

NIST CYBERSECURITY PRACTICE GUIDE

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

How-To Guide

for Security Engineers

Joshua Franklin Kevin Bowler

Christopher Brown

Sallie Edwards Neil McNab

Matthew Steele

NIST SPECIAL PUBLICATION 1800-4c

DRAFT



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

DRAFT

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-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

1 Contents

2	1 Introduction.....	1
3	1.1 Practice Guide Structure.....	2
4	1.2 Build Overview	3
5	1.3 Typographical Conventions	4
6	2 How to Build a Cloud-Based Solution to Mobile Device Security.....	5
7	2.1 Cloud Build Setup and Configuration.....	5
8	2.1.1 Cloud Build Components	5
9	2.1.2 Office 365 Setup	6
10	2.1.3 Office 365 MDM Setup	16
11	2.1.3.1 Configure Push Certificate for iOS Devices	21
12	3 How to Build an On-Premises Solution for Mobile Device Security	29
13	3.1 Hybrid Build Setup and Configuration.....	30
14	3.2 Hybrid Detailed Architecture	30
15	3.2.1 Hybrid Build Components	32
16	3.2.2 Enterprise Network and Firewall	33
17	3.2.3 Enterprise Software Components for Hybrid	36
18	3.2.3.1 Active Directory Domain Services	36
19	3.2.3.2 Active Directory Federation Service	37
20	3.2.3.3 Active Directory Federation Services Proxy	39
21	3.2.3.4 Systems Center Configuration Manager	39
22	3.2.3.5 Azure Active Directory Sync Services	39
23	3.2.4 Cloud Services Instances	39
24	3.2.4.1 Office 365 Setup.....	39
25	3.2.4.2 Intune Setup	40
26	3.2.4.3 Lookout Setup	42
27	3.2.5 Hybrid Integration	43
28	3.2.5.1 Office 365 with Active Directory Federation Setup.....	43
29	3.2.5.2 Azure Active Directory Sync Services	43
30	3.2.5.3 Sync Intune with Office 365 Exchange.....	48
31	3.2.5.4 Manage Intune with SCCM	48
32	3.2.5.4.1 Configure Active Directory User Discovery	49
33	3.2.5.4.2 Register SCCM with Intune	51
34	3.2.5.4.3 Configure Push Certificate for iOS Devices	60
35	3.2.5.4.4 Mobile Policy Creation.....	64
36	3.2.5.4.5 Create Mobile Application Policy.....	76
37	3.2.5.5 Configure SCCM with Lookout Application	83
38	4 Device Configuration.....	91
39	4.1 Device Enrollment with Office 365	92
40	4.1.1 iOS.....	93

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 Lookout MTP Enrollment	130
49	4.3.1 Android	132
50	Appendix A Acronyms	135
51	Appendix B References	137
52		
53		

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.....	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
65		
66		

67 **List of Tables**

68	Table 1.1 Typographical Conventions	4
69	Table 2.1 Cloud Build Components	5

70	Table 3.1 Components	32
71	Table 3.2 Enterprise Software Components	36

72

1 Introduction

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

6 The following guides show IT professionals and security engineers how we implemented this
7 example solution to the challenge of securing email, contacts and calendaring in mobile
8 devices. We cover all the products that we employed in this reference design. We do not
9 recreate the product manufacturer's documentation, which is presumed to be widely available.
10 Rather, these guides show how we incorporated the products together in our environment.

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

13 1.1 Practice Guide Structure

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

17 Depending on their roles in an organization, different people will use this guide in different
18 ways.

19 This guide contains three volumes:

- 20 ■ NIST SP 1800-4a: Executive Summary
- 21 ■ NIST SP 1800-4b: Approach, Architecture, and Security Characteristics - what we built and
22 why
- 23 ■ NIST SP 1800-4c: How-To Guides - instructions for building the example solution (you are
24 here)

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

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

- 28 ■ challenges enterprises face in implementing and using mobile devices
- 29 ■ example solution built at the NCCoE
- 30 ■ benefits of adopting the example solution

31 **Technology or security program managers** who are concerned with how to identify,
32 understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP
33 1800-4b, which describes what we did and why. The following sections will be of particular
34 interest:

- 35 ■ Section 4.3, Risk Assessment, provides a detailed description of the risk analysis we
36 performed.
- 37 ■ Section 4.4, Security Characteristics and Controls Mapping, maps the security
38 characteristics of this example solution to cybersecurity standards and best practices.

39 You might share the Executive Summary, NIST SP 1800-4a, with your leadership team members
40 to help them understand the importance of adopting standards-based enterprise mobility
41 management (EMM) approaches to protect your organization's digital assets.

42 IT professionals who want to implement an approach like this will find the whole practice guide
43 useful. You can use the How-To portion of the guide, NIST SP 1800-4c, to replicate all or parts of
44 the build created in our lab. The How-To guide provides specific product installation,

45 configuration, and integration instructions for implementing the example solution. We do not
46 re-create the product manufacturers' documentation, which is generally widely available.
47 Rather, we show how we incorporated the products together in our environment to create an
48 example solution.

49 This guide assumes that IT professionals have experience implementing security products
50 within the enterprise. While we have used a suite of commercial products to address this
51 challenge, this guide does not endorse these particular products. Your organization can adopt
52 this solution or one that adheres to these guidelines in whole, or you can use this guide as a
53 starting point for tailoring and implementing parts of a solution that would support the
54 deployment of mobile devices and the corresponding business processes. Your organization's
55 security experts should identify the products that will best integrate with your existing tools
56 and IT system infrastructure. We hope you will seek products that are congruent with
57 applicable standards and best practices.

58 A NIST Cybersecurity Practice Guide does not describe *the* solution, but a possible solution. This
59 is a draft guide. We seek feedback on its contents and welcome your input. Comments,
60 suggestions, and success stories will improve subsequent versions of this guide. Please
61 contribute your thoughts to mobile-nccoe@nist.gov, and join the discussion at
62 <https://nccoe.nist.gov/forums/mobile-device-security>.

63 1.2 Build Overview

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

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

79 1.3 Typographical Conventions

80 The following table presents typographic conventions used in this volume.

81 **Table 1.1 Typographical Conventions**

Typeface/ Symbol	Meaning	Example
<i>Italics</i>	references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, command buttons and fields	Choose File > Edit .
Courier	command-line input, on-screen computer output, sample code examples, status codes	<code>mkdir</code>
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

¹ **2** How to Build a Cloud-Based Solution to Mobile Device Security²

³ **2.1** Cloud Build Setup and Configuration

⁴ The following How-To will guide an implementer through the process of creating and
⁵ configuring the cloud architecture depicted below. No software resources are necessary for this
⁶ build because it is completely cloud based. The only hardware requirement is that the
⁷ organization that implements this build uses mobile devices that are compatible with the cloud
⁸ MDM. This building block chose to use mobile devices running iOS, Android, and Windows
⁹ 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.

¹⁴ The implementer will also need access to an Apple developer account to generate a push
¹⁵ notification certificate for iOS devices. A push certificate allows the Office365 instance to send
¹⁶ push notifications to enrolled devices. Refer to the Apple website for pricing information and
¹⁷ more details regarding certificates².

¹⁸ Further, during the configuration of the Office365 MDM you will be prompted to allow or block
¹⁹ devices from Office365 that cannot be managed. This can occur when a user has a device with
²⁰ an unsupported operating system. Select **Block** during this step to enhance the security of
²¹ Office365 services.

²² Finally, we have chosen in this simple cloud build to leverage the MDM capabilities that are
²³ available within Office365. This offers a more limited feature set than what is available through
²⁴ the Intune MDM service. Implementers looking for more capabilities should consider the
²⁵ Intune portion of the Hybrid How-To guide.

²⁶ **2.1.1** Cloud Build Components

²⁷ Table 2.1 lists the components used for this building block:

²⁸ **Table 2.1** Cloud 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

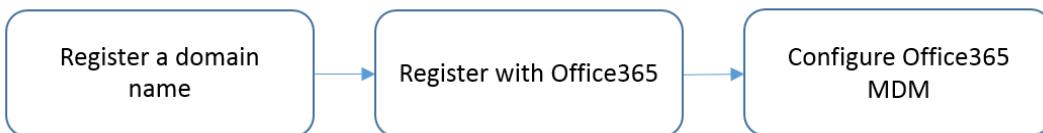
¹[1.https://www.icann.org/registrar-reports/accredited-list.html](https://www.icann.org/registrar-reports/accredited-list.html)

²[2. https://developer.apple.com/](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, Cloud Build Process](#). The following sections in the How-To guide will focus on the second and third steps.

Figure 2.1 Cloud Build Process

2.1.2 Office 365 Setup

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

To start the process, use a Web browser to access the following URL:

<https://products.office.com/en-us/business/office-365-enterprise-e3-business-software>

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.

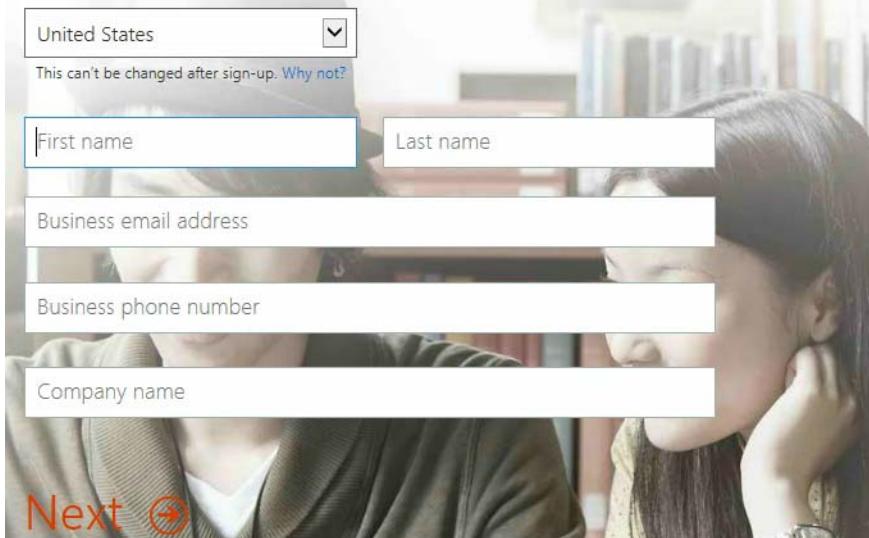
\$20.00 user/month
annual commitment

Buy now

Free trial →

1. Choose a commitment level.

Welcome, Let's get to know you



42

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



43

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

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

Creating your account...

44

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

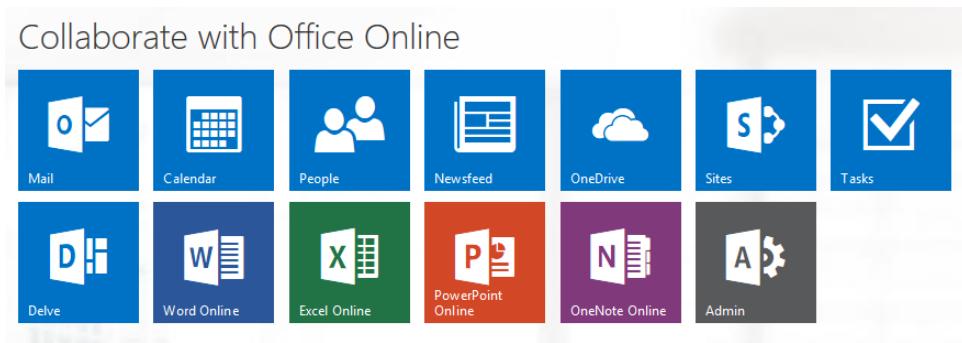
Your Office 365 user ID
nmcnab@cmdssbb.onmicrosoft.com

★ Bookmark the sign-in page

You're ready to go... ➔

45

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



47

- 48 3. Choose Admin from the set of services.

A screenshot of the Microsoft Office 365 Admin Center dashboard. The left sidebar shows a navigation menu with sections like DASHBOARD, SETUP, USERS, COMPANY PROFILE, CONTACTS, SHARED MAILBOXES, MEETING ROOMS, GROUPS, DOMAINS, PUBLIC WEBSITE, BILLING, EXTERNAL SHARING, SERVICE SETTINGS, REPORTS, SERVICE HEALTH, SUPPORT, PURCHASE SERVICES, MESSAGE CENTER, TOOLS, and ADMIN. Under ADMIN, there are links for Exchange, Lync, SharePoint, Compliance, Azure AD, and Bing Places for Business. The main content area has sections for Service overview, Current health (listing Exchange, Identity Service, Lync, Office 365 Portal, Office Subscription, Rights Management Service, SharePoint, and Yammer Enterprise), and Included services. On the right side, there are admin shortcuts (Reset user passwords, Add new users, Assign user licenses, Download software), resources (Working with domain names, Setting up mobile devices, Setting up user permissions in SharePoint, Office 365 Admin Help, Known issues, Information on Yammer), and community links (Ask a question in the forums, Check out our blog, Participate in the community).

49

- 50 4. In the next steps we will configure the domain name with Office 365. Choose the **Domains** option.
- 51

The screenshot shows the 'Manage domains' page in the Microsoft 365 admin center. At the top, there are two buttons: '+ Add domain' and 'Buy domain'. Below is a table with columns: DOMAIN NAME, STATUS, and ACTION. One row is selected, showing 'cmdssbb.onmicrosoft.com (Default)' with 'Setup complete' status and 'No action required' in the ACTION column. To the right of this row, there is a link 'Manage DNS'.

DOMAIN NAME	STATUS	ACTION
cmdssbb.onmicrosoft.com (Default)	Setup complete	No action required

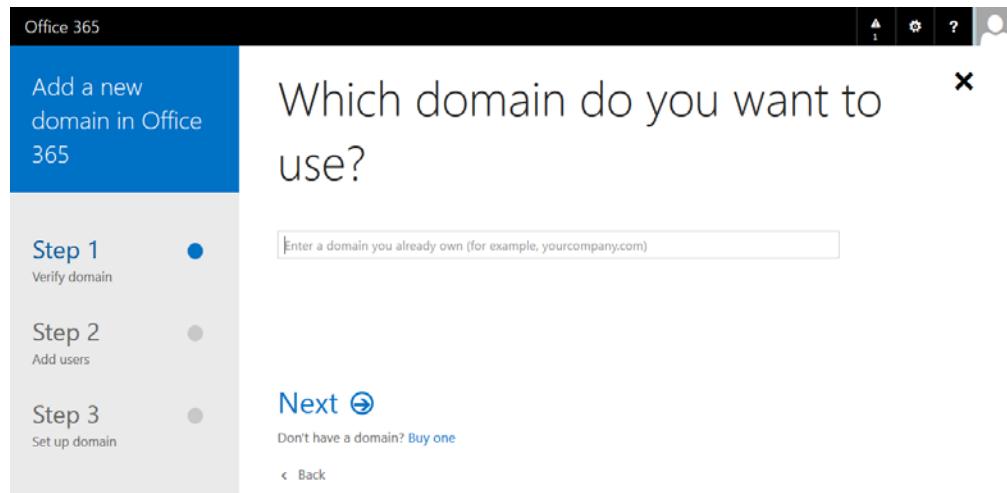
52

- 53 5. Choose **Add domain**.

The screenshot shows the 'Add a new domain in Office 365' wizard. On the left, a sidebar lists 'Step 1 Verify domain', 'Step 2 Add users', and 'Step 3 Set up domain'. The main content area is titled 'What you need to know about domains and DNS'. It explains that a domain name identifies a school or business on the internet, provides examples of email and URLs, and describes how DNS directs email to a mailbox. A 'Let's get started' button is at the bottom.

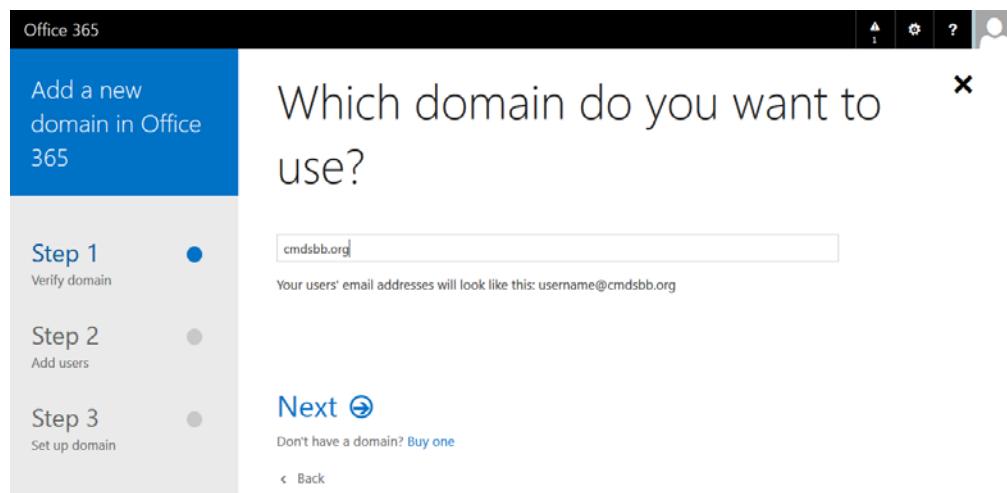
54

- 55 6. Choose **Let's get started**.



56

- 57 7. Enter your public domain name.



58

- 59 8. Choose **Next**.

Add this TXT record to show you own cmdsb.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.

```

C:\> nslookup
Default Server: hawk.nist.gov
Address: 129.6.16.1

> set type=txt
> cmdsb.org
Server: hawk.nist.gov
Address: 129.6.16.1

Non-authoritative answer:
cmdsb.org      text =
    "MS=ms37771077"
cmdsb.org      text =
    "v=spf1 include:spf.protection.outlook.com -all"

cmdsb.org      nameserver = be8.nist.gov
cmdsb.org      nameserver = gea.nist.gov
cmdsb.org      nameserver = bea.nist.gov
bea.nist.gov   internet address = 132.163.4.10
bea.nist.gov   AAAA IPv6 address = 2610:20:6b01:4::10
gea.nist.gov   internet address = 129.6.13.3
gea.nist.gov   AAAA IPv6 address = 2610:20:6005:13::3
>

```

63

- 64 10. Verify the Domain Name Service (DNS) settings. The TXT record should match what was
65 presented in the previous step. Note that it may take several minutes for the record to
66 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 

67

- 68 11. Choose **Next**.

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

Select the users you want to update from cmdsb.onmicrosoft.com to cmdsb.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.

<input checked="" type="checkbox"/>	Name	Current email address	Email address after update
	Neil		
<input checked="" type="checkbox"/>	McNab (this is you)	nmcnab@cmdsb.onmicrosoft.com	nmcnab@cmdsb.org

Update selected users

69

12. Choose **Update selected users**.

70

Sign out to complete the change

Sign out, and then sign in using nmcnab@cmdsb.org. Don't worry, we'll bring you right back here to continue setting up.

[Sign out](#)

71

72

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?](#)

Next 

73

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 

75

15. Choose **Next**.

Which services do you want to use with cmdsb.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 required for your Office 365 services to work on cmdsb.org. [How do DNS records work?](#)

Next →

77

16. Choose **Next**.

Add the following DNS records for cmdsb.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	@	cmdsb.org.mail.protection.outlook.com	3600

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

79

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

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

Okay, I've added the records →

80

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

83 **2.1.3 Office 365 MDM Setup**

84 In the next section, you will be guided through the device management setup through Office
 85 365.

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

87

- 88 1. Choose **Get Started**.

The screenshot shows the 'Groups' section of the Office 365 Admin Center. On the left, a sidebar lists various administrative tasks, with 'GROUPS' currently selected. The main area displays a table with one row, showing a user named 'NCCoE Operators' with the email address 'NCCoE@cmdsbb.org' and the status 'In cloud'. A message at the top right encourages activating Windows. The bottom right corner shows the date and time as '5/14/2015 5:30 PM'.

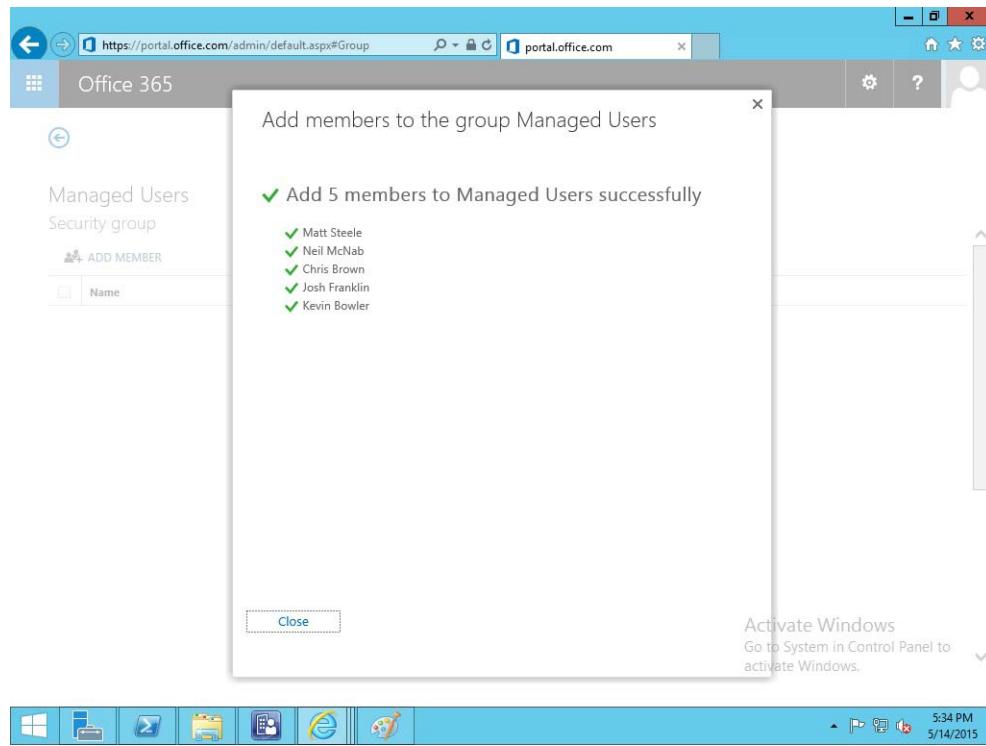
89

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

The screenshot shows the 'Create security group' dialog box. It has fields for 'Group name' (containing 'Managed Users') and 'Description' (containing 'Managed mobile device users'). At the bottom are 'Create' and 'Cancel' buttons. The background shows the same Admin Center interface as the previous screenshot, with the 'Groups' section active.

92

- 93 3. Add a title and description for the group.



94

95

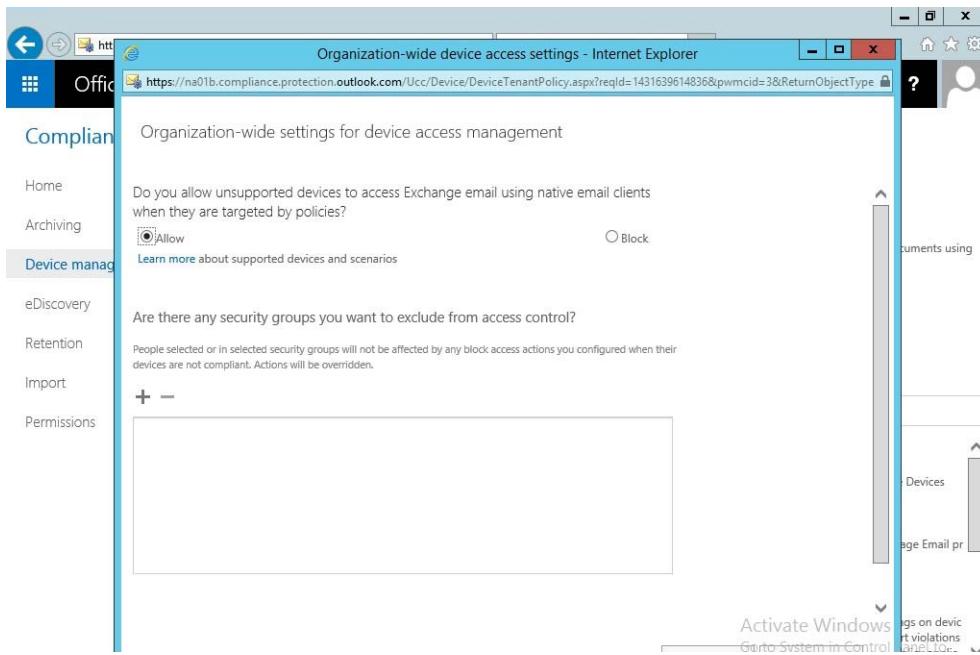
4. Add members to the group to be managed.

The screenshot shows the 'Mobile device management' section of the Compliance Center. On the left, a sidebar lists 'Home', 'Archiving', 'Device management' (which is selected), 'eDiscovery', 'Retention', 'Import', and 'Permissions'. The main area shows a table for policies, with one entry: 'Baseline Policy for Mobile Devices' (Status: On, Modified on: 5/14/2015 12:...). To the right, detailed settings for this policy are shown, including 'Name' (Baseline Policy for Mobile Devices), 'Description' (Require a password, Manage Email profiles, disable camera), and 'Settings' (Configure following settings on devices. Block access and report violations). A note at the bottom states: 'Go to System in Control Panel to activate Windows. Devices that have this policy applied are not compliant with these settings.' The taskbar at the bottom indicates it's 5:38 PM on 5/14/2015.

96

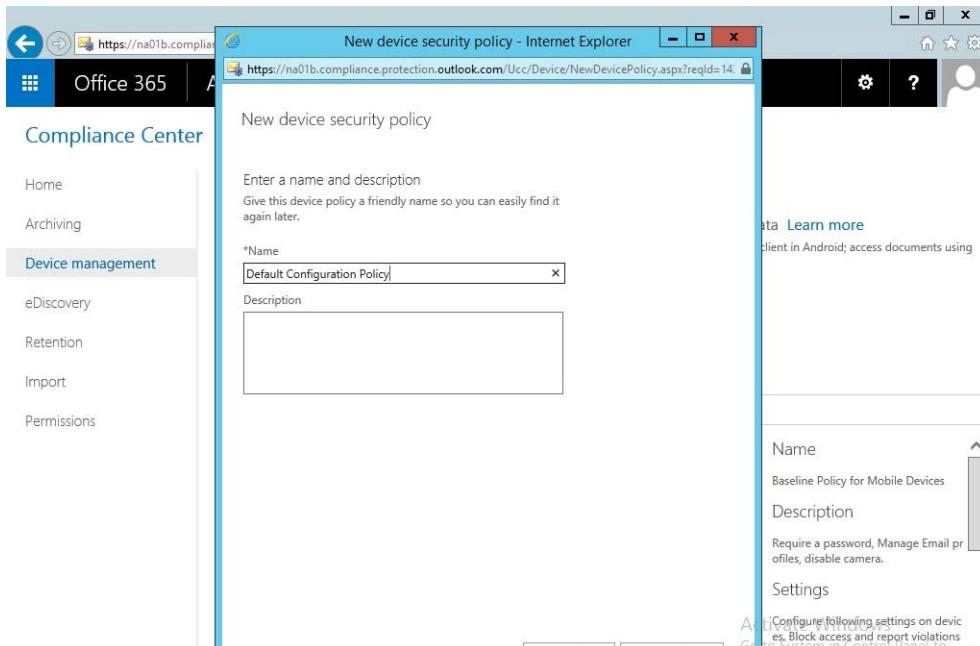
97
98

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



99

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



101

- 102 7. Set the name for the device policy.

103

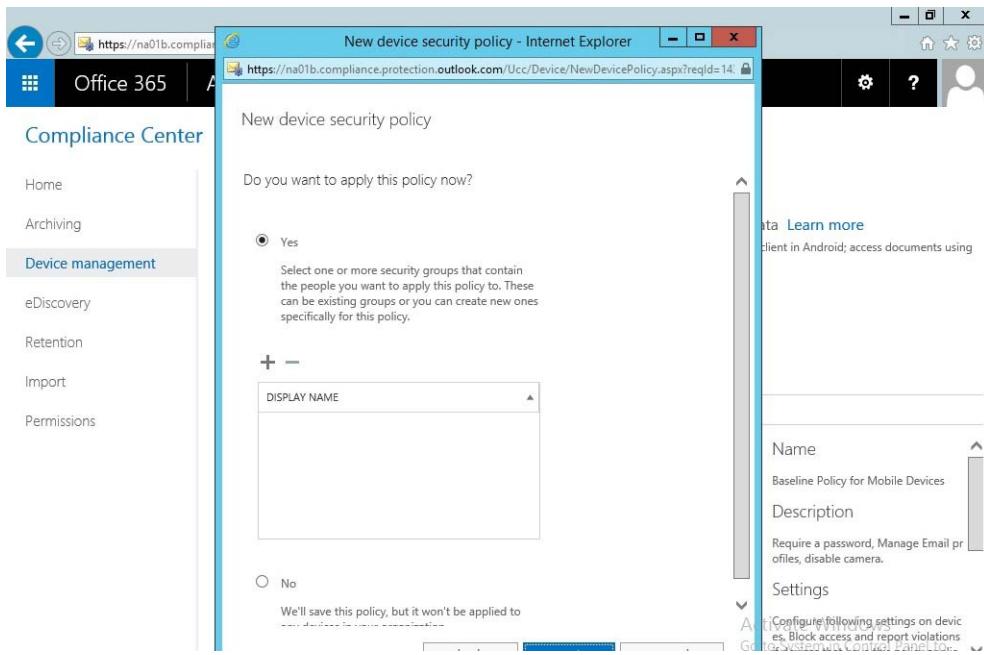
104

8. Set rules for the device policy.

105

106

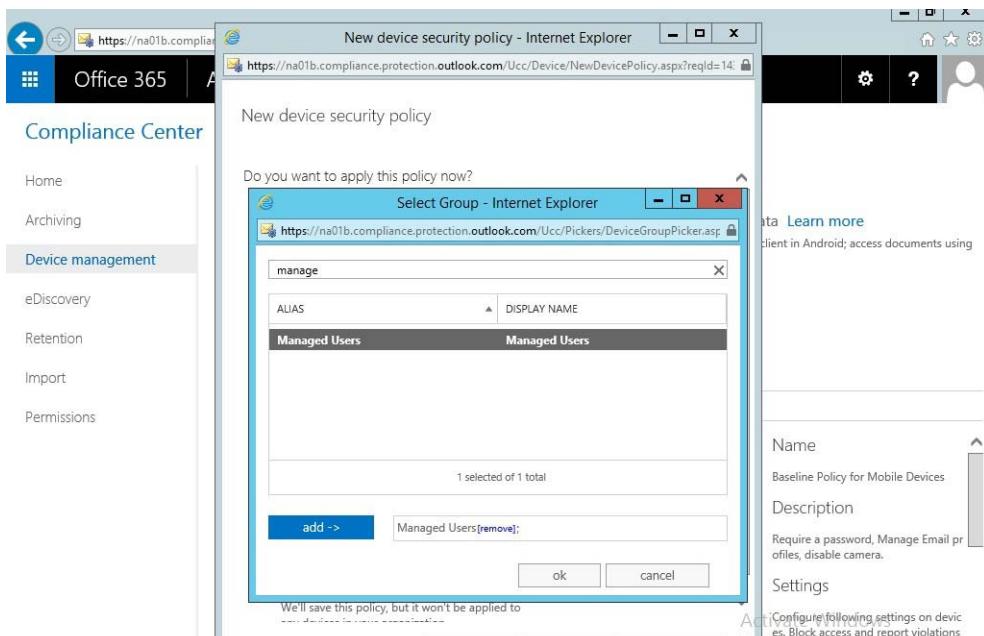
9. Set additional hardware restrictions.



107

108

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



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.

Mobile Device Management for Office 365

The following mobile devices have been enrolled in Mobile Device Management by users in your tenant. You can view device properties, access reports, wipe devices and enforce device security policies.

Manage device security policies and access rules
See device compliance report

Select a view: All

DEVICE NAME	OPERATING SYSTEM	OS VERSION
Matt Steele - iPhone 6 8.3	iPhone	8.3
Matt Steele - msteele_Android_5/1...	Android	5.1
Matt Steele - msteele_WindowsPho...	WindowsPhone	8.10.14219.341

Settings

- APNs Certificate for iOS devices

Manage settings

Full wipe Selective wipe
Learn more about full vs. selective wipe.

Status: Windows Managed
Go to System in Control Panel to activate Windows.
Device Model Lumia 830

Feedback

114

115

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

Set up mobile device management

There are a few steps to complete before you can start using mobile device management (MDM) in your organization.

Required steps

- Configure domains for MDM [Set up | Learn more](#)
- Configure an APNs Certificate for iOS devices [Set up | Learn more](#)

You'll need an Apple Push Notifications (APNs) Certificate to manage the iPhones and iPads that connect to your organization. You can skip this if you don't want to manage these devices.

Recommended steps

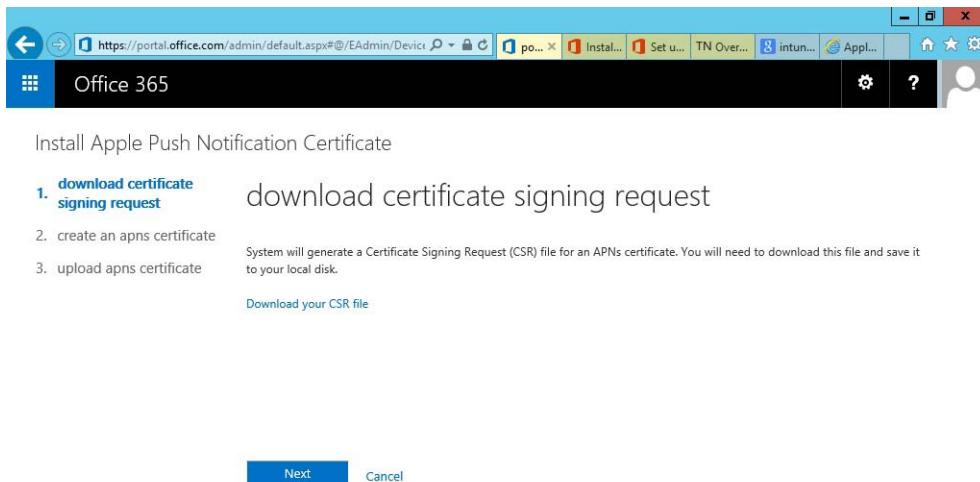
- Set up multi-factor authentication [Set up | Learn more](#)
- To better secure the connection between your servers to devices, we recommend setting up multifactor authentication.
- Manage device security policies [Set up | Learn more](#)
- We recommend setting up a device security policies to enforce users to enroll their devices. You can configure security settings on devices and define access criteria.

