# **NIST SPECIAL PUBLICATION 1800-4C**

# Mobile Device Security

**Cloud and Hybrid Builds** 

Volume C: How-to Guides

### Joshua Franklin

National Institute of Standards and Technology Information Technology Laboratory

Kevin Bowler Christopher Brown Spike E. Dog Sallie Edwards Neil McNab Matthew Steele The MITRE Corporation McLean, VA

February 2019

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-4

The original draft of this publication is available free of charge from: <u>https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid</u>





### **DISCLAIMER**

Certain commercial entities, equipment, products, 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, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-4C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-4C, 109 pages, February 2019, CODEN: NSPUE2

## **FEEDBACK**

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at <u>mobile-nccoe@nist.gov</u>.

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

National Cybersecurity Center of Excellence National Institute of Standards and Technology 100 Bureau Drive Mailstop 2002 Gaithersburg, MD 20899 Email: <u>nccoe@nist.gov</u>

# NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

# 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 and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

# ABSTRACT

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**

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

# **ACKNOWLEDGMENTS**

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

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

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

Technology Partner/Collaborator	Build Involvement
<u>Intel</u>	Lenovo Miix 2.8 Mobile Device
<u>Lookout</u>	Enterprise Mobility Management Application
Microsoft	Microsoft Cloud Service, Company Portal, Intune, Office 365 Enterprise E3, Outlook & Community Portal Mobile

Technology Partner/Collaborator	Build Involvement
	Applications, System Center 2012 R2 Configuration Man- ager SP1, Windows Phone Operating System
<u>Symantec</u>	X.509 Certificate

# Contents

1	Intr	oduct	ion	1
	1.1	Practio	ce Guide Structure	1
	1.2	Build (	Overview	2
	1.3	Typog	raphic Conventions	2
2	Ηο	w-To: I	Build a Cloud-Based Solution to Mobile Device Security	4
	2.1	Cloud	Build Setup and Configuration	4
		2.1.1	Cloud Build Components	4
		2.1.2	Office 365 Setup	5
		2.1.3	Office 365 MDM Setup	14
3	Ηο	<mark>w-To:</mark> l	Build an On-Premises Solution for Mobile Device Security	.25
	3.1	Hybric	Build Setup and Configuration	25
	3.2	Hybrid	Detailed Architecture	25
		3.2.1	Hybrid Build Components	27
		3.2.2	Enterprise Network and Firewall	28
		3.2.3	Enterprise Software Components for Hybrid	31
		3.2.4	Cloud Services Instances	34
		3.2.5	Hybrid Integration	37
4	Ηο	w-To: l	Device Configuration	.84
	4.1	Device	e Enrollment with Office 365	84
		4.1.1	iOS	84
		4.1.2	Android	88
		4.1.3	Windows Phone 8.1	90
		4.1.4	Email Setup	94
		4.1.5	Lookout MTP Enrollment	.103

# **List of Figures**

Figure 2-1 Cloud Build Process	5
Figure 3-1 Hybrid Build Process	25
Figure 3-2 Detailed Architecture	26
Figure 3-3 Detailed Architecture with Network Addresses and Host Names	27
Figure 3-4 List of Configured Interfaces	28
Figure 3-5 WAN	29
Figure 3-6 WAN Firewall Rules	29
Figure 3-7 DMZ Firewall Rules	30
Figure 3-8 LAN Firewall Rules	30
Figure 3-9 Management Firewall Rules	31

# **List of Tables**

Table 1-1 Typographic Conventions	2
Table 2-1 Cloud Build Components	4
Table 3-1 Legend for Detailed Architecture Diagrams	26
Table 3-2 Hybrid Build Components	27
Table 3-3 On-Premise Components of the Hybrid Build	31

# **1** Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented the example solutions to the challenge of securing email, contacts, and calendaring in mobile devices. We cover all the products that we employed in this reference design. We do not recreate the product manufacturer's documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

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

### **1.1 Practice Guide Structure**

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates standards-based reference designs and provides users with the information they need to replicate this approach to mobile device security. This reference design is modular and can be deployed in whole or in part.

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
- NIST SP 1800-4C: How-To guides instructions for building the example solution (you are here)

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

**Business decision makers, including chief security and technology officers,** will be interested in the *Executive Summary* (NIST SP 1800-4A), which describes the following topics:

- challenges enterprises face in implementing and using mobile devices
- example solutions built at the NCCoE
- benefits of adopting the example solutions

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-4B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.3, Risk, which provides a description of the risk analysis we performed
- Section 3.4.4, Security Control Map, which 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 enterprise mobility management (EMM) 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 solutions. 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 mobile devices and the corresponding business processes. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices.

### **1.2 Build Overview**

The NCCoE constructed the Mobile Device Security building block by using a virtualized environment and a physical wireless access point. The servers hosted by the virtualized environment were built to satisfy the hardware specifications of the specific software components in a small test environment (hard drive capacity, memory, etc.). The wireless access point was configured to use a closed lab network rather than directly internet connected. The mobile devices used in the build were configured to use this access point to simulate usage outside the traditional corporate network boundaries. Readers of this guide should assess the hardware needs of their environment carefully before implementation. Further, this build requires internet accessibility for some of the on-premise components that connect to commercial cloud services. We recommend configuring your firewall or other equipment to allow only internet access from on-premise systems to a specific internet protocol (IP) space provided by your cloud provider.

Finally, this document makes heavy use of screenshots from cloud services set up through a web browser. The reader should be aware that the rapid development of cloud services may cause some differences in what is presented here with screenshots and what the implementer experiences. Refer to vendor documentation to address significant variations.

## **1.3 Typographic Conventions**

The following table presents typographic conventions used in this volume.

Table 1-1 Typographic Conventions

Typeface/ Symbol	Meaning	Example
Italics	File names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit.
Monospace	command-line input, on-screen computer output, sample code examples, status codes	mkdir
Monospace Bold	command-line user input con- trasted with computer output	service sshd start
<u>blue text</u>	link to other parts of the docu- ment, a web URL, or an email address	All publications from NIST's NCCoE are available at <u>https://nccoe.nist.gov</u> .

# 2 How-To: Build a Cloud-Based Solution to Mobile Device Security

This section of the practice guide contains detailed instructions for creating and configuring the cloud architecture depicted below. No software resources are necessary for this build because it is completely cloud based. The only hardware requirement is that the organization that implements this build uses mobile devices that are compatible with the cloud mobile device management (MDM). This building block chose to use mobile devices running iOS, Android, and Windows Phone — the top three operating systems in terms of market share [1].

This How-To guide details the creation, configuration, and enrollment aspects of each cloud service. Keep in mind, a prerequisite to the cloud is an internet domain name. If the implementer does not already have a domain name, one can be obtained from an accredited registrar [2]. You will need to be able to edit the resource records to prove ownership of the domain.

The implementer will also need access to an Apple developer account to generate a push notification certificate for iOS devices. A push certificate allows the Office 365 instance to send push notifications to enrolled devices. Refer to the Apple website for pricing information and more details regarding certificates [3].

Further, during the configuration of the Office 365 MDM, you will be prompted to allow or block devices from Office 365 that cannot be managed. This can occur when a user has a device with an unsupported operating system. Select Block during this step to enhance the security of Office 365 services.

Finally, we have chosen in this simple cloud build to leverage the MDM capabilities that are available within Office 365. This offers a more limited feature set than what is available through the Intune MDM service. Implementers looking for more capabilities should consider the Intune portion of the Hybrid How-To guide.

# 2.1 Cloud Build Setup and Configuration

### 2.1.1 Cloud Build Components

The following components are used for this building block:

Make	Model	Version	Quantity
Microsoft	Office 365 Tenant	Business Premium	1
Google	Nexus (Android)	6 (5.1)	1
Apple	iPhone (iOS)	6 (8.3)	1
Nokia	Lumia (Windows Phone)	830 (8.10.14219.341)	1
N/A	Public Domain Name	N/A	1

Table 2-1 Cloud Build Components

The cloud building block build process can be completed with the following high-level steps in Figure 2-1. The following sections in the How-To guide will focus on the final two steps.

Figure 2-1 Cloud Build Process



### 2.1.2 Office 365 Setup

Office 365 is the central piece to the functionality of the cloud building block. The only prerequisite to this step is a public domain name. Keep in mind these steps may change as this is a web-based procedure.

To start the process, use a web browser to access the following URL to start the process: <u>https://products.office.com/en-us/business/office-365-enterprise-e3-business-software</u>.

Office 365 Ent	erprise E3
Move your business ahead with the wide range of integrated collaboration with advanced compliance feature	ne latest full Office, plus a ation services coupled es and full IT power.
\$20.00 user/month annual commitment	Buy now

1. Choose a commitment level



Prove. You're. N	ot. A. Robot.
○ Send text message	
(+1) 2403146858 X	You can't use a VOIP phone for verification. Please use a mobile phone or a landline.
Call me	

Office 365 sign-in page https://portal.office.com

Your Office 365 user ID nmcnab@cmdsbb.onmicrosoft.com

Creating your account...



2. Fill in the requested information in the next several screens

Collaborate with Office Online						
Mail	Calendar	People	Newsfeed	OneDrive	Sites	Tasks
Delve	Word Online	Excel Online	P P PowerPoint Online	OneNote Online	Admin	

3. Choose Admin from the set of services

Office 365				🐴 🛱 ? 🔎
Office 365 admin center «				NCCoE (Edit)
Search users, adminitasks an 👂	Welcome to Office 365 Enterprise!			admin shortcuts
DASHB OARD	Watch the video to get an overview			Reset user passwords
SETUP	Set up your services			Add new users
USERS	Download the latest version of Office			Assign user licenses
COMPANY PROFILE	Get information on Yammer			Download software
CONTACTS				resources
SHARED MAILBOXES	Watch the video to get started guickly			Working with domain names
MEETING ROOMS				Setting up mobile devices
GROUPS				Setting up user permissions in SharePoint
DOMAINS	Service overview			Office 365 Admin Help
DUBLIC WERSTE				Known issues
- multic	Service health	Current health		Information on Yammer
FORLING	1 issue	Exchange	Restoring service 👻	community
SERVICE SETTINGS	Service requests	I Identity Service	No issues	Ask a question in the forums
REPORTS	No oneo service requests	Lync	Service restored *	Check out our blog
SERVICE HEALTH	the open service requests	Office 365 Portal	Service restored 💌	Participate in the community
SUPPORT	Inactive email users	Office Subscription	No issues	
PURCHASE SERVICES	0 users have not signed in for 30 days or more.	Rights Management Service	No issues	
MESSAGE CENTER	Mail protection	SharaDhint	No issues	
TOOLS	1 messages received, 0 processed by filtering.	Manager Estamples	Malanuar	
# ADMIN		Tammer Enterprise	NO ISSUES	
Exchange	Message center	View details and history		
lync	2 new messages in the past 7 days			
Share Point.	Included services	Planned maintenance		
Compliance	included services	No planned maintenance scheduled.		
Azure AD		the president mentionence scheduber.		
Bing Places for Business				

4. In the next steps, we will configure the domain name with Office 365. Choose the **Domains** option

Ma	nage domains			
Add	a domain you already own t	o Office 365, or buy a new do	omain. What is a domain?	
	+ Add domain 🛒	Buy domain STATUS	ACTION	
•	+ Add domain DOMAIN NAME * cmdsbb.onmicrosoft. com (Default)	Buy domain STATUS Setup complete	ACTION No action required	cmdsbb.onmicro

### 5. Choose Add domain

Office 365	A & ? 🔍
Add a new domain in Office 365	What you need to know about * domains and DNS
Step 1 Verify domain•Step 2 Add users•Step 3 Set up domain•	Your domain name identifies your school or business on the internet. In the examples below, <b>yourcompany.com</b> is the domain name: you@ <b>yourcompany.com</b> http://www. <b>yourcompany.com</b> DNS (domain name system) works like an address book on the internet. When someone sends you email, DNS directs it to your mailbox. Up next, we'll help you set up your domain and update DNS records to work with Office 365. Learn more about domains and DNS
	Let's get started ⊖

6. Choose Let's get started



7. Enter your public domain name

Office 365	A 0 ? 🔍
Add a new domain in Office 365	Which domain do you want to * use?
Step 1 Verify domain Step 2 Add users	cmdsbb.org
Step 3 Set up domain	Next Don't have a domain? Buy one K Back

8. Choose Next

Show you own cmdsbb.org         Note: Only the domain owner can update DNS records, so we ask you to add this TXT record         Adding this TXT record won't affect your current email or other services.         To add the record:         • Go to your DNS host (Change)         • Copy the values from the following table and add them at your DNS host.         TXT records (Step-by-step instructions for adding a TXT record)         TXT name       TXT value
Note: Only the domain owner can update DNS records, so we ask you to add this TXT record         Adding this TXT record won't affect your current email or other services.         To add the record:         • Go to your DNS host (Change)         • Copy the values from the following table and add them at your DNS host.         TXT records (Step-by-step instructions for adding a TXT record)         TXT name       TXT value
To add the record:         • Go to your DNS host (Change)         • Copy the values from the following table and add them at your DNS host.         TXT records (Step-by-step instructions for adding a TXT record)         TXT name       TXT value
Go to your DNS host (Change)     Copy the values from the following table and add them at your DNS host.      TXT records (Step-by-step instructions for adding a TXT record)     TXT name     TXT value     TTL
Copy the values from the following table and add them at your DNS host.      TXT records (Step-by-step instructions for adding a TXT record)      TXT name     TXT value     TTL
TXT records (Step-by-step instructions for adding a TXT record)       TXT name     TXT value
TXT name TXT value TTL
@ MS=ms37771077 3600

9. At this point you need to add this information to the TXT record of your domain name. This functionality should be available from your registrar



10. Verify the Domain Name System (DNS) settings. The TXT record should match what was presented in the previous step. Note that it may take several minutes for the record to propagate to the Office 365 DNS servers



### 11. Choose Next

# Let's update your current Office 365 users to cmdsbb.org

Select the users you want to update from cmdsbb.onmicrosoft.com to cmdsbb.org.

