NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security:

Bring Your Own Device (BYOD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz
Jason G. Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

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

DRAFT

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

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security: Bring Your Own Device (BYOD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)

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.*

DRAFT

March 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Acting NIST Director and Acting Under Secretary of Commerce for Standards and Technology

NIST SPECIAL PUBLICATION 1800-22A

Mobile Device Security:

Bring Your Own Device (BYOD)

Volume A:
Executive Summary

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

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Many organizations now provide employees the flexibility to use their personal mobile devices to perform work-related activities. An ineffectively secured personal mobile device could expose an organization or employee to data loss or a privacy compromise. Ensuring that an organization's data is protected when it is accessed from personal devices poses unique challenges and threats.

Allowing employees to use their personal mobile devices for work-related activities is commonly known as a bring your own device (BYOD) deployment. A BYOD deployment offers a convenient way to remotely access organizational resources, while avoiding the alternative of carrying both a work phone and personal phone. This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-based, commercially available products to help meet their BYOD security and privacy needs.

CHALLENGE

BYOD devices can be used interchangeably for work and personal purposes throughout the day. While flexible and convenient, BYOD can introduce challenges to an enterprise. These challenges can include additional responsibilities and complexity for information technology (IT) departments caused by supporting many types of personal mobile devices used by the employees, enterprise security threats arising from unprotected personal devices, as well as challenges protecting the privacy of employees and their personal data stored on their mobile devices.

> ***An ineffectively secured personal mobile device*** *could expose an organization or employee to data loss or a privacy compromise*

SOLUTION

The National Cybersecurity Center of Excellence (NCCoE) collaborated with the mobile device community and cybersecurity technology providers to build a simulated BYOD environment. Using commercially available products, the example solution's technologies and methodologies can enhance the security posture of the adopting organization and help protect employee privacy and organizational information assets.

This practice guide can help your organization:

- **protect data** from being accessed by unauthorized persons when a device is stolen or misplaced
- **reduce risk to employees** through enhanced privacy protections
- **improve the security of mobile devices and applications** by deploying mobile device technologies
- **reduce risks to organizational data** by separating personal and work-related information from each other
- **enhance visibility** into mobile device health to facilitate identification of device and data compromise, and permit efficient user notification
- **leverage industry best practices** to enhance mobile device security and privacy

The example solution uses technologies and security capabilities (shown below) from our project collaborators. The technologies used in the solution support security and privacy standards and guidelines including the NIST Cybersecurity Framework and NIST Privacy Framework, among others. Both iOS and Android devices are supported by this guide's example solution.

Collaborator	Security Capability or Component
IBM	Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance
kryptowire	Application Vetting to determine if an application demonstrates behaviors that could pose a security or privacy risk
paloalto NETWORKS	Firewall and Virtual Private Network that controls network traffic and provides encrypted communication channels between mobile devices and other hosts
Qualcomm	Trusted Execution Environment that helps protect mobile devices from computer code with integrity issues
ZIMPERIUM. MOBILE THREAT DEFENSE	Mobile Threat Defense detects unwanted activity and informs the device owner and BYOD administrators to prevent or limit harm that an attacker could cause

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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 solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-22a: Executive Summary*, to understand the impetus for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use the following:

- *NIST SP 1800-22b: Approach, Architecture, and Security Characteristics,* which describes what we built and why, the risk analysis performed, and the security/privacy control mappings.

- *NIST SP 1800-22 Supplement: Example Scenario: Putting Guidance into Practice,* which provides an example of a fictional company using this practice guide and other NIST guidance to implement a BYOD deployment with their security and privacy requirements.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-22c: How-To Guides*, which provides specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device. Help the NCCoE make this guide better by sharing your thoughts with us. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at mobile-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

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

NIST SPECIAL PUBLICATION 1800-22B

Mobile Device Security:

Bring Your Own Device (BYOD)

Volume B:
Approach, Architecture, and Security Characteristics

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. 1800-22B, 121 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
Kevin Stine	NIST
Chris Brown	The MITRE Corporation

Name	Organization
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
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

List of Figures

List of Tables

1 Summary

This section familiarizes the reader with

- Bring Your Own Device (BYOD) concepts
- Challenges, solutions, and benefits related to BYOD deployments

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 mobile phone BYOD deployments.

Incorporating BYOD capabilities in an organization can provide greater flexibility in how employees work and can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of in-office processes with mobile device technologies enables portable communication approaches and adaptive workflows. Other organizations may adopt a mobile-first approach in which their employees communicate and collaborate primarily using their mobile devices.

Extending mobile device use by enabling BYOD capabilities in the enterprise can introduce new information technology (IT) risks to organizations. Solutions that are designed to help secure corporate devices and the data located on those corporate devices do not always provide an effective cybersecurity solution for BYOD.

Deploying effective solutions can be challenging due to the unique risks that BYOD deployments impose. Some of the features that make personal mobile devices increasingly flexible and functional also present unique security and privacy challenges to both employers and device owners.

Additionally, enabling BYOD capabilities can introduce new privacy risks to employees by providing their employer a degree of access to their personal devices, opening the possibility of mobile device observation and control that would not otherwise exist.

This practice guide helps organizations deploy BYOD capabilities by providing an example solution that helps address BYOD challenges, solutions, and benefits. In this practice guide, the term mobile phone is used to describe an Apple iOS or Android mobile telephone device. Additionally, this practice guide's scope for BYOD does not include the deployment of laptops or devices similar to laptops.

1.1 Challenge

Many organizations now authorize employees to use their personal mobile devices to perform work-related activities. This provides employees with increased flexibility to access organizational information resources. However, BYOD architectures can also introduce vulnerabilities in the enterprise’s IT infrastructure because personally owned mobile devices are typically unmanaged and may lack mobile device security protections. Unmanaged devices are at greater risk of unauthorized access to sensitive information, email phishing, eavesdropping, misuse of device sensors, or compromise of organizational data due to lost devices to name but a few risks.

BYOD deployment challenges can include:

Supporting a broad ecosystem of mobile devices

- with diverse technologies that rapidly evolve and vary in manufacturer, operating system (OS), and age of the device
- where each device has unique security and privacy requirements and capabilities
- whose variety can present interoperability issues that might affect organizational integration

Reducing organizational risk and threats to the enterprise's sensitive information

- posed by applications like games that may not usually be installed on devices issued by an organization
- that result from lost, stolen, or sold mobile devices that still contain or have access to organizational data
- created by a user who shares their personally owned device with friends and family members when that personally owned device may also be used for work activities
- due to personally owned mobile devices being taken to places that increase the risk of loss of control for the device
- that result from malicious applications compromising the device and subsequently the data to which the device has access
- produced by network-based attacks that can traverse a device's always-on connection to the internet
- caused by phishing attempts that try to collect user credentials or entice a user to install malicious software

Protecting the privacy of employees

- by helping to keep their personal photos, documents, and other data private and inaccessible to others (including the organization)
- by helping to ensure separation between their work and personal data while simultaneously meeting the organization's objectives for business functions, usability, security, and employee privacy
- by providing them with concise and understandable information about what data is collected and what actions are allowed and disallowed on their devices

Clearly communicating BYOD concepts

- among an organization's information technology team so it can develop the architecture to address BYOD's unique security and privacy concerns while using a repeatable, standardized, and clearly communicated risk framework language
- to organizational leadership and employees to obtain support in deploying BYOD

- related to mobile device security technologies so that the organization can consistently plan for and implement the protection capabilities of their security tools

Given these challenges, it can be complex to manage the security and privacy aspects of personally owned mobile devices that access organizational information assets. This document provides an example solution to help organizations address these challenges.

1.2 Solution

To help organizations benefit from BYOD's flexibility while protecting themselves from many of its critical security and privacy challenges, this National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide provides an example solution using standards-based, commercially available products and step-by-step implementation guidance.

In our lab at the National Cybersecurity Center of Excellence (NCCoE), engineers built an environment that contains an example solution for managing the security and privacy of BYOD deployments. In this guide, we show how an enterprise can leverage the concepts presented in this example solution to implement enterprise mobility management (EMM), mobile threat defense (MTD), application vetting, a trusted execution environment (TEE) supporting secure boot/image authentication, and virtual private network (VPN) services to support a BYOD solution.

We configured these technologies to protect organizational assets and employee privacy and provide methodologies to enhance the data protection posture of the adopting organization. The standards and best practices on which this example solution is based help ensure the confidentiality, integrity, and availability of enterprise data on BYOD Android and Apple mobile phones as well as the predictability, manageability, and disassociability of employee's data.

The example solution in this practice guide helps

- detect and protect against installing mobile malware, phishing attempts, and network-based attacks
- enforce passcode usage
- protect organizational data by enabling selective device wipe capability of organizational data and applications
- protect against organizational data loss by restricting an employee's ability to copy and paste, perform a screen capture, or store organizational data in unapproved locations
- organizations view BYOD risks and remediate threats (e.g., risks from jailbroken or rooted devices)
- provide users with access to protected business resources (e.g., SharePoint, knowledge base, internal wikis, application data)
- support executed code authenticity, runtime state integrity, and persistent memory data confidentiality
- protect data from eavesdropping while traversing a network

- vet the security of mobile applications used for work-related activities
- organizations implement settings to protect employee privacy
- an organization deploy its own BYOD solution by providing a series of how-to guides—step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture—to help security and privacy engineers rapidly deploy and evaluate a mobile device solution in their test environment

Commercial, standards-based products such as the ones used in this practice guide are readily available and interoperable with existing IT infrastructure and investments. Organizations can use this guidance in whole or in part to help understand and mitigate common BYOD security and privacy challenges.

1.2.1 Standards and Guidance

This guide leverages many standards and guidance, including the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1], the *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework) [2], NIST Special Publication (SP) 800-181 *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017)* [3], the NIST Risk Management Framework [4], and the NIST Mobile Threat Catalogue [5]. For additional information, see Appendix D, Standards and Guidance.

1.3 Benefits

Carrying two mobile devices, one for work and one for personal use, introduces inconveniences and disadvantages that some organizations and employees are looking to avoid. Recognizing that BYOD is being adopted, the NCCoE worked to provide organizations with guidance for improving the security and privacy of these solutions.

For organizations, the potential benefits of this example solution include

- enhanced protection against both malicious applications and loss of data if a device is stolen or misplaced
- reduced adverse effects if a device is compromised
- visibility for system administrators into mobile security compliance, enabling automated identification and notification of a compromised device
- a vendor-agnostic, modular architecture based on technology roles
- demonstrated enhanced security options for mobile access to organizational resources such as intranet, email, contacts, and calendar

For employees, the potential benefits of this example solution include

- safeguards to help protect their privacy
- better protected personal devices by screening work applications for malicious capability before installing them

- enhanced understanding about how their personal device will integrate with their organization through a standardized BYOD deployment

2 How to Use This Guide

This section familiarizes the reader with

- this practice guide's content
- the suggested audience for each volume
- typographic conventions used in this volume

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this BYOD example solution. 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* – high-level overview of the challenge, example solution, and benefits of the practice guide
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- 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

Depending on your role in your organization, you might use this guide in different ways:

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

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

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

- Appendix G, Example Security Subcategory and Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.
- Appendix H, Example Privacy Subcategory and Control Map, describes how the privacy control map identifies the privacy characteristic standards mapping for the products as they were used in the example solution.

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 deployments.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create 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 this guide's example solution for BYOD security management. Your organization's security experts should identify the products that will effectively address the BYOD risks identified for your organization and 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. Section 4.3, Technologies that Support the Security and Privacy Goals of the Example Solution, lists the products 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, *Example Scenario: Putting Guidance into Practice*.

- Appendix F of the Supplement, describes the risk analysis we performed, using an example scenario.
- Appendix G of the Supplement, describes how to conduct a privacy risk assessment and use it to improve mobile device architectures, using an example scenario.

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.

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

2.1 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.

3 Approach

This section familiarizes the reader with

- this guide's intended audience, scope, and assumptions
- mobile device security and privacy risk assessments

To identify the cybersecurity challenges associated with deploying a BYOD solution, the team surveyed reports of mobile device security trends and invited the mobile device security community to engage in a discussion about pressing cybersecurity challenges.

Two broad and significant themes emerged from this research:

- Administrators wanted to better understand what policies and standards should be implemented.
- Employees were concerned about the degree to which enterprises have control over their personally owned mobile devices and might have visibility into the personal activity that takes place on them.

The team addressed these two challenges by reviewing the primary standards, best practices, and guidelines contained within Appendix D, Standards and Guidance.

3.1 Audience

This practice guide is intended for organizations that want to adopt a BYOD architecture that enables use of personal mobile phones and tablets. The target audience is executives, security managers, privacy managers, engineers, administrators, and others who are responsible for acquiring, implementing, communicating with users about, or maintaining mobile enterprise technology. This technology can include centralized device management, secure device/application security contexts, application vetting, and endpoint protection systems.

This document will interest system architects already managing mobile device deployments and those looking to integrate a BYOD architecture into existing organizational wireless systems. It assumes that readers have a basic understanding of mobile device technologies and enterprise security and privacy principles. Please refer to Section 2 for how different audiences can effectively use this guide.

3.2 Scope

The scope of this build includes managing Apple or Android mobile phones and tablets deployed in a BYOD configuration with cloud-based EMM. We excluded laptops and mobile devices with minimal computing capability, including feature phones, and wearables. We also do not address classified systems, devices, data, and applications within this publication.

While this document is primarily about mobile device security for BYOD implementations, BYOD introduces privacy risk to the organization and its employees who participate in the BYOD program. Therefore, the NCCoE found addressing privacy risk to be a necessary part of developing the BYOD architecture. The scope of privacy in this build is limited to those employees who use their devices as part of their organization’s BYOD solution. The build does not explicitly address privacy considerations of other individuals whose information is processed by the organization through an employee’s personal device.

We intend for the example solution proposed in this practice guide to be broadly applicable to enterprises, including both the public and private sectors.

3.3 Assumptions

This project is guided by the following assumptions:

- The example solution was developed in a lab environment. While the environment is based on a typical organization’s IT enterprise, the example solution does not reflect the complexity of a production environment.
- The organization has access to the skills and resources required to implement a mobile device security and privacy solution.
- The example security and privacy control mappings provided as part of this practice guide are focused on mobile device needs, and do not include general control mappings that would also typically be used in an enterprise. Those general control mappings that do not specifically apply to this guide’s mobile device security example solution are outside the scope of this guide’s example solution.
- Because the organizational environment in which this build could be implemented represents a greater level of complexity than is captured in the current guide, we assume that organizations

will first examine the implications for their current environment before implementing any part of the proposed example solution.

- The organization has either already invested or is willing to invest in the security of mobile devices used within it and in the privacy of participating employees, and in the organization's IT systems more broadly. As such, we assume that the organization either has the technology in place to support this implementation or has access to the off-the shelf technology used in this build, which we assume will perform as described by the respective product vendor.
- The organization has familiarized itself with existing standards and any associated guidelines (e.g., NIST Cybersecurity Framework [1]; *NIST Privacy Framework* [2]; NIST SP 800-124 Revision 2 (Draft), *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]; NIST SP 1800-4 *Mobile Device Security: Cloud and Hybrid Builds* [7]) relevant to implementation of the example solution proposed in this practice guide. We also assume that any existing technology used in the example solution has been implemented in a manner consistent with these standards.
- The organization has instituted relevant mobile device security and privacy policies, and these will be updated based on implementation of this example solution.
- The organization will provide guidance and training to its employees regarding BYOD usage and how to report device loss or suspected security issues in which their devices are involved. This guidance will be periodically reviewed and updated, and employees will be regularly trained on BYOD usage.

3.4 Risk Assessment

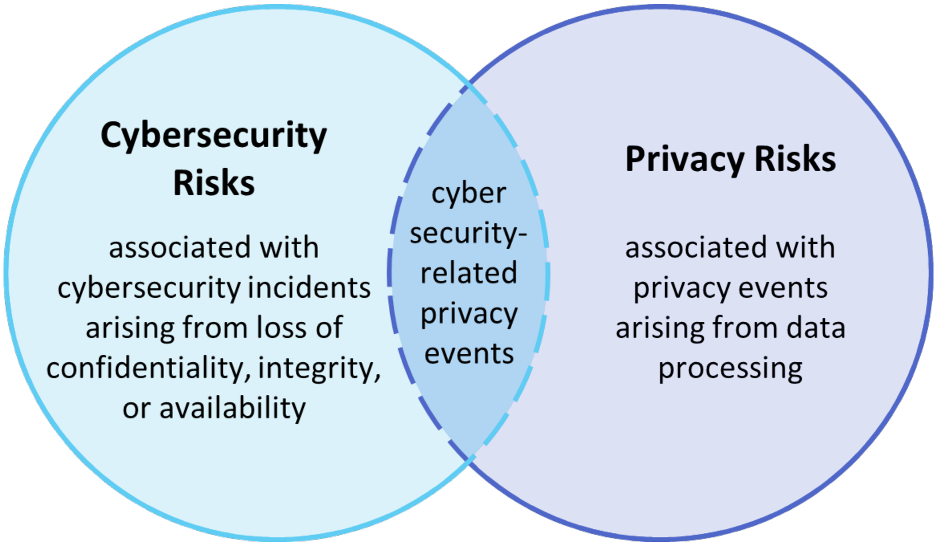
NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—material that is available to the public. The Risk Management Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

We identified the security and privacy risks for this BYOD example solution by examining the relationship of risk between cybersecurity and privacy. Cybersecurity and privacy are two distinct risk areas, though the two intersect in significant ways. As noted in Section 1.2.1 of the *NIST Privacy Framework* [2], having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Figure 3-1 illustrates this relationship, showing that some privacy risks arise from cybersecurity risks, and some are unrelated to cybersecurity risks. Allowing an unauthorized device to connect to the organization’s network through its BYOD implementation is an example of a security risk that may not impact privacy.

An example of a security risk that may also be considered a privacy risk is an employer having increased access to an employee’s personal use applications such as personal contacts and personal calendars on their device. An example of a privacy risk that is not driven by a security risk is a BYOD implementation being used to track employee location, which may reveal information about the places they visit.

Figure 3-1 Cybersecurity and Privacy Risk Relationship


Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

The security capabilities in this build help address some of the privacy risks that arise for employees. This build also uses the *NIST Privacy Framework* [2] and Privacy Risk Assessment Methodology (PRAM) [8] to identify and address privacy risks that are beyond the scope of security risks. Regardless of whether cybersecurity and privacy are situated in the same part of the organization or in different parts, the two capabilities must work closely together to address BYOD risks.

A risk assessment can include additional analysis areas. For more information on the example solution’s:

- **Security and privacy threats**, and **goals to remediate those threats**, see Section 4.1
- **Vulnerabilities** that influenced the reference architecture, see Appendix Section F-5 of the Supplement
- **Risks** that influenced the architecture development, see Appendix Section F-6 of the Supplement
- **Security Control Mapping** to cybersecurity and privacy standards and best practices, see Appendix G and Appendix H

4 Architecture

This section helps familiarize the reader with

- threats to BYOD architectures
- example solution goals to remediate threats to BYOD architectures
- how organizations might leverage the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide to implement their mobile device solution
- technologies to support the example solution goals
- the example solution's architecture
- how the example solution's products were integrated
- mobile device data collection

4.1 Understanding Common BYOD Architecture Threats and the Example Solution's Goals to Remediate Those Threats

This section contains examples of common security and privacy concerns in BYOD architectures. We provide a list of goals to address those challenges. Once completed, the architecture provides organizations with a security and privacy-enhanced design for their mobile devices. The example solution's challenges and goals are highlighted below, followed by the architecture that supports those goals.

4.1.1 Threat Events

Leveraging a system life cycle approach [9], this build considered threats relating to BYOD deployments. Information from the Open Web Application Security Project Mobile Top 10 [10], which provides a consolidated list of mobile application risks, and information from the NIST Mobile Threat Catalogue [5], which examines the mobile information system threats in the broader mobile ecosystem were used to develop applicable threats. Table 4-1 gives each threat an identifier for the purposes of this build, a description of each threat event (TE), and the related NIST Mobile Threat Catalogue Threat identifiers (IDs).

We limited inclusion of threat events to those that we generally expected to have a high likelihood of occurrence and high potential for adverse impact. Organizations applying this build should evaluate the NIST Mobile Threat Catalogue for additional threats that may be relevant to their architecture. For an example of how to determine the risk from these threats, see Appendix F in the Supplement.

Table 4-1 Examples of BYOD Deployment Threats

Threat Event ID	Threat Event Description	NIST Mobile Threat Catalogue Threat ID
TE-1	privacy-intrusive applications	APP-2, APP-12
TE-2	account credential theft through phishing	AUT-9
TE-3	malicious applications	APP-2, APP-5, APP-31, APP-40, APP-32, AUT-10
TE-4	outdated phones	APP-4, APP-26, STA-0, STA-9, STA-16
TE-5	camera and microphone remote access	APP-32, APP-36
TE-6	sensitive data transmissions	APP-0, CEL-18, LPN-2
TE-7	brute-force attacks to unlock a phone	AUT-2, AUT-4
TE-8	weak password practices protection	APP-9, AUT-0
TE-9	unmanaged device protection	EMM-5
TE-10	lost or stolen data protection	PHY-0
TE-11	protecting data from being inadvertently backed up to a cloud service	EMM-9
TE-12	personal identification number (PIN) or password-sharing protection	AUT-0, AUT-2, AUT-4, AUT-5

4.1.2 Privacy Problematic Data Actions

This build also considered operational activities of the example solution that interact with employee data during BYOD processes ("data actions"). Additionally, it identified those that potentially cause privacy-related problems for individuals ("problematic data actions"). Problematic data actions (PDAs) are those actions that may cause an adverse effect for individuals.

The NIST PRAM [8] and accompanying Catalog of Problematic Data Actions and Problems [11] were used to conduct this analysis. Table 4-2 provides the results of this analysis. See Appendix G of the Supplement for an example of determining the privacy risks based on these data actions.

Table 4-2 Examples of BYOD Potential Privacy Events and Problematic Data Actions

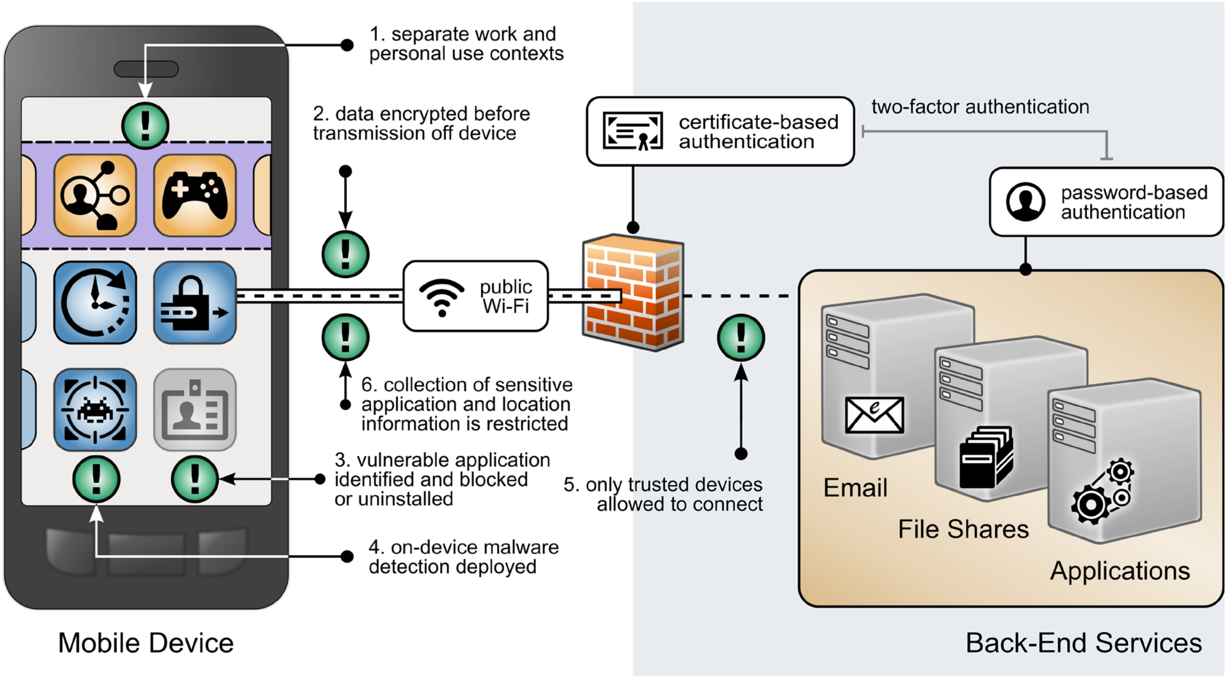
Problematic Data Action ID	Mobile Data Actions	Problematic Data Actions
PDA-1	Devices can be wiped and reset to factory settings based on inputs regarding anomalous activity and untrusted applications.	Unwarranted restriction: Blocking device access or wiping devices entirely may result in loss of personal data, which can cause employee loss of autonomy in their interactions with their device, economic loss to recover personal data, or loss of trust in the organization's BYOD implementation.

Problematic Data Action ID	Mobile Data Actions	Problematic Data Actions
PDA-2	The BYOD infrastructure comprehensively monitors device interactions related to enterprise connectivity and data processing.	Surveillance: Monitoring BYOD resources on personal devices provides a degree of visibility into personal devices that employers would not otherwise have, which in turn can result in the employer creating an incomplete narrative about employees that could lead to issues such as discrimination or employee loss of trust in the employer if the employee discovers unanticipated monitoring. Additionally, employees who connect their personal mobile device to the organization's network may not be aware of the degree of visibility into their personal activities and data and may not want this to occur. For example, employers may be able to collect location information or application data that provides insights into employee health. Employees may feel as though they are being surveilled.
PDA-3	Data about individuals and their devices flows between various applications and analytical tools, some of which may be shared with third parties and publicly.	Unanticipated revelation: Transmission of employee device information and personal data to the employer and third parties beyond the employer may occur through monitoring, data sharing across parties for analytics, and other operational purposes. Administrator and co-worker awareness of otherwise private activities on devices may reveal information about employees that results in dignity losses, such as embarrassment or emotional distress. Data transmission about individuals and their devices among a variety of different parties could be confusing for employees who might not know who has access to information about them. This transmission could reveal personal information about the employee to parties they would not expect to have such information. This lack of employee visibility and awareness of data-sharing practices may also cause employee loss of trust in the employer.

4.1.3 Security and Privacy Goals

To address the challenges stated in the previous sections, the architecture for this build addresses the high-level security and privacy goals illustrated in Figure 4-1.

Figure 4-1 Security and Privacy Goals


1. separate work and personal use contexts
2. data encrypted before transmission off device
certificate-based authentication
two-factor authentication
password-based authentication
public Wi-Fi
6. collection of sensitive application and location information is restricted
3. vulnerable application identified and blocked or uninstalled
5. only trusted devices allowed to connect
4. on-device malware detection deployed
Email
File Shares
Applications
Mobile Device
Back-End Services

The following goals were highlighted above in Figure 4-1 Security and Privacy Goals, with a green exclamation mark:

1. **Separate organization and personal information.** BYOD deployments can place organizational data at risk by allowing it to travel outside internal networks and systems when it is accessed on a personal device. BYOD deployments can also place personal data at risk by capturing information from employee devices. To help mitigate this, organizational and personal information can be separated by restricting data flow between organizationally managed and unmanaged applications. The goals include helping to prevent sensitive data from crossing between work and personal contexts.

2. **Encrypt data in transit.** Devices deployed in BYOD scenarios can leverage nonsecure networks, putting data at risk of interception. To help mitigate this, mobile devices can connect to the organization over a VPN or similar solution to encrypt all data before it is transmitted from the device, protecting otherwise unencrypted data from interception. A user would not be able to access the organization's resources without an active VPN connection and required certificates.

3. **Identify vulnerable applications.** Employees may install a wide range of applications on their personally owned devices, some of which may have security weaknesses. When vulnerable personal applications are identified, an organization can remove the employee's work profile or configuration file from the device rather than uninstalling the employee's personal applications.

4. **Detect malware.** On personally owned devices without restriction policies in place, users may obtain applications outside official application stores, increasing the risk of installing malware in disguise. To help protect from this risk, an organization could deploy malware detection to devices to identify malicious applications and facilitate remediation.

5. **Trusted device access.** Because mobile devices can connect from unknown locations, an organization can provision mobile devices with a security certificate that allows identifying and authenticating them at the connection point, which combines with user credentials to create two-factor authentication from mobile devices. An employee would not be able to access the organization's resources without the required certificates.

6. **Restrict information collection.** Mobile device management tools can track application inventory and location information, including physical address, geographic coordinates, location history, internet protocol (IP) address, and Secure Set Identifier (SSID). These capabilities may reveal sensitive information about employees, such as frequently visited locations or habits. Device management tools can be configured to exclude application and location information. Excluding the collection of information further protects employee privacy when device and application data is shared outside the organization for monitoring and analytics.

4.2 Example Scenario: Putting Guidance into Practice

The example solution's high-level goals underscore the need to use a thorough risk assessment process for organizations implementing mobile device security capabilities. To learn more about how your organization might implement this example solution, reference the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide. The supplement provides an example approach for developing and deploying a BYOD architecture that directly addresses the mobile device threat events and problematic data actions discussed in this guide.

The example scenario supplement shows how a fictional organization used the guidance in NIST's Cybersecurity Framework [1], Privacy Framework [2], Risk Management Framework [9], and PRAM [8] to identify and address their BYOD security and privacy goals.

4.3 Technologies that Support the Security and Privacy Goals of the Example Solution

This section describes the mobile-specific technology components used within this example solution. These technologies were selected to address the security goals, threat events, and problematic data actions identified in Section 4.1. This section provides a brief description of each technology and discusses the security and privacy capabilities that each component provides.

The technology components in this section are combined into a cohesive enterprise architecture to help address BYOD security threats and problematic data actions and provide security-enhanced access to enterprise resources from mobile devices. The technologies described in this section provide protection for enterprise resources accessed by BYOD users.

4.3.1 Trusted Execution Environment

A trusted execution environment (TEE) is “a tamper-resistant processing environment that runs on a ‘separation kernel’. It guarantees the authenticity of the executed code, the integrity of the runtime states (e.g., central processing unit (CPU) registers, memory and sensitive I/O), and the confidentiality of its code, data and runtime states stored on a persistent memory. In addition, it shall be able to provide remote attestation that proves its trustworthiness for third-parties” [12]. The TEE helps protect the mobile devices from executed code with integrity issues. This is important in BYOD environments due to an enterprise’s limited control over an employee’s personally owned device. Users can install and run many types of applications on personally owned devices without restriction from the enterprise.

4.3.2 Enterprise Mobility Management

Organizations use EMM solutions to secure the mobile devices of users who are authorized to access organizational resources. Such solutions generally have two main components. The first is a backend service that mobile administrators use to manage the policies, configurations, and security actions applied to registered mobile devices. The second is an on-device agent, usually in the form of a mobile application, that integrates between the mobile OS and the solution’s backend service. iOS also supports a web-based EMM enrollment use case, which we do not discuss in this document.

At a minimum, an EMM solution can perform mobile device management (MDM) functions, which include the ability to provision configuration profiles to devices, enforce security policies on devices, and monitor compliance with those policies. The on-device MDM agent can typically notify the device user of any noncompliant settings and may be able to remediate some noncompliant settings automatically. The organization can use policy compliance data to inform its access control decisions so that it grants access only to a device that demonstrates the mandated level of compliance with the security policies in place.

EMM solutions commonly include any of the following capabilities: mobile application management, mobile content management, and implementations of or integrations with device- or mobile-OS-specific containerization solutions, such as Samsung Knox. These capabilities can be used in the following ways:

- Mobile application management can be used to manage the installation and usage of applications based on their trustworthiness and work relevance.
- Mobile content management can control how managed applications access and use organizational data.
- Containerization solutions can strengthen the separation between a user’s personal and professional usage of the device.
- Also, EMM solutions often have integrations with a diverse set of additional tools and security technologies that enhance their capabilities.

For further reading on this topic, NIST SP 800-124 Revision 2 (Draft), *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6] provides additional information on mobile device management with EMM solutions. The National Information Assurance Partnership’s (NIAP’s) *Protection*

Profile for Mobile Device Management Servers and Extended Package for Mobile Device Management Agents [13] describes important capabilities and security requirements to look for in EMM systems.

EMMs can help BYOD deployments improve the security posture of the organization by providing a baseline of controls to limit attack vectors and help protect enterprise information that is on a personally owned device. EMMs can also provide an additional layer of separation between enterprise data and personal data on a mobile device.

4.3.3 Virtual Private Network

A VPN gateway increases the security of remote connections from authorized mobile devices to an organization's internal network. A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communication channel for data and system control information transmitted between networks. VPNs are used most often to protect communications carried over public networks from eavesdropping and interception. A VPN can provide several types of data protection, including confidentiality, integrity, authentication of data origin, replay protection, and access control that help reduce the risks of transmitting data between network components.

VPN connections apply an additional layer of encryption to the communication between remote devices and the internal network, and VPN gateways can enforce access control decisions by limiting what devices or applications can connect to them. Integration with other security mechanisms allows a VPN gateway to base access control decisions on more risk factors than it may be able to collect on its own; examples include a device's level of compliance with mobile security policies or the list of installed applications as reported by an integrated EMM and/or MTD.

NIAP's *Module for Virtual Private Network (VPN) Gateways 1.0* [14], in combination with *Protection Profile for Network Devices* [15], describes important capabilities and security requirements to expect from VPN gateways.

In a BYOD deployment, an enterprise can also leverage a per-application VPN to provide a secure connection over the VPN tunnel strictly when using enterprise applications on the mobile device. Personal applications on the device would not be allowed to use the VPN, ensuring the enterprise has visibility into enterprise traffic only. This is especially important to BYOD deployments, whose devices may connect over a wide variety of wireless networks. It also provides a layer of privacy protection for employees by preventing personal mobile device traffic from being routed through the enterprise.

4.3.4 Mobile Application Vetting Service

Mobile application vetting services use a variety of static, dynamic, and behavioral techniques to determine if an application demonstrates any behaviors that pose a security or privacy risk. The risk may be to a device owner or user, to parties that own data on the device, or to external systems to which the application connects. The set of detected behaviors is often aggregated to generate a singular score that estimates the level of risk (or conversely, trustworthiness) attributed to an application. Clients can often adjust the values associated with given behaviors (e.g., hardcoded cryptographic keys) to tailor the score for their unique risk posture. Those scores may be further aggregated to present a score that represents the overall risk or trustworthiness posed by the set of applications currently installed on a given device.

Mobile applications, malicious or benign, can affect both security and user privacy negatively. A malicious application can contain code intended to exploit vulnerabilities present in potentially any targeted hardware, firmware, or software on the device. Alternatively, or in conjunction with exploit code, a malicious application may misuse any device, personal, or behavioral data to which it has been explicitly or implicitly granted access, such as contacts, clipboard data, or location services. Benign applications may still present vulnerabilities or weaknesses that malicious applications can exploit to gain unauthorized access to the device's data or functionality. Further, benign applications may place user privacy at risk by collecting more information than is necessary for it to deliver the functionality desired by the user.

While not specific to applications, some services may include device-based risks (e.g., lack of disk encryption or vulnerable OS version) in their analysis to provide a more comprehensive assessment of the risk or trustworthiness presented by a device when running an application or service.

While NIAP does not provide a protection profile for application vetting services, their *Protection Profile for Application Software* [16] describes security requirements to be expected from mobile applications. Many mobile application vetting vendors provide capabilities to automate evaluation of applications against NIAP's requirements.

Application vetting services help improve the security and privacy posture of the mobile devices by assessing the risk of the applications that may be installed on a personally owned device. Depending on the deployment strategy, the application vetting service may analyze all installed applications, enterprise-only applications, or no applications.

4.3.5 Mobile Threat Defense

MTD generally takes the form of an application that is installed on the device that provides information about the device's threat posture based on risks, security, and activity on the device. This is also known as endpoint protection. Ideally, the MTD solution will be able to detect unwanted activity and properly inform the user and BYOD administrators so they can act to prevent or limit the harm that an attacker could cause. Additionally, MTD solutions may integrate with EMM solutions to leverage the MTD agent's greater on-device management controls and enforcement capabilities, such as blocking a malicious application from being launched until the user can remove it.

While detecting threats, MTD products typically analyze device-based threats, application-based threats, and network-based threats. Device-based threats include outdated OS versions, nonsecure configurations, elevation of privileges, unmanaged profiles, and compromised devices. Application-based threat detection can provide similar functionality to that of dedicated application vetting services. However, application-based threat detection may not provide the same level of detail in its analysis as dedicated application vetting services. Network-based threats include use of unencrypted and/or public Wi-Fi networks and attacks such as active attempts to intercept and decrypt network traffic.

Because BYOD mobile phones can have a wide variety of installed applications and usage scenarios, MTD helps improve the security and privacy posture by providing an agent-based capability to detect unwanted activity.

4.3.6 Mobile Operating System Capabilities

Mobile OS capabilities are available without the use of additional security features. They are included as part of the mobile device's core capabilities. The following mobile OS capabilities can be found in mobile devices, particularly mobile phones.

4.3.6.1 Secure Boot

Secure boot is a general term that refers to a system architecture that is designed to prevent and detect any unauthorized modification to the boot process. A system that successfully completes a secure boot has loaded its start-up sequence information into a trusted OS. A common mechanism is for the first program executed (a boot loader) to be immutable (stored on read-only memory or implemented strictly in hardware). Further, the integrity of mutable code is cryptographically verified by either immutable or verified code prior to execution. This process establishes a chain of trust that can be traced back to immutable, implicitly trustworthy code. Using an integrated TEE as part of a secure boot process is preferable to an implementation that uses software alone [17].

4.3.6.2 Device Attestation

This is an extension of the secure boot process that involves the OS (or more commonly, an integrated TEE) providing cryptographically verifiable proof that it has a known and trusted identity and is in a trustworthy state. This means that all software running on the device is free from unauthorized modification.

Device attestation requires cryptographic operations using an immutable private key that can be verified by a trusted third party, which is typically the original equipment manufacturer of the TEE or device platform vendor. Proof of possession of a valid key establishes the integrity of the first link in a chain of trust that preserves the integrity of all other pieces of data used in the attestation. It will include unique device identifiers, metadata, the results of integrity checks on mutable software, and possibly metrics from the boot or attestation process itself [17].

4.3.6.3 Mobile Device Management Application Programming Interfaces

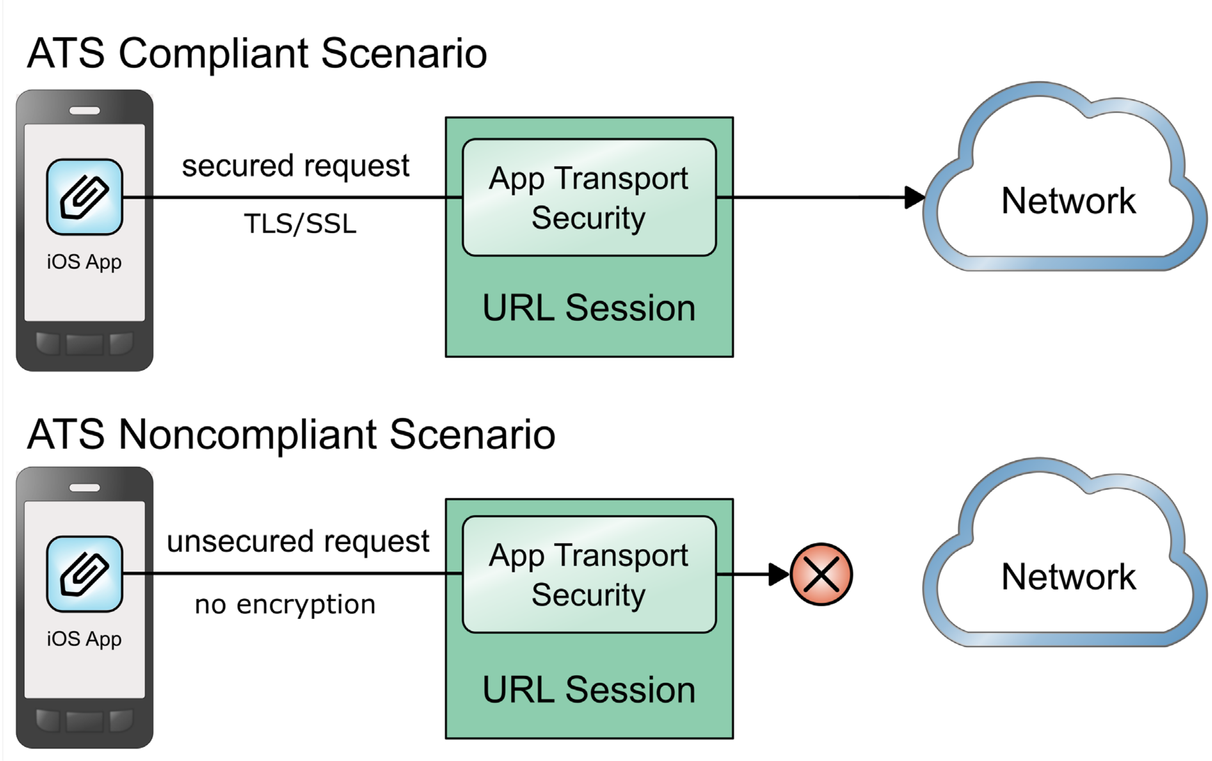
Mobile OS and platform-integrated firmware can provide a number of built-in security features that are generally active by default. Examples include disk- and file-level encryption, verification of digital signatures for installed software and updates, a device unlock code, remote device lock, and automatic device wipe following a series of failed device unlock attempts. The user can directly configure some of these features via a built-in application or through a service provided by the device platform vendor.

Additionally, mobile operating systems expose an application programming interface (API) to MDM products that allow an organization that manages a device to have greater control over these and many more settings that might not be directly accessible to the device user. Management APIs allow enterprises using integrated EMM or MDM products to manage devices more effectively and efficiently than they could by using the built-in application alone.

4.3.6.4 iOS App Transport Security

App Transport Security (ATS) is a networking security feature on Apple iOS devices that increases data integrity and privacy for applications and extensions [18], [19]. ATS requires that the network connections made by applications are secured through the Transport Layer Security protocol, which uses reliable cipher suites and certificates. In addition, ATS blocks any connection that does not meet minimum security requirements. For applications linked to iOS 9.0 and later, ATS is enabled by default. Figure 4-2 shows how ATS compliant and noncompliant applications function. As demonstrated in the figure, secured application requests are allowed, and nonsecure requests are blocked.

Figure 4-2 iOS App Transport Security



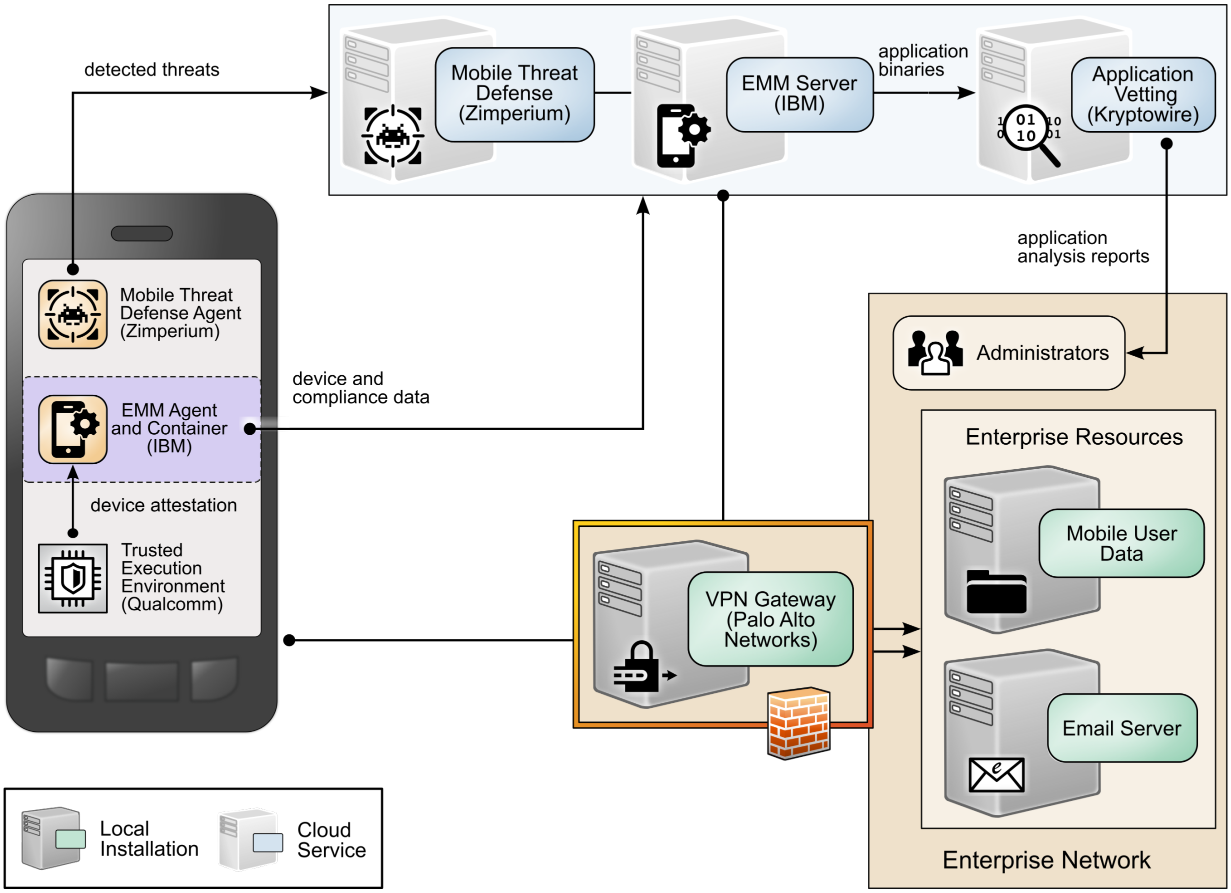
4.3.6.5 Android Network Security Configuration

With data privacy becoming even more important, Google released mobile OS enhancements to protect data that traverses Android devices and endpoints [20], [21]. The Android Network Security Configuration prevents applications from transmitting sensitive data unintentionally in unencrypted cleartext. By default, `cleartextTrafficPermitted` is set to `false`. Through the Android Network Security Configuration feature, developers can designate what certification authorities are trusted to ensure secure communications and issue certificates.

4.4 Architecture Description

The example solution architecture consists of the security technologies described in Section 4.3. The security technologies are further integrated with broader enterprise security mechanisms and a VPN gateway as shown in Figure 4-3. This example solution provides a broad range of capabilities to securely provision and manage devices, protect against and detect device compromise, and provide secure access to enterprise resources to only authorized mobile users and devices.

Figure 4-3 Example Solution Architecture


detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
01
10
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Local Installation
Cloud Service
Enterprise Network

The NCCoE worked with industry experts to develop an open, standards-based, architecture using commercially-available products to address the threats and problematic data actions identified in Section 4.1.

Where possible, the architecture uses components that are present on the NIAP Product Compliant List, meaning that the product has been successfully evaluated against a NIAP-approved protection profile. The NIAP collaborates with a broad community, including industry, government, and international partners, to publish technology-specific security requirements and tests in the form of protection profiles. The requirements and tests in these protection profiles are intended to ensure that evaluated products address identified security threats and provide risk mitigation measures.

The security and privacy characteristics of the architecture result from many of the capability integrations outlined in Section 4.5.

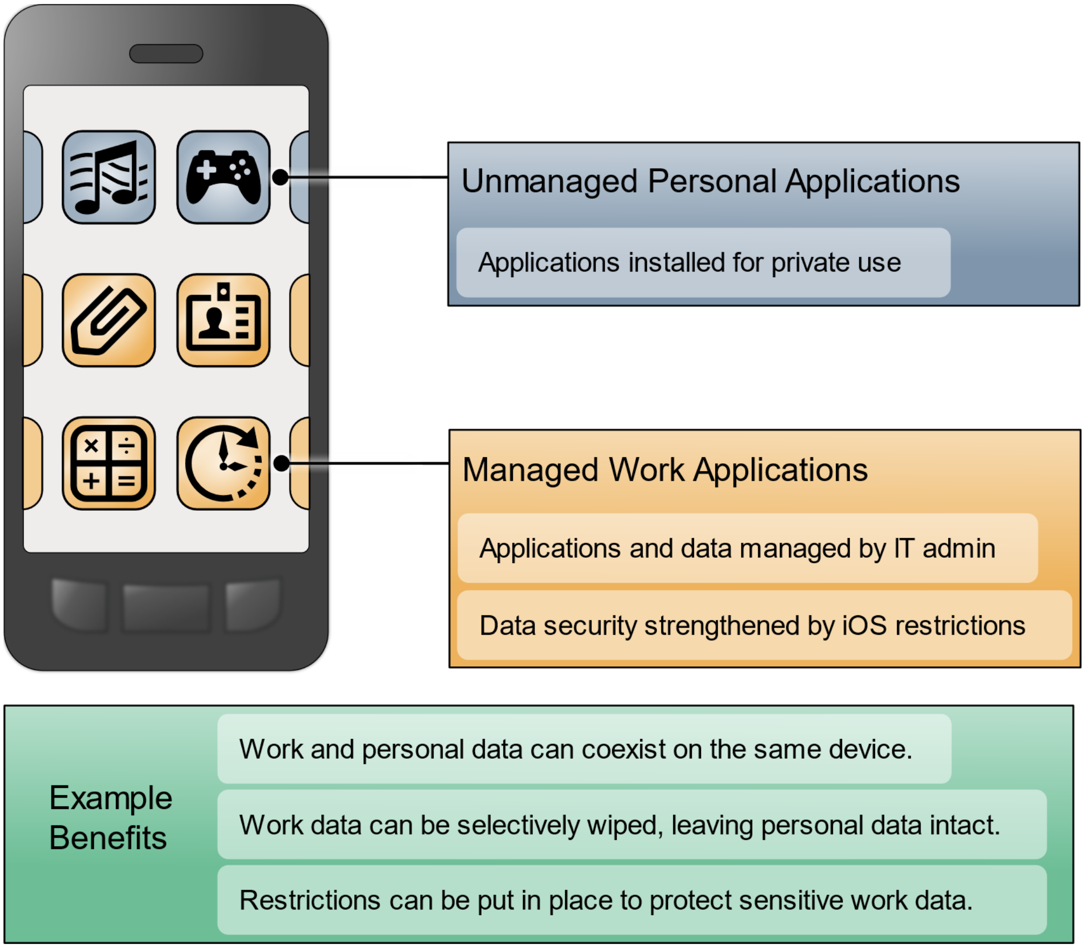
4.5 Enterprise Integration of the Employees' Personally Owned Mobile Devices

One key benefit of BYOD solutions for employees is the ability to access both work and personal data on the same device. While the technical approaches differ between iOS and Android devices, both operating systems offer the following types of features for managing the coexistence of work and personal data on devices [22], [23]:

- data flow restriction between enterprise and personal applications
- restriction of application installation from unknown sources
- selective wiping to remove enterprise data and preserve personal data
- device passcode requirement enforcement
- application configuration control
- identity and certificate authority certificate support

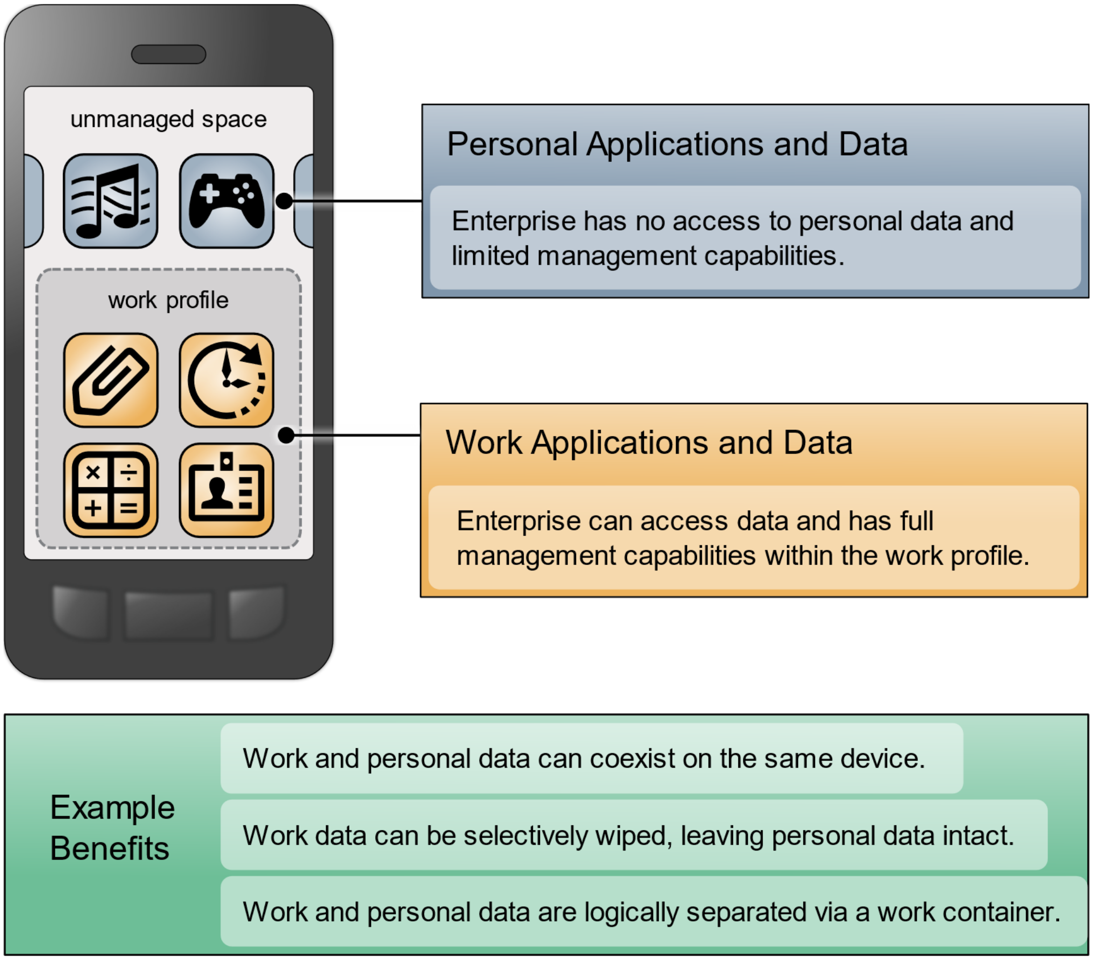
Illustrating this concept, Figure 4-4 iOS Application Management and Benefits, shows enterprise integration for managed and unmanaged applications on iOS devices. To protect sensitive work data, application restrictions, such as preventing the ability to copy data between work and personal application, are applied.

