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

The MITRE Corporation
McLean, VA

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

March 2021

DRAFT

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

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.

National Institute of Standards and Technology Special Publication 1800-22B Natl. Inst. Stand. Technol. Spec. Publ. 1800-22C, 61 pages, (March 2021), 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: March 18, 2021 through May 03, 2021

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, Md.

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 Apple 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

Name	Organization
Kevin Stine	NIST
Chris Brown	The MITRE Corporation
Nancy Correll	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Erin Wheeler	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward	IBM
Cesare Coscia	IBM
Chris Gogoel	Kryptowire
Tom Karygiannis	Kryptowire
Jeff Lamoureaux	Palo Alto Networks
Sean Morgan	Palo Alto Networks

Name	Organization
Kabir Kasargod	Qualcomm
Viji Raveendran	Qualcomm
Mikel Draghici	Zimperium

*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	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

147 # 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 I, Example Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

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

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

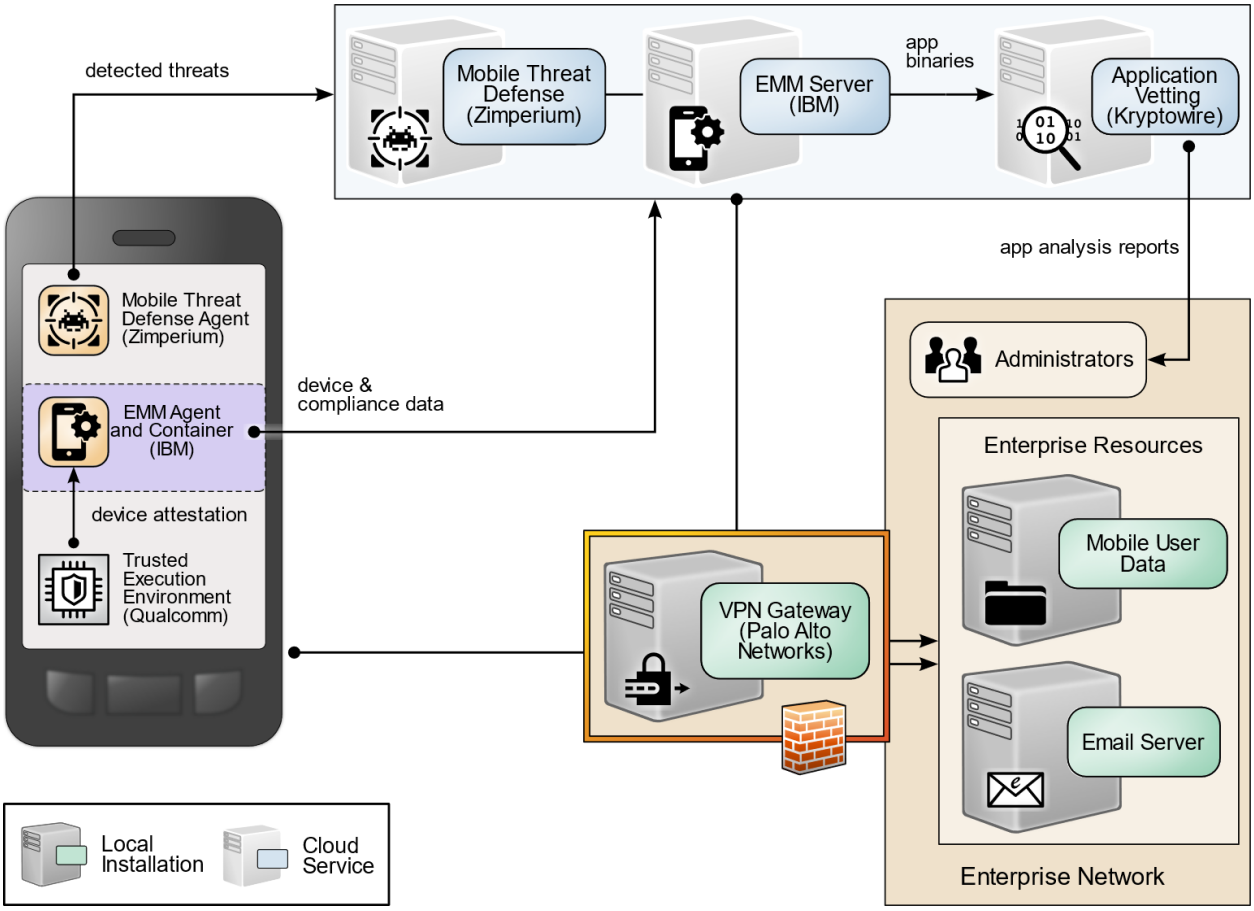
Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide.*
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`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

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



268 2 Product Installation Guides

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

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

274 2.1 Network Device Enrollment Services Server

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

2.1.1 Certificate Authority (CA) Configuration

The guide followed for the build is linked below, followed by the specific configuration changes used.

Configuration guide: https://gallery.technet.microsoft.com/Windows-Server-2016-Active-165e88d1

Configuration changes that were made:

- The Root CA Name was changed to ROOT-CA.
- The Issuing CA Name was changed to SUB-CA.
- The entry for `DC=srv,DC=lab` was replaced with `DC=enterprise,DC=mds,DC=local` at various points throughout the guide.

2.1.1.1 Export Certificates

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

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

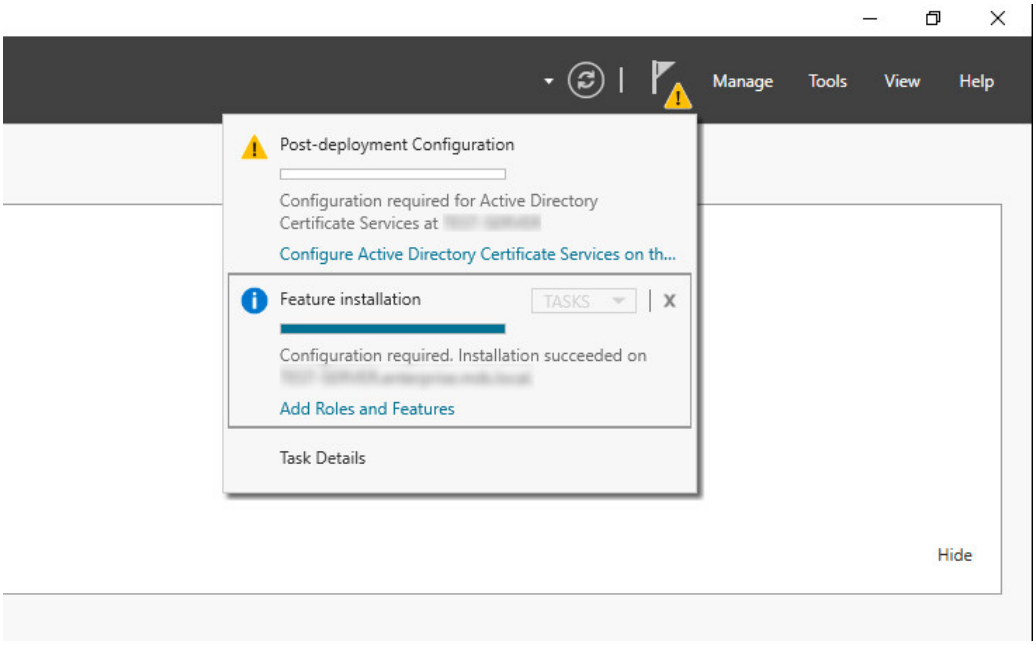
2.1.2 NDES Configuration

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

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

5. Uncheck **Certification Authority.** Check **Network Device Enrollment Service.**
6. Click **Add Features** on the pop-up.
7. Click **Next** three times.
8. Click **Install**.
9. When installation completes, click the flag in the upper right-hand corner, and click **Configure Active Directory Certificate Services.**

Figure 2-1 Post-Deployment Configuration



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

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

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

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

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

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

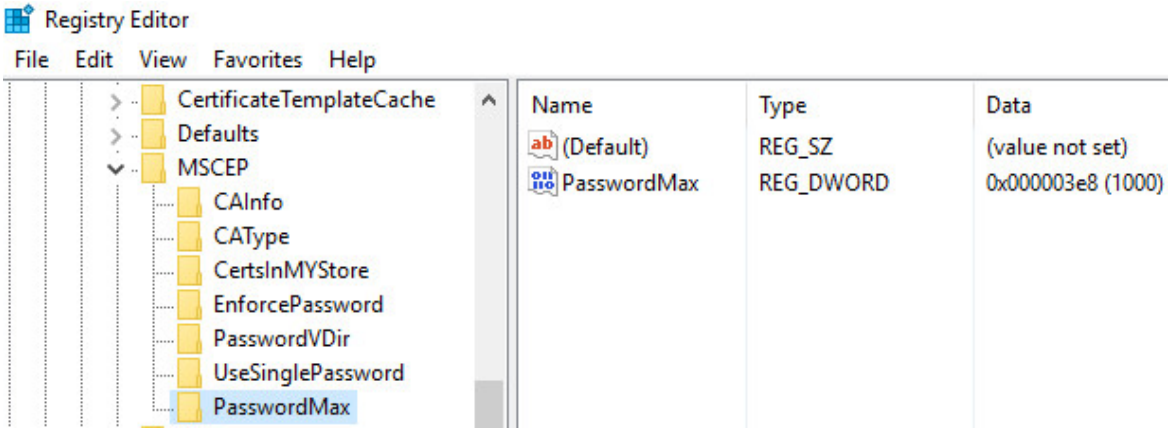
f. Click **Apply,** and click **OK**.

g. Close all windows except the NDES configuration window.

13. Click **Select** next to the box, and enter the service account credentials. Click **Next**.
14. Because the NDES runs on its own server, we will target it at the SUB-CA. Select **Computer name** and click **Select.** Type in the computer name—in this case, SUB-CA. Click **Check Names,** and if no errors occurred, click **OK**.
15. Click **Next** three times.
16. Click **Configure.**
17. On the SUB-CA, open the Certification Authority application.
18. Expand the SUB-CA node, right-click on **Certificate Templates,** and click **Manage**.
19. Right-click on **IPSec (Offline Request)**, and click **Duplicate Template**.
20. Under the **General** tab, set the template display name to **NDES**.
21. Under the **Security** tab, click **Add**.
22. Select the previously configured NDES service account.
23. Click **OK**. Ensure the NDES service account is highlighted, and check **Read** and **Enroll**.
24. Click **Apply**.
25. In the Certification Authority program, right-click on **Certificate Templates,** and select **New > Certificate Template to Issue**.
26. Select the NDES template created in step 24.
27. Click **OK.**
28. On the NDES server, open the Registry Editor (`regedit`).
29. Expand the following key: `HKLM\SOFTWARE\Microsoft\Cryptography`.
30. Select the `MSCEP` key and update all entries besides (Default) to be **NDES**.

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

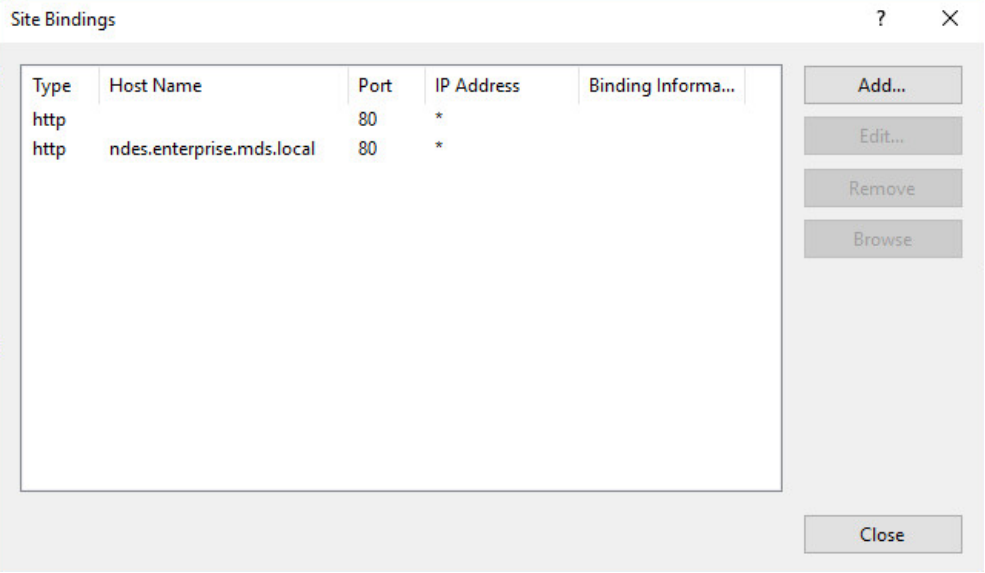
Figure 2-2 PasswordMax Registry Configuration



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

1. In an elevated command prompt, execute `%windir%\system32\inetsrv\appcmd set config /section:requestFiltering /requestLimits.maxQueryString:8192` to increase the maximum query string. This prevents requests longer than 2,048 bytes from being dropped.
2. Open the **Internet Information Services (IIS) Manager**.
3. On the left, expand **NDES > Sites,** and select **Default Web Site**.
4. On the right, click **Bindings…**
5. Click **Add.**
6. Below **Host Name,** enter the host name of the server. For this implementation, *ndes.enterprise.mds.local* was used.
7. Click **OK**.

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



370

371 8. Click **Close,** and close the IIS Manager.

