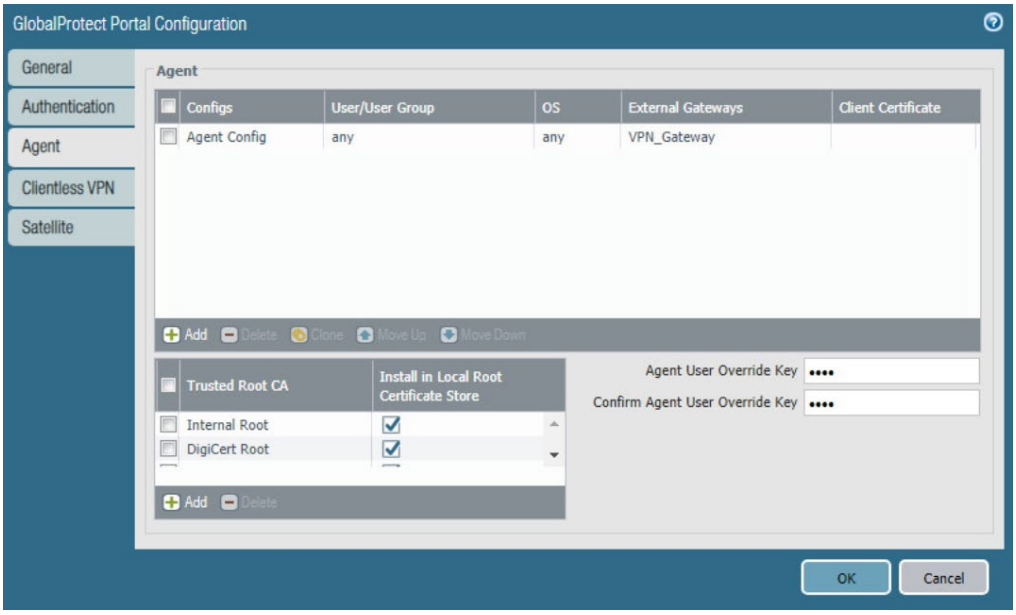
1084 26. Next to **Welcome Page,** select **factory-default**.

1085 27. Click **OK**.

1086 28. Click **Add** under **Trusted Root CA**.

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

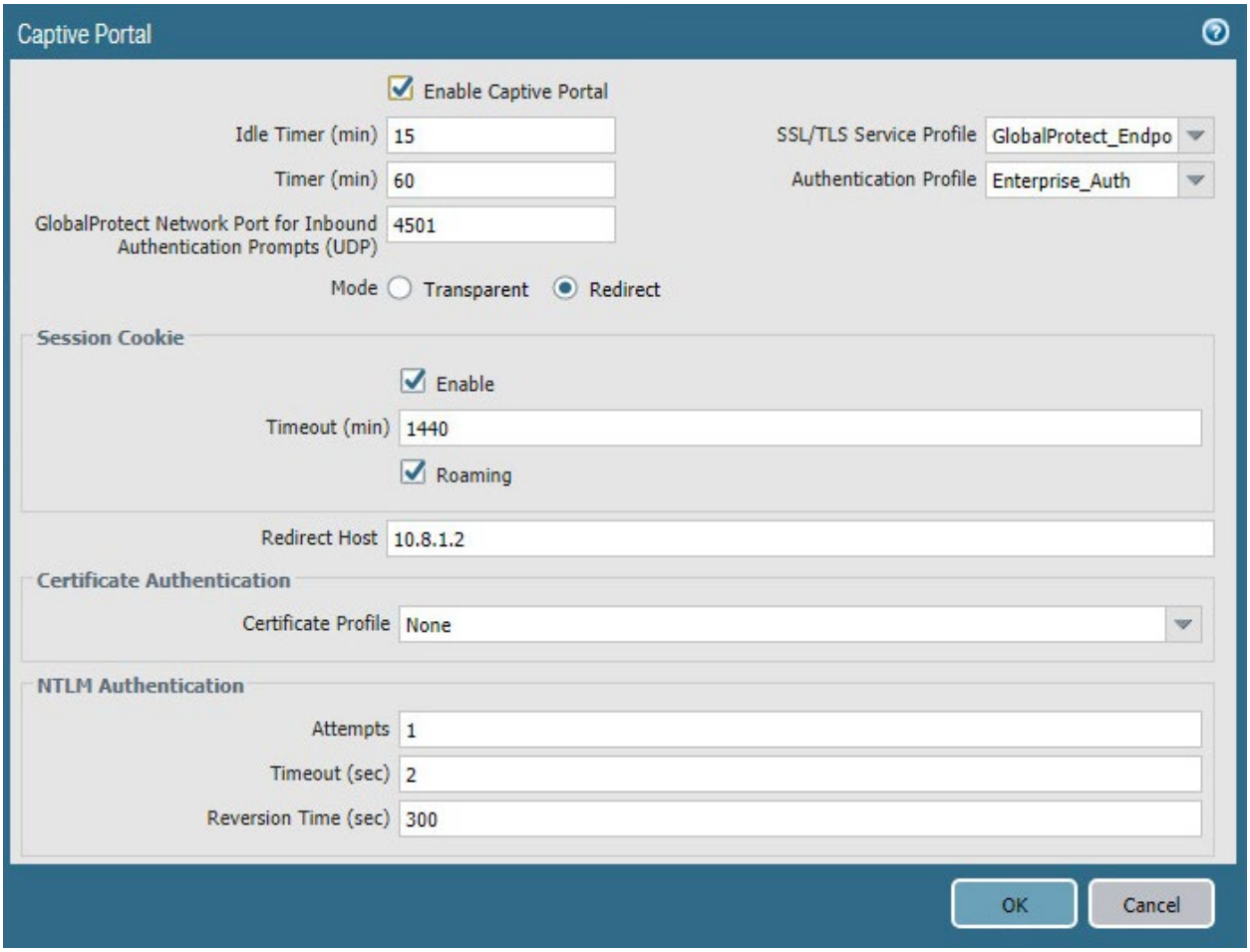


33. Click **OK.**

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**.

1102 **Figure 2-44 Captive Portal Configuration**



1103 6. Click **OK**.

1104 7. Commit the changes.

1105 ### *2.4.7.4 Activate the GlobalProtect Client*

1106 1. Navigate to **Device > GlobalProtect Client**.

1107 2. Acknowledge pop up messages.

1108 3. Click **Check Now** at the bottom of the page.

1109 4. Click **Download** next to the **first release** that comes up. In this implementation, version 5.0.2ate-
1110 was used.

1111 5. Click **Activate** next to the **downloaded release.**

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.

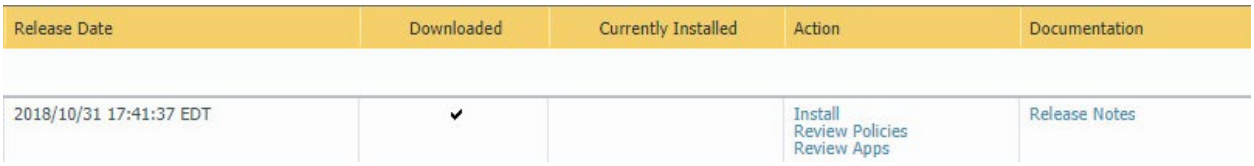
2.4.8 Enable Automatic Application and Threat Updates

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



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

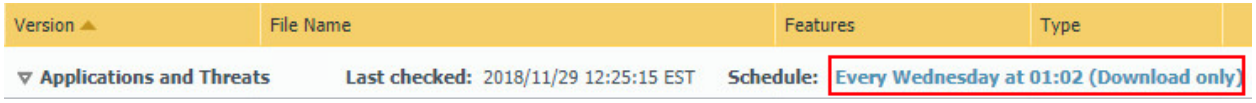
e. Click **Continue Installation,** leaving the displayed box unchecked. Installation will take a few minutes.