Figure 4-4 iOS Application Management and Benefits


Unmanaged Personal Applications
Applications installed for private use
Managed Work Applications
Applications and data managed by IT admin
Data security strengthened by iOS restrictions
Example Benefits
Work and personal data can coexist on the same device.
Work data can be selectively wiped, leaving personal data intact.
Restrictions can be put in place to protect sensitive work data.

As illustrated in Figure 4-5, for Android devices, work applications can be separated into a container, with data access restricted between the personal and work container applications.

Figure 4-5 Android Application Management and Benefits


unmanaged space
work profile
Personal Applications and Data
Enterprise has no access to personal data and limited management capabilities.
Work Applications and Data
Enterprise can access data and has full management capabilities within the work profile.
Example Benefits
Work and personal data can coexist on the same device.
Work data can be selectively wiped, leaving personal data intact.
Work and personal data are logically separated via a work container.

4.5.1 Microsoft Active Directory Integration

The example solution is integrated with Microsoft Active Directory (AD), which provides both enterprise identity management and certificate enrollment services via public key infrastructure. International Business Machines (IBM) MaaS360 connects directly to the domain controller and the Network Device Enrollment Service (NDES) servers via an IBM Cloud Extender installed on the local intranet, while GlobalProtect connects to the domain controller via the Palo Alto Networks firewall’s Lightweight Directory Access Protocol service route.

By integrating directly with the AD infrastructure, administrators can configure MaaS360 to accept enrollment requests based on user groups in AD. GlobalProtect can inherit these roles and enforce access control protocols to restrict/deny permissions to the VPN. The AD integration is also used within MaaS360 to provide policy-based access to the MaaS360 administration console.

The Certificate Integration module within the MaaS360 Cloud Extender allows user certificates to be installed on the user's devices when enrolling with MaaS360. These certificates are then validated in GlobalProtect during the VPN authentication sequence, along with the user's corporate username and password. The Cloud Extender requests these certificates from the NDES server by using the Simple Certificate Enrollment Protocol (SCEP).

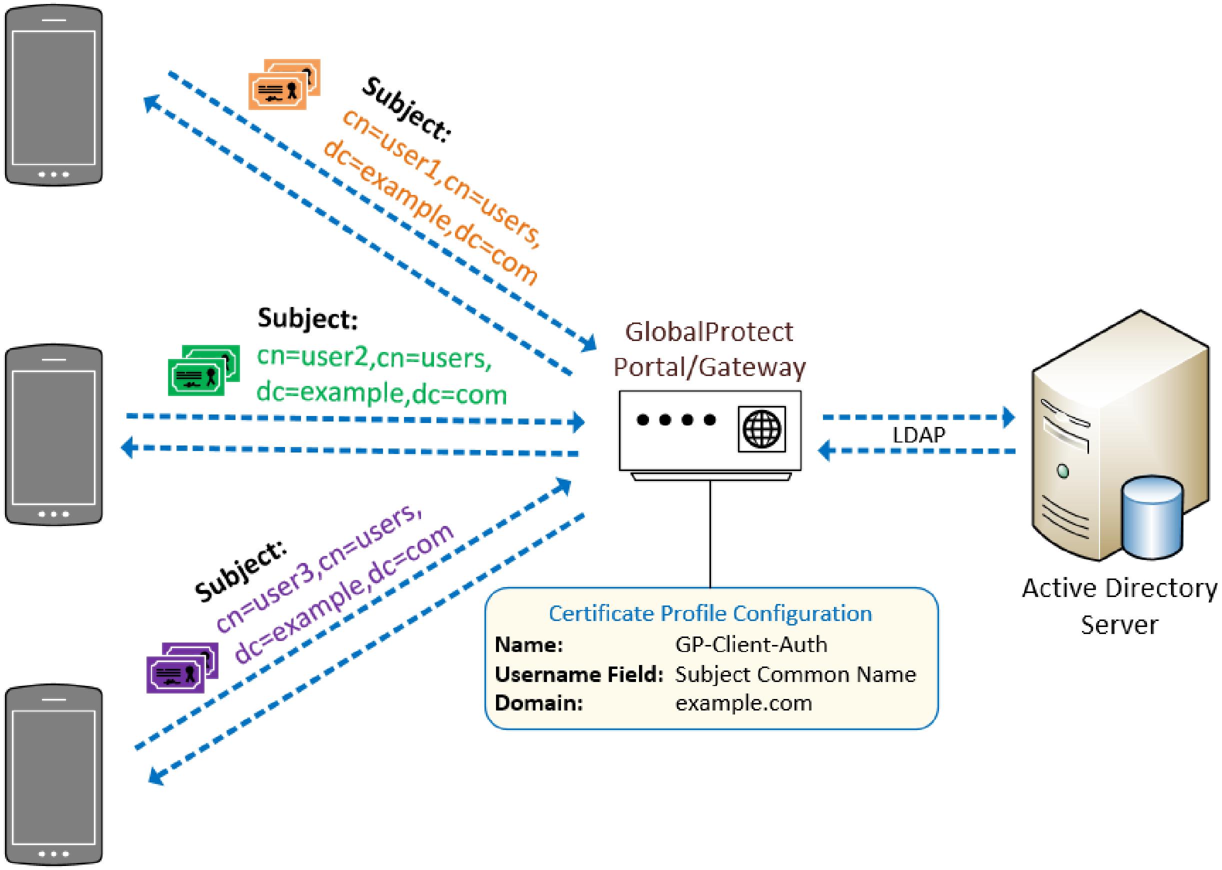
4.5.2 Mobile Device Enrollment

The example solution shown in Figure 4-6 mitigates the potential for SCEP to be remotely exploited by restricting certificate enrollment to mobile devices that are connected to a dedicated enterprise-managed Wi-Fi network. The uniform resource locator (URL) of the NDES server is resolvable only on this managed Wi-Fi network.

Furthermore, the NDES server is configured to require a dynamic challenge with each request. The Cloud Extender does this by including a one-time password with each request. This helps prevent unknown devices from requesting certificates. These certificates can then be used to prove identity when authenticating with the GlobalProtect VPN.

The certificate template includes the user's username and email address. This allows the GlobalProtect gateway to enforce access control and identity verification.

903 **Figure 4-6 Example Solution VPN Authentication Architecture**



904 4.6 Mobile Components Integration

905 IBM MaaS360 supports integration of third-party applications and cloud services via a representational
906 state transfer (REST) API [24]. External services are authenticated via access tokens, obtained through
907 MaaS360 support. Zimperium and Kryptowire used the REST API [25].

908 Table 4-3 identifies the commercially available products used in this example solution and how they
909 align with the mobile security technologies. For additional information, Appendices G and H contain a
910 mapping of these technologies to the cybersecurity and privacy standards and best practices that each
911 product provides in the example solution.

Table 4-3 Commercially Available Products Used

Commercially Available Product	Mobile Security Technology
IBM MaaS360 Mobile Device Management (SaaS) Version 10.73 IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android) IBM MaaS360 Cloud Extender Cloud Extender Modules: Certificate Integration Module Version 2.96.000 Cloud Extender Base Module Version 2.96.000 Cloud Extender Basic Module Device Version 2.96.000 MaaS360 Configuration Utility Module Version 2.96.200 Mobile Device Management Module Version 2.31.020 User Authentication Module Version 2.96.200	mobile device management
Kryptowire Cloud Service	application vetting
Palo Alto Networks PA-VM-100 Version 9.0.1 Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android)	firewall virtual private network
Qualcomm (Version is mobile device dependent)	trusted execution environment
Zimperium Defense Suite Zimperium Console Version vGA-4.23.1 Zimperium zIPS Agent Version 4.9.2 (Android and iOS)	mobile threat defense

4.6.1 Zimperium–MaaS360

Through the MaaS360 REST API, Zimperium can retrieve various device attributes, such as device name, model, OS, OS version, and owner's email address. It then continuously monitors the device's risk posture through the Zimperium Intrusion Prevention System (zIPS) application and reports any changes in the posture to MaaS360. This enables MaaS360 administrators to apply different device policies and enforcement actions based on the risk posture of a device.

When a device is enrolled with MaaS360, the zIPS application is automatically installed and configured on the device. When the user first launches the zIPS application, it will automatically enroll the device in Zimperium's MTD service. zIPS will then continuously monitor the device for threats, and any detected threats will be reported to Zimperium. Zimperium can then report to MaaS360 if any changes in risk posture occurred.

MaaS360 can respond to the following risk posture levels, as assigned by Zimperium:

- low
- normal
- elevated
- critical

4.6.2 Kryptowire–MaaS360

Through the MaaS360 REST API, Kryptowire can retrieve a list of enrolled devices, device metadata, and the inventory of applications installed on those devices. This allows Kryptowire to automatically analyze all new applications installed on enrolled devices, ensuring that the risk posture of the devices, and therefore the enterprise, stays at an acceptable level.

Kryptowire also has configurable threat scores for various factors, such as requested permissions and hardcoded encryption keys.

The threat scores can be configured to one of four levels:

- low
- medium
- high
- critical

The administrator can configure a threat score alert threshold and an email address to receive alerts when an application's threat score is at or above the threshold. The administrator can then take appropriate action on the device in MaaS360.

Further, Kryptowire can provide information about applications including the latest version, when it was last seen, when tracking began, and the number of versions that have been seen.

4.6.3 Palo Alto Networks–MaaS360

Palo Alto Networks GlobalProtect VPN secures remote connections from mobile devices. MaaS360 offers specific configuration options for the GlobalProtect client, using certificate-based authentication to the GlobalProtect gateway and available for Android and iOS, that facilitate deployment of VPN clients and enabled VPN access. Section 4.5 presents details of the certificate enrollment process.

Two components of the Palo Alto Networks next-generation firewall compose the VPN architecture used in this example solution–a GlobalProtect portal and a GlobalProtect gateway. The portal provides the management functions for the VPN infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s). A GlobalProtect gateway provides security enforcement for network traffic. The GlobalProtect gateway in this example solution is configured to provide mobile device users with access to specific enterprise resources from the secure contexts after a successful authentication and authorization decision.

The VPN tunnel negotiation between the VPN endpoint/mobile device context and the VPN gateway has four steps: (1) The portal provides the client configuration, (2) a user logs into the system, (3) the agent automatically connects to the gateway and establishes a VPN tunnel, and (4) the security policy on the gateway enables access to internal and external applications.

For this example solution, a per-application VPN configuration is enforced on iOS and an always-on work container VPN configuration on Android. This configuration forces the device to automatically establish a VPN connection to the GlobalProtect gateway whenever an application in the predefined list of applications runs on the device or when an application in the work container is launched.

4.6.4 iOS and Android MDM Integration

Both iOS and Android integrate directly with MaaS360. Configuration profiles manage iOS devices. Configuration profiles can force security policies such as VPN usage, ActiveSync support, access to cloud services, application compliance, passcode policy, device restrictions, and Wi-Fi settings.

Android devices are managed by Android Enterprise, which provides controls for both the device itself and the work container. The work container is a special folder on the phone that stores all the enterprise applications and data, ensuring separation from personal applications and data. This is implemented as a profile owner solution, as opposed to Corporate-Owned Personally-Enabled (COPE), which is implemented as a device owner solution.

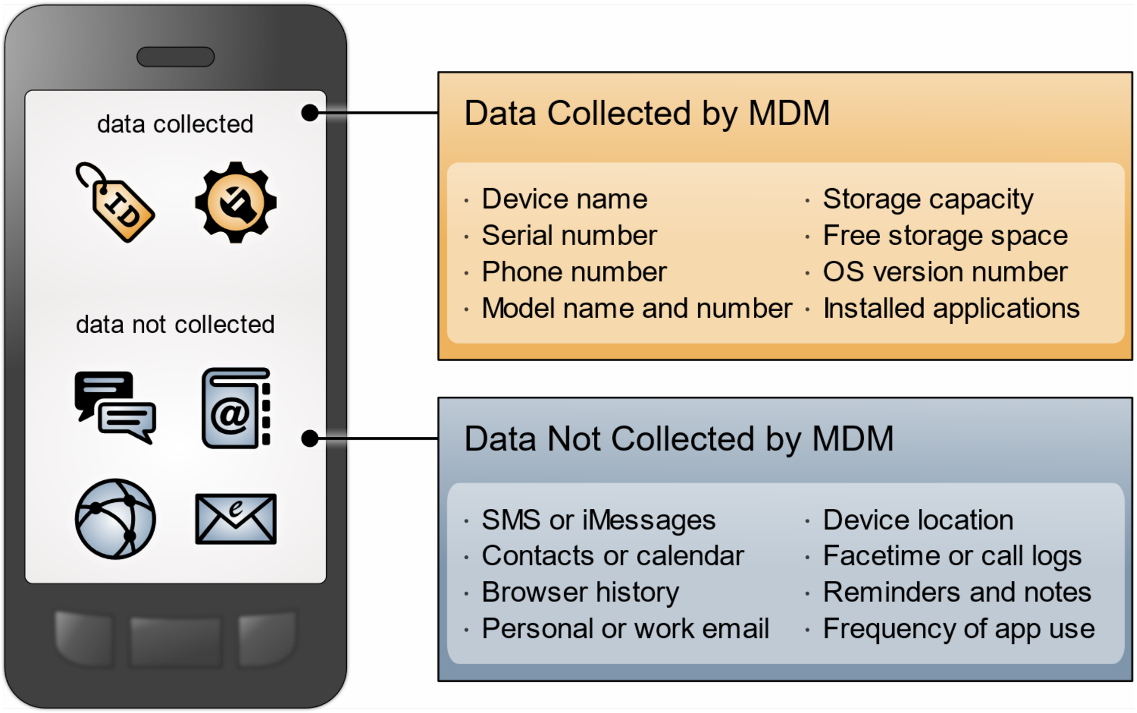
4.7 Privacy Settings: Mobile Device Data Processing

This section takes a look at components within the example architecture and the type of information an enterprise may access from an employee’s personal mobile device through those components. Understanding the type of data an enterprise has access to can be helpful when understanding any privacy implications.

4.7.1 EMM: MaaS360

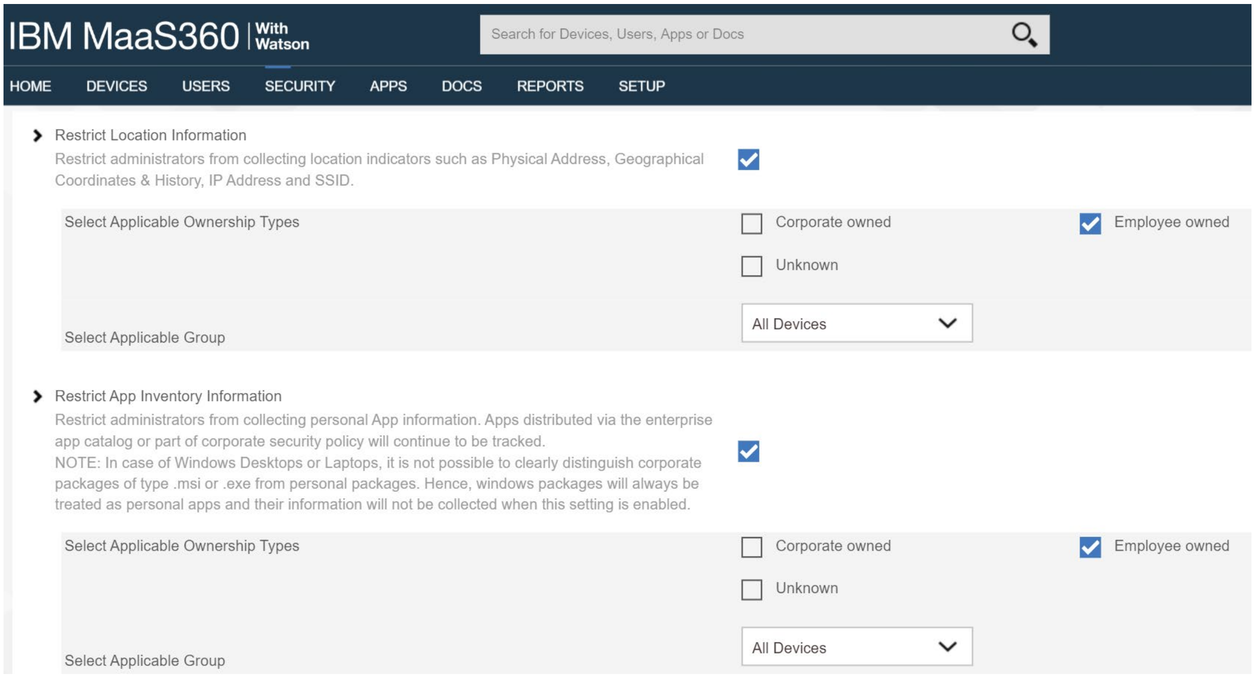
When a personal mobile phone is connected to an EMM system, some data is collected and visible to the enterprise. While additional data can be collected, our example solution collects only the data shown in Figure 4-7 to help protect employee privacy. This information is provided by MaaS360 to Kryptowire’s application vetting capability. Kryptowire then uses the MaaS360 supplied information to determine application security characteristics. IBM provides documentation with more details on the information that MaaS360 collects and processes [26].

989 **Figure 4-7 Data Collected by Example Solution Mobile Device Management**



As shown in Figure 4-8, administrators can restrict collection of location and/or application inventory information. When an administrator restricts location collection, the administrator cannot see any location information about devices. Similarly, when an administrator restricts application inventory information, MaaS360 will not collect applications that are not distributed through the enterprise and therefore, will not transmit them to third-party application-vetting services. Both privacy controls can be applied to specific device groups—for example, COPE devices could have their location information collected—but location collection can be disabled for personal devices.

Figure 4-8 Example Solution Mobile Device Management Privacy Settings



Restrict Location Information ☑

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

Select Applicable Ownership Types: □ Corporate owned ☑ Employee owned □ Unknown

Select Applicable Group: All Devices

Restrict App Inventory Information ☑

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

Select Applicable Ownership Types: □ Corporate owned ☑ Employee owned □ Unknown

Select Applicable Group: All Devices

4.7.2 MTD: Zimperium

Zimperium provides configurable settings for both what data is collected, as well as when it is collected. Data is collected:

- at login when the user launches the zIPS application
- when a threat is reported
- periodically, when the zIPS application checks in to the zConsole

Table 4-4 shows the data that is collected during each of the three scenarios above. Additional information regarding data item contents follows the table.

Note: Administrators who are managing Zimperium cannot disable the collection of the bolded data items (Network, Device, and Carrier Information) shown in Table 4-4 Data Collected by Zimperium.

Table 4-4 Data Collected by Zimperium

Time	Data Item
At login	Location (Street, City, or Country) Application Binaries (Android) **Network** **Device** Application Forensics **Carrier Information** User Details
Threat	Location (Street, City, or Country) Network Application Forensics Running Processes (Android) Site Insight Risky URLs Attacker's Network
Periodically	Location (Street, City, or Country) Network Application Binaries (Android) Application Forensics

The Device data item contains the following information:

- root/jailbreak status
- OS version
- OS known vulnerabilities
- developer mode enabled
- process list
- file system changes

- device international mobile equipment identity (IMEI)
- device IP
- device media access control (MAC) address
- location

The Network data item contains the following information:

- address resolution tables
- routing tables
- nearby networks
- network SSID
- external IP
- gateway MAC

The Application data item contains the following information:

- application ID
- application version
- hash
- malware detection (yes or no with type of malware)
- libraries used
- permissions
- privacy risk
- security risk
- location in device file system
- network connections

zIPS must collect certain data items to properly communicate with the zConsole. These items include:

- user credentials (email address, Zimperium-specific password)
- device hash (MD5 of IMEI or serial number as an identifier)
- device operating system
- device push token
- hash of local z9 database
- time and name of threat detection when a threat occurs

4.7.3 VPN: Palo Alto Networks

The Palo Alto Networks VPN uses information about the device as it establishes VPN connections. The data collected by the VPN includes information about:

- device name
- logon domain
- operating system
- app version
- mobile device network information to which the device is connected
- in addition, GlobalProtect collects whether the device is rooted or jailbroken

5 Security and Privacy Analysis

This section familiarizes the reader with:

- the example solution's assumptions and limitations
- results of the example solution's laboratory testing
- scenarios and findings that show the security and privacy characteristics addressed by the reference design
- the security and privacy control capabilities of the example solution

The purpose of the security and privacy characteristics evaluation is to understand the extent to which the project meets its objectives of demonstrating capabilities for securing mobile devices within an enterprise by deploying EMM, MTD, application vetting, secure boot/image authentication, and VPN services while also protecting the privacy of employees participating in the BYOD implementation.

5.1 Analysis Assumptions and Limitations

The security and privacy characteristics analysis has the following limitations:

- It is neither a comprehensive test of all security and privacy components nor a red-team exercise.
- It does not identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

5.2 Build Testing

Test activities are provided to show how the example architecture addresses each threat event and problematic data action. The NIST SP 1800-22 Supplement, *Example Scenario: Putting Guidance into*

Practice, provides insights into how an organization may determine its susceptibility to the threat before implementing the architecture detailed in this practice guide. The test activities contained in Appendix E, Build Testing Details, demonstrate to the reader how Great Seneca validated their desired outcomes for the identified threat events and problematic data actions. Appendix F, Threat Event Test Information, shows examples of test results for this build.

5.3 Scenarios and Findings

One aspect of the security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory. Using the Cybersecurity Framework Subcategories as a basis for organizing the analysis, allowed systematic consideration of how well the reference design supports the intended security characteristics.

This section of the publication provides findings for the security and privacy characteristics that the example solution was intended to support. These topics are described in the following subsections:

- development of the Cybersecurity Framework and NICE Framework mappings
- threat events related to security and example solution architecture mitigations
- problematic data actions related to privacy and potential mitigations that organizations could employ

An example scenario that demonstrates how an organization may use NIST SP 1800-22 and other NIST tools to implement a BYOD use case is discussed more in the NIST SP 1800-22 Supplement, *Example Scenario: Putting Guidance into Practice* of this practice guide.

5.3.1 Cybersecurity Framework and NICE Framework Work Roles Mappings

As we installed, configured, and used the products in the architecture, we determined and documented the example solution's functions and their corresponding Cybersecurity Framework Subcategories, along with other guidance alignment.

This mapping will help users of this practice guide communicate with their organization's stakeholders regarding the security controls that the practice guide recommends for helping mitigate BYOD threats, and the workforce capabilities that the example solution will require.

The products, frameworks, security controls, and workforce mappings are in Appendix G.

5.3.2 Threat Events and Findings

As part of the findings, the threat events were mitigated in the example solution architecture using the concepts and technology shown in Table 5-1. Each threat event was matched with functions that helped mitigate the risks posed by the threat event.

Note: TEE provided tamper-resistant processing environment capabilities that helped mitigate mobile device runtime and memory threats in the example solution. We do not show the Qualcomm TEE capability in the table because it is built into the phones used in this build.

Table 5-1 Threat Events and Findings Summary

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 1: unauthorized access to sensitive information via a malicious or privacy-intrusive application	Provides administrators with insight into what corporate data that applications can access.	MTD EMM
Threat Event 2: theft of credentials through a short message service (SMS) or email phishing campaign	Utilized PAN-DB and URL filtering to block known malicious websites.	Firewall
Threat Event 3: unauthorized applications installed via URLs in SMS or email messages	Alerted the user and administrators to the presence of a sideloaded application.	EMM MTD
Threat Event 4: confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	Alerted the user that their OS is non-compliant.	EMM MTD
Threat Event 5: violation of privacy via misuse of device sensors	Application vetting reports indicated the sensors to which an application requested access.	Application vetting
Threat Event 6: loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	Application vetting reports indicated if an application sent data without proper encryption.	Application vetting
Threat Event 7: compromise of device integrity via observed, inferred, or brute-forced device unlock code	Enforced mandatory device wipe capabilities after ten failed unlock attempts.	EMM MTD
Threat Event 8: unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	Application vetting reports indicated if an application used credentials improperly.	Application vetting

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 9: unauthorized access of enterprise resources from an unmanaged and potentially compromised device	Devices that were not enrolled in the EMM system were not able to connect to the corporate VPN.	VPN
Threat Event 10: loss of organizational data due to a lost or stolen device	Enforced passcode policies and device-wipe capabilities protected enterprise data.	EMM
Threat Event 11: loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	Policies that enforce data loss prevention were pushed to devices.	EMM
Threat Event 12: unauthorized access to work applications via bypassed lock screen	The VPN requires the user to reenter their password after a predefined amount of time.	VPN

5.3.3 Privacy Problematic Data Actions and Findings

The privacy risk analysis found that three data actions in the build were potentially problematic data actions for individuals. We identified potential technical mitigations that an organization could use to lessen their impact, as shown below in Table 5-2. Organizations may also need to supplement these technical mitigations with supporting policies and procedures.

Table 5-2 Summary of Privacy Problematic Data Actions and Findings

Problematic Data Actions (for Employees)	How the Example Solution Architecture Helps Mitigate the Problematic Data Action	The Technology Function that Helps Mitigate the Problematic Data Action
PDA-1: unwarranted restriction	Blocks staff access to enterprise resources by removing the device from MDM control instead of wiping the device.	EMM

Problematic Data Actions (for Employees)	How the Example Solution Architecture Helps Mitigate the Problematic Data Action	The Technology Function that Helps Mitigate the Problematic Data Action
	Enables only selectively wiping corporate resources on the device. Restricts staff access to system capabilities that permit removing device access or performing wipes.	
PDA-2: surveillance	Restricts staff access to system capabilities that permit reviewing data about employees and their devices. Limits or disables collection of specific data elements (e.g., location data).	EMM
PDA-3: unanticipated revelation	De-identifies personal and device data when not necessary to meet processing objectives. Encrypts data transmitted between parties. Limits or disables access to data. Limits or disables the collection of specific data elements.	EMM

5.4 Security and Privacy Control Mappings

The security and privacy capabilities of the example solution were identified, and example security and privacy control maps were developed to show these in a standardized methodology.

The control maps show the security and privacy characteristics for the products used in the example solution.

The security control map can be found in Appendix G. The privacy control map is in Appendix H.

6 Example Scenario: Putting Guidance into Practice

To demonstrate how an organization may use NIST SP 1800-22 and other NIST tools to implement a BYOD use case, the NCCoE created the *Example Scenario: Putting Guidance into Practice* supplement for this practice guide.

This example scenario shows how a fictional, small-to-mid-size organization (Great Seneca Accounting) can successfully navigate common enterprise BYOD security challenges.

In the narrative example, Great Seneca Accounting completes a security risk assessment by using the guidance in NIST SP 800-30 [27] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to the organization. The company then uses the NIST PRAM [8] to perform a privacy risk assessment. Appendix F and Appendix G of the Supplement describe these risk assessments in more detail. These risk assessments produce two significant conclusions:

1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the controls discussed in the example solution are relevant to their environment.
2. The organization determines that it has a high-impact system, based on the impact guidance in NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* [28], and needs to implement more controls beyond those identified in NIST SP 1800-22 to support the additional system components in its own solution (e.g., underlying OS, the data center where the equipment will reside).

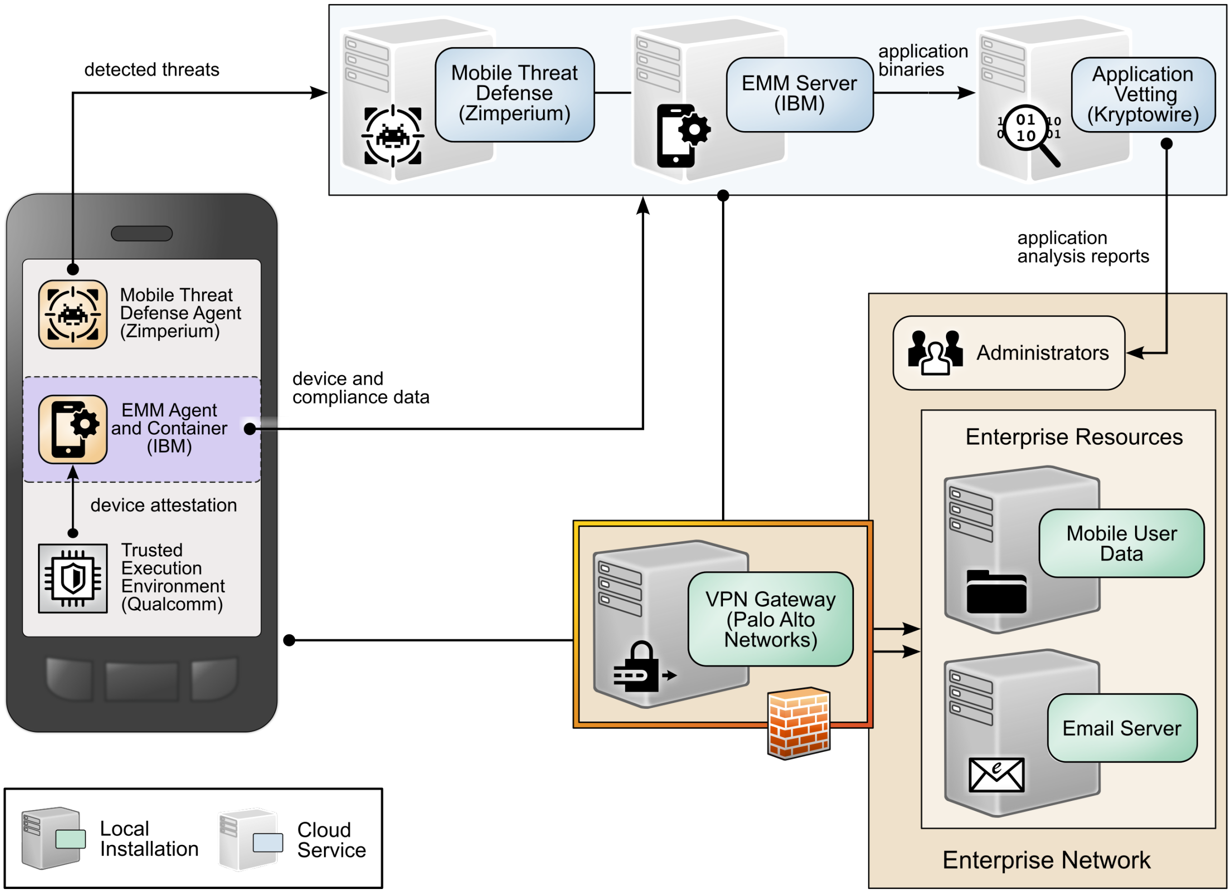
As part of their review of NIST FIPS 200, Great Seneca Accounting selects security and privacy controls from NIST SP 800-53 [29] for their BYOD architecture implementation. They then tailor the control baselines based on the needs identified through the priority Subcategories in its cybersecurity and privacy Target Profiles.

A detailed description of the implementation process that the fictional organization Great Seneca Accounting followed is provided in the NIST SP 1800-22 *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

7 Conclusion

This practice guide provides an explanation of mobile device security and privacy concepts and an example solution for organizations implementing a BYOD deployment. As shown in Figure 7-1, this example solution applied multiple mobile device security technologies. These included a cloud-based EMM solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities that support the example solution.

Figure 7-1 Example Solution Architecture


detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
01 10
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device attestation
Trusted Execution Environment (Qualcomm)
device and compliance data
Administrators
Enterprise Resources
Mobile User Data
Email Server
VPN Gateway (Palo Alto Networks)
Enterprise Network
Local Installation
Cloud Service

Our fictional Great Seneca Accounting organization example scenario contained in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide illustrates how the concepts and architecture from this guide may be applied by an organization. Great Seneca started with an information technology infrastructure that lacked mobile device security architecture concepts. Great Seneca then employed multiple NIST cybersecurity and privacy risk management tools to understand the gaps in its architecture and the methods available today to enhance the security and privacy of its BYOD deployment.

This practice guide also includes in Volume C a series of how-to guides—step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture—to help security engineers rapidly deploy and evaluate our example solution in their test environment.

The example solution uses standards-based, commercially available products that can be used by an organization interested in deploying a BYOD solution. The example solution provides recommendations for enhancing the security and privacy infrastructure by integrating on-premises and cloud-hosted mobile security technologies. This practice guide provides an example solution that an organization may use in whole or in part as the basis for creating a custom solution that best supports their unique needs.

8 Future Build Considerations

For a future build, the team is considering a virtual mobile infrastructure (VMI) or unified endpoint management (UEM) solution.

The VMI deployment could include installing an application on a device at enrollment time, which would grant access to a virtual phone contained within the corporate infrastructure. The virtual phone would then contain the corporate-supplied applications that an employee would require for performing standard mobile work tasks. The thin client deployment limits the storage of organizational data on the device and helps ensure that access to the organization's data uses security-enhancing capabilities.

UEM would entail managing a user's mobile device ecosystem, potentially including laptops, mobile phones, and IoT devices (e.g., smart watches and Bluetooth headsets).

Appendix A List of Acronyms

AD	Active Directory
API	Application Programming Interface
ATS	App Transport Security
BYOD	Bring Your Own Device
CIS	Center for Internet Security
COPE	Corporate-Owned Personally-Enabled
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile Device Management
MTD	Mobile Threat Defense
NCCoE	National Cybersecurity Center of Excellence
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PII	Personally Identifiable Information
PIN	Personal Identification Number
REST	Representational State Transfer
RMF	Risk Management Framework
SCEP	Simple Certificate Enrollment Protocol
SMS	Short Message Service
SP	Special Publication
SSL	Secure Sockets Layer
TE	Threat Event

TEE	Trusted Execution Environment
TLS	Transport Layer Security
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
VPN	Virtual Private Network

Appendix B Glossary

Access Management Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [30].

Availability Ensure that users can access resources through remote access whenever needed [31].

Bring Your Own Device (BYOD) A non-organization-controlled telework client device [31].

Confidentiality Ensure that remote access communications and stored user data cannot be read by unauthorized parties [31].

Data Actions System operations that process PII [32].

Disassociability Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [32].

Eavesdropping An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant [33] (definition located under eavesdropping attack).

Firewall Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [34].

Integrity Detect any intentional or unintentional changes to remote access communications that occur in transit [31].

Manageability Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [32].

Mobile Device A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [29].

Personally Identifiable Information (PII) Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual‘s identity, such as name, Social Security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [35] (adapted from Government Accountability Office Report 08-536).

Predictability Enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by a system [32].

Privacy Event The occurrence or potential occurrence of problematic data actions [2].

Problematic Data Action A data action that could cause an adverse effect for individuals [2].

Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [27].

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [27].

Appendix C References

[1] National Institute of Standards and Technology (NIST). NIST *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Cybersecurity Framework). Apr. 16, 2018. [Online]. Available: https://www.nist.gov/cyberframework.

[2] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework). Jan. 16, 2020. [Online]. Available: https://www.nist.gov/privacy-framework.

[3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST Special Publication (SP) 800-181 (2017 version), NIST, Gaithersburg, Md., Aug. 2017. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final.

[4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.

[5] NIST. Mobile Threat Catalogue. [Online]. Available: https://pages.nist.gov/mobile-threat-catalogue/.

[6] J. Franklin et al., *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST SP 800-124 Revision 2 (Draft), NIST, Gaithersburg, Md., Mar. 2020. Available: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft.

[7] J. Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds,* NIST SP 1800-4, NIST, Gaithersburg, Md., Feb. 21, 2019. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid.

[8] NIST. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available: https://www.nist.gov/privacy-framework/nist-pram.

[9] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[10] Open Web Application Security Project (OWASP). “OWASP Mobile Top 10,.” [Online]. Available: https://owasp.org/www-project-mobile-top-10/.

[11] NIST. Privacy Engineering Program: Privacy Risk Assessment Methodology, Catalog of Problematic Data Actions and Problems. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[12] M. Sabt, “Trusted Execution Environment: What It is, and What It is Not.” 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Helsinki, Finland, Aug. 2015. Available: https://hal.archives-ouvertes.fr/hal-01246364/file/trustcom_2015_tee_what_it_is_what_it_is_not.pdf.

[13] National Information Assurance Partnership (NIAP). U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 3.0. Nov. 21, 2016. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/ep_mdm_agent_v3.0.pdf.

[14] NIAP. U.S. Government Approved Protection Profile—Module for Virtual Private Network (VPN) Gateways 1.1. July 01, 2020. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=449&id=449.

[15] NIAP. U.S. Government Approved Protection Profile—collaborative Protection Profile for Network Devices Version 2.2e. Mar. 27, 2020. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=447&id=447.

[16] NIAP. Approved Protection Profiles. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[17] Qualcomm. “Qualcomm Secure Boot and Image Authentication Technical Overview.” [Online]. Available: https://www.qualcomm.com/media/documents/files/secure-boot-and-image-authentication-technical-overview-v1-0.pdf.

[18] Apple Inc. “Preventing Insecure Network Connections.” [Online]. Available: https://developer.apple.com/documentation/security/preventing_insecure_network_connections.

[19] Apple Inc. " Identifying the Source of Blocked Connections," [Online]. Available: https://developer.apple.com/documentation/security/preventing_insecure_network_connections/identifying_the_source_of_blocked_connections.

[20] Android.com. “Network security configuration.” Dec. 27, 2019. [Online]. Available: https://developer.android.com/training/articles/security-config.

[21] NowSecure.com. “A Security Analyst’s Guide to Network Security Configuration in Android P.” [Online]. Available: https://www.nowsecure.com/blog/2018/08/15/a-security-analysts-guide-to-network-security-configuration-in-android-p/.

[22] Apple Inc. “Overview: Managing Devices & Corporate Data on iOS.” July 2018. [Online]. Available: https://www.apple.com/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf.

[23] Google Android. “Build Android management solutions for enterprises.” [Online]. Available: https://developers.google.com/android/work.

[24] International Business Machines (IBM). “Web Services Integration Details.” [Online]. Available: https://developer.ibm.com/security/maas360/maas360-getting-started/maas360-web-services-integration-details/.

[25] IBM. “IBM Community Public Wikis.” [Online]. Available: https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usage.

[26] IBM. “IBM MaaS360 GDPR Data Map (Persona Data Attributes).” [Online]. Available: http://public.dhe.ibm.com/software/security/products/maas360/GDPR/Personal_Data_in_IBM_MaaS360.pdf.

[27] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments,* NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[28] NIST. *Minimum Security Requirements for Federal Information and Information Systems,* Federal Information Processing Standards Publication (FIPS) 200, Mar. 2006. Available: https://csrc.nist.gov/publications/detail/fips/200/final.

[29] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems and Organizations,* NIST SP 800-53, NIST, Gaithersburg, Md., Jan. 2015. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[30] IDManagement.gov. “Federal Identity, Credential, and Access Management Architecture.” [Online]. Available: https://arch.idmanagement.gov/services/access/.

[31] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,* NIST SP 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

[32] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems,* NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[33] P. Grassi et al., *Digital Identity Guidelines,* NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[34] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security,* NIST SP 800-82 Revision 2, NIST, Gaithersburg, Md., May 2015. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[35] E. McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[36] J. Franklin et al., *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE),* NIST SP 1800-21, NIST, Gaithersburg, Md., July 22, 2019. Available: https://csrc.nist.gov/News/2019/NIST-Releases-Draft-SP-1800-21-for-Comment.

[37] NIST, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,* NIST SP 800-52 Revision 2, August 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final.

[38] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations (Final Public Draft),* NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[39] S. Frankel et al., *Guide to SSL VPNs,* NIST SP 800-113, NIST, Gaithersburg, Md., July 2008. Available: https://csrc.nist.gov/publications/detail/sp/800-113/final.

[40] M. Souppaya and K. Scarfone, *User's Guide to Telework and Bring Your Own Device (BYOD) Security,*, NIST SP 800-114 Revision 1, NIST, Gaithersburg, Md., July 2016. Available: https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final.

[41] M. Ogata et al., *Vetting the Security of Mobile Applications,* NIST SP 800-163 Revision 1, NIST, Gaithersburg, Md., Apr. 2019. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf.

[42] NIST, *Protecting Controlled Unclassified Information in Nonfederal SystemsI,* NIST SP 800-171 Revision 2, February 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[43] Center for Internet Security. Center for Internet Security home page. [Online]. Available: https://www.cisecurity.org/.

[44] Executive Office of the President, "Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," Aug. 23, 2012. Available: https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device.

[45] Federal CIO Council and Department of Homeland Security. *Mobile Security Reference Architecture Version 1.0.* May 23, 2013. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf.

[46] Digital Services Advisory Group and Federal Chief Information Officers Council. *Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis,.* Dec. 2012. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf.

[47] International Organization for Standardization. “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.” Oct. 2013. [Online]. Available: https://www.iso.org/standard/54534.html.

[48] “Mobile Computing Decision.” [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf.

[49] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC). “Mobility Strategy Development Guidelines, Working Group Document.” June 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12997/Agency_Mobility_Strategy_Deliverable.pdf.

[50] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC). “Mobile Threat Protection App Vetting and App Security, Working Group Document.” July 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category-team/9658/docs/12996/Mobile_Threat_Protection_Deliverable.pdf.

[51] Mobile Services Category Team (MSCT). “Device Procurement and Management Guidance.” Nov. 2016. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/information-technology/4485/mobile-device-procurement-and-management-guidance.

[52] Mobile Services Category Team (MSCT). “Mobile Device Management (MDM), MDM Working Group Document.” Aug. 2017. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf.

[53] Mobile Services Category Team (MSCT). “Mobile Services Roadmap (MSCT Strategic Approach).” Sept. 23, 2016. [Online]. Available: https://atarc.org/project/mobile-services-roadmap-msct-strategic-approach/.

[54] NIAP. U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 2.0. Dec. 31, 2014. [Online]. Available: https://www.niap-ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf.

[55] NIAP. Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version 3.1,. June 16, 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=417&id=417.

[56] NIAP. Approved Protection Profiles—Protection Profile for Mobile Device Management Version 4.0. Apr. 25, 2019. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=428&id=428.

[57] NIAP. Product Compliant List. [Online]. Available: https://www.niap-ccevs.org/Product/.

[58] Office of Management and Budget, Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services, Aug. 4, 2016. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_20.pdf.

[59] NIST. United States Government Configuration Baseline (in development). [Online]. Available: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline.

[60] Department of Homeland Security (DHS). "DHS S&T Study on Mobile Device Security." Apr. 2017. [Online]. Available: https://www.dhs.gov/publication/csd-mobile-device-security-study.

[61] NIST, NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*, Mar. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf.

[62] NIST Privacy Framework and Cybersecurity Framework to NIST Special Publication 800-53, Revision 5 Crosswalk. [Online]. Available: https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53.

Appendix D Standards and Guidance

- National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) Version 1.1 [1]
- *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework) [2]
- NIST Mobile Threat Catalogue [5]
- NIST Risk Management Framework [4]
- NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [7]
- NIST SP 1800-21, *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* [36]
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [27]
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [9]
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [31]
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [37]
- NIST SP 800-53 Revision 4 (Final)*, Security and Privacy Controls for Information Systems and Organizations* [29]
- NIST SP 800-53 Revision 5 (Final), *Security and Privacy Controls for Information Systems and Organizations* [38]
- NIST SP 800-63-3, *Digital Identity Guidelines* [33]
- NIST SP 800-113, *Guide to SSL VPNs* [39]
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [40]
- NIST SP 800-124 Revision 2 (Draft)*, Guidelines for Managing the Security of Mobile Devices in the Enterprise* [6]
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [41]
- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [42]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2017)* [3]
- NIST Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems* [28]

- NIST Privacy Risk Assessment Methodology [8]
- Center for Internet Security [43]
- Executive Office of the President, Bring Your Own Device toolkit [44]
- Federal Chief Information Officers Council and Department of Homeland Security *Mobile Security Reference Architecture*, Version 1.0 [45]
- Digital Services Advisory Group and Federal Chief Information Officers Council, *Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis* [46]
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, “Information technology – Security techniques – Information security management systems – Requirements” [47]
- Mobile Computing Decision example case study [48]
- Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), “Mobility Strategy Development Guidelines Working Group Document” [49]
- MSCT ATARC, “Mobile Threat Protection App Vetting and App Security,” Working Group Document [50]
- MSCT, “Device Procurement and Management Guidance” [51]
- MSCT, “Mobile Device Management (MDM),” MDM Working Group Document [52]
- MSCT, “Mobile Services Roadmap, MSCT Strategic Approach” [53]
- National Information Assurance Partnership (NIAP), U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 2.0 [54]
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version 3.1 [55]
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Management Version 4.0 [56]
- NIAP, Product Compliant List [57]
- Office of Management and Budget, *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services* [58]
- United States Government Configuration Baseline [59]
- Department of Homeland Security (DHS), “DHS S&T Study on Mobile Device Security” [60]
- NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework* [61]

Appendix E 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 problematic data actions defined from the risk assessment.

E.1 Threat Event 1

Summary: Unauthorized access to sensitive information via a malicious or privacy-intrusive application is tested.

Test Activity: Place mock sensitive enterprise contact list and calendar entries on devices, then attempt to install and use applications that access and back up those entries.

Desired Outcome: The enterprise's security architecture would either detect or prevent use of these applications, or it would block the applications from accessing enterprise-controlled contact list and calendar entries. The enterprise's security architecture should identify presence of the applications and the fact that they access contact and calendar entries. The security architecture should block these applications from installing, block them from running, or detect their presence and cause another appropriate response, such as blocking the mobile device from accessing enterprise resources until the applications are removed.

Alternatively, built-in device mechanisms such as Apple's managed applications functionality and Google's Android enterprise work profile functionality could be 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. The user should not be able to manually provision their enterprise email account. Only the EMM should be able to provision the account, enabling enterprise controls on the enterprise contact list and calendar data.

Observed Outcome: Once MaaS360 was aware that an application had access to sensitive data (e.g., calendar entries, contacts), it applied a policy to the device and took appropriate actions automatically. MaaS360 sent an alert to the mobile device about an application compliance policy violation and requested that the user remove the application(s) within an administrator-set time frame. In our test, the simulated user account did not remove the restricted applications within the predefined time frame, and MaaS360 removed mobile device management (MDM) control from the mobile device.

E.2 Threat Event 2

Summary: A fictional phishing event was created to test protection against the theft of credentials through a short message service (SMS) or 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.
- Then send the web page's uniform resource locator (URL) via SMS or email and 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 use 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. However, if the malicious URL were not present in PAN-DB, the user would be allowed to access the website.

E.3 Threat Event 3

Summary: Testing to discover for unauthorized applications that are not present on the official Apple App Store or Google Play Store, that can be installed via URL links in SMS, email messages, or third-party websites.

Test Activity (Android):

- Send an email to the user with a message urging the user to click the link to install the application.
- On the device, if not already enabled, attempt to enable the Unknown Sources toggle setting in the device security settings to allow installing applications from sources other than the Google Play Store.
- On the device, read the received email, click the link, and attempt to install the application.
- Observe whether the application could be successfully installed. If so, observe whether the enterprise detected and responded to installation of the unauthorized application.

Test Activity (iOS):

- Send an email to the user with a message urging the user to click the link to install the application.
- On the device, read the received email, click the link, and attempt to install the application.

Desired Outcome: Zimperium should alert both the administrators and user of the presence of a side-loaded application.

Observed Outcome: Zimperium alerted both the user and MaaS360 about the presence of a side-loaded application. MaaS360 sent an email notification to the user and administrator about the presence of side-loaded applications and required actions.

E.4 Threat Event 4

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

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

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

Observed Outcome: Zimperium was able to identify devices that were running an outdated version of iOS or Android, and it informed MaaS360 when a device was out of compliance.

E.5 Threat Event 5

Summary: This threat event test shows collection of location, camera, or microphone data by an application that has no need to access this data.

Note: Not all applications that have access to location, camera, or microphone data are malicious. However, when applications are found collecting this information, additional vetting or testing may be required to determine the intent of its use and then to determine if the application is malicious.

Test Activity: Upload the application to Kryptowire; observe the output report.

Desired Outcome: Output report identifies the use of location, camera, or microphone by the application.

Observed Outcome: The Kryptowire report identified the usage of privacy-intrusive permissions when not required.

E.6 Threat Event 6

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 container, a container-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.

E.7 Threat Event 7

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.
- Attempt to continually unlock the device, confirming that the device is factory reset after 10 failed attempts.

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, require a minimum complexity for the device unlock code, and factory resetting the device after 10 failed unlock attempts.

Additionally, Zimperium can identify and report devices with a disabled lock screen.

Observed Outcome: MaaS360 applies a policy to the devices to enforce a mandatory PIN and device-wide capability. Zimperium reports devices with a disabled lock screen.

E.8 Threat Event 8

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

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

Desired Outcome: Discover and report credential weaknesses.

Observed Outcome: Kryptowire recognized within an application that the application uses hardcoded credentials. The application's use of hardcoded credentials could introduce vulnerabilities if unauthorized entities used the hardcoded credentials to access enterprise resources.

E.9 Threat Event 9

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

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

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

Observed Outcome: Devices that were not enrolled in MaaS360 were unable to access enterprise resources as the GlobalProtect VPN gateway prevented the devices from authenticating without proper client certificates—obtainable only through enrolling in the EMM.

E.10 Threat Event 10

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

Test Activity: Attempt to download enterprise data onto a mobile device that is not enrolled in the EMM system (may be performed in conjunction with TE-9). Attempt to remove (in conjunction with TE-7) the screen lock passcode or demonstrate that the device does not have a screen lock passcode in place. Attempt to locate and selectively wipe the device through the EMM console (will fail if the device is not enrolled in the EMM).

Desired Outcome: It should be possible to locate or wipe EMM enrolled devices in response to a report that they have been lost or stolen. As demonstrated by TE-9, only EMM enrolled devices should be able to access enterprise resources. As demonstrated by TE-7, 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. After 10 attempts to access the device, the device was selectively wiped, removing all enterprise data. 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 9, only enrolled devices could access enterprise services. 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.

E.11 Threat Event 11

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

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

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

Observed Outcome: Through MaaS360 device policies, an administrator could prevent the following actions on BYODs:

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

E.12 Threat Event 12

Summary: Unauthorized access to work applications via bypassed lock screen (e.g., sharing the device's PIN with family members).

Test Activity: Assume the user is an unauthorized person attempting to access enterprise resources. Unlock the device and attempt to open a work application.

Desired Outcome: The user will be prompted to log in to the VPN using their corporate username and password. Because the user does not know this password, they are unable to log in and access corporate resources. However, if the user attempts to access a work application within the idle log-out time, they will be granted access because no password will be requested.

Observed Outcome: GlobalProtect prompted the unauthorized user for a password. Not knowing the password, the unauthorized user was unable to access corporate resources.

