



Check for updates

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

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

September 2023

FINAL

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



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)*

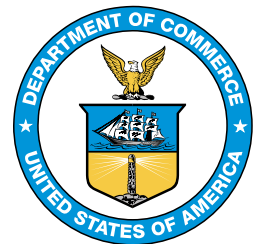
Kaitlin Boeckl  
Nakia Grayson  
Gema Howell  
Naomi Lefkowitz  
*Applied Cybersecurity Division  
Information Technology Laboratory*

Jason Ajmo  
R. Eugene Craft  
Milissa McGinnis\*  
Kenneth Sandlin  
Oksana Slivina  
Julie Snyder  
Paul Ward  
*The MITRE Corporation  
McLean, VA*

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

FINAL

September 2023



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

National Institute of Standards and Technology  
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

# 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 Ajmo**

**R. Eugene Craft**

**Milissa McGinnis\***

**Kenneth Sandlin**

**Oksana Slivina**

**Julie Snyder**

**Paul Ward**

The MITRE Corporation  
McLean, VA

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

September 2023

FINAL

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



# Executive Summary

Many organizations 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 National Institute of Standards and Technology (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 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 associated 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
- **engage stakeholders** to develop an enterprise-wide policy to inform management and employees of acceptable practices

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
<a href="#">IBM</a>	Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance
<a href="#">Kryptowire</a> (now known as Quokka)	Application Vetting to determine if an application demonstrates behaviors that could pose a security or privacy risk
<a href="#">Palo Alto Networks</a>	Firewall and Virtual Private Network that controls network traffic and provides encrypted communication channels between mobile devices and other hosts
<a href="#">Qualcomm</a>	Trusted Execution Environment that helps protect mobile devices from computer code with integrity issues
<a href="#">Zimperium</a>	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

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

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](mailto: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.

# Mobile Device Security:

## Bring Your Own Device (BYOD)

---

**Volume B:**  
**Approach, Architecture, and Security Characteristics**

**Kaitlin Boeckl**

**Nakia Grayson**

**Gema Howell**

**Naomi Lefkowitz**

Applied Cybersecurity Division  
Information Technology Laboratory

**Jason Ajmo**

**R. Eugene Craft**

**Milissa McGinnis\***

**Kenneth Sandlin**

**Oksana Slivina**

**Julie Snyder**

**Paul Ward**

The MITRE Corporation  
McLean, VA

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

September 2023

FINAL

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



## DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-22B Natl. Inst. Stand. Technol. Spec. Publ. 1800-22B, 88 pages, (September 2023), CODEN: NSPUE2

## FEEDBACK

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

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

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

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

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution

## ABSTRACT

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

Incorporating BYOD deployments into an organization can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of traditional in-office processes with mobile device technologies enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-first approach in which their employees communicate and collaborate primarily using their mobile devices.

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

Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks. Solutions that are designed to secure corporate devices and on-premises data do not provide an effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new privacy risks to employees by providing their employer a degree of access to their personal devices, opening up the possibility of observation and control that would not otherwise exist.

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

Name	Organization
William Newhouse	NIST
Cherilyn Pascoe	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST
Chris Brown	The MITRE Corporation
Nancy Correll*	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston*	The MITRE Corporation
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Jessica Walton	The MITRE Corporation
Erin Wheeler*	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward*	IBM
Cesare Coscia*	IBM
Chris Gogoel	Kryptowire (now known as Quokka)
Tom Karygiannis*	Kryptowire (now known as Quokka)
Jeff Lamoureux	Palo Alto Networks
Sean Morgan	Palo Alto Networks



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

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

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

Technology Partner/Collaborator	Build Involvement
IBM	Mobile Device Management
Kryptowire (now known as Quokka)	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

## DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

## PATENT DISCLOSURE NOTICE

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

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

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

# Contents

<b>1</b>	<b>Summary</b>	<b>1</b>
1.1	Challenge	1
1.2	Solution	3
1.2.1	Standards and Guidance	4
1.2.2	Benefits of this Example Solution	4
<b>2</b>	<b>How to Use This Guide</b>	<b>5</b>
2.1	Typographic Conventions	6
<b>3</b>	<b>Approach</b>	<b>7</b>
3.1	Audience	7
3.2	Scope	8
3.3	Assumptions	8
3.4	Risk Assessment	9
3.4.1	Security Threats	9
3.4.2	Vulnerabilities	10
3.4.3	Problematic Data Actions	10
3.4.4	Risks	10
3.5	Applying Risk Assessments to this BYOD Example Solution	10
<b>4</b>	<b>Architecture</b>	<b>11</b>
4.1	Common BYOD Risks and Potential Objectives to Remediate Those Risks	12
4.1.1	Threat Events	12
4.1.2	Privacy Risks	13
4.1.3	Security and Privacy Objectives	14
4.2	Example Scenario: Putting Guidance into Practice	15
4.3	Technologies that Support the Security and Privacy Objectives of the Example Solution	16
4.3.1	Trusted Execution Environment	16
4.3.2	Enterprise Mobility Management	16
4.3.3	Virtual Private Network	17
4.3.4	Mobile Application Vetting Service	18
4.3.5	Mobile Threat Defense	18
4.3.6	Mobile Operating System Capabilities	19

4.4	Architecture Description .....	21
4.5	Enterprise Integration of the Employees' Personally Owned Mobile Devices .....	22
4.5.1	Microsoft Active Directory Integration .....	23
4.5.2	Mobile Device Enrollment .....	24
4.6	Mobile Components Integration .....	25
4.6.1	Zimperium–MaaS360 .....	26
4.6.2	Kryptowire–MaaS360 .....	27
4.6.3	Palo Alto Networks–MaaS360 .....	27
4.6.4	iOS and Android MDM Integration .....	28
4.7	Privacy Settings: Mobile Device Data Processing .....	28
4.7.1	EMM: MaaS360 .....	28
4.7.2	MTD: Zimperium .....	30
4.7.3	Application Vetting: Kryptowire .....	31
4.7.4	VPN: Palo Alto Networks .....	32
<b>5</b>	<b>Security and Privacy Analysis .....</b>	<b>32</b>
5.1	Analysis Assumptions and Limitations .....	32
5.2	Build Testing .....	32
5.3	Scenarios and Findings .....	33
5.3.1	Cybersecurity Framework, Privacy Framework, and NICE Framework Work Roles Mappings .....	33
5.3.2	Threat Events and Findings .....	34
5.3.3	Privacy Risk Findings .....	35
<b>6</b>	<b>Example Scenario: Putting Guidance into Practice .....</b>	<b>37</b>
<b>7</b>	<b>Conclusion .....</b>	<b>37</b>
<b>8</b>	<b>Future Build Considerations .....</b>	<b>39</b>
<b>Appendix A</b>	<b>List of Acronyms .....</b>	<b>40</b>
<b>Appendix B</b>	<b>Glossary .....</b>	<b>42</b>
<b>Appendix C</b>	<b>References .....</b>	<b>44</b>
<b>Appendix D</b>	<b>Standards and Guidance .....</b>	<b>49</b>
<b>Appendix E</b>	<b>Example Security Subcategory and Control Map .....</b>	<b>51</b>
<b>Appendix F</b>	<b>Example Privacy Subcategory and Control Map .....</b>	<b>70</b>

# List of Figures

- Figure 3-1 Cybersecurity and Privacy Risk Relationship.....11
- Figure 4-1 Security and Privacy Objectives .....14
- Figure 4-2 iOS App Transport Security.....21
- Figure 4-3 Example Solution Architecture .....22
- Figure 4-4 Mobile Device Application Management and Benefits .....23
- Figure 4-5 Example Solution VPN Authentication Architecture .....25
- Figure 4-6 Data Collected by Example Solution Mobile Device Management.....29
- Figure 4-7 Example Solution Mobile Device Management Privacy Settings .....30
- Figure 7-1 Example Solution Architecture .....38

# List of Tables

- Table 4-1 Examples of BYOD Deployment Threats .....12
- Table 4-2: Example Privacy Risks and Problematic Data Actions .....13
- Table 4-3 Commercially Available Products Used .....25
- Table 5-1 Threat Events and Findings Summary .....34
- Table 5-2 Summary of Privacy Risks and Findings .....35
- Table E-1 Example Solution’s Cybersecurity Standards and Best Practices Mapping .....51
- Table F-1 Example Solution’s Privacy Standards and Best Practices Mapping .....71

# 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 iOS mobile device 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 them 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 device is used to describe an Apple iOS or Google Android phone or tablet. This practice guide's scope for BYOD does not include 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 security and privacy protections. Unmanaged devices are at greater risk of unauthorized access to sensitive information, tracking, 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 risk to the confidentiality, integrity, and availability of the enterprise's sensitive information**
  - posed by applications 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
  - that results from the increased value of employees' mobile devices due to enterprise data being present
- **Protecting the privacy of employees**
  - by helping to keep their personal photos, documents, location, 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 IT 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 and providing transparency 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 iOS mobile devices 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 understand 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.

### 1.2.2 Benefits of this Example Solution

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 BYOD 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 E](#), Example Security Subcategory and Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.
- [Appendix F](#), 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 that 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 Objectives 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 a volume titled NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice*, which explores 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](mailto:mobile-nccoe@nist.gov).

Acronyms used in figures can be found in [Appendix A](#), List of Acronyms.

## 2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

### 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 potential 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 devices. 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](#) of this document for how different audiences can effectively use this guide.

## 3.2 Scope

The scope of this build includes managing iOS or Android mobile devices 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 (e.g., an employee's family members) 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, *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.

Our BYOD risk assessments helped to identify and mitigate potential security threats, vulnerabilities, problematic data actions, and risks. The following sections define these terms.

#### 3.4.1 Security Threats

NIST SP 800-30 Revision 1 defines a threat as “any circumstance or event with the potential to adversely impact organizational operations and 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”. Threats are actions that may compromise a system’s confidentiality, integrity, or availability [8]. Threats evolve, and an organization needs to perform its own analysis when evaluating threats and risks that the organization faces.

### 3.4.2 Vulnerabilities

As defined in NIST SP 800-30 Revision 1, a vulnerability is a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source” [8]. Vulnerabilities may exist in a broader context. That is, they may be found in organizational governance structures, external relationships, and mission/business processes.

### 3.4.3 Problematic Data Actions

This build considered operational activities of the example solution that interact with employee data during architectural processes (“data actions”) and identified those that potentially cause problems to individuals (“problematic data actions”).

The NIST Privacy Framework defines a problematic data action as “a data action that could cause an adverse effect for individuals.” [9] Problematic data actions can result in privacy risk to individuals and prevent an organization from developing a solution that meets the privacy engineering objectives of:

- predictability: enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service
- manageability: providing the capability for granular administration of data, including alteration, deletion, and selective disclosure
- disassociability: enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

An organization should perform a risk assessment to determine contextual application of the problematic data actions. The discussion about problematic data actions and risks in Appendix G of the Great Seneca Supplement introduces the PRAM and provides a more detailed analysis of the privacy risks in this build.

### 3.4.4 Risks

As noted in Section 3.4, NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, defines risk as “a measure of the extent to which an entity is threatened by potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” [8]

Risk is the adverse impact or the result when a threat (attack) successfully leverages one or more vulnerabilities. As organizations consider risk, they should note that risk is not discreet. One may realize multiple risks based on a successful attack. And, those attacks may involve strictly cybersecurity threat events, the realization of privacy risks, or both.

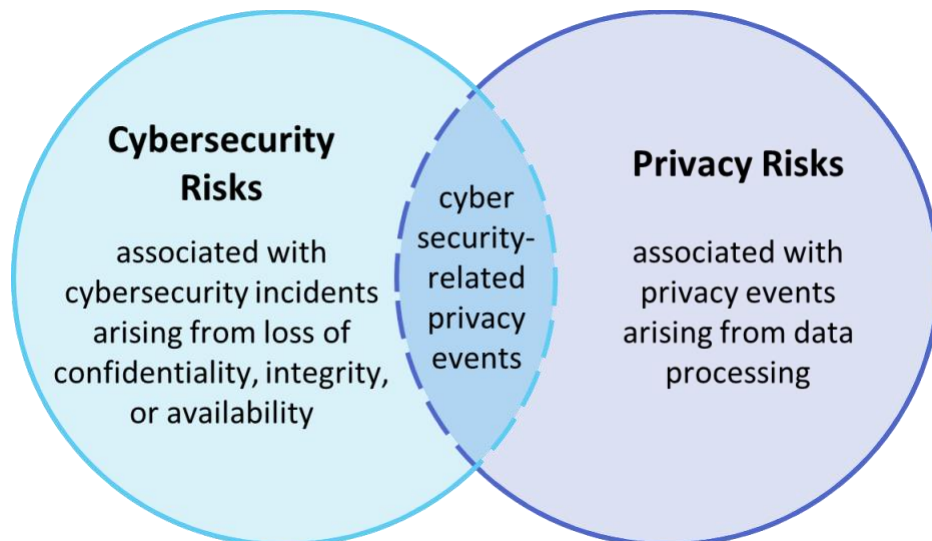
## 3.5 Applying Risk Assessments to this BYOD Example Solution

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.

Figure 3-1 Cybersecurity and Privacy Risk Relationship



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) [9] 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 might include the following additional analysis areas. For more information on the example solution risk methodology employed for this BYOD example solution, see the referenced sections:

- **Security threats and objectives to remediate those threats**, see [Section 4.1](#)
- **Data actions** that introduce privacy problems (i.e., problematic data actions) and the methods to address those problems, see Section 4.1 and Appendix G of the Supplement
- **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 Great Seneca Supplement
- **Security and Privacy Control Mapping** to cybersecurity and privacy standards and best practices, see [Appendix E](#) and [Appendix F](#) in this volume

## 4 Architecture

This section helps familiarize the reader with:

- threats to BYOD architectures



- example solution methods 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 objectives
- the example solution’s architecture
- how the example solution’s products were integrated
- mobile device data collection

## 4.1 Common BYOD Risks and Potential Objectives to Remediate Those Risks

This section contains examples of common security and privacy risks in BYOD deployments. We provide a list of objectives to manage those risks. Once completed, the example solution’s architecture provides organizations with a security and privacy-enhanced design that can be leveraged for the BYOD deployments of mobile devices. The challenges addressed by the example solution’s and risk remediation objectives are highlighted below, followed by the architecture that supports those objectives.

### 4.1.1 Threat Events

Leveraging a system life cycle approach [10], this build considered threats relating to BYOD deployments. Information from the Open Web Application Security Project Mobile Top 10 [11], 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 TEs 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.

The threat events are also used in Appendix F in the 1800-22 Supplement to identify relevant mobile threats in the example scenario and Appendix D in 1800-22 Volume C to test the security characteristics of the lab build.

**Table 4-1 Examples of BYOD Deployment Threats**

Threat Event ID	Threat Event Description	NIST Mobile Threat Catalogue Threat ID
TE-1	Intrusive application practices	APP-2, APP-12
TE-2	Account credential theft through phishing	AUT-9
TE-3	Outdated phones	APP-4, APP-26, STA-0, STA-9, STA-16

Threat Event ID	Threat Event Description	NIST Mobile Threat Catalogue Threat ID
TE-4	Sensitive data transmissions	APP-0, CEL-18, LPN-2
TE-5	Brute-force attacks to unlock a phone	AUT-2, AUT-4
TE-6	Application credential storage vulnerability	APP-9, AUT-0
TE-7	Unmanaged device protection	EMM-5
TE-8	Lost or stolen data protection	PHY-0
TE-9	Protecting enterprise data from being inadvertently backed up to a cloud service	EMM-9

### 4.1.2 Privacy Risks

In addition to the TEs just discussed, this practice guide’s example solution also considers and helps mitigate privacy risks that can apply to BYOD deployments. Privacy risks for individuals can present themselves through problematic data actions. The NIST Privacy Framework defines a problematic data action as “a data action that could cause an adverse effect for individuals.” [2] Example problematic data actions are shown in the table below:

Table 4-2: Example Privacy Risks and Problematic Data Actions

Privacy Risk ID	Description	Problematic Data Action
PR-1	Wiping Activities on the Employee’s Device May Inadvertently Delete the Employee’s Personal Data	Unwarranted Restriction
PR-2	Organizational Collection of Device Data May Subject Employees to Feeling of Being Surveilled	Surveillance
PR-3	Data Collection and Transmission Between Integrated Security Products May Expose Employee Data	Unanticipated Revelation
PR-4	Employees Might Feel Compelled to Participate in Data Processing Practices Inconsistent with Expectations	Appropriation Induced Disclosure
PR-5	Unauthorized or Invasive Application Processing of Information Exposes Employee Data	Surveillance Unanticipated Revelation

The Privacy Risks are also used in Appendix F in the 1800-22 Supplement to identify relevant mobile privacy risks in the example scenario and Appendix D in 1800-22 Volume C to test the privacy characteristics of the lab build.

### 4.1.2.1 Privacy Risk Examples and Mitigation Methodologies

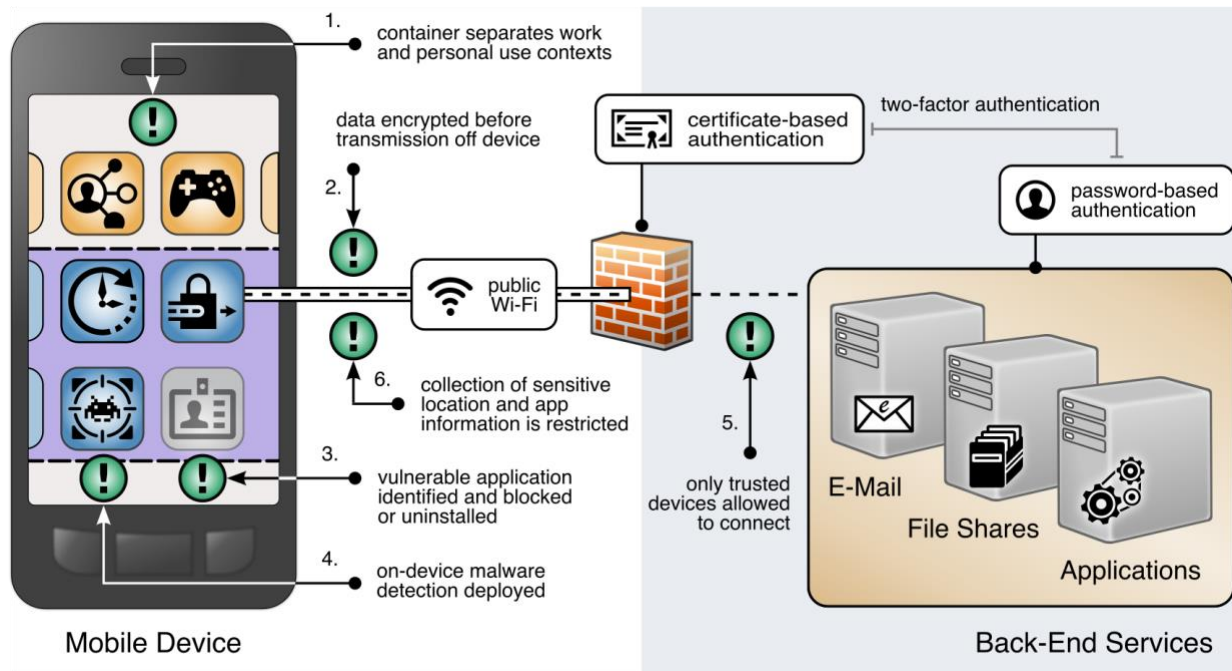
The example solution contained in this guide identifies and helps to mitigate some common privacy risks that a BYOD deployment may encounter. The privacy risks and their accompanying problematic data actions were identified using NIST-developed methodologies.

The NIST PRAM [9] and accompanying Catalog of Problematic Data Actions and Problems [12] (see Section 4.1.2) are standardized methodologies for identifying privacy challenges that were used to conduct our privacy risk analysis. This publication provides the results of our privacy risk analysis for a fictional organization as an exemplar for the reader's use, as well as suggested privacy architecture enhancements. See Appendix G of the Supplement for an example of how the privacy risks for this practice guide's BYOD deployment example solution were developed. The following section, 4.1.3, outlines the security and privacy objectives of this publication's example solution architecture.

### 4.1.3 Security and Privacy Objectives

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

Figure 4-1 Security and Privacy Objectives



The following are a list of security and privacy objectives (as highlighted above in Figure 4-1, 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 objectives 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 (e.g., work applications such as work email) or configuration file from the device rather than uninstalling the employee's personal applications.
4. **Prevent or detect malware.** On personally owned devices, 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 within the work profile or managed applications and facilitate remediation. Additionally, security features that are built-in to the OS could aid in preventing or detecting the installation of malware.
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.** Depending on how devices are enrolled, mobile device management tools can sometimes track application inventory and location information, including physical address, geographic coordinates, location history, internet protocol (IP) address, and service 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 objectives 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 NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice*. The supplement provides an example approach for developing and deploying a BYOD architecture that directly addresses the mobile device TEs and problematic data actions discussed in this guide.

The supplement shows how a fictional organization used the guidance in NIST’s Cybersecurity Framework [1], Privacy Framework [2], RMF [10], and PRAM [9] to identify and address their BYOD security and privacy objectives.

### 4.3 Technologies that Support the Security and Privacy Objectives 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 objectives, TEs, 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 TEE is “a controlled and separated environment outside the high-level operating system that is designed to allow trusted execution of code and to protect against viruses, Trojans, and root kits.” [13] By providing a controlled and separated environment, the TEE helps enable applications and features that can provide enhanced security and privacy functionality.

#### 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 enrolled 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. Both iOS and Android also support a bulk EMM enrollment use case (Apple Business Manager for iOS devices and Android Enterprise Enrollment for Android devices), 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 user profile solutions, such as Android Enterprise or iOS User Enrollment. These capabilities can be used in the following ways in a BYOD deployment:

- Mobile application management can be used to manage the installation and usage of an organization's applications based on their trustworthiness and work relevance.
- Mobile content management can control how managed applications access and use organizational data.
- The EMM works with operating system data separation and isolation capabilities that 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, *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* [14] 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.

In addition, EMMs may also provide mobile application wrapping functionality. The wrapping process encapsulates enterprise-developed applications in a vendor-created wrapper that intercepts application programming interface (API) calls and provides additional layers of security. Wrapping is useful in many different scenarios, for example, to force an application's traffic to go through the corporate VPN. Wrapping typically occurs when applications are uploaded to the EMM's app store for distribution to enrolled devices [15].

### 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* [16], in combination with *Protection Profile for Network Devices* [17], describes important capabilities and security requirements to expect from VPN gateways.

In a BYOD deployment, an enterprise can also leverage a per-application or full enterprise profile 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 only has visibility into enterprise traffic. 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, whether malicious or benign, can negatively affect both security and user privacy. 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., a 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* [18] 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 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-, application-, and network-based threats. Device-based threats include outdated OS versions, insecure configurations, elevation of privileges, unauthorized device 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 devices can have a wide variety of installed applications and usage scenarios, an MTD profile helps improve the security and privacy posture by providing an agent-based capability to detect unwanted activity within the work profile.

To further enhance device protection and analytic capabilities, MTD services may offer additional integrations with 3<sup>rd</sup> party threat intelligence services such as MITRE ATT&CK for Mobile or VirusTotal. These services could aid in enriching the data acquired from devices, providing more contextual and technical information on the discovered threats. Then, the enriched data could be forwarded to other services for additional analysis or triage, such as a Security Information and Event Management service.

### 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.

#### 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.

#### 4.3.6.2 *Device Attestation*

Device attestation is an extension of the secure boot process that involves the OS (or more commonly, an integrated TEE and/or Hardware Security Model) 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 [\[19\]](#).

#### *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 of how management APIs can enhance device security include verification of digital signatures for installed software and updates, requiring a device unlock code, initiating remote device lock actions, and requiring 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 [\[20\]](#).

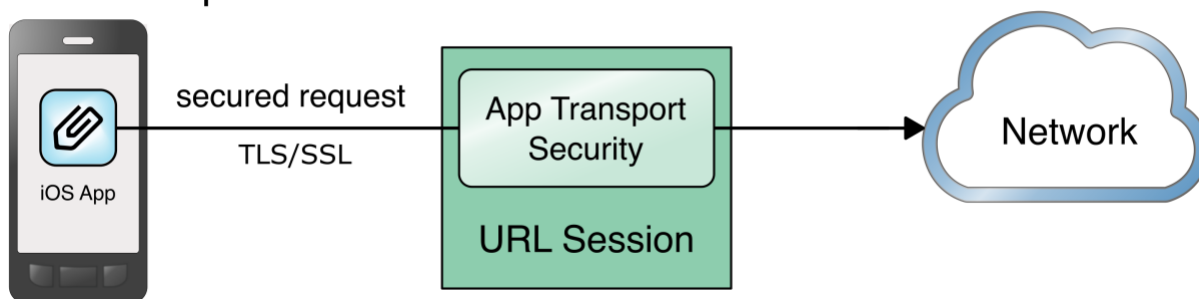
Additionally, mobile operating systems expose an API to MDM products that allow an organization that manages a device to have greater control over these and many more settings that might not be directly accessible to the device user. Management APIs allow enterprises using integrated EMM or MDM products 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*

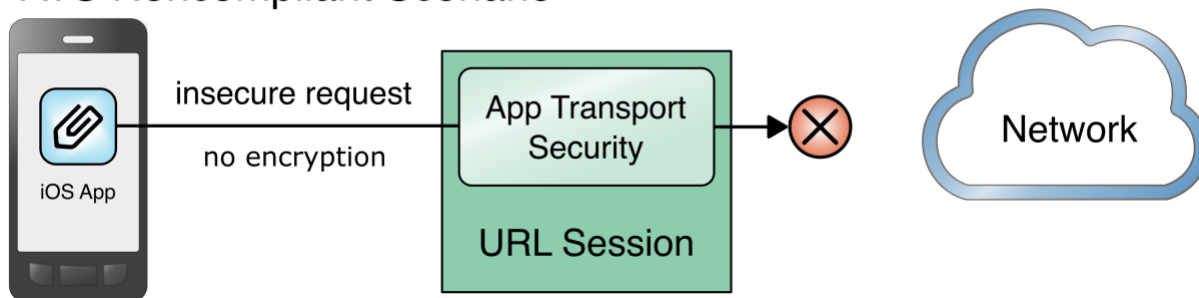
App Transport Security (ATS) is a networking security feature on Apple iOS devices that increases data integrity and privacy for applications and extensions [\[21\]](#), [\[22\]](#). ATS requires that the network connections made by applications are secured through the Transport Layer Security protocol, 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 insecure requests are blocked.

Figure 4-2 iOS App Transport Security

### ATS Compliant Scenario



### ATS Noncompliant Scenario



#### 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 [23], [24]. 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 and pin specific certificates to ensure secure communications and issue certificates.

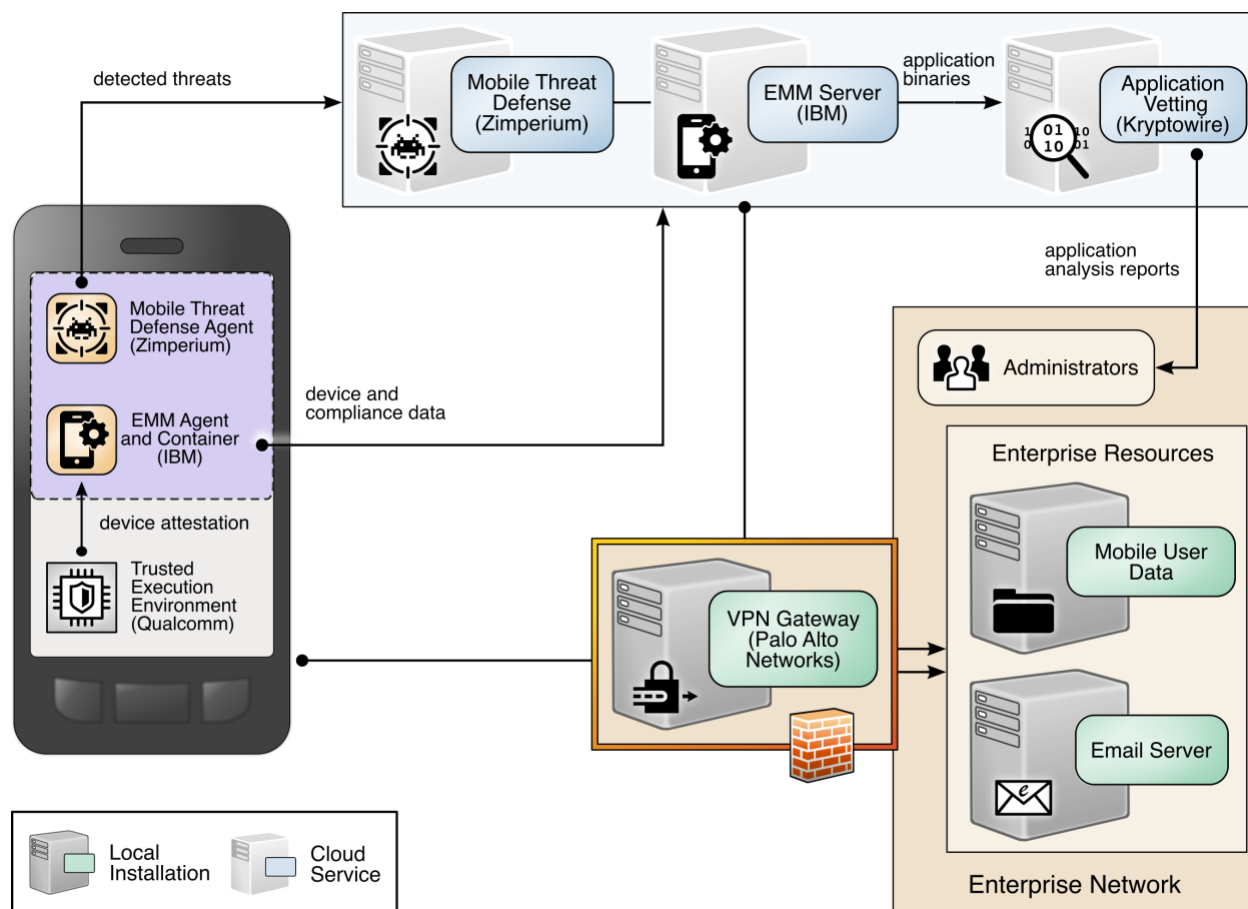
#### 4.3.6.6 Application Sandboxing

Both Android and iOS impose sandboxing restrictions on applications running on the device. These security and privacy controls help isolate applications into their own runtime environments. The sandboxing restrictions then help prevent applications from accessing other applications' data or data on the underlying operating system not exposed by official APIs.