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

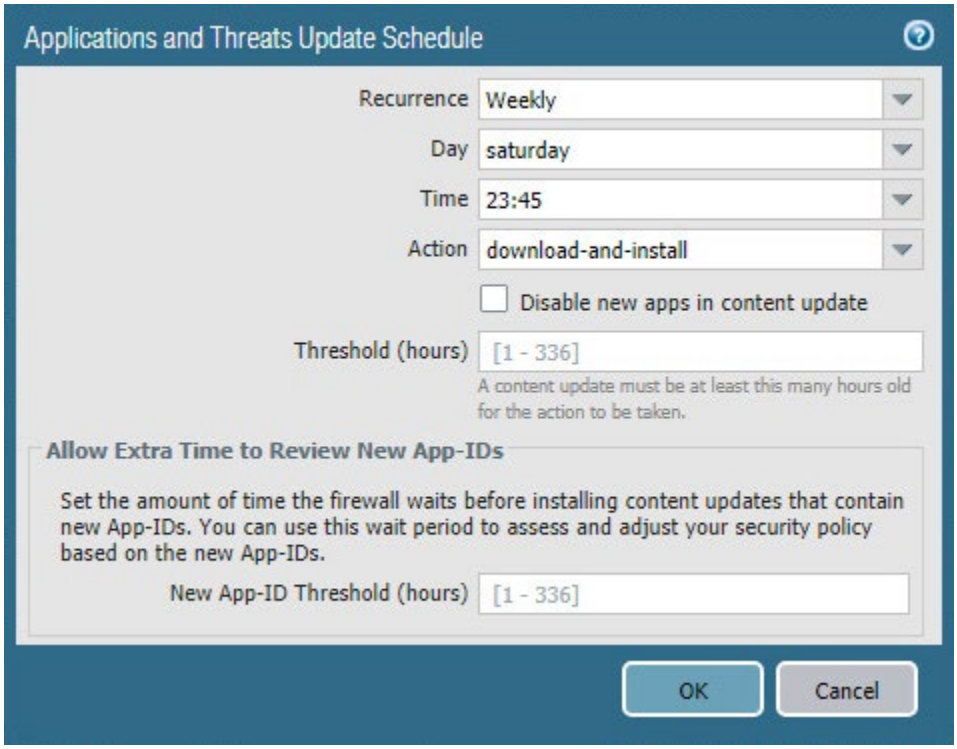


b. Select the **desired recurrence.** For this implementation, weekly was used.

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.**

1140 **Figure 2-48 Application and Threats Update Schedule**



1141 e. Click **OK.**

1142 f. Commit the changes.

1143 2.5 Kryptowire

1144 Kryptowire was used as an application vetting service via a custom active directory-integrated web
1145 application.

1146 2.5.1 Kryptowire and MaaS360 Integration

1147 1. Contact IBM support to provision API credentials for Kryptowire.

1148 2. Contact Kryptowire support to enable the MaaS360 integration, including the MaaS360 API cre-
1149 dentials.

1150 3. In the Kryptowire portal, click the **logged-in user's email address** in the upper right-hand corner
1151 of the portal. Navigate to **Settings > Analysis**.

1152 4. Set the **Threat Score Threshold** to the desired amount. In this sample implementation, 75 was
1153 used.

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

AD	Active Directory
API	Application Programming Interface
CA	Certificate Authority
CN	Common Name
DC	Domain Controller
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HKEY	Handle to Registry Key
HKLM	HKEY_LOCAL_MACHINE
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machines
IIS	Internet Information Services
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MDSE	Mobile Device Security for Enterprise
NCCoE	National Cybersecurity Center of Excellence
NDES	Network Device Enrollment Service
NIST	National Institute of Standards and Technology

OU	Organizational Unit
PKI	Public Key Infrastructure
SCEP	Simple Certificate Enrollment Protocol
SP	Special Publication
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network

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.

[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

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 Figures 2-49 and 2-50 which show how a contact created in a work profile cannot be seen by a personal profile. Also, Figures 2-51 and 2-52 show how a contact created in a managed application cannot be seen by an unmanaged application.

Figure 2-49 Contact Created in Work Profile

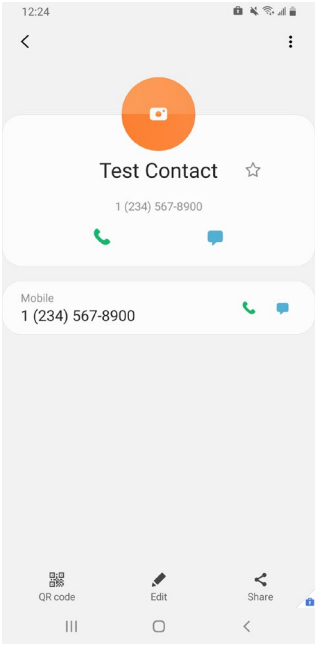


Figure 2-50 Personal Profile Can't See Work Contacts

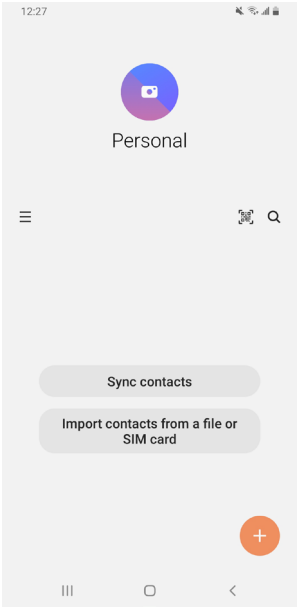


Figure 2-51 Contact Created in Managed App

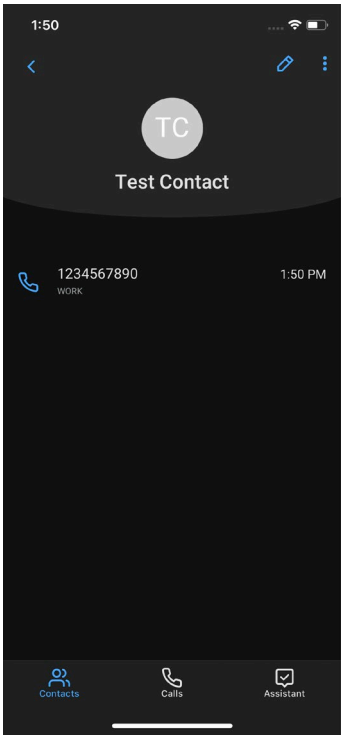
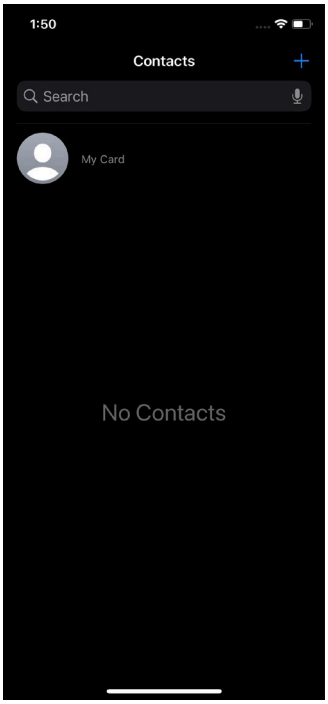


Figure 2-52 Unmanaged App Can't See Managed Contacts



D.2 Threat Event 2

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

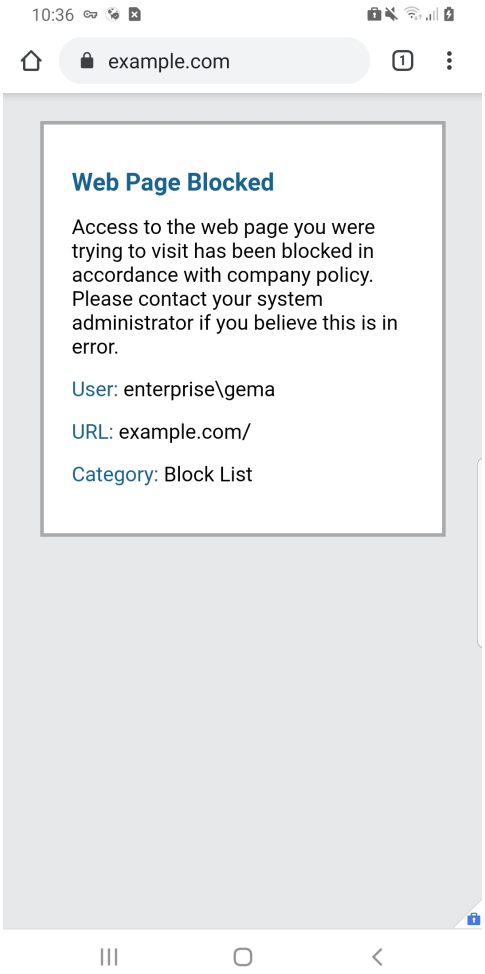
Test Activity:

- 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 2-53 shows the observed outcome of the phishing webpage being blocked from within the work profile.