Done

116

117

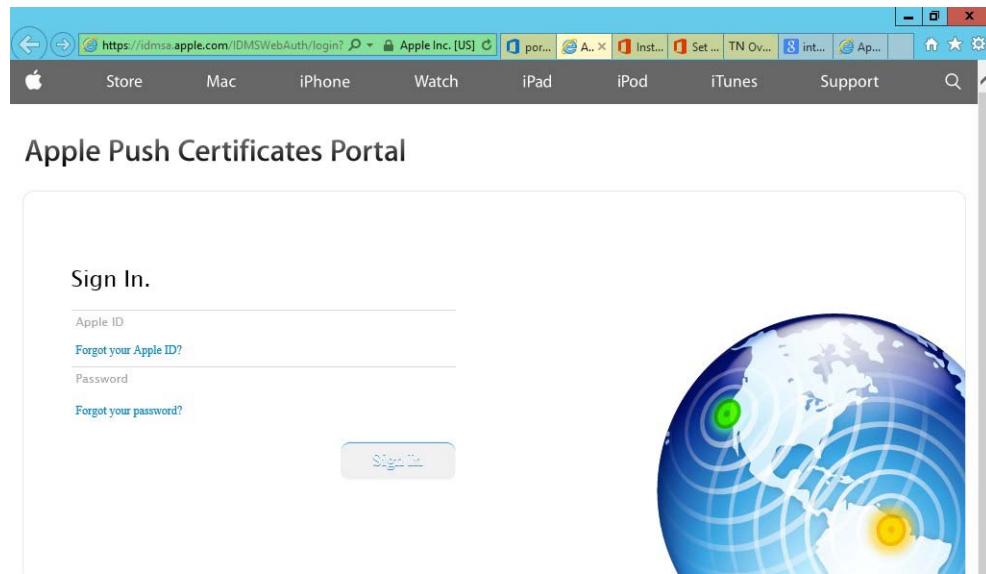
2. Configure APNs Certificate for iOS devices -> Setup



118

- 119 3. Download certificate signing request (CSR).
- 120 a. Once the CSR is generated, it can be submitted to Apple for signing.
- 121 b. Use a browser to visit³ <https://identity.apple.com/pushcert/>
- 122 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.

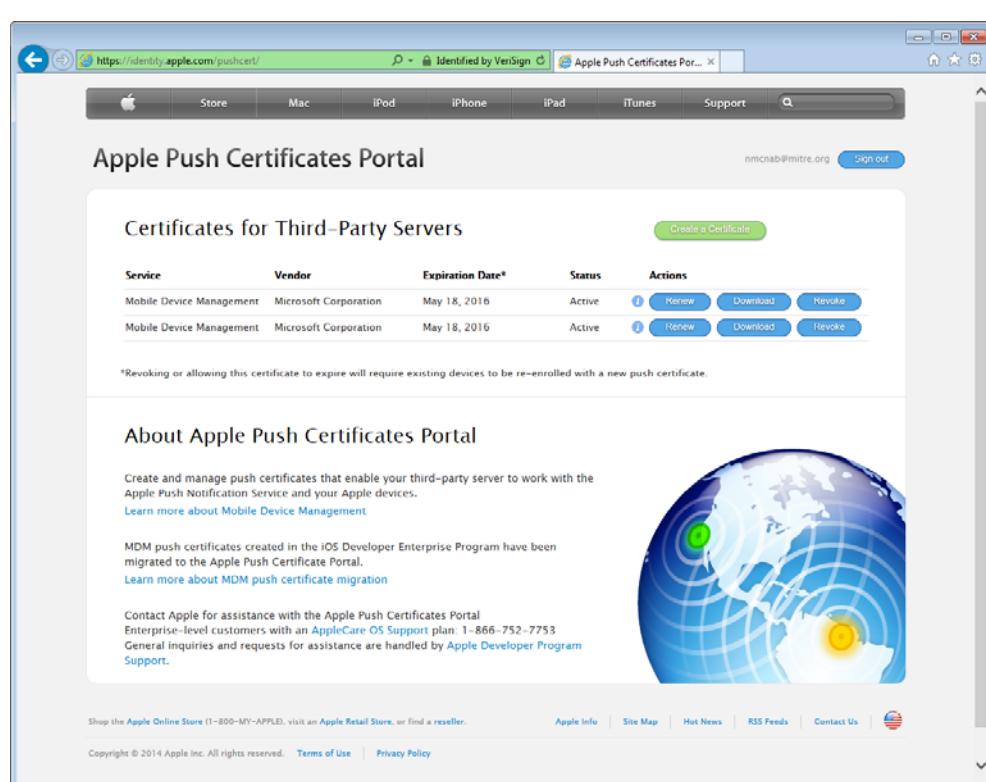


The screenshot shows the sign-in page of the Apple Push Certificates Portal. It features a login form with fields for 'Apple ID' and 'Password', and links for 'Forgot your Apple ID?' and 'Forgot your password?'. A 'Sign In' button is at the bottom right. To the right is a large graphic of a globe with a green dot over North America and a yellow dot over South America, with concentric blue lines radiating from the center.

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#). [Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#) | [Windows](#)
 Copyright © 2015 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)



A small portion of the Windows taskbar is visible at the top, showing the browser window and other open applications like File Explorer, Control Panel, and Task Manager.



The screenshot shows the 'Certificates for Third-Party Servers' page. It lists two certificates:

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	May 18, 2016	Active	Renew Download Revoke
Mobile Device Management	Microsoft Corporation	May 18, 2016	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

About Apple Push Certificates Portal

Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices. [Learn more about Mobile Device Management](#)

MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal. [Learn more about MDM push certificate migration](#)

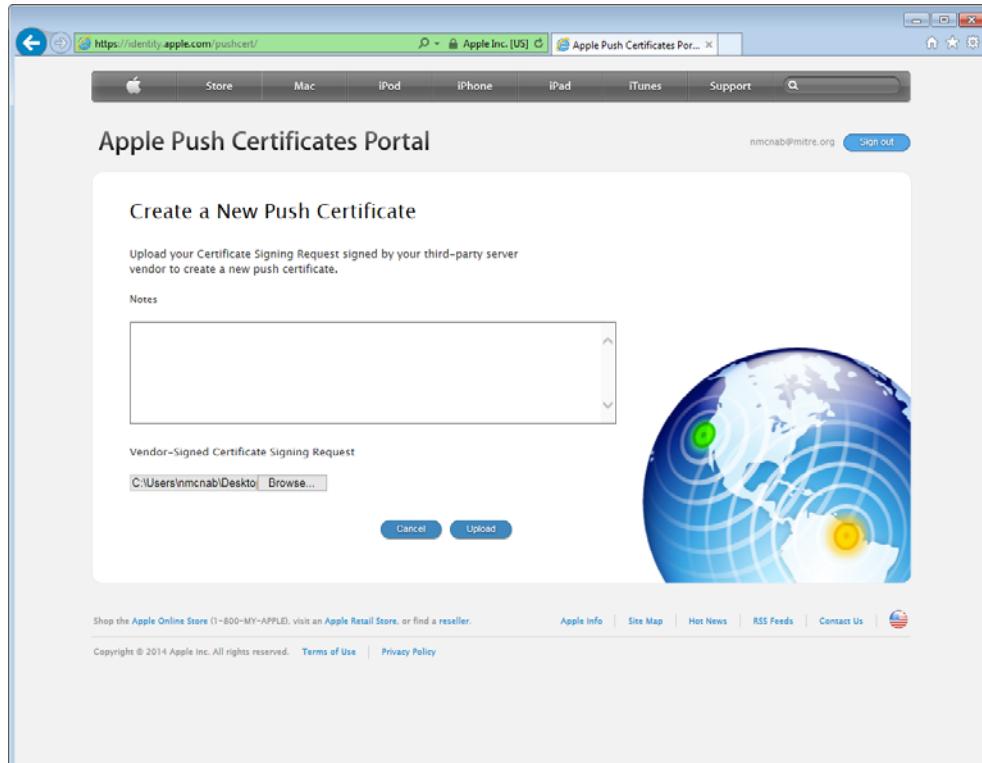
Contact Apple for assistance with the Apple Push Certificates Portal. Enterprise-level customers with an [AppleCare OS Support plan](#) 1-866-752-7753. General inquiries and requests for assistance are handled by [Apple Developer Program Support](#).

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#). [Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#) | [Windows](#)
 Copyright © 2014 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

124

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

- 126
- 127
- 128
- 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**.



129

- 130
- 131
- 132
5. 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.

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	May 18, 2016	Active	Renew Download Revoke
Mobile Device Management	Microsoft Corporation	May 18, 2016	Active	Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

About Apple Push Certificates Portal

Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.

[Learn more about Mobile Device Management](#)

MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.

[Learn more about MDM push certificate migration](#)

Contact Apple for assistance with the Apple Push Certificates Portal
Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
General inquiries and requests for assistance are handled by [Apple Developer Program Support](#).

133

Install Apple Push Notification Certificate

- download certificate signing request
- create an apns certificate
- upload apns certificate**

upload apns certificate

Lastly, upload the APNs certificate that you have created in Apple Push Certificates portal and downloaded to your system.
 [Browse...](#)

Certificate Uploaded Successfully

[Finish](#)

Activate Windows
Go to System in Control Panel to activate Windows.

[Feedback](#)

11:25 AM
5/19/2015

134

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

Mobile Device Management for Office 365

The following mobile devices have been enrolled in Mobile Device Management by users in your tenant. You can view device properties, access reports, wipe devices and enforce device security policies.

Manage device security policies and access rules
See device compliance report

Select a view: All

DEVICE NAME	OPERATING SYSTEM	OS VERSION
Matt Steele - iPhone 6 8.3	iPhone	8.3
Matt Steele - msteele_Android_5/1...	Android	5.1
Matt Steele - msteele_WindowsPho...	WindowsPhone	8.10.14219.341

Settings

- APNs Certificate for iOS devices expires 5/18/2016

Status

Device Model

Activate Windows

Platform Go to System in Control Panel to activate Windows.

Platform Version 10:26 AM 5/20/2015

Feedback

136

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

137

138

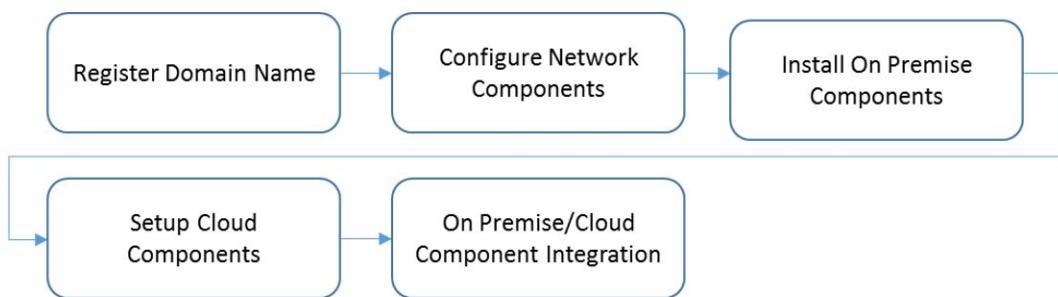
¹ **3** How to Build an On-Premises Solution for ² Mobile Device Security

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

3.1 Hybrid Build Setup and Configuration

Figure 3.1 depicts the high-level procedures to reproduce the hybrid build used in this building block. First, the implementer must own an Internet domain name or have permission to edit resource records within a domain. This is a prerequisite to integration with the cloud services used within this build. The next set of steps configure the on-premises components. The 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 final set of steps instantiate the cloud services and integrate them into the on-premises components.

Figure 3.1 Hybrid Build Process



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.

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.

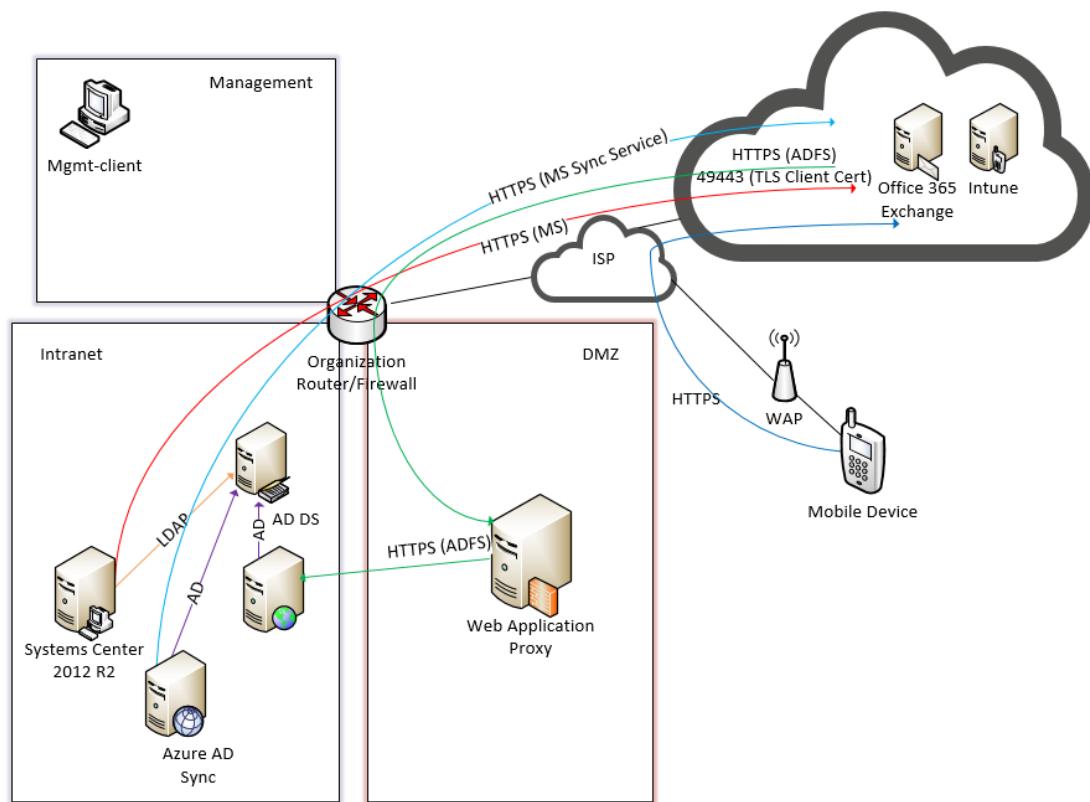
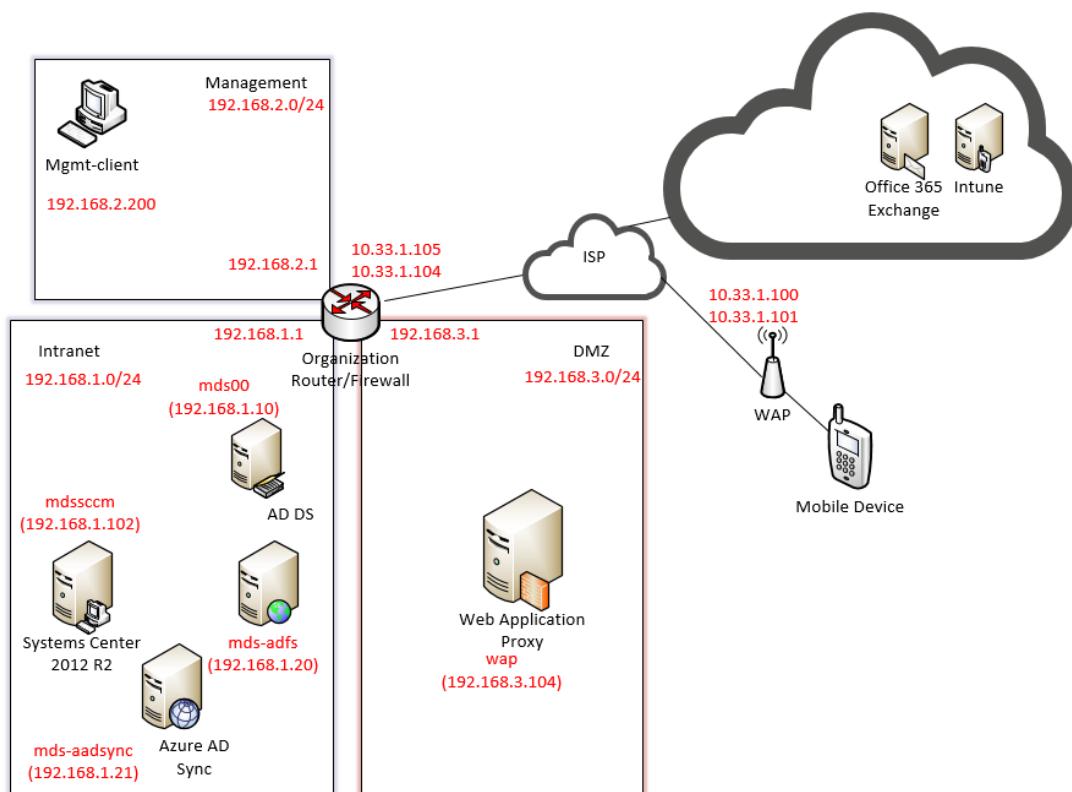
Figure 3.2 Detailed Architecture

Figure 3.3 Detailed Architecture with IP Addresses

40 3.2.1 Hybrid Build Components

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

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

⁴⁴ The build uses PFSense for the organization router/firewall (see [Table 3.2](#)). It is a combination
⁴⁵ router and firewall configured as a virtual device. This subsection describes the configuration
⁴⁶ used in the build and how to create it.

⁴⁷ A single firewall configuration was chosen for simplicity and flexibility in a lab environment.⁴
⁴⁸ Only IPv4 is used.⁵

⁴⁹ Implementers should refer to PFSense documentation for installation and configuration
⁵⁰ instructions. To recreate the configuration, follow the instructions in the documentation and
⁵¹ use the configuration files⁶ made available by PFSense.

⁵² The following screen shots show the final configuration of the PFSense device. Access PFSense
⁵³ through its Web interface. The default screen includes a list of interfaces described as part of
⁵⁴ the architecture in [section 3.2](#). The individual interfaces are described below with the firewall
⁵⁵ 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

Interfaces		
	<u>WAN</u>	1000baseT <full-duplex> 10.33.1.105
	<u>LAN</u>	1000baseT <full-duplex> 192.168.1.1
	<u>MGMT</u>	1000baseT <full-duplex> 192.168.2.1
	<u>DMZ</u>	1000baseT <full-duplex> 192.168.3.1

57

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

60

Figure 3.5 WAN

Firewall: NAT: Port Forward									
Port Forward 1:1 Outbound NPt									
	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>		WAN	TCP	*	*	10.33.1.104	443 (HTTPS)	192.168.3.104	443 (HTTPS)
<input type="checkbox"/>		WAN	TCP	*	*	10.33.1.104	49443	192.168.3.104	49443

pass
 linked rule

61

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

65

Figure 3.6 WAN Firewall Rules

Firewall: Rules										
Floating WAN LAN MGMT DMZ										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.3.104	443 (HTTPS)	*	none		NAT Microsoft ADFS
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.3.104	49443	*	none		NAT Microsoft ADFS Smart Card
<input type="checkbox"/>		IPv4 ICMP	WAN net	*	*	*	*	none		Allow ICMP for Debugging

pass
 pass (disabled)
 match
 match (disabled)
 block
 block (disabled)
 reject
 reject (disabled)
 log
 log (disabled)

66

67 The WAN configuration information is specific to our Internet service provider. In this lab, we
68 are provided the 10.33.1.0/24 network from which to statically assign addresses. The PFSense
69 device's IP address is 10.33.1.105, and 10.33.1.104 is also assigned as a virtual IP address for the

70 Web application proxy (WAP) service. Firewall rules are configured to allow Internet access to
 71 the WAP in the DMZ in order for ADFS to function.

72 **Figure 3.7 DMZ Firewall Rules**

Firewall: Rules

Floating	WAN	LAN	MGMT	DMZ	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
					<input type="checkbox"/>		IPv4 TCP/UDP	192.168.3.104	*	192.168.1.10	53 (DNS)	*	none		Internal DNS Name Resolution	
					<input type="checkbox"/>		IPv4 TCP/UDP	192.168.3.104	*	192.168.1.20	443 (HTTPS)	*	none		ADFS Sync through WAP	
					<input type="checkbox"/>		IPv4 *	*	*	MGMT net	*	*	none		Block to MGMT	
					<input type="checkbox"/>		IPv4 *	*	*	LAN net	*	*	none		Block to LAN	
					<input type="checkbox"/>		IPv4 TCP/UDP	DMZ net	*	*	*	*	none		Default allow DMZ to any rule	

pass
 pass (disabled)
 match
 match (disabled)
 block
 block (disabled)
 reject
 reject (disabled)
 log
 log (disabled)

73 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.

74 **Figure 3.8 LAN Firewall Rules**

Firewall: Rules

Floating	WAN	LAN	MGMT	DMZ	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
					<input type="checkbox"/>		*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
					<input type="checkbox"/>		IPv4 *	*	MGMT net	*	*	none		Block to MGMT	
					<input type="checkbox"/>		IPv4 TCP/UDP	LAN net	*	*	*	*		Default allow LAN to any rule	

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

Figure 3.9 Management Firewall Rules

Floating	WAN	LAN	MGMT	DMZ					
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	IPv4 TCP	MGMT net	*	MGMT address	443 (HTTPS)	*	none		This pfSense Web Interface Anti-Lockout
<input type="checkbox"/>	IPv4 TCP/UDP	MGMT net	*	*	*	*	none		Default Allow Any

pass
 pass (disabled)
 match
 match (disabled)
 block
 block (disabled)
 reject
 reject (disabled)
 log
 log (disabled)

83

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

84

85

3.2.3 Enterprise Software Components for Hybrid

86

87

88

89

90

91

92

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

93

94

95

96

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

98

99

100

101

102

103

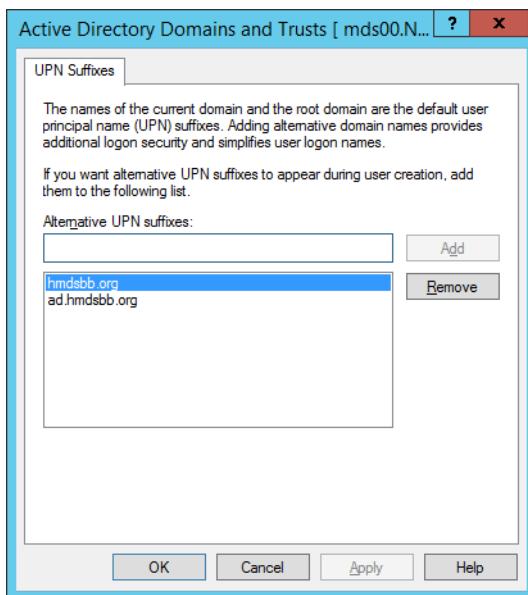
The Active Directory Domain Services (ADDS) instance used in the hybrid build was created using basic configuration settings offered through the Add Roles and Features Wizard. The system was deployed as a new forest with a domain name of nccoe.local. Implementers of this guide who seek more details on an ADDS installation should consult [Install Active Directory Domain Services \[4\]](#) Technet article. Alternatively, implementers may wish to reproduce their production environment.⁷

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

108 The domain controller will find the user's account based upon the userPrincipalName in the
 109 certificate's Subject Alternative Name field. The original domain controller was set up with a
 110 domain of nccoe.local; however, a more likely scenario would have an organization create an
 111 instance under a well-known TLD. We have addressed this issue by adding a user principle
 112 name (UPN) suffix for hmdsbb.org in the ADDS configuration. All users in this configuration are
 113 required to have a UPNsuffix of <user>@hmdsbb.org. Identity federation between Intune and
 114 on-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:

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



120

121 3.2.3.2 Active Directory Federation Service

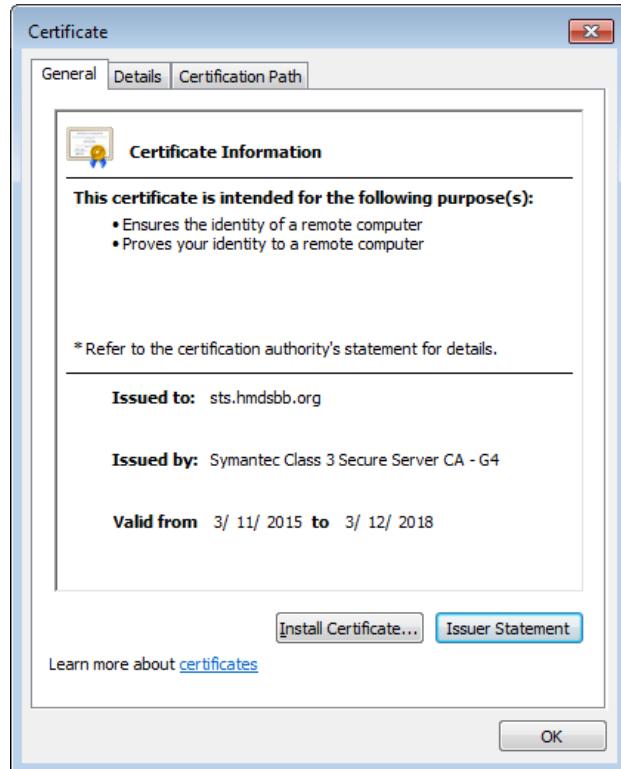
122 Refer to Microsoft documentation for specific installation instructions for your environment.
 123 Consult the following articles as a starting point for installation [6] [7].

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

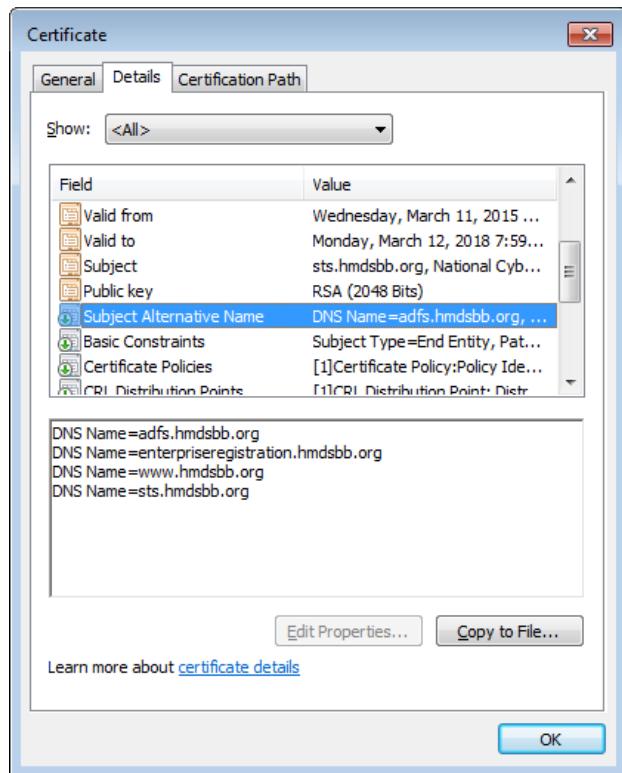
7.<http://blogs.technet.com/b/jratsch/archive/2012/02/17/creating-a-test-lab-from-a-production-environment-using-hyper-v-and-gpmc-scripts.aspx>

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.

128 Screen shots below are of the certificates from Symantec used in the build.



129



130

[3.2.3.3 Active Directory Federation Services Proxy](#)

Refer to the articles referenced in [section 3.2.3.2](#) for specific installation instructions.

[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].

[3.2.3.5 Azure Active Directory Sync Services](#)

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

[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.

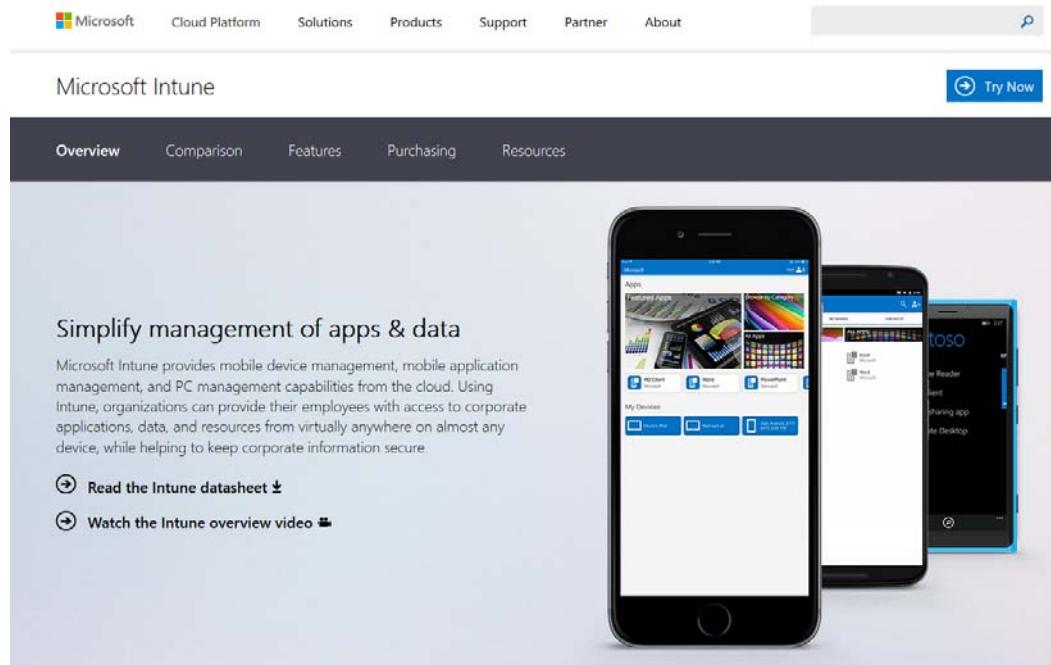
[3.2.4.1 Office 365 Setup](#)

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

145 **3.2.4.2 Intune Setup**

146 Use a browser to access the following URL to start the Intune creation process:

147 <http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/>



148

149 1. Choose Try now.

Microsoft Intune

If 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's important to sign up with the same User ID. [Sign in](#) * Required

* Country or region: Select Can't be changed after signup. [Why?](#)

* Organization language: English

* First name:

* 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](#)

150

151

- Choose **Sign in**. Sign in when prompted.

Microsoft Intune

[Check out](#)

[Confirm order](#)

Microsoft Intune | 30 day term

100 user licenses

[Try now](#) [Cancel](#)

152

153

154

155

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

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.

Add users

Add users first, so they can enroll their mobile devices in the Microsoft Intune service.
(This option is recommended for trial accounts)

Other ways to add users

Enable single sign-on, Active Directory synchronization and more.

 Microsoft Intune services are not available for one of these reasons:

- You are not subscribed to any services.
- There is a network delay.
- A technical error has occurred.

If you believe that you have reached this page in error, please try again later. If the problem persists, please consult the Microsoft Intune Community or contact Support.

156

157
158

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

159

3.2.4.3 Lookout Setup

160
161
162

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.



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](#)

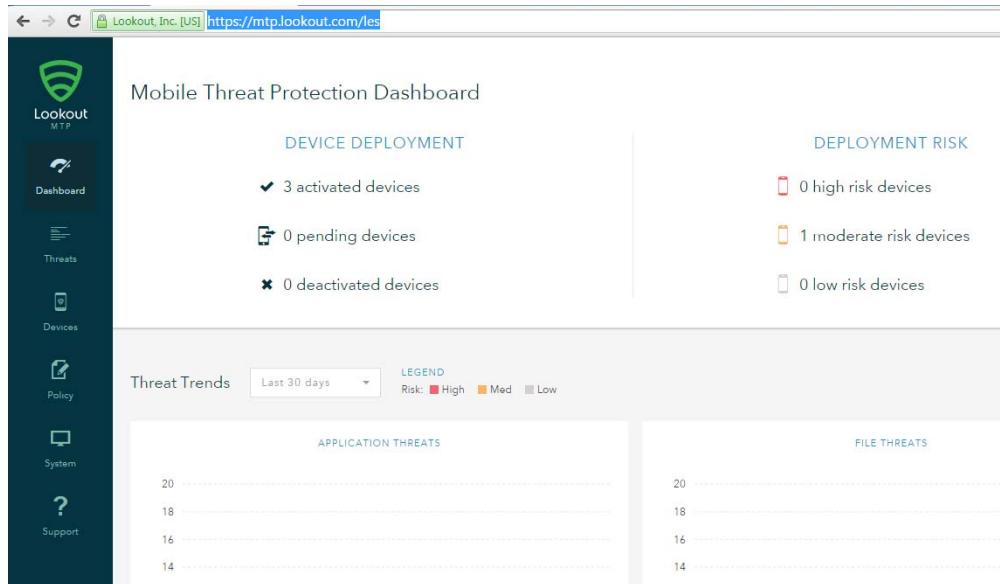
You will be able to update your account password from there. No changes will be made to your account until you visit the link. If you did not request this change then please disregard this message.

Sincerely,
The Lookout Team

163

164
165

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



166

167

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

168

169

3.2.5 Hybrid Integration

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

175

176

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 365 as 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].
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.