## 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



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

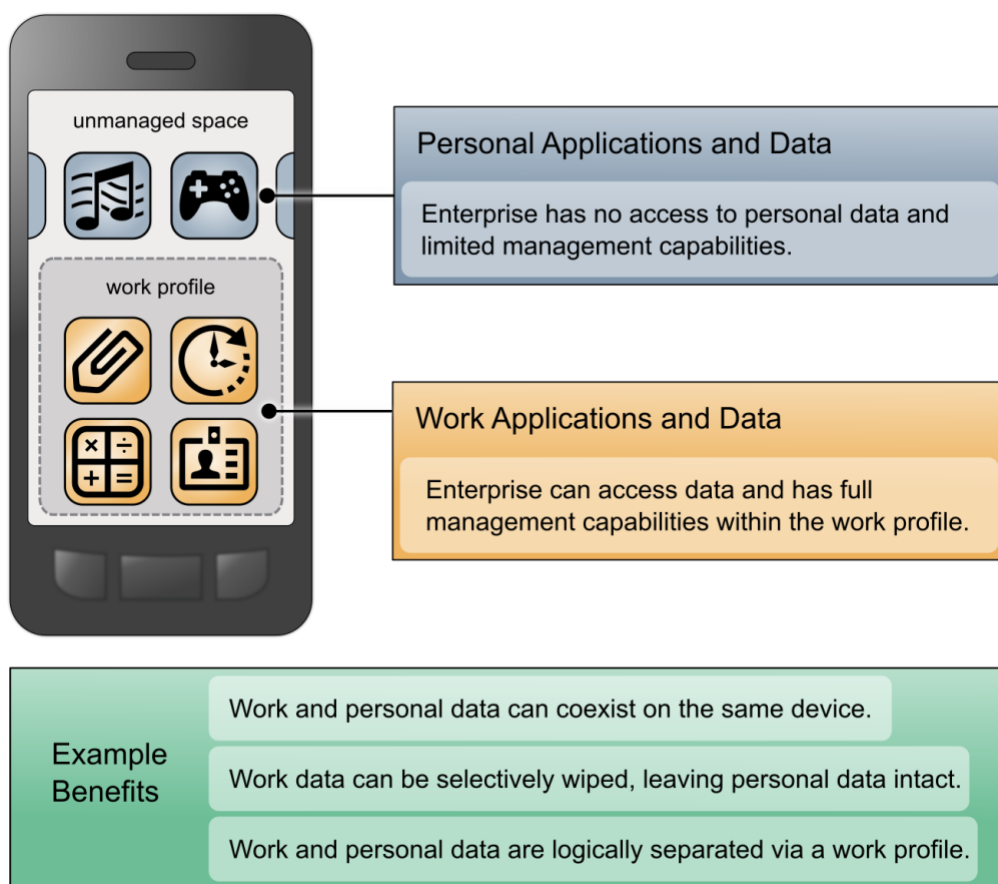
One key benefit of BYOD solutions for employees is the ability to access both work and personal data on the same device. While the technical approaches differ between iOS and Android devices, both

operating systems offer the following types of features for managing the coexistence of work and personal data on devices [25], [26]:

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

Illustrating this concept, Figure 4-4 shows enterprise integration for managed and unmanaged applications on mobile devices. To protect sensitive work data and employee privacy, work applications can be separated into a work profile, with data access restricted between the personal and work container profile applications.

Figure 4-4 Mobile Device Application Management and Benefits



#### 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.

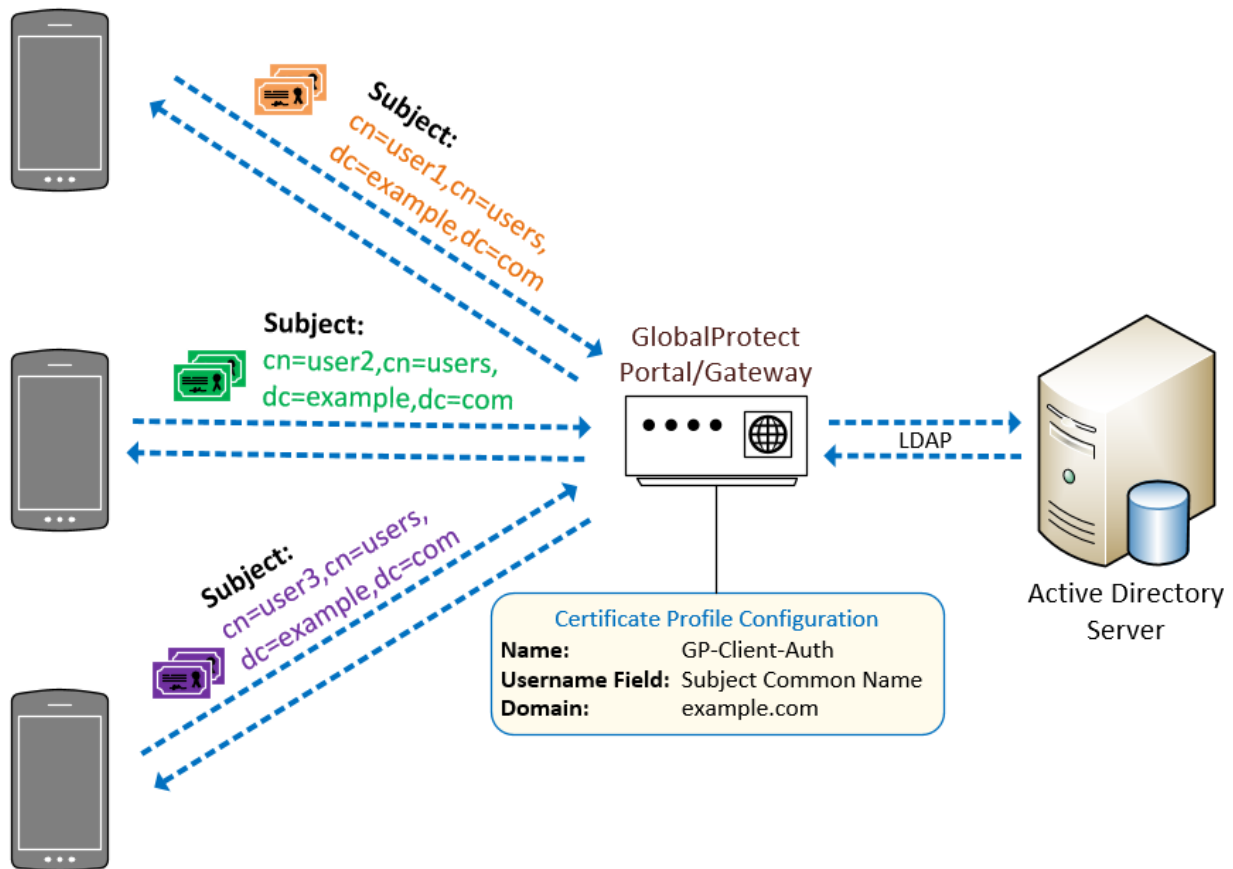
#### 4.5.2 Mobile Device Enrollment

The example solution shown in [Figure 4-5](#) mitigates the potential for Simple Certificate Enrollment Protocol (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.

Figure 4-5 Example Solution VPN Authentication Architecture



## 4.6 Mobile Components Integration

IBM MaaS360 supports integration of third-party applications and cloud services via a representational state transfer (REST) API [27]. External services are authenticated via access tokens, obtained through MaaS360 support. Zimperium and Kryptowire used the REST API [28].

Table 4-3 identifies the commercially available products used in this example solution and how they align with the mobile security technologies. For additional information, Appendices G and H contain a mapping of these technologies to the cybersecurity and privacy standards and best practices that each 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 10.82 IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)	mobile device management

Commercially Available Product	Mobile Security Technology
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	
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
Apple iOS Version 13 Google Android Version 10	mobile device operating system

#### 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 the 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 in the work profile on the device. When the user first launches the zIPS application from within the work profile, 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 (such as device ID, enterprise username, and device name), and the inventory of enterprise 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 profile 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 profile is launched.

#### 4.6.4 iOS and Android MDM Integration

Both iOS and Android integrate directly with MaaS360. iOS devices are enrolled into MaaS360 using User Enrollment, which is Apple's BYOD solution. User Enrollment creates a second persona on the device, which places the work data on a separate encrypted partition on the device. User Enrollment also requires managed user IDs, which are created in Apple Business Manager. This allows the enterprise to associate the work data with the managed Apple ID, while the user associates their personal data with their personal Apple ID.

Android devices are managed by Android Enterprise, which provides controls for both the device itself and the work profile. The work profile is a separated, isolated, and encrypted environment based on an SELinux user profile that stores all the enterprise applications and data, ensuring separation from personal applications and data.

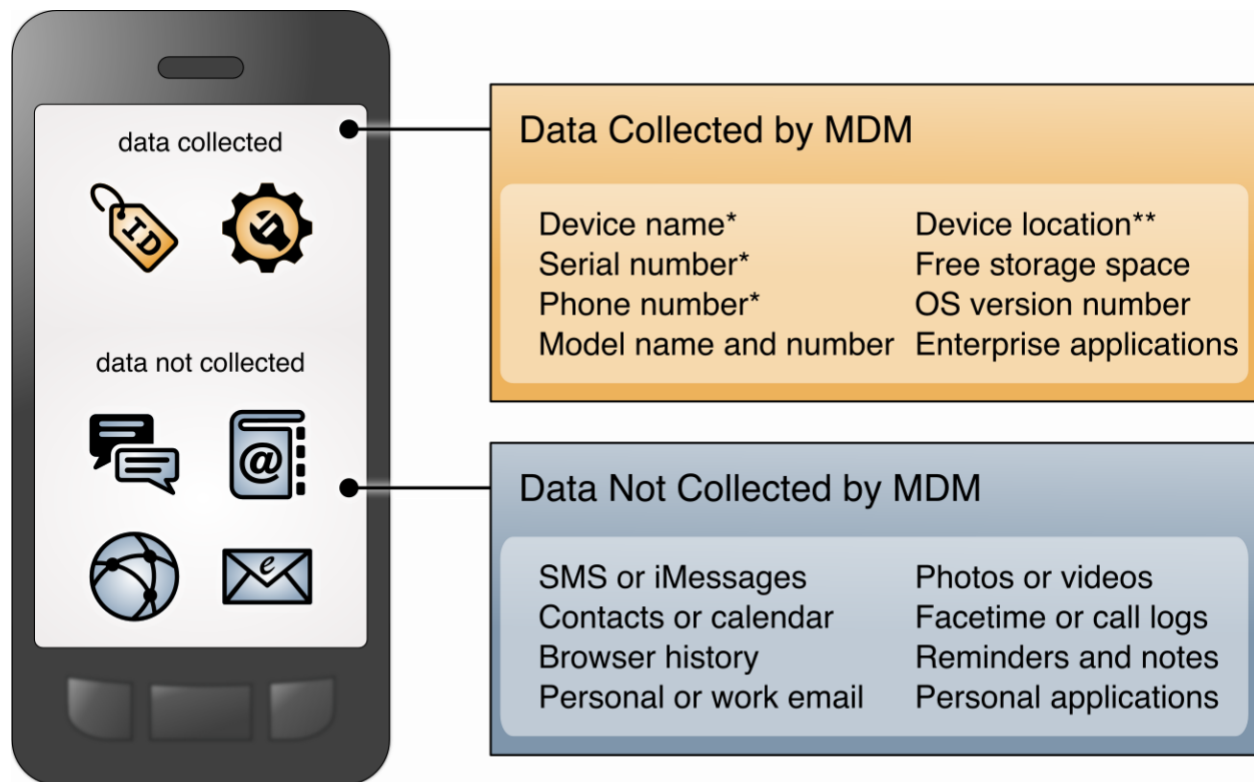
### 4.7 Privacy Settings: Mobile Device Data Processing

This section looks 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 device is connected to an EMM system, some data is collected and visible to the enterprise. While additional data can be collected (depending on how devices are enrolled), our example solution collects only the data shown in [Figure 4-6](#) to help protect employee privacy. IBM provides documentation with more details on the information that MaaS360 collects and processes [\[29\]](#).

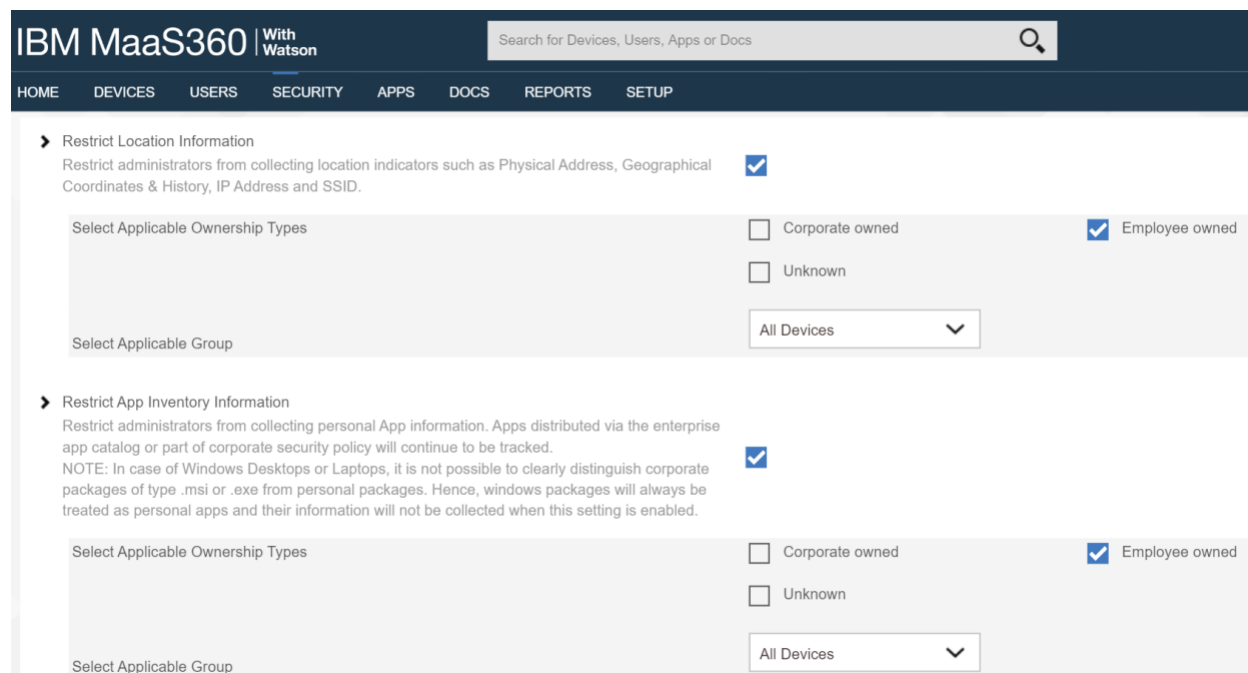
Figure 4-6 Data Collected by Example Solution Mobile Device Management



\*: Android only  
 \*\*: With user consent

As shown in [Figure 4-7](#) below, 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 only collect applications that are distributed through the enterprise and, therefore, will not transmit any personal applications to third-party application-vetting services. Both privacy controls can be applied to specific device groups—for example, location collection can be disabled for personally owned devices. These privacy controls typically only apply to devices that are enrolled as fully managed devices. Devices enrolled using Android Enterprise (work profile mode) or Apple User Enrollment have controls in place that prevent the EMM from accessing application inventory and location collection regardless of privacy control configuration.

Figure 4-7 Example Solution Mobile Device Management Privacy Settings



## 4.7.2 MTD: Zimperium

Zimperium provides configurable settings for what data is collected. In the list below, the top-level bullets can be disabled. Sub-bullets follow the enabled or disabled setting of the top-level. Zimperium also provides preset templates that can be utilized, including High, Medium, Low, and General Data Protection Regulation (GDPR). When using the Custom template type, the enterprise can configure exactly what data is collected. Data collected can include:

- device location (configurable granularity: street, city, county, none)
- device operating system
- device model
- device IP address
- device running processes (Android only)
- network connection details
  - SSID
  - BSSID
  - external IP address
  - gateway IP
  - gateway MAC
  - nearby Wi-Fi networks
  - ARP table

- routing table
- carrier information
- attacker IP & MAC
- risky or unapproved sites
- phishing protection risky URLs
- application forensics
- application binaries (Android only)
- application inventory (Android only)

zIPS also collects some information that cannot be disabled. These items include:

- device root/jailbreak status
- USB debug mode status (Android only)
- developer mode status (Android only)
- 3<sup>rd</sup> party app store presence (Android only)
- mobile OS-specific vulnerability status (e.g., Stagefright)
- device encryption status (Android only)
- device protection status
- screen lock status

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

- user credentials (email address, Zimperium-specific password)
- mobile network operator
- mobile network country code
- device operating system
- device push token
- hash of local z9 database
- time and name of threat detection when a threat occurs

### 4.7.3 Application Vetting: Kryptowire

Kryptowire collects certain pieces of device information through the MaaS360 REST API for analytics and application association purposes. The data collected includes:

- MDM device ID
- MDM device name
- MDM username
- last MDM sync date

- MDM enrollment data
- enterprise and non-app store installed applications

#### 4.7.4 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
- device root/jailbreak status

## 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 TE 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. Also, NIST SP 1800-22 Volume C, Appendix D shows the test activities that were used to demonstrate how this practice guide's example solution addresses TEs and privacy risks.

### 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 and Privacy 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 these subcategories as a basis for organizing the analysis allowed systematic consideration of how well the reference design supports the intended security and privacy 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
- development of the Privacy Framework mappings
- TEs 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, Privacy 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 E](#) (Cybersecurity Framework) and [Appendix F](#) (Privacy Framework).

Developing profiles utilizing frameworks such as the Cybersecurity and Privacy Frameworks can help with identifying whether or not an organization is meeting their security and privacy expectations.

### 5.3.2 Threat Events and Findings

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

*Note: The 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
<b>Threat Event 1:</b> Unauthorized access to sensitive information via a malicious or intrusive application practices	OS-level controls provide data separation between corporate and personal data.	EMM
<b>Threat Event 2:</b> Theft of credentials through a short message service or email phishing campaign	Utilized PAN-DB and URL filtering to block known malicious websites.	Firewall
<b>Threat Event 3:</b> 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
<b>Threat Event 4:</b> 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
<b>Threat Event 5:</b> Compromise of device integrity via observed, inferred, or brute-forced device unlock code	The EMM enforces a required passcode. GlobalProtect requires periodic re-authentication.	EMM VPN
<b>Threat Event 6:</b> 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
<b>Threat Event 7:</b> 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	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
<b>Threat Event 8:</b> Loss of organizational data due to a lost or stolen device	Enforced passcode policies and device-wipe capabilities protected enterprise data.	EMM
<b>Threat Event 9:</b> 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

The technologies in Table 5-1 are mapped to cybersecurity and privacy control mappings in [Appendix E](#) and [Appendix F](#).

### 5.3.3 Privacy Risk Findings

The risk analysis found that five data actions in the build were potential privacy risks 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 Risks and Findings**

Privacy Risk (for Employees) and Related Problematic Data Actions	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
<p><b>Privacy Risk 1:</b> Wiping Activities on the Employee’s Device May Inadvertently Delete the Employee’s Personal Data</p> <p><b>Related Problematic Data Action:</b> Unwarranted Restriction</p>	<p>In the event of a security issue, employee access to enterprise resources can be prevented by removing the device from EMM control or restricting device access to organizational systems instead of wiping the device.</p> <p>The EMM enables selective wiping of only corporate resources from the device.</p> <p>To further protect the employee’s privacy, the ability to perform selective device information wipe activities can be limited to a small number of IT administrative staff.</p>	EMM



Privacy Risk (for Employees) and Related Problematic Data Actions	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
<p><b>Privacy Risk 2:</b> Organizational Collection of Device Data May Subject Employees to Feeling of Being Surveilled</p> <p><b>Related Problematic Data Action:</b> Surveillance</p>	<p>The example solution restricts staff access to system capabilities that permit reviewing data about employees and their devices.</p> <p>Additionally, the example solution limits or disables collection of specific data elements (e.g., location data).</p>	EMM
<p><b>Privacy Risk 3:</b> Data Collection and Transmission Between Integrated Security Products May Expose Employee Data</p> <p><b>Related Problematic Data Action:</b> Unanticipated Revelation</p>	<p>The example solution:</p> <ul style="list-style-type: none"> <li>De-identifies employee data when it is not required to meet processing objectives.</li> <li>Encrypts data transmitted between parties.</li> <li>Limits or disables access to data.</li> <li>Limits or disables the collection of specific data elements.</li> </ul>	EMM
<p><b>Privacy Risk 4:</b> Employees Might Feel Compelled to Participate in Data Processing Practices Inconsistent with Expectations</p> <p><b>Related Problematic Data Action:</b> Appropriation</p>	<p>The example solution provides a configurable pop-up banner to employees during device enrollment to provide notice regarding data processing practices in the BYOD solution, including what data is collected and what data is not collected. It can also provide information about where the employee can find more in-depth information regarding the organization’s privacy policies and practices.</p>	EMM
<p><b>Privacy Risk 5:</b> Unauthorized or Invasive Application Processing of Information Exposes Employee Data</p> <p><b>Related Problematic Data Action:</b> Surveillance, Unanticipated revelation</p>	<p>EMM leverages OS-related separation between enterprise and employee personal data.</p> <p>The BYOD solution provides malware protection through Zimperium, which protects the device against advanced</p>	EMM Zimperium

Privacy Risk (for Employees) and Related Problematic Data Actions	How the Example Solution Architecture Helps Mitigate the Privacy Risk	The Technology Function that Helps Mitigate the Privacy Risk
	threats, while providing privacy protections.	

## 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 document 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 [8] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to the organization. The company then uses the NIST PRAM [9] to perform a privacy risk assessment. Appendix F and Appendix G of the Supplement of this practice guide, 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 Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems* [30], 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 [31] 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.

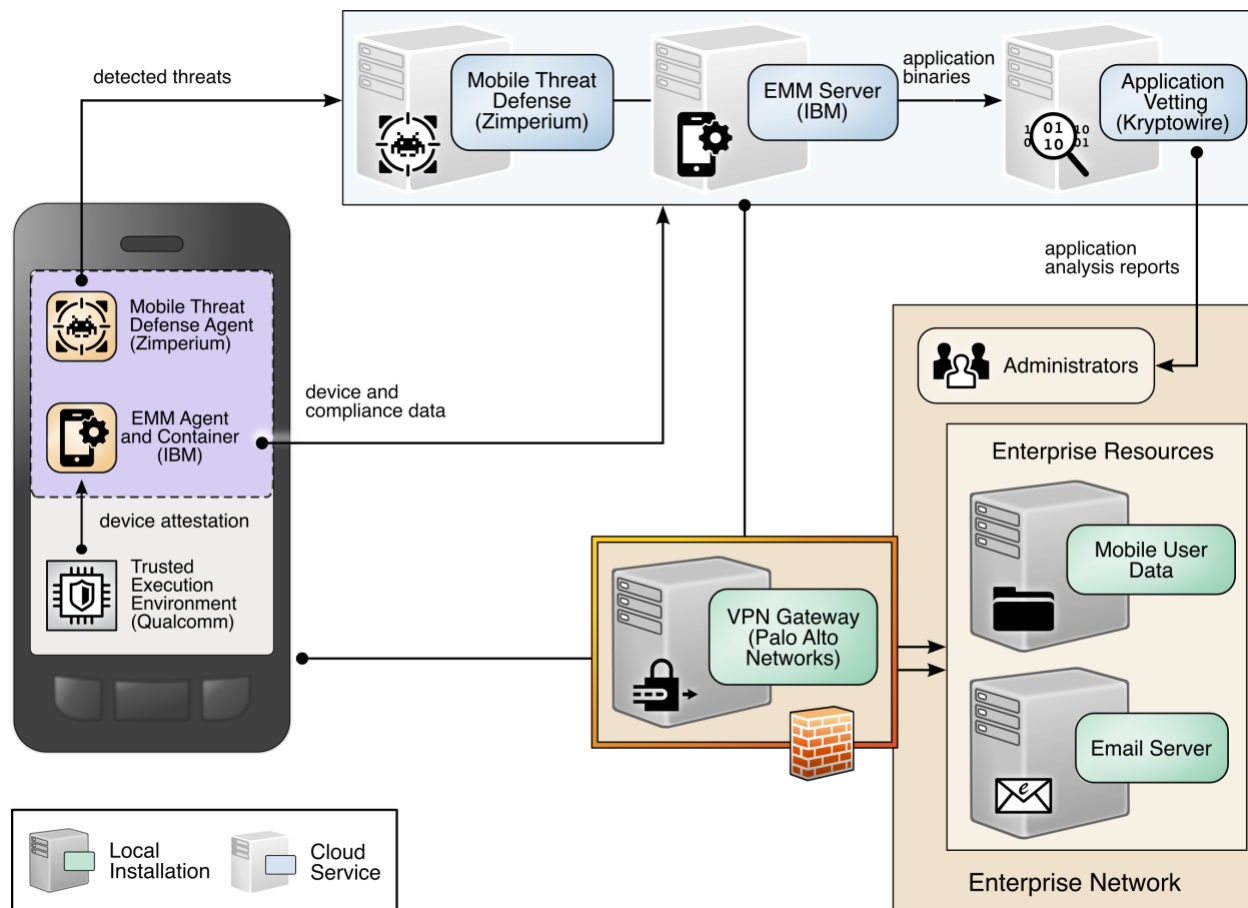
A detailed description of the implementation process that the fictional organization Great Seneca Accounting followed is provided in the NIST SP 1800-22 *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

## 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



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 IT 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.

In Volume C, this practice guide also includes 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 future builds, the team is involved in projects that relate to mobile device security including [Implementing a Zero Trust Architecture](#) and [Digital Identities – Mobile Driver’s License \(mDL\)](#).

## Appendix A List of Acronyms

<b>AD</b>	Active Directory
<b>API</b>	Application Programming Interface
<b>ATARC</b>	Advanced Technology Academic Research Center
<b>ATS</b>	App Transport Security
<b>BYOD</b>	Bring Your Own Device
<b>CIS</b>	Center for Internet Security
<b>CN</b>	Common Name
<b>COMSEC</b>	Communications Security
<b>COPE</b>	Corporate-Owned Personally-Enabled
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>DHS</b>	Department of Homeland Security
<b>DN</b>	Distinguished Name
<b>EMM</b>	Enterprise Mobility Management
<b>FIPS</b>	Federal Information Processing Standards
<b>GDPR</b>	General Data Protection Regulation
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>IBM</b>	International Business Machines
<b>ICS</b>	Industrial Control System
<b>IEC</b>	International Electrotechnical Commission
<b>iOS</b>	iPhone Operating System
<b>IP</b>	Internet Protocol
<b>ISO</b>	International Organization for Standardization
<b>ITL</b>	Information Technology Laboratory
<b>mDL</b>	Mobile Driver's License
<b>MDM</b>	Mobile Device Management
<b>MSCT</b>	Mobile Services Category Team
<b>MTD</b>	Mobile Threat Defense

<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NDES</b>	Network Device Enrollment Service
<b>NIAP</b>	National Information Assurance Partnership
<b>NICE</b>	National Initiative for Cybersecurity Education
<b>NIST</b>	National Institute of Standards and Technology
<b>NISTIR</b>	NIST Interagency Report
<b>OS</b>	Operating System
<b>OWASP</b>	Open Web Application Security Project
<b>PII</b>	Personally Identifiable Information
<b>PRAM</b>	Privacy Risk Assessment Methodology
<b>REST</b>	Representational State Transfer
<b>SCEP</b>	Simple Certificate Enrollment Protocol
<b>SMTP</b>	Simple Mail Transport Protocol
<b>SP</b>	Special Publication
<b>SSID</b>	Service Set Identifier

## Appendix B Glossary

<b>Access Management</b>	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 <a href="#">[32]</a> .
<b>Availability</b>	Ensure that users can access resources through remote access whenever needed <a href="#">[33]</a> .
<b>Bring Your Own Device (BYOD)</b>	A non-organization-controlled telework client device <a href="#">[33]</a> .
<b>Confidentiality</b>	Ensure that remote access communications and stored user data cannot be read by unauthorized parties <a href="#">[33]</a> .
<b>Data Actions</b>	System operations that process personally identifiable information (PII) <a href="#">[34]</a> .
<b>Disassociability</b>	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system <a href="#">[34]</a> .
<b>Eavesdropping</b>	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 <a href="#">[35]</a> (definition located under eavesdropping attack).
<b>Firewall</b>	Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures <a href="#">[36]</a> .
<b>Integrity</b>	Detect any intentional or unintentional changes to remote access communications that occur in transit <a href="#">[33]</a> .
<b>Manageability</b>	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure <a href="#">[34]</a> .
<b>Mobile Device</b>	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 <a href="#">[31]</a> .

<b>Personally Identifiable Information (PII)</b>	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 <a href="#">[37]</a> (adapted from Government Accountability Office Report 08-536).
<b>Predictability</b>	Enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by a system <a href="#">[34]</a> .
<b>Privacy Event</b>	The occurrence or potential occurrence of problematic data actions <a href="#">[2]</a> .
<b>Problematic Data Action</b>	A data action that could cause an adverse effect for individuals <a href="#">[2]</a> .
<b>Threat</b>	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 <a href="#">[8]</a> .
<b>Vulnerability</b>	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source <a href="#">[8]</a> .



## 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 rev. 1, NIST, Gaithersburg, Md., Nov. 2020. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>.
- [4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](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, NIST, Gaithersburg, Md., May. 2023. Available: <https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/final>.
- [7] J. Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds*, NIST SP 1800-4, NIST, Gaithersburg, Md., Feb. 21, 2019. Available <https://doi.org/10.6028/NIST.SP.1800-4>.
- [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. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available: <https://www.nist.gov/privacy-framework/nist-pram>.
- [10] 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>.
- [11] Open Web Application Security Project (OWASP). “OWASP Mobile Top 10,” [Online]. Available: <https://owasp.org/www-project-mobile-top-10/>.
- [12] 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>.
- [13] Qualcomm. “Mobile Security Solutions.” [Online]. Available: <https://www.qualcomm.com/products/features/mobile-security-solutions>.

- [14] 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](https://www.niap-ccevs.org/MMO/PP/ep_mdm_agent_v3.0.pdf).
- [15] International Business Machines (IBM). About enterprise app wrapping. Aug. 09, 2022 last updated. [Online]. Available: <https://www.ibm.com/docs/en/maas360?topic=overview-about-enterprise-app-wrapping>.
- [16] 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>.
- [17] 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>.
- [18] NIAP. Approved Protection Profiles. [Online]. Available: <https://www.niap-ccevs.org/Profile/PP.cfm>.
- [19] 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>.
- [20] Google Android. Android Management API. [Online]. Available: <https://developers.google.com/android/management>.
- [21] Apple Inc. “Preventing Insecure Network Connections.” [Online]. Available: [https://developer.apple.com/documentation/security/preventing\\_insecure\\_network\\_connections](https://developer.apple.com/documentation/security/preventing_insecure_network_connections).
- [22] 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](https://developer.apple.com/documentation/security/preventing_insecure_network_connections/identifying_the_source_of_blocked_connections).
- [23] Android.com. “Network security configuration.” Dec. 27, 2019. [Online]. Available: <https://developer.android.com/training/articles/security-config>.
- [24] 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/>.
- [25] 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](https://www.apple.com/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf).
- [26] Google Android. “Build Android management solutions for enterprises.” [Online]. Available: <https://developers.google.com/android/work>.
- [27] International Business Machines (IBM). “Web Services.” [Online]. Available: <https://www.ibm.com/docs/en/maas360?topic=web-services>.

- [28] 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](https://www.ibm.com/developerworks/community/wikis/home?lang=en-us#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/MaaS360%20REST%20API%20Usage).
- [29] IBM. "MaaS360 Data Privacy Information." [Online]. Available: <https://www.ibm.com/support/pages/maas360-data-privacy-information>
- [30] 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>.
- [31] 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>.
- [32] IDManagement.gov. "Federal Identity, Credential, and Access Management Architecture." [Online]. Available: <https://arch.idmanagement.gov/services/access/>.
- [33] 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>.
- [34] 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>.
- [35] 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>.
- [36] 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>.
- [37] 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>.
- [38] 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>.
- [39] 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>.
- [40] 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>.

- [41] 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>.
- [42] 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>.
- [43] 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>.
- [44] NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems*, NIST SP 800-171 Revision 2, February 2020. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>.
- [45] Center for Internet Security. Center for Internet Security home page. [Online]. Available: <https://www.cisecurity.org/>.
- [46] 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>.
- [47] 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>.
- [48] 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](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf).
- [49] 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>.
- [50] "Mobile Computing Decision." [Online]. Available: <https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf>.
- [51] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC). "Navigating the Future of Mobile Services." Oct. 2017. [Online]. Available: <https://atarc.org/wp-content/uploads/2019/01/ATARC-MSCT-Report-Navigating-Future-of-Mobile-Services-2.pdf>.
- [52] 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>.