After the update, these users will need to sign in to Office 365 using their new email addresses. Their passwords will stay the same.

7	Name	Current email address	Email address after update
2	Neil McNab (this is you)	nmcnab@cmdsbb.onmicrosoft.com	nmcnab@cmdsbb.org

# Update selected users ③

### 12. Choose Update selected users



13. Sign out to complete the change, and then sign in with your identification.

# Get ready to update DNS records to work with Office 365

Next, we'll determine which DNS records you need. You will have to sign into your DNS host to update these DNS Records.

What are DNS records?

# Next Θ

#### 14. Choose Next

# Do you want us to set up DNS records for Office 365 for you?

If you don't have a website published for www.cmdsbb.org, we can make things easy for you by setting up and managing the DNS records for Office 365.

- Yes, I want to transfer DNS management in the next step
- No, I have an existing website or prefer to manage my own DNS records

# Next Θ

15. Choose Next

# Which services do you want to use with cmdsbb.org?

Outlook for email, calendar, and contacts

Lync for instant messaging and online meetings

Next, we'll show you the DNS records you need to add at your DNS host. These records are requir for your Office 365 services to work on cmdsbb.org. How do DNS records work?

# Next Θ

#### 16. Choose Next

# Add the following DNS records for cmdsbb.org

Add the records at your DNS host (Change)

Priority	Host name	Points to address or value	TTL
0 @		cmdsbb-	
		org.mail.protection.outiook.com	
AME rec	ords (Step-by-st	tep instructions for adding a CNAME re	ecord)
AME rec lost nam	e over	tep instructions for adding a CNAME re Points to address or value	ecord) TTL 3600

<i>t</i> +	
v=spf1	
include:spf.protection.outlook.com	3600
-all	

17. Add the resource records presented in this step to your domain name. These are necessary for full functionality of the Office 365 tenant

### 2.1.3 Office 365 MDM Setup

In the next section, you will be guided through the device management setup through Office 365.

https://portal.office.com/Admin/Default.aspx#IntuneInventoryPage

1. Choose Get Started

https://portal.office.com/Adm	nin/Default.acps#IntunedriventoryPage	🔀 🕐 Y C 🔤 🔍 Seamh	☆ 白 ♣ ★ ♥ 🖬 😳 - 📓 🗄
III Office 365			¢ ? 🤇
Office 365 admin center «	CASHEGARD MOBILE DEVICES		NCCoE (Edit)
Search users, adminitasks an $\mathcal{P}$	Set up Mobile Device Management for Office	365	
SETUP USERS COMMANY PROTILE COMMANY PROTILE COMMANY GROUPS DOMMANY PRELICE VERSITE HELLING	Start using mobile device management (MDM) to manage and enhance the • View an investrory of all the devices that are another into MDM. • Orstart and manage device sourcing policies and access rules: • Perform common management tasks like wijning devices • View detailed devices and reports Learn more about Mobile Device Management for Office 365. At it a separat # We've setting things up for you. This may take a few hours, so check ba	confine service with its own privacy and security commitments is applied service with its own privacy and security commitments it again shortly	
EXTERNAL SHARING MORE E DEVICES			
SERVICE SETTINGS     REPORTS			
SUPPORT     PURCHASE SERVICES			
MESSAGE CENTER TOOLS			
# ADMIN Exchange			
Skype for Business SharePoint			
Rinn Paces for Rusiness ps://portal.office.com/Admin/Defaul	Larps#		Feedback

https://portal.office.com	/admin/de	efault.aspx≢Group	,Q ~ ≙ C [] port	al.office.com	× n *
Office 365					¢ ?
ffice 365 admin center «	0	DASHBOARD G	ROUPS		NCCoE (Edit)
DASHBOARD	Use si Use d Excha	ecurity groups to assign istribution lists in Exchain nge admin center.	permissions for SharePoint nge to manage email distrib	groups. sution. Set up distribution	n lists and other Exchange groups in the
▶ USERS		Name	Email address	Status	
COMPANY PROFILE IMPORT CONTACTS SHARED MAILBOXES MEETING ROOMS		NCCoE Operators	NCCoE@cmdsbb.org	In cloud	
DOMAINS PUBLIC WEBSITE BILLING EXTERNAL SHARING MOBILE DEVICES					
SERVICE SETTINGS REPORTS SERVICE HEALTH					Activate Windows Go to System in Control Panel to activate Windows.

 Next, a security group needs to be created in order to apply the policy to a group of users. Navigate to Office 365 > Admin Center > Groups > +

		- 0 ×
Office 365	m <sup>1</sup> admin/default.aspi <sup>s</sup> Group	¢ ?
Office 365 admin center    «	CASHEGARD GROUPS	NCCoE (Edit)
Search users, admin tasks an $  ho$		
	Create security group	nge groups in the
DASHBOARD	*Group name	
SETUP	Managed Users	
▶ USERS		
COMPANY PROFILE	Description	
IMPORT	Managed mobile device users.	
CONTACTS		
SHARED MAILBOXES		
MEETING ROOMS		
DOMAINS		
PUBUC WEBSITE		
▶ BILLING	Create Cancel	
EXTERNAL SHAJUNG		
MOBILE DEVICES		
SERVICE SETTINGS		Activate Windows
REPORTS		Go to System in Control Panel to activate Windows.
▶ SERVICE HEALTH	c	Feedback
		• 🖻 🖓 (b. 529 PM

3. Add a title and description for the group

- O Ittps://portal.office.co	m/admin/default.aspx#Group	(_  <b>0 ×</b> ∩ ★ 0
Office 365	-	Ø ? 🜔
©	Add members to the group Managed Users	×
Managed Users Security group AA ADO MEMBER	<ul> <li>✓ Add 5 members to Managed Users successfully</li> <li>✓ Matt Steele</li> <li>✓ Neil McNab</li> <li>✓ Chris Brown</li> <li>✓ Josh Franklin</li> <li>✓ Kevin Bowler</li> </ul>	
	Close	Activate Windows Go to System in Control Panel to activate Windows.
- 2 3		► P 💯 🕒 534 PM

### 4. Add members to the group to be managed

				_ 0
+ 🕘 🛁 https://na01b.com	mpliance.protection.outlook.com/ucc/?p=devic .O	👻 📾 😋 🕞 Mobile devi	ce managemen X	÷ 1
Office 365	Admin			¢ ?
Compliance Cent	er			
Home	Mobile device management			
Archiving	Create and apply device manage	ement policies to pro	otect your organization's d	ata Learn more
Device management	Examples of supported scenarios of contro OneDrive for Business app in iPhone. Some	lling access: access corpora e scenarios might work diffe	ite Exchange mail using native mail erently from your expectation.	client in Android; access documents usir
eDiscovery	Learn more about supported devices and s	cenarios		
Retention	Show list of managed devices			
mport	+ 🖉 🖮 😂			
Permissions	Name	Status	Modified on 👻	
	Baseline Policy for Mobile Devices	On	5/14/2015 12:	Name
				Baseline Policy for Mobile Devices
				Description
				Require a password, Manage Email p ofiles, disable camera.
				Settings
			Ad Go ac	Configure Solidoving settings on devi es. Block access and report violation if devices that have this policy applie of are not contoliant with these setting
		1 selected of 1 total		
- 占 🛛	📜 🖪 🌔 🎻 👘			► P 🐨 😘 538 Pi

5. Go to **Office 365 > Admin Center > Mobile Devices > Manage device security policies** to configure a device policy to apply to enrolled devices



### 6. Choose to Block unsupported devices

		_ 0 ×
🗲 🕘 ঝ https://na01b.compliar	New device security policy - Internet Explorer	⊕ ★ @
Image: Office 365     A       Compliance Center	https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqId=14: A New device security policy	¢?
Home Archiving	Enter a name and description Give this device policy a friendly name so you can easily find it again later.	ita Learn more
Device management	Default Configuration Policy X	,,
eDiscovery	Description	
Retention		
Import		
Permissions		
		Name ^
		Baseline Policy for Mobile Devices
		Description
		Require a password, Manage Email pr
		Settings
	A	Configure for a contract of the section of the sect

7. Set the name for the actual device policy



### 8. Set rules for the device policy



9. Set additional restrictions



### 10. Select whether to deploy the policy and to what group

and the second se		- D X
😑 🛞 ঝ https://na01b.comp	New device security policy - Internet Explorer	<b>∂</b> ★ (
III Office 365	Https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?regld=14.	ti ?
Compliance Center	New device security policy	
Home	Do you want to apply this policy now?	
Archiving	Select Group - Internet Explorer	ita Learn more
Device management	manage	client in Android; access documents using
eDiscovery	ALIAS * DISPLAY NAME	
Retention	Managed Users Managed Users	
Import		
Permissions		
		Name
	1 selected of 1 total	Baseline Policy for Mobile Devices
		Description
	add -> Managed Users(remove);	Require a password, Manage Email pr
	ok cancel	ofiles, disable camera.
		Settings
	vre in save uns poincy, our in work to be applied to	Configure following settings on devic es. Block access and report violations

### 11. Select the group created earlier to apply the policy

### 2.1.3.1 Configure Push Certificate for iOS Devices

As noted in the introduction to this section, an Apple push notification (APN) certificate is required for full functionality with Apple iOS devices. Only Apple can sign these certificates.



1. Set up APN in **Office 365 > Admin Center > MobileDevices > Manage Settings** 



2. Configure an APNs Certificate for iOS devices > Set up



3. **Download certificate signing request** (CSR). Once the CSR is generated, it can be submitted to Apple for signing. Use a browser to visit: <u>https://identity.apple.com/pushcert/</u>.

)@	//idmsa.	apple.com/IDMSW	ebAuth/login? 🔎 👻 👔	Apple Inc. [US]	🚺 por 🧭 A	🔍 × 🚺 inst 🚺	Set TN Ov	S int 🦪 Ap	
	Store	Mac	iPhone	Watch	iPad	iPod	iTunes	Support	۵
pp	le Push	Certific	ates Port	al					
2	sign in.								
1	Apple ID Forgot your Apple ID	07					-		-
1	Password								3
1	Forgot your password	0					(6)	P-	
				ante:		A	A.	11	-
							The	Lint	$\mathbf{X}$
								De la	
							H		7
									100
the A	pple Online Store (1-	800-MY-APPLID, vis	it an Apple Retail Store, o	r find a reseller.	Appl	le Info Site Map	Hot NewACTIV	ast Good/in Cleanue	r Us 🔰 🧉
right (	© 2015 Apple Inc. All	Erights reserved.	ferms of Use Privac	Policy			Go to	e Windows.	
									;
1	L 2							• 🖻 🕸	(b 11:24 5/19/

4. You will be prompted for your Apple Developer account credentials. Sign in



5. Once authenticated, choose Create a certificate. Review the terms and conditions screen

🖉 🖉 https://identity.apple.com/pushcert/ 🖉 - 🔒 Apple 1	nc. [US] C @ Apple Push Certificates Por × ① 값
Store Mac Bod Bhone Apple Push Certificates Portal	iPad iTunes Support Q
Create a New Push Certificate Upload your Certificate Signing Request signed by your third-party se vendor to create a new push certificate.	rver
Notes	
Vendor-Signed Certificate Signing Request C:Users'inmcnabiDeskto( Browse Carcet Users	
Shop the Apple Online Store (1-800-80'-APPLD, visit an Apple Retail Store, or find a reseller. Copyright & 2014 Apple Inc. All rights reserved. Terms of Use Privacy Policy	Apple Info   Site Map   Hot News   RSS Feeds   Contact Us   😝

6. When creating the certificate, you will be presented with a screen to submit your CSR. Use the **Browse** button to navigate to where you stored your CSR file and choose **Upload** 



 After the upload, refresh the page. You will be presented with a list of signed certificates. Choose the download option for your new certificate, which will allow you to save the signed certificate in privacy enhanced mail (PEM) format



8. Return to Office 365, and upload the signed APN certificate from Apple's developer portal

Office 365				φ ?
ffice 365 admin center «	DASHBOARD   MOBILE DE	VICES		NCCoE (Edit)
DOMAINS PUBLIC WEBSITE	Mobile Device Manager The following mobile devices have been your tenant. You can view device proper security policies.	ment for Office enrolled in Mabile Devic ties, access reports, wipe	365 e Management by users in devices and enforce device	Settings APNs Certificate for iOS devices expires
BILLING     EXTERNAL SHARING     MOBILE OFVICES	Manage device security policies and acc See device compliance report	ess rules		5/18/2016 Manage settings
SERVICE SETTINGS REPORTS SERVICE HEALTH	Select a view: All	OPERATING SYSTEM	OS VERSION	
SUPPORT PURCHASE SERVICES MESSAGE CENTER TOOLS ADMIN Exchange Skype for Business SharePoint Azure AD Bing Places for Business V	Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/1 Matt Steele - msteele_WindowsPho	iPhone Android WindowsPhone	8.3 5.1 8.10.14219.341	Full wipe Selective wipe Learn more about full vs. selective wipe. Status Device Model Activate Windows Generation in Control Panel to activate Windows. Platform Version Platform Version

9. Verify that the APN is working correctly. It should have an expiration date listed

# 3 How-To: Build an On-Premises Solution for Mobile Device Security

### 3.1 Hybrid Build Setup and Configuration

Figure 3-1 depicts the high-level procedures to reproduce the hybrid build used in this building block. First, the implementer must own an internet domain name or have permission to edit resource records within a domain. This is a prerequisite to integration with the cloud services used within this build. The next set of steps configure the on-premise components. The procedures assume that no on-premise components have been installed, however implementers may wish to skip to the configuration sections if these components are already in place. In general, this guide defers to vendor documentation for installation procedures. The final set of steps instantiate the cloud services and integrate them into the on-premise components.

