NIST CYBERSECURITY PRACTICE GUIDE

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

How-To Guide

for Security Engineers

Joshua Franklin Kevin Bowler Sallie Edwards Neil McNab

Christopher Brown Matthew Steele

NIST SPECIAL PUBLICATION 1800-4c





NIST Special Publication 1800-4c

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

DRAFT

Joshua Franklin National Cybersecurity Center of Excellence Information Technology Laboratory

> Kevin Bowler Christopher Brown Neil McNab Matthew Steele The MITRE Corporation McLean, VA



November 2015

U.S. Department of Commerce Penny Pritzker, Secretary

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



DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-4c, Natl. Inst. Stand. Technol. Spec. Publ. 1800-4c, 137 pages, (November 2015), CODEN: NSPUE2

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

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

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

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

DRAFT

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices.

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

ABSTRACT

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

KEYWORDS

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



ACKNOWLEDGMENTS

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

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

Contents

2 1	Intr	oduct	ion			1
3	1.1	Pract	ice Guid	e Structure	9	2
4	12	Build	Overvie	w		3
5	1.3	Typo	araphica	l Conventi	ons	
	-	71 - 3	5 1			
6 2	Hov	to B	uild a C	Cloud-Ba	sed Solution to Mobile Device Security	5
7	2.1	Cloud	Build S	etup and (Configuration	5
8		2.1.1	Cloud B	uild Compo	nents	5
9		2.1.2	Office 3	65 Setup		6
10		2.1.3	Office 3	65 MDM Se	etup	16
11			2.1.3.1	Configure	Push Certificate for iOS Devices	21
12 3	Hov	v to B	uild an	On-Prem	nises Solution for Mobile Device Security	
13	3.1	Hybri	d Build S	Setup and	Configuration	
14	3.2	Hybri	d Detaile	ed Archited	ture	
15		, 3.2.1	Hybrid E	Build Comp	onents	
16		3.2.2	Enterpri	ise Network	and Firewall	
17		3.2.3	Enterpri	ise Software	Components for Hybrid	
18			3.2.3.1	Active Dire	ectory Domain Services	
19			3.2.3.2	Active Dire	ectory Federation Service	
20			3.2.3.3	Active Dire	ectory Federation Services Proxy	
21			3.2.3.4	Systems (Center Configuration Manager	
22			3.2.3.5	Azure Acti	ve Directory Sync Services	
23		3.2.4	Cloud S	Services Inst	ances	
24			3.2.4.1	Office 365	Setup	
25			3.2.4.2	Intune Set	up	40
26			3.2.4.3	Lookout S	etup	
27		3.2.5	Hvbrid I	ntegration .		
28			3.2.5.1	Office 365	with Active Directory Federation Setup	
29			3.2.5.2	Azure Acti	ve Directory Sync Services	
30			3.2.5.3	Svnc Intur	ne with Office 365 Exchange	
31			3.2.5.4	Manage Ir	ntune with SCCM	
32				3.2.5.4.1	Configure Active Directory User Discovery	
33				3.2.5.4.2	Register SCCM with Intune	
34				3.2.5.4.3	Configure Push Certificate for iOS Devices	
35				3.2.5.4.4	Mobile Policy Creation	64
36				3.2.5.4.5	Create Mobile Application Policy	
37			3.2.5.5	Configure	SCCM with Lookout Application	83
38 4	Dev	ice Co	onfigur	ation		
39	4.1	Devic	e Enroll	ment with	Office 365	92
40	7.1	411	iOS			۵۵ مع
		7.1.1				

41		4.1.2	Android	101
42		4.1.3	Windows Phone 8.1	107
43	4.2	Email	Setup	114
44		4.2.1	iOS	115
45		4.2.2	Android	119
46		4.2.3	Windows Phone 8.1	126
47		4.2.4	Windows 8.1	128
48	4.3	Looko	out MTP Enrollment	130
49		4.3.1	Android	132
50 A p	opend	lix A	Acronyms	135
51 A r	opend	lix B	References	137

54 List of Figures

55 Figure 2.1	Cloud Build Process	6
56 Figure 3.1	Hybrid Build Process	30
57 Figure 3.2	Detailed Architecture	31
58 Figure 3.3	Detailed Architecture with IP Addresses	32
59 Figure 3.4	List of Configured Interfaces	34
60 Figure 3.5	WAN	34
61 Figure 3.6	WAN Firewall Rules 3	34
62 Figure 3.7	DMZ Firewall Rules	35
63 Figure 3.8	LAN Firewall Rules	35
64 Figure 3.9	Management Firewall Rules	36

66

67 List of Tables

68 Table 1.1	Typographical Conventions4
69 Table 2.1	Cloud Build Components

70 Table 3.1	Components	2
71 Table 3.2	Enterprise Software Components	6



2	1.1	Practice Guide Structure	2
3	1.2	Build Overview	3
4	1.3	Typographical Conventions	4
5			

8

9

The following guides show IT professionals and security engineers how we implemented this example solution 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 guides show how we incorporated the products together in our environment. 10

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.

13 1.1 Practice Guide Structure

- This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and 14 provides users with the information they need to replicate this approach to mobile device 15 security. The reference design is modular and can be deployed in whole or in parts. 16 Depending on their roles in an organization, different people will use this guide in different ways. 18 This guide contains three volumes: NIST SP 1800-4a: Executive Summary 20 NIST SP 1800-4b: Approach, Architecture, and Security Characteristics - what we built and 21 why 22 NIST SP 1800-4c: How-To Guides - instructions for building the example solution (you are here) 24 Depending on your role in your organization, you might use this guide in different ways: 25 Business decision makers, including chief security and technology officers will be interested in 26 the Executive Summary (NIST SP 1800-4a), which describes the: challenges enterprises face in implementing and using mobile devices example solution built at the NCCoE 29 benefits of adopting the example solution 30 Technology or security program managers who are concerned with how to identify, 31 understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-4b, which describes what we did and why. The following sections will be of particular 33 interest: 34 Section 4.3, Risk Assessment, provides a detailed description of the risk analysis we 35 performed. 36
- Section 4.4, Security Characteristics and Controls Mapping, maps the security characteristics of this example solution to cybersecurity standards and best practices. 38
- You might share the Executive Summary, NIST SP 1800-4a, with your leadership team members 39 to help them understand the importance of adopting standards-based enterprise mobility 40 management (EMM) approaches to protect your organization's digital assets. 41
- IT professionals who want to implement an approach like this will find the whole practice guide 42 useful. You can use the How-To portion of the guide, NIST SP 1800-4c, to replicate all or parts of 43 the build created in our lab. The How-To guide provides specific product installation, 44

- 45 configuration, and integration instructions for implementing the example solution. We do not
- re-create the product manufacturers' documentation, which is generally widely available.
- Rather, we show how we incorporated the products together in our environment to create an
 example solution.
- This guide assumes that IT professionals have experience implementing security products 49 within the enterprise. While we have used a suite of commercial products to address this 50 challenge, this guide does not endorse these particular products. Your organization can adopt 51 this solution or one that adheres to these guidelines in whole, or you can use this guide as a 52 starting point for tailoring and implementing parts of a solution that would support the 53 deployment of mobile devices and the corresponding business processes. Your organization's 54 security experts should identify the products that will best integrate with your existing tools 55 and IT system infrastructure. We hope you will seek products that are congruent with 56 applicable standards and best practices. 57
- A NIST Cybersecurity Practice Guide does not describe *the* solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to mobile-nccoe@nist.gov, and join the discussion at https://nccoe.nist.gov/forums/mobile-device-security.

63 1.2 Build Overview

The NCCoE constructed the Mobile Device Security building block using a virtual environment 64 and a physical wireless access point. The servers hosted by the virtual environment were built 65 to satisfy the hardware specifications of the specific software components in a small test 66 environment (hard drive capacity, memory, etc). The wireless access point was configured to 67 use a closed lab network rather than directly Internet connected. The mobile devices used in 68 the build were configured to use this access point to simulate usage outside of the traditional 69 corporate network boundaries. Readers of this guide should assess the hardware needs of their 70 environment carefully before implementation. Further, this build requires Internet accessibility for some of the on premise components which connect to commercial cloud services. We recommend configuring your firewall or other equipment to only allow Internet access from on 73 premise systems to a specific IP space provided by your cloud provider. 74

Finally, this document makes heavy use of screen shots from cloud services setup 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 screen shots and what the implementer
 experiences. Refer to vendor documentation to address significant variations.

79 1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

Table 1.1 Typographical Conventions

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

How to Build a Cloud-Based Solution to Mobile Device Security

32.1 Cloud Build Setup and Configuration

The following How-To will guide an implementer through the process of 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 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].

10 This How-To details the creation, configuration, and enrollment aspects of each cloud service. 11 Keep in mind, a prerequisite to the cloud is an Internet domain name. If the implementer does 12 not already have a domain name, one can be obtained from an accredited registrar¹. You will 13 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 Office365 instance to send push notifications to enrolled devices. Refer to the Apple website for pricing information and more details regarding certificates².

Further, during the configuration of the Office365 MDM you will be prompted to allow or block
 devices from Office365 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
 Office365 services.

Finally, we have chosen in this simple cloud build to leverage the MDM capabilities that are
 available within Office365. 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.

26 2.1.1 Cloud Build Components

27 28

4

5

6

7

8

9

Table 2.1 lists the components used for this building block:

Table 2.1Cloud Build Components

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

^{1.}https://www.icann.org/registrar-reports/accredited-list.html

^{2.} https://developer.apple.com/

Table 2.1 **Cloud Build Components**

Make	Model	Version	Quantity
Nokia	Lumia (Windows Phone)	830 (8.10.14219.341)	1
N/A	Public Domain Name	N/A	1

The cloud building block build process can be completed with the high-level steps in figure 2.1, 29 Cloud Build Process. The following sections in the How-To guide will focus on the second and 30 third steps.

Figure 2.1 **Cloud Build Process** 32



33

31

34 2.1.2 Office 365 Setup

35	Office 365 is central to the functionality of the cloud building block. The only prerequisite to
36	this step is a public domain name. Keep in mind these steps may change, as this is a Web based
37	procedure.

- To start the process, use a Web browser to access the following URL: 38
- https://products.office.com/en-us/business/office-365-enterprise-e3-business-software 39

Office 365 Enterprise E3

Move your business ahead with the latest full Office, plus a wide range of integrated collaboration services coupled with advanced compliance features and full IT power.

\$20.00 user/month annual commitment	Buy now
Free trial ④	

40

41

1. Choose a commitment level.





Prove. You're. Not. A. Robot.





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



3. Choose **Admin** from the set of services.

III Office 365				A 🔅 ?
Office 365 admin center 🔍				NCCoE (Edit)
Search users, admin tasks an $ ho$				
	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 quickly			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 WEBSITE				Known issues
Poblic Hebare	Service health	Current health		Information on Yammer
BILLING	1 issue	Exchange	Restoring service 💌	
EXTERNAL SHARING		Literative Consistent	No income	community
SERVICE SETTINGS	Service requests	Identity service	100 03065	Ask a question in the forums
REPORTS	No open service requests	Lync	Service restored 💌	Check out our blog
SERVICE HEALTH		Office 365 Portal	Service restored 👻	Participate in the community
SUPPORT	Inactive email users	Office Subscription	No issues	
PURCHASE SERVICES	o users have not signed in for au days or more.	Rights Management Service	No issues	
MESSAGE CENTER	Mail protection	SharePoint	No issues	
TOOLS	1 messages received, 0 processed by filtering.	Vammer Enterrorise	No issues	
ADMIN		 Martine Cried Science 		
Exchange	Message center	View details and history		
Lync	2 new messages in the past 7 days			
SharePoint		Planned maintenance		
Compliance	Included services			
Azure AD		No planned maintenance scheduled.		
Bing Places for Business				

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

0	DASHBOARD DOMA	INS				
Ma Add	Manage domains Add a domain you already own to Office 365, or buy a new domain. What is a domain?					
	+ Add domain 🛒 B	uy domain	ACTION			
۲	cmdsbb.onmicrosoft. com (Default)	Setup complete	No action required	cmdsbb.onmicro		
				🍄 Manage DNS		

5. Choose Add domain.

Office 365	
Add a new domain in Office 365	What you need to know about * domains and DNS
Step 1 Verify domain Step 2	Your domain name identifies your school or business on the internet. In the examples below, yourcompany.com is the domain name: you@ yourcompany.com http://www. yourcompany.com
Add users	DNS (domain name system) works like an address book on the internet. When someone sends you email, DNS directs it to your mailbox.
Step 3 • Set up domain	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 Θ

6. Choose Let's get started.



7. Enter your public domain name.

	Office 365	
	Add a new domain in Office 365	Which domain do you want to × use?
	Step 1 Verify domainStep 2	cmdsbb.org Your users' email addresses will look like this: username@cmdsbb.org
	Add users Step 3 Set up domain	Next Don't have a domain? Buy one K Back
8.	Choose Next .	



