NIST CYBERSECURITY PRACTICE GUIDE

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

Approach, Architecture, and Security Characteristics

for CIOs, CISOs, and Security Managers

Joshua Franklin Kevin Bowler Christopher Brown

Sallie Edwards Neil McNab Matthew Steele

NIST SPECIAL PUBLICATION 1800-4b

DRAFT

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-4b

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

DRAFT

Joshua Franklin

National Cybersecurity Center of Excellence
Information Technology Laboratory

Kevin Bowler

Christopher Brown

Neil McNab

Matthew Steele

The MITRE Corporation
McLean, VA

November 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-4b,
Natl. Inst. Stand. Technol. Spec. Publ. 1800-4b, 53 pages, (November 2015),
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

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

Public comment period: November 2, 2015 through January 8, 2016

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002) Rockville, MD 20850
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://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 more easily with relevant standards and best practices.

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

ABSTRACT

This document proposes a reference design on how to architect enterprise-class protection for mobile devices accessing corporate resources. The example solutions presented here can be used by any organization implementing an enterprise mobility management solution. This project contains two distinct builds: cloud and hybrid. The cloud build makes use of cloud-based services and solutions, while the hybrid build achieves the same functionality, but hosts the data and services within an enterprise's own infrastructure. The example solutions and architectures presented here are based upon standards-based, commercially available products.

KEYWORDS

mobility management; mobile; mobile device; mobile security; mobile device management

ACKNOWLEDGMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Nate Lesser	NIST National Cybersecurity Center of Excellence
Kevin Fiftel	Intel
Steve Taylor	Intel
Tim LeMaster	Lookout
Rick Engle	Microsoft
Rene Peralta	Microsoft
Paul Fox	Microsoft
Atul Shah	Microsoft
Adam Madlin	Symantec
Kevin McPeak	Symantec
Steve Kruse	Symantec

Contents

List of Figures

List of Tables

1 Summary

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide addresses the challenge of securely deploying and managing mobile devices in an enterprise. In many organizations, mobile devices are adopted on an ad hoc basis, possibly without the appropriate policies and infrastructure to manage and secure the enterprise data they process and store. Introducing devices in this fashion increases the attack surface of an enterprise, requiring that additional controls be implemented to reduce the risk of intrusion.

The NIST 1800-4 series of documents contain:

- descriptions of a mobile device deployment alongside an associated enterprise mobility management (EMM) system to implement a set of security characteristics and capabilities, along with a rationale for doing so
- a series of How-To Guides-including installation and configuration of the necessary services-showing system administrators and security engineers how to achieve similar outcomes

The solutions and architectures presented are built upon standards-based, commercially available products, and can be used by any organization deploying mobile devices in the enterprise that is willing to have at least part of the solution hosted within a public cloud. This project contains two distinct builds - cloud and hybrid. The cloud build uses cloud-based data storage and management services for mobile devices, while the hybrid build achieves the same functionality as the cloud build, but hosts a portion of the data, services, and physical equipment within an enterprise's own infrastructure.

1.1 The Challenge

Mobile devices allow an organization's users to access information resources wherever they are, whenever they need, presenting both opportunities and challenges. The constant Internet access available via a mobile device's cellular and Wi-Fi connections has the potential to make business practices more efficient and effective, but it can be challenging to ensure the confidentiality, integrity, and availability of the information that a mobile device accesses, stores, and processes. As mobile technologies mature, users increasingly want to use both organization issued and personally owned mobile devices to access enterprise services, data, and other resources to perform work-related activities. Despite the security risks posed by today's mobile devices, organizations are under pressure to accept them due to several factors, including anticipated cost savings increased productivity and users' demand for more convenience.

1.2 The Solution

This NIST Cybersecurity Practice Guide demonstrates how commercially available technologies can enable secure access to the organization's sensitive email, contacts, and calendar information from users’ mobile devices. In our lab at the National Cybersecurity Center of Excellence (NCCoE) at NIST, we built an environment to simulate a lightweight enterprise architecture, including common components present in most organizations such as directory services.

Our approach to mobile device security includes:

1. determining the security characteristics required to mitigate in large part the risks of storing enterprise data on mobile devices and transmitting enterprise data to and from mobile devices
2. mapping security characteristics to standards and best practices from NIST and other organizations recognized for promulgating security information, such as the National Security Agency (NSA) and the Defense Information Systems Agency (DISA)
3. architecting a design for our example solution
4. selecting mobile devices and EMM systems that provide the necessary controls
5. evaluating our example solution

Although corporately owned and personally enabled (COPE) and bring your own device (BYOD) scenarios are not specifically addressed directly by this project, the necessary features to enable a secure demonstration of either scenario are available. Those making IT policy and infrastructure decisions within an organization will need to use their own judgment to decide where on the device management spectrum they choose to exist. To make these security controls available, organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, operating system (OS), management agent, and the applications used to accomplish business objectives. This document provides but **one** method of accomplishing this task.

1.3 Benefits

This proposed solution provides the following value to organizations:

1. reduces risk so that employees are able to access the necessary enterprise data from nearly any location, over any network, using a wide variety of mobile devices
2. enables the use of BYOD, COPE, and other mobile device deployment models, which may provide cost savings and increased flexibility for organizations
3. enhances visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
4. implements industry standard mobile security controls reducing long term costs and decreasing the risk of vendor lock-in

1.4 Technology Partners

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partner (NCEP). NCEPs are IT and cybersecurity firms that have pledged to support the NCCoE's mission of accelerating the adoption of standards-based, secure technologies. They contribute hardware, software, and expertise. In this project, we worked with:

- Intel
- Lookout

- Microsoft
- Symantec

1.5 Feedback

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

- email mobile-nccoe@nist.gov
- participate in our forums at https://nccoe.nist.gov/forums/mobile-device-security

Or learn more by arranging a demonstration of this example solution by contacting us at https://nccoe.nist.gov/forums/mobile-device-security

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to mobile device security. The reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-4a: *Executive Summary*
- NIST SP 1800-4b: *Approach, Architecture, and Security Characteristics* - what we built and why (you are here)
- NIST SP 1800-4c: *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 and technology officers will be interested in the *Executive Summary* (*NIST SP 1800-4a*), which describes the:

- challenges enterprises face in implementing and using mobile devices
- 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 this part of the guide, *NIST SP 1800-4b*, which describes what we did and why. The following sections will be of particular interest:

- Section 4.4.3, Risk, provides a description of the risk analysis we performed.
- Section 4.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary*, *NIST SP 1800-4a*, with your leadership team members to help them understand the importance of adopting standards-based access management approaches to protect your organization's digital assets.

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 1800-4c*, to replicate all or parts of the build created in our lab. The How-To 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 a solution that would support the deployment of an ABAC system and the corresponding business processes.[1] Your organization's

security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 4.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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, and join the discussion at https://nccoe.nist.gov/forums/mobile-device-security.

1.Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept. Such identification is not intended to imply recommendation or endorsement by NIST or the NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

3 Introduction

Enterprises traditionally established boundaries to separate their trusted internal information technology (IT) network(s) from untrusted external networks. When enterprise users consume and generate organizational information on mobile devices, this traditional boundary erodes. Due to the rapid changes in today's mobile platforms, enterprises have the challenge of ensuring that mobile devices connected to their networks can be trusted to protect sensitive data as it is stored, processed, and transmitted while still giving users the features they have come to expect from mobile devices. Additionally, some enterprises host enterprise data in a public cloud infrastructure, which also needs to be protected.

This guide proposes a system of commercially available technologies that provide enterprise-class protection for mobile platforms accessing and interacting with enterprise resources. The implementations presented here can be used by any organization interested in implementing an enterprise mobility management (EMM) solution. This project contains two distinct builds: one focuses on cloud-based data, management, and services, while the other leverages the same EMM infrastructure in-house. The cloud build may be useful to smaller organizations wanting to rapidly deploy a mobile solution or offload services hosted in-house to the cloud. The hybrid build uses the same services as the cloud build, but hosts some of these same services at an organization's premises.

4 Approach

When conceptualizing the project, the build team looked to EMM systems deployed by industry, where users were sometimes frustrated with policies pushed from enterprises, and system administrators were confused about the most appropriate policies to push to mobile devices. This information was the impetus for creating the scenarios included in the building block definition document [1].

A number of security characteristics and capabilities are documented within the building block definition. To create them, we analyzed the content and concepts from multiple standards to generate the necessary security characteristics. These include NIST Special Publication (SP) 800-124 [2], NIST SP 800-164 (DRAFT) [3], NSA mobile capabilities package [8], and the appropriate National Information Assurance Partnership (NIAP) protection profiles [12] [13] [14].

The cloud build is geared toward organizations wanting to operate and maintain systems external to their enterprise environment to lower operational expenses. These organizations elect to leverage a Software as a Service (SaaS) cloud provider for services such as office productivity tools for workstations. The addition of mobile devices into this environment adds complexity because the organization requires protection of its sensitive data, but this data is not directly under its control.

The hybrid build is meant for organizations that are concerned with the risks associated with storing and processing confidential enterprise information in the cloud. These organizations have the willingness and technical expertise to implement and manage the necessary infrastructure to host the services on premises, and may have the need to prevent cloud-based authentication and not wish to expose their existing identity repository to the cloud. The hybrid build includes a combination of enterprise assets likely to be present in an organization's existing network and adds cloud services for EMM, making it a starting point for an organization that has significant investment in or dependence on an internal AD server.

4.1 Audience

This Practice Guide is for organizations that want to securely deploy and manage mobile devices, such as smartphones and tablets, within their enterprises. It is intended for executives, security managers, engineers, administrators and others who are responsible for acquiring, implementing, and maintaining EMM deployments. This document will be of particular interest to those looking to deploy mobile devices in the near term and system architects already managing a mobile deployment. Please refer to section 2 for how different audiences can effectively use this guide.

4.2 Scope

This publication seeks to assist organizations in developing and implementing sound EMM deployments for securely accessing email, contacts, and calendaring. It provides practical, real-world guidance on developing, implementing, and maintaining secure, effective mobile devices, mobile applications, and EMM solutions in an enterprise. The publication presents EMM technologies from a high-level viewpoint and then provides a step-by-step guide to implementing a specific solution. The operating systems and applications storing and transmitting the data must be securely configured and implemented, which is accomplished in part via EMM.