E.13 Problematic Data Action 1

Summary: The user retains personal data and applications while access to corporate applications and data is removed.

Test Activity: Selectively wipe a device using MaaS360.

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.

Observed Outcome: Corporate data and applications are removed while personal data is untouched.

E.14 Problematic Data Action 2

Summary: Collection of application and location data is restricted.

Test Activity: Disable location and application inventory collection in MaaS360.

Desired Outcome: The MDM does not collect an inventory of applications on the device and does not collect location information, including physical address, geographic coordinates and history, internet protocol (IP) address, and secure set identifier (SSID).

Observed Outcome: When inspecting a device, location and application inventory information are not shown to the user, and application inventory information is not transmitted to Kryptowire.

E.15 Problematic Data Action 3

Summary: Access to monitoring data from the device is restricted to administrators. Application and location data are not 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.

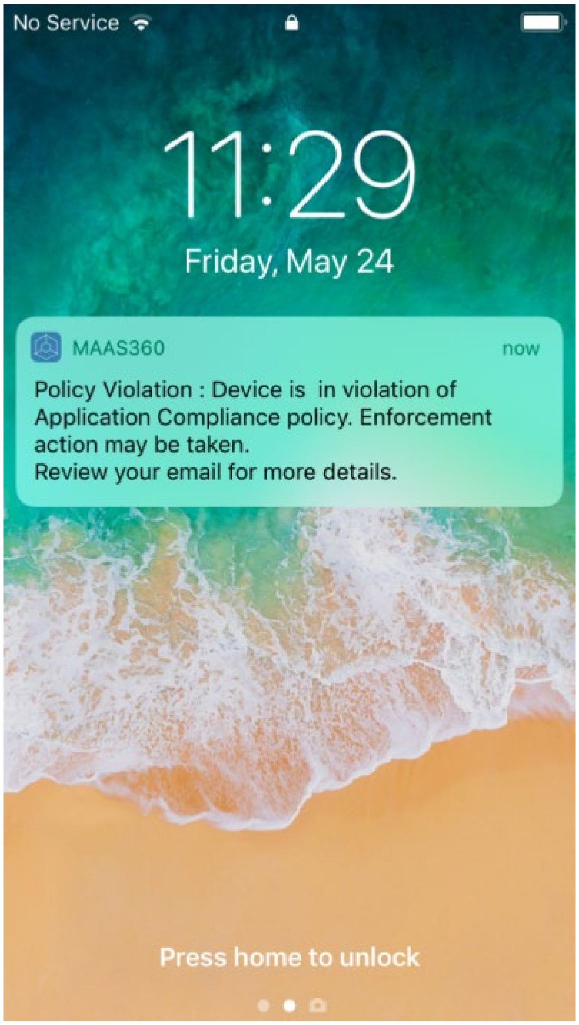
Appendix F Threat Event Test Information

Detailed information for some of this practice guide’s threat events and their testing results appears below.

F.1 Threat Event 1

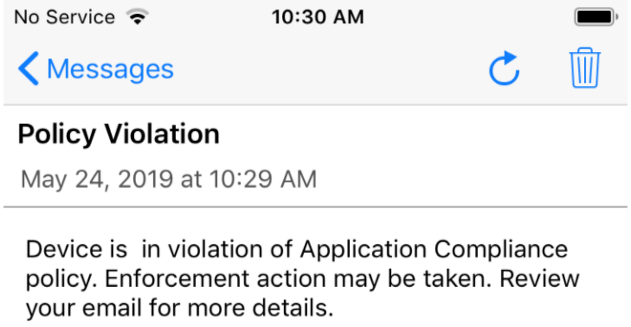
Threat Event 1 demonstrates unauthorized access attempts to sensitive information via a malicious or privacy-intrusive application. The following figures show the alerts that the device user received regarding the policy violations and their remediation actions.

Figure F-1 Policy Violation Notification



Policy Violation : Device is in violation of Application Compliance policy. Enforcement action may be taken.
Review your email for more details.

Figure F-2 Policy Violation Email

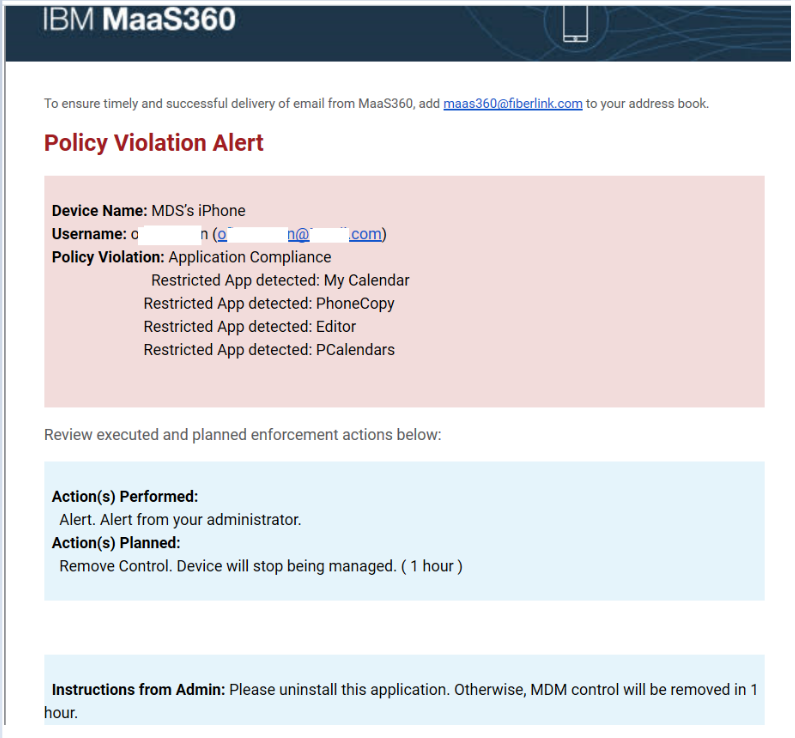


Policy Violation

May 24, 2019 at 10:29 AM

Device is in violation of Application Compliance policy. Enforcement action may be taken. Review your email for more details.

Figure F-3 Policy Violation Alert Details Email



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Policy Violation Alert

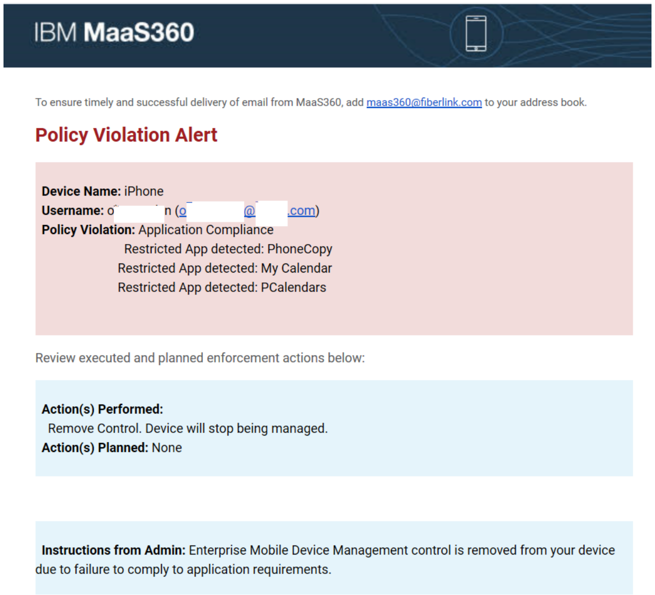
Device Name: MDS's iPhone
Username: o[redacted]n (o[redacted]n@[redacted].com)
Policy Violation: Application Compliance
Restricted App detected: My Calendar
Restricted App detected: PhoneCopy
Restricted App detected: Editor
Restricted App detected: PCalendars

Review executed and planned enforcement actions below:

Action(s) Performed:
Alert. Alert from your administrator.
Action(s) Planned:
Remove Control. Device will stop being managed. (1 hour)

Instructions from Admin: Please uninstall this application. Otherwise, MDM control will be removed in 1 hour.

Figure F-4 Enterprise Mobility Management Removal Alert



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Policy Violation Alert

Device Name: iPhone
Username: o[redacted]n (o[redacted]@[redacted].com)
Policy Violation: Application Compliance
Restricted App detected: PhoneCopy
Restricted App detected: My Calendar
Restricted App detected: PCalendars

Review executed and planned enforcement actions below:

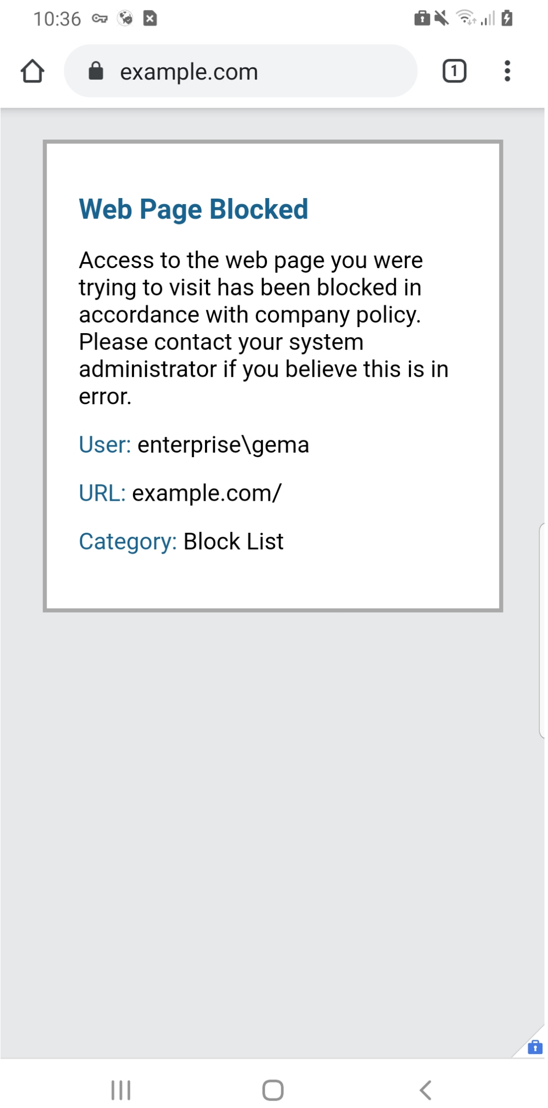
Action(s) Performed:
Remove Control. Device will stop being managed.
Action(s) Planned: None

Instructions from Admin: Enterprise Mobile Device Management control is removed from your device due to failure to comply to application requirements.

F.2 Threat Event 2

The following screen capture shows Threat Event 2's testing outcome, where Palo Alto Networks' PAN-DB is blocking a website manually added to the malicious uniform resource locator (URL) database.

1679 **Figure F-5 PAN-DB Blocked Website**



Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: enterprise\gema

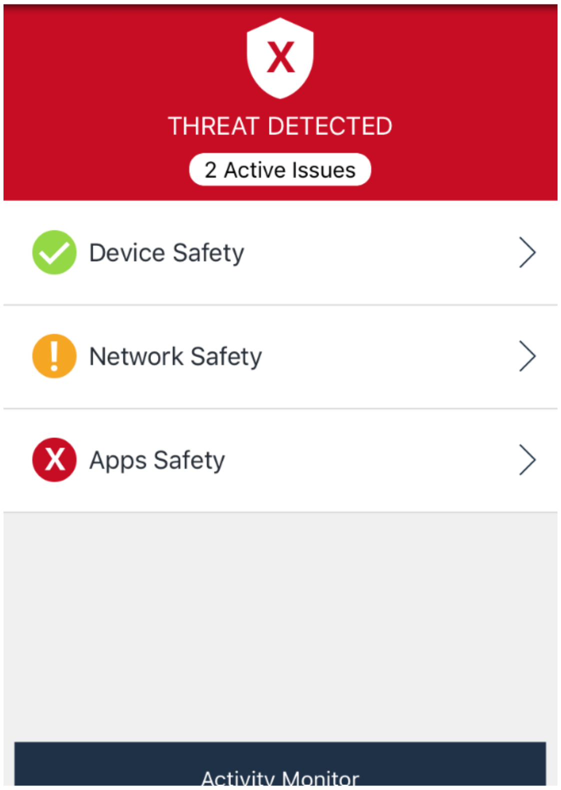
URL: example.com/

Category: Block List

1680 F.3 Threat Event 3

1681 Threat Event 3 shows applications that are not present on the official Apple App Store or Google Play
1682 Store being installed via unauthorized means (sideloading).

1683 **Figure F-6 Zimperium Threat Detected**



THREAT DETECTED

2 Active Issues

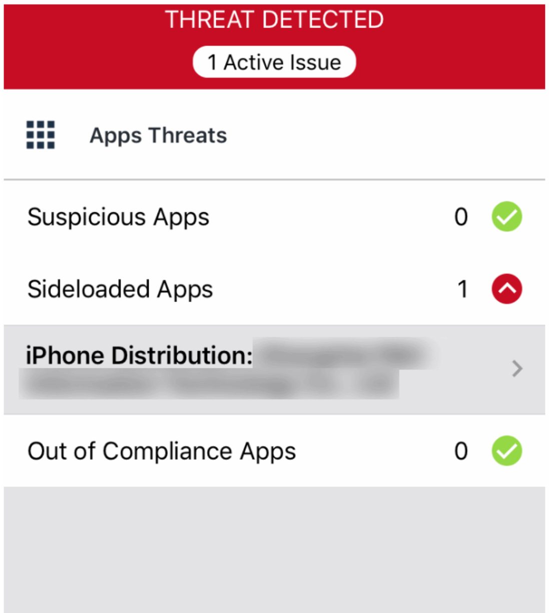
✓ Device Safety

! Network Safety

X Apps Safety

Activity Monitor

Figure F-7 Zimperium Sideloaded Application Alert



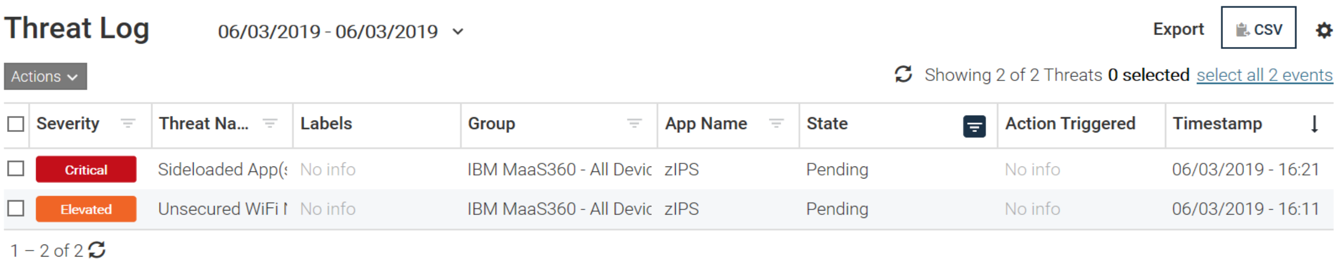
THREAT DETECTED

1 Active Issue

Apps Threats

Suspicious Apps	0	✓
Sideloaded Apps	1	⌃
iPhone Distribution: [redacted]		›
Out of Compliance Apps	0	✓

Figure F-8 Zimperium Threat Log with Sideloaded Application Alert



Threat Log 06/03/2019 - 06/03/2019

Export CSV

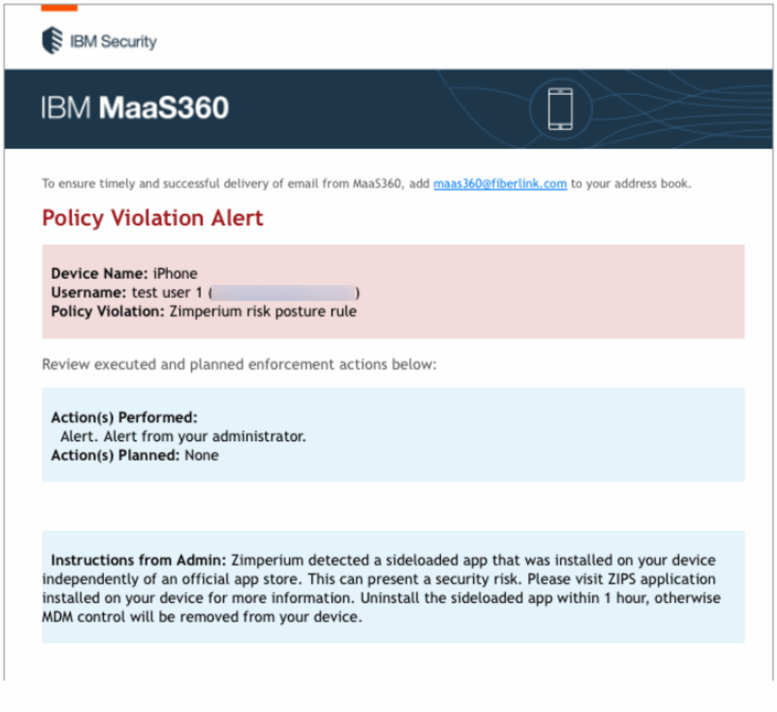
Actions

Showing 2 of 2 Threats **0 selected** select all 2 events

□	Severity	Threat Na...	Labels	Group	App Name	State	Action Triggered	Timestamp
□	Critical	Sideloaded App(s	No info	IBM MaaS360 - All Devic	zIPS	Pending	No info	06/03/2019 - 16:21
□	Elevated	Unsecured WiFi I	No info	IBM MaaS360 - All Devic	zIPS	Pending	No info	06/03/2019 - 16:11

1 – 2 of 2

Figure F-9 Email Regarding MaaS360 Policy Violation Alert



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Policy Violation Alert

Device Name: iPhone
Username: test user 1 ([redacted])
Policy Violation: Zimperium risk posture rule

Review executed and planned enforcement actions below:

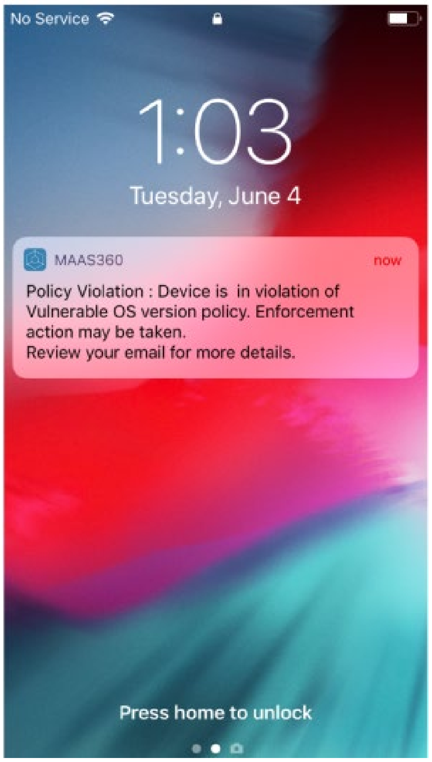
Action(s) Performed:
Alert. Alert from your administrator.
Action(s) Planned: None

Instructions from Admin: Zimperium detected a sideloaded app that was installed on your device independently of an official app store. This can present a security risk. Please visit ZIPS application installed on your device for more information. Uninstall the sideloaded app within 1 hour, otherwise MDM control will be removed from your device.

F.4 Threat Event 4

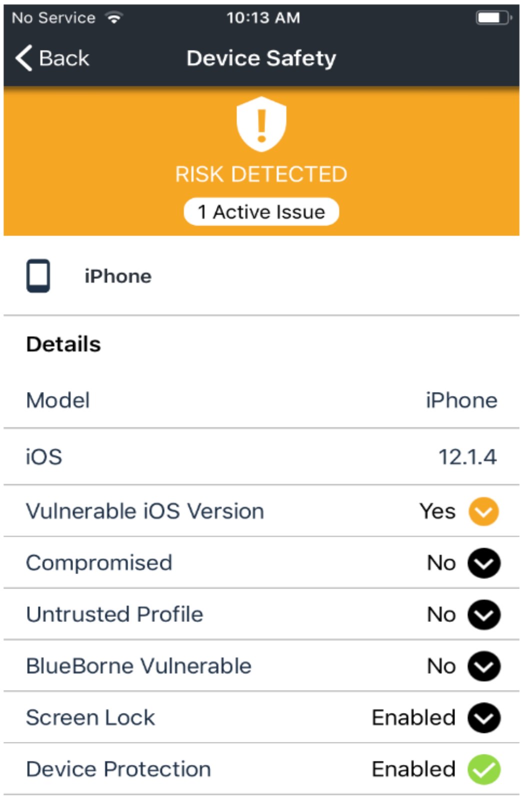
Threat Event 4 shows a risk detection during an operating system rules compliance status check.

1689 **Figure F-10 MaaS360 Policy Violation Alert**



Policy Violation : Device is in violation of Vulnerable OS version policy. Enforcement action may be taken.
Review your email for more details.

1690 **Figure F-11 Zimperium Risk Detected**



No Service 10:13 AM

Back

Device Safety

RISK DETECTED

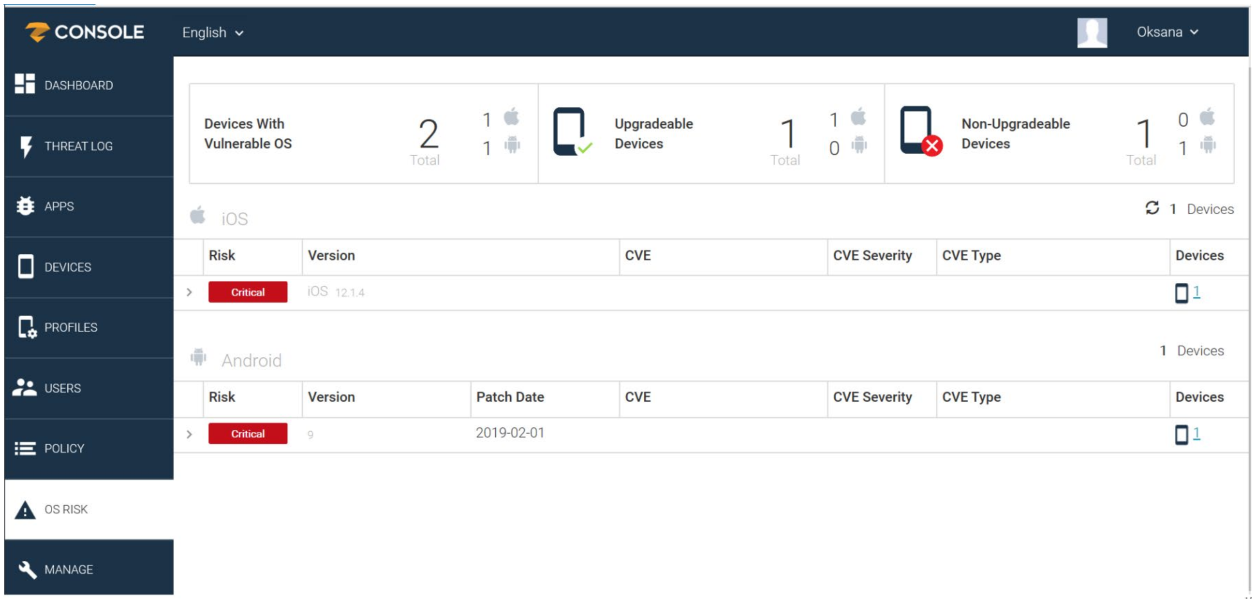
1 Active Issue

iPhone

Details

Model	iPhone
iOS	12.1.4
Vulnerable iOS Version	Yes
Compromised	No
Untrusted Profile	No
BlueBorne Vulnerable	No
Screen Lock	Enabled
Device Protection	Enabled ✓

Figure F-12 Zimperium OS Risk



Devices With Vulnerable OS	2 Total	1 1
Upgradeable Devices	1 Total	1 0
Non-Upgradeable Devices	1 Total	0 1

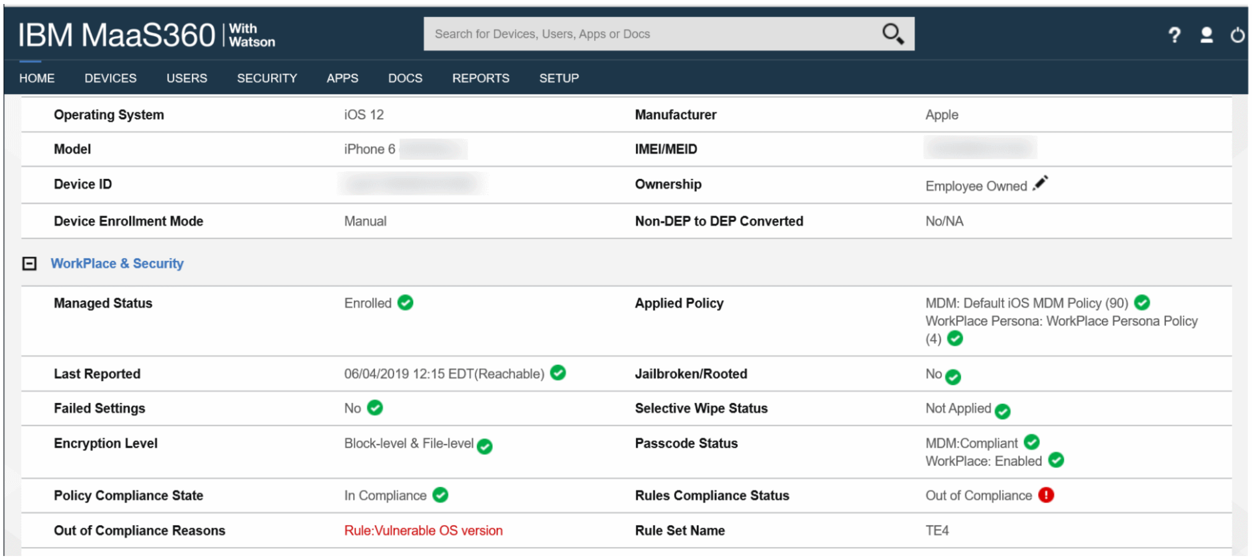
iOS — 1 Devices

Risk	Version	CVE	CVE Severity	CVE Type	Devices
Critical	iOS 12.1.4				1

Android — 1 Devices

Risk	Version	Patch Date	CVE	CVE Severity	CVE Type	Devices
Critical	9	2019-02-01				1

Figure F-13 MaaS360 Compliance Rule Violation

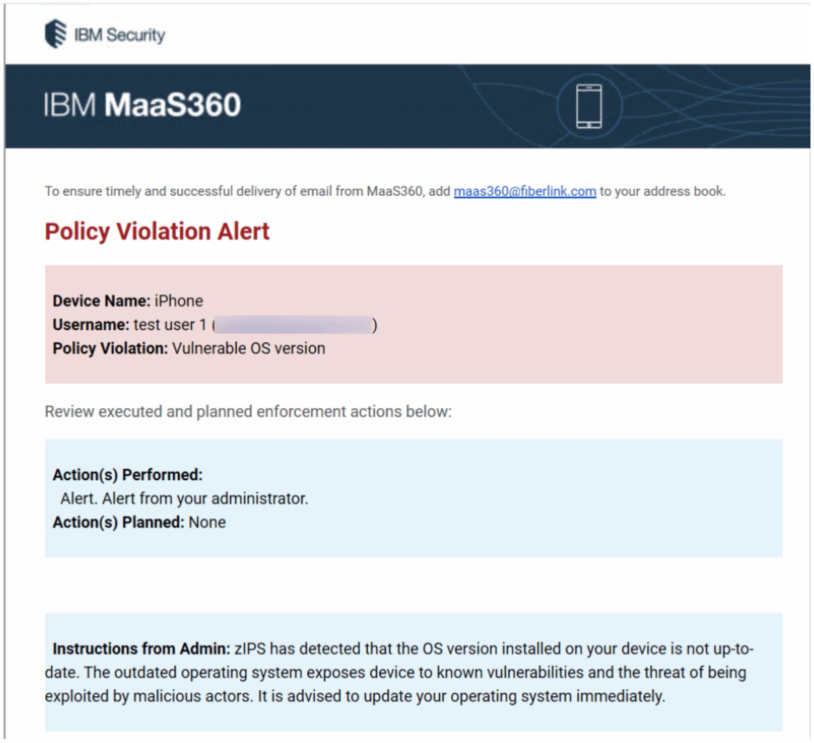


Operating System	iOS 12	Manufacturer	Apple
Model	iPhone 6 [redacted]	IMEI/MEID	[redacted]
Device ID	[redacted]	Ownership	Employee Owned
Device Enrollment Mode	Manual	Non-DEP to DEP Converted	No/NA

WorkPlace & Security

Managed Status	Enrolled ✓	Applied Policy	MDM: Default iOS MDM Policy (90) ✓ WorkPlace Persona: WorkPlace Persona Policy (4) ✓
Last Reported	06/04/2019 12:15 EDT(Reachable) ✓	Jailbroken/Rooted	No ✓
Failed Settings	No ✓	Selective Wipe Status	Not Applied ✓
Encryption Level	Block-level & File-level ✓	Passcode Status	MDM:Compliant ✓ WorkPlace: Enabled ✓
Policy Compliance State	In Compliance ✓	Rules Compliance Status	Out of Compliance !
Out of Compliance Reasons	Rule:Vulnerable OS version	Rule Set Name	TE4

Figure F-14 MaaS360 Policy Violation Email



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Policy Violation Alert

Device Name: iPhone
Username: test user 1 ([redacted])
Policy Violation: Vulnerable OS version

Review executed and planned enforcement actions below:

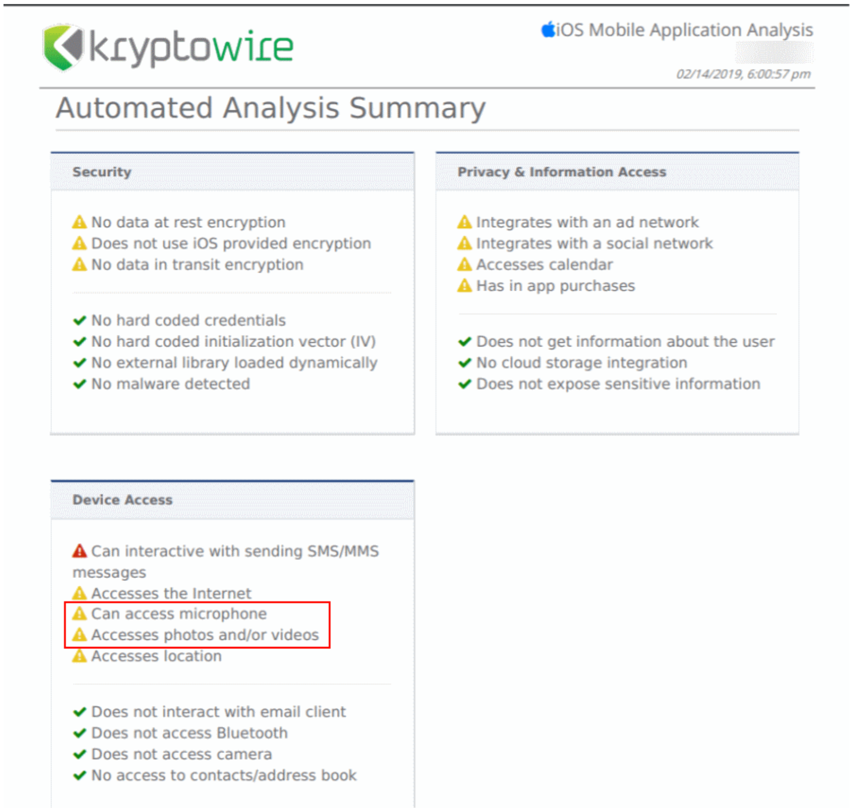
Action(s) Performed:
Alert. Alert from your administrator.
Action(s) Planned: None

Instructions from Admin: zIPS has detected that the OS version installed on your device is not up-to-date. The outdated operating system exposes device to known vulnerabilities and the threat of being exploited by malicious actors. It is advised to update your operating system immediately.

F.5 Threat Event 5

Threat Event 5 demonstrates a report detailing **c**ollection of information such as location, camera, or microphone data by an application.

1697 **Figure F-15 Kryptowire iOS Application Report**



kryptowire

iOS Mobile Application Analysis

02/14/2019, 6:00:57 pm

Automated Analysis Summary

Security

⚠ No data at rest encryption
⚠ Does not use iOS provided encryption
⚠ No data in transit encryption

✓ No hard coded credentials
✓ No hard coded initialization vector (IV)
✓ No external library loaded dynamically
✓ No malware detected

Privacy & Information Access

⚠ Integrates with an ad network
⚠ Integrates with a social network
⚠ Accesses calendar
⚠ Has in app purchases

✓ Does not get information about the user
✓ No cloud storage integration
✓ Does not expose sensitive information

Device Access

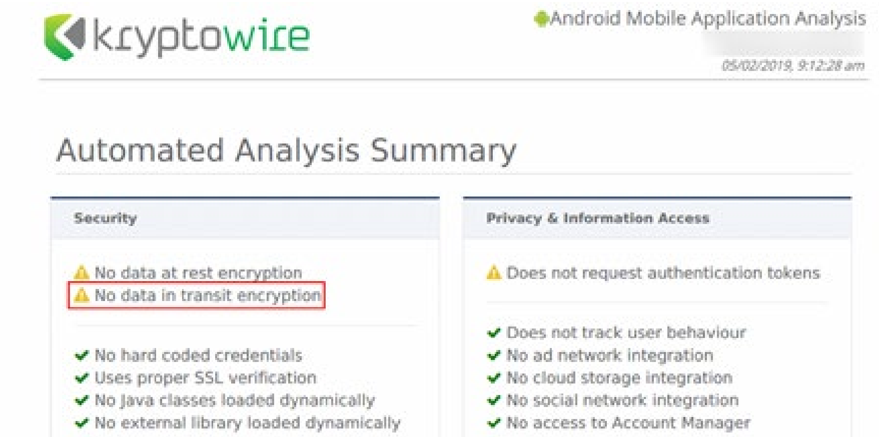
⚠ Can interactive with sending SMS/MMS messages
⚠ Accesses the Internet
⚠ Can access microphone
⚠ Accesses photos and/or videos
⚠ Accesses location

✓ Does not interact with email client
✓ Does not access Bluetooth
✓ Does not access camera
✓ No access to contacts/address book

1698 F.6 Threat Event 6

1699 Threat Event 6 demonstrates a report of an application that can lose confidentiality of sensitive
1700 information via eavesdropping on unencrypted device communications.

Figure F-16 Kryptowire Android Application Report



kryptowire

Android Mobile Application Analysis

[redacted]

05/02/2019, 9:12:28 am

Automated Analysis Summary

Security	Privacy & Information Access
⚠ No data at rest encryption ⚠ No data in transit encryption	⚠ Does not request authentication tokens
✓ No hard coded credentials ✓ Uses proper SSL verification ✓ No Java classes loaded dynamically ✓ No external library loaded dynamically	✓ Does not track user behaviour ✓ No ad network integration ✓ No cloud storage integration ✓ No social network integration ✓ No access to Account Manager

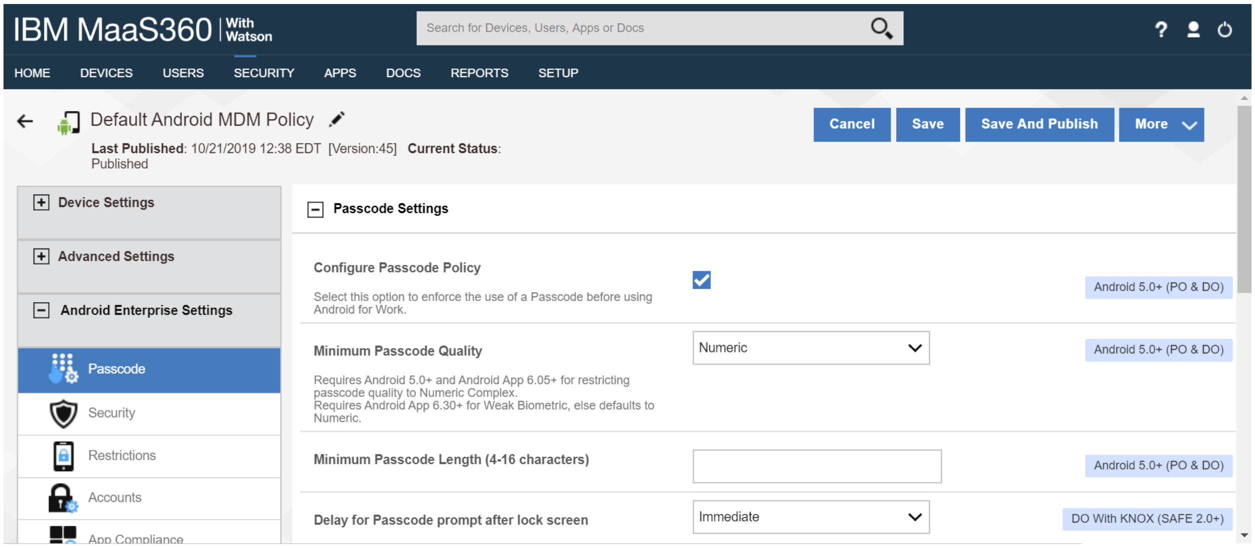
F.7 Threat Event 7

Two scenarios are shown for Threat Event 7:

- The first scenario shows MaaS360 applying a policy to the devices to enforce a mandatory PIN and device-wipe capability.
- The second scenario shows Zimperium reporting a disabled lock screen.

The diagram shows the MaaS360 configuration requirements for Passcode Settings for its managed devices, including a mandatory PIN configuration.

Figure F-17 MaaS360 Applying Mandatory PIN Policy



Default Android MDM Policy

Last Published: 10/21/2019 12:38 EDT [Version:45] **Current Status**: Published

Passcode Settings

Configure Passcode Policy ☑ Android 5.0+ (PO & DO)

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

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

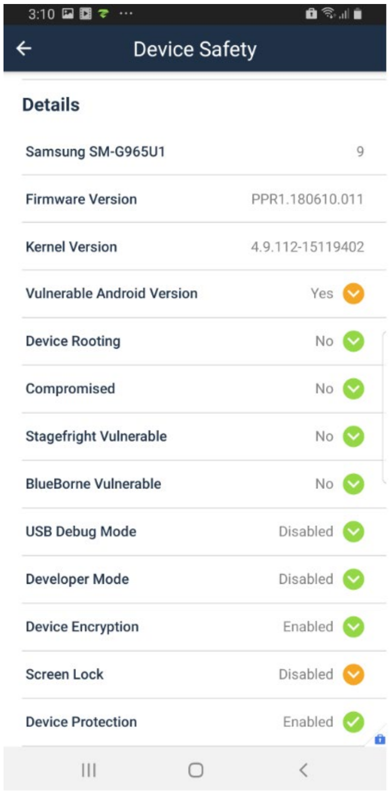
Requires Android 5.0+ and Android App 6.05+ for restricting passcode quality to Numeric Complex.
Requires Android App 6.30+ for Weak Biometric, else defaults to Numeric.

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

Delay for Passcode prompt after lock screen Immediate DO With KNOX (SAFE 2.0+)

The figure shows Zimperium reporting discovery of a disabled lock screen.

Figure F-18 Zimperium Reporting Devices with a Disabled Lock Screen



Device Safety

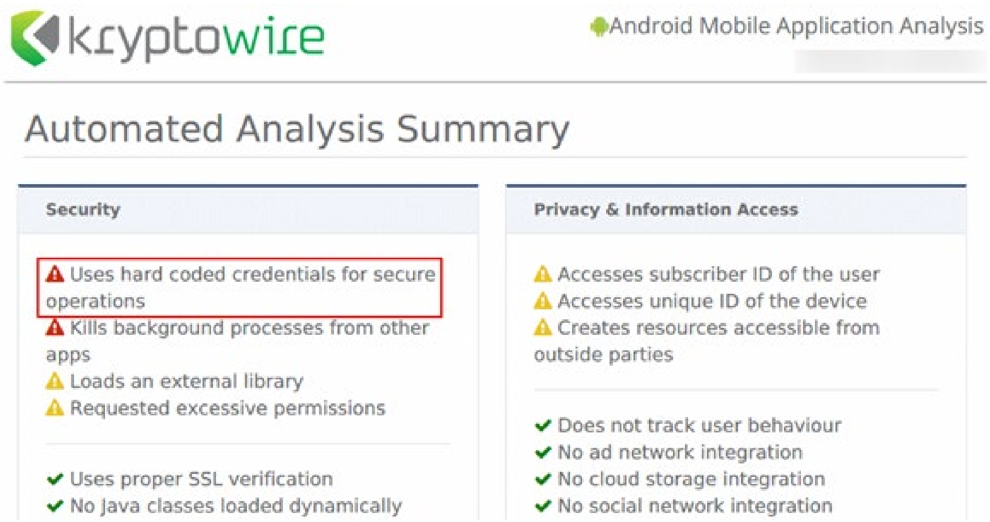
Details

Samsung SM-G965U1	9	
Firmware Version	PPR1.180610.011	
Kernel Version	4.9.112-15119402	
Vulnerable Android Version	Yes	✓
Device Rooting	No	✓
Compromised	No	✓
Stagefright Vulnerable	No	✓
BlueBorne Vulnerable	No	✓
USB Debug Mode	Disabled	✓
Developer Mode	Disabled	✓
Device Encryption	Enabled	✓
Screen Lock	Disabled	✓
Device Protection	Enabled	✓

F.8 Threat Event 8

Threat Event 8 testing images show a report that detected unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications.

Figure F-19 Application Report with Hardcoded Credentials



Automated Analysis Summary

Security

- ⚠ Uses hard coded credentials for secure operations
- ⚠ Kills background processes from other apps
- ⚠ Loads an external library
- ⚠ Requested excessive permissions

- ✓ Uses proper SSL verification
- ✓ No Java classes loaded dynamically

Privacy & Information Access

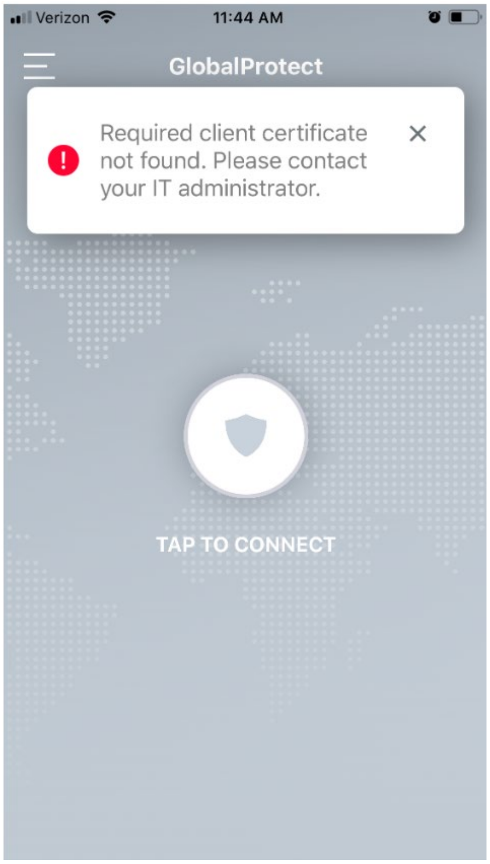
- ⚠ Accesses subscriber ID of the user
- ⚠ Accesses unique ID of the device
- ⚠ Creates resources accessible from outside parties

- ✓ Does not track user behaviour
- ✓ No ad network integration
- ✓ No cloud storage integration
- ✓ No social network integration

F.9 Threat Event 9

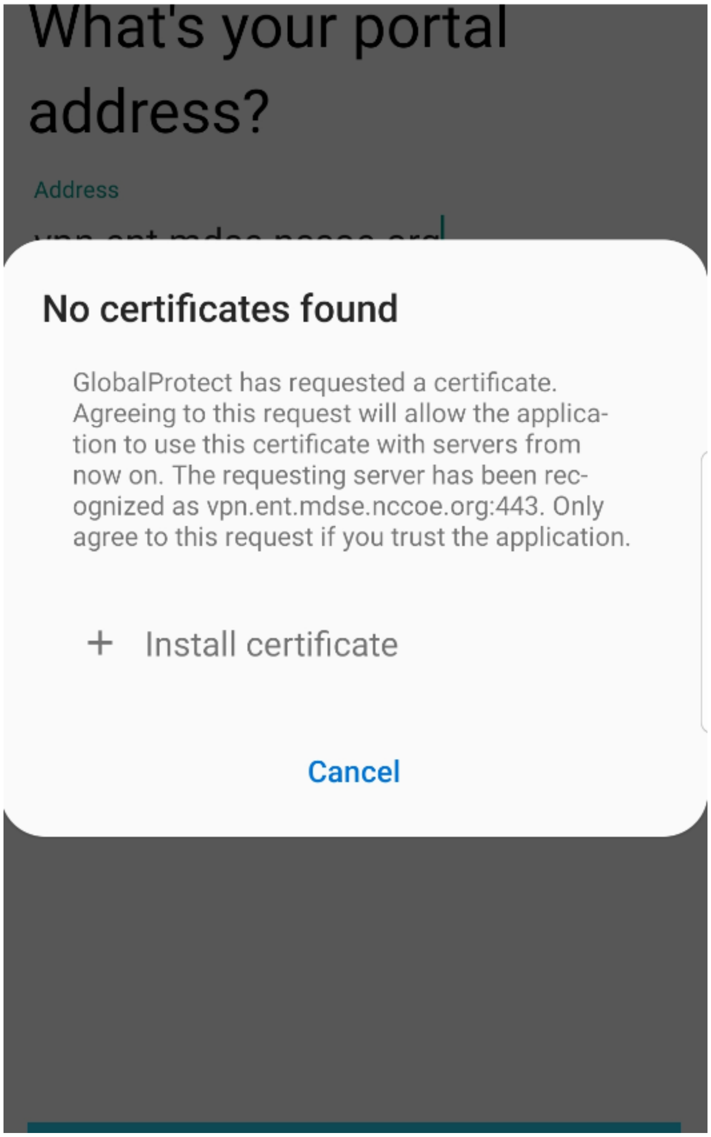
Threat Event 9 shows an unsuccessful attempt to access enterprise resources from an unmanaged and potentially compromised device.

1719 **Figure F-20 Attempting to Access the Virtual Private Network (VPN) on an Unmanaged Device**



Required client certificate not found. Please contact your IT administrator.

1720 **Figure F-21 Android: Attempting to Access the VPN on an Unmanaged Device**

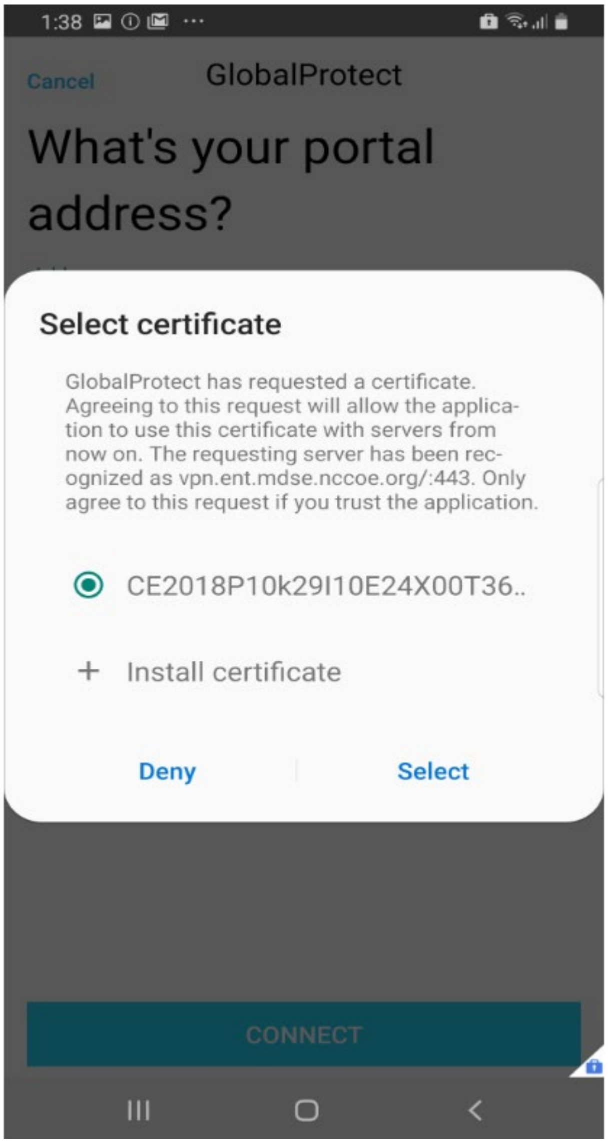


What's your portal address?

No certificates found

GlobalProtect has requested a certificate. Agreeing to this request will allow the application to use this certificate with servers from now on. The requesting server has been recognized as vpn.ent.mdse.nccoe.org:443. Only agree to this request if you trust the application.

1721 **Figure F-22 Android: Attempting to Access the VPN on a Managed Device**



Select certificate

GlobalProtect has requested a certificate. Agreeing to this request will allow the application to use this certificate with servers from now on. The requesting server has been recognized as vpn.ent.mdse.nccoe.org/:443. Only agree to this request if you trust the application.

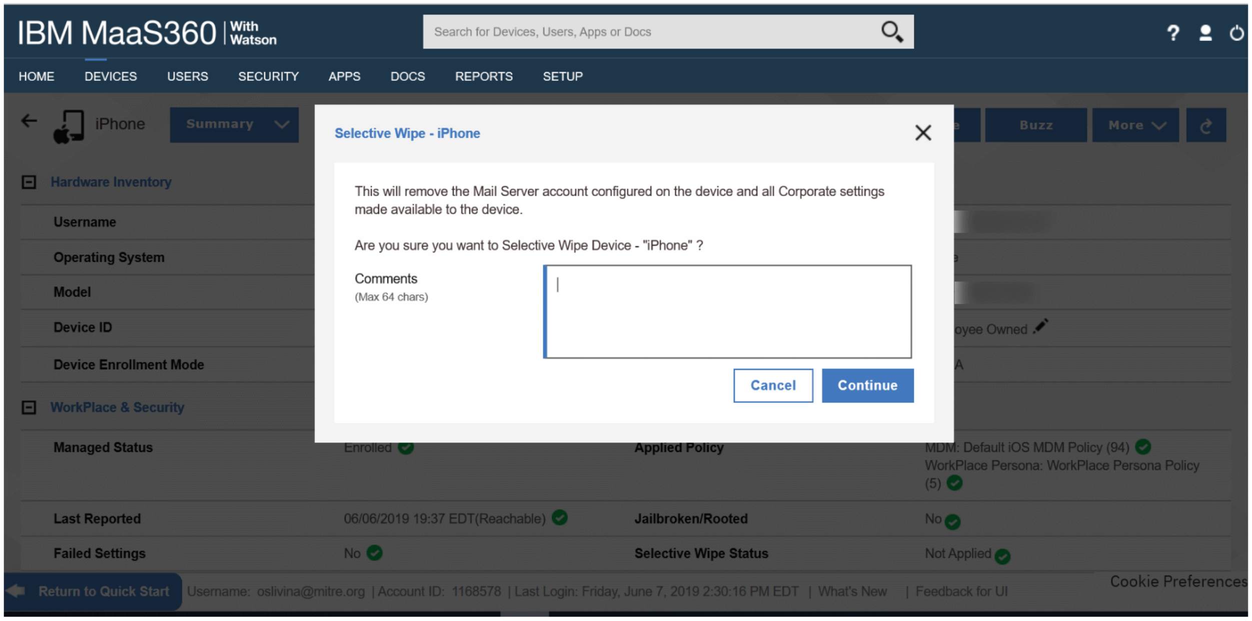
● CE2018P10k29I10E24X00T36..

+ Install certificate

1722 F.10 Threat Event 10

1723 These screen captures show selectively wiping the device to remove organizational data. This prevents
1724 the loss of organizational data due to a lost or stolen device.

Figure F-23 Selectively Wiping an iOS Device



Selective Wipe - iPhone

This will remove the Mail Server account configured on the device and all Corporate settings made available to the device.

Are you sure you want to Selective Wipe Device - "iPhone" ?