Add this TXT record to 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	TTL
@	MS=ms37771077	3600

Okay, I've added the record ⊖

Can't add a TXT record? Use an MX record instead

60

61 62 9. Add this information to the **TXT record** of your domain name. This functionality should be available from your registrar.

🔤 Command Prompt - nslookup	
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	<u> </u>
C:\Users\ncm2>nslookup Default Server: hawk.nist.gov Address: 129.6.16.1	=
> set type=txt > cmdsbb.org Server: hawk.nist.gov Address: 129.6.16.1	
Non-authoritative answer: cmdsbb.org text =	
"MS=ms37771077" cmdsbb.org text =	
"v=spf1 include:spf.protection.outlook.com -all"	
cmdsbb.orgnameserver = be8.nist.govcmdsbb.orgnameserver = gea.nist.govcmdsbb.orgnameserver = bea.nist.govcmdsbb.orgnameserver = bea.nist.govbea.nist.govinternet address = 132.163.4.10bea.nist.govAAAA IPv6 address = 2610:20:6601:4::10gea.nist.govinternet address = 129.6.13.3gea.nist.govAAAA IPv6 address = 2610:20:6005:13::3	

- 64 65
- 65 66

10. Verify the Domain Name Service (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.

We've verified that you own cmdsbb.org

Now, let's update email addresses for your current users in Office 365.



Next 🏵

68 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.

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

Update selected users ⊖

69 70

71

72

12. Choose Update selected users.

Sign ou	it <mark>to comple</mark>	ete the char	nge		
Sign out, an setting up.	d then sign in using	nmcnab@cmdsbb.	org . Don't worry, w	ve'll brin <mark>g y</mark> ou righ	t back here to continu
					Sian out

13. Skip adding new users, and choose skip this step.

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?

73

74

75

Next 🏵

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 🗩

76 **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?

78

Next 🏵

16. Choose Next.

Add the following DNS records for cmdsbb.org

Add the records at your DNS host (Change)

MX records (Step-by-step instructions for adding a MX record)

Priority	Host name	Points to address or value	TTL	
0	0	cmdsbb-	3600	
0	^w	org.mail.protection.outlook.com	5000	

CNAME records (Step-by-step instructions for adding a CNAME record)

Host name	Points to address or value	TTL
autodiscover	autodiscover.outlook.com	3600
msoid	clientconfig.microsoftonline-p.net	3600

TXT name	TXT value	TTL
	v=spf1	
D	include:spf.protection.outlook.com	3600
	-all	

Okay, I've added the records €

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

83 2.1.3 Office 365 MDM Setup

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

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

() # https://pertal.office.com/Ad	drive Default augerflottandrivertoryPage	3 0 = C 0, Sranh	☆ 白 ♣ ★ Ө 🖸 🤜 🗮
III Office 365			0 ? 🔍
Office 365 admin center	DASHEGARD MOBILE DEVICES		NCCoE (Edd)
Search users, administration of	Set up Mobile Device Management for Office 365		
SETUP	a Start using mobile device management (MSM) to manage and enhance the security	of the mobile desires that connect to usue constitution.	
+ USERS	View an inventory of all the devices that are enrolled into MOM		
COMPANY PROFILE	 Create and manage device security policies and access rules Perform common management tasks like wiging devices 		
CONTACTS	View detailed devices and reports		
SHARED MALEOXES	Although Mobile Device Management is available in Office 365, it is a separate onlin	eservice with its own privacy and security commitments	
MEETING RODMS			
GROUPS	We're setting things up for you. This may take a few hours, so check lack again	n shartiy	
DOMAINS			
PUBLIC WEBSITE			
+ BLUNG			
• EXTERNAL SHARING			
MOBILE DEVICES			
» SERVICE SETTINGS			
REPORTS	1		
SERVICE HEALTH			
+ SUPPORT			
PURCHASE SERVICES			
MESSAGE CENTER			
10015			
# ADMIN			
Exchange			
Skype for Business			
Share Point			
Abure AD			
Rana Places for Resident	and a second		# Feedback

87

88

80

81

82

1. Choose Get Started.

0.0					_ 0 ×
+ https://portal.office.	com /admin/	default.aspx#Group	,O + 🗎 C 🚺 port	tal.office.com ×	
III Office 365					* ?
Office 365 admin center	« @	DASHBOARD G	ROUPS		NCCoE (Edit)
Search users, admin tasks an	Use	security groups to assign	permissions for SharePoint	groups.	
DASHBOARD	Use Excl	distribution lists in Excha nange admin center.	nge to manage email distrib	oution. Set up distribution l	ists and other Exchange groups in the
SETUP	- +	- > B			
▶ USERS		Name	Email address	Status	
COMPANY PROFILE		NCCoE Operators	NCCoE@cmdsbb.org	In cloud	
IMPORT		j weede operators	Neccelections	in cloud	
CONTACTS					
SHARED MAILBOXES					
MEETING ROOMS					
GROUPS					
DOMAINS					
PUBLIC WEBSITE					
▶ BILLING					
EXTERNAL SHARING					
MOBILE DEVICES					
SERVICE SETTINGS					Activate Windows
REPORTS					Go to System in Control Panel to
SERVICE HEALTH	~ _				activate windows.
					5:30 PM
		1 🕝 🖗 🧐			▲ 10 11/2015

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

Office 365		¢?
fice 365 admin center	CC DASHBOARD GROUPS	NCCoE (Edit)
earch users, admin tasks an		~
	Create security group	nge groups in the
DASHBOARD	* Group name	
	Managed Users	
	Description	
IMPORT	Management	
	Managed mobile device users.	
SHARED MAILBOXES		
MEETING ROOMS		
GROUPS		
DOMAINS		
PUBLIC WEBSITE		
BILLING	Create Cancel	
EXTERNAL SHARING		
MOBILE DEVICES		
SERVICE SETTINGS		Activate Windows
REPORTS		Go to System in Control Panel to activate Windows
SERVICE HEALTH		activate windows.

3. Add a title and description for the group.



95

4. Add members to the group to be managed.

🕀 🗟 https://na01b.con	npliance.protection. outlook.com /ucc/?p=de	vic 🔎 🗕 🕈 🕞 Mobile devic	e managemen ×	ŵ 1
Office 365	Admin			₿?
Compliance Cente	er			
Home	Mobile device managem	ent		
Archiving	Create and apply device ma	nagement policies to pro	tect your organization's	data Learn more
Device management	Examples of supported scenarios of OneDrive for Business app in iPhone	controlling access: access corporate . Some scenarios might work differ	e Exchange mail using native ma rently from your expectation.	ill client in Android; access documents u
eDiscoverv	Learn more about supported devices	and scenarios		
Potention	Manage device access settings Show list of managed devices			
Import	+ / = 2			
Dormissions	Name	Status	Modified on	
Permissions	Baseline Policy for Mobile Device	s On	5/14/2015 12:	Name
				Baseline Policy for Mobile Devices
				Description
				Require a password, Manage Emai ofiles, disable camera.
				Settings
			A G a	t Configure following settings on de es. Block access and report violatic fridevices that have this policy app viv a are not compliant with these set
		1 selected of 1 total		

96 97

98

5. Navigate to **Office 365 -> Admin Center -> Mobile Devices -> Manage device security policies** to configure a device policy to hand out to enrolled devices.

		-	٥	x
🧲 🕘 🖳 htt	Organization-wide device access settings - Internet Explorer		6 T	3 🔯
📰 Offic	🙀 https://na01b.compliance.protection.outlook.com/Ucc/Device/DeviceTenantPolicy.aspx?reqld=1431639614836&pwmcid=3&ReturnObjectType	?		9
Complian	Organization-wide settings for device access management			
Home	Do you allow unsupported devices to access Exchange email using native email clients			
Archiving	when they are targeted by policies?			12
Device manag	Learn more about supported devices and scenarios	tum	ients L	sing
eDiscovery	Are there any security groups you want to exclude from access control?			
Retention	People selected or in selected security groups will not be affected by any block access actions you configured when their			
Import	devices are not compliant. Actions will be overnoden.			
Permissions				
		De	vices	Ê
		age	Email	pr
	Activate Windows	igs o rt vi	on de olatio	vic ns

100

6. Choose to block what Office365 cannot manage and configure the user group white list.

🔶 💿 🖼 https://na01b.complia	Sew device security policy - Internet Explorer	n 🖈 6
Office 365	https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqld=14:	t# ? 🔎
Compliance Center	New device security policy	
Home	Enter a name and description	
Archiving	Give this device policy a friendly name so you can easily find it again later.	ta Learn more
Archiving	*Name	client in Android; access documents using
evice management	Default Configuration Policy ×	50 5253
Discovery	Description	
etention		
mport		
Permissions		-
		Name
		Baseline Policy for Mobile Devices
		Description
		Require a password, Manage Email pr ofiles, disable camera.
		Settings
	, /	Configure following settings on devic es. Block access and report violations

101

102

7. Set the name for the device policy.



8. Set rules for the device policy.

		_ 0 ×
https://na01b.comp	🐻 🖉 New device security policy - Internet Explorer 📃 🗖 🗙	ሰ 🖈 🗄
Office 365	Imps://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?regld=14;	¢?
Compliance Center	New device security policy	
Home	What else do you want to configure?	
Archiving	Require encrypted backup Block cloud backup	ata Learn more
Device management	Block document synchronization Block photo synchronization	tlient in Android; access documents using
eDiscovery	☑ Block screen capture	
Retention	 □ Block video conferences on device ☑ Block sending diagnostic data from devices 	
mport	☐ Block access to application store	
Permissions	Require password when accessing application store	
	Block connection with removable storage Block Bluetooth connection	Name
	The settings show will be configured on ware' devices and	Baseline Policy for Mobile Devices
	violations will be reported	Description
		Require a password, Manage Email pr ofiles, disable camera.
		Settings
	A	Configure following settings on devic es. Block access and report violations recoverement. Control Panel for

9. Set additional hardware restrictions.



108

10. Select whether or not to deploy the policy and to what group.

https://na01b.comp	a 🥔 New device security policy - Internet Explorer 📃 🗖 🗙	\$ €
Office 365	https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqld=14:	¢?
Compliance Center	New device security policy	
Home	Do you want to apply this policy now?	
rchiving	Select Group - Internet Explorer Attps://na01b.compliance.protection.outlook.com/Ucc/Pickers/DeviceGroupPicker.as;	ata Learn more
Device management	manage X	client in Android; access documents usin
Discovery	ALIAS AUSPLAY NAME	
etention	Managed Users Managed Users	
nport		
permissions		
		Name
	1 selected of 1 total	Baseline Policy for Mobile Devices
		Description
	add -> Managed Users[remove];	Require a password, Manage Email pr
		ofiles, disable camera.
	OK Cancel	Settings
	We'll save this policy, but it won't be applied to	Configure following settings on devic
	G	to System in Control Panel to

109

110 **11.** Select the group created earlier and apply the policy.

111 2.1.3.1 Configure Push Certificate for iOS Devices

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



1. Set up Apple APN in Office 365 -> Admin Center -> Mobile Devices -> Manage Settings.



2. Configure APNs Certificate for iOS devices -> Setup





c. You will be prompted for your Apple Developer account credentials.