177

178

179

```
Set-MsolAdfscontext -Computer <AD FS server FQDN>
Convert-MsolDomainToFederated -DomainName <domain name>
```

180

181

182

3.2.5.2 Azure Active Directory Sync Services

183

184

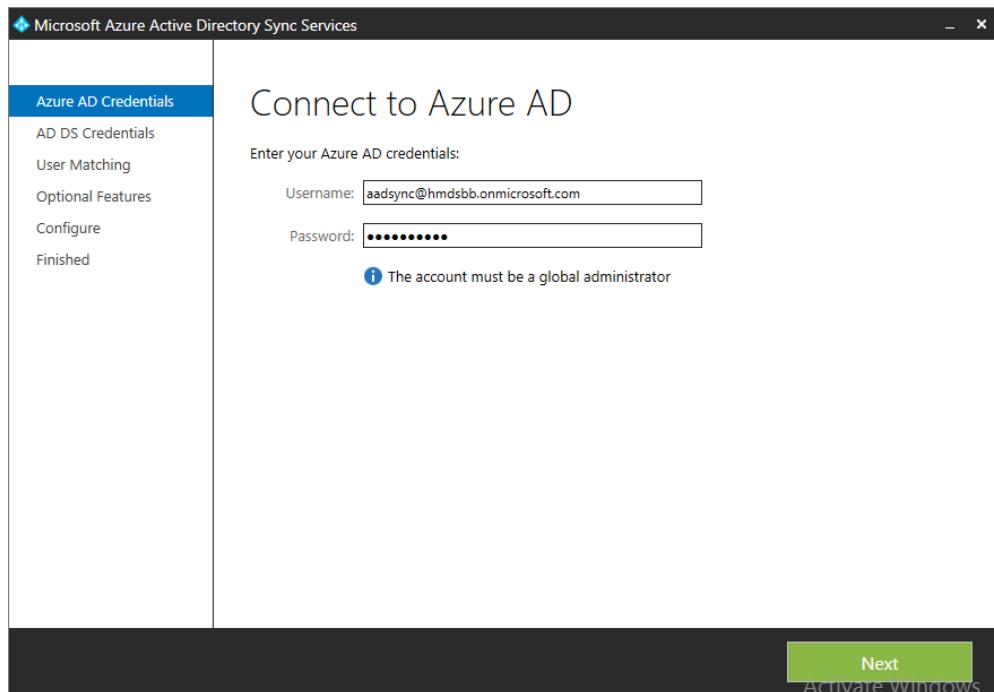
185

186

187

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.

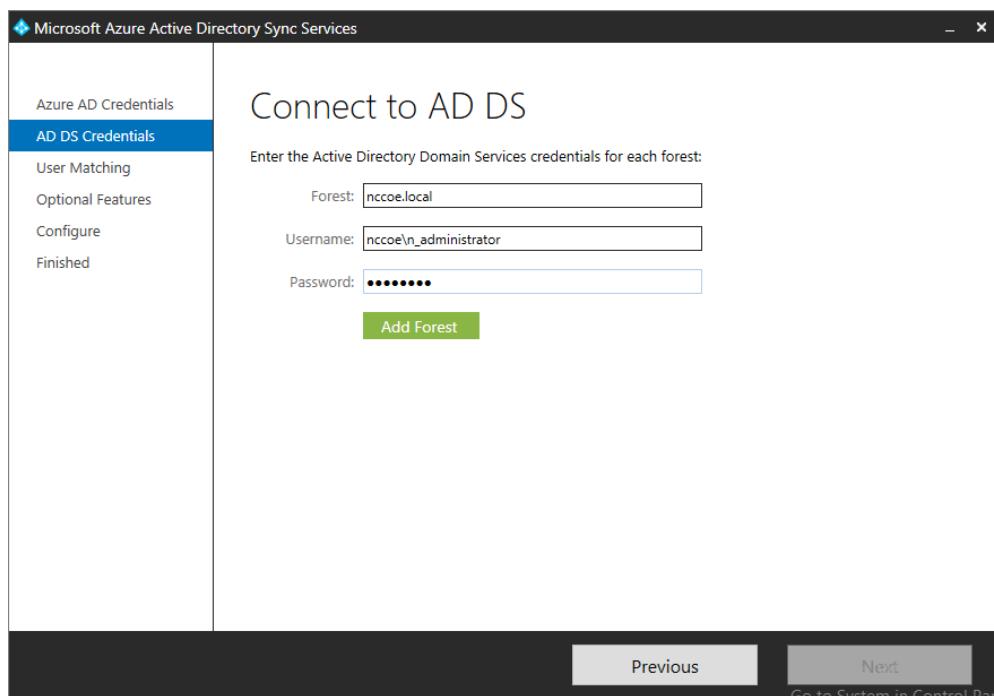
188



189
190

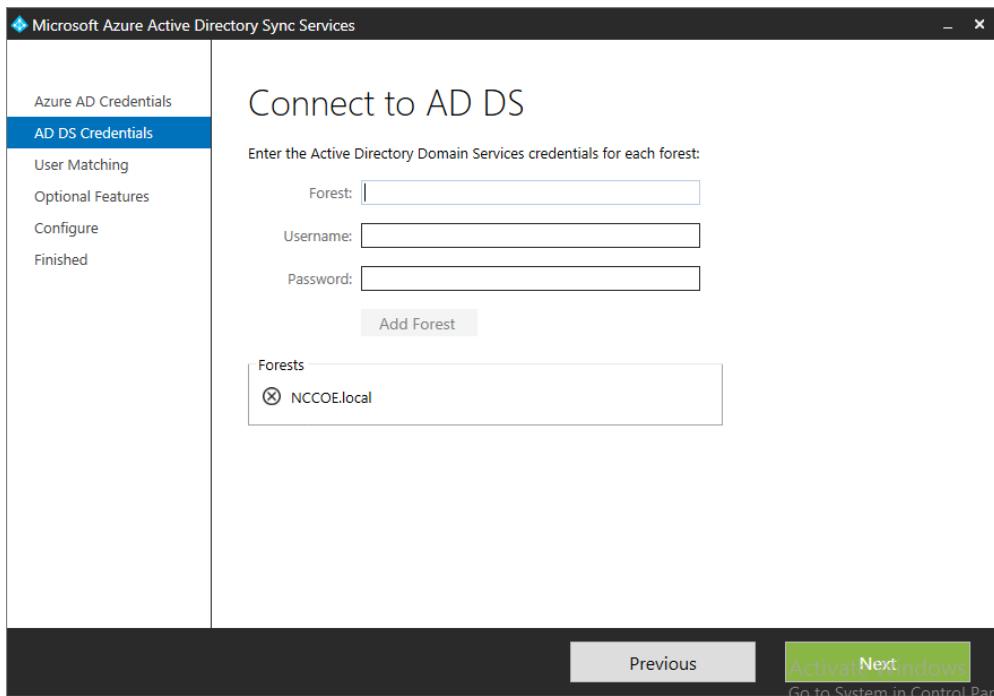
1. Launch the Sync Services Configuration Tool. Input the global administrator credentials for the Office 365 instance and click **Next**.

191



192

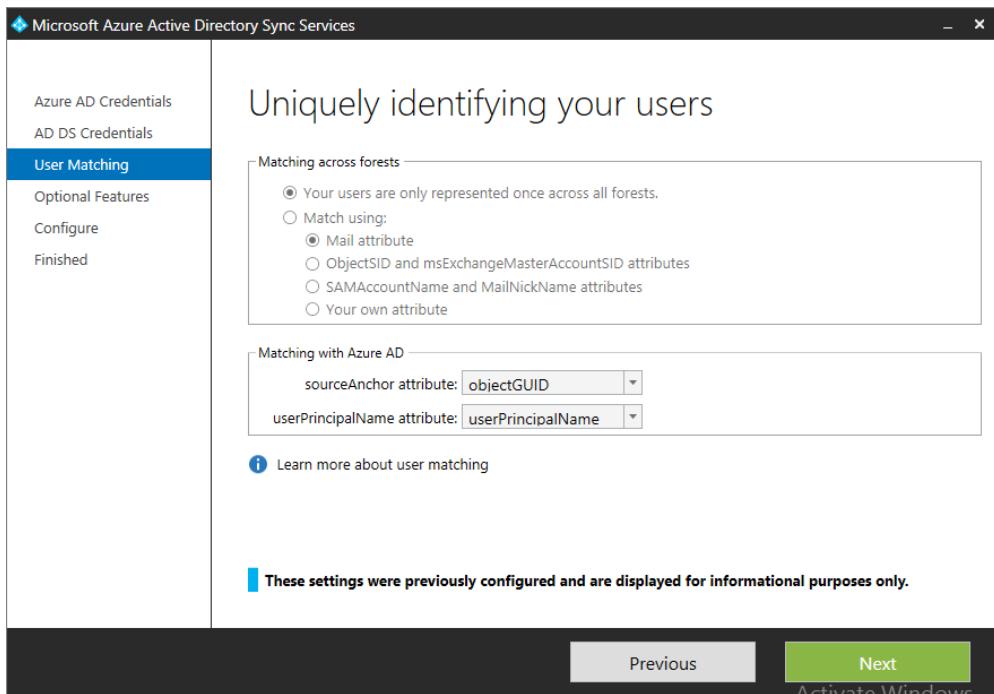
2. Input the Forest name and credentials of the administrator. Click **Add Forest**.



193

194

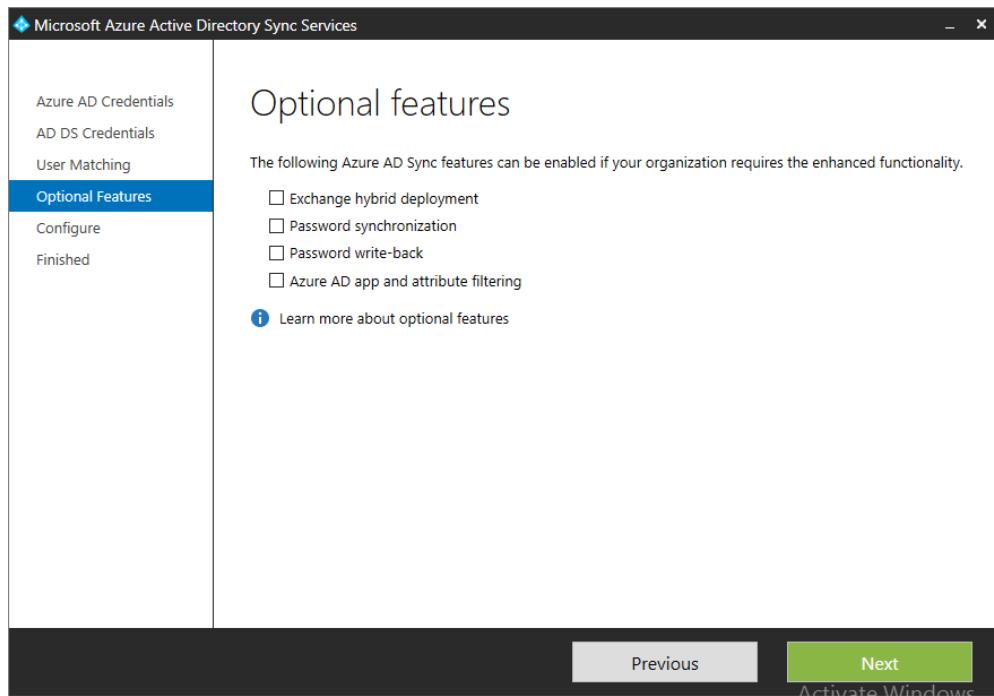
3. Click Next.



195

196

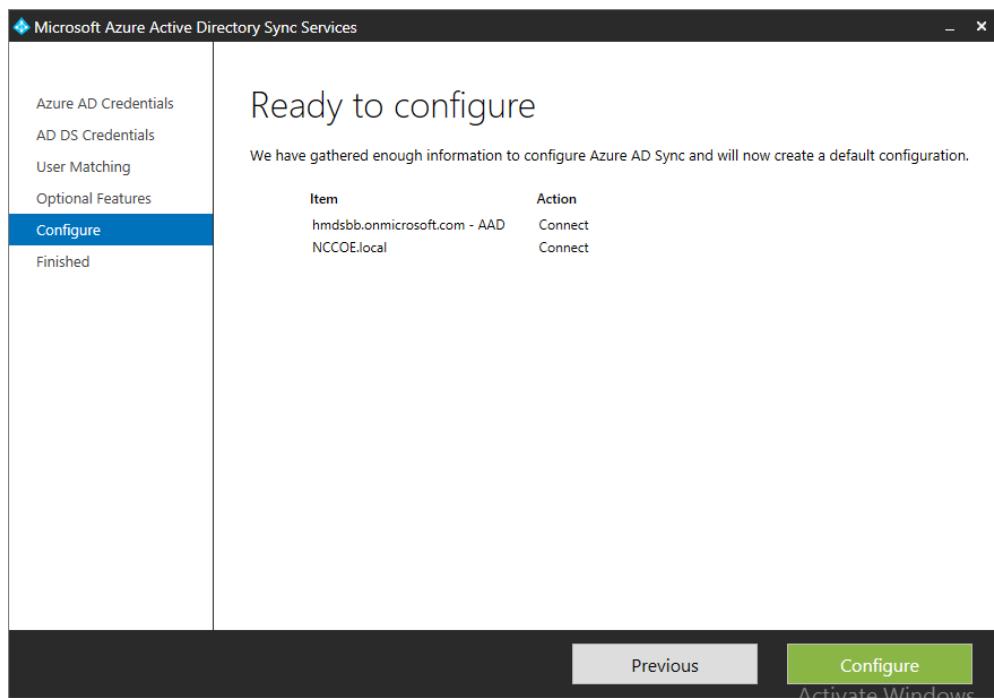
4. Accept the defaults for uniquely identifying your users.



197

198

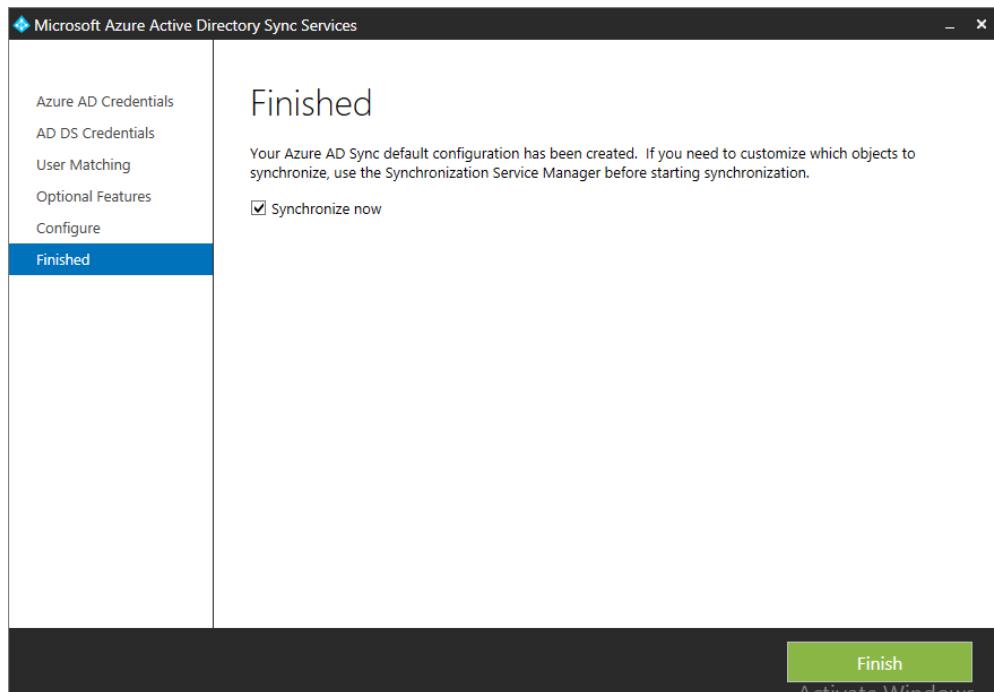
5. Do not choose any of the optional features. Click **Next**.



199

200

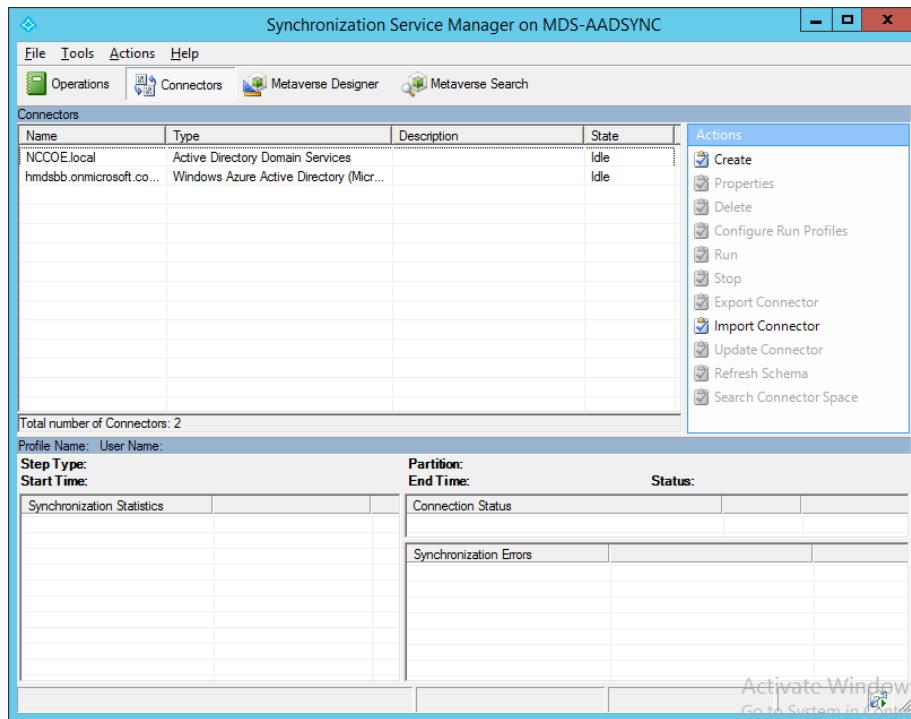
6. Click **Configure**.



201

202

7. Choose Synchronize now and click Finish.



203

204
205

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

207
208
209
210
The following steps will establish a backend connection between the Intune and Office 365 instances you have created in the Cloud Services Instances section. When this step is completed, Intune will be able to enforce conditional access policies on all enrolled mobile devices.

Set Up Exchange Connection

Microsoft Intune On-Premises Connector for On-Premises or Hosted Exchange

1. Prepare a computer that has access to your Exchange environment and complies with the On-Premises Connector system requirements.
[Learn about the system requirements](#)
2. Create a user account in Active Directory that has permission to run the required Exchange cmdlets. For Hosted Exchange environments, either create a user in Active Directory or MSODS that has permission to run the required Exchange cmdlets, or use an existing tenant administrator that has these permissions.
[Learn about the Exchange cmdlet requirements](#)
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.
[Download On-Premises Connector](#)

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 Service to Service Connector](#)

- 211
212
213
214
1. 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**.

Microsoft Exchange Mobile Device Management

Run quick sync

Run Quick Sync

Microsoft Intune sent a synchronization request to Exchange.

Microsoft Intune will synchronize new mobile devices and mobile devices with changes to their Exchange state.

To view the updated mobile device list after Quick Sync completes, go to the Groups workspace.

- 215
216
217
2. The configuration with Office 365 will occur in the background. No further actions are required.

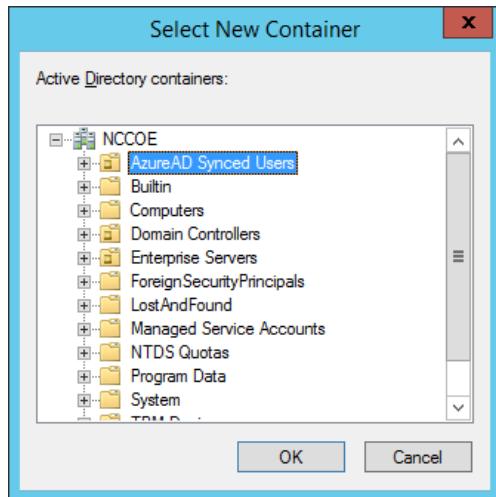
218 3.2.5.4 Manage Intune with SCCM

219
220
221
222
223
To allow the Intune tenant to be administered remotely, SCCM must be configured on the enterprise network. The following steps add test accounts to an SCCM user collection and syncs with the Intune tenant. While Intune will be available through the browser-based administrative console after this exercise, the account will be permanently configured to manage devices through SCCM.

224 **3.2.5.4.1 Configure Active Directory User Discovery**

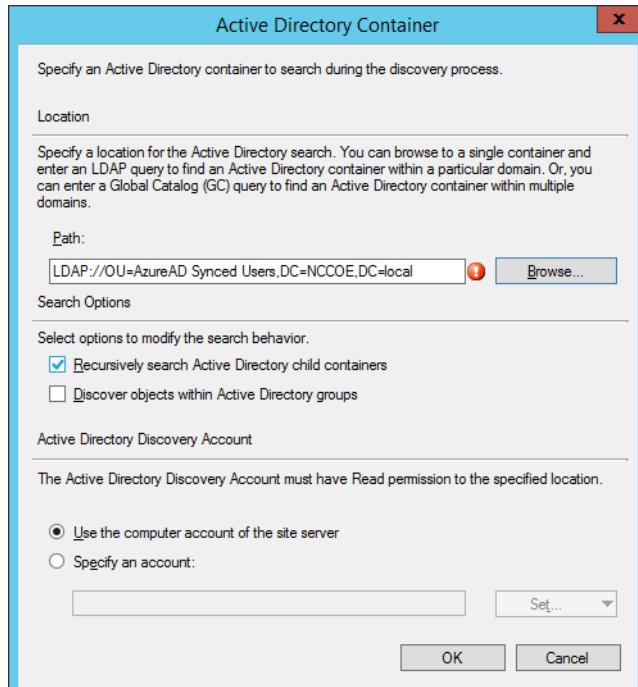
225 When these steps have been completed, the SCCM instance will be able to automatically
226 discover Intune users by way of an Active Directory container.

- 227 1. Launch the Configuration Manager console. Navigate to **System Center Configuration**
228 **Manager / Site Database / Site Management /<site name>/ Site Settings / Discovery**
229 **Methods.**
- 230 2. Right-click **Active Directory User Discovery**, and then click **Properties**.
- 231 3. On the General tab, click the **New** icon to specify a new Active Directory container.
- 232 4. On the New Active Directory Container dialog box, specify **Local Domain**.



233

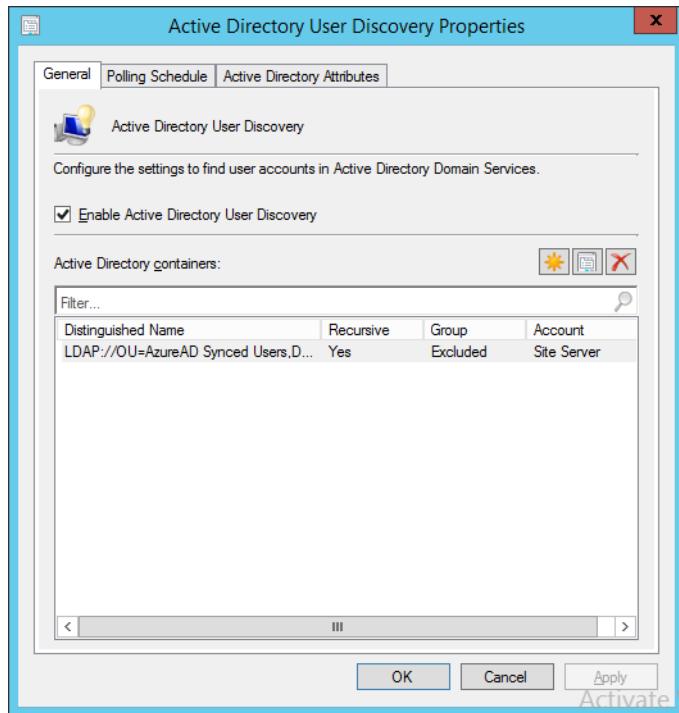
- 234 5. Select the **AzureAD Synced Users** container.



235

236

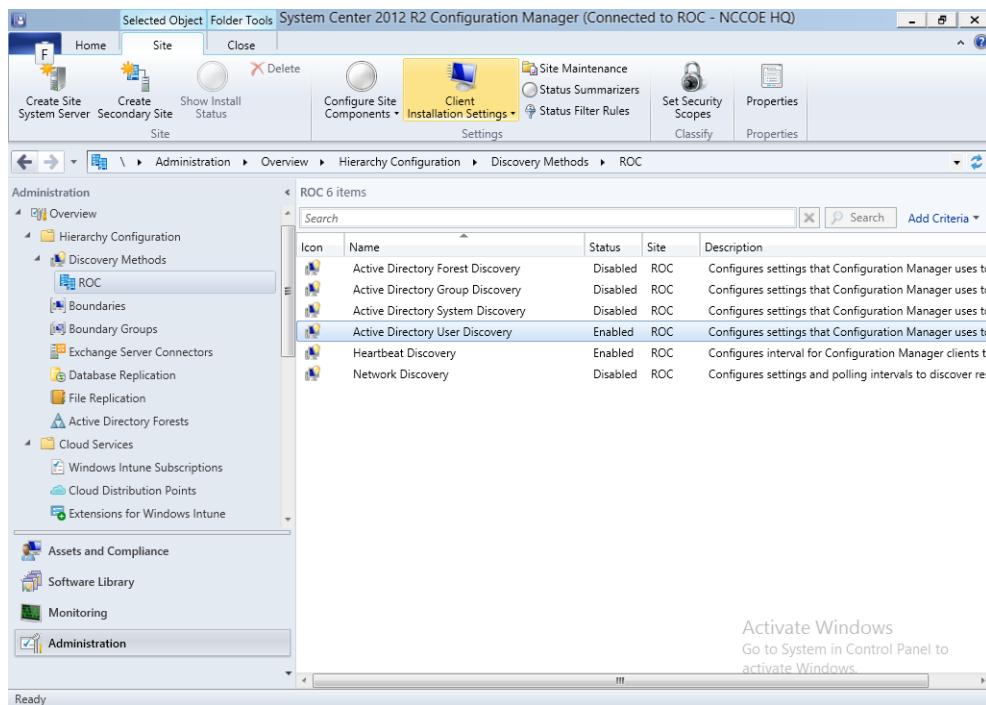
- The path will reflect the container chosen in the previous step.



237

238

- Ensure that **Enable Active Directory User Discovery** is selected.



239

240

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

The screenshot shows the System Center 2012 R2 Configuration Manager interface. The title bar reads "System Center 2012 R2 Configuration Manager (Connected to ROC - NCCOE HQ)". The ribbon tabs include "Selected Object", "Folder Tools", and "System Center 2012 R2 Configuration Manager". Below the ribbon are several icons: "Add Selected Items", "Manage Affinity Requests", "Update Membership", "Collection", "Add Resources", "Copy", "Delete", "Export", "Deploy", and "Properties". The main pane displays a list titled "All Users 8 items" with columns: Icon, Name, Domain, and Resource Type. The data is as follows:

Icon	Name	Domain	Resource Type
User icon	NCCOE\bsisko (Benjamin Sisko)	NCCOE	User
User icon	NCCOE\hsulu (Hikaru Sulu)	NCCOE	User
User icon	NCCOE\jkirk (James T. Kirk)	NCCOE	User
User icon	NCCOE\jpicard (Jean-Luc Picard)	NCCOE	User
User icon	NCCOE\jsmith (John Smith)	NCCOE	User
User icon	NCCOE\mobrien (Miles O'Brien)	NCCOE	User
User icon	NCCOE\nuhura (Nyota Uhura)	NCCOE	User
User icon	NCCOE\pchevikov (Pavel Chekov)	NCCOE	User

The left sidebar shows the navigation path: Assets and Compliance > Overview > Users > All Users. The bottom left pane shows "Assets and Compliance" sections: Overview, Users (selected), Devices, User Collections, Device Collections, User State Migration, Asset Intelligence, Software Metering, Compliance Settings, Endpoint Protection, Antimalware Policies, Windows Firewall Policies, Software Library, Monitoring, Administration. The bottom right pane shows the details for "NCCOE\bsisko (Benjamin Sisko)" under "General Information": Name: NCCOE\bsisko (Benjamin Sisko), Domain or Workgroup: NCCOE. It also shows a "Related Objects" section with a link to "Activate Windows".

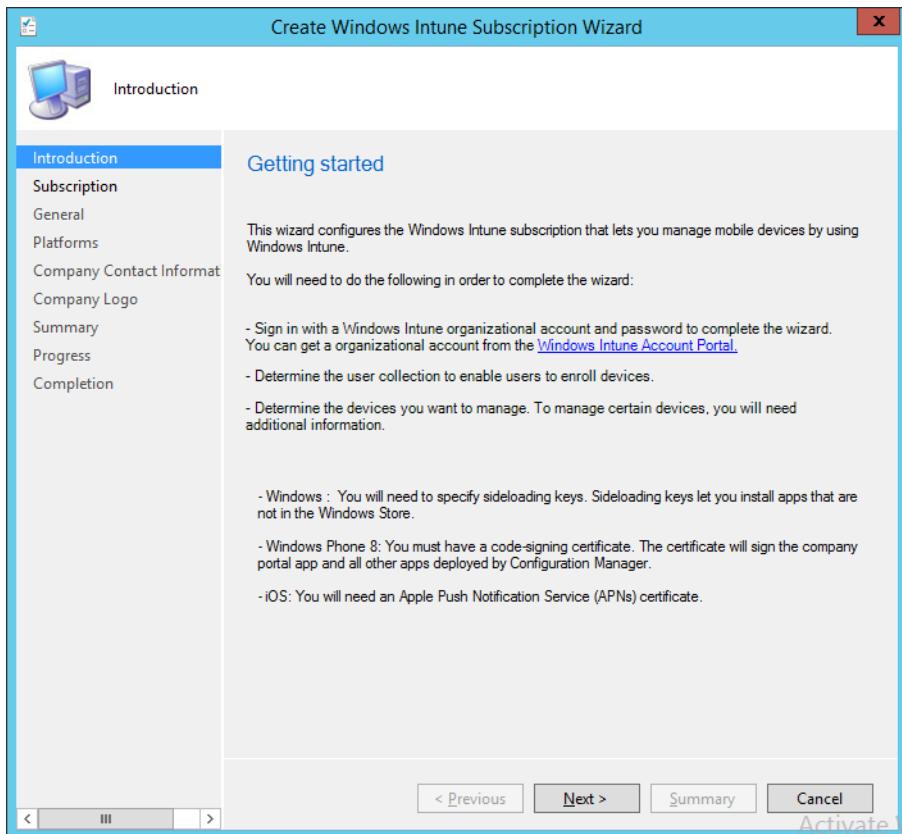
241

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

243 **3.2.5.4.2 Register SCCM with Intune**

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

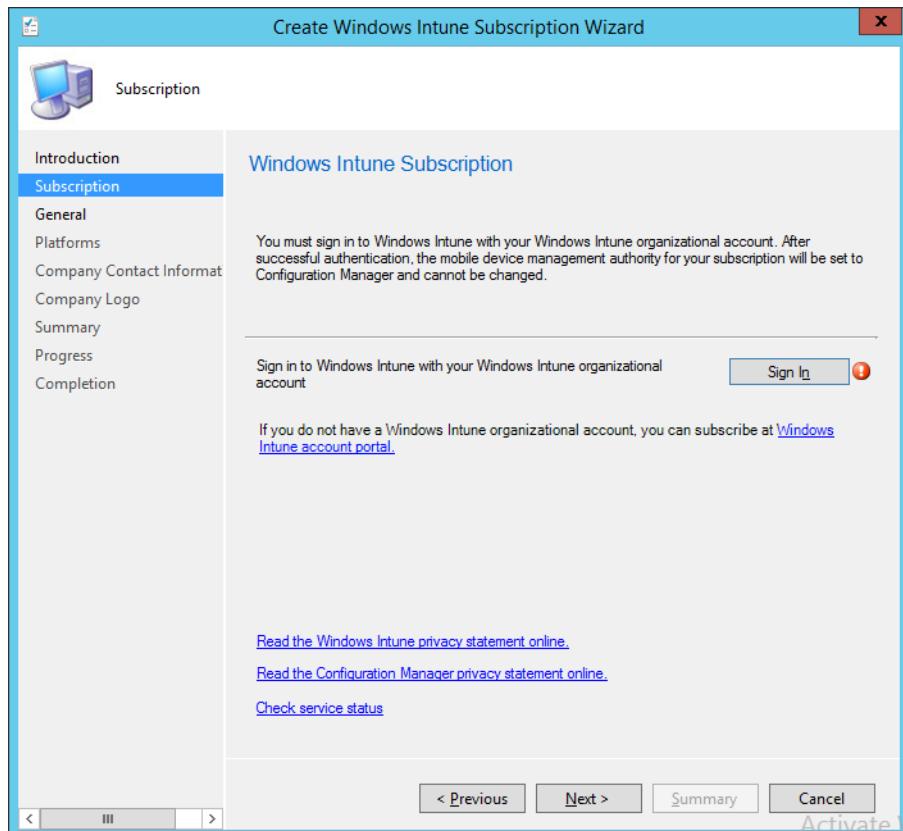
- 247 1. Start the Intune Subscription wizard by opening the Configuration Manager. In the
248 Administration section, expand Cloud Services, and click **Microsoft Intune Subscriptions**.
249 Click on the **Home** tab and then **Add Microsoft Intune Subscription**.