Figure 3-1 Hybrid Build Process



An important prerequisite to using Active Directory Federation Services (ADFS) in this hybrid arrangement is a third-party public key certificate issued from a reputable certificate authority. In this build we used Symantec's Secure Site Pro service. You may also want to purchase a third-party certificate to secure the Transport Layer Security channel on the system that hosts the application proxy to avoid web browser warnings/errors when users authenticate to the enterprise. Please refer to TechNet articles [4] and [5] for specific requirements.

Finally, there are several cloud-based services that provide functionality similar to the one chosen in this build. We use Microsoft's Office 365 for email/calendaring/contacts management and Intune to manage mobile devices. The implementer should note that email/calendaring/contact and MDM from different vendors may not offer the same out-of-the-box integration as what we have chosen here. For example, we have set a compliance rule that forces the mobile device to be enrolled with the MDM before it is given access to email/calendaring/contacts.

# 3.2 Hybrid Detailed Architecture

The following architecture diagrams depict the final architecture of the hybrid build after implementing this guide. Figure 3-2 calls out the various protocols implemented among the on-premise, cloud, and mobile device components. Figure 3-3 is a similar view but details the network addressing and host names that were used during the build.





### Table 3-1 Legend for Detailed Architecture Diagrams

Acronym	Term
AD	Active Directory
ADDS	Active Directory Domain Service
ADFS	Active Directory Federation Services
DMZ	Demilitarized Zone
HTTPS	Hyper Text Transfer Protocol Secure
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MGMT	Management Network
TLS	Transport Layer Security
WAP	Wireless Access Point





## 3.2.1 Hybrid Build Components

The following components are used for this building block:

Table 3-2 Hybrid Build Components

Make	Model	Version	Quantity
Lookout Mobile Security	Lookout Security for Work Ap- plication	2.0.150	1
Lookout Mobile Security	Mobile Threat Protection		1
Microsoft	Office 365 Tenant	Business Premium	1
Lenovo	Miix (Windows)	2.8 (8.1)	1
Google	Nexus (Android)	6 (5.1)	1
Apple	iPhone (iOS)	6 (8.3)	1
Nokia	Lumia (Windows Phone)	830 (8.10.14219.341)	1
Microsoft	Windows Server	2012 R2	5
Open Source	pfSense		1
Microsoft	Windows	7	1

Make	Model	Version	Quantity
Microsoft	System Center Configuration Manager (SCCM)		1
Microsoft	AD DS		1
Microsoft	AD FS		1
Microsoft	AAD Sync		1
Microsoft	Web Application Proxy		1
Microsoft	Intune	N/A	1
Symantec	Public Certificates	N/A	
N/A	Public Domain Name	N/A	1

### 3.2.2 Enterprise Network and Firewall

The build uses pfSense for the organization router/firewall (see figure above). It is a combination router and firewall configured as a virtual device. This subsection describes the configuration used in the build and how to create it.

A single firewall configuration was chosen for simplicity and flexibility in a lab environment, but a dual firewall configuration could also be implemented. Only IPv4 is used and IPv6 is disabled for simplicity.

To install and configure pfSense, implementers should refer to pfSense documentation for installation and configuration instructions. To re-create the build's configuration, follow the instructions in the documentation and use the configuration files made available by pfSense (pfSense Configuration Files: Interfaces — *interfaces-config-pfSense.localdomain-20150402160851.xml;* NAT — *nat-config-pfSense.localdomain-20150402160838.xml;* Firewall — *filter-config-pfSense.localdomain-20150402160823.xml*;

The following screenshots show the final configuration of the pfSense device. Access pfSense through its web interface. The default screen includes a list of interfaces described as part of the architecture in the Hybrid Build Architecture section. The individual interfaces are described below with the firewall rules.

Figure 3-4 List of Configured Interfaces

Interfaces		
P3 WAN		1000baseT <full-duplex></full-duplex>
		10.33.1.105
CI LAN		1000baseT <full-duplex></full-duplex>
		192.168.1.1
PLUCHT	1	1000baseT <full-duplex></full-duplex>
<u>MGM1</u>		192.168.2.1
PI DMZ		1000baseT <full-duplex></full-duplex>
DMZ		192.168.3.1

The build network is configured to use network address translation (NAT). The following port forwarding is set up to allow communication from outside the lab into the build network.

#### Figure 3-5 WAN

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
ø	WAN	TCP	8	*	10.33.1.104	443 (HTTPS)	192.168.3.104	443 (HTTPS)	Microsoft ADFS
α	WAN	ТСР	*	*	10.33.1.104	49443	192.168.3.104	49443	Microsoft ADFS Smart Card

Several firewall rules are configured to control access through the subnetworks. The following screenshots show these rules for the wide-area network (WAN), demilitarized zone (DMZ), local area network (LAN), and management network (MGMT).

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	34
		IPv4 TCP	*	*	192.168.3.104	443 (HTTPS)	*	none		NAT Microsoft ADFS	
٥		IPv4 TCP	8	*	192.168.3.104	49443	*	none		NAT Microsoft ADFS Smart Card	
۵		IPv4 ICMP	WAN net	.*	*	*	*	none		Allow ICMP for Debugging	

Figure 3-6 WAN Firewall Rules

The WAN configuration information is specific to our Internet Service Provider (ISP). In this lab, we provided the 10.33.1.0/24 network from which to statically assign addresses. 10.33.1.105 is the pfSense device's IP address, and 10.33.1.104 is also assigned as a virtual IP address for the WAP service. Firewall rules are configured to allow internet access to the WAP in the DMZ in order for Microsoft's ADFS to function.
#### Figure 3-7 DMZ Firewall Rules

1	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	120
3		IPv4 TCP/UDP	192.168.3.104	8	192.168.1.10	53 (DNS)	*	none		Internal DNS Name Resolution	
3		IPv4 TCP/UDP	192.168.3.104	8	192.168.1.20	443 (HTTPS)	*	none		ADFS Sync through WAP	
3		IPv4 *	*	*	MGMT net	*	*	none		Block to MGMT	
3		IPv4 *	*	*	LAN net	*	*	none		Block to LAN	
2		IPv4 TCP/UDP	DMZ net	*	*	*	*	none		Default allow DMZ to any rule	

In pfSense our DMZ is assigned as DMZ (OPT2) using the network 192.168.3.0/24. It is not allowed to access the intranet or management networks, except for specific rules for DNS and ADFS access. 192.168.1.10 is the IP address of the Active Directory server. 192.168.1.20 is the IP address of the ADFS server.

9	w/	IN LAN	MGMT	4Z							
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	3
1		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	2
3		IPv4 *	8	8	MGMT net	*	*	none		Block to MGMT	3
		IPv4 TCP/UDP	LAN net	8	*	*	*	none		Default allow LAN to any rule	

Figure 3-8 LAN Firewall Rules

In pfSense our LAN is using the network 192.168.1.0/24. It is not allowed to access the MGMT network.

Figure	3-9	Management	<b>Firewall</b>	<b>Rules</b>
--------	-----	------------	-----------------	--------------

п	) Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	CXL+
•	IPv4 TCP	MGMT net	*	MGMT address	443 (HTTPS)	*	none		This pfSense Web Interface Anti-Lockout	
2	IPv4 TCP/UDP	MGMT net	8	*	*	*	none		Default Allow Any	

In pfSense our management network is assigned as MGMT (OPT1) using the network 192.168.2.0/24. It has access to all networks.

# 3.2.3 Enterprise Software Components for Hybrid

The following section describes installation of the on-premise components of the hybrid build. As noted previously, this guide provides references to the vendor's documentation for installation to better customize the component to the target environment. Alternatively, implementers may replicate this build exactly by using the following table, which maps each component to the exact system used in architecture diagram Figure 3-2, Detailed Architecture.

Component	Host Name	IP Address
Active Directory Domain Services	mds00	192.168.1.10
Active Directory Federation Services	mds-adfs	192.168.1.20
Active Directory Federation Services Proxy	wap	192.168.3.104
Systems Center Configuration Manager	mdssccm	192.168.1.102
Azure Active Directory Sync Services	mds-adsync	192.168.1.21

In order to increase security from the default server configuration, the Security Configuration Wizard (SCW) included with Windows Server 2012 R2 was used on each server after installation. These policies were saved as XML files and are available for download. They can be viewed, edited, and applied with the SCW tool.

# 3.2.3.1 Active Directory Domain Services

The Active Directory Domain Services (ADDS) instance used in the hybrid build was created by using basic configuration settings offered through the Add Roles and Features Wizard. The system was deployed as a new forest with a domain name of nccoe.local. Implementers of this guide who seek more

details of an ADDS installation can consult an Install Active Directory Domain Services [6] TechNet article. Alternatively, implementers may wish to use a lab environment for their development [7].

After installation, the implementer should create an organizational unit (OU) to hold users who are to be synced with the Office 365 tenant. Create test accounts in this OU of users that will represent individual device owners. Or, as mentioned previously, create users from a production environment.

The domain controller will find the user's account based upon the userPrincipalName in the certificate's Subject Alternative Name field. The original domain controller was set up with a domain of nccoe.local. However, a more likely scenario would have an organization create an instance under a well-known top-level domain. We have addressed this issue by adding a User Principal Name (UPN) for hmdsbb.org in the ADDS configuration. All users in this configuration are required to have a UPN of <user>@hmdsbb.org. Identity federation between Intune and on-premise ADFS will fail if the users do not have the appropriate UPN.

The procedures to configure a UPN suffix are as follows:

- 1. Launch Active Directory Domain and Trusts snap-in
- 2. Right-click on the top-level Active Directory Domains and Trusts
- 3. Select Properties
- 4. In UPN Suffixes tab add hmdsbb.org and ad.hmdsbb.org domain suffixes



# 3.2.3.2 Active Directory Federation Service

Readers of this guide should refer to Microsoft documentation for specific installation instructions for their environment. Consult the referenced articles as a starting point for installation [8], [9].

Implementers should note the requirement of a certificate issued from a certificate authority that is recognized/trusted by Microsoft. In this demonstration, the build team procured certificates from Symantec's Secure Site Pro Secure Sockets Layer (SSL) service. Ensure that the provider is able to populate the Subject Alternative Name extension of the certificates used in the implementation.

Screenshots below are of the certificates from Symantec used in the build.



Certificate		×							
General Details Certification Pa	th	_							
Show: <all></all>	•								
Field	Value								
Valid from	Wednesday, March 11, 2015								
Valid to	Monday, March 12, 2018 7:59								
Subject	sts.hmdsbb.org, National Cyb 😑								
Public key	RSA (2048 Bits)								
Subject Alternative Name	DNS Name=adfs.hmdsbb.org,								
Basic Constraints	Subject Type=End Entity, Pat								
Certificate Policies	[1]Certificate Policy:Policy Ide								
CRI Distribution Points	[1]CRI Distribution Point: Distr								
DNS Name =adts.hmdsbb.org DNS Name =netreprisergistration DNS Name =www.hmdsbb.org DNS Name =sts.hmdsbb.org	DNS Name=adfs.hmdsbb.org DNS Name=enterpriseregistration.hmdsbb.org DNS Name=www.hmdsbb.org DNS Name=sts.hmdsbb.org								
Learn more about <u>certificate deta</u>	Edit Properties								

# 3.2.3.3 Active Directory Federation Services Proxy

Refer to the articles referenced in the Active Directory Federation Service section for specific installation instructions.