The problem statement for this building block [1] describes a large number of security and functional characteristics and capabilities. It is important to note that this document does not exercise each and every one of them. The specific security characteristics and capabilities used in the cloud and hybrid builds are noted later in section 5.3. The scope of these builds is the successful execution of the following capabilities:

- secure implementation of email, contacts, and calendaring
- installation, implementation, and configuration of an EMM system
- hardened mobile devices securely accessing enterprise data for which the user and device are authorized

4.3 Assumptions

The following assumptions exist for this project:

- Both the cloud and hybrid builds are highly dependent on Microsoft's cloud platform, including Microsoft Office 365 and Microsoft Intune. Organizations trust these services to function properly and to appropriately handle sensitive information.
- Organizations manage their own domains, with the ability to alter Domain Name System (DNS) information on an ad hoc basis to prove ownership of a DNS name space so it can be associated to Office 365 services, email authority, MX records, and establishment of federation services.
- Within the hybrid build, organizations expose a system that proxies the connection between their Active Directory Domain Services (ADDS) and Microsoft's cloud services.
- Organizations trust the mobile operating systems within this build (e.g., Android, iOS, Windows) to store and process sensitive information

4.4 Risk Assessment

According to NIST SP 800-30, *Risk Management Guide for Information Technology Systems* [19], "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* [20], material available to the public. The risk management framework (RMF) guidance as a whole proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

The nature of mobile devices creates a set of unique risks in the modern enterprise. While we do not present a full risk assessment, it is useful to highlight the broad categories of threats and vulnerabilities. We have used NIST SP 800-124 [2] and United States Computer Emergency Readiness Team (US-CERT) Technical Information Paper-TIP-10-105-01, Cyber Threats to Mobile Devices [21] as sources for this section, which should not be considered an exhaustive list of threats to mobile devices.

4.4.1 Threats

Below are common threats to mobile devices:

- mobile malware
- social engineers
- stolen data due to loss, theft, or disposal
- unauthorized access
- electronic eavesdropping
- electronic tracking
- access to data by legitimate third party applications

4.4.2 Vulnerabilities

Vulnerabilities are commonly associated with applications that are installed on mobile devices. However, it is important to recognize that vulnerabilities can be exploited at all levels in the mobile device stack, which is outlined below in figure 4.1:

Figure 4.1 Mobile Technology Stack

Note that on mobile devices, the firmware and hardware levels are not as clearly defined as figure 4.1 depicts. Mobile devices with access to a cellular network contain a baseband processor comprising a distinct telephony subsystem used solely for telephony services (e.g., voice calls, texts, data transfer via the cellular network) [22]. This processor and the associated software/firmware on which it operates are separated from the mobile operating system running on the application processor. Furthermore, some mobile devices contain additional security-specific hardware and firmware used to assist with making security decisions and

storing important information, such as encryption keys, certificates and credentials [15] [16] [17].

For up-to-date information regarding vulnerabilities, we recommend security professionals leverage the National Vulnerability Database (NVD). The NVD is the U.S. government repository of standards-based vulnerability management data [24].

4.4.3 Risk

Using the common threats identified previously as a guide, we identified risks that an organization might face when deploying mobile devices. In general these risks focus on data leakage and compromise. Since modern mobile devices process many types of information (e.g., personal, enterprise, medical), there are many types of data leakages, each with their own level of severity in a given context. The following are common reasons for data leakage and/or compromise:

- lack of mobile access control (e.g. loss of the mobile device, lock screen protection, enabling smudge attacks)
- lack of confidentiality protection (e.g., encryption of data in transit) of information due to operating on unsafe or untrusted networks (e.g. WiFi, Cellular)
- unpatched firmware, operating system, or application software bypassing the operating systems security architecture (e.g., rooted/jailbroken device)
- users running malicious mobile applications which may glean information via misuse of inter-process communication (IPC) or other access control mechanisms
- device interaction with cloud services outside corporate control
- misuse or misconfiguration of location services, such as GPS
- acceptance of fake mobility management profiles, providing malicious actors with a high degree of device control
- social engineering via voice, text or email communication

4.4.4 Security Control Map

Using this risk information, we extrapolated security characteristics. Table 4.1 maps these characteristics to the controls from the NIST Cybersecurity Framework (CSF) [28], NIST SP 800-53 Revision 4 [29], International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) 27002 [30], and the Council on CyberSecurity's Critical Security Controls for Effective Cyber Defense [31]. Note: Before transfer to the Council on Cybersecurity, [31] was informally known as the Sysadmin, Audit, Networking, and Security (SANS) Consensus Audit Guidelines (CAG) 20.

142 **Table 4.1 Security Control Map**

Example Characteristic		Cybersecurity Standards & Best Practices					
Security Characteristic	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4	IEC/ISO 27002	CAG20
Data Protection	protected storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe; protected communications: virtual private network (VPN), to include per-app VPN; data protection in process: encrypted memory, protected execution environments	Protect	Data Security, Protective Technologies	PR.DS-1, PR.DS-2, PR.DS-5, PR.PT-4	AC-20, AU-9, IA-6, IA-7, MP-6, SA-13, SC-8, SC-11, SC-12, SC-13, SC-17, SI-12	6.2.1, 9.4.3, 9.4.4, 9.4.5, 10.1.2, 12.4.2, 12.4.3, 13.1.1, 13.2.1, 13.2.3, 14.1.3	CSC-15
Data Isolation	virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation	Protect	Data Security, Protective Technologies	PR.DS-1, PR.DS-5, PR.PT-3	CM-11, SA-13, SC-3, SC-11, SC-35, SC-39, SC-40, SI-16	6.2.1, 6.2.2, 9.4.1, 9.4.4, 12.2.1	CSC-7, CSC-12, CSC-14
Device Integrity	baseband integrity checks, application black/whitelisting, device integrity checks: boot validation, application verification, verified application and OS updates, trusted integrity reports, policy integrity verification	Protect, Detect	Data Protection, Anomalies and Events, Security Continuous Monitoring	PR.DS-6, DC.CM-4, DE.CM-5, DE.CM-6	AC-20, CM-3, IA-3, IA-10, SA-12, SA-13, SA-19, SC-16, SI-3, SI-4, SI-7	6.2.1, 12.2.1, 14.2.4, 15.1.3	CSC-3, CSC-6, CSC-12

Table 4.1 Security Control Map (Continued)

Example Characteristic		Cybersecurity Standards & Best Practices					
Security Characteristic	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST SP 800-53 rev4**	**IEC/ISO 27002**	**CAG20**
Monitoring	canned reports and ad-hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection[a], geo-fencing	Identify, Protect, Detect	Asset Management, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes	ID.AM-1, ID.AM-2, PR.DS-3, PR.MA-2, PR.PT-1, DE.AE-1, DE.AE-1, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8, DE.DP-2, DE.DP-4	AC-2, AC-3, AC-7, AC-21, AC-25, AU-3, AU-5, AU-5, AU-7, AU-8, AU-9, AU-10, AU-12, AU-13, AU-14, AU-15, AU-16, CA-7, CM-2, CM-3, CM-6, CM-8, CM-11, IA-4, IR-4, IR-5, IR-7, IR-9, MA-6, SA-13, SA-22, SC-4, SC-5, SC-7, SC-18, SC-42, SC-43, SI-3, SI-4, SI-5	6.1.4, 6.2.1, 6.2.2, 8.1.1, 8.1.2, 9.2.3, 9.2.5, 9.4.4, 9.4.5, 10.1.2, 12.2.1, 12.4.1, 12.4.2, 12.4.3, 12.5.1, 12.6.1, 12.7.1, 13.1.1, 15.1.3, 16.1.2, 16.1.4, 16.1.5, 18.2.3	CSC-1, CSC-2, CSC-5, CSC-6, CSC-10, CSC-11, CSC-12, CSC-13, CSC-14, CSC-18

Table 4.1 Security Control Map (Continued)

Example Characteristic		Cybersecurity Standards & Best Practices					
Security Characteristic	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST SP 800-53 rev4**	**IEC/ISO 27002**	**CAG20**
Identity and Authorization	local user authentication to applications, local user authentication to device, remote user authentication, remote device authentication, implementation of user and device roles for authorization, credential and token storage and use, device provisioning and enrollment, device provisioning and enrollment	Protect, Detect	Access Control, Protective Technologies, Asset Management	ID.AM-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.PT-3, DE.CM-3, DE.CM-7	AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-16, AC-17, AC-18, AC-19, AC-20, AU-16, CM-5, CM-7, IA-2, IA-3, IA-5, IA-6, IA-7, IA-8, IA-9, IA-11, MP-2, SA-9, SA-13, SA-19, SC-4, SC-16, SC-40	6.2.1, 6.2.2, 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 13.1.1, 13.1.2, 13.2.2, 13.2.3, 14.1.2, 14.1.3	CSC-8, CSC-9
Privacy Protection	informed consent of user, data monitoring minimization, privacy notification provided to user	Identify, Protect	Governance, Training and Awareness	ID.GV-3, PR.AT-1	AR-4, AR-7, DM-1, IP-1, IP-2, SE-1, TR-1, UL-1	18.1.4	CSC-17

a. In this case, the operating system or application monitors the device to determine if it has been rooted or jailbroken.

4.5 Technologies

Following the draft publication of NIST SP 800-164 [2], NIST began looking for additional ways to foster mobile security in the enterprise. The three mobility security principles of NIST SP 800-164 (i.e., device integrity, isolation, and protected storage) were used as a baseline. Moving forward, we used other standards and guidance relating to mobility to build upon these principles to create the full list of security characteristics and capabilities in section 5.3.

The initial document describing this project's security challenge was released in 2014 [1]. After incorporating public comments and revising the document, the NCCoE MDS team consulted with NCCoE's National Cybersecurity Excellence Partnership (NCEP) partners to understand which technologies would be applicable to this project. The technologies used in this project are listed in table 4.2.