1207 **Figure 2-53 Fictitious Phishing Webpage Blocked**



1208

1209 D.3 Threat Event 3

1210 **Summary:** Confidentiality and integrity loss due to the exploitation of a known vulnerability in the
1211 operating system or firmware.

1212 **Test Activity:** Attempt to access enterprise resources from a mobile device with known vulnerabilities
1213 (e.g., running an older, unpatched version of iOS or Android).

1214 **Desired Outcome:** The enterprise's security architecture should identify the presence of devices that are
1215 running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be
1216 possible, when warranted by the risks, to block devices from accessing enterprise resources until system
1217 updates are installed.

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 2-54 and 2-55 shows the security architecture identifying the presence of outdated operating systems.

Figure 2-54 iOS MaaS360 OS Compliance Alert

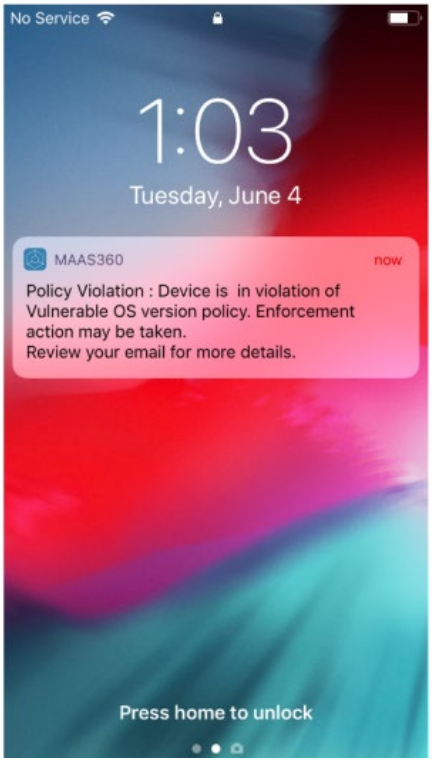
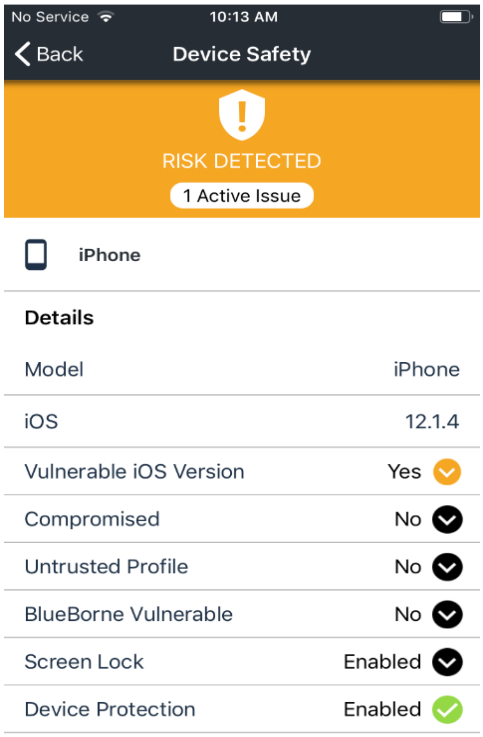


Figure 2-55 Zimperium Risk Detected



D.4 Threat Event 4

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

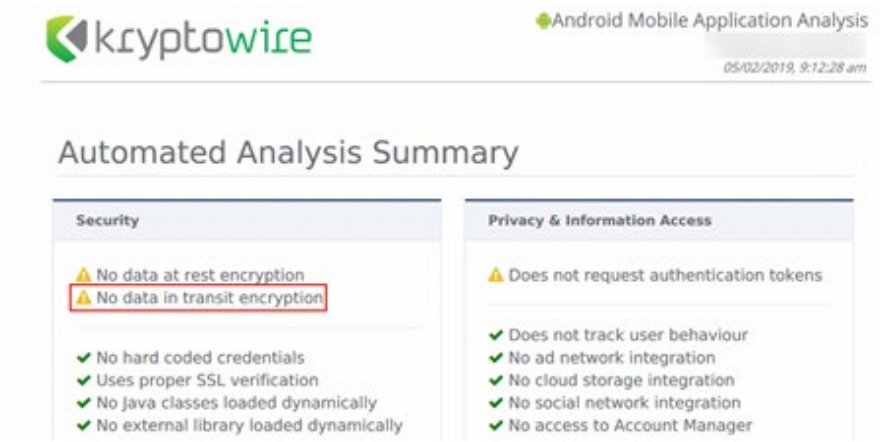
Test Activity: Test if applications will attempt to establish a hypertext transfer protocol or unencrypted connection.

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 2-56 shows the analysis summary finding of no in transit data encryption in use.

Figure 2-56 Kryptowire Application Report



D.5 Threat Event 5

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 lockscreen 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. Figures 2-57 through 2-59 show the passcode and lockscreen configuration settings.