# 3.2.3.4 Systems Center Configuration Manager

Readers of this guide should refer to Microsoft documentation for specific installation instructions for their environment. Consult the following Test Lab Guide as a starting point for installation [10].

# 3.2.3.5 Azure Active Directory Sync Services

Refer to the referenced article for Azure Active Directory Sync Tool installation procedures [11]. Default options were used for this build.

## 3.2.4 Cloud Services Instances

After the on-premise components have been installed, the cloud services must be created. This section walks the implementer through the basic steps of creating Office 365, Intune, and Lookout accounts.

## 3.2.4.1 Office 365 Setup

The setup of the Office 365 service is the same as what has been previously described for the cloud build in section 3.1. We replaced cmdsbb.org with hmdsbb.org for this build.

#### 3.2.4.2 Intune Setup

Use a browser to access the following URL to start the Intune creation process: <a href="http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/">http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/</a>



1. Choose Try Now

Sign up				Trial
				Microsoft Intune
If your company is a	already using Microsoft Online Serv	rices for service	s such as	100 User Licenses
Microsoft Office 36 more about why it i	5, we recommend that you use the s important to sign up with the sam	same user ID to te User ID. <mark>Sign</mark>	sign up. Learn in *Required	Microsoft Intune helps organization provide their employees with access
* Country or	Select			to corporate applications, data, an
region:	Can't be changed after signup. Why?	000		any device, while helping secure
<ul> <li>Organization</li> <li>Ianguage:</li> </ul>	English			corporate information.
* First name:				
* Last name:				
* Organization name:				
* Address 1:				
Address 2:				
· City:				
* State:	Alabama			
* ZIP or postal				
code:				
Fronte number.				
Email address:				
name:	onmicro	soft.com Che	ck availability	

#### 2. Sign up for a trial license when prompted

Microsoft Intune	
Check out	
Confirm order	
Microsoft Intune   30 day term	
100 user licenses	
Truner Court	
Try now Cancel	

## 3. Choose Try Now

Sign-up is complete, and you should be redirected to the Intune management console at <u>https://manage.microsoft.com</u>.

Note that the Silverlight 3.0 browser support is required to load the management console.



#### Important! Do not proceed any further with Intune if you want to manage devices via SCCM.

# 3.2.4.3 Lookout Setup

Contact the enterprise sales team at <a href="mailto:support@lookout.com">support@lookout.com</a> to create an account.

# 뎡 Lookout

We got a request to reset your account password. To do that just visit this link, which will be valid for 12 hours:

#### Password Reset

You will be able to update your account password from there. No changes will be made to your account until you visit the link. If you did not request this change then please disregard this message.

Sincerely, The Lookout Team

1. After your account has been created, the designated administrators will receive an email instructing them to reset their password. Click the link and reset the password

← → C 🔒	Lookout, Inc. [US] https://mtp.lookout.com/les	
Lookout	Mobile Threat Protection Dashboard	
	DEVICE DEPLOYMENT	DEPLOYMENT RISK
Deshboard	✓ 3 activated devices	0 high risk devices
Threats	G pending devices	📋 1 moderate risk devices
Devices	✗ 0 deactivated devices	0 low risk devices
Policy	Threat Trends Last 30 days * Risk: High Med E Low	
<b>L</b>	APPLICATION THREATS	FILE THREATS
-	20	20
?	18	18
Support	16	16
	14	14

2. Open the Lookout administrative console to access the Lookout administrator functions by using a browser and navigating to <a href="https://mtp.lookout.com/les">https://mtp.lookout.com/les</a>

# 3.2.5 Hybrid Integration

This section documents the integration of cloud and on-premise services.

## 3.2.5.1 Office 365 with Active Directory Federation Setup

In this step, an on-premise ADFS server is integrated with the Office 365 service. The purpose of this integration is to provide identity federation between Office 365 and enterprise authentication service. You should have previously added your public domain to Office 365 in the Office 365 Setup section. If not, follow the procedures from TechNet Magazine [12]. Detailed integration information can be found in the referenced TechNet article [9].

1. Connect ADFS with your Office 365 instance by issuing the following two commands. This step will automatically exchange the required metadata to implement federation with Office 365

Set-MsolAdfscontext -Computer <AD FS server FQDN>

Convert-MsolDomainToFederated -DomainName <domain name>

# 3.2.5.2 Azure Active Directory Sync Services

For this step, we configure synchronization of the organization's enterprise Active Directory with the Office 365 directory. This service will periodically sync identities — adding, deleting, or otherwise modifying from the on-premise Active Directory to the Azure Active Directory instance when this step is completed. This build accepted the default syncing schedule, but it may be tuned at a later time.

	Connectity Among AD
AD DS Credentials User Matching Optional Features Configure Finished	COTIFIECT TO AZUTE AD         Enter your Azure AD credentials:         Username:         addsync@hmdsbb.onmicrosoft.com         Password:         ••••••••••••••••••••••••••••••••••••
	Next

1. Launch the Sync Services Configuration Tool. Input the global administrator credentials for the Office 365 instance and click **Next** 

Microsoft Azure Active Direction	rectory Sync Services	_ ×
Azure AD Credentials AD DS Credentials User Matching Optional Features Configure Finished	Connect to AD DS   Iter the Active Directory Domain Services credentials for each forest:   Forest:   Iccoelocal   Username:   Iccoeloc_administrator   Add Forest	
	Previous	

2. Input the Forest name and credentials of the administrator. Click Add Forest

Microsoft Azure Active Dir	rectory Sync Services _ X
Azure AD Credentials AD DS Credentials User Matching Optional Features Configure Finished	Connect to AD DS Enter the Active Directory Domain Services credentials for each forest: Forest: Username: Password: Add Forest  ✓ NCCOELIOCAI
	Previous Activat Next Indows

#### 3. Click Next

🔷 Microsoft Azure Active Di	irectory Sync Services _ X
Azure AD Credentials AD DS Credentials	Uniquely identifying your users
Optional Features Configure Finished	Your users are only represented once across all forests.      Match using:     Mail attribute     ObjectSID and msExchangeMasterAccountSID attributes     SAMAccountName and MailNickName attributes     Your own attribute
	Matching with Azure AD sourceAnchor attribute: objectGUID * userPrincipalName attribute: userPrincipalName *
	These settings were previously configured and are displayed for informational purposes only.
	Previous Next

4. Accept the defaults for uniquely identifying your users. Click Next



5. Do not choose any of the optional features. Click Next

🔶 Microsoft Azure Active Di	rectory Sync Services		_ <b>×</b>
Azure AD Credentials AD DS Credentials User Matching Optional Features Configure Finished	Ready to configure We have gathered enough information to Item Indsbb.onmicrosoft.com - AAD NCCOE.local	Configure Azure AD Sync and will now of Action Connect Connect	reate a default configuration.
		Previous	Configure

6. Click Configure

Microsoft Azure Active Di	rectory Sync Services _ >
Azure AD Credentials AD DS Credentials User Matching	Finished Your Azure AD Sync default configuration has been created. If you need to customize which objects to synchronize, use the Synchronization Service Manager before starting synchronization.
Optional Features Configure Finished	Synchronize now
	Finish

#### 7. Choose to Synchronize now and click Finish

ile <u>T</u> ools <u>A</u> c	tions <u>H</u> elp				
Operations	Connector	ors 🦉 Metaverse Designer	( Metaverse Search		
onnectors					
Name	Туре		Description	State	Actions
NCCOE.local	Active	Directory Domain Services		Idle	Create
hmdsbb.onmicrosof	t.co Windo	ws Azure Active Directory (Micr		Idle	Properties
					🕲 Delete
					🗑 Configure Run Profiles
					🛱 Run
					Stop
					R Export Connector
					Import Connector
					B Undate Connector
					B Referch Scheme
					Conclusion Schema
					Search Connector space
Total number of Con	nectors: 2				
Profile Name: User	Name:		Partition		
CONTRACT OF MERICA			End Time:		Status:
Start Time:					
Start Time: Synchronization St	atistics		Connection Status		
Start Time: Synchronization St	atistics		Connection Status		
Start Time: Synchronization St	atistics		Synchronization Errors		
Start Time: Synchronization St	atistics		Synchronization Errors		
Start Time: Synchronization St	atistics	]	Synchronization Errors		
Start Time: Synchronization St	atistics		Synchronization Errors		
Start Time: Synchronization St	atistics		Synchronization Errors		
Start Time: Synchronization St	atistics		Synchronization Errors		
Synchronization S	atistics		Synchronization Errors		Activate Wind

8. If successful, the added connectors will be displayed in the Synchronization Service Manager

# 3.2.5.3 Sync Intune with Office 365 Exchange

The following steps will establish a back-end connection between the Intune and Office 365 instances, which were created in the Cloud Services Instances section. When this step is completed, Intune will have the ability to enforce conditional access policies on all enrolled mobile devices.



1. Open the Intune administrative console with a browser. Click ADMIN



- 2. Click Set Up Exchange Connection within the Microsoft Exchange section
- 3. Click Set Up Service to Service Connector

The configuration with Office 365 will occur in the background. No further actions are required.

#### 3.2.5.4 Manage Intune with SCCM

To allow the Intune tenant to be administered remotely, SCCM must be configured on the enterprise network. The following steps add test accounts to an SCCM user collection and syncs with the Intune tenant. While Intune will be available through the browser-based administrative console after this exercise, the account will be permanently configured to manage devices through SCCM.

#### 3.2.5.4.1 Configure Active Directory User Discovery

When these steps have been completed, the SCCM instance will be able to automatically discover Intune users by way of an Active Directory container.

1. Launch the Configuration Manager console. Navigate to System Center Configuration Manager /Site Database/Site Management/<site name>/Site Settings/Discovery Methods

- 2. Right-click Active Directory User Discovery, and then click Properties
- 3. On the General tab, click the New icon to specify a new Active Directory container
- 4. On the New Active Directory Container dialogue box, specify Local Domain

- ,	
NCCOE     AzureAD Synced Users	^
E Builtin	
Domain Controllers	
Enterprise Servers	≡
Foreign SecurityPrincipals	
LostAndFound     Managed Service Accounts	
E _ NTDS Quotas	
😟 🎦 Program Data	
🗄 🔛 System	V

5. Select the AzureAD Synced Users container

Active Directory Container	×
Specify an Active Directory container to search during the discovery process	s.
Location	
Specify a location for the Active Directory search. You can browse to a sing enter an LDAP query to find an Active Directory container within a particular can enter a Global Catalog (GC) query to find an Active Directory container domains.	le container and domain. Or, you within multiple
Path:	
LDAP://OU=AzureAD Synced Users,DC=NCCOE,DC=local	Browse
Search Options	
Select options to modify the search behavior.	
Recursively search Active Directory child containers	
Discover objects within Active Directory groups	
Active Directory Discovery Account	
The Active Directory Discovery Account must have Read permission to the	specified location.
Les the computer account of the site server	
O Specify an account:	
	Set 👻
ОК	Cancel
At the second	Albert Contraction of the

6. The path will reflect the container chosen in the previous step. Click **OK** 

Active Directory U	Jser Discove	ry Properties	; 🛛 🗙					
Seneral Polling Schedule Active Directory Attributes								
Active Directory User Discovery								
Configure the settings to find user accounts	Configure the settings to find user accounts in Active Directory Domain Services.							
Enable Active Directory User Discovery								
Active Directory <u>c</u> ontainers:			* 🛛 🗙					
Filter			2					
Distinguished Name	Recursive	Group	Account					
LDAP://OU=AzureAD Synced Users,D	Yes	Excluded	Site Server					
<	Ш		>					
	ОК	Cance	Activate					

7. Ensure Enable Active Directory User Discovery is selected. Click OK

Selected Object Folder Tools S	System C	enter 2012 R2 Configuration Manage	r (Connect	ed to ROC	- NCCOE HQ) - 8 ×
Home Site Close					^ 😢
Create Site Create Show Install System Server Secondary Site Status	ete Co Co	infigure Site • Client Installation Settings • Settings	aintenance Summarizers Filter Rules	Set Sect Scope Classi	urity Properties es ify Properties
← → ▼ 🙀 \ → Administration → Over	view 🕨	Hierarchy Configuration    Discovery Method	ds 🕨 ROC	2	• 2
Administration	ROC 6	items			
▲ Eff Overview	* Search	1			X Search Add Criteria -
<ul> <li>Hierarchy Configuration</li> </ul>	Icon	Name	Statur	Site	Description
<ul> <li>Methods</li> </ul>		Active Directory Forest Discovery	Disabled	ROC	Configures settings that Configuration Manager uses to
ROC	a 🕺	Active Directory Group Discovery	Disabled	ROC	Configures settings that Configuration Manager uses to
🛤 Boundaries	N.	Active Directory System Discovery	Disabled	ROC	Configures settings that Configuration Manager uses to
🔊 Boundary Groups	1	Active Directory User Discovery	Enabled	ROC	Configures settings that Configuration Manager uses to
Exchange Server Connectors		Heartbeat Discovery	Enabled	ROC	Configures interval for Configuration Manager clients to
🕞 Database Replication	1	Network Discovery	Disabled	ROC	Configures settings and polling intervals to discover rest
File Replication					
Active Directory Forests					
Cloud Services					
🖆 Windows Intune Subscriptions					
Cloud Distribution Points					
Extensions for Windows Intune	-				
ssets and Compliance					
🗃 Software Library					
Monitoring					A stimule MGs dame
C Administration					ACTIVATE WINDOWS Go to System in Control Panel to activate Windows
Death.	•				•
neady					