151 **Table 4.2 Participating Companies and Contributions Mapped to Controls**

Application	Company	Product	Use	CSF Categories	NIST SP 800-53 rev4 Controls
EMM	Microsoft	Intune	Web service used to define and send policies to mobile devices	PT, CM	AC-3, CM-7
Cloud Platform	Microsoft	Office 365 Enterprise E3	Provides directory and EMM services	PT, CM, AC	AC-3, CM-7, AC-2
Configuration Management	Microsoft	System Center 2012 R2 Configuration Manager SP 1	Provides IT asset management and also delivers policies to Microsoft cloud services	AM, DS	CM-8, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
Outlook &Community Portal Mobile Applications	Microsoft	Outlook & Community Portal Mobile Applications	Provides provisioning, email, contacts, and calendaring capabilities	DS, PT	AC-20, AU-9, IA-3, IA-6, MP-6, SC-7, SC-8, SC-11, SC-12, SC-13, SC-17, SI-12
Mobile Device	Intel	Lenovo Miix 2.8	Mobile Device	DS, PT	AC-20, AU-9, IA-6, IA-7, MP-6, SA-13, SC-8, SC-11, SC-12, SC-13, SC-17, SI-12
Digital Certificate	Symantec	X.509 Certificate	Used for authentication of endpoints throughout the projects	DS	SC-8
Malware and OS Integrity Detection	Lookout	Lookout Android application	Used to identify malicious software and root detection on a mobile device	CM	SI-3, RA-5

152

5 Architecture

This section documents the functional and network architectures of both the cloud and hybrid builds. Before continuing, it is useful to describe a notional EMM deployment. An EMM can consist of multiple services, including mobile device management (MDM), mobile application management (MAM), and other mobile computing services. Enterprises use EMMs to define a set of policies, push those policies to a mobile device, and then enforce these policies on a mobile device via an enforcement mechanism on the device (e.g., OS, mobile application). Before policies can be pushed to a given device, an enterprise must enroll that device into the management services. Once enrolled, policies, such as the requirement to use an eight-digit passcode, are defined and then pushed to the device via a secure communications channel. These processes and technologies enable users to work inside and outside the enterprise network with a securely configured mobile device with the following functional and security capabilities:

- protected storage - We leverage device encryption, application-level encryption, and remote wipe capabilities.
- protected communications - All network communication channels in the architecture use Transport Layer Security (TLS).
- sandboxing - We leverage OS mechanisms that isolate user-level applications from each other to prevent data leakage between applications.
- device integrity checks - We use device-specific implementations of boot validation, verified application and OS updates.
- auditing and logging - Device, mobile operating system, and application information is available through an on-premises configuration manager (hybrid build) or a device management administration portal (cloud build).
- asset management - The configuration manager identifies and tracks devices that access enterprise email, contacts, and calendaring. Although minimally included in the cloud build, a more robust set of asset management capabilities is included in the hybrid build.
- authentication of device owner - The MDM service enforces authentication of the device owner using their enterprise credentials when using identity federation.
- device provisioning, deprovisioning, and enrollment - Device owners are provisioned and deprovisioned access to email/contact/calendaring services on approved mobile devices. Device owners may enroll remotely with their enterprise credentials.
- privacy notifications - Device owners are informed of privacy implications of certain device and application functionality during device management enrollment.
- automatic, regular device integrity and compliance checks - The MDM and mobile threat protection (MTP) clients periodically scan the device for threats and compliance. Results are accessible to system administrators.
- automated alerts for policy violations - The MDM and MTP services alert designated personnel when policy violations occur, such as when a device is out of compliance or when a software threat is installed on the device.
- security incident remediation - The organization can perform remote remediation when a security incident is detected on the device. Options include disabling access to email/ contacts/calendaring from the server side or remotely wiping the mobile device.

This project installs, configures, and integrates two distinct MDMs from Microsoft: Office 365 and Microsoft Intune. These MDMs offer varying levels of functionality - security and otherwise.

The integration of the various technologies within these builds would be extremely difficult without the use of standards and best practices. The following standards are crucial to a successful implementation:

- NIST SP 800-124 Rev 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise [2]
- NIST SP 800-164 (Draft): Guidelines on Hardware-Rooted Security in Mobile Devices [3]
- NIST SP 800-147: BIOS Protection Guidelines [4]
- NIST SP 800-155: BIOS Integrity Measurement Guidelines [5]
- NIST SP 800-88 Rev. 1: Guidelines for Media Sanitization [6]
- NIST SP 800-163: Vetting the Security of Mobile Applications [7]
- NSA Mobility Capability Package 2.3 [8]
- Department of Defense Commercial Mobile Device Implementation Plan [9]
- CIO Council: Digital Government Strategy Government Mobile and Wireless Security Baseline [10]
- GSA Managed Mobility Program Request for Technical Capabilities [11]
- NIAP Protection Profile for Mobile Device Management Version 1.1 [12]
- NIAP Protection Profile for Mobile Device Fundamentals 2.0 [13]
- NIAP Protection Profile - Extended Package for Mobile Device Management Agents [14]
- Global Platform Specifications for Secure Element and Trusted Execution Environment [15] [16]
- Trusted Computing Group specifications for Trusted Platform Module [17]

Section 5.1, Cloud Build: Architecture Description and section 5.2, Hybrid Build: Architecture Description describe the cloud and hybrid architectures, respectively, as well as their benefits and security features.

5.1 Cloud Build: Architecture Description

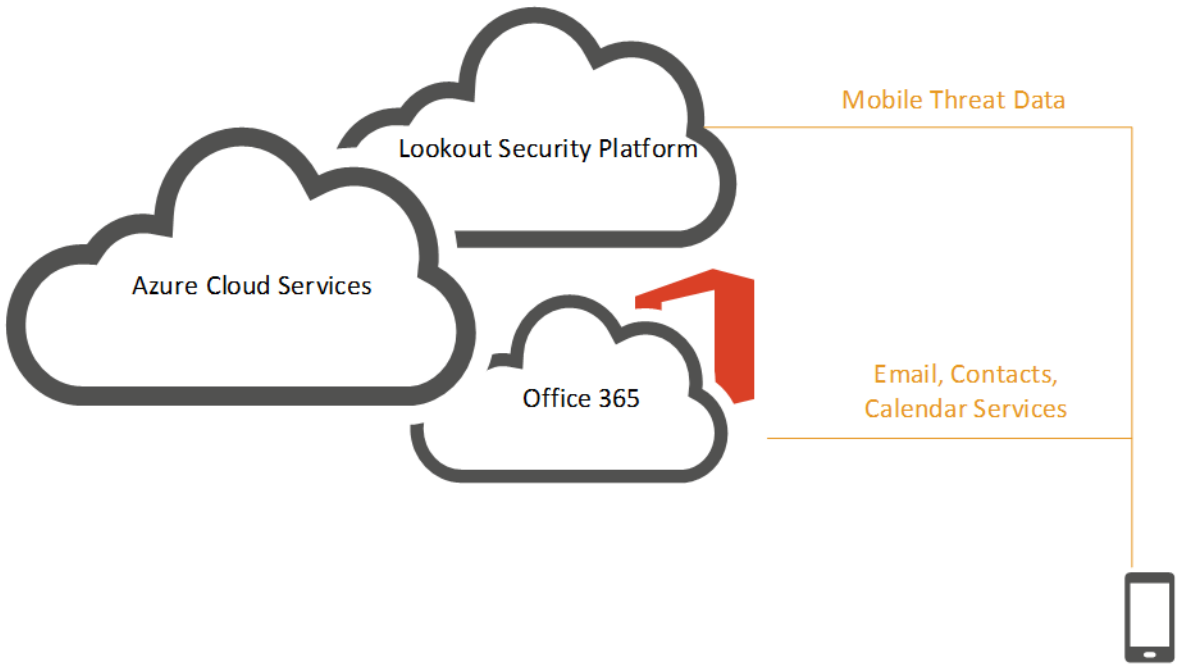
The cloud build is intended to assist organizations wanting to leverage mobile devices and manage these devices via the cloud. They may include entities needing to stand up mobile deployments with minimal effort, or entities with established enterprise mobile deployments wanting to leverage the benefits of cloud computing. This build can be quickly deployed within enterprises without an internal AD server. Although this build uses the MDM system included with Office 365, an organization could choose to leverage Intune instead in this instance. Office 365 was chosen to diversify the MDMs used within this project.

This solution can be easily configured and operated as a cloud service to onboard personally or enterprise-owned mobile devices into the EMM. This allows users to access enterprise resources and enterprise managers to push policies to mobile devices. Office 365 allows for a

variety of policies to be pushed to the device (detailed in appendix C), but offers a significantly reduced feature set when compared with Microsoft Intune.

Figure 5.1 provides the overall architecture of the cloud build.

Figure 5.1 Cloud Build Architecture



Mobile devices communicate with Office 365 over a public communications network, which then accesses Microsoft's mobile applications such as Word and Excel. System administrators manage devices via the Office 365 admin center. In order to make full use of cloud services, a globally recognized commercial domain is required. For our test purposes we acquired cmdsbb.org[1] from a commercial domain registrar and used it throughout this guide. The exact method for DNS acquisition and management is unique for each registrar and enterprise, and is out of scope for this guide.

5.1.1 Cloud Architecture Benefits

The security benefits of a cloud architecture will depend heavily on the service provider that is chosen. NIST SP 800-146 states that in a public cloud scenario, "the details of provider system operation are usually considered proprietary information and are not divulged to consumers … Consequently, consumers do not (at the time of this writing) have a guaranteed way to monitor or authorize access to their resources in the cloud" [25]. However, organizations that lack security subject matter experts can realize a benefit because "clouds may be able to improve on some security update and response issues." We recommend that readers consider the

1.CMDSBB is an acronym for cloud mobile device building block.

recommendations in Section 9.3 of NIST SP 800-146 [25] before choosing a cloud service provider.

Functionally, the cloud architecture benefits from the rapid development of features - a trait found in modern web-based services. The MDM service used within the cloud build is able to keep pace with the quick-changing landscape of mobile devices. For example, mobile device vendors can add device management features as they iterate through OS versions. These features can be immediately available through the cloud service rather than delayed by a traditional on-premises software upgrade cycle.

Another benefit of the cloud architecture is the ability to manage mobile devices from anywhere. Our cloud MDM portal is available to administrators through a web interface; the only requirements are a modern web browser and an Internet connection. This allows administrators to take action while outside the boundaries of the enterprise network. Further, it reduces reliance on desktop applications that may not be available on all workstations.

5.1.2 Cloud Build Security Characteristics

Much of the security of the cloud build relies on the protections provided by the mobile device, the policies implemented by the MDM, and the Microsoft Outlook mobile application. The initial selection of the mobile device makes a large difference in the security features available due to low-level boot firmware and/or OS integrity checks. Some mobile devices provide some form of secure boot rooted in hardware or firmware, while other devices offer no boot integrity at all. Another feature available only on certain mobile devices is secure key storage, which may or may not be rooted in hardware. Organizations may wish to ensure that the devices they support include these desirable hardware/firmware capabilities.

An individual who decides to participate in a managed scenario, must download the Microsoft Community Portal application and input the required information. Then the device is provisioned into the EMM, and the default set of policies listed in appendix C is applied to the device. This includes local authentication to the mobile OS via a lockscreen and the encryption capabilities provided by the mobile OS to protect data on the device. The Outlook application provides an additional layer of application-level encryption to email and Outlook application-related data via the Microsoft managed application policies [26].