250

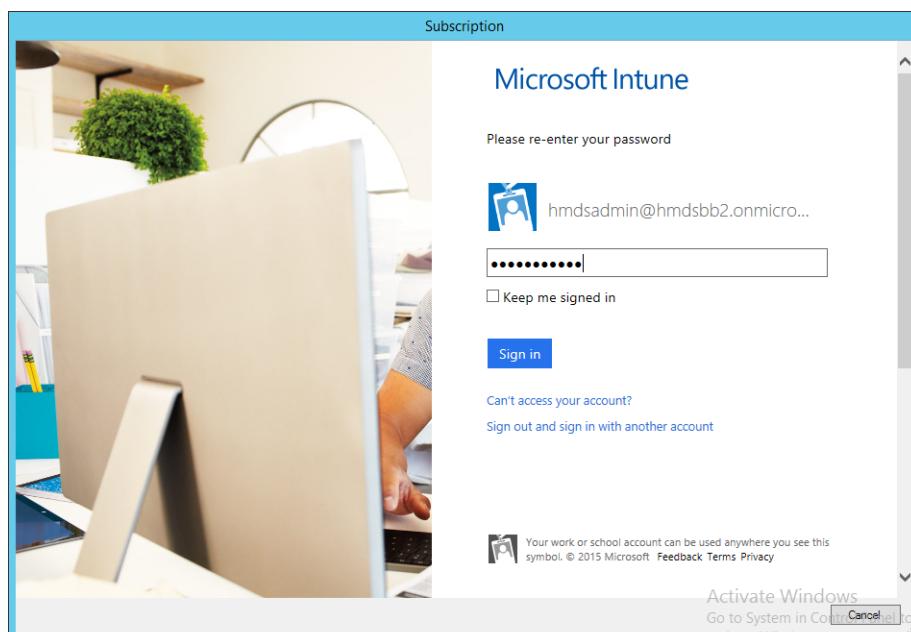
251

2. Click **Next**.



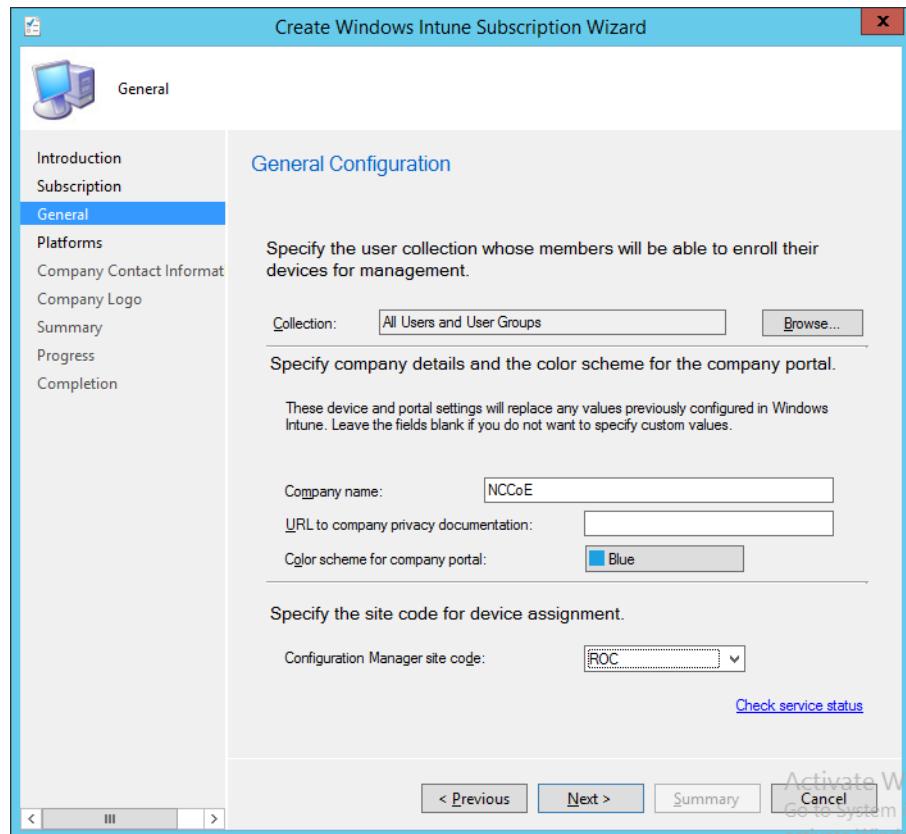
252

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



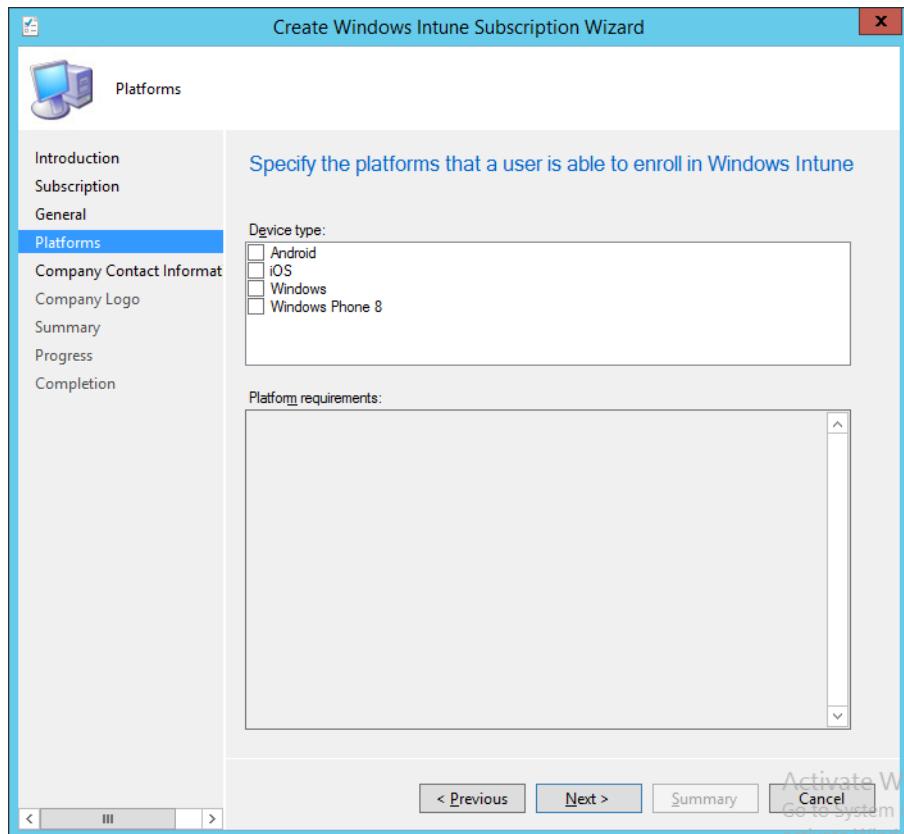
254

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



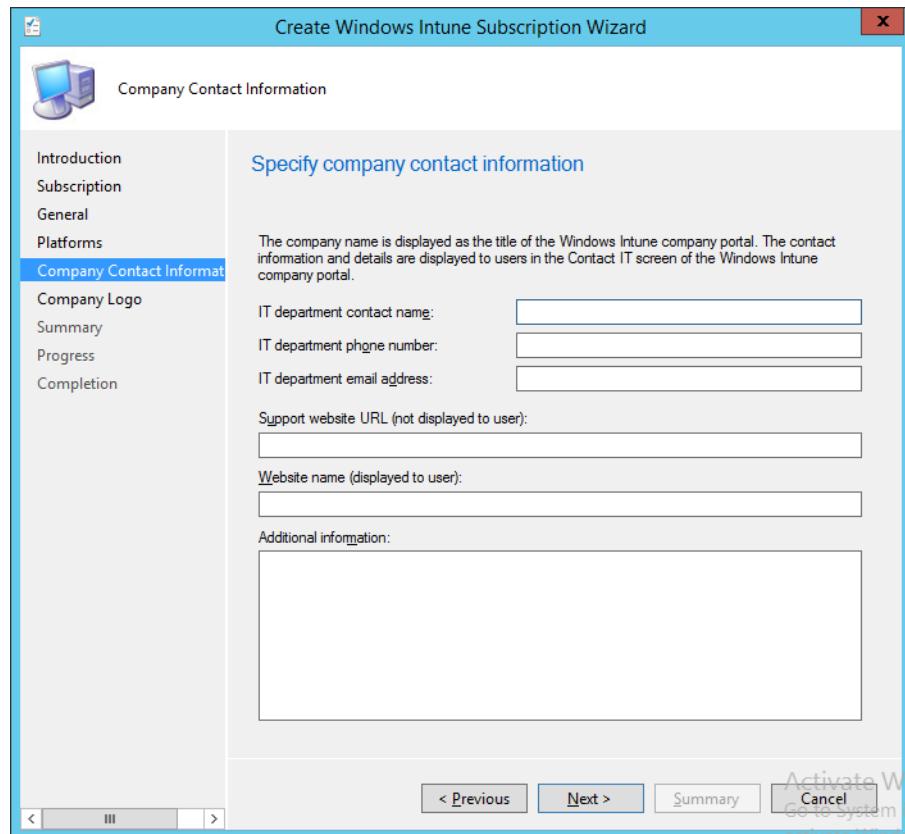
256

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



258

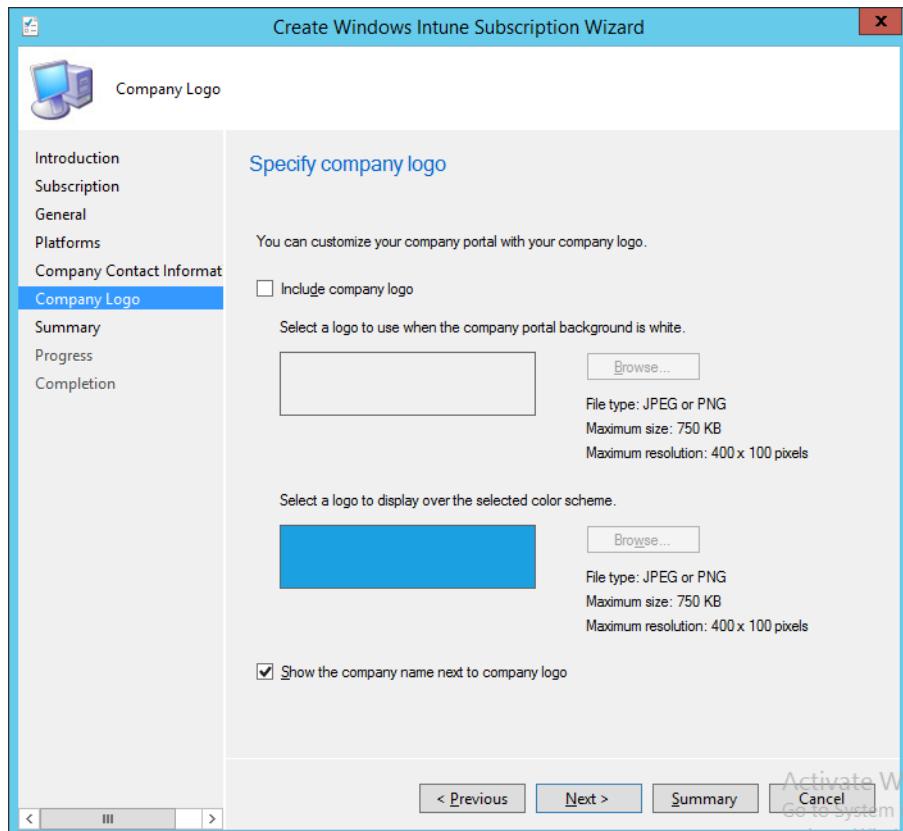
- 259 6. You may choose to configure device types in this step. However, we chose to configure these in a later step.
- 260



261

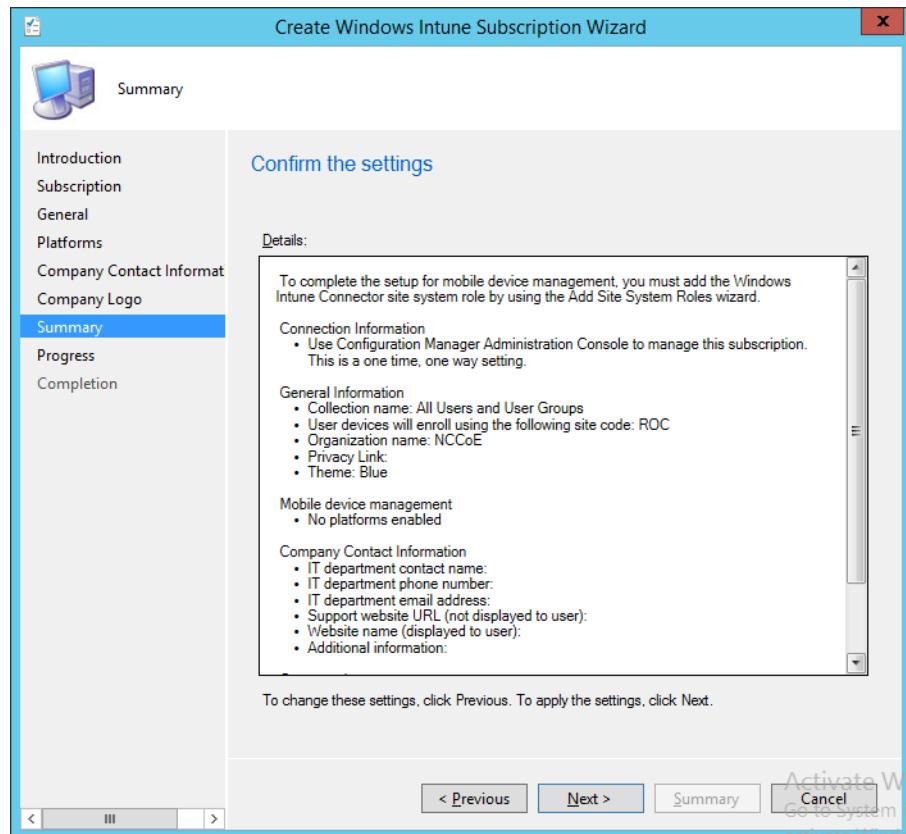
262

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



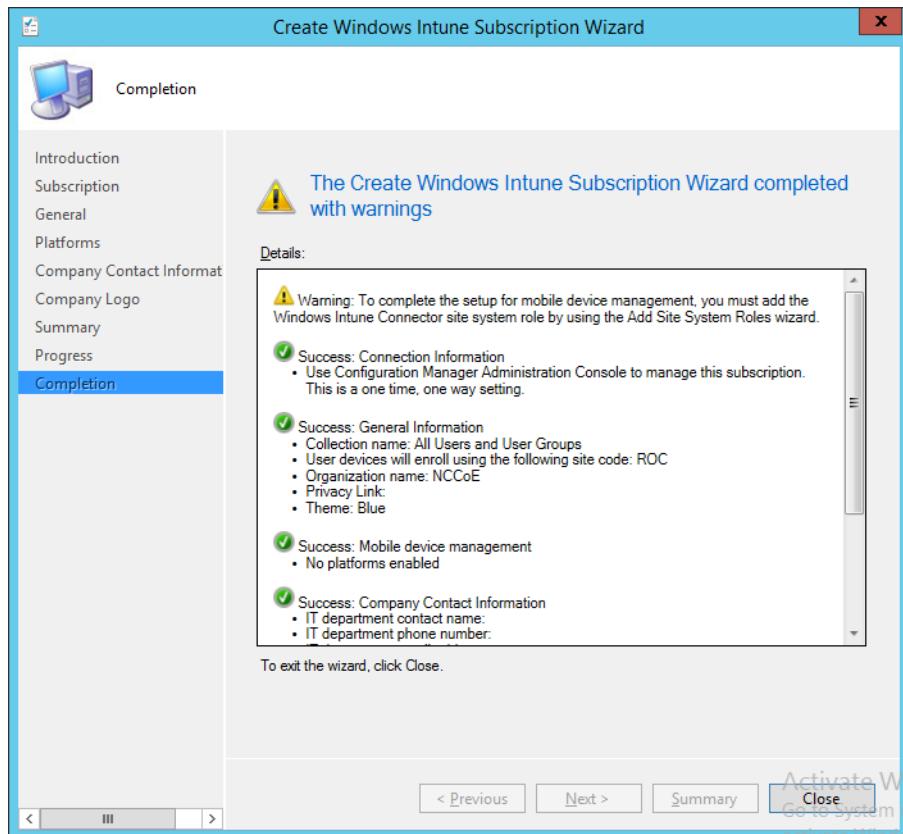
263

8. Submit an organizational logo, if desired.



265

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



267

268
269

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

Microsoft Intune

DASHBOARD

GROUPS

ALERTS

APPS

POLICY

REPORTS

ADMIN

Administration

Overview

Alerts and Notifications

Alert Types

Recipients

Notification Rules

Administrator Management

Service Administrators

Tenant Administrators

Device Enrollment Managers

Client Software Download

Storage Use

Mobile Device Management

Company Portal

Mobile Device Management Authority

Set to Configuration Manager

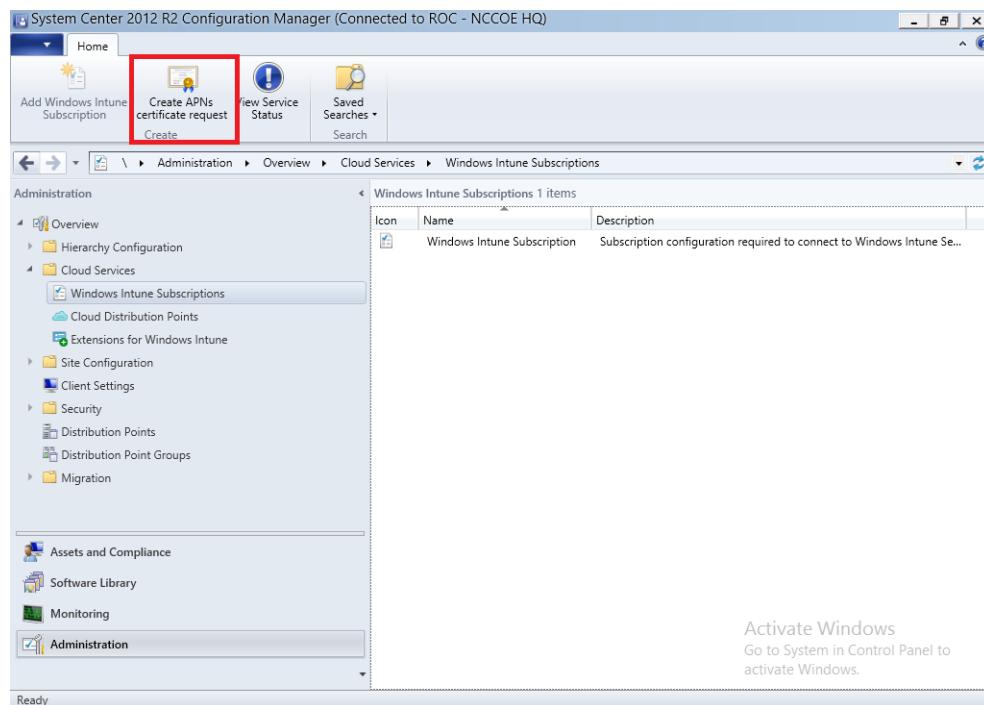
270

271
272

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

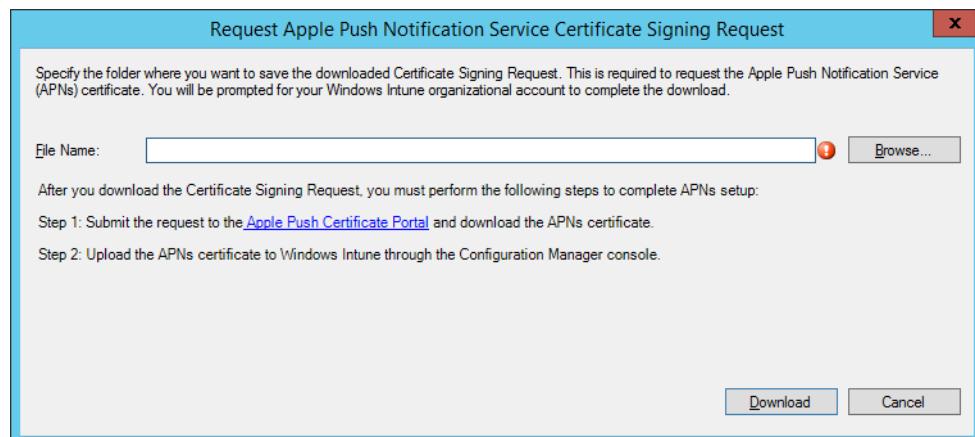
273 **3.2.5.4.3 Configure Push Certificate for iOS Devices**

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



277

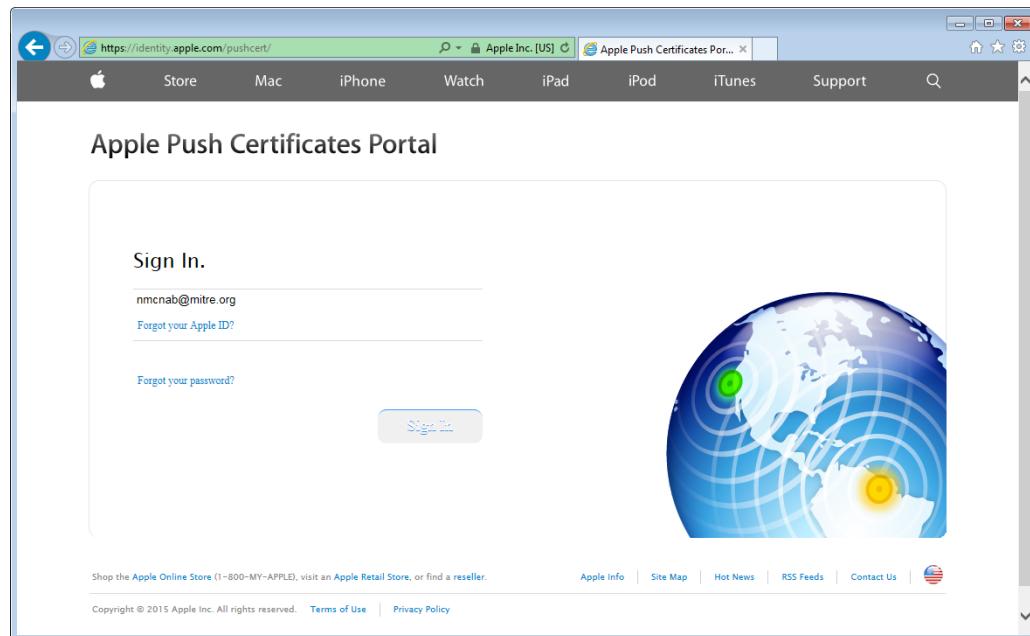
- 278 1. Click **Create APNs certificate request** in the SCCM console.



279

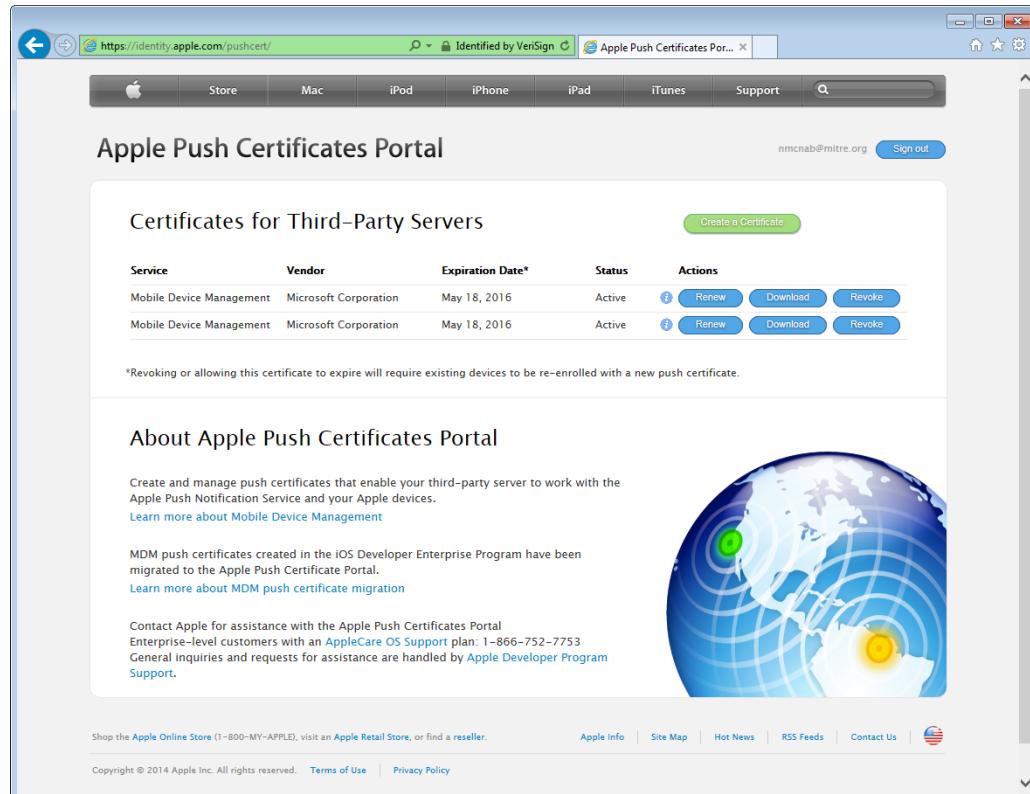
- 280 2. Save the CSR to local storage. You'll need this file for the next step.
 281 3. Use a browser to visit <https://identity.apple.com/pushcert/>⁸. You will be prompted for your
 282 Apple Developer account credentials.

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



283

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



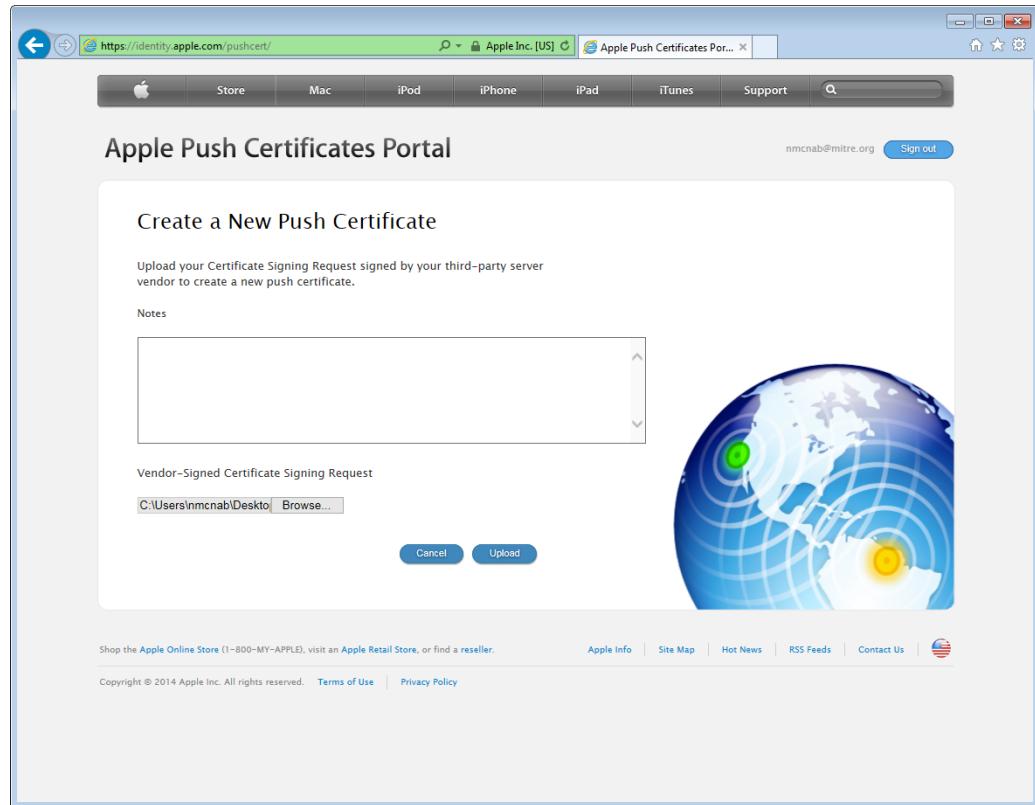
285

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

286

287

288



289

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

The screenshot shows the Apple Push Certificates Portal interface. At the top, there's a navigation bar with links for Store, Mac, iPod, iPhone, iPad, iTunes, Support, and a search bar. The main content area has a title "Apple Push Certificates Portal" and a sub-section "Certificates for Third-Party Servers". Below this is a table with columns: Service, Vendor, Expiration Date*, Status, and Actions. There are two entries in the table:

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Microsoft Corporation	May 18, 2016	Active	Renew Download Revoke
Mobile Device Management	Microsoft Corporation	May 18, 2016	Active	Renew Download Revoke

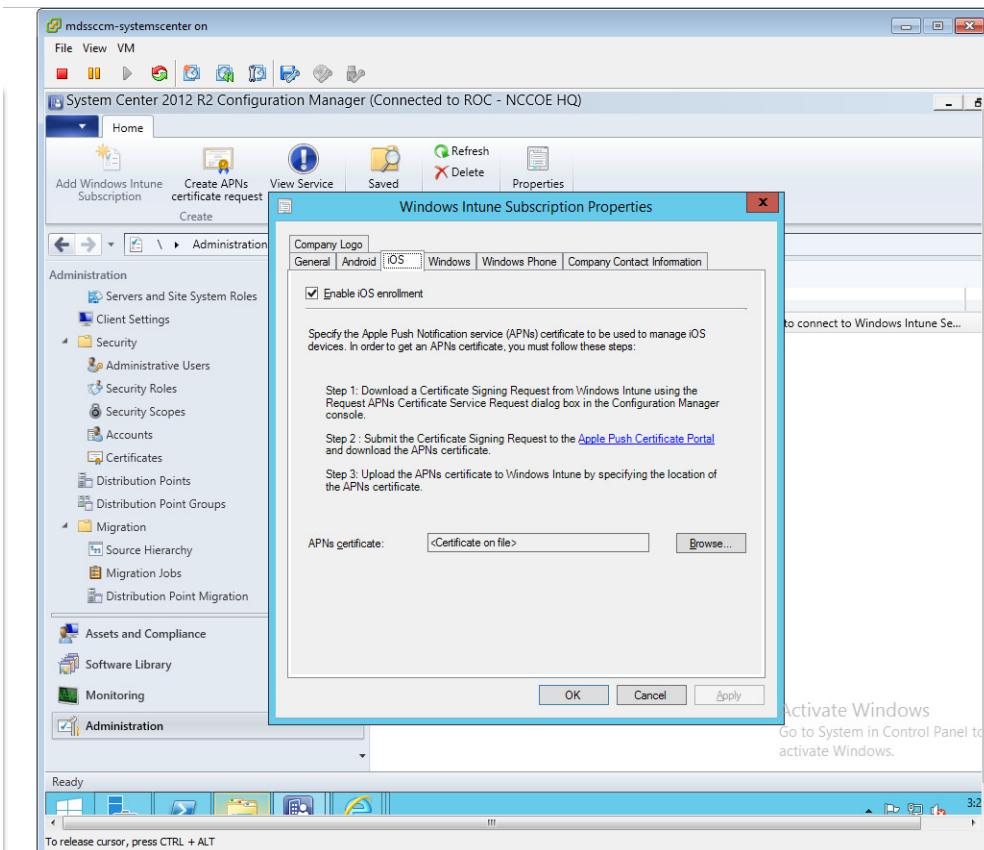
*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

Below the table, there's a section titled "About Apple Push Certificates Portal" with text about creating and managing push certificates for third-party servers. It also mentions MDM push certificate migration and contact information for assistance. To the right of the text is a graphic of a globe with signal waves emanating from it.

At the bottom of the page, there are links for the Apple Online Store, Apple Retail Store, reseller, Apple Info, Site Map, Hot News, RSS Feeds, Contact Us, and a flag icon for the United States. Copyright information and terms of use are also present at the very bottom.