^{3.} This website has degraded compatibility with IE 11, but the process will complete.





4. Once authenticated, choose **Create a certificate**.

a. 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**.

🔶 🕘 🏼 https://identity.a	pple.com/pushcert/		, م	- 🔒 Apple Inc. [U	S] C 💋 Apple	Push Certificates P	or ×		-
É	Store	Mac	iPod	iPhone	iPad	iTunes	Support	٩	
Apple	Push Cer	tificates	Portal				nr	ncnab@mitre.org	Sign out
Crea Upload vendor Notes	Ate a New F your Certificate Sig to create a new put	Push Cert ning Request sig sh certificate.	ificate	ird-party server					
						Ŷ			
C:/User	-Signed Certificate	Signing Request Browse	Cancel	Upload					
Shop the Apple On	line Store (1–800–MY–Al	PPLE), visit an Apple R i	etail Store, or find a	reseller.	Apple Info	o Site Map	Hot News R	SS Feeds Contact U	. 🔒
Copyright © 2014	Apple Inc. All rights rese	rved. Terms of Use	Privacy Policy						

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.



6. Upload the signed APN certificate from Apple's developer portal.

Office 265				# 2
ffice 365 admin center «				NCCoE (Edit)
Search users, admin tasks an 🔎		E DEVICES	265	
DOMAINS	Mobile Device Mana	gement for Office	: 365	Settings
PUBLIC WEBSITE	The following mobile devices have your tenant. You can view device p security policies.	been enrolled in Mobile Devic roperties, access reports, wipe	e Management by users in devices and enforce device	APNs Certificate for iOS devices expires 5/18/2016
EXTERNAL SHARING	Manage device security policies and	d access rules		Manage settings
MOBILE DEVICES	See device compliance report			
SERVICE SETTINGS	Select a view: All		~	
REPORTS				
	р С			
SERVICE HEALTH	P C DEVICE NAME	A OPERATING SYSTEM	OS VERSION	
SERVICE HEALTH SUPPORT PLIRCHASE SERVICES	P DEVICE NAME Matt Steele - iPhone 6 8.3	OPERATING SYSTEM iPhone	OS VERSION 8.3	
SERVICE HEALTH SUPPORT PURCHASE SERVICES MESSAGE (ENTER	P 2 DEVICE NAME Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/	OPERATING SYSTEM iPhone Android	OS VERSION 8.3 5.1	Full wipe Selective wipe Learn more about full vs.
SUPPORT PURCHASE SERVICES MESSAGE CENTER TOOLS	P B DEVICE NAME Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/ Matt Steele - msteele_WindowsPh	OPERATING SYSTEM iPhone Android WindowsPhone	OS VERSION 8.3 5.1 8.10.14219.341	Full wipe Selective wipe Learn more about full vs. selective wipe.
SERVICE HEALTH SUPPORT PURCHASE SERVICES MESSAGE CENTER TOOLS ADMIN	DEVICE NAME Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/ Matt Steele - msteele_WindowsPh	OPERATING SYSTEM iPhone iAndroid windowsPhone	OS VERSION 8.3 5.1 8.10.14219.341	Full wipe Selective wipe Learn more about full vs. selective wipe. Status
SERVICE HEALTH SUPPORT PURCHASE SERVICES MESSAGE CENTER TOOLS ADMIN Exchange	DEVICE NAME DEVICE NAME Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/ Matt Steele - msteele_WindowsPh	OPERATING SYSTEM iPhone Android windowsPhone	OS VERSION 8.3 5.1 8.10.14219.341	Full wipe Selective wipe Learn more about full vs. selective wipe. Status
SERVICE HEALTH SUPPORT PURCHASE SERVICES MESSAGE CENTER TOOLS ADMIN Exchange Stype for Business	DEVICE NAME Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/ Matt Steele - msteele_WindowsPh	OPERATING SYSTEM iPhone Android windowsPhone	OS VERSION 8.3 5.1 8.10.14219.341	Full wipe Selective wipe Learn more about full vs. selective wipe. Status Device Model
SERVICE HEALTH SUPPORT PURCHASE SERVICES MESSAGE CENTER TOOLS ADMIN Exchange Skype for Business SharePoint	P P DEVICE NAME Matt Steele - iPhone 6 8.3 Matt Steele - msteele_Android_5/ Matt Steele - msteele_WindowsPh	OPERATING SYSTEM iPhone Android windowsPhone	OS VERSION 8.3 5.1 8.10.14219.341	Full wipe Selective wipe Learn more about full vs. selective wipe. Status Device Model Activate Windows Go to system in Control Panel to

- 7. Verify that the APN is working correctly; it should have an expiration date listed.

How to Build an On-Premises Solution for Mobile Device Security

3	3.1	Hybrid Build Setup and Configuration	30
4	3.2	Hybrid Detailed Architecture	30
5			
⁶3.1 Hybrid Build Setup and Configuration

Figure 3.1 depicts the high-level procedures to reproduce the hybrid build used in this building 7 block. First, the implementer must own an Internet domain name or have permission to edit 8 resource records within a domain. This is a prerequisite to integration with the cloud services 9 used within this build. The next set of steps configure the on-premises components. The 10 procedures assume that no on-premises 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 13 final set of steps instantiate the cloud services and integrate them into the on-premises 14 components. 15

16 Figure 3.1 Hybrid Build Process



17

An important prerequisite to using Microsoft's Active Directory Federation Service (ADFS) in this hybrid arrangement is a third-party public key certificate issued by 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 (TLS) 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 [2] and [3] for specific requirements.

Finally, several cloud based services 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. 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.

31 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 between the on-premises, cloud and mobile device components. Figure 3.3 is a similar view, but details the network addressing and hostnames that were used during the build.

Figure 3.2 Detailed Architecture



37

36

38 Figure 3.3 Detailed Architecture with IP Addresses



39

40 3.2.1 Hybrid Build Components

- 41
- Table 3.1 lists the components used for this building block.

42

Table 3.1 Components

Make	Model	Version	Quantity
Lookout Mobile Security	Lookout Security for Work App	2.0.150	1
Lookout Mobile Security	Mobile Threat Protection		1
Microsoft	Office 365 Tenant	Business Premium	1
Lenovo	Miix (Windows) ^a	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

Table 3.1	Components		
Make	Model	Version	Quantity
Microsoft	SCCM		1
Microsoft	AD DS		1
Microsoft	AD FS		1
Microsoft	AAD Sync		1
Microsoft	WAP		1
Microsoft	Intune	N/A	1
Symantec	Public Certificates	N/A	
N/A	Public Domain Name	N/A	1

a. Intel loaned a Lenovo Miix 2.8 tablet with Windows 8.1.

43 3.2.2 Enterprise Network and Firewall

- The build uses PFSense for the organization router/firewall (see Table 3.2). 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.⁴
 Only IPv4 is used.⁵
- Implementers should refer to PFSense documentation for installation and configuration
 instructions. To recreate the configuration, follow the instructions in the documentation and
 use the configuration files⁶ made available by PFSense.
- The following screen shots 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 section 3.2. The individual interfaces are described below with the firewall rules.

^{4.}A dual firewall configuration could also be implemented.

^{5.}IPv6 is disabled for simplicity.

^{6.}pfSense Configuration Files:

Interfaces - interfaces-config-pfSense.localdomain-20150402160851.xml

NAT - nat-config-pfSense.localdomain-20150402160838.xml

Firewall - filter-config-pfSense.localdomain-20150402160823.xml

56 Figure 3.4 List of Configured Interfaces

WAN

Interfaces		
		1000baseT <full-duplex></full-duplex>
	1.0	10.33.1.105
		1000baseT <full-duplex></full-duplex>
		192.168.1.1
- MONT		1000baseT <full-duplex></full-duplex>
<u>mgmi</u>		192.168.2.1
P DM7		1000baseT <full-duplex></full-duplex>
	т.	192.168.3.1

57

58

59

60

61

62

63

64

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.



A number of firewall rules are configured to control access through the sub-networks. The following screen shots show these rules for the wide-area network (WAN), demilitarized zone (DMZ), local area network (LAN), and management network (MGMT).



Figure 3.5

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

66

The WAN configuration information is specific to our Internet service provider. In this lab, we are provided the 10.33.1.0/24 network from which to statically assign addresses. The PFSense device's IP address is 10.33.1.105, and 10.33.1.104 is also assigned as a virtual IP address for the Web application proxy (WAP) service. Firewall rules are configured to allow Internet access to
 the WAP in the DMZ in order for ADFS to function.

72 Figure 3.7 DMZ Firewall Rules

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	5
		IPv4 TCP/UDP	192.168.3.104	*	192.168.1.10	53 (DNS)	*	none		Internal DNS Name Resolution	
		IPv4 TCP/UDP	192.168.3.104	*	192.168.1.20	443 (HTTPS)	*	none		ADFS Sync through WAP	
		IPv4 *	*	*	MGMT net	*	*	none		Block to MGMT	
1		IPv4 *	*	*	LAN net	*	*	none		Block to LAN	
1		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 MGMT networks, except under specific rules for DNS and ADFS access. The IP address of the Active Directory server is 192.168.1.10. The IP address of the ADFS server is 192.168.1.20.

Figure 3.8 LAN Firewall Rules

Floating WAN LAN MGMT DMZ

Firewall: Rules

F0 | ?

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
	IPv4 *	*	*	MGMT net	*	*	none		Block to MGMT
	IPv4 TCP/UDP	LAN net	*	*	*	*	none		Default allow LAN to any rule

79

80

81

73

74

75

76

77

78

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

pass pass (disabled)

Firew	all:	Rules								
Floating	l w	AN LAN	MGMT DI	ız						
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		IPv4 TCP	MGMT net	*	MGMT address	443 (HTTPS)	*	none		This pfSense Web Interface Anti-Lockout
		TDu4	MGMT net	*	*	*	*	none		Default Allow Any

83

84

85

92

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

block block (disabled)

reject (disabled)

86 3.2.3 Enterprise Software Components for Hybrid

match match (disabled)

This section describes the installation of the on-premises 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 table 3.2, which maps each component to the exact system used in figure 3.2.

Table 3.2 Enterprise Software Components

Component	Hostname	IP Address
Active Directory Domain Services	mds00	192.168.1.10
Active Directory Federation Services	mds-adfs	192.168.120
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

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

97 3.2.3.1 Active Directory Domain Services

The Active Directory Domain Services (ADDS) instance used in the hybrid build was created 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 on an ADDS installation should consult Install Active Directory Domain Services [4] Technet article. Alternatively, implementers may wish to reproduce their production environment.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.

108The domain controller will find the user's account based upon the userPrincipalName in the109certificate's Subject Alternative Name field. The original domain controller was set up with a110domain of nccoe.local; however, a more likely scenario would have an organization create an111instance under a well-known TLD. We have addressed this issue by adding a user principle112name (UPN) suffix for hmdsbb.org in the ADDS configuration. All users in this configuration are113required to have a UPNsuffix of <user>@hmdsbb.org. Identity federation between Intune and114on-premises ADFS will fail if the users do not have the appropriate UPN suffix.

- 115 The procedures to configure a UPN suffix are as follows:
- 1. Launch Active Directory Domain and Trusts snap-in.
- 117 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.

Active Directory Domains and Trusts [mds00).N	?	x
UPN Suffixes			
The names of the current domain and the root domain are I principal name (UPN) suffixes. Adding alternative domain n additional logon security and simplifies user logon names.	he def ames p	fault u provid	ser es
If you want alternative UPN suffixes to appear during user them to the following list.	creatio	n, ado	1
Altemative UPN suffixes:			
		Add	
hmdsbb.org ad hmdsbb.org	E	lemov	e
OK Cancel Apply		He	elp

120

119

121 3.2.3.2 Active Directory Federation Service

- Refer to Microsoft documentation for specific installation instructions for your environment. Consult the following articles as a starting point for installation [6] [7].
- 124 Implementers should note the requirement of a certificate issued by a certificate authority that 125 is recognized/trusted by Microsoft. In this demonstration, the build team procured certificates

^{7.}http://blogs.technet.com/b/jratsch/archive/2012/02/17/creating-a-test-lab-from-a-producti on-environment-using-hyper-v-and-gpmc-scripts.aspx

- 126 from Symantec's Secure Site Pro SSL service. Ensure that the provider is able to populate the
- ¹²⁷ Subject Alternative Name extension of the certificates used in the implementation.
- Screen shots below are of the certificates from Symantec used in the build.

Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
Ensures the identity of a remote computer Proves your identity to a remote computer
* Refer to the certification authority's statement for details.
Issued to: sts.hmdsbb.org
Issued by: Symantec Class 3 Secure Server CA - G4
Valid from 3/ 11/ 2015 to 3/ 12/ 2018
Install Certificate Issuer Statement Learn more about certificates
OK

Certificate	
General Details Certification Path	
Show: <ali></ali>	-
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)
Basic Constraints	Subject Type=End Entity, Pat
Certificate Policies	[1]Certificate Policy:Policy Ide
CRI Distribution Points	[1]CRI_Distribution Point: Distr
DNS Name=adfs.hmdsbb.org DNS Name=enterpriseregistration.1 DNS Name=www.hmdsbb.org DNS Name=sts.hmdsbb.org	nmdsbb.org
Ec	lit Properties Copy to File
	ОК

131 3.2.3.3 Active Directory Federation Services Proxy

132 Refer to the articles referenced in section 3.2.3.2 for specific installation instructions.

133 3.2.3.4 Systems Center Configuration Manager

Refer to Microsoft documentation for specific installation instructions for your environment. Consult the following Test Lab Guide as a starting point for installation [8].

136 3.2.3.5 Azure Active Directory Sync Services

137 Refer to the referenced article for Azure Active Directory Sync Tool installation procedures [9].

138 3.2.4 Cloud Services Instances

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

142 3.2.4.1 Office 365 Setup

143The setup of the Office 365 service is the same as previously described for the cloud Office 365144setup. We replaced cmdsbb.org with hmdsbb.org for this build.





Microsoft Intune

fl your company is already using Microsoft Online Services for services such as Microsoft Office 365, we recommend that you use the same user ID to sign up, Learn more about why it is important to sign up with the same User ID. Sign in * Country or Select • * Required * Country or Select • * Country or Can't be changed after signup. Why? * Organization Inguage: English • * * * * * * * * * * * * * * * * * *	oigir up		Trial
<pre>ff your company is already using Microsoft Online Services for services such as Microsoft Office 365, we recommend that you use the same user ID to sign up. Learn more about why it is important to sign up with the same User ID. Sign in</pre>			Microsoft Intune
Intersection why it is important to sign up with the same User ID. Sign in *Required * Country or region: Select *Required * Organization language: English * * First name: Important to sign up with the same User ID. Sign in *Required * Address 1: Important to sign up with the same User ID. Sign in * * Corganization language: English * * Last name: Important to sign up why? * * Organization language: English * * Last name: Important to sign up why? * * Organization language: Important to sign up why? * * City: Important to sign up why? * * State: Alabama * * ZP or postal code: .onmicrosoft.com Check availability * New domain name: .onmicrosoft.com Check availability	If your company is Microsoft Office 36	already using Microsoft Online Services for services such as	100 User Licenses
Country or region: Cart be changed after signup. Why? Organization language: First name: Corganization name: Address 1: Corganization Address 2: City: State: Alabama Address 2: City: State: Alabama Address Corganization code: Phone number: Email address: New domain name: .oomicrosoft.com Check availability	more about why it i	s important to sign up with the same User ID. Sign in * Required	Microsoft Intune helps organization provide their employees with acces
region: Can't be changed after signup. Why? any device, while helping secure corporate information. • Organization language: • First name: • Corganization name: • Last name: • Organization name: • Organization name: • Organization name: • Organization name: • Organization name: • Address 1: • Organization name: • Organization name: • Address 2: • Organization name: • Organization name: • City: • Organization name: • Organization name: • State: Alabama • • ZIP or postal code: • Organization name: • Organization name: • Phone number: • Organization name: • Organization name: • New domain name: • onmicrosoft.com Check availability • Organization name:	* Country or	Select	to corporate applications, data, an resources from anywhere on almos
• Organization Inglish • First name: • Last name: • Organization • Organization • Address 1: • Address 2: • City: • State: Alabama • ZIP or postal • code: • Phone number: • Email address: • New domain name: • New domain name:	region:	Can't be changed after signup. Why?	any device, while helping secure
 First name: Last name: Organization name: Address 1: Address 2: City: State: Alabama ZP or postal code: Phone number: Email address: New domain name: .onmicrosoft.com Check availability 	* Organization language:	English	corporate information.
 Last name: Organization name: Address 1: Address 2: City: State: Alabama ZIP or postal code: Phone number: Email address: New domain name: Onmicrosoft.com Check availability 	* First name:	Ê.	
 Organization name: Address 1: Address 2: City: State: Alabama ZIP or postal code: Phone number: Email address: New domain name: Onmicrosoft.com Check availability 	* Last name:		
 Address 1: Address 2: City: State: Alabama ZIP or postal code: Phone number: Email address: New domain name: Check availability 	* Organization name:		
Address 2: City: State: Alabama ZIP or postal code: Phone number: Email address: New domain name: Check availability	* Address 1:		
* City:	Address 2:		
 State: Alabama ZIP or postal code: Phone number: Email address: New domain name: .onmicrosoft.com Check availability 	* City:		
ZP or postal code: Phone number: Email address: New domain name: .onmicrosoft.com Check availability	* State:	Alabama	
code: Phone number: Email address: New domain name: .onmicrosoft.com Check availability	* ZIP or postal		
Phone number: Email address: New domain name: .onmicrosoft.com Check availability	co de:		
Email address: New domain name: .onmicrosoft.com Check availability	* Phone number:		
New domain name: .onmicrosoft.com Check availability	* Email address:		
name:	* New domain	.onmicrosoft.com Check availability	
	name.		

150

151

2. Choose Sign in. Sign in when prompted.



Check out Confirm order

Microsoft Intune | 30 day term 100 user licenses

Try now Cancel

152



3. Choose Try now. When signup is complete, you should be redirected to the Intune 153 management console at https://manage.microsoft.com. Note that Silverlight 3.0 browser 154 support is required to load the management console. 155

Microsoft Intune Account Portal

In the Microsoft Intune Account Portal you can add and manage users, your subscription, and your domain. After you have added users, you can begin enrolling and managing devices in the Microsoft Intune Admin Console.



156

Note: Important! Do not proceed any farther with Intune if you want to manage devices via
 SCCM.

159 3.2.4.3 Lookout Setup

No online workflow was available to create an instance of enterprise Lookout MTP at the time
 this document was written. Contact the enterprise sales team at support@lookout.com 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

163

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

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

 Open the Lookout administrative console by using a browser and navigating to https://mtp.lookout.com/les.

169 3.2.5 Hybrid Integration

166

167

168

181

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

171 3.2.5.1 Office 365 with Active Directory Federation Setup

172 173 174	1.	In this step, an on-premises 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 added your public domain to Office
175 176		365as described in section 2.1.2. If not, follow the procedures from TechNet Magazine [10]. Detailed integration information can be found in the referenced TechNet article [7].
177 178 179	2.	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.
180		Set-MsolAdfscontext -Computer <ad fqdn="" fs="" server=""></ad>

Convert-MsolDomainToFederated -DomainName <domain name>

182 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-premises 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.

🔶 Microsoft Azure Active Dir	rectory Sync Services _ X
Azure AD Credentials AD DS Credentials User Matching Optional Features Configure Finished	Connect to Azure AD Enter your Azure AD credentials: Username: aadsync@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 Di	irectory Sync Services _ X
Azure AD Credentials	Connect to AD DS
AD DS Credentials	
User Matching	Enter the Active Directory Domain Services credentials for each forest:
Optional Features	Forest: nccoe.local
Configure	Licername: accools administrator
Finished	
	Password:
	Add Forest
	Previous
	Go to System in Control Pa

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

Microsoft Azure Active Di	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 Forests NCCOE.local
	Previous Activat Next indows

3. Click Next.

Microsoft Azure Active Dir	ectory Sync Services _ X
Azuro AD Crodontials	Lipiquely identifying your users
Azure AD Credentiais	Uniquely identifying your users
AD DS Credentials	
User Matching	Matching across forests
Optional Features	Our users are only represented once across all forests.
Configure	O Match using:
e i i i i	Mail attribute
Finished	 ObjectSID and msExchangeMasterAccountSID attributes
	SAMAccountName and MailNickName attributes
	O Your own attribute
	Matching with Azure AD
	sourceAnchor attribute: objectGUID 🔹
	userPrincipalName attribute: userPrincipalName
	1 Learn more about user matching
	These settings were previously configured and are displayed for informational purposes only.
	Previous Next
	Activate Windows

4. Accept the defaults for uniquely identifying your users.



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



6. Click Configure.



7. Choose Synchronize now and click Finish.

\$	Synchronization	Service Manager on M	DS-AADSYNC	_ 🗆 🗙
<u>File T</u> ools <u>A</u> ctions	<u>H</u> elp			
Operations	Connectors Metaverse Designer	🚑 Metaverse Search		
Connectors	1-	1-		
Name	Туре	Description	State	Actions
NCCOE.local	Active Directory Domain Services		Idle	😴 Create
hmdsbb.onmicrosoft.co	Windows Azure Active Directory (Micr		Idle	Properties
				🕅 Delete
				Configure Run Profiles
				Run .
				Stop
				Export Connector
				Import Connector
				Update Connector
				Refresh Schema
				📓 Search Connector Space
Total number of Connecto	rs: 2			
Profile Name: User Name	E.			
Step Type: Start Time:		Partition: End Time:	Stat	us:
Synchronization Statistic	s	Connection Status		
		Synchronization Errors		
			,	
		_		
1				Activate Window
				Contractor in Art

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

206 3.2.5.3 Sync Intune with Office 365 Exchange

207The following steps will establish a backend connection between the Intune and Office 365208instances you have created in the Cloud Services Instances section. When this step is209completed, Intune will be able to enforce conditional access policies on all enrolled mobile210devices.

Microsoft Intune			
DASHBOARD	Administration Overview Alerts and Notifications	Set Up Exchange Connection	
GROUPS	 Alert Types Recipients 	Introduction a function On Preferences to Standard environment and complies with the On-Premises Connector system requirements. Learn about the system requirements	L) E
ALERTS	Administrator Management Service Administrators Tenant Administrators	2. Create a user scout in Active Directory that has permission to num the required Schange condition. For Hoste Dechange environment, either create a user in Active Directory or MSDDS that has permission to run the required Exchange condition, or use an existing tenant administrator that has these permissions. Learn Book the Echange condition requirements.	
APPS	Device Enrollment Managers Client Software Download	3. Download the On-Premises Connector software, extracting the contents into a secure location on the computer you prepared. Install and configure the On-Premises Connector using the user account from step 2.	
POLICY	Storage Use Mobile Device Management Windows	Download Cin-Premises Connector	
REPORTS	Windows Phone iOS Microsoft Exchange	Microsoft Intune Service to Service Connector for Hosted Exchange Click Set Up Service to Service Connector to set up a connection to your Exchange hosted environment. An Office 365 account that has an Exchange 2013 tenant is required.	
	Set Up Exchange Connection Multi-factor Authentication NDES Connector	Set Up Service to Service Connector	

211

212

213

214

 Open the Intune administrative console with a browser. Click ADMIN. Then click Set Up Exchange Connection within the Microsoft Exchange section. Click Set Up Service to Service Connector.

https://portal.office	e.: ×) 🚺 Microsoft Intune: Mi: × (TN Start managing IOS : ×		
← → C @ https:	//manage.microsoft.com/MicrosoftIntune/Home?accountid=cf1e73ed-90c4-45ac-8	07b-096142fecc43#Workspace/administration/index#1P=//administration/Exchar	geConnectionPage/&A={GID=2a522080-4e2e=4b12-99e4-53104109dr 😥 😨 🚖 📕
Microsoft Intune			Hulp Sign Out Welcome MCColl
	Microsoft Exchange Mobile Device Management		
	Microsoft Exchange Microsoft Exchange Microsoft Exchange account for equival taxe in en.e. This years you		
	Deckange Connection Information houses projection in Malikang fishings Connector type Moreover balance Service to Service Connector for House Environ Moreover balance Service to Service		
REPORTS		Run Quick Sync 📧	
14 Achier		Microsoft Intune sent a synchronization request to Exchange. Microsoft Inture will syndroxiste new mobile device and mobile devices with changes to the lickney extern.	
		To view the updated mobile device fait after Quick Sync completes, go to the Groups workspace.	
Microsoft © 2015 Micr	osoft All rights reserved. Privacy & Cookies. Feedback		Remote Tasks

215

216

217

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

218 3.2.5.4 Manage Intune with SCCM

219To allow the Intune tenant to be administered remotely, SCCM must be configured on the220enterprise network. The following steps add test accounts to an SCCM user collection and syncs221with the Intune tenant. While Intune will be available through the browser-based222administrative console after this exercise, the account will be permanently configured to223manage devices through SCCM.