- [53] 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](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf).
- [54] 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/>.
- [55] 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](https://www.niap-ccevs.org/MMO/PP/pp_mdm_agent_v2.0.pdf).
- [56] 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>.
- [57] 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>.
- [58] NIAP. Product Compliant List. [Online]. Available: <https://www.niap-ccevs.org/Product/>.
- [59] 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://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m\\_16\\_20.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_20.pdf).
- [60] NIST. United States Government Configuration Baseline (in development). [Online]. Available: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>.
- [61] 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>.
- [62] 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/2021/NIST.IR.8170-upd.pdf>.
- [63] 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

The following are references that informed the writing of this publication.

- 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)* [\[38\]](#)
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [\[8\]](#)
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [\[10\]](#)
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [\[33\]](#)
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [\[39\]](#)
- NIST SP 800-53 Revision 4 (Final), *Security and Privacy Controls for Information Systems and Organizations* [\[31\]](#)
- NIST SP 800-53 Revision 5 (Final), *Security and Privacy Controls for Information Systems and Organizations* [\[40\]](#)
- NIST SP 800-63-3, *Digital Identity Guidelines* [\[35\]](#)
- NIST SP 800-113, *Guide to SSL VPNs* [\[41\]](#)
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [\[42\]](#)
- NIST SP 800-124 Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [\[6\]](#)
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [\[43\]](#)
- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [\[44\]](#)
- 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* [\[30\]](#)
- NIST Privacy Risk Assessment Methodology [\[9\]](#)
- Center for Internet Security [\[45\]](#)

- Executive Office of the President, Bring Your Own Device toolkit [\[46\]](#)
- Federal Chief Information Officers Council and Department of Homeland Security *Mobile Security Reference Architecture*, Version 1.0 [\[47\]](#)
- Digital Services Advisory Group and Federal Chief Information Officers Council, *Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis* [\[48\]](#)
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, “Information technology – Security techniques – Information security management systems – Requirements” [\[49\]](#)
- Mobile Computing Decision example case study [\[50\]](#)
- MSCT ATARC, “Navigating the Future of Mobile Services,” Working Group Document [\[51\]](#)
- MSCT, “Device Procurement and Management Guidance” [\[52\]](#)
- MSCT, “Mobile Device Management (MDM),” MDM Working Group Document [\[53\]](#)
- MSCT, “Mobile Services Roadmap, MSCT Strategic Approach” [\[54\]](#)
- National Information Assurance Partnership (NIAP), U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 2.0 [\[55\]](#)
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Fundamentals Version 3.1 [\[56\]](#)
- NIAP, Approved Protection Profiles—Protection Profile for Mobile Device Management Version 4.0 [\[57\]](#)
- NIAP, Product Compliant List [\[58\]](#)
- Office of Management and Budget, *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services* [\[59\]](#)
- United States Government Configuration Baseline [\[60\]](#)
- Department of Homeland Security (DHS), “DHS S&T Study on Mobile Device Security” [\[61\]](#)
- NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework* [\[62\]](#)



## Appendix E 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* [40]; International Organization for Standardization (ISO); International Electrotechnical Commission (IEC) 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* [49]; the Center for Internet Security’s (CIS) control set Version 6 [45]; and NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Work Roles from 2017 version)* [3].

Table E-1 below 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 E-1 Example Solution’s Cybersecurity Standards and Best Practices Mapping**

Specific product used	Function	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)
<b>Kryptowire Cloud Service</b>	Application Vetting	<b>ID.RA-1:</b> Asset vulnerabilities are identified and documented.	<b>CA-2, CA-7, CA-8:</b> Security Assessment and Authorization  <b>RA-3, RA-5:</b> Risk Assessment  <b>SA-4:</b> Acquisition Process  <b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.12.6.1:</b> Control of technical vulnerabilities  <b>A.18.2.3:</b> Technical Compliance Review	<b>CSC 4:</b> Continuous Vulnerability Assessment and Remediation	<b>SP-RSK-002:</b> Security Control Assessor  <b>SP-ARC-002:</b> Security Architect  <b>OM-ANA-001:</b> Systems Security Analyst



Specific product used	Function	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)
		<p><b>ID.RA-3:</b> Threats, both internal and external, are identified and documented.</p>	<p><b>RA-3:</b> Risk Assessment</p> <p><b>SI-7:</b> Software, Firmware, and Information Integrity</p> <p><b>PM-12, PM-16:</b> Insider Threat Program</p>	<p><b>6.1.2:</b> Information risk assessment process</p>	<p><b>CSC 4:</b> Continuous Vulnerability Assessment and Remediation</p>	<p><b>SP-RSK-002:</b> Security Control Assessor</p> <p><b>OM-ANA-001:</b> Systems Security Analyst</p> <p><b>OV-SPP-001:</b> Cyber Workforce Developer and Manager</p> <p><b>OV-TEA-001:</b> Cyber Instructional Curriculum Developer</p> <p><b>PR-VAM-001:</b> Vulnerability Assessment Analyst</p> <p><b>PR-VAM-001:</b> Vulnerability Assessment Analyst</p>

Specific product used	Function	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)
		<b>DE.CM-4:</b> Malicious code is detected.	<b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.12.2.1:</b> Controls Against Malware	<b>CSC 4:</b> Continuous Vulnerability Assessment and Remediation <b>CSC 7:</b> Email and Web Browser Protections <b>CSC 8:</b> Malware Defenses <b>CSC 12:</b> Boundary Defense	<b>PR-CIR-001:</b> Cyber Defense Incident Responder <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>DE.CM-5:</b> Unauthorized mobile code is detected.	<b>SC-18:</b> Mobile Code <b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.12.5.1:</b> Installation of Software on Operational Systems <b>A.12.6.2:</b> Restrictions on Software Installation	<b>CSC 7:</b> Email and Web Browser Protections <b>CSC 8:</b> Malware Defenses	<b>PR-CDA-001:</b> Cyber Defense Analyst <b>SP-DEV-002:</b> Secure Software Assessor

Specific product used	Function	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)
<b>Zimperium Console version vGA-4.23.1</b>	Cloud service that complements the zIPS Agent	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried.	<b>CM-8:</b> Information System Component Inventory <b>PM-5:</b> Information System Inventory	<b>A.8.1.1:</b> Inventory of Assets <b>A.8.1.2:</b> Ownership of Assets	<b>CSC 1:</b> Inventory of Authorized and Unauthorized Devices	<b>OM-STS-001:</b> Technical Support Specialist <b>OM-NET-001:</b> Network Operations Specialist <b>OM-ADM-001:</b> System Administrator
<b>zIPS agent Version 4.9.2 (iOS), 4.9.2 (Android)</b>	Endpoint security for mobile device threats	<b>ID.AM-2:</b> Software platforms and applications within the organization are inventoried.	<b>CM-8:</b> Information System Component Inventory <b>PM-5:</b> Information System Inventory	<b>A.8.1.1:</b> Inventory of Assets <b>A.8.1.2:</b> Ownership of Assets <b>A.12.5.1:</b> Installation of Software on Operational Systems	<b>CSC 2:</b> Inventory of Authorized and Unauthorized Software	<b>SP-DEV-002:</b> Secure Software Assessor <b>SP-DEV-001:</b> Software Developer <b>SP-TRD-001:</b> Research and Development Specialist

Specific product used	Function	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)
		<b>DE.CM-8:</b> Vulnerability scans are performed.	<b>RA-5:</b> Vulnerability Monitoring and Scanning	<b>A.12.6.1:</b> Management of technical vulnerabilities	<b>CSC 4:</b> Continuous Vulnerability Assessment and Remediation  <b>CSC 20:</b> Penetration Tests and Red Team Exercises	<b>PR-VAM-001:</b> Vulnerability Assessment Analyst  <b>PR-INF-001:</b> Cyber Defense Infrastructure Support Specialist  <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>DE.AE-5:</b> Incident alert thresholds are established.	<b>IR-4:</b> Incident Handling  <b>IR-5:</b> Incident Monitoring  <b>IR-8:</b> Incident Response Plan	<b>A.16.1.4:</b> Assessment of and decision on information security events	<b>CSC 6:</b> Maintenance, Monitoring, and Analysis of Audit Logs  <b>CSC 19:</b> Incident Response and Management	<b>PR-CIR-001:</b> Cyber Defense Incident Responder  <b>AN-TWA-001:</b> Threat/Warning Analyst

Specific product used	Function	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)
		<b>DE.CM-5:</b> Unauthorized mobile code is detected.	<b>SC-18:</b> Mobile Code <b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.12.5.1:</b> Installation of Software on Operational Systems <b>A.12.6.2:</b> Restrictions on Software Installation	<b>CSC 7:</b> Email and Web Browser Protections <b>CSC 8:</b> Malware Defenses	<b>PR-CDA-001:</b> Cyber Defense Analyst <b>SP-DEV-002:</b> Secure Software Assessor
<b>IBM MaaS360 Mobile Device Management (SaaS) Version 10.73</b>	Enforces organizational mobile endpoint security policy	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried.	<b>CM-8:</b> System Component Inventory <b>PM-5:</b> System Inventory	<b>A.8.1.1:</b> Inventory of Assets <b>A.8.1.2:</b> Ownership of Assets	<b>CSC 1:</b> Inventory of Authorized and Unauthorized Devices	<b>OM-STS-001:</b> Technical Support Specialist <b>OM-NET-001:</b> Network Operations Specialist <b>OM-ADM-001:</b> System Administrator

Specific product used	Function	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)
		<b>ID.AM-2:</b> Software platforms and applications within the organization are inventoried.	<b>CM-8:</b> System Component Inventory <b>PM-5:</b> System Inventory	<b>A.8.1.1:</b> Inventory of Assets <b>A.8.1.2:</b> Ownership of Assets <b>A.12.5.1:</b> Installation of Software on Operational Systems	<b>CSC 2:</b> Inventory of Authorized and Unauthorized Software	<b>SP-DEV-002:</b> Secure Software Assessor <b>SP-DEV-001:</b> Software Developer <b>SP-TRD-001:</b> Research and Development Specialist

		<p><b>PR.AC-1:</b> Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.</p>	<p><b>AC-3:</b> Access Enforcement</p> <p><b>IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11:</b> Identification and Authentication Family</p>	<p><b>A.9.2.1:</b> User Registration and De-Registration</p> <p><b>A.9.2.2:</b> User Access Provisioning</p> <p><b>A.9.2.3:</b> Management of Privileged Access Rights</p> <p><b>A.9.2.4:</b> Management of Secret Authentication Information of Users</p> <p><b>A.9.2.6:</b> Removal or Adjustment of Access Rights</p> <p><b>A.9.3.1:</b> Use of Secret Authentication Information</p> <p><b>A.9.4.2:</b> Secure logon Procedures</p> <p><b>A.9.4.3:</b> Password Management System</p>	<p><b>CSC 1:</b> Inventory of Authorized and Unauthorized Devices</p> <p><b>CSC 5:</b> Controlled Use of Administrative Privileges</p> <p><b>CSC 15:</b> Wireless Access Control</p> <p><b>CSC 16:</b> Account Monitoring and Control</p>	<p><b>OV-SPP-002:</b> Cyber Policy and Strategy Planner</p> <p><b>OM-ADM-001:</b> System Administrator</p> <p><b>OV-MGT-002:</b> Communications Security (COMSEC) Manager</p>
--	--	---	---	---	---	---

Specific product used	Function	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)
		<b>PR.AC-3:</b> Remote access is managed.	<b>AC-1:</b> Access Control Policy and Procedures <b>AC-17:</b> Remote Access <b>AC-19:</b> Access Control for Mobile Devices <b>AC-20:</b> Use of External Systems <b>SC-15:</b> Collaborative Computing Devices and Applications	<b>A.6.2.1:</b> Mobile Device Policy <b>A.6.2.2:</b> Teleworking <b>A.11.2.6:</b> Security of equipment and assets off premises <b>A.13.1.1:</b> Network Controls <b>A.13.2.1:</b> Information Transfer Policies and Procedures	<b>CSC 12:</b> Boundary Defense	<b>OV-SPP-002:</b> Cyber Policy and Strategy Planner <b>OV-MGT-002:</b> Communications Security (COMSEC) Manager
		<b>PR.AC-6:</b> Identities are proofed and bound to credentials and asserted in interactions.	<b>AC-1, AC-3:</b> Access Control Policy and Procedures <b>IA-2, IA-4, IA-5:</b> Identification and Authentication <b>PE-2:</b> Physical Access Authorizations	<b>A.7.1.1:</b> Screening <b>A.9.2.1:</b> User Registration and De-Registration	<b>CSC 16:</b> Account Monitoring and Control	<b>OV-SPP-002:</b> Cyber Policy and Strategy Planner <b>OV-MGT-002:</b> Communications Security (COMSEC) Manager



Specific product used	Function	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)
		<p><b>PR.IP-1:</b> A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).</p>	<p><b>CM-8:</b> System Component Inventory</p> <p><b>SA-10:</b> Developer Configuration Management</p>	<p><b>A.12.1.2:</b> Change Management</p> <p><b>A.12.5.1:</b> Installation of Software on Operational Systems</p> <p><b>A.12.6.2:</b> Restrictions on Software Installation</p> <p><b>A.14.2.2:</b> System Change Control Procedures</p> <p><b>A.14.2.3:</b> Technical Review of Applications After Operating Platform Changes</p> <p><b>A.14.2.4:</b> Restrictions on Changes to Software Packages</p>	<p><b>CSC 3:</b> Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers</p> <p><b>CSC 9:</b> Limitation and Control of Network Ports, Protocols, and Services</p> <p><b>CSC 11:</b> Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</p>	<p><b>SP-ARC-002:</b> Security Architect</p> <p><b>OV-SPP-002:</b> Cyber Policy and Strategy Planner</p> <p><b>SP-SYS-001:</b> Information Systems Security Developer</p> <p><b>OM-ADM-001:</b> System Administrator</p> <p><b>PR-VAM-001:</b> Vulnerability Assessment Analyst</p>

Specific product used	Function	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)
<b>IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)</b>	Endpoint software that compliments IBM MaaS360 Mobile Device Management console—provides root/jailbreak detection and other functions	<b>PR.DS-6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.	<b>SC-16:</b> Transmission of Security and Privacy Attributes  <b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.12.2.1:</b> Controls Against Malware  <b>A.12.5.1:</b> Installation of Software on Operational Systems  <b>A.14.1.2:</b> Securing Application Services on Public Networks  <b>A.14.1.3:</b> Protecting Application Services Transactions  <b>A.14.2.4:</b> Restrictions on Changes to Software Packages	<b>CSC 2:</b> Inventory of Authorized and Unauthorized Software  <b>CSC 3:</b> Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	<b>OV-SPP-002:</b> Cyber Policy and Strategy Planner  <b>SP-ARC-001:</b> Enterprise Architect

Specific product used	Function	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)
<b>Qualcomm (version is mobile device dependent)</b>	Secure boot and image integrity	<b>PR.DS-1:</b> Data-at-rest is protected.	<b>SC-28:</b> Protection of Information at Rest	<b>A.8.2.3:</b> Handling of Assets	<b>CSC 13:</b> Data Protection <b>CSC 14:</b> Controlled Access Based on the Need to Know	<b>OV-SPP-002:</b> Cyber Policy and Strategy Planner <b>PR-INF-001:</b> Cyber Defense Infrastructure Support Specialist <b>OV-LGA-002:</b> Privacy Officer/Privacy Compliance Manager <b>OV-MGT-002:</b> Communications Security (COMSEC) Manager

Specific product used	Function	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)
		<p><b>PR.DS-6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p><b>SA-10(1):</b> Developer Configuration Management</p> <p><b>SI-7:</b> Software, Firmware, and Information Integrity</p>	<p><b>A.12.2.1:</b> Controls Against Malware</p> <p><b>A.12.5.1:</b> Installation of Software on Operational Systems</p> <p><b>A.14.1.2:</b> Securing Application Services on Public Networks</p> <p><b>A.14.1.3:</b> Protecting Application Services Transactions</p> <p><b>A.14.2.4:</b> Restrictions on Changes to Software Packages</p>	<p><b>CSC 2:</b> Inventory of Authorized and Unauthorized Software</p> <p><b>CSC 3:</b> Secure Configurations for Hardware and Software on Mobile</p>	<p><b>OV-SPP-002:</b> Cyber Policy and Strategy Planner</p> <p><b>PR-CDA-001:</b> Cyber Defense Analyst</p> <p><b>SP-ARC-001:</b> Enterprise Architect</p>

Specific product used	Function	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)
		<b>PR.DS-8:</b> Integrity checking mechanisms are used to verify hardware integrity.	<b>SA-10:</b> Developer Configuration Management <b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.11.2.4:</b> Equipment maintenance	Not applicable	<b>OM-ADM-001:</b> System Administrator <b>SP-ARC-001:</b> Enterprise Architect
		<b>DE.CM-4:</b> Malicious code is detected.	<b>SC-35:</b> External Malicious Code Identification <b>SI-7:</b> Software, Firmware, and Information Integrity	<b>A.12.2.1:</b> Controls Against Malware	<b>CSC 4:</b> Continuous Vulnerability Assessment and Remediation <b>CSC 7:</b> Email and Web Browser Protections <b>CSC 8:</b> Malware Defenses <b>CSC 12:</b> Boundary Defense	<b>PR-CDA-001:</b> Cyber Defense Analyst <b>PR-INF-001:</b> Cyber Defense Infrastructure Support Specialist

Specific product used	Function	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)
<b>Palo Alto Networks PA-220</b>	Enforces network security policy for remote devices	<b>PR.AC-3:</b> Remote access is managed.	<b>AC-1, AC-3:</b> Access Control Policy and Procedures <b>AC-19:</b> Access Control for Mobile Devices	<b>A.6.2.1:</b> Mobile Device Policy <b>A.6.2.2:</b> Teleworking <b>A.11.2.6:</b> Security of equipment and assets off-premises <b>A.13.1.1:</b> Network Controls <b>A.13.2.1:</b> Information Transfer Policies and Procedures	<b>CSC 12:</b> Boundary Defense	<b>OV-SPP-002:</b> Cyber Policy and Strategy Planner <b>OV-MGT-002:</b> Communications Security (COMSEC) Manager

Specific product used	Function	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)
		<b>PR.AC-5:</b> Network integrity is protected (e.g., network segregation, network segmentation).	<b>AC-3:</b> Access Enforcement <b>SC-7:</b> Boundary Protection	<b>A.13.1.1:</b> Network Controls <b>A.13.1.3:</b> Segregation in Networks <b>A.13.2.1:</b> Information Transfer Policies and Procedures <b>A.14.1.2:</b> Securing Application Services on Public Networks <b>A.14.1.3:</b> Protecting Application Services Transactions	<b>CSC 9:</b> Limitation and Control of Network Ports, Protocols, and Services <b>CSC 14:</b> Controlled Access Based on the Need to Know <b>CSC 15:</b> Wireless Access Control <b>CSC 18:</b> Application Software Security	<b>PR-CDA-001:</b> Cyber Defense Analyst <b>OM-ADM-001:</b> System Administrator

Specific product used	Function	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)
		<p><b>PR.AC-6:</b> Identities are proofed and bound to credentials and asserted in interactions.</p>	<p><b>AC-3:</b> Access Enforcement</p> <p><b>IA-2, IA-4, IA-5, IA-8:</b> Identification and Authentication (Organizational Users)</p> <p><b>PE-2:</b> Physical Access Authorizations</p> <p><b>PS-3:</b> Personnel Screening</p>	<p><b>A.7.1.1:</b> Screening</p> <p><b>A.9.2.1:</b> User Registration and De-Registration</p>	<p><b>CSC 16:</b> Account Monitoring and Control</p>	<p><b>OV-SPP-002:</b> Cyber Policy and Strategy Planner</p> <p><b>OV-MGT-002:</b> Communications Security (COMSEC) Manager</p>



Specific product used	Function	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)
		<p><b>PR.DS-2:</b> Data-in-transit is protected.</p>	<p><b>AC-17(2):</b> Protection of Confidentiality and Integrity Using Encryption</p> <p><b>SC-8:</b> Transmission Confidentiality and Integrity</p>	<p><b>A.8.2.3:</b> Handling of Assets</p> <p><b>A.13.1.1:</b> Network Controls</p> <p><b>A.13.2.1:</b> Information Transfer Policies and Procedures</p> <p><b>A.13.2.3:</b> Electronic Messaging</p> <p><b>A.14.1.2:</b> Securing Application Services on Public Networks</p> <p><b>A.14.1.3:</b> Protecting Application Services Transactions</p>	<p><b>CSC 13:</b> Data Protection</p> <p><b>CSC 14:</b> Controlled Access Based on the Need to Know</p>	<p><b>OV-SPP-002:</b> Cyber Policy and Strategy Planner</p> <p><b>OV-MGT-002:</b> Communications Security (COMSEC) Manager</p> <p><b>OV-LGA-002:</b> Privacy Officer/Privacy Compliance Manager</p>

Specific product used	Function	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)
		<p><b>PR.PT-4:</b> Communications and control networks are protected.</p>	<p><b>AC-3, AC-4, AC-17, AC-18:</b> Access Control Family  <b>CP-2:</b> Contingency Plan  <b>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:</b> System and Communications Protection Family</p>	<p><b>A.13.1.1:</b> Network Controls  <b>A.13.2.1:</b> Information Transfer Policies and Procedures  <b>A.14.1.3:</b> Protecting Application Services Transactions</p>	<p><b>CSC 8:</b> Malware Defenses  <b>CSC 12:</b> Boundary Defense  <b>CSC 15:</b> Wireless Access Control</p>	<p><b>PR-INF-001:</b> Cyber Defense Infrastructure Support Specialist  <b>OV-SPP-002:</b> Cyber Policy and Strategy Planner  <b>PR-CDA-001:</b> Cyber Defense Analyst</p>

## Appendix F 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 [\[40\]](#); 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.

The table also 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 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 [\[63\]](#).

Table F-1 Example Solution’s Privacy Standards and Best Practices Mapping

Product	Function	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 administrators what data is collected from each enrolled device.	<b>ID.IM-P7:</b> The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	<b>CM-12:</b> Information Location <b>CM-13:</b> Data Action Mapping <b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>PT-3:</b> Personally Identifiable Information Processing Purposes <b>RA-3:</b> Risk Assessment <b>RA-8:</b> Privacy Impact Assessment	<b>OV-LGA-002:</b> Privacy Officer/Privacy Compliance Manager  <b>OV-TEA-001:</b> Cyber Instructional Curriculum Developer
	Administrators can view data elements in the administration portal. Users can see collected data within the MaaS360 application on their device. Users are advised about data collection practices in a window during enrollment. Data can be edited and deleted from within the	<b>CT.DM-P1:</b> Data elements can be accessed for review.	<b>AC-2:</b> Account Management <b>AC-3:</b> Access Enforcement <b>AC-3(14):</b> Access Enforcement   Individual Access <b>PM-21:</b> Accounting of Disclosures	<b>OM-DTA-002:</b> Data Analyst
		<b>CT.DM-P3:</b> Data elements can be accessed for alteration.	<b>AC-2:</b> Account Management <b>AC-3:</b> Access Enforcement <b>AC-3(14):</b> Access Enforcement   Individual Access <b>PM-21:</b> Accounting of Disclosures <b>SI-18:</b> Personally Identifiable Information Quality Operations	<b>OM-DTA-002:</b> Data Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
	administration console.	<b>CT.DM-P4:</b> Data elements can be accessed for deletion.	<b>AC-2:</b> Account Management <b>AC-3:</b> Access Enforcement <b>SI-18:</b> Personally Identifiable Information Quality Operations	<b>OM-DTA-002:</b> Data Analyst
		<b>CT.DM-P5:</b> Data are destroyed according to policy.	<b>MP-6:</b> Media Sanitization <b>SA-8(33):</b> Security and Privacy Engineering Principles   Minimization <b>SI-18:</b> Personally Identifiable Information Quality Operations <b>SR-12:</b> Component Disposal	<b>OM-DTA-002:</b> Data Analyst
		<b>CT.DP-P4:</b> System or device configurations permit selective collection or disclosure of data elements.	<b>CM-6:</b> Configuration Settings <b>SA-8(33):</b> Minimization <b>SC-42(5):</b> Collection Minimization <b>SI-12(1):</b> Information Management and Retention   Limit Personally Identifiable Information Elements	<b>OV-LGA-002:</b> Privacy Officer/Privacy Compliance Manager
	Devices may be backed up to the cloud.	<b>PR.PO-P3:</b> Backups of information are conducted, maintained, and tested.	<b>CP-4:</b> Contingency Plan Testing <b>CP-6:</b> Alternate Storage Site <b>CP-9:</b> System Backup	<b>OM-ADM-001:</b> System Administrator

Product	Function	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 are issued identity certificates via on-premises certificate infrastructure.	<b>PR.AC-P1:</b> Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	<b>IA-2:</b> Identification and Authentication (Organizational Users) <b>IA-3:</b> Device Identification and Authentication <b>IA-4:</b> Identifier Management <b>IA-4(4):</b> Identifier Management   Identifier User Status	<b>SP-ARC-002:</b> Security Architect <b>PR-CDA-001:</b> Cyber Defense Analyst
	MaaS360 enforces a device personal identification number for access.	<b>PR.AC-P2:</b> Physical access to data and devices is managed.	<b>PE-2:</b> Physical Access Authorizations <b>PE-3:</b> Physical Access Control <b>PE-3(1):</b> System Access <b>PE-4:</b> Access Control for Transmission <b>PE-5:</b> Access Control for Output Devices <b>PE-6:</b> Monitoring Physical Access <b>PE-18:</b> Location of System Components <b>PE-20:</b> Asset Monitoring and Tracking	<b>OM-DTA-001:</b> Database Administrator <b>OM-DTA-002:</b> Data Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<b>PR.DS-P1:</b> Data-at-rest is protected.	<b>MP-2:</b> Media Access <b>MP-4:</b> Media Storage <b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>SC-28:</b> Protection of Information at Rest	<b>OM-DTA-001:</b> Database Administrator <b>OM-DTA-002:</b> Data Analyst
	Data flowing between the device and MaaS360 is encrypted with Transport Layer Security.	<b>PR.DS-P2:</b> Data-in-transit is protected.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>SC-8:</b> Transmission Confidentiality and Integrity	<b>PR-CIR-001:</b> Cyber Defense Incident Responder
	Restrictions are used that prevent data flow between enterprise and personal applications.	<b>PR.DS-P5:</b> Protections against data leaks are implemented.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>AC-4:</b> Information Flow Enforcement	<b>PR-CIR-001:</b> Cyber Defense Incident Responder
	Devices that are jailbroken or otherwise modified beyond original equipment manufacturer status can be detected.	<b>PR.DS-P6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.	<b>PM-22:</b> Personally Identifiable Information Quality Management <b>SI-7:</b> Software, Firmware, and Information Integrity <b>SI-18:</b> Personally Identifiable Information Quality Operations	<b>OM-DTA-002:</b> Data Analyst <b>OM-ANA-001:</b> Systems Security Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
<b>Zimperium</b>	Zimperium checks the device for unauthorized modifications.	<b>PR.DS-P1:</b> Data-at-rest is protected.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>SC-28:</b> Protection of Information at Rest	<b>SP-ARC-002:</b> Security Architect <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>PR.DS-P2:</b> Data-in-transit is protected.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>SC-8:</b> Transmission Confidentiality and Integrity <b>SC-11:</b> Trusted Path	<b>OM-DTA-002:</b> Data Analyst <b>OM-ANA-001:</b> Systems Security Analyst
		<b>PR.DS-P6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.	<b>PM-22:</b> Personally Identifiable Information Quality Management <b>SC-16:</b> Transmission of Security Attributes <b>SI-7:</b> Boundary Protection <b>SI-10:</b> Network Disconnect <b>SI-18:</b> Personally Identifiable Information Quality Operations	<b>OM-DTA-002:</b> Data Analyst <b>OM-ANA-001:</b> Systems Security Analyst



Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
<b>Kryptowire (now known as Quokka)</b>	Kryptowire can identify applications that do not use best practices, such as lack of encryption or hardcoded credentials.	<b>CM.AW-P1:</b> 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 are established and in place.	<b>AC-8:</b> System Use Notification	<b>SP-ARC-002:</b> Security Architect  <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>CM.AW-P3:</b> System/ product/ service design enables data processing visibility.	<b>PL-8:</b> Security and Privacy Architecture  <b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information	<b>SP-ARC-002:</b> Security Architect  <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>CM.AW-P6:</b> Data provenance and lineage are maintained and can be accessed for review or transmission/ disclosure.	<b>AC-16:</b> Security and Privacy Attributes  <b>SC-16:</b> Transmission of Security Attributes	<b>SP-ARC-002:</b> Security Architect  <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>PR.DS-P1:</b> Data-at-rest is protected.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information  <b>SC-28:</b> Protection of Information at Rest	<b>SP-ARC-002:</b> Security Architect  <b>PR-CDA-001:</b> Cyber Defense Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<b>PR.DS-P2:</b> Data-in-transit is protected.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>SC-8:</b> Transmission Confidentiality and Integrity <b>SC-11:</b> Trusted Path	<b>SP-ARC-002:</b> Security Architect <b>PR-CDA-001:</b> Cyber Defense Analyst
<b>Palo Alto Networks PA-220</b>	Provides firewall and virtual private network capabilities.	<b>PR.DS-P2:</b> Data-in-transit is protected.	<b>PM-5(1):</b> System Inventory   Inventory of Personally Identifiable Information <b>SC-8:</b> Transmission Confidentiality and Integrity <b>SC-11:</b> Trusted Path	<b>SP-ARC-002:</b> Security Architect <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>PR.AC-P4:</b> Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	<b>AC-2:</b> Account Management <b>AC-3:</b> Access Enforcement <b>AC-5:</b> Separation of Duties <b>AC-6:</b> Least Privilege <b>AC-24:</b> Access Control Decisions	<b>SP-ARC-002:</b> Security Architect <b>PR-CDA-001:</b> Cyber Defense Analyst
		<b>PR.AC-P5:</b> Network integrity is protected (e.g., network segregation, network segmentation).	<b>AC-4:</b> Information Flow Enforcement <b>AC-10:</b> Access Control <b>SC-7:</b> Boundary Protection <b>SC-10:</b> Network Disconnect	<b>OM-DTA-002:</b> Data Analyst <b>OM-ANA-001:</b> Systems Security Analyst

Product	Function	Applicable Privacy Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Privacy-Related Controls	Applicable NIST SP 800-181, NICE Framework Work Roles (2017)
		<p><b>PR.PT-P3:</b> Communications and control networks are protected.</p>	<p><b>AC-12:</b> Session Termination</p> <p><b>AC-17:</b> Remote Access</p> <p><b>AC-18:</b> Wireless Access</p> <p><b>SC-5:</b> Denial of Service Protection</p> <p><b>SC-7:</b> Boundary Protection</p> <p><b>SC-10:</b> Network Disconnect</p> <p><b>SC-11:</b> Trusted Path</p> <p><b>SC-21:</b> Secure Name/Address Resolution Service (Recursive or Caching Resolver)</p> <p><b>SC-23:</b> Session Authenticity</p>	<p><b>OV-LGA-002:</b> Privacy Officer/Privacy Compliance Manager</p> <p><b>PR-CDA-001:</b> Cyber Defense Analyst</p>
<p><b>Qualcomm</b></p>	<p>The trusted execution environment provides data confidentiality and integrity.</p>	<p><b>PR.DS-P6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p><b>PM-22:</b> Personally Identifiable Information Quality Management</p> <p><b>SC-16:</b> Transmission of Security and Privacy Attributes</p> <p><b>SI-7:</b> Software, Firmware, and Information Integrity</p> <p><b>SI-10:</b> Information Input Validation</p> <p><b>SI-18:</b> Personally Identifiable Information Quality Operations</p>	<p><b>PR-INF-001:</b> Cyber Defense Infrastructure Support Specialist</p> <p><b>OM-ANA-001:</b> Systems Security Analyst</p>

# Mobile Device Security:

## Bring Your Own Device (BYOD)

---

**Supplement:**

**Example Scenario: Putting Guidance into Practice**

**Kaitlin Boeckl**

**Nakia Grayson**

**Gema Howell**

**Naomi Lefkowitz**

Applied Cybersecurity Division  
Information Technology Laboratory

**Jason Ajmo**

**R. Eugene Craft**

**Milissa McGinnis\***

**Kenneth Sandlin**

**Oksana Slivina**

**Julie Snyder**

**Paul Ward**

The MITRE Corporation  
McLean, VA

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

September 2023

FINAL

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



## DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-22 Supplement Natl. Inst. Stand. Technol. Spec. Publ. 1800-22 Supplement, 61 pages, (September 2023), CODEN: NSPUE2

## FEEDBACK

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

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

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

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

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution

## ABSTRACT

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

Incorporating BYOD deployments into an organization can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of traditional in-office processes with mobile device technologies enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-first approach in which their employees communicate and collaborate primarily using their mobile devices.