293

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



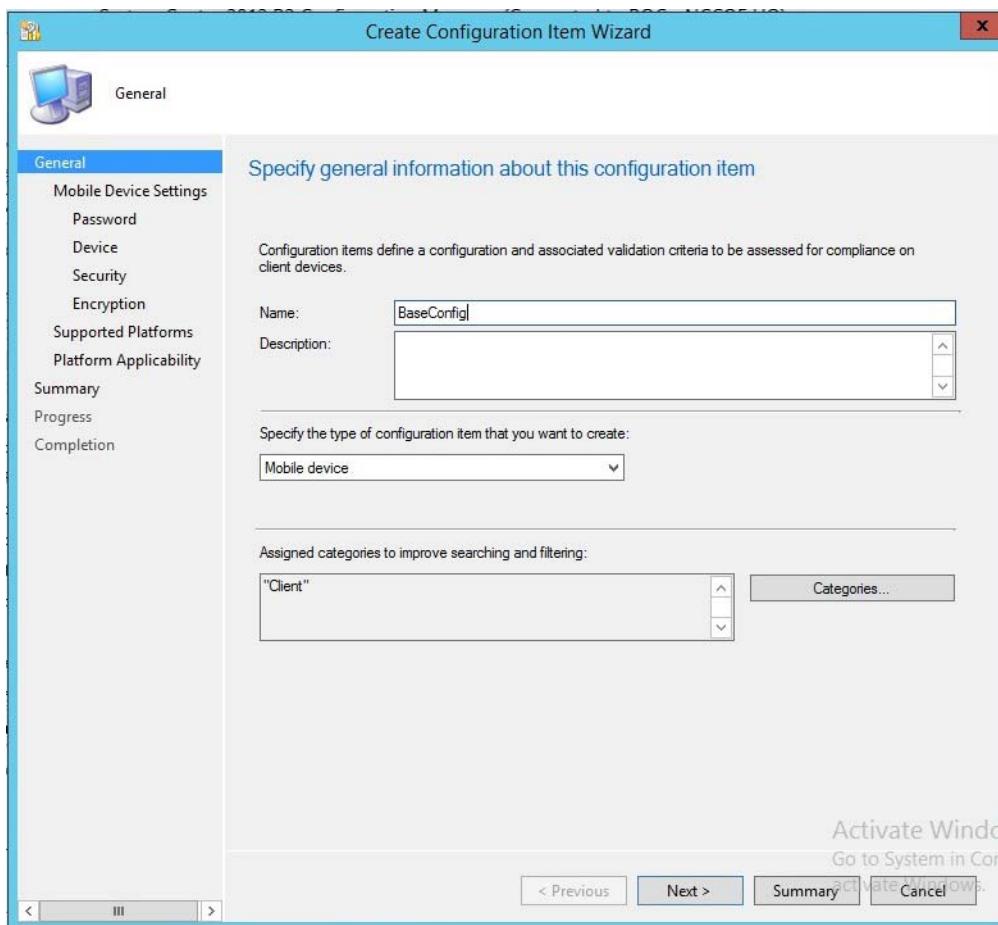
297

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

300 **3.2.5.4.4 Mobile Policy Creation**

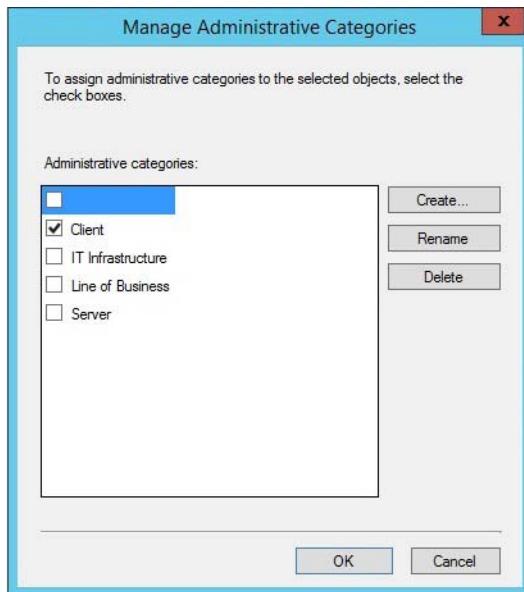
301 This section depicts the creation and deployment of a security policy for mobile devices in the
302 building block test environment. The reader should note that not all options are available to
303 every mobile operating system. Generally, iOS offers more fine-grained device management
304 capabilities than Android; however, a KNOX enabled Samsung Android device augments the
305 base Android capabilities with additional management functions. More information regarding
306 specific capabilities of supported mobile platforms can be found on Technet [5].

- 307 1. Launch the Create Configuration Item Wizard from the SCCM Configuration Manager. In the
308 Assets and Compliance section, click **Configuration Items** in the Compliance Settings folder.
309 Click **Create Configuration Item** from the tool bar.



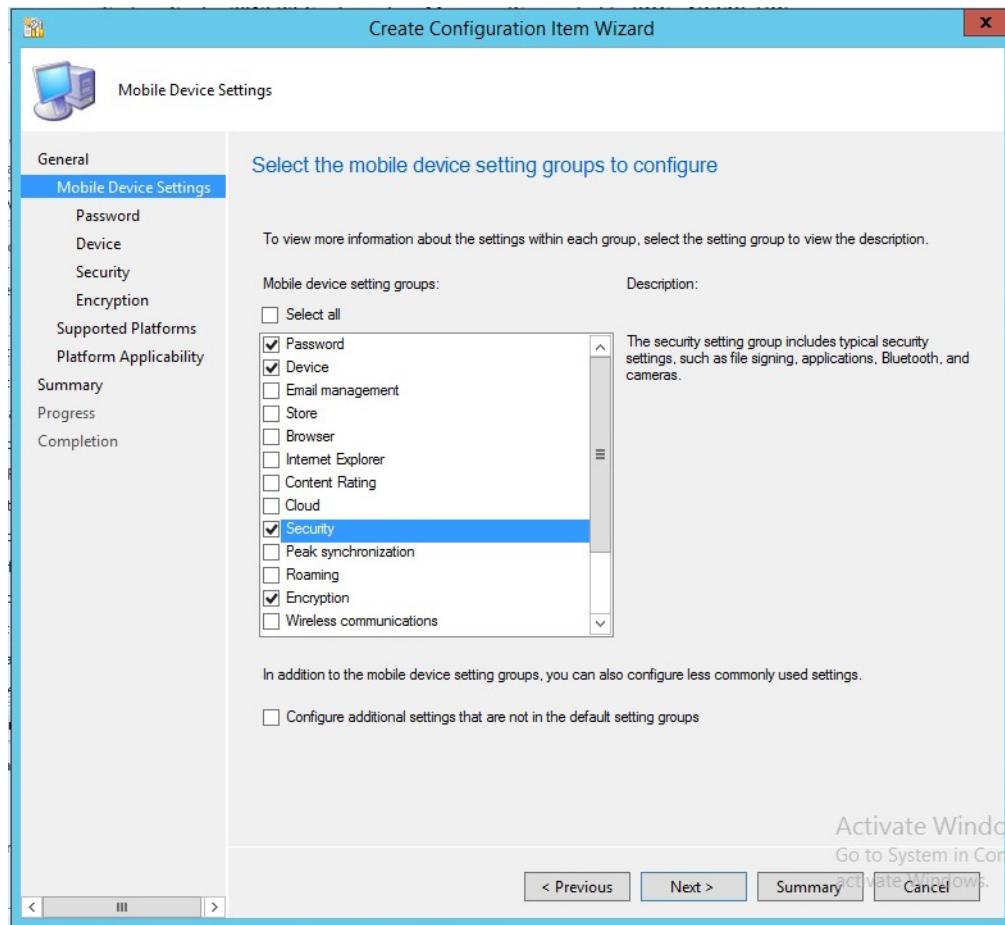
310

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



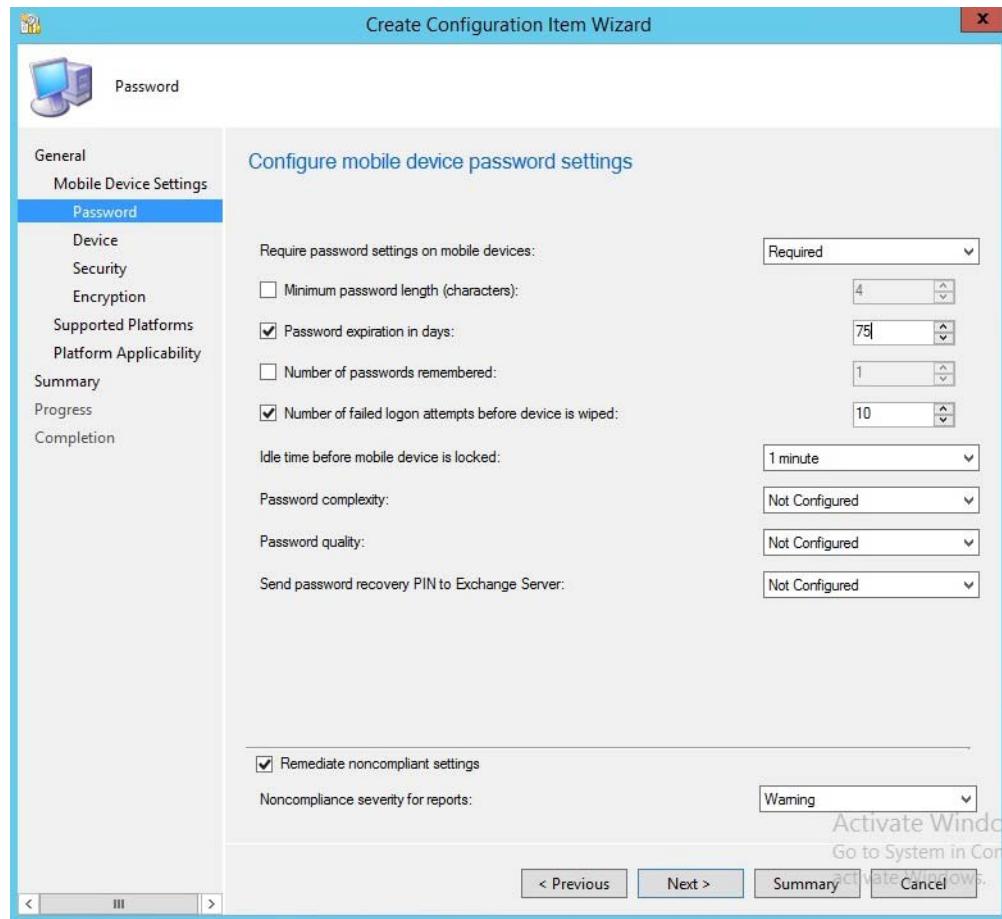
313

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



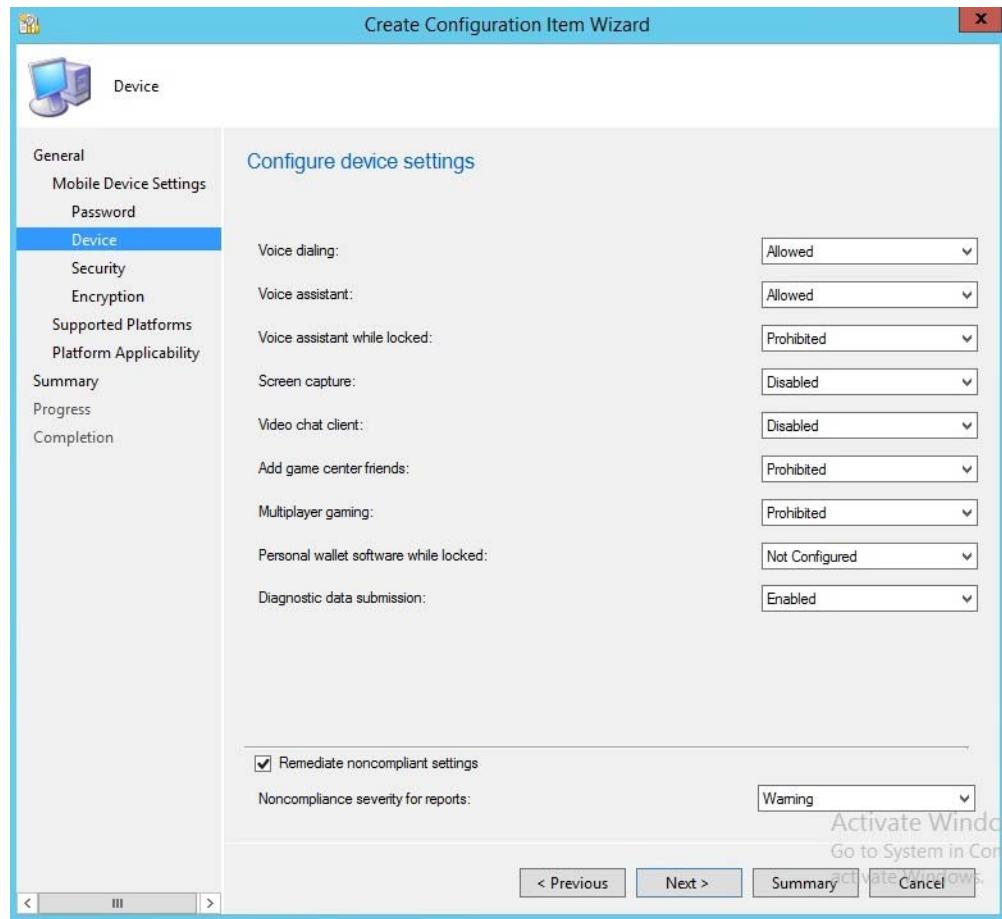
315

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



317

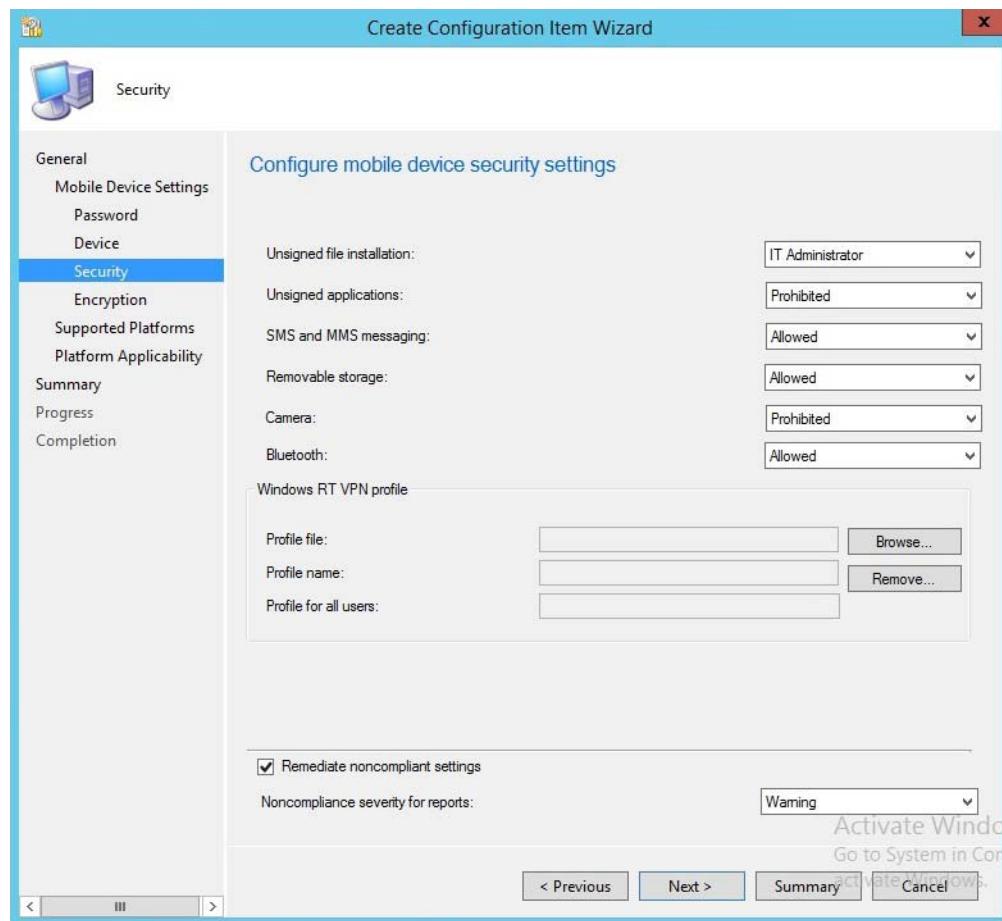
- 318 5. Configure the password requirements based on your local requirements.



319

320

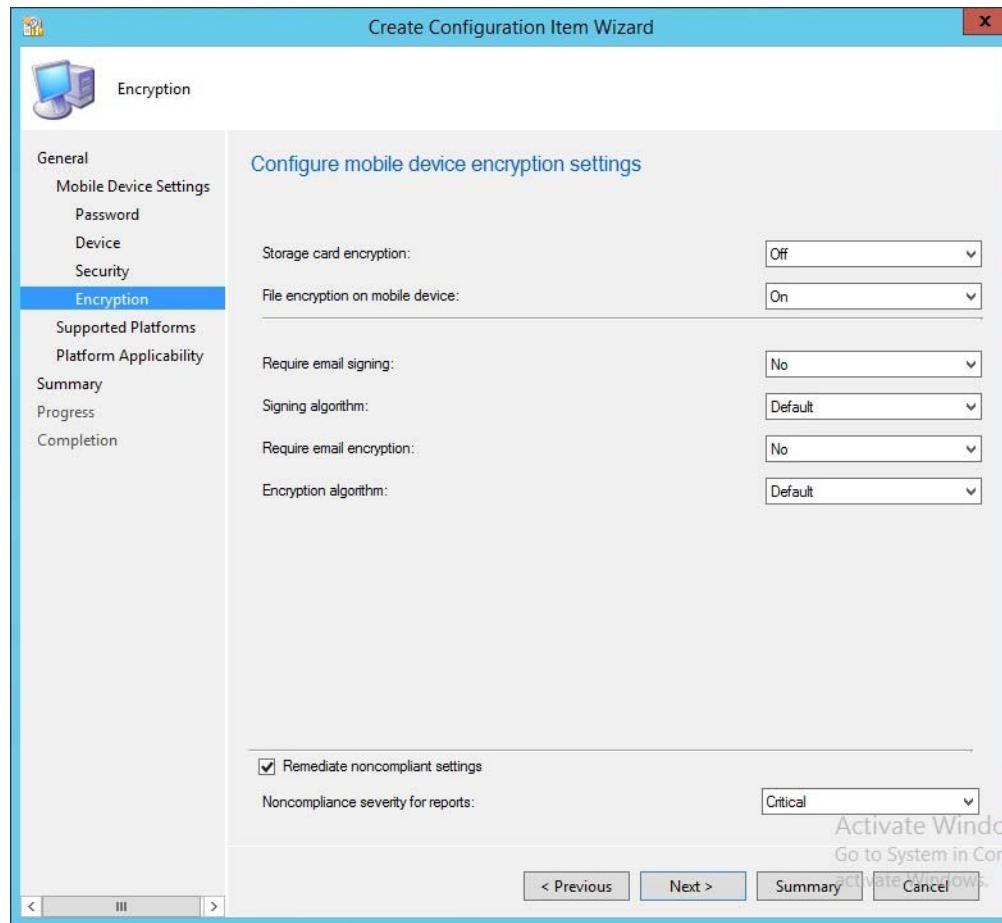
6. Configure the device settings based on your local requirements.



321

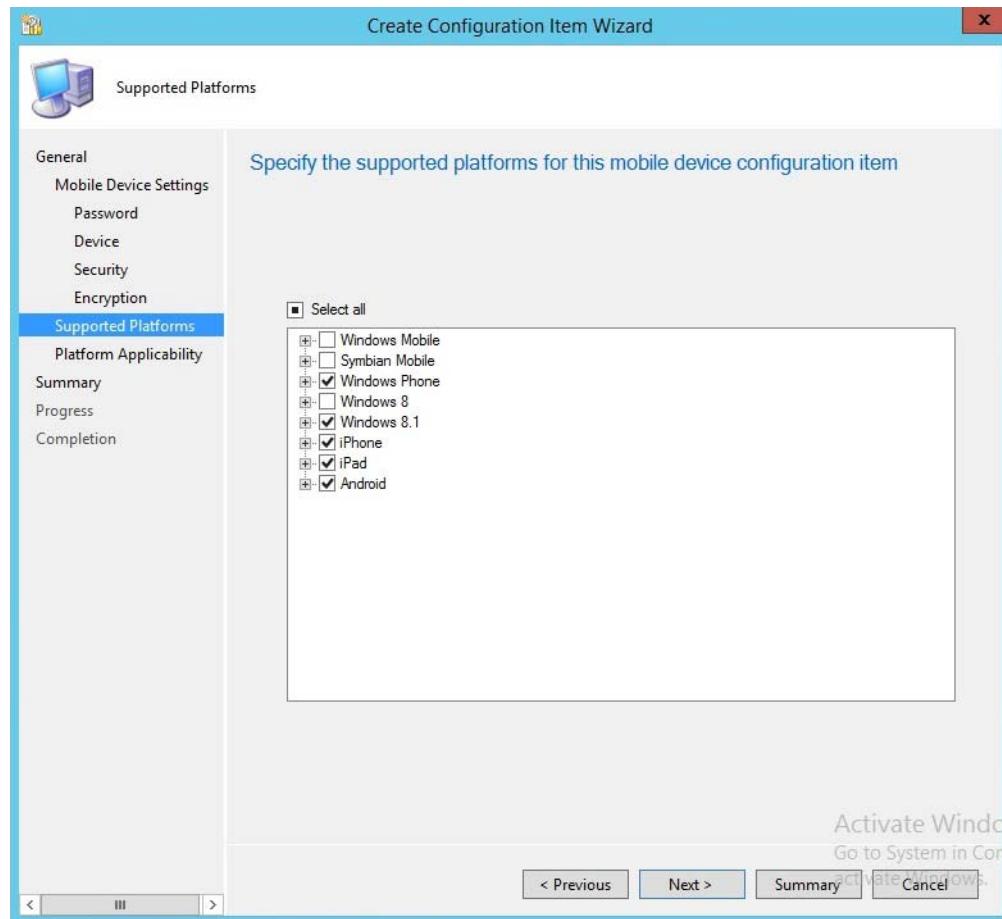
322

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



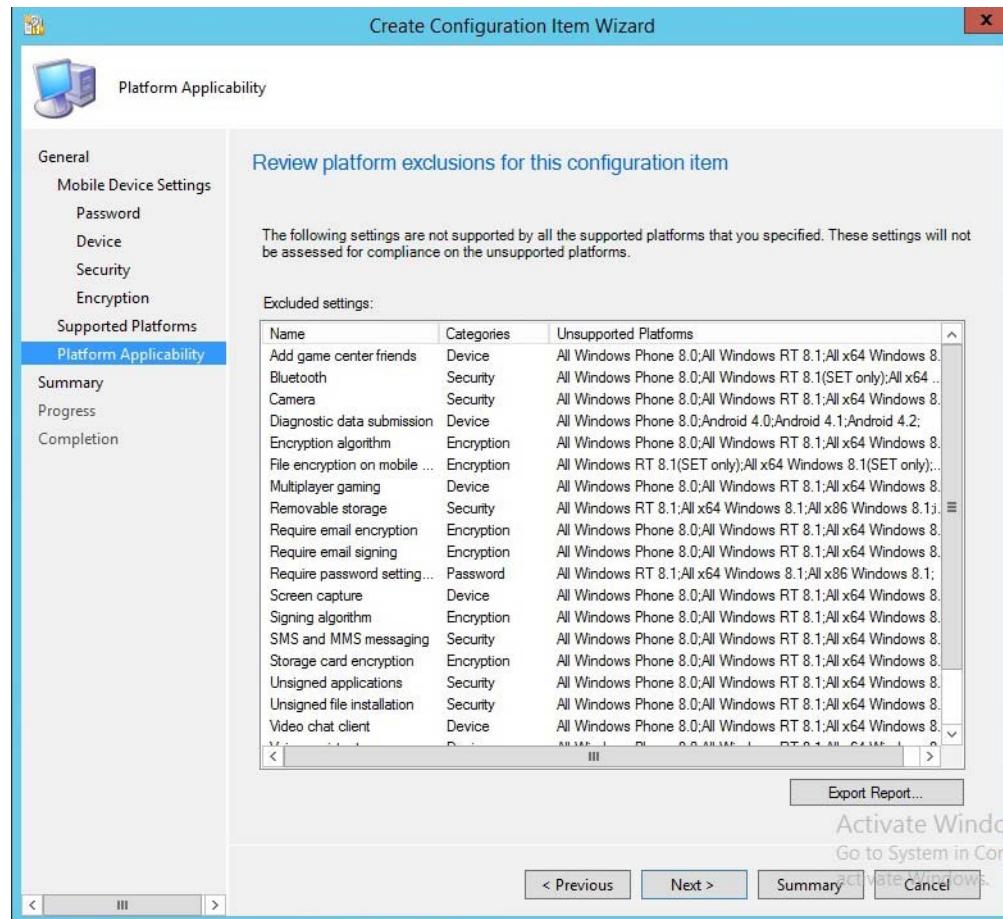
323

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



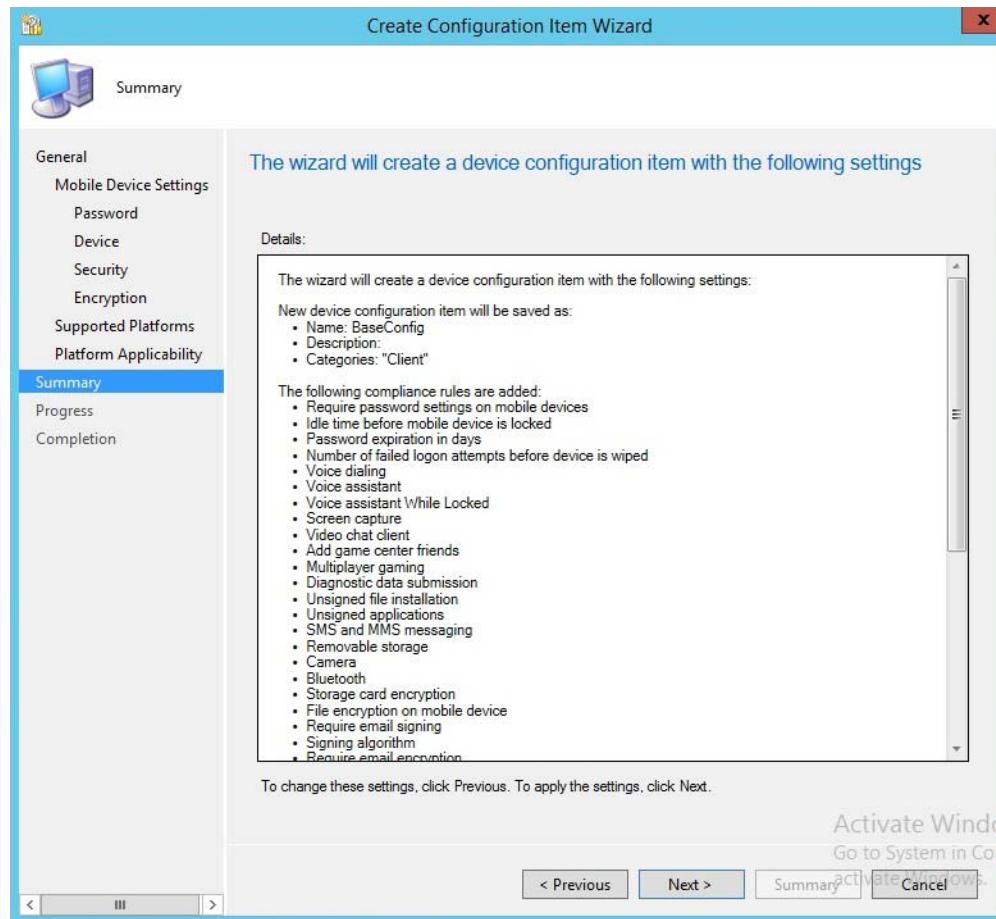
325

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



327

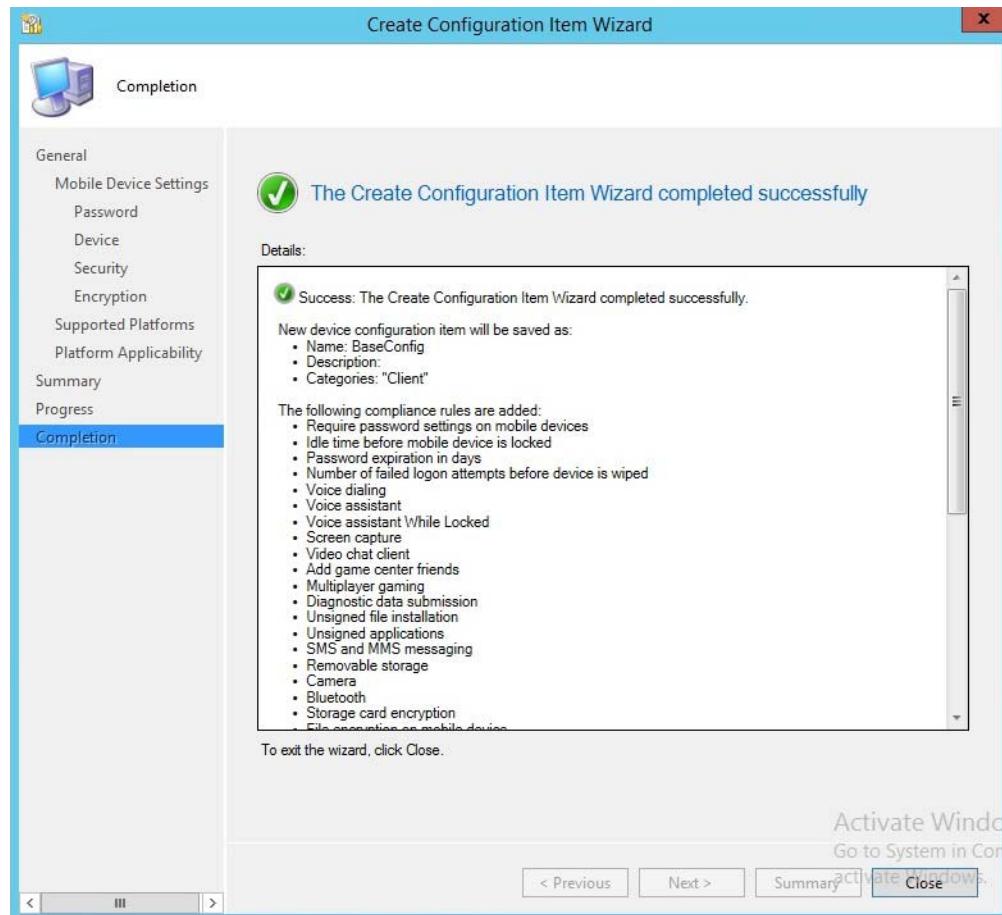
10. Click **Next**.



329

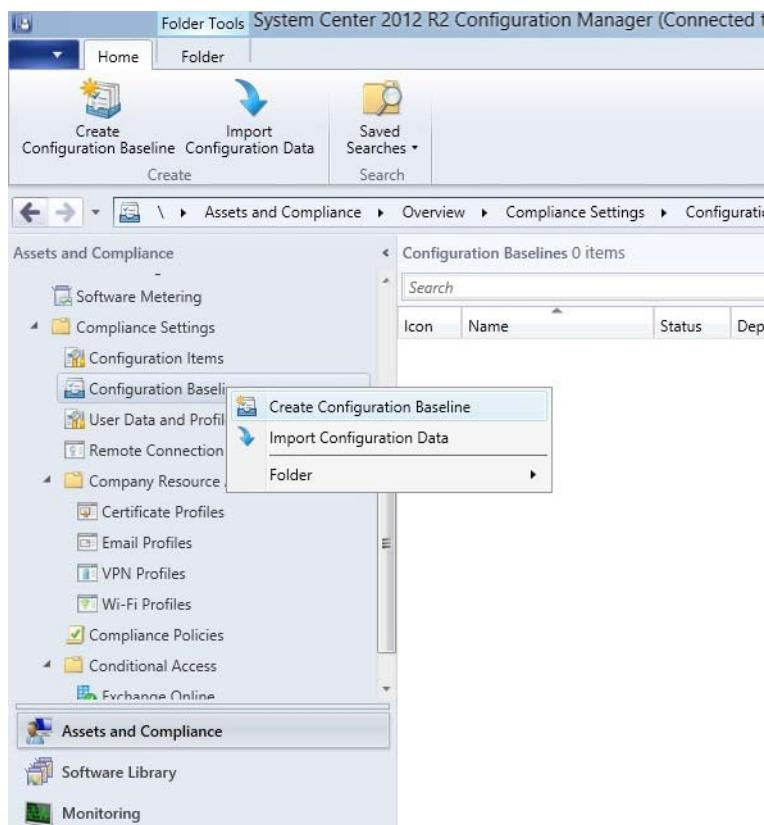
330

11. Click **Next.**



331

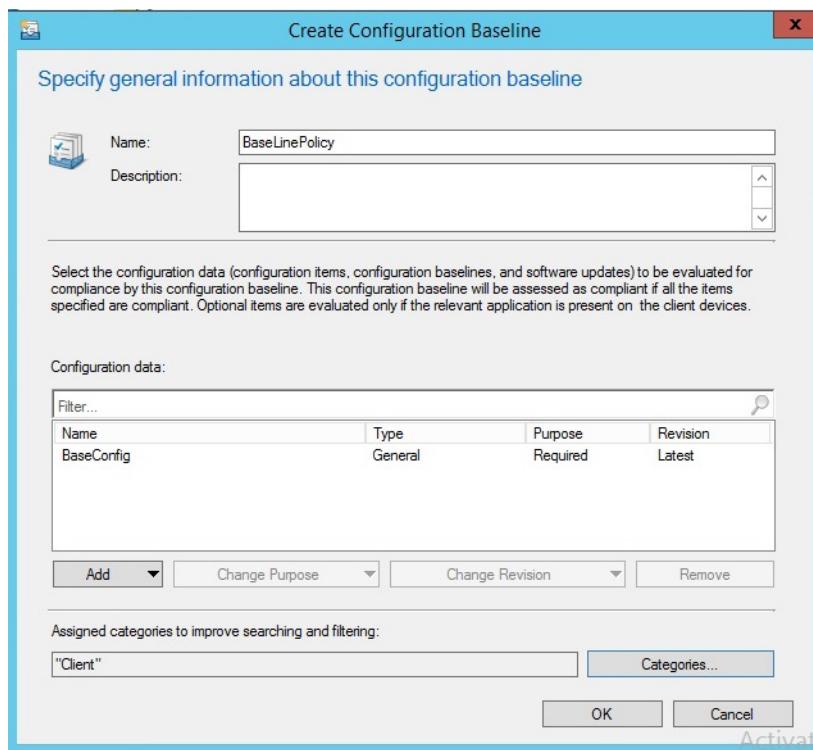
12. Click Close.