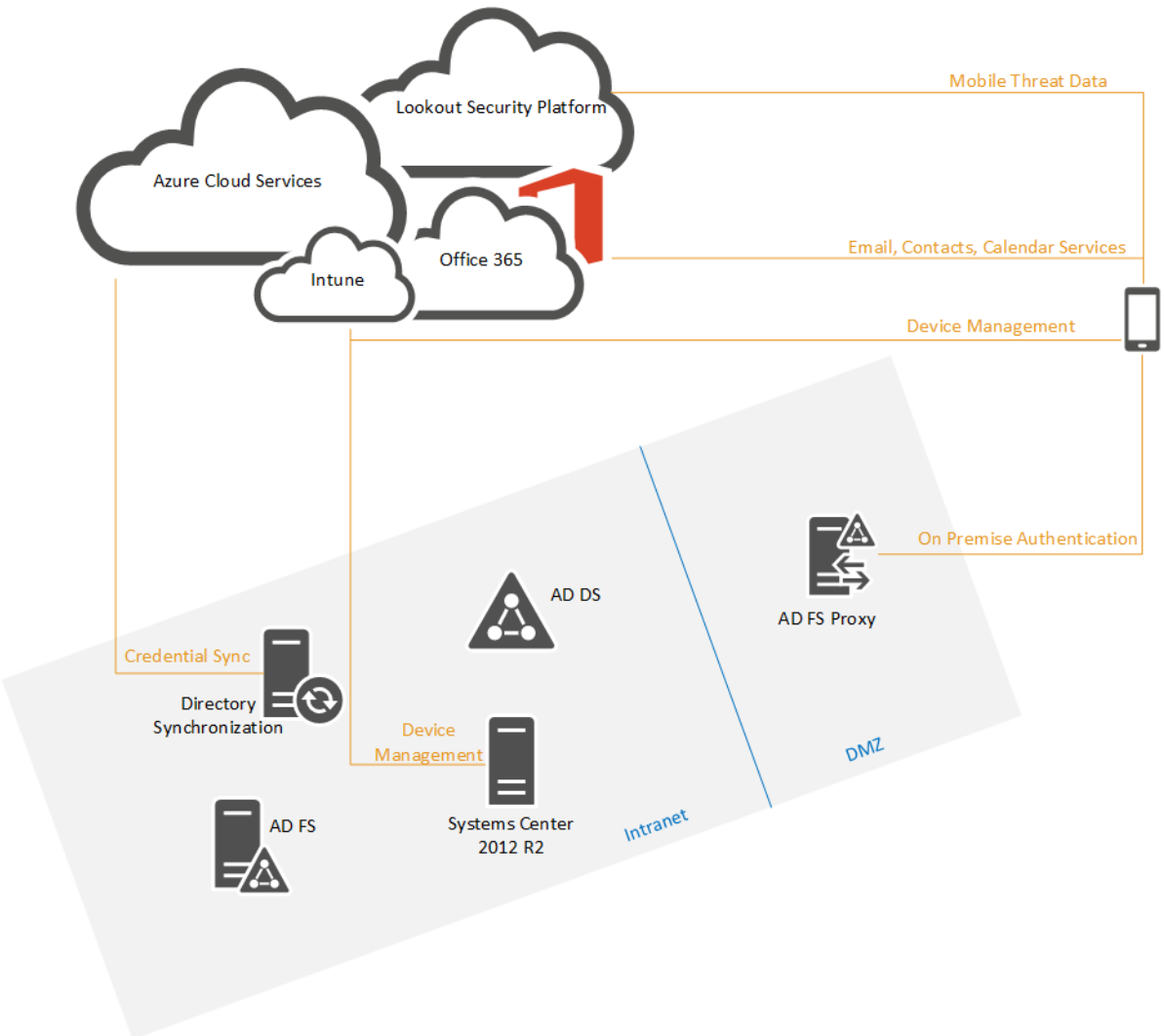
The Outlook application uses a TLS 1.2 tunnel to communicate with the Office 365 email, calendaring, and contact services, and does the same for the cloud-based AD service offered by Office 365. The management interface to access the Office 365 EMM and other administrative functions is also protected via a TLS 1.2 tunnel over the Internet. Further, if a user is not in compliance with the policies specified in appendix C, then the system administrator is notified. As an additional layer of protection, the inclusion of the Lookout for Enterprise application also provides anti-malware protection alongside jailbreak/root detection.

5.2 Hybrid Build: Architecture Description

The hybrid build leverages the same cloud-based services from the cloud build, but integrates them into the network in a different manner. It includes a combination of enterprise assets likely to be present within an organization's existing network, including EMM capabilities, and adds cloud services for MDM. This build might be a starting point for an organization that has significant investment in or dependence on an internal AD server. The cornerstone of the hybrid

build is the existing AD server housing user data and associated credentials. Figure 5.2 depicts the high-level hybrid build architecture.

Figure 5.2 Hybrid Build Architecture



Microsoft Intune functions as the EMM for this solution, which can be easily configured and operated as a cloud service to onboard personally or enterprise-owned mobile devices into the EMM. This allows users to access enterprise resources and allows those involved with enterprise management to push policies to mobile devices.

The hybrid build contains the following elements:

- In the cloud:
  - Intune provides MDM, MAM, and endpoint management capabilities. Devices outside the enterprise firewall can connect to Intune for configuration management and monitoring.

- Office 365 synchronizes with AD Domain Services 2012R2 to provide email, contacts, and calendaring services. It also has its own user database, which can be selectively synced with AD Domain Services (DS) via the Azure AD Sync Tool.
- The Lookout Security Platform provides the backend to the threat protection mobile application to identify risks on the device.

- In the enterprise intranet:
  - AD DS stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches. It is used to centrally manage servers and users and information is synchronized with cloud services.[1]
  - AD Federation Services (FS) 2012R2 is a standards-based service that allows the secure sharing of AD DS identity information between trusted business partners across an extranet.[2]
  - Azure AD Sync Services is used to mirror Azure AD and Office 365 with a single-forest or multi-forest on premises AD. It does not require access to the Azure AD tenant that is created with the associated Office 365 subscription.
  - Systems Center Configuration Manager (SCCM) provides unified management across on-premises, service provider, and Azure environments for both Windows computers and mobile devices.[3]
- In the enterprise demilitarized zone (DMZ):
  - The Web Application Proxy (WAP) provides reverse proxy functionality for AD FS to allow access to users on any device from outside the enterprise network. It acts as a security barrier by not allowing direct access into the AD environment from the Internet and is not joined to the domain itself.
- From the Internet:
  - Mobile applications (Lookout MTP, Intune MDM client, Outlook) deployed to the device that support the functional and security characteristics of this build.

Additional components not pictured:

Fully making use of cloud services requires a globally recognized commercial domain. For our test purposes we acquired hmdsbb.org from a commercial domain registrar and used it throughout this Practice Guide. The exact method for DNS management will be unique for each registrar and organization, and it is out of scope for this Practice Guide.

The build team generated a certificate from the Symantec Secure Site Pro Secure Sockets Layer (SSL) Certificates service to fulfill prerequisite requirements from AD FS to federate with Office 365.

A router/firewall is used to simulate various network and security enclaves within an organization.

1.https://technet.microsoft.com/en-us/library/Cc770946(v=WS.10).aspx
2.https://msdn.microsoft.com/en-us/library/Bb897402.aspx
3.http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/

5.2.1 Hybrid Architecture Benefits

The hybrid architecture leverages the flexibility of cloud services discussed in section 5.1, while benefiting from security enhancements by using on-premises services. First, we made the architectural decision to use identity federation services that are realized through AD FS and Microsoft's AD Authentication Library (ADAL) service. This build leverages federation when the device owner is required to authenticate to Intune and Office 365 cloud services. This allows an organization to act as an identity provider - device owner passwords are shared only with on premises systems and never with third-party cloud services.

We also made the architectural decision in this build to use a WAP. The WAP serves as a front end for requests to the on-premises AD FS system. This setup has the security benefit of adding a layer of defense by isolating front-end requests from the corresponding back-end requests to the protected federation service. This is important because the AD FS holds sensitive cryptographic keys such as the token-signing and service identity key. In this way, the AD FS system is protected within the enterprise network boundaries and not exposed to internet-facing networks.[1]

Functionally, the architecture provides the benefit of managing enterprise identities within the traditional workflow of an on-premises AD system. Many organizations utilize identity management systems that require on-premises AD services, but would also like to leverage cloud services without having two disparate identity systems. To solve this issue, we made the architectural decision to add an on-premises system dedicated to syncing identities between the on-premises AD and the cloud-based Office 365 environment.

SCCM is another instance of how our hybrid architecture benefits from on-premises and cloud services. This build could leverage traditional workstation configuration capabilities while enjoying the benefits of using a cloud MDM service. This is possible because our on-premises SCCM system is integrated with the Intune cloud service. Therefore, administrators can continue their normal workflow from the SCCM console and have a complete picture of enterprise assets from a single view.

5.2.2 Hybrid Build Security Characteristics

The security characteristics of the hybrid build resemble closely the characteristics in section 5.1.2, Cloud Build Security Characteristics. The Outlook mobile application uses a TLS tunnel to communicate with the Office 365 email, calendaring, and contact services that live in the cloud. However, in the hybrid build, mobile traffic is directed through a proxy before communicating with internal enterprise services when communicating with the enterprise for authentication services. Additionally, on-premises systems communicate with Microsoft cloud services via a TLS tunnel. This includes the SCCM system and the AD Sync systems.

1.In-depth discussion of this topic can be found in Microsoft's whitepaper "Office 365 Single Sign-On with ADFS 2.0," https://www.microsoft.com/en-us/download/details.aspx?id=28971.

5.3 Security Characteristics and Capabilities

The security characteristics and capabilities presented in appendix C are founded on the principles identified in NIST SP 800-164 and NIST SP 800-124. Security characteristics are the goals we are trying to achieve, while security capabilities are the individual mechanism(s) to accomplish these goals. An ultimate goal would be to implement the identified characteristics and capabilities with verifiable integrity via continued assertions that the device has not been compromised. This would ensure that key firmware or operating system files have not been tampered with, that the device has not been rooted or jail broken, and that the device's security policies are verified as those being issued by the enterprise. Unfortunately, this is not possible using what is offered in today's mobile marketplace. Therefore, these characteristics and capabilities should be implemented at the lowest possible level; for instance, firmware is preferred to an application layer service.

