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

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-4c

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

DRAFT

Joshua Franklin
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

November 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

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

DISCLAIMER

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

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Contents

52

53

54 List of Figures

65

66

67 List of Tables

72

1 Introduction

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

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

1.1 Practice Guide Structure

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

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

This guide contains three volumes:

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

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

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

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

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

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

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

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

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

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

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

1.2 Build Overview

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

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

1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

Table 1.1 Typographical Conventions

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

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

2.1 Cloud Build Setup and Configuration

The following How-To will guide an implementer through the process of creating and configuring the cloud architecture depicted below. No software resources are necessary for this build because it is completely cloud based. The only hardware requirement is that the organization that implements this build uses mobile devices that are compatible with the cloud MDM. This building block chose to use mobile devices running iOS, Android, and Windows Phone - the top three operating systems in terms of market share [1].

This How-To details the creation, configuration, and enrollment aspects of each cloud service. Keep in mind, a prerequisite to the cloud is an Internet domain name. If the implementer does not already have a domain name, one can be obtained from an accredited registrar[1]. You will need to be able to edit the resource records to prove ownership of the domain.

The implementer will also need access to an Apple developer account to generate a push notification certificate for iOS devices. A push certificate allows the Office365 instance to send push notifications to enrolled devices. Refer to the Apple website for pricing information and more details regarding certificates[2].

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

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

2.1.1 Cloud Build Components

Table 2.1 lists the components used for this building block:

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

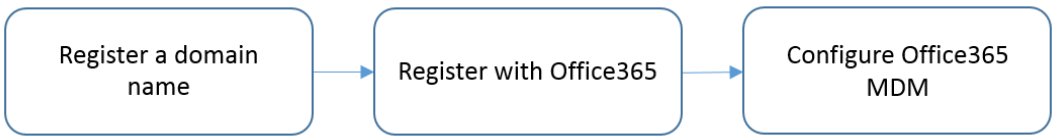
1.https://www.icann.org/registrar-reports/accredited-list.html
2. https://developer.apple.com/

Table 2.1 Cloud Build Components

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

The cloud building block build process can be completed with the high-level steps in figure 2.1, 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

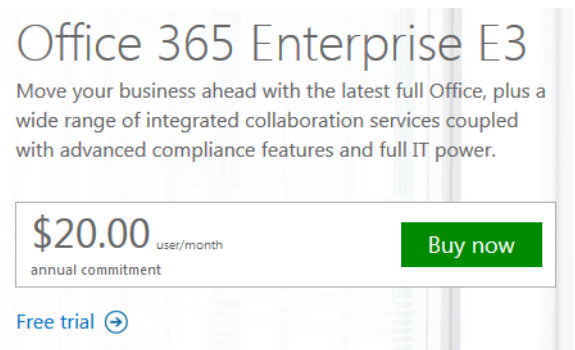


2.1.2 Office 365 Setup

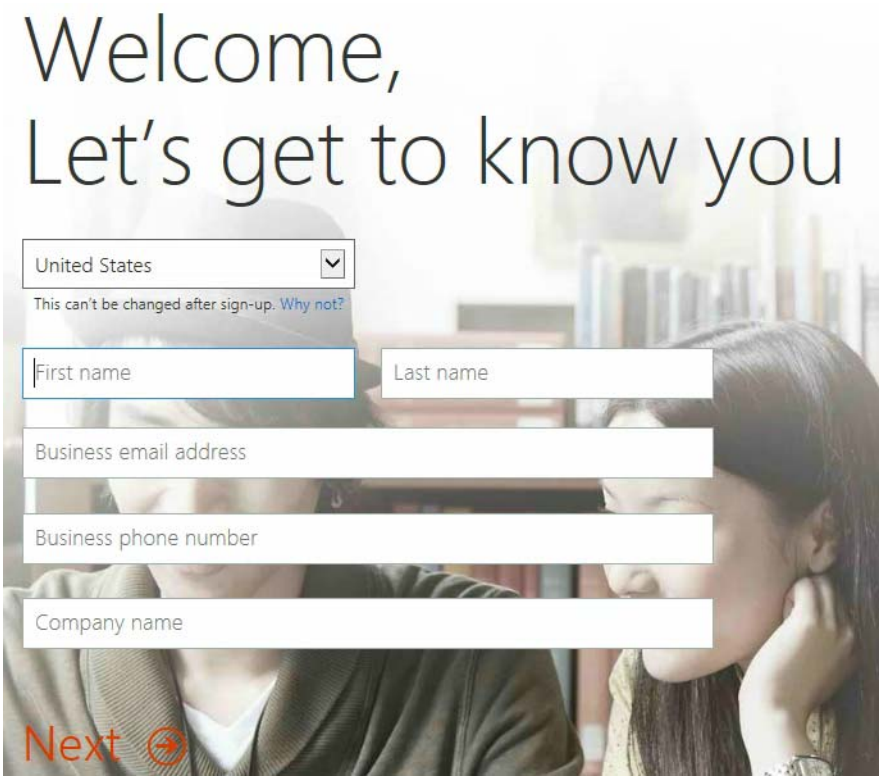
Office 365 is central to the functionality of the cloud building block. The only prerequisite to this step is a public domain name. Keep in mind these steps may change, as this is a Web based procedure.

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

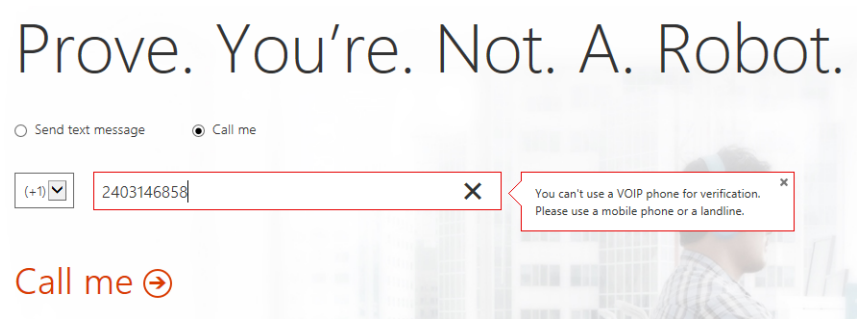
https://products.office.com/en-us/business/office-365-enterprise-e3-business-software



1. Choose a commitment level.


Welcome,
Let's get to know you
United States
This can't be changed after sign-up. Why not?
First name
Last name
Business email address
Business phone number
Company name
Next

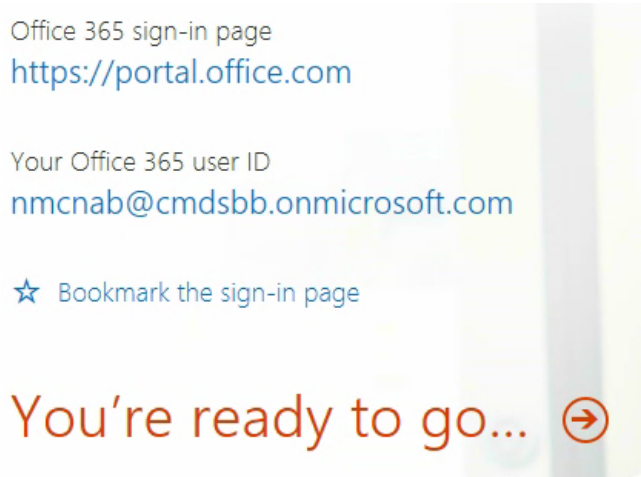
42


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

43

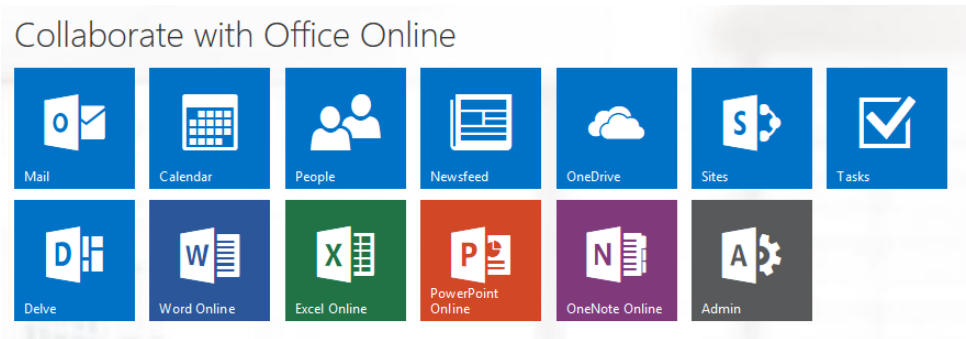

Office 365 sign-in page
https://portal.office.com
Your Office 365 user ID
nmcnab@cmdsbb.onmicrosoft.com
Creating your account...

44



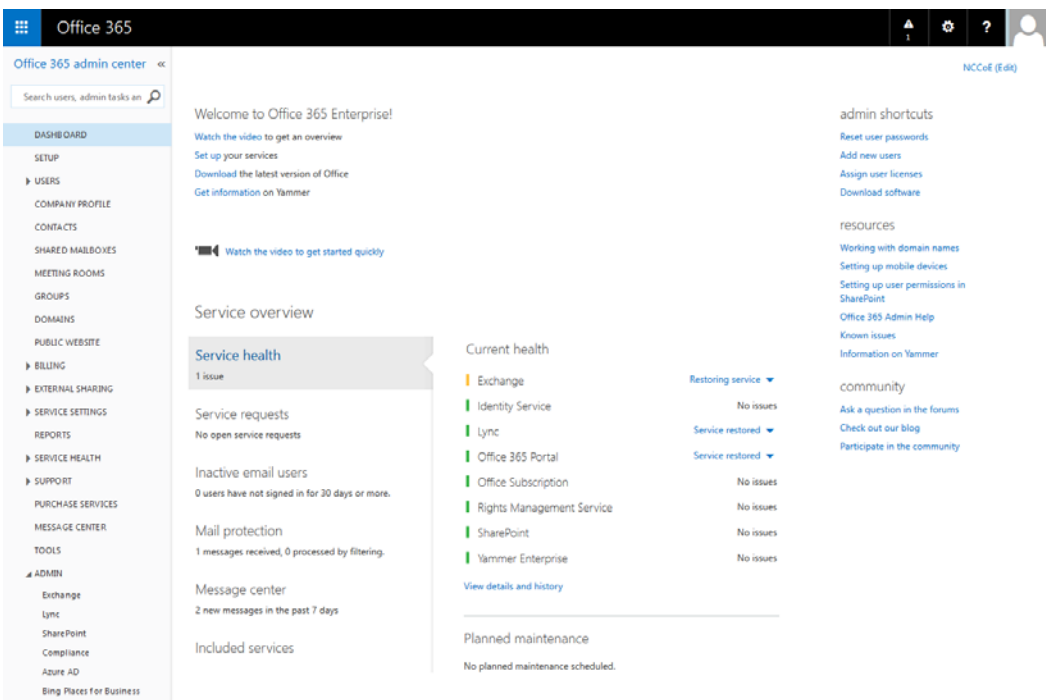
45

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



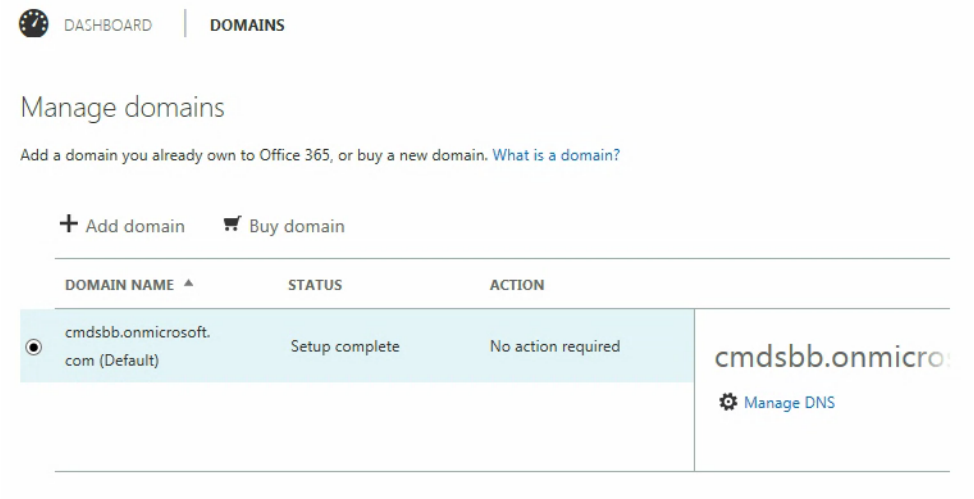
47

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

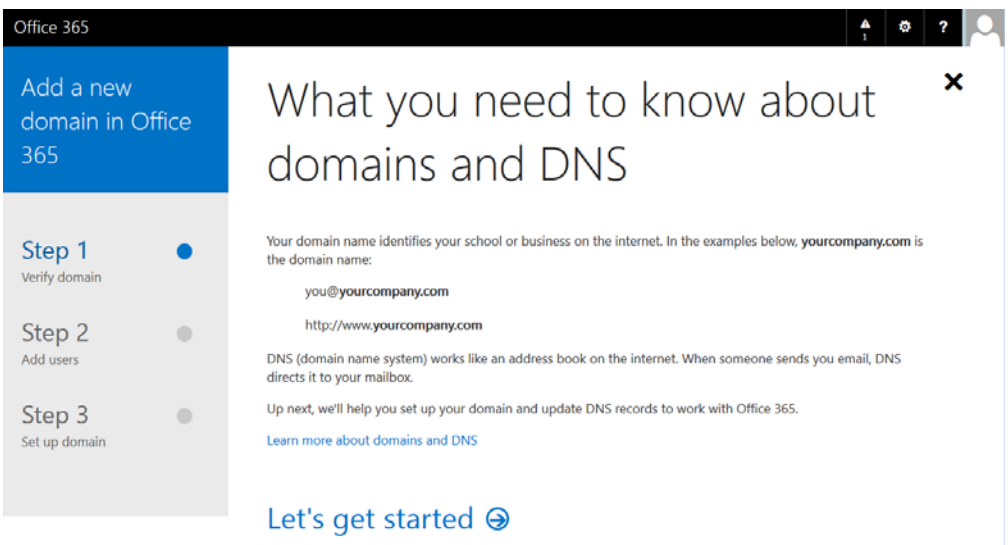


49

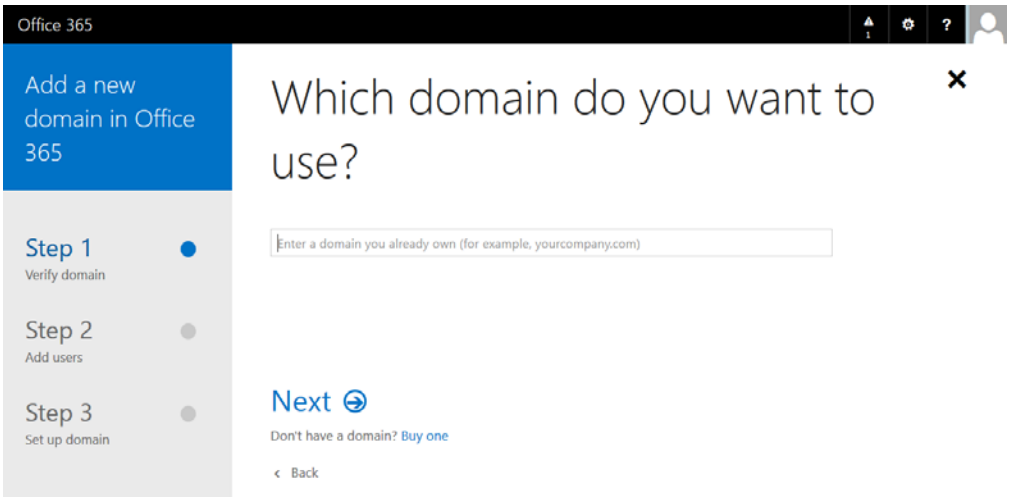
4. In the next steps we will configure the domain name with Office 365. Choose the **Domains** option.



5. Choose **Add domain**.

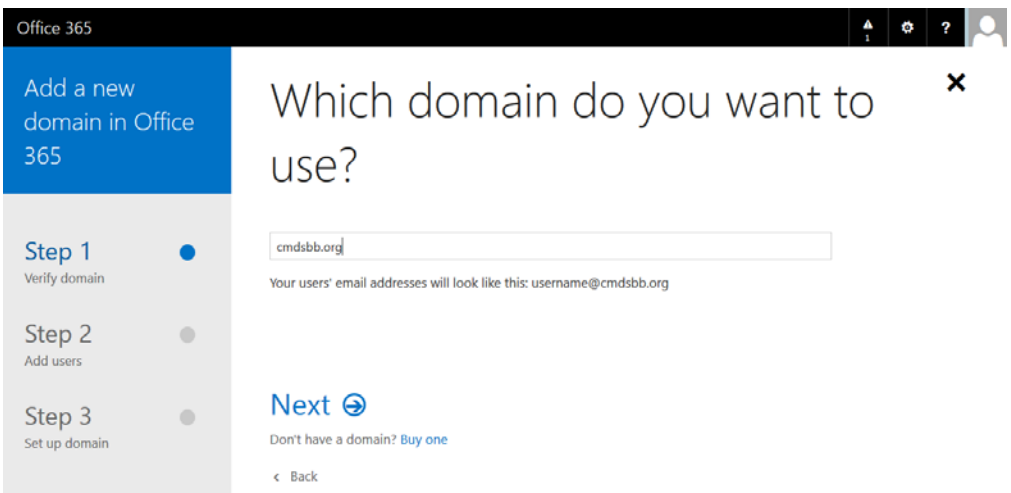


6. Choose **Let's get started**.



56

57 7. Enter your public domain name.



58

59 8. Choose **Next**.

Add this TXT record to show you own cmdsbb.org

Note: Only the domain owner can update DNS records, so we ask you to add this TXT record. Adding this TXT record won't affect your current email or other services.

To add the record:

- Go to your DNS host (Change)
- Copy the values from the following table and add them at your DNS host.

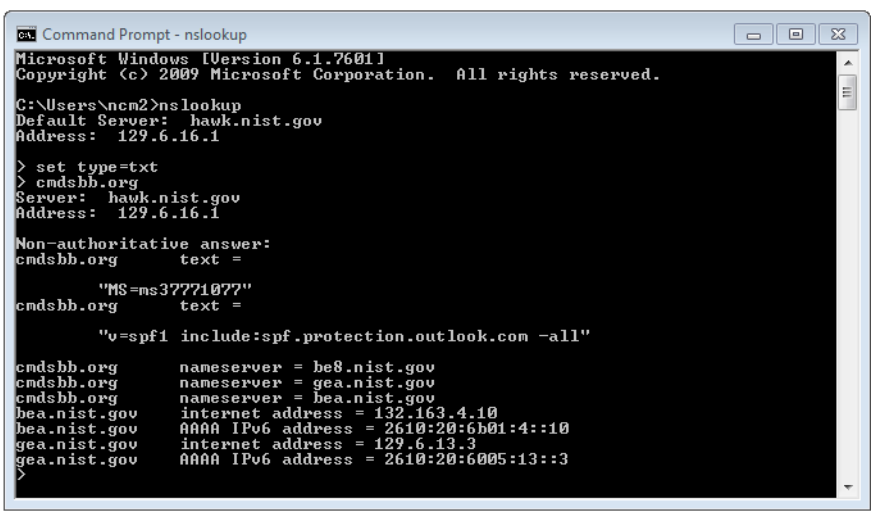
TXT records (Step-by-step instructions for adding a TXT record)

TXT name	TXT value	TTL
@	MS=ms37771077	3600

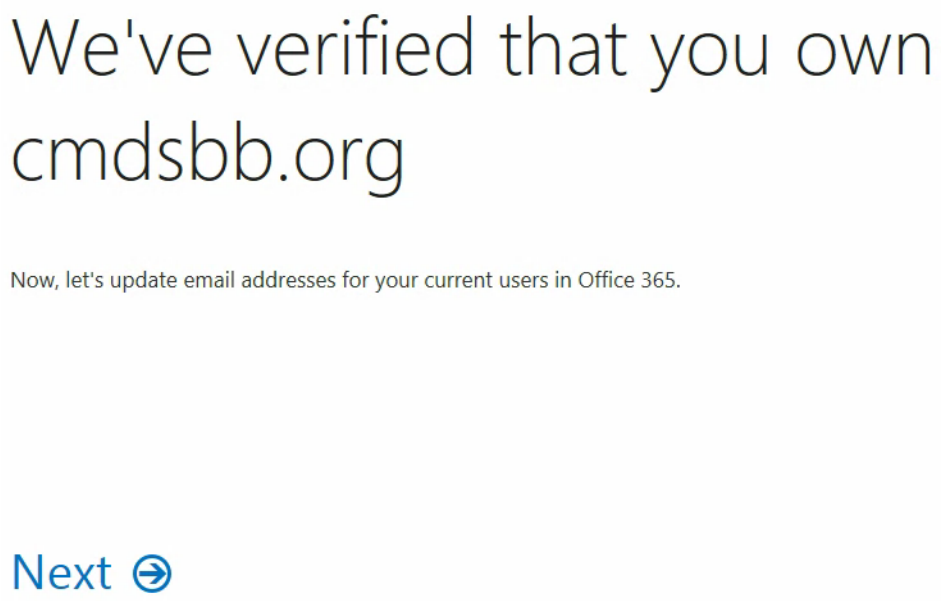
Okay, I've added the record ➔

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

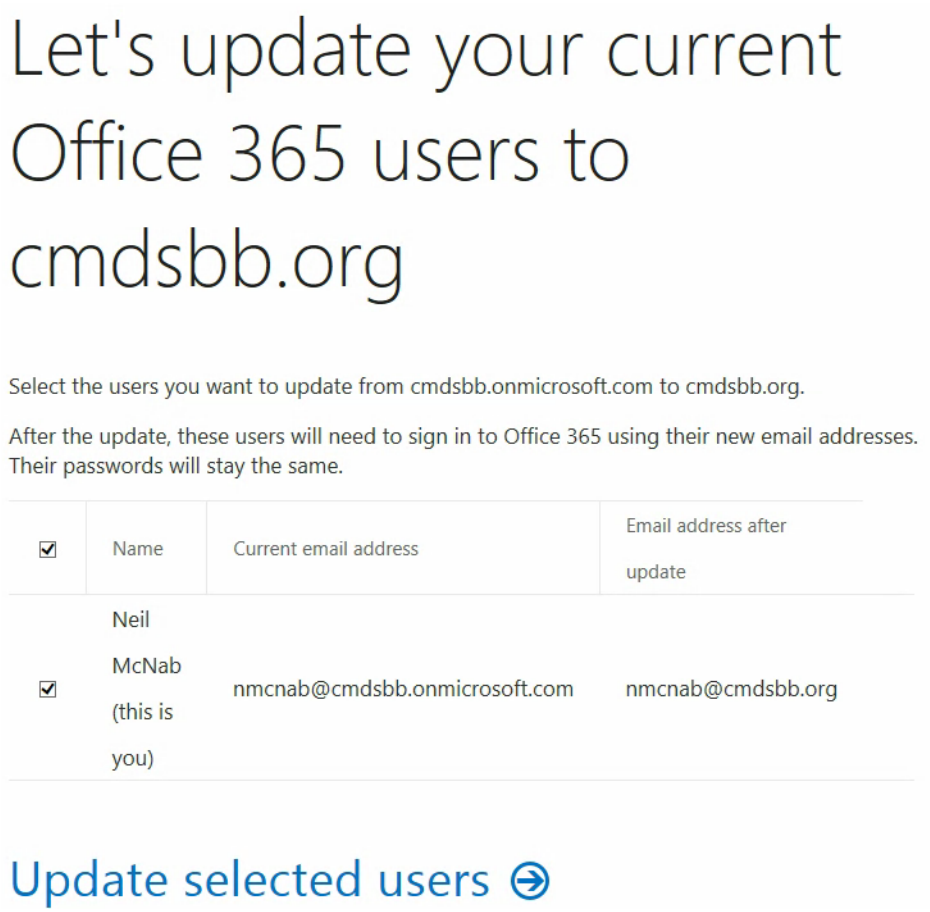
9. Add this information to the **TXT record** of your domain name. This functionality should be available from your registrar.



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

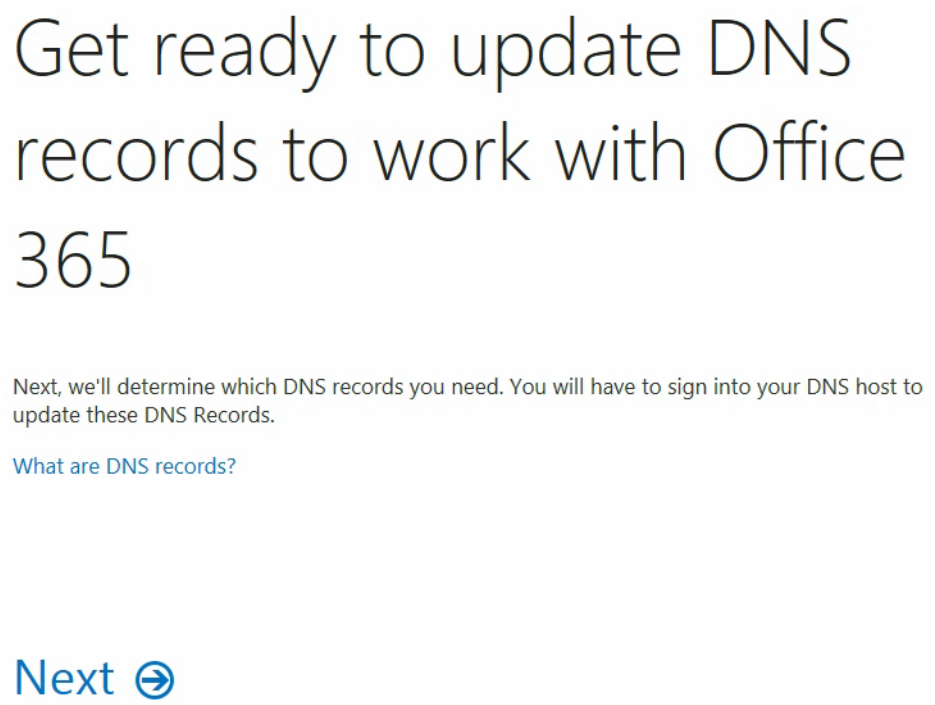


11. Choose **Next**.



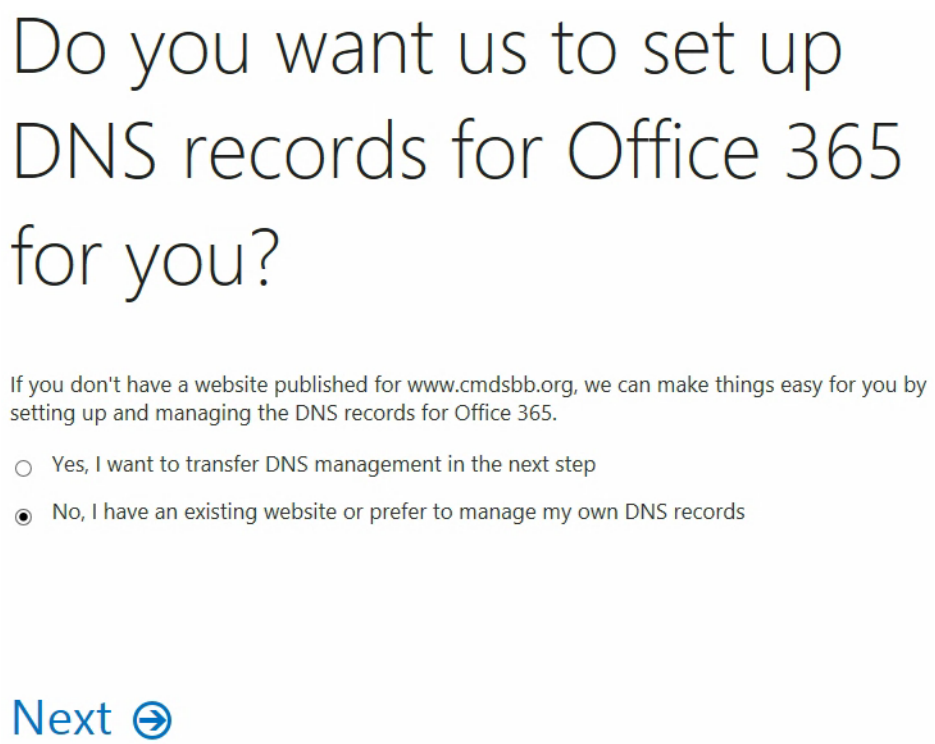
12. Choose **Update selected users**.

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



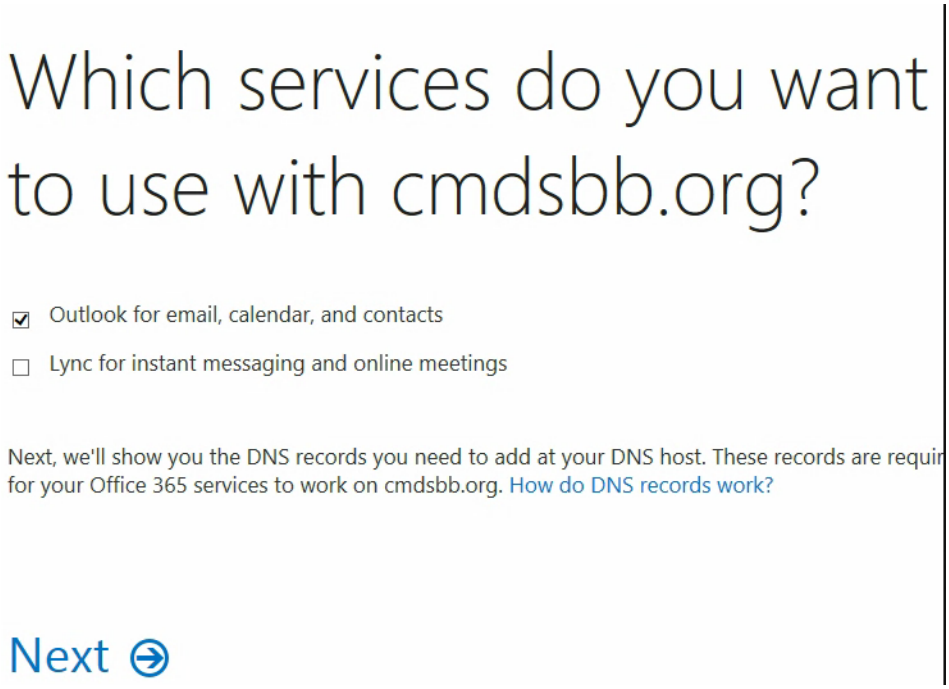
73

74 14. Choose **Next**.