333

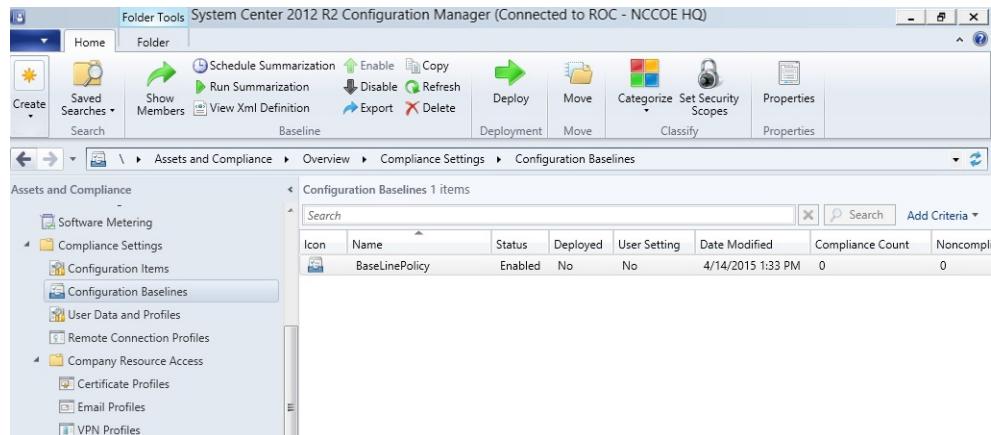
334
335

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



336

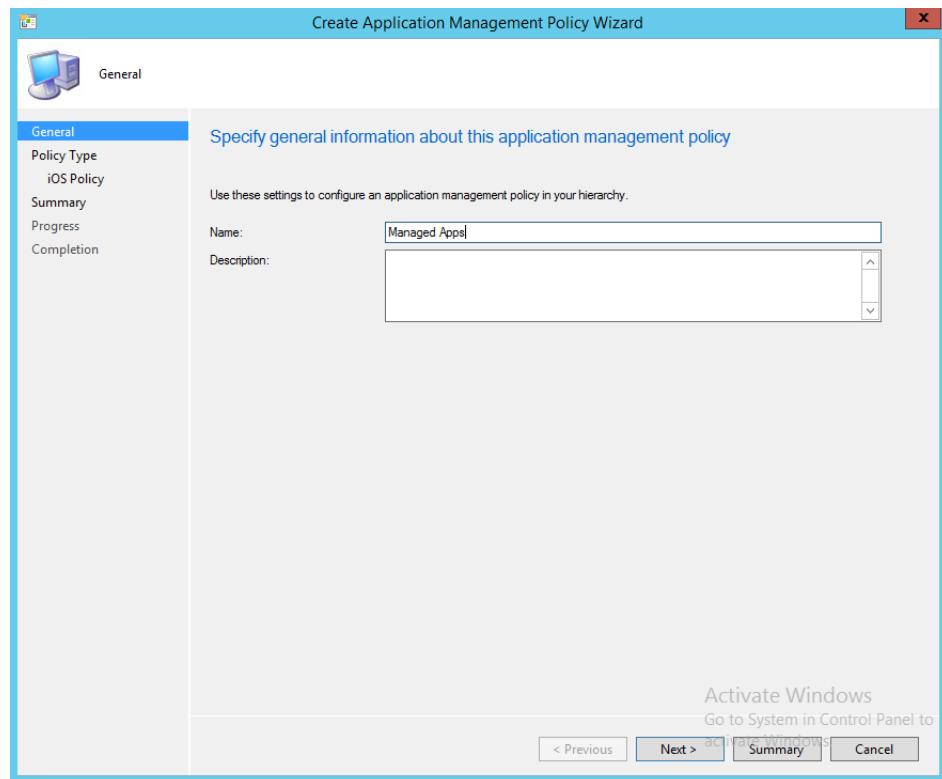
- 337 14. Name the baseline policy. Add the baseline configuration created in the previous steps and click **OK**.
- 338



339

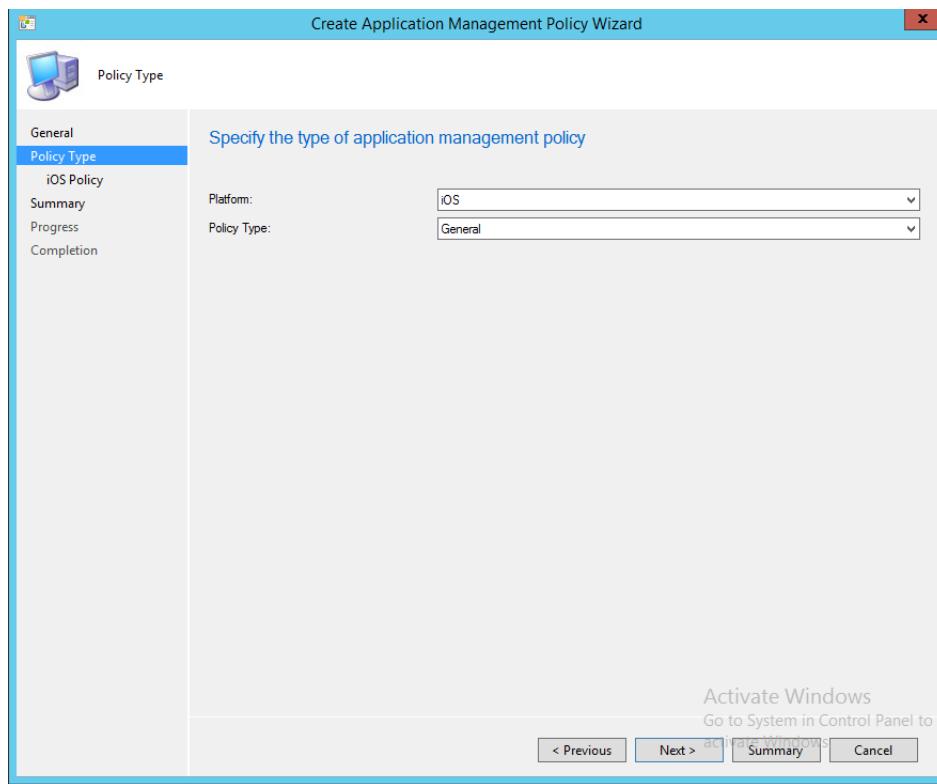
340 3.2.5.4.5 Create Mobile Application Policy

341 This section describes how to roll out mobile application policy for the Outlook mobile
 342 application. The policy is automatically deployed when the device owner installs the application
 343 for the first time. First, the SCCM administrator will create a new application management
 344 policy, then associate an application to the newly created policy. The following procedures
 345 feature the iOS platform, but the process is essentially the same for other platforms.



346

- 347 1. To start the wizard, navigate to **Under Software Library > Application Management >**
 348 **Application Management Policies: Create Policy** in the SCCM console. Click **Next**.

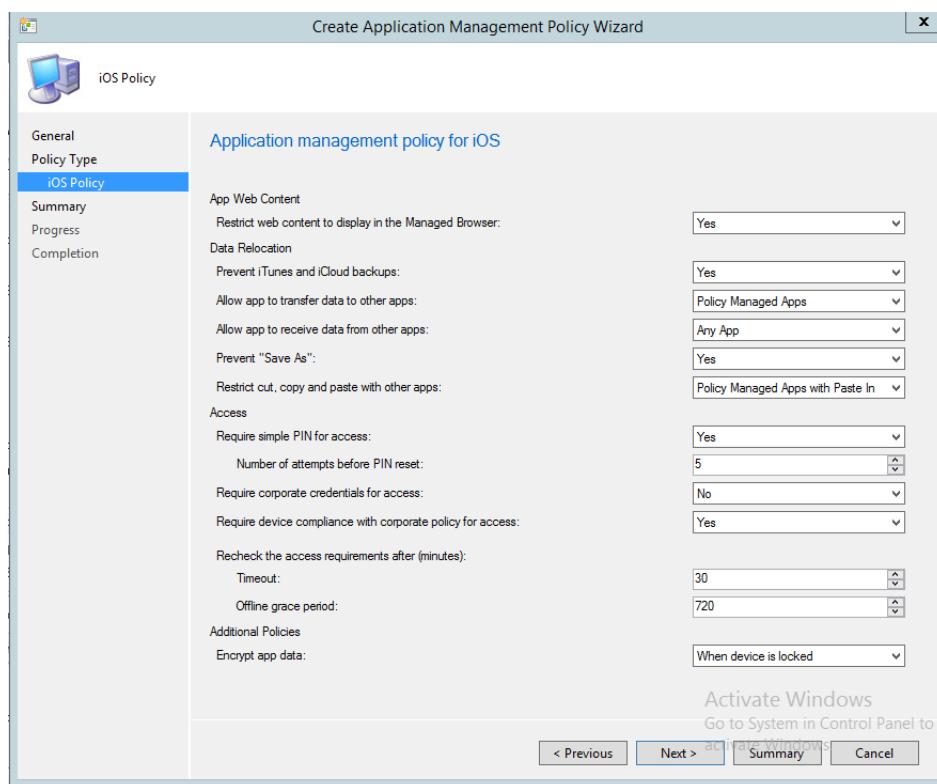


349

350

351

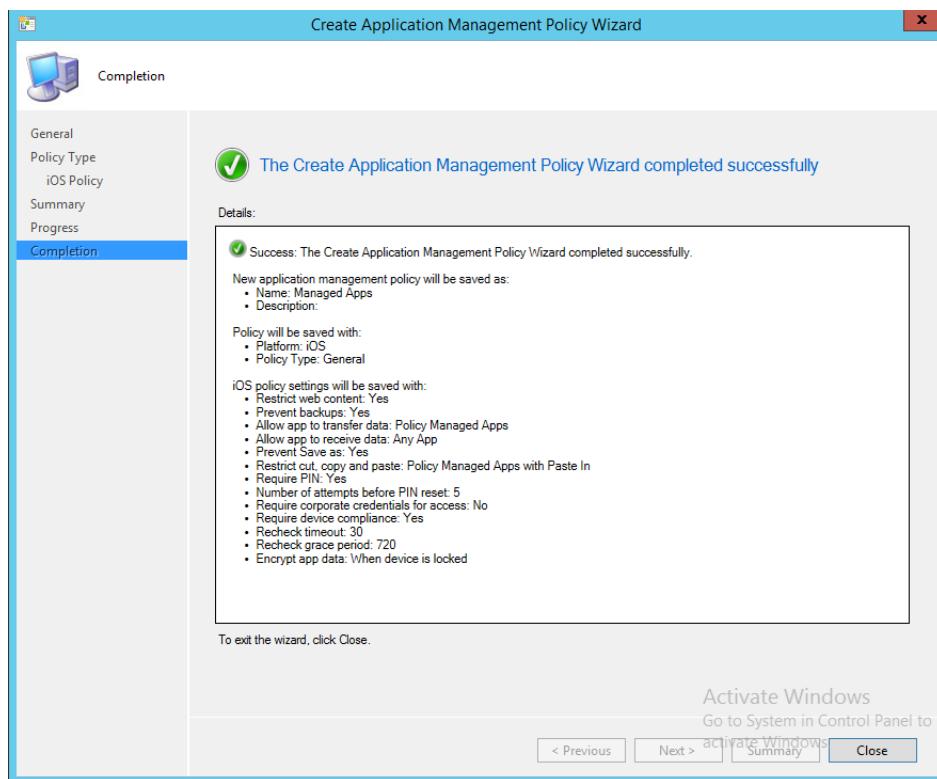
2. Choose the platform type and policy type. In this example, a policy is being deployed to an iOS app. Click **Next**.



352

353

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

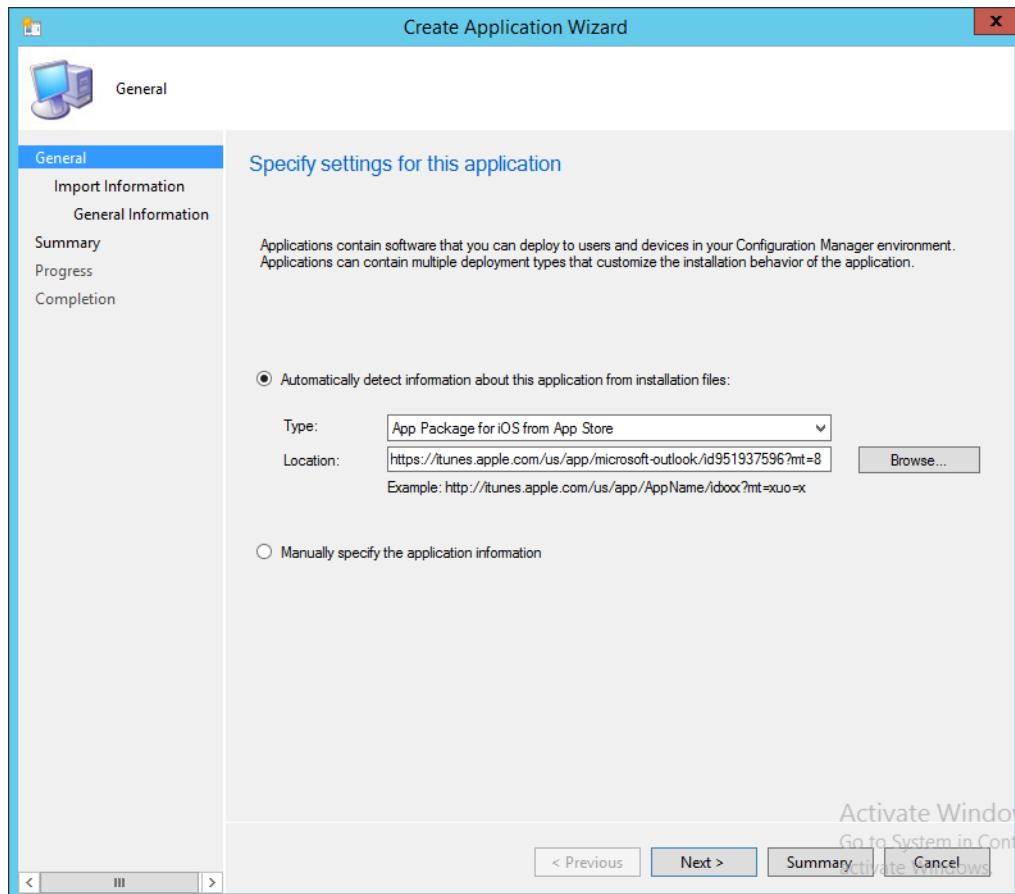


354

- 355
356 4. Upon successful creation, an overview is displayed. The policy needs to be matched with an application before it can be used.

357
358

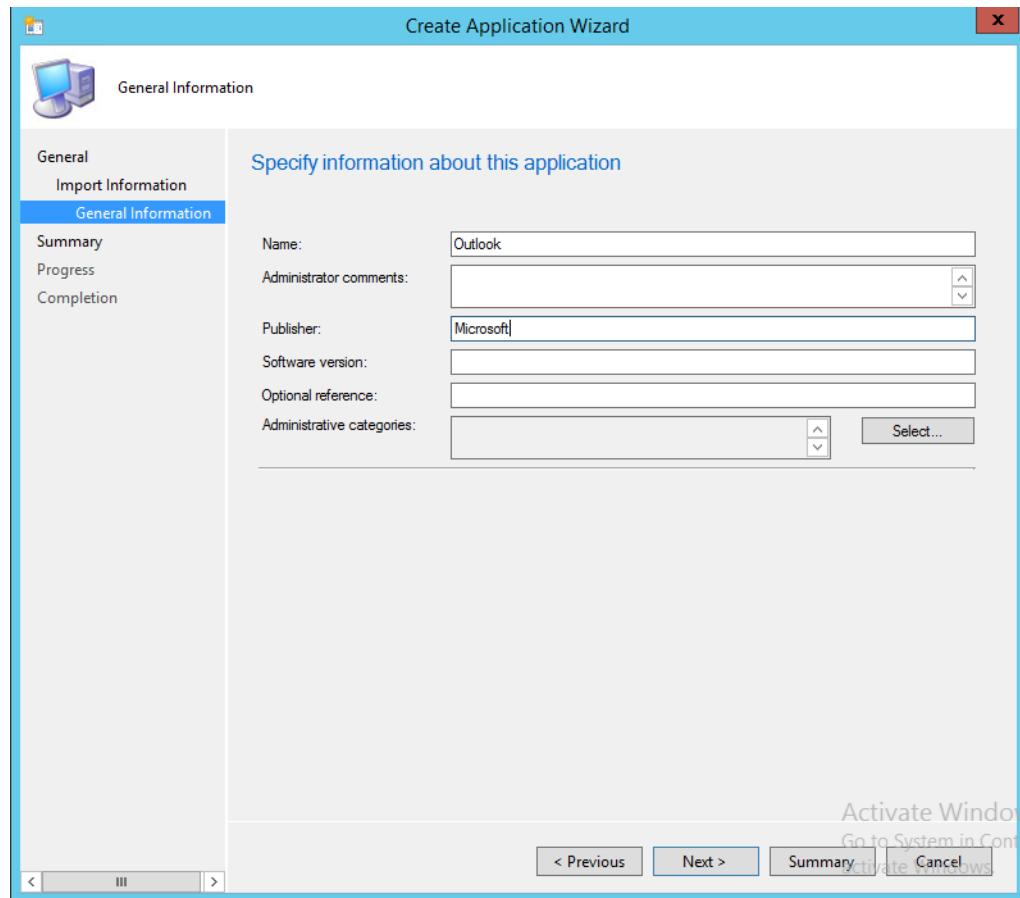
In the next section, the Outlook application is linked to the iOS App store through Company Portal and associated with the previously created application policy.



359

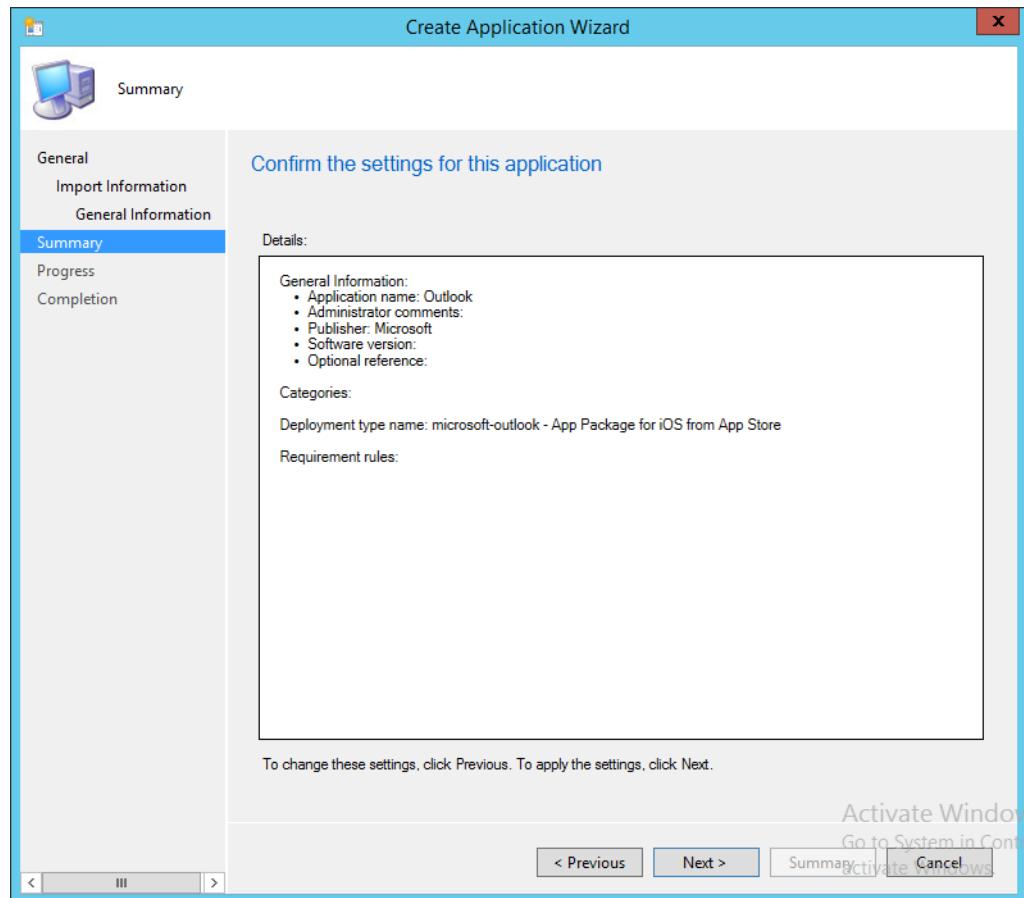
360
361
362

1. 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.



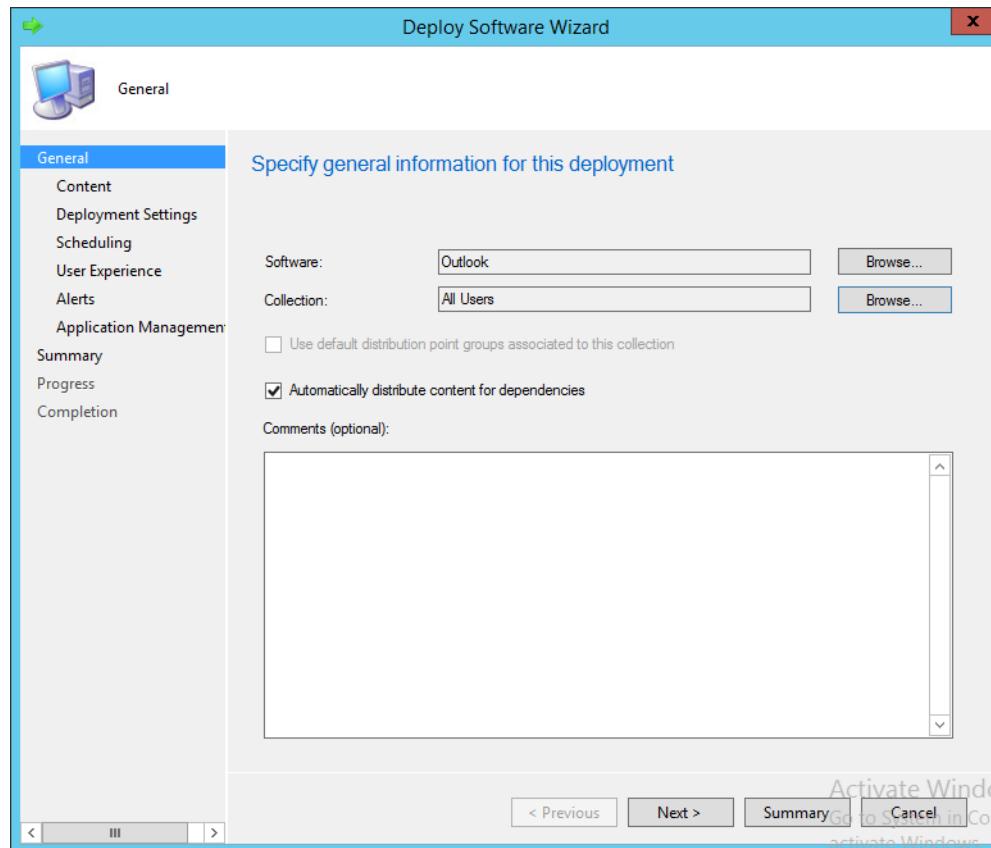
363

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



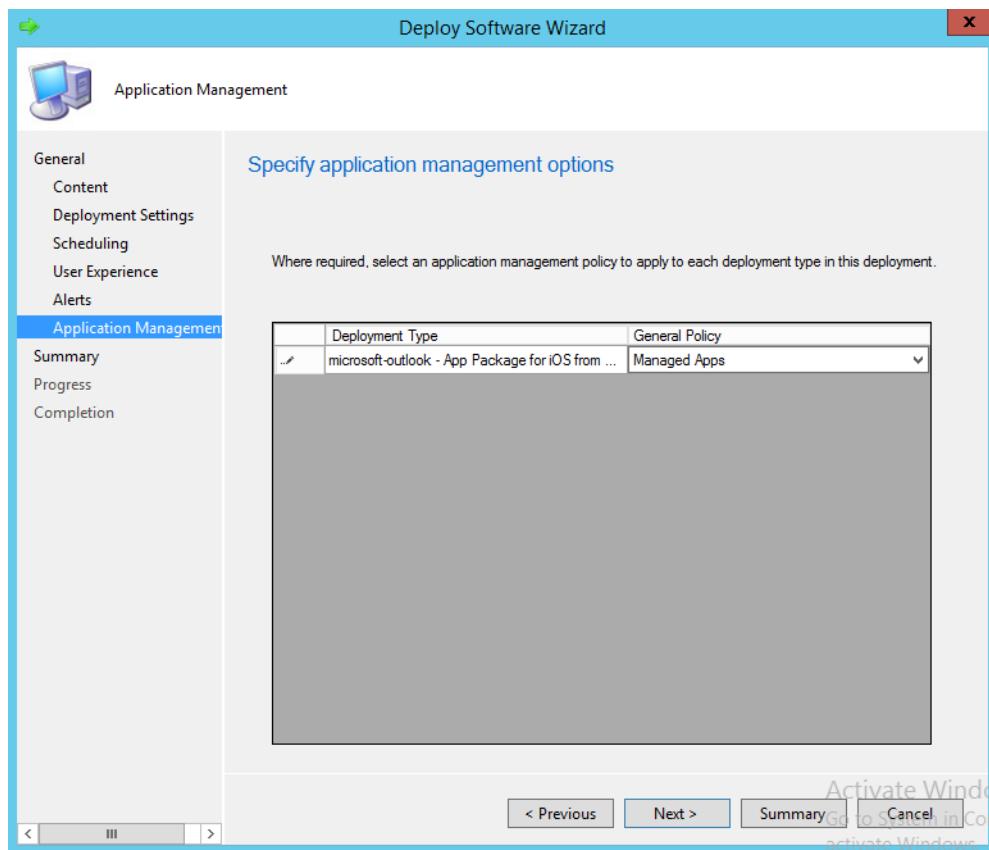
365

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



367

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



369

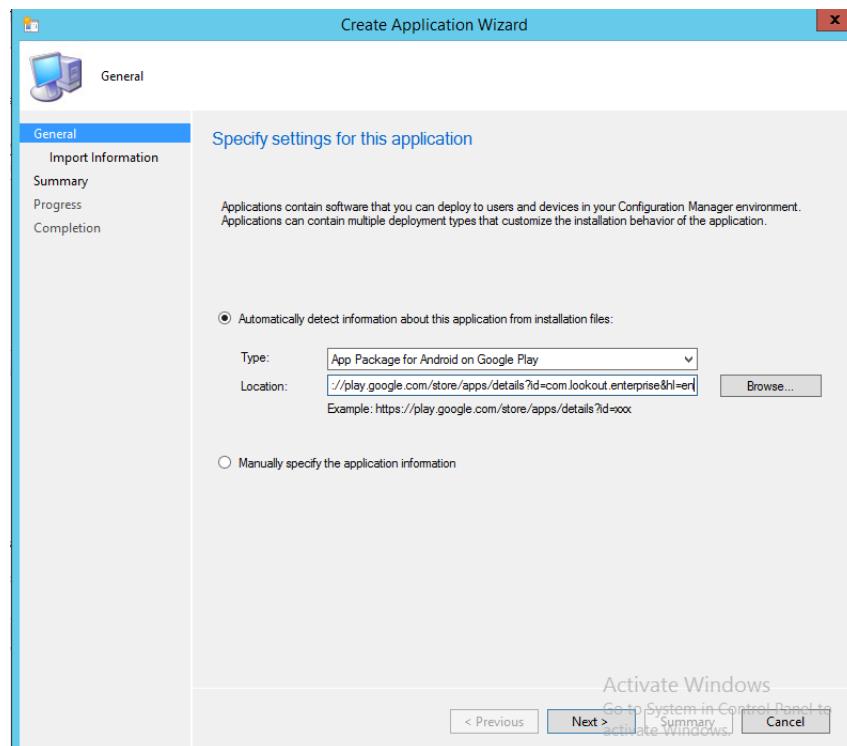
370
371

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

3.2.5.5 Configure SCCM with Lookout Application

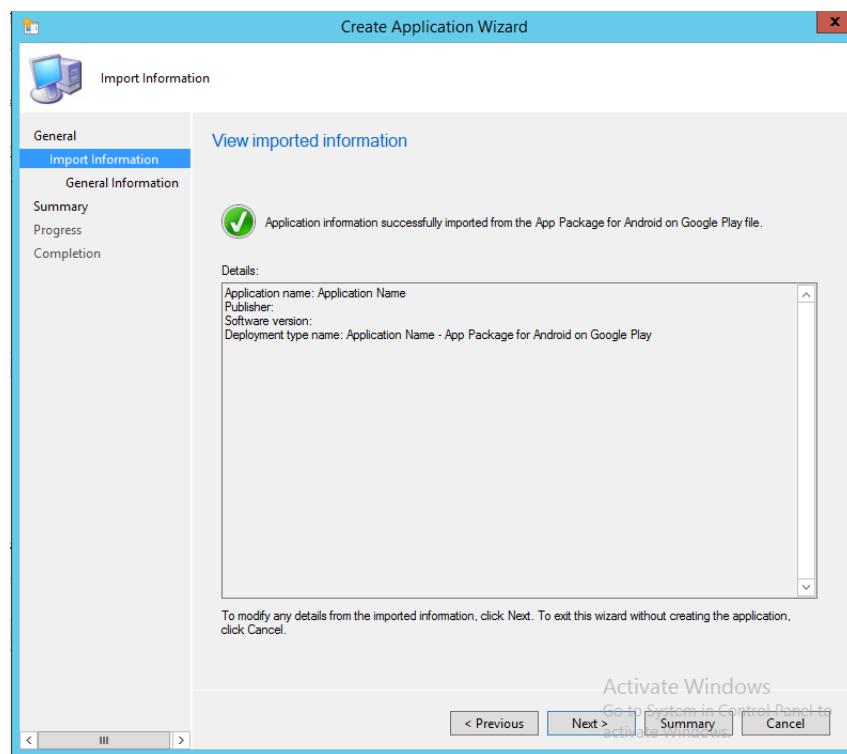
372
373
374
375
376
377

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.



378

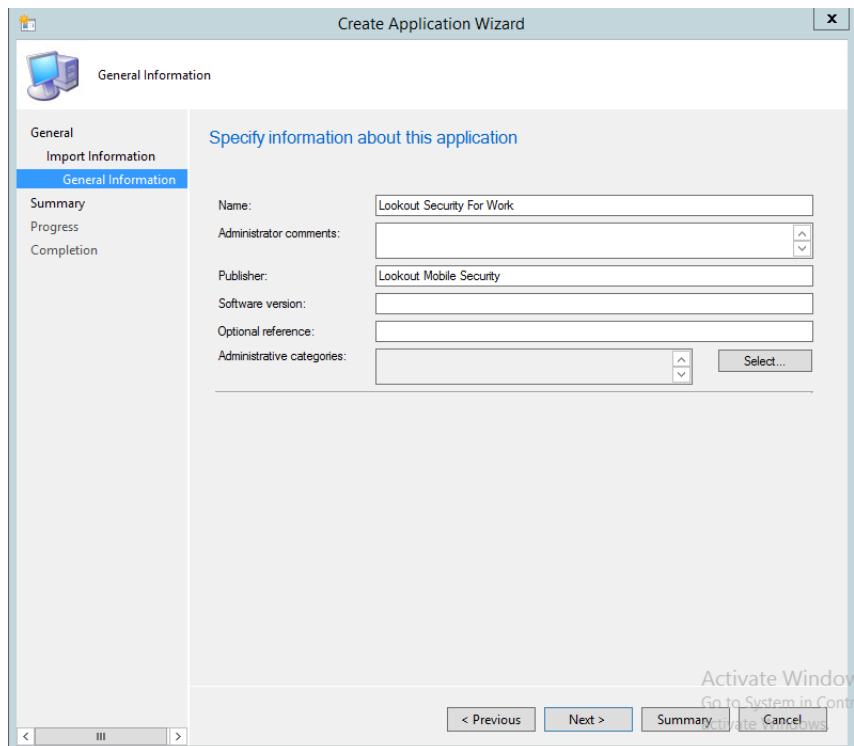
- 379 1. To start the wizard, navigate to General. Select **App Package for Android on Google Play** in
 380 the **Type** drop down. Type
 381 <https://play.google.com/store/apps/details?id=com.lookout.enterprise&hl=en> in the location
 382 field.