The original problem definition document [1] defines a superset of security characteristics and capabilities. This project does not implement every item within that document. What we have achieved in the context of this project is detailed below in appendix C, along with implementation notes for the build. Finally, note that many of the terms used below are not standardized throughout industry. Therefore, the descriptions provided alongside the capabilities reflect our meaning in the context of this project.

5.3.1 Default Policies

Multiple standards espouse management policies that should be applied to user devices. Specifically, NIST SP 800-124 Revision 1 and the NIAP protection profile for MDMs suggest desirable features and functionality for an enterprise MDM policy. Table 5.1 shows the default policy used in this project and pushed to devices within this building block, fulfilling our goals of a reasonable balance between security and user functionality. Suggested policies such as turning off Bluetooth and Wi-Fi, while reducing the threat surface to which a mobile device is exposed, remove important functionality required by users. Some of these policies may be accomplished by the underlying mobile OS (e.g., Android, iOS, Windows Phone), while others require application-level features, and still others are accomplished via the MDM. Although the following policies were used for the building block, organizations need to perform their own assessments to understand the risks associated with their systems. Guidance for performing this assessment and selecting appropriate policies can be found within NIST 800-124 r1 [2].

264

Table 5.1 Default EMM Policy

NIST SP 800-124r1 EMM/MDM Policy	SCCM/Intune Capability	Note
Automatically monitor, detect, and report when policy violations occur, such as changes from the approved security configuration baseline, and automatically take action when possible and appropriate.	Reporting	Each configurable section in a compliance policy has the ability to set an event and warning level for non-compliance with a setting. Implementation creates an alert for administrators when the compliance for the baseline policy falls below 90%.
Limit or prevent access to enterprise services based on the mobile device's operating system version (including whether the device has been rooted/jailbroken), vendor/ brand, model, or mobile device management software client version (if applicable).	Conditional access	Conditional access is set through SCCM Exchange connector. Mobile users are not allowed to access enterprise email services until the target device is compliant (i.e., phone is encrypted and not rooted/jailbroken).
Strongly encrypt data communications between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of secure protocols and encryption.	Intune Company Portal client application and Apple MDM protocol	The Intune client application encrypts data over a TLS tunnel from the device to the Intune cloud service. For hybrid deployments, SCCM traffic is also encrypted.
Strongly encrypt stored data on built-in storage.	File encryption on mobile device Encrypt app data	Device encryption implementation varies among device manufacturers. "Encrypt app data" is a managed application policy applied to the Outlook app.
Wipe the device (to scrub its stored data) before reissuing it to another user, retiring the device, etc.	Retire/wipe	Administrators are able to wipe devices by selecting the device from the SCCM console.
Remotely wipe the device (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party	Retire/wipe	Administrators are able to selectively wipe devices by choosing the device from the SCCM console.
A device often can also be configured to wipe itself after a certain number of incorrect authentication attempts.	Number of failed logon attempts before device is wiped	The number of failed logon attempts is set to five.

Table 5.1 Default EMM Policy (Continued)

NIST SP 800-124r1 EMM/MDM Policy	SCCM/Intune Capability	Note
Require a device password/ passcode and/or other authentication (e.g., token-based authentication, network-based device authentication, domain authentication) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device).	Password complexity Require password	Mobile devices are required to have a complex password with a minimum length of eight characters.
If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device.	Passcode reset	
Have the device automatically lock itself after it is idle for a period (e.g., five minutes).	Idle time before mobile device is locked (minutes)	This policy is set to five minutes.
Under the direction of an administrator, remotely lock the device if it is suspected that the device has been left in an unlocked state in an unsecured location.	Remote lock	
Restrict the use of operating system and application synchronization services (e.g., local device synchronization, remote synchronization services and websites).	Allow Google account auto sync Allow backup to iCloud Allow document sync to iCloud Allow Photo Stream sync to iCloud	
Verify digital signatures on applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified.	N/A	This is accomplished at the OS level of iOS, Android, and Windows Phone 8.
Query the current version of the hardware model of the device.	Hardware inventory	SCCM collects various data on all devices including manufacturer, model, Unique Identifier (UDID), International Mobile Station Equipment Identity (IMEI), and storage capacity.

Table 5.1 Default EMM Policy (Continued)

NIST SP 800-124r1 EMM/MDM Policy	SCCM/Intune Capability	Note
Alert the administrator to security events.	Alerting	Implementation creates an alert for administrators when the compliance for the baseline policy falls below 90%.
Import keys/secrets into the secure key storage locations.	N/A	This is accomplished at the OS level of iOS, Android, and Windows Phone 8.

6 Outcome

This section discusses the building block from the perspective of the user and the system administrator. We define system administrator as a person within the organization who has elevated privileges on the management systems in the build.

6.1 The User's Experience

When users access enterprise services on their device, their devices will be enrolled into the control of an EMM. The EMM will provide access to email, contacts, and calendaring services via the Microsoft Outlook mobile application. Device enrollment is accomplished by downloading and installing the Microsoft Company Portal application, available in the iOS and Android application store. Windows Phone devices have some management capability built into the OS, but also require the Company Portal application to relay information to the enterprise. The Company Portal application can be downloaded directly onto the device from the Windows Application Store.

In general, the specific hardware of a mobile device will make little difference in how information is presented to the user. Accordingly, boot integrity has no impact on the workflow, unless a user needs the capability to modify the mobile OS (e.g., jailbreaking, rooting). Enrolling a mobile device into the EMM causes a number of policies to be applied to it. One of the items most affecting a user's experience is the case where a user does not have local authentication on the device, since the default EMM policies espoused within appendix C require authentication to the OS lockscreen. The exact complexity of the authentication solution (e.g., PIN, passcode, gesture) is subject to the needs of the enterprise.

The user's enrollment authentication experience remains largely the same between the cloud and hybrid builds, even though the hybrid build supports identity federation between the enterprise and Microsoft cloud services. The hybrid build leverages ADAL-based sign in - which uses a Security Assertion Markup Language (SAML) based AD FS identity provider. This allows the user to keep a familiar workflow with the added security benefit of keeping passwords within the enterprise boundary.

To receive the Lookout security services, users should download the Lookout application from their device's application store in one of two ways. First, during the EMM enrollment process, users are presented with a direct link to the device's application store in the Company Portal. Second, the user is sent an invitation to enroll with Lookout through email. There is no technical control in this build, however, to require the installation of the Lookout app in this build. Implementers of this build may wish to consider policy controls as a means to enforce the installation of the Lookout application.

To enroll into the Lookout service, a user will have to supply the application with his or her email address and a unique code received via email. The Lookout application generally only interacts with users if there is a security violation on the device.

Figure 6.1, figure 6.2, and figure 6.3 present the high-level workflow of device owner enrollment on the Android, iOS, and Windows Phone platforms, respectively.