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

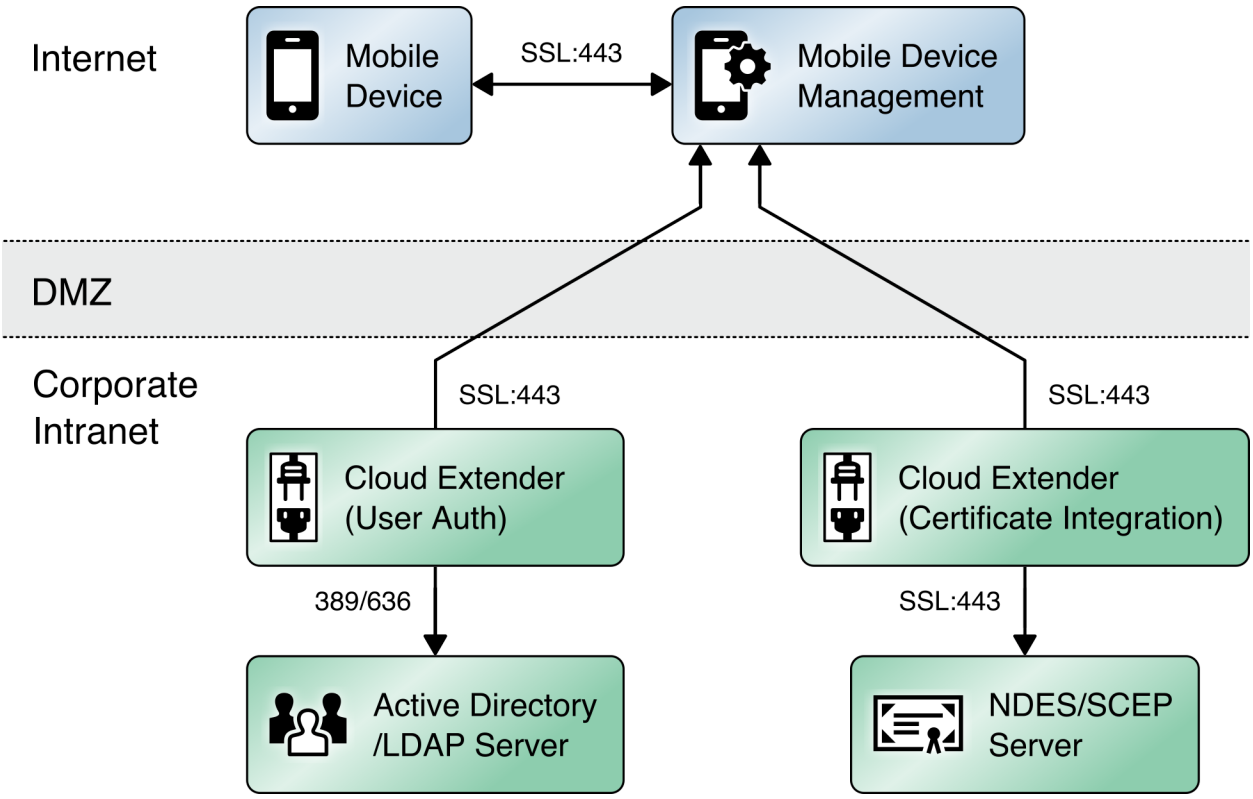
373 2.2 International Business Machines MaaS360

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

377 2.2.1 Cloud Extender

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

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



383 ### *2.2.1.1 Cloud Extender Download*

384 1. Log in to the MaaS360 web portal.

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

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

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

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

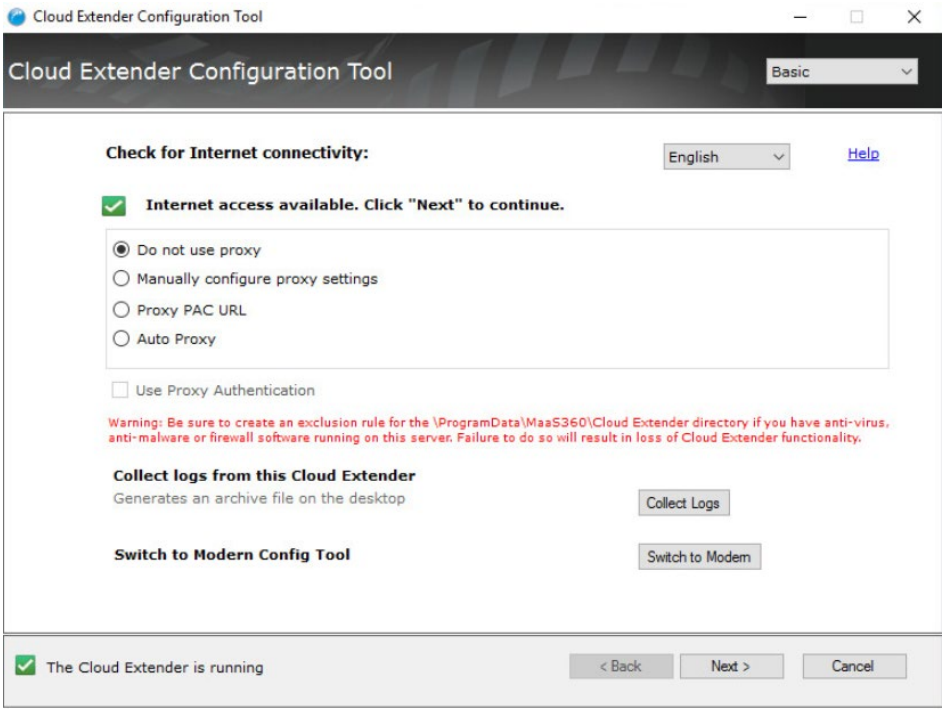
391 6. Install **.NET 3.5 Features** in the **Server Manager** on the machine where the MaaS360 Cloud Ex-
392 tender will run.

393 ### *2.2.1.2 Cloud Extender Active Directory Configuration*

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

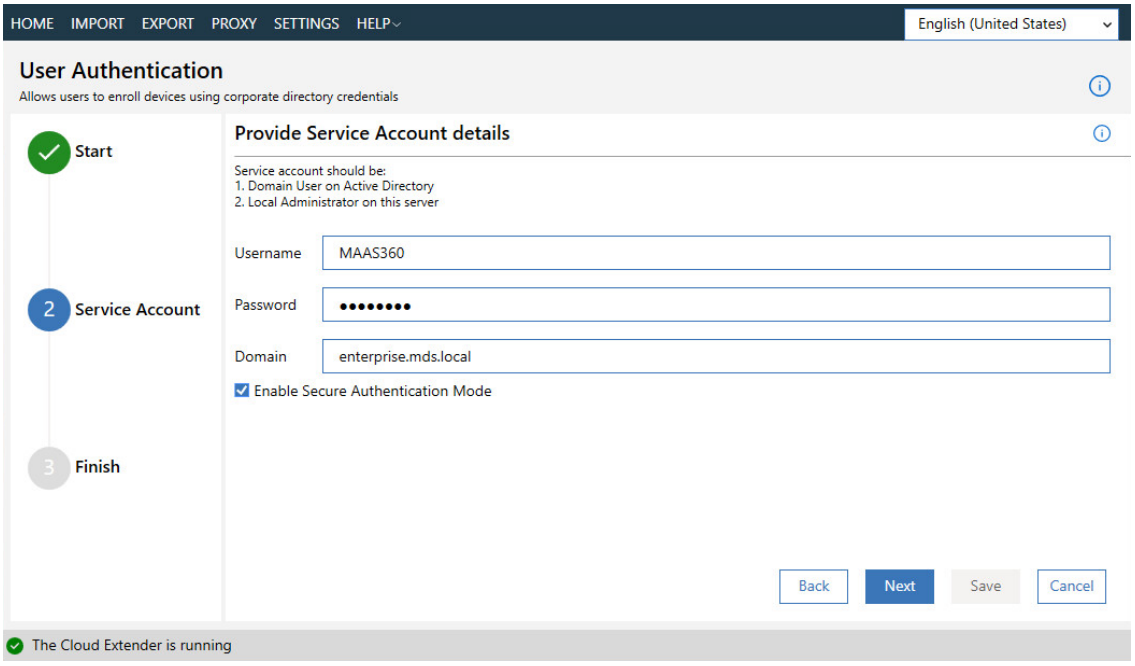
2. Enter the license key when prompted.
3. Proceed through the setup until the Cloud Extender Configuration Utility opens.
4. If using the old cloud extender interface, click **Switch to Modern.**

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.

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



403 7. Click **Next**.

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

405 9. Click **Save**.

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

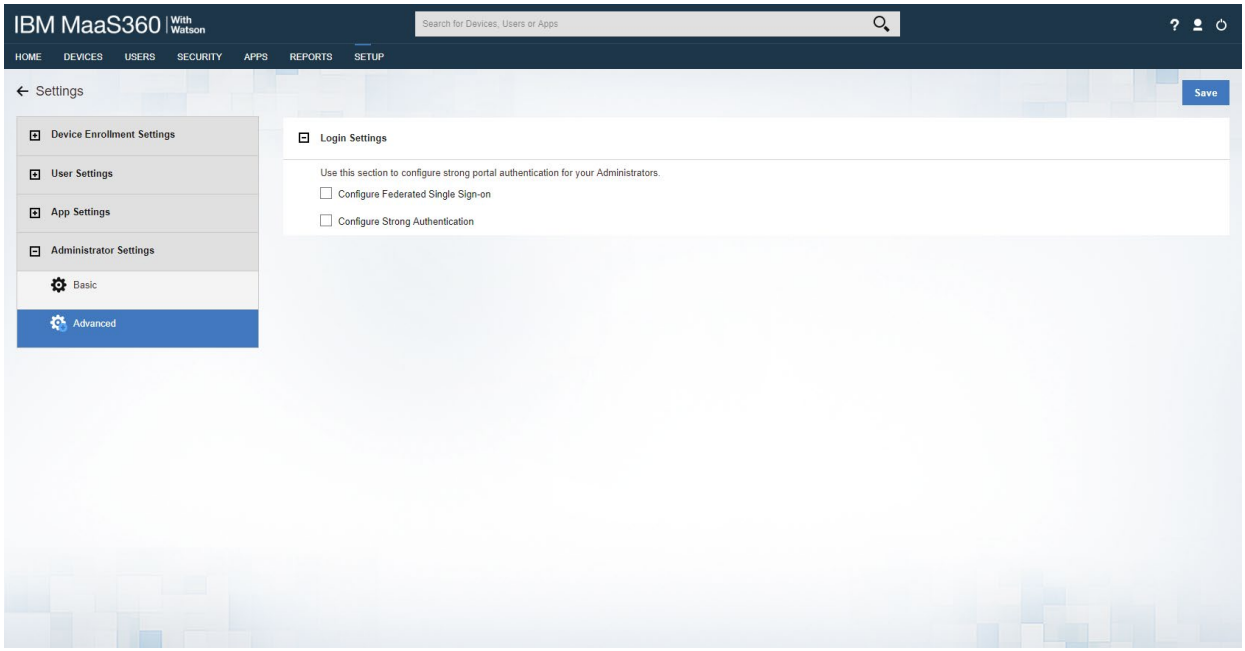
408 *2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration*

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

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

411 3. Expand **Administrator Settings,** and click **Advanced**.

412 **Figure 2-7 Administrator Settings**



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

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

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

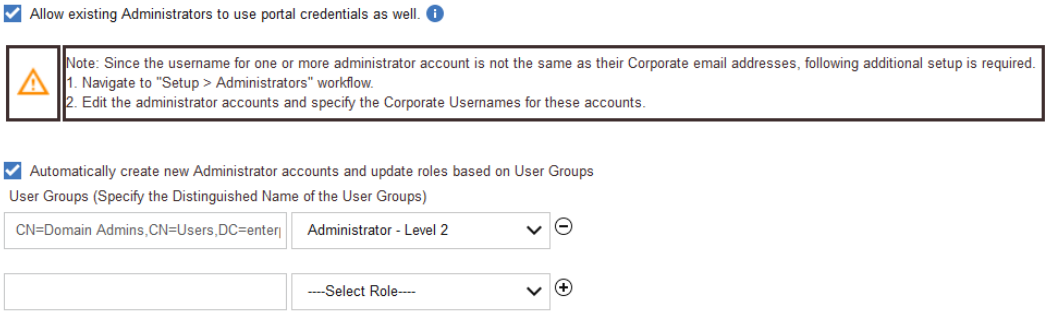
417 7. Check the box next to **Allow existing Administrators to use portal credentials as well**.

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

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

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

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



426 11. Click **Save.**

427 ### *2.2.1.4 Cloud Extender NDES Integration*

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

430 1. Log in to the server running the MaaS360 Cloud Extender.

431 2. Launch the Cloud Extender Configuration Tool.

432 3. Toggle the button below Certificate Integration.

433 4. Click **Add New Template.**

434 5. Ensure **Microsoft CA** and **Device Identity Certificates** are selected.

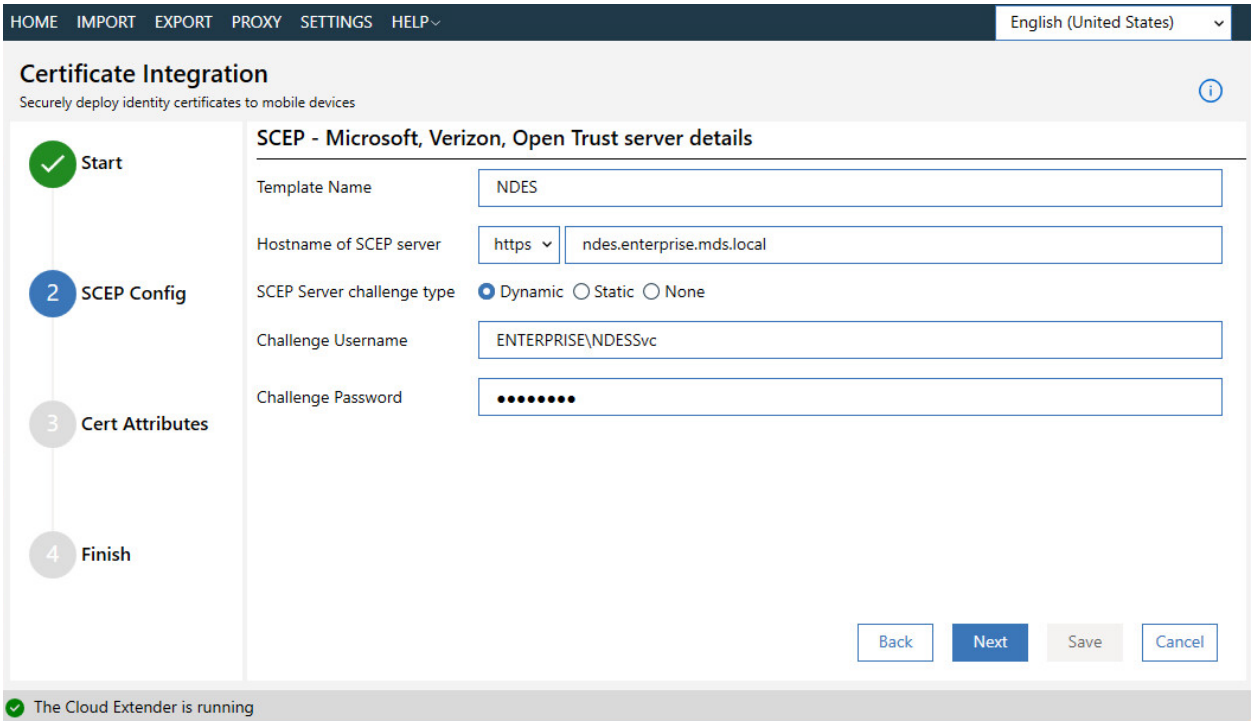
435 6. Click **Next.**

436 7. Enter **NDES** for the Template Name and SCEP Default Template.