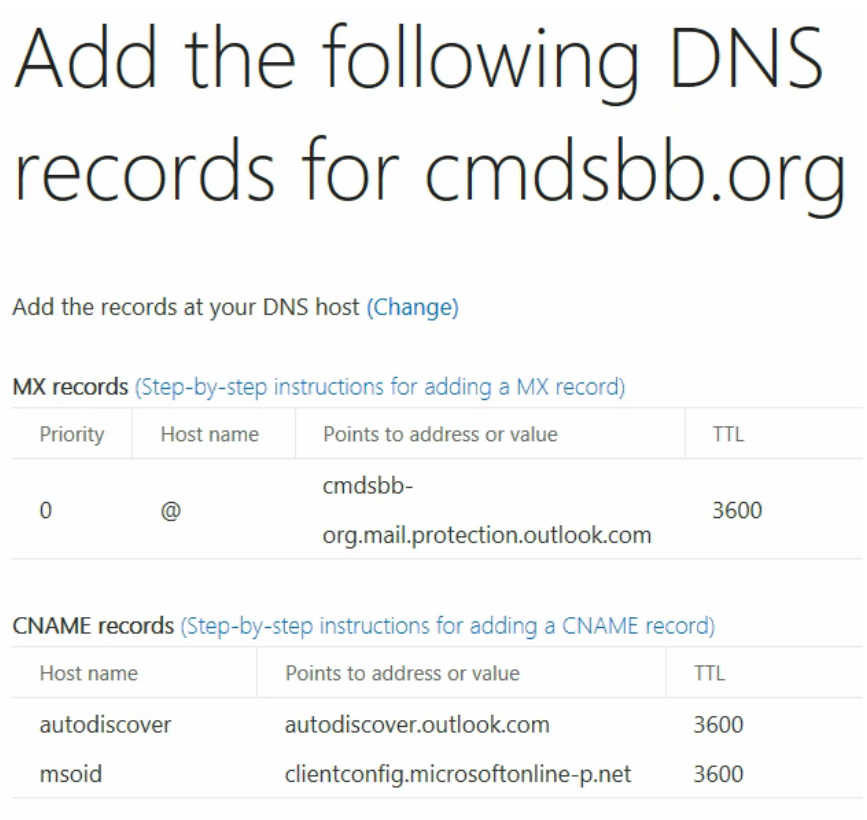


75

76 15. Choose **Next**.



16. Choose **Next**.



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

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

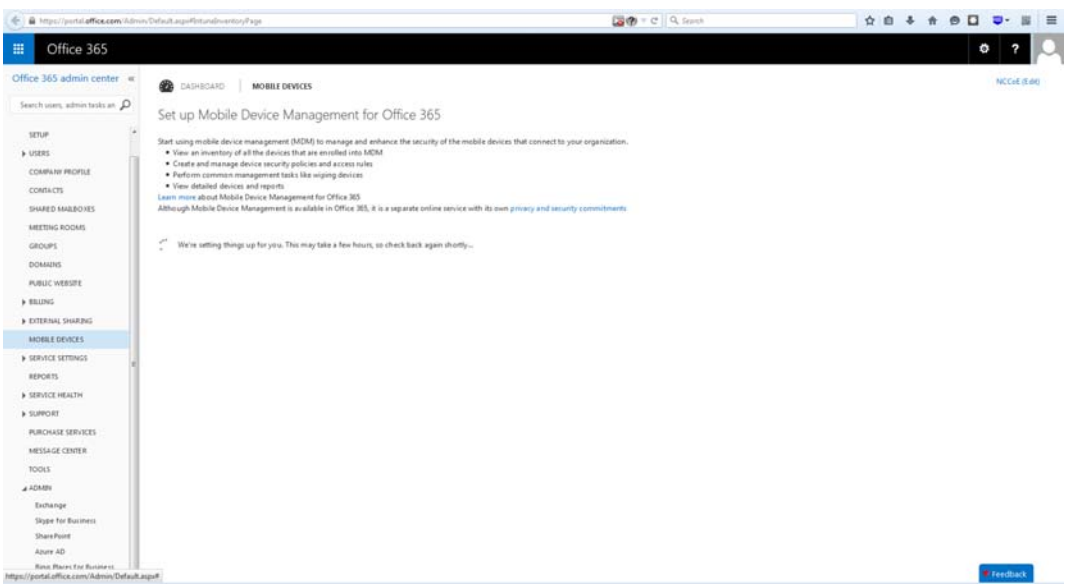
Okay, I've added the records

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

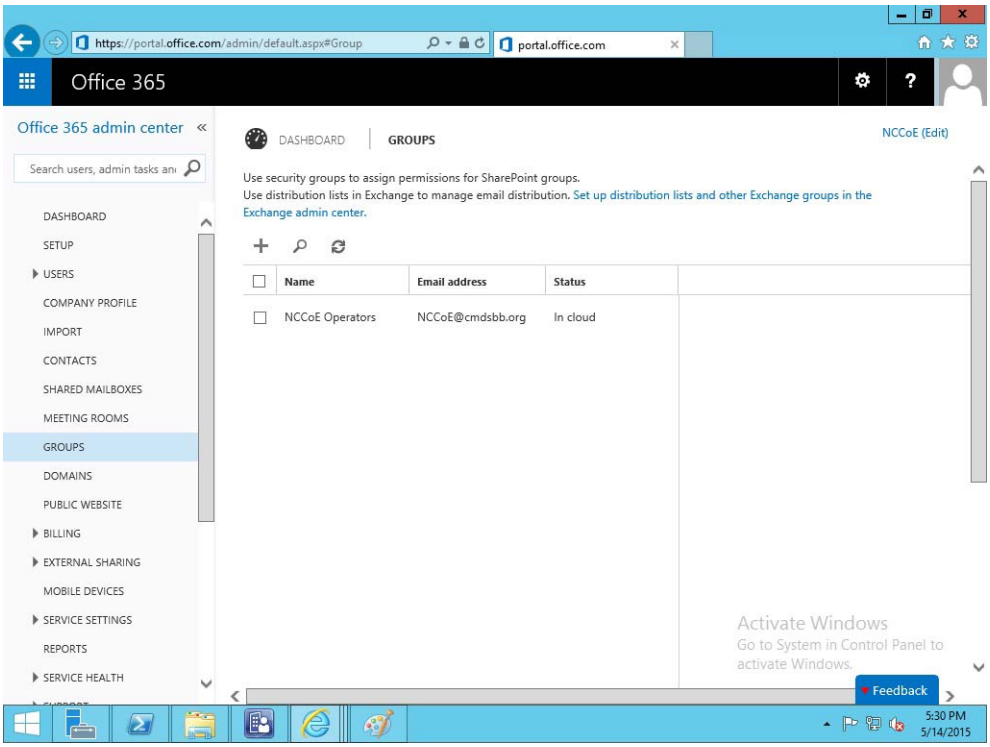
2.1.3 Office 365 MDM Setup

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

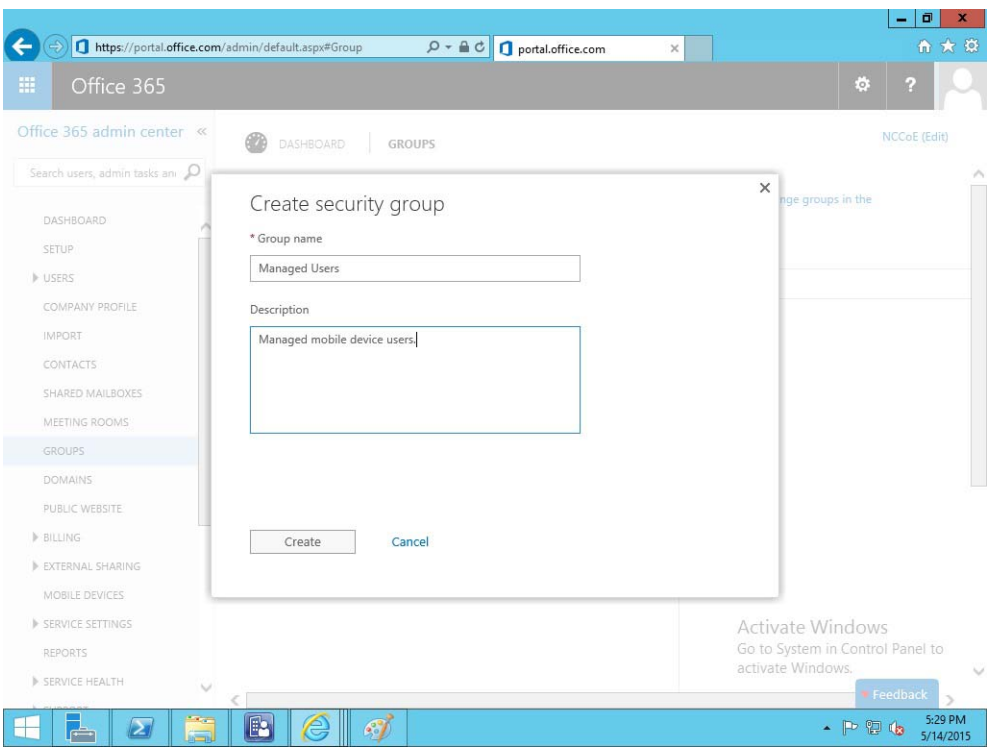
https://portal.office.com/Admin/Default.aspx#IntuneInventoryPage



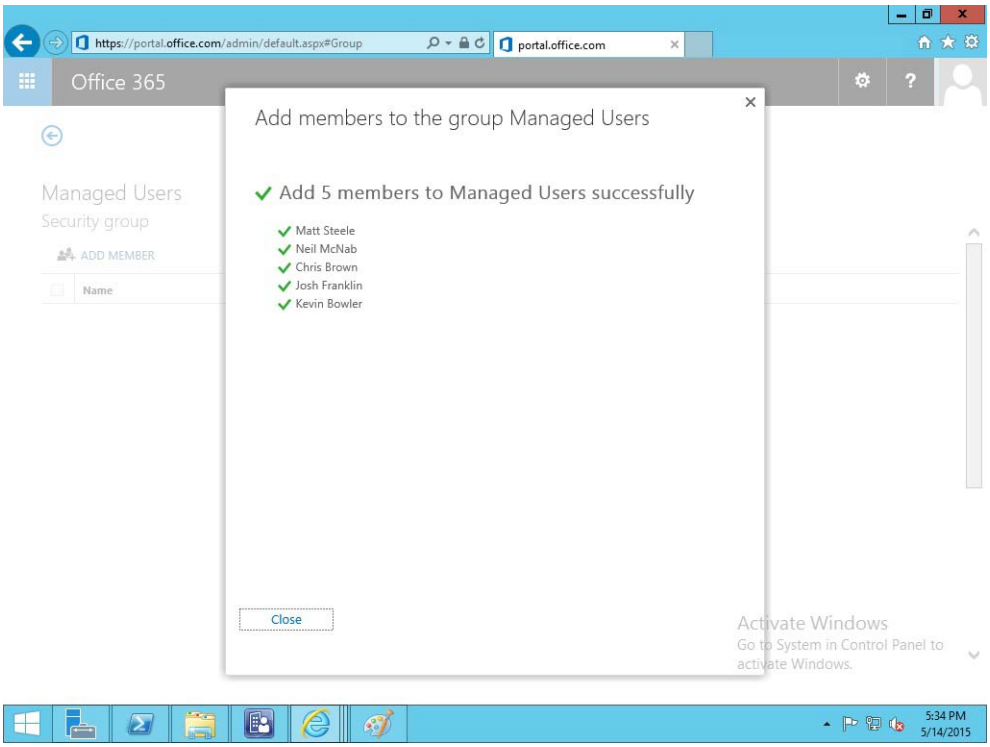
1. Choose **Get Started**.



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

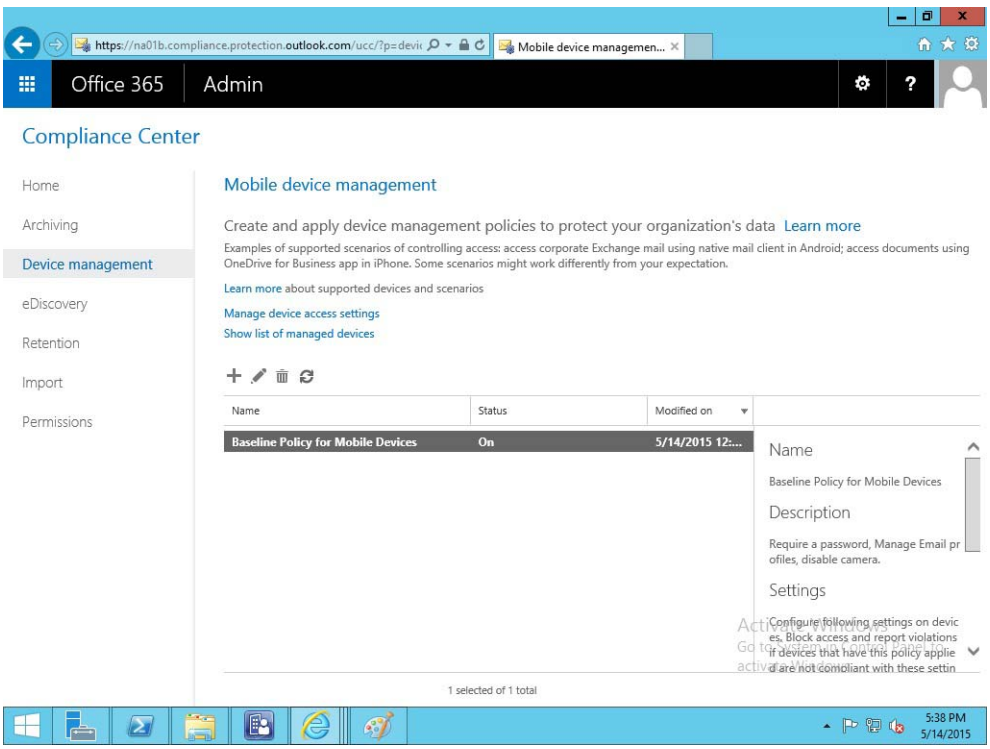


3. Add a title and description for the group.



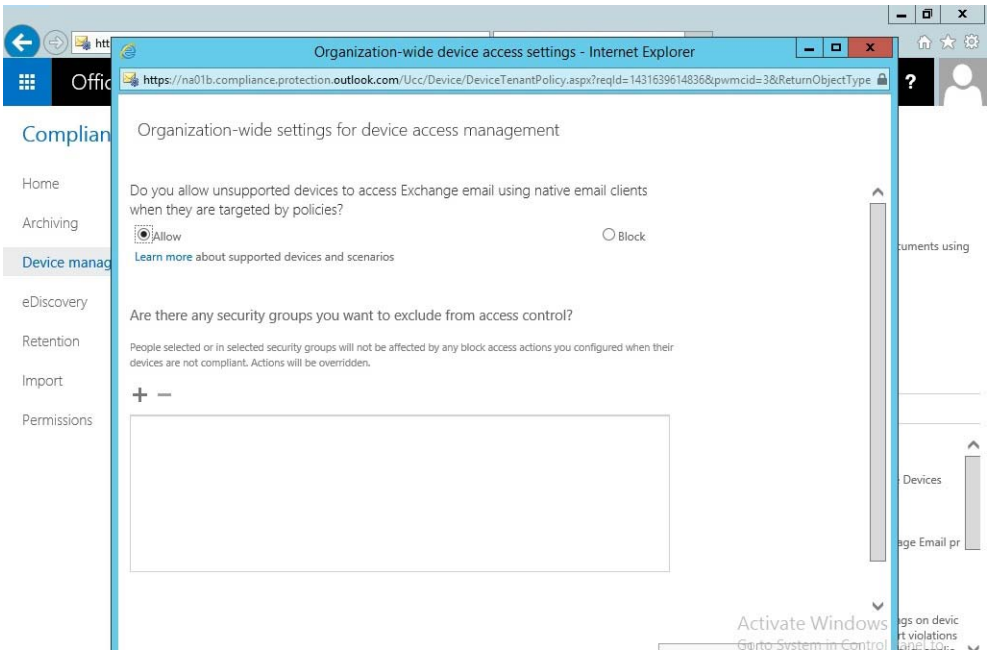
94

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



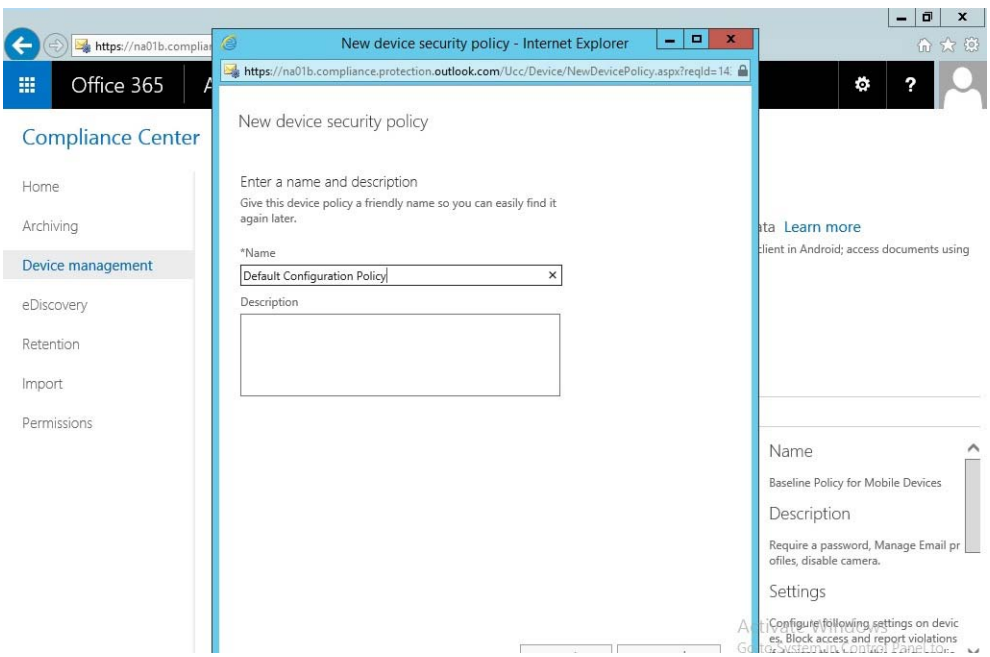
96

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



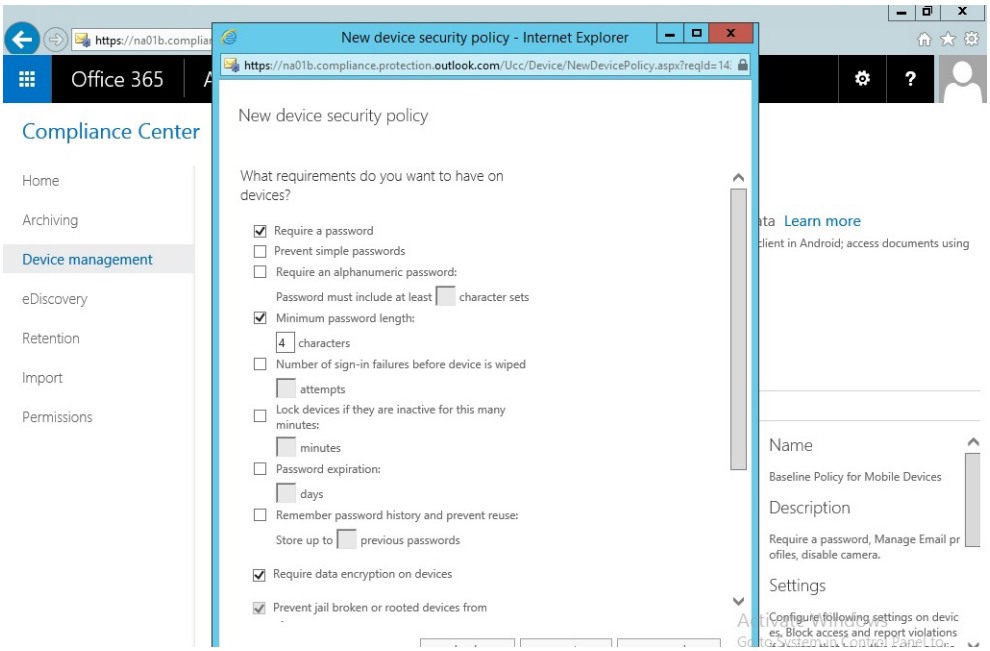
99

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



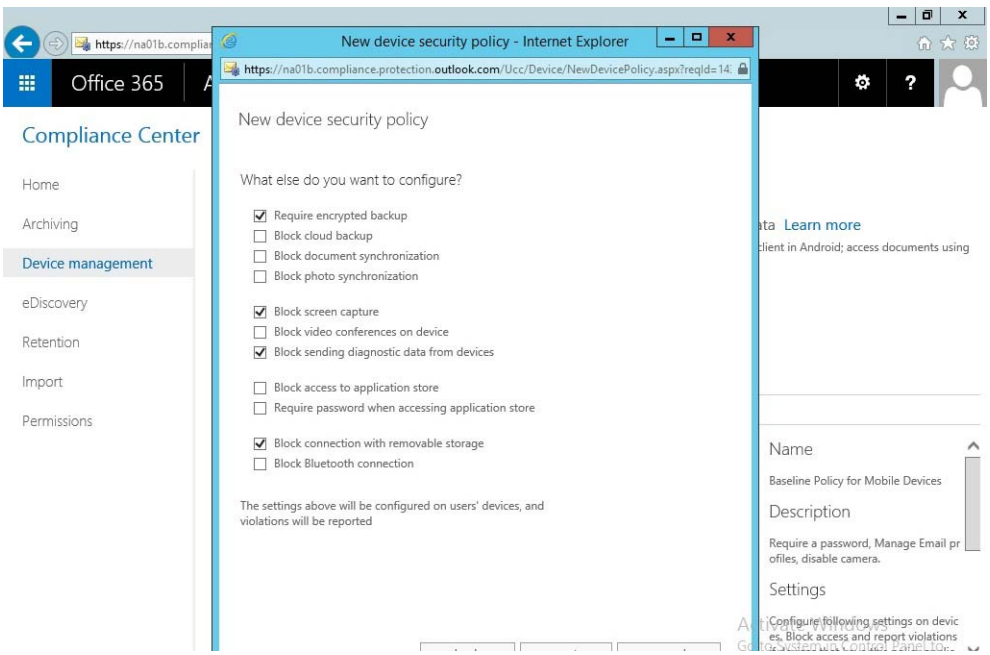
101

102 7. Set the name for the device policy.



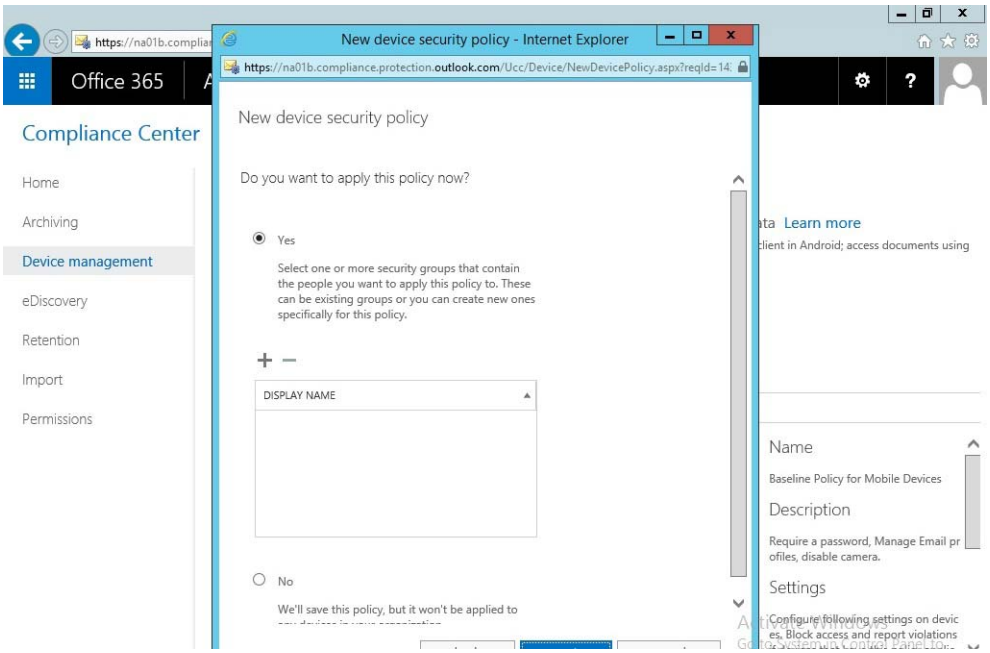
103

104 8. Set rules for the device policy.



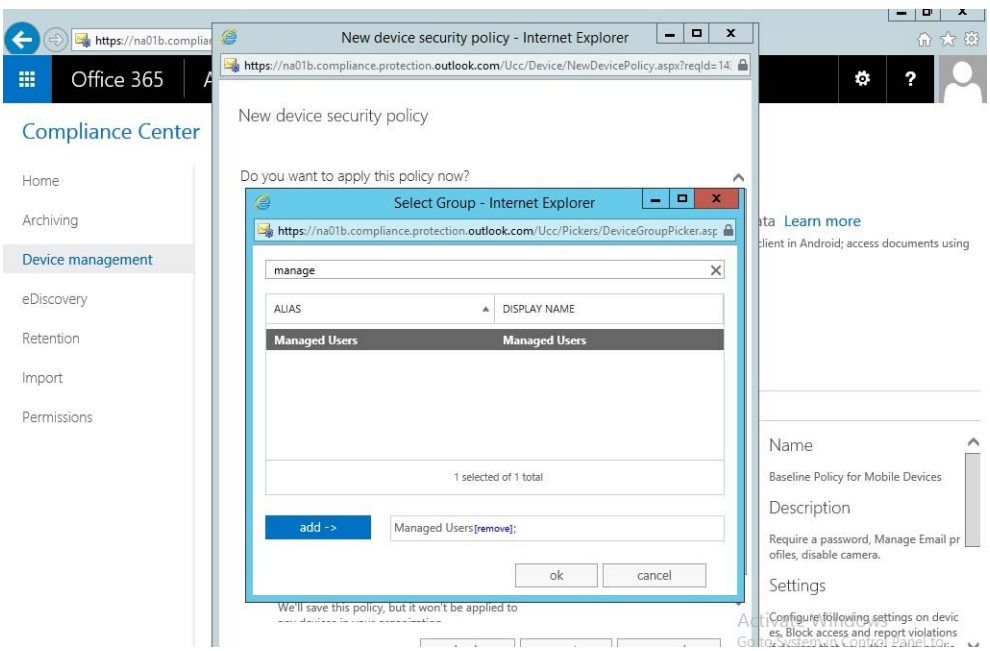
105

106 9. Set additional hardware restrictions.



107

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

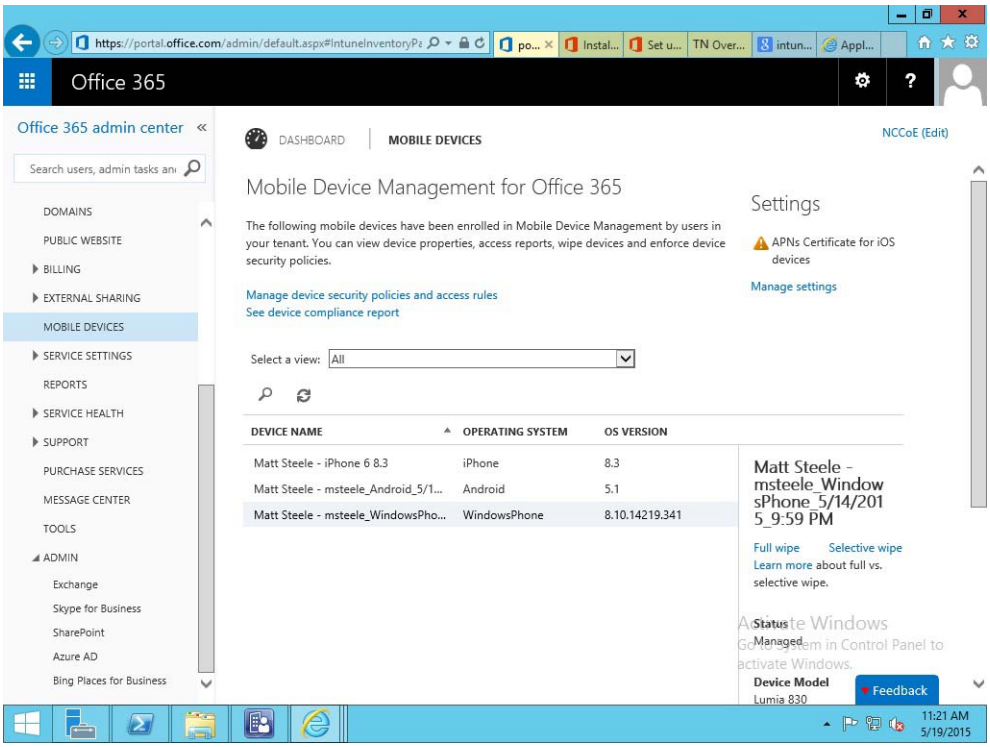


109

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

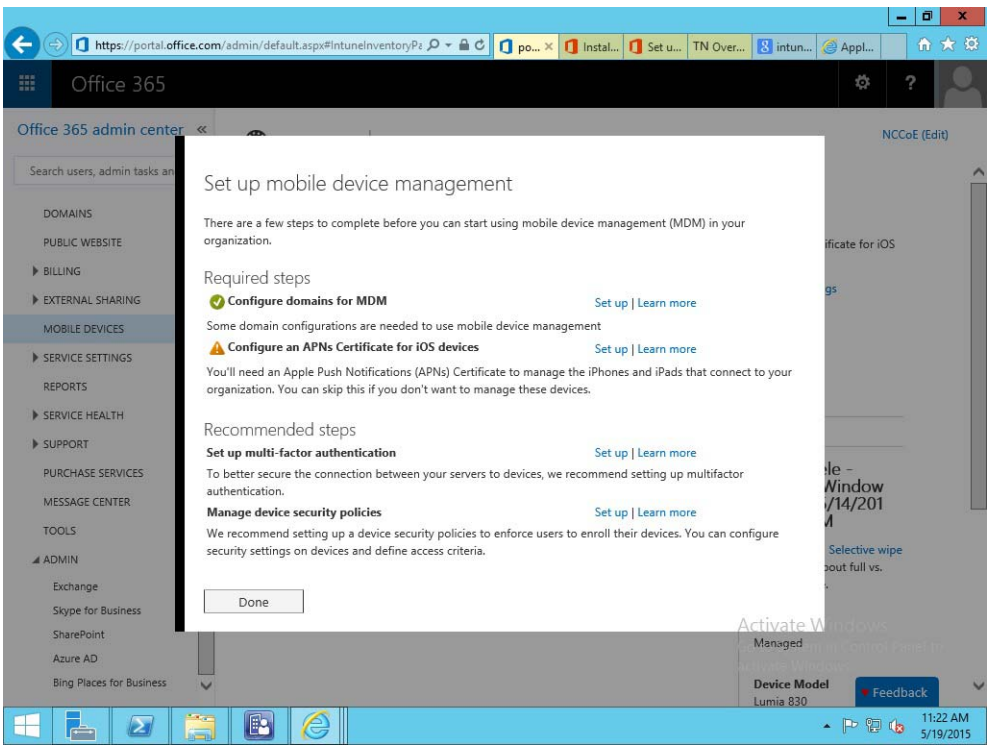
111 2.1.3.1 Configure Push Certificate for iOS Devices