Figure 2-57 Android Passcode Configuration

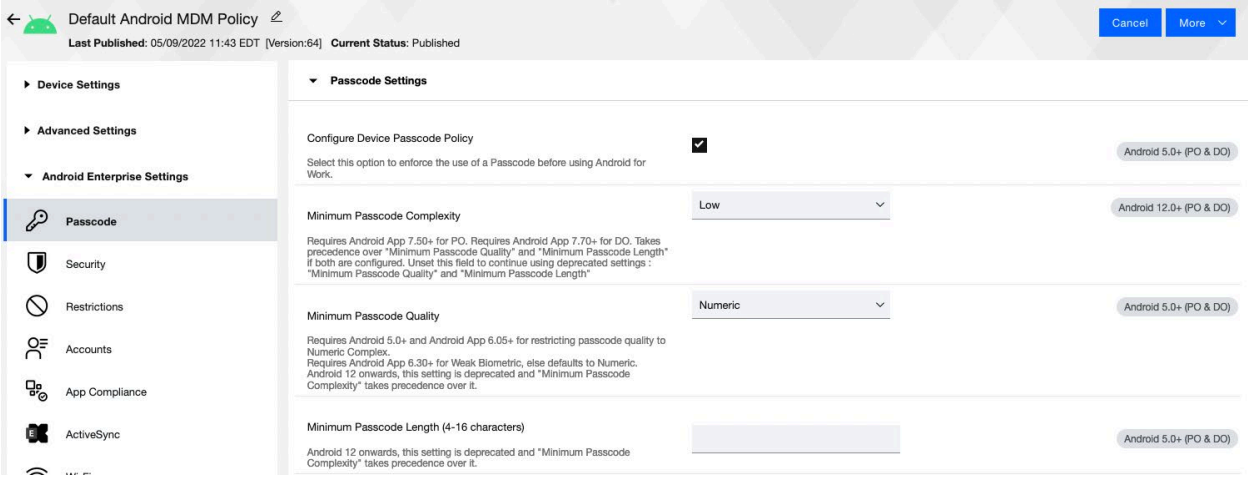
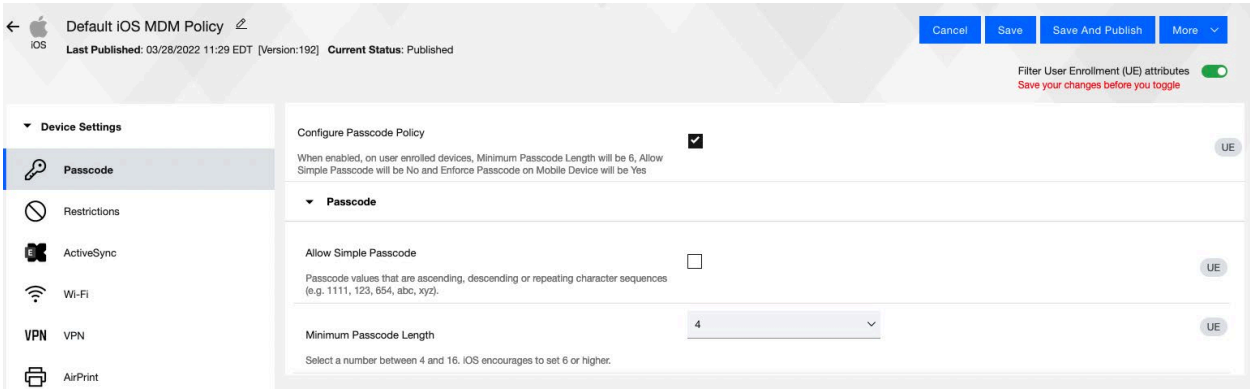
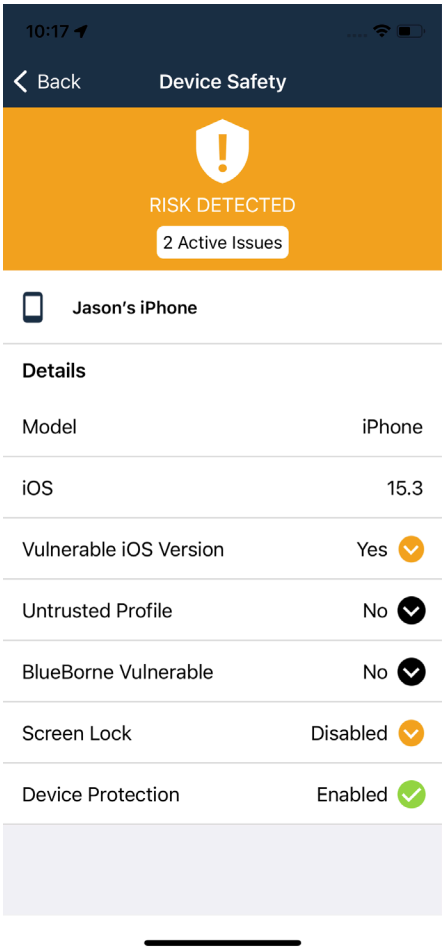


Figure 2-58 iOS Passcode Configuration



1260 **Figure 2-59 Zimperium Detecting Disabled Lockscreen**



1261 ## D.6 Threat Event 6

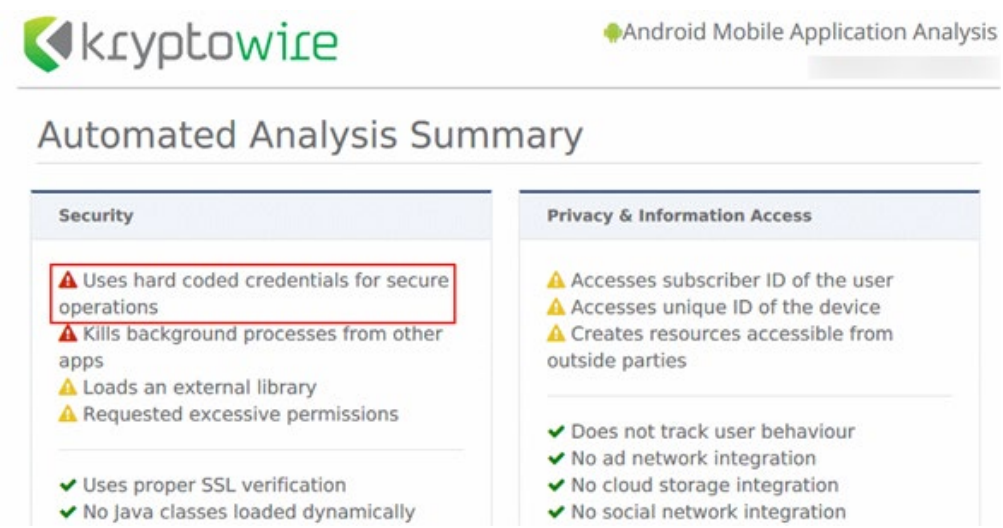
1262 **Summary:** Unauthorized access to backend services via authentication or credential storage
1263 vulnerabilities in internally developed applications.

1264 **Test Activity:** Application was submitted to Kryptowire for analysis of credential weaknesses.

1265 **Desired Outcome:** Discover and report credential weaknesses.

1266 **Observed Outcome:** Kryptowire recognized that the application uses hardcoded credentials. The
1267 application's use of hardcoded credentials could introduce vulnerabilities if unauthorized entities used
1268 the hardcoded credentials to access enterprise resources. Figure 2-60 shows the discovery of hardcoded
1269 credentials.

1270 **Figure 2-60 Application Report with Hardcoded Credentials**



1271 D.7 Threat Event 7

1272 **Summary:** Unauthorized access of enterprise resources from an unmanaged and potentially
1273 compromised device.

1274 **Test Activity:** Attempt to directly access enterprise services, e.g., Exchange email server or corporate
1275 VPN, on a mobile device that is not enrolled in the EMM system.

1276 **Desired Outcome:** Enterprise services should not be accessible from devices that are not enrolled in the
1277 EMM system. Otherwise, the enterprise is not able to effectively manage devices to prevent threats.

1278 **Observed Outcome:** Devices that were not enrolled in MaaS360 were unable to access enterprise
1279 resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper
1280 client certificates—obtainable only through enrolling in the EMM. Figures 2-61 through 2-63 show the
1281 desired outcome of the VPN gateway protecting the enterprise.