8. After configuration, the status of the Active Directory User Discovery will be Enabled

Home Collection Close	8 4 n	ldd Reso	Export Delete Dept	ploy Properties oyment Properties			^ @
Assets and Compliance   Assets and Compliance		All Use Search	rs 8 items Name NCCOE\bsisko (Benjamin Sisko NCCOE\bsiko (Benjamin Sisko NCCOE\bsiko (Benjamin Sisko NCCOE\bsiko (James T. Kirk) NCCOE\jciard (Jean-Luc Picar NCCOE\jciard (Jean-Luc Picar NCCOE\jciard (John Smith) NCCOE\mobrien (Miles O'Brier NCCOE\mobrien (Miles O'Brier NCCOE\pchekov (Pavel Chekov	Domain NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE	Resource Type User User User User User User User Use	X Search	Add Criteria *
Windows Firewall Policies  Assets and Compliance  Software Library  Monitoring  Administration		NCC Gene Na Do	OE\bsisko (Benjamin Sisko) eral Information me: NCCOE\ main or Workgroup: NCCOE	bsisko (Benjamin Sisk	o) /	Related Objects Primary Device Activate Windows So to System in Control activate Windows	• Panel to

9. Navigate to Users > All Users to view accounts synced from Active Directory

#### 3.2.5.4.2 Register SCCM with Intune

The following sequence of steps enrolls an SCCM instance with the Intune tenant. After this step you will no longer be able to create and deploy policies from the Intune web management portal.

 Start the Intune Subscription wizard by opening the Configuration Manager. In the Administration section, expand Cloud Services, and click Microsoft Intune Subscriptions. Click on the Home tab and then Add Microsoft Intune Subscription

8	Create Windows Intune Subscription Wizard
Introduction	
Introduction Subscription General Platforms Company Contact Informat Company Logo Summary Progress Completion	Getting started         This wizard configures the Windows intune subscription that lets you manage mobile devices by using Windows intune.         You will need to do the following in order to complete the wizard:         • yoing in with a Windows intune organizational account and password to complete the wizard. You can get a organizational account from the <u>Windows Intune Account Portal.</u> • Determine the user collection to enable users to enroll devices.         • Determine the devices you want to manage. To manage certain devices, you will need additional information.         • Windows : You will need to specify sideloading keys. Sideloading keys let you install apps that are not in the Windows Strue.         • Windows Phone & You must have a code signing certificate. The certificate will sign the company notal algo all other apps deployed by Configuration Manager.         • OS: You will need an Apple Push Notification Service (APNs) certificate.
	< <u>Previous</u> <u>Next</u> > <u>Summary</u> Cancel

#### 2. Click Next



3. Click the Sign In button



4. Sign in using an administrative user from the Intune tenant

1	Create Windows Intune Subscription Wizard	×
General		
Introduction Subscription	General Configuration	
Platforms Company Contact Informat	Specify the user collection whose members will be able to enroll their devices for management.	
Summary	Collection: All Users and User Groups Browse	
Progress Completion	Specify company details and the color scheme for the company portal. These device and portal settings will replace any values previously configured in Windows Intune. Leave the fields blank if you do not want to specify custom values.	
	Company name: NCCoE	
	URL to company privacy documentation:	
	Color scheme for company portal:	
	Specify the site code for device assignment.	
	Configuration Manager site code: ROC v	tus
< 111 >	< Previous Next > Summary Cancel	<del>ite</del> V <del>yste</del> m

5. Authorize a collection of users to enroll with Intune. Click Next

	Create Windows Intune Subscription Wizard
Platforms	
Introduction Subscription General Platforms Company Contact Informat Company Logo Summary Progress Completion	Specify the platforms that a user is able to enroll in Windows Intune
< III >	< Previous Next > Summary Cancel Gate System

6. You may choose to configure device types in this step. However, we chose to configure these in a later step. Click **Next** 

<u>ن</u>	Create Windows Intune Subscription Wizard	x
Company Cont	act Information	
Introduction Subscription General	Specify company contact information	
Platforms Company Contact Informat	The company name is displayed as the title of the Windows Intune company portal. The contact information and details are displayed to users in the Contact IT screen of the Windows Intune company portal.	
Company Logo Summary Progress Completion	IT department contact namg: IT department physe number: IT department email address: Support website URL (not displayed to user): Website name (displayed to user): Additional information:	] ] ]
< III >	< Previous Next > Summary Cancel	te W

7. Enter the contact information for your organization. This is optional. Click Next

8	Create Windows Intune Subscription Wizard	x
Company Logo		
Introduction Subscription General	Specify company logo	
Platforms Company Contact Informat	You can customize your company portal with your company logo.	
Company Logo	Include company logo	
Summary Progress Completion	Select a logo to use when the company portal background is white.	
	Show the company name next to company logo	
< III >	< Previous Next > Summary Cancel	<del>te</del> W

8. Submit an organizational logo, if desired. Click Next

<b>2</b>	Create Windows Intune Subscription Wizard	×
Summary		
Introduction Subscription General Platforms	Confirm the settings	
Company Contact Informat Company Logo	To complete the setup for mobile device management, you must add the Windows intune Connector site system role by using the Add Site System Roles wizard.	1.
Summary Progress Completion	Connection Information • Use Configuration Manager Administration Console to manage this subscription. This is a one time, one way setting. General Information • Collection name: All Users and User Groups • User devices will enroll using the following site code: ROC • Organization name: NCCoE • Privacy Link: • Theme: Blue Mobile device management • No platforms enabled Company Contact Information • IT department phone number: • IT department phone number: • IT department phone number: • Support website URL (not displayed to user): • Website name (displayed to user): • Mebsite nam	m l
7	To change these settings, click Previous. To apply the settings, click Next.	ivate V

9. Review the settings and click Next



10. Close the wizard after the configuration completes. A green check mark indicates success for that task

Microsoft Intur	ne	
DASHBOARD GROUPS ALERTS APPS	Administration Overview Alerts and Notifications Alert Types Recipients Notification Rules Administrator Management Service Administrators Tenant Administrators Device Enrollment Managers Client Software Download	Mobile Device Management Mobile Device Management Authority Set to Configuration Manager
	Storage Use Mobile Device Management Company Portal	

11. The Intune administrative console reflects SCCM management after configuration has been completed

#### 3.2.5.4.3 Configure Push Certificate for iOS Devices

A push notification certificate is required for full functionality with Apple iOS devices. Only Apple can sign these certificates. Once the CSR is generated, it can be submitted to Apple for signing. The following procedure shows how to create the CSR within SCCM.

System Center 2012 R2 Configuration Manager (C	Connected to ROC - NCCOE HQ)	- 8 ×
Home		^ <b>(</b>
Add Windows Intune Subscription Create APNs Certificate request Create	ved ches - arch	
← → ▼ 🗹 \ → Administration → Overview → O	Cloud Services   Windows Intune Subscription	ons 🗾 😴 🌮
Administration	Windows Intune Subscriptions 1 items	
Pil Overview	Icon Name	Description
Hierarchy Configuration     Goud Services	Windows Intune Subscription	Subscription configuration required to connect to Windows Intune Se
🖆 Windows Intune Subscriptions		
Cloud Distribution Points		
Stressions for Windows Intune		
Site Configuration		
Sclient Settings		
Security		
Distribution Points		
Distribution Point Groups		
Migration		
Assets and Compliance	-	
Software Library		
Monitoring		
- montoning		Activate Windows
Administration		Go to System in Control Panel to activate Windows.
Ready	Laurenteen	

#### 1. Click Create APNs certificate request in the SCCM console

	Req	uest Apple Push Not	tification Service C	Certificate Signing	Request	x
Specify the fol (APNs) certific	der where you want ate. You will be prom	to save the downloaded Ce pted for your Windows Intu	rtificate Signing Request. ne organizational account	This is required to request to complete the downloa	st the Apple Push Notifi ad.	cation Service
Ele Name:						Browse
After you dow	nload the Certificat	e Signing Request, you mu	ast perform the following	steps to complete APNs	s setup:	
Step 1: Subm	it the request to the	Apple Push Certificate Por	rtal and download the AF	Ns certificate.		
Step 2: Uploa	d the APNs certifica	ate to Windows Intune through	ugh the Configuration Ma	anager console.		
					Download	Cancel

2. Save the CSR to local storage. You'll need this file for the next step

👌 https://	identity apple.com	'pushcert/		,Q + 🔒 Apple Ir	ic. [US] C 🥶	Apple Push Certifi	icates Por_ ×		
Ś	Store	Mac	iPhone	Watch	iPad	iPod	iTunes	Support	Q
Арр	le Push	Certific	ates Por	tal					
	Sign In.								
	nmcnab@mitre.o	g							
	Forgot your Apple II	57					6		3
	Forgot your passwor	47						RA	
				Sign II.			Y	THE	5
							H	10	
							H		2
Shop the J	Apple Online Store (1-	-800-MY-APPLD, via	iit an Apple Retail Store	, or find a reseller.	App	le Info 🔰 Site Ma	p Hot News	RSS Feeds Contact U	

3. Use a browser to visit <u>https://identity.apple.com/pushcert/</u>. You will be prompted for your Apple Developer account credentials.



4. Once authenticated, choose Create a certificate



5. Review the terms and conditions screen. You will be presented with a screen to submit your CSR. Use the **Browse...** button to navigate to where you stored your CSR file, and choose **Upload** 



 After the upload, refresh the page. You will be presented with a list of signed certificates. Choose the download option for your new certificate, which will allow you to save the signed certificate in PEM format



- Load the signed certificate into SCCM. Navigate to Administration > Overview > Cloud Services
   > Windows Intune Subscriptions. Right-click on Windows Intune Subscription and choose
   Properties
- 8. Check the box to enable iOS enrollment and use the **Browse...** button to import the PEM certificate you downloaded from Apple. Click **OK**

#### 3.2.5.4.4 Mobile Policy Creation

The following section depicts creation and deployment of a security policy to mobile devices in the building block test environment. The reader should note that not all options are available to every mobile operating system. Generally, iOS offers more fine-grain device management capabilities than Android; however, a KNOX-enabled Samsung Android device augments the base Android capabilities with additional management functions. More information regarding specific capabilities of supported mobile platforms can be found on TechNet [13].

 Launch the Create Configuration Item Wizard from the SCCM Configuration Manager. In the Assets and Compliance section, click Configuration Items in the Compliance Settings folder. Click Create Configuration Item from the toolbar

8	Create Configuration Item Wizard
General	
General Mobile Device Settings Password Device Security	Specify general information about this configuration item Configuration items define a configuration and associated validation criteria to be assessed for compliance on client devices.
Encryption Supported Platforms Platform Applicability Summary	Name: BaseConfig
Progress	Specify the type of configuration item that you want to create:
Completion	Mobile device v
	Assigned categories to improve searching and filtering:
	"Client"
	Activate Win
	Go to System in C
	< Previous Next > Summary Cancel

2. Give the configuration a name and specify in the drop-down that this configuration item is for mobile devices. Click **Categories...** 

Administrative categories:	
	Create
✓ Client	Rename
Line of Business	Delete
Server	

3. Select the **Client** category. Click **OK** 



4. Select Password, Device, Security, and Encryption setting groups. Click Next

8	Create Configuration Item Wizard			×
Password				
General Mobile Device Settings	Configure mobile device password settings			
Device	Require password settings on mobile devices:	Required		~
Encryption	Minimum password length (characters):		4	A V
Supported Platforms	Password expiration in days:		75	
Platform Applicability Summary	Number of passwords remembered:		1	A
Progress	✓ Number of failed logon attempts before device is wiped:		10	0
Completion	Idle time before mobile device is locked:	1 minute		~
	Password complexity:	Not Configu	red	~
	Password quality:	Not Config.	ired	~
	Send password recovery PIN to Exchange Server:	Not Configu	red	~
	Remediate noncompliant settings			
	Noncompliance seventy for reports:	Warning	Activat	~
			Go to Sys	tem in Co
	< Previous Next >	Summary	ct le c	ancel
III >				

5. Configure the password requirements based on your local requirements

8	Create Configuration Item Wiza	rd
Device		
General Mobile Device Settings Password	Configure device settings	
Device Security	Voice dialing:	Allowed 🗸
Encryption	Voice assistant:	Allowed V
Supported Platforms Platform Applicability	Voice assistant while locked:	Prohibited V
ummary	Screen capture:	Disabled v
rogress ompletion	Video chat client:	Disabled v
	Add game center friends:	Prohibited ~
	Multiplayer gaming:	Prohibited v
	Personal wallet software while locked:	Not Configured V
	Diagnostic data submission:	Enabled 🗸
	17 Development atting	
	Improve the settings	
	reports:	Activate Win
		Go to System in C
	< Previous	Next > Summary Cancel