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

Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks. Solutions that are designed to secure corporate devices and on-premises data do not provide an effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new privacy risks to employees by providing their employer a degree of access to their personal devices, opening up the possibility of observation and control that would not otherwise exist.

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

Name	Organization
William Newhouse	NIST
Cherilyn Pascoe	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST
Chris Brown	The MITRE Corporation
Nancy Correll*	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston*	The MITRE Corporation
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Jessica Walton	The MITRE Corporation
Erin Wheeler*	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward*	IBM
Cesare Coscia*	IBM
Chris Gogoel	Kryptowire (now known as Quokka)
Tom Karygiannis*	Kryptowire (now known as Quokka)
Jeff Lamoureux	Palo Alto Networks
Sean Morgan	Palo Alto Networks



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

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

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

Technology Partner/Collaborator	Build Involvement
IBM	Mobile Device Management
Kryptowire (now known as Quokka)	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

## DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

## **PATENT DISCLOSURE NOTICE**

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

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

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

## Contents

<b>1</b>	<b>Applying This Build: Example Scenario</b>	<b>1</b>
1.1	Standards and Guidance Used in this Example Scenario	1
<b>2</b>	<b>About Great Seneca Accounting</b>	<b>2</b>
2.1	Great Seneca Accounting’s Business/Mission Objectives	5
<b>3</b>	<b>Great Seneca Accounting’s Target Profiles</b>	<b>6</b>
<b>4</b>	<b>Great Seneca Accounting Embraces BYOD</b>	<b>13</b>
<b>5</b>	<b>Applying NIST Risk Management Methodologies to Great Seneca Accounting’s BYOD Architecture</b>	<b>15</b>
5.1	Using Great Seneca Accounting’s Target Profiles	15
5.2	Great Seneca Uses the Target Profiles to Help Prioritize Security and Privacy Control Deployment	16
5.2.1	Identifying and Tailoring the Baseline Controls	17
5.3	Great Seneca Accounting Performs a Risk Assessment	18
5.4	Great Seneca Accounting Tailors Their Security and Privacy Control Baselines	18
5.4.1	An Example Tailoring of the System and Communications Protection Security Control Family	18
<b>Appendix A</b>	<b>List of Acronyms</b>	<b>21</b>
<b>Appendix B</b>	<b>Glossary</b>	<b>22</b>
<b>Appendix C</b>	<b>References</b>	<b>24</b>
<b>Appendix D</b>	<b>A Note Regarding Great Seneca Accounting</b>	<b>26</b>
<b>Appendix E</b>	<b>How Great Seneca Accounting Applied NIST Risk Management Methodologies</b>	<b>27</b>
E.1	Overview of Risk Frameworks and Tools That Great Seneca Used	27
E.1.1	Overview of the NIST Cybersecurity Framework	27
E.1.2	Overview of the NIST Privacy Framework	28
E.1.3	Overview of the NIST Risk Management Framework	28
E.1.4	Overview of the NIST Privacy Risk Assessment Methodology	29
E.2	Using Frameworks to Establish or Improve Cybersecurity and Privacy Programs	29

**Appendix F How Great Seneca Accounting Used the NIST Risk Management Framework.....32**

- F.1 Understanding the Risk Assessment Process..... 32
- F.2 Risk Assessment of Great Seneca Accounting’s BYOD Program ..... 33
- F.3 Development of Threat Event Descriptions ..... 34
- F.4 Great Seneca Accounting’s Leadership and Technical Teams Discuss BYOD’s Potential Threats to Their Organization..... 35
  - F.4.1 Threat Event 1 ..... 36
  - F.4.2 Threat Event 2 ..... 36
  - F.4.3 Threat Event 3 ..... 37
  - F.4.4 Threat Event 4 ..... 38
  - F.4.5 Threat Event 5 ..... 38
  - F.4.6 Threat Event 6 ..... 39
  - F.4.7 Threat Event 7 ..... 39
  - F.4.8 Threat Event 8 ..... 40
  - F.4.9 Threat Event 9 ..... 41
  - F.4.10 Threat Event 10 ..... 41
  - F.4.11 Threat Event 11 ..... 42
  - F.4.12 Threat Event 12 ..... 42
- F.5 Identification of Vulnerabilities and Predisposing Conditions..... 43
- F.6 Summary of Risk Assessment Findings ..... 43

**Appendix G How Great Seneca Accounting Used the NIST Privacy Risk Assessment Methodology .....46**

- G.1 Privacy Risk 1: Wiping Activities on the User’s Device May Inadvertently Delete the User’s Personal Data ..... 46
- G.2 Privacy Risk 2: Organizational Collection of Device Data May Subject Users to Feeling or Being Surveilled ..... 47
- G.3 Privacy Risk 3: Data Collection and Transmission Between Integrated Security Products May Expose User Data ..... 48
- G.4 Mitigations Applicable Across Various Privacy Risks ..... 49
- G.5 Privacy References for Example Solution Technologies ..... 50

# List of Figures

- Figure 2-1 Great Seneca Accounting’s Work Environments .....3
- Figure 2-2 Example Solution Architecture .....4
- Figure 2-3 Great Seneca Accounting's Security and Privacy Risk Management Steps .....5
- Figure 4-1 Great Seneca Accounting’s Current Mobile Deployment Architecture (Before Security and Privacy Enhancements).....14
- Figure 5-1 Cybersecurity Framework Subcategory to Informative Reference Mapping .....16
- Figure 5-2 Security and Privacy Objectives .....17
- Figure 5-3 Subcategory DE.CM-5 Mapping to BYOD-Related Business/Mission Objectives.....19
- Figure 5-4 Subcategory PR.AC-5 Mapping to BYOD-Related Business/Mission Objectives.....20
- Figure E-1 Comparing Framework Processes to Establish or Improve Programs.....30
- Figure F-1 Risk Assessment Process .....33
- Figure F-2 NIST SP 800-30 Generic Risk Model.....34

# List of Tables

- Table 3-1 Great Seneca Accounting’s Cybersecurity Framework Target Profile .....8
- Table 3-2 Great Seneca Accounting’s Privacy Target Profile .....10
- Table F-1 Great Seneca Accounting’s BYOD Deployment Threats .....34
- Table F-2 Threat Event Mapping to the Mobile Threat Catalogue .....35
- Table F-3 Identify Vulnerabilities and Predisposing Conditions .....43
- Table F-4 Summary of Risk Assessment Findings .....44
- Table G-1 Privacy References for the Example Solution Technologies .....50

# 1 Applying This Build: Example Scenario

This document provides guidance for leveraging standards and tools to reduce cybersecurity and privacy risks in a Bring Your Own Device (BYOD) implementation. This document uses an example scenario - using a fictional company named Great Seneca Accounting—to outline specific steps an organization could take. The example shows how BYOD objectives can align with a fictional organization’s security and privacy priorities using 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 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) [\[1\]](#)
- 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.

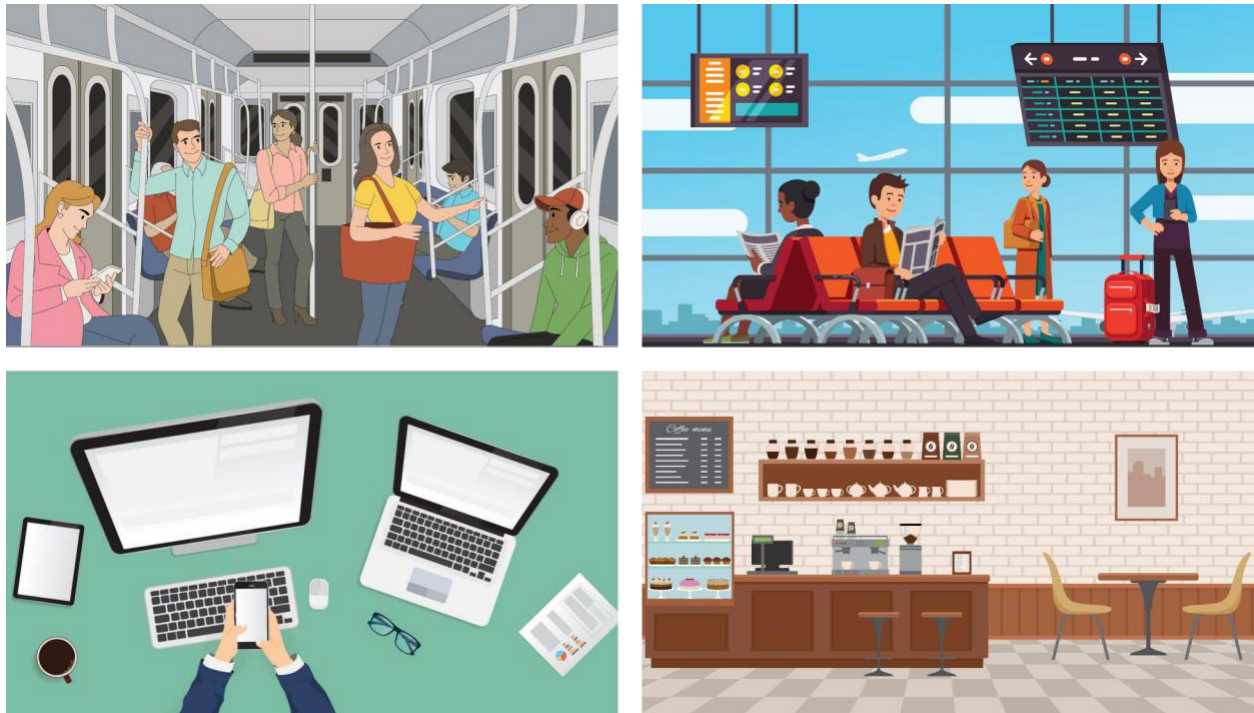
When the firm was first created, most of its employees worked from the Great Seneca Accounting office, with minimal use of mobile devices. They were able to do this without actively embracing mobile device usage because most of the employees worked at their desks at the company's single location.

Over the years, the Great Seneca Accounting company grew from a local company, where all 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, the need to support employees to work remotely as a strategic priority, while both traveling and working from a customer location. Consequently, the company wants to embrace BYOD solutions to support its remote work.

Figure 2-1 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 2-1 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 2-2, 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

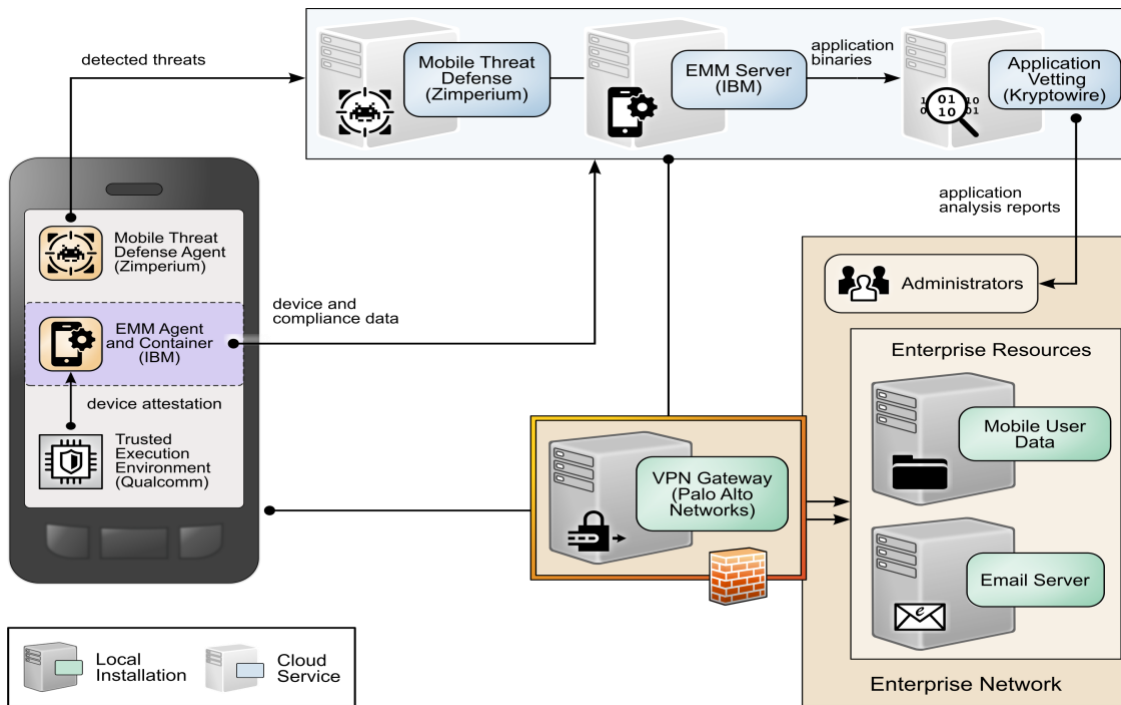
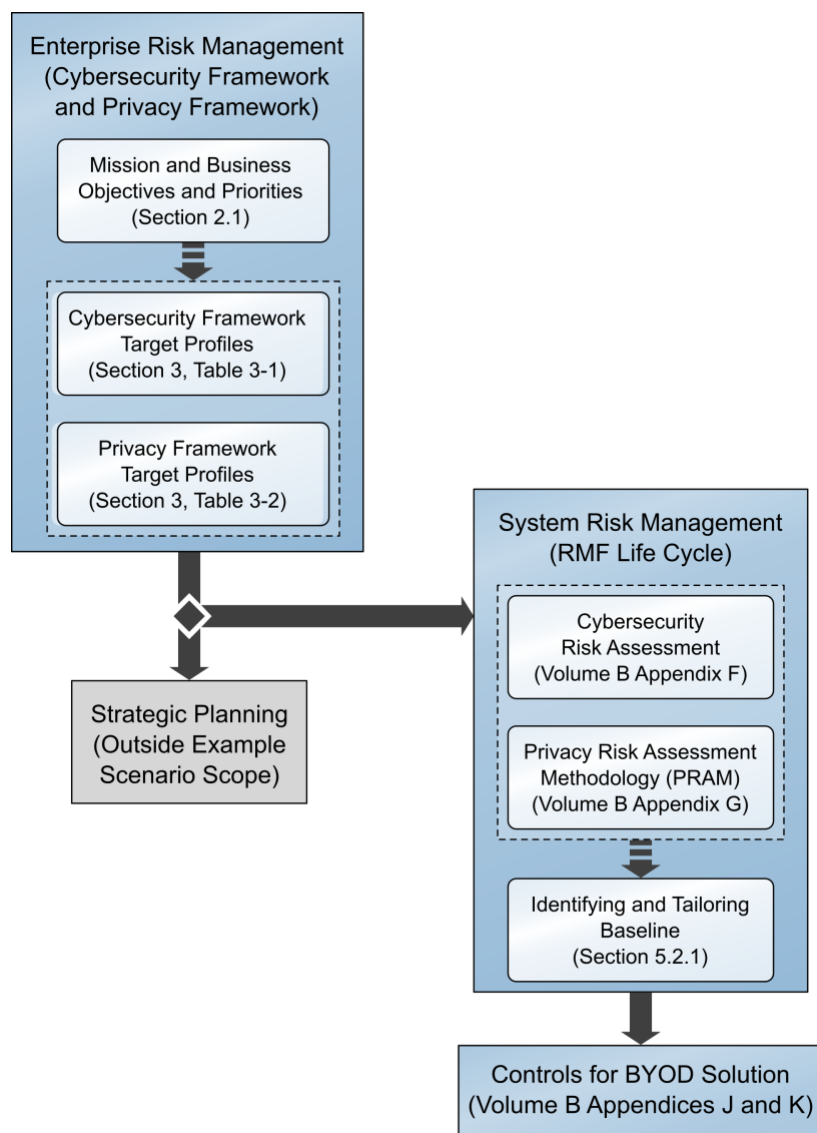


Figure 2-3 shows the overall process that Great Seneca Accounting plans to follow. It highlights key activities from various NIST guidance documents related to security and privacy risk management, each of which is discussed in the sections identified in Figure 2-3. Please note that this process is an 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



## 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:

- Mission Objective 1—Provide good data stewardship

- Mission Objective 2—Enable timely communication with clients
- Mission Objective 3—Provide innovative financial services
- Mission Objective 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

Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
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 segregation, network segmentation).	high	high	high	high
		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

Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
		<b>PR.DS-8:</b> Integrity checking mechanisms are used to verify hardware integrity.	moderate	moderate	moderate	low
	<b>Information Protection Processes and Procedures</b>	<b>PR.IP-1:</b> A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.	moderate	moderate	moderate	low
	<b>Protective Technology</b>	<b>PR.PT-4:</b> Communications and control networks are protected.	low	moderate	moderate	low
<b>DETECT</b>	<b>Anomalies and Events</b>	<b>DE.AE-5:</b> Incident alert thresholds are established.	high	high	high	high
	<b>Security Continuous Monitoring</b>	<b>DE.CM-4:</b> Malicious code is detected.	high	high	high	high
		<b>DE.CM-5:</b> Unauthorized mobile code is detected.	moderate	moderate	moderate	low
		<b>DE.CM-8:</b> Vulnerability scans are performed.	high	high	high	high

Table 3-2 Great Seneca Accounting’s Privacy Target Profile

Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
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
		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

Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
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 selective collection or disclosure of data elements.	high	high	high	high
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,	PR.AC-P2: Physical access to data and devices is managed.	high	moderate	high	moderate



Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
	<b>Authentication, and Access Control</b>	<b>PR.AC-P4:</b> Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	high	moderate	high	moderate
		<b>PR.AC-P5:</b> Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high
		<b>PR.DS-P1:</b> Data-at-rest is protected.	high	moderate	moderate	high
	<b>Data Security</b>	<b>PR.DS-P2:</b> Data-in-transit is protected.	moderate	high	moderate	high
		<b>PR.DS-P5:</b> Protections against data leaks are implemented.	high	moderate	high	moderate
		<b>PR.DS-P6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		<b>PR.PT-P3:</b> 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. In order to be able to work in all 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 was recently 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)

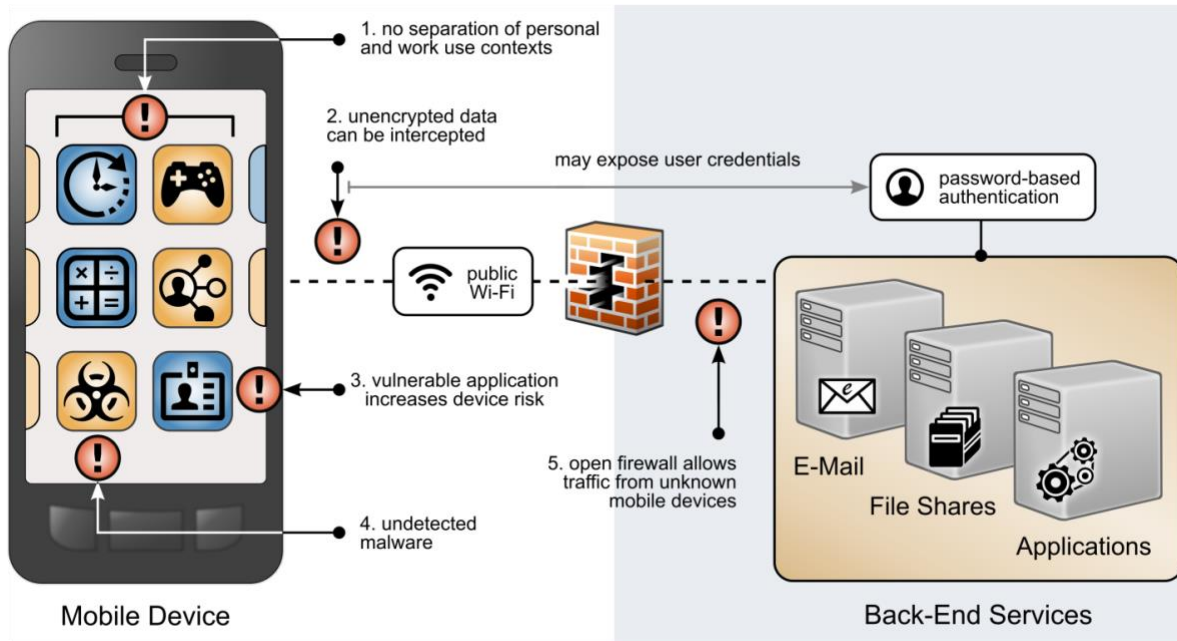


Figure 4-1 highlights the following vulnerabilities with a red exclamation mark:

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

[Section 2](#) and [Section 3](#) above describe 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 Appendices E and F for additional information on the security and privacy outcomes that this document’s example solution supports. Appendices E and F 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 E provides the Cybersecurity Framework Subcategory mappings, and Volume B’s Appendix F provides the Privacy Framework Subcategory mappings.

## 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.

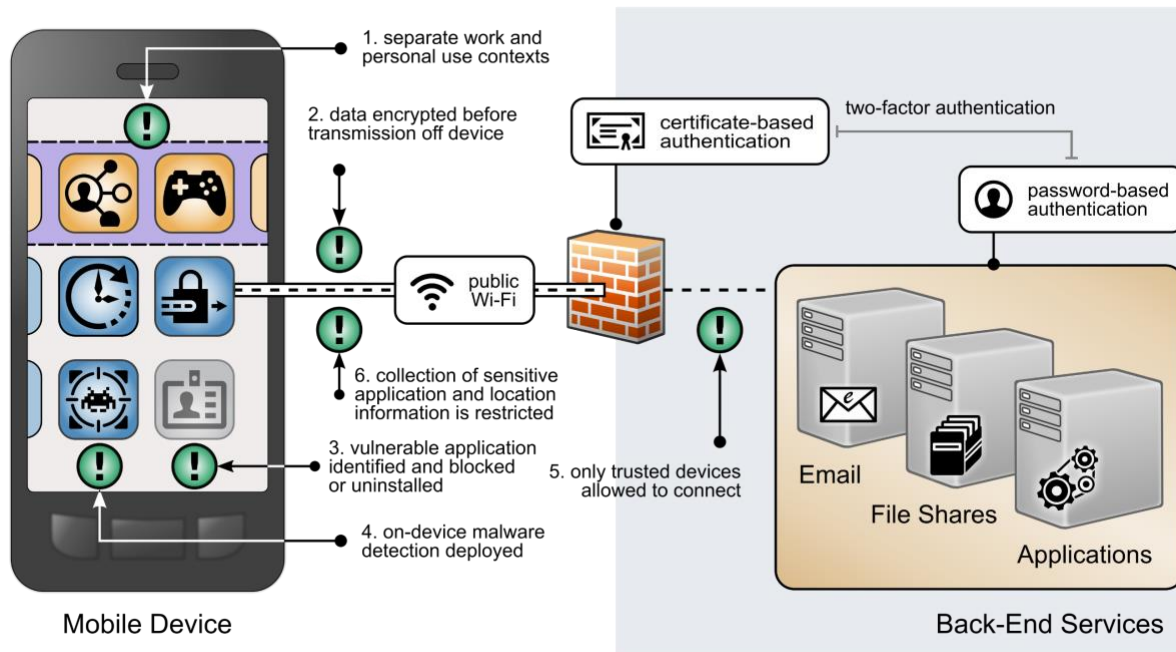
By comparing its Cybersecurity Framework Target Profile (Table 3-1) with the Subcategories supported by the example solution that are shown in Volume B’s Appendix F, Great Seneca Accounting determines that the example solution will help it achieve its desired Cybersecurity Framework Target Profile outcomes.

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 objectives, 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 objectives shown in Figure 5-2, they 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 5-2 Security and Privacy Objectives



Volume B’s Appendices E and F 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 Appendix G in this document 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 using a green box in Figure 5-3.

**Figure 5-3 Subcategory DE.CM-5 Mapping to BYOD-Related Business/Mission Objectives**

Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
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

- 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 support 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 is highlighted using a green box in Figure 5-4. All



Subcategory prioritizations (including PR.AC-5's shown below) can be found in [Table 3-1](#).

**Figure 5-4 Subcategory PR.AC-5 Mapping to BYOD-Related Business/Mission Objectives**

Function	Category	Subcategory	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4
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 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 control implementations (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 reassess 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 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.*

## Appendix A List of Acronyms

<b>BYOD</b>	Bring Your Own Device
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>EMM</b>	Enterprise Mobility Management
<b>FIPS</b>	Federal Information Processing Standards
<b>IBM</b>	International Business Machines
<b>ICS</b>	Industrial Control System
<b>iOS</b>	iPhone Operating System
<b>IP</b>	Internet Protocol
<b>ITL</b>	Information Technology Laboratory
<b>MDM</b>	Mobile Device Management
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NICE</b>	National Initiative for Cybersecurity Education
<b>NIST</b>	National Institute of Standards and Technology
<b>NISTIR</b>	NIST Interagency Report
<b>OS</b>	Operating System
<b>PII</b>	Personally Identifiable Information
<b>PIN</b>	Personal Identification Number
<b>PRAM</b>	Privacy Risk Assessment Methodology
<b>RMF</b>	Risk Management Framework
<b>SC</b>	Systems and Communications Protection
<b>SMS</b>	Short Message Service
<b>SP</b>	Special Publication
<b>URL</b>	Uniform Resource Locator
<b>VPN</b>	Virtual Private Network

## Appendix B Glossary

<b>Access Management</b>	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 <a href="#">[11]</a> .
<b>Availability</b>	Ensure that users can access resources through remote access whenever needed <a href="#">[12]</a> .
<b>Bring Your Own Device (BYOD)</b>	A non-organization-controlled telework client device <a href="#">[12]</a> .
<b>Confidentiality</b>	Ensure that remote access communications and stored user data cannot be read by unauthorized parties <a href="#">[12]</a> .
<b>Data Actions</b>	System operations that process PII <a href="#">[13]</a> .
<b>Disassociability</b>	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system <a href="#">[13]</a> .
<b>Eavesdropping</b>	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 <a href="#">[14]</a> (definition located under eavesdropping attack).
<b>Firewall</b>	Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures <a href="#">[15]</a> .
<b>Integrity</b>	Detect any intentional or unintentional changes to remote access communications that occur in transit <a href="#">[12]</a> .
<b>Manageability</b>	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure <a href="#">[13]</a> .
<b>Mobile Device</b>	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 <a href="#">[10]</a> .

<b>Personally Identifiable Information (PII)</b>	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 <a href="#">[16]</a> (adapted from Government Accountability Office Report 08-536).
<b>Problematic Data Action</b>	A data action that could cause an adverse effect for individuals <a href="#">[2]</a> .
<b>Threat</b>	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 <a href="#">[8]</a> .
<b>Vulnerability</b>	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source <a href="#">[8]</a> .

## 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 rev. 1, NIST, Gaithersburg, Md., Nov. 2020. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>.
- [4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](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>.

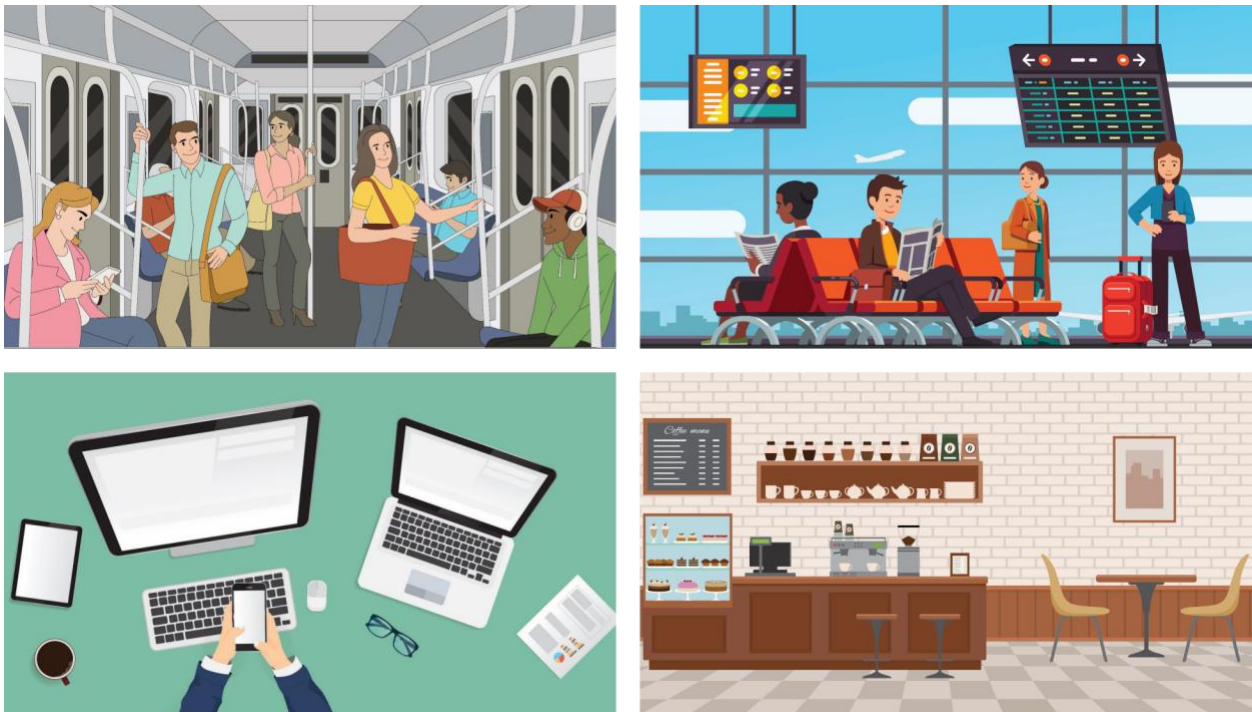
- [13] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.
- [14] P. Grassi et al., *Digital Identity Guidelines*, 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/2021/NIST.IR.8170-upd.pdf>.

## 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.

[Section E.1](#) below 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 Volume B 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 systems, products, and services while protecting individuals' privacy. It follows the structure of the NIST 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 are supported by the system.