224 3.2.5.4.1 Configure Active Directory User Discovery

- 225 When these steps have been completed, the SCCM instance will be able to automatically 226 discover Intune users by way of an Active Directory container.
- Launch the Configuration Manager console. Navigate to System Center Configuration
 Manager / Site Database / Site Management /<site name>/ Site Settings / Discovery
 Methods.
- 230 **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 dialog box, specify Local Domain.

Select New Container	x
Active Directory containers:	
AzureAD Synced Users	
🗄 📲 Builtin	
🗄 🔚 Computers	
🗄 💼 Domain Controllers	
🗄 💼 Enterprise Servers	
Foreign SecurityPrincipals	
🗄 🔚 LostAndFound	
🗄 🔚 Managed Service Accounts	
😟 🛗 NTDS Quotas	
🗄 🔚 Program Data	
🗄 🔚 System	
OK Cance	el

233

234

5. Select the AzureAD Synced Users container.

Active Directory Container	x			
Specify an Active Directory container to search during the discovery process.				
Location				
Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.				
Path:				
LDAP://OU=AzureAD Synced Users,DC=NCCOE,DC=local				
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				
○ Sp <u>e</u> cify an account:				
Set	-			
	_			
OK Cancel				

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

H		Active Directory U	lser Discove	ry Properties	;	x	
Γ	General Polling Schedule Active Directory Attributes						
	Active Directory User Discovery						
	Configure the settings to find user accounts in Active Directory Domain Services. Image: Setting to find user accounts in Active Directory Domain Services.						
	Active	Directory <u>c</u> ontainers:			*]	
	Filter						
	Distin	guished Name	Recursive	Group	Account		
	LDAP	://OU=AzureAD Synced Users,D	Yes	Excluded	Site Server		
	5		11				
			ОК	Cance	Activ	ate	

237

238

7. Ensure that Enable Active Directory User Discovery is selected.



239

240

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

Selected Object Folder Tools	System Center 2012 R2 Configuration M	lanager (Connected	to ROC - NCCO	E HQ)	- 8 :
Home Collection Close					^
Add Add Requests Update Selected Items - Manage Affinity Update Membership Collection Add Add Requests Add Requests Add Compliance Collection Colle	Add Resources Export Delete Export Delete Deployme Overview + Users + All Users All Users 8 items Search Icon Name NCCOEVbisko (Benjamin Sisko) NCCOEVbisko (Benjamin Sisko) NCCOEVbisko (Benjamin Sisko) NCCOEVbisko (James T. Kirk) NCCOEVbisko (James T. Kirk) NCCOEVbis	Properties Properties Properties Domain F NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE NCCOE	Resource Type User User User User User User User Use	X Search	Add Criteria
Antimalware Policies Windows Firewall Policies Sets and Compliance Software Library Monitoring	NCCOE\bsisko (Benjamin Sisko) General Information Name: NCCOE\bsisk	co (Benjamin Sisko)		Related Objects Primary Device	
Administration	Domain or Workgroup: NCCOE		Go	to System in Control	Panel to

242

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

243 3.2.5.4.2 Register SCCM with Intune

- 244The following sequence of steps enrolls an SCCM instance with the Intune tenant. After this245step you will no longer be able to create and deploy policies from the Intune Web management246portal.
- 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.



251

2. Click Next.



3. Click the **Sign In** button.



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

2	Create Windows Intune Subscription Wizard	x
General		
Introduction Subscription	General Configuration	
General Platforms Company Contact Informat Company Logo Summary Progress Completion	Specify the user collection whose members will be able to enroll their devices for management. Qollection: All Users and User Groups Browse 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: Blue Cajor scheme for company portal: Blue Specify the site code for device assignment. Configuration Manager site code:	
	Check service stat	<u>US</u>
< III >	< Previous Next > Summary Cancel	ite W /ste m

257

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

	Create Windows Intune Subscription Wizard	x
Platforms		
Introduction Subscription General	Specify the platforms that a user is able to enroll in Windows Intune	Э
Platforms	Device type:	
Company Contact Informat	i OS	
Company Logo	Windows	
Summary		
Progress		
Completion		
	Platform requirements:	1
		1
	A stir	to M
	< Previous Next > Summary Cancel	He VV
< III >		yste m

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

2	Create Windows Intune Subscription Wizard	x
Company Conta	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 name:	
< III >	<u>Previous</u> <u>Next</u> Summary	a W

262

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

E	Create Windows Intune Subscription Wizard
Company Logo	
Introduction Subscription General	Specify company logo
Platforms	You can customize your company portal with your company logo.
Company Contact Informat Company Logo	Include company logo
Summary	Select a logo to use when the company portal background is white.
Progress Completion	Browse File type: JPEG or PNG Maximum size: 750 KB Maximum resolution: 400 x 100 pixels Select a logo to display over the selected color scheme. Browse
	File type: JPEG or PNG
	Maximum size: 750 KB
	Maximum resolution: 400 X 100 pixels
< III >	<u>Previous</u> <u>Next</u> > <u>Summary</u> <u>Activate</u> W <u>Cancel</u> m

264

8. Submit an organizational logo, if desired.



266

9. Review the settings and click **Next**.



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



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

273 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 describes how to create the CSR within SCCM.

📧 System Center 2012 R2 Configuration Manager (Connect	ected to ROC - NCCOE HQ)	8 ×
Home			^ 🔞
Add Windows Intune Certificate request Status Create APNs Certificate request Status Sea	aved irches • earch		
← → ▼ 🔄 \ → Administration → Overview →	Cloud Ser	Services Windows Intune Subscriptions	- 2
Administration	< Wi	Windows Intune Subscriptions 1 items	
Overview	lco	Icon Name Description	
 Hierarchy Configuration 	Ľ	🖆 Windows Intune Subscription Subscription configuration required to connect to Windows Int	une Se
A 🧮 Cloud Services			
🕑 Windows Intune Subscriptions			
a Cloud Distribution Points			
🗟 Extensions for Windows Intune			
Eile Configuration			
🖳 Client Settings			
Einstein Security			
Distribution Points			
E Distribution Point Groups			
Migration			
Assets and Compliance			
Software Library			
Monitoring			
Administration		Activate Windows	
		Go to System in Control Par activate Windows	iei to
	•		

277

278

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

Request Apple Push Notification Service Certificate Signing Request
Specify the folder where you want to save the downloaded Certificate Signing Request. This is required to request the Apple Push Notification Service (APNs) certificate. You will be prompted for your Windows Intune organizational account to complete the download.
Ele Name: Browse
After you download the Certificate Signing Request, you must perform the following steps to complete APNs setup:
Step 1: Submit the request to the Apple Push Certificate Portal and download the APNs certificate.
Step 2: Upload the APNs certificate to Windows Intune through the Configuration Manager console.
Download Cancel

- 279
- 280

281

282

- 2. Save the CSR to local storage. You'll need this file for the next step.
- 3. Use a browser to visit https://identity.apple.com/pushcert/⁸. You will be prompted for your Apple Developer account credentials.

^{8.} This website has degraded compatibility with IE 11, but the process will complete.



284

4. Once authenticated, choose Create a certificate

https://identity.	apple.com/pushcert/		🔎 👻 🔒 Identified by VeriSig	n 🖒 🥖 Apple Pus	h Certificates Por >		ŵ
Ś	Store	Mac iPo	d iPhone	iPad	iTunes S	upport Q	
Annala	Duch Com	tificatos Da	what				
Apple	Push Cer	tificates Pol	rtal			nmcnab@mitre.org	Sign out
Cert	ificates for	⁻ Third-Party	Servers		Create a C	Certificate	
Service		Vendor	Expiration Date*	Status	Actions		
Mobile D	evice Management	Microsoft Corporation	May 18, 2016	Active	() Renew	Download Revo	ke
Mobile D	evice Management	Microsoft Corporation	May 18, 2016	Active	Renew	Download Revo	ke
Aboi Create a	ut Apple Pi	ush Certificat ertificates that enable y	t es Portal our third-party server to v	ork with the			
Apple Pi Learn m	ish Notification Ser ore about Mobile D	vice and your Apple de Device Management	vices.				
MDM pu	sh certificates crea	ited in the iOS Develope	r Enterprise Program have	been			
migrate Learn m	d to the Apple Push ore about MDM pu	1 Certificate Portal.					
		· · · · · · · · · · · · · · · · · · ·				ALTHA	
Contact Enterpri	Apple for assistant se-level customers	ce with the Apple Push (with an AppleCare OS)	Certificates Portal Support plan: 1-866-752-	7753			
General	inquiries and requ	ests for assistance are h	andled by Apple Develope	r Program			
Support						-+-11	
Shop the Apple Onl	ine Store (1-800-MY-AP	PLE), visit an Apple Retail Store	e, or find a reseller.	Apple Info	Site Map Hot Ne	ws RSS Feeds Cont	act Us 🔰 🚔
Copyright © 2014 /	Apple Inc. All rights reser	rved. Terms of Use Priv	vacy Policy				

285

286

287

288

 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**.



290

291

292

 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.



294

295 296 Load the signed certificate into SCCM. Navigate to Administration -> Overview -> Cloud Services -> Windows Intune Subscriptions. Right-click on Windows Intune Subscription and choose Properties.

A		
File View VM		
System Center 2012 K2 Conligura	ition Manager (connected to ROC - NCCOE HQ)	
Home		
Add Windows Intune Create APNs V	iew Service Saved Properties	
Create	Windows Intune Subscription Properties	
←→ · ► Administration	Company Lono	
	General Android IOS Windows Windows Phone Company Contact Information	
Administration	✓ Enable iOS enrollment	
Client Settings		
Security	Specify the Apple Push Notification service (APNs) certificate to be used to manage iOS	to connect to Windows Intune Se
Administrative Users	devices, in order to get an Arrivs Certificate, you must rollow these steps:	
🕉 Security Roles	Step 1: Download a Certificate Signing Request from Windows Intune using the	
Security Scopes	Request APNs Certificate Service Request dialog box in the Configuration Manager console.	
🛃 Accounts	Step 2 : Submit the Certificate Signing Request to the Apple Push Certificate Portal	
Certificates	and download the APNs certificate.	
Distribution Points	Step 3: Upload the APNs certificate to Windows Intune by specifying the location of the APNs certificate.	
Distribution Point Groups		
 Migration 	APNs catificate on file)	
Source Hierarchy		
Migration Jobs Josephine Migration		
Ustribution Point Migration		
Assets and Compliance		
🗃 Software Library		
Monitoring	OK Canad Analy	
	Carlos Appy	Activate Windows
Administration		Go to System in Control Pane
	•	activate Windows.
Ready	II II	
		• P 🖸 ሱ
Fo release cursor, press CTRL + ALT		

298

299

8. Check the box to **Enable iOS enrollment** and use the **Browse** button to import the PEM certificate you downloaded from Apple. Click **OK**.

300 3.2.5.4.4 Mobile Policy Creation

This section depicts the creation and deployment of a security policy for 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-grained 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 [5].