Figure 6.1 Android Workflow

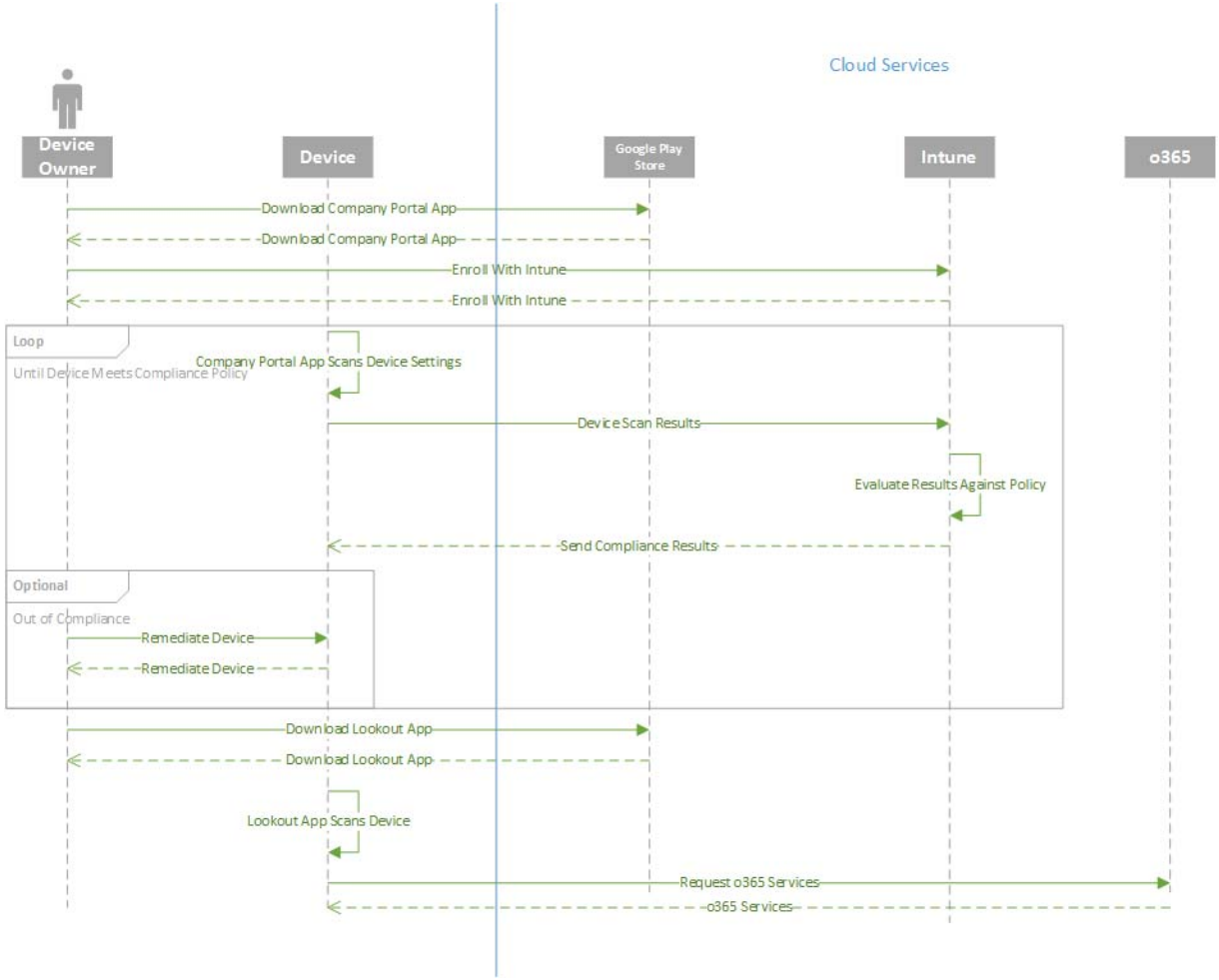
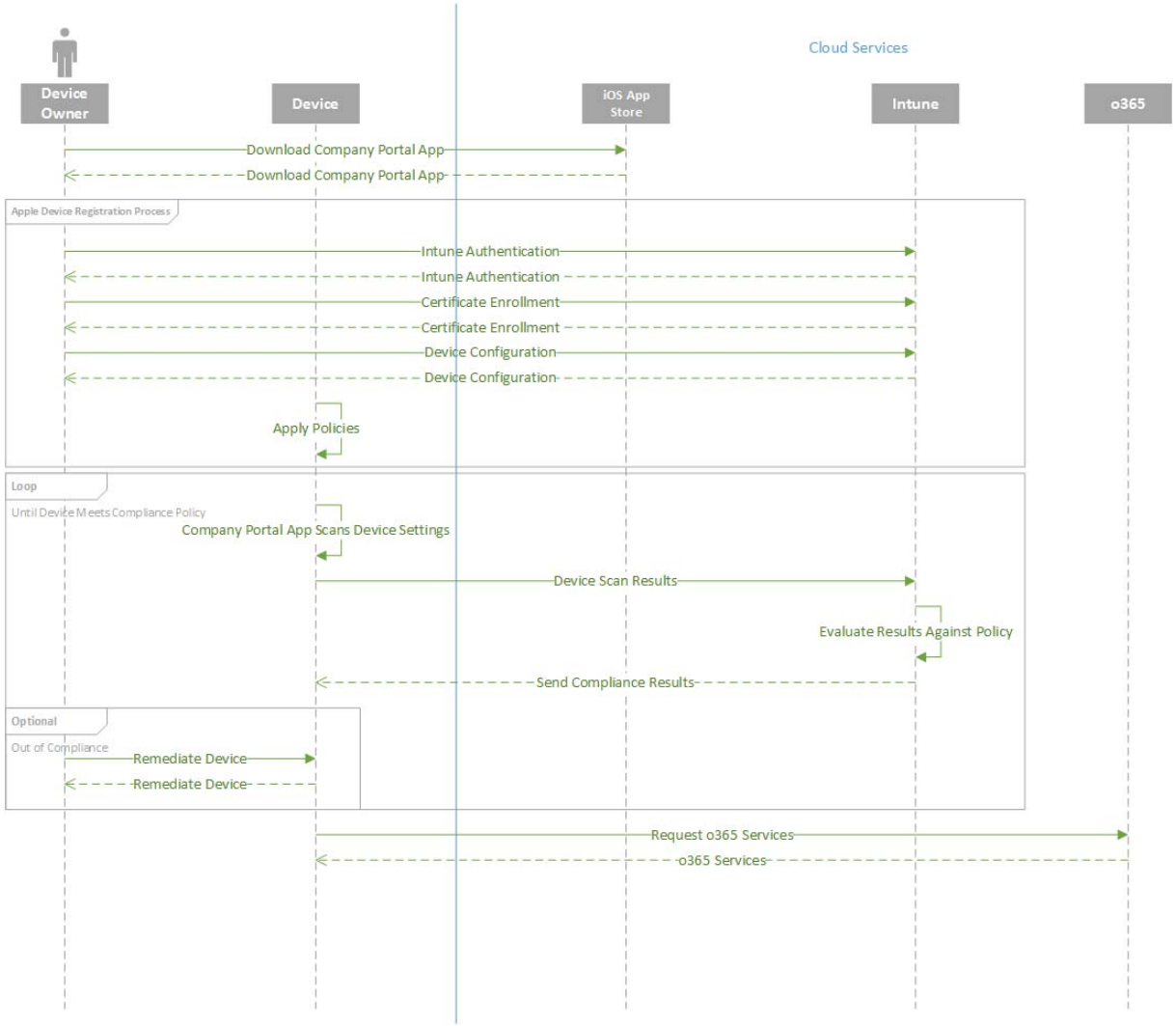
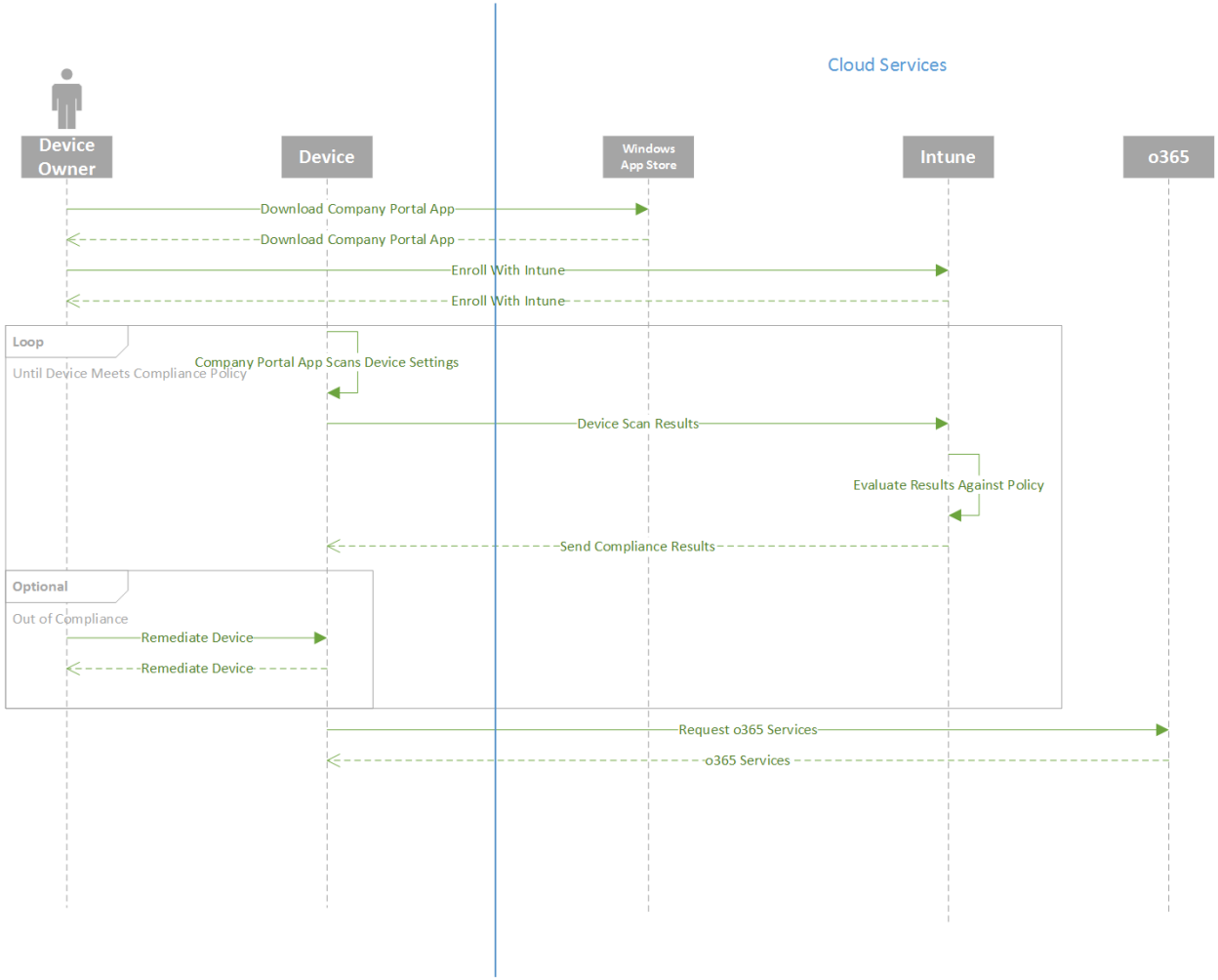


Figure 6.2 iOS Workflow



47

Figure 6.3 Windows Phone Workflow



48

6.2 The System Administrator's Experience

The experience of the system administrator will be different based on whether they are using the hybrid or cloud builds, mostly due to the type and granularity of policies available via the EMM interfaces. Installation, configuration, and deployment of the management systems are relatively simple if an organization decides to adopt the cloud-based EMM services, where setup can be accomplished in less than a few hours. The installation of the EMM and associated services on premises is significantly more complex, with installation time estimated in hours at least. Defining EMM policies within the web interface of the EMMs is relatively simple, as is distribution to mobile devices.

Provisioning and deprovisioning of email/contacts/calendaring services on mobile devices is an important capability of this build. The process by which provisioning occurs will differ for the system administrator in the cloud and hybrid scenarios. Since the MDM functions are embedded within Office 365, provisioning mobile devices is quite simple in the cloud scenario. While creating a new user within the Office 365 administrative console, the system administrator has the option to allow the user mobile access.

The complex nature of the hybrid architecture, however, necessitates a slightly more complex process. The high-level process is as follows:

1. A new enterprise user is created in the on-premises AD. The means by which this happens is outside of the scope of this building block; however, many organizations choose to use a third-party identity management system (IDMS).
2. The user is placed within a specific group within AD that is configured to sync identities. The user is synchronized by the on-premises Azure AD Sync system to the cloud Azure AD service.
3. The on-premises SCCM system detects the new user, who is automatically added to the Intune collection. A collection represents a group of users who have mobile devices to be managed.
4. The Windows Intune Connector extension installed on the SCCM system syncs the new user to the Intune cloud service.
5. The new user can now enroll in the Intune service using the Company Portal application.

Deprovisioning is a simple task for the system administrator in both the cloud and hybrid builds. In the cloud build, the user to be deprovisioned is disabled or deleted from the Office 365 administrative console. In the hybrid build, the user is removed from the Intune collection on the SCCM system. Implementers should note that deprovisioning actions may not be immediate. They will depend on the syncing periodicity configured in the Intune extension.

While Lookout services offer direct integration with selected EMM providers, this build did not use a compatible EMM. As a result, the system operator would not receive predefined alerts (e.g., malware on a device) through the SCCM workflow. The system operator must configure the Lookout administrative console to send email alerts to designated personnel when threats are present on user devices. In practice, the operator would receive an email with a warning of malware on a user's device. The operator would then find the user within SCCM and take appropriate action on the device. Further, in this build there is no technical mechanism to enforce the installation and use of Lookout technologies. An administrator could, however, periodically compare the list of enrolled users in Lookout and the EMM. Users who were absent

from the Lookout enrollment could be encouraged to download and install the application through an out-of-band means.