437 8. Enter the uniform resource locator (URL) of the NDES server next to **SCEP Server.**

438 9. Enter credentials of a user with enroll permissions on the template for **Challenge Username** and
439 **Challenge Password.** For this demo implementation, we use the NDES service account.

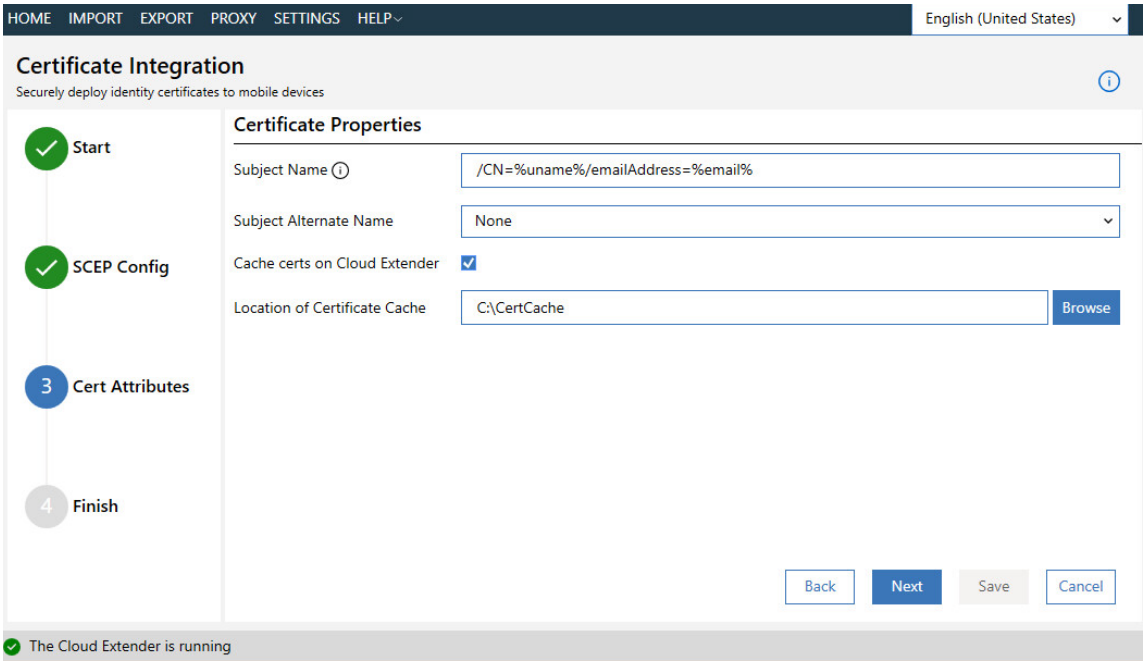
440 **Figure 2-9 Cloud Extender SCEP Configuration**



441 10. Click **Next.**

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

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



445 12. Click **Next.**

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

448 14. Click **Save.**

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

450 2.2.2 Android Enterprise Configuration

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

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

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

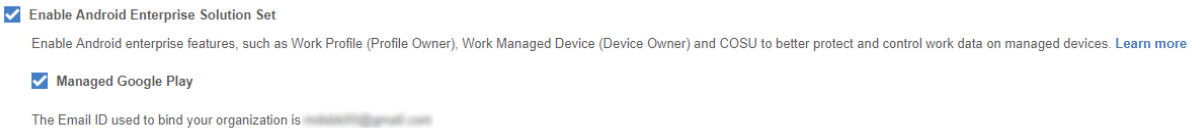
456 3. Click **Mobile Device Management.**

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

458 5. Enter your password, and click **Enable.**

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 Android Configuration

2.2.4.1 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.

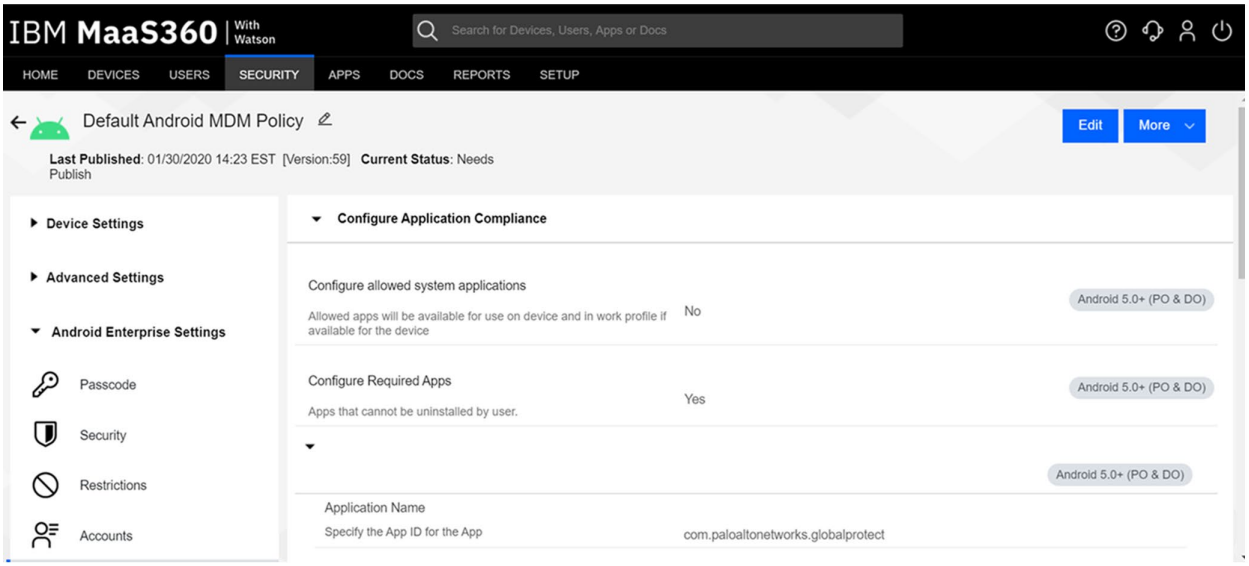
6. Configure the passcode settings based on corporate requirements.
7. Navigate to **Android Enterprise Settings > Restrictions.**
8. Check the box next to Configure Restrictions.
9. Configure restrictions based on corporate requirements.
10. Click **Save.**

2.2.4.2 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 container.)
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.

530 **Figure 2-12 Android GlobalProtect Application Compliance**



531 ## 2.2.5 iOS Configuration

532 ### *2.2.5.1 Policy Configuration*

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

543 ### *2.2.5.2 VPN Configuration*

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

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. Click **Apps**.
15. Click **Add > iOS > iTunes App Store App**.
16. Search for **GlobalProtect**.
17. Select the **non-Legacy** version.
18. Click **Policies and Distribution**.
19. Check all three boxes next to **Remove App on**.
20. Select **All Devices** next to **Distribute to**.
21. Check the box next to **Instant Install.**
22. Click **Add**.
23. Navigate to **Security > Policies**.
24. Click the used iOS policy.
25. Click **Application Compliance**.

26. Click **Edit**.
27. Click the **+** next to the first row under **Configure Required Applications**.
28. Search for **GlobalProtect.**
29. Select the **non-Legacy** result.
30. Navigate to **Advanced Settings > Certificate Credentials**.
31. Check the box next to **Configure Credentials for Adding Certificates on the Device.**
32. Click **Add New.**
33. Give the certificate a name, such as Internal Root.
34. Click **Browse**, and navigate to the exported root CA certificate from earlier in the document.
35. Click **Save.**
36. Select **Internal Root** from the drop-down next to **CA Certificate.**
37. Click the **+** icon on the far right.
38. Repeat steps 33–35 with the internal sub CA certificate.
39. 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**.
40. 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.

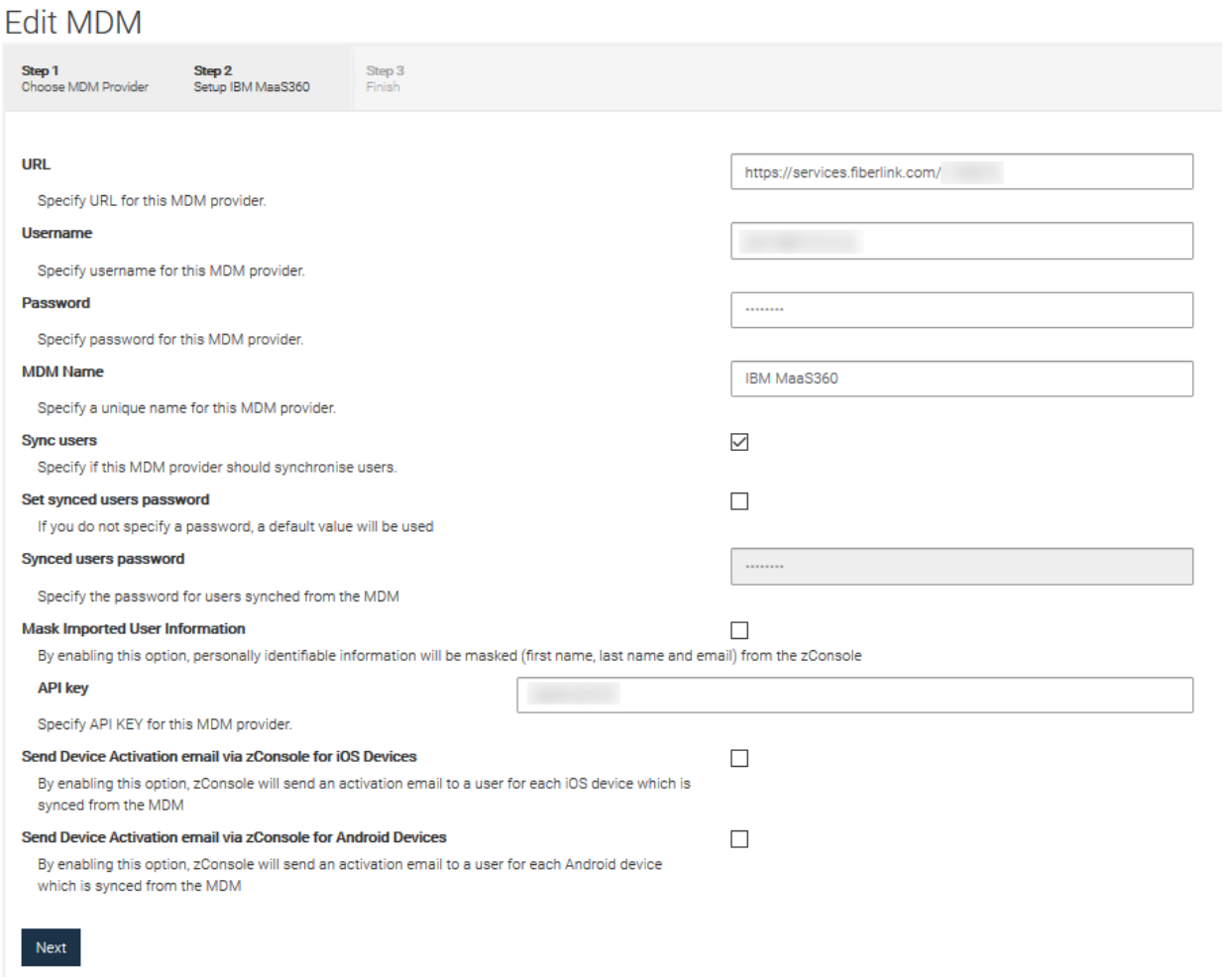
2.3.1 Zimperium and MaaS360 Integration

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**.

Figure 2-13 Zimperium MaaS360 Integration Configuration



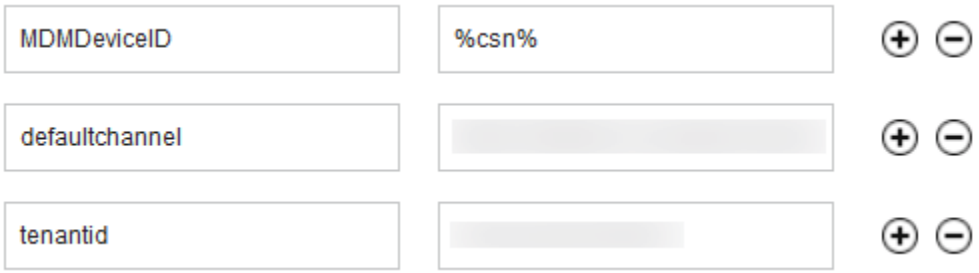
7. Click **Next**.
8. Select the MaaS360 groups to synchronize with Zimperium. In this case, **All Devices** was selected**.**
9. Click **Finish**. Click **Sync Now** to synchronize all current MaaS360 users and devices.