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

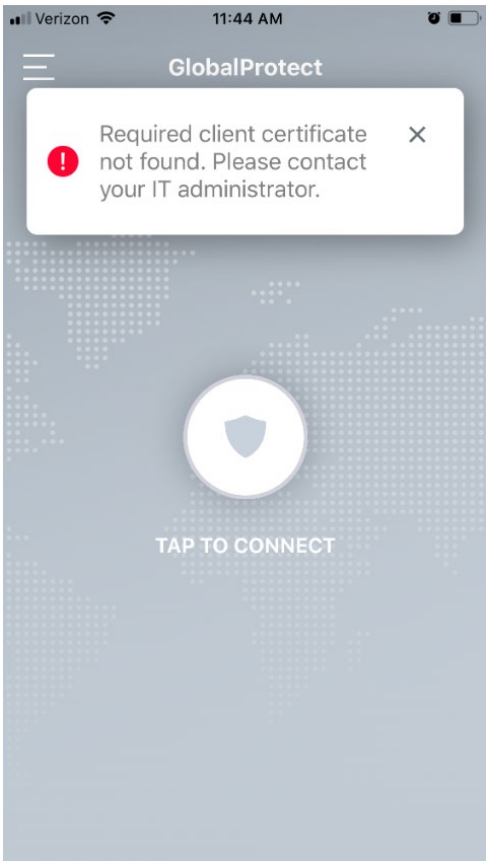
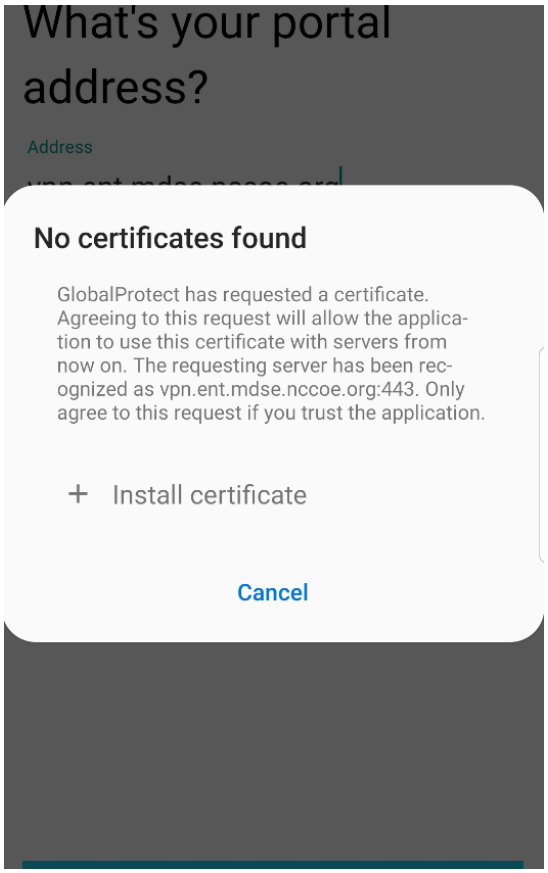
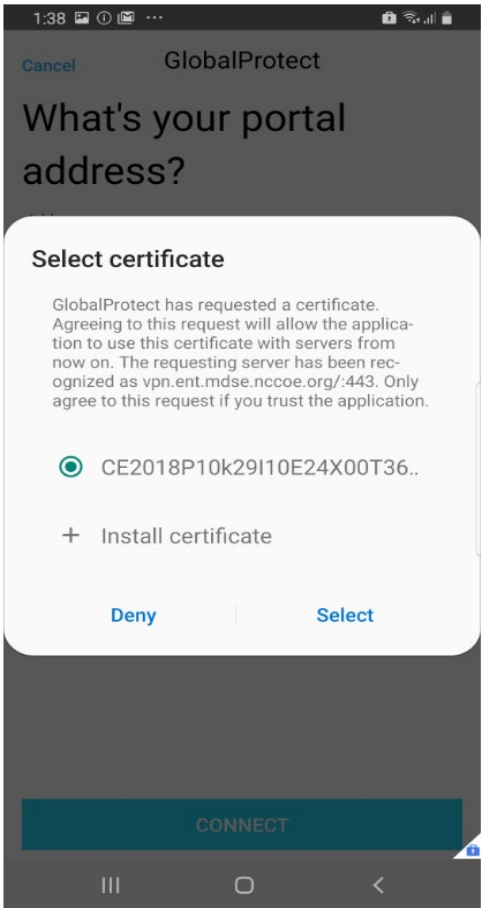


Figure 2-62 Attempting to Access the VPN on an Unmanaged Android Device



1282 **Figure 2-63 Attempting to Access the VPN on a Managed Android Device**



1283 D.8 Threat Event 8

1284 **Summary:** Loss of organizational data due to a lost or stolen device.

1285 **Test Activity:** Attempt to download enterprise data onto a mobile device that is not enrolled in the
1286 EMM system (may be performed in conjunction with TE-7). Attempt to remove (in conjunction with TE-
1287 5) the screen lock passcode or demonstrate that the device does not have a screen lock passcode in
1288 place. Attempt to locate and selectively wipe the device through the EMM console (will fail if the device
1289 is not enrolled in the EMM).

1290 **Desired Outcome:** It should be possible to locate or wipe EMM enrolled devices in response to a report
1291 that they have been lost or stolen. As demonstrated by TE-7, only EMM enrolled devices should be able
1292 to access enterprise resources. As demonstrated by TE-5, EMM enrolled devices can be forced to have a

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. Figures 2-64 through 2-67 show the removal of only organization data using selective wipe features.

Figure 2-64 Selective Wiping a Device

1309 **Figure 2-65 Selective Wipe Complete**

Applied Policy	MDM: Default iOS MDM Policy (192) WorkPlace Persona: WorkPlace Persona Policy (9)
Jailbroken/Rooted	No
Selective Wipe Status	Completed (05/23/2022 14:28 EDT)
Passcode Status	MDM:Compliant WorkPlace: Enabled
Rules Compliance Status	In Compliance
Rule Set Name	Zimperium - Critical

Figure 2-66 Corporate Data Removal Confirmation Notification on iOS

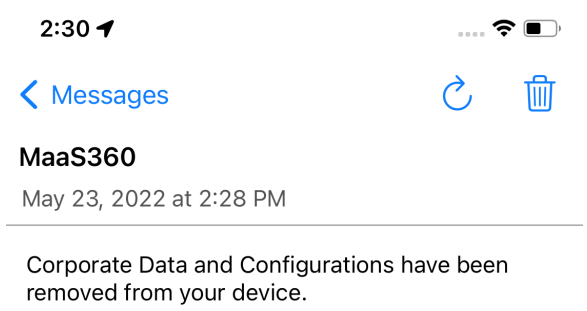
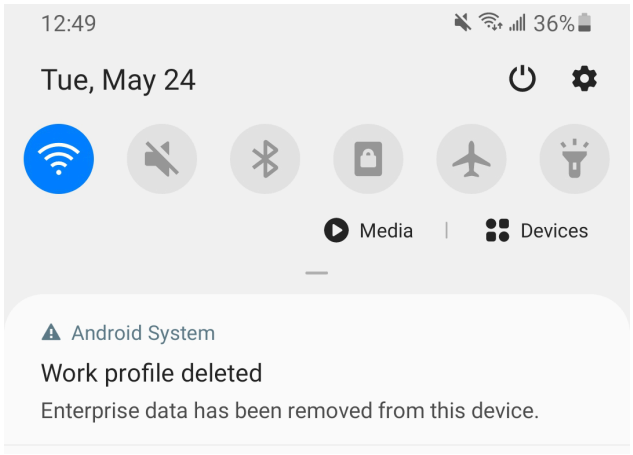


Figure 2-67 Work Profile Removal Notification on Android



1310 D.9 Threat Event 9

1311 **Summary:** Loss of confidentiality of organizational data due to its unauthorized storage in non-
1312 organizationally managed services.

1313 **Test Activity:** Connect to the enterprise VPN. Open an enterprise website or application. Attempt to
1314 extract enterprise data by taking a screenshot, or copy/paste and send it via an unmanaged email
1315 account.