A step-by-step description of setup, installation, and configuration is available in *NIST SP 1800-4c*.

7 Evaluation

The purpose of the security characteristic evaluation is to understand the extent to which the building block meets its objective of demonstrating a method of protecting organizational data while permitting users the freedom to access and process data via mobile devices. In addition, it seeks to understand the security benefits and drawbacks of the reference design.

7.1 Assumptions and Limitations

This security characteristic evaluation has the following limitations:

- It is not a comprehensive test of all security components, nor is it a red team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that its devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

7.2 Testing

The evaluation included analysis of the building block to identify weaknesses and to discuss mitigations. The focus of this portion of the evaluation was hands-on testing of the laboratory build and examination of product manuals and documentation. Our objective was to evaluate the building block and not specific products; however, the presence of three primary OSs for mobile devices (Android, iOS, and Windows) made complete product independent hands-on testing unrealistic.

Table 7.1 describes the goals of each test case. A detailed test report can be found in NIST SP 1800-4c.

Table 7.1 Evaluation Objectives

Test ID	CSF Subcategory	Related NIST SP 800-53 Controls	Evaluation Objective
Data Protection			
1	PR.DS?1: Data-at-rest is protected	SC-28 Protection of Information at Rest	Data is accessible only to authorized users and services. Data is protected during storage and processing.
2	PR.DS-2: Data-in-transit is protected	SC-8 Transmission Confidentiality & Integrity SC-13 Cryptographic Protection	The confidentiality and integrity of information is protected while in transit (SC-8) using a cryptographic mechanism. A Federal Information Processing Standard (FIPS) 140-2 compliant mechanism is used to secure data in transit.
Data Isolation			
14	PR.DS-5: Protections against data leaks are implemented	SC-7 Boundary Protection	Monitor and control communications at the external boundary of the system and at key internal boundaries within the system

Table 7.1 Evaluation Objectives (Continued)

Test ID	CSF Subcategory	Related NIST SP 800-53 Controls	Evaluation Objective
Device Integrity			
16	PR.DS?6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7 Software, Firmware, and Information Integrity	Integrity mechanisms are running to check the integrity of software and information files.
17	DE.CM-4: Malicious code is detected	SI-3 Malicious Code Protection	Malicious code protection is installed on mobile devices. Anti-malware software (e.g., antivirus software) is installed.
18	DE.CM-5: Unauthorized mobile code is detected	SC-18 Mobile Code	Only mission appropriate content may be uploaded within the application. The application should employ functionality to restrict upload of file types to those expressly required for operations (e.g., TIFF, JPEG, and PDF).
Monitoring			
20	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8 Information System Component Inventory	Mobile devices are inventoried within the SCCM database.
21	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8 Information System Component Inventory	Software and licensing are inventoried within the SCCM database.
28	DE.AE-5: Incident alert thresholds are established	IR-5 Incident Monitoring	When alerts exceed the established threshold, the administrator is notified.
37	DE.CM-8: Vulnerability scans are performed	RA-5 Vulnerability Scanning	Scanning mechanisms are implemented and effective. Vulnerability scanners provide comprehensive coverage and employ best practices.
Identity and Authorization			
41	PR.AC-1: Identities and credentials are managed for authorized devices and users	IA Controls	The architecture accounts for multiple user roles with access privileges assigned to each role. Access controls are documented.
42	PR.AC-1	AC-2 Account Management; IA Controls	Only enrolled/managed devices can access email, contacts, and calendaring. Information is available only to authorized devices.

Table 7.1 Evaluation Objectives (Continued)

Test ID	CSF Subcategory	Related NIST SP 800-53 Controls	Evaluation Objective
Privacy Protection			
54	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	800-53 "-1" Controls	The system is capable of displaying a customized warning banner to users. The warning banner provides language that consents to lack of privacy by using the system.

7.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics it was intended to support. The CSF subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to that subcategory. The cited sections provide validation points that the building block would be expected to exhibit. Using the CSF subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the security characteristics identified in the building block.

The remainder of this subsection discusses how the reference architecture solution addresses the six desired security characteristics that are listed in table 4.1.

7.3.1 Data Protection

We chose to examine the capability of protecting data-at-rest and data-in-transit. The primary means used by this building block to accomplish data protection is encryption. Android, iOS and Windows Phone devices used as part of this build deployed device encryption. Android devices used dm-crypt, a crypto library that is FIPS 140 validated when used on Red Hat Enterprise Linux (RHEL) 6.2. The Android implementation of this has not been FIPS 140-2 validated, although it uses the same crypto library as the RHEL validation. For environments where FIPS 140-2 validation is necessary, organizations could consider using a 3rd-party data and application isolation solution, such as a secure container providing application level encryption.

Our Apple devices use Apple OS X CoreCrypto Kernel Module v5.0. As of this year (2015), it has received FIPS 140-2 level 1 validation on iOS 8.x devices. The Windows phones used in this exercise are FIPS 140-2 compliant. The Microsoft Kernel Mode Cryptographic Primitives Library has met FIPS 140-2 compliance at level 1 using a Qualcomm Snapdragon 800 system on a chip (SoC).

Finally, the Outlook application provides an additional level of encryption. Microsoft protects the Outlook data via AES-128 encryption in cipher block chaining (CBC) mode utilizing Android's

cryptography libraries. The iOS application-level encryption was not evaluated, as Microsoft indicated that information is encrypted via the OS cryptographic engine.

As an extra step, we used a packet capture tool to analyze the traffic being passed on our wireless access points. Our review of the captured traffic provided evidence to support that encryption is in use.

7.3.2 Data Isolation

When a device is utilized for organizational and personal activities, the ability to isolate data is essential. We inspected the sandboxing capability of devices and found that each of the OSs in use offers native isolation functions. Android, iOS, and Windows run applications in a sandbox that prevents a third-party application from accessing, gathering, or modifying information from other applications. While this is a valuable security feature, it does not replace the need to educate device users of the potential dangers of downloading unknown and untrusted applications.

7.3.3 Device Integrity

Each of the mobile platforms has integrity checking mechanisms. We examined the native file integrity mechanisms as well as malicious code protection. Each platform requires application authors to digitally sign applications before they are available for users. This demonstrates a developer's identity. Since Android devices may access applications from third-party providers, the application verification capability exists and should be enabled. The integrity checking mechanism does not ensure that the application itself is secure or free of malware. To protect devices from malware, the MDS building block specifies that antivirus software be installed on mobile devices. The build restricts the ability to download file types via email by enabling the file attachment filter in Office 365. We verified this by disallowing PDF file types. A user then attempted to send an email with a PDF file attached. The intended recipient was notified that an email addressed to them was blocked according to policy.

7.3.4 Monitoring

Our examination of security monitoring provided evidence of basic monitoring and scanning being performed. Devices enrolled in the MDM tool were displayed within the configuration management system console. This can be used for hardware inventory reporting as the MDM tools have customizable reports. We were only able to use software reporting to a limited degree. Intune provided software reporting only for applications published under the organization's application store. It did not monitor and inventory applications downloaded from other sources such as Google Play.

The MDM provides the capability to tailor compliance policy for devices. When a device exceeds the organizational-defined threshold for compliance, the administrator receives an alert showing which device is out of compliance. As an additional precaution, an organization may desire to restrict devices from downloading outside of its own organizational application store if the potential for unknown applications exceeds the organization's risk appetite.

Finally, the Lookout MTP service provides monitoring of enrolled devices for malware risks on Android devices. In this build, the administrator periodically reviewed the status of enrolled

devices in the enterprise through the MTP web console. More sophisticated notification systems, however, could be developed for larger deployments.

7.3.5 Identity and Authorization

Identity and authorization are integrated within the enterprise. We wanted to verify that only users authorized access via mobile devices were able to exercise that access. Since our lab was built as a Microsoft environment, access control was implemented via AD. Our test users were members of a domain users group synchronized through AD FS. We had users who were not members of the appropriate group attempt to access their email on an enrolled mobile device, and those attempts failed.

We also sought to verify device authorization. We wanted to ensure that only currently enrolled devices could access organizational resources. Our verification included devices never enrolled and devices previously enrolled.

Access attempts for devices not enrolled produced the following results:

- iOS redirected the user to the organization portal, then directed the user to enroll his or her device. Email was not accessible until the device was enrolled and compliant with the organization's mobile device policy.
- Android attempted to enroll the device with the active sync policy when not managed by Intune. Android would not retrieve email until the device was enrolled in SCCM and compliant with policy.
- When attempting to access Office 365 services from out-of-compliance devices, users could activate the email client on the device, but were unable to retrieve email.

7.3.6 Privacy Protection

NCCoE focuses on technical solutions. Privacy frequently focuses on management controls for enforcement; however, there are elements relevant to this building block. We wanted the ability to display a warning banner that a user must accept before gaining access, but we were unable to produce that capability. As an alternative, we produced a redirect sending users to an organizational website containing a sample privacy policy.

8 Future Build Considerations

As we expand this work to future builds and continue to enhance the build documented in this document, our objective is to solicit feedback from the user community toward prioritization of additional capabilities and solicit suggestions from the EMM vendor community on commercial products that provide those capabilities.

The following outlines some of the potential technical capabilities that may be added to this build:

- enhanced integration between Lookout MTP and Intune
- integration between Android for Work and Intune

In additional to potential updates and add-ons to this first build, there is potential for the development and implementation of new MDS architectures under this build. To explore these various architectures, the NCCoE would like to engage with any individual or company with commercially or publicly available technology relevant to MDS. The NCCoE published a Federal Register notice (https://www.federalregister.gov/articles/2015/08/14/2015-20040/national-cybersecurity-center-of-excellence-mobile-device-security-building-block) inviting parties to submit a letter of interest to express their desire and ability to contribute to this effort. Interested parties would be required to enter into a consortium Cooperative Research And Development Agreement (CRADA) partnership.

Some topics of interest for future builds include:

- baseband integrity
- containerization technology
- rogue base station detection
- enhanced identity services, such as two-factor authentication (2FA), derived personal identity verification (PIV) as demonstrated in NIST Interagency Report 8055, or the use of the FIDO Alliance's technology

All interested parties are encouraged to engage the NCCoE with additional ideas and system requirements by reaching out to mobile-nccoe@nist.gov.