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



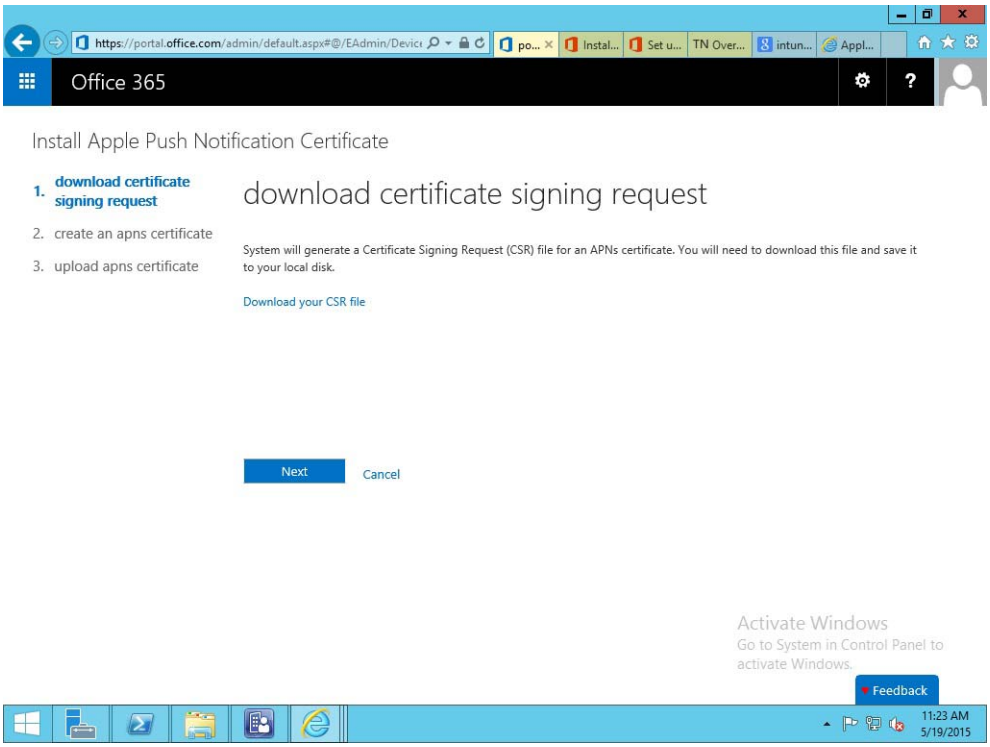
114

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



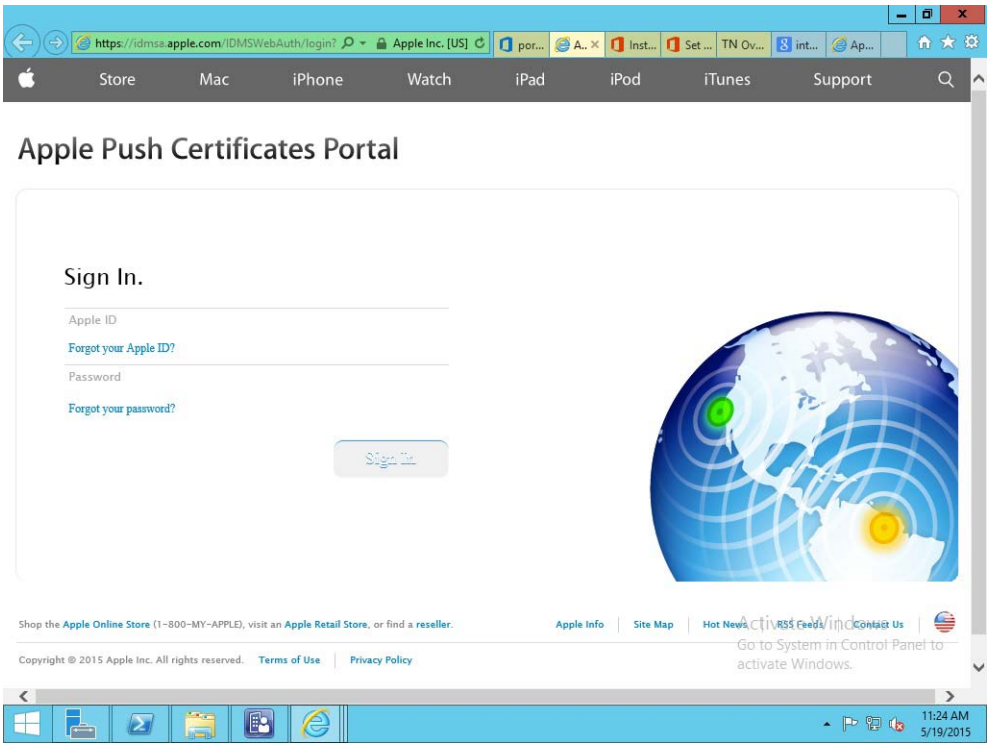
116

117 2. **Configure APNs Certificate for iOS devices -> Setup**

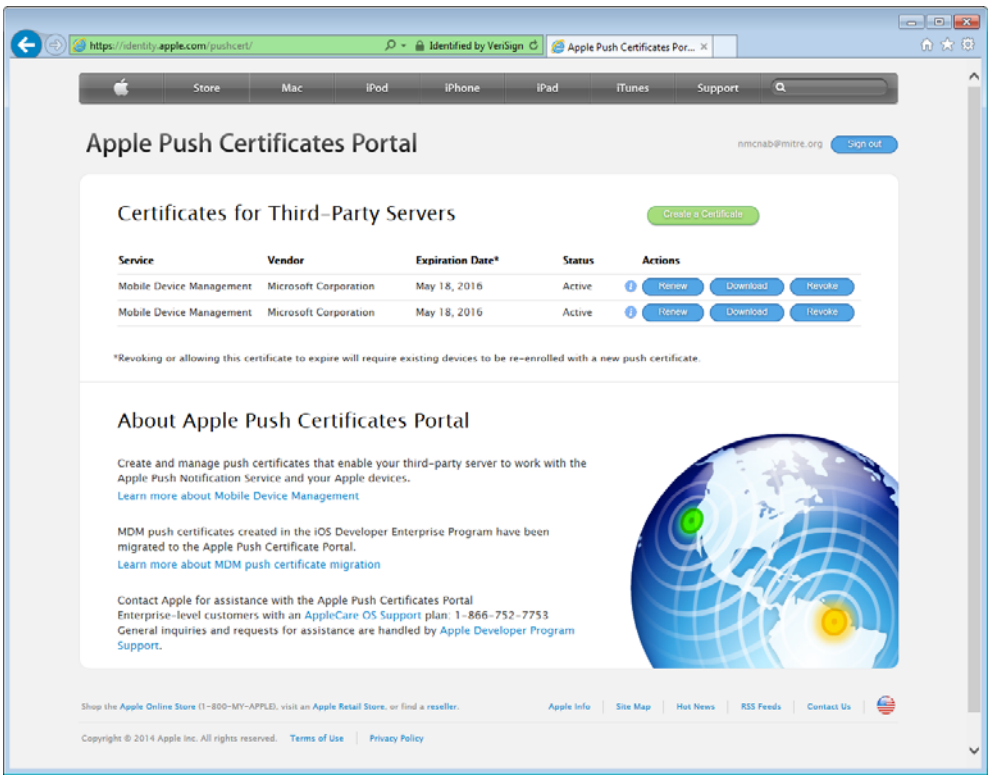


3. Download certificate signing request (CSR).
   a. Once the CSR is generated, it can be submitted to Apple for signing.
   b. Use a browser to visit[3] https://identity.apple.com/pushcert/
   c. You will be prompted for your Apple Developer account credentials.

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



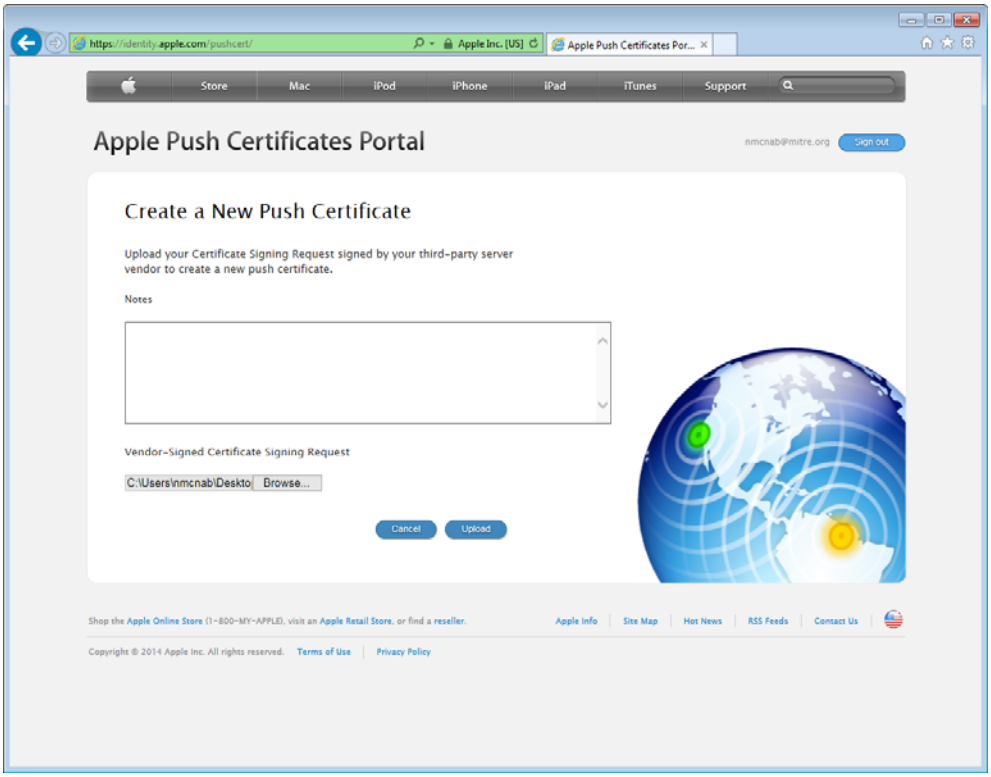
123



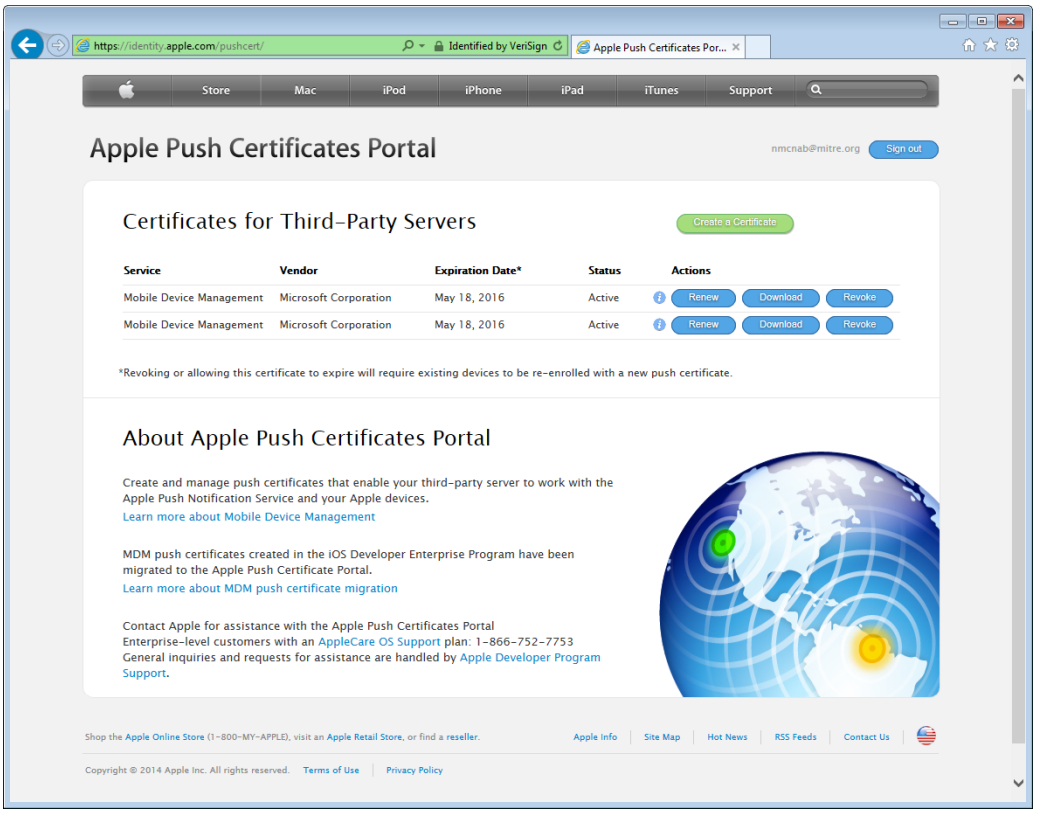
124

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

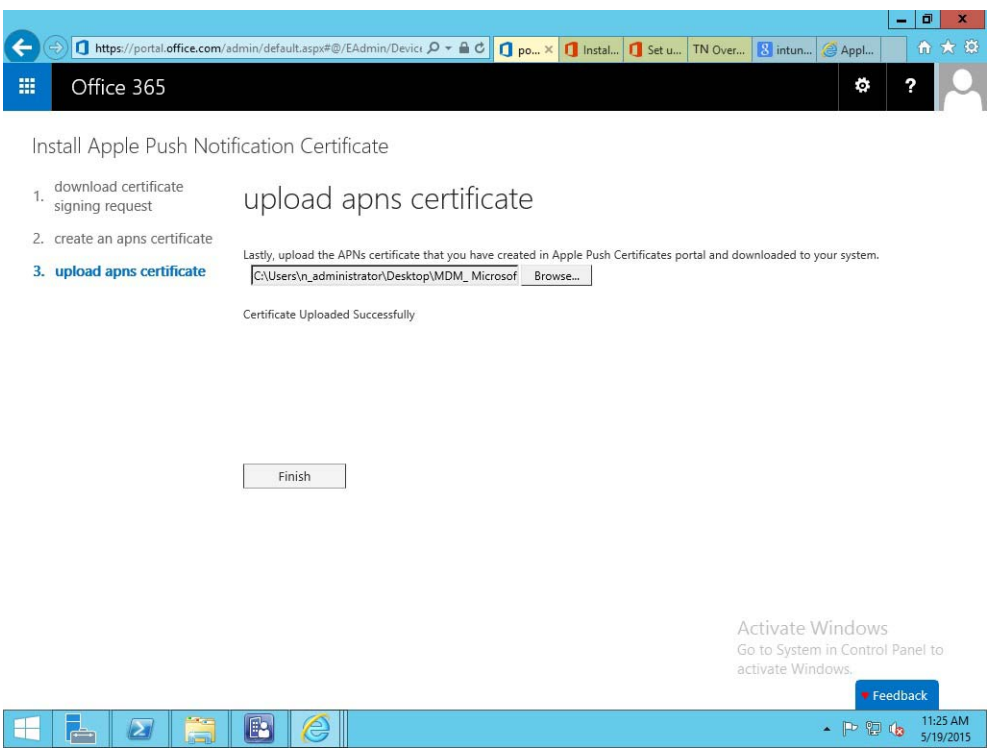
a. Review the terms and conditions screen. You will be presented with a screen to submit your CSR. Use the **Browse** button to navigate to where you stored your CSR file and choose **Upload**.



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.

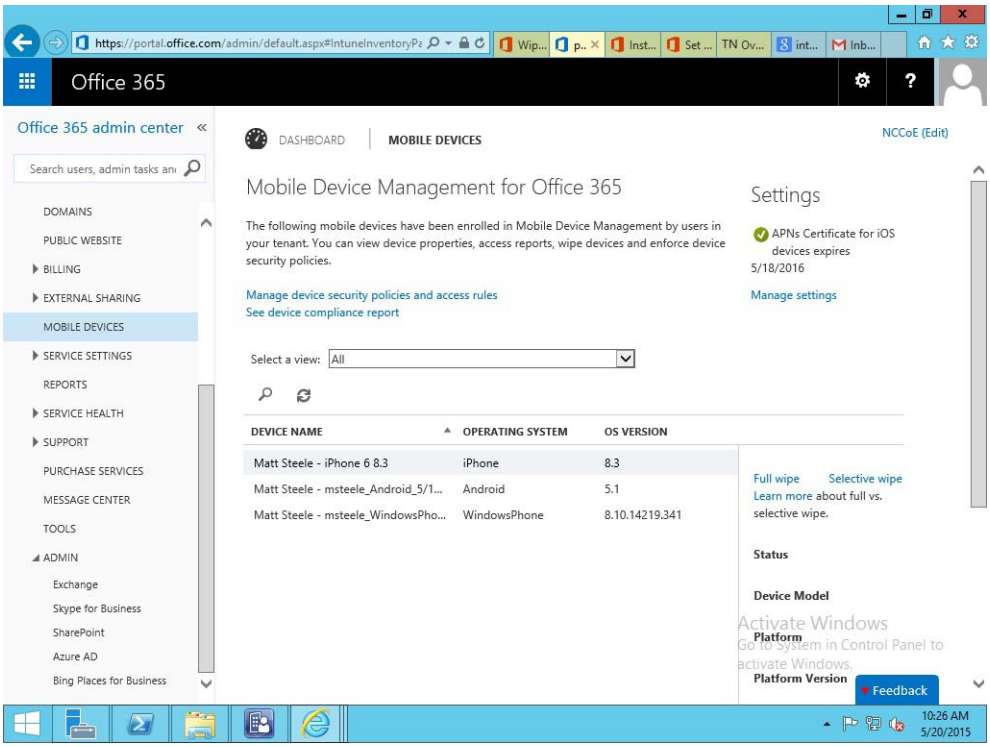


133



134

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



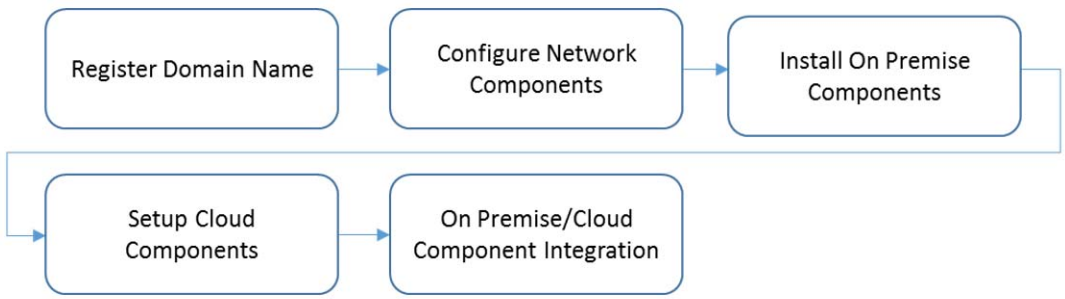
7. Verify that the APN is working correctly; it should have an expiration date listed.

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

3.1 Hybrid Build Setup and Configuration

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



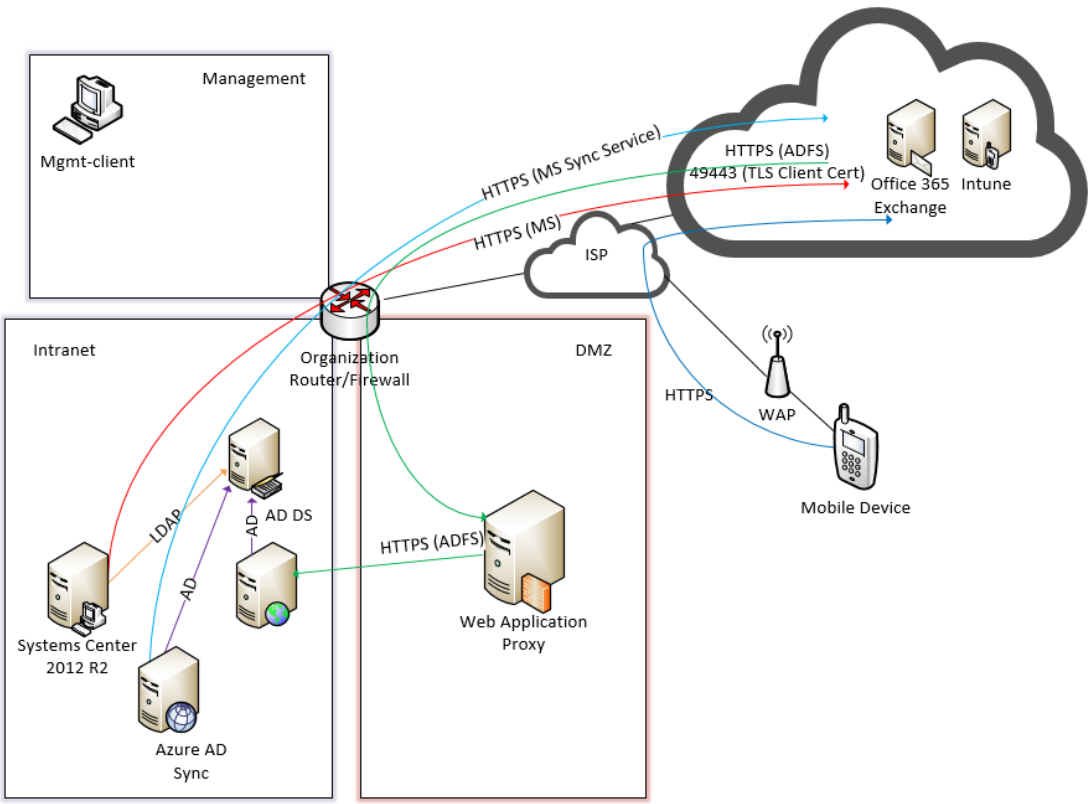
An important prerequisite to using Microsoft's Active Directory Federation Service (ADFS) in this hybrid arrangement is a third-party public key certificate issued bya reputable certificate authority. In this build we used Symantec's Secure Site Pro service. You may also want to purchase a third-party 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

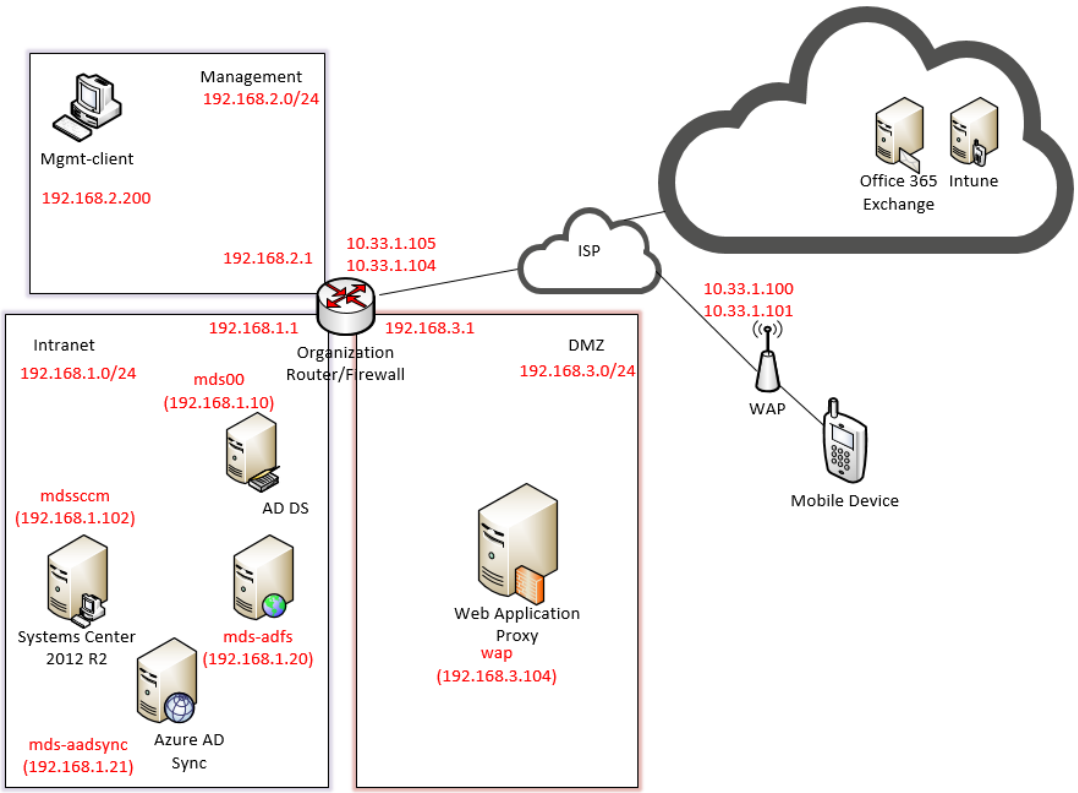
The following architecture diagrams depict the final architecture of the hybrid build after implementing this guide. Figure 3.2 calls out the various protocols implemented between the on-premises, cloud and mobile device components. Figure 3.3 is a similar view, but details the network addressing and hostnames that were used during the build.

36 **Figure 3.2 Detailed Architecture**



37

38 **Figure 3.3 Detailed Architecture with IP Addresses**



39

40 3.2.1 Hybrid Build Components

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

42

Table 3.1 Components

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

Table 3.1 Components

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

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

3.2.2 Enterprise Network and Firewall

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

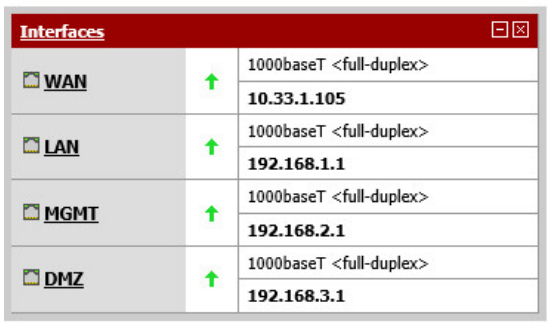
A single firewall configuration was chosen for simplicity and flexibility in a lab environment.[4] Only IPv4 is used.[5]

Implementers should refer to PFSense documentation for installation and configuration instructions. To recreate the configuration, follow the instructions in the documentation and use the configuration files[6] made available by PFSense.

The following screen shots show the final configuration of the PFSense device. Access PFSense through its Web interface. The default screen includes a list of interfaces described as part of the architecture in section 3.2. The individual interfaces are described below with the firewall rules.

4.A dual firewall configuration could also be implemented.
5.IPv6 is disabled for simplicity.
6.pfSense Configuration Files:
Interfaces - interfaces-config-pfSense.localdomain-20150402160851.xml
NAT - nat-config-pfSense.localdomain-20150402160838.xml
Firewall - filter-config-pfSense.localdomain-20150402160823.xml

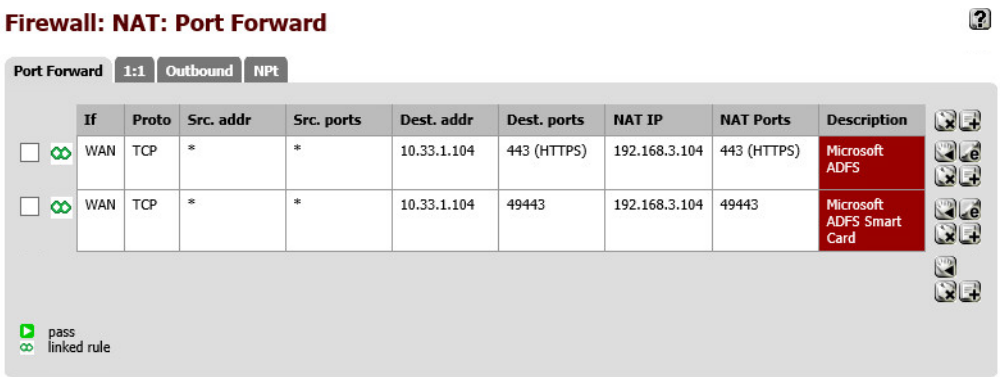
56 **Figure 3.4 List of Configured Interfaces**



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.

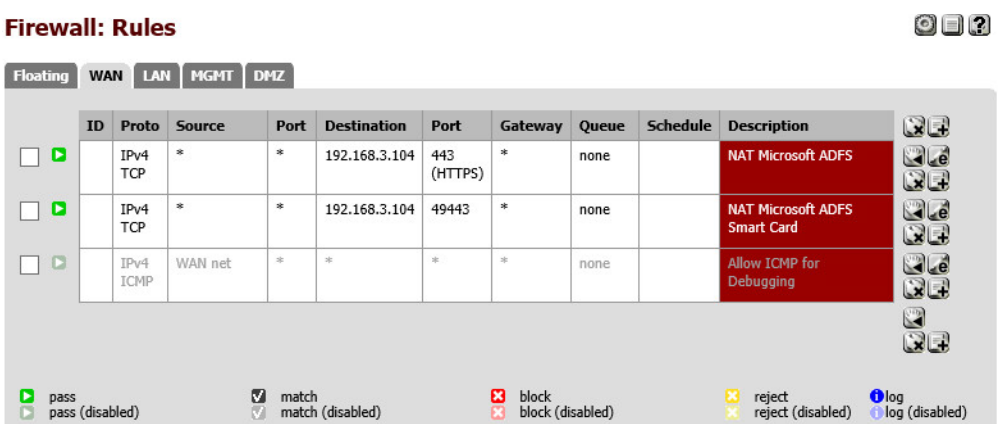
60 **Figure 3.5 WAN**



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**

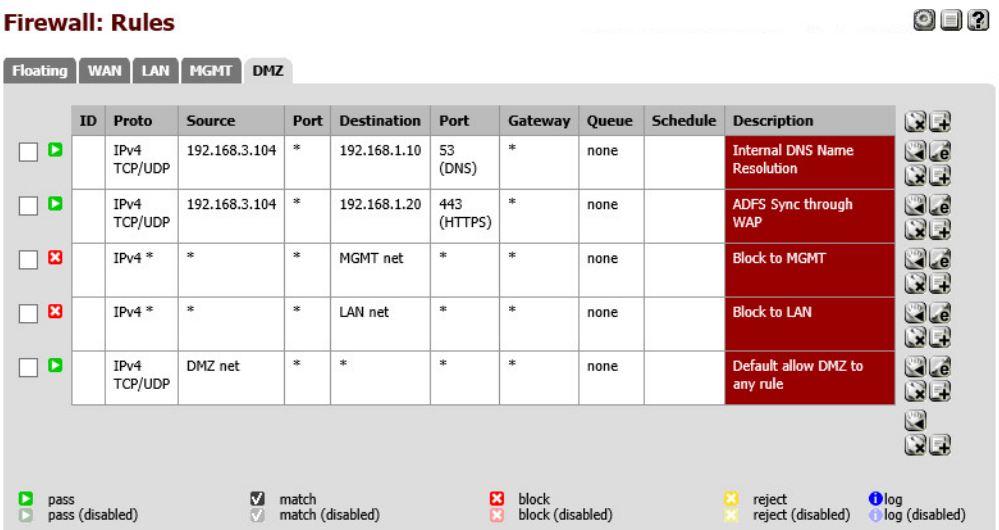


66

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

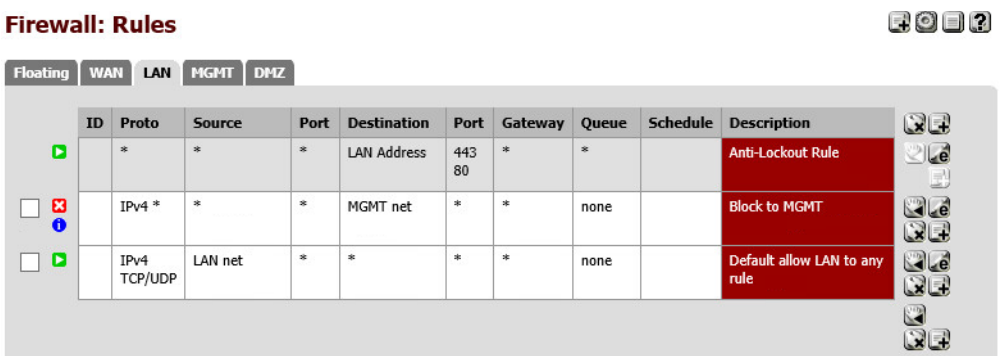
Web application proxy (WAP) service. Firewall rules are configured to allow Internet access to the WAP in the DMZ in order for ADFS to function.