6. Configure the device settings based on your local requirements

8	Create Configuration	Item Wizard		
Security				
General Mobile Device Settings Password	Configure mobile device security	settings		
Device	Unsigned file installation:		IT Administrator	
Encryption	Unsigned applications:		Prohibited	
Supported Platforms	SMS and MMS messaging:		Allowed	
Platform Applicability Summary	Removable storage:		Allowed	
Progress	Camera:		Prohibited	
Completion	Bluetooth:		Allowed	
	Windows RT VPN profile			
	Profile file:			Browse
	Profile name:		F	Remove
	Profile for all users:			
	Remediate noncompliant settings			
	Noncompliance severity for reports:		Warning Acti	vate Wir
			Go to	
	<	Previous Next >	Summary	Cancel

7. Configure the security settings based on your local requirements

k	Create Configuration	on Item Wizard		
Encryption				
Seneral Mobile Device Settings Password	Configure mobile device encryp	tion settings		
Device	Storage card encryption:		Off	v
Encryption	File encryption on mobile device:		On	v
Supported Platforms				
Platform Applicability	Require email signing:		No	v
ummary	Signing algorithm:		Default	~
Completion	Require email encontion:		No	
	Encryption algorithm:		Default	~
	T2 Devices and the second second			
	<ul> <li>Remediate noncompliant settings</li> </ul>		1	
	Noncompliance severity for reports:		Critical	•
	Noncompliance severity for reports:		Activa Go to S	ate Win ystem in 0

8. Configure the encryption settings based on your local requirements

8	Create Configuration Item Wizard	×
Supported Platfo	rms	
General Mobile Device Settings Password Device Security Encryption	Specify the supported platforms for this mobile device configuration item	
Supported Platforms Platform Applicability	<ul> <li>B- ☐ Windows Mobile</li> <li>B- ☐ Symbian Mobile</li> </ul>	
Summary		
Completion	B	
	Activate	Wind
	Go to System	n in Co
< m >	< Previous Next > Summary Cancel	elow

9. Select the mobile platforms you wish to support. Click Next

Platform Applica	Create C	Configuratio	n Item Wizard	
General Mobile Device Settings Password Device Security Encryption	Review platform excl The following settings are n be assessed for compliance Excluded settings:	usions for ot supported by on the unsupp	this configuration item all the supported platforms that you specified. These settings w orted platforms.	ill not
Supported Platforms Platform Applicability Summary Progress Completion	Name Add game center friends Bluetooth Camera Diagnodic data submission Encryption algorithm File encryption algorithm File encryption algorithm Require enail encryption Require enail encryption Require enail encryption Require password setting Screen capture Signing algorithm SMS and MKS messaging Storage card encryption Unsigned algolications Unsigned dile installation Video chat client	Categories Device Security Security Device Encryption Encryption Security Encryption Password Device Encryption Security Encryption Security Security Security Security Device Partice Security	Unsupported Platforms Al Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Al Windows Phone 8.0.Al Windows RT 8.1.Start Al Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.Al x54 Windows I Bl Windows Phone 8.0.Al Windows RT 8.1.	
		[	< Previous Next > Summary <sup>CI</sup>	m in C

# 10. Click Next

8	Create Configuration Item Wizard	×
Summary		
General Mobile Device Settings Password Device	The wizard will create a device configuration item with the following settings Details:	
Security Encryption Supported Platforms Platform Applicability Progress Completion	The wizard will create a device configuration item with the following settings: New device configuration item will be saved as: Name: BaseConfig Description: Categories: "Client" Categories: "Client" The following compliance rules are added: Require password settings on mobile devices Idel time before mobile device is toked Password septration in days Number of failed logon attempts before device is wiped Voice dailing Voice assistant Voile cassistant Voice assistant Vihile Locked Screen capture Voice dailing Diagnotic data submission Unsigned file installation Unsigned file installation Unsigned file installation Unsigned file installation Passe card encryption Removable storage Camera Bluetooth Screen enable device Screen enable dev	* E
	To change these settings, click Previous. To apply the settings, click Next. Activate V Go to System	Vind
< III >	< Previous Next > Summarg <sup>2</sup> Cl Varia Cance	iova.

11. Click Next

Completion	Create Configuration Item Wizard	
General Mobile Device Settings Password Device Security	The Create Configuration Item Wizard completed successfully      Details:	
Encryption Supported Platforms Platform Applicability jummary Progress Completion	<ul> <li>Success: The Create Configuration Item Wilzard completed successfully.</li> <li>New device configuration item will be saved as:         <ul> <li>Name: BaseConfig</li> <li>Description:</li> <li>Categories: "Client"</li> </ul> </li> <li>The following compliance rules are added:         <ul> <li>Require password settings on mobile devices</li> <li>Idle time before mobile devices</li> <li>BaseConfiguration in days</li> <li>Number to before mobile attempts before device is kicked</li> <li>Resumed explanation in days</li> <li>Vision assistant</li> <li>Vision assistant</li> <li>Vision assistant</li> <li>Scaren capture</li> <li>Vision substration</li> <li>Add game conter friends</li> <li>Multiplayer gaming</li> <li>Diagnostic fails submission</li> <li>Using the submission</li> <li>StMS and Mission</li> <li>Elsevorth</li> </ul> </li> </ul>	
	To exit the wizard, click Close. Activat Go to Sys	e Win tem in G

#### 12. Click Close

3	Folder Tool	s System (	Center 2	012 R2	Configura	tion Manag	er (Conne	cted
Hor	ne Folder							
Create Configuration I	In Baseline Configu Create	nport aration Data	Save Search Searc	d es •				
<b>←</b> → - [	🔄 🔪 🕨 Asse	ts and Comp	liance 🔸	Overvi	ew 🕨 Com	pliance Setting	ıs ► Conf	igurat
ssets and Com	pliance		<	Config	juration Basel	ines 0 items		
Softwa	- re Metering		*	Searc	h			
4 🧾 Compli	iance Settings			lcon	Name	^	Status	De
😭 Confi	iguration Items							
Conf	iguration Baseli	Create (	Configurati	on Base	line			
🔐 User	Data and Profil	Import (	Configurat	ion Data	1			
🖸 Remo	ote Connection	Folder	-			-		
- Com	tificate Profiles		1	-				
Em	ail Profiles							
VPI	N Profiles							
💽 Wi	Fi Profiles							
🛃 Com	pliance Policies							
🔺 📔 Cond	litional Access							
En Fyr	hanne Online							
Assets ar	nd Compliance							
Software	Library							

# 13. Click **Create Configuration Baseline** by right-clicking **Configuration Baseline** from the **Configuration Manager**

60

Name:	BaseLinePolicy				
Description:					^
					~
ompliance by this configu pecified are compliant. Of onfiguration data:	iration baseline. This conf ptional items are evaluate	iguration baseline d only if the releva	will be assessed as on nt application is pres	compliant if all the	t devices.
ompliance by this configu pecified are compliant. Of configuration data: Filter Name	ration baseline. This conf ptional items are evaluate	iguration baseline d only if the relevant Type	will be assessed as on application is pres	Revisi	e rems t devices.
ompliance by this configu pecified are compliant. Of onfiguration data: Filter Name BaseConfig	iration baseline. This conf ptional items are evaluate	iguration baseline : d only if the relevant Type General	will be assessed as o nt application is pres Purpose Required	Revisi	ion
ompliance by this configu pecified are compliant. Of onfiguration data: Filter Name BaseConfig	iration baseline. This conf ptional items are evaluate	iguration baseline : d only if the relevant Type General	will be assessed as o nt application is pres Purpose Required	Revisi Latest	ion
ompliance by this configu pecified are compliant. Of ionfiguration data: Filter Name BaseConfig	ration baseline. This conf ptional items are evaluate change Purpose	guration baseline - d only if the relevant Type General	will be assessed as o nt application is pres Purpose Required	Revisi     Revisi     Latest     Re	pion t emove

14. Name the baseline policy. Add the baseline configuration created in the previous steps and click **OK** 

Folder Tools System Center	2012 R	2 Configuration Manag	ger (Connec	ted to RO	C - NCCOE H	IQ)		- 8 ×
Home Folder								^ 🔞
Create Saved Searches Search	marization nition Baseline	n 👚 Enable 📄 Copy Isable 🖓 Refresh Export X Delete	Deploy Deployment	Move Move	Categorize Se	et Security Scopes ify Properti	<b>es</b>	
🗲  👻 🔛 🔪 • Assets and Compliance	Over	view 🔸 Compliance Settin	igs 🕨 Config	juration Base	elines			- 2
Assets and Compliance	< Confi	iguration Baselines 1 items						
🗒 Software Metering	Sear	ch			1		× P Search	Add Criteria *
<ul> <li>Compliance Settings</li> </ul>	lcon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	t Noncompl
📸 Configuration Items	<b>E</b>	BaseLinePolicy	Enabled	No	No	4/14/2015 1:33 PM	0	0
Configuration Baselines								
😭 User Data and Profiles								
😨 Remote Connection Profiles								
4 🛄 Company Resource Access								
Certificate Profiles								
Email Profiles	E							
VPN Profiles								

#### 3.2.5.4.5 Create Mobile Application Policy

This section describes how to roll out mobile application policy for the Outlook mobile application. The policy is automatically deployed when the device owner installs the application for the first time. First, the SCCM administrator will create a new application management policy, then associate an application

to the newly created policy. The following procedures feature the iOS platform, but the process is essentially the same for other platforms.

	Create Ap	plication Management Policy Wizard
General		
General Policy Type iOS Policy Summary Progress Completion	Specify general information of the settings to configure and Name: Description:	application management policy application management policy in your hierarchy. Managed Apps
		Activate Windows Go to System in Control Panel to < Previous Next > activate Windows Cancel

 To start the wizard, navigate to Under Software Library > Application Management > Application Management Policies: Create Policy in the SCCM console. Name the policy and click Next

1	Create Application Management Policy Wi	zard	L
iOS Policy			
eneral olicy Type iOS Policy	Application management policy for iOS		
immary ogress	App Web Content Restrict web content to display in the Managed Browser:	Yes	~
ompletion	Data Relocation Prevent iTunes and iCloud backups:	Yes	~
	Allow app to transfer data to other apps: Allow app to receive data from other apps:	Policy Managed Apps	~
	Prevent "Save As":	Yes	~
	Restrict cut, copy and paste with other apps: Access	Policy Managed Apps with P	'aste In   ❤
	Require simple PIN for access: Number of attempts before PIN reset:	Yes 5	*
	Require corporate credentials for access: Bequire device compliance with comprate policy for access:	No	~
	Recheck the access requirements after (minutes):	100	•
	Timeout: Offline grace period:	30 720	<>
	Additional Policies Encrypt app data:	When device is locked	*
		Activate Windo Go to System in Co	OWS ntrol Pane
	< Previous	Next > C Summary	Cancel

2. Choose the platform type and policy type. In this example, a policy is being deployed to an iOS application. Click **Next** 

<b>E</b>	Create Application Management Po	licy Wizard	x
iOS Policy			
General Policy Type iOS Policy Summary	Application management policy for iOS App Web Content Restrict web content to display in the Managed Browser;	Yes	~
Progress	Data Relocation		
completion	Prevent iTunes and iCloud backups:	Yes	~
	Allow app to transfer data to other apps:	Policy Managed Apps	~
	Allow app to receive data from other apps:	Any App	~
	Prevent "Save As":	Yes	~
	Restrict cut, copy and paste with other apps:	Policy Managed Apps with Paste	n v
	Access	0.70	
	Require simple PIN for access:	Yes	~
	Number of attempts before PIN reset:	5	~
	Require corporate credentials for access:	No	~
	Require device compliance with corporate policy for access:	Yes	~
	Recheck the access requirements after (minutes);		
	Timeout:	30	\$
	Offline grace period:	720	\$
	Additional Policies		
	Encrypt app data:	When device is locked	~
5-		Activate Windows Go to System in Contro	s I Panel to
	<	Previous Next > Summary Ca	ancel

3. Set the specifics of the policy as pictured. Click Next

<b>8</b>	Create Application Management Policy Wizard	×
Completion Completion General Policy Type iOS Policy Summary Progress Completion	Image: Create Application Management Policy Wizard completed successfully         Details:         Image: Success: The Create Application Management Policy Wizard completed successfully.         New application management policy will be saved as:         Name: Managed Apps         Description:         Policy will be saved with:         Policy Type: General         IOS policy settings will be saved with:	X
Completion	<ul> <li>Success: The Create Application Management Policy Wizard completed successfully.</li> <li>New application management policy will be saved as:         <ul> <li>Name: Managed Apps</li> <li>Description:</li> </ul> </li> <li>Policy will be saved with:             <ul> <li>Platform: IOS</li> <li>Policy Type: General</li> <li>IOS policy settings will be saved with:                 <ul> <li>Restrict web content: Yes</li> <li>Prevent backups: Yes</li> <li>Allow app to transfer data: Policy Managed Apps</li> <li>Allow app to transfer data: Any App</li> <li>Prevent Save as: Yes</li> <li>Restrict cut. copy and paste: Policy Managed Apps with Paste In</li> <li>Require PIN: Yes</li> <li>Number of attempts before PIN reset: 5</li> <li>Require compate credentials for access: No</li> <li>Require device compliance: Yes</li> <li>Recheck timeout: 30</li> <li>Recheck timeout: 20</li> <li>Encrypt app data: When device is locked</li> </ul> </li> </ul></li></ul>	
	To exit the wizard, click Close. Activate Windows Go to System in Control P < Previous Next > activate Windows Close	anel to

Upon successful creation, an overview is displayed. In order to use this policy, it needs to be matched with an application.