Comments (Max 64 chars)

Cancel | Continue

Hardware Inventory

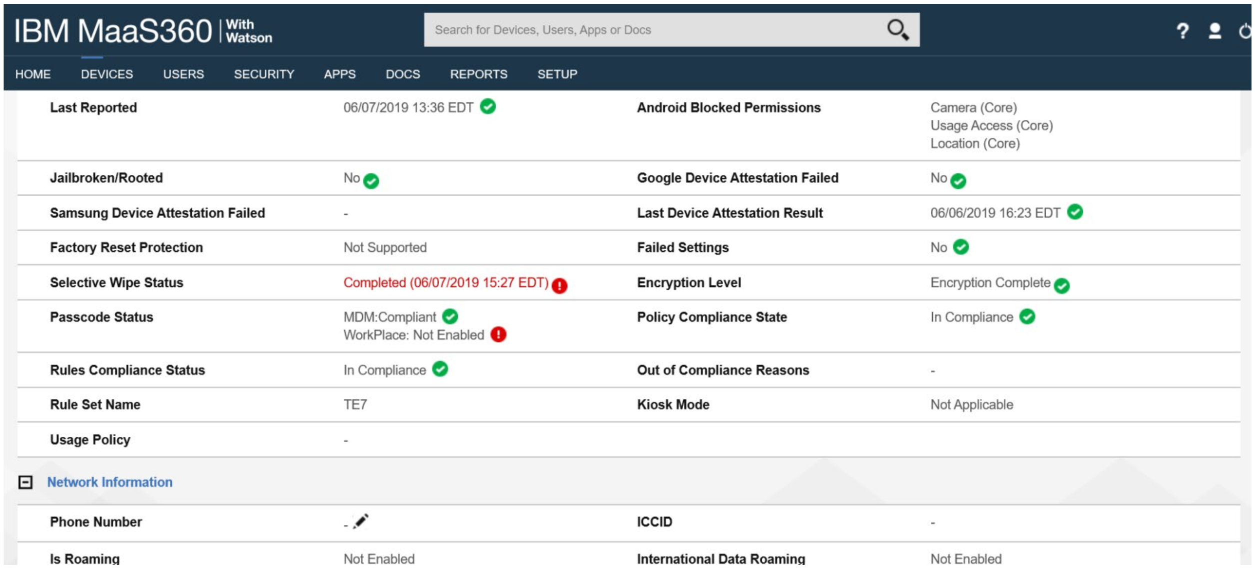
Username			
Operating System			
Model			
Device ID			oyee Owned
Device Enrollment Mode			A

WorkPlace & Security

Managed Status	Enrolled ✓	Applied Policy	MDM: Default iOS MDM Policy (94) ✓ WorkPlace Persona: WorkPlace Persona Policy (5) ✓
Last Reported	06/06/2019 19:37 EDT(Reachable) ✓	Jailbroken/Rooted	No ✓
Failed Settings	No ✓	Selective Wipe Status	Not Applied ✓

Return to Quick Start | Username: oslivina@mitre.org | Account ID: 1168578 | Last Login: Friday, June 7, 2019 2:30:16 PM EDT | What's New | Feedback for UI | Cookie Preferences

Figure F-24 Selective-Wipe Completed

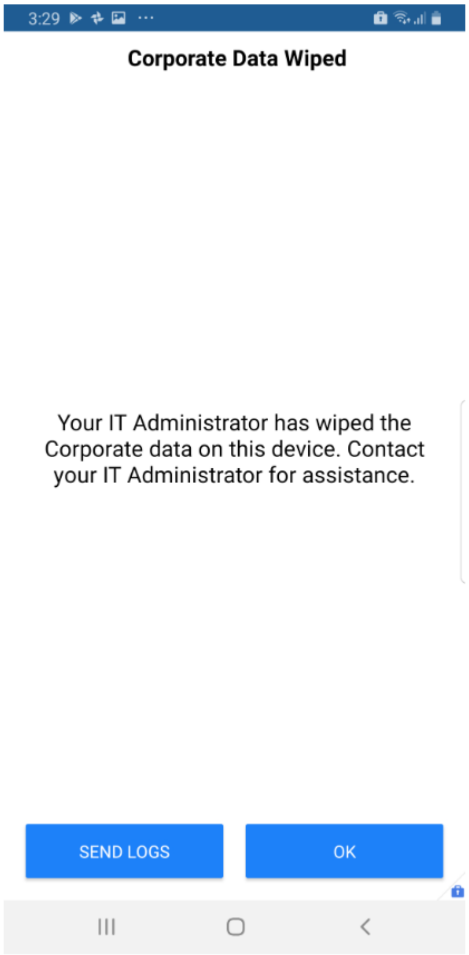


Last Reported	06/07/2019 13:36 EDT ✓	Android Blocked Permissions	Camera (Core) Usage Access (Core) Location (Core)
Jailbroken/Rooted	No ✓	Google Device Attestation Failed	No ✓
Samsung Device Attestation Failed	-	Last Device Attestation Result	06/06/2019 16:23 EDT ✓
Factory Reset Protection	Not Supported	Failed Settings	No ✓
Selective Wipe Status	Completed (06/07/2019 15:27 EDT) !	Encryption Level	Encryption Complete ✓
Passcode Status	MDM:Compliant ✓ WorkPlace: Not Enabled !	Policy Compliance State	In Compliance ✓
Rules Compliance Status	In Compliance ✓	Out of Compliance Reasons	-
Rule Set Name	TE7	Kiosk Mode	Not Applicable
Usage Policy	-		

Network Information

Phone Number	-	ICCID	-
Is Roaming	Not Enabled	International Data Roaming	Not Enabled

Figure F-25 No Corporate Data Left on Device



3:29

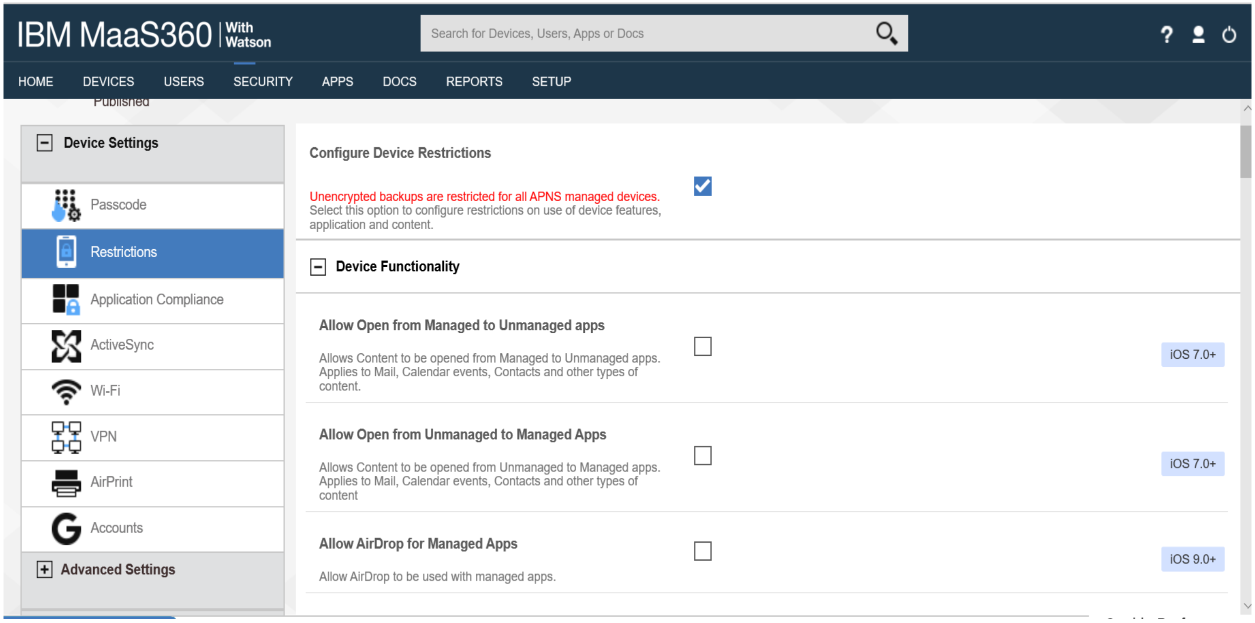
Corporate Data Wiped

Your IT Administrator has wiped the Corporate data on this device. Contact your IT Administrator for assistance.

F.11 Threat Event 11

These images show an example configuration and outcome to prevent data from being pasted from one application to another application.

1731 **Figure F-26 MaaS360 DLP Configuration**



Configure Device Restrictions ☑

Unencrypted backups are restricted for all APNS managed devices.
Select this option to configure restrictions on use of device features, application and content.

Device Functionality

Allow Open from Managed to Unmanaged apps □ iOS 7.0+

Allows Content to be opened from Managed to Unmanaged apps. Applies to Mail, Calendar events, Contacts and other types of content.

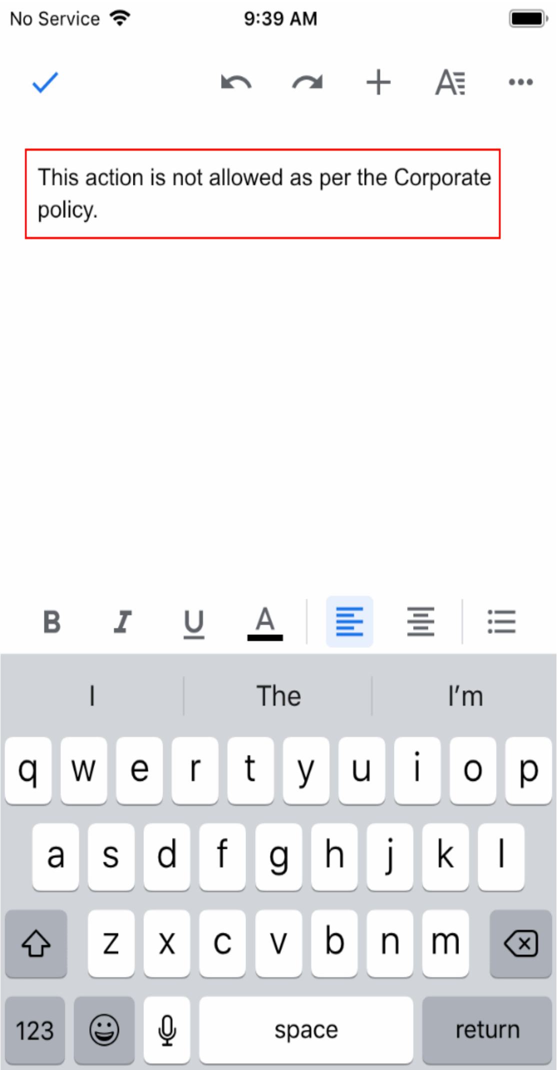
Allow Open from Unmanaged to Managed Apps □ iOS 7.0+

Allows Content to be opened from Unmanaged to Managed apps. Applies to Mail, Calendar events, Contacts and other types of content

Allow AirDrop for Managed Apps □ iOS 9.0+

Allow AirDrop to be used with managed apps.

Figure F-27 Attempting to Paste Text on iOS

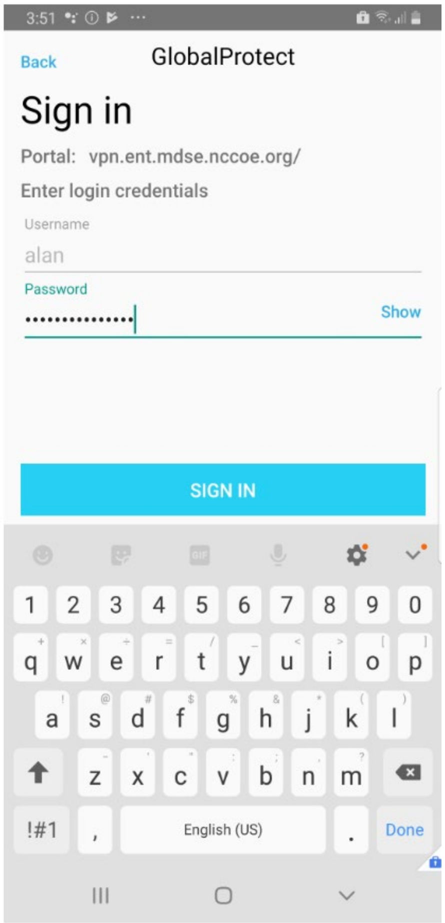


This action is not allowed as per the Corporate policy.

F.12 Threat Event 12

This image shows a required password to prevent unauthorized access to work applications via a bypassed lock screen. If the lock screen is bypassed, individuals would not be able to connect to the VPN without knowing the user's domain password.

1737 **Figure F-28 GlobalProtect Requires the User's Password**



Portal: vpn.ent.mdse.nccoe.org/

Enter login credentials

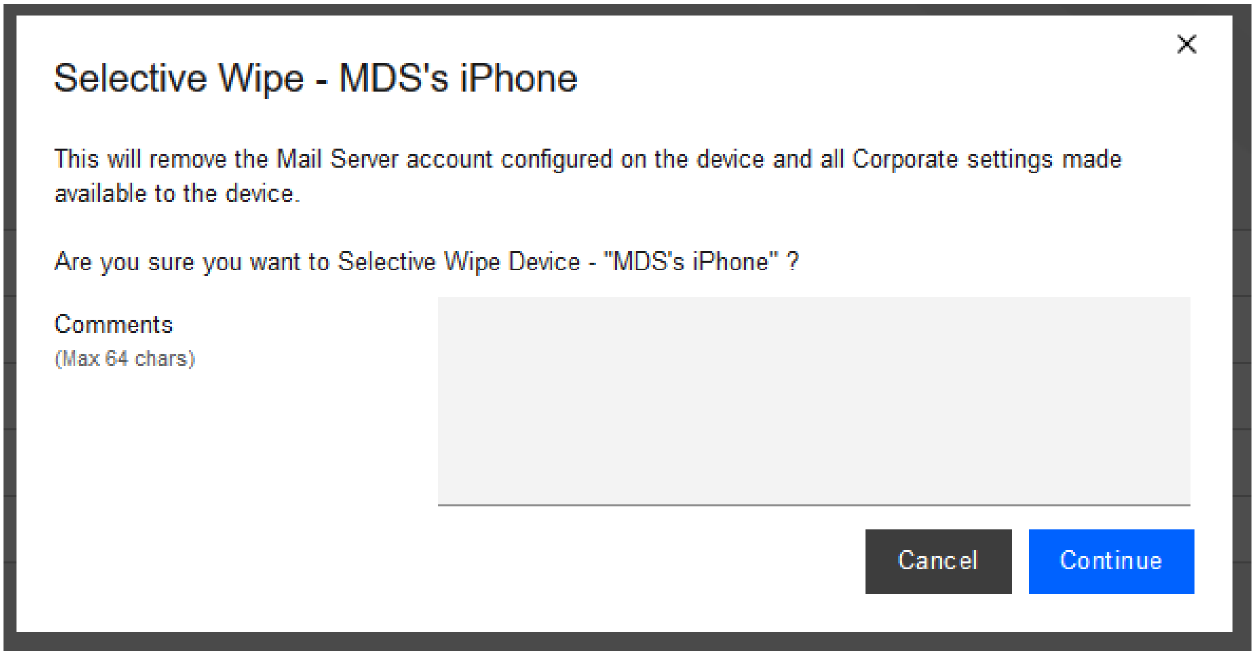
Username: alan

Password: •••••••••••••••

1738 F.13 Problematic Data Action 1

1739 This image shows initiation of a selective wipe. The selective wipe will remove the Mail Server account
1740 and all corporate settings available to the device.

Figure F-29 Initiating a Selective Wipe



Selective Wipe - MDS's iPhone

This will remove the Mail Server account configured on the device and all Corporate settings made available to the device.

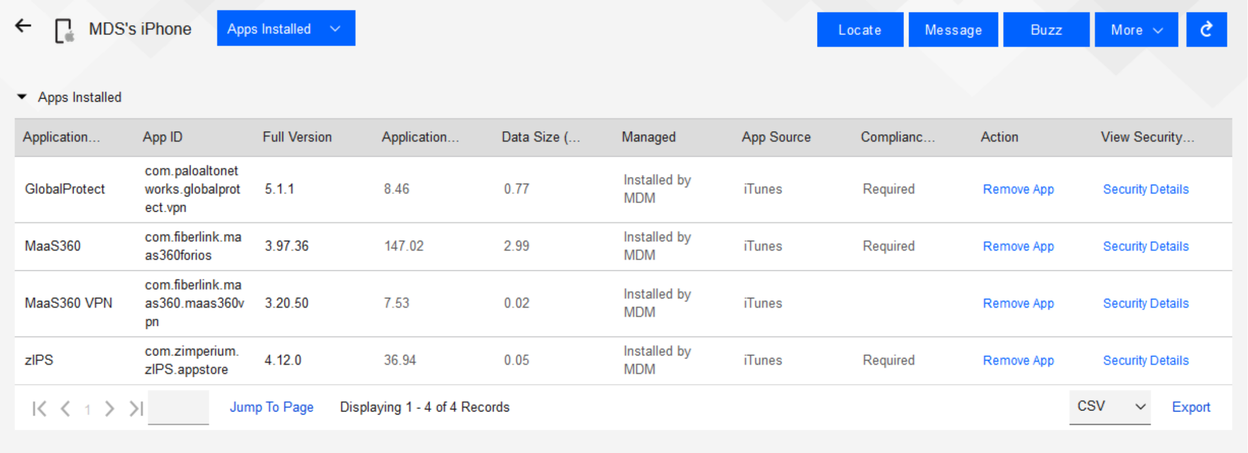
Are you sure you want to Selective Wipe Device - "MDS's iPhone" ?

Comments
(Max 64 chars)

F.14 Problematic Data Action 2

This shows inventory information for applications and the location information restriction.

Figure F-30 Application Inventory Information



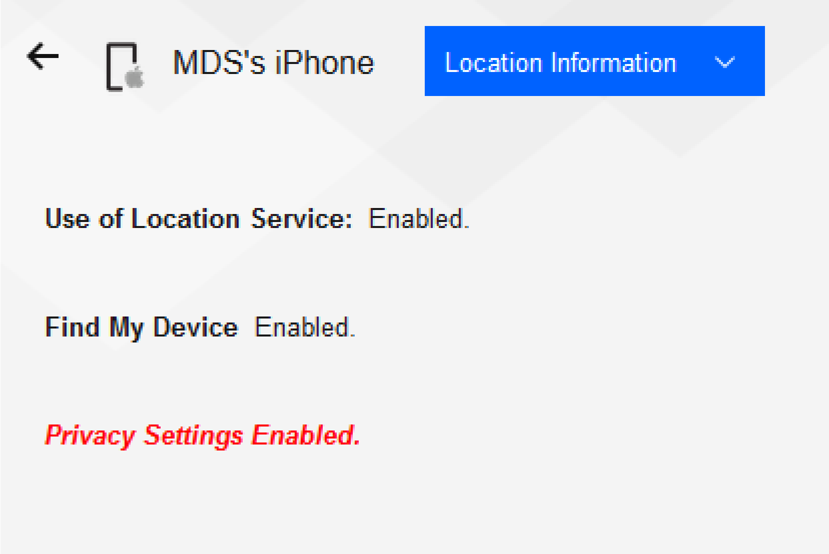
Apps Installed

Application...	App ID	Full Version	Application...	Data Size (...	Managed	App Source	Complianc...	Action	View Security...
GlobalProtect	com.paloaltonetworks.globalprotect.vpn	5.1.1	8.46	0.77	Installed by MDM	iTunes	Required	Remove App	Security Details
MaaS360	com.fiberlink.maas360forios	3.97.36	147.02	2.99	Installed by MDM	iTunes	Required	Remove App	Security Details
MaaS360 VPN	com.fiberlink.maas360.maas360vpn	3.20.50	7.53	0.02	Installed by MDM	iTunes		Remove App	Security Details
zIPS	com.zimperium.zIPS.appstore	4.12.0	36.94	0.05	Installed by MDM	iTunes	Required	Remove App	Security Details

Displaying 1 - 4 of 4 Records

When privacy restrictions are configured, only corporate application inventory information is collected.

Figure F-31 Location Information Restricted



Use of Location Service: Enabled.

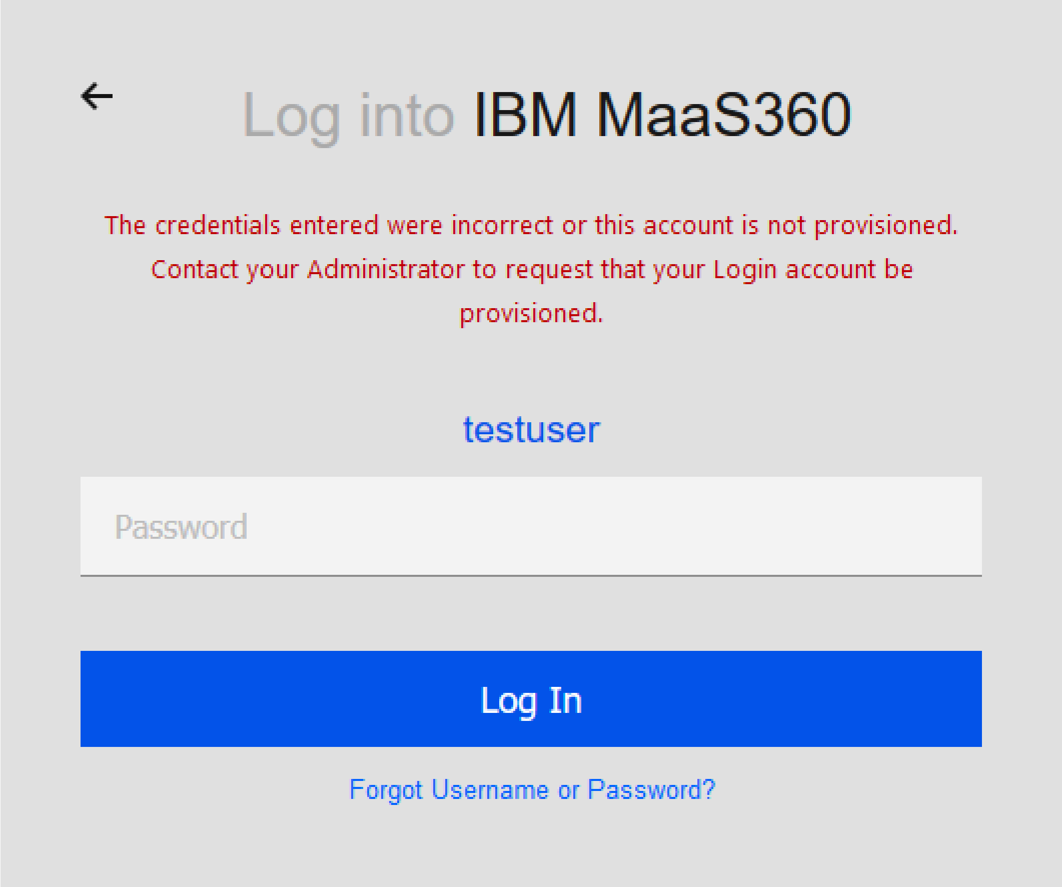
Find My Device Enabled.

Privacy Settings Enabled.

F.15 Problematic Data Action 3

This demonstrates how a non-administrator account will be prevented from logging in to the MaaS360 portal.

1750 **Figure F-32 Non-Administrator Failed Portal Login**



Log into IBM MaaS360

The credentials entered were incorrect or this account is not provisioned. Contact your Administrator to request that your Login account be provisioned.

testuser

Appendix G Example Security Subcategory and Control Map

Using the developed risk information as input, the security characteristics of the example solution were identified. A security control map was developed documenting the example solution's capabilities with applicable Subcategories from the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1]; NIST Special Publication (SP) 800-53 Revision 5*, Security and Privacy Controls for Information Systems and Organizations* [38]; International Organization for Standardization (ISO); International Electrotechnical Commission (IEC) 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* [47]; the Center for Internet Security's (CIS) control set Version 6 [43]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

Table G-1's example security control map identifies the security characteristic standards mapping for the products as they were used in the example solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended that the mapping not be used as a reference for all of the security capabilities these products may be able to address.

Table G-1 Example Solution's Cybersecurity Standards and Best Practices Mapping

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Mobile Threat Defense						
Kryptowire Cloud Service	Application Vetting	**ID.RA-1:** Asset vulnerabilities are identified and documented.	**CA-2, CA-7, CA-8:** Security Assessment and Authorization **RA-3, RA-5:** Risk Assessment **SA-4:** Acquisition Process	**A.12.6.1:** Control of technical vulnerabilities **A.18.2.3:** Technical Compliance Review	**CSC 4:** Continuous Vulnerability Assessment and Remediation	**SP-RSK-002:** Security Control Assessor **SP-ARC-002:** Security Architect **OM-ANA-001:** Systems Security Analyst

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			SI-7: Software, Firmware, and Information Integrity			
		ID.RA-3: Threats, both internal and external, are identified and documented.	**RA-3:** Risk Assessment **SI-7:** Software, Firmware, and Information Integrity **PM-12, PM-16:** Insider Threat Program	**6.1.2:** Information risk assessment process	**CSC 4:** Continuous Vulnerability Assessment and Remediation	**SP-RSK-002:** Security Control Assessor **OM-ANA-001:** Systems Security Analyst **OV-SPP-001:** Cyber Workforce Developer and Manager **OV-TEA-001:** Cyber Instructional Curriculum Developer **PR-VAM-001:** Vulnerability Assessment Analyst

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
						PR-VAM-001: Vulnerability Assessment Analyst
		DE.CM-4: Malicious code is detected.	**SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware	**CSC 4:** Continuous Vulnerability Assessment and Remediation **CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses **CSC 12:** Boundary Defense	**PR-CIR-001:** Cyber Defense Incident Responder **PR-CDA-001:** Cyber Defense Analyst
		DE.CM-5: Unauthorized mobile code is detected.	**SC-18:** Mobile Code **SI-7:** Software, Firmware, and	**A.12.5.1:** Installation of Software on Operational Systems	**CSC 7:** Email and Web Browser Protections	**PR-CDA-001:** Cyber Defense Analyst

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			Information Integrity	**A.12.6.2:** Restrictions on Software Installation	**CSC 8:** Malware Defenses	**SP-DEV-002:** Secure Software Assessor
Zimperium Console version vGA-4.23.1	Cloud service that complements the zIPS Agent	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	**CM-8:** Information System Component Inventory **PM-5:** Information System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets	**CSC 1:** Inventory of Authorized and Unauthorized Devices	**OM-STS-001:** Technical Support Specialist **OM-NET-001:** Network Operations Specialist **OM-ADM-001:** System Administrator

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
zIPS agent Version 4.9.2 (iOS), 4.9.2 (Android)	Endpoint security for mobile device threats	**ID.AM-2:** Software platforms and applications within the organization are inventoried.	**CM-8:** Information System Component Inventory **PM-5:** Information System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets **A.12.5.1:** Installation of Software on Operational Systems	**CSC 2:** Inventory of Authorized and Unauthorized Software	**SP-DEV-002:** Secure Software Assessor **SP-DEV-001:** Software Developer **SP-TRD-001:** Research and Development Specialist
		DE.CM-8: Vulnerability scans are performed.	**RA-5:** Vulnerability Monitoring and Scanning	**A.12.6.1:** Management of technical vulnerabilities	**CSC 4:** Continuous Vulnerability Assessment and Remediation **CSC 20:** Penetration Tests and Red Team Exercises	**PR-VAM-001:** Vulnerability Assessment Analyst **PR-INF-001:** Cyber Defense Infrastructure Support Specialist **PR-CDA-001:** Cyber Defense Analyst

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		DE.AE-5: Incident alert thresholds are established.	**IR-4:** Incident Handling **IR-5:** Incident Monitoring **IR-8:** Incident Response Plan	**A.16.1.4:** Assessment of and decision on information security events	**CSC 6:** Maintenance, Monitoring, and Analysis of Audit Logs **CSC 19:** Incident Response and Management	**PR-CIR-001:** Cyber Defense Incident Responder **AN-TWA-001:** Threat/Warning Analyst
		DE.CM-5: Unauthorized mobile code is detected.	**SC-18:** Mobile Code **SI-7:** Software, Firmware, and Information Integrity	**A.12.5.1:** Installation of Software on Operational Systems **A.12.6.2:** Restrictions on Software Installation	**CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses	**PR-CDA-001:** Cyber Defense Analyst **SP-DEV-002:** Secure Software Assessor
Enterprise Mobility Management						
IBM MaaS360 Mobile Device Management (SaaS)	Enforces organizational mobile endpoint security policy	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	**CM-8:** System Component Inventory **PM-5:** System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets	**CSC 1:** Inventory of Authorized and Unauthorized Devices	**OM-STS-001:** Technical Support Specialist **OM-NET-001:** Network Operations Specialist

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Version 10.73						**OM-ADM-001:** System Administrator
		ID.AM-2: Software platforms and applications within the organization are inventoried.	**CM-8:** System Component Inventory **PM-5:** System Inventory	**A.8.1.1:** Inventory of Assets **A.8.1.2:** Ownership of Assets **A.12.5.1:** Installation of Software on Operational Systems	**CSC 2:** Inventory of Authorized and Unauthorized Software	**SP-DEV-002:** Secure Software Assessor **SP-DEV-001:** Software Developer **SP-TRD-001:** Research and Development Specialist

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	**AC-3:** Access Enforcement **IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11:** Identification and Authentication Family	**A.9.2.1:** User Registration and De-Registration **A.9.2.2:** User Access Provisioning **A.9.2.3:** Management of Privileged Access Rights **A.9.2.4:** Management of Secret Authentication Information of Users **A.9.2.6:** Removal or Adjustment of Access Rights **A.9.3.1:** Use of Secret Authentication Information	**CSC 1:** Inventory of Authorized and Unauthorized Devices **CSC 5:** Controlled Use of Administrative Privileges **CSC 15:** Wireless Access Control **CSC 16:** Account Monitoring and Control	**OV-SPP-002:** Cyber Policy and Strategy Planner **OM-ADM-001:** System Administrator **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
				A.9.4.2: Secure logon Procedures **A.9.4.3:** Password Management System		

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.AC-3: Remote access is managed.	**AC-1:** Access Control Policy and Procedures **AC-17:** Remote Access **AC-19:** Access Control for Mobile Devices **AC-20:** Use of External Systems **SC-15:** Collaborative Computing Devices and Applications	**A.6.2.1:** Mobile Device Policy **A.6.2.2:** Teleworking **A.11.2.6:** Security of equipment and assets off premises **A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures	**CSC 12:** Boundary Defense	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	**AC-1, AC-3:** Access Control Policy and Procedures **IA-2, IA-4, IA-5:** Identification	**A.7.1.1:** Screening **A.9.2.1:** User Registration and De-Registration	**CSC 16:** Account Monitoring and Control	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			and Authentication **PE-2:** Physical Access Authorizations			(COMSEC) Manager
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	**CM-8:** System Component Inventory **SA-10:** Developer Configuration Management	**A.12.1.2:** Change Management **A.12.5.1:** Installation of Software on Operational Systems **A.12.6.2:** Restrictions on Software Installation **A.14.2.2:** System Change Control Procedures **A.14.2.3:** Technical Review of Applications After Operating Platform Changes	**CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers **CSC 9:** Limitation and Control of Network Ports, Protocols, and Services **CSC 11:** Secure Configurations for Network Devices such as	**SP-ARC-002:** Security Architect **OV-SPP-002:** Cyber Policy and Strategy Planner **SP-SYS-001:** Information Systems Security Developer **OM-ADM-001:** System Administrator **PR-VAM-001:** Vulnerability Assessment Analyst

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
				A.14.2.4: Restrictions on Changes to Software Packages	Firewalls, Routers, and Switches	

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)	Endpoint software that compliments IBM MaaS360 Mobile Device Management console–provides root/jailbreak detection and other functions	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**SC-16:** Transmission of Security and Privacy Attributes **SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware **A.12.5.1:** Installation of Software on Operational Systems **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions **A.14.2.4:** Restrictions on Changes to Software Packages	**CSC 2:** Inventory of Authorized and Unauthorized Software **CSC 3:** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	**OV-SPP-002:** Cyber Policy and Strategy Planner **SP-ARC-001:** Enterprise Architect

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Trusted Execution Environment						
Qualcomm (version is mobile device dependent)	Secure boot and image integrity	**PR.DS-1:** Data-at-rest is protected.	**SC-28:** Protection of Information at Rest	**A.8.2.3:** Handling of Assets	**CSC 13:** Data Protection **CSC 14:** Controlled Access Based on the Need to Know	**OV-SPP-002:** Cyber Policy and Strategy Planner **PR-INF-001:** Cyber Defense Infrastructure Support Specialist **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**SA-10(1):** Developer Configuration Management **SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware **A.12.5.1:** Installation of Software on Operational Systems **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions **A.14.2.4:** Restrictions on Changes to Software Packages	**CSC 2:** Inventory of Authorized and Unauthorized Software **CSC 3:** Secure Configurations for Hardware and Software on Mobile	**OV-SPP-002:** Cyber Policy and Strategy Planner **PR-CDA-001:** Cyber Defense Analyst **SP-ARC-001:** Enterprise Architect
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	**SA-10:** Developer Configuration Management	**A.11.2.4:** Equipment maintenance	Not applicable	**OM-ADM-001:** System Administrator

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			SI-7: Software, Firmware, and Information Integrity			**SP-ARC-001:** Enterprise Architect
		DE.CM-4: Malicious code is detected.	**SC-35:** External Malicious Code Identification **SI-7:** Software, Firmware, and Information Integrity	**A.12.2.1:** Controls Against Malware	**CSC 4:** Continuous Vulnerability Assessment and Remediation **CSC 7:** Email and Web Browser Protections **CSC 8:** Malware Defenses **CSC 12:** Boundary Defense	**PR-CDA-001:** Cyber Defense Analyst **PR-INF-001:** Cyber Defense Infrastructure Support Specialist
Virtual Private Network						
Palo Alto Networks PA-220	Enforces network security policy for remote devices	**PR.AC-3:** Remote access is managed.	**AC-1, AC-3:** Access Control Policy and Procedures	**A.6.2.1:** Mobile Device Policy **A.6.2.2:** Teleworking	**CSC 12:** Boundary Defense	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:**

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			AC-19: Access Control for Mobile Devices	**A.11.2.6:** Security of equipment and assets off-premises **A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures		Communications Security (COMSEC) Manager
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	**AC-3:** Access Enforcement **SC-7:** Boundary Protection	**A.13.1.1:** Network Controls **A.13.1.3:** Segregation in Networks **A.13.2.1:** Information Transfer Policies and Procedures **A.14.1.2:** Securing Application	**CSC 9:** Limitation and Control of Network Ports, Protocols, and Services **CSC 14:** Controlled Access Based on the Need to Know **CSC 15:** Wireless Access Control	**PR-CDA-001:** Cyber Defense Analyst **OM-ADM-001:** System Administrator

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
				Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions	**CSC 18:** Application Software Security	
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	**AC-3:** Access Enforcement **IA-2, IA-4, IA-5, IA-8:** Identification and Authentication (Organizational Users) **PE-2:** Physical Access Authorizations **PS-3:** Personnel Screening	**A.7.1.1:** Screening **A.9.2.1:** User Registration and De-Registration	**CSC 16:** Account Monitoring and Control	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
		PR.DS-2: Data-in-transit is protected.	**AC-17(2):** Protection of Confidentiality and Integrity Using Encryption **SC-8:** Transmission Confidentiality and Integrity	**A.8.2.3:** Handling of Assets **A.13.1.1:** Network Controls **A.13.2.1:** Information Transfer Policies and Procedures **A.13.2.3:** Electronic Messaging **A.14.1.2:** Securing Application Services on Public Networks **A.14.1.3:** Protecting Application Services Transactions	**CSC 13:** Data Protection **CSC 14:** Controlled Access Based on the Need to Know	**OV-SPP-002:** Cyber Policy and Strategy Planner **OV-MGT-002:** Communications Security (COMSEC) Manager **OV-LGA-002:** Privacy Officer/Privacy Compliance Manager
		PR.PT-4: Communications and control networks are protected.	**AC-3, AC-4, AC-17, AC-18:** Access Control Family	**A.13.1.1:** Network Controls	**CSC 8:** Malware Defenses	**PR-INF-001:** Cyber Defense Infrastructure

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
			CP-2: Contingency Plan **SC-7, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-38, SC-39, SC-40, SC-41, SC-43:** System and Communications Protection Family	**A.13.2.1:** Information Transfer Policies and Procedures **A.14.1.3:** Protecting Application Services Transactions	**CSC 12:** Boundary Defense **CSC 15:** Wireless Access Control	Support Specialist **OV-SPP-002:** Cyber Policy and Strategy Planner **PR-CDA-001:** Cyber Defense Analyst

Appendix H Example Privacy Subcategory and Control Map

Using the developed privacy information as input, we identified the privacy characteristics of the example solution. We developed a privacy control map documenting the example solution's capabilities with applicable Functions, Categories, and Subcategories from the National Institute of Standards and Technology *(NIST) Privacy Framework* [2]; and NIST SP 800-53 Revision 5 [38]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

The table that follows maps component functions in the build to the related Subcategories in the NIST Privacy Framework as well as to controls in the NIST SP 800-53, Revision 5 controls catalog. Each column maps independently to the build component's functions and, given the specific capabilities of this mobile device security solution, may differ from other NIST-provided mappings for the Privacy Framework and SP 800-53 revision. For example, build functions may provide additional capabilities beyond what is contemplated by a Privacy Framework Subcategory or that are implemented by additional controls beyond those that NIST identified as an informative reference for the Subcategory.

Table H-1's example privacy control map identifies the privacy characteristic mapping for the products as they were used in the example solution. The products may have additional capabilities that we did not use in this example solution. For that reason, it is recommended that the mapping not be used as a reference for all of the privacy capabilities these products may be able to address. The comprehensive mapping of the NIST Privacy Framework to NIST SP 800-53, Revision 5 controls can be found on the NIST Privacy Framework Resource Repository website, in the event an organization's mobile device security solution is different to determine other controls that are appropriate for their environment [62].

Table H-1 Example Solution's Privacy Standards and Best Practices Mapping

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
IBM MaaS360	MaaS360 can be used to capture an inventory of the types and number of devices deployed and shows the administra-	**ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	**CM-12:** Information Location **CM-13:** Data Action Mapping	**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager **OV-TEA-001:** Cyber Instructional Curriculum Developer

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	tors what data is collected from each enrolled device.		**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **PT-3:** Personally Identifiable Information Processing Purposes **RA-3:** Risk Assessment **RA-8:** Privacy Impact Assessment	
	Administrators can view data elements in the administration portal. Users can see collected data within the MaaS360 application on their device. Data can be edited and deleted from within the administration console.	**CT.DM-P1:** Data elements can be accessed for review.	**AC-2:** Account Management **AC-3:** Access Enforcement **AC-3(14):** Access Enforcement | Individual Access **PM-21:** Accounting of Disclosures	**OM-DTA-002:** Data Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		CT.DM-P3: Data elements can be accessed for alteration.	**AC-2:** Account Management **AC-3:** Access Enforcement **AC-3(14):** Access Enforcement | Individual Access **PM-21:** Accounting of Disclosures **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst
		CT.DM-P4: Data elements can be accessed for deletion.	**AC-2:** Account Management **AC-3:** Access Enforcement **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		CT.DM-P5: Data are destroyed according to policy.	**MP-6:** Media Sanitization **SA-8(33):** Security and Privacy Engineering Principles | Minimization **SI-18:** Personally Identifiable Information Quality Operations **SR-12**: Component Disposal	**OM-DTA-002:** Data Analyst
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	**CM-6:** Configuration Settings **SA-8(33):** Minimization **SC-42(5):** Collection Minimization **SI-12(1):** Information Management and Retention | Limit Personally Identifiable Information Elements	**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	Devices may be backed up to the cloud.	**PR.PO-P3:** Backups of information are conducted, maintained, and tested.	**CP-4:** Contingency Plan Testing **CP-6:** Alternate Storage Site **CP-9:** System Backup	**OM-ADM-001:** System Administrator
	Devices are issued identity certificates via on-premises certificate infrastructure.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	**IA-2:** Identification and Authentication (Organizational Users) **IA-3:** Device Identification and Authentication **IA-4:** Identifier Management **IA-4(4):** Identifier Management | Identifier User Status	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
	MaaS360 enforces a device personal identification number (PIN) for access.	**PR.AC-P2:** Physical access to data and devices is managed.	**PE-2:** Physical Access Authorizations **PE-3:** Physical Access Control **PE-3(1):** System Access	**OM-DTA-001:** Database Administrator **OM-DTA-002:** Data Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			PE-4: Access Control for Transmission **PE-5:** Access Control for Output Devices **PE-6:** Monitoring Physical Access **PE-18:** Location of System Components **PE-20:** Asset Monitoring and Tracking	
		PR.DS-P1: Data-at-rest are protected.	**MP-2:** Media Access **MP-4:** Media Storage **PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-28:** Protection of Information at Rest	**OM-DTA-001:** Database Administrator **OM-DTA-002:** Data Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	Data flowing between the device and MaaS360 is encrypted with Transport Layer Security.	**PR.DS-P2:** Data-in-transit are protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity	**PR-CIR-001:** Cyber Defense Incident Responder
	Restrictions are used that prevent data flow between enterprise and personal applications.	**PR.DS-P5:** Protections against data leaks are implemented.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **AC-4:** Information Flow Enforcement	**PR-CIR-001:** Cyber Defense Incident Responder
	Devices that are jailbroken or otherwise modified beyond original equipment manufacturer status can be detected.	**PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PM-22:** Personally Identifiable Information Quality Management **SI-7:** Software, Firmware, and Information Integrity **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
Zimperium	Zimperium checks the device for unauthorized modifications.	**PR.DS-P1:** Data-at-rest are protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-28:** Protection of Information at Rest	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.DS-P2: Data-in-transit are protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity **SC-11:** Trusted Path	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PM-22:** Personally Identifiable Information Quality Management **SC-16:** Transmission of Security Attributes **SI-7:** Boundary Protection **SI-10:** Network Disconnect **SI-18:** Personally Identifiable Information Quality Operations	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst
Kryptowire	Kryptowire can identify applications that do not use best practices, such as lack of encryption or hardcoded credentials.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests	**AC-8:** System Use Notification	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		are established and in place.		
		CM.AW-P3: System/ product/ service design enables data processing visibility.	**PL-8:** Security and Privacy Architecture **PM-5(1):** System Inventory | Inventory of Personally Identifiable Information	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/ disclosure.	**AC-16:** Security and Privacy Attributes **SC-16:** Transmission of Security Attributes	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.DS-P1: Data-at-rest are protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-28:** Protection of Information at Rest	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.DS-P2: Data-in-transit are protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			SC-8: Transmission Confidentiality and Integrity **SC-11:** Trusted Path	
Palo Alto Networks PA-220	Provides firewall and virtual private network capabilities.	**PR.DS-P2:** Data-in-transit are protected.	**PM-5(1):** System Inventory | Inventory of Personally Identifiable Information **SC-8:** Transmission Confidentiality and Integrity **SC-11:** Trusted Path	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**AC-2:** Account Management **AC-3:** Access Enforcement **AC-5:** Separation of Duties **AC-6:** Least Privilege **AC-24:** Access Control Decisions	**SP-ARC-002:** Security Architect **PR-CDA-001:** Cyber Defense Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**AC-4:** Information Flow Enforcement **AC-10:** Access Control **SC-7:** Boundary Protection **SC-10:** Network Disconnect	**OM-DTA-002:** Data Analyst **OM-ANA-001:** Systems Security Analyst
		PR.PT-P3: Communications and control networks are protected.	**AC-12:** Session Termination **AC-17:** Remote Access **AC-18:** Wireless Access **SC-5:** Denial of Service Protection **SC-7:** Boundary Protection **SC-10:** Network Disconnect **SC-11:** Trusted Path	**OV-LGA-002:** Privacy Officer/Privacy Compliance Manager **PR-CDA-001:** Cyber Defense Analyst

Product	How the component functions in the build	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
			SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver) **SC-23:** Session Authenticity	
Qualcomm	The trusted execution environment provides data confidentiality and integrity.	**PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PM-22:** Personally Identifiable Information Quality Management **SC-16:** Transmission of Security and Privacy Attributes **SI-7:** Software, Firmware, and Information Integrity **SI-10:** Information Input Validation **SI-18:** Personally Identifiable Information Quality Operations	**PR-INF-001:** Cyber Defense Infrastructure Support Specialist **OM-ANA-001:** Systems Security Analyst

NIST SPECIAL PUBLICATION 1800-22 Supplement

Mobile Device Security:

Bring Your Own Device (BYOD)

Supplement:
Example Scenario: Putting Guidance into Practice

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

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

1 Applying This Build: Example Scenario

An example scenario about a fictional company named Great Seneca Accounting illustrates how organizations can use this practice guide's example solution. The example shows how Bring Your Own Device (BYOD) objectives can align with a fictional organization's security and privacy priorities through the use of risk management standards, guidance, and tools.

To demonstrate how an organization may use this National Institute of Standards and Technology (NIST) Special Publication (SP) and other NIST tools to implement a BYOD use case, the National Cybersecurity Center of Excellence created an example scenario that centers around a fictional, small-to-mid-size organization called Great Seneca Accounting. This scenario exemplifies the issues that an organization may face when addressing common enterprise BYOD security challenges.

1.1 Standards and Guidance Used in this Example Scenario

In addition to the Executive Summary contained in Volume A, and the architecture description in Volume B, this practice guide also includes a series of how-to instructions in Volume C. The how-to instructions in Volume C provide step-by-step instructions covering the initial setup (installation or provisioning) and configuration for each component of the architecture. These step-by-step instructions can help security engineers rapidly deploy and evaluate the example solution in their test environment.

The example solution uses standards-based, commercially available products that can be used by an organization interested in deploying a BYOD solution. The example solution provides recommendations for enhancing the security and privacy infrastructure by integrating on-premises and cloud-hosted mobile security technologies. This practice guide provides an example solution that an organization may use in whole or in part as the basis for creating a custom solution that best supports their unique needs.

The fictional Great Seneca Accounting organization illustrates how this guide may be applied by an organization, starting with a mobile device infrastructure that lacked mobile device security architecture concepts. Great Seneca employed multiple NIST cybersecurity and privacy risk management tools to understand the gaps in its architecture and methods to enhance security of its systems and privacy for its employees.

This example scenario provides useful context for using the following NIST Frameworks and other relevant tools to help mitigate some of the security and privacy challenges that organizations may encounter when deploying BYOD capabilities:

- NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework) [1]
- the *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework) [2]
- NIST Special Publication (SP) 800-181 *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [3]
- NIST Risk Management Framework [4]

- NIST Mobile Threat Catalogue [5]

For additional information, see Volume B’s Appendix D.

2 About Great Seneca Accounting

In the example scenario, Great Seneca Accounting is a fictional accounting firm that grew from a single office location into a larger firm with a regional presence. Great Seneca Accounting performs accounting functions related to capturing, communicating, processing, transmitting, and analyzing financial data and accounting services for its customers.

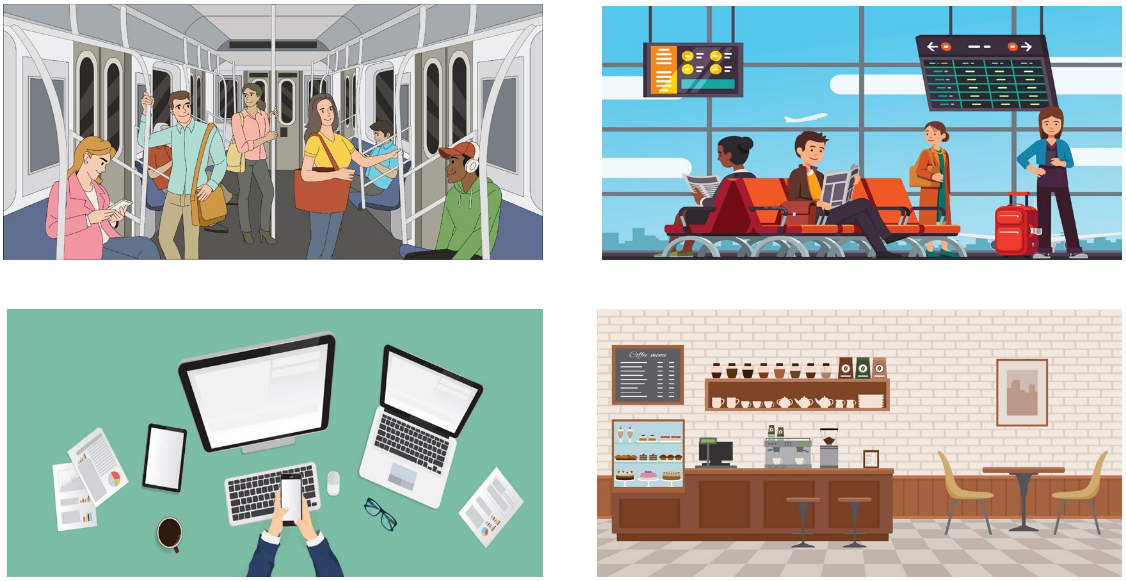
When the firm was first created, most of its employees worked from the Great Seneca Accounting office, with minimal use of mobile devices. They were able to do this without actively embracing mobile device usage because most of the employees worked at their desks at the company’s single location.

Over the years, the Great Seneca Accounting company grew from a local company, where all of its employees performed work at their desks by using desktop computers provided by the organization, into a regional firm with employees who work remotely and who support regional customers.

Now, many of the employees spend part of their week traveling and working from customer or other remote locations. This has prompted the organization to specify, as a strategic priority, the need to support employees to work remotely, while both traveling and working from a customer location. As such, the company wants to embrace BYOD solutions to support its remote work.

Figure 1-1 shows an overview of the typical work environments for a Great Seneca Accounting employee. Many employees work remotely while using their own mobile phones and tablets to perform both work and personal activities throughout the day.

Figure 1-1 Great Seneca Accounting’s Work Environments



Great Seneca Accounting's corporate management initiated a complete review of all policies, procedures, and technology relating to its mobile deployment to ensure that the company is well protected against attacks involving personal mobile devices. This includes mitigating risks against its devices, custom applications, and corporate infrastructure supporting mobile services. Management identified NIST's Risk Management Framework (RMF) [4] and Privacy Risk Assessment Methodology (PRAM) [6] as useful tools for supporting this analysis. The company developed Cybersecurity Framework and Privacy Framework Target Profiles to guide Great Seneca Accounting's decision-making because the Target Profiles link Great Seneca Accounting's mission and business priorities with supporting cybersecurity and privacy activities.

Great Seneca Accounting identified the scope of their mobile solution to be both Android and Apple personally owned mobile phones and tablets. While this example scenario intends to provide an exemplar of organization guidance with a description of BYOD concepts and how to apply those concepts, this example scenario should not suggest a limit on BYOD uses.

Great Seneca Accounting plans to use NIST SP 1800-22 (this practice guide) to inform its updated BYOD architecture as well as NIST's Mobile Threat Catalogue to identify threats to mobile deployment. These NIST frameworks and tools used are described further in Appendix E.

As shown in Figure 2-1, this example solution applied multiple mobile device security technologies. These included a cloud-based Enterprise Mobility Management solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities that support the example solution.