Figure 3.7 DMZ Firewall Rules



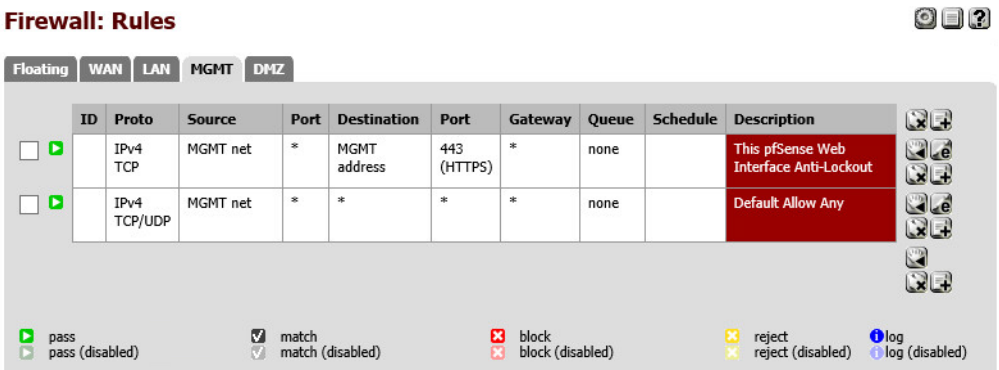
In PFSense, our DMZ is assigned as DMZ (OPT2) using the network 192.168.3.0/24. It is not allowed to access the Intranet or MGMT networks, except under specific rules for DNS and ADFS access. The IP address of the Active Directory server is 192.168.1.10. The IP address of the ADFS server is 192.168.1.20.

Figure 3.8 LAN Firewall Rules



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

82 **Figure 3.9 Management Firewall Rules**



83

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

86 3.2.3 Enterprise Software Components for Hybrid

87 This section describes the installation of the on-premises components of the hybrid build. As
88 noted previously, this guide provides references to the vendor's documentation for installation
89 to better customize the component to the target environment. Alternatively, implementers
90 may replicate this build exactly by using table 3.2, which maps each component to the exact
91 system used in figure 3.2.
92

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

97 3.2.3.1 Active Directory Domain Services

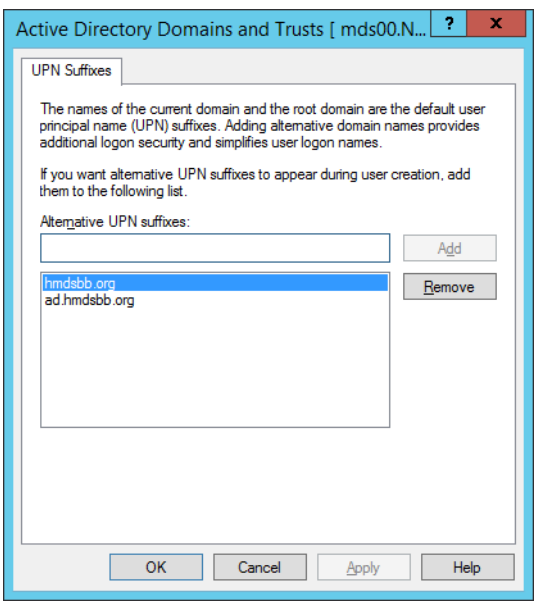
98 The Active Directory Domain Services (ADDS) instance used in the hybrid build was created
99 using basic configuration settings offered through the Add Roles and Features Wizard. The
100 system was deployed as a new forest with a domain name of nccoe.local. Implementers of this
101 guide who seek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

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

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

The procedures to configure a UPN suffix are as follows:

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



3.2.3.2 Active Directory Federation Service

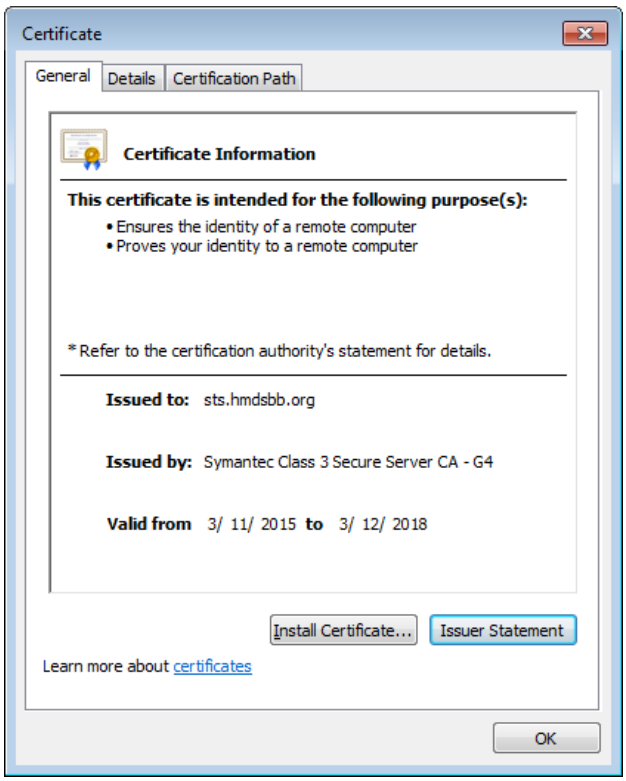
Refer to Microsoft documentation for specific installation instructions for your environment. Consult the following articles as a starting point for installation [6] [7].

Implementers should note the requirement of a certificate issued by a certificate authority that is recognized/trusted by Microsoft. In this demonstration, the build team procured certificates

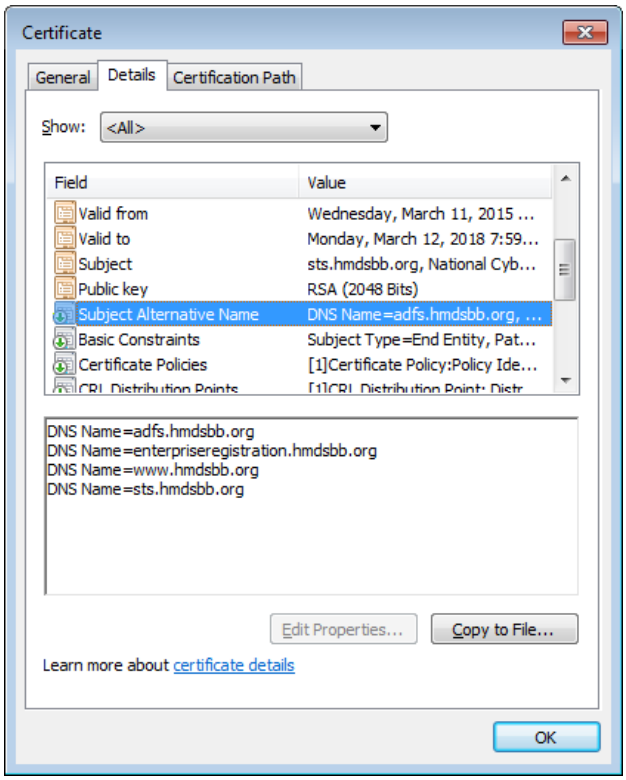
7.http://blogs.technet.com/b/jratsch/archive/2012/02/17/creating-a-test-lab-from-a-production-environment-using-hyper-v-and-gpmc-scripts.aspx

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

131 3.2.3.3 Active Directory Federation Services Proxy

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

133 3.2.3.4 Systems Center Configuration Manager

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

136 3.2.3.5 Azure Active Directory Sync Services

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

138 3.2.4 Cloud Services Instances

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

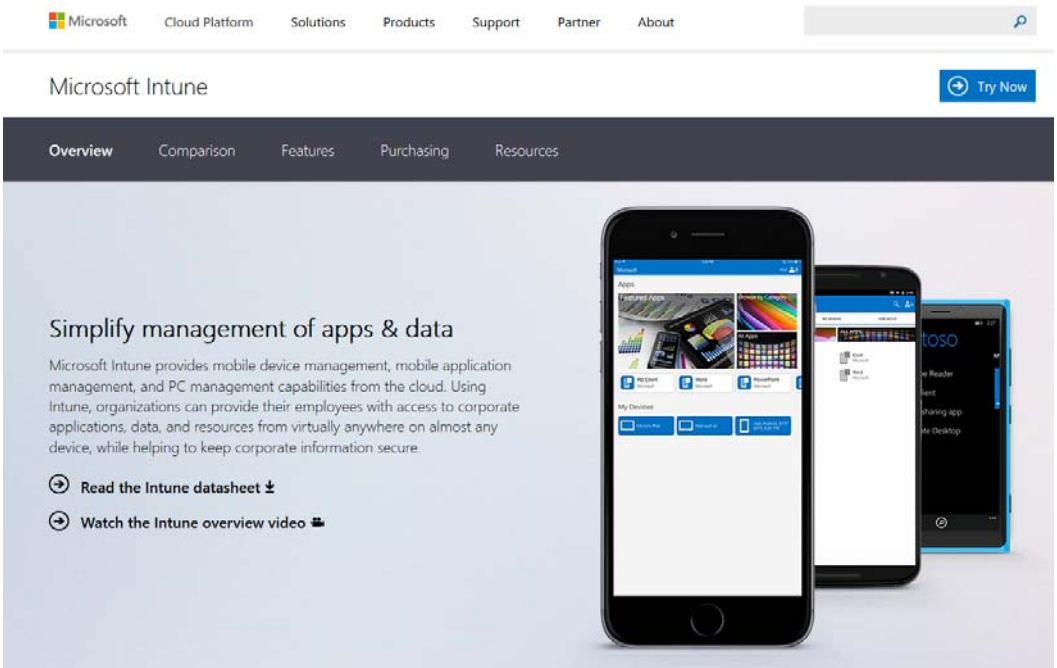
142 3.2.4.1 Office 365 Setup

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

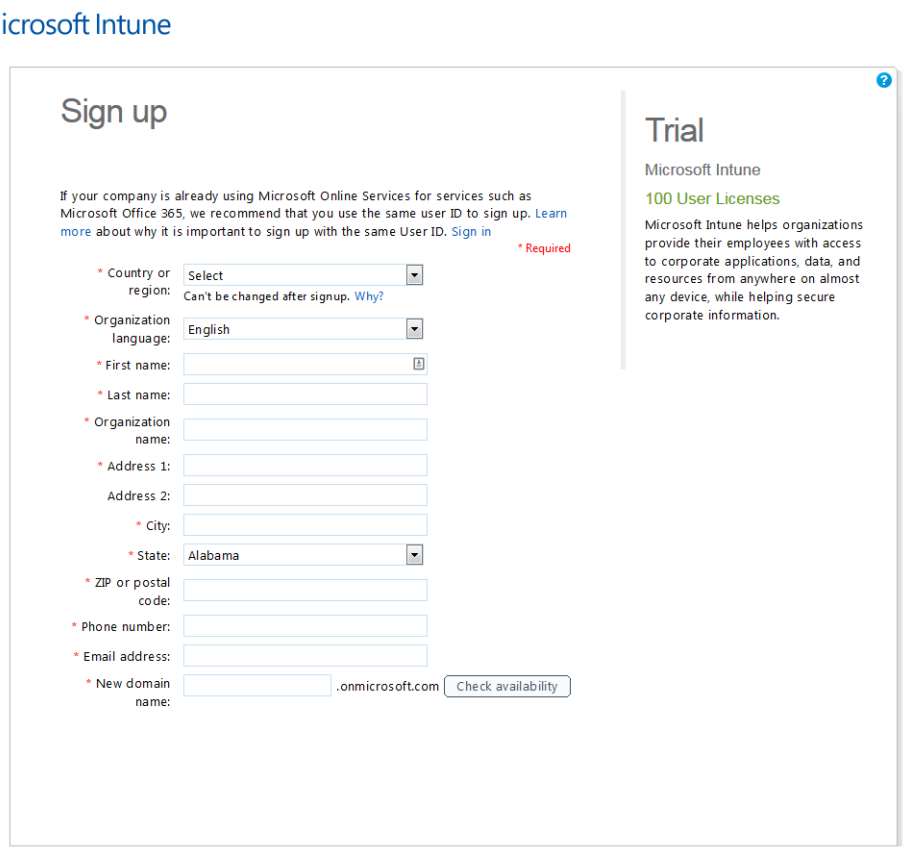
3.2.4.2 Intune Setup

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

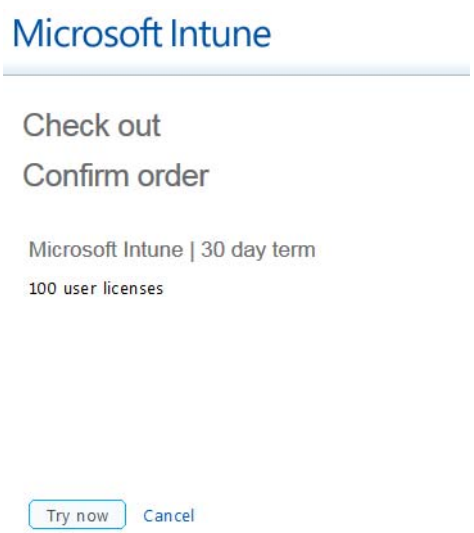
http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/



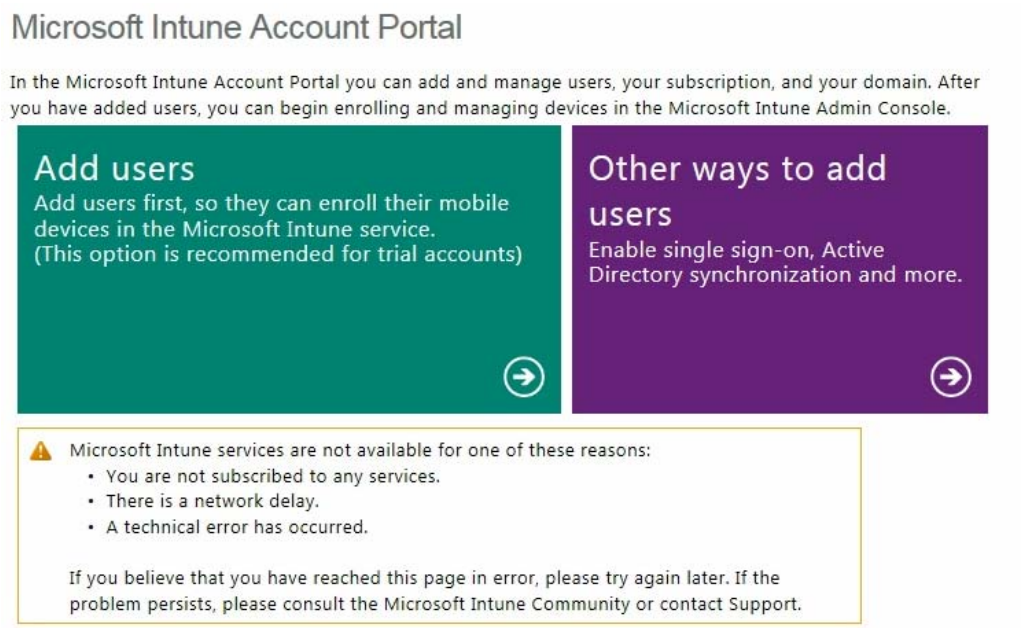
1. Choose **Try now**.



2. Choose **Sign in**. Sign in when prompted.



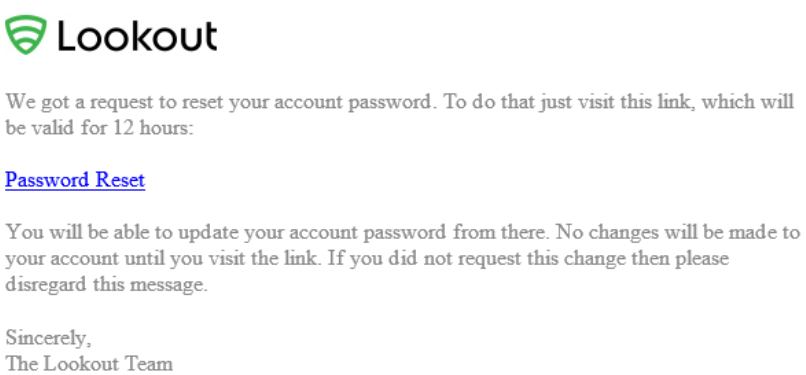
3. Choose **Try now**. When signup is complete, you should be redirected to the Intune management console at https://manage.microsoft.com. Note that Silverlight 3.0 browser support is required to load the management console.



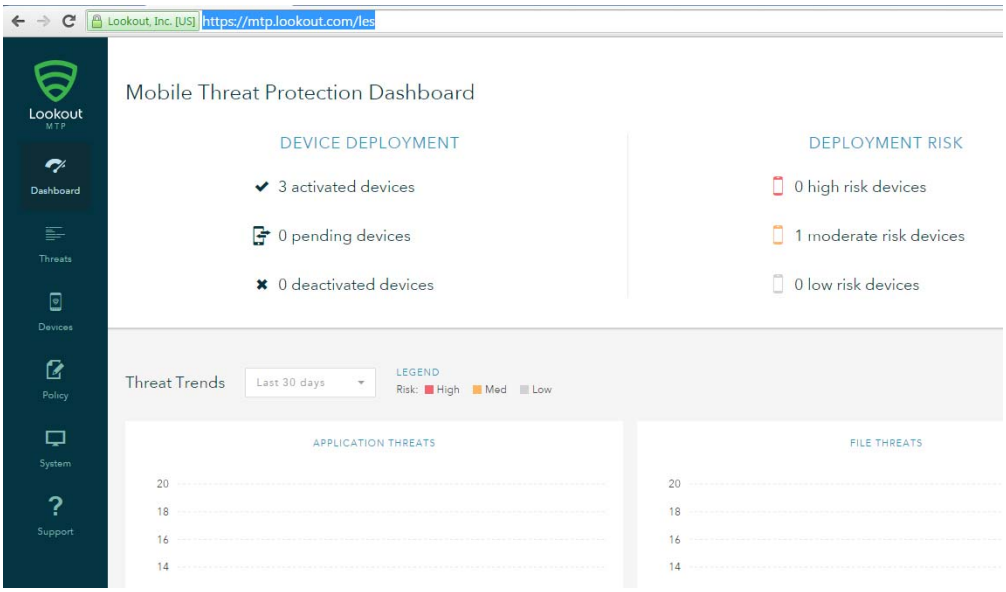
Note: *Important! Do not proceed any farther with Intune if you want to manage devices via SCCM.*

3.2.4.3 Lookout Setup

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



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.



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

3.2.5 Hybrid Integration

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

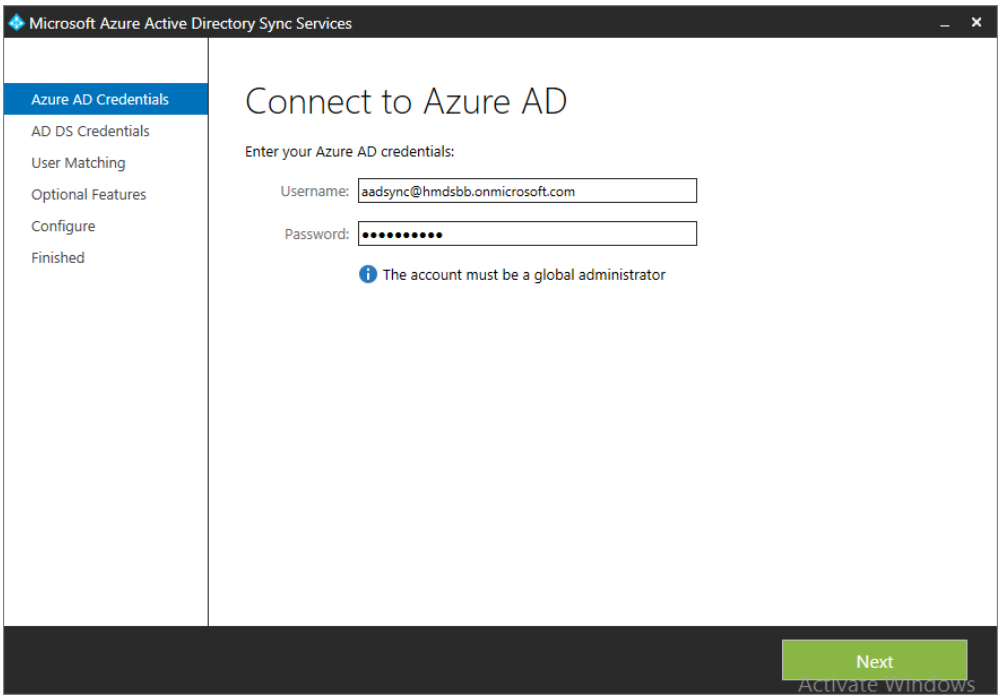
3.2.5.1 Office 365 with Active Directory Federation Setup

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 365as described in section 2.1.2. If not, follow the procedures from TechNet Magazine [10]. Detailed integration information can be found in the referenced TechNet article [7].
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.

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

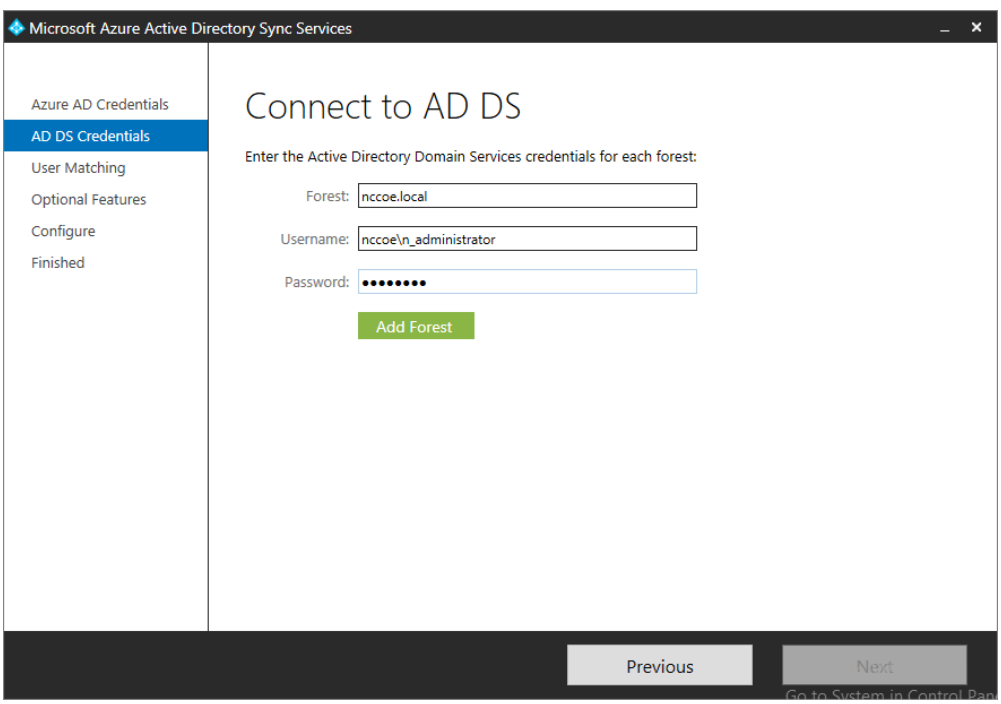
3.2.5.2 Azure Active Directory Sync Services

For this step we configure synchronization of the organization's enterprise Active Directory with the Office 365 directory. This service will periodically sync identities--adding, deleting or otherwise modifying from the on-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.



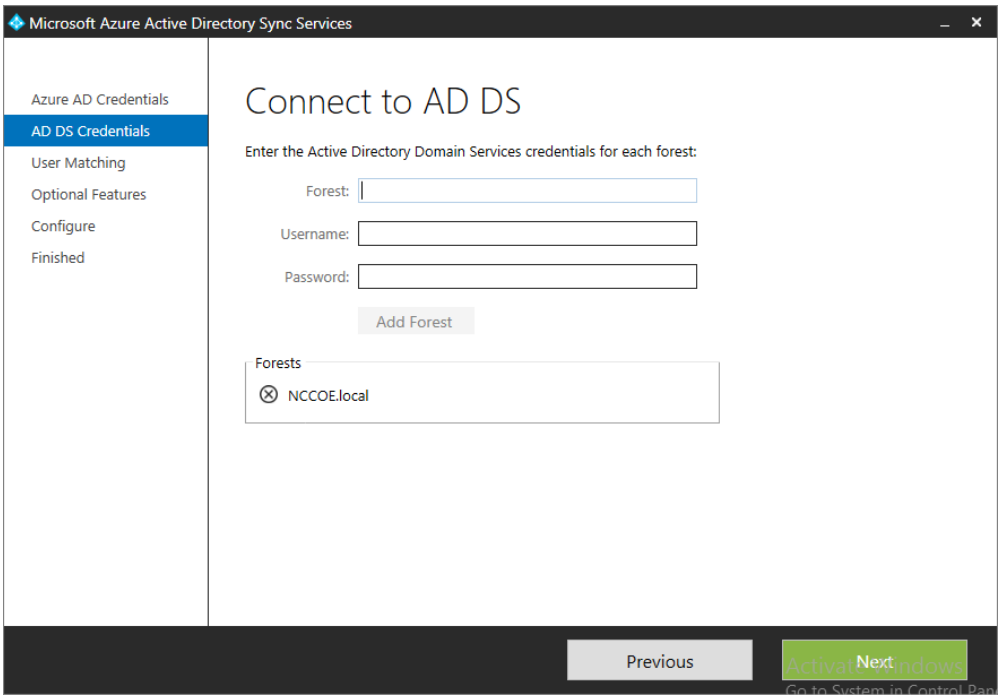
188

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



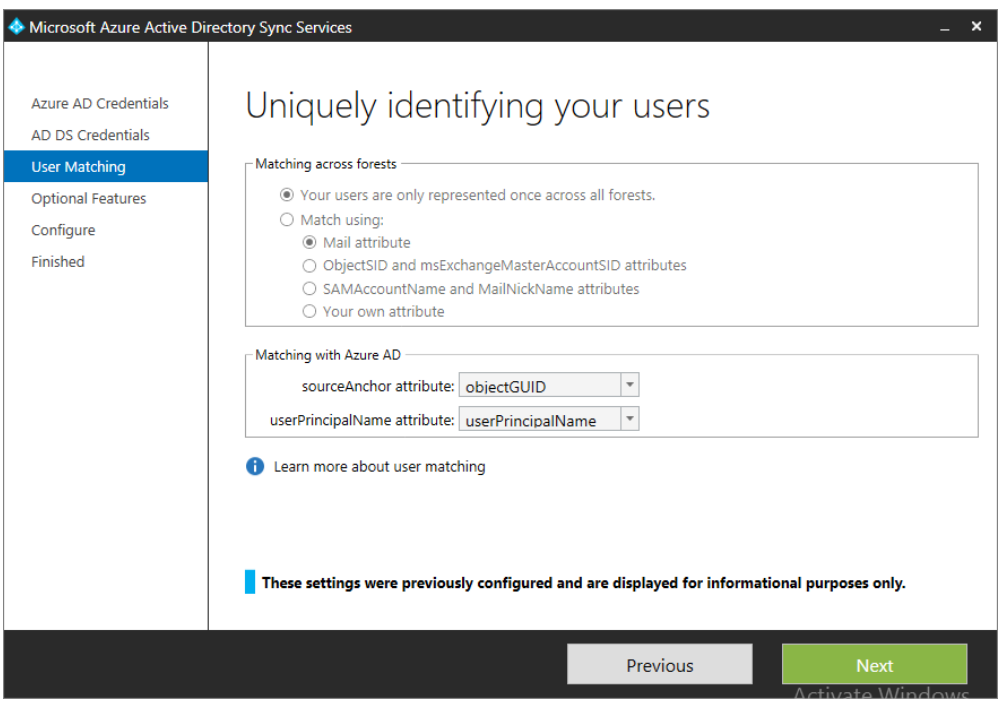
191

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



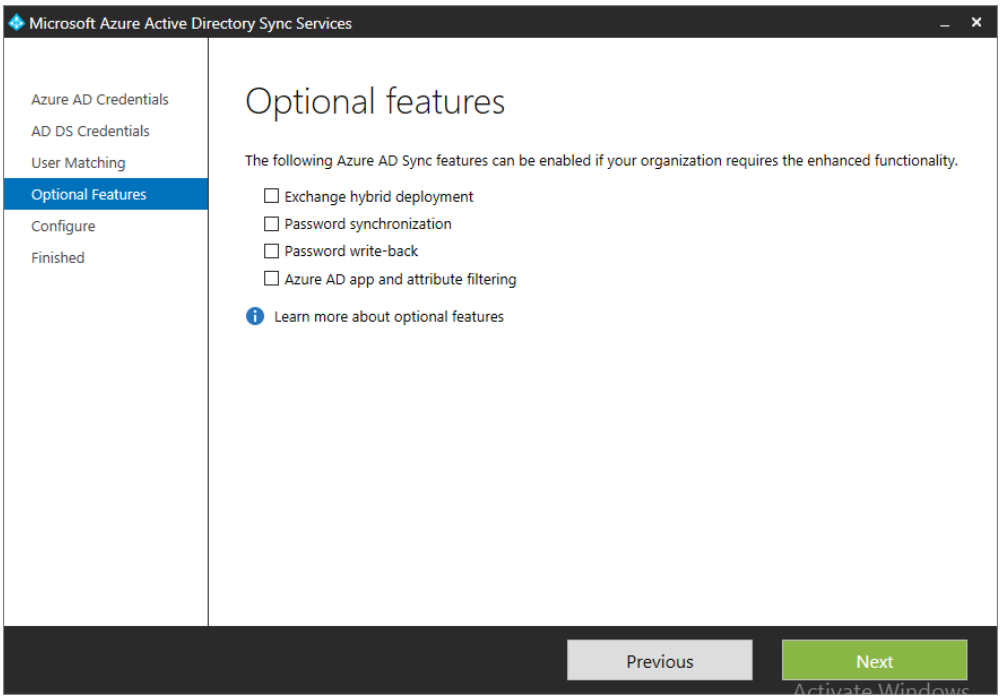
193

194 3. Click **Next**.



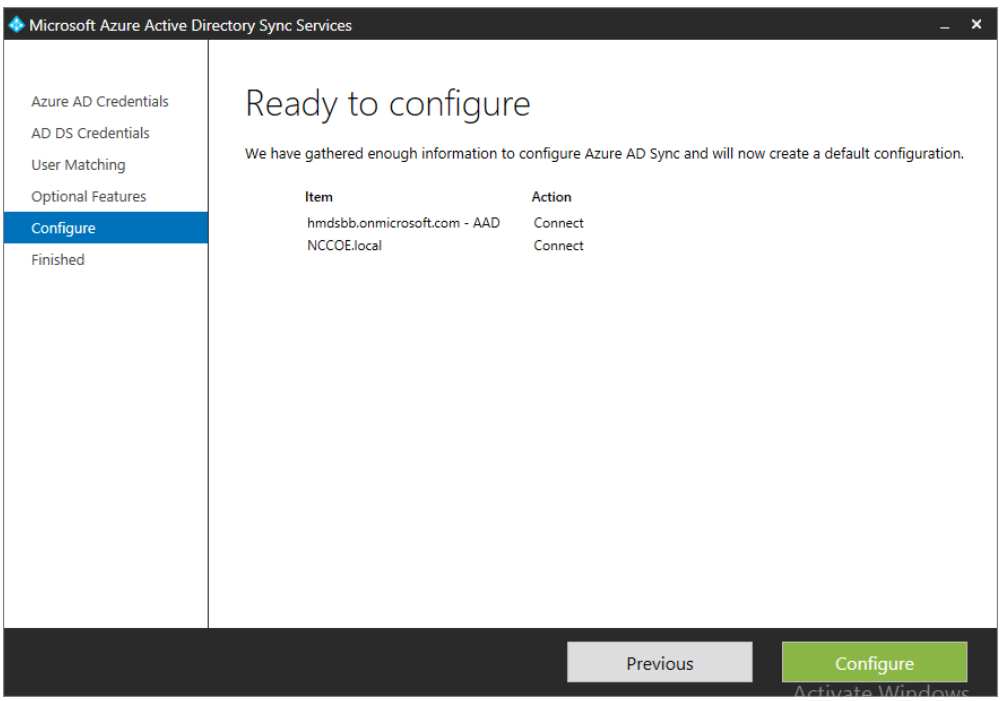
195

196 4. Accept the defaults for uniquely identifying your users.