 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 tool bar.

General Specify general information about this configuration item Mobile Device Settings Password Device Configuration items define a configuration and associated validation criteria to be assessed for complicient devices. Security Encryption Supported Platforms Description: Platform Applicability Description: Summary Specify the type of configuration item that you want to create: Mobile device v	×
General Specify general information about this configuration item Mobile Device Settings Password Device Configuration items define a configuration and associated validation criteria to be assessed for complicient devices. Supported Platforms Name: Platform Applicability Description: Summary Progress Completion Specify the type of configuration item that you want to create: Mobile device v	
Device Configuration items define a configuration and associated validation criteria to be assessed for complication devices. Security Encryption Supported Platforms Description: Platform Applicability Description: Summary Progress Completion Specify the type of configuration item that you want to create: Mobile device v	
Encryption Name: BaseConfig Supported Platforms Description: Platform Applicability Description: Summary Progress Completion Specify the type of configuration item that you want to create: Mobile device V	iance on
Supported Platforms Description: Platform Applicability Description: Summary Progress Completion Specify the type of configuration item that you want to create: Mobile device V	
Progress Completion Mobile device	× ×
Completion Mobile device.	
Assigned categories to improve searching and filtering:	
	es
Act	tivate Windo
< Previous Next > Summarv	vate Cancel owb.

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

Administrative categories:	
	Create
✓ Client	Rename
II Infrastructure	Delete

313

314

3. Select the **Client** category. Click **OK**.
| - | 1 | | Create Configuration Item Wiza | ard X |
|---|--|------|--|---|
| 1 | Mobile Devic | e Se | tings | |
| | General
Mobile Device Setting
Password
Device
Security
Encryption
Supported Platforms
Platform Applicability
Summary
Progress
Completion | S | Select the mobile device setting groups to | configure
b, select the setting group to view the description.
Description:
The security setting group includes typical security
ettings, such as file signing, applications. Bluetooth, and
ameras. |
| | m | > | < Previous | Activate Windo
Go to System in Con
Next > Summary Cl Vate Cancel Own. |



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

	Create Configuration Item Wizard	x
Password		
General Mobile Device Settings Password	Configure mobile device password settings	
Device	Require password settings on mobile devices:	Required 🗸
Encryption	Minimum password length (characters):	4
Supported Platforms	✓ Password expiration in days:	75
Platform Applicability Summary	Number of passwords remembered:	1
Progress	✓ Number of failed logon attempts before device is wiped:	10
Completion	Idle time before mobile device is locked:	1 minute 🗸
	Password complexity:	Not Configured
	Password quality:	Not Configured
	Send password recovery PIN to Exchange Server:	Not Configured
	Remediate noncompliant settings	
	Noncompliance severity for reports:	Waming ↓ Activate Windo
		Go to System in Con
< III >	< Previous Next >	Summary Clarcel OW

318

5. Configure the password requirements based on your local requirements.

81	Create Configuration Item V	Vizard 🔀
Device		
General Mobile Device Settings Password	Configure device settings	
Device Security	Voice dialing:	Allowed
Encryption	Voice assistant:	Allowed
Supported Platforms Platform Applicability	Voice assistant while locked:	Prohibited V
Summary	Screen capture:	Disabled V
Progress Completion	Video chat client:	Disabled 🗸
	Add game center friends:	Prohibited ¥
	Multiplayer gaming:	Prohibited V
	Personal wallet software while locked:	Not Configured 🗸
	Diagnostic data submission:	Enabled v
	✓ Remediate noncompliant settings	
	Noncompliance severity for reports:	Waming ✓ Activate Windo
		Go to System in Col
	< Previou	s Next > Summary Ct Vate Cancel OW

320

6. Configure the device settings based on your local requirements.

2	Create Configuration Item Wiza	rd 🗾
Security		
General Mobile Device Settings Password	Configure mobile device security settings	
Device Security	Unsigned file installation:	IT Administrator V
Encryption Supported Platforms	Unsigned applications: SMS and MMS messaging:	Prohibited v
Summary Progress	Removable storage:	Allowed ~
Completion	Camera: Bluetooth:	Prohibited V Allowed V
	Windows RT VPN profile Profile file:	Browse
	Profile name: Profile for all users:	Remove
	 Kemediate noncompliant settings Noncompliance severity for reports: 	Waming v Activate Wind
<	< Previous	Next > Summary Club System in C

322

7. Configure the security settings based on your local requirements.



324

8. Configure the encryption settings based on your local requirements.

88	Create Configuration Item Wizard	x
Supported Platfo	orms	
General Mobile Device Settings Password Device Security Encryption Supported Platforms Platform Applicability Summary Progress Completion	Specify the supported platforms for this mobile device configuration item Select all Symbian Mobile Symbian Mobile Windows 8.1 Vindows 8.1 Vindows 8.1 Vindows 1 Android	
< III >	Activate Go to Syster < Previous Next > Summary ²	Windo n in Cor gowa.

326

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

	ionity			
General Mobile Device Settings Password Device Security Encountion	Review platform exclusion of the following settings are no be assessed for compliance	usions for ot supported by on the unsupp	this configuration item all the supported platforms that you specified. These settings w orted platforms.	ill n
Supported Platforms	Excluded settings.	a		_
Platform Applicability Summary Progress Completion	Add game center friends Bluetooth Camera Diagnostic data submission Encryption algorithm File encryption on mobile Multiplayer gaming Removable storage Require email encryption Require email encryption Require mail encryption Require password setting Screen capture Signing algorithm SMS and MMS messaging Storage card encryption Unsigned applications	Device Security Security Device Encryption Device Security Encryption Encryption Password Device Encryption Security Encryption Security	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1(SET only);All x64 . All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.1; All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.1; All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.1; All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.1; All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.1; All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.1; All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8 All Windows Phone 8.	
	Video chat client	Device	All Windows Phone 8.0:All Windows RT 8.1:All x64 Windows 8	W

10. Click Next.



11. Click Next.



12. Click Close.

	Folder Tools	System Ce	nter 20)12 R2	Configuration Man	ager (Conne	cted 1	
- Home	e Folder							
Create Configuration Ba	Impo Iseline Configurat Create	ort ion Data	Savec Searche Searc	h				
	Assets a	and Compliar	nce 🕨	Overvie	W Compliance Sett	ings F Cont	gurati	
Assets and Comp	liance -		4	Config	uration Baselines O Item	IS		
🔀 Software	Metering			Search	*	Ī		
 Complia 	Compliance Settings			lcon	Name	Status	Dep	
Config	Configuration Items							
Config	User Data and Profil Remote Connection		nfiguratio	on Basel	ine			
Bernot			nfigurati	on Data				
A Compa			Folder •					
Certi	ficate Profiles							
📴 Emai	l Profiles		E					
VPN	Profiles							
😨 Wi-F	i Profiles							
🗾 Compl	iance Policies		24.54					
🔺 🛄 Condit	ional Access							
Fin Fych	anne Online							
Assets and	Compliance							
Software L	ibrary							
Monitoring	9							

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

	Create	Configuration E	Baseline	
pecify general i	nformation about	this configurati	ion baseline	
Name:	BaseLinePolicy			
Description:				^
specified are compliant	. Uptional items are evalu	ated only if the relevan	it application is present o	n the client devices.
Filter				
Name		Туре	Purpose	Revision
Name BaseConfig		Type General	Purpose Required	Revision Latest
Name BaseConfig	Change Purpose	Type General	Purpose Required	Revision Latest
Filter Name BaseConfig Add Assigned categories to	Change Purpose	Type General	Purpose Required	Revision Latest
Fritter Name BaseConfig Add Assigned categories to "Client"	Change Purpose improve searching and fi	Type General	Purpose Required	Revision Latest
Filter Name BaseConfig Add Assigned categories to "Client"	Change Purpose improve searching and fi	Type General	Purpose Required	Revision Latest Categories Cancel

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



340 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.

2	Create Applicat	ion Management Policy Wizard
General		
General Policy Type	Specify general information a	about this application management policy
Summary	Use these settings to configure an applicat	ion management policy in your hierarchy.
Progress	Name: Manag	ed Apps
Completion	Description:	^
		×
		Activate Windows
		Go to System in Control Panel to
		Cancel

346

347

348

339

 To start the wizard, navigate to Under Software Library > Application Management > Application Management Polices: Create Policy in the SCCM console. Click Next.

	Create Applicatio	on Management Policy Wizard	x
Policy Type			
General	Specify the type of application	n management policy	
Policy Type	1 7 71 11	5 1 5	
iOS Policy	Dist.		
Summary			¥
Progress	Policy Type:	General	×
Completion			
			A stivate Mindows
			Activate windows
			activate Windows
		< Previous Next >	Summary Cancel

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

E	Create Application Management	nt Policy Wizard		x
iOS Policy				
General Policy Type	Application management policy for iOS			
Summary Progress Completion	App Web Content Restrict web content to display in the Managed Browser: Data Relocation Prevent iTunes and iCloud backups: Allow app to transfer data to other apps:		Yes v Yes v Policy Managed Apps v]
	Allow app to receive data from other apps: Prevent "Save As": Restrict cut, copy and paste with other apps:		Any App Ves Yes Ves Policy Managed Apps with Paste In Ves]
	Access Require simple PIN for access: Number of attempts before PIN reset:		Yes 5 5]
	Require corporate credentials for access: Require device compliance with corporate policy for access: Recheck the access requirements after (minutes):		No Ves Ves]
	Timeout: Offline grace period: Additional Policies Encryot apo data:		30 720 When device is locked	
			Activate Windows Go to System in Control Pan	ei to
		< Previous Next	> Summary Cancel	

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



- Upon successful creation, an overview is displayed. The policy needs to be matched with an application before it can be used.
- In the next section, the Outlook application is linked the iOS App store through Company Portal
 and associated with the previously created application policy.

1	Create Application Wizard	x
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. Automatically detect information about this application from installation files:	
	Type: App Package for iOS from App Store v Location: https://tunes.apple.com/us/app/microsoft-outlook/id951937596?mt=8 Browse Example: http://tunes.apple.com/us/app/AppName/iddox?mt=xuo=x	
	Manually specify the application information	
	Activate Win	ndo
< III >	< Previous Next > Summary city at e Canceby	ws.

3601. Navigate to Software Library > Applications and Create Application. Enter the URL for the
application you wish to link to in the Location field. Search for the Outlook application using
a search engine and copy the link to obtain the URL.

1	Cre	ate Application Wizard	x		
General Informa	General Information				
General Import Information General Information	Specify information a	about this application			
Summary	Name:	Outlook			
Progress Completion	Administrator comments:	\$	-		
	Publisher:	Microsoft			
	Software version:				
	Optional reference:				
	Administrative categories:	Select			
		Activate Wi	ndo		
< 111 >		< Previous Next > Summary_ti_/ate_Cancel	ws.		

2. Set the name, version and publisher information for the application link as pictured.



366

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

*		Deploy Software Wizard	x
General			
General Content Deployment Settings Scheduling User Experience	Specify genera	al information for this deployment Outlook Browse	
Alerts Application Managemen Summary Progress Completion	Collection: Use default distr Automatically dis Comments (optional)	All Users Browse Iribution point groups associated to this collection istribute content for dependencies It:	
		μ	<
< III >		<pre>< Previous Next > SummaryGd Scance</pre>	<u>Vinde</u> h in Co

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

٠	Deploy Software Wizard			
Application Mar	agement			
General Content Deployment Settings Scheduling	Specify a	application management options		
User Experience Alerts	Where re	equired, select an application management policy to	o apply to each deployment type in this deployment.	
Application Management		Deployment Type	General Policy	
Summary	J	microsoft-outlook - App Package for iOS from	Managed Apps	
Progress				
Completion				
<		< Previous	Next > Summary G	<u>/ind</u>

5. After setting the general settings for deploying the application, you will get a chance to link an application profile.