Figure 2-2 Example Solution Architecture

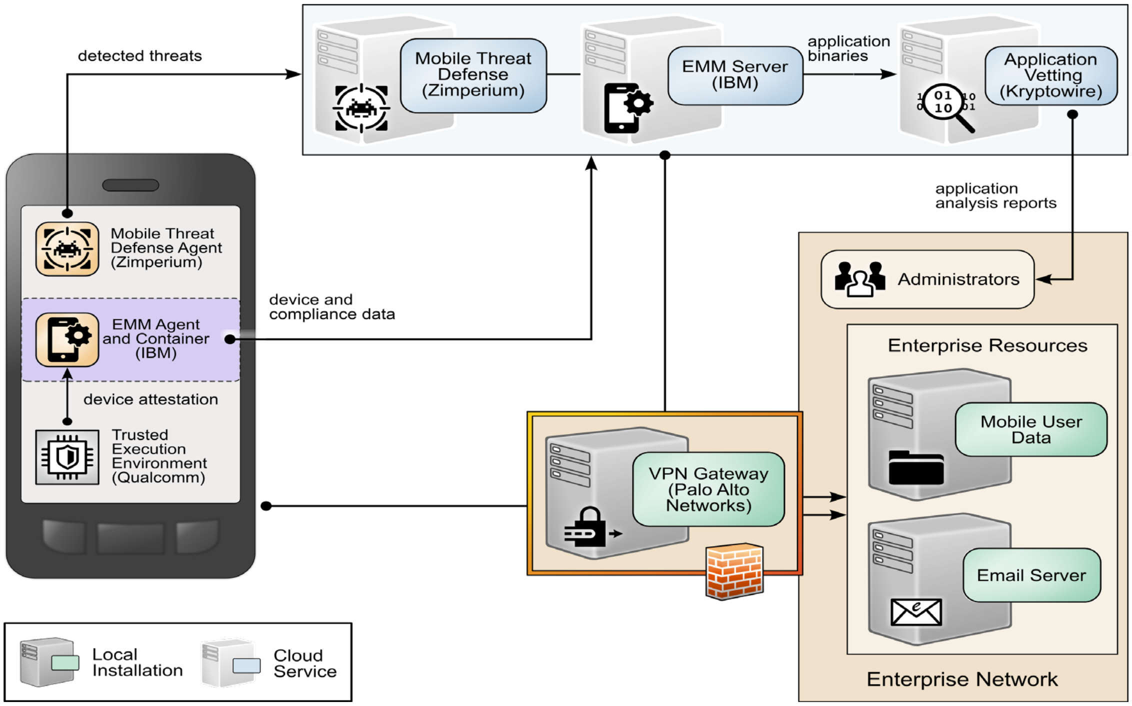
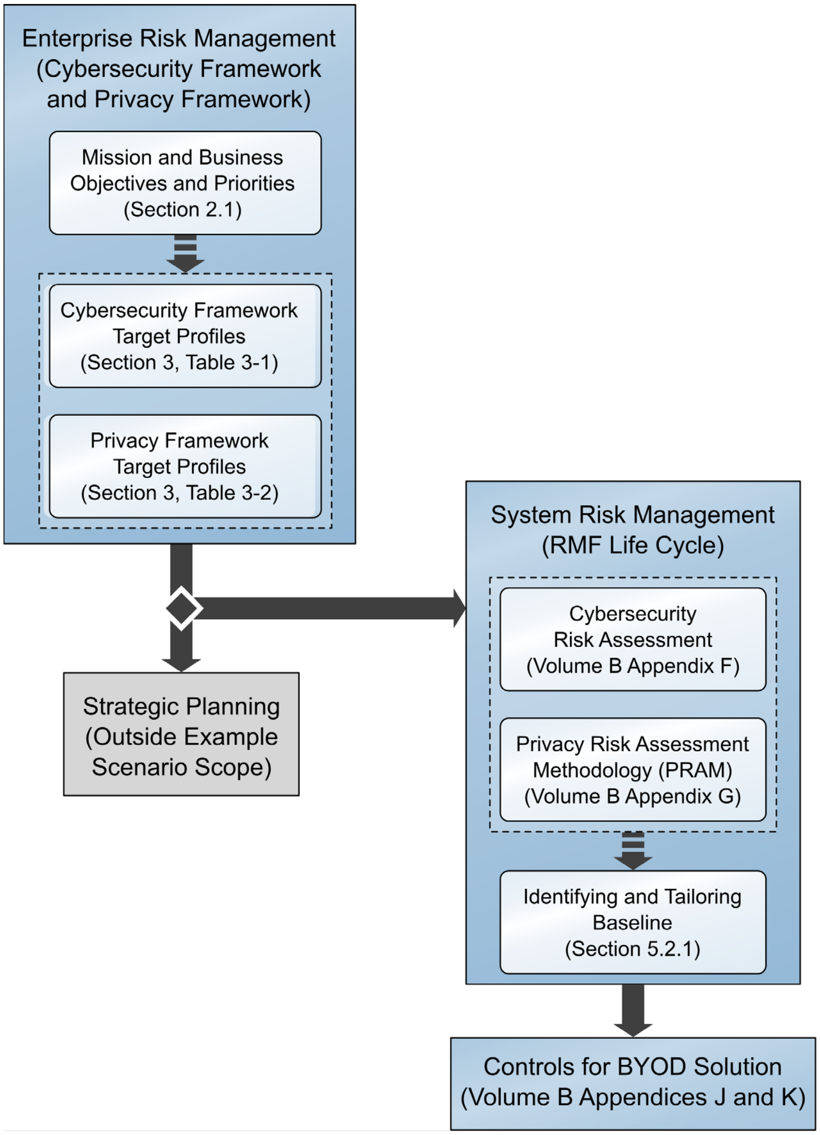

detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Enterprise Network
Local Installation
Cloud Service

Figure 2-2 shows the overall process that Great Seneca Accounting plans to follow. It highlights key activities from various NIST guidance documents related to security and privacy risk management, each of which is discussed in the sections identified in Figure 2-2. Please note that this process is an abbreviated version of steps provided in NIST SP 800-37 Revision 2 [7], which shows how some available resources may be used by any organization.

Figure 2-3 Great Seneca Accounting's Security and Privacy Risk Management Steps


Enterprise Risk Management (Cybersecurity Framework and Privacy Framework)
Mission and Business Objectives and Priorities (Section 2.1)
Cybersecurity Framework Target Profiles (Section 3, Table 3-1)
Privacy Framework Target Profiles (Section 3, Table 3-2)
Strategic Planning (Outside Example Scenario Scope)
System Risk Management (RMF Life Cycle)
Cybersecurity Risk Assessment (Volume B Appendix F)
Privacy Risk Assessment Methodology (PRAM) (Volume B Appendix G)
Identifying and Tailoring Baseline (Section 5.2.1)
Controls for BYOD Solution (Volume B Appendices J and K)

2.1 Great Seneca Accounting's Business/Mission Objectives

Great Seneca Accounting developed a mission statement and a set of supporting business/mission objectives to ensure that its activities align with its core purpose. The company has had the same mission since it was founded:

Mission Statement

Provide financial services with integrity and responsiveness

While Great Seneca Accounting has a number of business/mission objectives, those below relate to its interest in BYOD, listed in priority order:

1. Provide good data stewardship.
2. Enable timely communication with clients.
3. Provide innovative financial services.
4. Enable workforce flexibility.

3 Great Seneca Accounting's Target Profiles

Great Seneca Accounting used the NIST Cybersecurity Framework and *NIST Privacy Framework* as key strategic planning tools to improve its security and privacy programs. It followed the processes outlined in the frameworks, and as part of that effort, created *two* Target Profiles—one for cybersecurity and one for privacy.

These Target Profiles describe the desired or aspirational state of Great Seneca Accounting by identifying and prioritizing the cybersecurity and privacy activities and outcomes needed to support its enterprise business/mission objectives. The Subcategories in each Framework Core articulate those cybersecurity and privacy activities and outcomes.

Note: See Appendix E for a high-level description of the Cybersecurity Framework and Privacy Framework.

To understand what Subcategories to prioritize implementing in each framework, Great Seneca Accounting considered the importance of the Subcategories for accomplishing each business/mission objective. The Target Profiles reflect that discussion by designating prioritized Subcategories as low, moderate, or high.

Subcategory improvements important for BYOD deployment also became part of its Target Profiles because Great Seneca Accounting was upgrading its existing information technology infrastructure as part of its BYOD implementation.

The Cybersecurity Framework Target Profile in Table 3-1 and the Privacy Framework Target Profile in Table 3-2 are included as examples of Great Seneca Accounting's identification of the business/mission objectives that are relevant to their BYOD deployment.

Great Seneca Accounting chose to address the Subcategories that are prioritized as moderate and high for multiple business/mission objectives in its Target Profiles for this year's BYOD deployment with plans to address the low Subcategories in the future.

Table 3-1 and Table 3-2 include only those Subcategories that are prioritized as moderate or high for the business/mission Objectives. Any Subcategory designated as low is included in Table 3-1 and Table 3-2 only because it is high or moderate for another business/mission objective.

Great Seneca Accounting used the Target Profiles to help guide risk management decisions throughout the organization's activities, including making decisions regarding budget allocation, technology design, and staffing for its programs and technology deployments. Discussions for developing and using the Target Profiles include stakeholders in various parts of the organization, such as business/mission program owners, data stewards, cybersecurity practitioners, privacy practitioners, legal and compliance experts, and technology experts.

Note: Low, moderate, and high designations indicate the level of relative importance among Subcategories for Great Seneca to accomplish a business/mission objective.

Table 3-1 Great Seneca Accounting’s Cybersecurity Framework Target Profile

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	**Category**	**Subcategory**	**(1) Provide Good Data Stewardship**	**(2) Enable timely communication with clients**	**(3) Provide Innovative Financial Services**	**(4) Enable Workforce Flexibility**
IDENTIFY	**Asset Management**	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	moderate	moderate	moderate	low
		ID.AM-2: Software platforms and applications within the organization are inventoried.	moderate	moderate	moderate	low
	Risk Assessment	**ID.RA-1:** Asset vulnerabilities are identified and documented.	moderate	moderate	moderate	moderate
		ID.RA-3: Threats, both internal and external, are identified and documented.	moderate	moderate	moderate	moderate
PROTECT	**Identity Management and Access Control**	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	moderate	high	moderate	high
		PR.AC-3: Remote access is managed.	moderate	high	high	high
		PR.AC-5: Network integrity is protected (e.g., network	high	high	high	high

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		segregation, network segmentation).				
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	moderate	high	high	high
	Data Security	**PR.DS-1:** Data-at-rest is protected.	high	moderate	moderate	high
		PR.DS-2: Data-in-transit is protected.	moderate	high	moderate	high
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	moderate	moderate	moderate	low
	Information Protection Processes and Procedures	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.	moderate	moderate	moderate	low

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	**Category**	**Subcategory**	**(1) Provide Good Data Stewardship**	**(2) Enable timely communication with clients**	**(3) Provide Innovative Financial Services**	**(4) Enable Workforce Flexibility**
	Protective Technology	**PR.PT-4:** Communications and control networks are protected.	low	moderate	moderate	low
DETECT	**Anomalies and Events**	**DE.AE-5:** Incident alert thresholds are established.	high	high	high	high
	Security Continuous Monitoring	**DE.CM-4:** Malicious code is detected.	high	high	high	high
		DE.CM-5: Unauthorized mobile code is detected.	moderate	moderate	moderate	low
		DE.CM-8: Vulnerability scans are performed.	high	high	high	high

133 **Table 3-2 Great Seneca Accounting's Privacy Target Profile**

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	**Category**	**Subcategory**	**(1)** **Provide Good Data Stewardship**	**(2)** **Enable timely communication with clients**	**(3)** **Provide Innovative Financial Services**	**(4)** **Enable Workforce Flexibility**
IDENTIFY-P	**Inventory and Mapping**	**ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	high	high	high	high
GOVERN-P	**Governance Policies, Processes, and Procedures**	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.	high	high	high	high
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	high	high	high	high
	Monitoring and Review	**GV.MT-P3:** Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	high	high	high	high

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).	high	high	high	high
CONTROL-P	Data Management	**CT.DM-P1:** Data elements can be accessed for review.	high	moderate	high	moderate
		CT.DM-P3: Data elements can be accessed for alteration.	high	moderate	high	moderate
		CT.DM-P4: Data elements can be accessed for deletion.	high	moderate	high	moderate
		CT.DM-P5: Data are destroyed according to policy.	high	moderate	high	moderate
	Disassociated Processing	**CT.DP-P4:** System or device configurations permit	high	high	high	high

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		selective collection or disclosure of data elements.				
COMMUNICATE-P	**Data Processing Awareness**	**CM.AW-P5:** Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	high	moderate	moderate	moderate
PROTECT-P	**Data Protection Policies, Processes, and Procedures**	**PR.PO-P3:** Backups of information are conducted, maintained, and tested.	high	moderate	high	moderate
		PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	moderate	high	moderate	high
	Identity Management, Authentication, and Access Control	**PR.AC-P2:** Physical access to data and devices is managed.	high	moderate	high	moderate
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	high	moderate	high	moderate

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	**Category**	**Subcategory**	**(1) Provide Good Data Stewardship**	**(2) Enable timely communication with clients**	**(3) Provide Innovative Financial Services**	**(4) Enable Workforce Flexibility**
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high
		PR.DS-P1: Data-at-rest are protected.	high	moderate	moderate	high
	Data Security	**PR.DS-P2:** Data-in-transit are protected.	moderate	high	moderate	high
		PR.DS-P5: Protections against data leaks are implemented.	high	moderate	high	moderate
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		PR.PT-P3: Communications and control networks are protected.	moderate	high	moderate	high

4 Great Seneca Accounting Embraces BYOD

Great Seneca Accounting now allows its staff to use their personal mobile devices to perform their daily work duties on an as-needed basis. Accountants use the devices for various tasks including communicating with client organizations and other employees, collecting confidential client information, analyzing financial transactions, generating reports, accessing tax and payroll information, and creating and reviewing comprehensive financial statements.

Great Seneca accountants work from many locations including their corporate office building, their homes, their customers' offices, and other locations. And to be able to work in all of these locations, they require the use of mobile devices to perform their job functions.

Great Seneca Accounting's current mobile infrastructure enables accountants to perform their job duties by using their personally owned devices, despite minimal security installed and enforced on these devices. Examples of security concerns with the use of personally owned devices are:

- Employees can connect to any Wi-Fi network to perform work-related activities when they are working on the road, including at a client's site.
- Custom mobile applications being sideloaded onto devices that employees use.
- The personally owned devices allow users to install applications on an as-needed basis without separation of enterprise and personal data.

While not affecting Great Seneca Accounting, a string of well-publicized cybersecurity attacks have recently been reported in the news, and this prompted Great Seneca to review its mobile device security and privacy deployment strategy. When making BYOD deployment decisions, Great Seneca Accounting plans to prioritize implementing cybersecurity and privacy capabilities that would enable it to accomplish its business/mission objectives (i.e., its reasons for deploying BYOD capabilities).

To do this, Great Seneca Accounting conducted a technical assessment of its current BYOD architecture to help it understand ways to improve the confidentiality, integrity, availability, and privacy of data and devices associated with its BYOD deployment. The company identified several vulnerabilities based on its current mobile device deployment. Figure 4-1 below presents a subset of those vulnerabilities.

Figure 4-1 Great Seneca Accounting's Current Mobile Deployment Architecture (Before Security and Privacy Enhancements)

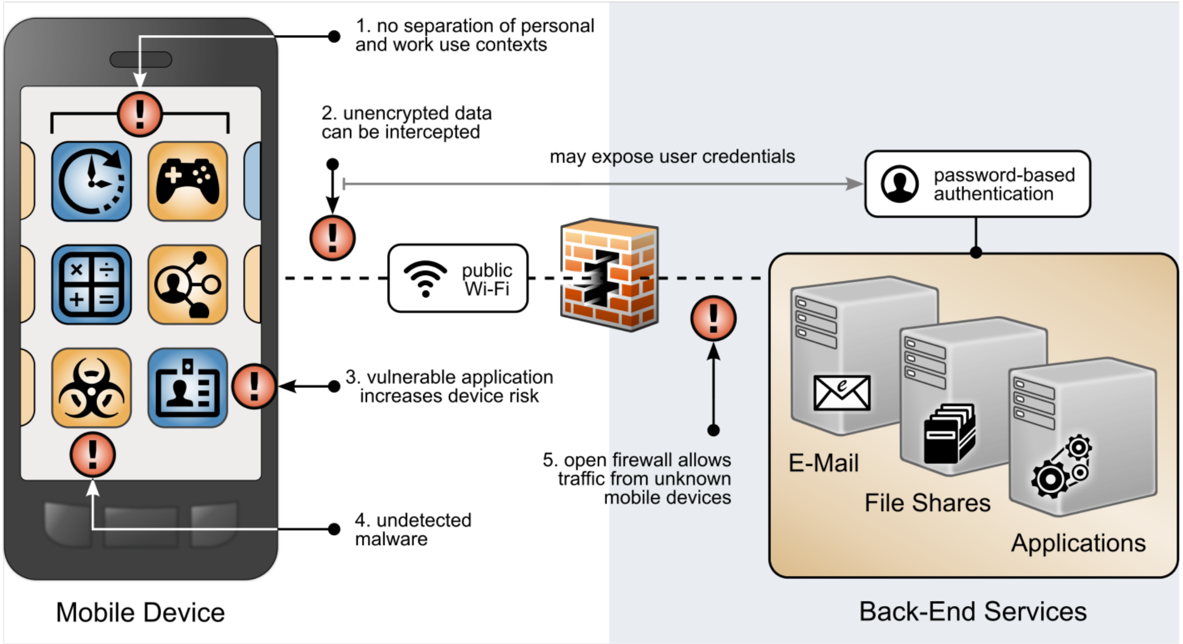

1. no separation of personal and work use contexts
2. unencrypted data can be intercepted
may expose user credentials
password-based authentication
public Wi-Fi
3. vulnerable application increases device risk
5. open firewall allows traffic from unknown mobile devices
4. undetected malware
E-Mail
File Shares
Applications
Mobile Device
Back-End Services

Figure 4-1 highlights the following vulnerabilities with a red exclamation mark:

1. BYOD deployments can place organizational and personal data, as well as employees' privacy, at risk. Organizational and personal data can become commingled if either the same application is used in both contexts or if multiple applications access shared device resources (e.g., contacts or calendar) as applications for both personal and work usage are installed. This also puts employees' privacy at risk, as the organization can have visibility into their personal life outside work.
2. BYOD deployments can leverage nonsecure networks. As employees use nonsecure Wi-Fi hotspots, mobile devices that are connecting to Great Seneca Accounting from those unencrypted networks place data transmitted prior to a secure connection at risk of discovery and eavesdropping, including passwords.
3. As employees install applications on their personally owned devices, the applications can have unidentified vulnerabilities or weaknesses that increase the risk of device compromise (e.g., applications that access contacts may now have access to the organization's client contact information). Further, legitimate, privacy-intrusive applications can legally collect data through terms and conditions and requested permissions.
4. On personally owned devices without restriction policies in place, employees may inadvertently download applications outside official application stores, which are malware in disguise.

5. Because personally owned mobile devices can connect from unknown locations, firewall rules must allow inbound connections from unrecognized, potentially malicious Internet Protocol addresses.

In addition to identifying the technical assets and the vulnerabilities, Great Seneca Accounting identified the scope of the mobile solution (i.e., both Android and Apple personally owned mobile phones and tablets) and the regulatory requirements or guidance that will apply to their deployment and solution (e.g., encryption will be Federal Information Processing Standards [FIPS]-validated to protect sensitive accounting information).

5 Applying NIST Risk Management Methodologies to Great Seneca Accounting's BYOD Architecture

Sections 2 and 3 described Great Seneca Accounting, their business mission, and what security and privacy areas they consider most important. Great Seneca created Target Profiles that mapped their BYOD-related mission/business objectives and priorities with the Functions, Categories, and Subcategories of both the Cybersecurity Framework and the Privacy Framework. Those Cybersecurity Framework and Privacy Framework Target Profiles are provided in Table 3-1 and Table 3-2 in Section 3 of this document.

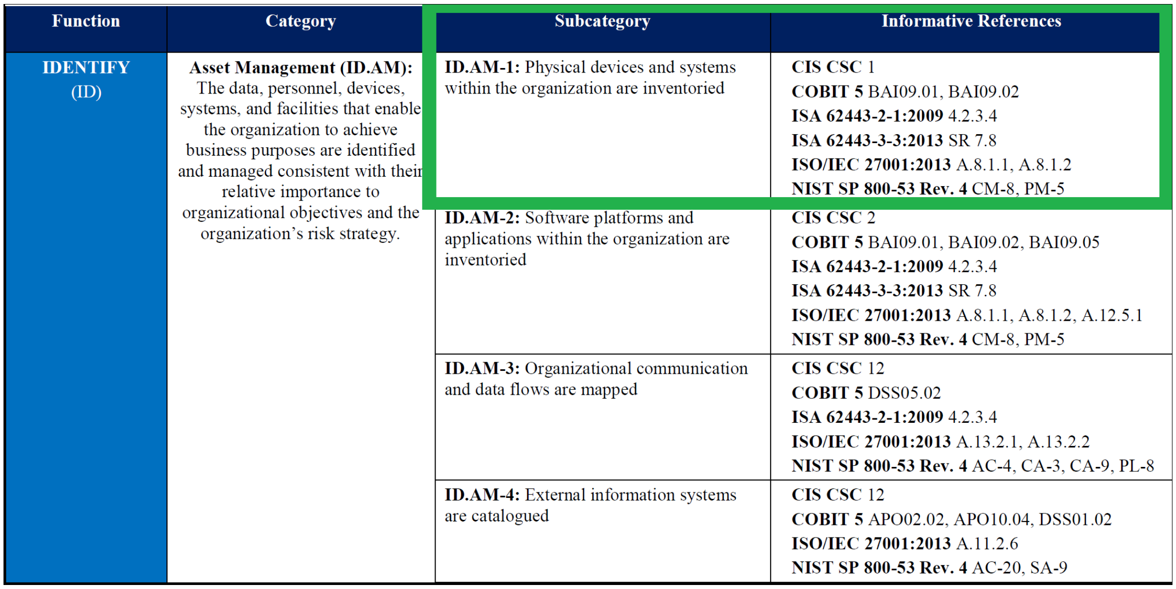
Now, the Target Profiles provided in Section 3 will demonstrate the role they play in identifying and prioritizing the implementation of the security and privacy controls, as well as the capabilities that Great Seneca would like to include in its new BYOD security and privacy-enhanced architecture.

5.1 Using Great Seneca Accounting's Target Profiles

The Cybersecurity Framework maps its Subcategories to Informative References. The Informative References contained in the Framework Core provide examples of methods that Great Seneca can use to achieve its desired outcomes. The Cybersecurity Framework's Subcategory and Informative References mappings include NIST SP 800-53 controls.

An illustrative segment of the Cybersecurity Framework's Framework Core is shown in Figure 5-1. Highlighted in the green box is an example of how the Cybersecurity Framework provides a mapping of Subcategories to Informative References.

Figure 5-1 Cybersecurity Framework Subcategory to Informative Reference Mapping



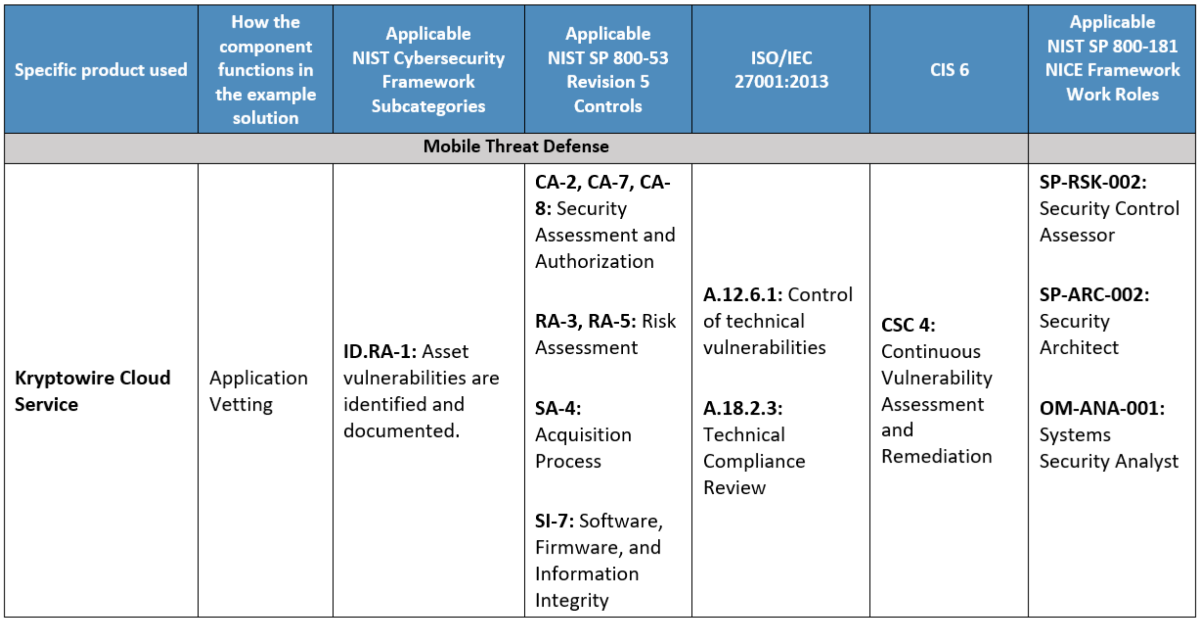
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9

To provide a starting point for Great Seneca's mapping of their Cybersecurity Framework and Privacy Framework Target Profiles to the NIST SP 800-53 security and privacy controls and capabilities, Great Seneca leveraged the mapping provided in the Cybersecurity Framework. An example of the Cybersecurity Framework's mapping is provided in Figure 5-1.

See Volume B's Appendixes G and H for additional information on the security and privacy outcomes that this document's example solution supports. Appendixes G and H provide a mapping of this document's example solution capabilities with the related Subcategories in the Cybersecurity Framework and Privacy Framework.

Volume B's Appendix G provides the Cybersecurity Framework Subcategory mappings, and Volume B's Appendix H provides the Privacy Framework Subcategory mappings. An excerpt of Volume B's Appendix G is shown below in Figure 5-2.

Figure 5-2 Volume B Appendix G Example Solution Cybersecurity Framework Mapping Excerpt



Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles
Mobile Threat Defense						
Kryptowire Cloud Service	Application Vetting	**ID.RA-1:** Asset vulnerabilities are identified and documented.	**CA-2, CA-7, CA-8:** Security Assessment and Authorization **RA-3, RA-5:** Risk Assessment **SA-4:** Acquisition Process **SI-7:** Software, Firmware, and Information Integrity	**A.12.6.1:** Control of technical vulnerabilities **A.18.2.3:** Technical Compliance Review	**CSC 4:** Continuous Vulnerability Assessment and Remediation	**SP-RSK-002:** Security Control Assessor **SP-ARC-002:** Security Architect **OM-ANA-001:** Systems Security Analyst

5.2 Great Seneca Uses the Target Profiles to Help Prioritize Security and Privacy Control Deployment

Due to budget constraints, Great Seneca Accounting will focus on implementing the higher priority security and privacy controls that were identified in the organization's two Target Profiles first. The company will then focus on implementing lower priority controls when more funding becomes available. This is accomplished by Great Seneca Accounting comparing the prioritized Subcategories contained in Section 3's Table 3-1 and Table 3-2 with the outcomes that the example solution supports.

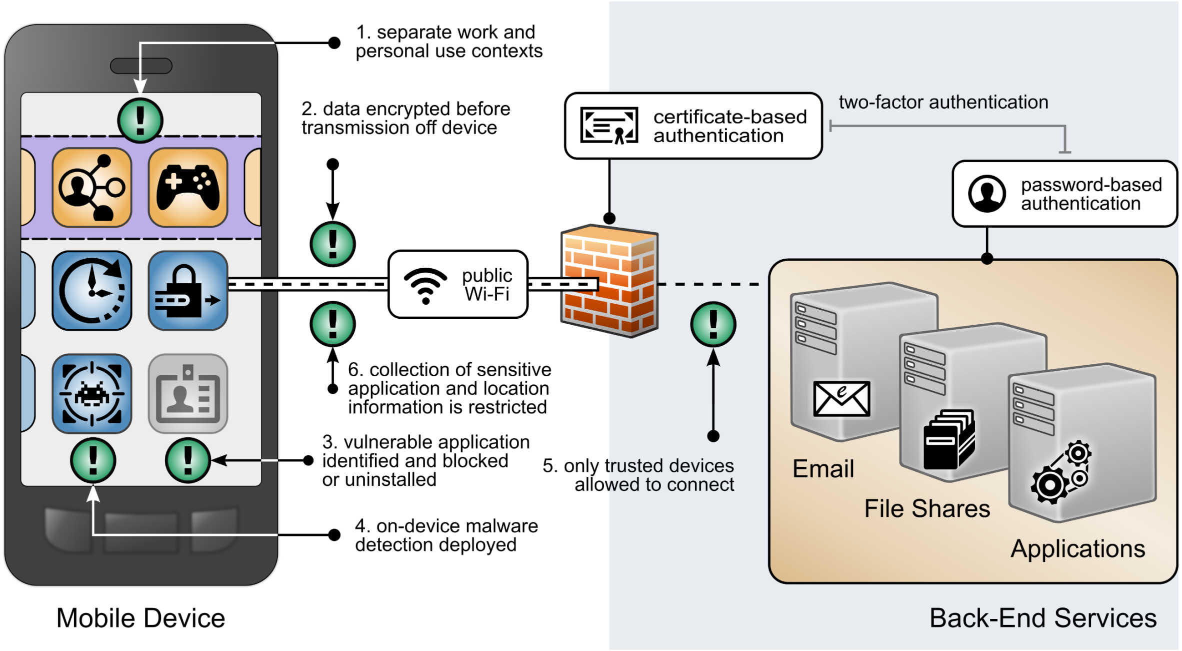
By comparing its Cybersecurity Framework Target Profile (Table 3-1) with the Subcategories supported by the example solution that are shown in Volume B's Appendix G, Great Seneca Accounting determines that the example solution will help it achieve its desired Cybersecurity Framework Target Profile outcomes.

Great Seneca performs a similar comparison of the Privacy Framework Target Profile in Table 3-2 with the Subcategories supported by the example solution that are shown in Volume B's Appendix H. From that comparison of the example solution's capabilities and Great Seneca's privacy-related architecture goals, Great Seneca determines that the example solution provided in this practice guide will help it to achieve the privacy-related outcomes that were identified in Table 3-2's Privacy Framework Target Profile.

5.2.1 Identifying and Tailoring the Baseline Controls

Now that Great Seneca Accounting understands how the Target Profiles will help prioritize the implementation of the high-level security and privacy goals shown in Figure 5-3, it would like to look more closely at the NIST SP 800-53 controls it will initially implement in its new BYOD architecture. This will help Great Seneca identify the capabilities it will deploy first to meet its architecture needs.

Figure 5-3 Security and Privacy Goals


1. separate work and personal use contexts
2. data encrypted before transmission off device
certificate-based authentication
two-factor authentication
password-based authentication
public Wi-Fi
6. collection of sensitive application and location information is restricted
3. vulnerable application identified and blocked or uninstalled
5. only trusted devices allowed to connect
4. on-device malware detection deployed
Email
File Shares
Applications
Mobile Device
Back-End Services

Volume B’s Appendix G and H provide a list of the controls that the example solution implements, including how the controls in the example solution align to the Subcategories in both the Cybersecurity Framework and Privacy Framework. Because these controls only focus on the example solution, Great Seneca will need to implement additional controls that address the unique risks associated with its environment.

To help identify the specific controls Great Seneca Accounting will be implementing to support the new BYOD architecture, it uses the NIST RMF process to manage security and privacy risk for its systems. The organization decides to follow the RMF guidance in NIST SP 800-37 [7] to conduct security and privacy risk assessments as it continues preparing to design its new solution.

5.3 Great Seneca Accounting Performs a Risk Assessment

Great Seneca Accounting completes a security risk assessment by using the guidance in NIST SP 800-30 [8] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to the organization. The company then uses the NIST PRAM [6] to perform a privacy risk assessment. Appendix F and G describe these risk assessments in more detail. These risk assessments produce two significant conclusions:

1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the controls discussed in the example solution are relevant to their environment.
2. The organization determines that it has a high-impact system, based on the impact guidance in NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* [9], and needs to implement more controls beyond those identified in NIST SP 1800-22 and its Target Profiles to support the additional system components in its own solution (e.g., underlying OS, the data center where the equipment will reside).

5.4 Great Seneca Accounting Tailors Their Security and Privacy Control Baselines

As part of their review of NIST FIPS 200 [9], Great Seneca Accounting selects the high controls baseline in NIST SP 800-53 [10] for their BYOD architecture implementation. They then tailor the control baselines based on the needs identified through the priority Subcategories in its cybersecurity and privacy Target Profiles.

Control baselines are tailored to meet their organization's needs. NIST SP 800-53 [10] defines tailoring as "The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation."

While not discussed in this example scenario, Great Seneca also plans to make tailoring decisions based on other unique needs in its environment (e.g., legal and regulatory requirements).

5.4.1 An Example Tailoring of the System and Communications Protection Security Control Family

As Great Seneca Accounting reviews the System and Communications Protection (SC) control family in NIST SP 800-53 [10], it notes there are opportunities for tailoring.

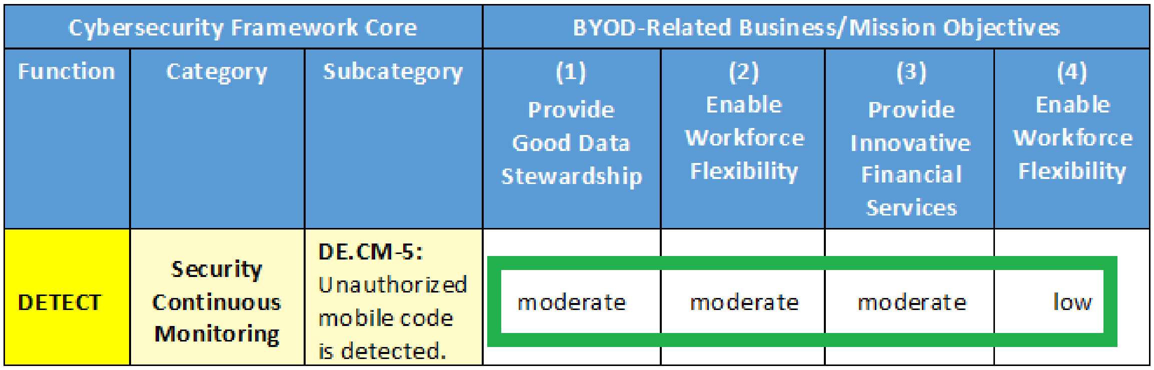
For example, the NIST SP 800-53 baseline includes control enhancements, whereas the Cybersecurity Framework Informative References contain only base controls. Great Seneca Accounting decides to implement the enhancements that are applicable to a high-impact system for the SC controls they have selected.

Using this decision as a guide, Great Seneca Accounting also makes the following tailoring decisions related to the NIST SP 800-53 SC control family:

- NIST SP 800-53 provides recommendations regarding implementation priorities for controls. The implementation priorities of controls related to some Cybersecurity Framework Subcategories were adjusted to be higher or lower based on their alignment with Subcategory prioritization in the Target Profile.

- For example, the implementation priority for Cybersecurity Framework Subcategory DE.CM-5 was identified as having low or moderate importance for accomplishing all four BYOD-Related Business/Mission Objectives. NIST SP 800-53 designates control SC-18, which supports the implementation of Cybersecurity Framework Subcategory DE.CM-5, as high priority. However, since Cybersecurity Framework Subcategory DE.CM-5 is moderate or low priority in this context, Great Seneca makes a tailoring decision to lower the implementation priority for the SC-18 NIST SP 800-53 control to moderate.
    - DE.CM-5's importance designations for accomplishing the BYOD-Related Business/Mission Objectives are highlighted in green in Figure 5-4.

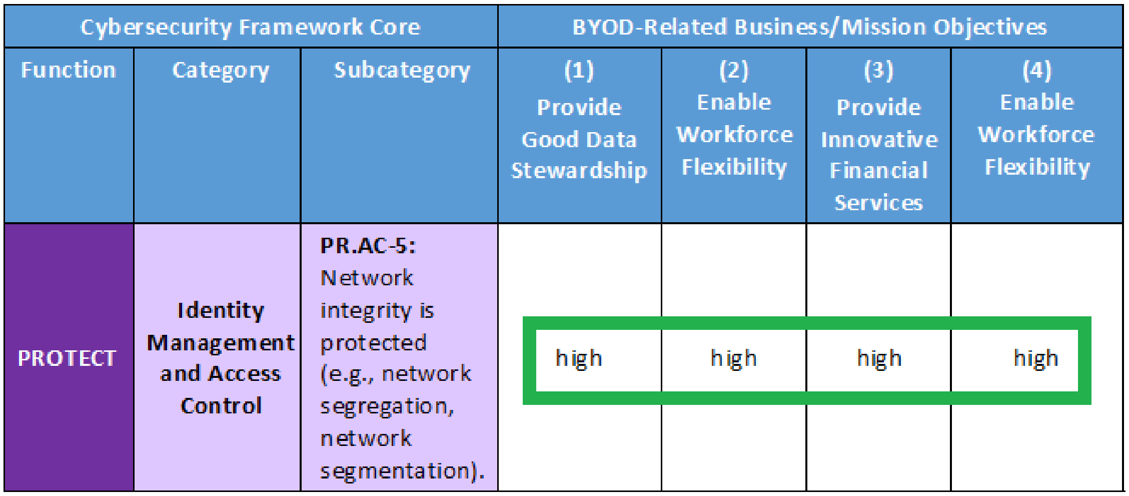
Figure 5-4 Subcategory DE.CM-5 Mapping to BYOD-Related Business/Mission Objectives



Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable Workforce Flexibility	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
DETECT	Security Continuous Monitoring	DE.CM-5: Unauthorized mobile code is detected.	moderate	moderate	moderate	low

- Conversely, just as the implementation priority for the NIST SP 800-53 control that supports implementation of Subcategory DC-CM-5 was lowered based on the Target Profile, the implementation priority for the NIST SP 800-53 controls that supports implementation of Cybersecurity Framework Subcategory PR.AC-5 was raised. This is because Subcategory PR.AC-5 was identified as having high importance for accomplishing all four BYOD-Related Business/Mission Objectives.
    - The NIST SP 800-53 SC Family security control related to the Cybersecurity Framework Subcategory PR.AC-5 is SC-7. NIST SP 800-53 prioritizes control SC-7 as low. Since control SC-7 supports the implementation of a Cybersecurity Framework Subcategory that is designated as high priority in Great Seneca's Target Profile (Cybersecurity Framework Subcategory PR.AC-5), Great Seneca makes a tailoring decision to increase the priority of NIST SP 800-53 control SC-7 to high.
    - PR.AC-5's high importance designation for accomplishing the BYOD-Related Business/Mission Objectives are highlighted in green in Figure 5-5. All Subcategory prioritizations (including PR.AC-5's shown below) can be found in Table 3-1.

Figure 5-5 Subcategory PR.AC-5 Mapping to BYOD-Related Business/Mission Objectives



Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable Workforce Flexibility	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
PROTECT	Identity Management and Access Control	**PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high

Great Seneca Accounting follows the same approach for the privacy controls in NIST SP 800-53, using the Privacy Framework Target Profile and controls identified through its PRAM analysis (for more information reference Appendix G).

Great Seneca Accounting will evaluate the security controls as they come up for review under its continuous monitoring program to determine whether there are enhancements to the implemented security controls that can be made over time.

In addition to identifying controls to select, the priorities articulated in Target Profiles will also help Great Seneca Accounting decide how to align financial resources for controls implementation (e.g., buying a tool to automate a control as opposed to relying on policy and procedures alone). The Target Profiles will help Great Seneca identify how robustly to re-assess the efficacy of implemented controls before new system components or capabilities are enabled in a production environment. Great Seneca will also be able to use the Target Profiles to help evaluate the residual risks of the architecture in the context of Great Seneca Accounting's business/mission objectives, and the frequency and depth of continued monitoring requirements over time.

Note: All of the tailoring decisions discussed above are for example purposes only. An organization's actual tailoring decision will be based upon their own unique business/mission objectives, risk assessment results, and organizational needs that may significantly vary from these examples.

341 Appendix A List of Acronyms

BYOD	Bring Your Own Device
FIPS	Federal Information Processing Standards
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
SP	Special Publication

Appendix B Glossary

Access Management Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [11].

Availability Ensure that users can access resources through remote access whenever needed [12].

Bring Your Own Device (BYOD) A non-organization-controlled telework client device [12].

Confidentiality Ensure that remote access communications and stored user data cannot be read by unauthorized parties [12].

Data Actions System operations that process PII [13].

Disassociability Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [13].

Eavesdropping An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant [14] (definition located under eavesdropping attack).

Firewall Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [15].

Integrity Detect any intentional or unintentional changes to remote access communications that occur in transit [12].

Manageability Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [13].

Mobile Device A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [10].

Personally Identifiable Information (PII) Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual‘s identity, such as name, Social Security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [16] (adapted from Government Accountability Office Report 08-536).

Problematic Data Action A data action that could cause an adverse effect for individuals [2].

Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [8].

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [8].

Appendix C References

[1] National Institute of Standards and Technology (NIST). NIST *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Cybersecurity Framework). Apr. 16, 2018. [Online]. Available: https://www.nist.gov/cyberframework.

[2] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework). Jan. 16, 2020. [Online]. Available: https://www.nist.gov/privacy-framework.

[3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST Special Publication (SP) 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final.

[4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.

[5] NIST. Mobile Threat Catalogue. [Online]. Available: https://pages.nist.gov/mobile-threat-catalogue/.

[6] NIST. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available: https://www.nist.gov/privacy-framework/nist-pram.

[7] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[8] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments,* NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[9] NIST. *Minimum Security Requirements for Federal Information and Information Systems,* Federal Information Processing Standards Publication (FIPS) 200, Mar. 2006. Available: https://csrc.nist.gov/publications/detail/fips/200/final.

[10] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems and Organizations,* NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[11] IDManagement.gov. "Federal Identity, Credential, and Access Management Architecture." [Online]. Available: https://arch.idmanagement.gov/services/access/.

[12] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,* NIST SP 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

[13] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems,* NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[14] P. Grassi et al., *Digital Identity Guidelines,* NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[15] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security,* NIST SP 800-82 Revision 2, NIST, Gaithersburg, Md., May 2015. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[16] E. McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[17] J. Franklin et al., *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*, NIST SP 1800-21, NIST, Gaithersburg, Md., July 22, 2019. Available: https://csrc.nist.gov/News/2019/NIST-Releases-Draft-SP-1800-21-for-Comment.

[18] NIST, NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*, Mar. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf.

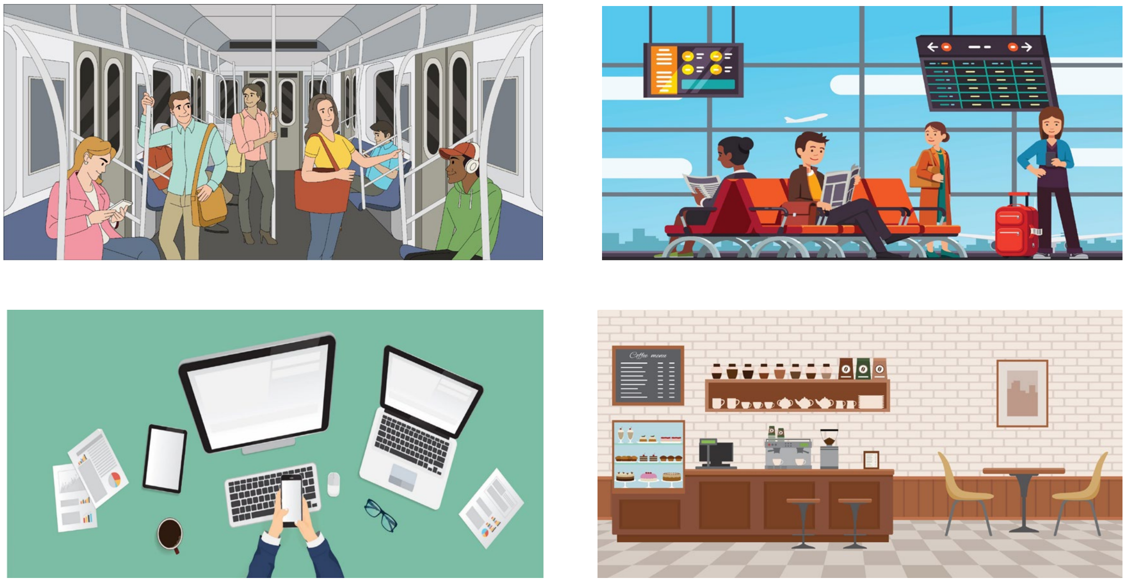
[19] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.

Appendix D A Note Regarding Great Seneca Accounting

A description of a fictional organization, Great Seneca Accounting, was included in the National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-22 Mobile Device Security: Bring Your Own Device (BYOD) Practice Guide.

This fictional organization demonstrates how a small-to-medium sized, regional organization implemented the example solution in this practice guide to assess and protect their mobile-device-specific security and privacy needs. It illustrates how organizations with office-based, remote-working, and travelling personnel can be supported in their use of personally owned devices that enable their employees to work while on the road, in the office, at customer locations, and at home.

Figure D-1 Great Seneca Accounting's Work Environments



Appendix E How Great Seneca Accounting Applied NIST Risk Management Methodologies

This practice guide contains an example scenario about a fictional organization called Great Seneca Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be in alignment with an organization's security and privacy capabilities and objectives.

The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

This appendix provides a brief description of some of the key NIST tools referenced in the example scenario supplement of this practice guide.

In this Appendix, Section E.1 provides descriptions of the risk frameworks and tools, along with a high-level discussion of how Great Seneca Accounting applied each framework or tool in the example scenario. Section E.2 describes how the *NIST Cybersecurity Framework* and *NIST Privacy Framework* can be used to establish or improve cybersecurity and privacy programs.

E.1 Overview of Risk Frameworks and Tools That Great Seneca Used

Great Seneca used NIST frameworks and tools to identify common security and privacy risks related to BYOD solutions and to guide approaches to how they were addressed in the architecture described in Section 4. Great Seneca used additional standards and guidance, listed in Appendix D of Volume B, to complement these frameworks and tools when designing their BYOD architecture.

Both the Cybersecurity Framework and Privacy Framework include the concept of Framework Profiles, which identify the organization's existing activities (contained in a Current Profile) and articulate the desired outcomes that support its mission and business objectives within its risk tolerance (that are contained in the Target Profile). When considered together, Current and Target Profiles are useful tools for identifying gaps and for strategic planning.

E.1.1 Overview of the NIST Cybersecurity Framework

Description: The NIST Cybersecurity Framework "is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders." [17]

Application: This guide refers to two of the main components of the Cybersecurity Framework: the Framework Core and the Framework Profiles. As described in Section 2.1 of the Cybersecurity Framework, the Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and reference examples of guidance to achieve those outcomes (e.g., controls found in NIST Special Publication [SP] 800-53). Section 2.3 of the Cybersecurity Framework identifies Framework Profiles as the alignment of the Functions, Categories, and Subcategories (i.e., the Framework Core) with the business requirements, risk tolerance, and resources of the organization.

The Great Seneca Accounting example scenario assumed that the organization used the Cybersecurity Framework Core and Framework Profiles, specifically the Target Profiles, to align cybersecurity outcomes and activities with its overall business/mission objectives for the organization. In the case of Great Seneca Accounting, its Cybersecurity Framework Target Profile helps program owners and system architects understand business and mission-driven priorities and the types of cybersecurity capabilities needed to achieve them. Great Seneca Accounting also used the NIST Interagency Report (NISTIR) 8170, *The Cybersecurity Framework, Implementation Guidance for Federal Agencies* [18], for guidance in using the NIST Cybersecurity Framework.

E.1.2 Overview of the NIST Privacy Framework

Description: The *NIST Privacy Framework* is a voluntary enterprise risk management tool intended to help organizations identify and manage privacy risk and build beneficial products and services while protecting individuals’ privacy. It follows the structure of the Cybersecurity Framework to facilitate using both frameworks together [2].

Application: This guide refers to two of the main components of the Privacy Framework: the Framework Core and Framework Profiles. As described in Section 2.1 of the Privacy Framework, the Framework Core provides an increasingly granular set of activities and outcomes that enable dialog about managing privacy risk as well as resources to achieve those outcomes (e.g., guidance in NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [13]). Section 2.2 of the Privacy Framework identifies Framework Profiles as the selection of specific Functions, Categories, and Subcategories from the core that an organization has prioritized to help it manage privacy risk.

Great Seneca Accounting used the Privacy Framework as a strategic planning tool for its privacy program as well as its system, product, and service teams. The Great Seneca Accounting example scenario assumed that the organization used the Privacy Framework Core and Framework Profiles, specifically Target Profiles, to align privacy outcomes and activities with its overall business/mission objectives for the organization. Its Privacy Framework Target Profile helped program owners and system architects to understand business and mission-driven priorities and the types of privacy capabilities needed to achieve them.

E.1.3 Overview of the NIST Risk Management Framework

Description: The NIST Risk Management Framework (RMF) “provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations" [19]. Two of the key documents that describe the RMF are NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy;* and NIST SP 800-30, *Guide for Conducting Risk Assessments*.

Application: The RMF has seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. These steps provide a method for organizations to characterize the risk posture of their information and systems and identify controls that are commensurate with the risks in the system's environment. They also support organizations with selecting beneficial implementation and assessment approaches, reasoning through the process to understand residual risks, and monitoring the efficacy of implemented controls over time.

The Great Seneca Accounting example solution touches on the risk assessment activities conducted under the *Prepare* step, identifying the overall risk level of the BYOD system architecture in the *Categorize* step, and, consistent with example approach 8 in NISTIR 8170, reasoning through the controls that are necessary in the *Select* step. The influence of the priorities provided in Great Seneca Accounting's Cybersecurity Framework Target Profile is also briefly mentioned regarding making decisions for how to apply controls during *Implement* (e.g., policy versus tools), how robustly to verify and validate controls during *Assess* (e.g., document review versus "hands on the keyboard" system testing), and the degree of evaluation required over time as part of the *Monitor* step.

E.1.4 Overview of the NIST Privacy Risk Assessment Methodology

Description: The NIST Privacy Risk Assessment Methodology (PRAM) is a tool for analyzing, assessing, and prioritizing privacy risks to help organizations determine how to respond and select appropriate solutions. A blank version of the PRAM is available for download on NIST's website.

Application: The PRAM uses the privacy risk model and privacy engineering objectives described in NISTIR 8062 to analyze for potential problematic data actions. Data actions are any system operations that process data. Processing can include, collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of data. A problematic data action is one that could cause an adverse effect, or problem, for individuals. The occurrence or potential occurrence of problematic data actions is a privacy event. While there is a growing body of technical privacy controls, including those found in NIST SP 800-53, applying the PRAM may result in identifying controls that are not yet available in common standards. This makes it an especially useful tool for managing risks that may otherwise go unaddressed.

The Great Seneca Accounting example solution assumed that a PRAM was used to identify problematic data actions and mitigating controls for employees. The controls in this build include some technical controls, such as controls that can be handled by security capabilities, as well as policy and procedure-level controls that need to be implemented outside yet supported by the system.

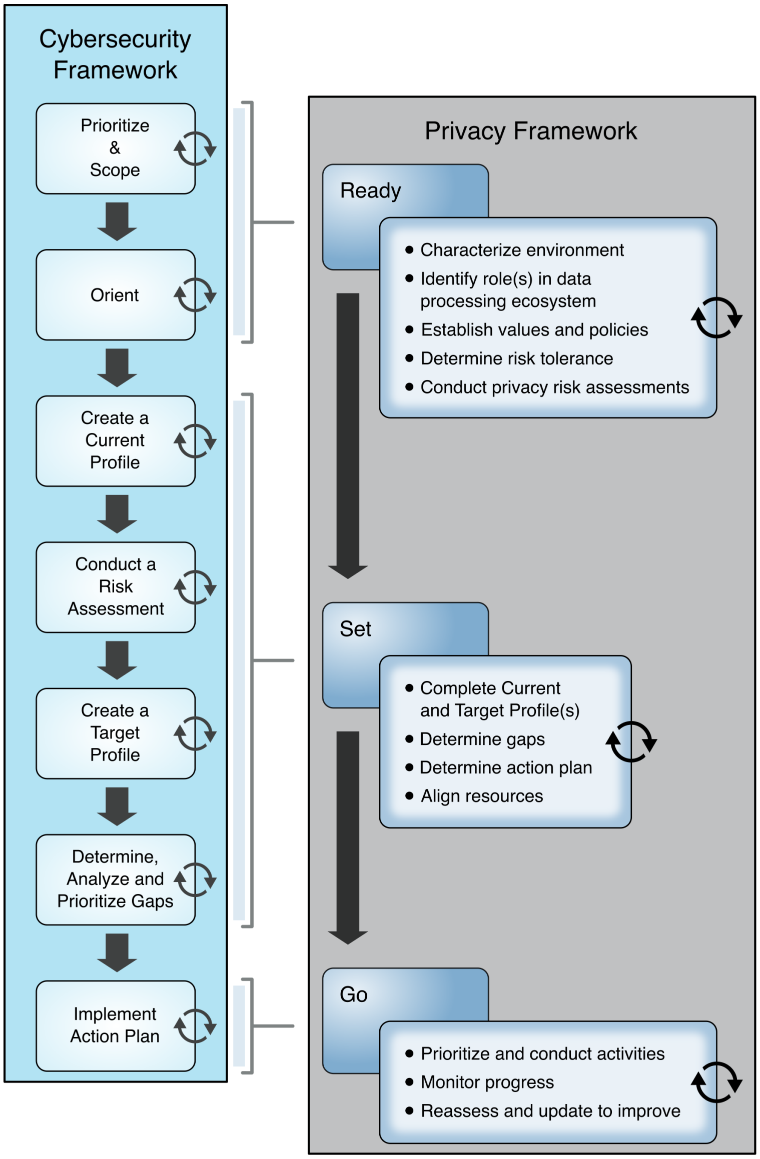
E.2 Using Frameworks to Establish or Improve Cybersecurity and Privacy Programs

While their presentation differs, the NIST Cybersecurity Framework and *NIST Privacy Framework* also both provide complementary guidance for establishing and improving cybersecurity and privacy programs. The NIST Cybersecurity Framework's process for establishing or improving programs provides seven steps that an organization could use iteratively and as necessary throughout the program's life cycle to continually improve its cybersecurity posture:

- Step 1: Prioritize and scope the organization's mission.
- Step 2: Orient its cybersecurity program activities to focus efforts on applicable areas.
- Step 3: Create a current profile of what security areas it currently supports.
- Step 4: Conduct a risk assessment.
- Step 5: Create a Target Profile of the security areas that the organization would like to improve in the future.
- Step 6: Determine, analyze, and prioritize cybersecurity gaps.
- Step 7: Implement an action plan to close those gaps.