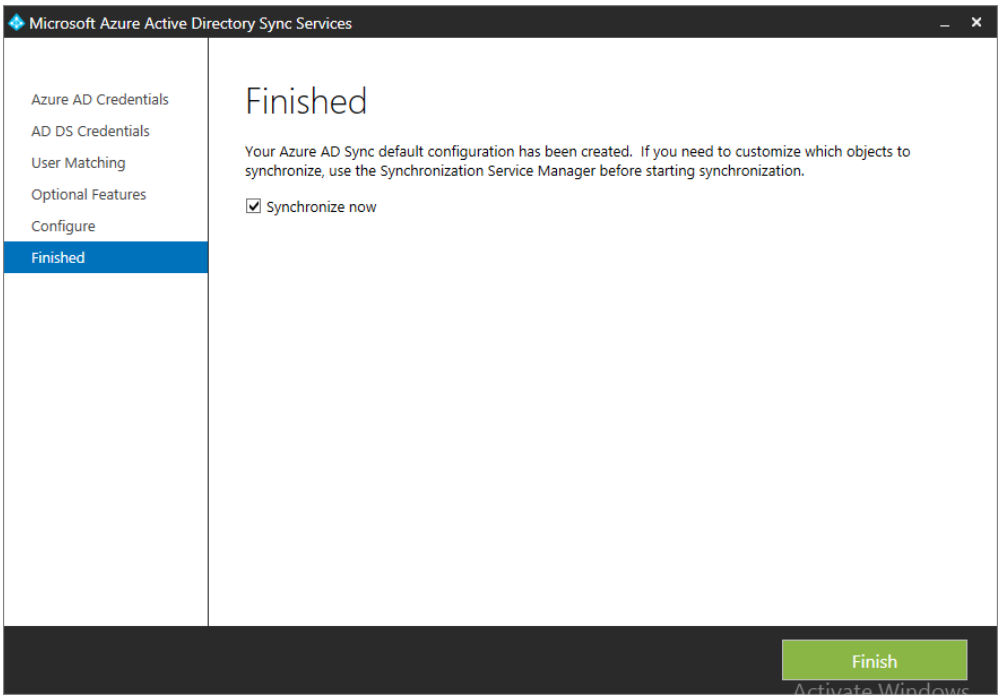
197

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



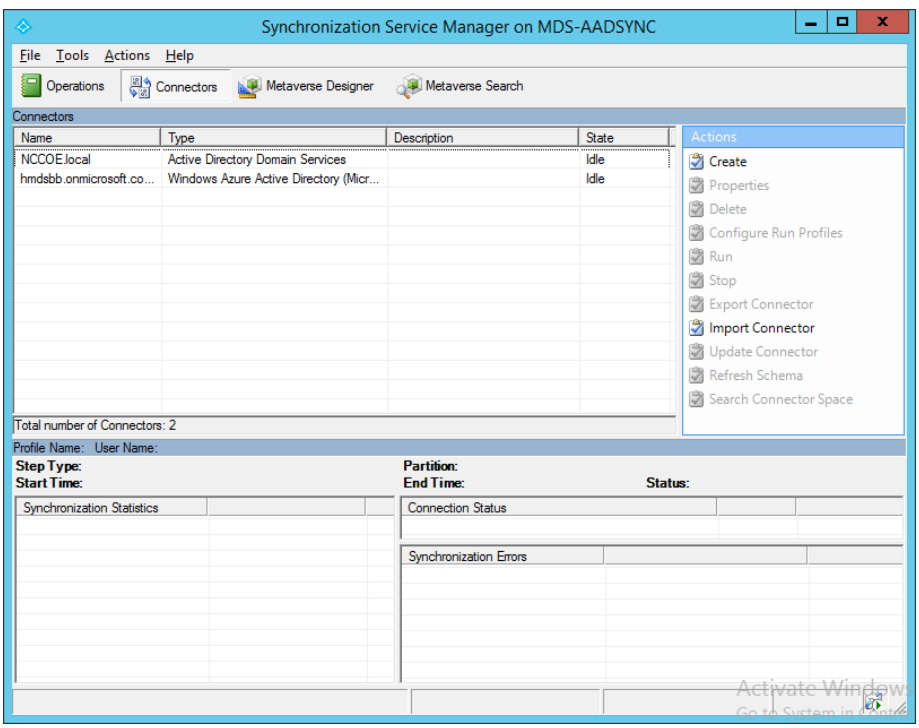
199

200 6. Click **Configure**.



201

202 7. Choose **Synchronize now** and click **Finish**.

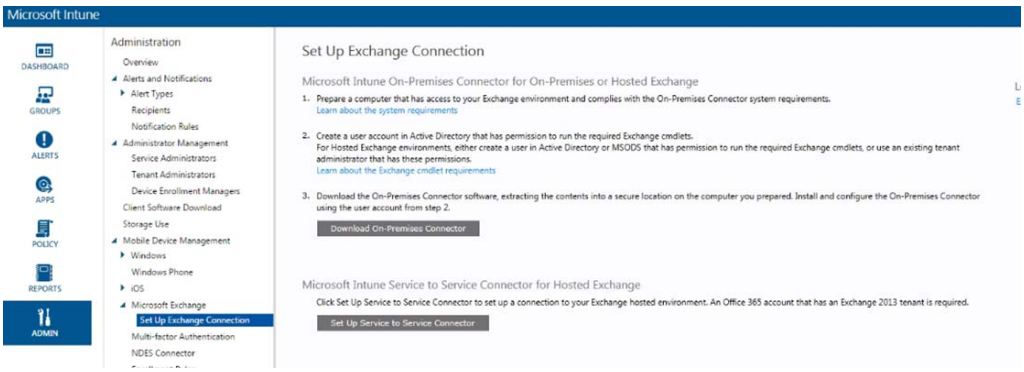


203

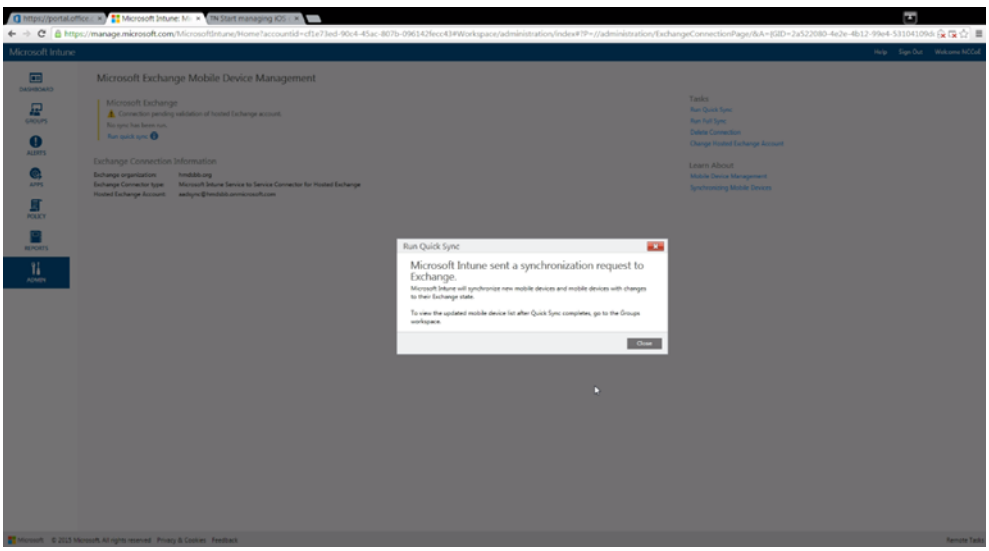
204 8. If successful, the added connectors will be displayed in the Synchronization Service
205 Manager.

3.2.5.3 Sync Intune with Office 365 Exchange

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.



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**.



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

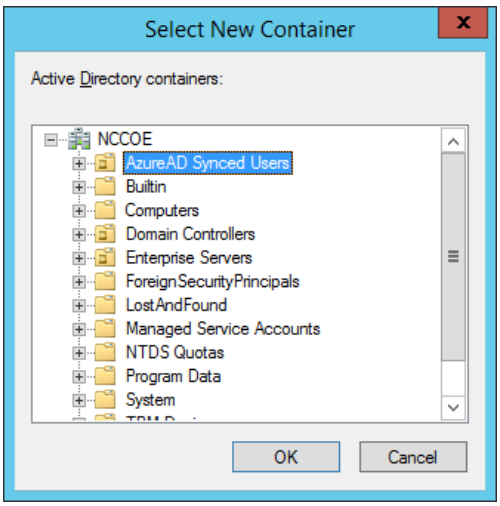
3.2.5.4 Manage Intune with SCCM

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

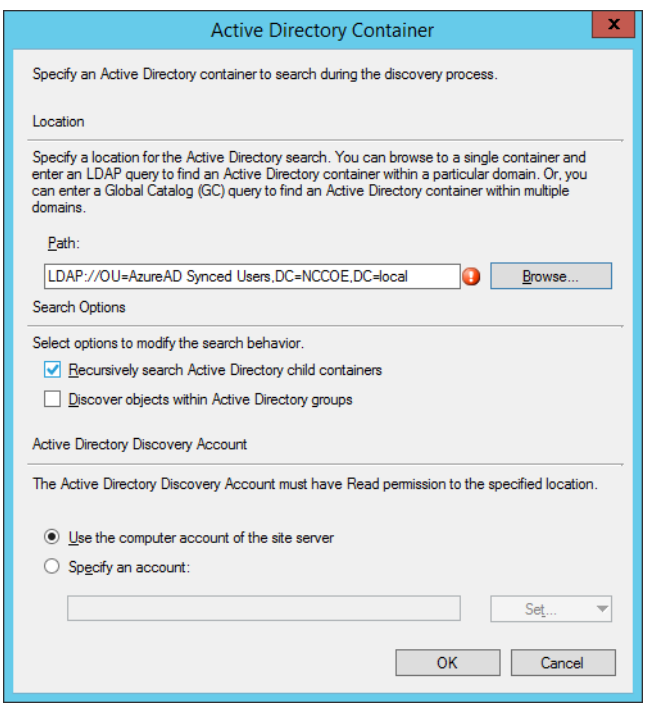
3.2.5.4.1 Configure Active Directory User Discovery

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

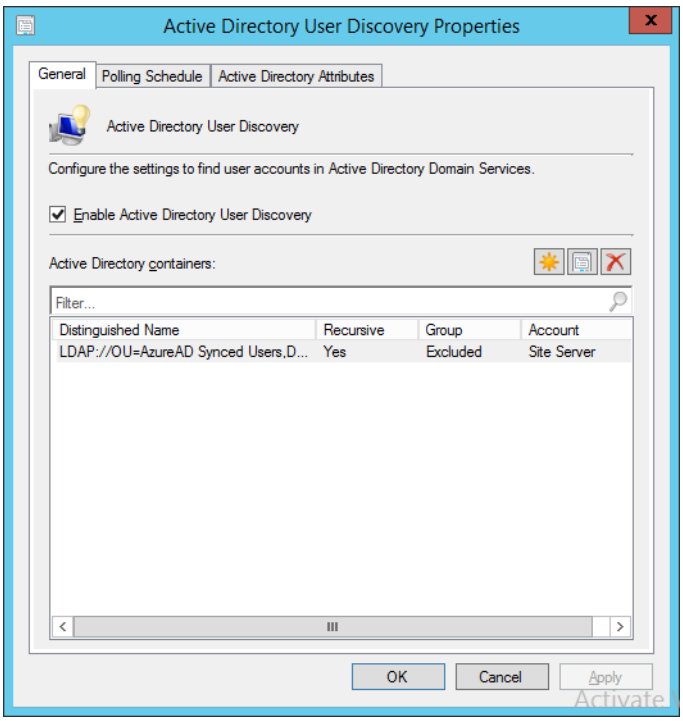
1. Launch the Configuration Manager console. Navigate to **System Center Configuration Manager / Site Database / Site Management /<site name>/ Site Settings / Discovery Methods.**
2. Right-click **Active Directory User Discovery**, and then click **Properties**.
3. On the General tab, click the **New**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



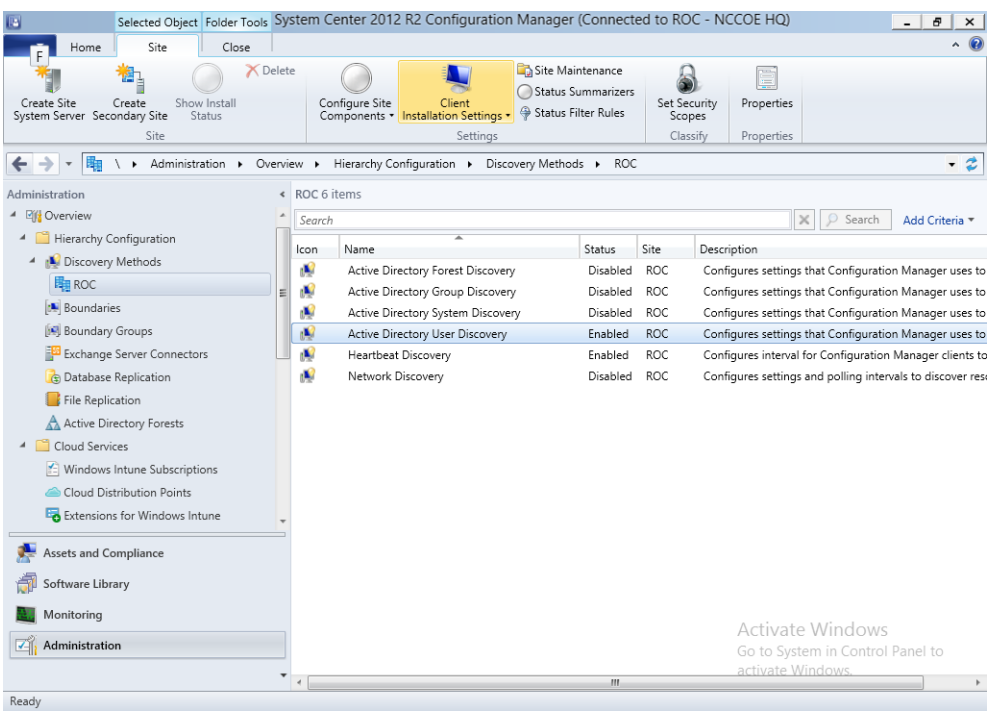
5. Select the **AzureAD Synced Users** container.



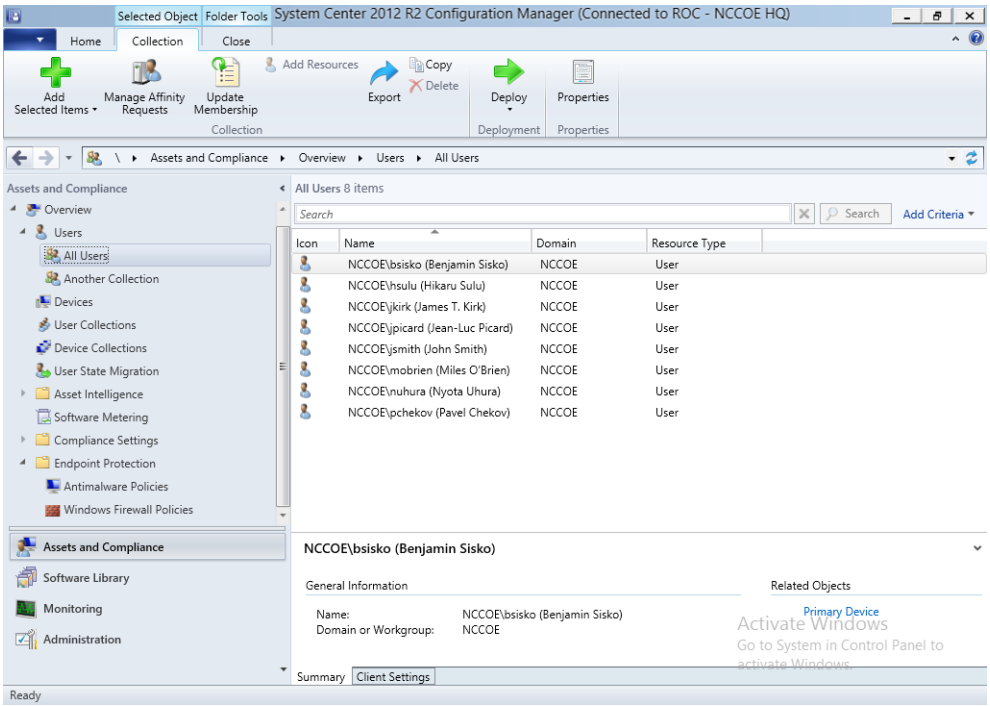
6. The path will reflect the container chosen in the previous step.



7. Ensurethat **Enable Active Directory User Discovery** is selected.



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

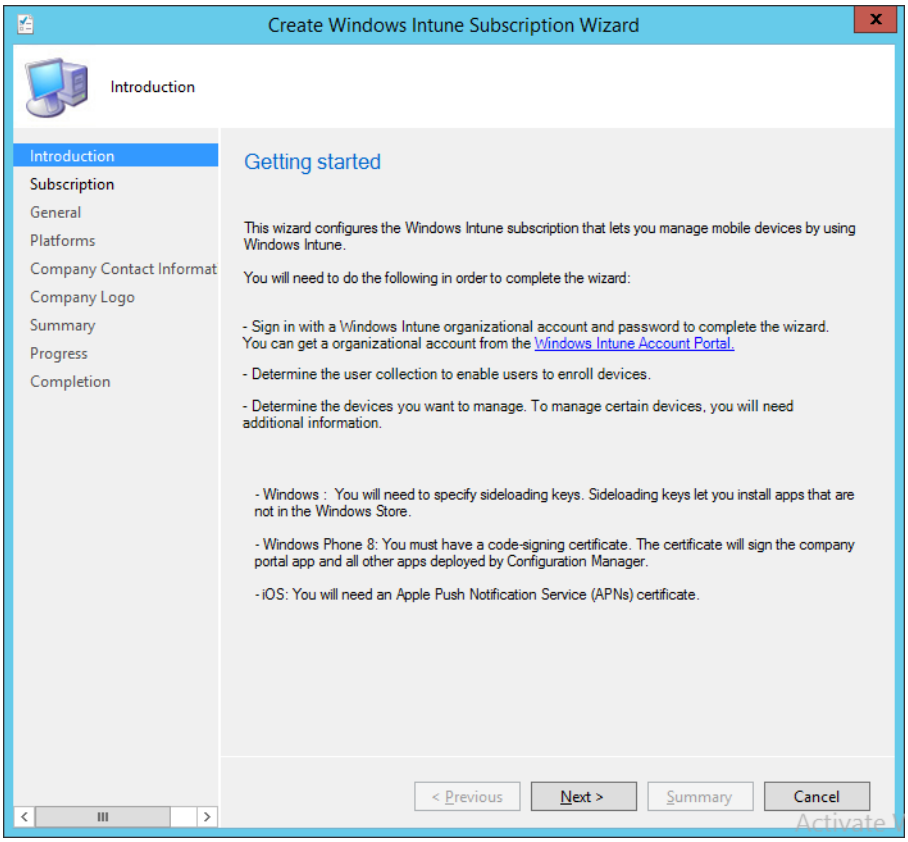


9. Navigate to **Users -> All Users** to view accounts synced from Active Directory.

3.2.5.4.2 Register SCCM with Intune

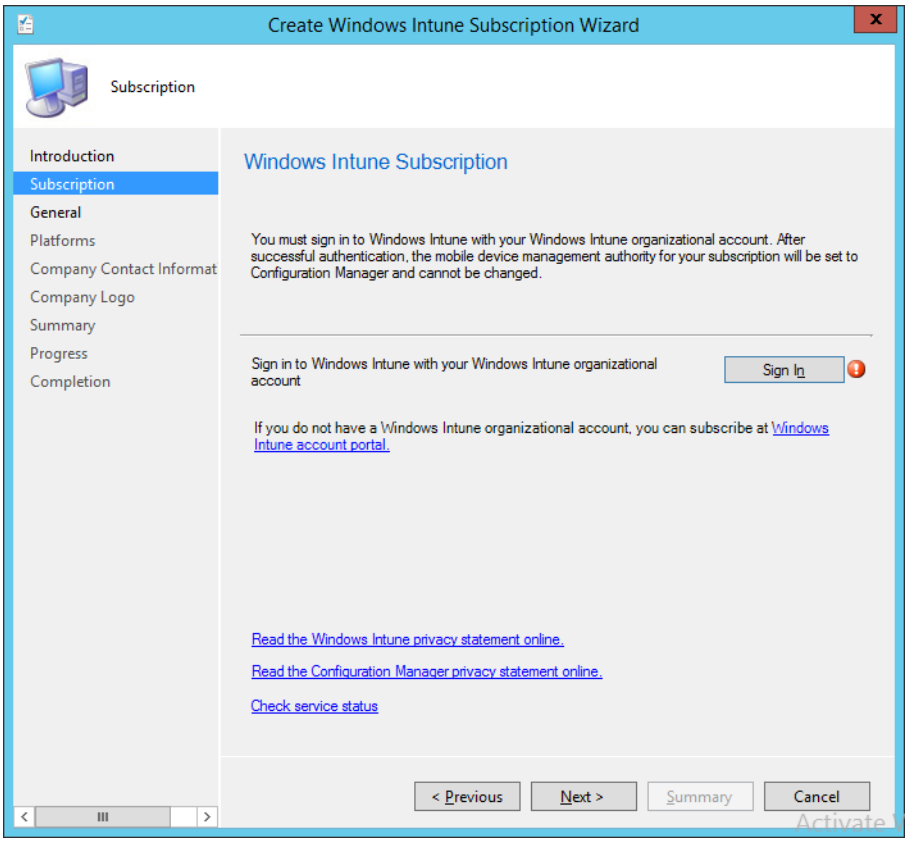
The following sequence of steps enrolls an SCCM instance with the Intune tenant. After this step you will no longer be able to create and deploy policies from the Intune Web management portal.

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



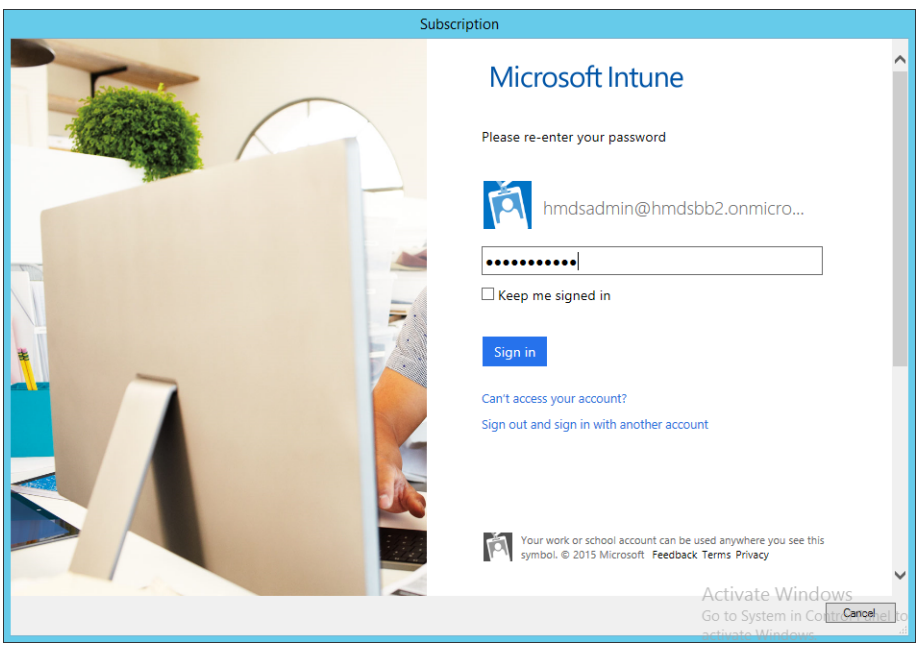
250

251 2. Click **Next**.