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

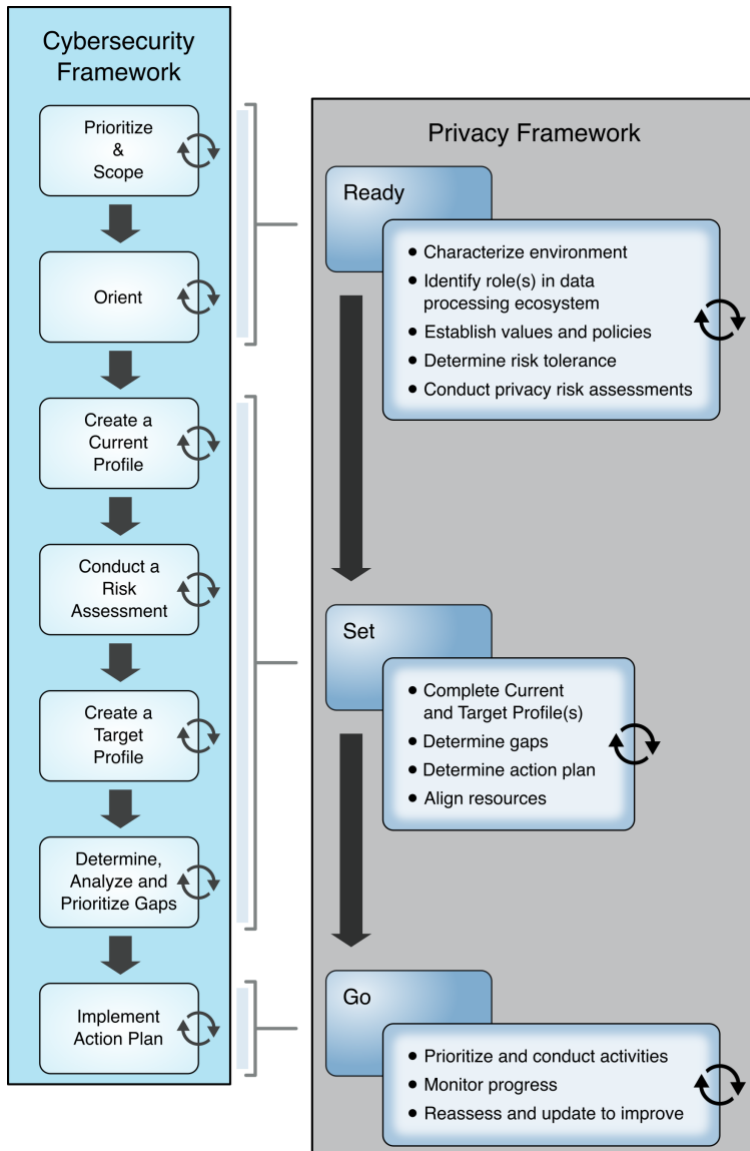
While their presentation differs, the NIST Cybersecurity Framework and NIST Privacy Framework also both provide complementary guidance for establishing and improving cybersecurity and privacy programs. The NIST Cybersecurity Framework’s process for establishing or improving programs provides seven steps 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 for 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**



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.

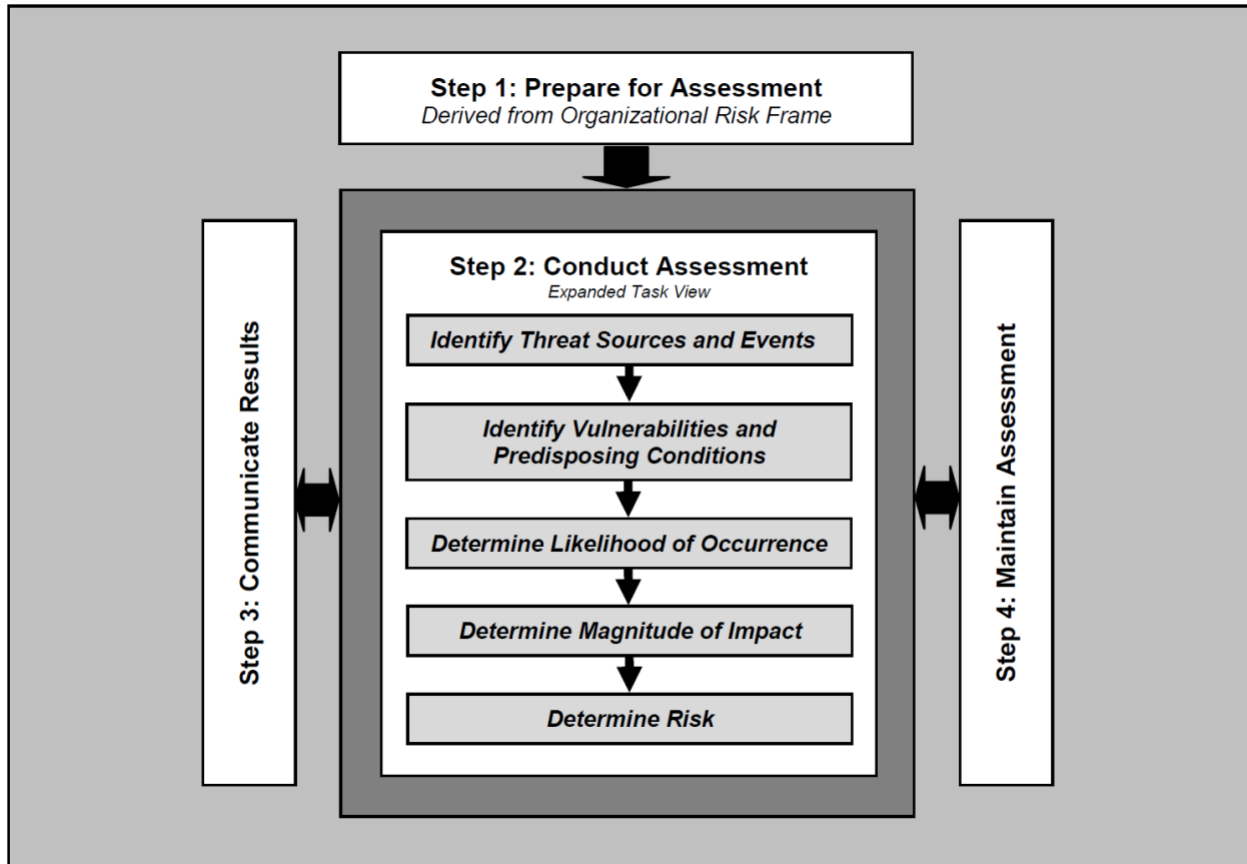
The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

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



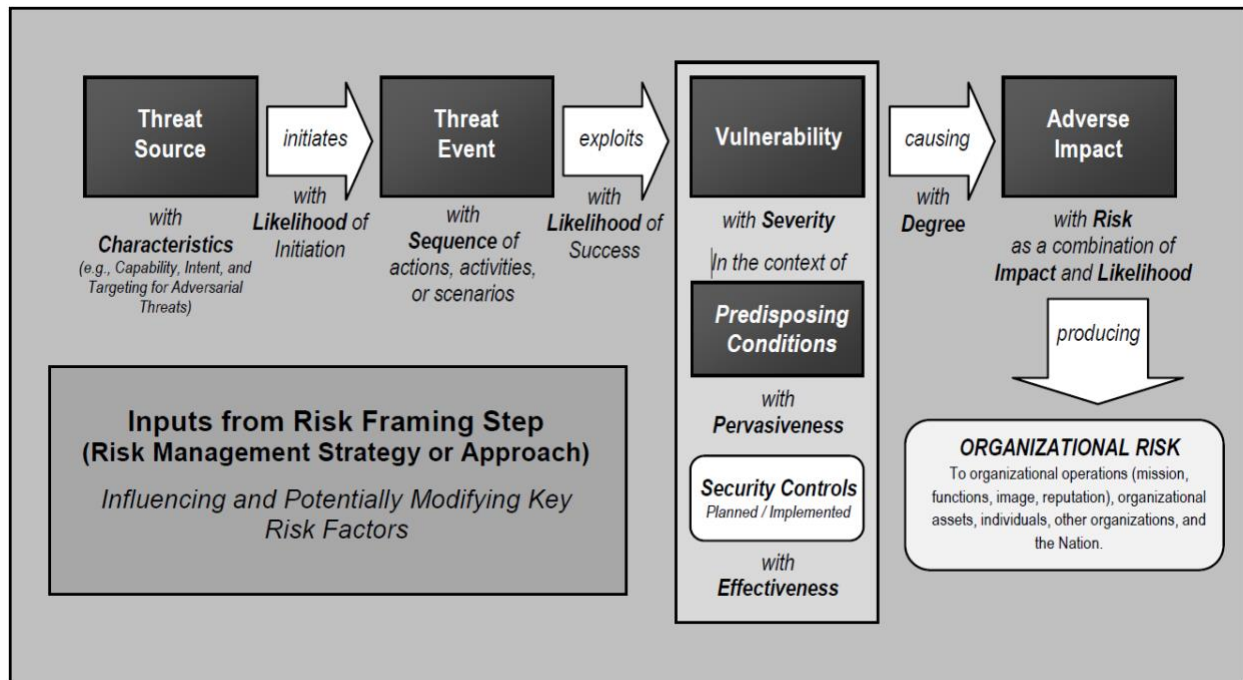
## F.2 Risk Assessment of Great Seneca Accounting’s BYOD Program

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



### 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

Great Seneca Accounting's Threat Event Identification Number	Threat Event Description
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
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. One goal of the example solution contained within this



practice guide is to mitigate the impact of these threat events. Reference Table 5-1 in Volume B 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 a 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 poor application development 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 Event 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 non-employee 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 an 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](#).

**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

## F.6 Summary of Risk Assessment Findings

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



**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
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	VULN-3	high	high	high

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
unauthorized storage in non-organizationally managed services				
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.

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 provided below, along with potential mitigations.

### G.1 Privacy Risk 1: Wiping Activities on the User's Device May Inadvertently Delete the User's Personal Data

**Privacy Risk:** Removal of personal data from a device.

**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 within the work container, but these photos are lost when their device is selectively wiped after anomalous activity is detected. This privacy risk is related to the Unwarranted Restriction Problematic Data Action.

#### Mitigations:

- **Block access to corporate resources by removing the 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 appropriately store and 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 and to not store personal data within the work container on their device.

- **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 Privacy Risk 2: Organizational Collection of Device Data May Subject Users to Feeling or Being Surveilled

**Privacy Risk:** The assessed infrastructure offers Great Seneca Accounting and its employees a number of security capabilities, including reliance on comprehensive monitoring capabilities, as noted in Volume B 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 or understand the way these interactions are being analyzed or used. If there is awareness, employees may feel compelled to allow for monitoring to occur for the ability to use their mobile devices for corporate access. 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 or loss of autonomy if the employee discovers monitoring that they did not anticipate or expect. This privacy risk is related to the Surveillance Problematic Data Action.

**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 Privacy Risk 3: Data Collection and Transmission Between Integrated Security Products May Expose User Data

**Privacy Risk:** 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 an unanticipated release of employee information. This privacy risk is related to the Unanticipated Revelation Problematic Data Action.

## Mitigations:

- **De-identify personal and device data when that 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 specific 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 Privacy Risks

Several mitigations benefit employees in all three privacy risks 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	<a href="https://www.ibm.com/docs/en/search/privacy">https://www.ibm.com/docs/en/search/privacy</a> <a href="https://www.ibm.com/support/pages/node/571227">https://www.ibm.com/support/pages/node/571227</a> <a href="https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_privacy.htm">https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_privacy.htm</a> <a href="https://www.ibm.com/support/pages/maas360-data-privacy-information">https://www.ibm.com/support/pages/maas360-data-privacy-information</a>
Kryptowire Cloud Service	application vetting	<a href="https://www.kryptowire.com">https://www.kryptowire.com</a>
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	<a href="https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/host-information/about-host-information/what-data-does-the-globalprotect-app-collect-on-each-operating-system">https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/host-information/about-host-information/what-data-does-the-globalprotect-app-collect-on-each-operating-system</a> <a href="https://www.paloaltonetworks.com/resources/datasheets/url-filtering-privacy-datasheet">https://www.paloaltonetworks.com/resources/datasheets/url-filtering-privacy-datasheet</a>

Commercially Available Product	Mobile Security Technology	Product Privacy Information Location
Qualcomm (Version is mobile device dependent)	trusted execution environment	<a href="https://www.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf">https://www.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf</a>
Zimperium Defense Suite Zimperium Console Version vGA-4.23.1 Zimperium zIPS Agent Version 4.9.2 (Android and iOS)	mobile threat defense	<a href="https://www.zimperium.com/mobile-app-protection">https://www.zimperium.com/mobile-app-protection</a>



# Mobile Device Security:

## Bring Your Own Device (BYOD)

---

**Volume C:**  
**How-To Guides**

**Kaitlin Boeckl**

**Nakia Grayson**

**Gema Howell**

**Naomi Lefkowitz**

Applied Cybersecurity Division  
Information Technology Laboratory

**Jason Ajmo**

**R. Eugene Craft**

**Milissa McGinnis\***

**Kenneth Sandlin**

**Oksana Slivina**

**Julie Snyder**

**Paul Ward**

The MITRE Corporation  
McLean, VA

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

September 2023

FINAL

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



## DISCLAIMER

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

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

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

## FEEDBACK

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

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

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

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

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution

## ABSTRACT

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

Incorporating BYOD deployments into an organization can increase the opportunities and methods available to access organizational resources. For some organizations, the combination of traditional in-office processes with mobile device technologies enables portable communication approaches and adaptive workflows. For others, it fosters a mobile-first approach in which their employees communicate and collaborate primarily using their mobile devices.

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

Enabling BYOD capabilities in the enterprise introduces new cybersecurity risks. Solutions that are designed to secure corporate devices and on-premises data do not provide an effective cybersecurity solution for BYOD. Finding an effective solution can be challenging due to the unique risks that BYOD deployments impose. Additionally, enabling BYOD capabilities introduces new privacy risks to employees by providing their employer a degree of access to their personal devices, opening up the possibility of observation and control that would not otherwise exist.

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

Name	Organization
William Newhouse	NIST
Cherilyn Pascoe	NIST
Murugiah Souppaya	NIST
Kevin Stine	NIST
Chris Brown	The MITRE Corporation
Nancy Correll*	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Parisa Grayeli	The MITRE Corporation
Marisa Harriston*	The MITRE Corporation
Brian Johnson*	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Steven Sharma*	The MITRE Corporation
Jessica Walton	The MITRE Corporation
Erin Wheeler*	The MITRE Corporation
Dr. Behnam Shariati	University of Maryland, Baltimore County
Jeffrey Ward*	IBM
Cesare Coscia*	IBM
Chris Gogoel	Kryptowire (now known as Quokka)
Tom Karygiannis*	Kryptowire (now known as Quokka)
Jeff Lamoureux	Palo Alto Networks
Sean Morgan	Palo Alto Networks

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

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

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

Technology Partner/Collaborator	Build Involvement
IBM	Mobile Device Management
Kryptowire (now known as Quokka)	Application Vetting
Palo Alto Networks	Firewall; Virtual Private Network
Qualcomm	Trusted Execution Environment
Zimperium	Mobile Threat Defense

## DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

## PATENT DISCLOSURE NOTICE

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

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

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

# Contents

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



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

## List of Figures

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

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

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

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

# 1 Introduction

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

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

## 1.1 Practice Guide Structure

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

This guide contains four volumes:

- NIST SP 1800-22A: *Executive Summary*
- NIST SP 1800-22B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-22 Supplement: *Example Scenario: Putting Guidance into Practice* – how organizations can implement this example solution's guidance
- NIST SP 1800-22C: *How-To Guides* – instructions for building the example solution (**you are here**)

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

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

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

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

- Section 3.4, Risk Assessment, describes the risk analysis we performed.
- Appendix E in Volume B, Example Security Subcategory and Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

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

**IT professionals** who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-22C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

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

**For those who would like to see how the example solution can be implemented**, this practice guide contains an example scenario about a fictional company called Great Seneca Accounting. The example scenario shows how BYOD objectives can align with an organization's priority security and privacy capabilities through NIST risk management standards, guidance, and tools. It is provided in this practice guide's supplement, *NIST SP 1800-22 Example Scenario: Putting Guidance into Practice*.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to [mobile-nccoe@nist.gov](mailto:mobile-nccoe@nist.gov).

## 1.2 Build Overview

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

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

### 1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

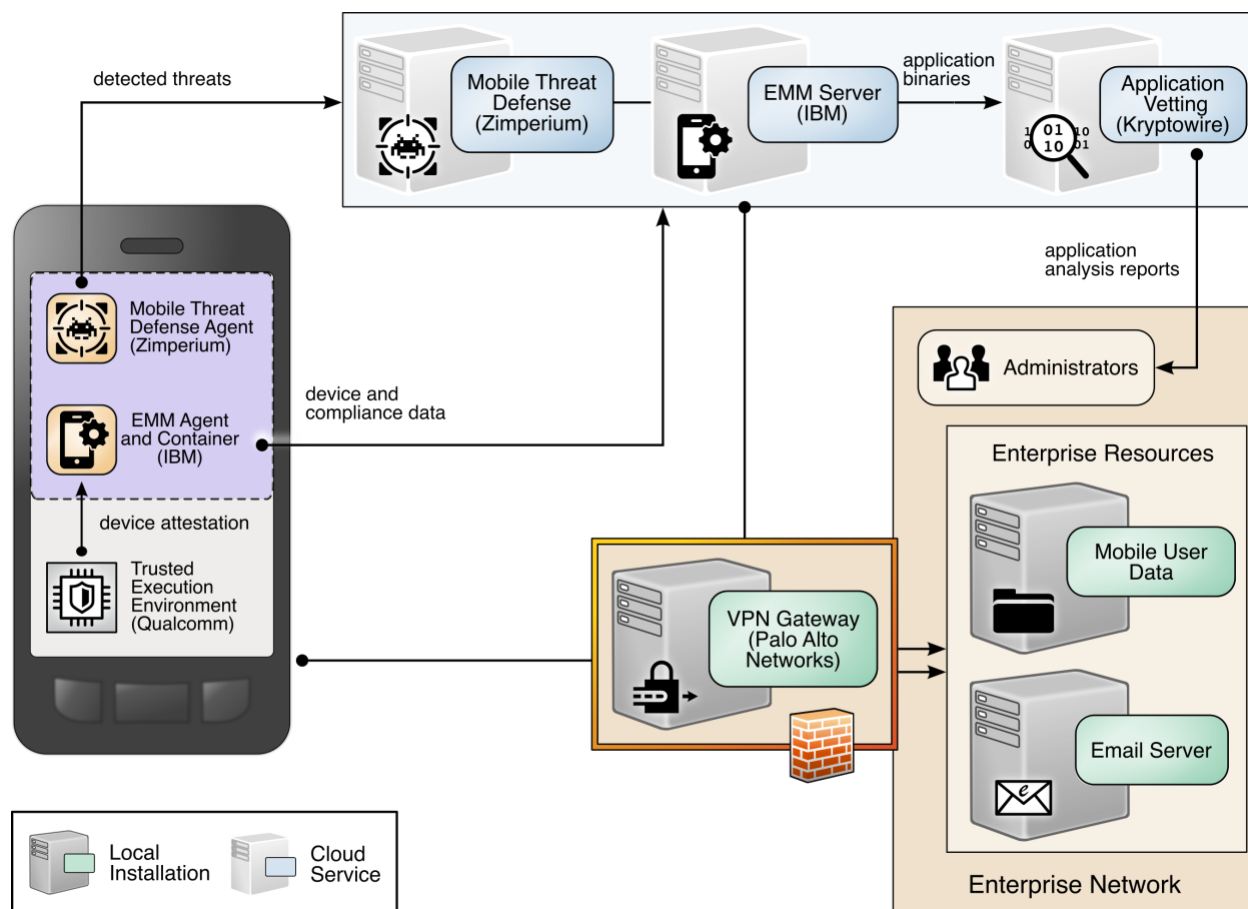
Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File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

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

### 1.4 Logical Architecture Summary

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

Figure 1-1 High-Level Build Architecture



## 2 Product Installation Guides

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

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

### 2.1 Network Device Enrollment Services Server

A Network Device Enrollment Service (NDES)/Simple Certificate Enrollment Protocol (SCEP) server was used to issue client certificates to new devices that were enrolled by using MaaS360. This guide assumes that a basic AD and certificate authority (CA) are in place, containing a root and subordinate CA, and that their certificates have been exported.

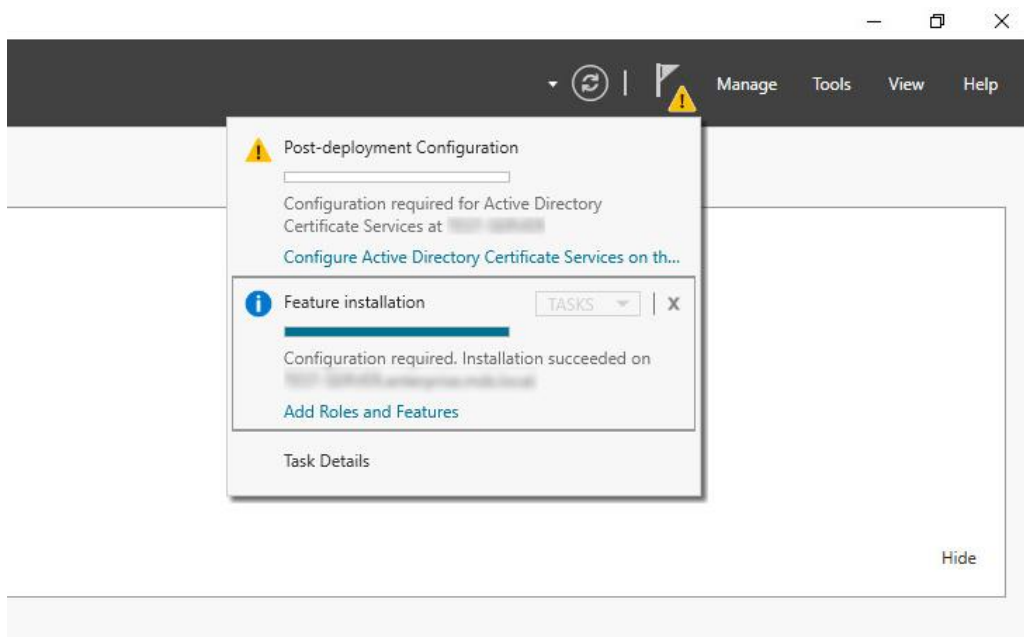
#### 2.1.1 NDES Configuration

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



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

Figure 2-1 Post-Deployment Configuration



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

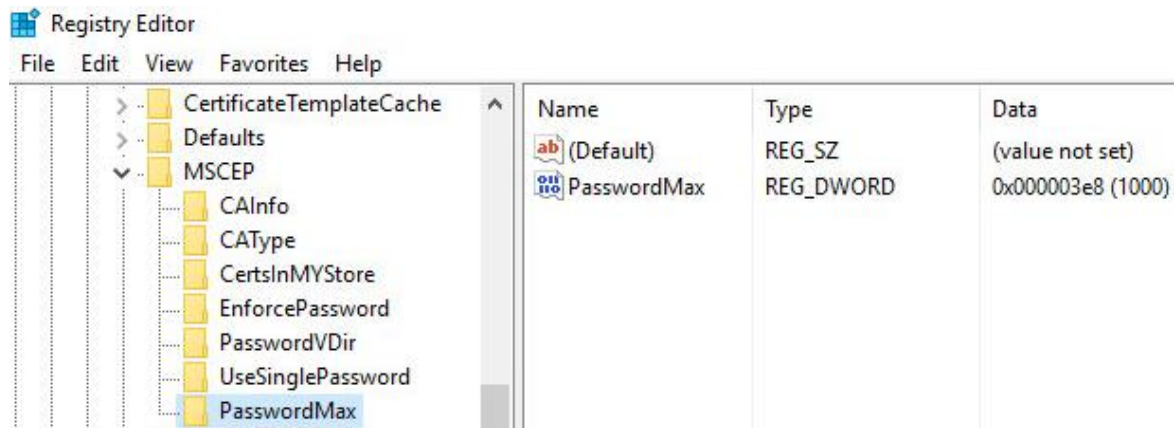
*Note: The domain administrator credentials are required only to configure the NDES. Once the service is configured, the service is executed as the NDES service account, which does not require domain administrator permissions, created in step 12 below.*

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

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

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

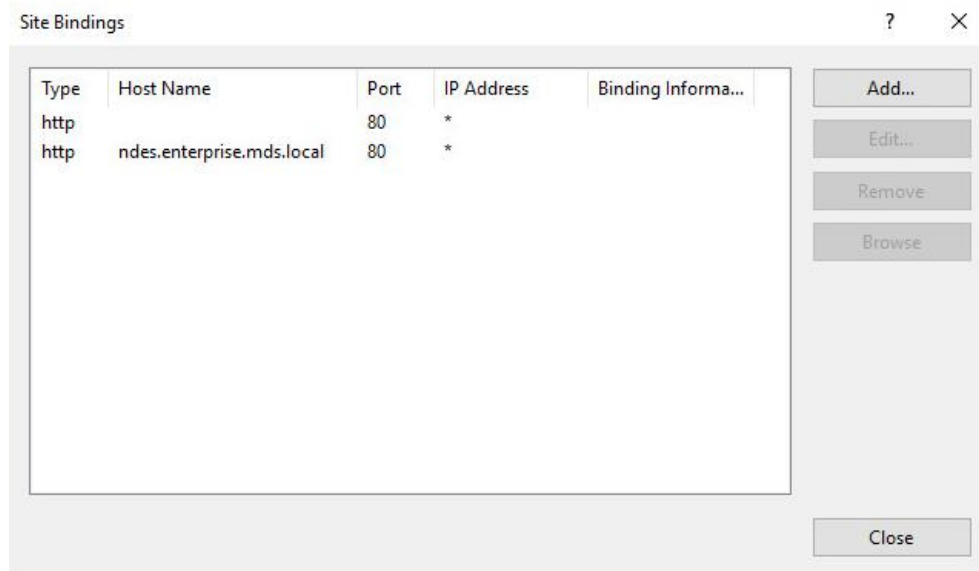
Figure 2-2 PasswordMax Registry Configuration



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

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

Figure 2-3 NDES Domain Bindings



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

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

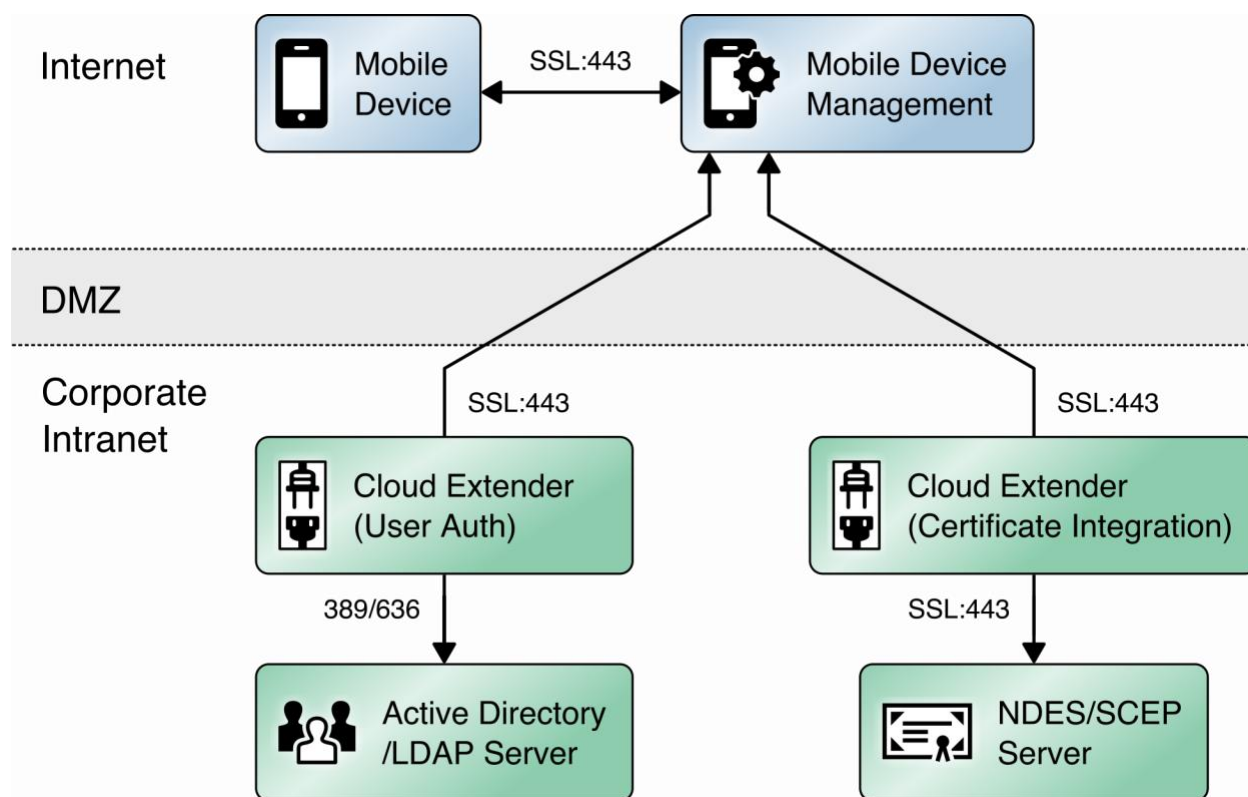
## 2.2 International Business Machines MaaS360

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

### 2.2.1 Cloud Extender

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

Figure 2-4 Cloud Extender Architecture



### 2.2.1.1 Cloud Extender Download

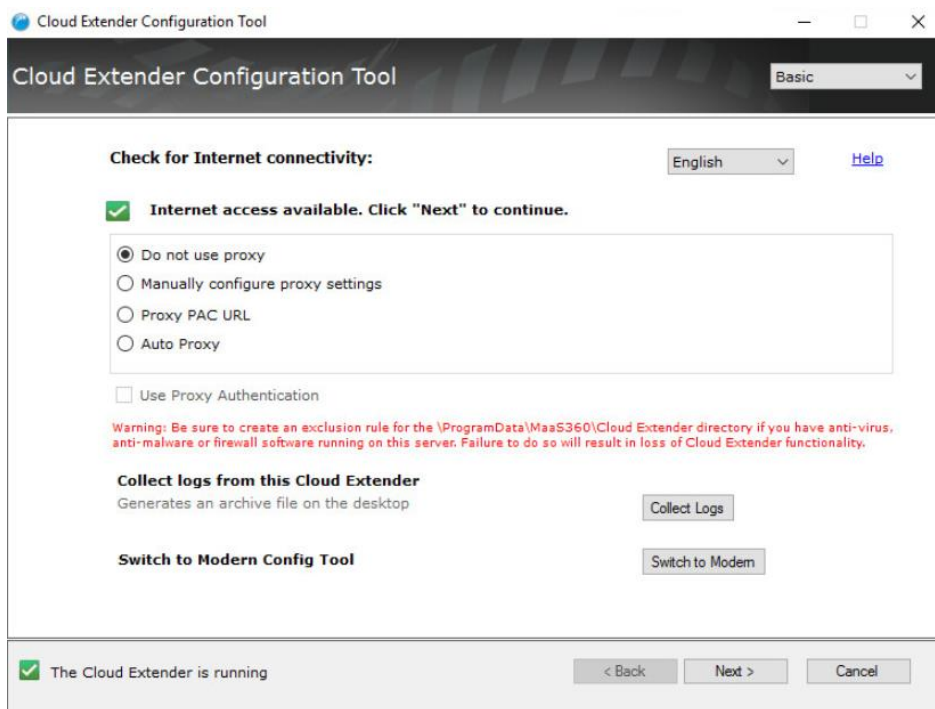
1. Log in to the MaaS360 web portal.
2. Click **Setup > Cloud Extender**.
3. Click the link that says **Click here to get your License Key**. The license key will be emailed to the currently logged-in user's email address.
4. Click the link that says **Click here to download the Cloud Extender**. Save the binary.
5. Move the binary to a machine behind the corporate firewall that is always online. Recommendation: Install it while logged in as a domain user on a machine that is not the domain controller.
6. Install **.NET 3.5 Features** in the **Server Manager** on the machine where the MaaS360 Cloud Extender will run.