The *NIST Privacy Framework* includes the same types of activities for establishing and improving privacy programs, described in a three-stage Ready, Set, Go model. Figure E-1 below shows a comparison of these two approaches, demonstrating their close alignment.

Figure E-1 Comparing Framework Processes to Establish or Improve Programs


Cybersecurity Framework
Prioritize & Scope
Orient
Create a Current Profile
Conduct a Risk Assessment
Create a Target Profile
Determine, Analyze and Prioritize Gaps
Implement Action Plan
Privacy Framework
Ready
Characterize environment
Identify role(s) in data processing ecosystem
Establish values and policies
Determine risk tolerance
Conduct privacy risk assessments
Set
Complete Current and Target Profile(s)
Determine gaps
Determine action plan
Align resources
Go
Prioritize and conduct activities
Monitor progress
Reassess and update to improve

Both approaches are equally effective. Regardless of the approach selected, an organization begins with orienting around its business/mission objectives and high-level organizational priorities and carry out the remaining activities in a way that makes the most sense for the organization. The organization repeats these steps as necessary throughout the program's life cycle to continually improve its risk posture.

Appendix F How Great Seneca Accounting Used the NIST Risk Management Framework

This practice guide contains an example scenario about a fictional organization called Great Seneca Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be in alignment with an organization's security and privacy capabilities and objectives.

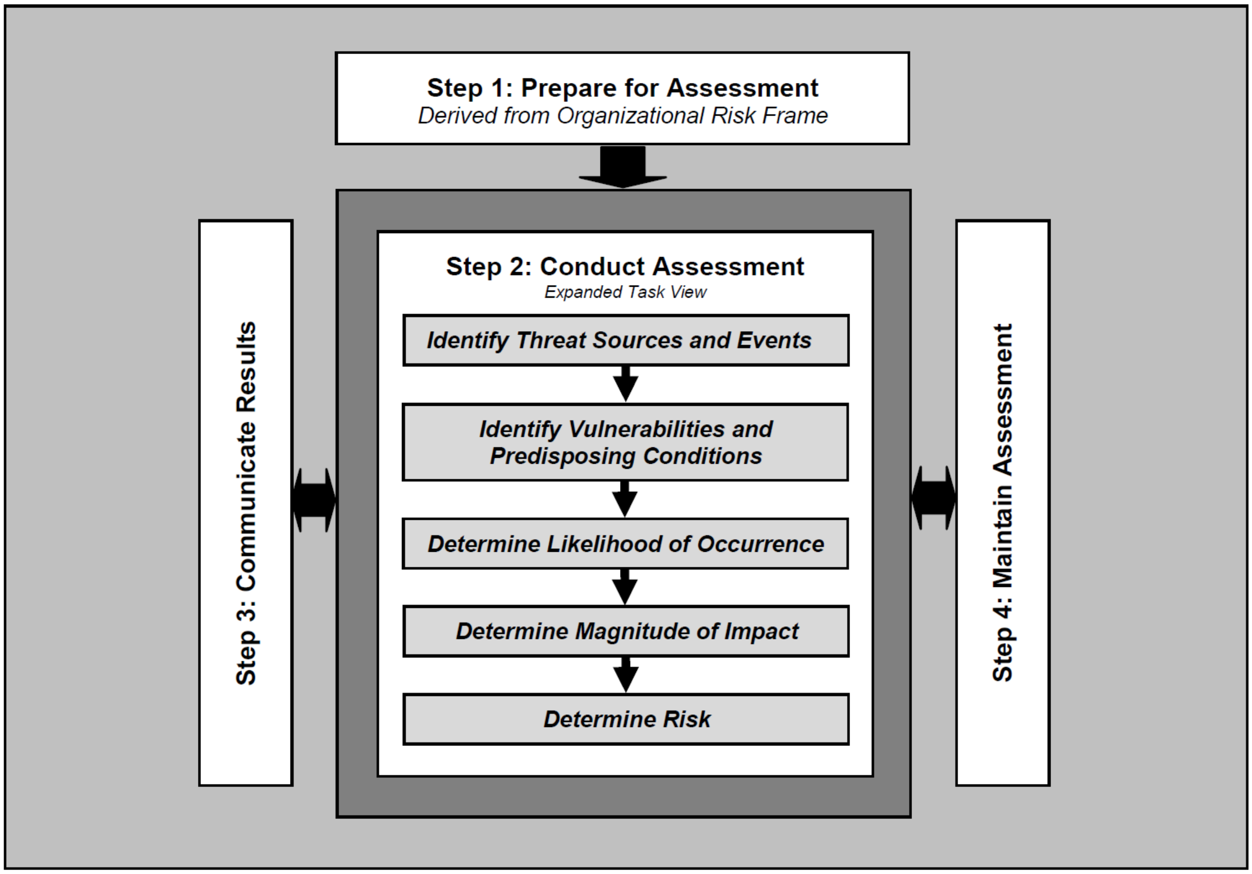
The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

In the example scenario supplement of this practice guide, Great Seneca Accounting decided to use the NIST Cybersecurity Framework, the *NIST Privacy Framework,* and the NIST Risk Management Framework to help improve its mobile device architecture. The following material provides information about how Great Seneca Accounting used the NIST Risk Management Framework to improve its BYOD deployment.

F.1 Understanding the Risk Assessment Process

This section provides information on the risk assessment process employed to improve the mobile security posture of Great Seneca Accounting. Typically, a risk assessment based on NIST SP 800-30 Revision 1 follows a four-step process as shown in Figure F-1: prepare for assessment, conduct assessment, communicate results, and maintain assessment.

Figure F-1 Risk Assessment Process


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

F.2 Risk Assessment of Great Seneca Accounting's BYOD Program

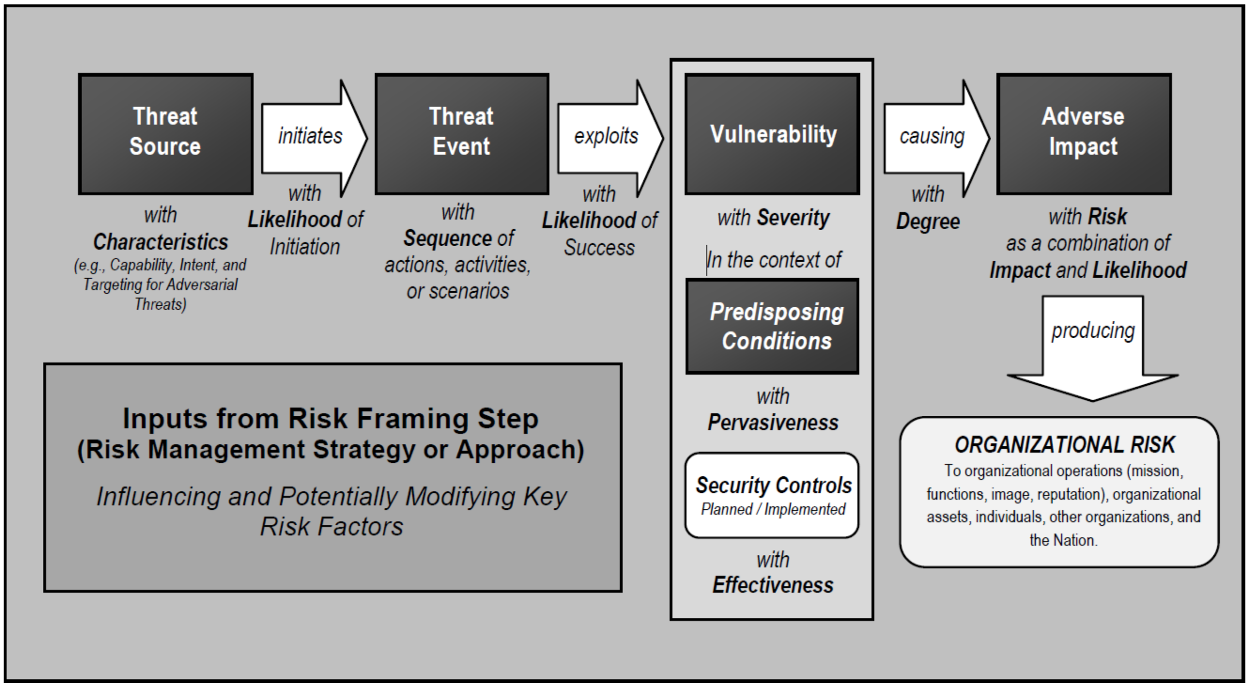
This risk assessment is scoped to Great Seneca Accounting's mobile deployment, which includes the mobile devices used to access Great Seneca Accounting's enterprise resources, along with any information technology components used to manage or provide services to those mobile devices.

Risk assessment assumptions and constraints were developed by using a NIST SP 800-30 Revision 1 generic risk model as shown in Figure F-2 to identify the following components of the risk assessment:

- threat sources
- threat events
- vulnerabilities
- predisposing conditions
- security controls

- adverse impacts
- organizational risks

Figure F-2 NIST SP 800-30 Generic Risk Model


Threat Source
initiates
with Likelihood of Initiation
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
Threat Event
exploits
with Likelihood of Success
with Sequence of actions, activities, or scenarios
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step
(Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

F.3 Development of Threat Event Descriptions

Great Seneca Accounting developed threat event tables based on NIST SP 800-30 Revision 1 and used those to help analyze the sources of mobile threats. Using this process, Great Seneca Accounting leadership identified the following potential mobile device threat events that are described in the following subsections.

A note about selection of the threat events:

This practice guide’s example solution helps protect organizations from the threat events shown in Table F-1. A mapping of these threat events to the NIST Mobile Threat Catalogue is provided in Table F-2.

Table F-1 Great Seneca Accounting's BYOD Deployment Threats

Great Seneca Accounting's Threat Event Identification Number	**Threat Event Description**
TE-1	privacy-intrusive applications
TE-2	account credential theft through phishing
TE-3	malicious applications
TE-4	outdated phones
TE-5	camera and microphone remote access
TE-6	sensitive data transmissions
TE-7	brute-force attacks to unlock a phone
TE-8	protection against weak password practices
TE-9	protection against unmanaged devices
TE-10	protection against lost or stolen data
TE-11	protecting data from being inadvertently backed up to a cloud service
TE-12	protection against sharing personal identification number (PIN) or password

Great Seneca Accounting's 12 threat events and their mapping to the NIST Mobile Threat Catalogue [5] are shown in Table F-2.

Table F-2 Threat Event Mapping to the Mobile Threat Catalogue

Great Seneca Accounting's Threat Event Identification Number	**NIST Mobile Threat Catalogue Threat ID**
TE-1	APP-2, APP-12
TE-2	AUT-9
TE-3	APP-2, APP-5, APP-31, APP-40, APP-32, AUT-10
TE-4	APP-4, APP-26, STA-0, STA-9, STA-16
TE-5	APP-32, APP-36

Great Seneca Accounting's Threat Event Identification Number	NIST Mobile Threat Catalogue Threat ID
TE-6	APP-0, CEL-18, LPN-2
TE-7	AUT-2, AUT-4
TE-8	APP-9, AUT-0
TE-9	EMM-5
TE-10	PHY-0
TE-11	EMM-9
TE-12	AUT-0, AUT-2, AUT-4, AUT-5

F.4 Great Seneca Accounting's Leadership and Technical Teams Discuss BYOD's Potential Threats to Their Organization

Great Seneca Accounting's leadership team wanted to understand real-world examples of each threat event and what the risk was for each. Great Seneca Accounting's leadership and technical teams then discussed those possible threats that BYOD could introduce to their organization.

The analysis performed by Great Seneca Accounting's technical team included analyzing the likelihood of each threat, the level of impact, and the threat level that the BYOD deployment would pose. The following are leadership's questions and the technical team's responses regarding BYOD threats during that discussion using real-world examples. A goal of the example solution contained within this practice guide is to mitigate the impact of these threat events. Reference Table 5-1 for a listing of the technology that addresses each of the following threat events.

F.4.1 Threat Event 1

What happens if an employee installs risky applications?

A mobile application can attempt to collect and exfiltrate any information to which it has been granted access. This includes any information generated during use of the application (e.g., user input), user-granted permissions (e.g., contacts, calendar, call logs, photos), and general device data available to any application (e.g., International Mobile Equipment Identity, device make and model, serial number). Further, if a malicious application exploits a vulnerability in other applications, the operating system (OS), or device firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or otherwise accessible through the device.

Risk assessment analysis:

Overall likelihood: very high

Justification: Employees have access to download any application at any time. If an employee requires an application that provides a desired function, the employee can download that application from any available source (trusted or untrusted) that provides a desired function. If an application performs an employee's desired function, the employee may download an application from an untrusted source and/or disregard granted privacy permissions.

Level of impact: high

Justification: Employees may download an application from an untrusted source and/or disregard granted privacy permissions. This poses a threat for sensitive corporate data, as some applications may include features that could access corporate data, unbeknownst to the user.

BYOD-specific threat: In a BYOD scenario, users are still able to download and install applications at their leisure. This capability allows users to unintentionally side-load or install a malicious application that may harm the device or the enterprise information on the device.

F.4.2 Threat Event 2

Can account information be stolen through phishing?

Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate ones and entice users to authenticate to them by distributing phishing messages over short message service (SMS) or email. Effective social engineering techniques such as impersonating an authority figure or creating a sense of urgency may compel users to forgo scrutinizing the message and proceed to authenticate to the fraudulent website; it then captures and stores the user's credentials before (usually) forwarding them to the legitimate website to allay suspicion.

Risk assessment analysis:

Overall likelihood: very high

Justification: Phishing campaigns are a very common threat that occurs almost every day.

Level of impact: high

Justification: A successful phishing campaign could provide the malicious actor with corporate credentials, allowing access to sensitive corporate data; or personal credentials that could lead to compromise of corporate data or infrastructure via other means.

BYOD-specific threat: The device-level controls applied to personal devices do not inhibit a user's activities. This allows the user to access personal/work messages and emails on their device that could be susceptible to phishing attempts. If the proper controls are not applied to a user's enterprise messages and email, successful phishing attempts could allow an attacker unauthorized access to enterprise data.

F.4.3 Threat Event 3

How much risk do malicious applications pose to Great Seneca Accounting?

Malicious actors may send users SMS or email messages that contain a uniform resource locator (URL) where a malicious application is hosted. Generally, such messages are crafted using social engineering techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby increasing the likelihood that they access the URL using their mobile device. If they do, it will attempt to download and install the application. Effective use of social engineering by the attacker will further compel an otherwise suspicious user to grant any trust required by the developer and all permissions requested by the application. Granting the former facilitates installation of other malicious applications by the same developer, and granting the latter increases the potential for the application to do direct harm.

Risk assessment analysis:

Overall likelihood: high

Justification: Installation of malicious applications via URLs is less common than other phishing attempts. The process for side-loading applications requires much more user input and consideration (e.g., trusting the developer certificate) than standard phishing, which solely requests a username and password. A user may proceed through sideloading an application to acquire a desired capability from an application.

Level of impact: high

Justification: Once a user installs a malicious side-loaded application, an adversary could gain full access to a mobile device, and therefore access to corporate data and credentials, without the user's knowledge.

BYOD-specific threat: Like Threat Event 1, BYOD deployments may have fewer restrictions to avoid preventing the user from performing desired personal functions. This increases the attack surface for malicious actors to take advantage.

F.4.4 Threat Event 4

What happens when outdated phones access Great Seneca Accounting's network?

When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and issues commands in the context of the root user or the OS kernel. This may be enough for some malicious actors to accomplish their goal, but those that are advanced will usually attempt to install additional malicious tools and to establish a persistent presence. If successful, the attacker will be able to launch further attacks against the user, the device, or any other systems to which the device connects. As a result, any data stored on, generated by, or accessible to the device at that time – or in the future – may be compromised.

Risk assessment analysis:

Overall likelihood: high

Justification: Many public vulnerabilities specific to mobile devices have been seen over the years. In these, users can jailbreak iOS devices and root Android devices to download third-party applications and apply unique settings/configurations that the device would not typically be able to apply/access.

Level of impact: high

Justification: Exploiting a vulnerability allows circumventing security controls and modifying protected device data that should not be modified. Jailbroken and rooted devices exploit kernel vulnerabilities and allow third-party applications/services root access that can also be used to bypass security controls that are built in or applied to a mobile device.

BYOD-specific threat: As with any device, personal devices are susceptible to device exploitation if not properly used or updated.

F.4.5 Threat Event 5

Can Great Seneca Accounting stop someone from turning on a camera or microphone?

Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera, gyroscope, Global Positioning System receiver, and radios) can use them to conduct surveillance. It may be directed at the user, as when tracking the device location, or it may be applied more generally, as when recording any nearby sounds. Captured sensor data may be immediately useful to a malicious actor, such as a recording of an executive meeting. Alternatively, the attacker may analyze the data in isolation or in combination with other data to yield sensitive information. For example, a malicious actor can use audio recordings of on-device or proximate activity to probabilistically determine user inputs to touchscreens and keyboards, essentially turning the device into a remote keylogger.

Risk assessment analysis:

Overall likelihood: very high

Justification: This has been seen on public application stores, with applications allegedly being used for data-collection. As mentioned in Threat Event 1, unbeknownst to the user, a downloaded application may be granted privacy intrusive permissions that allow access to device sensors.

Level of impact: high

Justification: When the sensors are being misused, the user is typically not alerted. This allows collection of sensitive enterprise data, such as location, without knowledge of the user.

BYOD-specific threat: Applications commonly request access to these sensors. In a BYOD deployment, the enterprise does not have control over what personal applications the user installs on their device. These personal applications may access sensors on the device and eavesdrop on a user's enterprise-related activities (e.g., calls and meetings).

F.4.6 Threat Event 6

Is sensitive information protected when the data travels between the employee's mobile device and Great Seneca Accounting's network?

Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as public Wi-Fi access points, which coffee shops and hotels commonly provide. While a device is connected to such a network, a malicious actor could gain unauthorized access to any data sent or received by the device for any session that has not already been protected by encryption at either the transport or application layers. Even if the transmitted data were encrypted, an attacker would be privy to the domains, internet protocol (IP) addresses, and services (as indicated by port numbers) to which the device connects; an attacker could use such information in future watering hole or person-in-the-middle attacks against the device user.

Additionally, visibility into network-layer traffic enables a malicious actor to conduct side-channel attacks against the network's encrypted messages, which can still result in a loss of confidentiality. Further, eavesdropping on unencrypted messages during a handshake to establish an encrypted session with another host or endpoint may facilitate attacks that ultimately compromise the security of the session.

Risk assessment analysis:

Overall likelihood: moderate

Justification: Unlike installation of an application, installations of enterprise mobility management (EMM)/mobile device management (MDM), network, virtual private network (VPN) profiles, and certificates require additional effort and understanding from the user to properly implement.

Level of impact: very high

Justification: If malicious actor can install malicious configuration profiles or certificates, they would be able to perform actions such as decrypting network traffic and possibly even control the device.

BYOD-specific threat: Like Threat Event 2, personal devices may not have the benefit of an always-on device-wide VPN. This leaves application communications at the discretion of the developer.

F.4.7 Threat Event 7

Is Great Seneca Accounting's data protected from brute-force PIN attacks?

A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the device; only the third technique requires physical access. However, applications with access to any peripherals that detect sound or motion (microphone, gyroscope, or accelerometer) can attempt side-channel attacks that infer the unlock code by detecting taps and swipes to the screen. Once the device unlock code has been obtained, a malicious actor with physical access to the device will gain immediate access to any data or functionality not already protected by additional access control mechanisms. Additionally, if the user employs the device unlock code as a credential to any other systems, the malicious actor may further gain unauthorized access to those systems.

Risk assessment analysis:

Overall likelihood: moderate

Justification: Unlike shoulder-surfing to observe a user's passcode, brute-force attacks are not as common or successful due to the built-in deterrent mechanisms. These mechanisms include exponential back-off/lockout period and device wipes after a certain number of failed unlock attempts.

Level of impact: very high

Justification: If a malicious actor can successfully unlock a device without the user's permission, they could have full control over the user's corporate account and thus gain unauthorized access to corporate data.

BYOD-specific threat: Because BYODs are prone to travel (e.g., vacations, restaurants, and other nonwork locations), the risk that the device's passcode is obtained increases due to the heightened exposure to threats in different environments.

F.4.8 Threat Event 8

Can Great Seneca Accounting protect its data from weak password practices?

If a malicious actor gains unauthorized access to a mobile device, they also have access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications that a malicious actor can subsequently use to gain access to sensitive data or backend services. This could result from weaknesses or vulnerabilities present in the authentication or credential storage mechanisms implemented within an in-house application.

Risk assessment analysis:

Overall likelihood: moderate

Justification: Often applications include hardcoded credentials for the default password of the admin account. Default passwords are readily available online. The user might not change these passwords to allow access and eliminate the need to remember a password.

Level of impact: high

Justification: Successful extraction of the credentials allows an attacker to gain unauthorized access to enterprise data.

BYOD-specific threat: The risk of hardcoded credentials residing in an application on the device is the same for any mobile device deployment scenario.

F.4.9 Threat Event 9

Can unmanaged devices connect to Great Seneca Accounting?

An employee who accesses enterprise resources from an unmanaged mobile device may expose the enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit from any security mechanisms deployed by the organization such as mobile threat defense, mobile threat intelligence, application vetting services, and mobile security policies. These unmanaged devices limit an organization’s visibility into the state of a mobile device, including if a malicious actor compromises the device. Therefore, users who violate security policies to gain unauthorized access to enterprise resources from such devices risk providing malicious actors with access to sensitive organizational data, services, and systems.

Risk assessment analysis:

Overall likelihood: very high

Justification: This may occur accidentally when an employee attempts to access their email or other corporate resources.

Level of impact: high

Justification: Unmanaged devices pose a sizable security risk because the enterprise has no visibility into their security or risk postures of the mobile devices. Due to this lack of visibility, a compromised device may allow an attacker to attempt to exfiltrate sensitive enterprise data.

BYOD-specific threat: The risk of an unmanaged mobile device accessing the enterprise is the same for any mobile deployment scenario.

F.4.10 Threat Event 10

Can Great Seneca Accounting protect its data when a phone is lost or stolen?

Due to the nature of the small form factor of mobile devices, they can be misplaced or stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

Risk assessment analysis:

Overall likelihood: very high

Justification: Mobile devices are small and can be misplaced. Enterprise devices may be lost or stolen at the same frequency as personally owned devices.

Level of impact: high

Justification: Similar to Threat Event 9, if a malicious actor can gain access to the device, they could access sensitive corporate data.

BYOD-specific threat: Due to the heightened mobility of BYODs, they are more prone to being accidentally lost or stolen.

F.4.11 Threat Event 11

Can data be protected from unauthorized cloud services?

If employees violate data management policies by using unmanaged services to store sensitive organizational data, the data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Further, storage of sensitive data in an unmanaged service may subject the user or the organization to prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate efforts by the organization to achieve remediation or recovery from any future losses, such as those resulting from public disclosure of trade secrets.

Risk assessment analysis:

Overall likelihood: high

Justification: This could occur either intentionally or accidentally (e.g., taking a screenshot and having pictures backed up to an unmanaged cloud service).

Level of impact: high

Justification: Storage in unmanaged services presents a risk to the confidentiality and availability of corporate data because the corporation would no longer control it.

BYOD-specific threat: In a BYOD deployment, employees are more likely to have some backup or automated cloud storage solution configured on their device, which may lead to unintentional backup of enterprise data.

F.4.12 Threat Level 12

Can Great Seneca Accounting protect its data from PIN or password sharing?

Many individuals choose to share the PIN or password to unlock their personal device with family members. This creates a scenario where a nonemployee can access the device, the work applications, and therefore the work data.

Risk assessment analysis:

Overall likelihood: moderate

Justification: Even though employees are conditioned almost constantly to protect their work passwords, personal device PINs and passwords are not always protected with that same level of security. Anytime individuals share a password or PIN, there is increased risk that it might be exposed or compromised.

Level of impact: very high

Justification: If a malicious actor can bypass a device lock and gain access to the device, they can potentially access sensitive corporate data.

BYOD-specific threat: The passcode of an individual's personal mobile device is more likely to be shared among family and/or friends to provide access to applications (e.g., games). Although sharing passcodes may be convenient for personal reasons, this increases the risk of an unauthorized individual gaining access to enterprise data through a personal device.

F.5 Identification of Vulnerabilities and Predisposing Conditions

In this section we identify vulnerabilities and predisposing conditions that increase the likelihood that identified threat events will result in adverse impacts for Great Seneca Accounting. We list each vulnerability or predisposing condition in Table F-3, along with the corresponding threat events and ratings of threat pervasiveness. More details on threat event ratings can be found in Appendix Section F.3.

843 **Table F-3 Identify Vulnerabilities and Predisposing Conditions**

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-1	Email and other enterprise resources can be accessed from anywhere, and only username/password authentication is required.	TE-2, TE-9, TE-10	very high
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their mobile devices.	TE-6	very high
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-10, TE-11, TE-12	very high

844 F.6 Summary of Risk Assessment Findings

845 Table F-4 summarizes the risk assessment findings. More detail about the methodology used to rate 846 overall likelihood, level of impact, and risk is in the Appendix Section F.3.

847 **Table F-4 Summary of Risk Assessment Findings**

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	very high	high	high
TE-2: theft of credentials through an SMS or email phishing campaign	VULN-1	very high	high	high
TE-3: malicious applications installed via URLs in SMS or email messages	VULN-3	high	high	high

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-4: confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	VULN-3	high	high	high
TE-5: violation of privacy via misuse of device sensors	VULN-3	very high	high	high
TE-6: loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2, VULN-3	moderate	very high	high
TE-7: compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	moderate	very high	high
TE-8: unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	moderate	high	high
TE-9: unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1, VULN-3	very high	high	high
TE-10: loss of organizational data due to a lost or stolen device	VULN-1, VULN-3	very high	high	high
TE-11: loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	VULN-3	high	high	high
TE-12: unauthorized access to work applications via bypassed lock screen	VULN-3	moderate	very high	high

Note 1: Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [8].

Note 2: The risk rating is derived from both the overall likelihood and level of impact using Table I-2 of Appendix I in NIST SP 800-30 Revision 1 [8]. Because these are modified interval scales, the combined overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two variables. The table above demonstrates this where levels of moderate weigh more heavily than other ratings.

Note 3: Ratings of risk relate to the probability and level of adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1, adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low), serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic (i.e., very high).

Appendix G How Great Seneca Accounting Used the NIST Privacy Risk Assessment Methodology

This practice guide contains an example scenario about a fictional organization called Great Seneca Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be in alignment with an organization's security and privacy capabilities and objectives.

The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

In the example scenario, Great Seneca Accounting decided to use the NIST Privacy Risk Assessment Methodology (PRAM) to conduct a privacy risk assessment and help improve the company's mobile device architecture. The PRAM helps an organization analyze and communicate about how it conducted its data processing to achieve business/mission objectives.

At Great Seneca Accounting, the PRAM helped elucidate how enabling employees to use their personal devices for work-related functions can present privacy concerns for individuals. The PRAM also supports the risk assessment task in the Prepare step of the NIST Risk Management Framework as discussed in Appendix section E.1. The privacy events that were identified are below, along with potential mitigations.

G.1 Problematic Data Action 1: Unwarranted restriction through blocking access and wiping devices

Data Action: Devices can be wiped and reset to factory settings based on inputs regarding anomalous activity and untrusted applications.

Potential Problem for Individuals: In a BYOD environment, employees are likely to use their devices for both personal and work-related purposes; thus, in a system that features robust security information and event management capable of wiping a device entirely, there could be an issue of employees losing personal data and employees may not even expect that this is a possibility. A hypothetical example is that a Great Seneca Accounting employee stores personal photos on their mobile device, but these photos are lost when their device is wiped after anomalous activity is detected.

Mitigations:

Block access to corporate resources by removing device from mobile device management (MDM) control instead of wiping devices.

As an alternative to wiping data entirely, section F.4.3, Threat Event 3, discusses blocking a device from accessing enterprise resources until an application is removed. Temporarily blocking access ensures that an individual will not lose personal data through a full wipe of a device. This approach may help bring the system's capabilities into alignment with employees' expectations about what can happen to their devices, especially if they are unaware that devices can be wiped by administrators—providing greater predictability in the system.

Related mitigation: If this mitigation approach is taken, the organization may also wish to consider establishing and communicating these remediation processes to employees. It is important to have a clear remediation process in place to help employees regain access to resources on their devices at the appropriate time. It is also important to clearly convey this remediation process to employees. A remediation process provides greater manageability in the system supporting employees' ability to access resources. If well communicated to employees, this also provides greater predictability as employees will know the steps to regain access.

Enable only selective wiping of corporate resources on the device.

An alternative mitigation option for wiping device data is to limit what can be wiped. International Business Machines' (IBM's) MaaS360 can be configured to selectively wipe instead of performing a full factory reset. When configured this way, a wipe preserves employees' personal configurations, applications, and data while removing only the corporate configurations, applications, and data. However, on Android, a selective wipe will preserve restrictions imposed via policy on the device. To fully remove MDM control, the Remove Work Profile action must be used.

Advise employees to back up the personal data maintained on devices.

If device wiping remains an option for administrators, encourage employees to perform regular backups of their personal data to ensure it remains accessible in case of a wipe.

Restrict staff access to system capabilities that permit removing device access or performing wipes.

Limit staff with the ability to perform a wipe to only those with that responsibility by using role-based access controls. This can help decrease the chances of accidentally removing employee data or blocking access to resources.

G.2 Problematic Data Action 2: Employee surveillance

Data Action: The assessed infrastructure offers Great Seneca Accounting and its employees a number of security capabilities, including reliance on comprehensive monitoring capabilities, as noted in Section 4, Architecture. Multiple parties could collect and analyze a significant amount of data relating to employees, their devices, and their activities.

Potential Problem for Individuals: Employees may not be aware that the organization has the ability to monitor their interactions with the system and may not want this monitoring to occur. Collection and analysis of information might enable Great Seneca Accounting or other parties to craft a narrative about an employee based on the employee's interactions with the system, which could lead to a power imbalance between Great Seneca Accounting and the employee and loss of trust in the employer if the employee discovers monitoring that they did not anticipate.

Mitigations:

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

This may be achieved using role-based access controls. Access can be limited to any dashboard in the system containing data about employees and their devices but is most sensitive for the MaaS360 dashboard, which is the hub for data about employees, their devices, and threats. Minimizing access to sensitive information can enhance disassociability for employees using the system.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. In the configuration of MaaS360, location services and application inventory collection may be disabled. iOS devices can be configured in MaaS360 to collect only an inventory of applications that have been installed through the corporate application store instead of all applications installed on the device.

While these administrative configurations may help provide disassociability in the system, there are also some opportunities for employees to limit the data collected. Employees can choose to disable location services in their device OS to prevent collection of location data. MaaS360 can also be configured to provide employees with the ability to manage their own devices through the IBM User Portal.

Each of these controls contributes to limiting the number of attributes regarding employees and their devices that is collected, which can impede administrators' ability to associate information with specific individuals.

Dispose of personally identifiable information (PII).

Disposing of PII after an appropriate retention period can help reduce the risk of entities building profiles of individuals. Disposal can also help bring the system's data processing into alignment with employees' expectations and reduce the security risk associated with storing a large volume of PII. Disposal may be particularly important for certain parties in the system that collect a larger volume of data or more sensitive data. Disposal may be achieved using a combination of policy and technical controls. Parties in the system may identify what happens to data, when, and how frequently.

G.3 Problematic Data Action 3: Unanticipated revelations through data sharing across parties

Data Action: The infrastructure involves several parties that serve different purposes supporting Great Seneca Accounting's security objectives. As a result, device usage information could flow across various parties.

Potential Problems for Individuals: This transmission among a variety of different parties could be confusing for employees who might not know who has access to information about them. If administrators and co-workers know which colleagues are conducting activity on their device that triggers security alerts, employees could be embarrassed by its disclosure. Information being revealed and associated with specific employees could also lead to stigmatization and even impact Great Seneca Accounting upper management in its decision-making regarding the employee. Further, clear text transmissions could leave information vulnerable to attackers and therefore to unanticipated release of employee information.

Mitigations:

De-identify personal and device data when such data is not necessary to meet processing objectives.

De-identifying data helps decrease the chances that a third party is aggregating information pertaining to one individual. While de-identification can help reduce privacy risk, there are residual risks of re-identification.

Encrypt data transmitted between parties.

Encryption reduces the risk of compromise of information transmitted between parties. MaaS360 encrypts all communications over the internet with Transport Layer Security.

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using access controls to limit staff access to compliance information, especially when associated with individuals, can be important in preventing association of specific events with particular employees.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. MaaS360 can be configured to limit collection of application and location data. Further, instead of collecting a list of all the applications installed on the device, MaaS360 can collect only the list of those applications that were installed through the corporate application store (called "managed applications"). This would prevent insight into the employees' applications that employees downloaded for personal use. Zimperium provides privacy policies that can be configured to collect or not collect data items when certain events occur.

Use contracts to limit third-party data processing.

Establish contractual policies to limit data processing by third parties to only the processing that facilitates delivery of security services and to no data processing beyond those explicit purposes.

G.4 Mitigations Applicable Across Various Data Actions

Several mitigations benefit employees in all three data actions identified in the privacy risk assessment. The following training and support mitigations can help Great Seneca Accounting appropriately inform employees about the system and its data processing.

Mitigations:

Train employees about the system, parties involved, data processing, and actions that administrators can take.

Training sessions can also highlight any privacy-preserving techniques used, such as for disclosures to third parties. Training should include confirmation from employees that they understand the actions that administrators can take on their devices and their consequences–whether this is blocking access or wiping data. Employees may also be informed of data retention periods and when their data will be deleted. This can be more effective than sharing a privacy notice, which research has shown, individuals are unlikely to read. Still, MaaS360 should also be configured to provide employees with access to a visual privacy policy, which describes what device information is collected and why, as well as what actions administrators can take on the device. This enables employees to make better informed decisions while using their devices, and it enhances predictability.

Provide ongoing notifications or reminders about system activity.

This can be achieved using notifications to help directly link administrative actions on devices to relevant threats and to also help employees understand why an action is being taken. MaaS360 also notifies employees when changes are made to the privacy policy or MDM profile settings. These notifications can help increase system predictability by setting employee expectations appropriately regarding the way the system processes data and the resulting actions.

Provide a support point of contact.

By providing employees with a point of contact in the organization who can respond to inquiries and concerns regarding the system, employees can better understand how the system processes their data, which enhances predictability.

G.5 Privacy References for Example Solution Technologies

Additional privacy information on the example solution’s technologies appears below.

Table G-1 Privacy References for the Example Solution Technologies

Commercially Available Product	Mobile Security Technology	Product Privacy Information Location
IBM MaaS360 Mobile Device Management (SaaS) Version 10.73 IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android) IBM MaaS360 Cloud Extender / Cloud Extender Modules	mobile device management	https://www.ibm.com/support/pages/node/1093156?mhsrc=ibm-search_a&mhq=maas360%20privacy https://www.ibm.com/support/pages/node/571227 https://www.ibm.com/support/knowledge-center/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_privacy.htm http://public.dhe.ibm.com/software/security/products/maas360/GDPR/
Kryptowire Cloud Service	application vetting	https://www.kryptowire.com
Palo Alto Networks PA-VM-100 Version 9.0.1 Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android)	virtual private network (VPN) and firewall/ filtering	https://docs.paloaltonetworks.com/globalprotect/8-0/globalprotect-admin/host-information/about-host-information/what-data-does-the-globalprotect-agent-collect# https://www.paloaltonetworks.com/resources/datasheets/url-filtering-privacy-datasheet
Qualcomm (Version is mobile device dependent)	trusted execution environment	https://www.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf
Zimperium Defense Suite Zimperium Console Version vGA-4.23.1 Zimperium zIPS Agent Version 4.9.2 (Android and iOS)	mobile threat defense	https://www.zimperium.com/mobile-app-protection

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

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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.

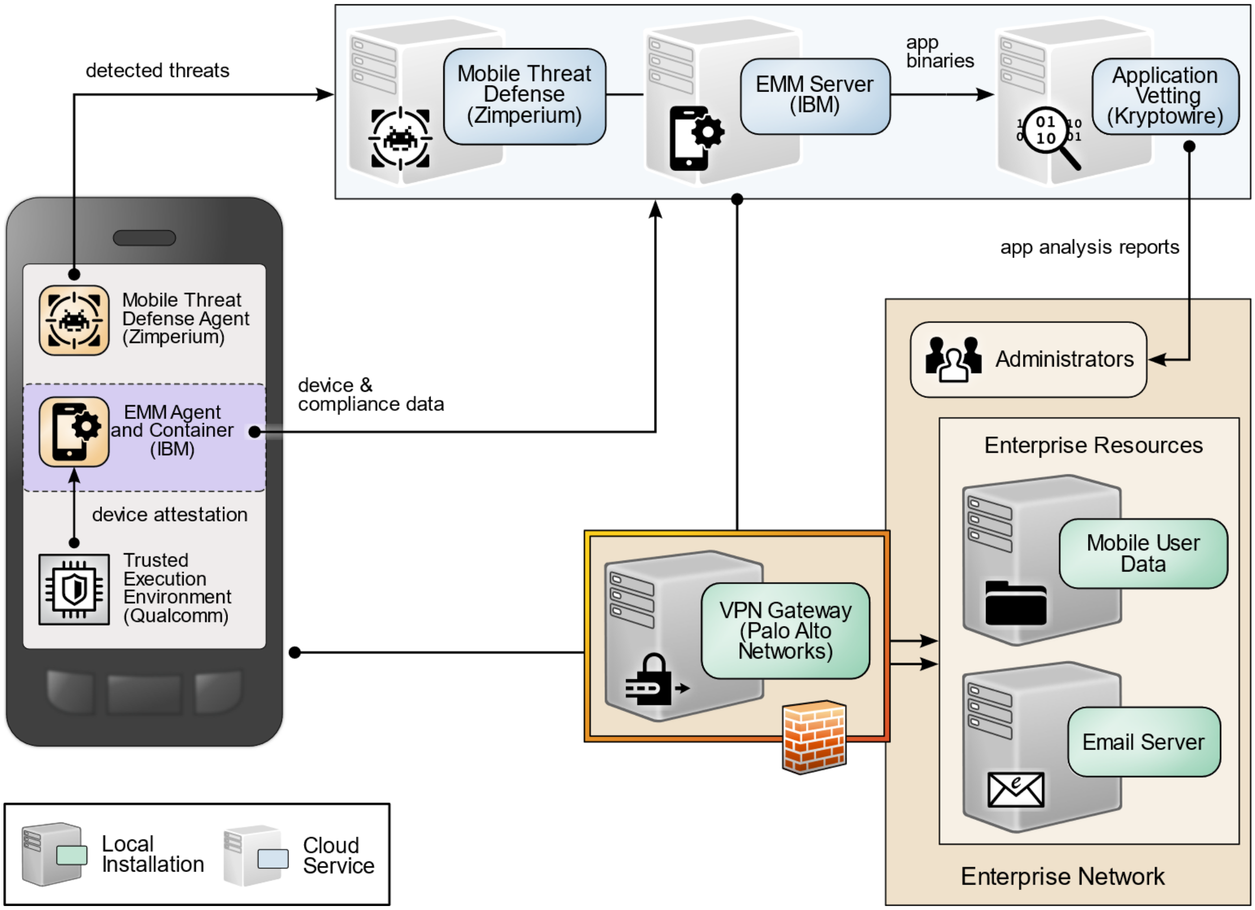
Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide.*
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit.**
`Monospace`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

Figure 1-1 High-Level Build Architecture



2 Product Installation Guides

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

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

2.1 Network Device Enrollment Services Server

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

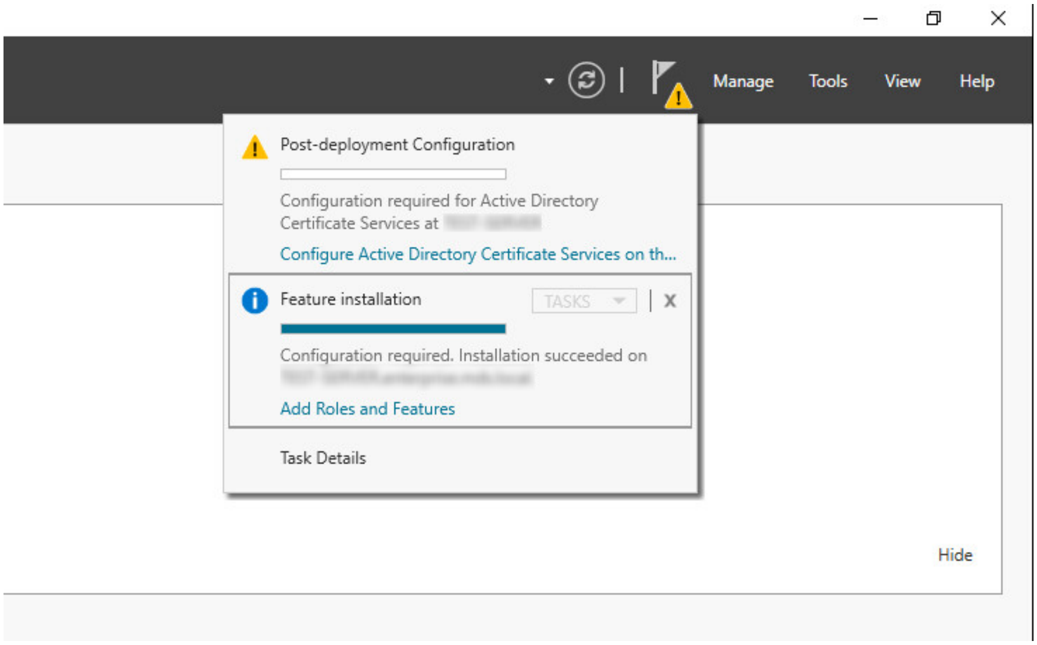
2.1.2 NDES Configuration

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



Post-deployment Configuration

Configuration required for Active Directory Certificate Services at [redacted]

Configure Active Directory Certificate Services on th...

Feature installation

Configuration required. Installation succeeded on [redacted]

Add Roles and Features

Task Details

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.

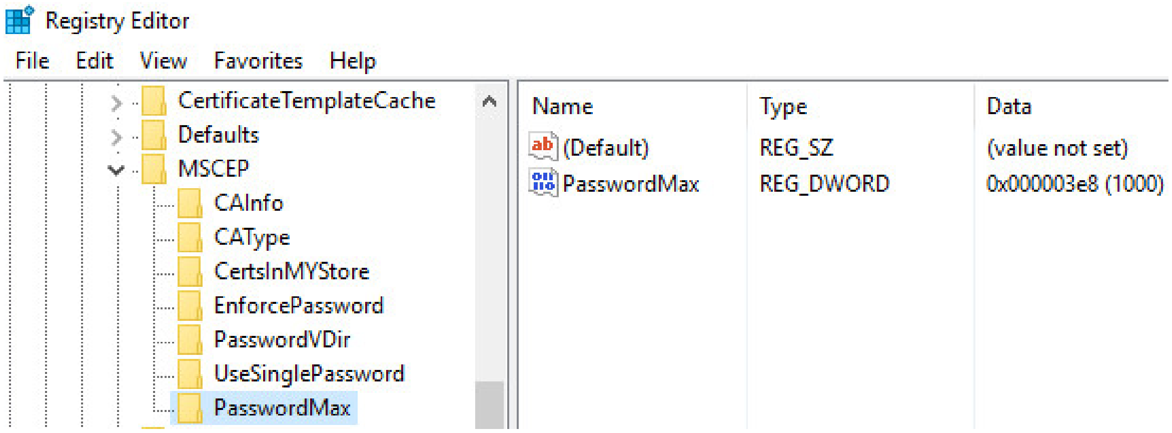
11. Check **Network Device Enrollment Service**. Click **Next.**
12. Configure an NDES service account by performing the following actions:
    a. On the active directory server, open **Active Directory Users and Computers.**
    b. Click **Users** and create a new user for the service. For this example, 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

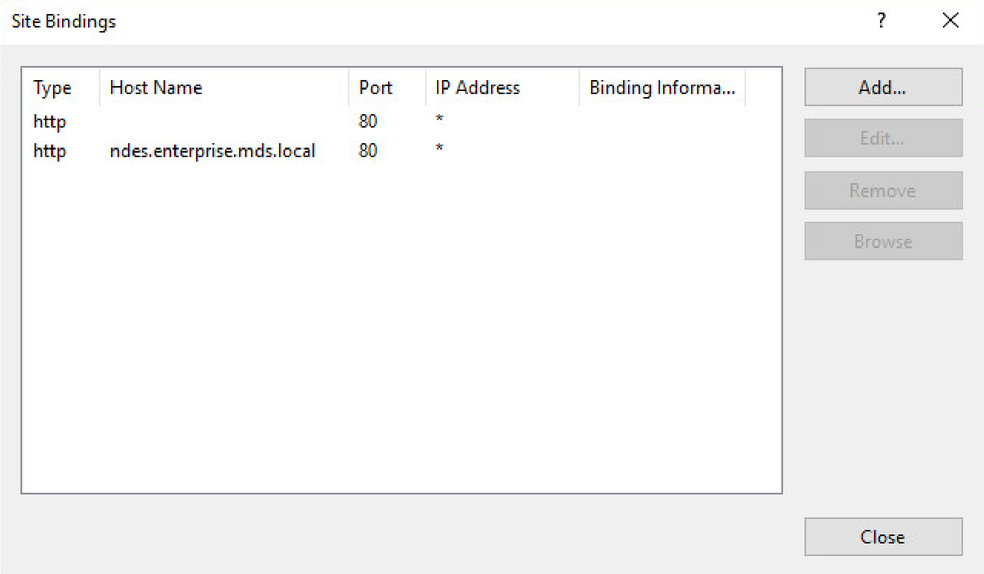


Name	Type	Data
(Default)	REG_SZ	(value not set)
PasswordMax	REG_DWORD	0x000003e8 (1000)

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**.

Figure 2-3 NDES Domain Bindings



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
http	ndes.enterprise.mds.local	80	*	

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

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

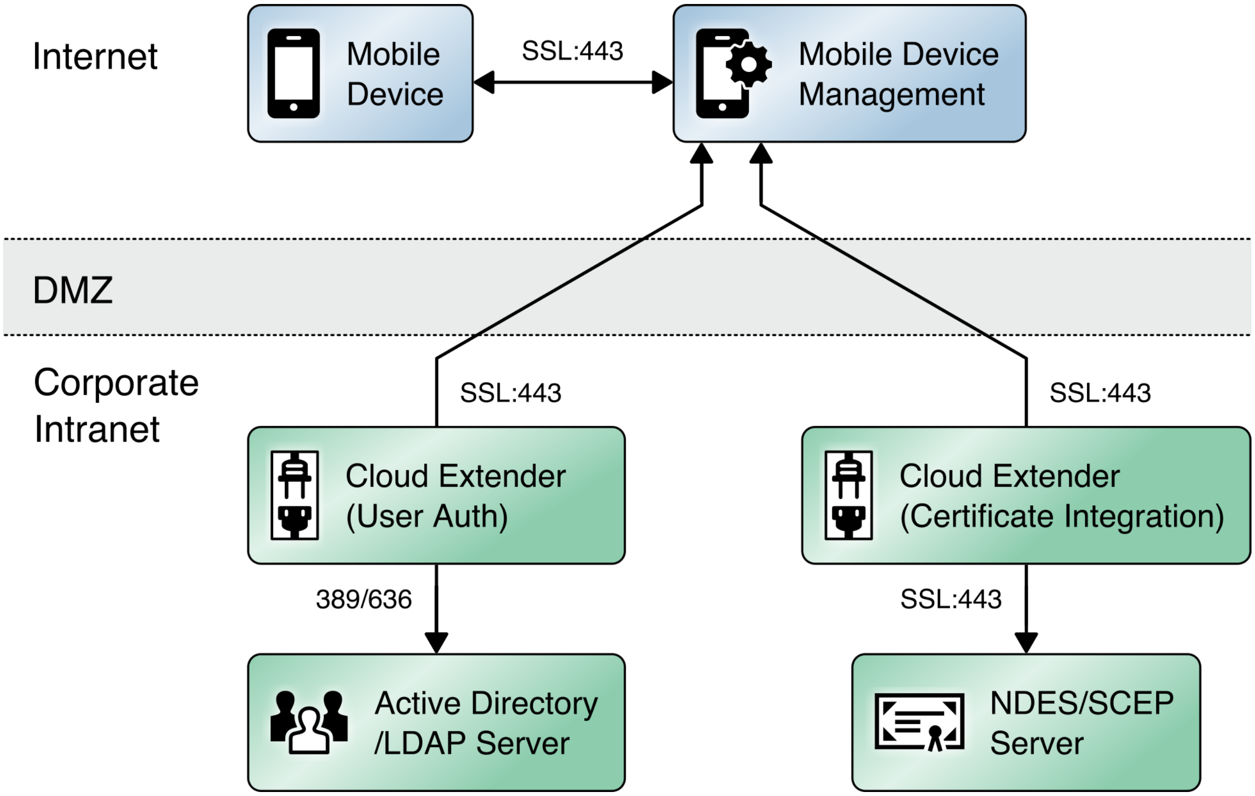
2.2 International Business Machines MaaS360

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

2.2.1 Cloud Extender

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

Figure 2-4 Cloud Extender Architecture



2.2.1.1 Cloud Extender Download

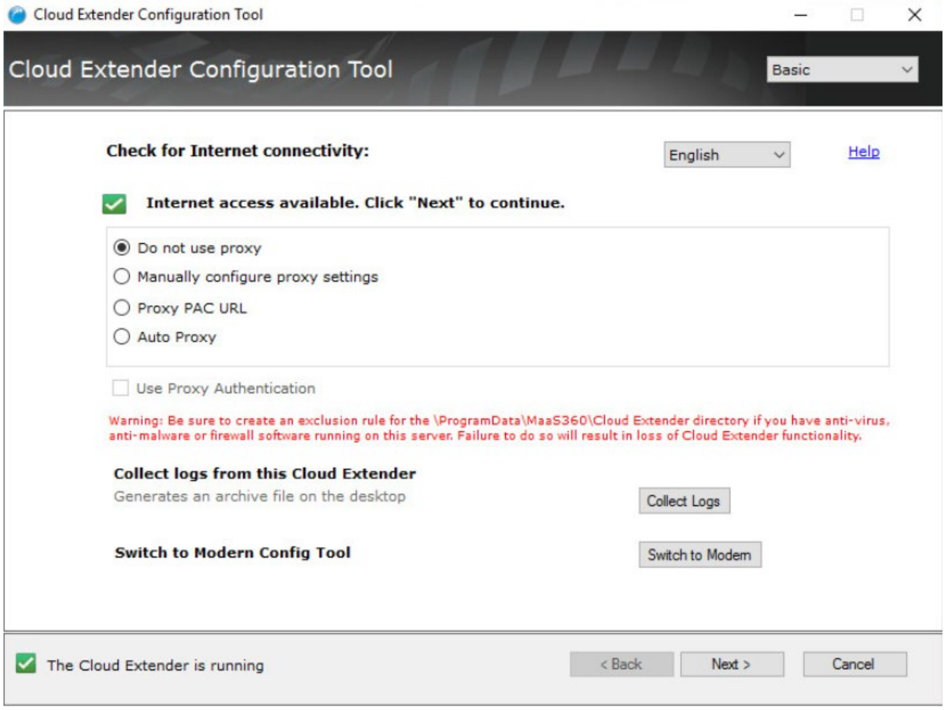
1. Log in to the MaaS360 web portal.
2. Click **Setup > Cloud Extender.**
3. Click the link that says **Click here to get your License Key.** The license key will be emailed to the currently logged-in user's email address.
4. Click the link that says **Click here to download the Cloud Extender.** Save the binary.
5. Move the binary to a machine behind the corporate firewall that is always online. Recommendation: Install it while logged in as a domain user on a machine that is not the domain controller.
6. Install **.NET 3.5 Features** in the **Server Manager** on the machine where the MaaS360 Cloud Extender will run.