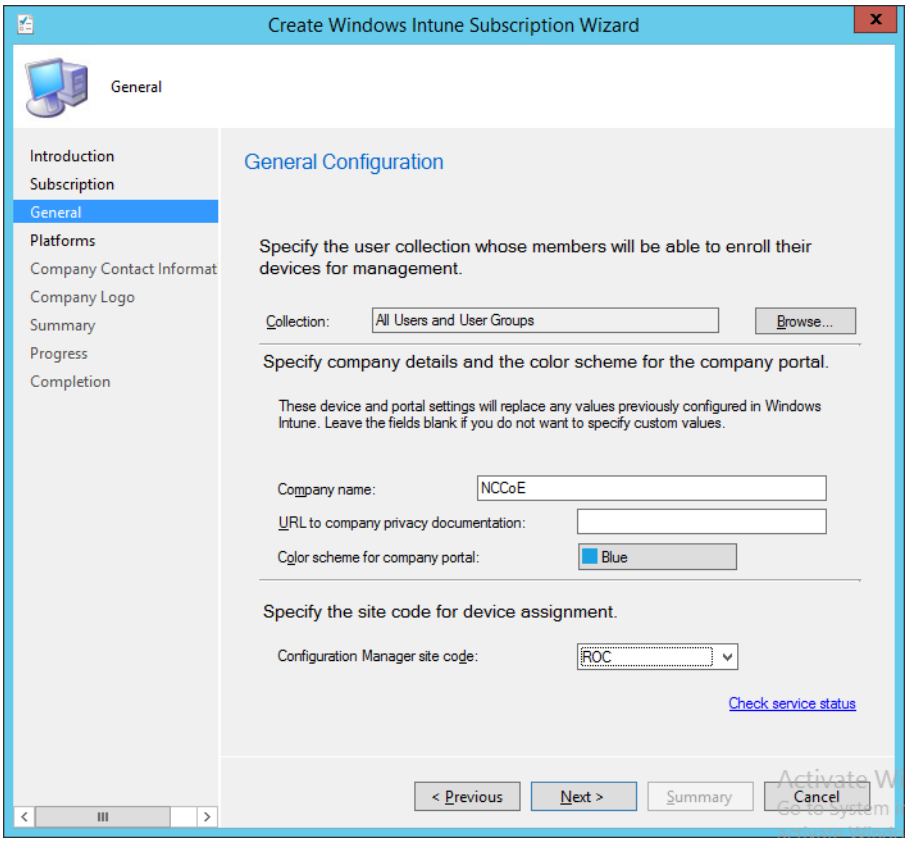
252

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



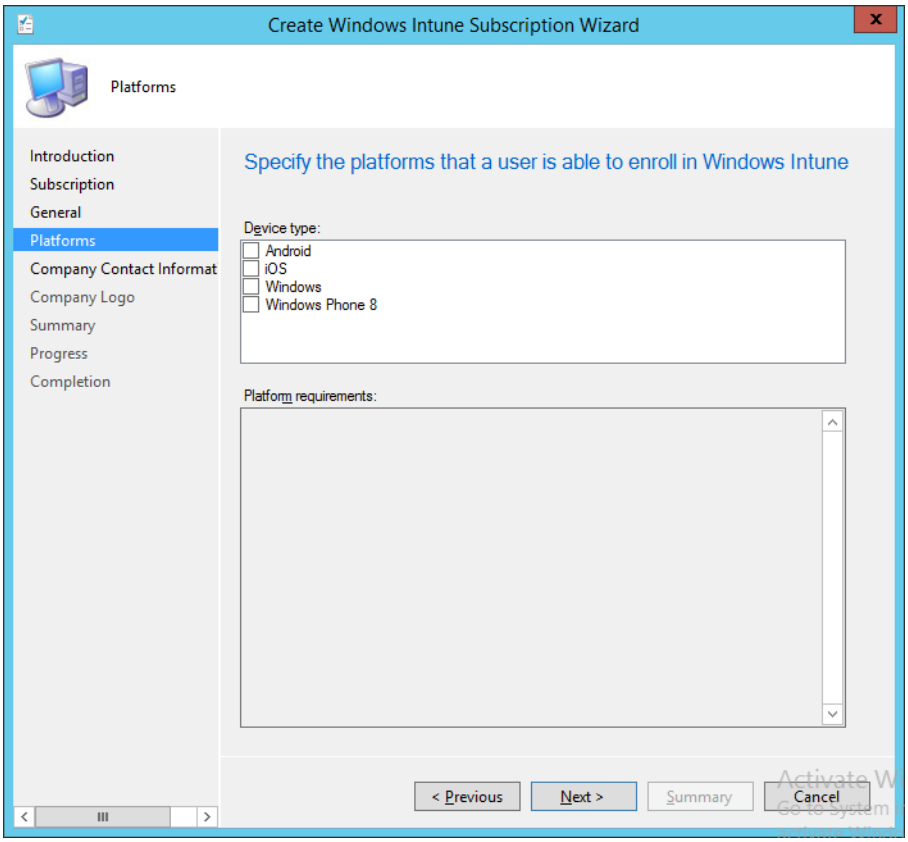
254

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

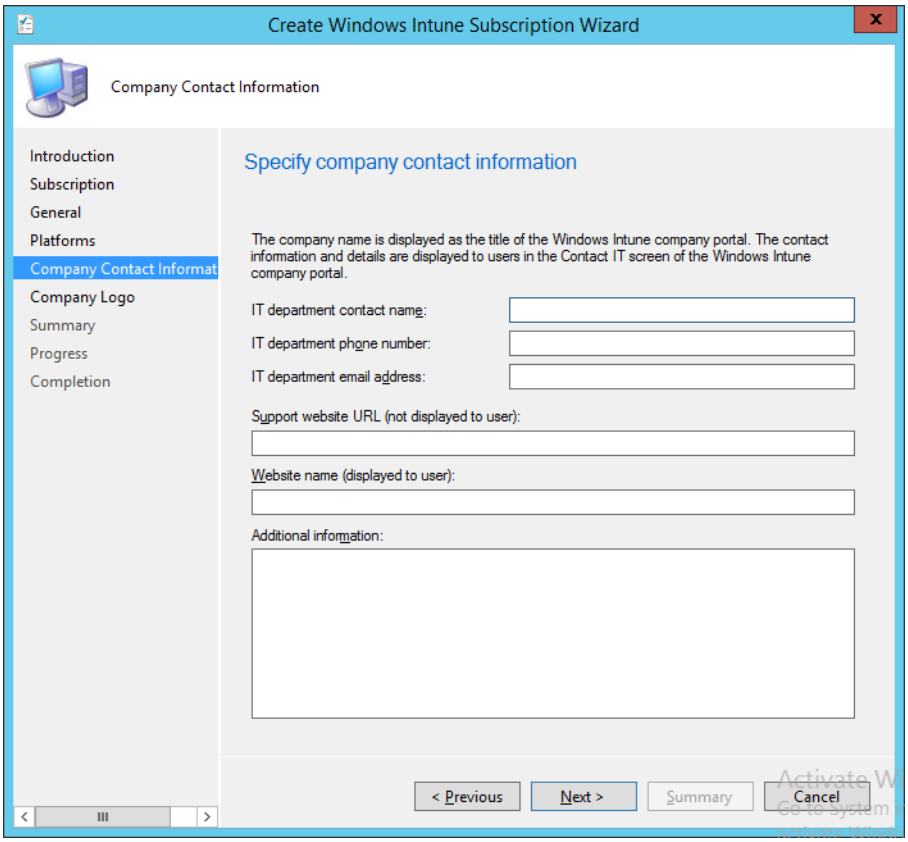


256

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

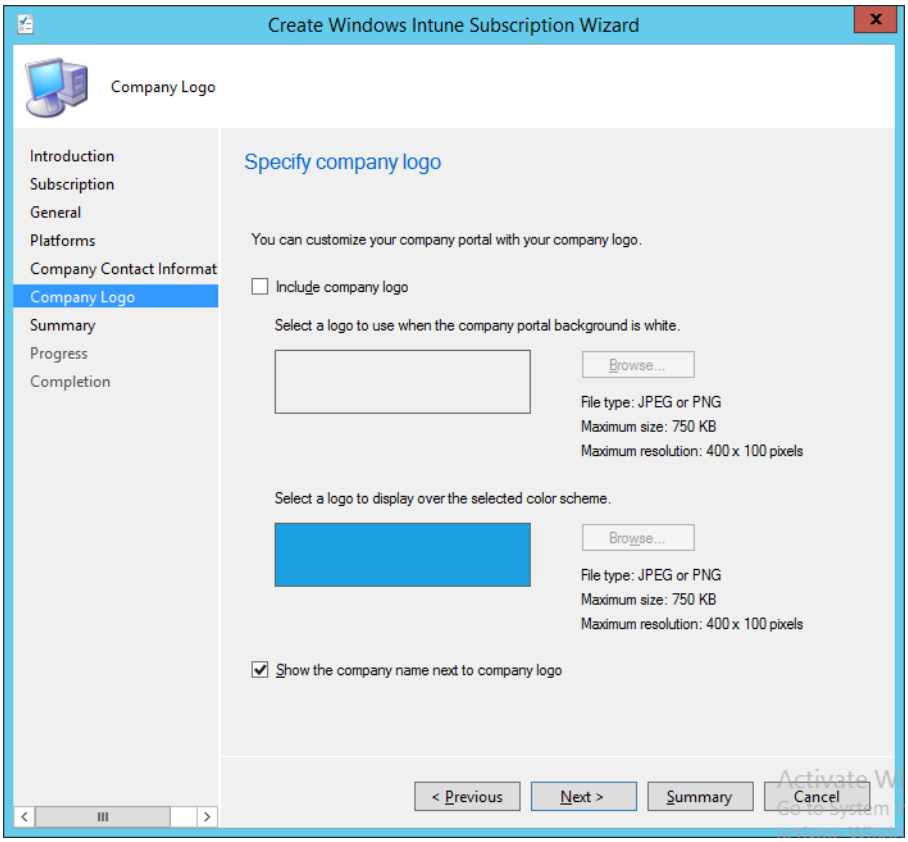


6. You may choose to configure device types in this step. However, we chose to configure these in a later step.



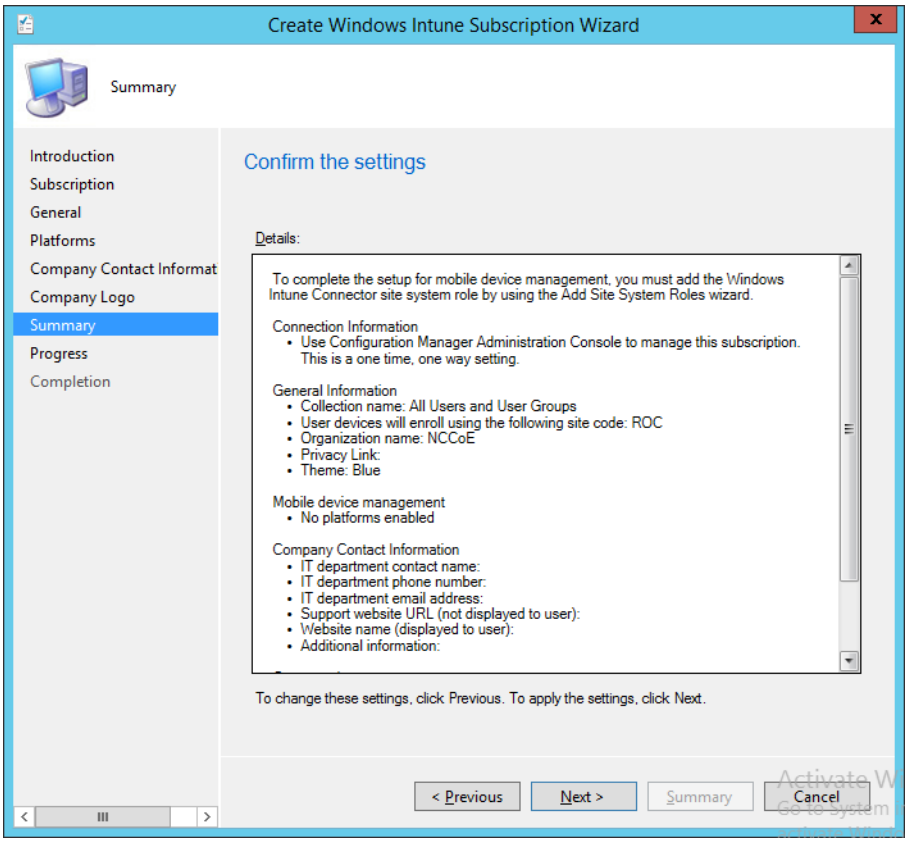
261

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



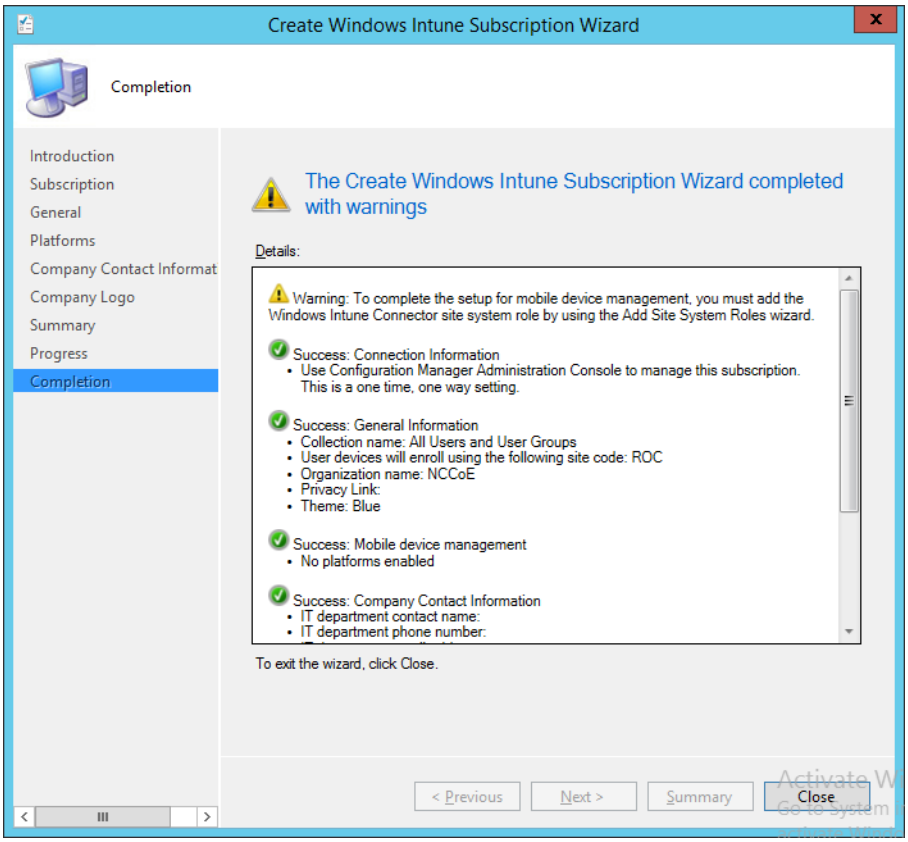
263

264 8. Submit an organizational logo, if desired.



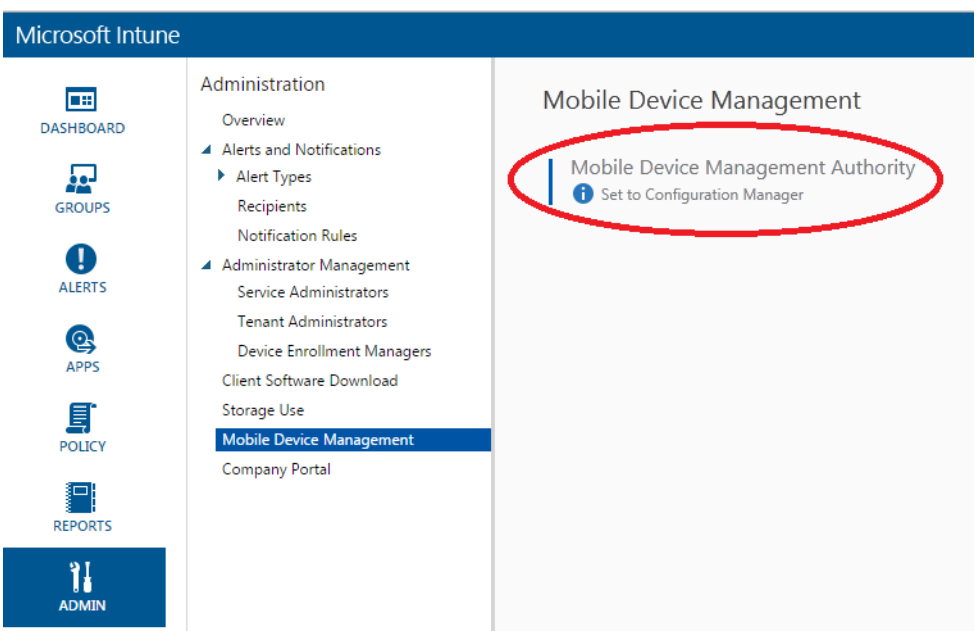
265

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



267

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

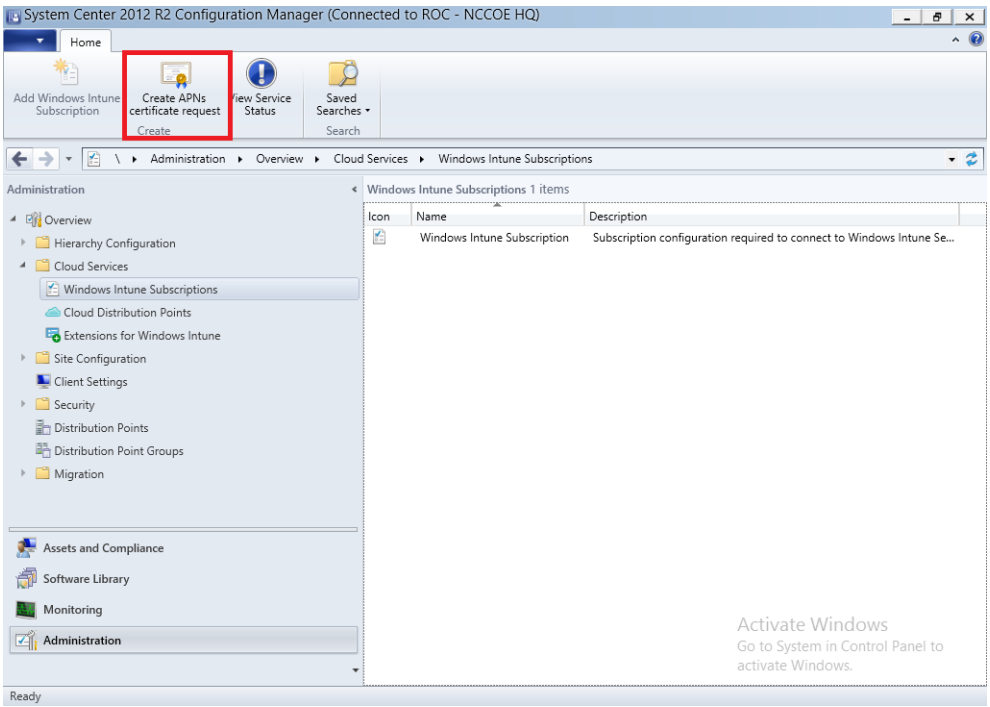


270

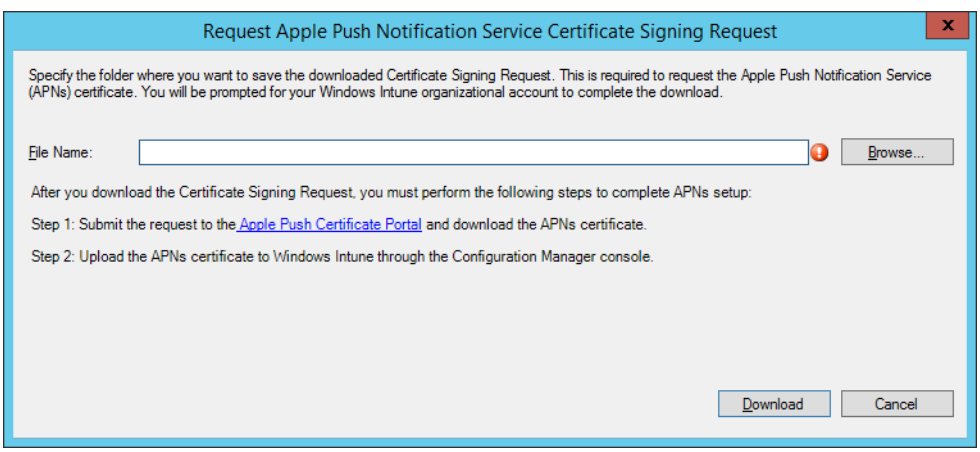
271 11. The Intune administrative console reflects SCCM management after configuration has been
272 completed.

3.2.5.4.3 Configure Push Certificate for iOS Devices

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



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

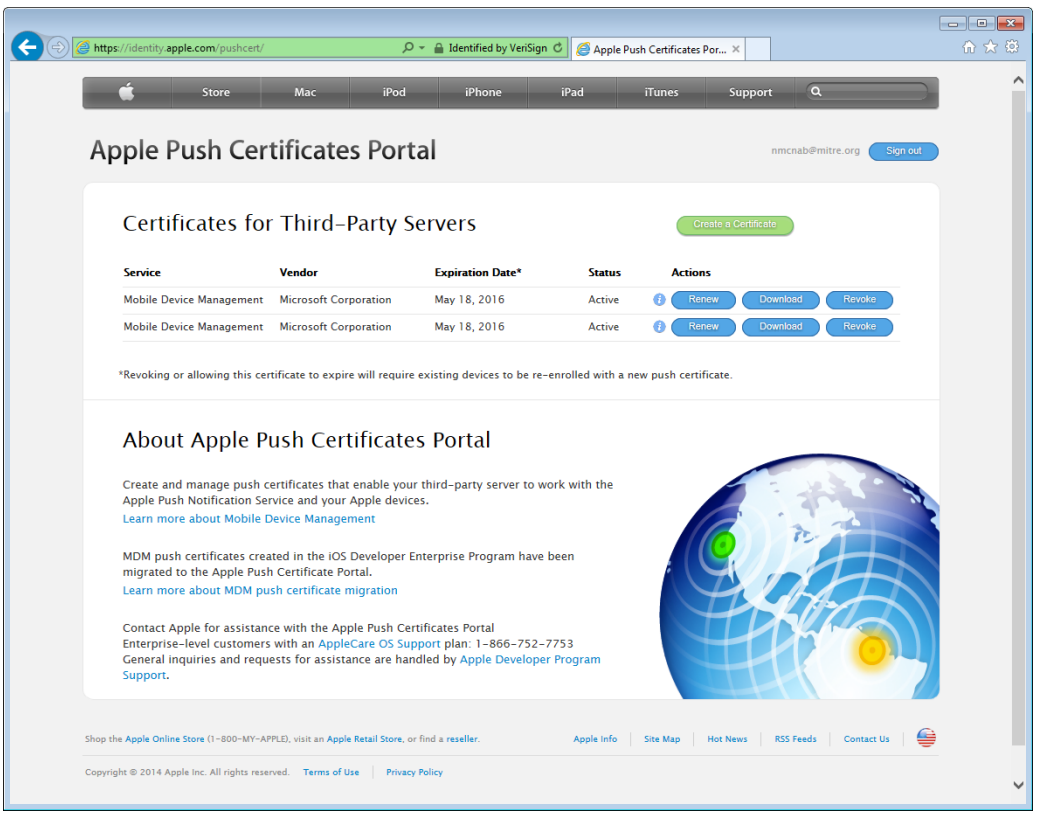


2. Save the CSR to local storage. You'll need this file for the next step.
3. Use a browser to visit https://identity.apple.com/pushcert/[8]. You will be prompted for your Apple Developer account credentials.

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

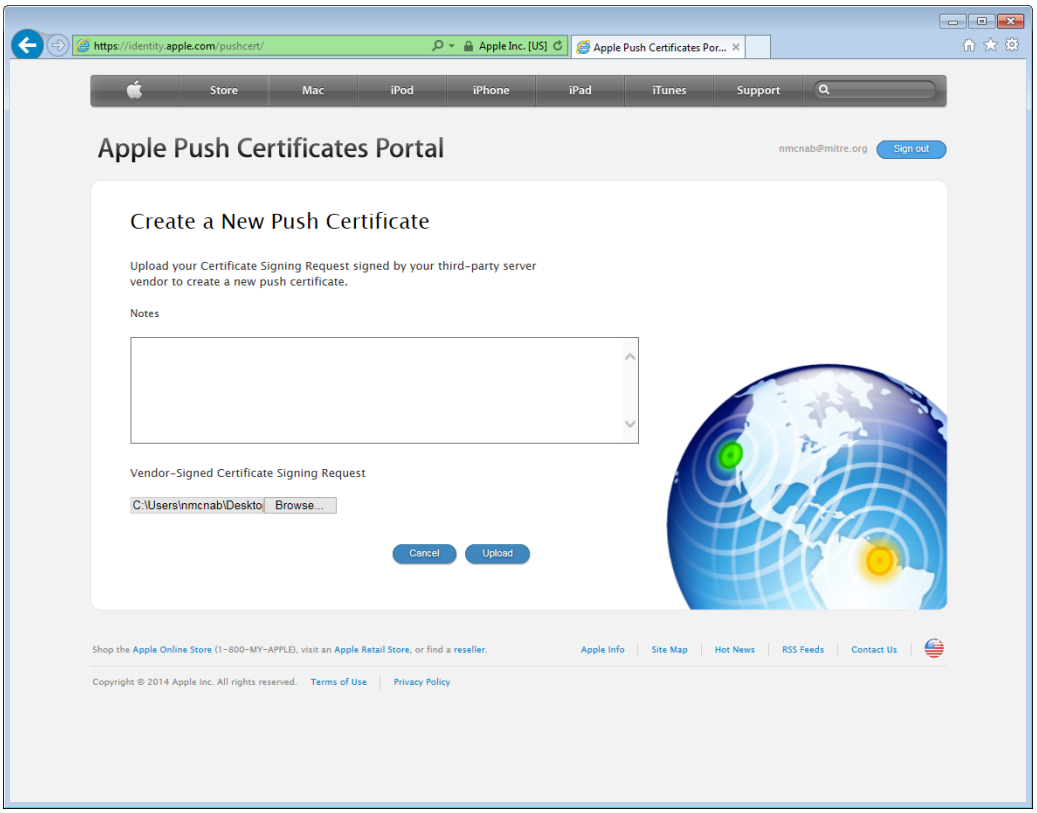
283

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



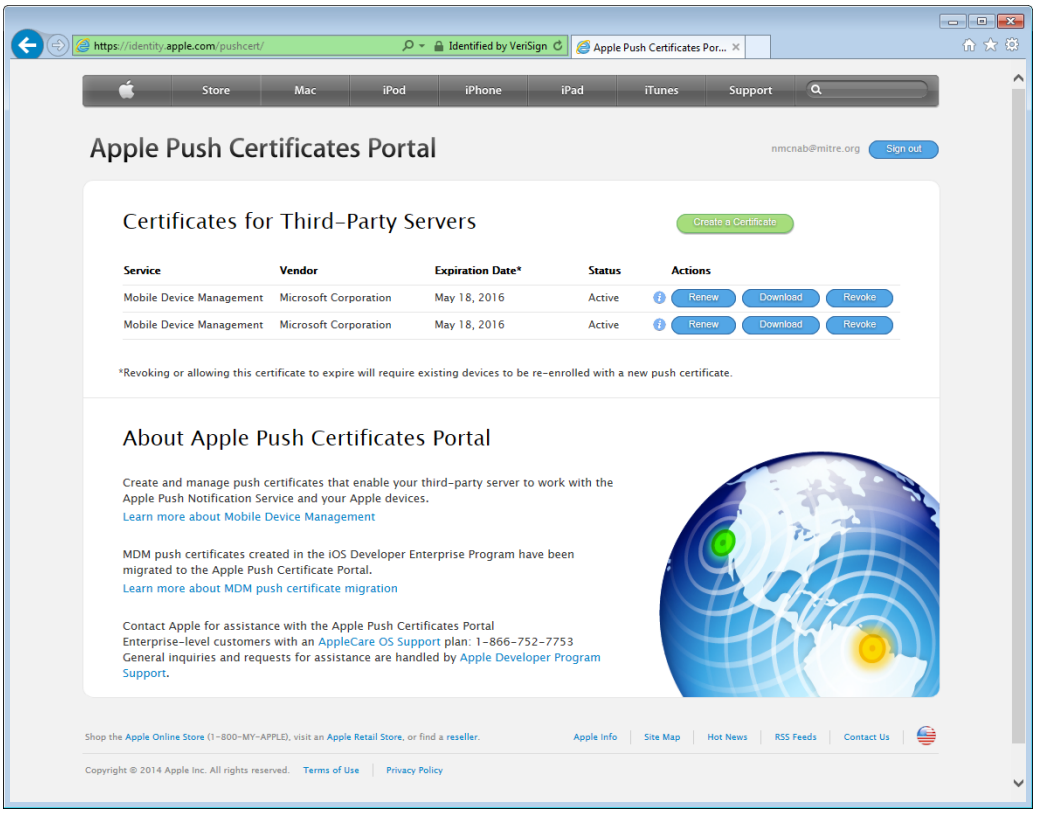
285

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

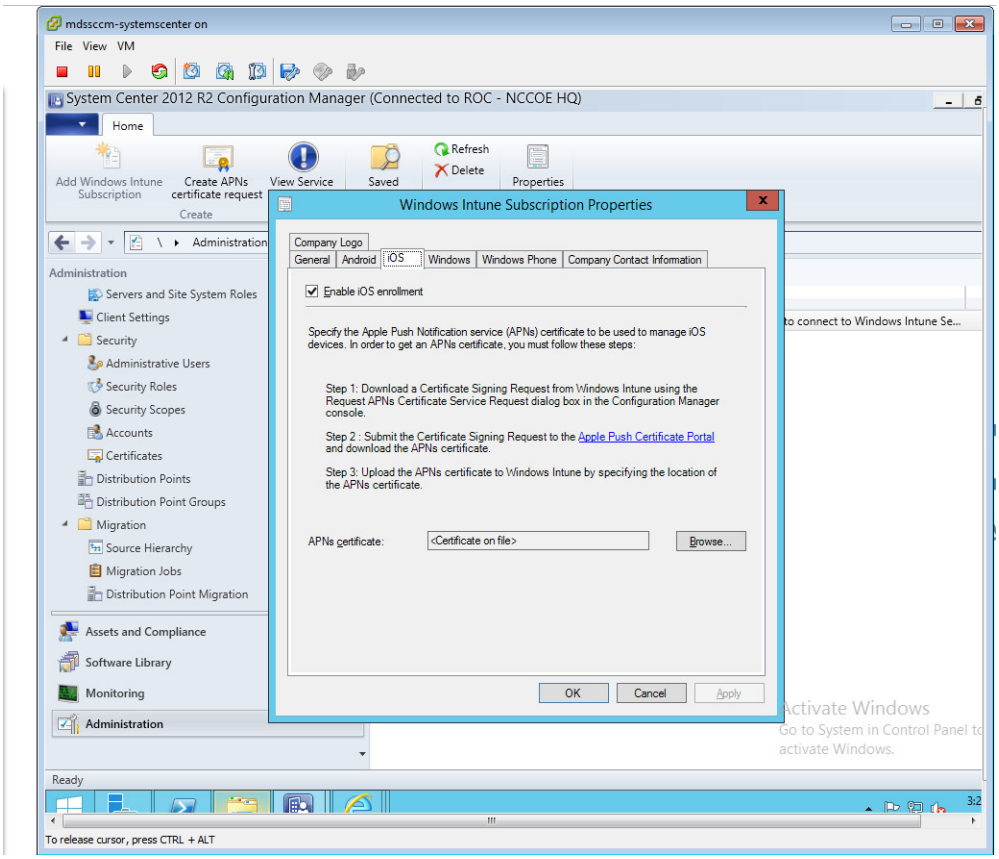


289

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.



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**.

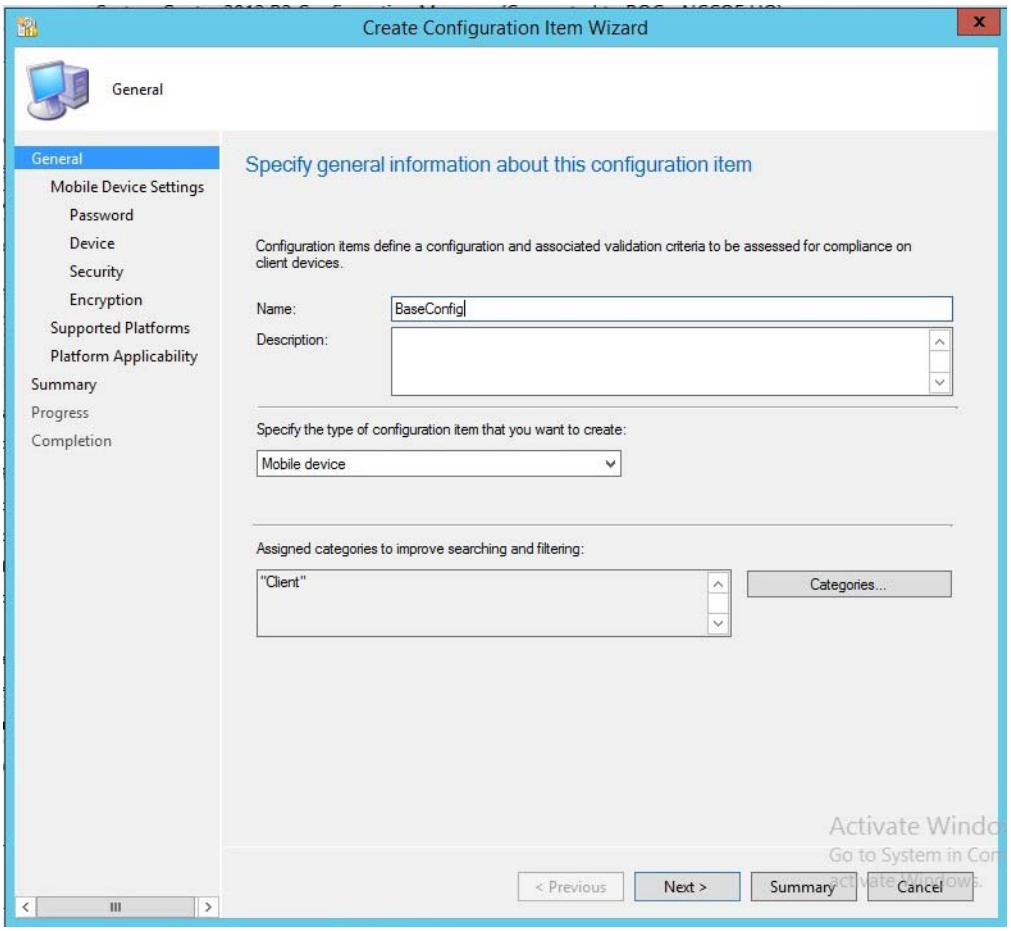


8. Check the box to **Enable iOS enrollment** and use the **Browse** button to import the PEM certificate you downloaded from Apple. Click **OK**.