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

Observed Outcome: As shown in Figures 2-68 through 2-70, MaaS360 device policies prevented the following actions on BYOD managed phones:

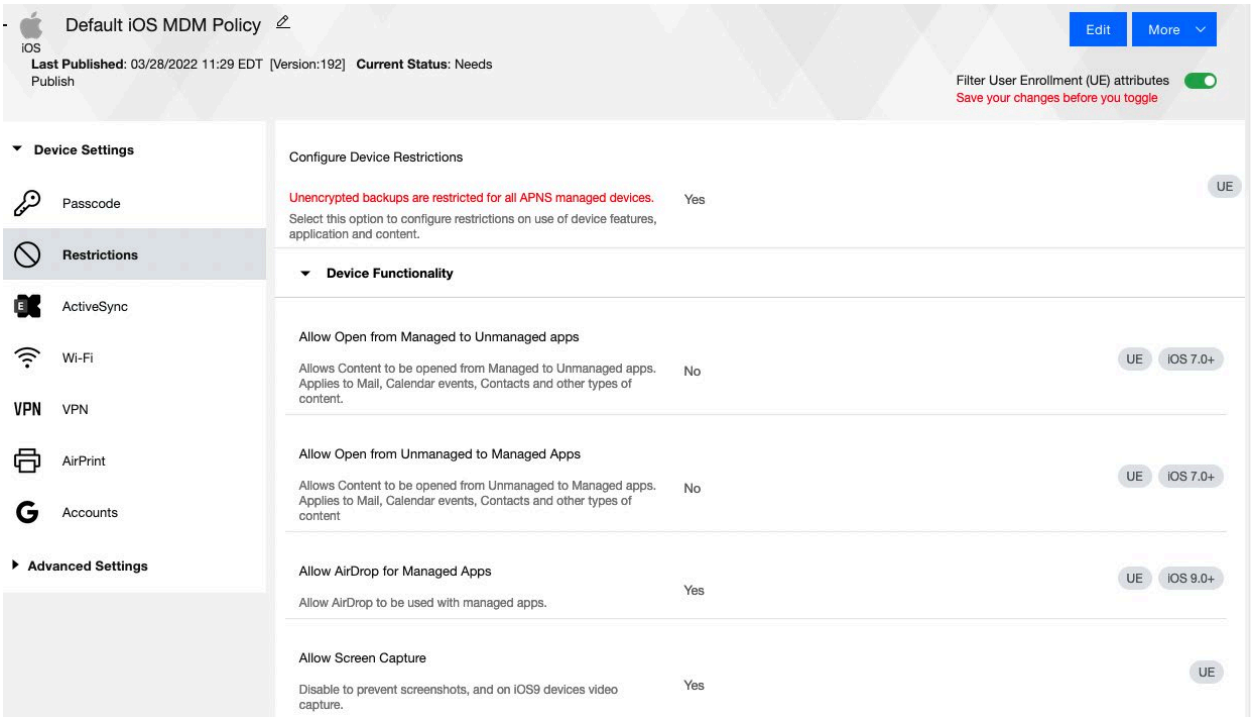
Android

- 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

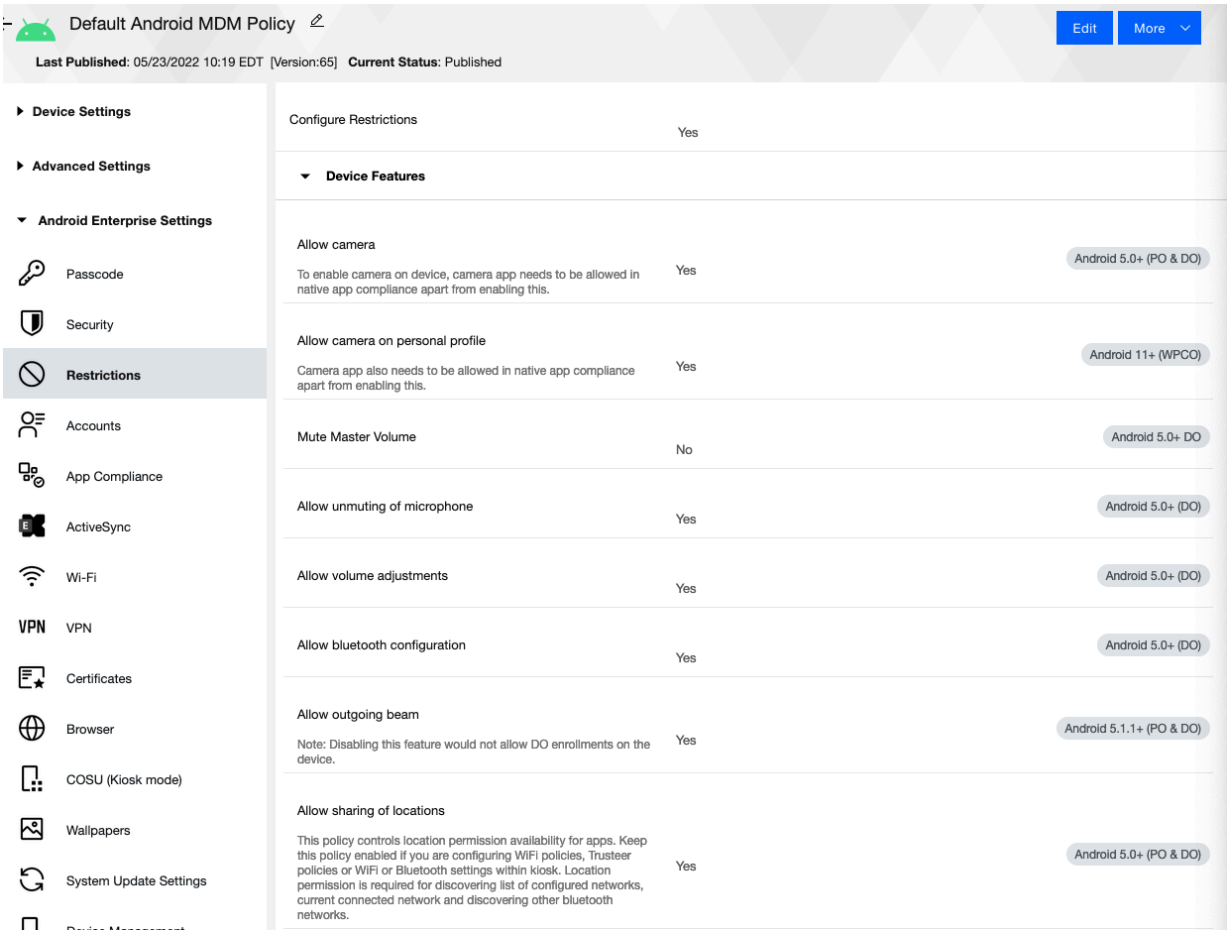
iOS

- 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

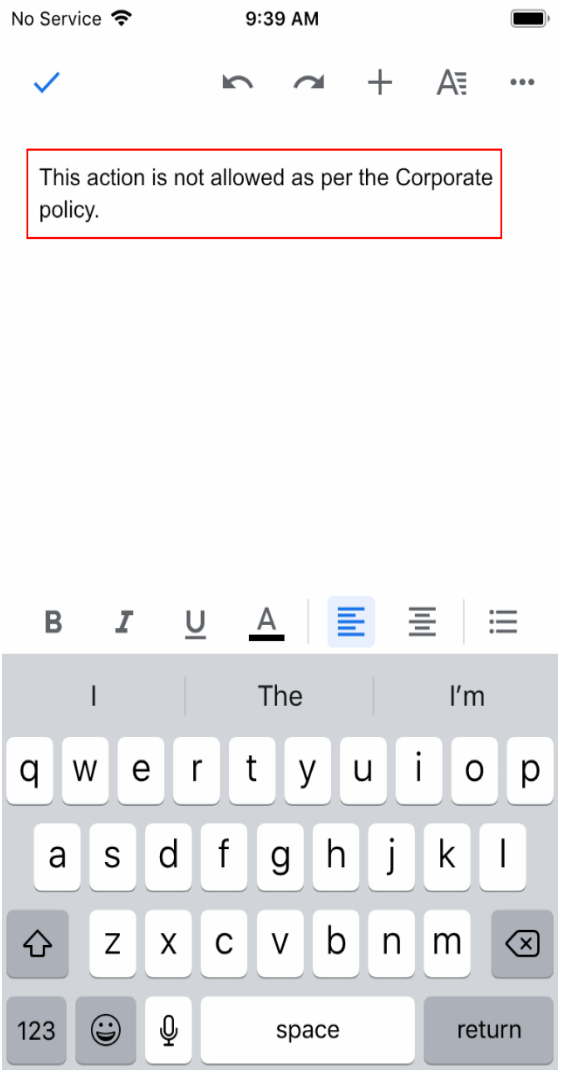
1341 **Figure 2-68 iOS DLP Configuration Options**



1342 **Figure 2-69 Android DLP Configuration**



1343 **Figure 2-70 Attempting to Paste Text on iOS Between Unmanaged and Managed Apps**



1344 D.10 Privacy Risk 1 – Wiping Activities on the User's Device May 1345 Inadvertently Delete the User's Personal Data

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

1348 **Test Activity:** Selectively wipe a device using MaaS360; restrict staff access to performing wiping of work
1349 profile data.