372 3.2.5.5 Configure SCCM with Lookout Application

This section describes the 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 vary based on the mobile platform. Android users will be directed to the Google Play Store, iOS users will be directed to the App Store, and Windows Phone users to the Windows Phone store.

t a	Create Application Wizard
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 v Location: //play google com/store/apps/details?d=com.lookout.enterprise&hi=ent Example: https://play.google.com/store/apps/details?d=cox Manually specify the application information
	Activate Windows

 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.

t	Create Application Wizard	x
Import Informat	ion	
General	View imported information	
General Information		
Summary Progress Completion	Application information successfully imported from the App Package for Android on Google Play file.	
	Details: Application name: Application Name Publisher: Software version: Deployment type name: Application Name - App Package for Android on Google Play	<
	To modify any details from the imported information, click Next. To exit this wizard without creating the application, click Cancel.	
	Activate Windows	
< III >	< Previous Go to System in Control Por Next > cturate unmary control Por Cance	el to

2. Click Next.

t a	Crea	te Application Wizard	
General Information			
General Import Information General Information	Specify information a	bout this application	
Summary	Name:	Lookout Security For Work	
Progress Completion	Administrator comments:		
	Publisher:	Lookout Mobile Security	
	Software version:		
	Optional reference:		
	Administrative categories:	Select	
		Activate Windov	
		< Previous Next > Summary tive Cancel ws	
< III >			

385

386

384

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

t	Create Application Wizard	x
Summary		
General Import Information General Information Summary Progress Completion	Details General Information: Application name: Lookout Security For Work Administrator comments: Publisher: Lookout biole Security For Work Optimal reference: Optimal reference: Deprovement type name: Application Name - App Package for Android on Google Play Requirement rules:	
< III >	<pre>Activate Winting Go to System in C Summag(ctivate Cance)</pre>	ont

387

388

4. Click Next.



5. Click Close.

+	Deploy Software Wizard
General	
General Content Deployment Settings Scheduling User Experience Alerts Summary Progress Completion	Specify general information for this deployment Software: Lookout Security For Work Browse Collection: Al Users Browse Use default distribute point groups associated to this collection Browse Automatically distribute content for dependencies Comments (optional):
	<pre></pre>

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 Wizard
Content	
General Content Deployment Settings	Specify the content destination
Scheduling User Experience	Distribution points or distribution point groups that the content has been distributed to:
Alerts	Name Type
Summary	There are no items to show in this view.
Progress	
Completion	
	Additional distribution points, distribution point arouns, and the distribution point arouns that are surrently
	associated with collections to distribute content to:
	Filter P Add V
	Name Description Associations Remove
	There are no items to show in this view.
	Activate Wind
	< Previous Next > Summary G Scancel in Co
	activate Windows

395

7. Click Next.

•	Deploy Software Wizard
Deployment Set	tings
General Content Deployment Settings Scheduling User Experience Alerts Summary Progress Completion	Action: Install Image: Purpose: Available Image: Require administrator approval if users request this application Image: Purpose:
	Activate Windo < Previous Next > SummaryGo Scanceh in Correction Scanceho Sc

396

397

398

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

•	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.
Summary Progress Completion	Time based on: UTC v Schedule the application to be available at: 7/29/2015 v 2:40 PM
	<pre></pre>

9. Click Next.

*	Deploy Software Wizard		
User Experience			
General Content Deployment Settings	Specify the user expe devices	rience for the installation of this software on the selected	
Scheduling User Experience	Specify user experience setting	for this deployment	
Alerts	User notifications:	Display in Software Center and show all notifications	
Summary Progress Completion	When the installation deadline window: Software Installation System restart. (frequ Write filter handling for Windov Commit changes at de If this option is not sele	is reached, allow the following activities to be performed outside the maintenance ired to complete the installation) vs Embedded devices adline or during a maintenance window (requires restarts) acted, content will be applied on the overlay and committed later.	
		Activate Window < Previous Next > SummaryG Scarcel in Constitution	

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

•	Deploy Software Wizard					
Alerts						
General Content Deployment Settings	Specify Configuration Manager and Operations Manager alert options					
Scheduling	Configuration Manager generates alerts when this application is deployed.					
User Experience	Threshold for successful deployment					
Summary	Create a deployment alert when the threshold is lower than the following:					
Progress	Percent success: 1					
Completion	After: 8/ 5/2015 V 10:40 AM					
	Threshold for failed deployment					
	Create a deployment alert when the threshold is higher than the following:					
	Percent failure: 0					
	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 > SummaryGo Scancel, inc					

11. Click Next.

٠	Deploy Software Wizard	X
Summary		
General Content Deployment Settings Scheduling User Experience Alerts Summary Progress Completion	Details: Details: Details: Operating in colocut Security For Work Operating in colocut Security For Work Details: Details:	E Vinde
	activate W	lindows.

12. Click Next.



13. Click Close.

curity						
neral Information	Application Catalog	References	Distribution Settings	Deployment Types	Content Locations	Supersedence
opecify information formation in a sp	n about how you war ecific language, sele	t to display this ct the language	application to users whether before you enter a dest	nen they browse the A scription.	Application Catalog.	To provide
elected language	e: [English (United	States) default		¥ .	Add/Remove
	L					
Localized applica	ation name:	Lookou	t Security For Work			
User categories:		"Google	e Play App''			Edit
User documentat	tion:					Browse
Link text:						biowse
Privacy URL:]
Localized descrip	otion:					
						^
Keywords:						
lcon:						Browse
Display this as	a featured app and h	iahliaht it in the	company portal			



2	4.1	Device Enrollment with Office 365	92
3	4.2	Email Setup	.114
4	4.3	Lookout MTP Enrollment	130
5			

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

94.1 Device Enrollment with Office 365

10The following sections depict the enrollment process of an iOS and Android device to the11Intune enterprise mobility management service. The reader should note that the Intune service12will automatically redirect the user to the Intune tenant owner's authentication service based13on the domain part presented in the user's email address. The authentication service must be14accessible via the Internet if users enroll remotely. Otherwise, an organization must make its15authentication 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.⁹ This is not necessary for
 Windows Phone devices because MDM management through this service is native to the
 device.

^{9.}The URLs for iOS and Android devices are https://itunes.apple.com/us/app/microsoft-intune-company-portal/id719171358?mt=8 and https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal&hl=en respectively.





1. Download the company portal application from the App store and log in using Office 365 credentials.



Enroll Cancel

24

25

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

No SIM ᅙ	11:34 AM	* 💼
Cancel	Install Profile	Install
	Management Profile	
Signed by	IOSProfileSigning.manage.microso	oft.com
Description	Install this profile to get access to apps	your company
Contains	Device Enrollment Challenge	
More Det	ails	>

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.

No SIM 🗢	11:35 AM	* 🔤
Done	Compliance Details	
iPhone	e 6 8.3	
🚺 This c	levice is not in compliance.	
Last che	cked: Dec 31, 1, 7:03 PM	
This dev organiza your poli is in corr	ice does not comply with tion's policies. After you cy issues, check that you ppliance.	your esolve device
Complia	ince state is Unknown	~
	Check Compliance	

33

34

35

 To gain full access to company resources, the user will need to check their device for compliance. This screen will appear when the user taps on their device inthe company portal.

No SIM 🗢	11:35 AM 🛛 🖇 💳 🕨
Done	Device Details
	iPhone 6 8.3
few minu	compliance. This may take a tes.
Original Nam iPhone 6 8.	e: 3
Manufacture Apple	0
Model: iPhone 6	
Operating Sy iOS	rstem:
Policy comp Checking c Last check	iance status: ompliance ed: May 20, 2015, 11:35 AM
Reset	Temove Rename

6. The compliance checking process will take a couple of minutes. The user can minimize the application during the compliance checking process.



41

7. Upon minimizing the company portal application during the compliance checking process, 40 the user is presented with the password remediation process, alerting the user to change their password within the hour. 42

No SIM 중	10:14 AM	* 🖚
Done	Device Details	
	iPhone 6 8.3	
This device policy.	ce is compliant with se	ecurity
Original Nam iPhone 6 8.	ie: 3	
Manufacture Apple	n	
Model: iPhone 6		
Operating Sy iOS	vstem:	
Policy compl In complian Last checke	iance status: ice ed: May 20, 2015, 1	0:13 AM
ی۔ Reset	Remove Ren	ame

8. After meeting compliance, the user's device should be listed in the company portal like the example above.

46 **4.1.2** Android

47



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 enrolling your device

Cancel Next	
-------------	--

1. After launching the Company Portal, Click **Next**.


50

2. Enter your email address.



3. If implementing a hybrid architecture, you will be redirected to your enterprise login site to enter your password. Click **Sign In**.



55

4. No action required.



57

5. No action required.



59

6. Click Activate to allow remote management of the device.

60 4.1.3 Windows Phone 8.1

ه (ر) کې	workplace	5:59
	Microsoft Intune	
	Sign in with your work or school account	
	msteele@cmdsbb.org	
	•••••	
	☐ Keep me signed in Sign in	
	Can't access your account?	

61

First the user must workplace join their device. Navigateto Settings -> System tab ->
 Workplace on Windows Phone 8.1 devices, or Settings -> System tab -> Company apps on
 Windows Phone 8 devices.



66

67

68

 The workplace application will attempt to connect to your company's management portal. In our case it did not find the server. We used manage.microsoft.com, the main portal for all Microsoft's Web management for Office365 and Intune.



70

71

72

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



4. Upon logging in to 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 checking the compliance manually (less than 5 minutes), the user's device is fully enrolled and should have the appropriate policies deployed.



6. How a compliant and fully enrolled device should look.

0 6.

3:40 You are receiving this message because your IT department requires that you take action in order to access Exchange email. This helps to protect corporate information in your organization.

You need to take the following actions in addition to any guidance received from your IT department:

1. Enroll your device (you may have already done this)

Enrolling this device involves signing in with your corporate credentials in the Workplace settings. Skip this step if Workplace settings says your device is already enrolled.

2. Check here to see if this device is compliant

You may need to set a passcode and enable encryption. By ensuring that all devices are compliant, you help your company protect its information.

3. Click here to activate your email

Once you know your device is compliant, click here to activate your email. If you've just recently enrolled, you may need to wait a couple of minutes to activate your email. Activating your email helps your company to keep track of devices accessing corporate information.

Please contact your IT department with any questions or problems.



81

82 83 7. Once compliance had been met the, user should be able to tap the activation link to activate their email access.

Activate Email for Your Device
Success
We have successfully activated email for this device.
It may take a few minutes before you are able to receive email. You may close this web page and return to your mail app.
TECHNICAL DETAILS



86

87

🕞 🔒 enterpriseregistration.wir 🗸

 The activation link will open a browser, and upon successful activation the user should be directed to this page. At this point the user should have full access to exchange email/contacts/calendar.

884.2 Email Setup

This 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 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 those applications.

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

97 **4.2.1** iOS



98

99 100

101

 When the user first opens the settings application either before/during/after the compliance check, they are prompted for their Office365 password for the exchange profile that is provisioned during the on-boarding process. This is a one-time occurrence.