2.3.2 Automatic Device Activation

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

1. Log in to MaaS360.
2. Click **Apps** on the navigation bar.
3. Click **Add > iOS > iTunes App Store App**.
4. Search for **Zimperium zIPS.** Click the result that matches the name.
5. Click **Policies and Distribution**.
6. Check the three checkboxes next to **Remove App on**.
7. Next to **Distribute to,** select **All Devices**.
8. Click **Configuration.**
9. Set App Config Source to **Key/Value**.
10. The configuration requires three parameters: uuid, defaultchannel, and tenantid. uuid can be set to **%csn%,** but defaultchannel and tenantid must come from Zimperium support.

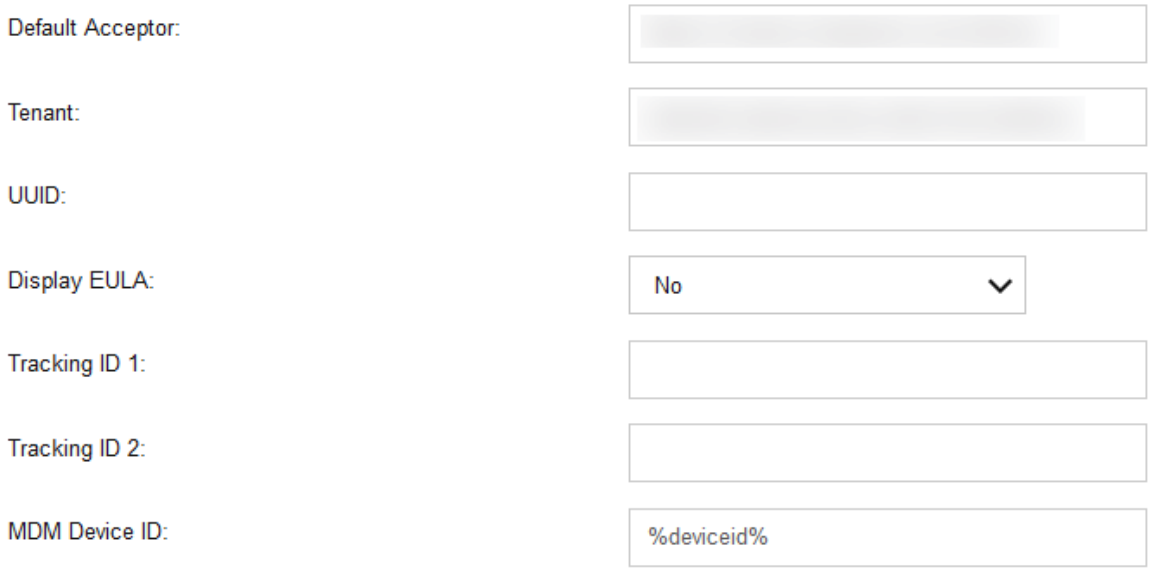
Figure 2-14 Zimperium zIPS iOS Configuration



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

17. Click **Policies and Distribution**.
18. Check all three boxes next to **Remove App on**.
19. Check **Instant Install**.
20. Select **All Devices** next to **Distribute to**.
21. Click **App Configurations**.
22. Check **Configure App Settings**.
23. Enter the values provided by Zimperium next to **Default Acceptor** and **Tenant**.
24. Next to **MDM Device ID,** insert **%deviceid%**.
25. Adjust any other configuration parameters as appropriate for your deployment scenario.

Figure 2-15 Zimperium zIPS Android Configuration



26. Click **Add.**

2.3.3 Enforce Application Compliance

From the IBM MaaS360 web portal:

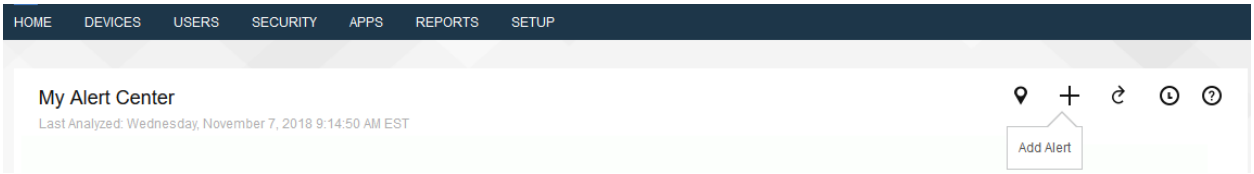
1. Navigate to **Security > Policies.**
2. Select the default Android policy.

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

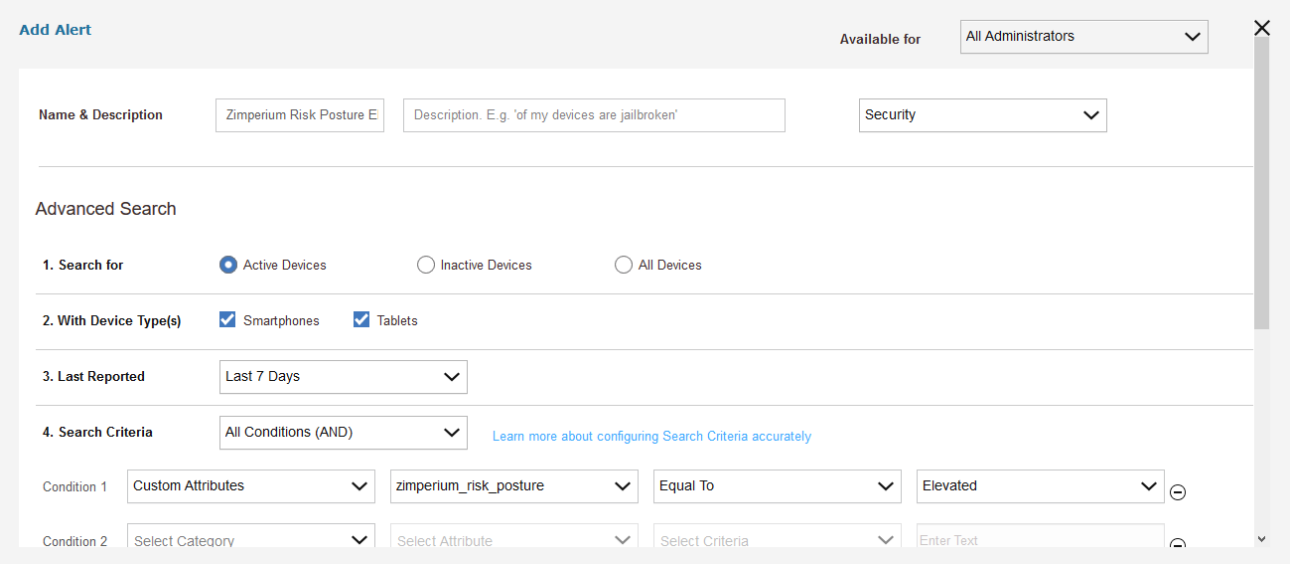
1. From the MaaS360 home screen, click the **+** button that says **Add Alert.**

Figure 2-16 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 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.

665 **Figure 2-17 Zimperium Risk Posture Alert Configuration**



666 8. Click **Update.**

667 2.4 Palo Alto Networks Virtual Firewall

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

669 2.4.1 Network Configuration

670 1. Ensure that all Ethernet cables are connected or assigned to the virtual machine and that the
671 management web user interface is accessible. Setup will require four Ethernet connections: one
672 for management, one for wide area network (WAN), one for local area network, and one for the
673 demilitarized zone (DMZ).

674 2. Reboot the machine if cables were attached while running.

675 3. Navigate to **Network > Interfaces > Ethernet.**

676 4. Click **ethernet1/1**, and set the Interface Type to be **Layer3.**

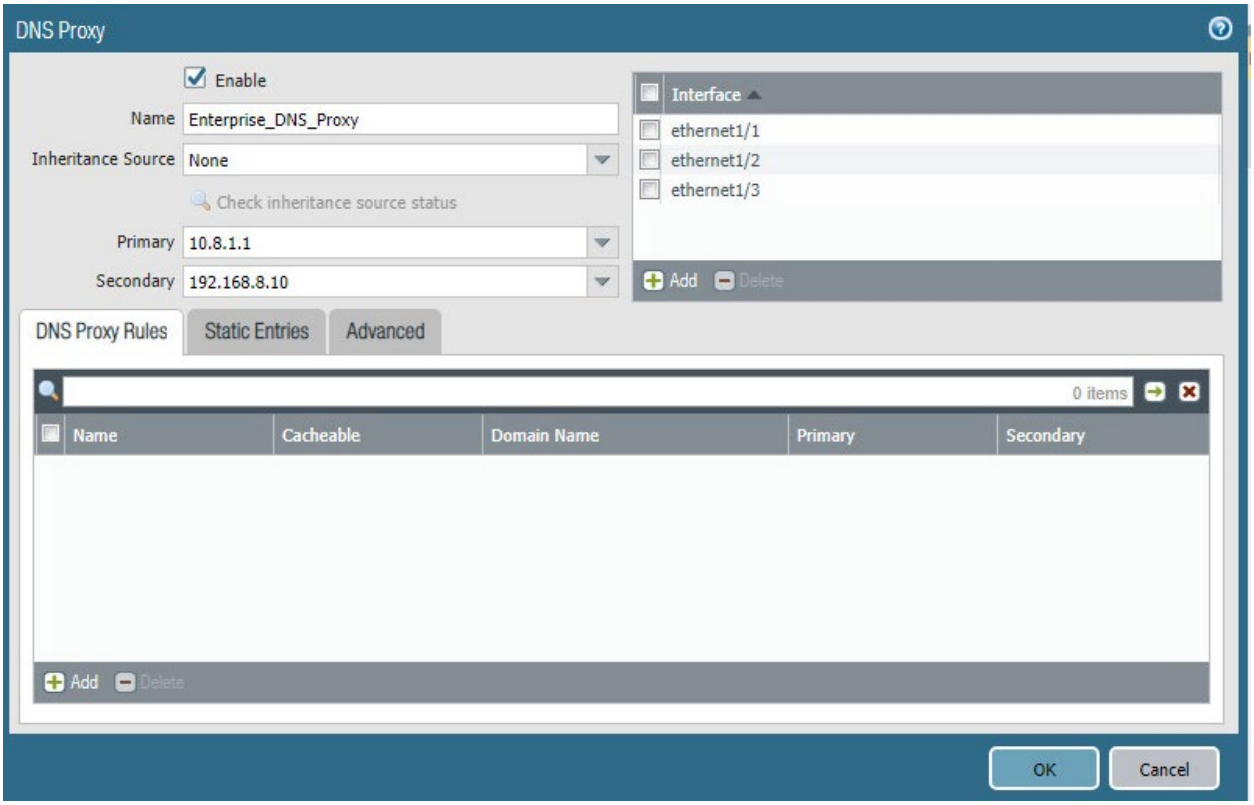
677 5. Click **IPv4,** ensure that **Static** is selected under Type, and click **Add** to add a new static address.

678 6. If the appropriate address does not exist yet, click **New Address** at the bottom of the prompt.

679 7. Once the appropriate interfaces are configured, commit the changes. The Link State icon should
680 turn green for the configured interfaces. The commit dialogue will warn about unconfigured
681 zones. That is an expected dialogue warning.

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.**

700 **Figure 2-18 DNS Proxy Object Configuration**



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

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

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

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

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

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

709 28. Click **OK**.

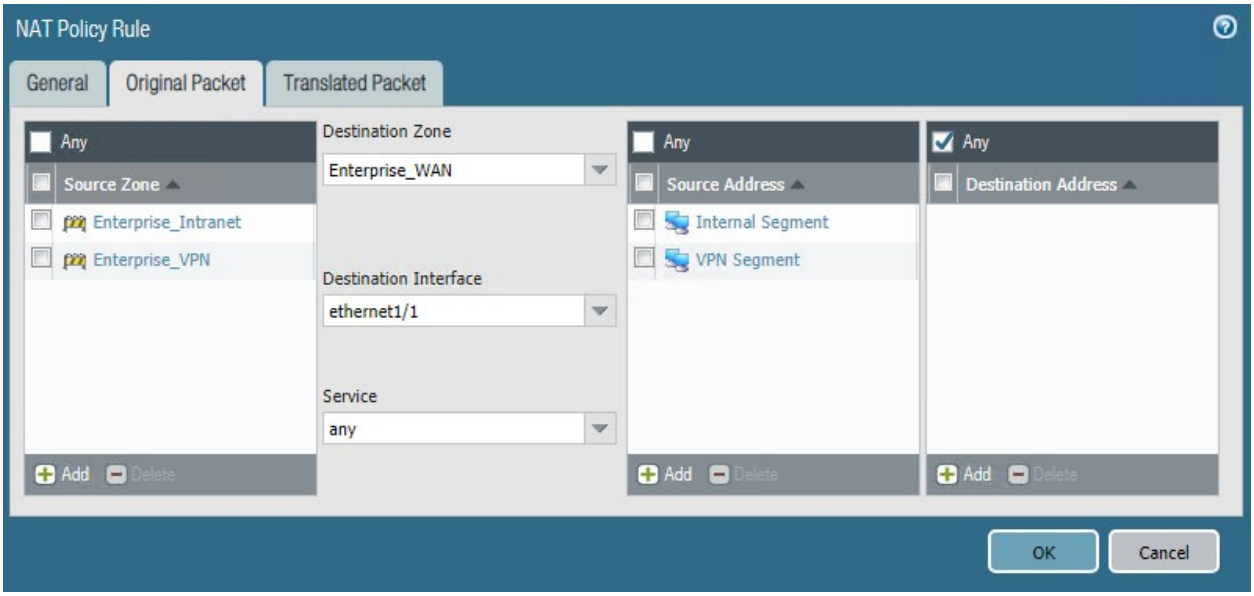
710 29. Once all devices are added, commit the changes.

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

712 31. Click **Add**.