2.2.1.2 Cloud Extender Active Directory Configuration

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

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

Figure 2-5 Old Cloud Extender Interface



Cloud Extender Configuration Tool
Cloud Extender Configuration Tool
Basic
English
Help
Collect Logs
Switch to Modern
< Back
Next >
Cancel

Check for Internet connectivity:

☑ **Internet access available. Click "Next" to continue.**

● Do not use proxy
○ Manually configure proxy settings
○ Proxy PAC URL
○ Auto Proxy

□ Use Proxy Authentication

Warning: Be sure to create an exclusion rule for the \ProgramData\MaaS360\Cloud Extender directory if you have anti-virus, anti-malware or firewall software running on this server. Failure to do so will result in loss of Cloud Extender functionality.

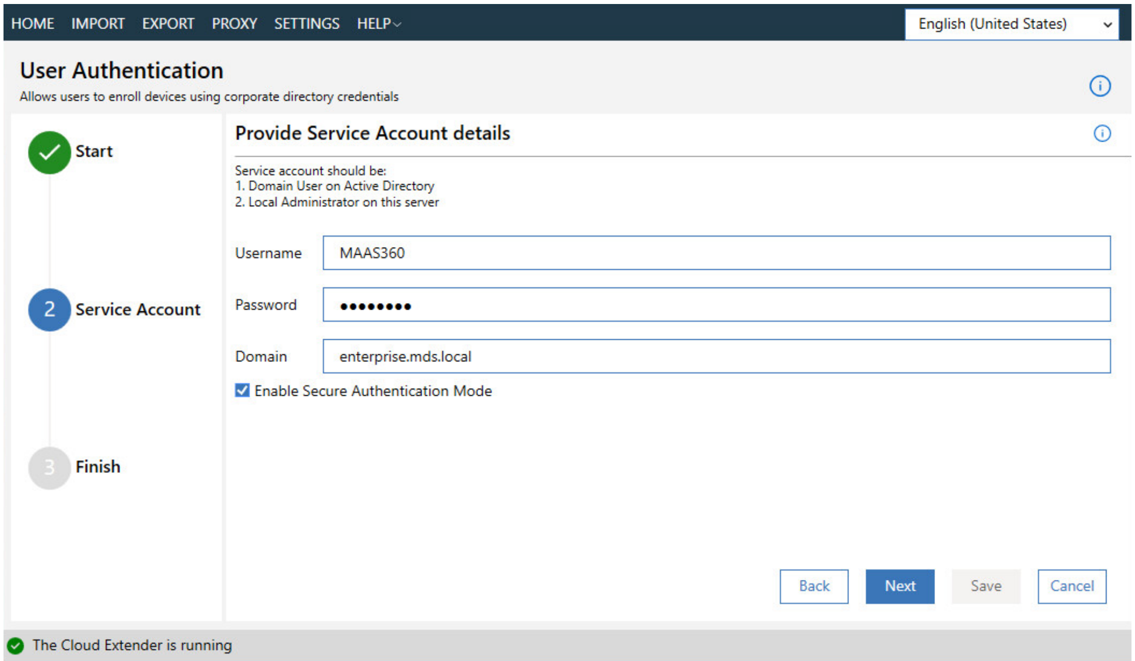
Collect logs from this Cloud Extender
Generates an archive file on the desktop

Switch to Modern Config Tool

☑ The Cloud Extender is running

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

Figure 2-6 Cloud Extender Service Account Details



User Authentication

Allows users to enroll devices using corporate directory credentials

Provide Service Account details

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

Username: MAAS360

Password: ••••••••

Domain: enterprise.mds.local

☑ Enable Secure Authentication Mode

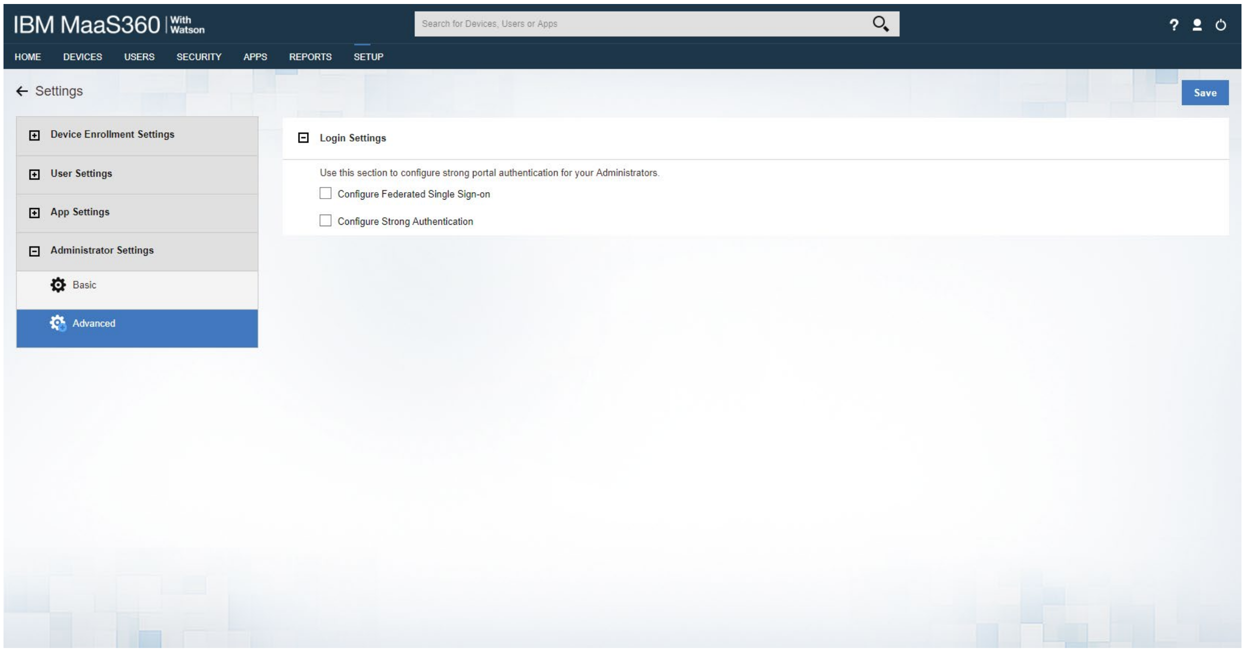
The Cloud Extender is running

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

2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration

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

Figure 2-7 Administrator Settings


IBM MaaS360 With Watson
Search for Devices, Users or Apps
HOME DEVICES USERS SECURITY APPS REPORTS SETUP
← Settings
Save
Device Enrollment Settings
User Settings
App Settings
Administrator Settings
Basic
Advanced

Login Settings

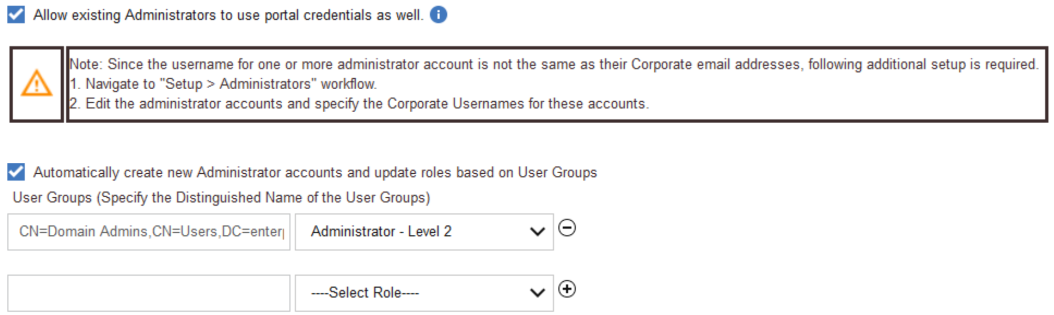
Use this section to configure strong portal authentication for your Administrators.

□ Configure Federated Single Sign-on

□ Configure Strong Authentication

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

Figure 2-8 Administrator Configuration Options



☑ Allow existing Administrators to use portal credentials as well.

Note: Since the username for one or more administrator account is not the same as their Corporate email addresses, following additional setup is required.
1. Navigate to "Setup > Administrators" workflow.
2. Edit the administrator accounts and specify the Corporate Usernames for these accounts.

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

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

CN=Domain Admins,CN=Users,DC=enterp	Administrator - Level 2
	----Select Role----

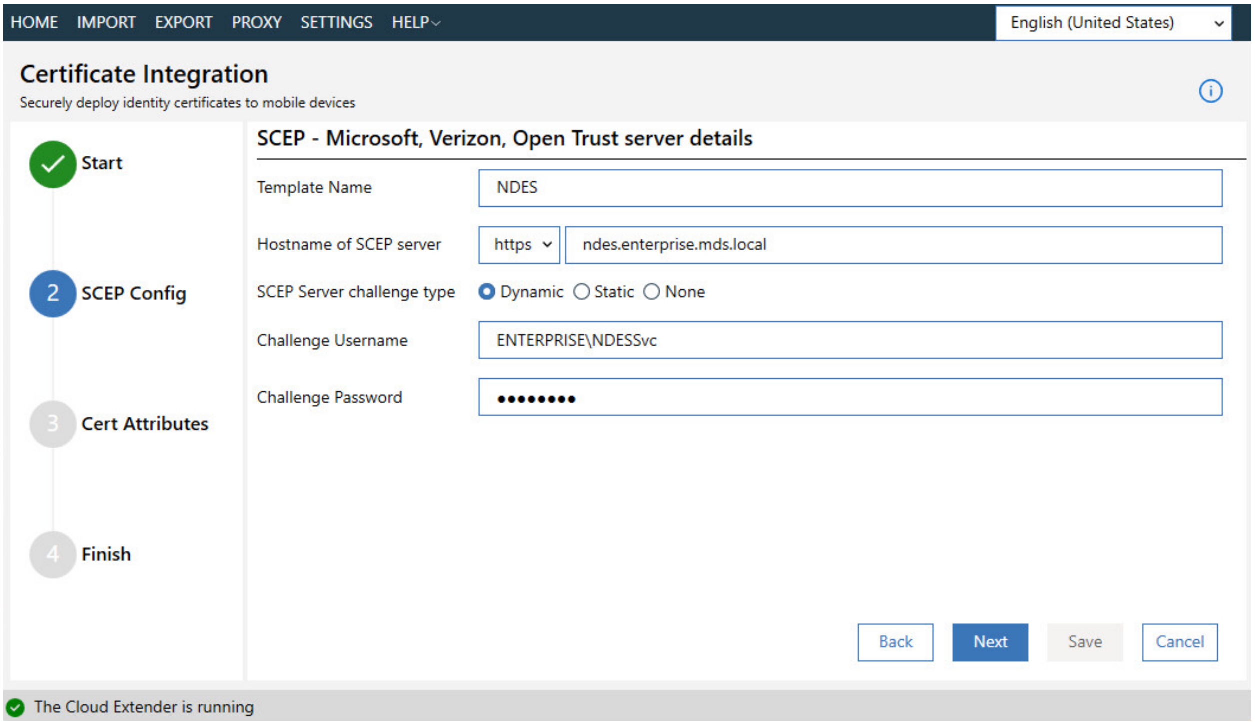
11. Click **Save.**

2.2.1.4 Cloud Extender NDES Integration

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

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

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



SCEP - Microsoft, Verizon, Open Trust server details

Template Name: NDES

Hostname of SCEP server: https ndes.enterprise.mds.local

SCEP Server challenge type: ● Dynamic ○ Static ○ None

Challenge Username: ENTERPRISE\NDESSvc

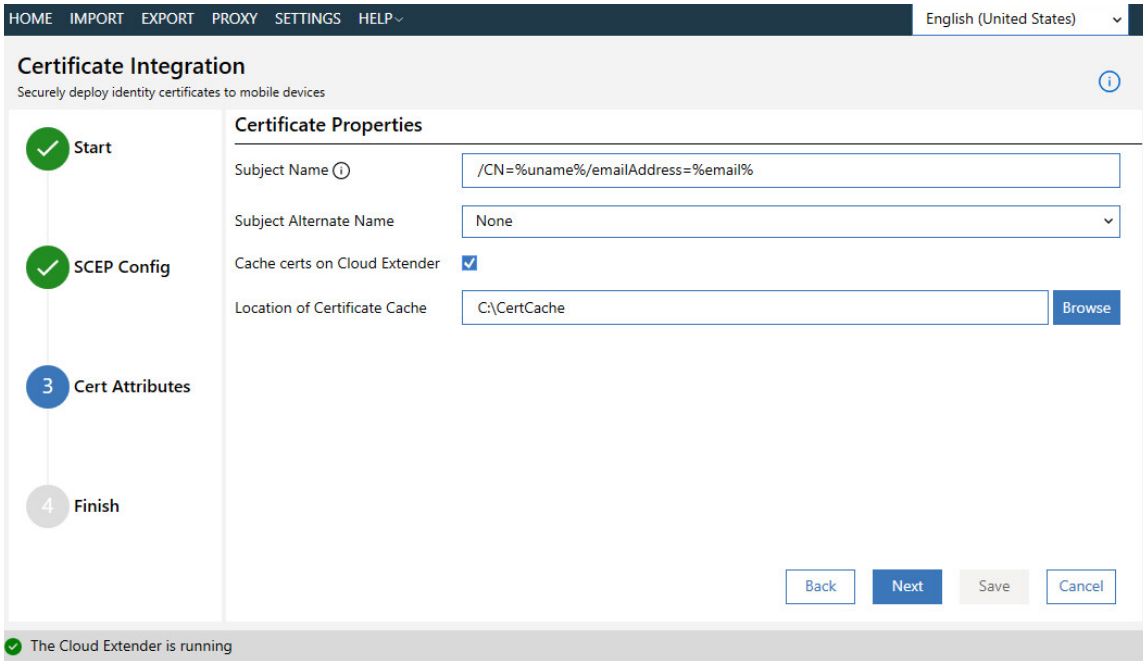
Challenge Password: ••••••••

The Cloud Extender is running

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.

Figure 2-10 Cloud Extender Certificate Properties



Certificate Properties

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

Subject Alternate Name: None

Cache certs on Cloud Extender: ☑

Location of Certificate Cache: C:\CertCache

The Cloud Extender is running

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

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

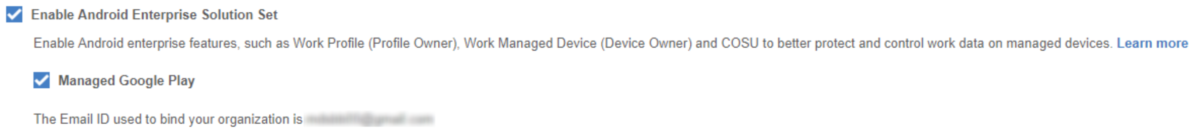
2.2.2 Android Enterprise Configuration

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

1. Create a Google account if you do not have one you wish to bind with.
2. From the MaaS360 portal, navigate to **Setup > Services.**
3. Click **Mobile Device Management.**
4. Check the box next to **Enable Android Enterprise Solution Set.**
5. Enter your password, and click **Enable.**

6. Click **Mobile Device Management.**
7. Click the radio button next to **Enable via Managed Google Play Accounts (no G Suite).**
8. Ensure all pop-up blockers are disabled. Click the link on the word **here.**
9. Enter your password, and click **Enable.**
10. In the new page that opens, ensure you are signed into the Google account you wish to bind.
11. Click **Get started.**
12. Enter your business name, and click **Next.**
13. If General Data Protection Regulation compliance is not required, scroll to the bottom, check the **I agree** box, and click **Confirm.** If compliance is required, fill out the requested information first.
14. Click **Complete Registration.**
15. Confirm binding on the **Setup** page under **Mobile Device Management.** The settings should look like Figure 2-11, where the blurred-out portion is the Google email address used to bind.

Figure 2-11 Enterprise Binding Settings Confirmation



☑ Enable Android Enterprise Solution Set

Enable Android enterprise features, such as Work Profile (Profile Owner), Work Managed Device (Device Owner) and COSU to better protect and control work data on managed devices. Learn more

☑ Managed Google Play

The Email ID used to bind your organization is [redacted]

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.

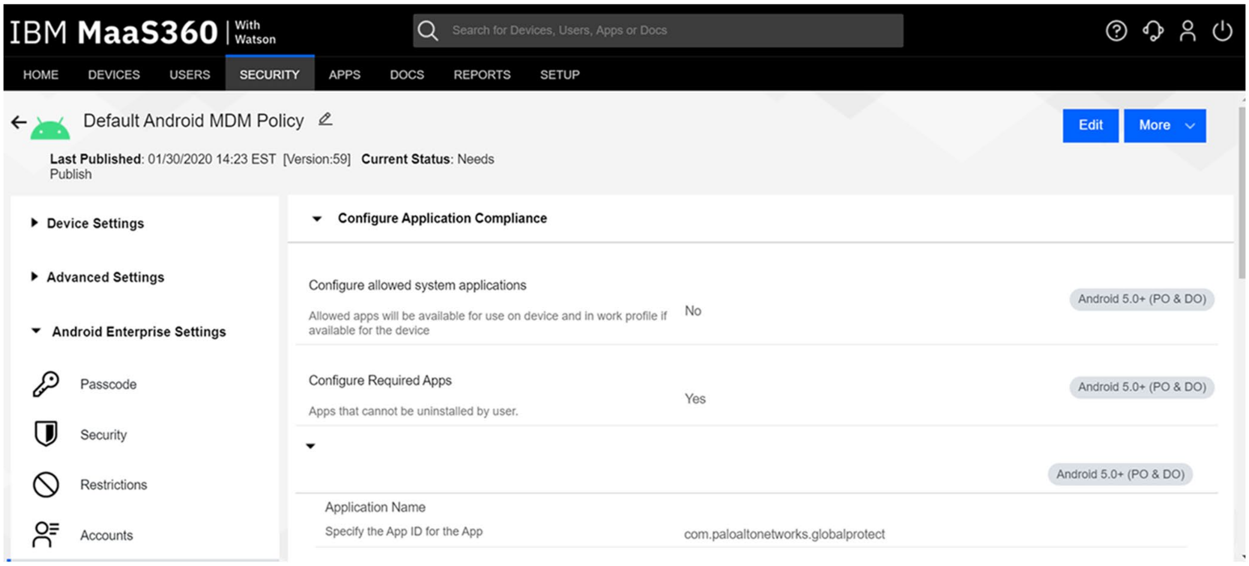
6. Configure the passcode settings based on corporate requirements.
7. Navigate to **Android Enterprise Settings > Restrictions.**
8. Check the box next to Configure Restrictions.
9. Configure restrictions based on corporate requirements.
10. Click **Save.**

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.

Figure 2-12 Android GlobalProtect Application Compliance



Default Android MDM Policy

Last Published: 01/30/2020 14:23 EST [Version:59] **Current Status**: Needs Publish

Configure Application Compliance

Configure allowed system applications — No — Android 5.0+ (PO & DO)
Allowed apps will be available for use on device and in work profile if available for the device

Configure Required Apps — Yes — Android 5.0+ (PO & DO)
Apps that cannot be uninstalled by user.

Android 5.0+ (PO & DO)

Application Name — com.paloaltonetworks.globalprotect
Specify the App ID for the App

2.2.5 iOS Configuration

2.2.5.1 Policy Configuration

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

2.2.5.2 VPN Configuration

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

2. Click **Edit**.
3. Next to **Configure for Type,** select **Custom SSL**.
4. Enter a name next to **VPN Connection Name.** In this sample implementation, **Great Seneca VPN** was used.
5. Next to **Identifier,** enter **com.paloaltonetworks.globalprotect.vpn**.
6. Next to **Host name of the VPN Server,** enter the URL of the VPN endpoint without http or https.
7. Next to **VPN User Account,** enter **%username%.**
8. Next to **User Authentication Type,** select **Certificate.**
9. Next to **Identity Certificate,** select the name of the certificate profile created during the NDES configuration steps. In this sample implementation, **NDES** was used.
10. Next to **Custom Data 1**, enter **allowPortalProfile=0**
11. Next to **Custom Data 2**, enter **fromAspen=1**
12. Next to **Apps to use this VPN,** enter the application identifications (IDs) of applications to go through the VPN. This will be the applications deployed to the devices as work applications.
13. Next to **Provider Type**, select **Packet Tunnel.**
14. 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.

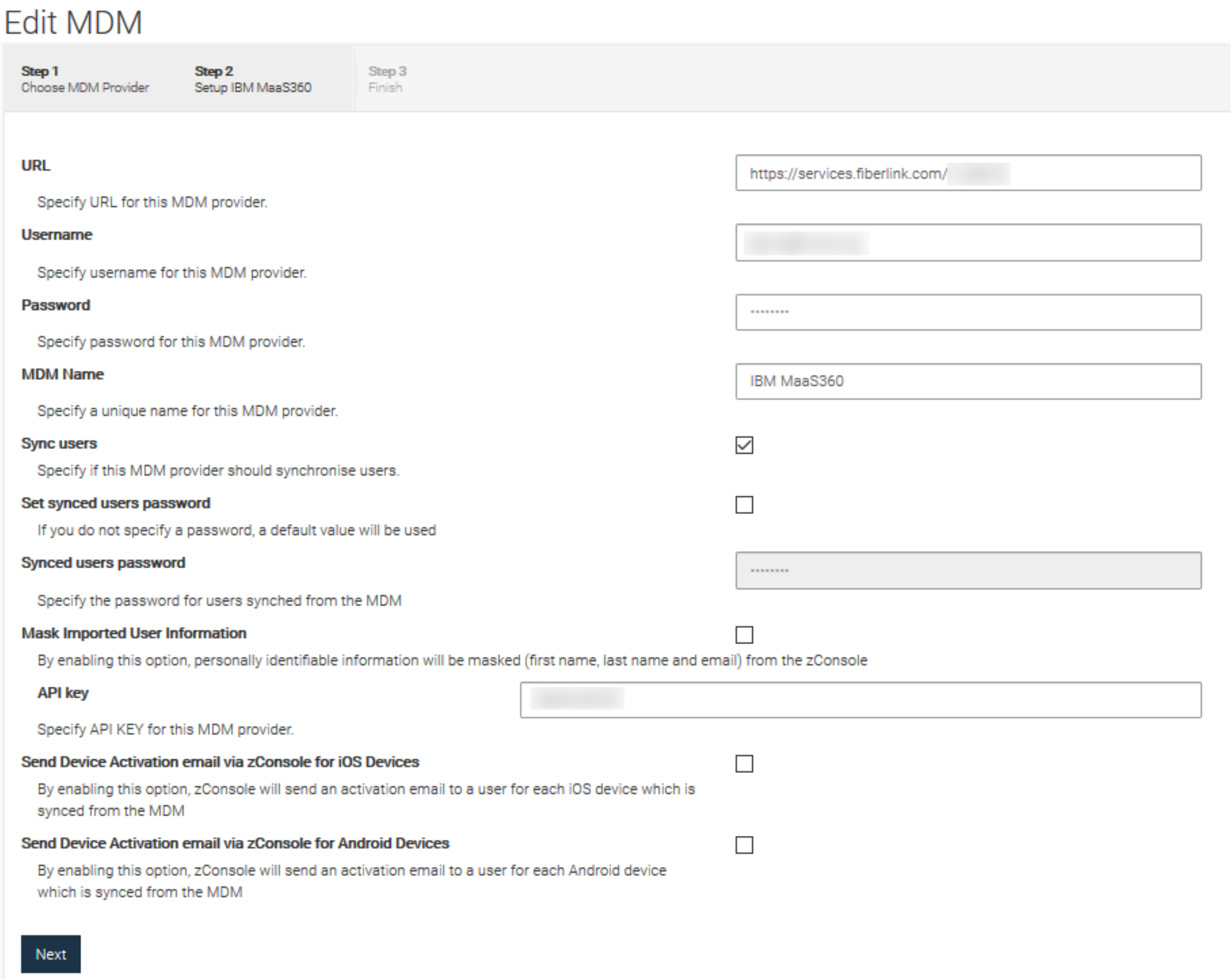
1. Log in to the zConsole.
2. Navigate to **Manage > MDM.**
3. Select **Add MDM > MaaS360**.

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



Edit MDM

Step 1 Choose MDM Provider | Step 2 Setup IBM MaaS360 | Step 3 Finish

URL https://services.fiberlink.com/[redacted]
Specify URL for this MDM provider.

Username [redacted]
Specify username for this MDM provider.

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

MDM Name IBM MaaS360
Specify a unique name for this MDM provider.

Sync users ☑
Specify if this MDM provider should synchronise users.

Set synced users password □
If you do not specify a password, a default value will be used

Synced users password ········
Specify the password for users synched from the MDM

Mask Imported User Information □
By enabling this option, personally identifiable information will be masked (first name, last name and email) from the zConsole

API key [redacted]
Specify API KEY for this MDM provider.

Send Device Activation email via zConsole for iOS Devices □
By enabling this option, zConsole will send an activation email to a user for each iOS device which is synced from the MDM

Send Device Activation email via zConsole for Android Devices □
By enabling this option, zConsole will send an activation email to a user for each Android device which is synced from the MDM

7. Click **Next**.

8. Select the MaaS360 groups to synchronize with Zimperium. In this case, **All Devices** was selected**.**

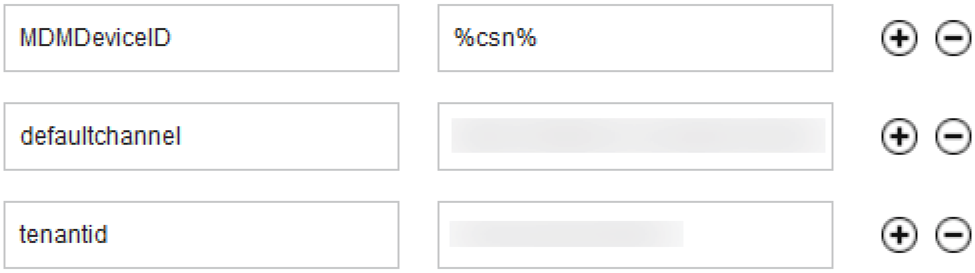
9. Click **Finish**. Click **Sync Now** to synchronize all current MaaS360 users and devices.

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

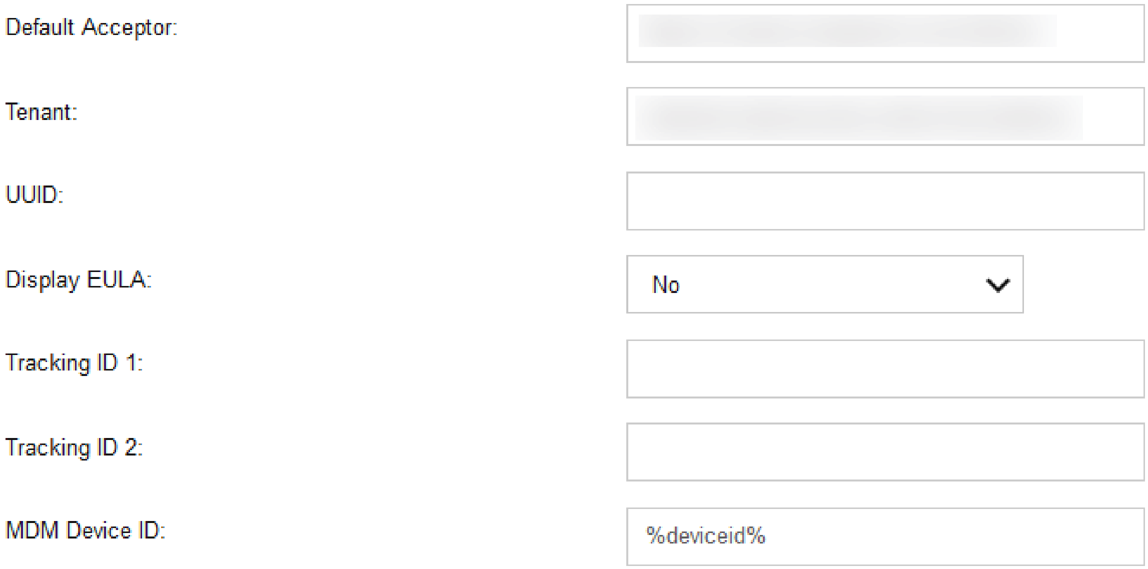


MDMDeviceID	%csn%
defaultchannel	[redacted]
tenantid	[redacted]

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



Default Acceptor: [redacted]

Tenant: [redacted]

UUID:

Display EULA: No

Tracking ID 1:

Tracking ID 2:

MDM Device ID: %deviceid%

26. Click **Add.**

2.3.3 Enforce Application Compliance

From the IBM MaaS360 web portal:

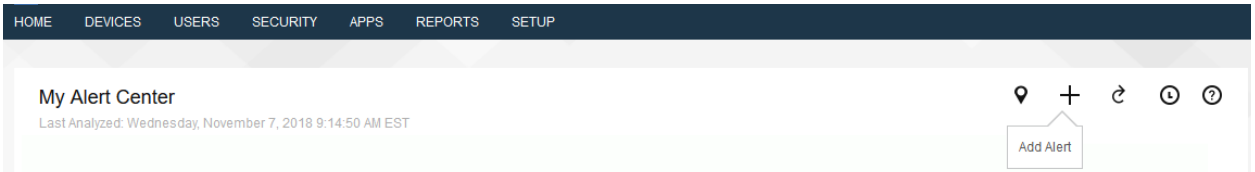
1. Navigate to **Security > Policies.**
2. Select the default Android policy.

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

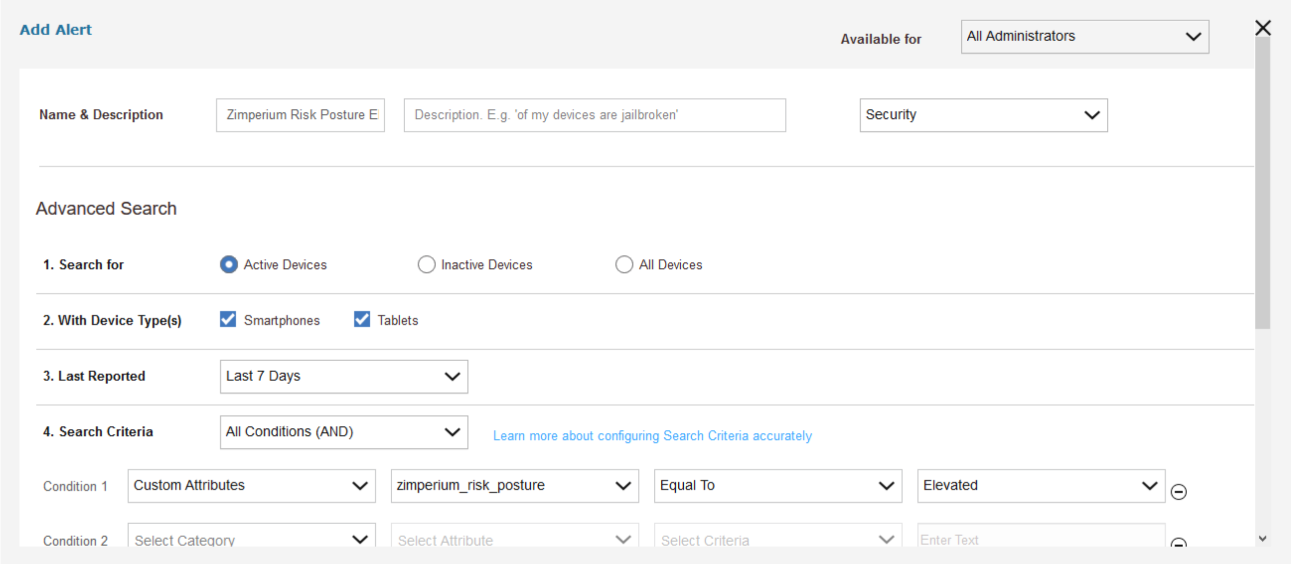


My Alert Center

Last Analyzed: Wednesday, November 7, 2018 9:14:50 AM EST

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.

Figure 2-17 Zimperium Risk Posture Alert Configuration



Add Alert

Available for: All Administrators

Name & Description: Zimperium Risk Posture E | Description. E.g. 'of my devices are jailbroken' | Security

Advanced Search

1. Search for: ● Active Devices ○ Inactive Devices ○ All Devices
2. With Device Type(s): ☑ Smartphones ☑ Tablets
3. Last Reported: Last 7 Days
4. Search Criteria: All Conditions (AND) — Learn more about configuring Search Criteria accurately

Condition 1: Custom Attributes | zimperium_risk_posture | Equal To | Elevated

Condition 2: Select Category | Select Attribute | Select Criteria | Enter Text

8. Click **Update.**

2.4 Palo Alto Networks Virtual Firewall

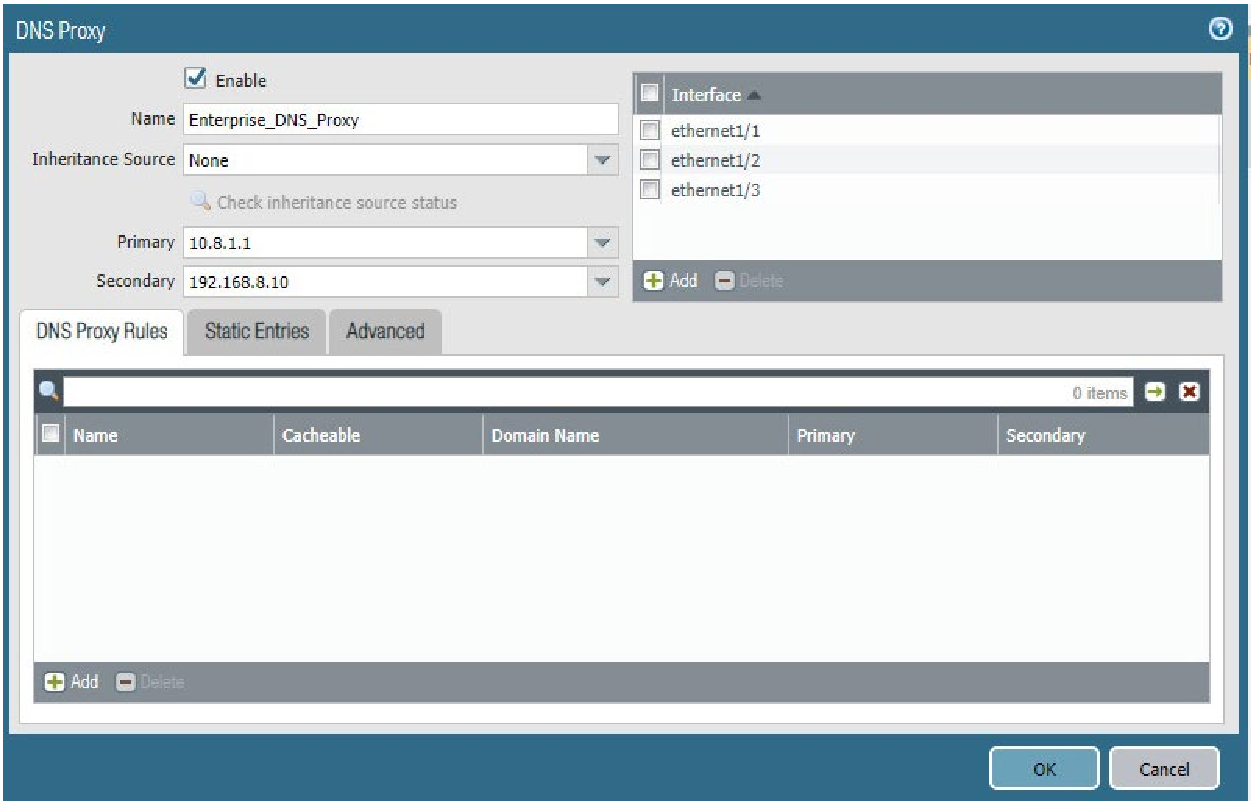
Palo Alto Networks contributed an instance of its VM-100 series firewall for use on the project.

2.4.1 Network Configuration

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

8. Navigate to **Network > Zones.**
9. Click **Add**. Give the zone an appropriate name, set the Type to **Layer3,** and assign it an interface.
10. Commit the changes.
11. Navigate to **Network > Virtual Routers**.
12. Click **Add**.
13. Give the router an appropriate name, and add the internal and external interfaces.
14. Click **Static Routes > Add**. Give the static route an appropriate name, e.g., WAN. Set the destination to be **0.0.0.0/0,** set the interface to be the WAN interface, and set the next hop internet protocol (IP) address to be the upstream gateway's IP address.
15. (optional) Delete the default router by clicking the checkbox next to it and clicking **Delete** at the bottom of the page.
16. Commit the changes. The commit window should not display any more warnings.
17. Navigate to **Network > DNS Proxy**.
18. Click **Add**.
19. Give the proxy an appropriate name. Under **Primary,** enter the primary domain name system (DNS) IP address.
20. (optional) Enter the secondary DNS IP address.
21. Add the interfaces under **Interface.** Click **OK.**

Figure 2-18 DNS Proxy Object Configuration



☑ Enable

Name: Enterprise_DNS_Proxy

Inheritance Source: None

Primary: 10.8.1.1

Secondary: 192.168.8.10

□	Interface
□	ethernet1/1
□	ethernet1/2
□	ethernet1/3

□	Name	Cacheable	Domain Name	Primary	Secondary

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

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

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

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

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

27. For each device on the network, click **Add**. Give the device an appropriate name, enter an optional description, and enter the IP address.

28. Click **OK**.

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

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

31. Click **Add**.

32. Give the network address translation rule a meaningful name, such as External Internet Access.

33. Click **Original Packet**.

34. Click **Add,** and add the zone representing the intranet—in this case, **Enterprise_Intranet.**

35. Repeat step 34 for the secure sockets layer (SSL) VPN zone.

36. Under **Source Address,** click **Add**.

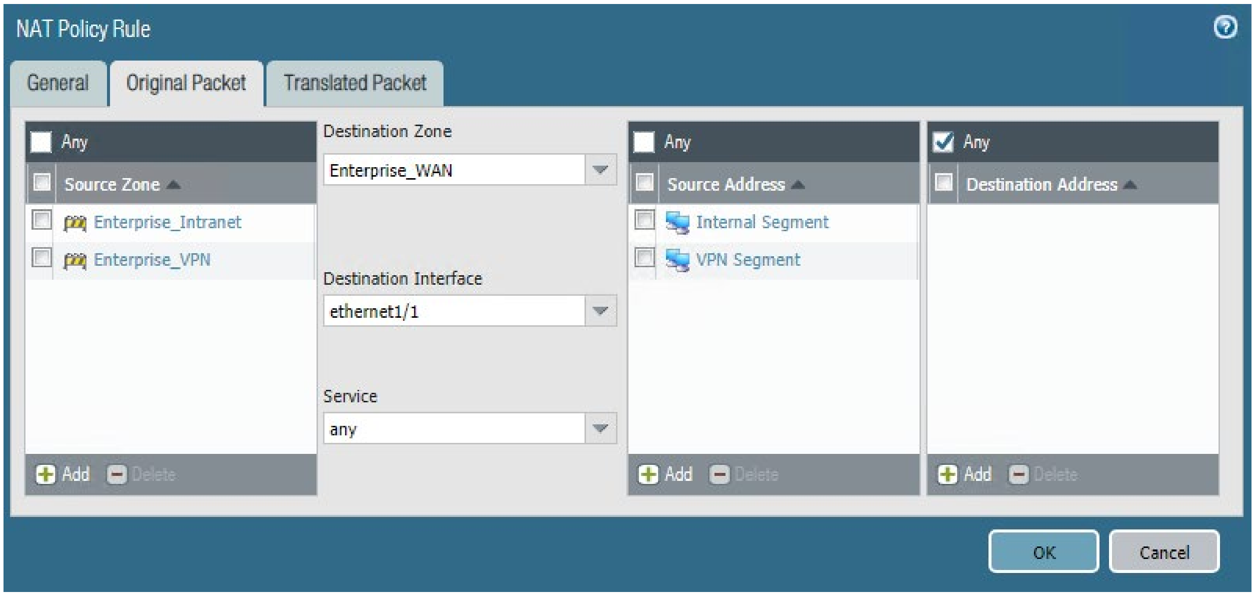
37. Enter the subnet corresponding to the intranet segment.

38. Repeat step 37 for the SSL VPN segment.

39. Click **Translated Packet.** Set the translation type to **Dynamic IP and Port.** Set Address Type to be **Interface Address.** Set Interface to be the WAN interface, and set the IP address to be the WAN IP of the firewall.

40. Click **OK** and commit the changes.

Figure 2-19 Original Packet Network Address Translation Configuration



NAT Policy Rule

General | Original Packet | Translated Packet

□ Any

□ Source Zone ▲
- □ Enterprise_Intranet
- □ Enterprise_VPN

Destination Zone: Enterprise_WAN

Destination Interface: ethernet1/1

Service: any

□ Any

□ Source Address ▲
- □ Internal Segment
- □ VPN Segment

☑ Any

□ Destination Address ▲

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

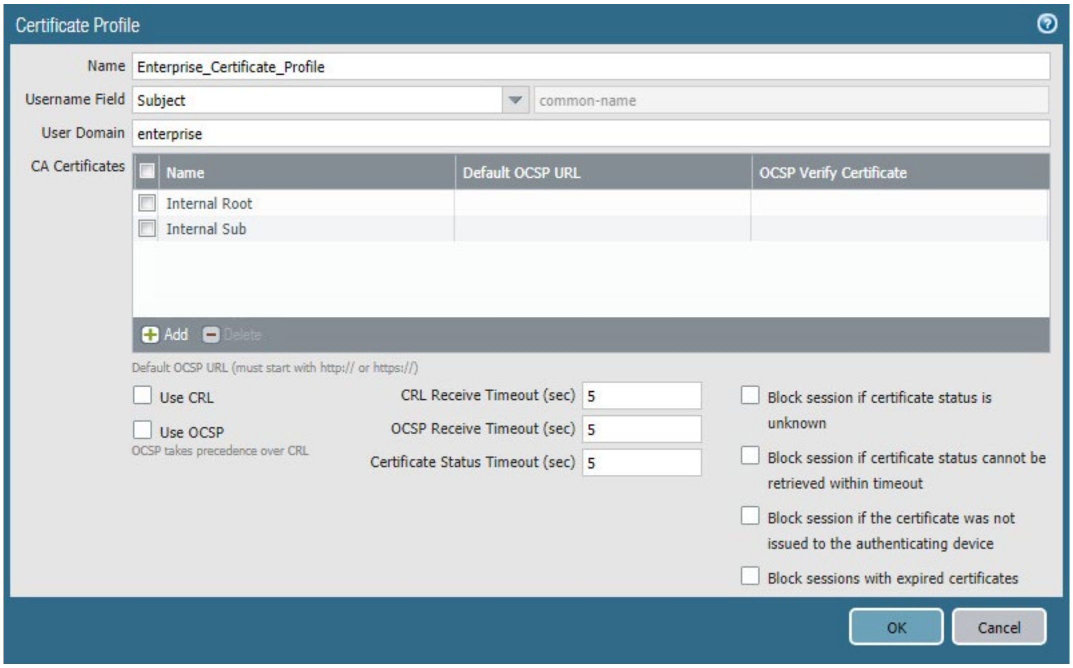
1. Navigate to **Policies > Security**.
2. Click **Add**.
3. Give the rule a meaningful name, such as Intranet Outbound.
4. Click **Source**. Click **Add** under source zone, and set the source zone to be the internal network.
5. Click **Destination.** Click **Add** under destination zone, and set the 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 2-20 Certificate Profile



Certificate Profile

Name: Enterprise_Certificate_Profile

Username Field: Subject ▾ common-name

User Domain: enterprise

CA Certificates

□ Name	Default OCSP URL	OCSP Verify Certificate
□ Internal Root		
□ Internal Sub		

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

□ Use CRL

□ Use OCSP
OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

□ Block session if certificate status is unknown

□ Block session if certificate status cannot be retrieved within timeout

□ Block session if the certificate was not issued to the authenticating device

□ Block sessions with expired certificates

2.4.5 Website Filtering Configuration

2.4.5.1 Configure Basic Website Blocking

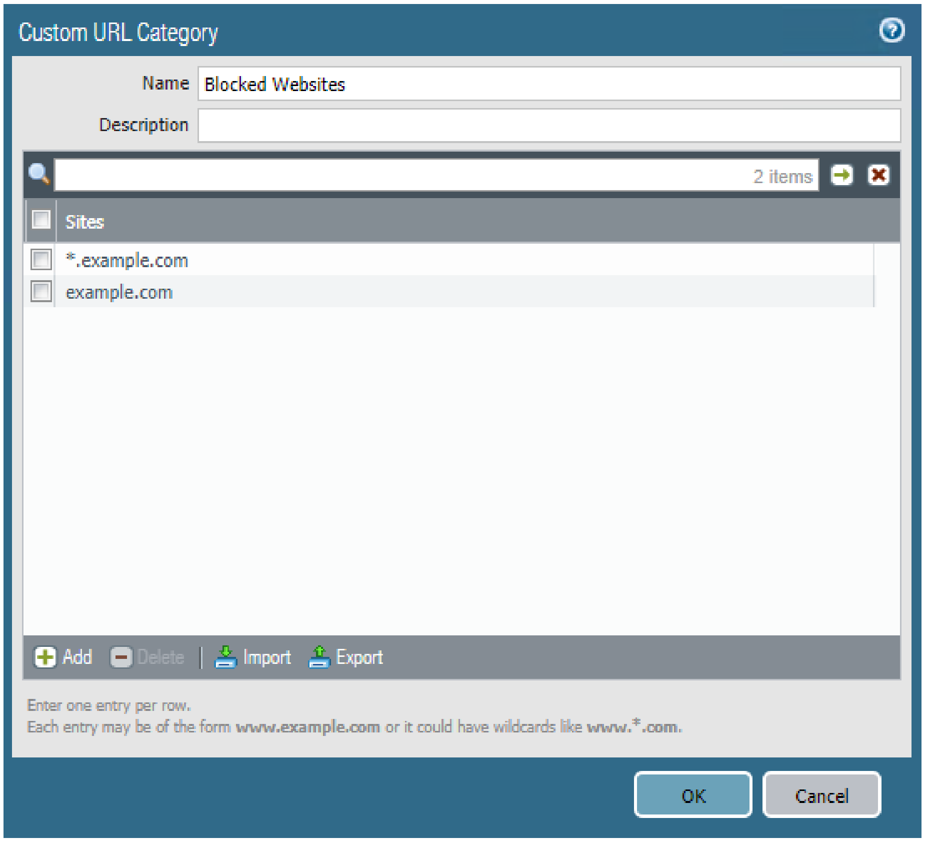
1. Navigate to **Objects > URL Category**.

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.

Figure 2-21 Custom URL Category



Custom URL Category

Name: Blocked Websites

Description:

2 items

☐ Sites
☐ *.example.com
☐ example.com

Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

5. Click **OK**.

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

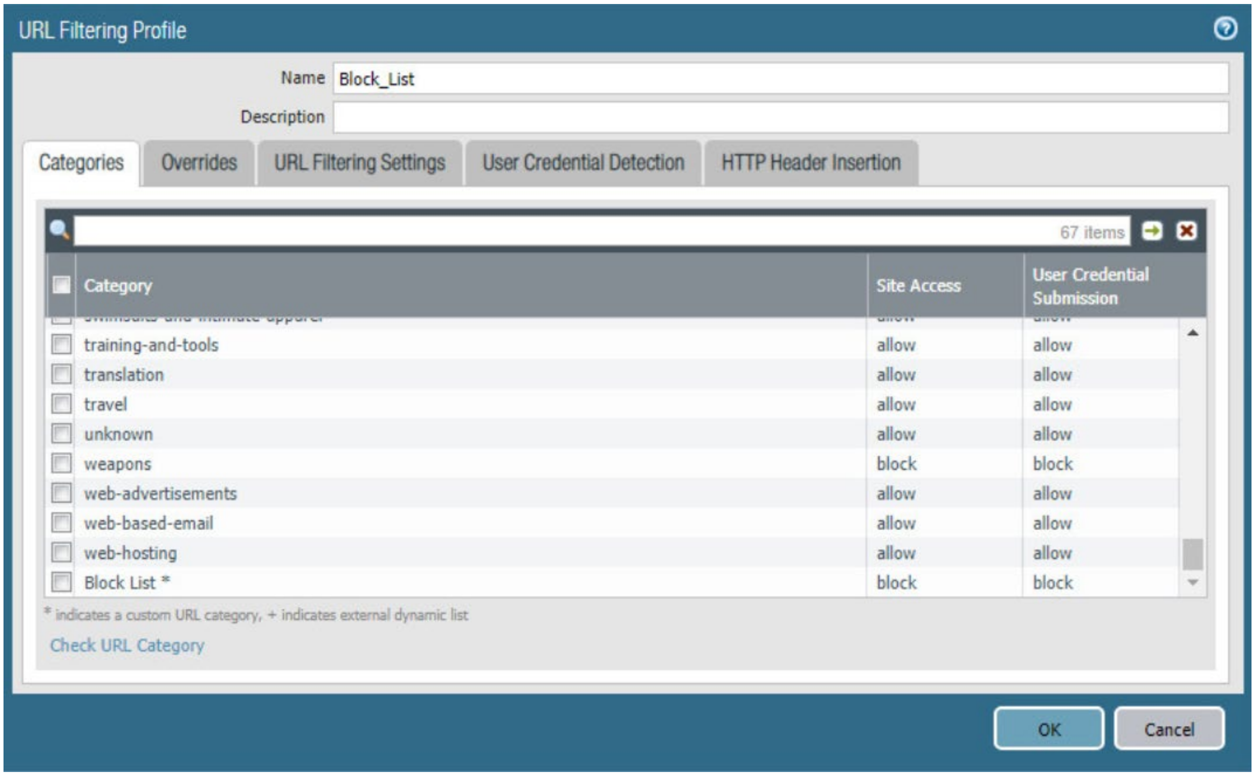
7. Click **Add**.