3.2.5.4.4 Mobile Policy Creation

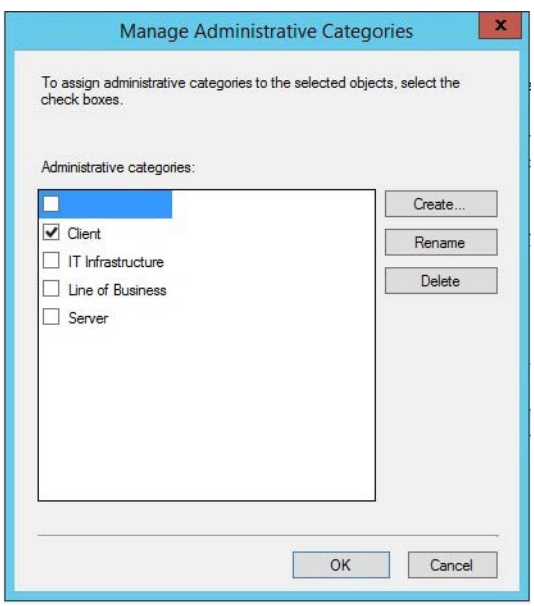
This section depicts the creation and deployment of a security policy for mobile devices in the building block test environment. The reader should note that not all options are available to every mobile operating system. Generally, iOS offers more fine-grained device management capabilities than Android;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

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



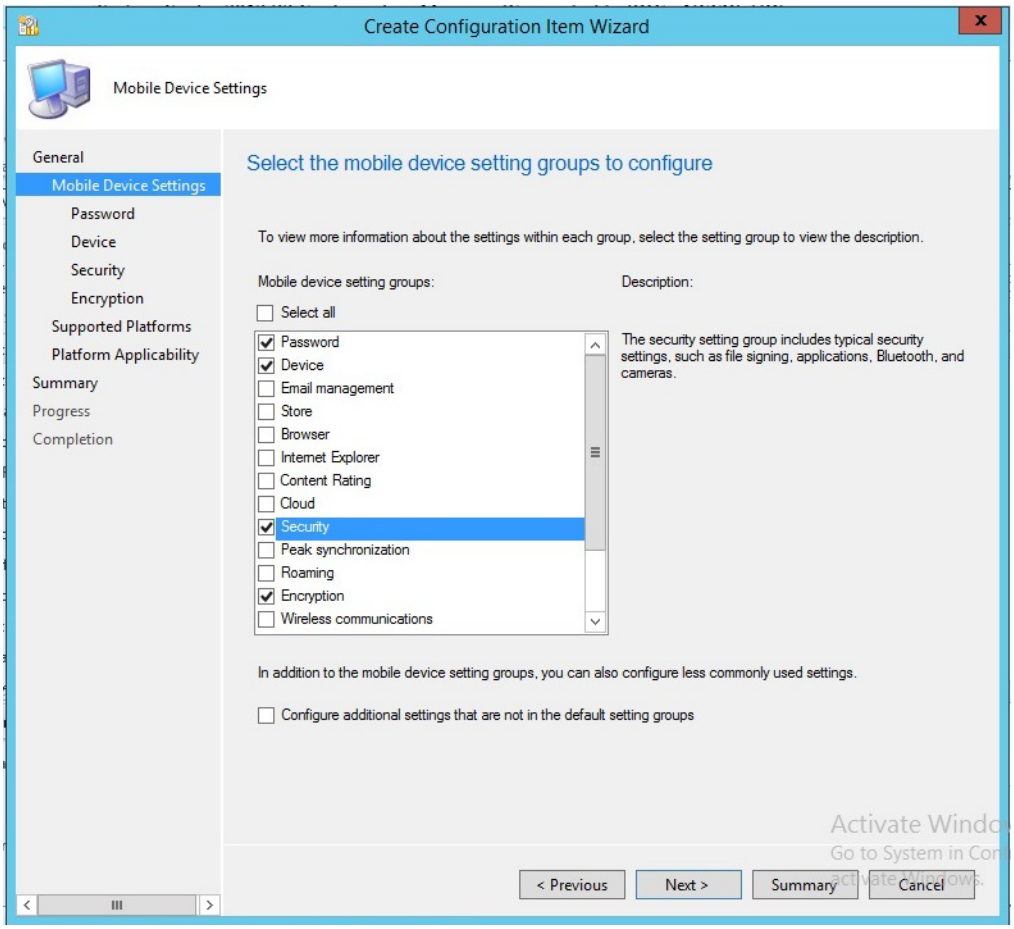
310

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



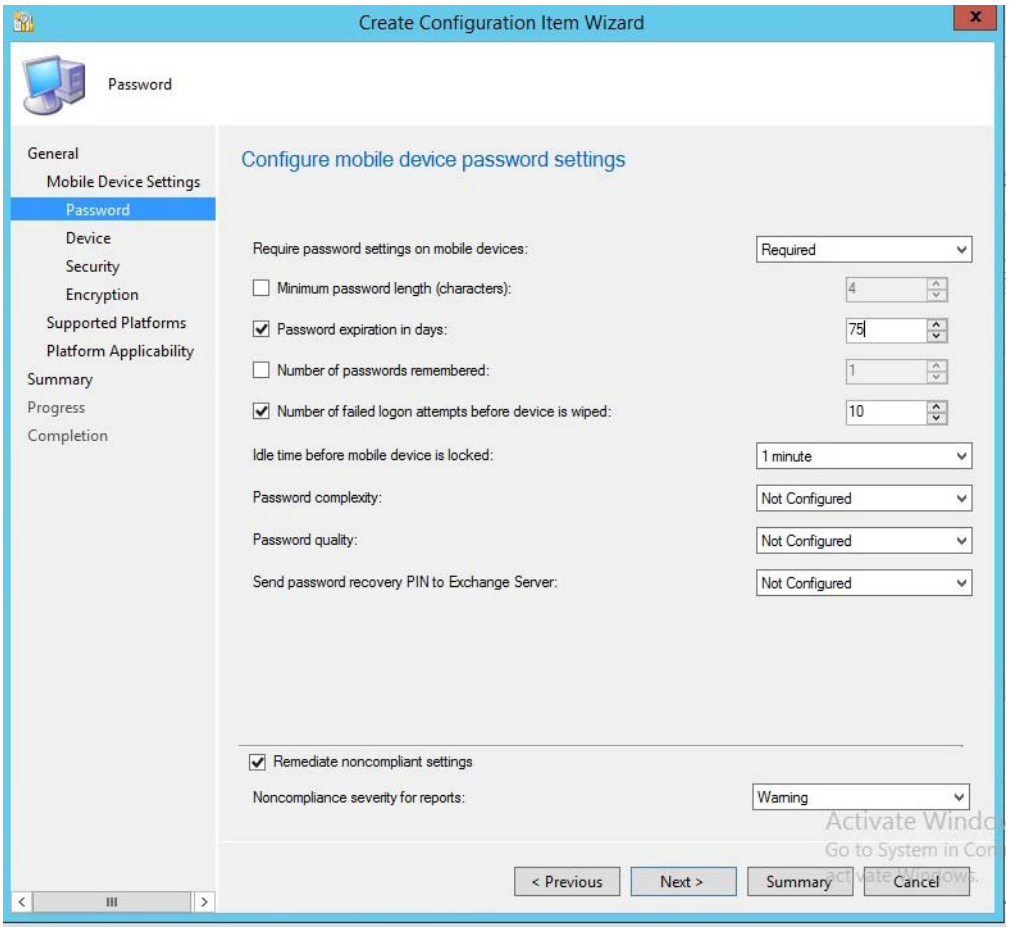
313

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

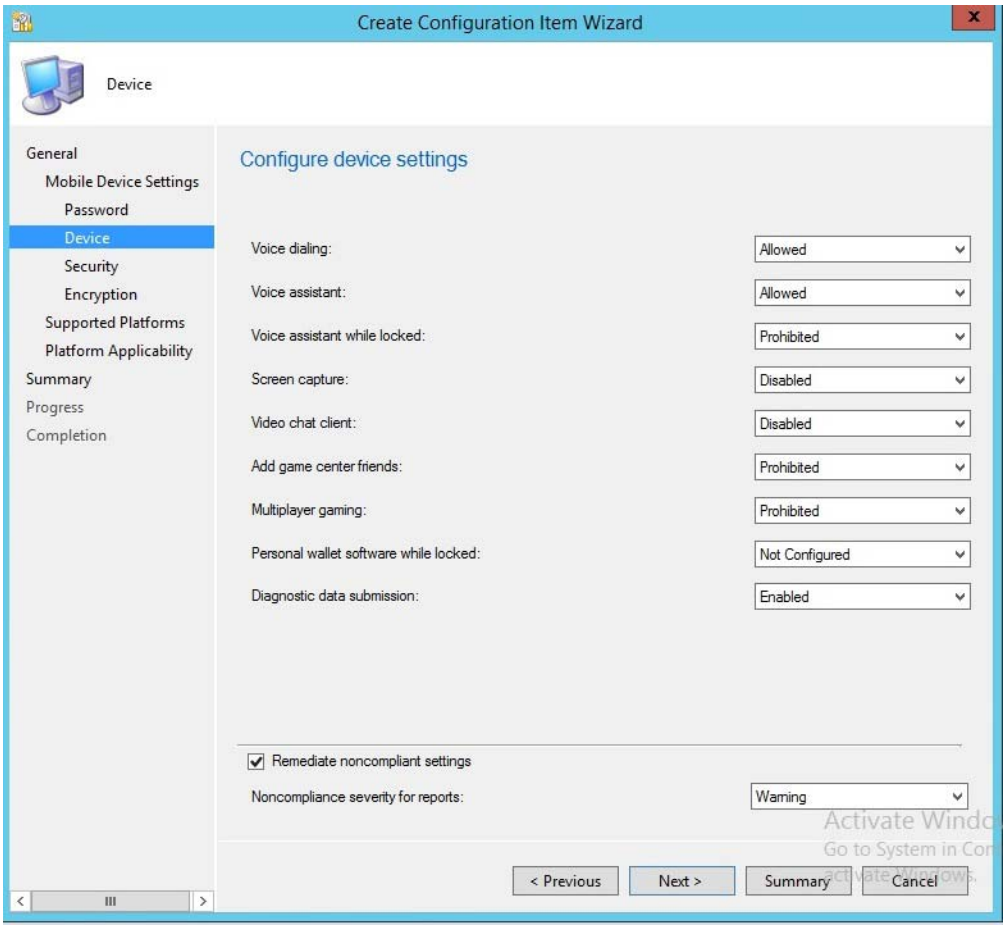


315

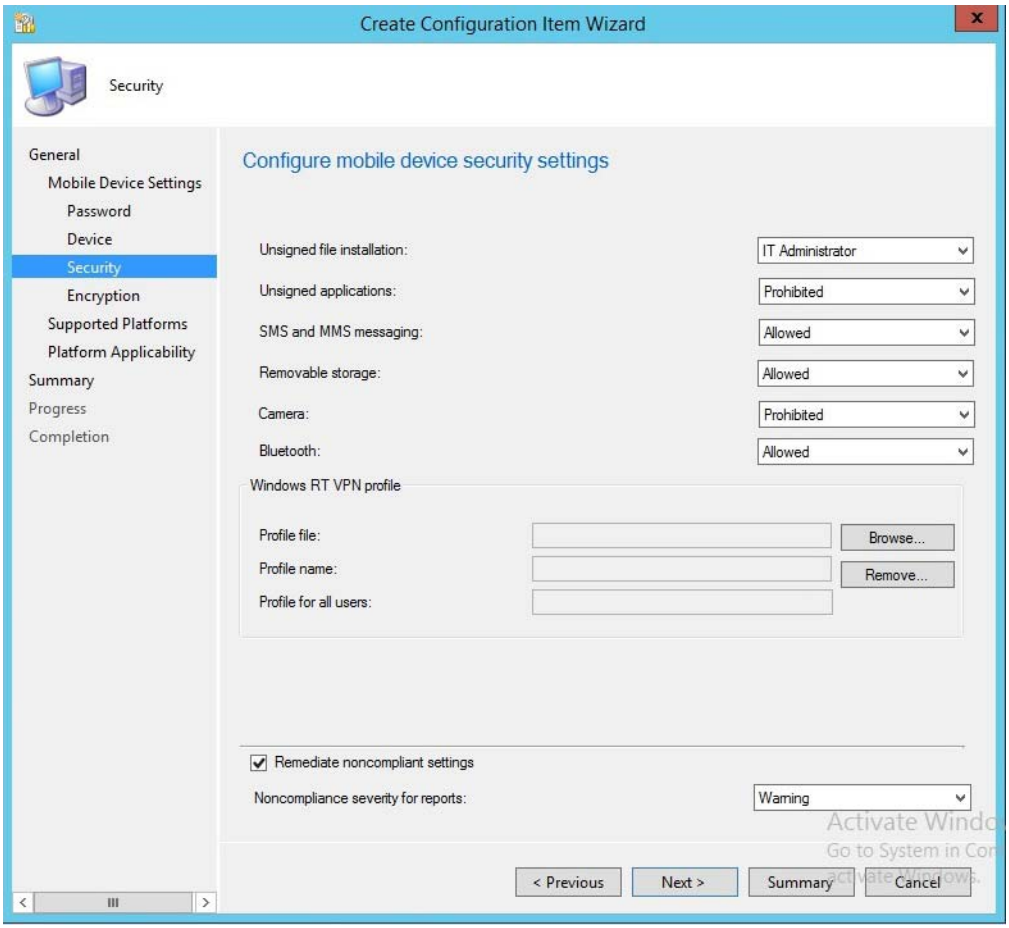
316 4. Select **Password**, **Device**, **Security** and **Encryption** setting groups. Click **Next**.



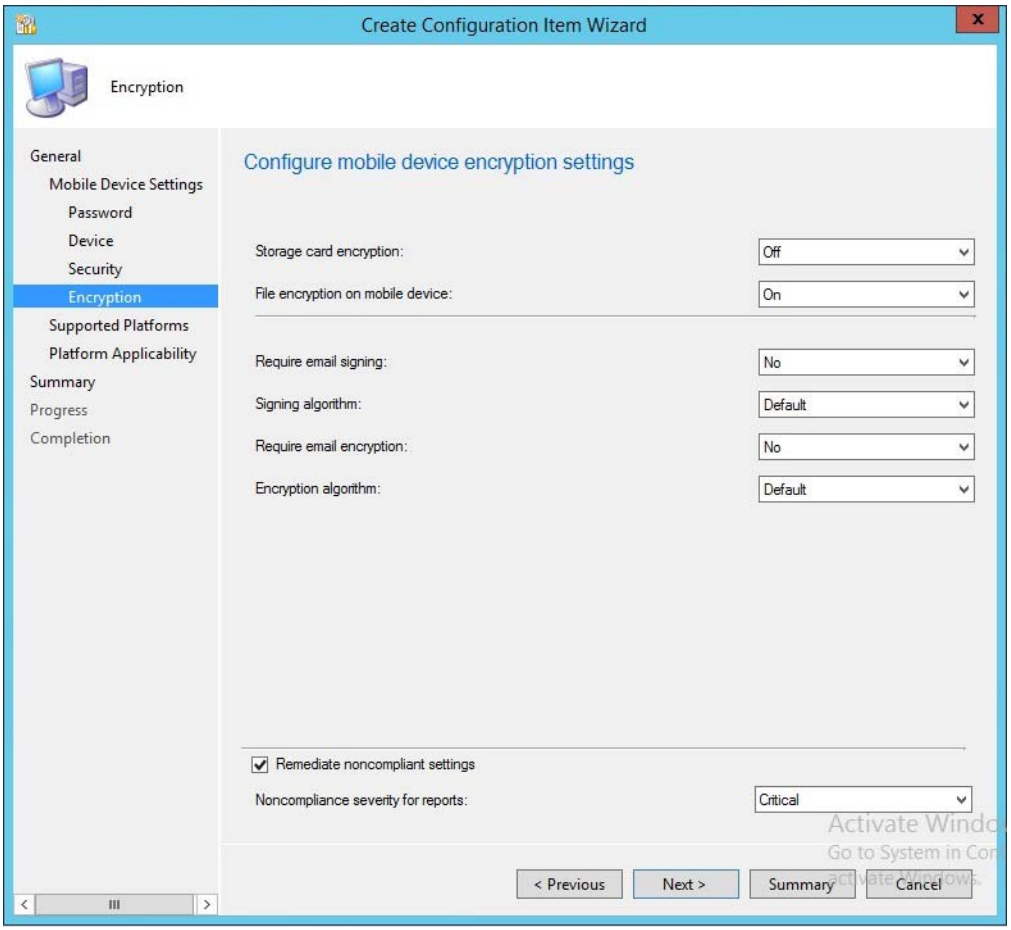
5. Configure the password requirements based on your local requirements.



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

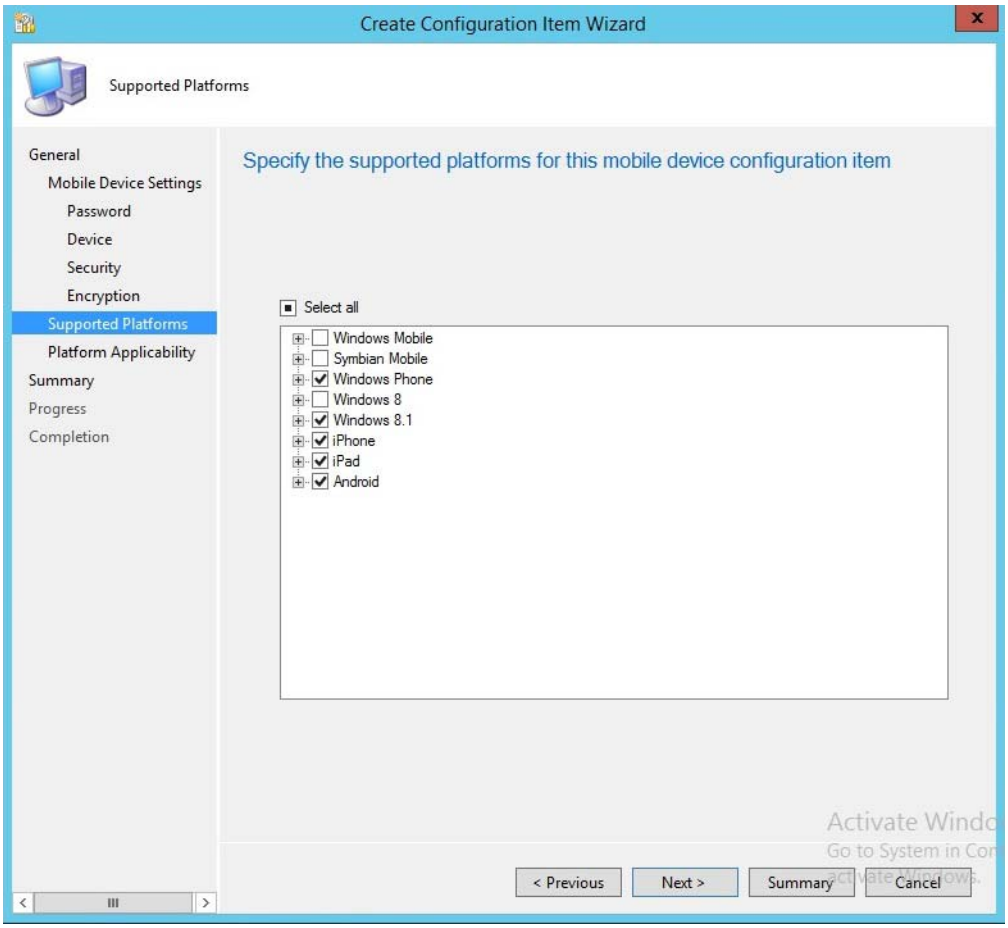


7. Configure the security settings based on your local requirements.



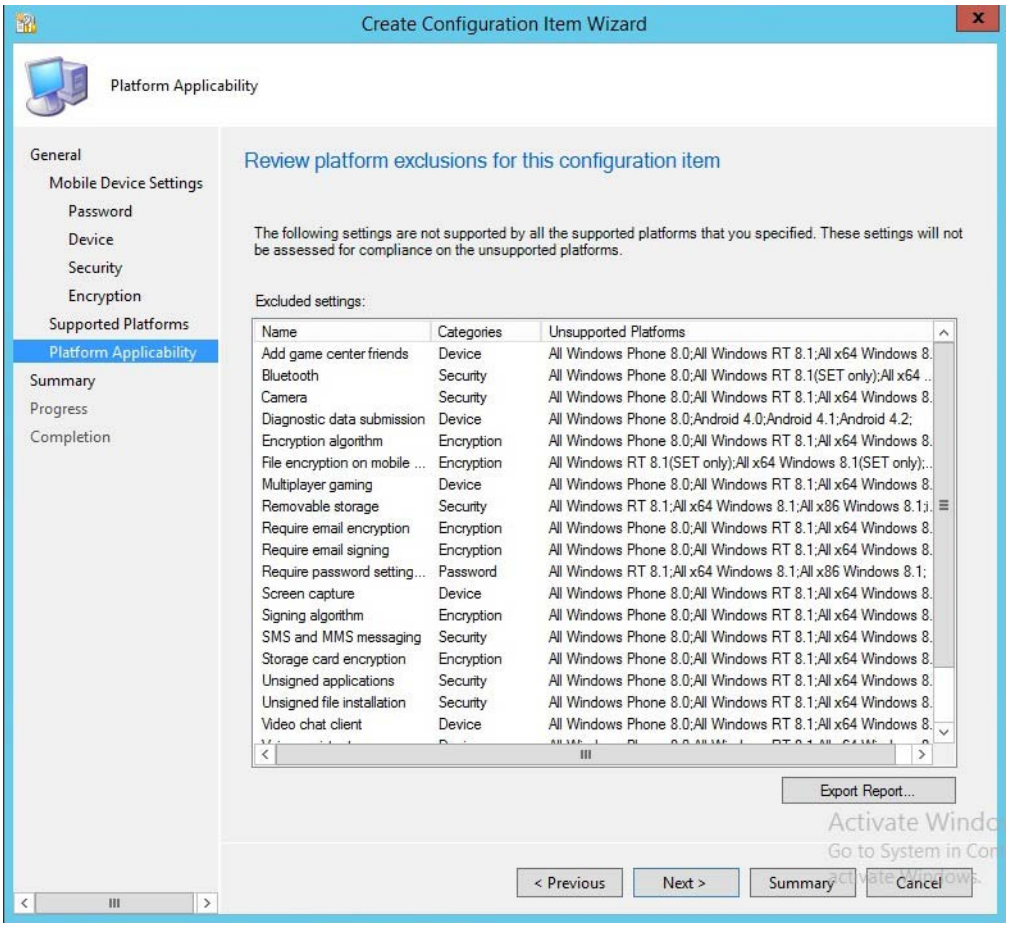
323

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

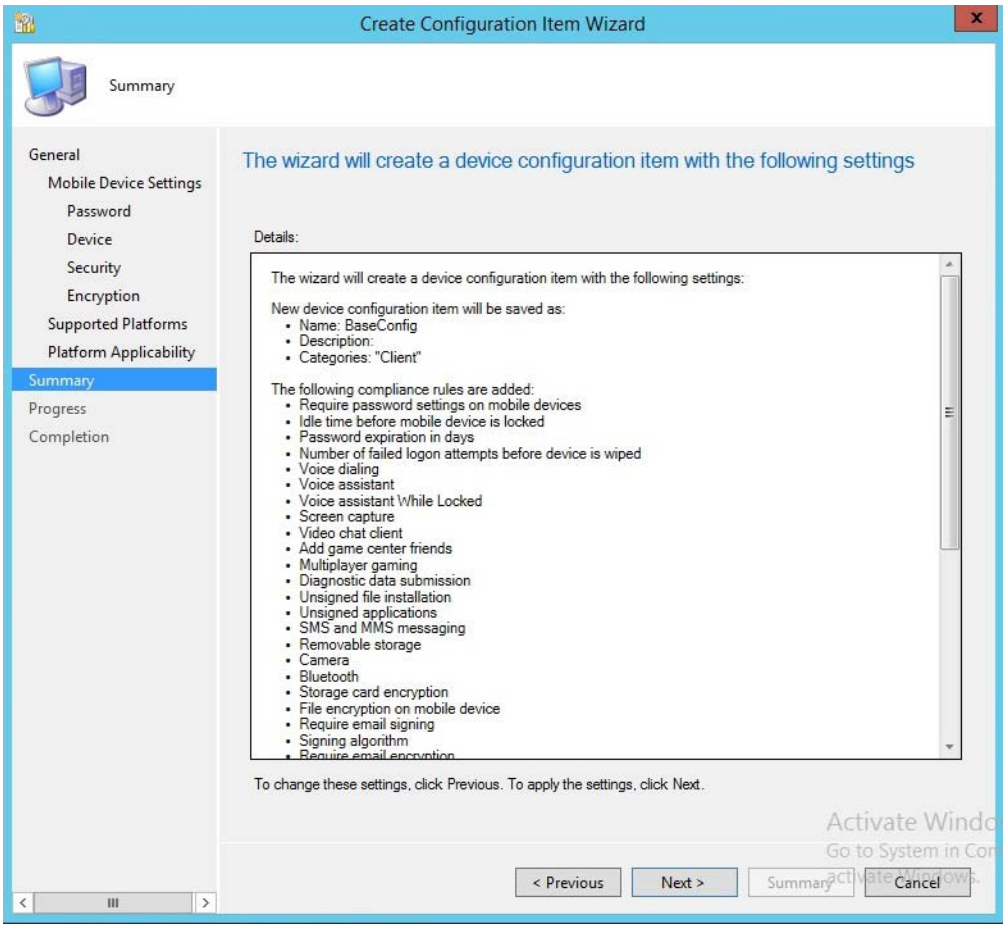


325

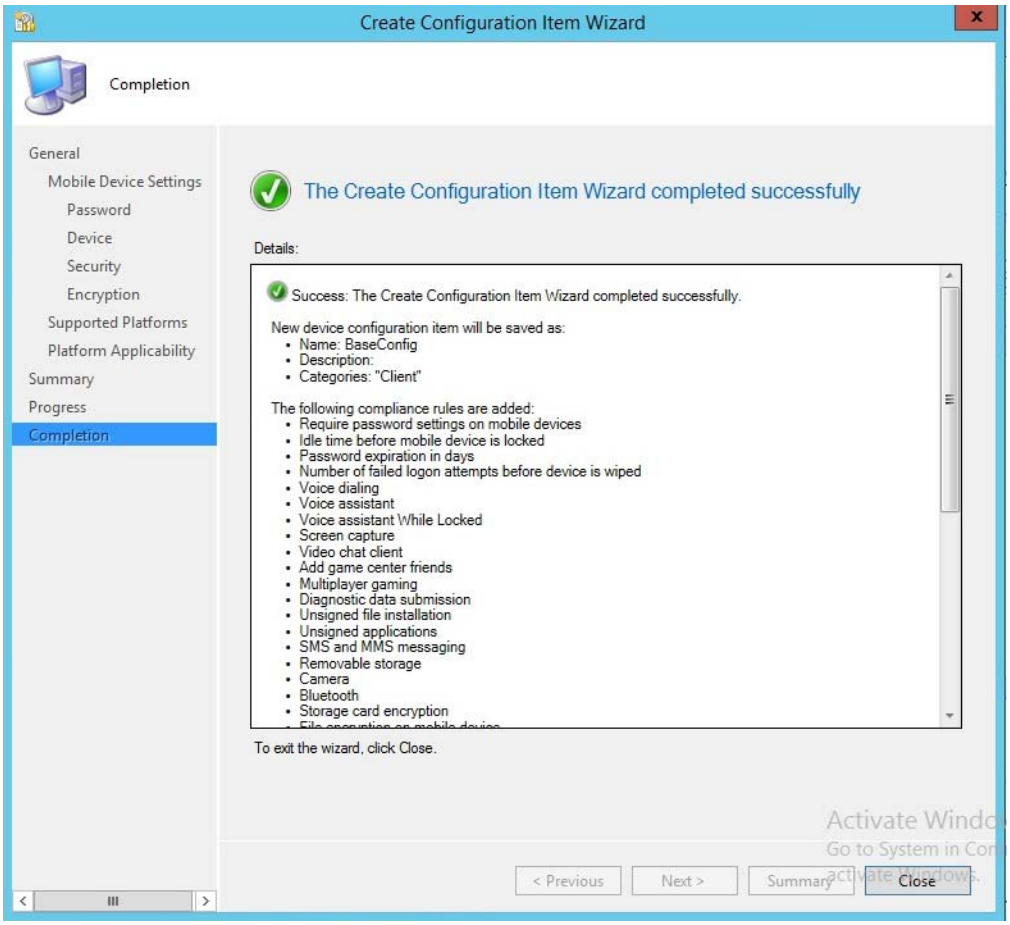
326 9. Select the mobile platforms you wish to support. Click **Next**.



10. Click **Next**.

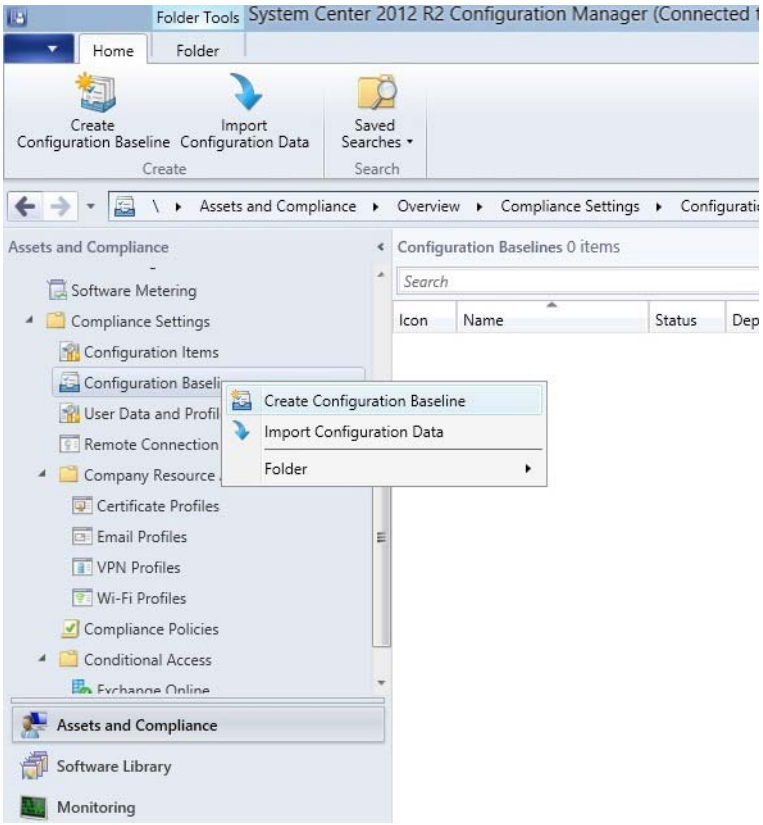


11. Click **Next**.



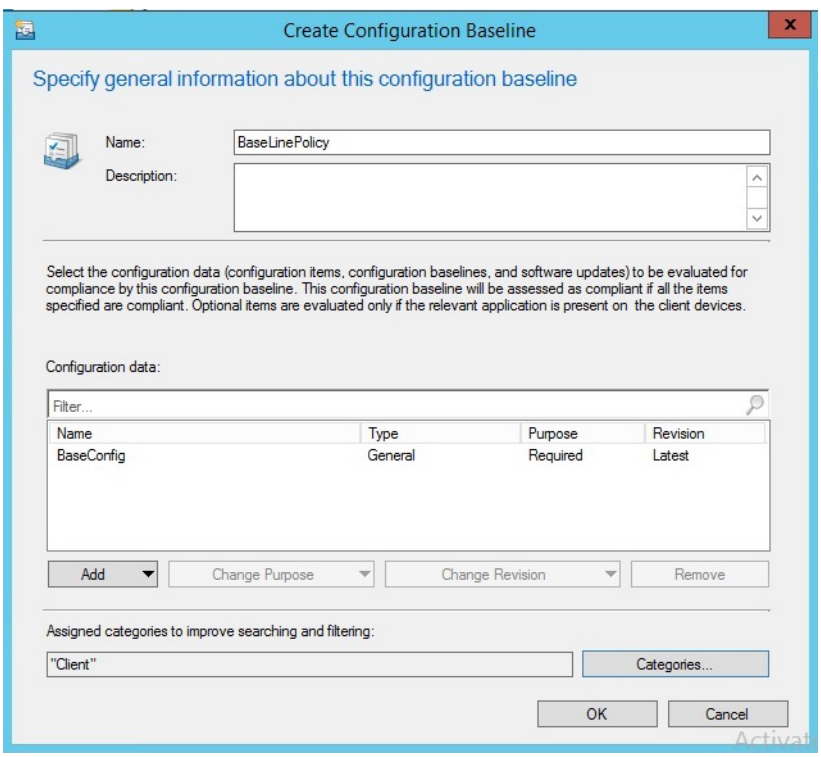
331

332 12. Click **Close**.