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 2-19 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

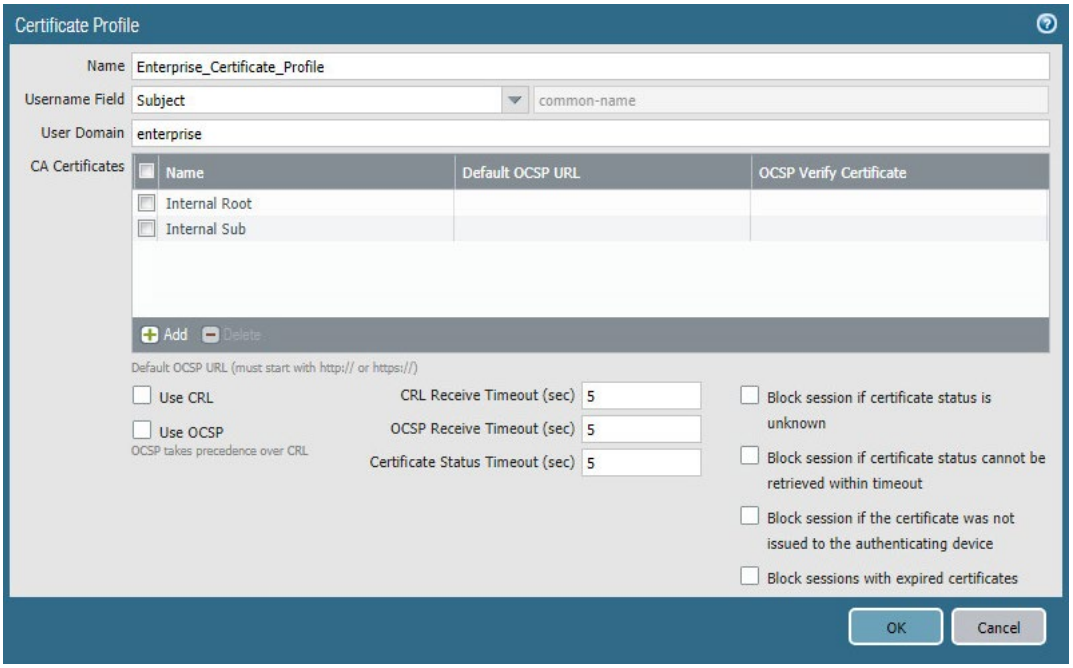
1. Navigate to **Policies > Security**.
2. Click **Add**.
3. Give the rule a meaningful name, such as Intranet Outbound.
4. Click **Source**. Click **Add** under source zone, and set the source zone to be the internal network.
5. Click **Destination.** Click **Add** under destination zone, and set the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

769 **Figure 2-20 Certificate Profile**



770 ## 2.4.5 Website Filtering Configuration

771 ### *2.4.5.1 Configure Basic Website Blocking*

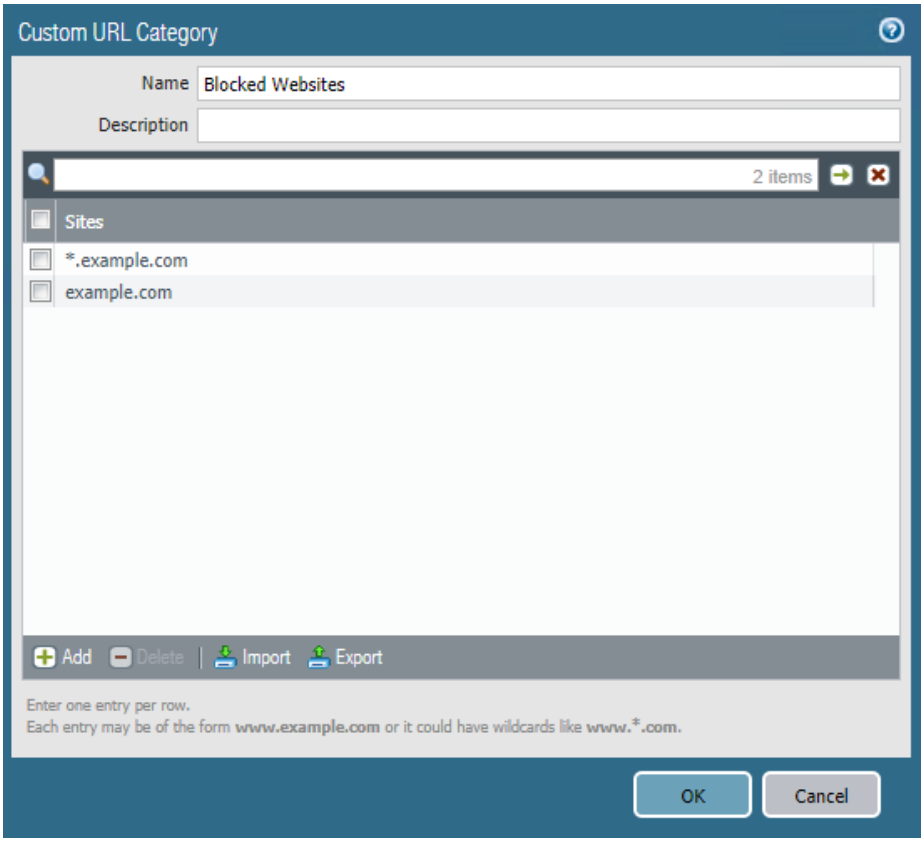
772 1. Navigate to **Objects > URL Category**.

773 2. Click **Add**.

774 3. Enter a name for the URL Category. Click **Add** on the bottom.

775 4. Add websites that should be blocked. Use the form **.example.com* for all subdomains and *ex-*
776 *ample.com* for the root domain.

777 **Figure 2-21 Custom URL Category**



778 5. Click **OK**.

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

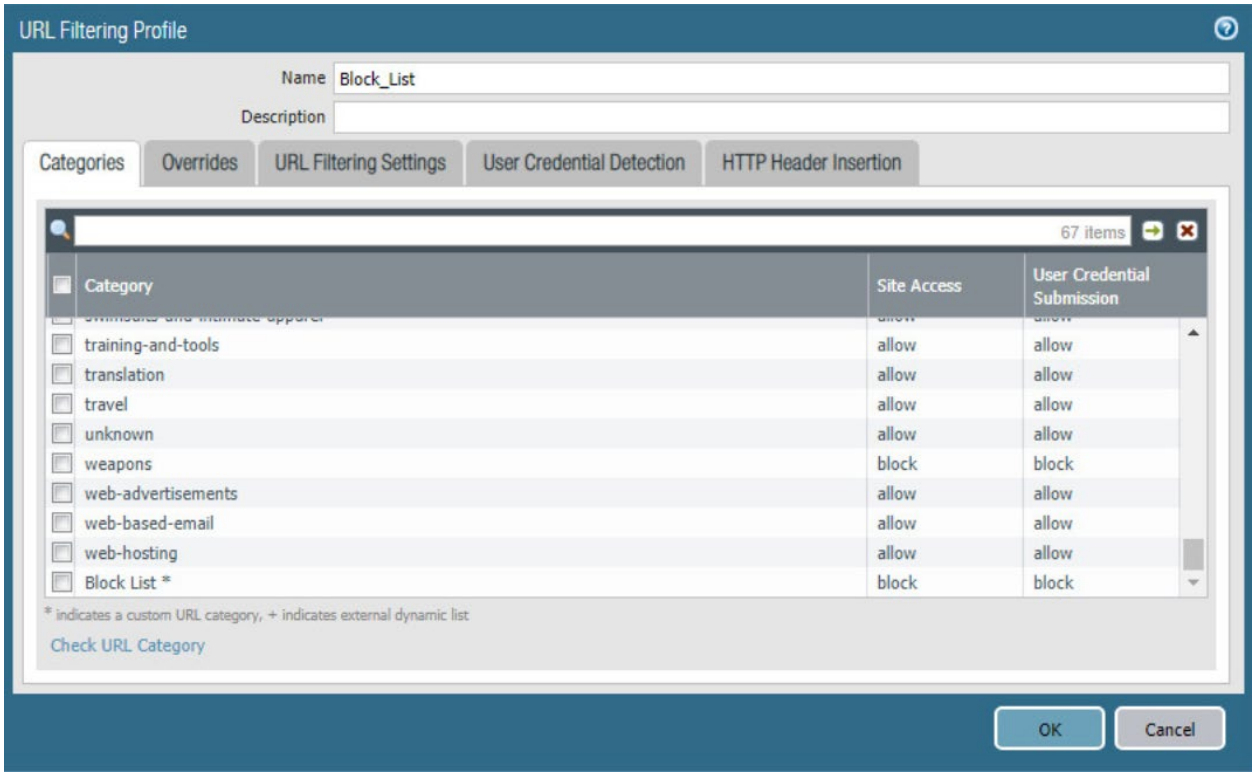
780 7. Click **Add**.

781 8. Give the filtering profile a name.

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

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

785 **Figure 2-22 URL Filtering Profile**



786 11. Click **OK**.

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

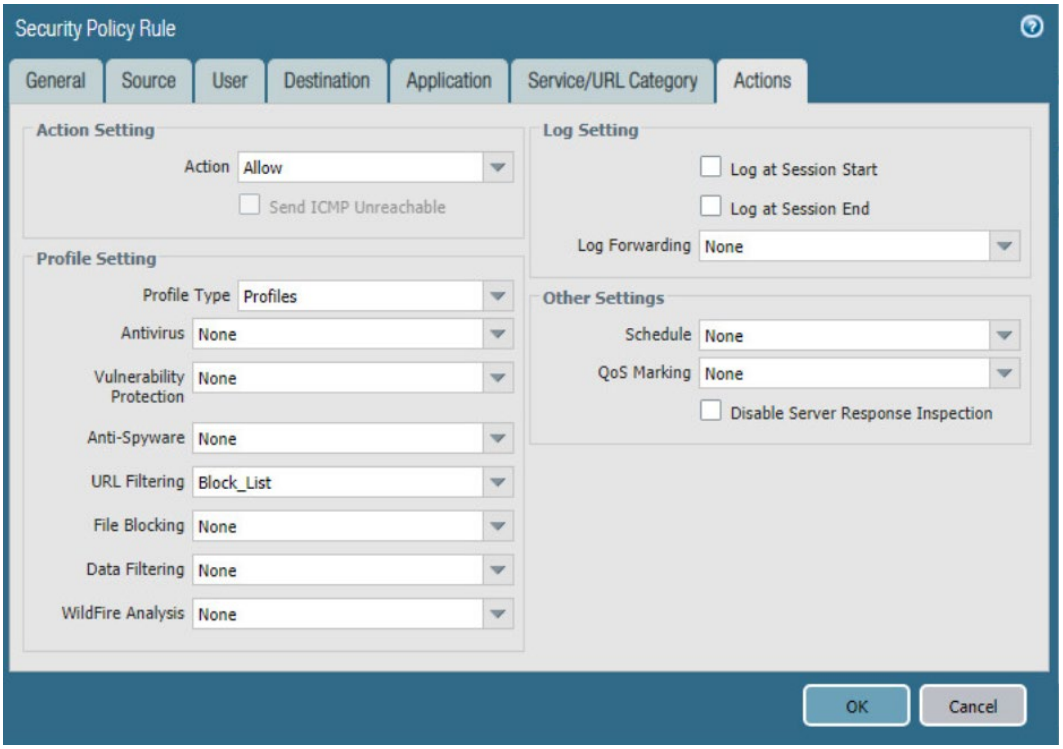
788 13. Select a policy to which to apply the URL filtering.

789 14. Select **Actions**.

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

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

792 **Figure 2-23 URL Filtering Security Policy**



793 17. Click **OK.**

794 18. Repeat steps 13–17 for any policies to which to apply the filtering profile.

795 19. Commit the changes.

796 ### *2.4.5.2 Configure SSL Website Blocking*

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

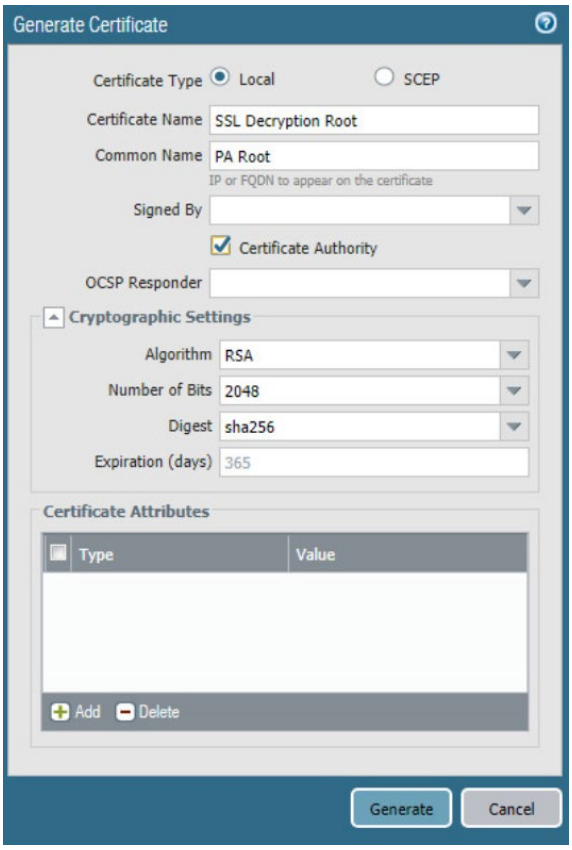
803 1. Navigate to **Device > Certificates**.

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

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

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

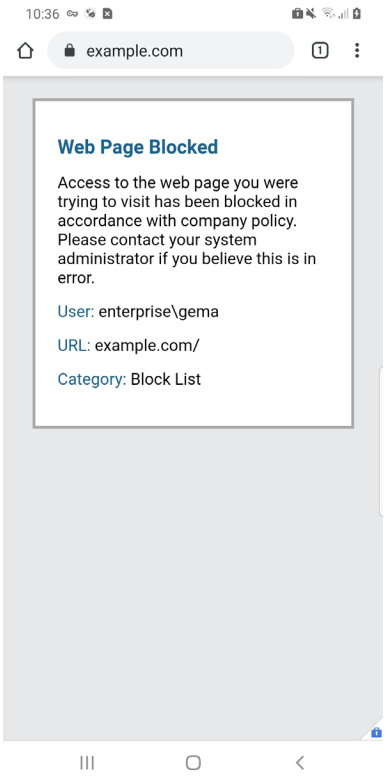
Figure 2-24 Generating the Root CA



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.