### 2.2.1.2 Cloud Extender Active Directory Configuration

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

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

Figure 2-5 Old Cloud Extender Interface



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

Figure 2-6 Cloud Extender Service Account Details

HOME IMPORT EXPORT PROXY SETTINGS HELP English (United States)

### User Authentication

Allows users to enroll devices using corporate directory credentials

**Start** (Completed) | **2 Service Account** (Current) | **3 Finish**

#### Provide Service Account details

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

Username: MAAS360  
Password: ●●●●●●●●  
Domain: enterprise.mds.local

Enable Secure Authentication Mode

Back Next Save Cancel

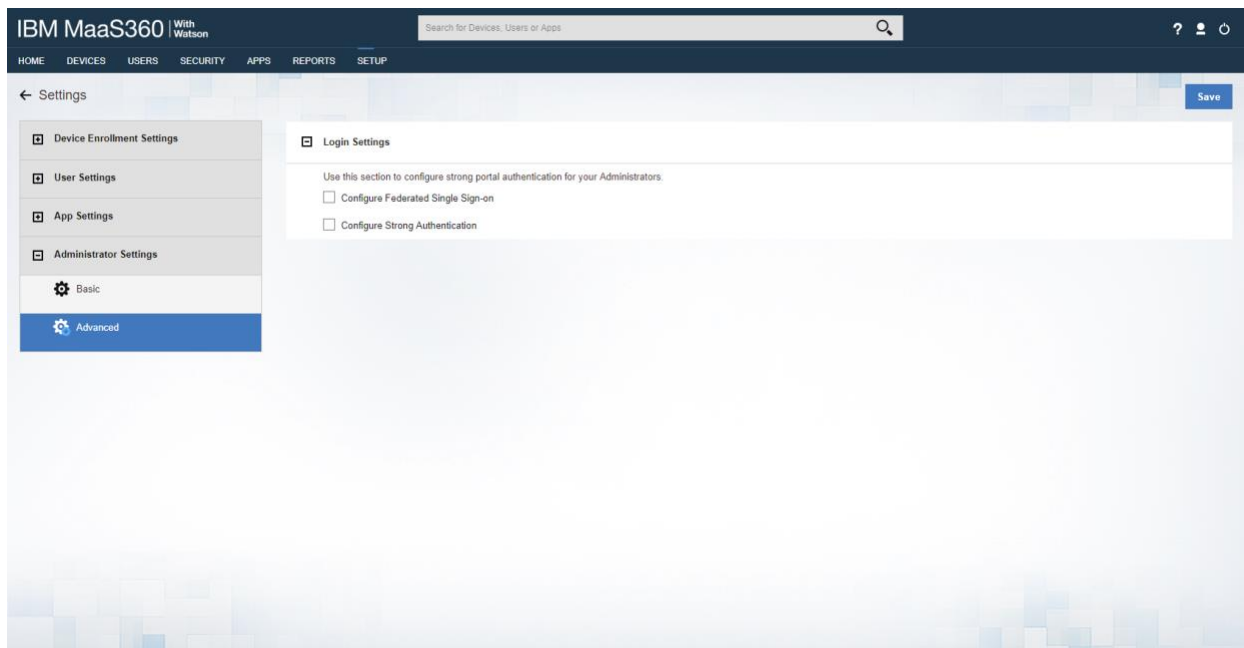
The Cloud Extender is running

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

### 2.2.1.3 MaaS360 Portal Active Directory Authentication Configuration

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

Figure 2-7 Administrator Settings




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



Figure 2-8 Administrator Configuration Options

Allow existing Administrators to use portal credentials as well. ⓘ

 Note: Since the username for one or more administrator account is not the same as their Corporate email addresses, following additional setup is required.

1. Navigate to "Setup > Administrators" workflow.
2. Edit the administrator accounts and specify the Corporate Usernames for these accounts.

Automatically create new Administrator accounts and update roles based on User Groups  
User Groups (Specify the Distinguished Name of the User Groups)

CN=Domain Admins,CN=Users,DC=enterj	Administrator - Level 2	⊖
	---Select Role---	⊕

11. Click **Save**.

#### 2.2.1.4 Cloud Extender NDES Integration

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

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

Figure 2-9 Cloud Extender SCEP Configuration

HOME IMPORT EXPORT PROXY SETTINGS HELP

English (United States)

### Certificate Integration

Securely deploy identity certificates to mobile devices

**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: .....

Back Next Save Cancel

The Cloud Extender is running

10. Click **Next**.

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

Figure 2-10 Cloud Extender Certificate Properties

HOME IMPORT EXPORT PROXY SETTINGS HELP

English (United States)

### Certificate Integration

Securely deploy identity certificates to mobile devices

**Certificate Properties**

Subject Name: /CN=%uname%/emailAddress=%email%

Subject Alternate Name: None

Cache certs on Cloud Extender:

Location of Certificate Cache: C:\CertCache

Back Next Save Cancel

The Cloud Extender is running

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

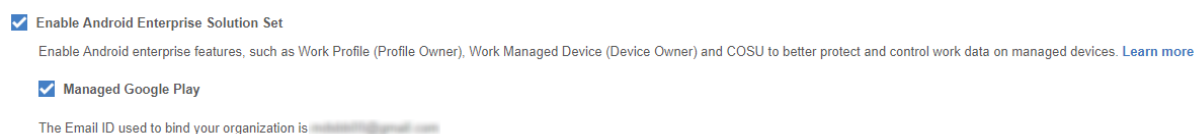
*Note: If a file access message appears, delete the file, and re-save the file.*

## 2.2.2 Android Enterprise Configuration

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

1. Create a Google account if you do not have one you wish to bind with.
2. From the MaaS360 portal, navigate to **Setup > Services**.
3. Click **Mobile Device Management**.
4. Check the box next to **Enable Android Enterprise Solution Set**.
5. Enter your password and click **Enable**.
6. Click **Mobile Device Management**.
7. Click the radio button next to **Enable via Managed Google Play Accounts (no G Suite)**.
8. Ensure all pop-up blockers are disabled. Click the link on the word **here**.
9. Enter your password and click **Enable**.
10. In the new page that opens, ensure you are signed into the Google account you wish to bind.
11. Click **Get started**.
12. Enter your business name and click **Next**.
13. If General Data Protection Regulation compliance is not required, scroll to the bottom, check the **I agree** box, and click **Confirm**. If compliance is required, fill out the requested information first.
14. Click **Complete Registration**.
15. Confirm binding on the **Setup** page under **Mobile Device Management**. The settings should look like Figure 2-11, where the blurred-out portion is the Google email address used to bind.

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



### 2.2.3 iOS APNs Certificate Configuration

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

### 2.2.4 Apple User Enrollment (UE) Configuration

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

#### 2.2.4.1 Apple Business Manager (ABM) Configuration

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

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

**Add Token** X

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

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

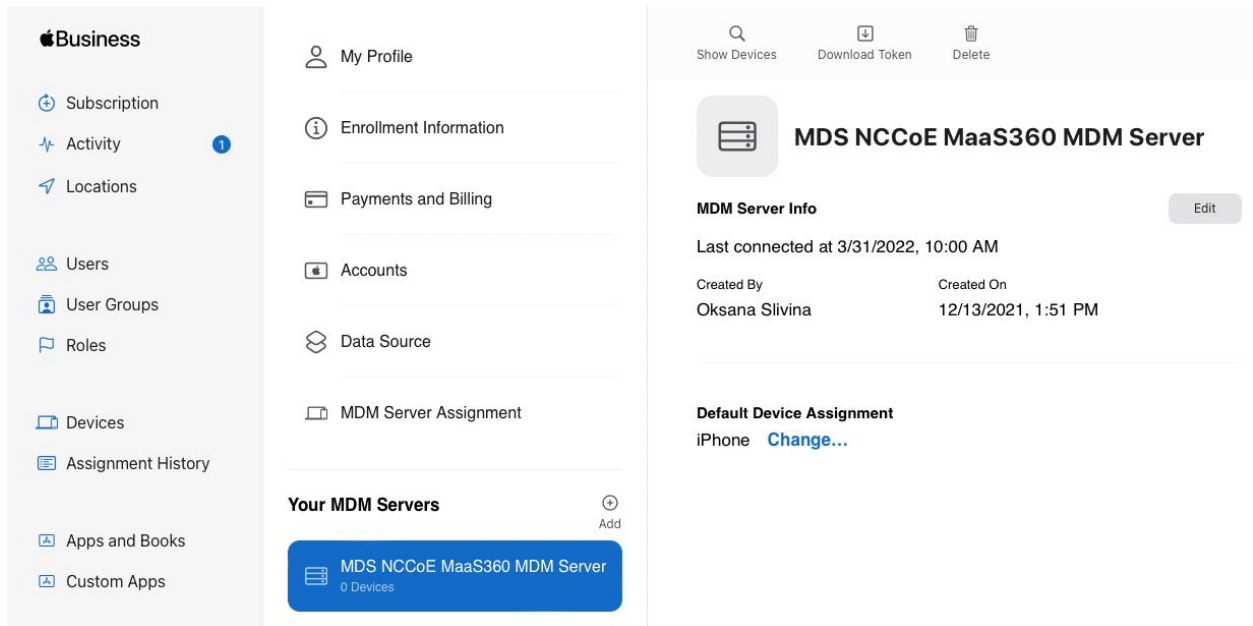
**Token Name\***  
Helps identifying token in future

**Token File.\***  
.p7m file from DEP Portal

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

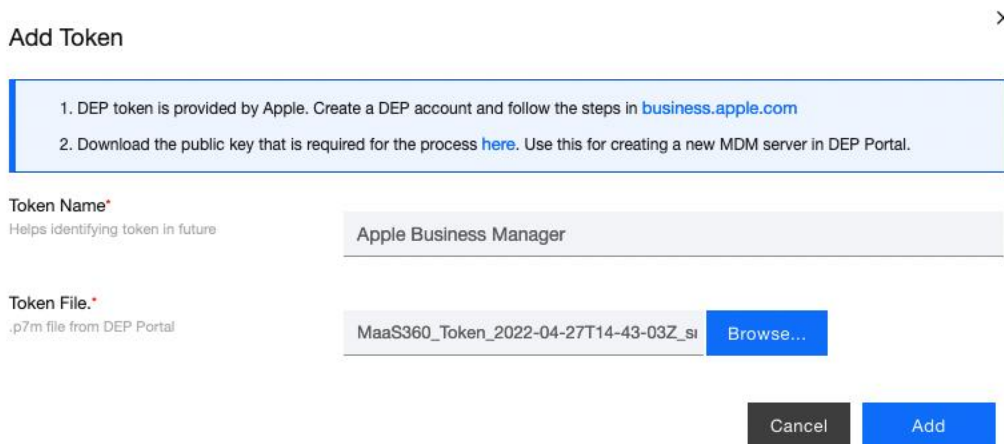
Figure 2-13 MDM configuration in Apple Business Manager



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

11. Click **Add**.

Figure 2-14 Creating the DEP token



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

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

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

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

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

**Figure 2-15 VPP token in MaaS360**

Token Name	Users	Country Na...	User Groups	Last Sync Time	Update Time	Expiry Date	Status	App Addition St...
VPP Token <a href="#">View</a> <a href="#">Update</a> <a href="#">Disable</a> <a href="#">More...</a>	0	United States	All Users		04/27/2022 13:15 EDT	04/26/2023 20:00 EDT	Active	NA

[|<](#) [<](#) [1](#) [>](#) [>|](#) [Jump To Page](#) Displaying 1 - 1 of 1 Records | Show 25 [v](#) Records

### 2.2.4.2 MaaS360 Configuration

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

**Figure 2-16 iOS Enrollment Configuration**

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

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

Managed mode - Manage entire device. ⓘ  
 User enrollment mode - Manage only corporate resources. ⓘ

When user enrollment mode is selected, MaaS360 currently does not support macOS enrollment into MDM(Managed Mode) as employee owned devices. Alternatively, the macOS devices can be enrolled as corporate owned.

## 2.2.5 Android Configuration

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

### 2.2.5.1 Policy Configuration

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

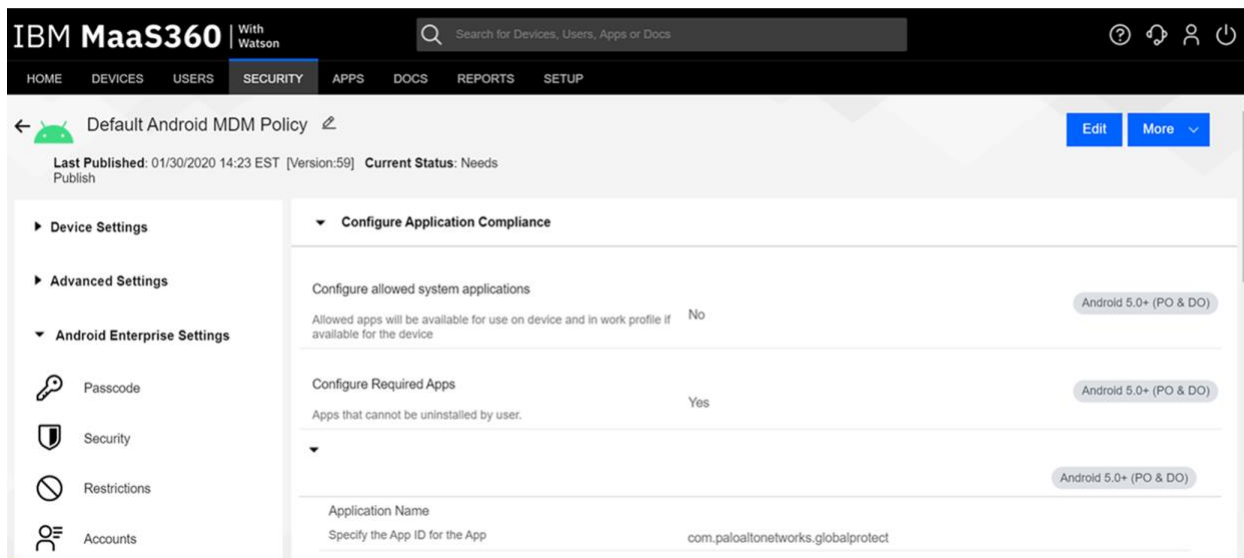
9. Configure restrictions based on corporate requirements.
10. Click **Save**.

### 2.2.5.2 VPN Configuration

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

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

Figure 2-17 Android GlobalProtect Application Compliance



## 2.2.6 iOS Configuration

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



### 2.2.6.1 Policy Configuration

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

### 2.2.6.2 VPN Configuration

1. Click **Device Settings > VPN**.
2. Click **Edit**.
3. Next to **Configure for Type**, select **Custom SSL**.
4. Enter a name next to **VPN Connection Name**. In this sample implementation, **Great Seneca VPN** was used.
5. Next to **Identifier**, enter **com.paloaltonetworks.globalprotect.vpn**.
6. Next to **Host name of the VPN Server**, enter the URL of the VPN endpoint without http or https.
7. Next to **VPN User Account**, enter **%username%**.
8. Next to **User Authentication Type**, select **Certificate**.
9. Next to **Identity Certificate**, select the name of the certificate profile created during the NDES configuration steps. In this sample implementation, **NDES** was used.
10. Next to **Custom Data 1**, enter **allowPortalProfile=0**.
11. Next to **Custom Data 2**, enter **fromAspen=1**.
12. Next to **Apps to use this VPN**, enter the application identifications (IDs) of applications to go through the VPN. This will be the applications deployed to the devices as work applications.
13. Next to **Provider Type**, select **Packet Tunnel**.
14. In Apple Business Manager, click **Apps and Books**.
15. Search for *GlobalProtect*.

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

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

## 2.3 Zimperium

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

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

### 2.3.1 Zimperium and MaaS360 Integration

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

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

*Note: For the MDM URL, append the account ID to the end. For example, if the account ID is 12345, the MDM URL would be <https://services.fiberlink.com/12345>.*

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

Figure 2-18 Zimperium MaaS360 Integration Configuration

### Edit MDM

**Step 1** Choose MDM Provider    **Step 2** Setup IBM MaaS360    **Step 3** Finish

**URL**  
Specify URL for this MDM provider.

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

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

**MDM Name**  
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 synced from the MDM

**Mask Imported User Information**   
By enabling this option, personally identifiable information will be masked (first name, last name and email) from the zConsole

**API key**   
Specify API KEY for this MDM provider.

**Send Device Activation email via zConsole for iOS Devices**   
By enabling this option, zConsole will send an activation email to a user for each iOS device which is synced from the MDM

**Send Device Activation email via zConsole for Android Devices**   
By enabling this option, zConsole will send an activation email to a user for each Android device which is synced from the MDM

**Next**

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

### 2.3.2 Automatic Device Activation

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

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

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

Figure 2-19 Zimperium zIPS iOS Configuration

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

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

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

Figure 2-20 Zimperium zIPS Android Configuration

Default Acceptor:	<input type="text"/>
Tenant:	<input type="text"/>
UUID:	<input type="text"/>
Display EULA:	<input type="text" value="No"/> ▼
Tracking ID 1:	<input type="text"/>
Tracking ID 2:	<input type="text"/>
MDM Device ID:	<input type="text" value="%deviceid%"/>

32. Click **Add**.

### 2.3.3 Enforce Application Compliance

From the IBM MaaS360 web portal:

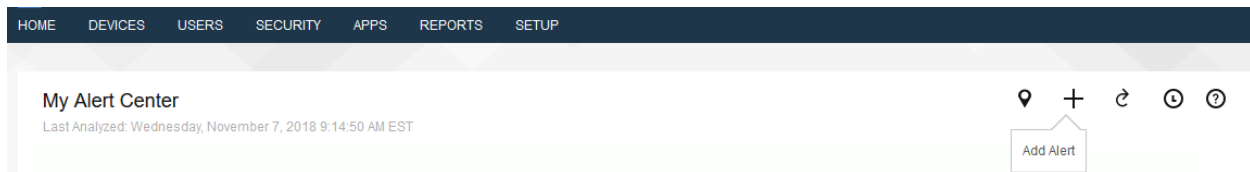
1. Navigate to **Security > Policies**.
2. Select the default Android policy.
3. Navigate to **Android Enterprise Settings > App Compliance**.
4. Click **Edit**.
5. Check the box next to **Configure Required Apps** if not checked already. If it is, click the + icon.
6. Enter **com.zimperium.zips** as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

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

### 2.3.4 MaaS360 Risk Posture Alerts

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

Figure 2-21 Add Alert Button



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

Figure 2-22 Zimperium Risk Posture Alert Configuration

**Add Alert** Available for: All Administrators

**Name & Description**  
Name: Zimperium Risk Posture E  
Description: E.g. 'of my devices are jailbroken'  
Category: 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.

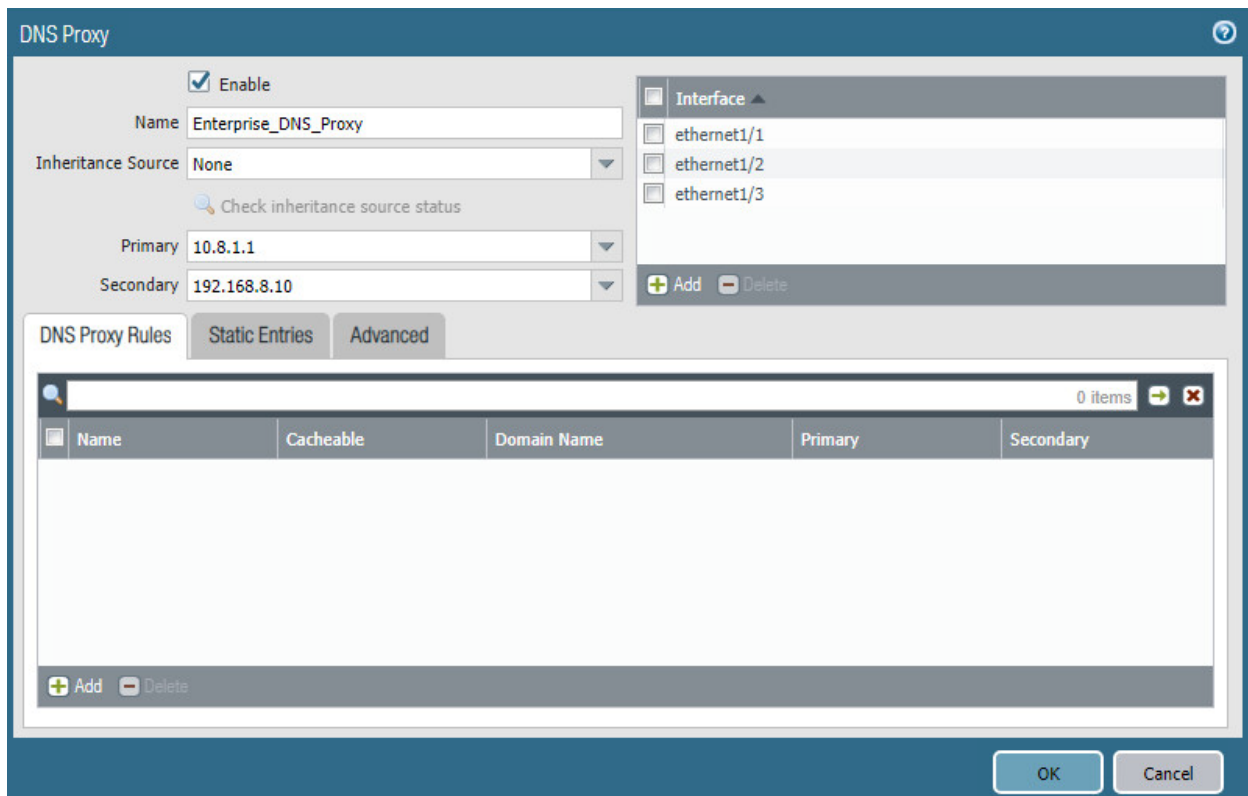
### 2.4.1 Network Configuration

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.



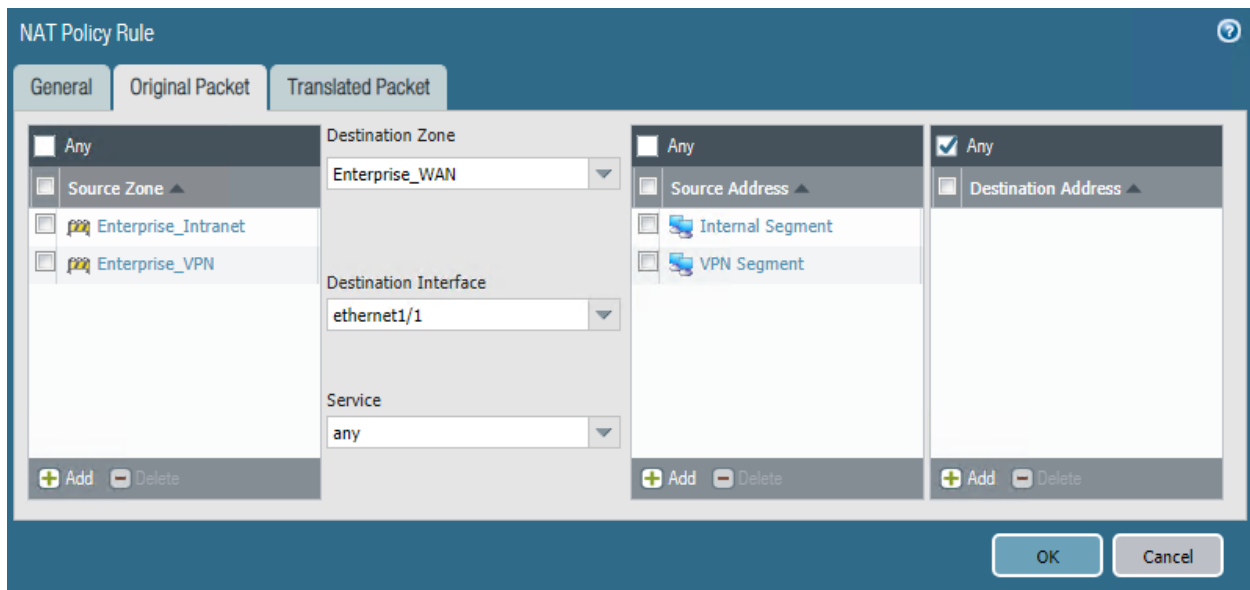
11. Navigate to **Network > Virtual Routers**.
12. Click **Add**.
13. Give the router an appropriate name and add the internal and external interfaces.
14. Click **Static Routes > Add**. Give the static route an appropriate name, e.g., WAN. Set the destination to be **0.0.0.0/0**, set the interface to 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 2-23 DNS Proxy Object Configuration



22. Navigate to **Device > Services**.
23. Click the **gear** in the top-right corner of the Services panel.
24. Under **DNS settings**, click the radio button next to **DNS Proxy Object**. Select the created DNS proxy object from the drop-down.
25. Click **OK** and commit the changes. This is where static DNS entries will be added in the future.
26. Navigate to **Objects > Addresses**.
27. For each device on the network, click **Add**. Give the device an appropriate name, enter an optional description, and enter the IP address.
28. Click **OK**.
29. Once all devices are added, commit the changes.
30. Navigate to **Policies > NAT**.
31. Click **Add**.
32. Give the network address translation rule a meaningful name, such as External Internet Access.
33. Click **Original Packet**.
34. Click **Add** and add the zone representing the intranet—in this case, **Enterprise\_Intranet**.
35. Repeat step 34 for the secure sockets layer (SSL) VPN zone.
36. Under **Source Address**, click **Add**.
37. Enter the subnet corresponding to the intranet segment.
38. Repeat step 37 for the SSL VPN segment.
39. Click **Translated Packet**. Set the translation type to **Dynamic IP and Port**. Set Address Type to be **Interface Address**. Set Interface to be the WAN interface and set the IP address to be the WAN IP of the firewall.
40. Click **OK** and commit the changes.

Figure 2-24 Original Packet Network Address Translation Configuration



## 2.4.2 Demilitarized Zone Configuration

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

## 2.4.3 Firewall Configuration

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

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

#### 2.4.4 Certificate Configuration

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

Figure 2-25 Certificate Profile

Certificate Profile

Name: Enterprise\_Certificate\_Profile

Username Field: Subject (dropdown) | common-name

User Domain: enterprise

Name	Default OCSF URL	OCSF Verify Certificate
Internal Root		
Internal Sub		

+ Add - Delete

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

Use CRL      CRL Receive Timeout (sec) 5

Use OCSP      OCSP Receive Timeout (sec) 5

OCSP takes precedence over CRL      Certificate Status Timeout (sec) 5

Block session if certificate status is unknown

Block session if certificate status cannot be retrieved within timeout

Block session if the certificate was not issued to the authenticating device

Block sessions with expired certificates

OK Cancel

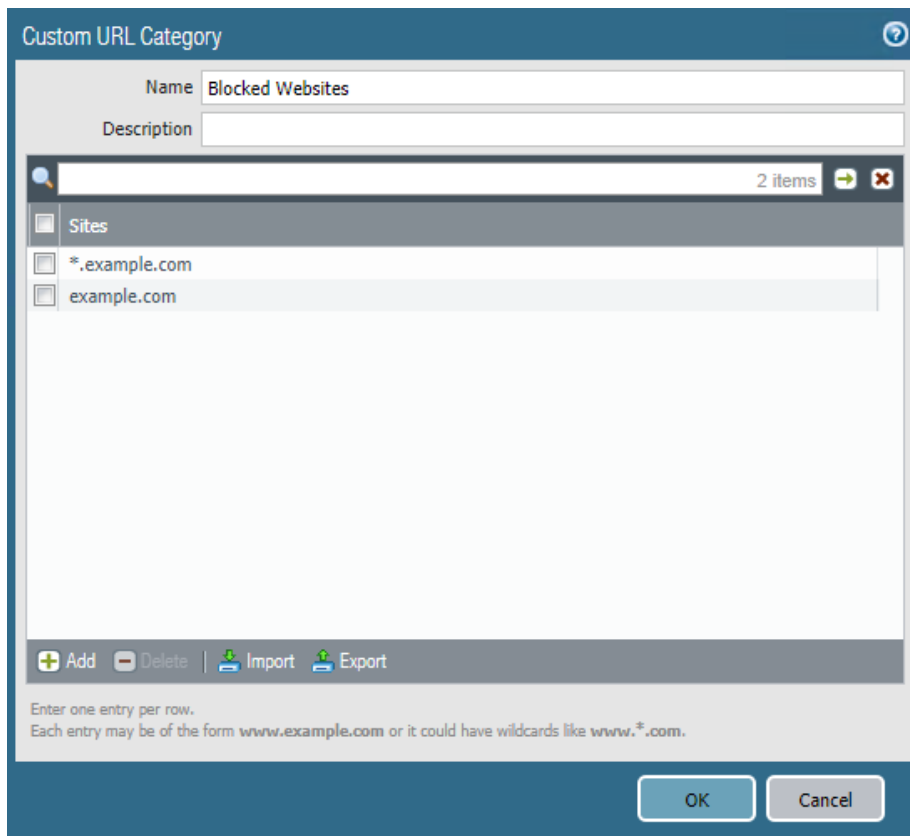
## 2.4.5 Website Filtering Configuration

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

### 2.4.5.1 Configure Basic Website Blocking

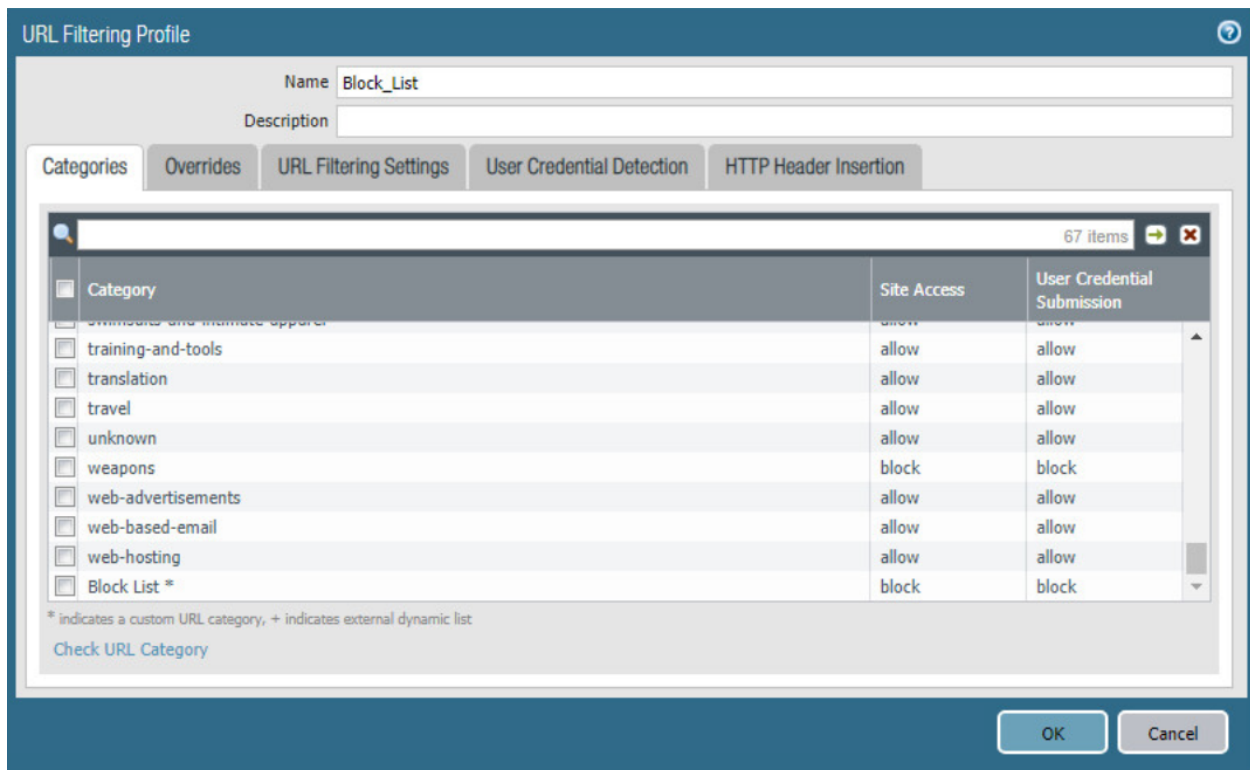
1. Navigate to **Objects > URL Category**.
2. Click **Add**.
3. Enter a name for the **URL Category**. Click **Add** on the bottom.
4. Add websites that should be blocked. Use the form *\*.example.com* for all subdomains and *example.com* for the root domain.