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 not 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 work profile wiping. Figure 2-71 shows initiation of a selective wipe. The selective wipe will remove the Mail Server account and all corporate settings available to the device.

Figure 2-71 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 Users to Feeling or Being Surveilled

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

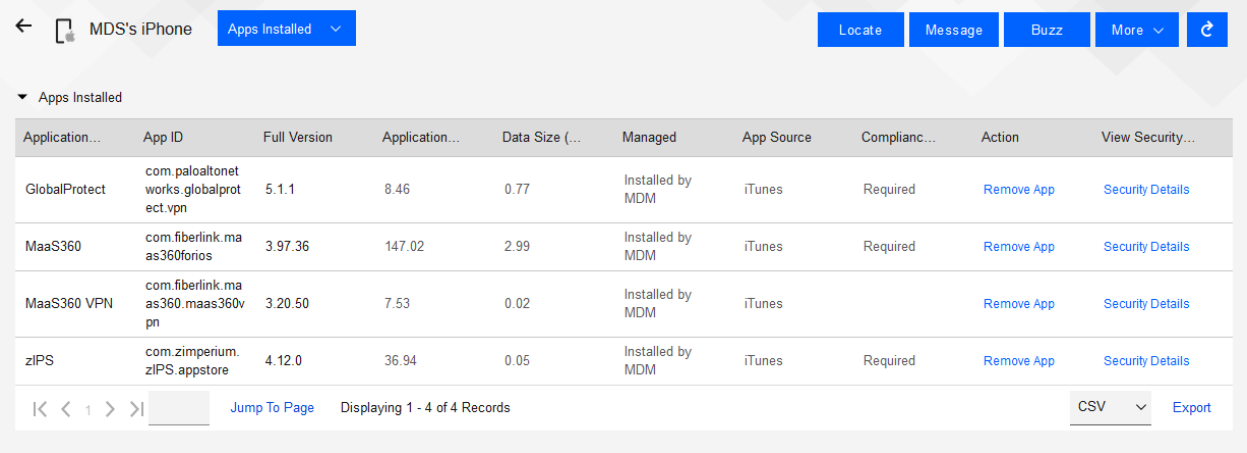
Test Activity: Disable location tracking and verify that applications outside of the organizationally controlled portions of the phone are not inventoried by the EMM.

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 are restricted by OS-level controls.

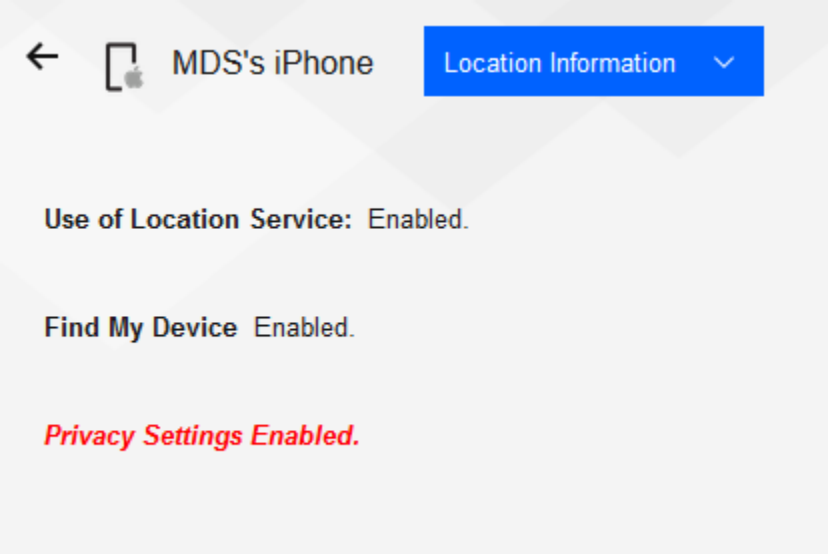
Figure 2-72 shows inventory information for **installed** applications**.** When privacy restrictions are configured, only corporate application inventory information is collected. No personal applications are found in the EMM's installed applications list.

Figure 2-72 Application Inventory Information



The following figure shows that privacy settings have been enabled to restrict collection of location information.

1383 **Figure 2-73 Location Information Restricted**



1384 **Additional Potential Mitigations:**

1385 • Restrict staff access to system capabilities that permit reviewing data about employees and their
1386 devices.
1387 • Limit or disable collection of specific data elements.
1388 • Dispose of personally identifiable information (PII).

1389 D.12 Privacy Risk 3 - Mobile security services may not alert users to what
1390 information is collected

1391 **Summary:** Users may not have knowledge of what information is collected and monitored by the
1392 organization.

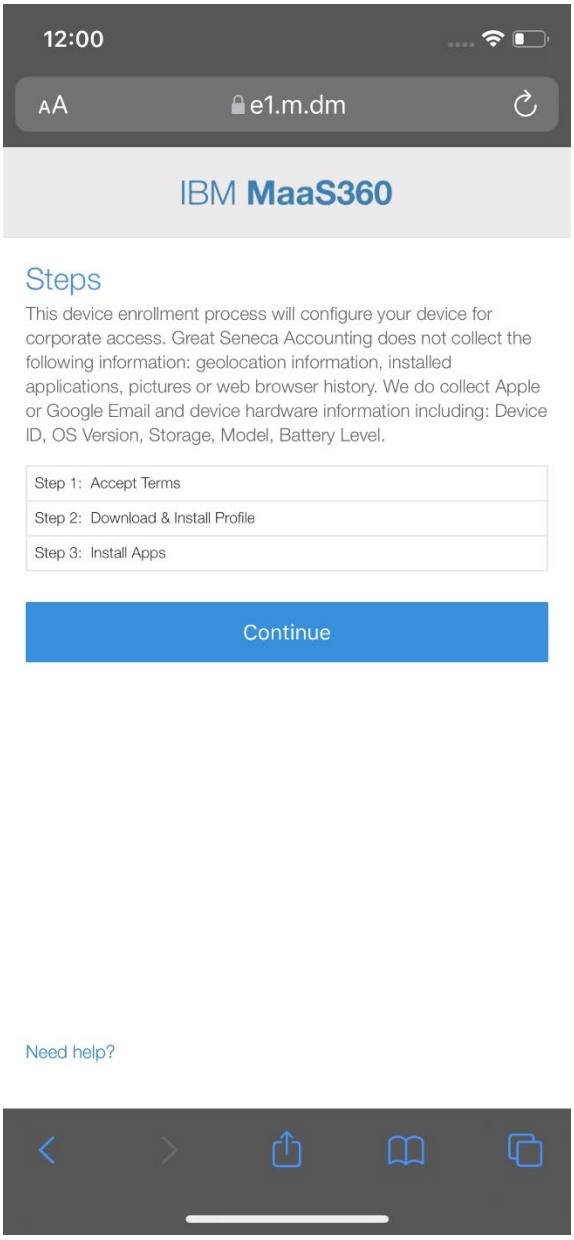
1393 **Test Activity:** Test to ensure that MDM provides custom notification to users detailing collected device
1394 information.

1395 **Desired Outcome:** MDM provides details of what information is collected during device enrollment.

1396 **Observed Outcome:** Device data collection information is displayed to users.

1397 Figure 2-74 demonstrates how users will be notified of what device information is collected by mobile
1398 security products during the device enrollment process.