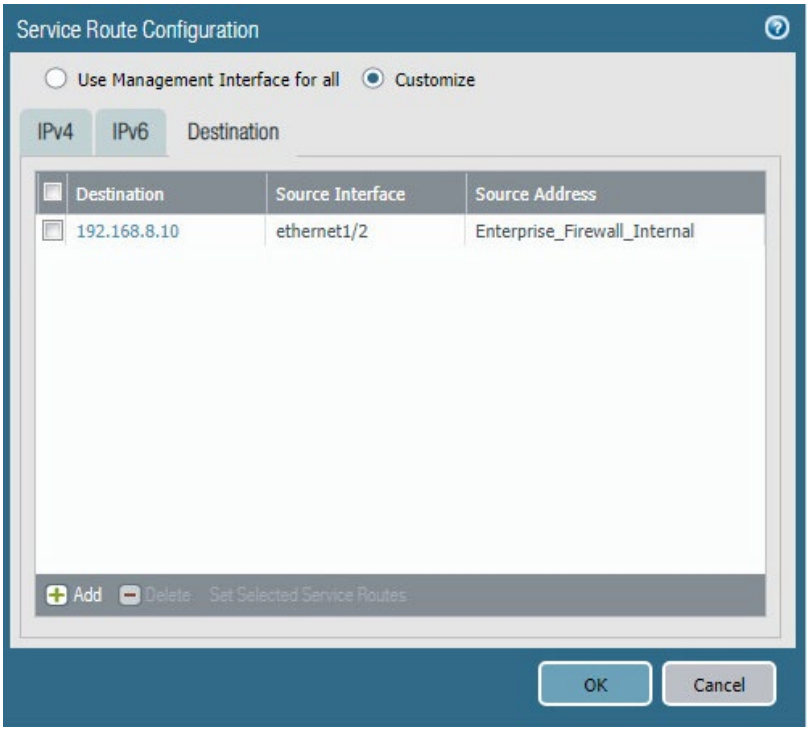
839 **Figure 2-25 Blocked Website Notification**



840 ## 2.4.6 User Authentication Configuration

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

848 **Figure 2-26 Service Route Configuration**



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

850 9. Click **Add**.

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

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

853 12. Under **Server Settings,** set the Type to active-directory.

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

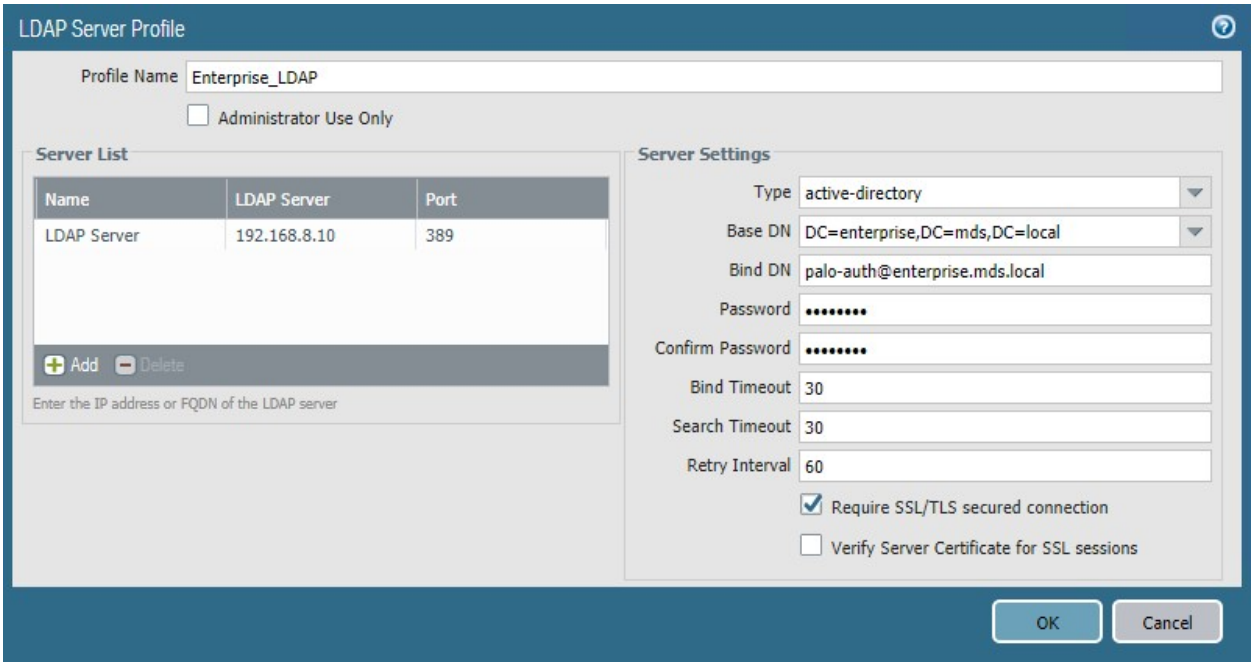
855 Note: In this implementation, a new user, palo-auth, was created in Active Directory. This user does not
856 require any special permissions or groups beyond the standard Domain Users group.

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

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

860 16. Click **OK.**

861 **Figure 2-27 LDAP Server Profile**



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

863 18. Click **Add**.

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

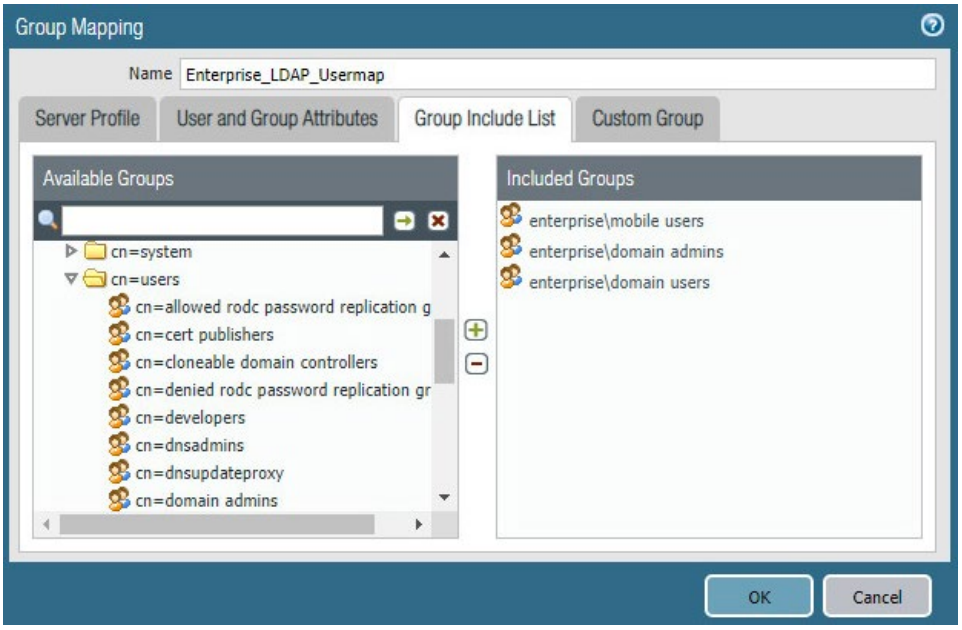
865 20. Select the **server profile,** and enter the **user domain—**in this case, Enterprise.

866 21. Click **Group Include List**.

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

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

871 **Figure 2-28 LDAP Group Mapping**



872 24. Click **OK**.

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

874 26. Click **Add**.

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

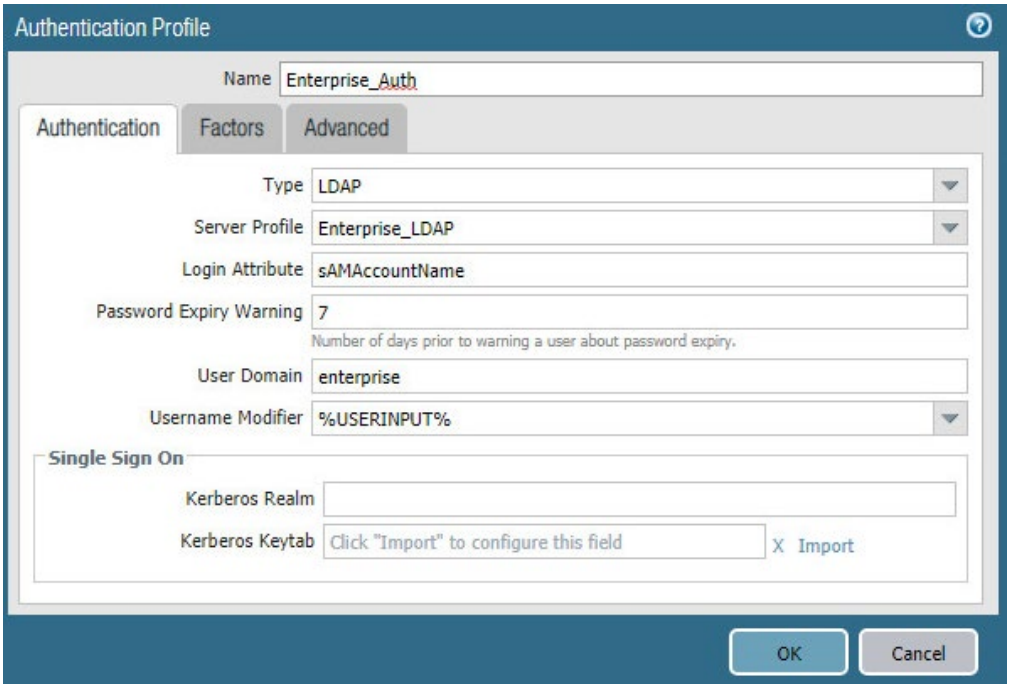
876 28. For the Type, select **LDAP**.

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

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

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

880 **Figure 2-29 LDAP User Authentication Profile**



881 32. Click on **Advanced.**

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

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

884 35. Click **OK.**

885 36. Commit the changes.

886 2.4.7 VPN Configuration

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

888 2. Click **Add.**

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

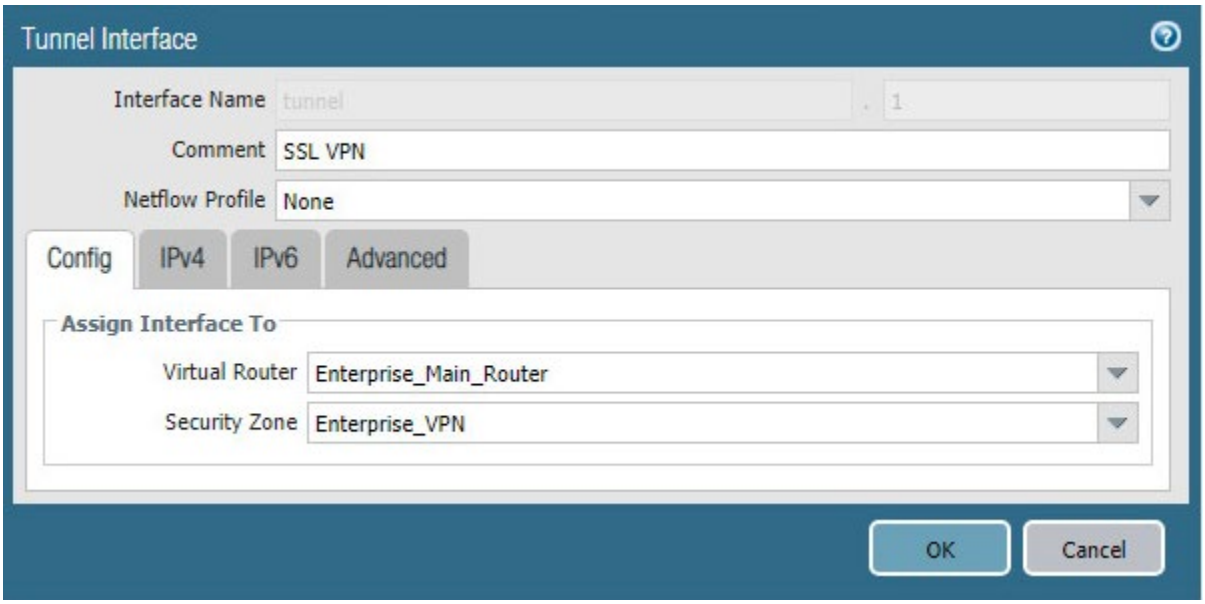
890 **Figure 2-30 Configured Tunnel Interfaces**

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

891

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 2-31 SSL VPN Tunnel Interface Configuration



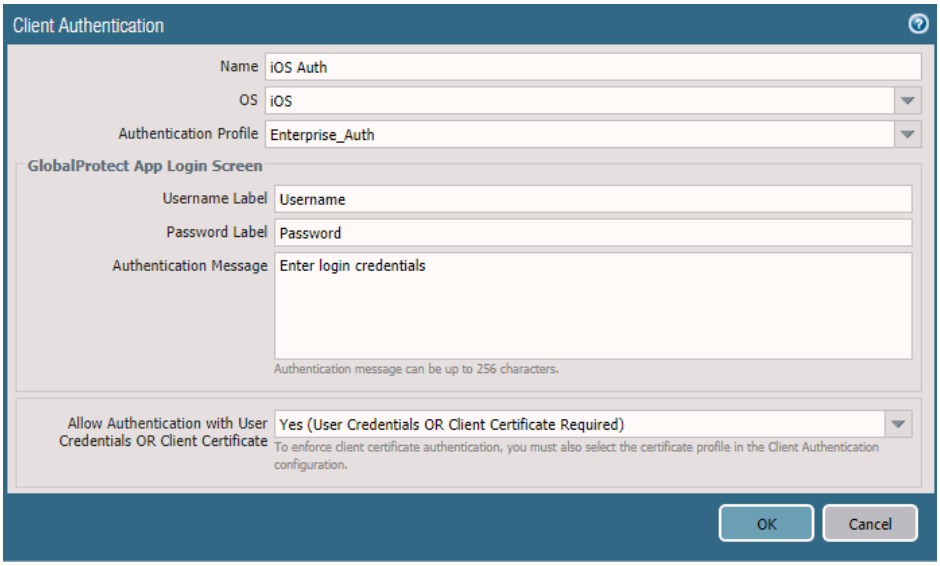
7. Commit the changes.
8. Navigate to **Policies > Authentication**.
9. Click **Add**.
10. Give the policy a **descriptive name**. For this example, the rule was named VPN_Auth.
11. Click **Source**.
12. Click **Add**, and add the VPN and WAN zones.
13. Click **Destination**.
14. Check the **Any** box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

924 **Figure 2-32 GlobalProtect iOS Authentication Profile**



925 14. Click **OK**.