383

384

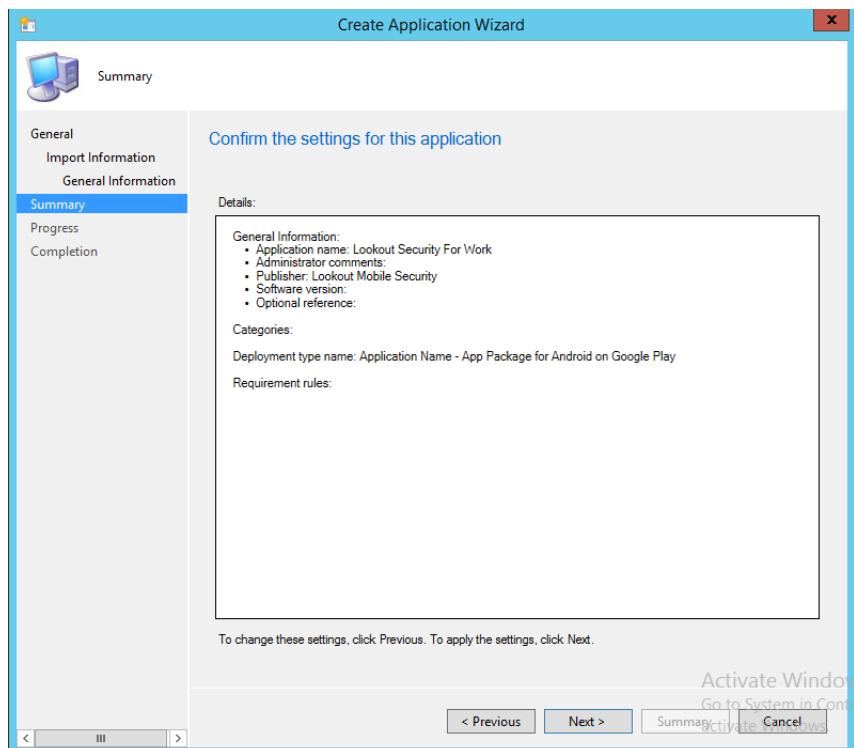
2. Click **Next.**



385

386

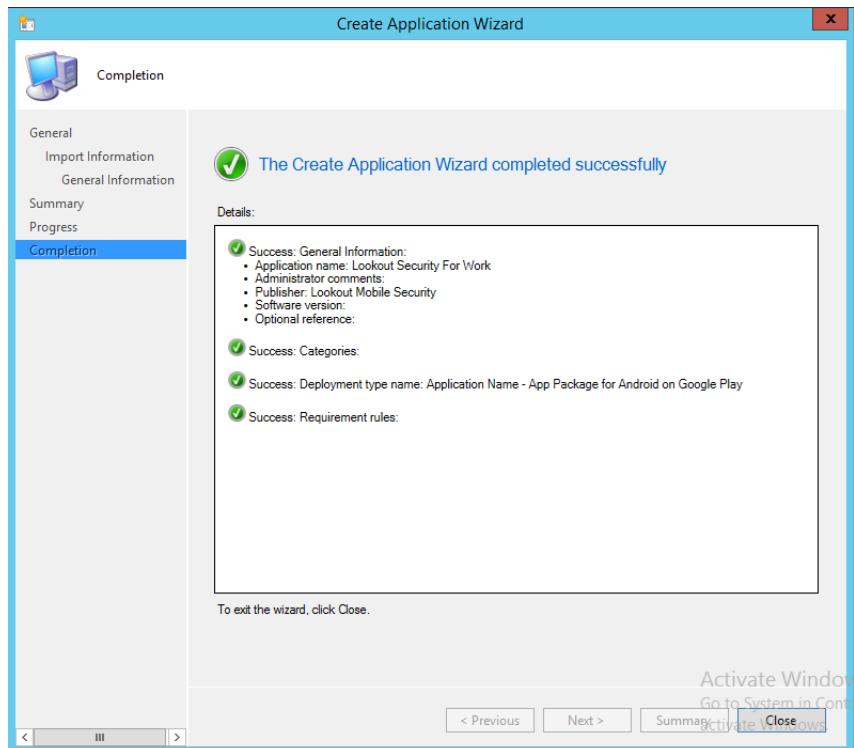
3. Use the suggested text in the **Name and **Publisher** fields. Click **Next**.**



387

388

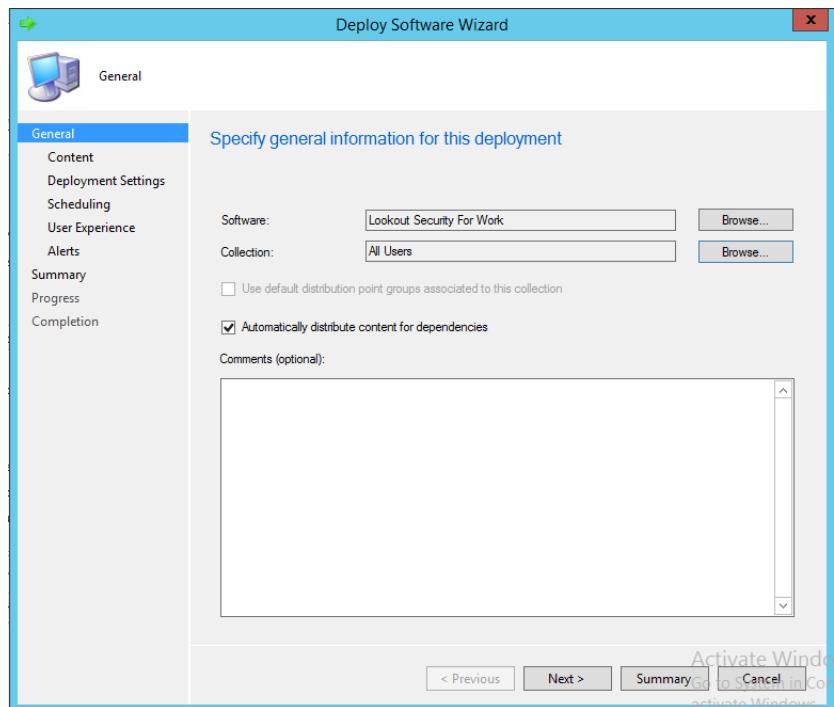
4. Click **Next.**



389

390

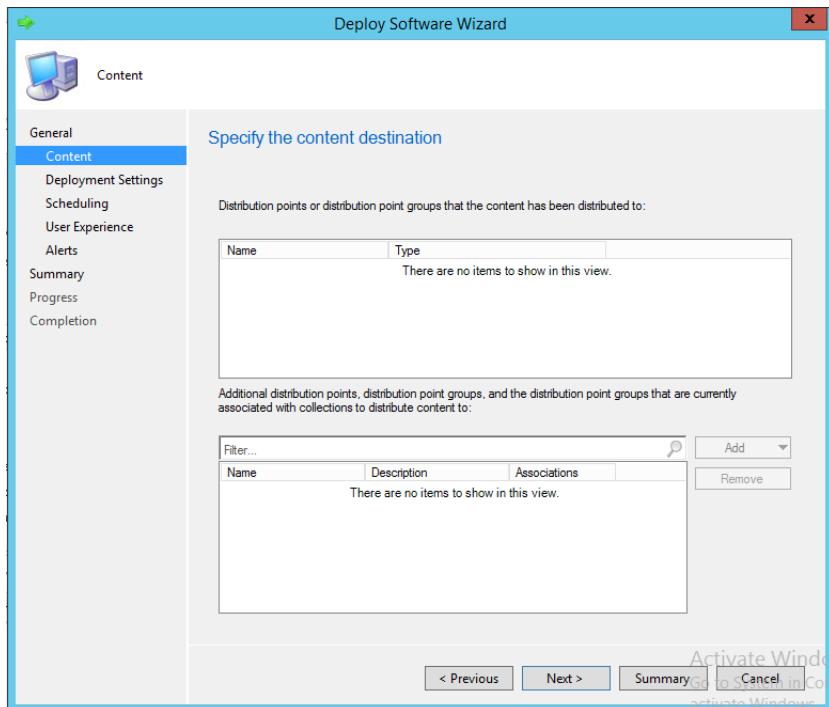
5. Click **Close**.



391

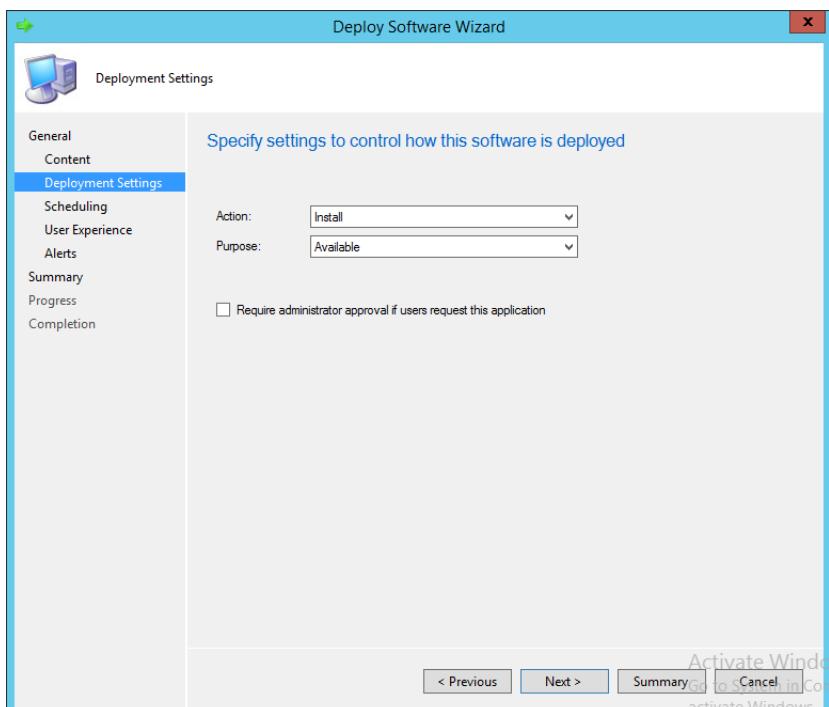
392
393

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



394

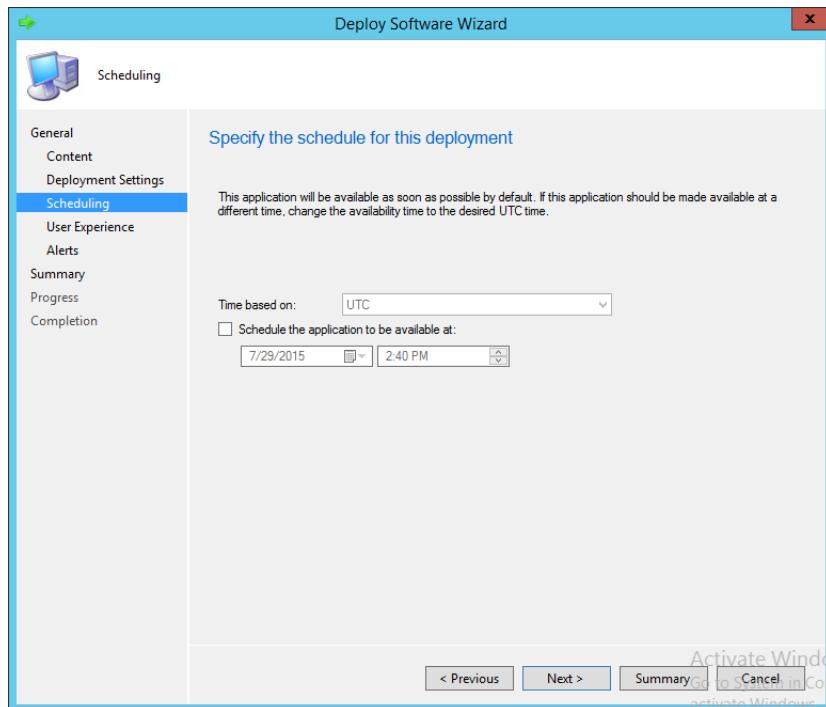
7. Click **Next.**



396

397
398

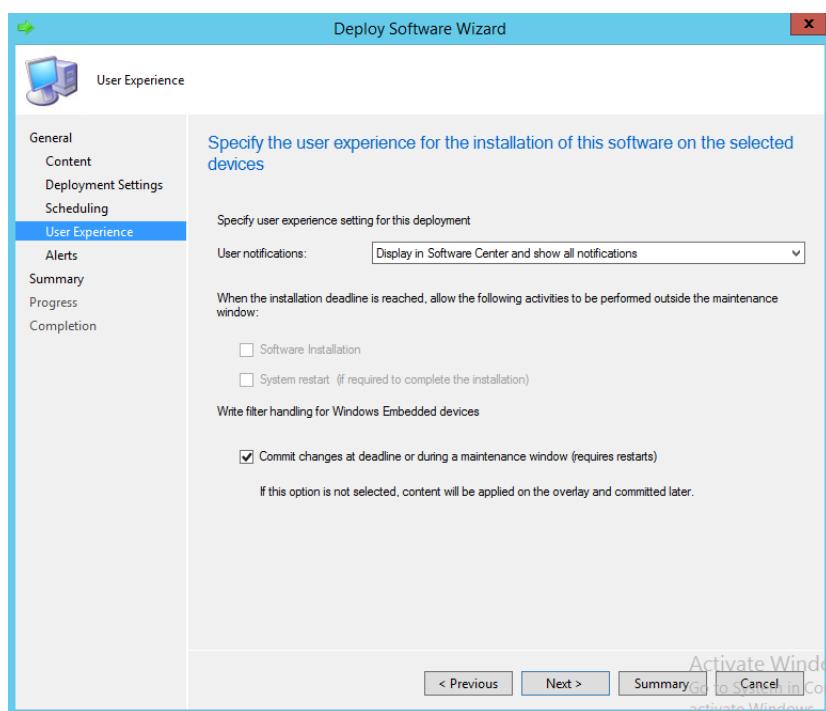
- 8. In the **Action** drop-down, choose **Install**. In the **Purpose** drop-down, choose **Available**. Click **Next**.**



399

400

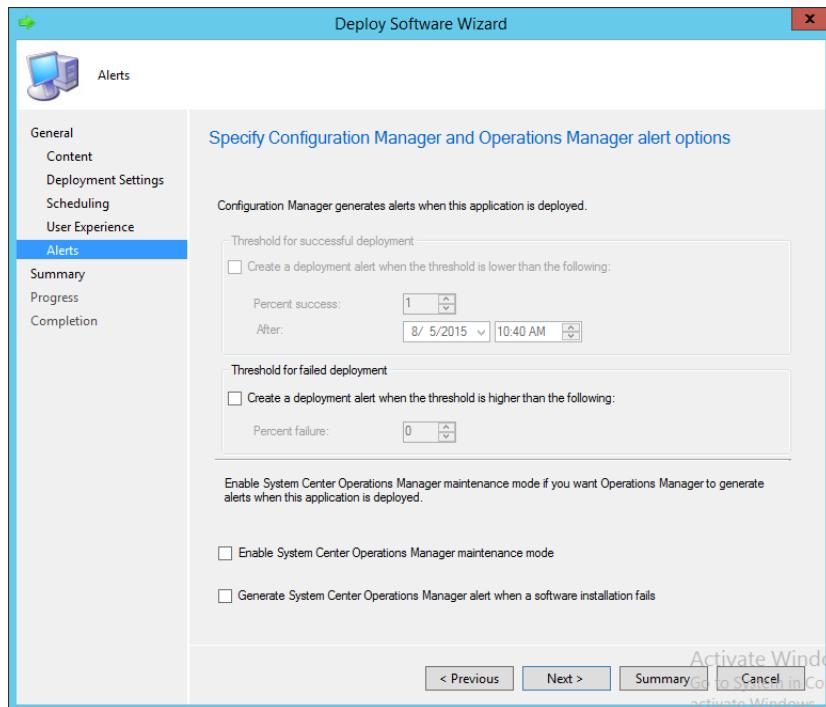
9. Click Next.



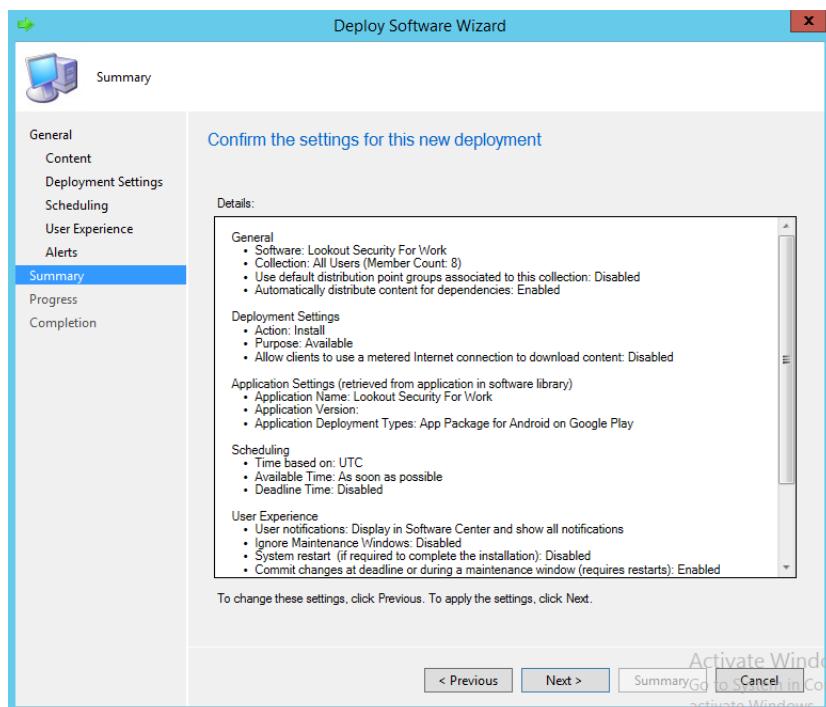
401

402
403

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



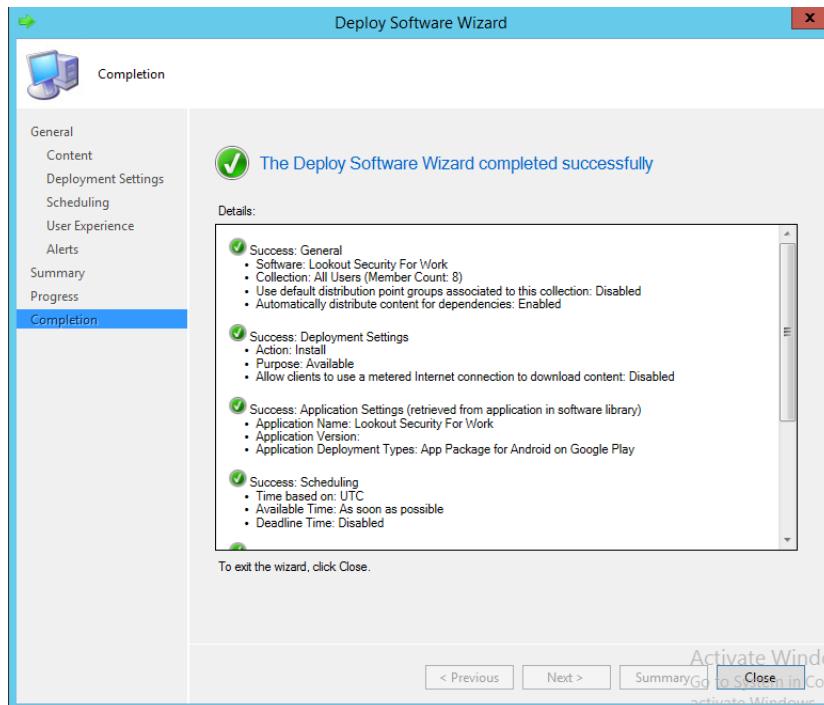
404

11. Click Next.

406

407

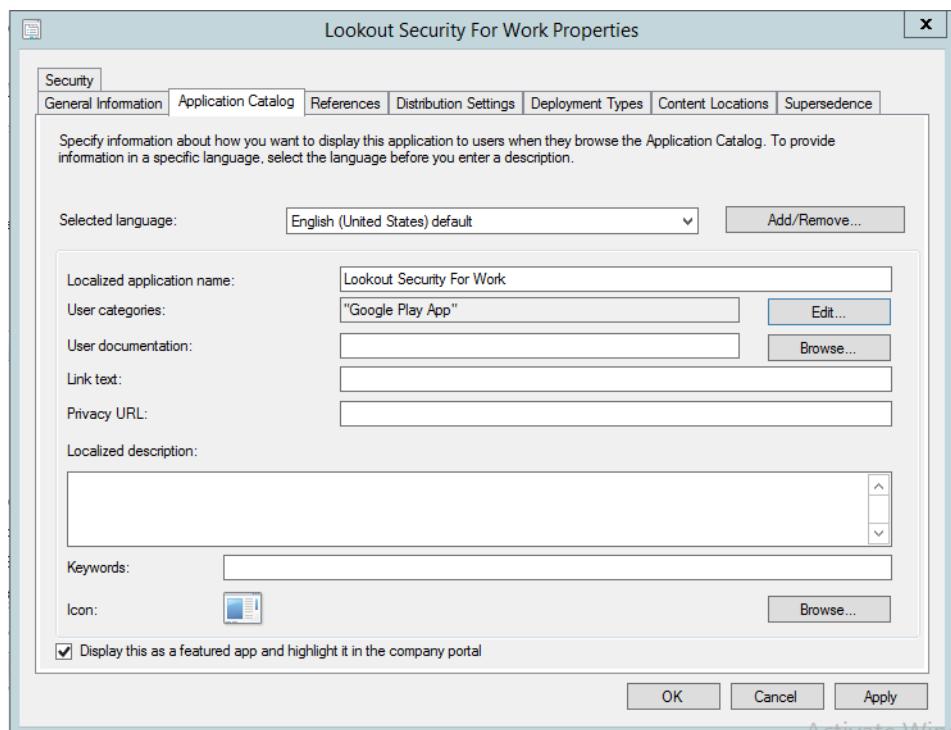
12. Click Next.



408

409

13. Click Close.



410

411

¹ **4** Device Configuration

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

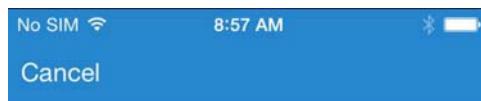
6 This section steps through the configuration of devices. This section is applicable to both cloud
7 and hybrid builds. Here, we feature enrollment and email configuration with iOS, Android and
8 Windows Phone operating systems.

9 4.1 Device Enrollment with Office 365

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

16 Instruct device owners to download the Company Portal application through the application
17 distribution point of their platform to start the enrollment process.⁹ This is not necessary for
18 Windows Phone devices because MDM management through this service is native to the
19 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.

²⁰ 4.1.1 iOS

Intune Company Portal

Sign in with your work or school account

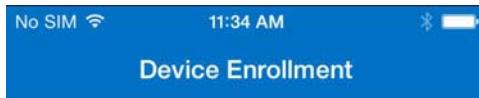
 [Can't access your account?](#)

Your work or school account can be used anywhere you see this symbol. © 2015 Microsoft [Terms of use](#)

[Privacy & Cookies](#)

2122
23

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



Company Portal allows you to connect your device to Microsoft Intune, and to download applications made available to you by your workplace.

If you choose to allow your company to manage your device using Microsoft Intune, your workplace may apply settings, collect info, install or remove apps, and may be able to wipe your device and return it to its factory settings. Talk with your IT admin or consult your company's privacy policy to learn more about your specific workplace.

If you select Enroll, you grant permission to allow your company to manage this device.

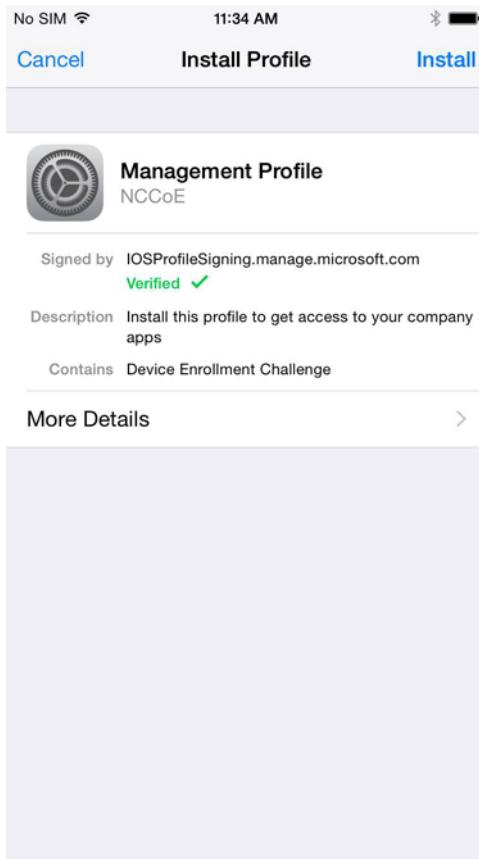
[More information about enrolling your device](#)

Enroll Cancel

24

25

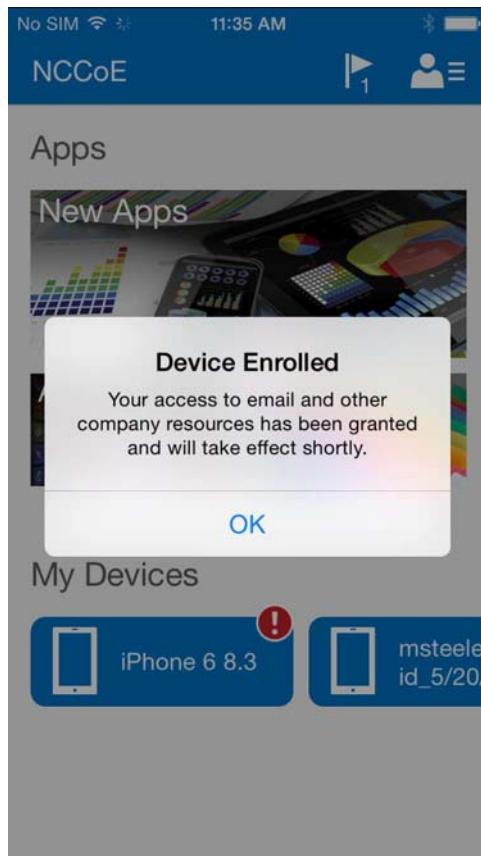
2. The user will then be asked to enroll their device and accept the organization's policies.



26

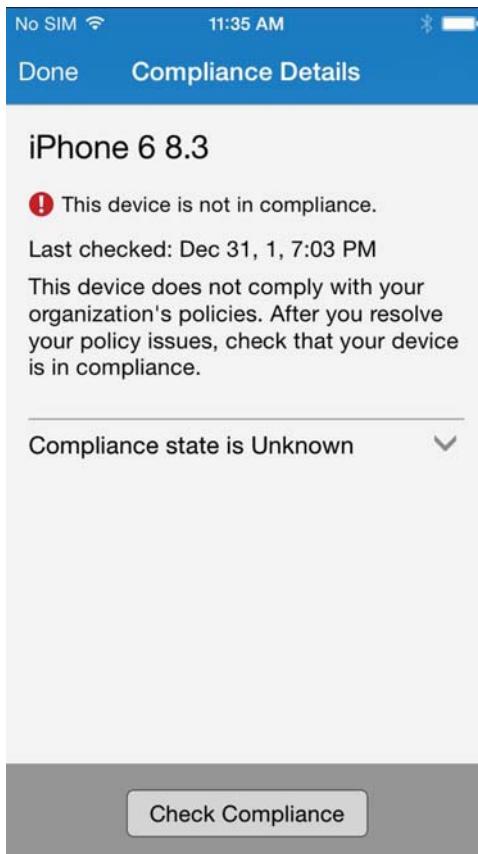
27
28

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



29

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



32

33

5. 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 in the company portal.

34

35

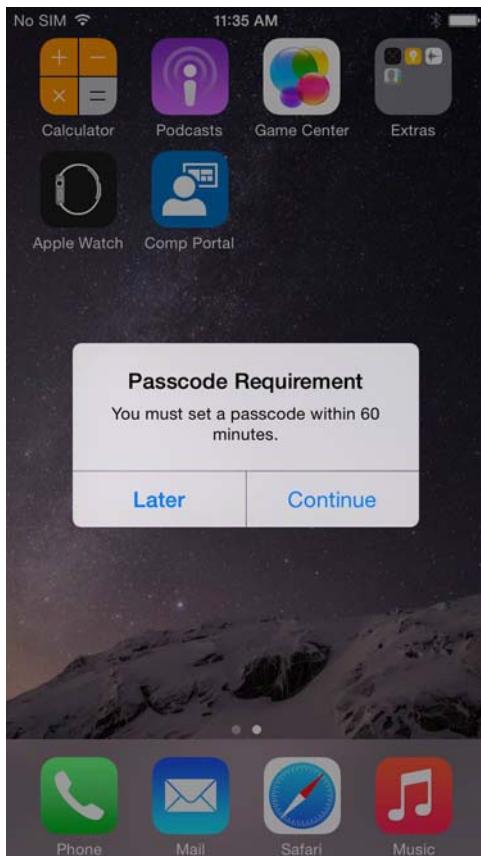


36

37

38

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



39

40
41
42

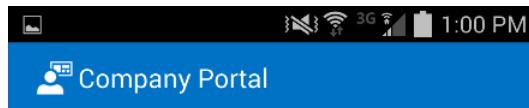
7. Upon minimizing the company portal application during the compliance checking process, the user is presented with the password remediation process, alerting the user to change their password within the hour.



43

44
45

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

⁴⁶ 4.1.2 Android

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](#)

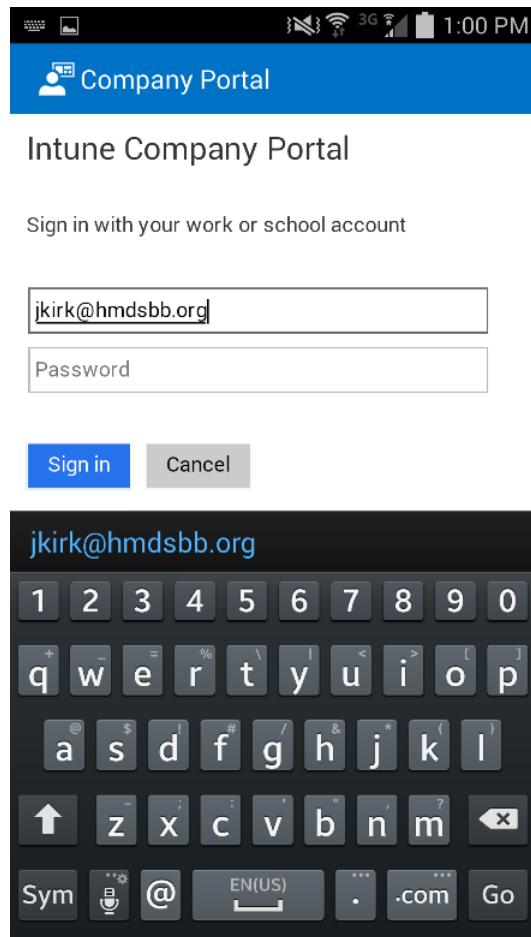
Cancel

Next

⁴⁷

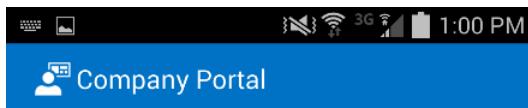
⁴⁸

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



49

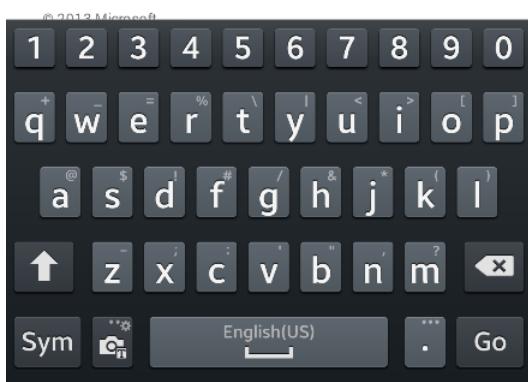
2. Enter your email address.



HMDSSB

Sign in with your organizational account

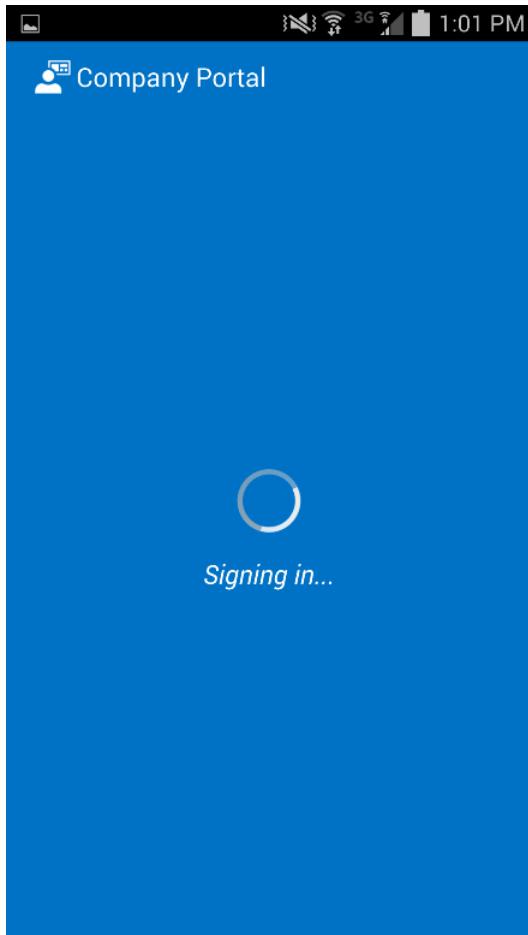
Sign in



51

52
53

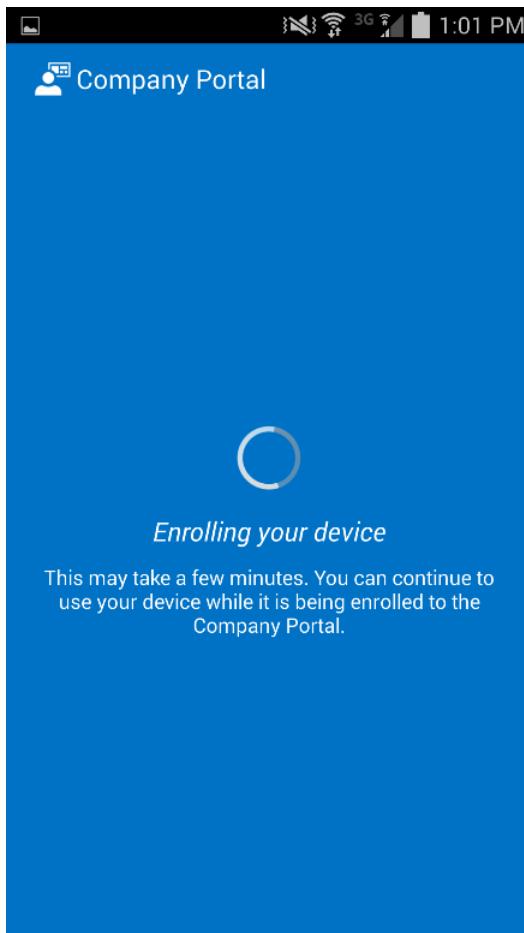
3. If implementing a hybrid architecture, you will be redirected to your enterprise login site to enter your password. Click **Sign In**.