Figure 2-26 Custom URL Category



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

Figure 2-27 URL Filtering Profile



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

Figure 2-28 URL Filtering Security Policy

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow' and 'Send ICMP Unreachable' unchecked. The 'Profile Setting' section has 'Profile Type' set to 'Profiles' and 'URL Filtering' set to 'Block\_List'. The 'Log Setting' section has 'Log at Session Start' and 'Log at Session End' unchecked, and 'Log Forwarding' set to 'None'. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None', and 'Disable Server Response Inspection' unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

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

#### 2.4.5.2 Configure SSL Website Blocking

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

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



Figure 2-29 Generating the Root CA

The screenshot shows a 'Generate Certificate' dialog box with the following settings:

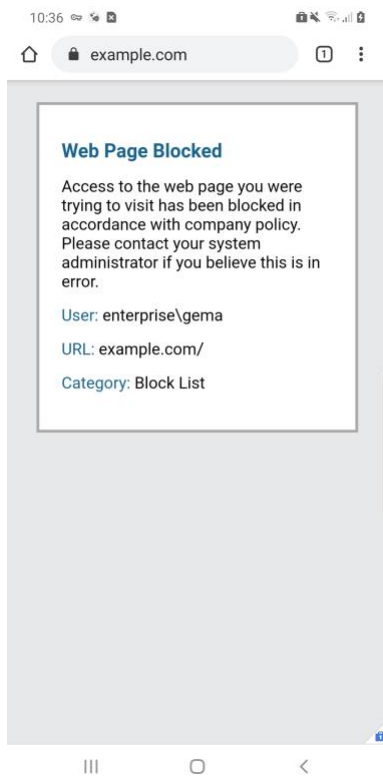
- Certificate Type:  Local,  SCEP
- Certificate Name: SSL Decryption Root
- Common Name: PA Root (with a note: IP or FQDN to appear on the certificate)
- Signed By: (empty dropdown)
- Certificate Authority
- OCSF Responder: (empty dropdown)
- Cryptographic Settings:**
  - Algorithm: RSA
  - Number of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

Buttons: Generate, Cancel

5. Click **Generate**.
6. Click **Generate** at the bottom of the page.
7. Give the certificate a name, such as SSL Decryption Intermediate.
8. Give the certificate a CN, such as PA Intermediate.
9. Next to **Signed By**, select the generated root CA. In this case, SSL Decryption Root was selected.
10. Check the box next to **Certificate Authority**.
11. Click **Generate**.
12. Click the newly created certificate.
13. Check the boxes next to **Forward Trust Certificate** and **Forward Untrust Certificate**.
14. Click **OK**.
15. Navigate to **Policies > Decryption**.
16. Click **Add**.
17. Give the policy a name and description.

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

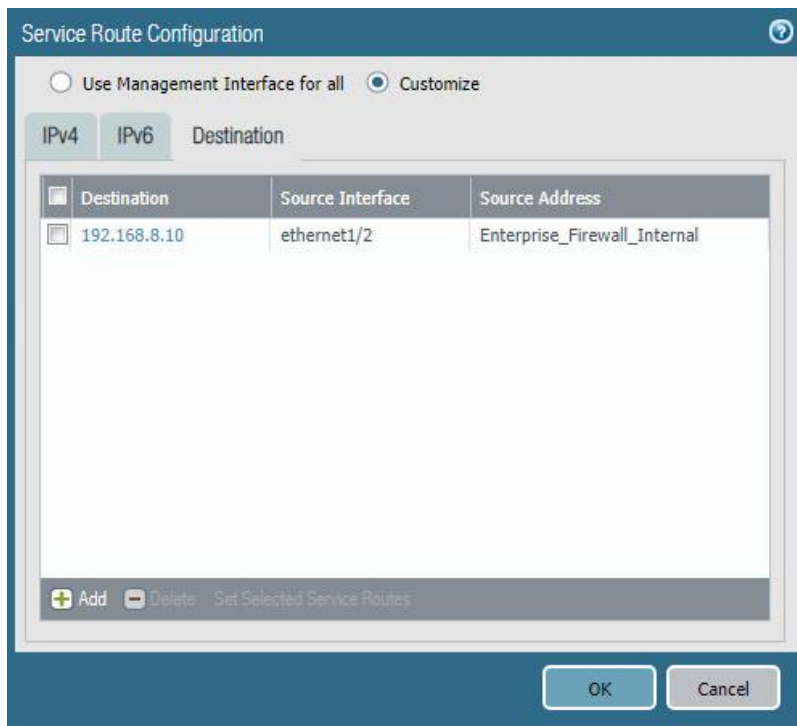
**Figure 2-30 Blocked Website Notification**



## 2.4.6 User Authentication Configuration

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

Figure 2-31 Service Route Configuration



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

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

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

Figure 2-32 LDAP Server Profile

LDAP Server Profile

Profile Name: Enterprise\_LDAP

Administrator Use Only

**Server List**

Name	LDAP Server	Port
LDAP Server	192.168.8.10	389

+ Add - Delete

Enter the IP address or FQDN of the LDAP server

**Server Settings**

Type: active-directory

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

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

Password: .....

Confirm Password: .....

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

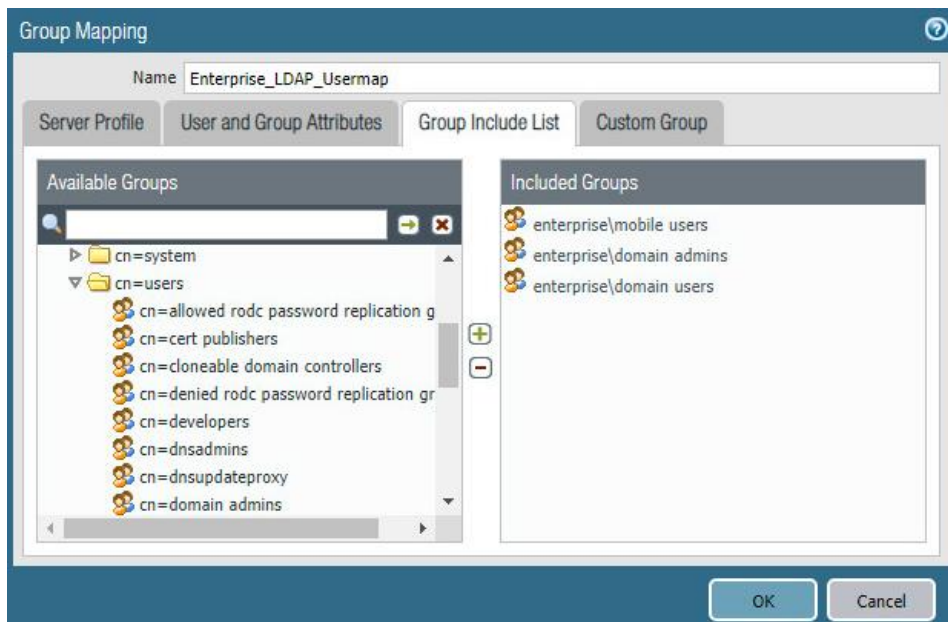
Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

OK Cancel

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

Figure 2-33 LDAP Group Mapping



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

Figure 2-34 LDAP User Authentication Profile

The screenshot shows the 'Authentication Profile' configuration window with the 'Advanced' tab active. The 'Name' field is 'Enterprise\_Auth'. Under the 'Authentication' section, 'Type' is 'LDAP', 'Server Profile' is 'Enterprise\_LDAP', 'Login Attribute' is 'sAMAccountName', 'Password Expiry Warning' is '7', 'User Domain' is 'enterprise', and 'Username Modifier' is '%USERINPUT%'. The 'Single Sign On' section has an empty 'Kerberos Realm' field and a 'Kerberos Keytab' field with the text 'Click "Import" to configure this field' and an 'Import' button.

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

### 2.4.7 VPN Configuration

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

Figure 2-35 Configured Tunnel Interfaces

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

4. Click the **newly created tunnel**.
5. Click the drop-down next to **Security Zone**. Select **New Zone**.
6. Give it a name and assign it to the newly created tunnel. Click **OK** twice.

Figure 2-36 SSL VPN Tunnel Interface Configuration

The screenshot shows a configuration window titled "Tunnel Interface". At the top, there are three input fields: "Interface Name" with the value "tunnel.1", "Comment" with the value "SSL VPN", and "Netflow Profile" with a dropdown menu set to "None". Below these fields are four tabs: "Config", "IPv4", "IPv6", and "Advanced". The "Config" tab is selected. Underneath the tabs is a section titled "Assign Interface To" which contains two dropdown menus: "Virtual Router" set to "Enterprise\_Main\_Router" and "Security Zone" set to "Enterprise\_VPN". At the bottom right of the window are two buttons: "OK" and "Cancel".

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

#### 2.4.7.1 Configure the GlobalProtect Gateway

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



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

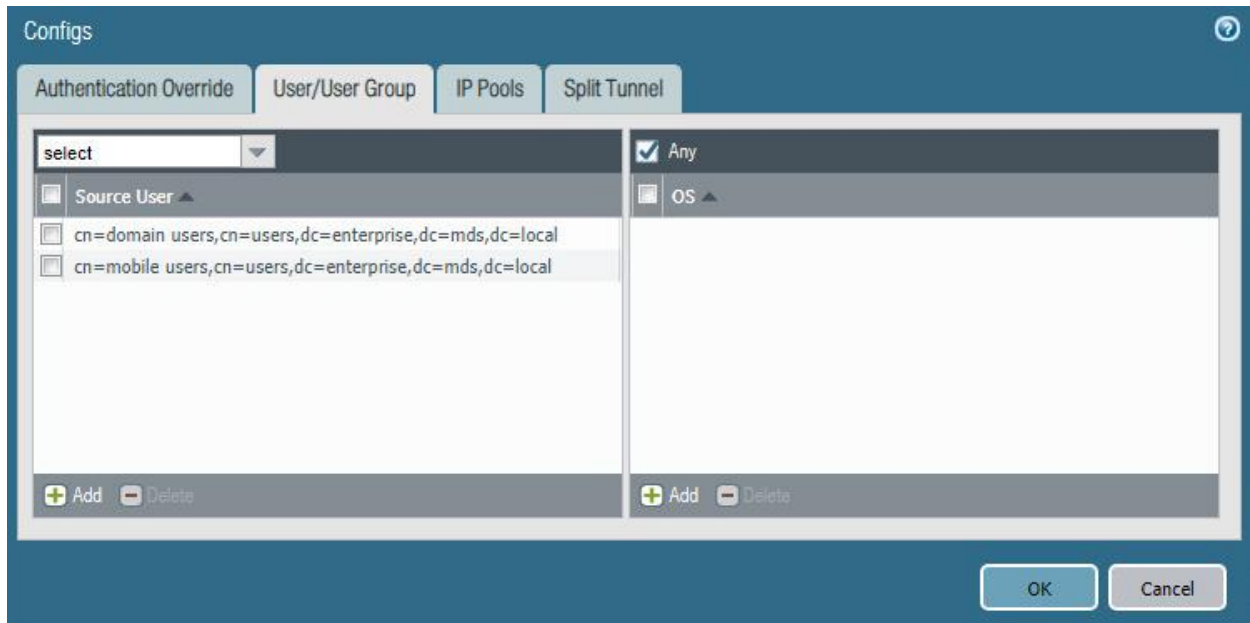
Figure 2-37 GlobalProtect iOS Authentication Profile

The screenshot shows the 'Client Authentication' configuration window. The 'Name' field is 'iOS Auth', 'OS' is 'iOS', and 'Authentication Profile' is 'Enterprise\_Auth'. Under 'GlobalProtect App Login Screen', 'Username Label' is 'Username', 'Password Label' is 'Password', and 'Authentication Message' is 'Enter login credentials'. At the bottom, 'Allow Authentication with User Credentials OR Client Certificate' is set to 'Yes (User Credentials OR Client Certificate Required)'. There are 'OK' and 'Cancel' buttons at the bottom right.

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

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

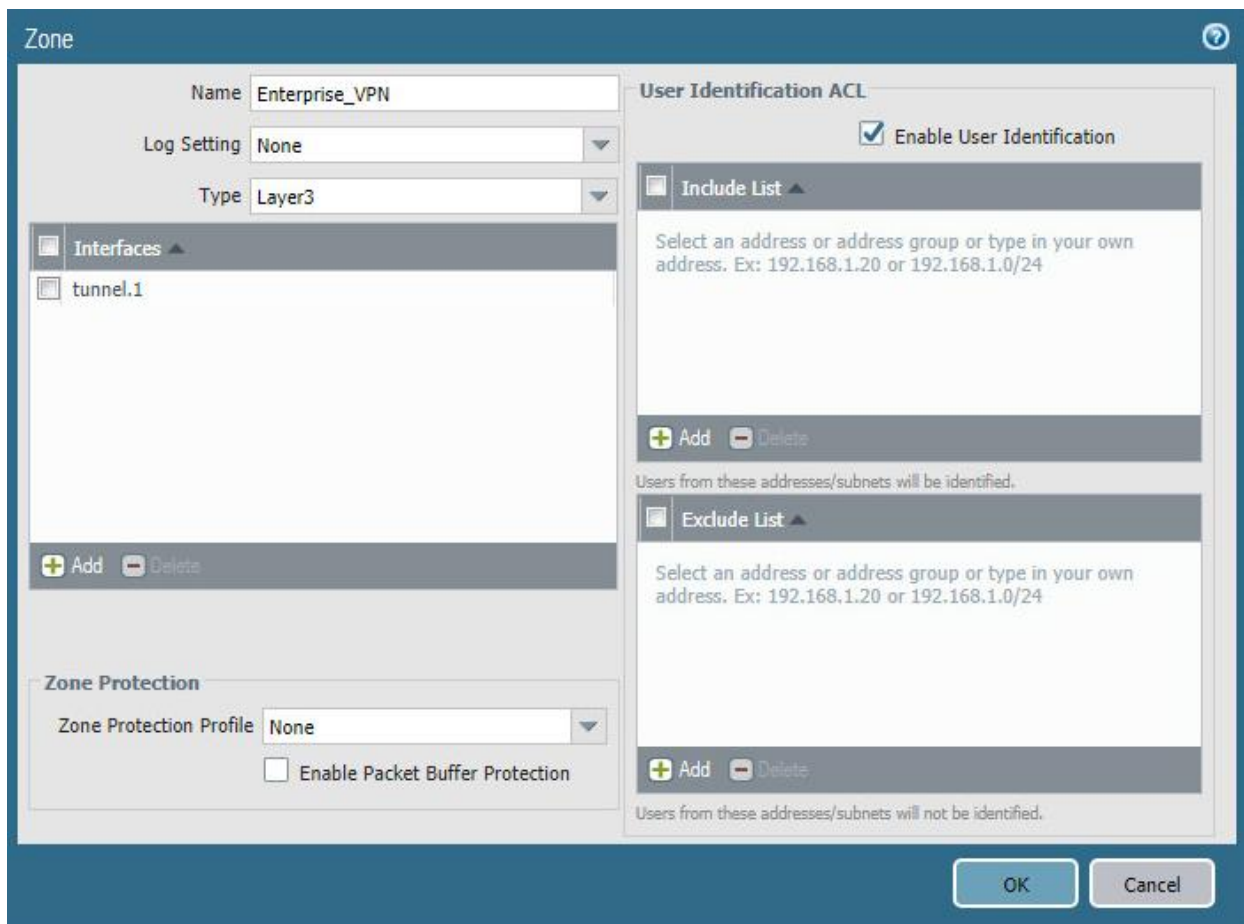
Figure 2-38 LDAP Authentication Group Configuration



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

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

Figure 2-39 VPN Zone Configuration



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

#### 2.4.7.2 Configure the GlobalProtect Portal

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

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

Figure 2-40 GlobalProtect Portal General Configuration

GlobalProtect Portal Configuration

General Name Enterprise\_VPN\_Portal

Authentication

Agent

Clientless VPN

Satellite

Network Settings

Interface ethernet1/1

IP Address Type IPv4 Only

IPv4 Address Enterprise\_Firewall\_External

Appearance

Portal Login Page factory-default

Portal Landing Page factory-default

App Help Page factory-default

OK Cancel

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

Figure 2-41 GlobalProtect Portal Authentication Configuration

The screenshot shows the 'GlobalProtect Portal Configuration' window with the 'Agent' tab selected. The 'Server Authentication' section has 'SSL/TLS Service Profile' set to 'GlobalProtect\_Endpoint'. The 'Client Authentication' section contains a table with one entry:

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

Below the table are buttons for 'Add', 'Delete', 'Clone', 'Move Up', and 'Move Down'. At the bottom, the 'Certificate Profile' is set to 'Enterprise\_Certificate\_Profile'. 'OK' and 'Cancel' buttons are at the bottom right.

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

Figure 2-42 GlobalProtect Portal Agent Authentication Configuration

The screenshot shows the 'Configurations' window for GlobalProtect Portal Agent Authentication. The 'Authentication' tab is selected. The configuration includes the following fields and options:

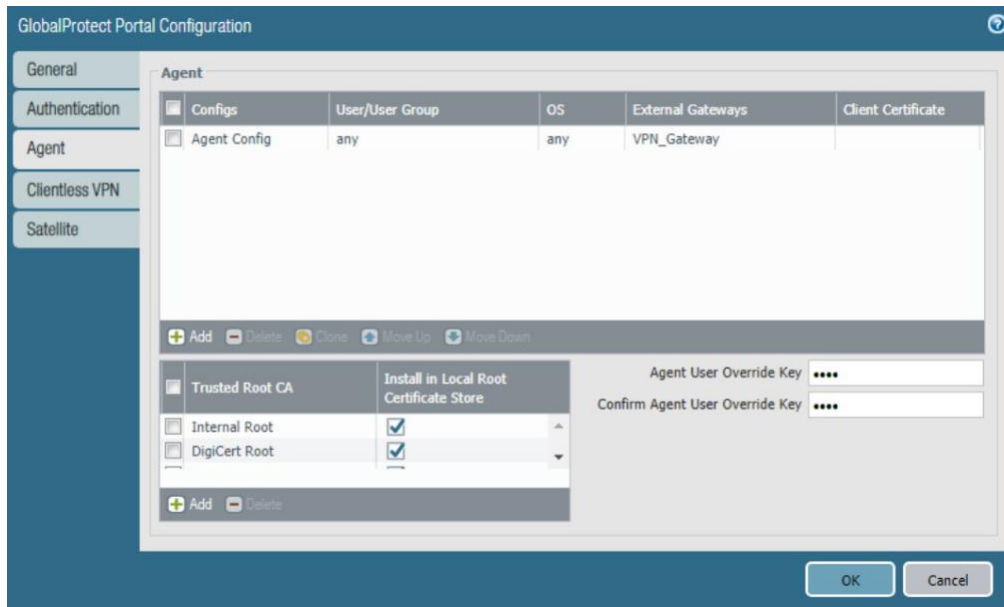
- Name:** Agent Config
- Client Certificate:** None
- Save User Credentials:** No
- Authentication Override:**
  - Generate cookie for authentication override
  - Accept cookie for authentication override
  - Cookie Lifetime:** Hours, 24
  - Certificate to Encrypt/Decrypt Cookie:** None
- Components that Require Dynamic Passwords (Two-Factor Authentication):**
  - Portal
  - Internal gateways-all
  - External gateways-manual only
  - External gateways-auto discovery

Buttons for 'OK' and 'Cancel' are located at the bottom right of the window.

18. Click **External**.
19. Click **Add** under **External Gateways**.
20. Give the gateway a name and enter the fully qualified domain name (FQDN) of the VPN end point.
21. Click **Add** under **Source Region** and select **Any**.
22. Check the box next to **Manual**.
23. Click **OK**.
24. Click **App**.
25. Under **App Configurations > Connect Method**, select **On-demand**.
26. Next to **Welcome Page**, select **factory-default**.
27. Click **OK**.
28. Click **Add** under **Trusted Root CA**.
29. Select the **internal root certificate** used to generate device certificates.
30. Click **Add** again. Select the **root certificate** used to create the VPN end-point SSL certificate. For this implementation, it is a DigiCert root certificate.

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

Figure 2-43 GlobalProtect Portal Agent Configuration



33. Click **OK**.

### 2.4.7.3 Activate Captive Portal

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

Figure 2-44 Captive Portal Configuration

Captive Portal

Enable Captive Portal

Idle Timer (min) 15

Timer (min) 60

GlobalProtect Network Port for Inbound Authentication Prompts (UDP) 4501

SSL/TLS Service Profile GlobalProtect\_Endpo

Authentication Profile Enterprise\_Auth

Mode  Transparent  Redirect

**Session Cookie**

Enable

Timeout (min) 1440

Roaming

Redirect Host 10.8.1.2

**Certificate Authentication**

Certificate Profile None

**NTLM Authentication**

Attempts 1

Timeout (sec) 2

Reversion Time (sec) 300

OK Cancel

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

#### 2.4.7.4 Activate the GlobalProtect Client

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



Figure 2-45 GlobalProtect Portal



*Note: If you intend to use the GlobalProtect agent with a self-signed certificate (e.g., internal PKI), be sure to download the SSL certificate from the VPN website and install it in the trusted root CA store.*

### 2.4.8 Enable Automatic Application and Threat Updates

1. In the **PAN-OS portal**, navigate to **Device > Dynamic Updates**.
2. Install the latest updates.
  - a. At the bottom of the page, click **Check Now**.
  - b. Under **Applications and Threats**, click **Download** next to the last item in the list with the latest Release Date. This will take a few minutes.
  - c. When the download completes click **Close**.

Figure 2-46 Downloaded Threats and Applications

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

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

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

Figure 2-47 Schedule Time Hyperlink

Version ▲	File Name	Features	Type
▼ Applications and Threats		Last checked: 2018/11/29 12:25:15 EST	Schedule: <b>Every Wednesday at 01:02 (Download only)</b>

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

Figure 2-48 Application and Threats Update Schedule

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

## 2.5 Kryptowire

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

### 2.5.1 Kryptowire and MaaS360 Integration

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

## Appendix A List of Acronyms

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

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

## Appendix B Glossary

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

## Appendix C    References

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

## Appendix D Example Solution Lab Build Testing Details

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

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

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

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

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

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

Figure D-1 Contact Created in Work Profile

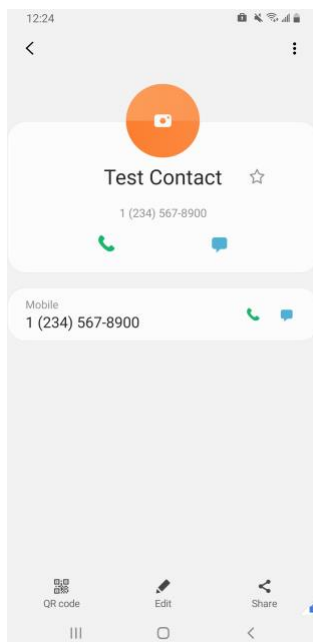




Figure D-2 Personal Profile Can't See Work Contacts

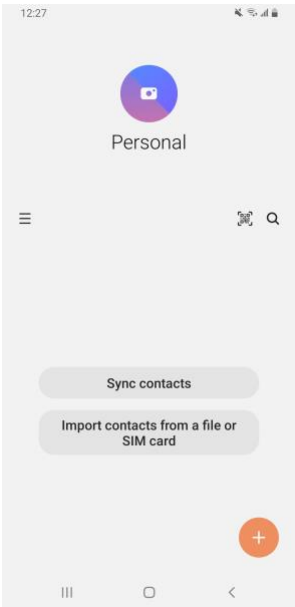


Figure D-3 Contact Created in Managed App

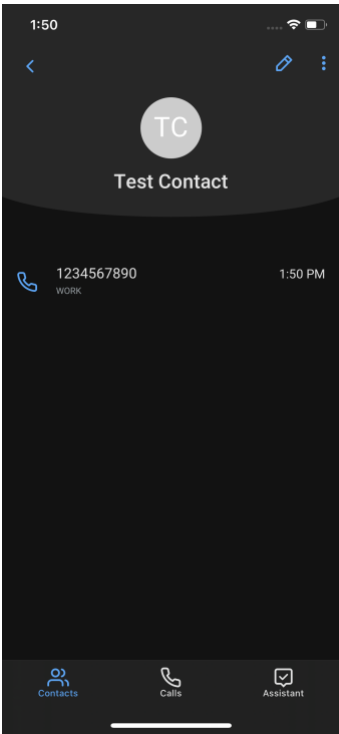
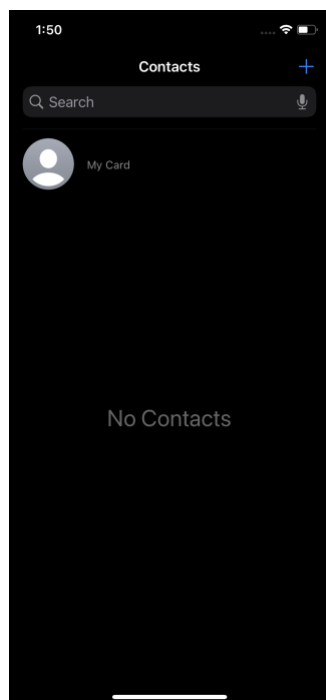


Figure D-4 Unmanaged App Can't See Managed Contacts



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

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

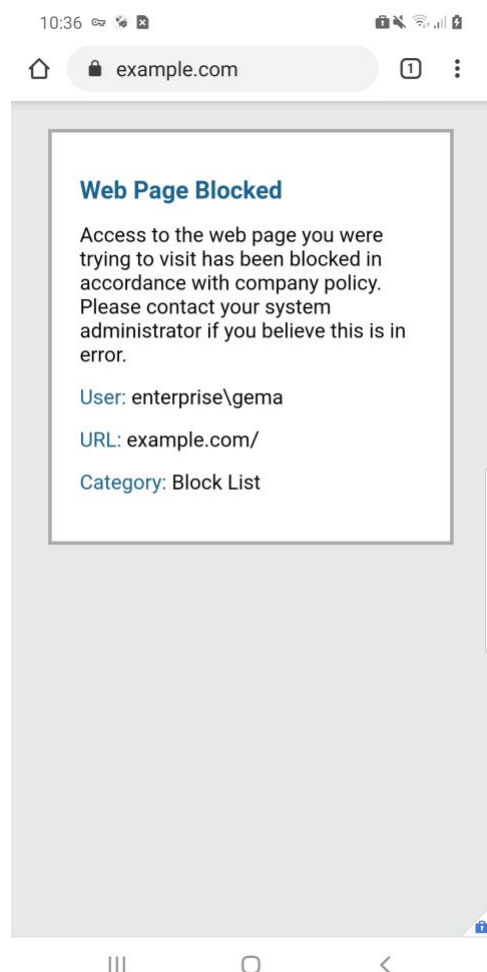
### Test Activity:

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

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

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

Figure D-5 Fictitious Phishing Webpage Blocked



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

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

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

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

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

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

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

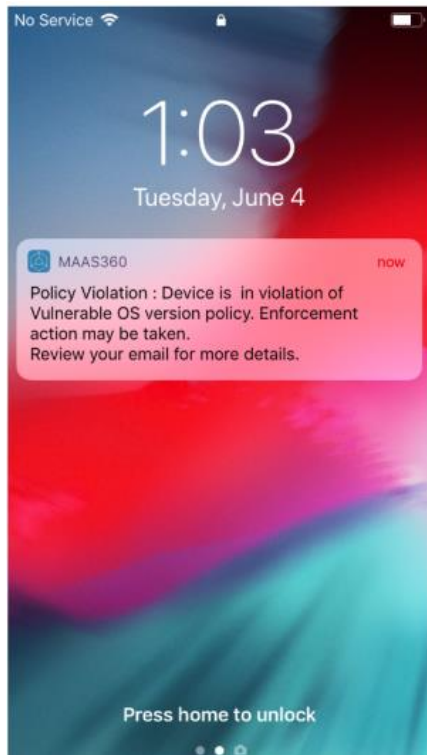
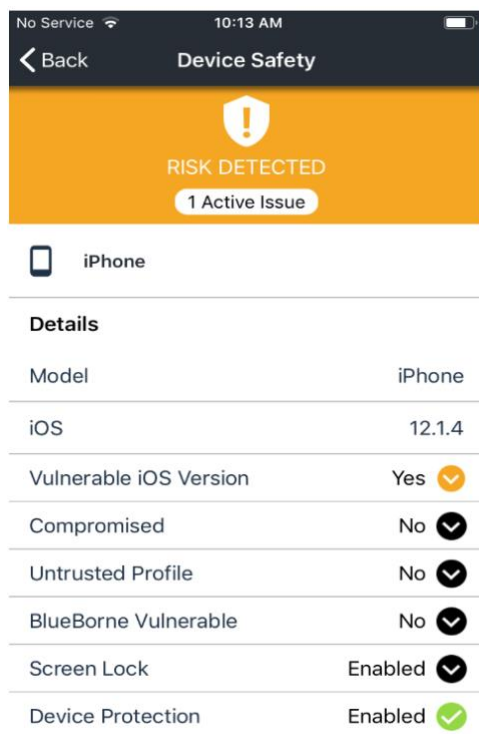


Figure D-7 Zimperium Risk Detected



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

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

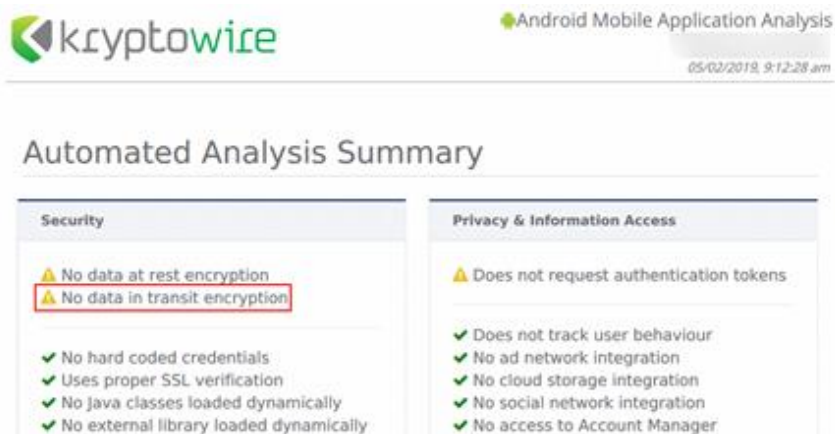
**Test Activity:** Test if applications will attempt to establish a hypertext transfer protocol or unencrypted connection.

**Desired Outcome:**

- Android: Because all work applications are inside a work profile, a profile-wide virtual private network (VPN) policy can be applied to mitigate this threat event; all communications, both encrypted and unencrypted, will be sent through the VPN tunnel. This will prevent eavesdropping on any communication originating from a work application.
- iOS: Apply a per-application VPN policy that will send all data transmitted by managed applications through the VPN tunnel. This will prevent eavesdropping on any unencrypted communication originating from work applications.
- Kryptowire can identify if an application attempts to establish an unencrypted connection.

**Observed Outcome:** The Kryptowire report indicated that the application did not use in-transit data encryption. When the managed version of that application was launched, an SSL VPN connection was automatically established. Figure D-8 shows the analysis summary finding of no in transit data encryption in use.

Figure D-8 Kryptowire Application Report



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

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

**Test Activity:**

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

**Desired Outcome:** Policies set on the device by the EMM (MaaS360) should require a device unlock code to be set, prevent the device unlock code from being removed, and require a minimum complexity for the device unlock code. The VPN (GlobalProtect) should require periodic re-authentication with multi-factor authentication to prevent devices with a bypassed lock screen from accessing on-premises enterprise resources.