In the next section, the Outlook application is linked to the iOS application store through Company Portal and associated with the previously created application policy.
#### 3.2.5.4.6 Link an Application to a Previously Created Mobile Application Policy

1	Create Application Wizard
General	
General Import Information General Information Summary Progress Completion	Specify settings for this application Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.
	<ul> <li>Automatically detect information about this application from installation files:</li> </ul>
	Type: App Package for iOS from App Store V
	Location: https://tunes.apple.com/us/app/microsoft-outlook/id951937596?mt=8 Browse
	Example: http://itunes.apple.com/us/app/AppName/idoox?mt=xuo=x
	Go to System in Cont
< III >	< Previous Next > Summary to Cancebus

 Navigate to Software Library > Applications and Create Application. The admin will be prompted for a link to the application store application that they wish to link in the Location field. Search for the Outlook application using a search engine, and copy the link

1	Crea	ate Application Wizard	x
General Informat	tion		
General Import Information General Information	Specify information a	bout this application	
Summary	Name:	Outlook	
Progress Completion	Administrator comments:		
	Publisher:	Microsoft	
	Software version:		]
	Optional reference:		
	Administrative categories:	Select	
		Activate Wi	ndov
		Go to System in	Cont
< III >		Cancel	<u>NS</u>

2. Set the Name, Publisher, and Software version information for the application link as pictured

-	Create Application Wizard	x
Summary		
General Import Information General Information Summary Progress Completion	Details:         General Information:         Application name: Outlook         Publisher: Microsoft         Publisher: Microsoft         Software version:         Optional reference:         Categories:         Deployment type name: microsoft-outlook - App Package for iOS from App Store         Requirement rules:	
	To change these settings, click Previous. To apply the settings, click rvext.	the star
	Activate W Go to System i	in Cont
< III >	< Previous Next > Summarctivate Cancel	ows

3. Click **Next** to confirm the settings

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-4.

<b>+</b>	l	Deploy Software Wizard	x
General			
General Content Deployment Settings Scheduling User Experience	Specify general in Software:	Outlook Browse	
Alerts Application Managemen Summary Progress Completion	Collection: Use default distribut Automatically distribut Comments (optional):	All Users Browse  tion point groups associated to this collection  oute content for dependencies	_
			<
< III >		< Previous Next > SummaryG	Vindo 1 in Co

4. Important: Deploy the application to a user collection instead of a device collection

<b>*</b>	Deploy Software Wizard	×
Application Mar	nagement	
General Content Deployment Settings	Specify application management options	
Scheduling User Experience	Where required, select an application management policy	to apply to each deployment type in this deployment.
Application Management		
Summany	Deployment Type	General Policy
Progress	microsoft-outlook - App Package for IUS from	Managed Apps
Completion		
		Activate Windo
< III >	< Previous	Next > Summary G Scancel in Co

5. After setting the general settings for deploying the application, the admin will get a chance to link an application profile. Further configuration of the General Settings was not required for our purposes

#### 3.2.5.4.7 Configure SCCM with Lookout Application

This section describes integration of the Lookout mobile application with SCCM. When completed, the mobile device user will receive a link to download the Lookout application after enrollment with the MDM. The link URL will differ based on the mobile platform. Android users will be directed to the Google Play Store, iOS users to the App Store, and Windows Phone users to the Windows Phone store.

1	Create Application Wizard	x
General		
General Import Information Summary Progress Completion	Specify settings for this application Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.   Automatically detect information about this application from installation files:	
	Type:       App Package for Android on Google Play         Location:       ://play.google.com/store/apps/details?id=com lookout.enterprise&hl=ent         Example: https://play.google.com/store/apps/details?id=xxxx	
	Activate Windows Previous           System in Control Panel to System in Control	1

1. To start the wizard, navigate to **General.** Select **App Package for Android on Google Play** in the Type drop-down. Type

https://play.google.com/store/apps/details?id=com.lookout.enterprise&hl=en in the Location field.

1	Create Application Wizard	×
Import Informati	on	
General Import Information General Information Summary Progress Completion	View imported information         View imported information successfully imported from the App Package for Android on Google Play file.         Detaile         Application name: Application Name         Publisher:         Software version:         Deployment type name: Application Name - App Package for Android on Google Play	^ 
< m >	Activate Windows Previous       Kext > ctivate       Summary	ncel

2. Click Next

<b>t</b>	Cre	ate Application Wizard	x
General Informa	tion		
General Import Information General Information	Specify information a	about this application	
Summary	Name:	Lookout Security For Work	
Progress Completion	Administrator comments:		^ ~
	Publisher:	Lookout Mobile Security	
	Software version:		
	Optional reference:		
	Administrative categories:	Select.	
		¥	
		Activate	Windor
		Go to Syste	m in Cont
< III >		vertevious ivext > Summary in the Car	nobws

3. Use the suggested text in the Name and Publisher fields. Click Next

<b>t</b>	Create Application Wizard	x
Summary		
General Import Information General Information Summary Progress Completion	Details:         General Information:         Administrator comments:         Administrator contements:         Publisher: Lookout Mobile Security         Software version:         Optional reference:         Deployment type name: Application Name - App Package for Android on Google Play         Requirement rules:	
	<pre>Activate W Go to System </pre>	/indo
< III >	activate vento	

# 4. Click Next

-	Create Application Wizard	×
Completion Seneral Import Information General Information Summary Progress Completion	Create Application Wizard  The Create Application Wizard completed successfully  Details:  Success: General Information:  Application name: Lookout Security For Work Administrator comments:  Publisher: Lookout Mobile Security  Software version:	×
	<ul> <li>Software version:</li> <li>Optional reference:</li> <li>Success: Categories:</li> <li>Success: Deployment type name: Application Name - App Package for Android on Google Play</li> <li>Success: Requirement rules:</li> </ul>	
	To exit the wizard, click Close.	indo
< III >	< Previous Next > Summa@ctivate (Close)	in Cont

5. Click Close

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-4.

٠		Deploy Software Wizard	×
General			
General Content Deployment Settings Scheduling	Specify general	I information for this deployment Lookout Security For Work Browse	
Alerts Summary Progress Completion	Collection: Use default distri Automatically dis Comments (optional):	All Users Browse ibution point groups associated to this collection stribute content for dependencies t	
		< Previous Next > Summary 6 Square Without W	₩indo

6. Open the application deployment wizard. In the **Software** field, browse for the Lookout application. In the **Collection** field, browse for **All Users** 

		Deploy Software Wi	izard			
Content						
General	Specify the cor	tent destination				
Content						
Deployment Settings						
Scheduling	Distribution points or	distribution point groups that th	ne content has been distributed	to:		
User Experience						_
Alerts	Name	Туре				-
Summary		There are no	items to show in this view.			
Progress						
Completion						
	Additional distribution	points, distribution point group	os, and the distribution point grou	ups that are c	urrently	
	associated with cont	content to distribute content to.	S			
	Filter			2	Add	Ŧ
	Filter Name	Description	Associations		Add Remove	*
	Filter Name	Description There are no items to st	Associations how in this view.	] 9	Add Remove	<b>V</b>
	Filter Name	Description There are no items to sl	Associations how in this view.		Add Remove	<b>•</b>
	Filter Name	Description There are no items to sl	Associations how in this view.		Add Remove	×
	Filter Name	Description There are no items to sl	Associations how in this view.		Add Remove	<b>V</b>
	Filter Name	Description There are no items to sl	Associations how in this view.		Add	•
	Filter Name	Description There are no items to sh	Associations how in this view.		Add	
	Filter Name	Description There are no items to sl	Associations how in this view.		Add	•
	Filter Name	Description There are no items to sl	Associations how in this view.		Add Remove	• Ni

## 7. Click Next

•	Deploy Software Wizard	x
Deployment Set	ttings	
General Content Deployment Settings Scheduling User Experience Alerts Summary Progress Completion	Specify settings to control how this software is deployed     Action:   Install   Purpose:   Available     Require administrator approval if users request this application	
	Activate     Summary G Scalary     Summary     Summary	e Windo nceh in Cor Vindows

8. In the Action drop-down, choose Install. In the Purpose drop-down, choose Available. Click Next

٠	Deploy Software Wizard	:
Scheduling		
General Content Deployment Settings Scheduling User Experience Alerts Summary	Specify the schedule for this deployment This application will be available as soon as possible by default. If this application should be made available at a different time, change the availability time to the desired UTC time.	
Progress Completion	Ime based on:       UTC       v         Schedule the application to be available at:       7/29/2015       v       2:40 PM         7/29/2015       v       2:40 PM       v	
	< Previous Next > Summary Science Window	de Jor

#### 9. Click Next

4	Deploy Software Wizard		
User Experience			
General Content Deployment Settings Scheduling	Specify the user experience for the installation of this software on the selected devices		
User Experience	Specify user experience setting for this deployment		
Alerts	User notifications: Display in Software Center and show all notifications V		
Summary Progress Completion	When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:      Software Installation     System restart (if required to complete the installation) Write filter handling for Windows Embedded devices      Commit changes at deadline or during a maintenance window (requires restarts)     If this option is not selected, content will be applied on the overlay and committed later.		
	< Previous Next > Summary Concerning Sciences Mindows		

10. In the User notifications drop-down, choose Display in Software Center and show all notifications

	Deploy Software Wizard		
Alerts			
General Content Deployment Settings Scheduling User Experience Alerts	Specify Configuration Manager and Operations Manager alert options Configuration Manager generates alerts when this application is deployed. Threshold for successful deployment		
Summary Progress Completion	Create a deployment alert when the threshold is lower than the following: Percent success:          1		
	Create a deployment alert when the threshold is higher than the following: Percent failure:  Example Surteen Creater Operations Manager maintenance mode if you want Operations Manager to percente		
	Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.  Enable System Center Operations Manager maintenance mode  Generate System Center Operations Manager alert when a software installation fails		
	< Previous Next > Summary G Scancel	Vinde in Co	

#### 11. Click Next

÷	Deploy Software Wizard	x
Summary   General   Content   Deployment Settings   Scheduling   User Experience   Alerts   Summary   Progress   Completion	Deploy Software Wizard Confirm the settings for this new deployment Details: General Software: Lookout Security For Work Oblection: All Users (Member Count: 8) Use default distribution point groups associated to this collection: Disabled Automatically distribute content for dependencies: Enabled Deployment Settings	×
Completion	Deployment Settings Action: Install Purpose: Available Allow clients to use a metered Internet connection to download content: Disabled Application Settings (retrieved from application in software library) Application Name: Lookout Security For Work Application Name: Lookout Security For Work Application Version: Application Deployment Types: App Package for Android on Google Play Scheduling Time based on: UTC Available Time: As soon as possible Deadline Time: Disabled User Experience User notifications: Display in Software Center and show all notifications Ignore Maintenance Windows: Disabled System restart (if required to complete the installation): Disabled Commit changes at deadline or during a maintenance window (requires restarts): Enabled To change these settings, click Previous. To apply the settings, click Next.	4 HI
	<pre></pre>	e Windo Seh in Co lindows

12. Click Next

\$	Deploy Software Wizard	x
General Content Deployment Settings Scheduling	Deploy Software Wizard  The Deploy Software Wizard completed successfully  Details:	
User Experience Alerts Summary Progress Completion	<ul> <li>Success: General</li> <li>Software: Lookout Security For Work</li> <li>Collection: All Users (Member Court. 8)</li> <li>Use default distribution point groups associated to this collection: Disabled</li> <li>Automatically distribute content for dependencies: Enabled</li> <li>Success: Deployment Settings</li> <li>Action: Install</li> <li>Purpose: Available</li> <li>Allow clients to use a metered Internet connection to download content: Disabled</li> <li>Application Name: Lookout Security For Work</li> <li>Application Deployment Types: App Package for Android on Google Play</li> <li>Success: Scheduling</li> <li>Itime based on: UTC</li> <li>Deadline Time: As soon as possible</li> <li>Deadline Time: Disabled</li> </ul>	e Windo

13. Click Close

# 4 How-To: Device Configuration

The following section steps through the configuration of devices. This section is applicable to both the cloud and hybrid builds. Here, we feature enrollment and email configuration with iOS, Android, and Windows Phone operating systems.