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

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

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

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

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

931 20. Click **Agent**.

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

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

934 23. Uncheck **Enable IPSec**.

935 24. Click **Timeout Settings**.

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

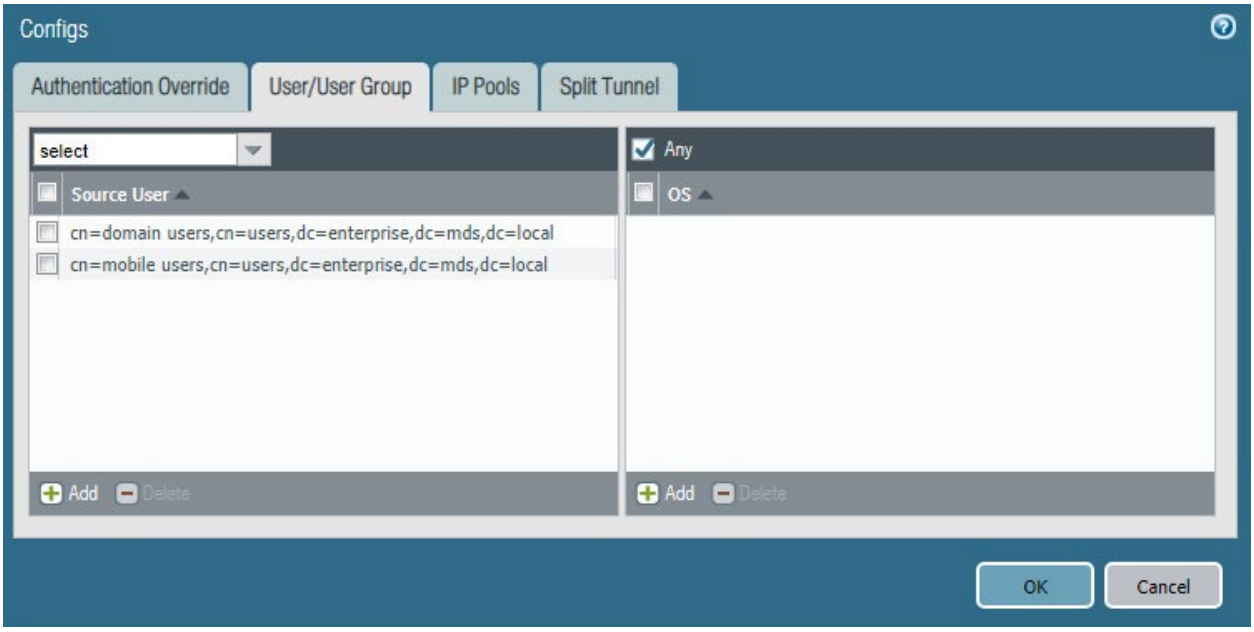
937 26. Click **Client IP Pool**.

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

939 28. Click **Client Settings**.

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.

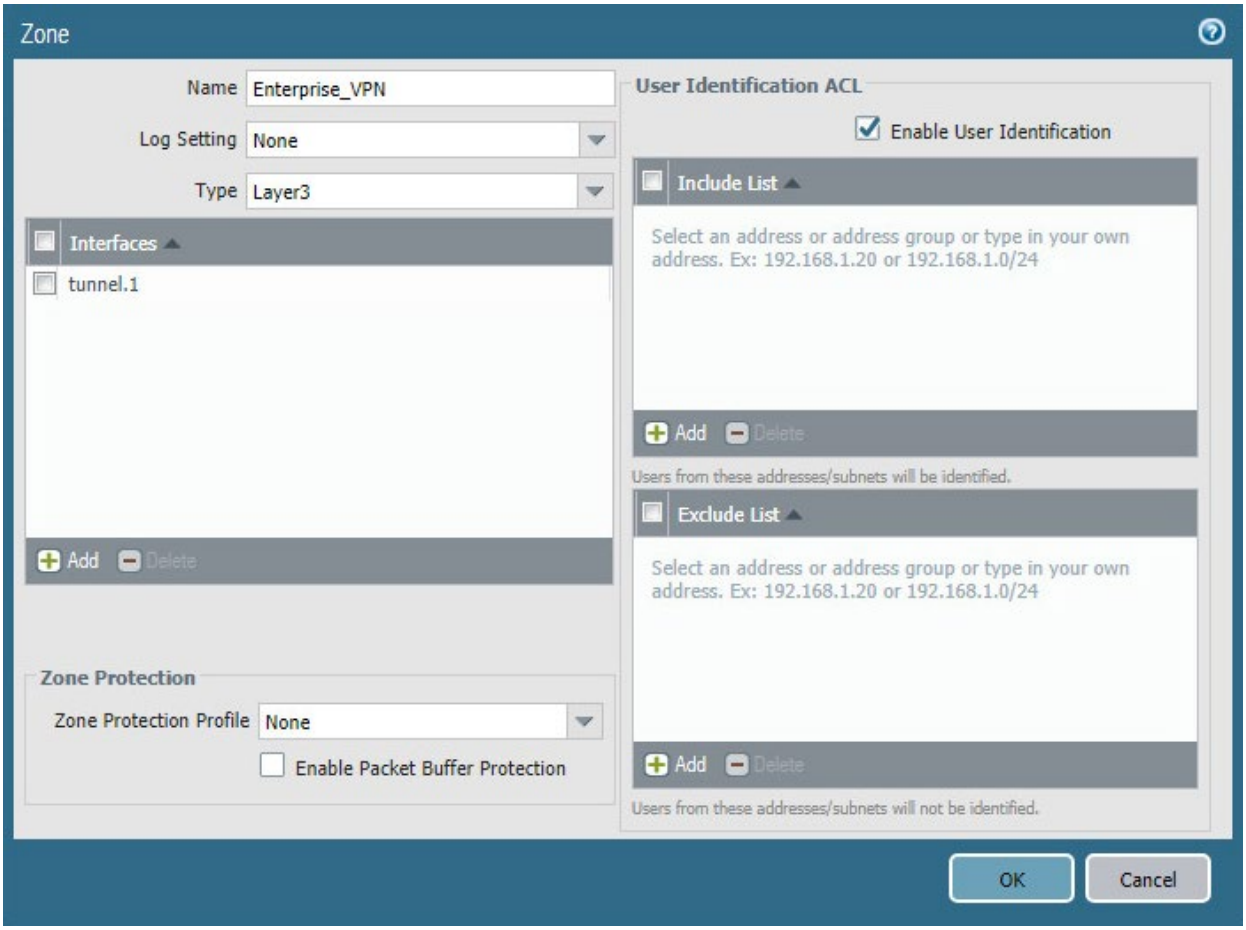
Figure 2-33 LDAP Authentication Group Configuration



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 2-34 VPN Zone Configuration



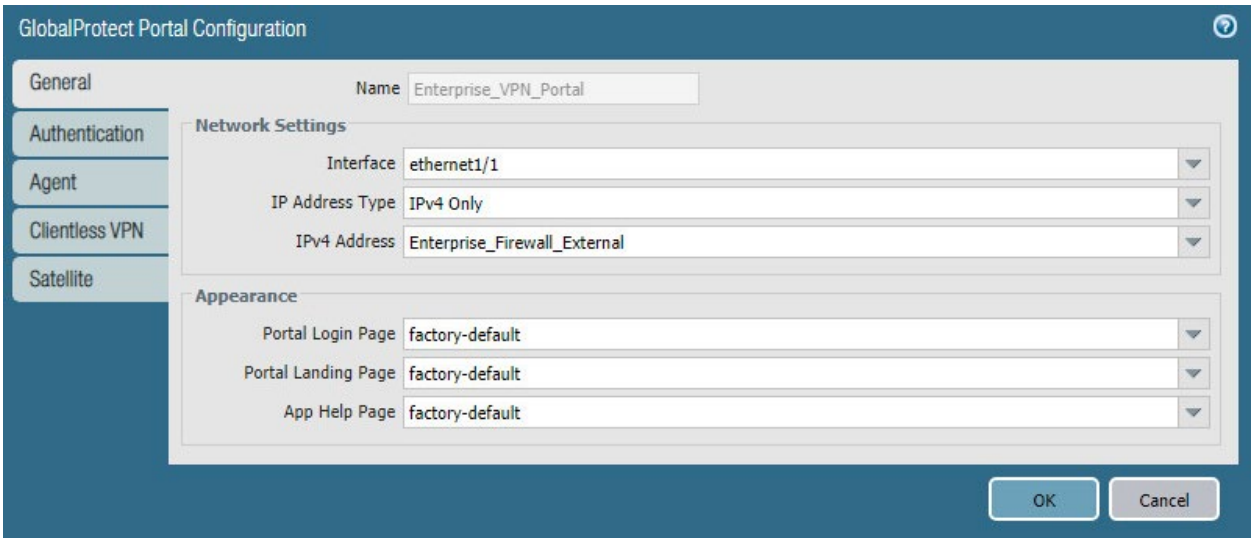
44. Click **OK**.
45. Commit the changes.

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.**

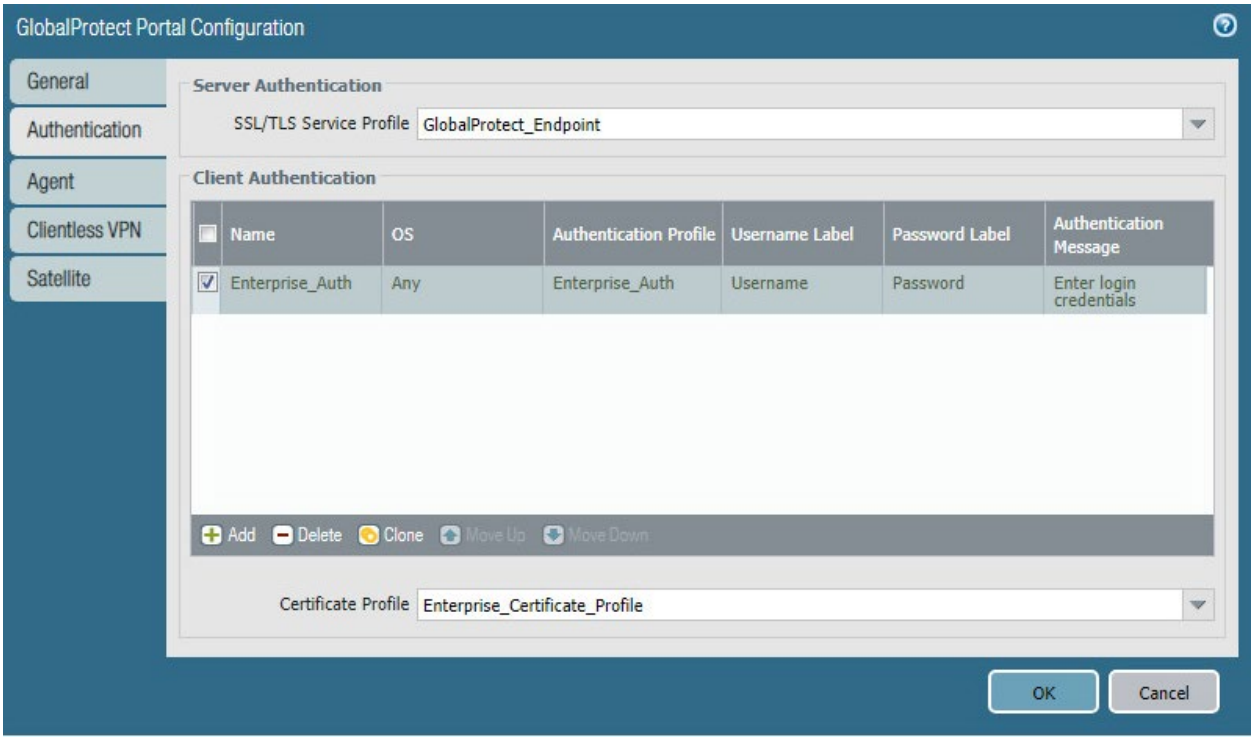
5. Set IP Address Type to **IPv4 Only**.
6. Set the IPv4 address to the firewall's **WAN address**.
7. Set all three appearance options to be **factory-default**.

Figure 2-35 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**.