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

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

Figure D-9 Android Passcode Configuration

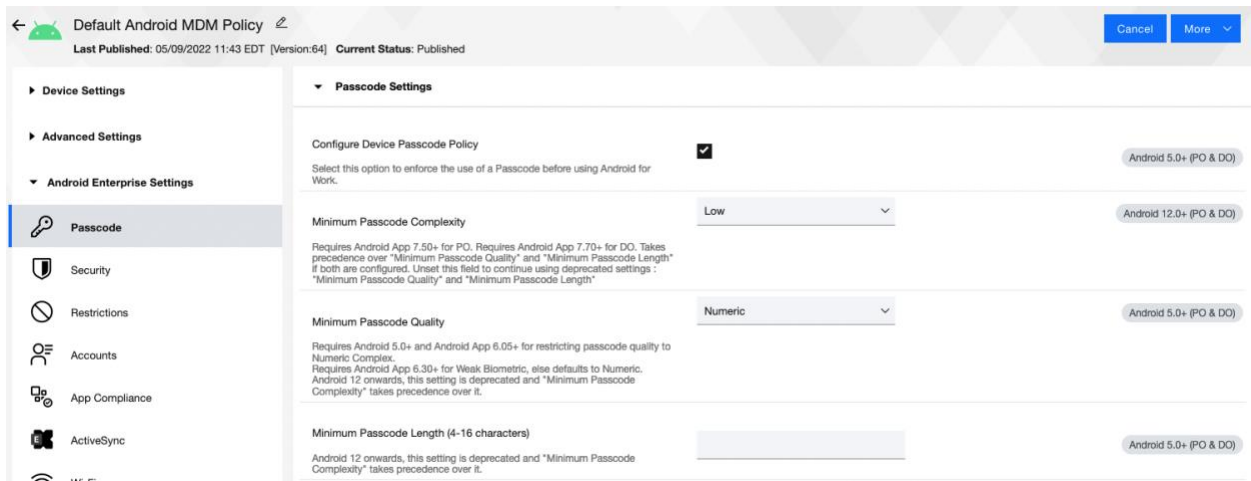


Figure D-10 iOS Passcode Configuration

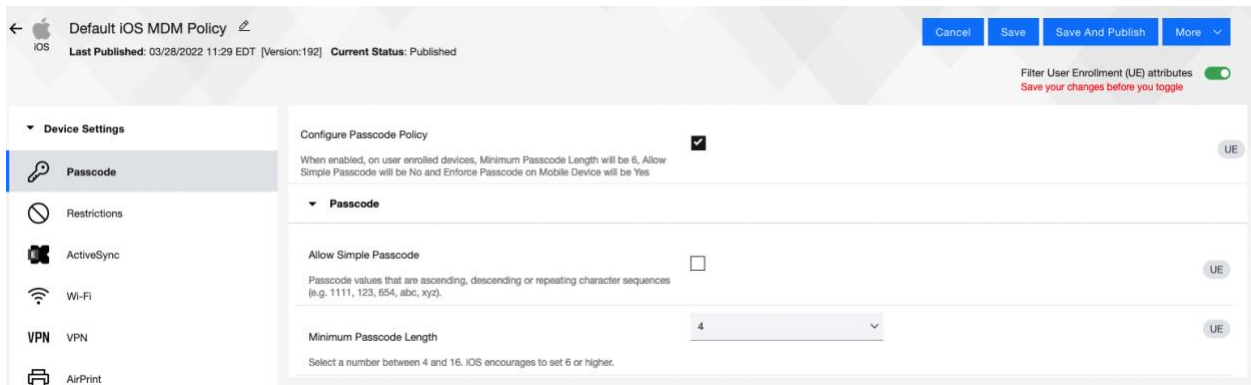
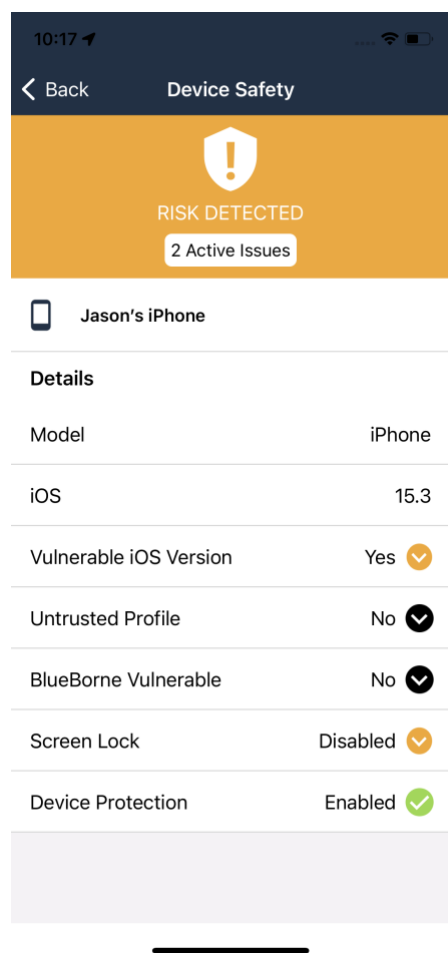


Figure D-11 Zimperium Detecting Disabled Lock screen



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

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

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

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

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



Figure D-12 Application Report with Hardcoded Credentials



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

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

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

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

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

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

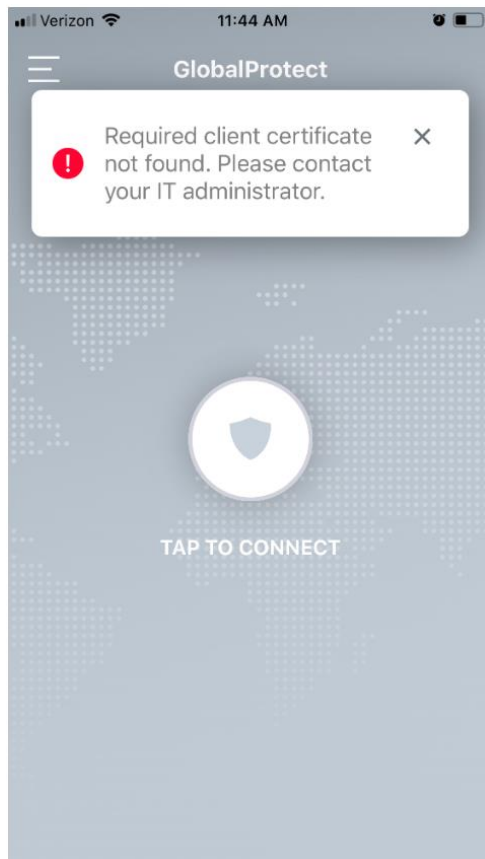


Figure D-14 Attempting to Access the VPN on an Unmanaged Android Device

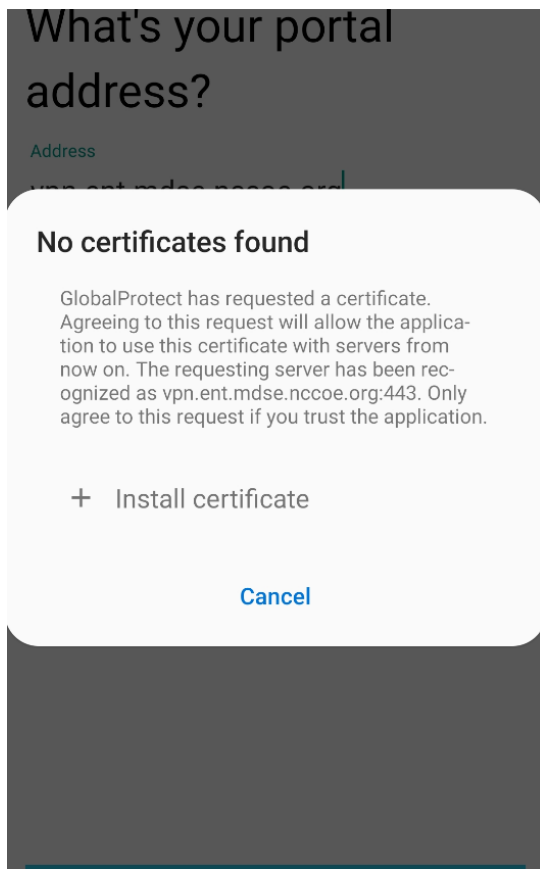
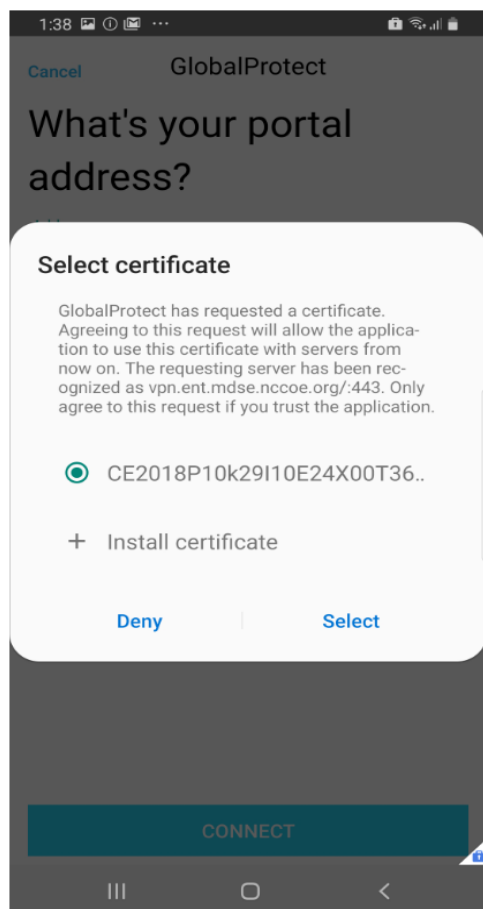


Figure D-15 Attempting to Access the VPN on a Managed Android Device



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

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

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

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

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

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

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

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

Figure D-16 Selective Wiping a Device

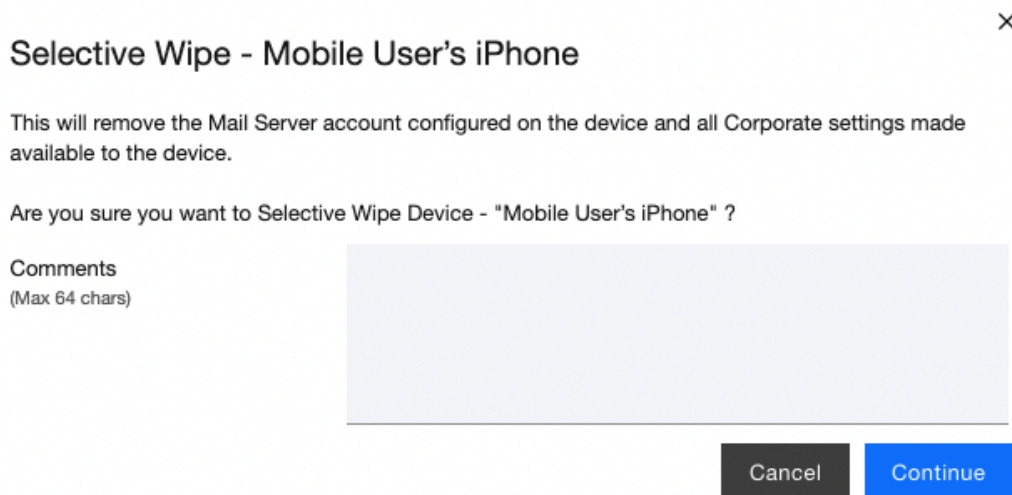


Figure D-17 Selective Wipe Complete

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

Figure D-18 Corporate Data Removal Confirmation Notification on iOS

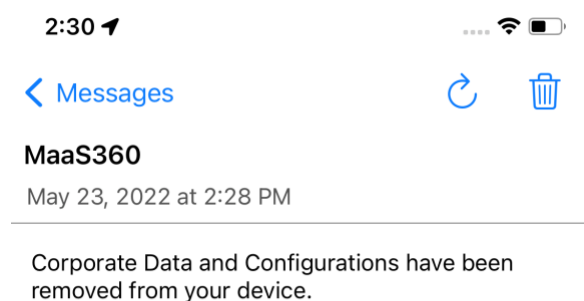
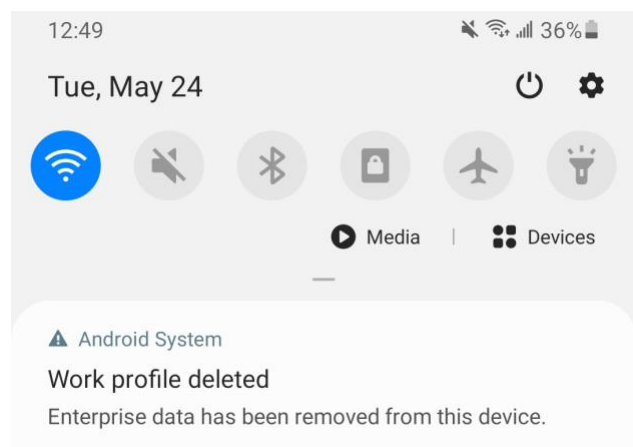


Figure D-19 Work Profile Removal Notification on Android



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

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

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

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

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

- **Android**

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

Figure D-20 iOS DLP Configuration Options

Default iOS MDM Policy [🔗](#)

Edit More ▾

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

Filter User Enrollment (UE) attributes

Save your changes before you toggle

**Device Settings**

- Passcode
- Restrictions**
- ActiveSync
- Wi-Fi
- VPN** VPN
- AirPrint
- Accounts

**Advanced Settings**

**Configure Device Restrictions**

**Unencrypted backups are restricted for all APNS managed devices.** Yes UE

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

---

**Device Functionality**

---

**Allow Open from Managed to Unmanaged apps**

Allows Content to be opened from Managed to Unmanaged apps. Applies to Mail, Calendar events, Contacts and other types of content. No UE iOS 7.0+

---

**Allow Open from Unmanaged to Managed Apps**

Allows Content to be opened from Unmanaged to Managed apps. Applies to Mail, Calendar events, Contacts and other types of content. No UE iOS 7.0+

---

**Allow AirDrop for Managed Apps**

Allow AirDrop to be used with managed apps. Yes UE iOS 9.0+

---

**Allow Screen Capture**

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



Figure D-21 Android DLP Configuration

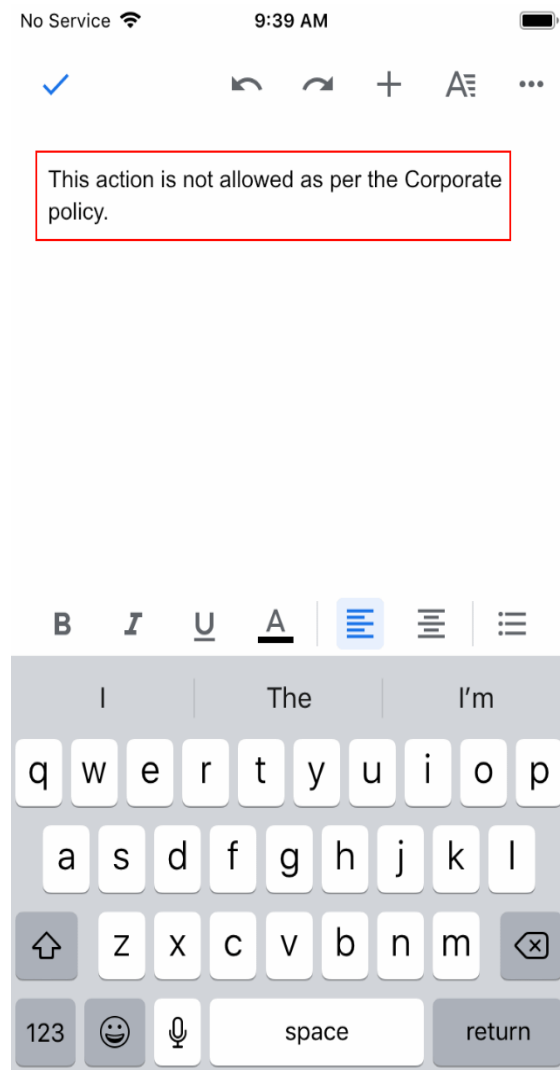
Default Android MDM Policy [Edit](#) [More](#)

Last Published: 05/23/2022 10:19 EDT [Version:65] Current Status: Published

- ▶ Device Settings
- ▶ Advanced Settings
- ▼ Android Enterprise Settings
  - Passcode
  - Security
  - Restrictions**
  - Accounts
  - App Compliance
  - ActiveSync
  - Wi-Fi
  - VPN
  - Certificates
  - Browser
  - COSU (Kiosk mode)
  - Wallpapers
  - System Update Settings
  - ...

Configure Restrictions	Yes	
▼ Device Features		
<b>Allow camera</b> To enable camera on device, camera app needs to be allowed in native app compliance apart from enabling this.	Yes	Android 5.0+ (PO & DO)
<b>Allow camera on personal profile</b> Camera app also needs to be allowed in native app compliance apart from enabling this.	Yes	Android 11+ (WPCO)
Mute Master Volume	No	Android 5.0+ (DO)
Allow unmuting of microphone	Yes	Android 5.0+ (DO)
Allow volume adjustments	Yes	Android 5.0+ (DO)
Allow bluetooth configuration	Yes	Android 5.0+ (DO)
<b>Allow outgoing beam</b> Note: Disabling this feature would not allow DO enrollments on the device.	Yes	Android 5.1.1+ (PO & DO)
<b>Allow sharing of locations</b> This policy controls location permission availability for apps. Keep this policy enabled if you are configuring WiFi policies, Trusteer policies or WiFi or Bluetooth settings within kiosk. Location permission is required for discovering list of configured networks, current connected network and discovering other bluetooth networks.	Yes	Android 5.0+ (PO & DO)

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



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

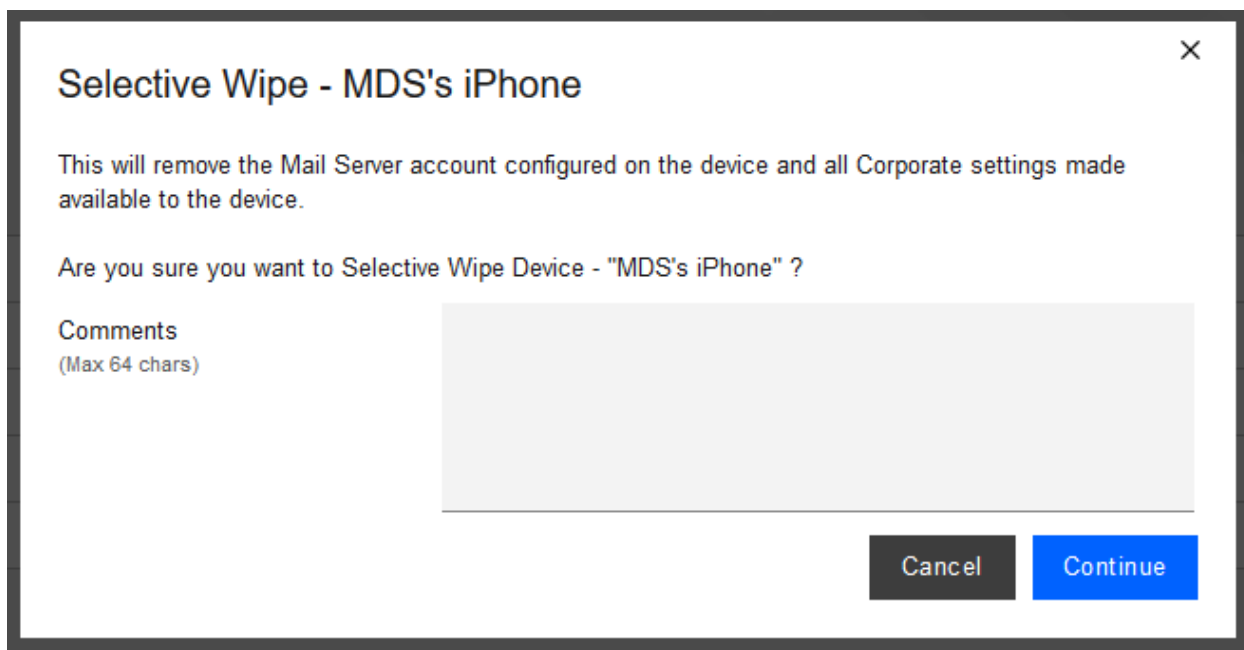
**Summary:** Personal data on the phone could be lost during a device wipe.

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

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

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

Figure D-23 Selective Wipe



**Additional Potential Mitigations:**

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

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

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

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

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

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

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

**Figure D-24 Application Inventory Information**

Application...	App ID	Full Version	Application...	Data Size (...)	Managed	App Source	Complianc...	Action	View Security...
GlobalProtect	com.paloaltonet.works.globalprotect.vpn	5.1.1	8.46	0.77	Installed by MDM	iTunes	Required	<a href="#">Remove App</a>	<a href="#">Security Details</a>
MaaS360	com.fiberlink.maas360forios	3.97.36	147.02	2.99	Installed by MDM	iTunes	Required	<a href="#">Remove App</a>	<a href="#">Security Details</a>
MaaS360 VPN	com.fiberlink.maas360.maas360vpn	3.20.50	7.53	0.02	Installed by MDM	iTunes	Required	<a href="#">Remove App</a>	<a href="#">Security Details</a>
zIPS	com.zimperium.ziPS.appstore	4.12.0	36.94	0.05	Installed by MDM	iTunes	Required	<a href="#">Remove App</a>	<a href="#">Security Details</a>

Navigation: < < 1 > > |  Jump To Page | Displaying 1 - 4 of 4 Records | CSV | Export

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

**Figure D-25 Location Information Restricted**

**IBM MaaS360** | With Watson | Search for Devices, Users, Apps or Docs

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

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

Select Applicable Ownership Types:  Corporate owned  Employee owned  Unknown

Select Applicable Group: All Devices

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

Select Applicable Ownership Types:  Corporate owned  Employee owned  Unknown

Select Applicable Group: All Devices

**Additional Potential Mitigations:**

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

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

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

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

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

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

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

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

Figure D-26 Non-Administrator Failed Portal Login

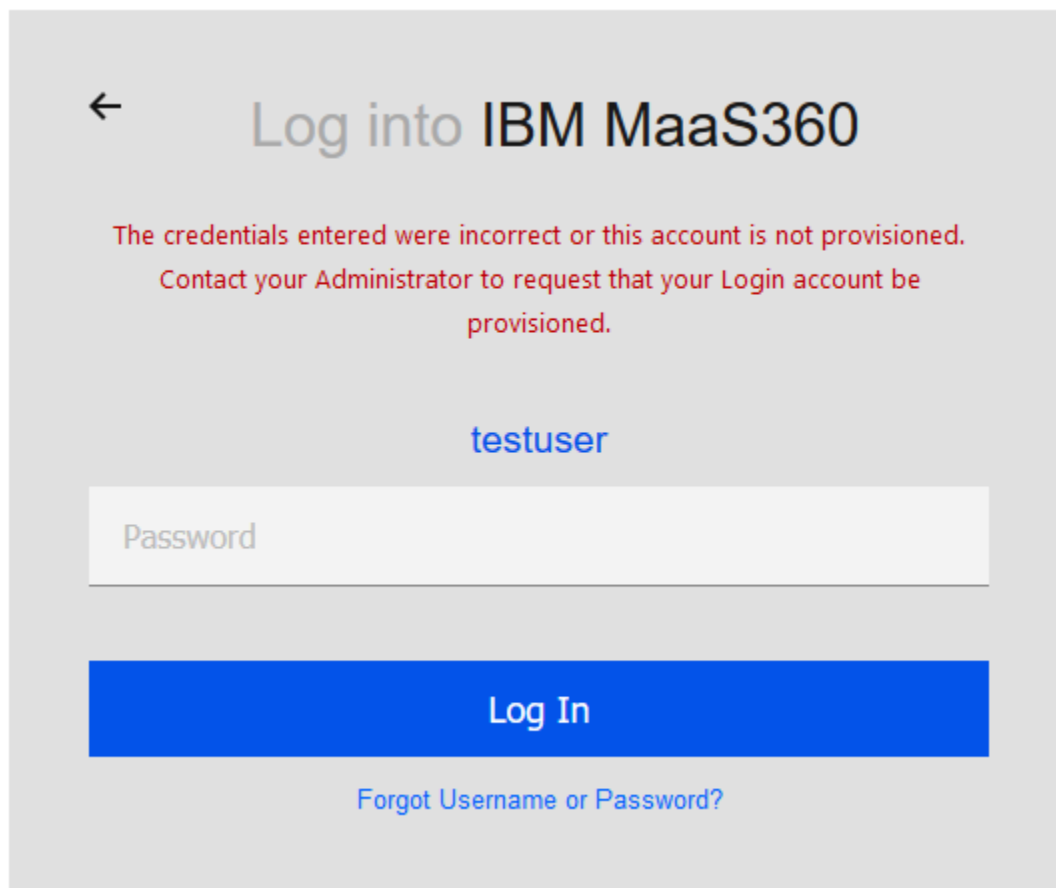


Figure D-27 Admin Login Settings

▼ Login Settings

Use this section to configure strong portal authentication for your Administrators.

**Note:** MaaS360 portal authentication mechanism will be used by default if Federated Single Sign-on is not used

Configure Federated Single Sign-on

- Use SAML for Single Sign-on
- Authenticate against Corporate User Directory

You will need to install Cloud Extender for this. For help with configuration refer to the [installation guide](#).

Default Domain

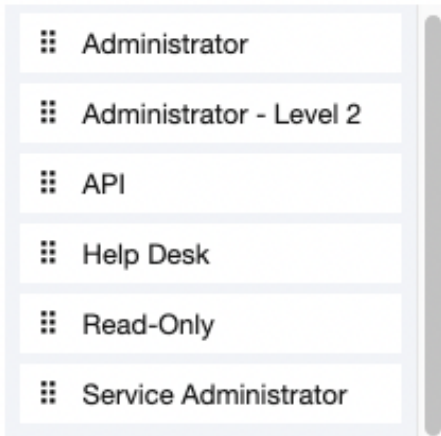
Custom login URL for your administrators: <https://m1.maas360.com/login?custID>

Automatically create new Administrator accounts and update roles based on User Groups

User Groups (Specify the Distinguished Name of the User Groups)

CN=Domain Admins,CN=Users,DC=enterj	Administrator - Level 2	▼ ⊖
	---Select Role---	▼ ⊕

Figure D-28 Administrator Levels



**Potential Mitigations:**

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

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

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

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

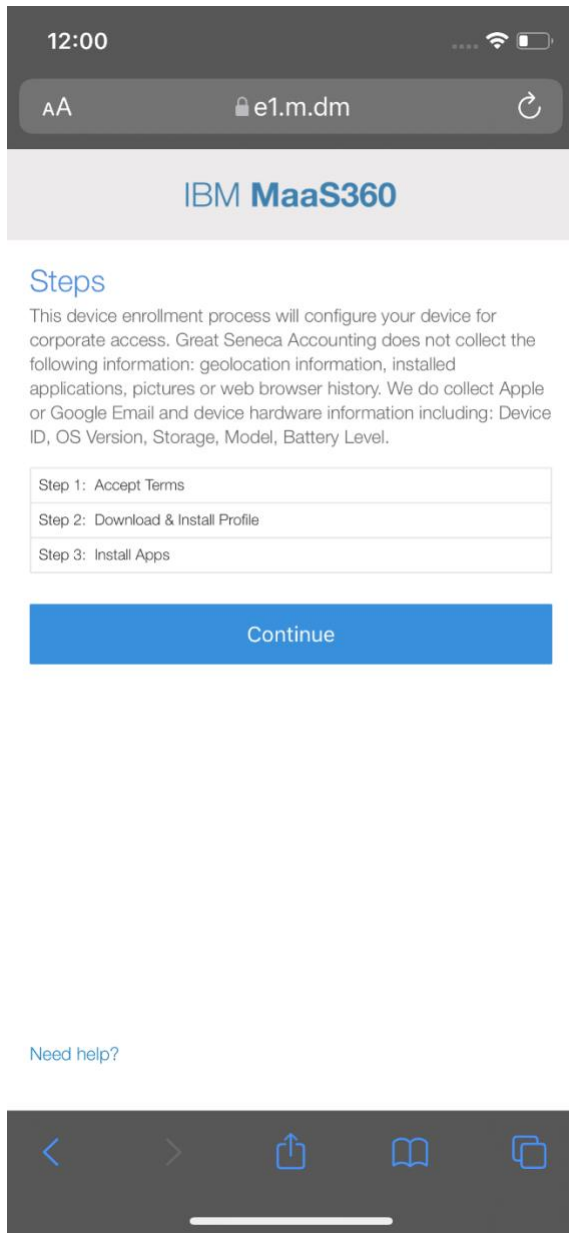
**Test Activity:** Test to ensure that MDM provides custom notification to users detailing collected device information.

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

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

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

Figure D-29 Mobile Device Information Collection Notification



**Additional Potential Mitigations:**

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



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

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

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

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

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

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

Figure D-30 Mobile Device Information Collection Notification

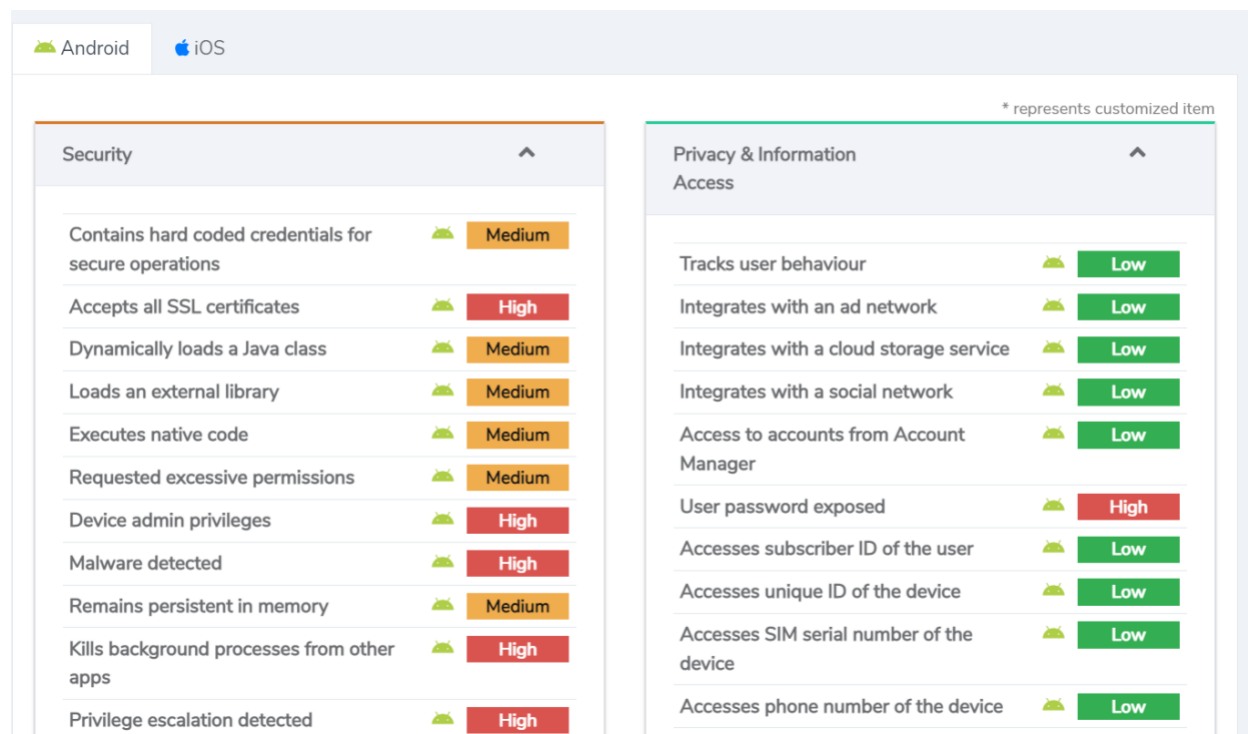


Figure D-31 Privacy and Information Access of the Application



















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

Figure D-32 Application Analysis

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

**Additional Potential Mitigations:**

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