Appendix A Acronyms

2FA	Two-Factor Authentication
AD	Active Directory
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
ADAL	Active Directory Authentication Library
BYOD	Bring Your Own Device
CAG	Consensus Audit Guidelines
CBC	Cipher Block Chaining
CIO	Chief Information Officer
COPE	Corporately Owned and Personally Enabled
COTS	Commercial Off-The-Shelf
CSD	Computer Security Division
CSF	Cybersecurity Framework
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GSA	General Services Administration
HTTP	Hypertext Transfer Protocol
IAD	Information Access Division
IEC	International Electrotechnical Commission
IDMS	Identity Management System
IMEI	International Mobile Station Equipment Identity
IPC	Inter-process Communication
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAM	Mobile Application Management

MDM	Mobile Device Management
MDS	Mobile Device Security
MMS	Multimedia Messaging Service
MTP	Mobile Threat Protection
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partnership
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OS	Operating System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RFTC	Request for Technical Capabilities
RMF	Risk Management Framework
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SANS	Sysadmin, Audit, Networking, and Security
SCCM	Systems Center Configuration Manager
SMS	Short Message Service
SoC	System on a Chip
SP	Special Publication
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDID	Unique Identifier
US-CERT	United States Computer Emergency Readiness Team
WAP	Web Application Proxy

Appendix B References

[1] NCCoE, *Mobile Device Security for Enterprises*, September 2014. http://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.pdf [accessed 8/23/15]

[2] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST SP 800-124 Revision 1, NIST, June 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [accessed 8/23/15].

[3] L. Chen, J. Franklin, and A. Regenscheid, *Guidelines on Hardware-Rooted Security in Mobile Devices (DRAFT)*, NIST SP 800-164 (DRAFT), NIST, October 2012. http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf [accessed 8/23/15].

[4] D. Cooper et. al., *BIOS Protection Guidelines*, NIST SP 800-147, NIST, April 2011. http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf [accessed 8/23/15].

[5] A. Regenscheid and K. Scarfone, *BIOS Integrity Measurement Guidelines (DRAFT)*, NIST SP 800-155 (DRAFT), NIST, December 2011. http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf [accessed 8/23/15].

[6] R. Kissel et. al., Guidelines for Media Sanitization, NIST SP 800-88 Revision 1, NIST, December 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf [accessed 8/23/15].

[7] S. Quirolgico et. al., *Vetting the Security of Mobile Applications*, NIST SP 800-163, NIST, January 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf [accessed 8/23/15].

[8] NSA, *Mobility Capability Package 2.3*, Enterprise Mobility Version 2.3, November 2013. https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_3.pdf [accessed 8/23/15].

[9] Department of Defense (DoD), *DoD Commercial Mobile Device Implementation Plan*, February 15, 2013. http://archive.defense.gov/news/DoDCMDImplementationPlan.pdf [accessed 9/3/15].

[10] CIO Council, Government Mobile and Wireless Security Baseline, May 23, 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf [accessed 8/23/15].

[11] CIO Council, *Government Mobile and Wireless Security Baseline*, May 23, 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf [accessed 8/23/15].

[12] NIAP, *Protection Profile for Mobile Device Management Version 2.0*, December 2014. https://www.niap-ccevs.org/pp/pp_mdm_v2.0.pdf [accessed 8/23/15].

[13] NIAP, *Protection Profile for Mobile Device Fundamentals Version 2.0*, September 2014. https://www.niap-ccevs.org/pp/pp_md_v2.0.pdf [accessed 8/23/15].

[14] NIAP, *Extended Package for Mobile Device Management Agents Version 2.0*, December 2014. https://www.niap-ccevs.org/pp/pp_mdm_agent_v2.0.pdf [accessed 8/23/15].

[15] Global Platform, *GlobalPlatform made simple guide: Secure Element.* http://www.globalplatform.org/mediaguideSE.asp [accessed 8/23/15].

[16] Global Platform, GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide. https://www.globalplatform.org/mediaguidetee.asp [accessed 8/23/15].

[17] Trusted Computing Group, *TPM Main Specification*. http://www.trustedcomputinggroup.org/resources/tpm_main_specification [accessed 8/23/15].

[18] The White House, *Bring Your Own Device - A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*, August 23, 2012. https://www.whitehouse.gov/digitalgov/bring-your-own-device [accessed 8/23/15].

[19] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, NIST, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf [accessed 8/27/15].

[20] National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-37 Revision 1, NIST, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [accessed 8/27/15].

[21] United States Computer Emergency Readiness Team, *Cyber Threats to Mobile Devices*, Technical Information Paper-TIP-10-105-01, US-CERT, April 2010. https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf [accessed 8/27/15].

[22] Delugré, Guillaume, *Reverse engineering a Qualcomm baseband*, Sogeti / ESEC R&D, 2011. https://events.ccc.de/congress/2011/Fahrplan/attachments/2022_11-ccc-qcombbdbg.pdf [accessed 8/27/15].

[23] United States Computer Emergency Readiness Team, *A Glossary of Common Cybersecurity Terminology*, 15. https://niccs.us-cert.gov/glossary [accessed 8/28/15].

[24] National Institute of Standards and Technology, *National Vulnerability Database*, 2015. http://nvd.nist.gov [accessed 9/2/2015].

[25] L. Badger et. al., *Cloud Computing Synopsis and Recommendations*, NIST SP 800-146, NIST, May 2012. http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf [accessed 9/2/15].

[26] Microsoft, *Protect data using mobile application management policies with Microsoft Intune*, Microsoft Technet, August 13, 2015.https://technet.microsoft.com/en-us/library/dn878026.aspx [accessed 9/2/15]

[27] Microsoft, *Windows Phone 8.1 Security Overview*, Windows Phone, April 2014. http://download.microsoft.com/download/B/9/A/B9A00269-28D5-4ACA-9E8E-E2E722B35A7D/Windows-Phone-8-1-Security-Overview.pdf [accessed 9/2/15].

[28] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Security*, Version 1.0, February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 9/9/15].

[29] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [accessed 9/9/15].

[30] International Organization for Standardization and International Electrotechnical Commission, Information technology - Security techniques - Code of practice for information security management., ISO/IEC 27002, 2013.

[31] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense*, Version 5.0, 2013. https://www.sans.org/media/critical-security-controls/CSC-5.pdf [accessed 9/9/15].

[32] Google, *Protect against harmful apps*. https://support.google.com/accounts/answer/2812853?hl=en [accessed 10/20/15]

[33] Lookout, *Change to sideloading apps in iOS 9 is a security win*. https://blog.lookout.com/blog/2015/09/10/ios-9-sideloading/ [accessed 10/20/15]

[34] Microsoft, *Try it out: restrict Windows Phone 8.1 apps*. https://technet.microsoft.com/en-us/windows/dn771706.aspx [accessed 10/20/15]

Appendix C Security Characteristics and Capabilities

Table C.1 Security Characteristics and Capabilities

Security Characteristic	Security Capability and Capability Description	Implementation Note
Data Protection	**Device encryption**: cryptographic protection of all or portions of a device's data storage locations - primarily flash memory locations	OS-level capability provided by each mobile OS
	Trusted key storage: protected locations in software, firmware or hardware in which long-term cryptographic keys can be held	**Android**: Android keystore, but may be device specific due to individual implementations of hardware/firmware-backed storage (e.g., TI's M-Shield) **iOS**: provided by secure enclave **Windows Phone**: has a Trusted Platform Module (TPM) capable of trusted key storage [27]
	Hardware security modules: tamper-resistant hardware used to perform cryptographic operations and secure storage that may be removable or physically part of the device	**Android**: device specific due to individual implementations of hardware/firmware-backed storage **iOS**: provided by secure enclave **Windows Phone**: has a TPM capable of common cryptographic operations
	Remote wipe: renders access to enterprise data stored on the device infeasible, but may only wipe a portion of flash memory	**Android**: provided via Android Device Manager **iOS**: provided by iCloud **Windows Phone**: provided by windowsphone.com **Note**: Intune and Office 365 also offer device wiping capabilities
	Data in transit protection: Use of a VPN	Communication to cloud services are protected by TLS

Table C.1 Security Characteristics and Capabilities (Continued)

Security Characteristic	Security Capability and Capability Description	Implementation Note
Data Isolation	**Sandboxing**: OS or application-level mechanisms utilizing multiple protection, isolation, and integrity capabilities to achieve higher levels of overall isolation	OS-level capability provided by each mobile OS
	Memory isolation: processes should be unable to access or modify another process's memory	OS-level capability provided by each mobile OS
	Trusted execution: a process is created and runs in a trustworthy and isolated execution environment leveraging distinct memory spaces and controlled interfaces	OS-level capability provided by each mobile OS
	Device resource management: ability to enable/disable device peripherals	**Android**: provided by Microsoft Intune **iOS**: N/A **Windows Phone**: provided by Microsoft Intune **Note**: unavailable in Office 365 MDM
	Boot validation: validation that the device is in a known working state and unmodified at boot (e.g., Basic Input-Output System (BIOS) integrity checks)	**Android**: optional capability that is device specific. **iOS**: provided by Secure Boot Chain **Windows Phone**: provided by Secure Boot
	Application verification: ensures that applications being installed come from a valid source	OS-level capability provided by each mobile OS to verify the digital signature of applications **Android**: Lookout MTP scanning and Android Application Verification [32] **iOS**: Apps installed from outside the App Store must be explicitly trusted [33] **Windows Phone**: App restriction platform capability [34]
	Verified application and OS updates: ensure that OS updates being installed come from a valid source	OS-level capability provided by each mobile OS to verify the digital signature of applications

Table C.1 Security Characteristics and Capabilities (Continued)

Security Characteristic	Security Capability and Capability Description	Implementation Note
Monitoring	**Auditing and logging**: capture and store device and application information	**Intune**: accomplished via compliance policies **Office 365**: accomplished via compliance policies
	Compliance checks: provide information about whether a device has remained compliant with a mandated set of policies	**Intune**: accomplished via compliance policies **Office 365**: accomplished via compliance policies
	Asset management: identifies and tracks devices, components, software, and services residing on a network	Provided by SCCM for hybrid build and Office 365 for cloud build
	Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised	**Intune**: accomplished via compliance policies **Office 365**: accomplished via compliance policies **Mobile OS**: provided by Lookout
	Canned reports and ad hoc queries	Provided by SCCM and Lookout components
Identity & Authorization	**Local authentication of user to applications**	Application specific, provided by Outlook
	Local authentication of user to device	Provided by all mobile OSs
	Remote authentication of user	Outlook requires enterprise credentials
	Device provisioning and enrollment	Provided by Intune and Office 365 MDM features
Privacy	**Notifications provided to users about the privacy implications of certain device and application functionality**	Implemented via privacy policy presented to users