1399 **Figure 2-74 Mobile Device Information Collection Notification**



1400 **Additional Potential Mitigations:**

1401 • Provide notification to the user
1402 • Train users on mobile device collection policy
1403 • Provide a point of contact for user questions regarding organizational data collection and use
1404 policies

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

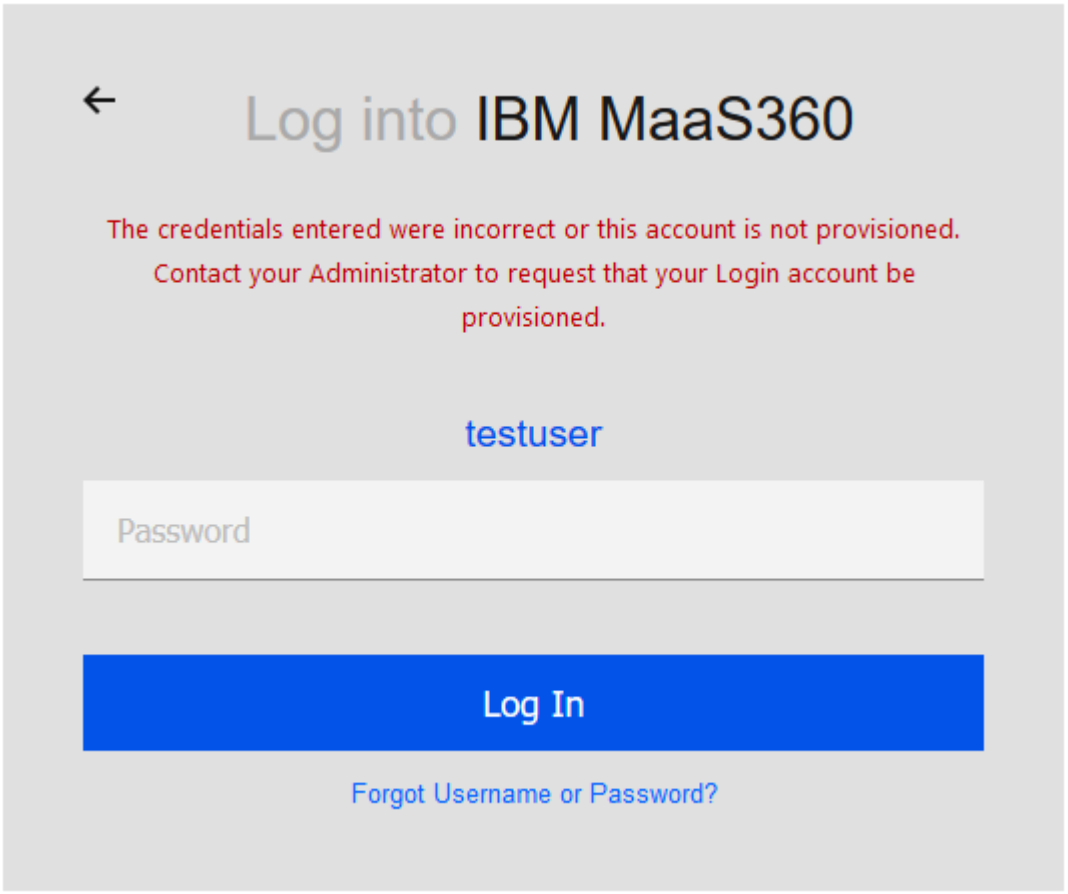
Test Activity: Attempt to log in to the MaaS360 admin portal without domain administrator permissions.

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.

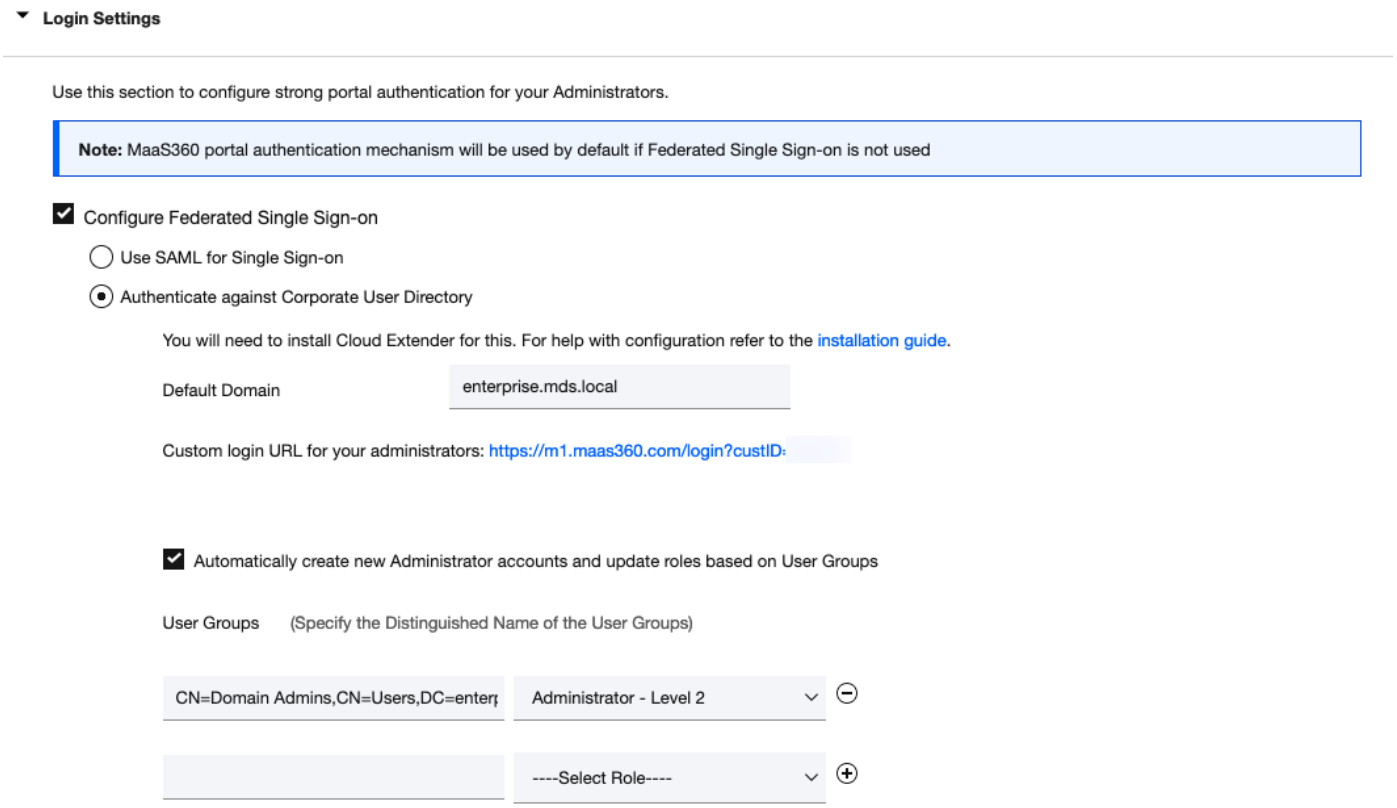
Observed Outcome: Domain administrators were allowed to log in, but non-administrator users were not.

Figure 2-75 demonstrates how a non-administrator account will be prevented from logging into the MaaS360 portal.

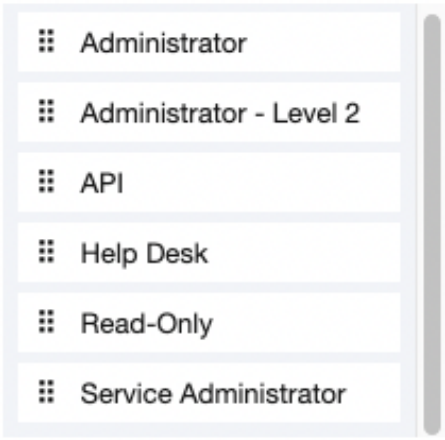
1418 **Figure 2-75 Non-Administrator Failed Portal Login**



1419 **Figure 2-76 - Admin Login Settings**



1420 **Figure 2-77 - Administrator Levels**



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