# 4.1 Device Enrollment with Office 365

The following sections depict the enrollment process of an iOS and Android device to the Intune enterprise mobility management service. The reader should note that the Intune service will automatically redirect the user to the Intune tenant owner's authentication service based on the domain part presented in the user's email address. The authentication service must be accessible via the internet if users enroll remotely. Otherwise, an organization must make its authentication service available on a local network accessible by device users.

Instruct device owners to download the Company Portal application through the application distribution point of their platform to start the enrollment process. The URLs for iOS and Android devices are <a href="https://itunes.apple.com/us/app/microsoft-intune-company-portal/id719171358?mt=8">https://itunes.apple.com/us/app/microsoft-intune-company-portal/id719171358?mt=8</a> and <a href="https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal&hl=en">https://itunes.apple.com/us/app/microsoft-intune-company-portal/id719171358?mt=8</a> and <a href="https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal&hl=en">https://itunes.apple.com/us/app/microsoft-intune-company-portal/id719171358?mt=8</a> and <a href="https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal&hl=en">https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal&hl=en</a> respectively. This is not necessary for Windows Phone devices because MDM management through this service is native to the device.

# 4.1.1 iOS

Device enrollment for iOS devices is described in the following material.

<sub>No SIM</sub> ବ Cancel	8:57 AM	* 📥
Intune Com	pany Portal	
Sign in with your v	work or school accour	nt
someone@exam	nple.com	
Password		
Sign in Ca	ancel	
Can't access your ac	count?	
Your work or see this symbol Privacy & Cool	chool account can be used ol. © 2015 Microsoft Terms kies	anywhere you of use

1. Download the Company Portal application from the application store and log in using Office 365 credentials



2. The user will then be asked to enroll their device and accept the organization's policies



3. Before accepting the management profile, the user can see the specifics of the profile and certificates that are issued



4. Upon accepting the management profile, the device will be enrolled, and the user will receive this confirmation message



In order to gain full access to company resources, the user will need to check their device for compliance. This screen will pop up when the user taps on their device in Company Portal



5. The compliance checking process will take a couple of minutes, and the user can minimize the application during this process



6. Upon minimizing the Company Portal application during the compliance checking process, the user is presented with the password remediation process, alerting the user to change their passcode within the hour



7. After meeting compliance, the user's device should be listed in the Company Portal like the example above

# 4.1.2 Android

🖬 🛛 🔛 🕄 😭 🖬 1:00 PM		
🖉 Company Portal		
Enroll your device		
Enrolling this device will give you access to email and other company resources and gives your organization the ability to manage this device. Tap Next to begin device enrollment.		
More information about en	rolling your device	
Cancel	Next	

1. After launching the Company Portal, click Next



#### 2. Enter your email address

📟 🖬 🛛 😹 🛜 💯 💼 1:00 PM	🖬 🛛 😹 🕱 📶 💼 1:01 PM	🖬 🛛 😹 🛜 💯 💼 1:01 PM
🖉 Company Portal	🚈 Company Portal	🚝 Company Portal
HMDSBB Sign in with your organizational account jkirk@hmdsbb.org	0	Enrolling your device
1 2 3 4 5 6 7 8 9 0 q w e r t y u i o p a s d f g h j k l ↑ z x c v b n m ≪ Sym e g e englisht(US) . Go	Signing in	This may take a few minutes. You can continue to use your device while it is being enrolled to the Company Portal.

3. If implementing a hybrid architecture, you will be redirected to your enterprise login site to enter your password. Otherwise, enter password and click **Sign In.** The user will be notified when they are signing into the Company Portal and when their device is being enrolled



4. Click Activate to allow remote management of the device

# 4.1.3 Windows Phone 8.1

ବ <i>ଲ</i> ଫୁ	workplace		5:59
	Microsoft Intune		
	Sign in with your work or school account		
	msteele@cmdsbb.org		
	Keep me signed in	_	
	Sign in		

 First, the user must add a workplace to their device. To do so on Windows Phone 8 and 8.1 devices navigate to settings > system tab > workplace (WP8.1) or settings > system tab > company apps (WP8)

and we've found them! 5:59
WORKPLACE
Email address
msteele@cmdsbb.org
Server
manage.microsoft.com
sign in

2. The workplace application will attempt to connect to your company's management portal. We used the manage.microsoft.com portal

and we've found them! 5:59
WORKPLACE
Email address
msteele@cmdsbb.org
manage.microsoft.com
sign in

3. After connecting to your company's portal, the device should now be able to be managed by Office 365. To do this, download Company Portal from the App Store to finish enrolling the device and receive your organization's policies



4. Upon logging into Company Portal for the first time, the user will be notified that their device hasn't met compliance and that some resources will be restricted



5. After the user checks the compliance manually (less than five minutes), the user's device is fully enrolled and should have the appropriate policies deployed



6. The screenshot above displays the details and policy compliance status of how a compliant and fully enrolled device should look



7. Once compliance has been met, the user should be able to tap the activation link to activate their email access



8. The activation link will open a browser. Upon successful activation, the user should receive this page. At this point, the user should have full access to Exchange email/contacts/calendar

# 4.1.4 Email Setup

The following section steps through the setup of email clients on iOS, Android, and Windows Phone. For iOS and Android, we use the Outlook client from Microsoft in the App Store and Play Store. The native email capabilities are used with Windows Phone. Other third-party applications are available, but this guide makes no assumptions regarding the security of these applications.

Implementers may choose to have users configure an email client on their devices manually or create an SCCM profile, which automatically configures enrolled devices. At the time of writing this practice guide, only iOS and Microsoft mobile devices were supported. Consult SCCM documentation for the latest capabilities.

# 4.1.4.1 iOS



1. When the user first opens the settings application — before, during, or after the compliance check — they are prompted for their Office 365 password for the Exchange profile that is provisioned during the onboarding process. (This is a onetime occurrence)

SIM 🗢	10:13 AM	* 🗖
Mailboxes	Inbox	Edi
	Q Search	
Microsoft Out	look	10:13 AM >
Action required	to access your	organization's
This email was	automatically ge	enerated by
Microsoft Excha	ange. You are re	ceiving this m
	Updated Just Now	

2. The user will receive this email the first time they open their email client



3. To activate their email access, the user will have to tap the link to activate the email and check for compliance



4. After activating their email, the user will be presented with an enrollment activated confirmation page

# 4.1.4.2 Android



1. Open the Outlook application on your device



2. Choose Office 365



3. Log in with your enterprise credentials

2 🖬						0	💎 🕱 I	10:20	
HMDSBB									
Sign in with your organizational account									
jkirk@	)hmdsb	b.org							
	1								
Siç	jn in								
© 2013	Microsoft								
q 1	N <sup>2</sup> 6	3 1	4	5	/° ι	7	i <sup>®</sup> C	° p°	
а	S	d	f	g	h	j	k	Т	
<u>+</u>	z	х	С	v	b	n	m	⊠	
?123	,							€	
	$\nabla$			0					

4. Note that if you are using the hybrid build, a single sign-on workflow is initiated. The device owner will be redirected to their local sign-in service



5. If the device has not been enrolled with the MDM, a prompt is presented to do so



6. A device that is out of compliance with the MDM policy will not have access to Office 365 services. The device owner is forced to remediate the device



The device owner is granted access to Office 365 after the device complies with policy

# 4.1.4.3 Windows Phone 8.1



- To get full access to Exchange resources as well as email, use the built-in email client to add an Exchange account. In the email client, tap the three horizontal dots on the bottom right and tap add account to bring up the account select page. Or under settings > email+ accounts add the Office 365 Exchange account credentials
- 2. Log in using Office 365 credentials; the server information should auto-populate



3. Upon successfully syncing the Exchange account, an email explaining the enrollment process should be received requesting that the user enroll/check for compliance

#### 4.1.4.4 Windows 8.1

Email profiles for Windows Mobile 8.1 were configured using the following steps.

1. The user can add their account to the built-in email application by selecting **Exchange account** and adding their email@customdomain and password. The email application should be able to pull the settings




2. Upon connecting to their Exchange account, the user should receive an email asking them to activate their email by clicking the link to check compliance

## 4.1.5 Lookout MTP Enrollment

← → C 🔒	Lookout, Inc. [US] https://mtp.lookout.c	om/les/devices/enroll	
କ୍ଷ	🗋 Devices 💄 Enroll 🖂 I	nvites	
Lookout	Enroll Devices		
<b>7</b> Dashboard	To invite employees to activate Lookout for by commas or semicolons.	Work on the their mobile devi	ces, either import a .csv consisting of just or
	IMPORT EMAILS FROM A .CSV	or	Enter emails separated by comm
Threats			ADD ADDRESSES
9 Devices			

 Open the Lookout Mobile Threat Protection (MTP) administrative console with a browser. Navigate to <u>https://mtp.lookout.com/les/devices/enroll</u> and type the target user's email address into the provided web field

8		
Protect yourself from mobile threats		
NIST - National Institute of Standards and Technology has partnered with Lookout to offer the most advanced protection and security for your mobile devices.		
Please click the button below to download the Lookout app on your tablet or phone.		
Install Lookout for Work		
Just launch the app when you're ready to activate protection for your device. If you have any trouble, try using this code:		
Your privacy is as important to us as your security, click here to learn how we safeguard your personal data.		

2. The mobile device user will receive an email with an activation code that must be used to activate the application

## 4.1.5.1 Android



1. Find the MTP application from the Google Play Store by searching "lookout"



2. Select the Lookout Security for Work application



3. Enter the activation code retrieved from the enrollment email



4. Select **OK** after the activation code is validated



5. The application will proceed to scan the device.



6. The application notifies the user of any threats on the device

## Appendix A List of Acronyms

AD	Active Directory
ADDS	Active Directory Domain Service
ADFS	Active Directory Federation Services
APN	Apple Push Notification
BYOD	Bring Your Own Device
COPE	Corporately Owned, Personally Enabled
DMZ	Demilitarized Zone
DNS	Domain Name System
EMM	Enterprise Mobility Management
НТТР	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ISP	Internet Service Provider
LAN	Local Area Network
MDM	Mobile Device Management
MDS	Mobile Device Security
MGMT	Management Network
МТР	Mobile Threat Protection
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OU	Organizational Unit
PEM	Privacy Enhanced Mail
scw	Security Configuration Wizard

SP	Special Publication
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPN	User Principal Name
WAN	Wide Area Network
WAP	Wireless Access Point

## Appendix B References

- [1] International Data Corporation, *Android and iOS Squeeze the Competition*, Feb. 24, 2015. Available: <u>https://www.businesswire.com/news/home/20150224006498/en/Android-iOS-Squeeze-Competition-Swelling-96.3-Smartphone</u>.
- [2] Internet Corporation for Assigned Names and Numbers-Accredited Registrars, Dec. 11, 2018. Available: <u>https://www.icann.org/registrar-reports/accredited-list.html.</u>
- [3] Apple website for pricing information and more details regarding certificates. Available: <u>https://developer.apple.com.</u>
- [4] Microsoft, "Plan for third-party SSL certificates for Office 365," Oct. 23, 2017. Available: https://docs.microsoft.com/en-us/office365/enterprise/plan-for-third-party-ssl-certificates.
- [5] Microsoft, "Understanding Certificate Requirements," July 22, 2014. Available: <u>https://docs.mi-crosoft.com/en-us/previous-versions/exchange-server/exchange-141/gg476123(v=exchg.141)</u>.
- [6] Microsoft, "Install Active Directory Domain Services (Level 100)," May 30, 2017. Available: https://technet.microsoft.com/en-us/library/hh472162.aspx.
- [7] Microsoft, "Use a lab environment for your devops," May 1, 2017. Available: <u>https://docs.mi-crosoft.com/en-us/visualstudio/test/lab-management/using-a-lab-environment-for-your-applica-tion-lifecycle?view=vs-2017.</u>
- [8] Microsoft, "How To Install ADFS 2012 R2 For Office 365," Apr. 28, 2014. Available: <u>http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-of-fice-365.aspx.</u>
- [9] Microsoft, Office 365 and ADFS...Active Directory Federation Service Installation, Feb. 10, 2018. Available: <u>https://social.technet.microsoft.com/wiki/contents/articles/9082.office-365-and-adfs-active-directory-federation-service-installation.aspx?Redirected=true</u>.
- [10] Microsoft, *Test Lab Guide: System Center 2012 Configuration Manager*. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=30443.
- [11] Microsoft, *Azure Active Directory Sync*, Nov. 8, 2015. Available: <u>https://docs.microsoft.com/en-us/previous-versions/azure/azure-services/dn790204(v%3dazure.100)</u>.
- [12] Microsoft, Geek of All Trades: Office 365 SSO: A Simplified Installation Guide, Aug. 30. 2016. Available: <u>https://docs.microsoft.com/en-us/previous-versions/technet-magazine/jj631606(v=msdn.10).</u>
- [13] Microsoft, *Manage settings and features on your devices with Intune policies*, June 13, 2018. Available: <u>https://technet.microsoft.com/en-us/library/dn913730.aspx</u>.