0 SIWI 🕈	10:13 AM	* 💼
Mailboxes	Inbox	Edit
	Q Search	
Microsoft Ou Action require This email was Microsoft Excl	utlook d to access your of s automatically ge hange. You are red	10:13 AM > organization's nerated by ceiving this m

103

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

Action required to access your organization's email on your mobile device May 20, 2015 at 10:13 AM This email was automatically generated by Microsoft Exchange. You are receiving this message because your IT department requires that you take action in order to access Exchange email. This helps to protect corporate information in your organization. You need to take the following actions in addition to any guidance received from your IT department: I. <u>Enroll your device</u> (you may have already done his) Enrolling this device involves installing the Microsoft ntune Company Portal app and signing in with your corporate credentials. Skip this step if you already have the Microsoft Intune Company Portal app nstalled. 2. <u>Check here to see if this device is compliant</u> You may need to set a passcode, enable encryption, and change your email configuration.	Microsoft Outlook To: Matt Steele more		
This email was automatically generated by Microsoft Exchange. You are receiving this message because your IT department requires that you take action in order to access Exchange email. This helps to protect corporate information in your organization. You need to take the following actions in addition to any guidance received from your IT department: I. <u>Enroll your device</u> (you may have already done his) Enrolling this device involves installing the Microsoft ntune Company Portal app and signing in with your corporate credentials. Skip this step if you already have the Microsoft Intune Company Portal app nstalled. 2. <u>Check here to see if this device is compliant</u> You may need to set a passcode, enable encryption, and change your email configuration.	Action required to organization's em May 20, 2015 at 10: ⁻	access you ail on your r 13 AM	ır nobile device
You are receiving this message because your IT department requires that you take action in order to access Exchange email. This helps to protect corporate information in your organization. You need to take the following actions in addition to any guidance received from your IT department: I. <u>Enroll your device</u> (you may have already done his) Enrolling this device involves installing the Microsoft ntune Company Portal app and signing in with your corporate credentials. Skip this step if you already have the Microsoft Intune Company Portal app nstalled. 2. <u>Check here to see if this device is compliant</u> You may need to set a passcode, enable encryption, and change your email configuration.	This email was automa Microsoft Exchange.	atically generate	ed by
You need to take the following actions in addition to any guidance received from your IT department: 1. <u>Enroll your device</u> (you may have already done his) Enrolling this device involves installing the Microsoft ntune Company Portal app and signing in with your corporate credentials. Skip this step if you already have the Microsoft Intune Company Portal app nstalled. 2. <u>Check here to see if this device is compliant</u> You may need to set a passcode, enable encryption, and change your email configuration.	You are receiving this r department requires th access Exchange ema corporate information	message becau at you take ac il. This helps to in your organiz	use your IT tion in order to protect ation.
Enroll your device (you may have already done his) Enrolling this device involves installing the Microsoft ntune Company Portal app and signing in with your corporate credentials. Skip this step if you already have the Microsoft Intune Company Portal app installed. Check here to see if this device is compliant four may need to set a passcode, enable encryption, and change your email configuration. Pure and the set of the se	You need to take the fo any guidance received	ollowing action from your IT d	s in addition to lepartment:
2. <u>Check here to see if this device is compliant</u> You may need to set a passcode, enable encryption, and change your email configuration.	1. <u>Enroll your device</u> (y this) Enrolling this device in Intune Company Porta corporate credentials. have the Microsoft Intu installed.	ou may have a volves installin I app and signi Skip this step i ine Company F	Iready done g the Microsoft ing in with your if you already Portal app
by ensuring that all devices are compliant, you help	2. <u>Check here to see if</u> You may need to set a encryption, and chang By ensuring that all de	this device is of passcode, ena e your email co vices are comp	compliant able onfiguration. bliant, you help

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



108

4. After activating their email, the user will be presented with this confirmation page.

4.2.2 Android



1. Open the Outlook application on your device.



2. Choose **Office 365**.



115

3. Log in with your enterprise credentials.

<u> </u>						\otimes	🕈 🛛 I	10:20
ΗM	1DSI	3B						
Sign i	n with yo	our orga	anizatio	onal acc	count			
jkirk(0hmdsb	b.org						
	۰							
Siq © 2013	<mark>gn in</mark> Microsoft							
q ¹ \	N ² 6	è r	• 1	t⁵)	, ι	7	i [®] c	⁹ p ⁰
а	S	d	f	g	h	j	k	I
	Z	Х	С	V	b	n	m	×
?123	,							Ð
	∇			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.





120

5. If your device has not been enrolled with the MDM, you will be prompted to do so.



You need to make changes to your device to comply with security policies before you can access your organization's resources. Click Details to see what changes are needed.

Details Cancel

121

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



7. The device owner will be granted access to Office 365 after the device complies with policy.

126 4.2.3 Windows Phone 8.1



127

1281.To get full access to exchange resources, as well as email, use the built-in email client to add129an exchange account. In the email client, tap the three horizontal dots on the bottom right130and tap Add an account to bring up the account select page. Or under Settings -> Email +131Accounts, you can add your Office365 exchange account credentials.



2. Log in using your Office365 credentials. The server info should auto-populate.

0 6 **3:39** Microsoft Outlook Action required to access your organization's email on your mobile device Thu 5/14, 3:35 PM To: Matt Steele This email was automatically generated by Microsoft Exchange. You are receiving this message because your IT department requires that you take action in order to access Exchange email. This helps to protect corporate information in your organization. You need to take the following actions in addition to any guidance received from your IT department: 1. Enroll your device (you may have already done this) Enrolling this device involves signing in with your corporate credentials in the Workplace settings. Skip this step if Workplace settings says your device is already enrolled. 2. Check here to see if this device is compliant You may need to set a passcode and enable encryption. By ensuring that all devices are ••• →

134

Upon successfully syncing the exchange account, the user should receive an email shortly
 thereafter explaining the enrollment process and requesting that the user enroll/check for
 compliance.

138 4.2.4 Windows 8.1

Intune with SCCM integration does not support email profiles for Windows 8.1, so email must
 be configured using another method.

Cutlent spec messages	Hmdsb	b	Inbo All ~	ox							م (+
Curle Solution Color Colo		~	Couldn't	sync me	ssages						
Source Image: Source	orans.										
Color	Sent										
Control of the second seco	Folders										
Clocket your Hindsbb account Update your Hindsbb account We can't you because your account into has changed. Update it and we'll try again. Image: Stream of the second s	2										
Update your Hmdsbb account Image: Compare the sector of the sector o	P										
We can't sync because your account into has changed. Update it and we'll try again. Email address juikit[hind]sborg Password Show more details Update Cancel	ų	Jpdate	your	Hmds	sbb a	ccoun				du.	
Email address juik @hmdsbb.org Password	. W	le can't sync	: because	vour acco	unt info h	as change	rd. Update	it and we	'll try agair	n.:	
jkirk@hmdsbb.org Pastword Show more details Update Cancel	6	nail address	6			1			0.5		
Pastword Show more details Update Cancel	[jkirk@hmds	bb.org								
Show more details Update Cancel	P	assword									
Show more details Update Cancel											
Update Cancel	5	how more d	etals								
							Up	date	Cance	L	
2 2 2 4 2 4 7 1 1 1 1 1											
1 2 3 4 5 6 7 B 1 0				_					-	_	
qwertyuiop 💌	q w	e	r	t	́у	u			p	Ø	
						T	-	T	T	T	
asdfghjkl' 44	a s	d	f	9	h	j	k	ļ,			ę
↑ z x c v b n m , . ? ↑	↑ z	×	c	v	ь	n	m		(n)		†
				-	n i	ir is	-	-	_		

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.

E	S	(+)	
Microsoft Outlook to James T. Kirk	F	ri, May 8	11:54 AM
Action required to access your organization's email of device	n your m	obile	Þ
This email was automatically generated by Microsoft Exchange. You are receiving this message because your IT department requires that you take action in order to access Excha helps to protect corporate information in your organization.	inge email. This		
You need to take the following actions in addition to any guidance received from your IT department:			
 Enroll your device (you may have already done this) Enrolling this device involves signing in with your corporate credentials in the Workplace settings. Skip this step if V says your device is already enrolled. 	Workplace settings		
 Check here to see if this device is compliant You may need to set a passcode and enable encryption. By ensuring that all devices are compliant, you help your information. 	company protect it	5	
3. Click here to activate your email Once you know your device is compliant, click here to activate your email. If you've just recently enrolled, you may couple of minutes to activate your email. Activating your email helps your company to keep track of devices access information.	y need to wait a sing corporate		
Please contact your IT department with any questions or problems.			

 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.

148 4.3 Lookout MTP Enrollment

← → C 🔒	Lookout, Inc. [US] https://mtp.lookou	t.com/les/devices/enr	oll
8	🛾 Devices 👤 Enroll 🛛	⊴ Invites	
	Enroll Devices		
✓ Dashboard	To invite employees to activate Lookout by commas or semicolons.	for Work on the their mobile	devices, either import a .csv consisting of just or
	IMPORT EMAILS FROM A .CSV	or	Enter emails separated by comm
Threats			ADD ADDRESSES
Devices			

149

150

151

152

- 1. Open the Lookout MTP administrative console with a browser. Navigate to
 - https://mtp.lookout.com/les/devices/enroll and type the target user's email address into the provided Web field.

	8
	8
Protect	t yourself from mobile threats
NIST - National Institu	ute of Standards and Technology has partnered with Lookout to
Please click the butt	eo protection and security for your mobile devices.
phone.	
	Install Lookout for Work
Just launch the app w any trouble, try using	Install Lookout for Work then you're ready to activate protection for your device. If you have this code:
Just launch the app w any trouble, try using	Install Lookout for Work then you're ready to activate protection for your device. If you have this code:

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

156 4.3.1 Android



157

158

1. Find the MTP application in the Play store by searching **lookout**.



159 160

2. Select the Lookout Security for Work application and tap Install.



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 user's device.



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

Appendix A Acronyms

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

34	MDM	Mobile Device Management
35	MDS	Mobile Device Security
36	MMS	Multimedia Messaging Service
37	MTP	Mobile Threat Protection
38	NCCoE	National Cybersecurity Center of Excellence
39	NCEP	National Cybersecurity Excellence Partnership
40	NIAP	National Information Assurance Partnership
41	NIST	National Institute of Standards and Technology
42	NSA	National Security Agency
43	NVD	National Vulnerability Database
44	OS	Operating System
45	PII	Personally Identifiable Information
46	PIV	Personal Identity Verification
47	RFTC	Request for Technical Capabilities
48	RMF	Risk Management Framework
49	SaaS	Software as a Service
50	SAML	Security Assertion Markup Language
51	SANS	Sysadmin, Audit, Networking, and Security
52	SCCM	Systems Center Configuration Manager
53	SMS	Short Message Service
54	SoC	System on a Chip
55	SP	Special Publication
56	TEE	Trusted Execution Environment
57	TLS	Transport Layer Security
58	TPM	Trusted Platform Module
59	UDID	Unique Identifier
60	US-CERT	United States Computer Emergency Readiness Team
61	WAP	Web Application Proxy

Appendix B References

2 [1]	IDC, Android and iOS Squeeze the Competition, February 24, 2015. http://www.idc.com/
3	getdoc.jsp?containerId=prUS25450615 [accessed 6/19/2015].
4 [2]	Microsoft, Plan for third-party SSL certificates for Office 365, https://support.office.com/en-sg/
5	article/Plan-for-third-party-SSL-certificates-for-Office-365-b48cdf63-07e0-4cda-8c12-
6	4871590f59ce?ui=en-US&rs=en-SG&ad=SG [accessed October 14, 2015].
7 [3]	Microsoft, Understanding Certificate Requirements, November 08, 2011. https://
8	technet.microsoft.com/library/gg476123.aspx [accessed October 14, 2015].
9 [4]	Microsoft, Install Active Directory Domain Services (Level 100), April 14, 2014. https://
10	technet.microsoft.com/en-us/library/hh472162.aspx [accessed October 14, 2015].
11 [5]	Microsoft, Mobile device security policy settings in Microsoft Intune, October 8, 2015. https://
12	technet.microsoft.com/en-us/library/dn913730.aspx [accessed October 14, 2015]
13 [6]	Microsoft, How To Install ADFS 2012 R2 For Office 365, April 28, 2014. http://
14	blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-
15	365.aspx [accessed October 14, 2015]
16 [7] 17 18	Microsoft, Office 365 and ADFSActive Directory Federation Service Installation, November 13, 2013. http://social.technet.microsoft.com/wiki/contents/articles/9082.office-365-and-adfs-active-directory-federation-service-installation.aspx [accessed October 14, 2015].
19 [8] 20	Microsoft, Test Lab Guide: System Center 2012 Configuration Manager, July 30, 2012. http://www.microsoft.com/en-us/download/details.aspx?id=30443 [accessed October 14, 2015].
21 [9]	Microsoft, Azure Active Directory Sync, July 22, 2015. https://msdn.microsoft.com/en-us/
22	library/azure/dn790204.aspx [accessed October 14, 2015].
23 [10] 24 25	Microsoft, Geek of All Trades: Office 365 SSO: A Simplified Installation Guide, https:// technet.microsoft.com/en-us/magazine/jj631606.aspx [accessed October 14, 2015].