54

55

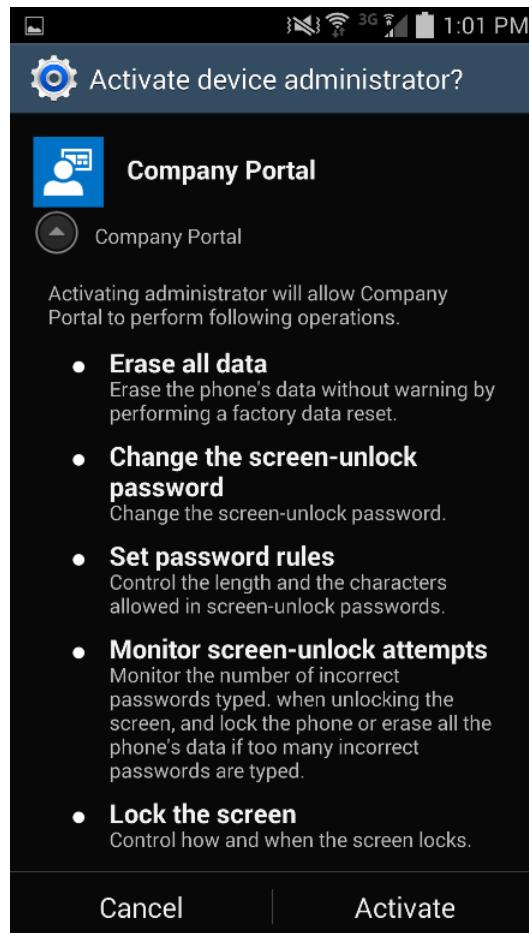
4. No action required.



56

57

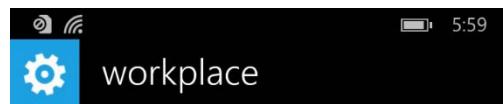
5. No action required.



58

- 59 6. Click **Activate** to allow remote management of the device.

60 4.1.3 Windows Phone 8.1



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

62

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

63

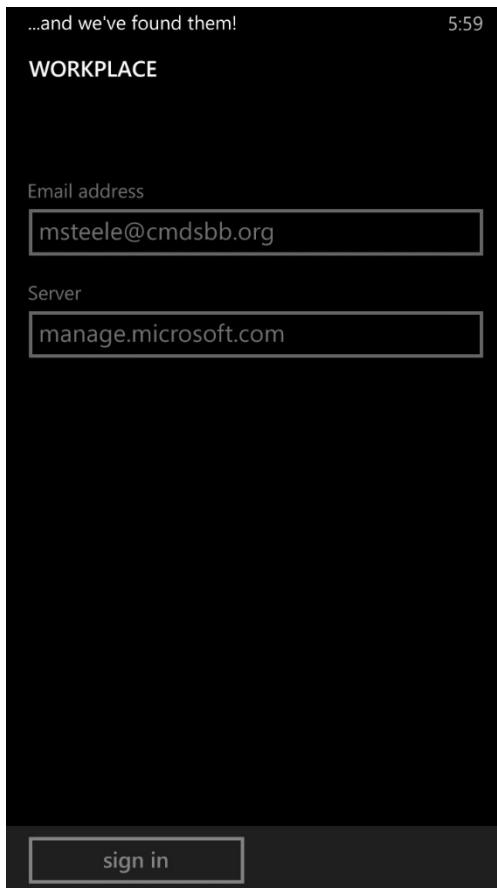
64



65

66
67
68

2. 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.



69

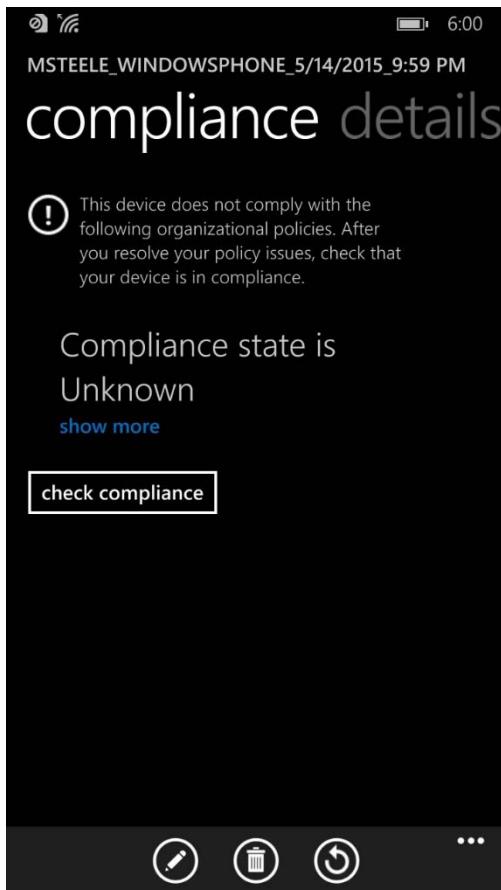
70
71
72

3. 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.



73

- 74 4. Upon logging in to company portal for the first time, the user will be notified that their
- 75 device hasn't met compliance and that some resources will be restricted.



76

77
78

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



79

80

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

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.

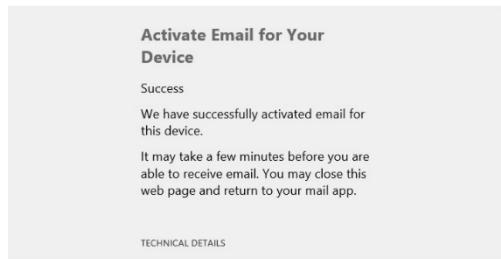
Please contact your IT department with any questions or problems.



81

82
83

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



84

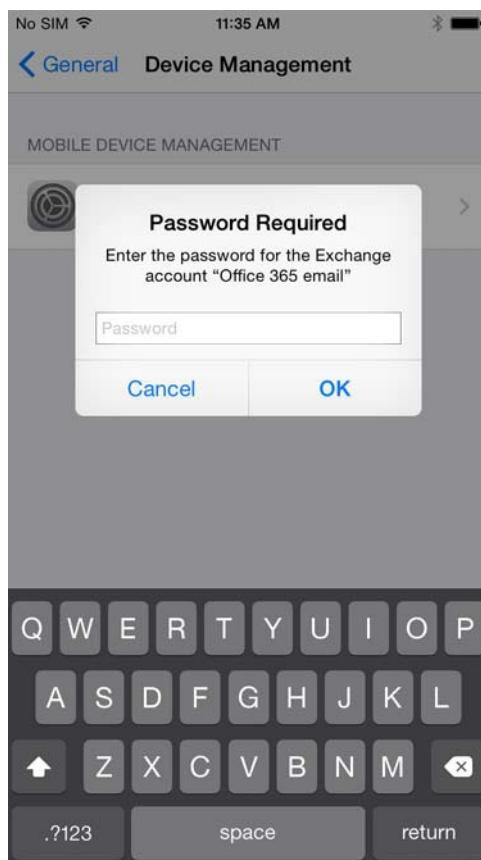
- 85 8. The activation link will open a browser, and upon successful activation the user should be
86 directed to this page. At this point the user should have full access to exchange
87 email/contacts/calendar.

88 4.2 Email Setup

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

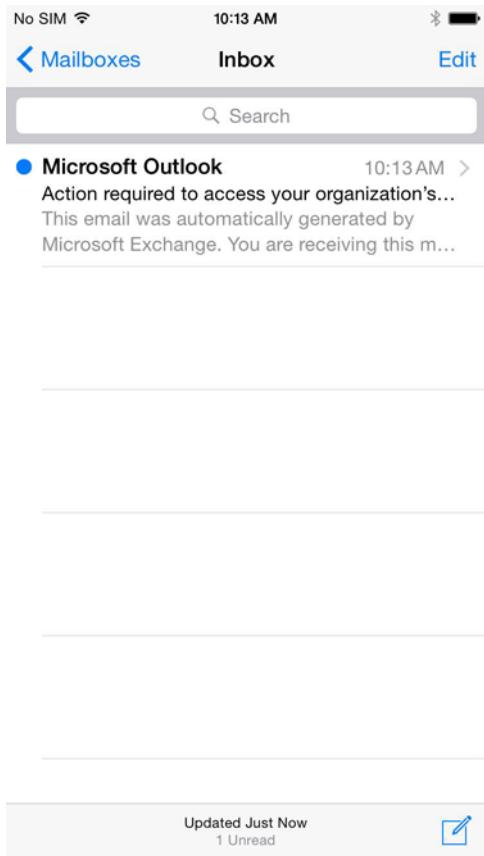
93 Implementers may choose to have users configure an email client on their devices manually or
94 create a SCCM profile, which automatically configures enrolled devices. At the time of writing
95 of this practice guide, only iOS and Microsoft mobile devices were supported. Consult SCCM
96 documentation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

97 4.2.1 iOS



98

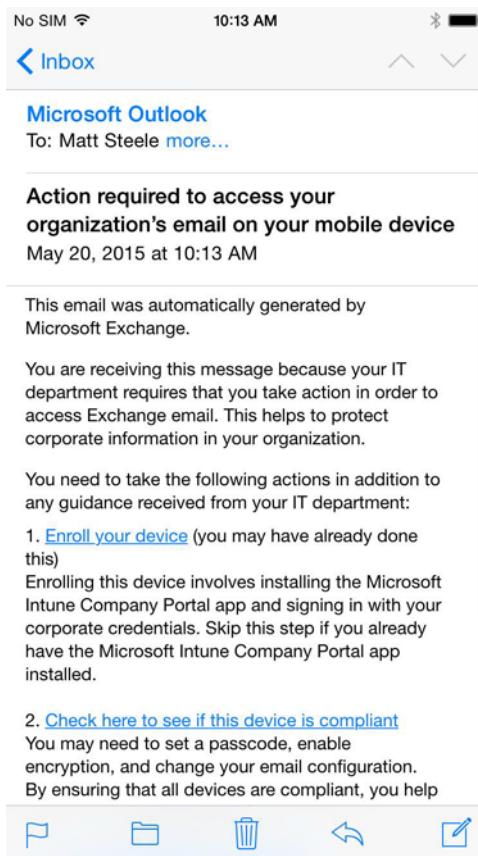
- 99
- 100
- 101
1. When the user first opens the settings application either before/during/after the compliance check, they are prompted for their Office365 password for the exchange profile that is provisioned during the on-boarding process. This is a one-time occurrence.



102

103

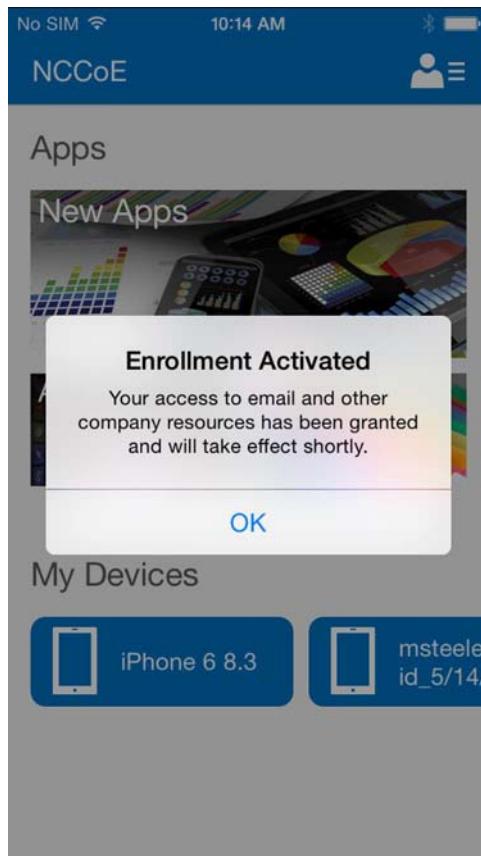
2. The user will receive this email the first time they open their email client.



104

105
106

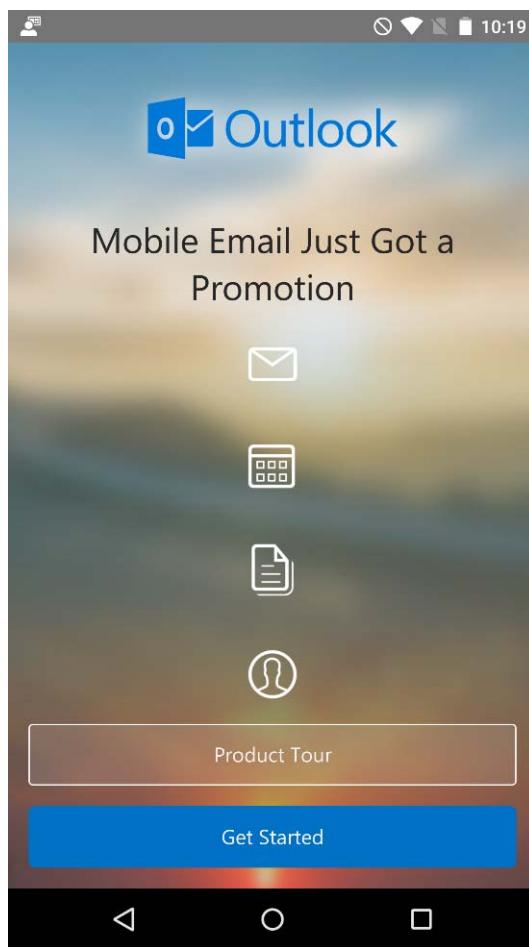
3. To activate their email access, the user will have to tap the link to activate the email and check for compliance.



107

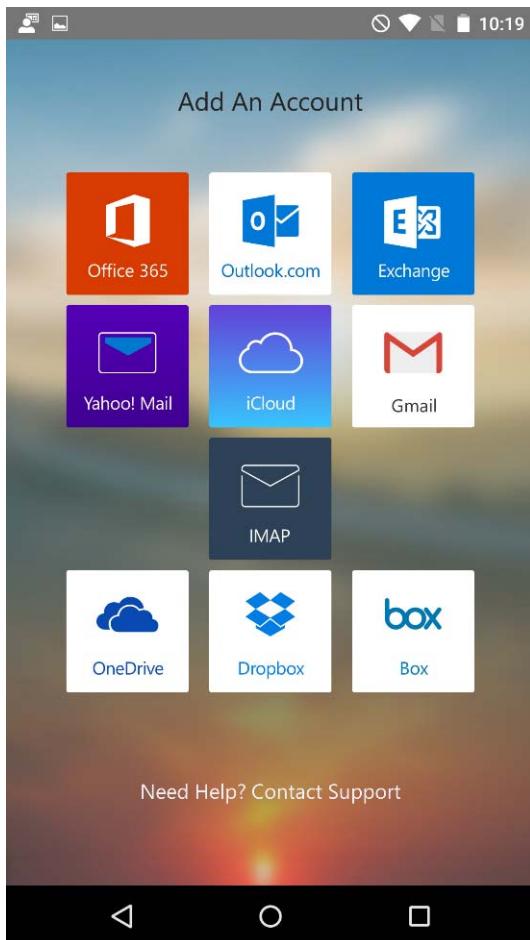
108

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

¹⁰⁹ 4.2.2 Android

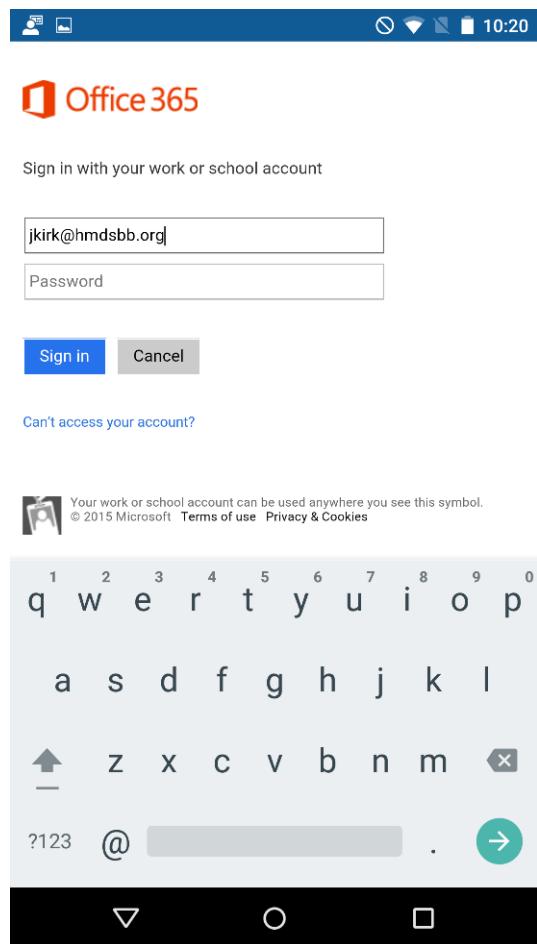
110

- 111 1. Open the Outlook application on your device.



112

2. Choose **Office 365**.



114

115

3. Log in with your enterprise credentials.

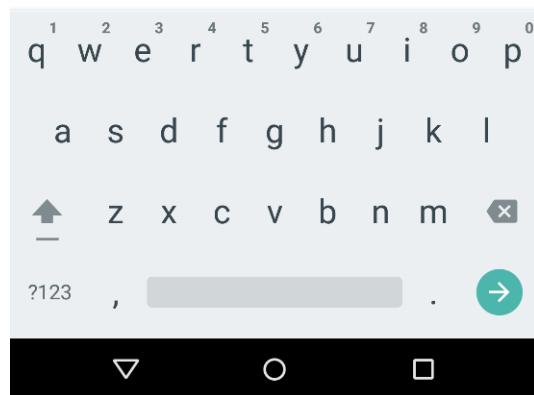


HMDSBB

Sign in with your organizational account

Sign in

© 2013 Microsoft



116

117
118

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.



Tell us about your device

You need to enroll this new device so that we can recognize it before you can access your organization's resources.

Enroll

Cancel



119

120

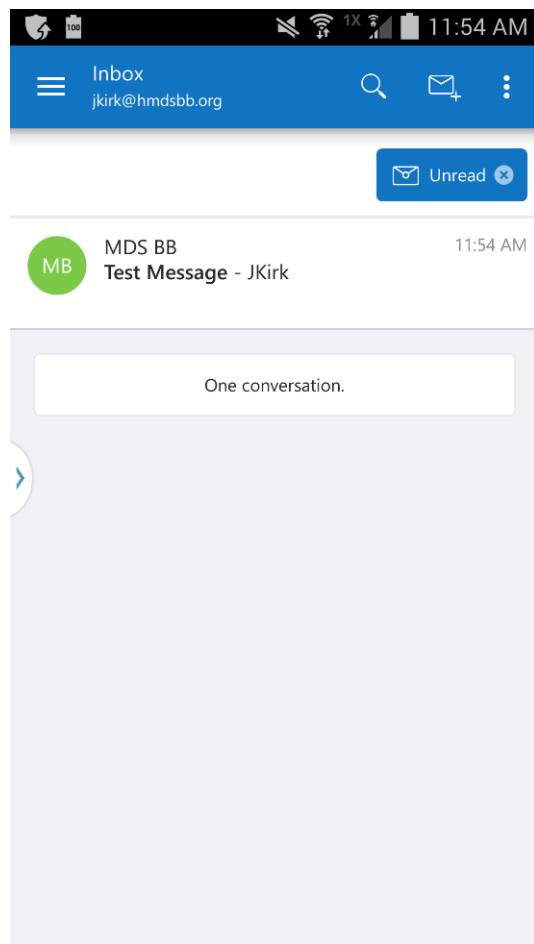
5. If your device has not been enrolled with the MDM, you will be prompted to do so.



121

122
123

6. 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.

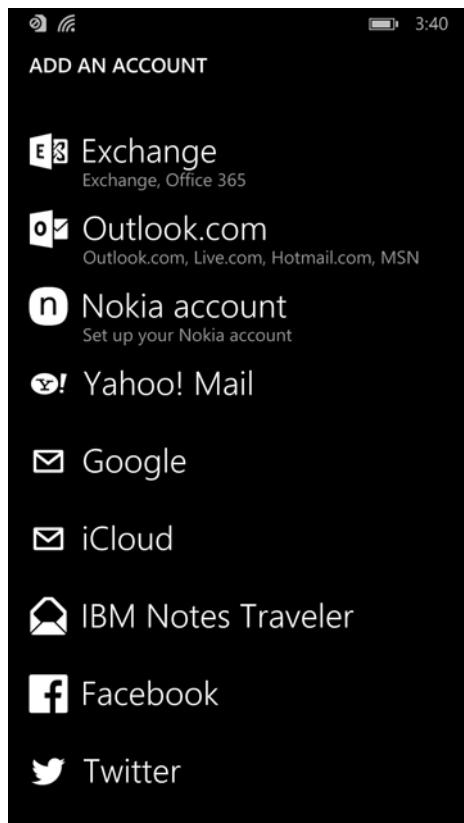


124

125

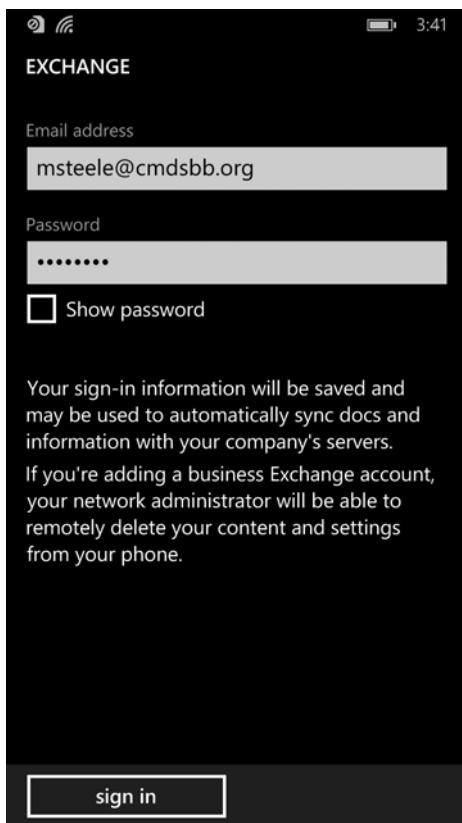
7. The device owner will be granted access to Office 365 after the device complies with policy.

126 **4.2.3 Windows Phone 8.1**



127

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



132

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



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



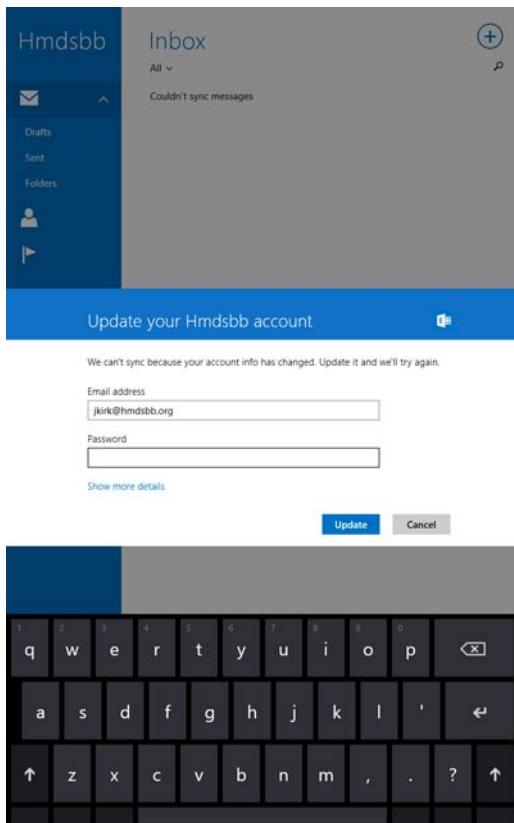
...

134

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

138 4.2.4 Windows 8.1

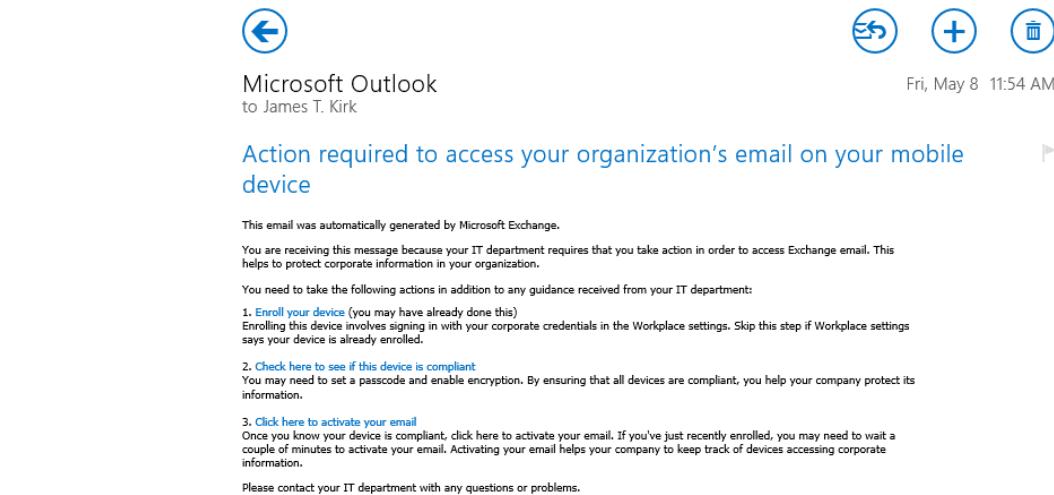
139 Intune with SCCM integration does not support email profiles for Windows 8.1, so email must
140 be configured using another method.



141

142

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.



145

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

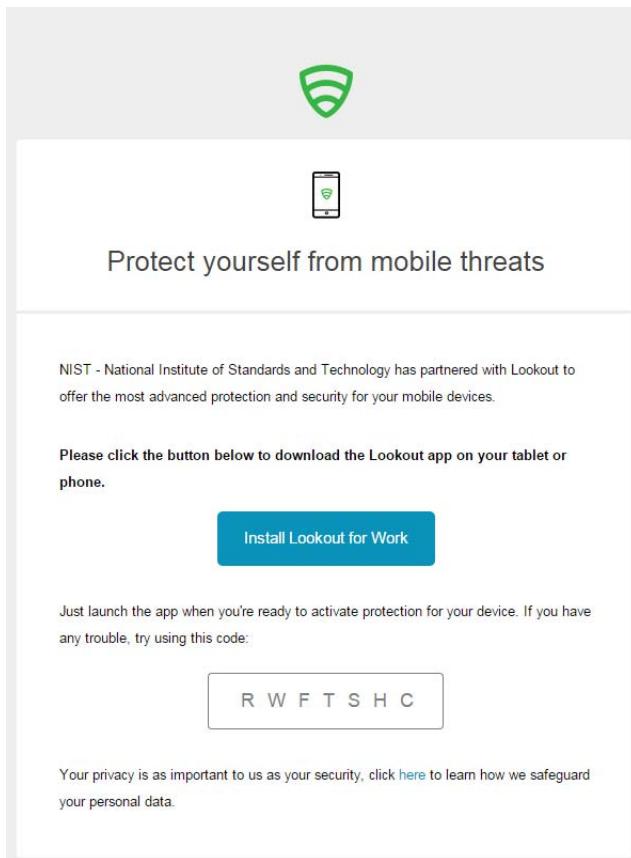
148

4.3 Lookout MTP Enrollment

The screenshot shows the Lookout MTP administrative console interface. The left sidebar has a dark theme with icons for Dashboard, Threats, and Devices. The main header bar shows the URL https://mtp.lookout.com/les/devices/enroll. Below the header, there are three tabs: Devices, Enroll (which is selected), and Invites. The main content area is titled "Enroll Devices" and contains instructions: "To invite employees to activate Lookout for Work on their mobile devices, either import a .csv consisting of just or by commas or semicolons." It provides two methods for adding email addresses: "IMPORT EMAILS FROM A .CSV" (highlighted in green) and "Enter emails separated by comma." There is also a "ADD ADDRESSES" button.

149

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

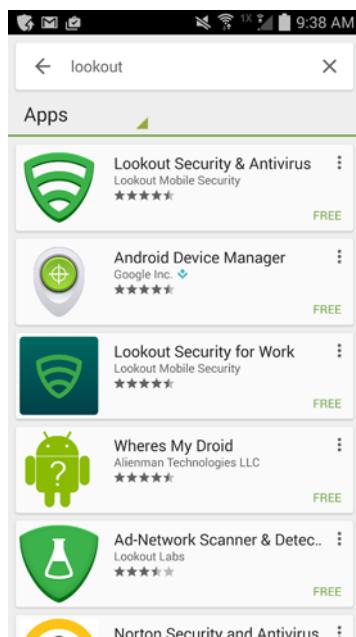


153

154
155

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**



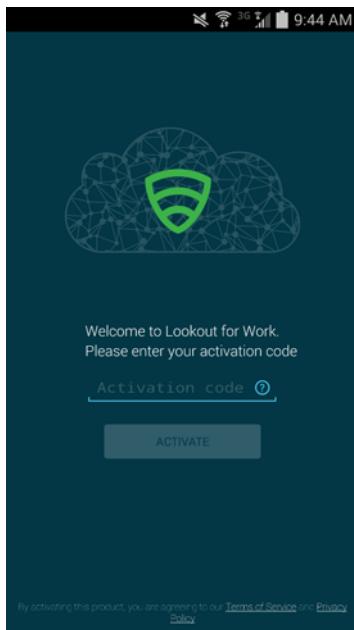
157

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



159

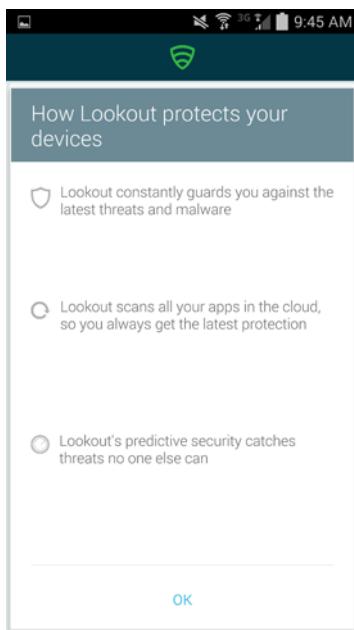
2. Select the **Lookout Security for Work** application and tap **Install**.



161

162

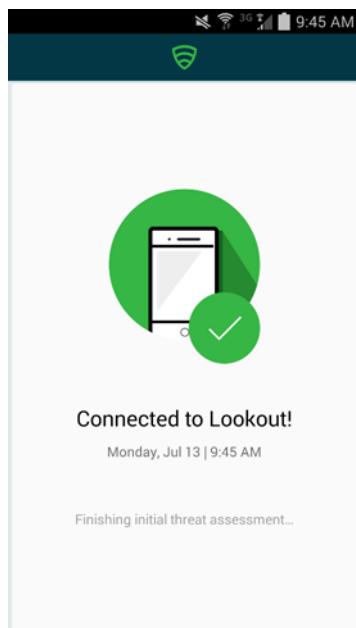
3. Enter the activation code retrieved from the enrollment email.



163

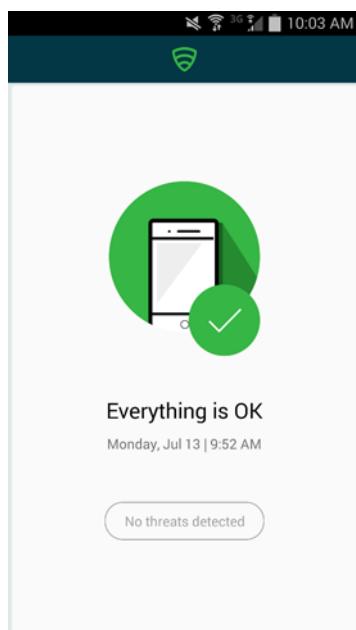
164

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



165

- 166 5. The application will proceed to scan the user's device.



167

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

169

¹ Appendix A Acronyms

2	2FA	Two-Factor Authentication
3	AD	Active Directory
4	AD DS	Active Directory Domain Services
5	AD FS	Active Directory Federation Services
6	ADAL	Active Directory Authentication Library
7	BYOD	Bring Your Own Device
8	CAG	Consensus Audit Guidelines
9	CBC	Cipher Block Chaining
10	CIO	Chief Information Officer
11	COPE	Corporately Owned and Personally Enabled
12	COTS	Commercial Off-The-Shelf
13	CSD	Computer Security Division
14	CSF	Cybersecurity Framework
15	DISA	Defense Information Systems Agency
16	DMZ	Demilitarized Zone
17	DNS	Domain Name System
18	DoD	Department of Defense
19	EMM	Enterprise Mobility Management
20	FIPS	Federal Information Processing Standard
21	GPS	Global Positioning System
22	GSA	General Services Administration
23	HTTP	Hypertext Transfer Protocol
24	IAD	Information Access Division
25	IEC	International Electrotechnical Commission
26	IDMS	Identity Management System
27	IMEI	International Mobile Station Equipment Identity
28	IPC	Inter-process Communication
29	ISO	International Organization for Standardization
30	ISP	Internet Service Provider
31	IT	Information Technology
32	LAN	Local Area Network
33	MAM	Mobile Application Management

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/getdoc.jsp?containerId=prUS25450615> [accessed 6/19/2015].
3
- 4 [2] Microsoft, Plan for third-party SSL certificates for Office 365, <https://support.office.com/en-sg/article/Plan-for-third-party-SSL-certificates-for-Office-365-b48cdf63-07e0-4cda-8c12-4871590f59ce?ui=en-US&rs=en-SG&ad=SG> [accessed October 14, 2015].
5
6
- 7 [3] Microsoft, Understanding Certificate Requirements, November 08, 2011. <https://technet.microsoft.com/library/gg476123.aspx> [accessed October 14, 2015].
8
- 9 [4] Microsoft, Install Active Directory Domain Services (Level 100), April 14, 2014. <https://technet.microsoft.com/en-us/library/hh472162.aspx> [accessed October 14, 2015].
10
- 11 [5] Microsoft, Mobile device security policy settings in Microsoft Intune, October 8, 2015. <https://technet.microsoft.com/en-us/library/dn913730.aspx> [accessed October 14, 2015]
12
- 13 [6] Microsoft, How To Install ADFS 2012 R2 For Office 365, April 28, 2014. <http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365.aspx> [accessed October 14, 2015]
14
15
- 16 [7] Microsoft, Office 365 and ADFS...Active 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].
17
18
- 19 [8] 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].
20
- 21 [9] Microsoft, Azure Active Directory Sync, July 22, 2015. <https://msdn.microsoft.com/en-us/library/azure/dn790204.aspx> [accessed October 14, 2015].
22
- 23 [10] 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].
24
25