8. Give the filtering profile a name.

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

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

Figure 2-22 URL Filtering Profile



Name: Block_List

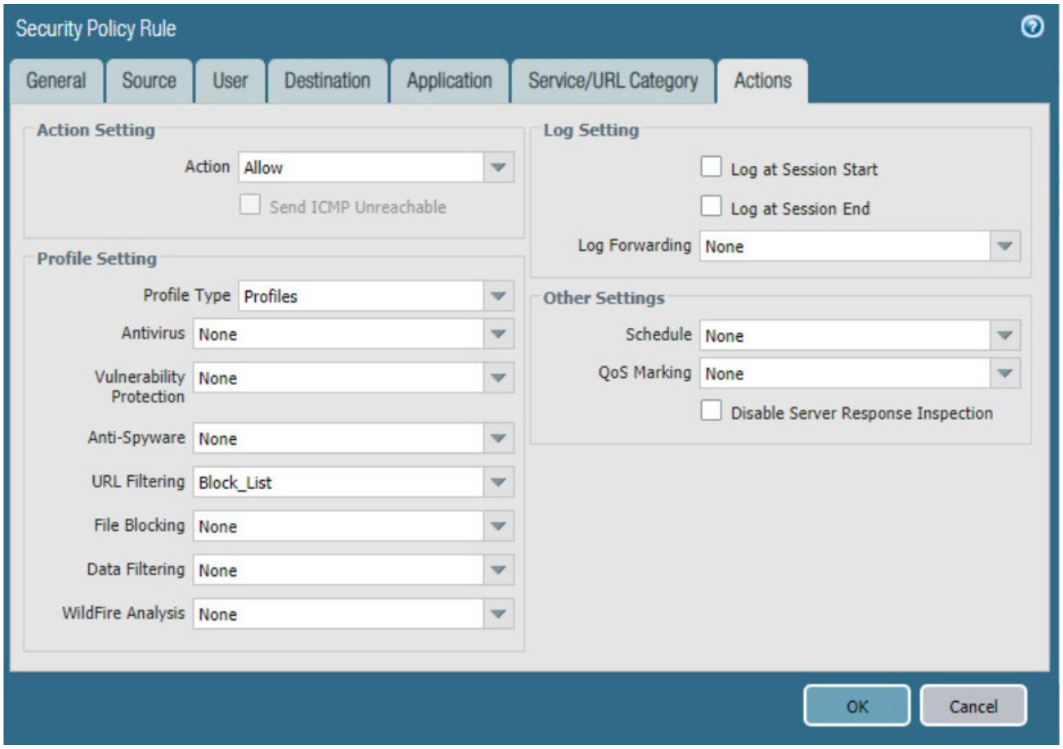
Description:

□	Category	Site Access	User Credential Submission
□	training-and-tools	allow	allow
□	translation	allow	allow
□	travel	allow	allow
□	unknown	allow	allow
□	weapons	block	block
□	web-advertisements	allow	allow
□	web-based-email	allow	allow
□	web-hosting	allow	allow
□	Block List *	block	block

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

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

Figure 2-23 URL Filtering Security Policy



Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

□ Log at Session Start

□ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: Block_List

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

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

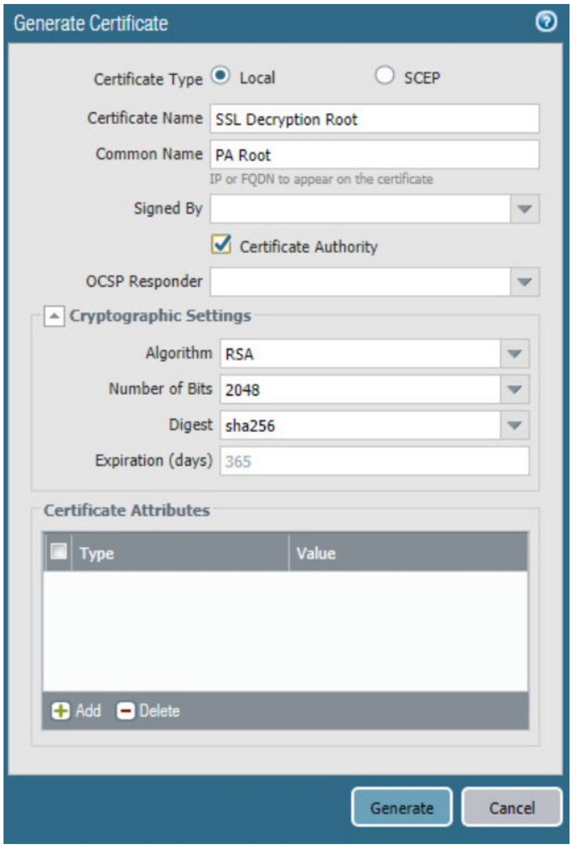
2.4.5.2 Configure SSL Website Blocking

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

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

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

Figure 2-24 Generating the Root CA



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: SSL Decryption Root

Common Name: PA Root

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate Authority

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

Digest: sha256

Expiration (days): 365

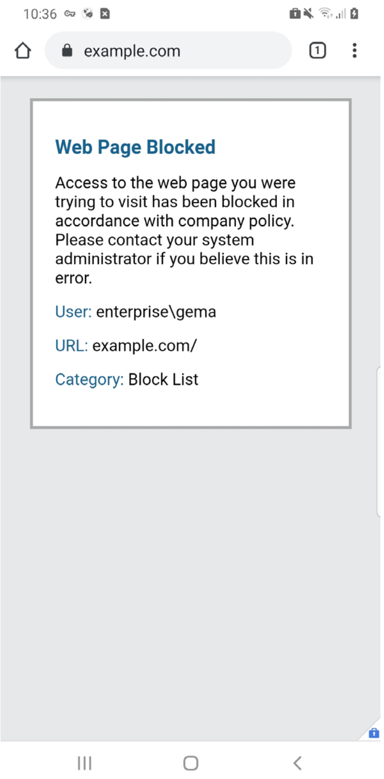
Certificate Attributes

□ Type	Value

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

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

Figure 2-25 Blocked Website Notification



Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: enterprise\gema

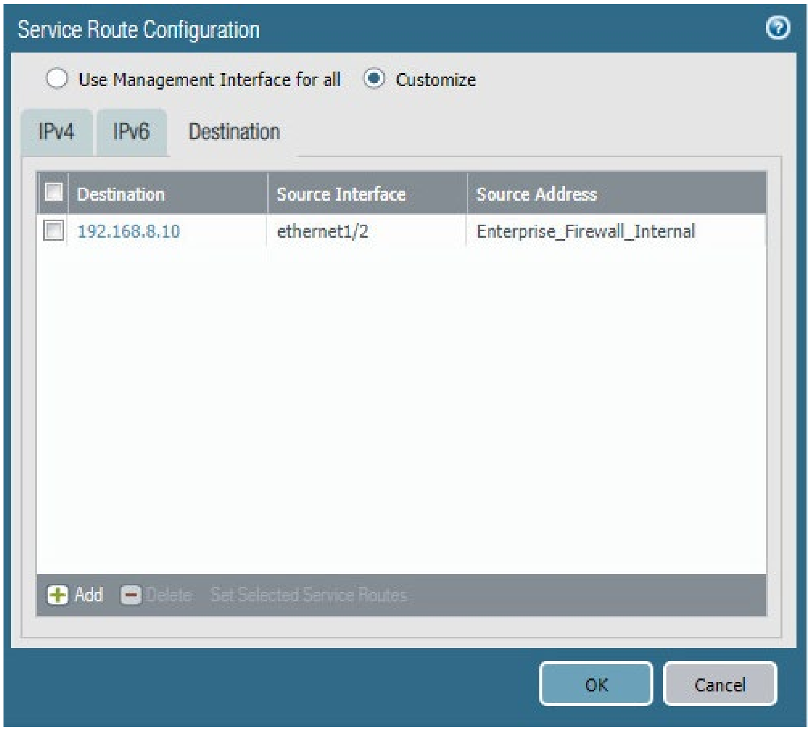
URL: example.com/

Category: Block List

2.4.6 User Authentication Configuration

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

Figure 2-26 Service Route Configuration



Service Route Configuration

○ Use Management Interface for all ● Customize

☐	Destination	Source Interface	Source Address
☐	192.168.8.10	ethernet1/2	Enterprise_Firewall_Internal

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

9. Click **Add**.

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

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

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

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

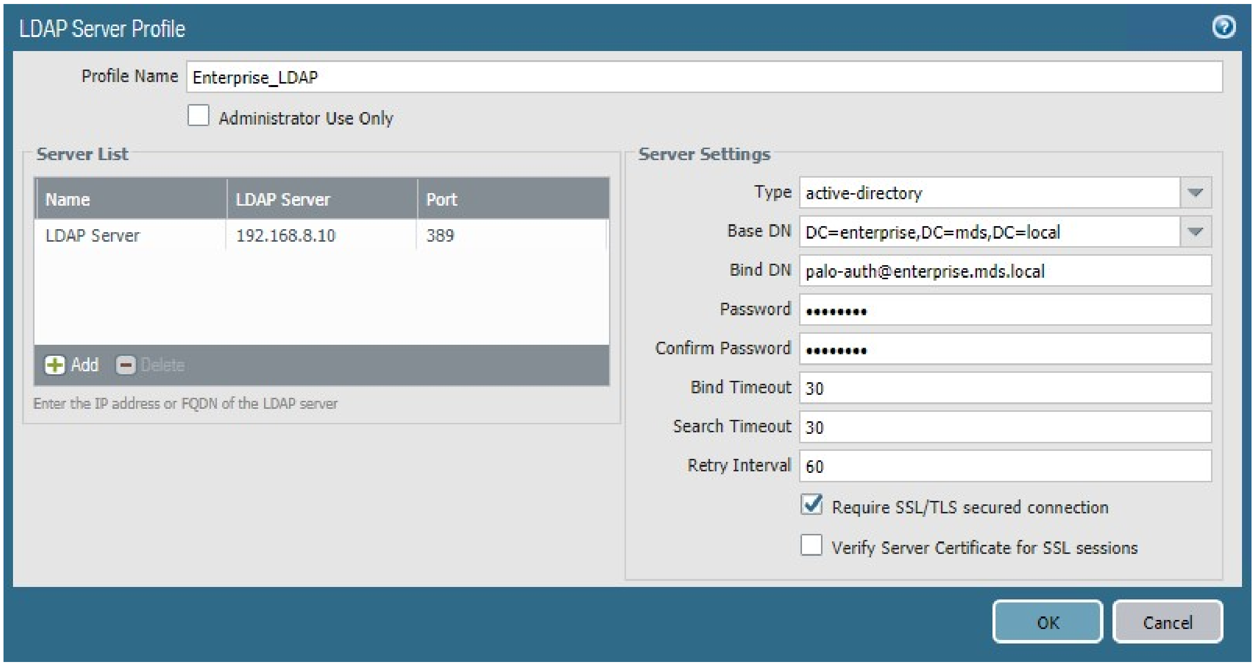
Note: In this implementation, a new user, palo-auth, was created in Active Directory. This user does not require any special permissions or groups beyond the standard Domain Users group.

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

15. Click the **down arrow** next to **Base DN**. If the connection is successful, the Base DN (Distinguished Name) should display.

16. Click **OK.**

Figure 2-27 LDAP Server Profile



LDAP Server Profile

Profile Name: Enterprise_LDAP

□ Administrator Use Only

Server List

Name	LDAP Server	Port
LDAP Server	192.168.8.10	389

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

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

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

Password: ••••••••

Confirm Password: ••••••••

Bind Timeout: 30

Search Timeout: 30

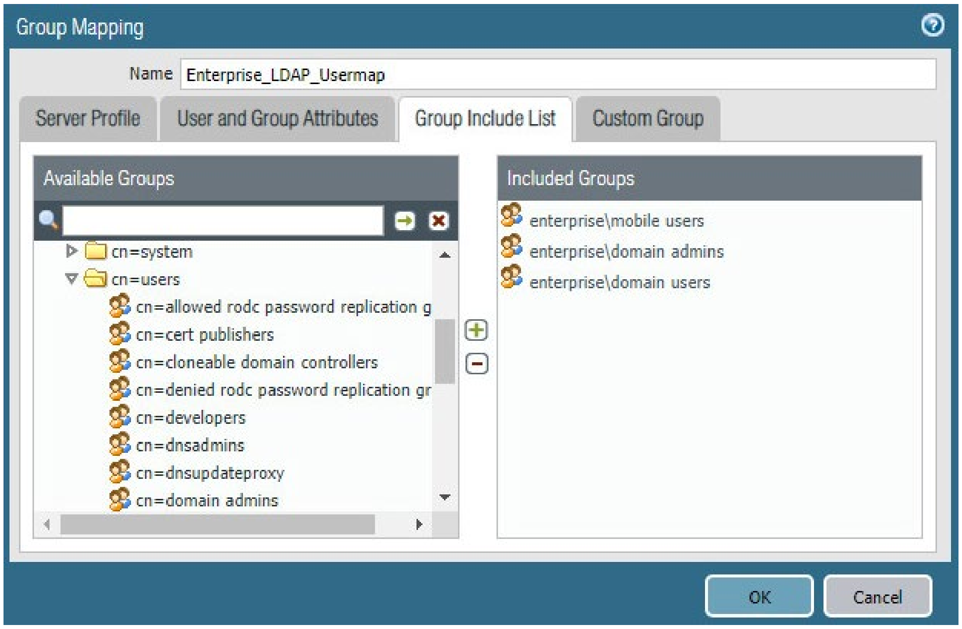
Retry Interval: 60

☑ Require SSL/TLS secured connection

□ Verify Server Certificate for SSL sessions

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

Figure 2-28 LDAP Group Mapping



Name Enterprise_LDAP_Usermap

Available Groups:

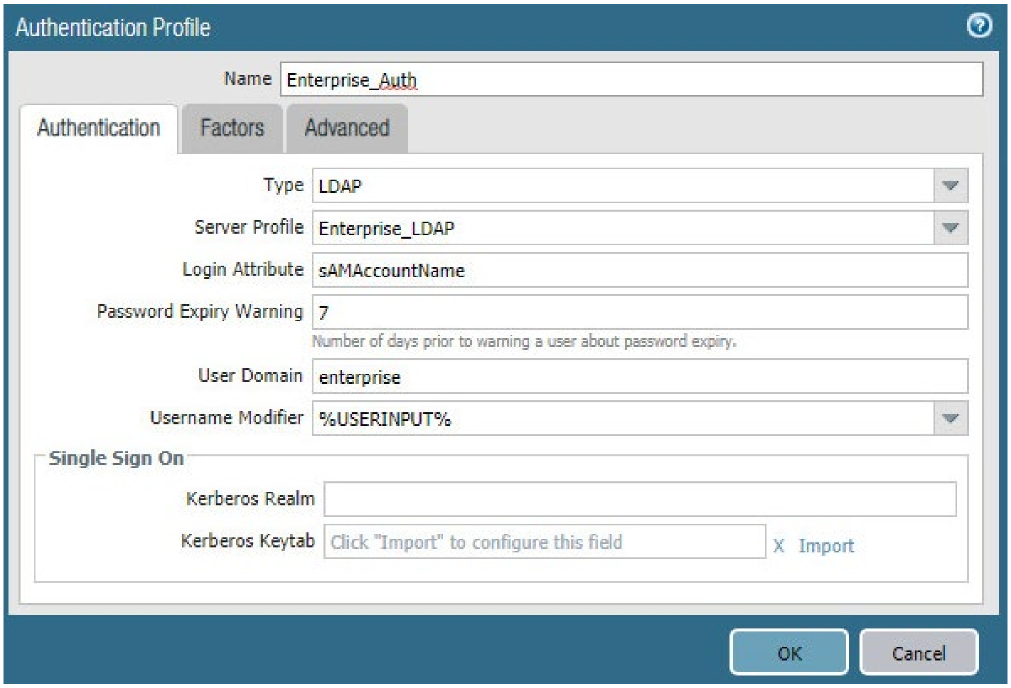
- cn=system
- cn=users
  - cn=allowed rodc password replication g
  - cn=cert publishers
  - cn=cloneable domain controllers
  - cn=denied rodc password replication gr
  - cn=developers
  - cn=dnsadmins
  - cn=dnsupdateproxy
  - cn=domain admins

Included Groups:

- enterprise\mobile users
- enterprise\domain admins
- enterprise\domain users

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

Figure 2-29 LDAP User Authentication Profile



Name: Enterprise_Auth

Type: LDAP

Server Profile: Enterprise_LDAP

Login Attribute: sAMAccountName

Password Expiry Warning: 7

Number of days prior to warning a user about password expiry.

User Domain: enterprise

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

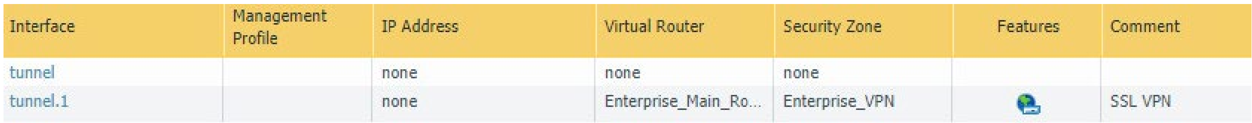
Kerberos Keytab: Click "Import" to configure this field X Import

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

2.4.7 VPN Configuration

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

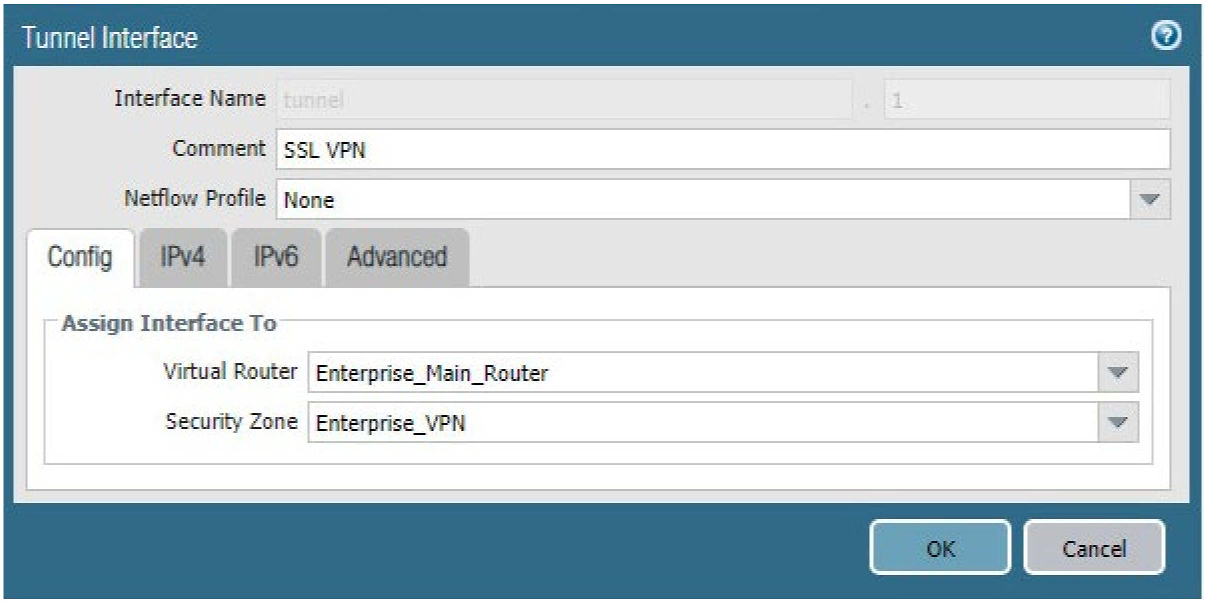
Figure 2-30 Configured Tunnel Interfaces



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

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



Tunnel Interface

Interface Name: tunnel . 1

Comment: SSL VPN

Netflow Profile: None

Assign Interface To

Virtual Router: Enterprise_Main_Router

Security Zone: Enterprise_VPN

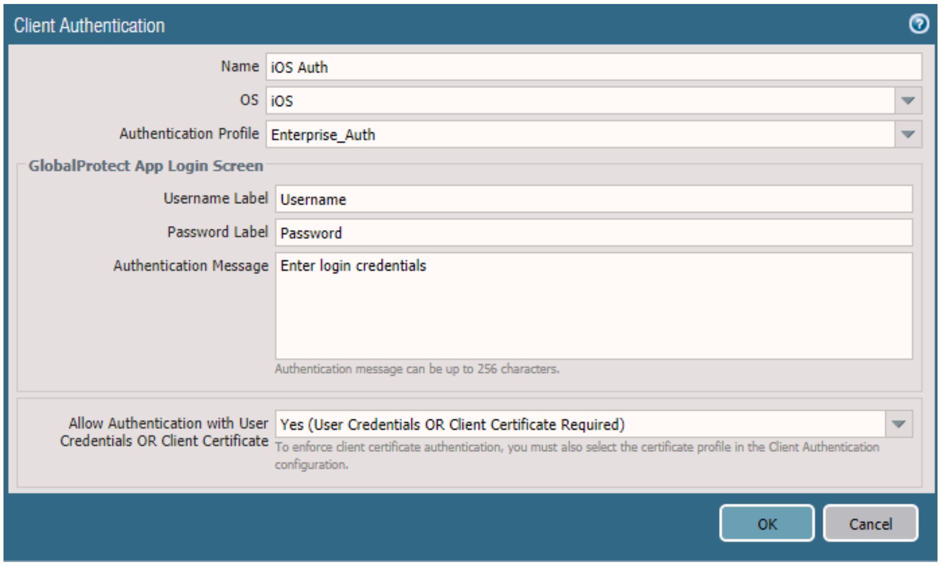
7. Commit the changes.
8. Navigate to **Policies > Authentication**.
9. Click **Add**.
10. Give the policy a **descriptive name**. For this example, the rule was named VPN_Auth.
11. Click **Source**.
12. Click **Add**, and add the VPN and WAN zones.
13. Click **Destination**.
14. Check the **Any** box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

18. Next to **Authentication Enforcement,** select **default-web-form**.
19. Click **OK**.

2.4.7.1 Configure the GlobalProtect Gateway

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

Figure 2-32 GlobalProtect iOS Authentication Profile



Client Authentication

Name: iOS Auth

OS: iOS

Authentication Profile: Enterprise_Auth

GlobalProtect App Login Screen

Username Label: Username

Password Label: Password

Authentication Message: Enter login credentials

Authentication message can be up to 256 characters.

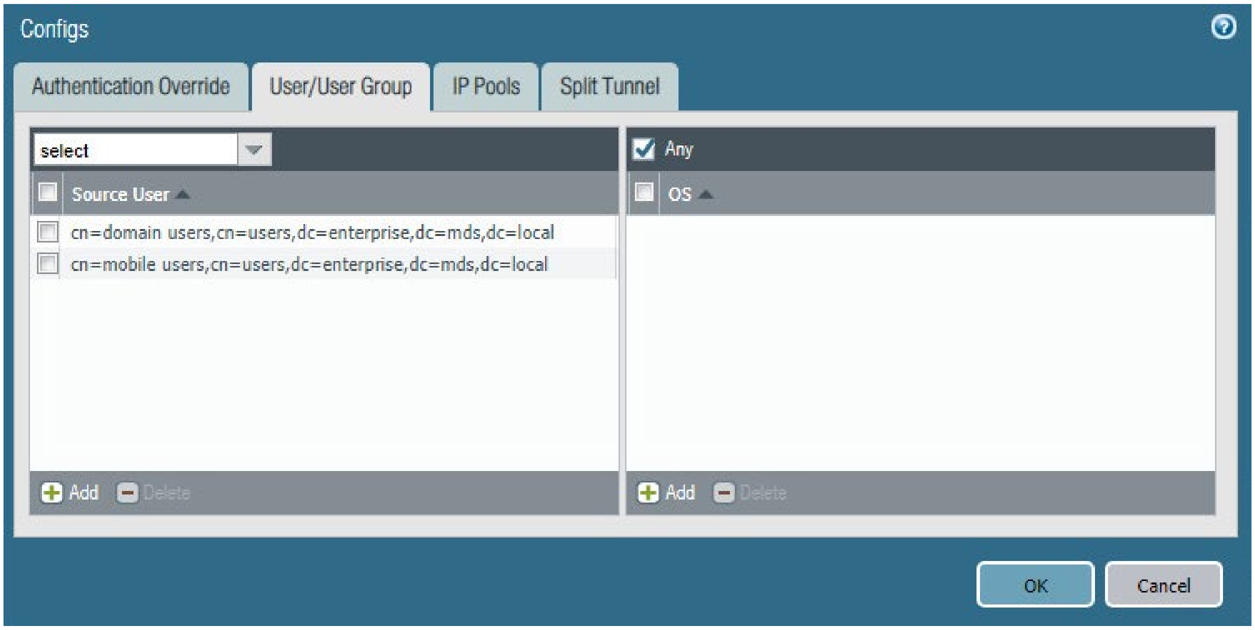
Allow Authentication with User Credentials OR Client Certificate: Yes (User Credentials OR Client Certificate Required)

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

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

29. Click **Add**.
30. Give the config a meaningful name, such as Enterprise_Remote_Access.
31. Click **User/User Group**.
32. Click **Add** under **Source User**.
33. Enter the **LDAP information** of the group allowed to use this rule. In this example, implementation, domain users, and mobile users were used.

Figure 2-33 LDAP Authentication Group Configuration



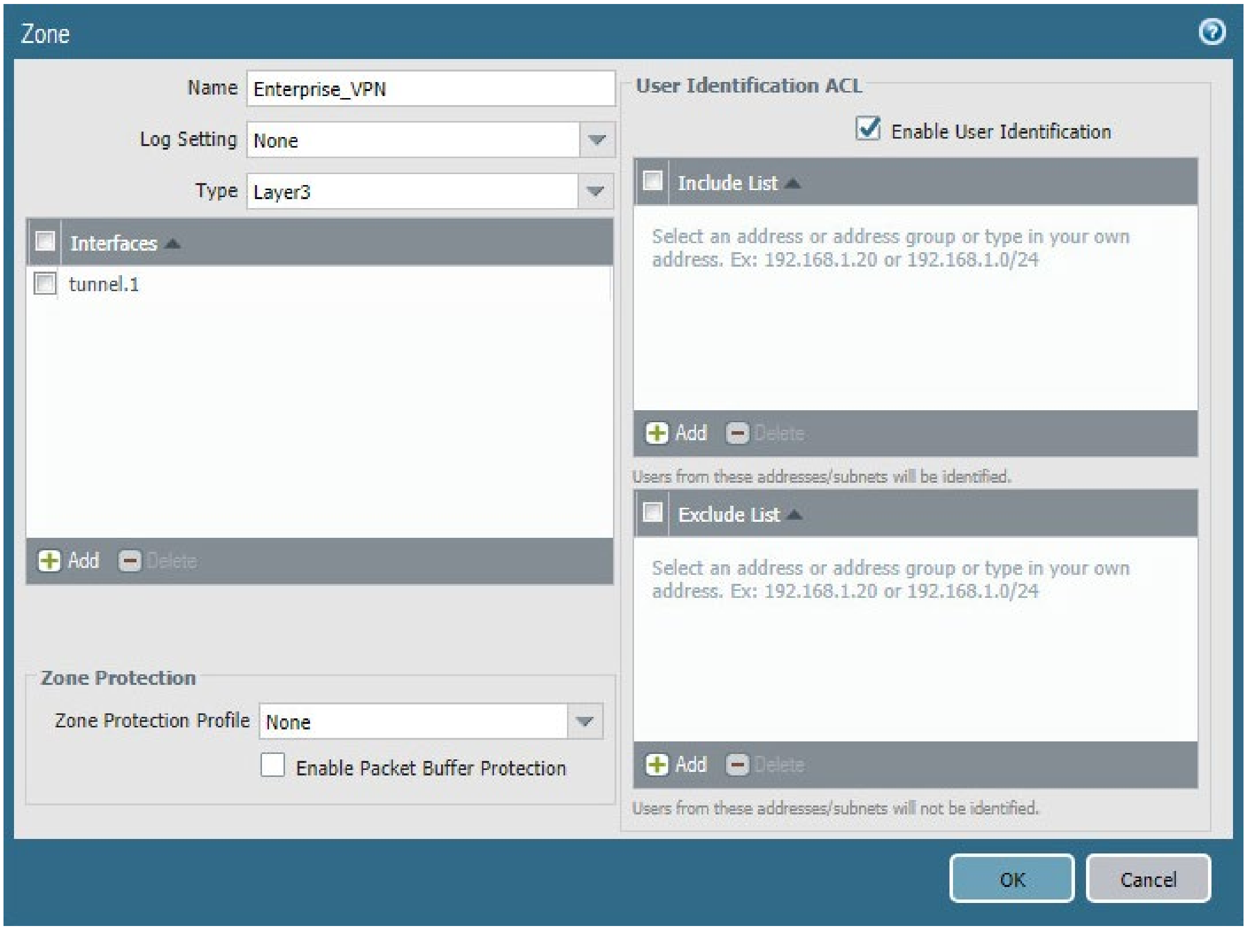
□ cn=domain users,cn=users,dc=enterprise,dc=mds,dc=local
□ cn=mobile users,cn=users,dc=enterprise,dc=mds,dc=local

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



Zone

Name: Enterprise_VPN

Log Setting: None

Type: Layer3

☐	Interfaces ▲
☐	tunnel.1

➕ Add ⊖ Delete

Zone Protection

Zone Protection Profile: None

☐ Enable Packet Buffer Protection

User Identification ACL

☑ Enable User Identification

☐ Include List ▲

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

➕ Add ⊖ Delete

Users from these addresses/subnets will be identified.

☐ Exclude List ▲

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

➕ Add ⊖ Delete

Users from these addresses/subnets will not be identified.

OK Cancel

44. Click **OK**.

45. Commit the changes.

2.4.7.2 Configure the GlobalProtect Portal

1. Navigate to **Network > GlobalProtect > Portals**.

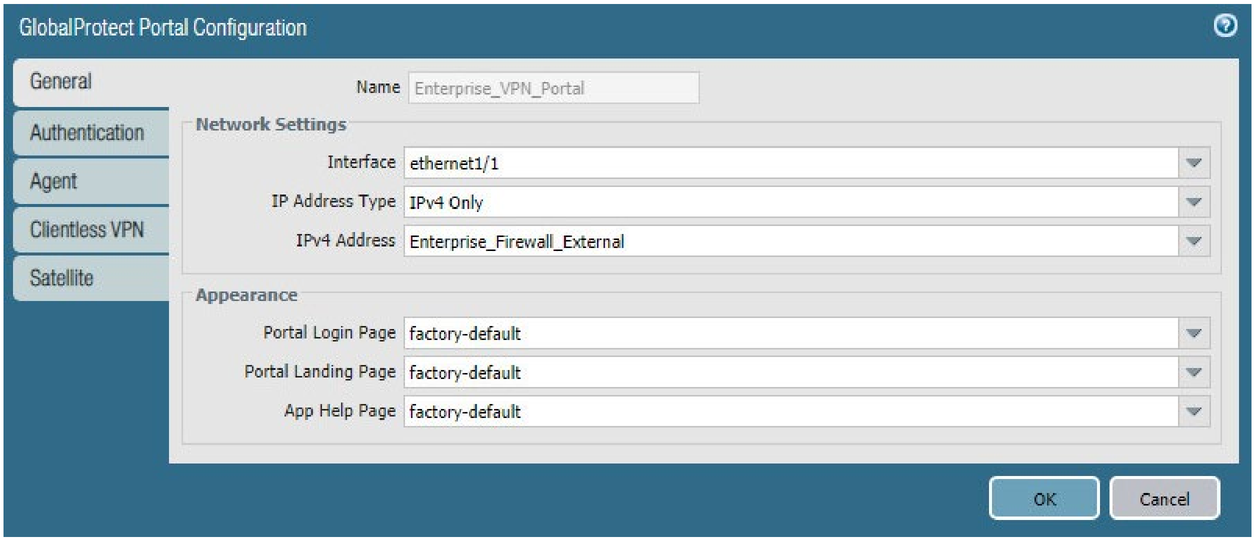
2. Click **Add**.

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



GlobalProtect Portal Configuration

Name: Enterprise_VPN_Portal

Network Settings

Interface: ethernet1/1

IP Address Type: IPv4 Only

IPv4 Address: Enterprise_Firewall_External

Appearance

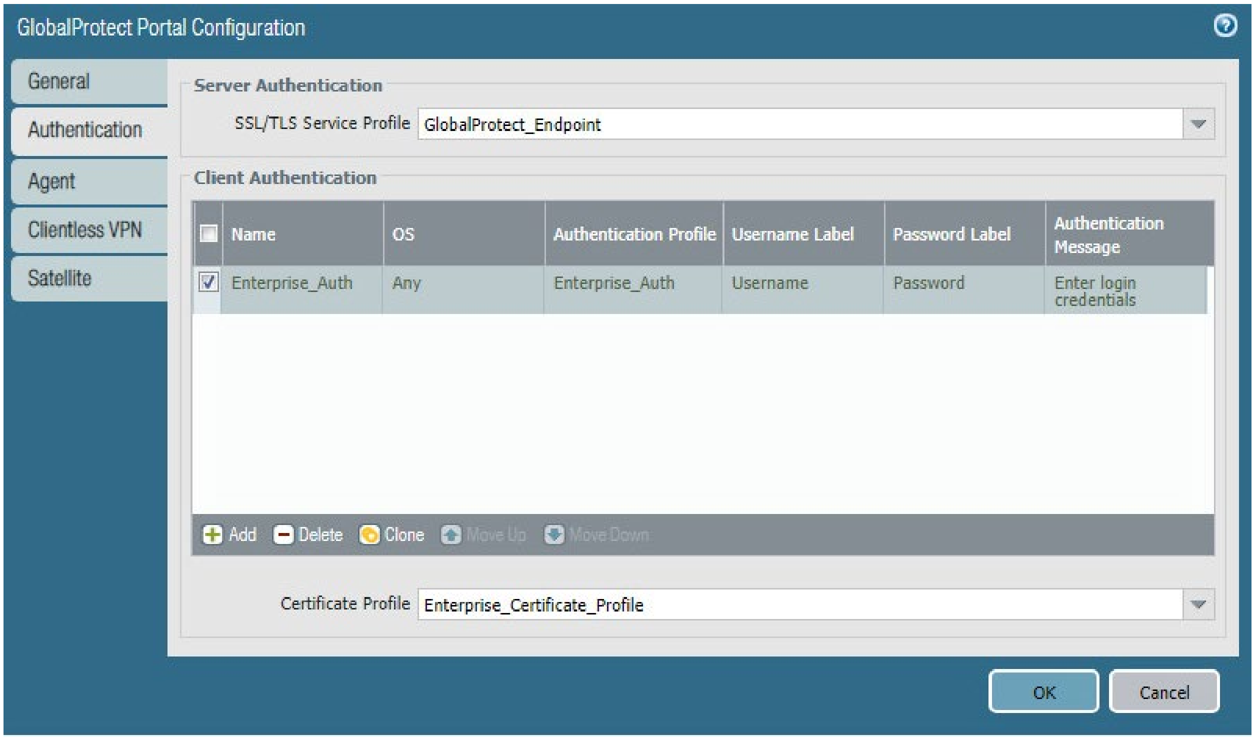
Portal Login Page: factory-default

Portal Landing Page: factory-default

App Help Page: factory-default

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**



GlobalProtect Portal Configuration

Server Authentication

SSL/TLS Service Profile: GlobalProtect_Endpoint

Client Authentication

☐	Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message
☑	Enterprise_Auth	Any	Enterprise_Auth	Username	Password	Enter login credentials

Certificate Profile: Enterprise_Certificate_Profile

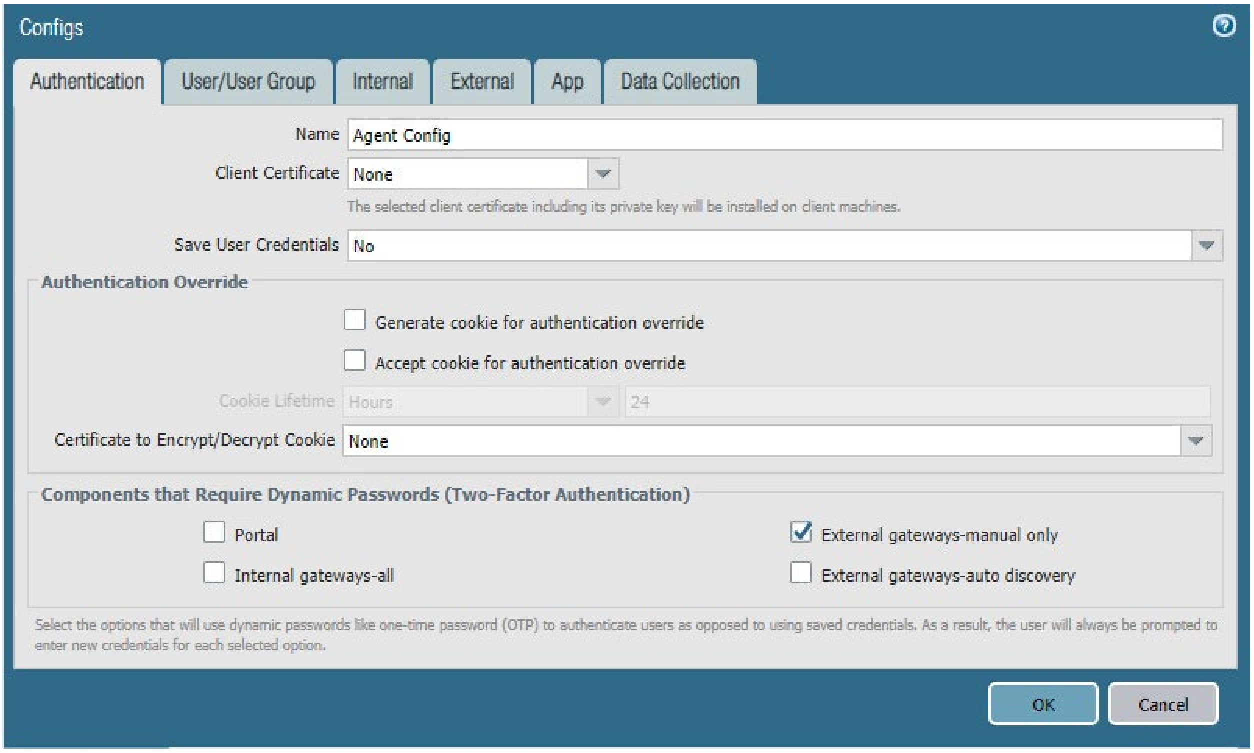
976 14. Click **Agent**, and click **Add** under **Agent**.

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**.

Figure 2-37 GlobalProtect Portal Agent Authentication Configuration



Configs

Name: Agent Config

Client Certificate: None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials: No

Authentication Override

□ Generate cookie for authentication override

□ Accept cookie for authentication override

Cookie Lifetime: Hours 24

Certificate to Encrypt/Decrypt Cookie: None

Components that Require Dynamic Passwords (Two-Factor Authentication)

□ Portal ☑ External gateways-manual only

□ Internal gateways-all □ External gateways-auto discovery

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

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

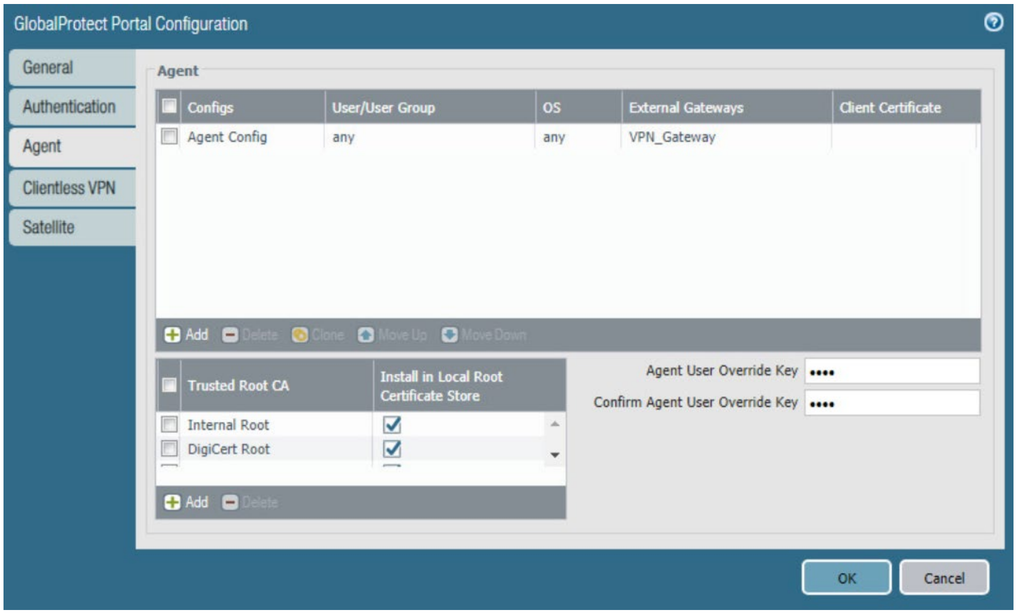
29. Select the **internal root certificate** used to generate device certificates.

30. Click **Add** again. Select the **root certificate** used to create the VPN end-point SSL certificate. For this implementation, it is a DigiCert root certificate.

31. Click **Add** again. Select the **root certificate** used for SSL URL filtering, created in a previous section.

32. Check the box next to **Install in Local Root Certificate Store** for all three certificates.

Figure 2-38 GlobalProtect Portal Agent Configuration



Agent

Configs	User/User Group	OS	External Gateways	Client Certificate
□ Agent Config	any	any	VPN_Gateway	

Trusted Root CA	Install in Local Root Certificate Store
□ Internal Root	☑
□ DigiCert Root	☑

Agent User Override Key ••••

Confirm Agent User Override Key ••••

33. Click **OK.**

2.4.7.3 Activate Captive Portal

1. Navigate to **Device > User Identification > Captive Portal Settings**.

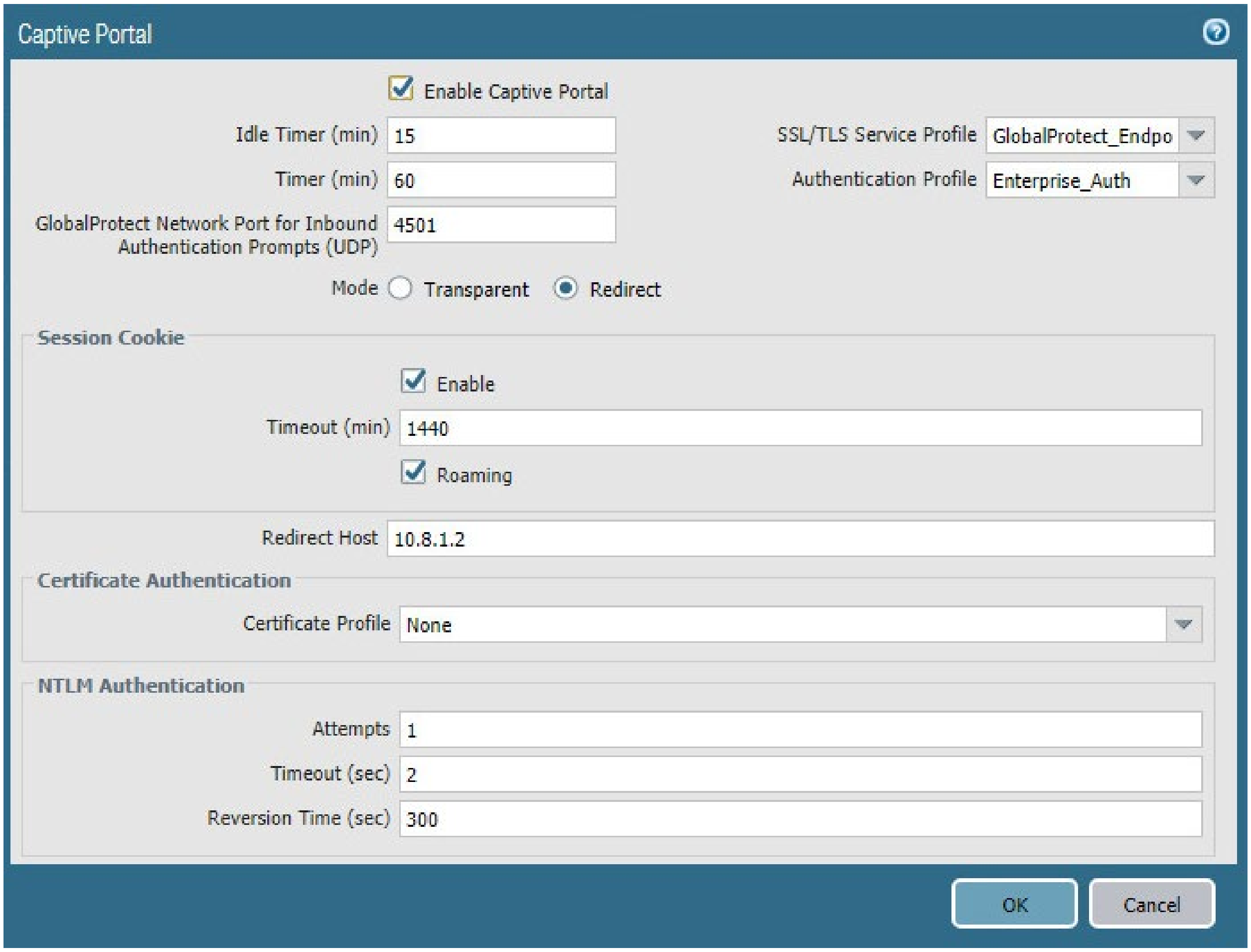
2. Click the **gear** icon on the top right of the Captive Portal box.

3. Select the **created SSL/TLS service profile and authentication profile**.

4. Click the radio button next to **Redirect**.

5. Next to **Redirect Host,** enter the **IP address** of the firewall’s WAN interface—in this case, **10.8.1.2**.

Figure 2-39 Captive Portal Configuration



Captive Portal

☑ Enable Captive Portal

Idle Timer (min) 15

Timer (min) 60

GlobalProtect Network Port for Inbound Authentication Prompts (UDP) 4501

Mode ○ Transparent ● Redirect

SSL/TLS Service Profile GlobalProtect_Endpo

Authentication Profile Enterprise_Auth

Session Cookie

☑ Enable

Timeout (min) 1440

☑ Roaming

Redirect Host 10.8.1.2

Certificate Authentication

Certificate Profile None

NTLM Authentication

Attempts 1

Timeout (sec) 2

Reversion Time (sec) 300

6. Click **OK**.

7. Commit the changes.

2.4.7.4 Activate the GlobalProtect Client

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

2. Acknowledge pop up messages.

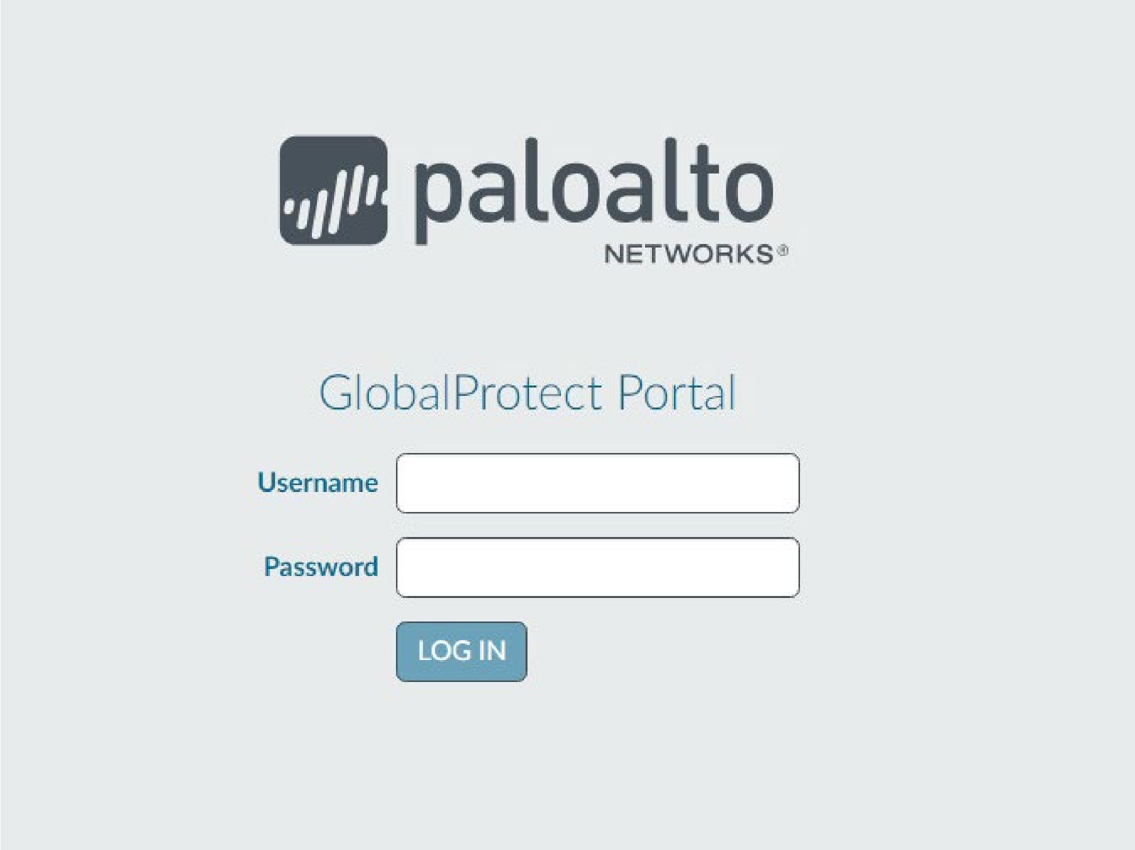
3. Click **Check Now** at the bottom of the page.

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

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

6. Navigate to the FQDN of the VPN. You should see the Palo Alto Networks logo and the GlobalProtect portal login prompt, potentially with a message indicating that a required certificate cannot be found. This is expected on desktops because there is nothing in place to seamlessly deploy client certificates.

Figure 2-40 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.

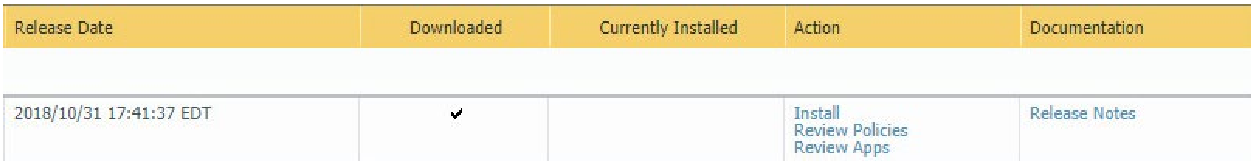
2.4.8 Enable Automatic Application and Threat Updates

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



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

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

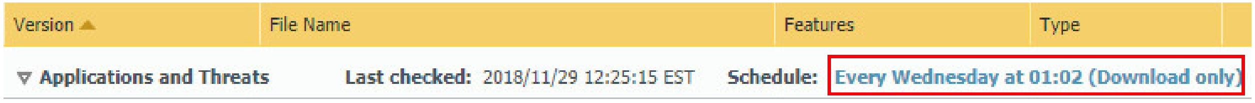
   e. Click **Continue Installation,** leaving the displayed box unchecked. Installation will take a few minutes.

   f. When the installation completes, click **Close.**

3. Enable automatic threat updates. (Note: Automatic threat updates are performed in the background and do not require a reboot of the appliance.)

   a. At the top of the page, next to **Schedule,** click the hyperlink with the date and time, as shown in Figure 2-42.

Figure 2-42 Schedule Time Hyperlink



Version ▲	File Name	Features	Type

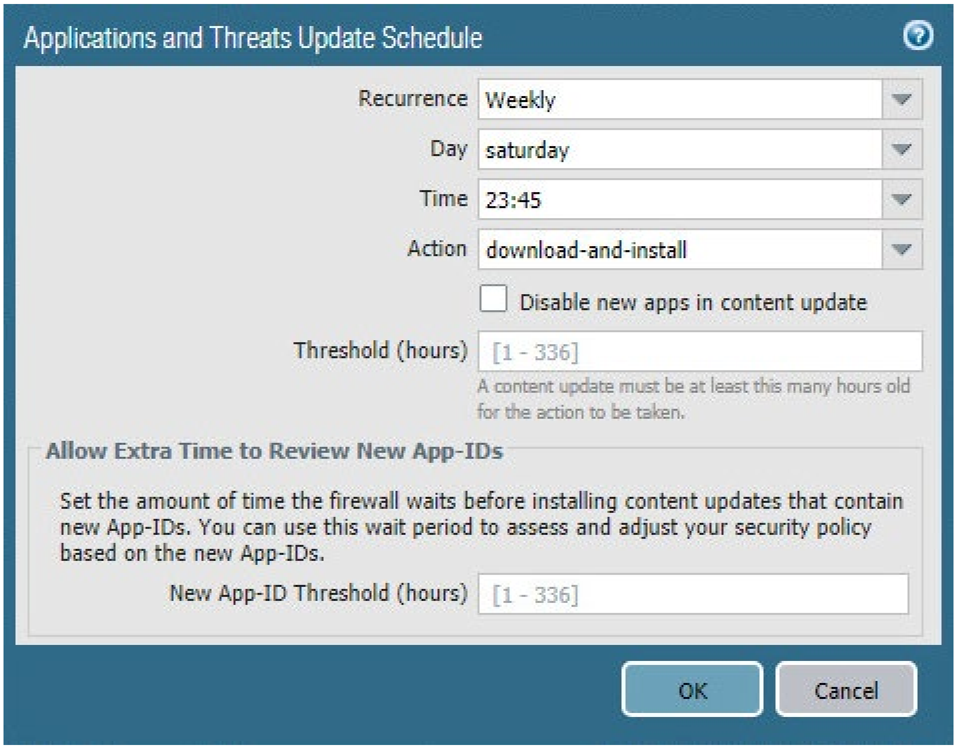
▽ **Applications and Threats** **Last checked:** 2018/11/29 12:25:15 EST **Schedule:** Every Wednesday at 01:02 (Download only)

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

   c. Select the **desired day and time** for the update to occur. For this implementation, Saturday at 23:45 was used.

   d. Next to **Action,** select **download-and-install.**

Figure 2-43 Application and Threats Update Schedule



Applications and Threats Update Schedule

Recurrence: Weekly

Day: saturday

Time: 23:45

Action: download-and-install

□ Disable new apps in content update

Threshold (hours): [1 - 336]

A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours): [1 - 336]

e. Click **OK.**

f. Commit the changes.

2.5 Kryptowire

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

2.5.1 Kryptowire and MaaS360 Integration

1. Contact IBM support to provision API credentials for Kryptowire.
2. Contact Kryptowire support to enable the MaaS360 integration, including the MaaS360 API credentials.
3. In the Kryptowire portal, click the **logged-in user's email address** in the upper right-hand corner of the portal. Navigate to **Settings > Analysis**.
4. Set the **Threat Score Threshold** to the desired amount. In this sample implementation, 75 was used.

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

Appendix A List of Acronyms

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.