975 **Figure 2-36 GlobalProtect Portal Authentication Configuration**



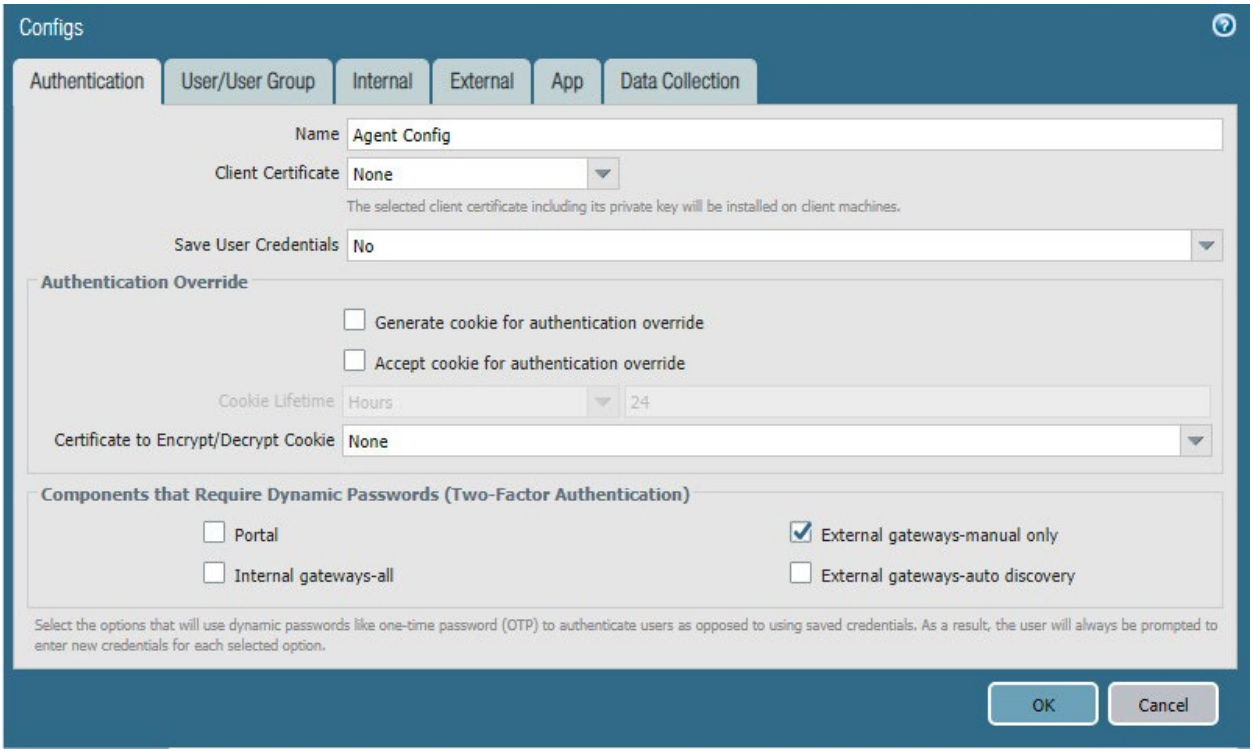
976 14. Click **Agent**, and click **Add** under **Agent**.

977 15. Give the agent configuration a name.

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

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

980 **Figure 2-37 GlobalProtect Portal Agent Authentication Configuration**



981 18. Click **External**.

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

983 20. Give the gateway a name, and enter the fully qualified domain name (FQDN) of the VPN end
984 point.

985 21. Click **Add** under **Source Region**, and select **Any**.

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

987 23. Click **OK**.

988 24. Click **App**.

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

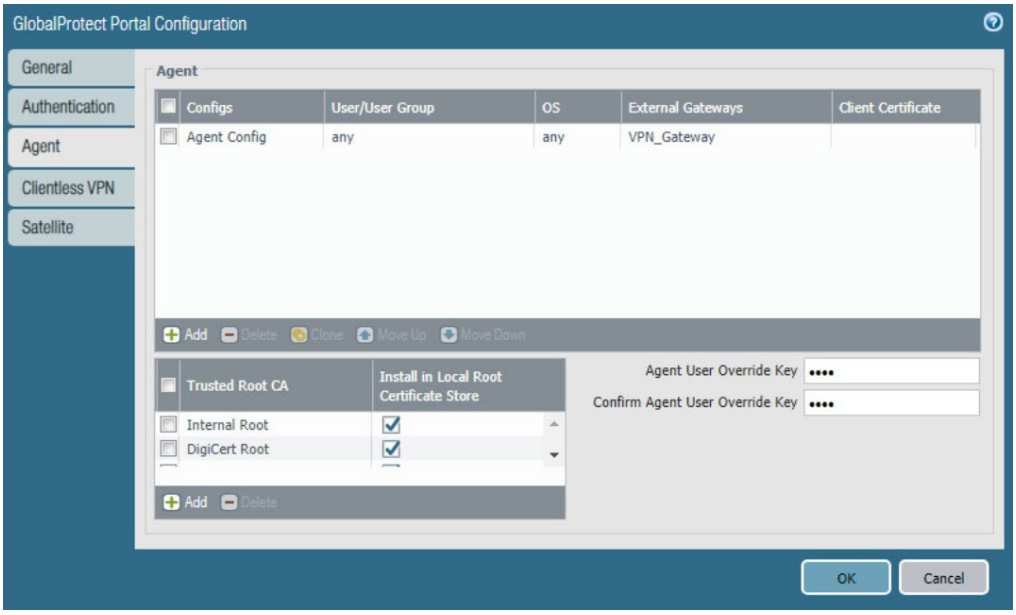
990 26. Next to **Welcome Page,** select **factory-default**.

991 27. Click **OK**.

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

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 2-38 GlobalProtect Portal Agent Configuration

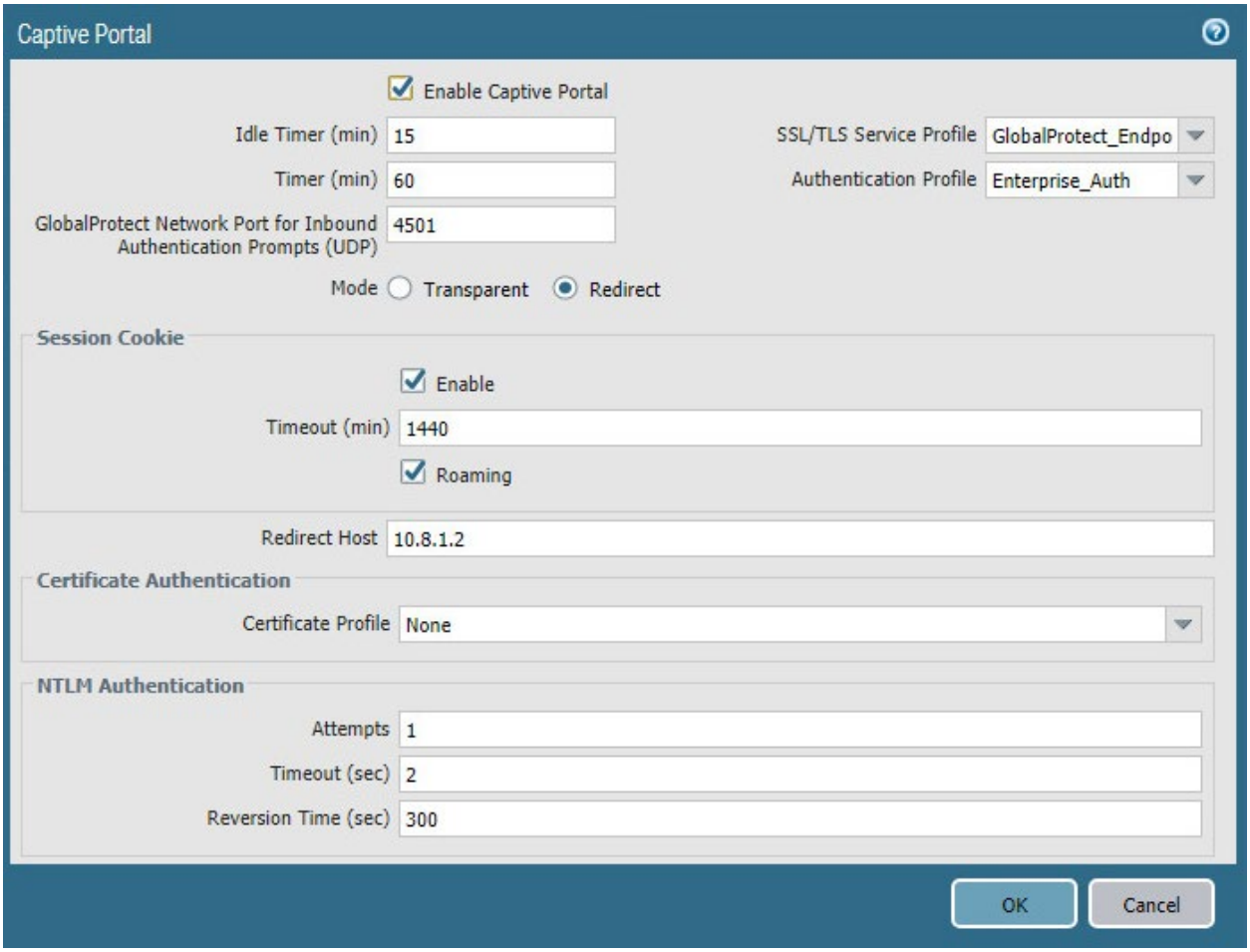


33. Click **OK.**

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**.

1008 **Figure 2-39 Captive Portal Configuration**



1009 6. Click **OK**.

1010 7. Commit the changes.

1011 ### *2.4.7.4 Activate the GlobalProtect Client*

1012 1. Navigate to **Device > GlobalProtect Client**.

1013 2. Acknowledge pop up messages.

1014 3. Click **Check Now** at the bottom of the page.

1015 4. Click **Download** next to the **first release** that comes up. In this implementation, version 5.0.2ate-
1016 was used.

1017 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 2-40 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.

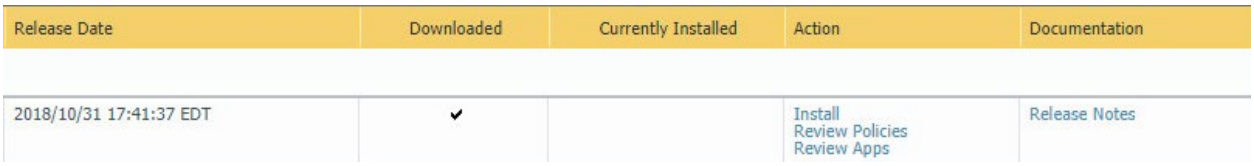
2.4.8 Enable Automatic Application and Threat Updates

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 2-41 Downloaded Threats and Applications



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

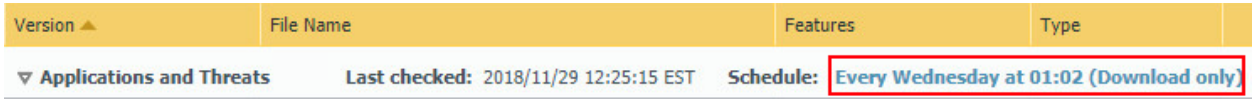
e. Click **Continue Installation,** leaving the displayed box unchecked. Installation will take a few minutes.

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 2-42.

Figure 2-42 Schedule Time Hyperlink

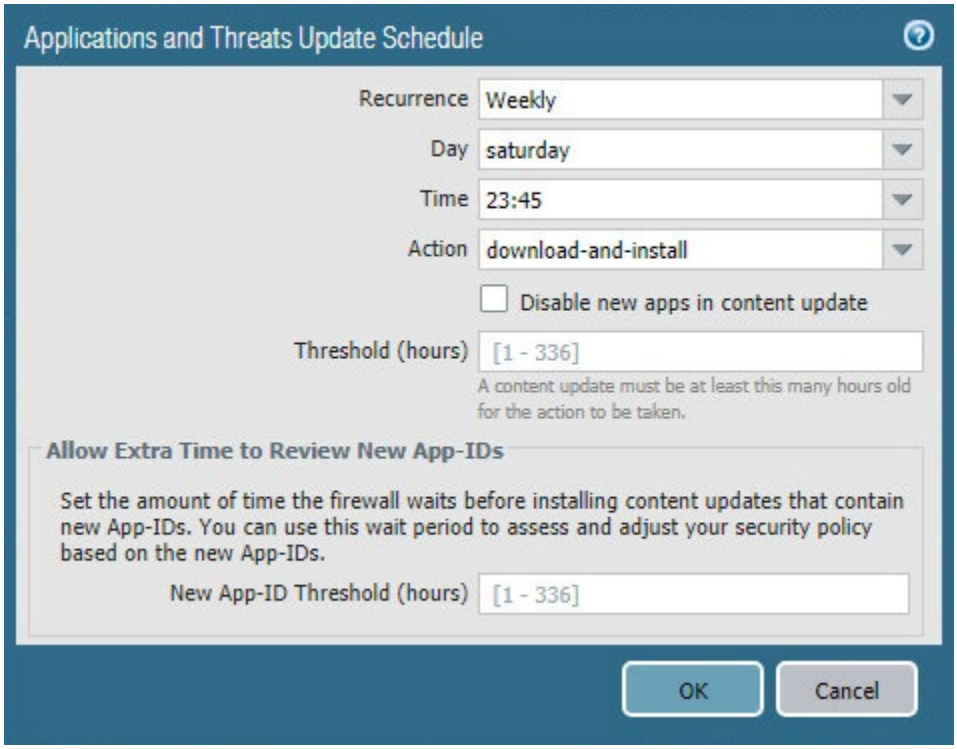


b. Select the **desired recurrence.** For this implementation, weekly was used.

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.**

1046 **Figure 2-43 Application and Threats Update Schedule**



1047 e. Click **OK.**

1048 f. Commit the changes.

1049 2.5 Kryptowire

1050 Kryptowire was used as an application vetting service via a custom active directory-integrated web
1051 application.

1052 2.5.1 Kryptowire and MaaS360 Integration

1053 1. Contact IBM support to provision API credentials for Kryptowire.

1054 2. Contact Kryptowire support to enable the MaaS360 integration, including the MaaS360 API cre-
1055 dentials.

1056 3. In the Kryptowire portal, click the **logged-in user's email address** in the upper right-hand corner
1057 of the portal. Navigate to **Settings > Analysis**.

1058 4. Set the **Threat Score Threshold** to the desired amount. In this sample implementation, 75 was
1059 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.