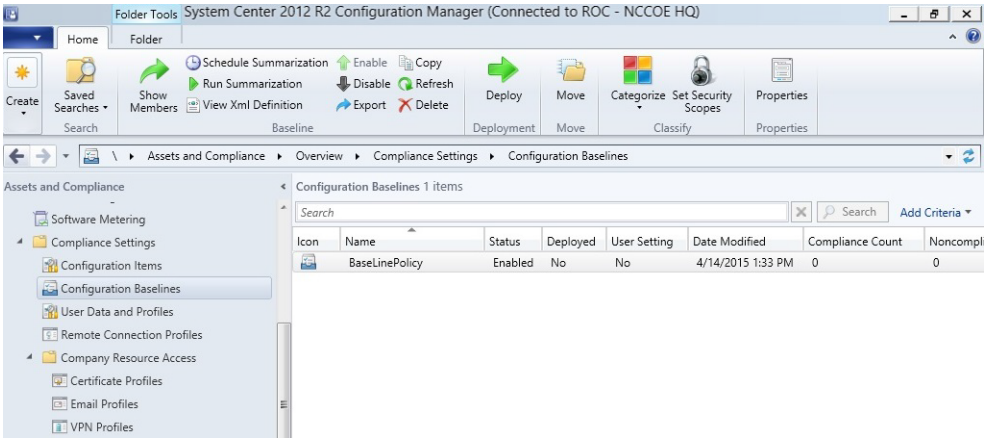
333

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



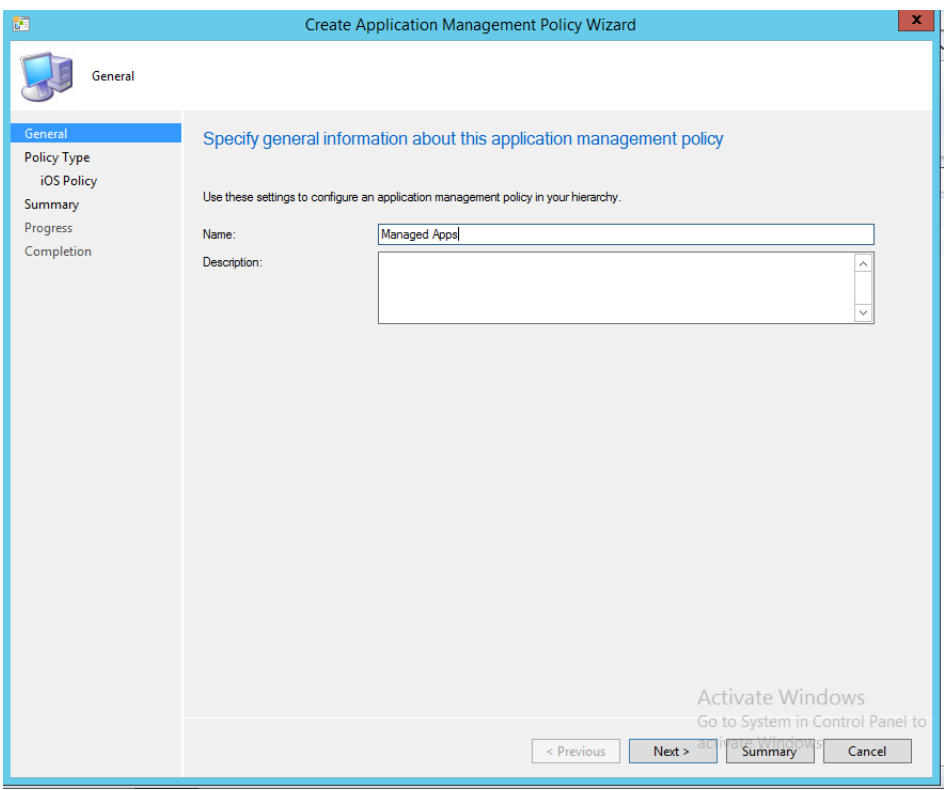
336

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

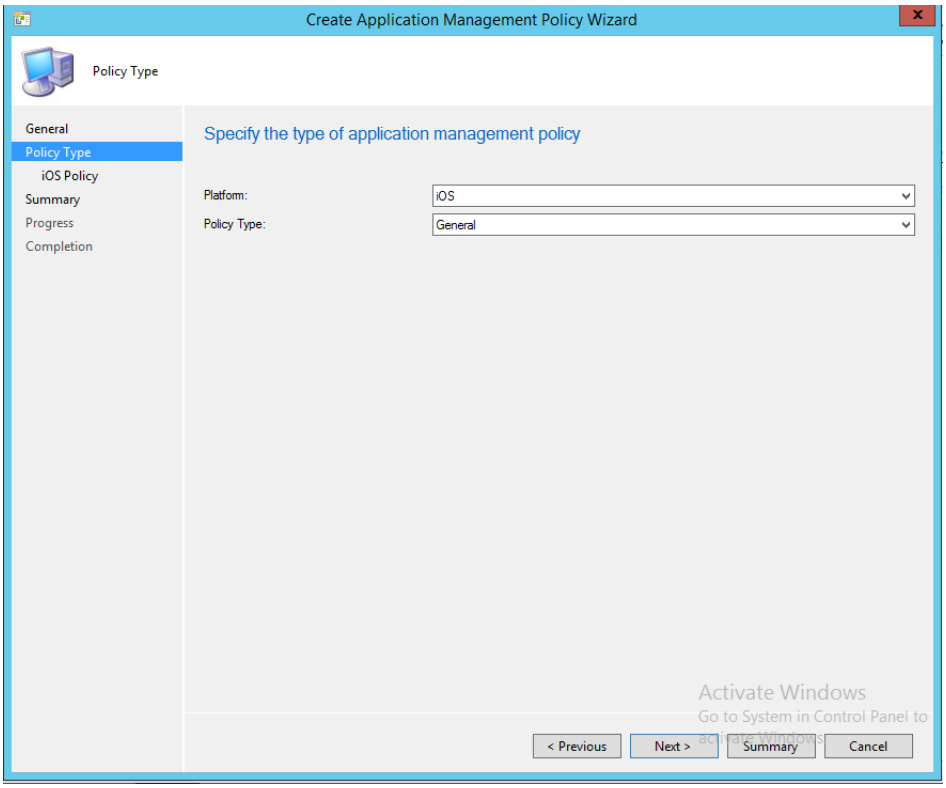


3.2.5.4.5 Create Mobile Application Policy

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

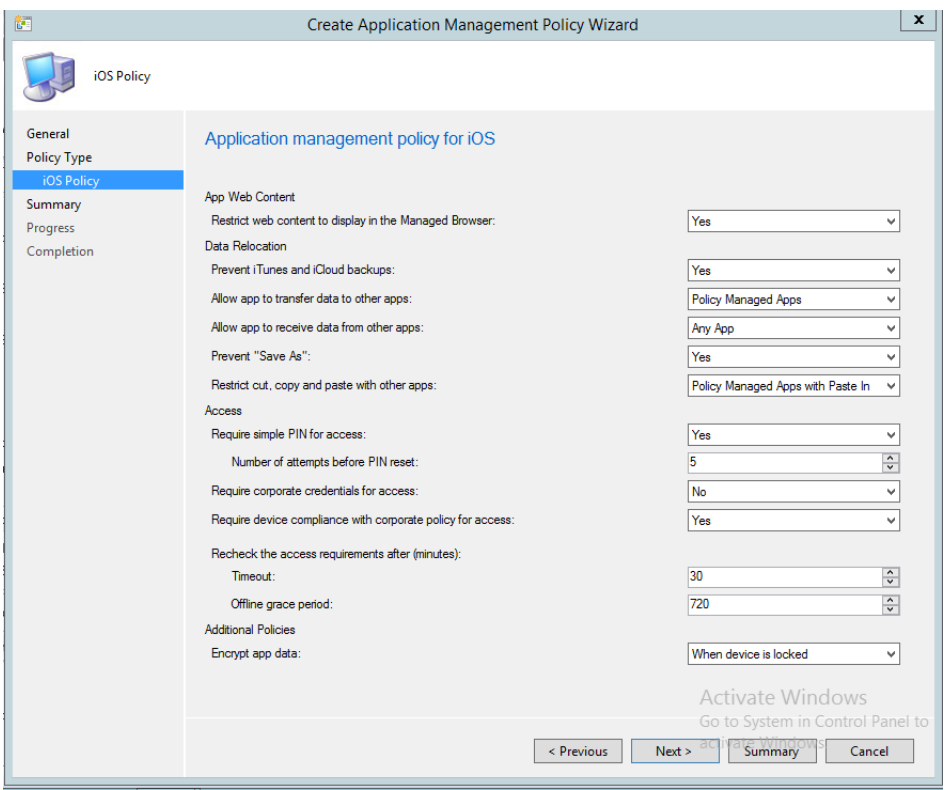


1. To start the wizard, navigate to **Under Software Library > Application Management > Application Management Polices: Create Policy** in the SCCM console. Click **Next**.



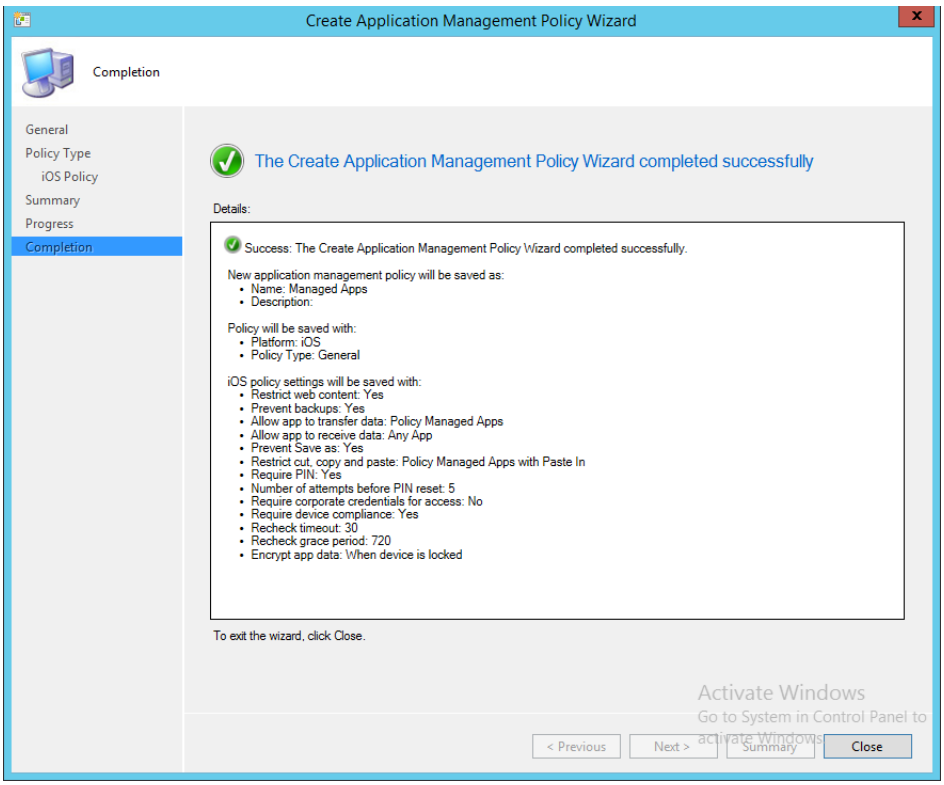
349

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



352

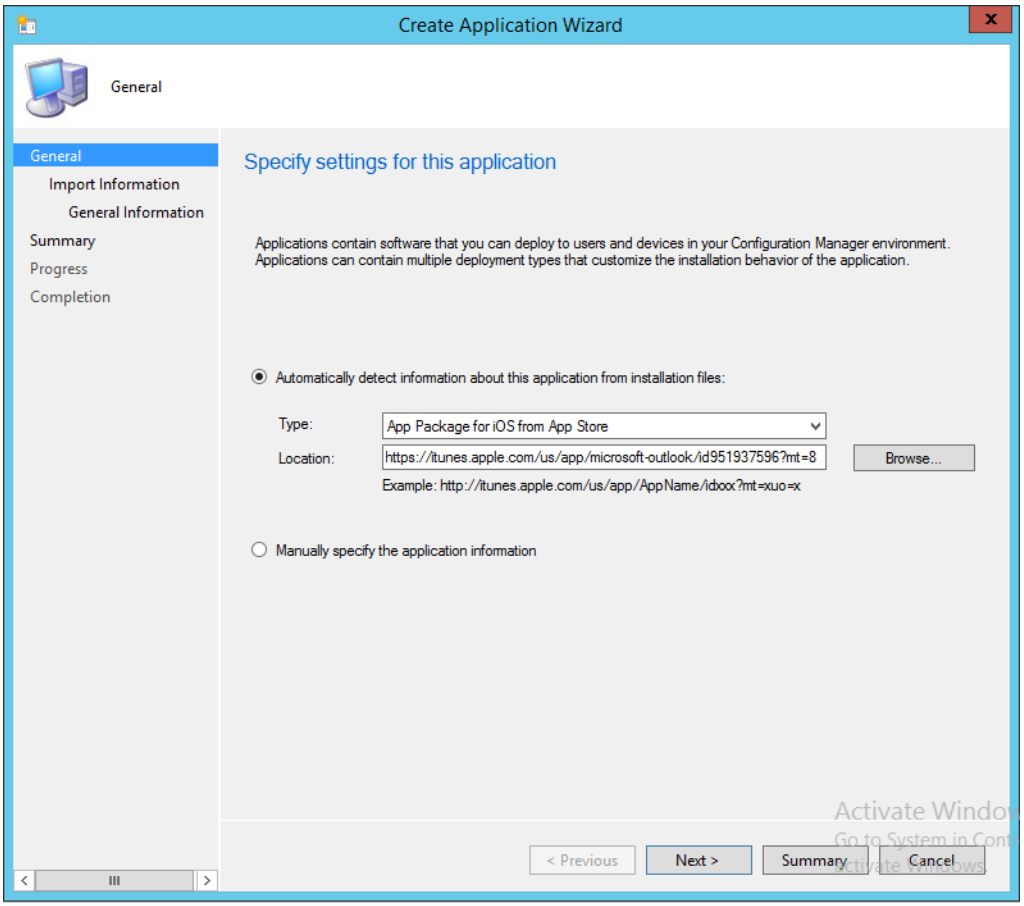
353 3. Set the specifics of the policy as pictured. Click **Next**.



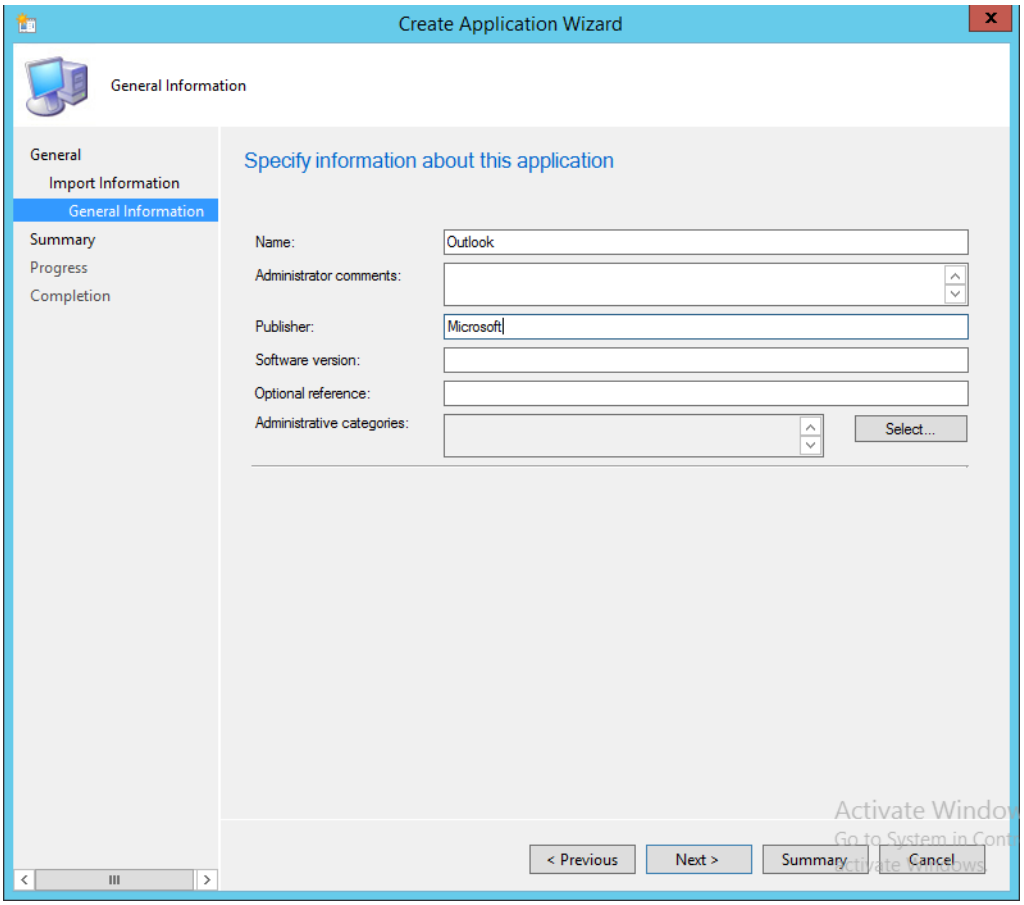
354

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

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

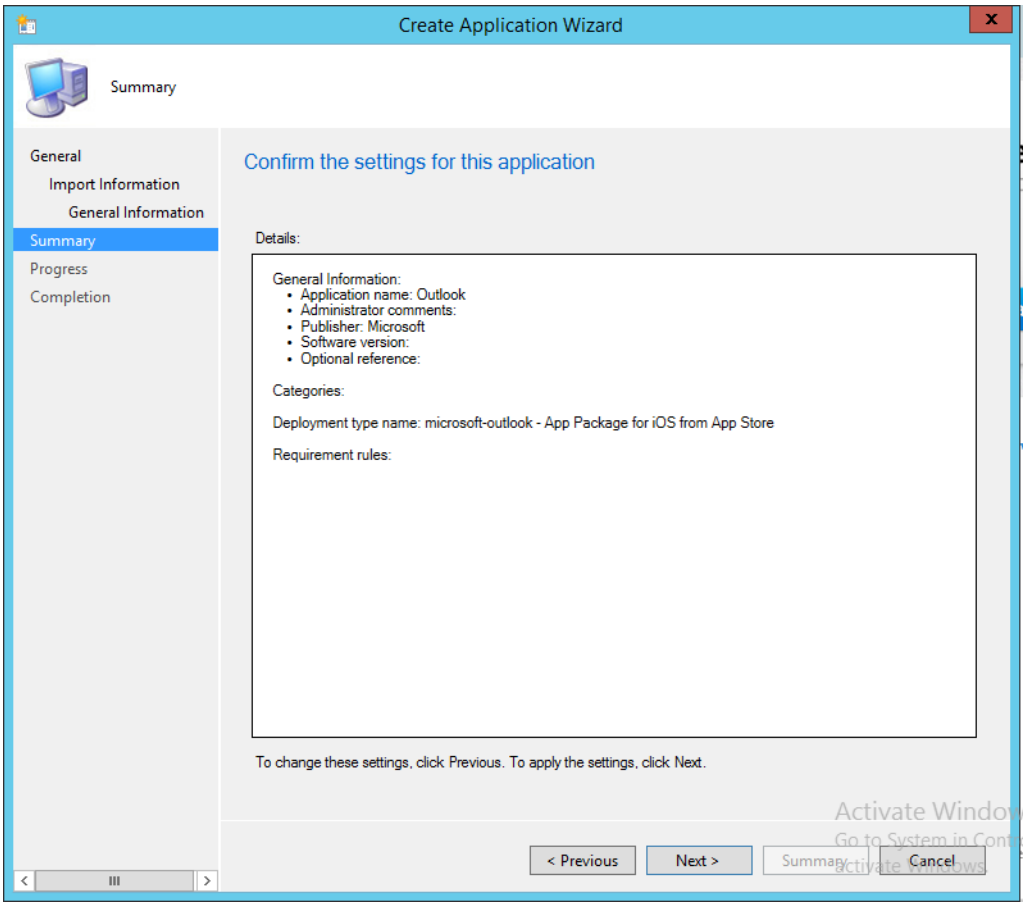


1. Navigate to **Software Library > Applications** and **Create Application**. Enter the URL for the application you wish to link to in the Location field. Search for the Outlook application using a search engine and copy the link to obtain the URL.

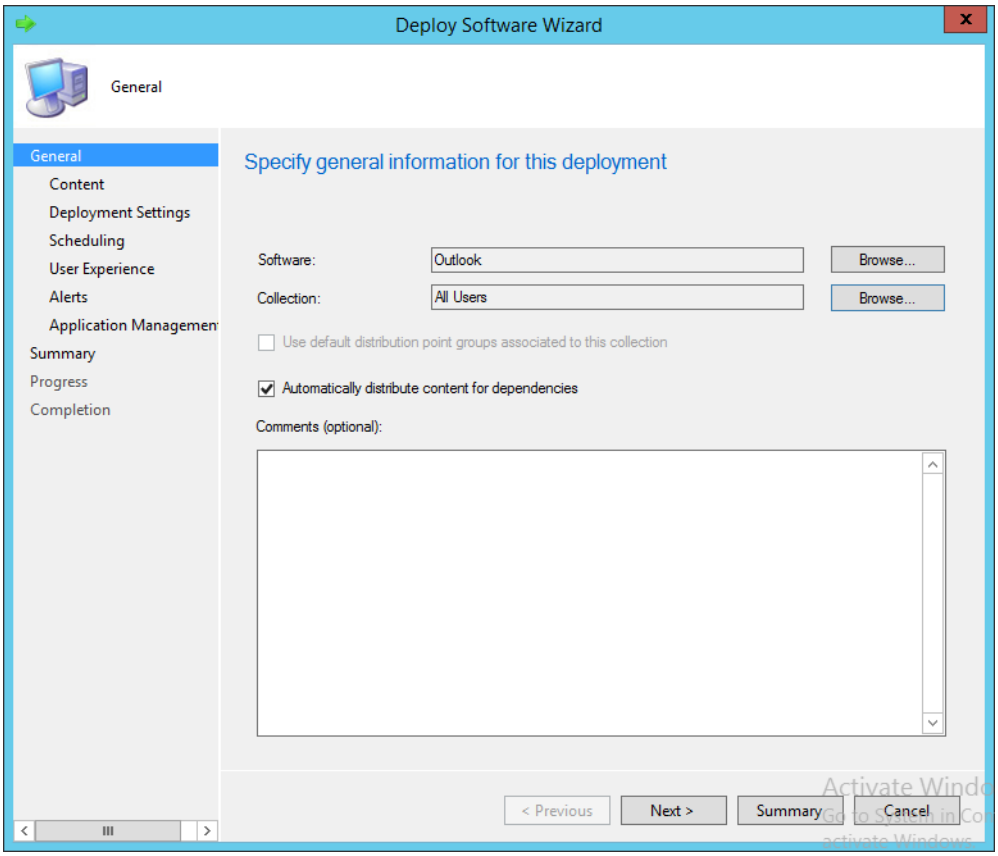


363

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

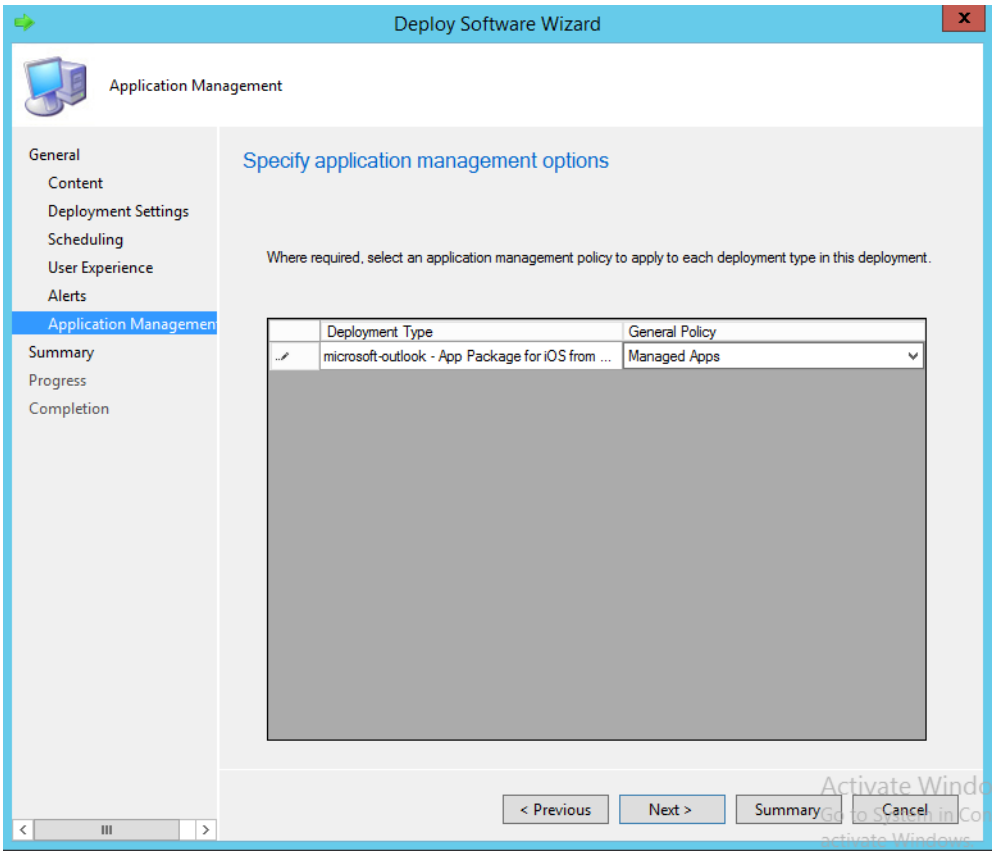


3. Click **Next** to confirm the settings.



367

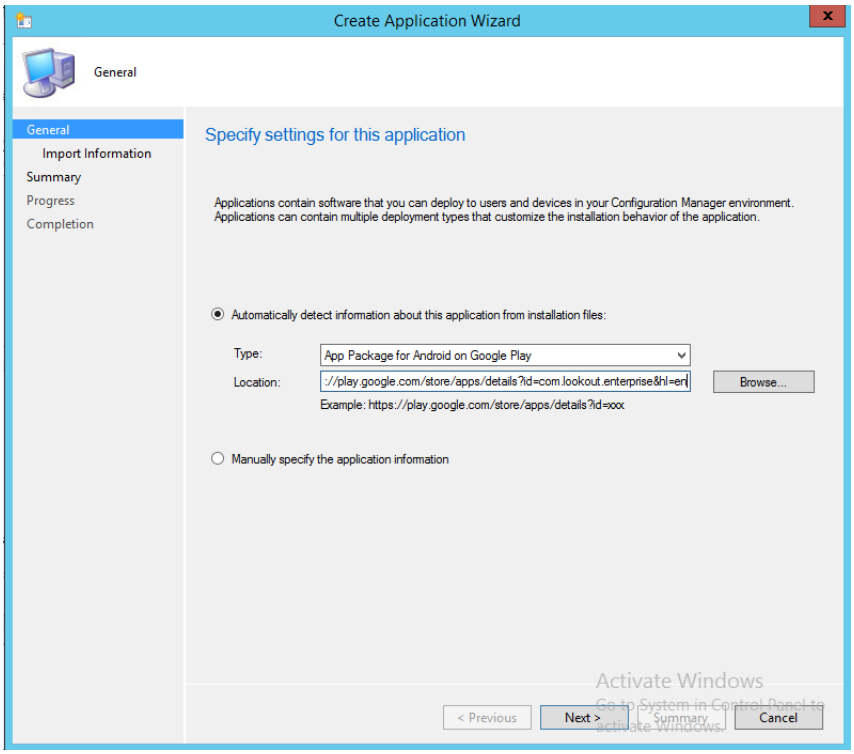
368 4. **Important**: Deploy the application to a user collection instead of a device collection.



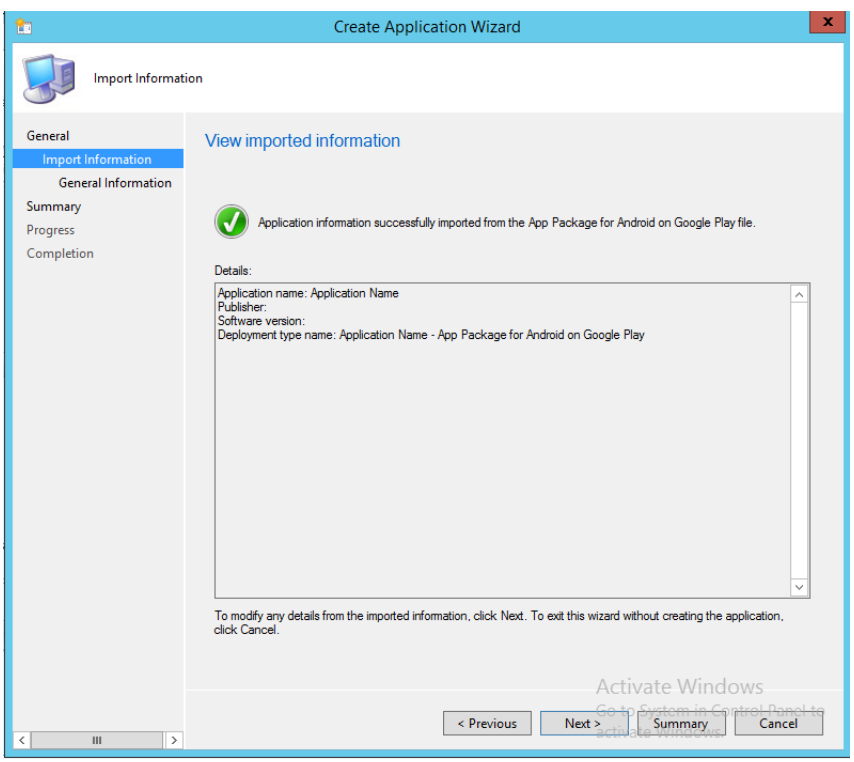
5. After setting the general settings for deploying the application, you will get a chance to link an application profile.

3.2.5.5 Configure SCCM with Lookout Application

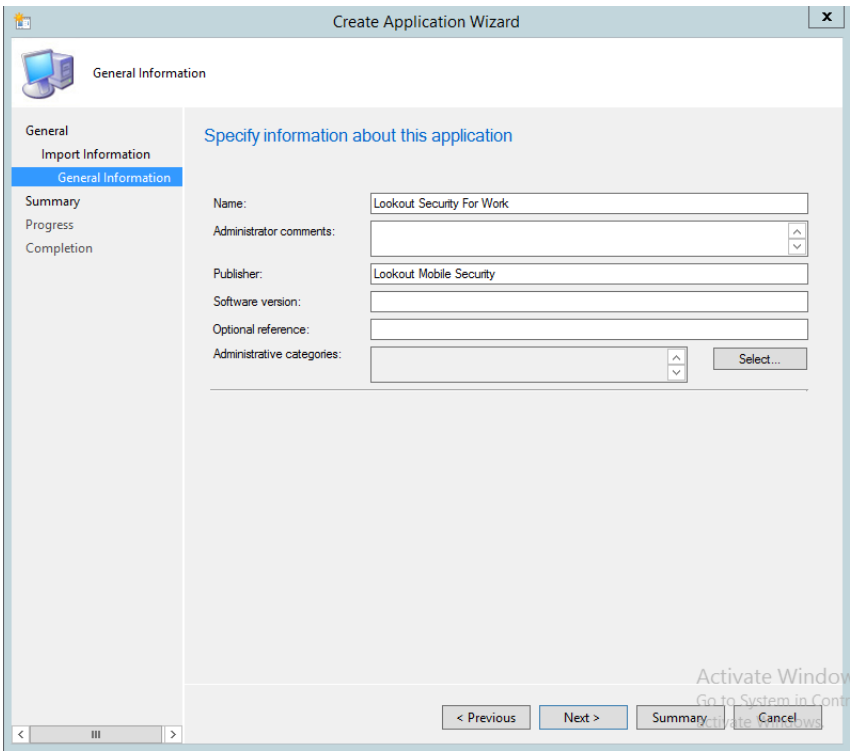
This section describes the integration of the Lookout mobile application with SCCM. When completed, the mobile device user will receive a link to download the Lookout application after enrollment with the MDM. The link URL will vary based on the mobile platform. Android users will be directed to the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



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

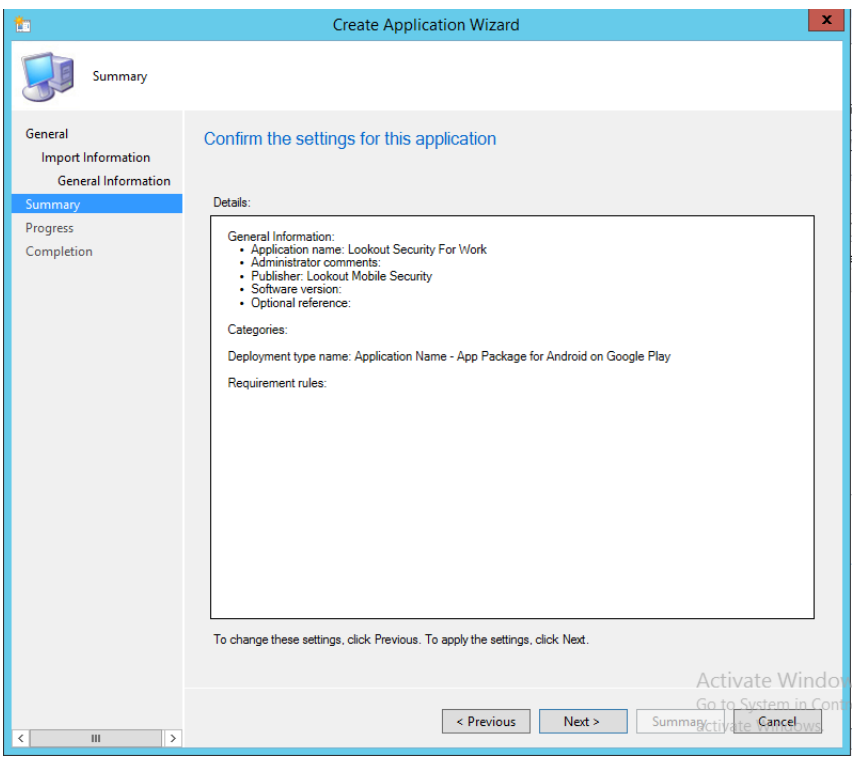


384 2. Click **Next**.



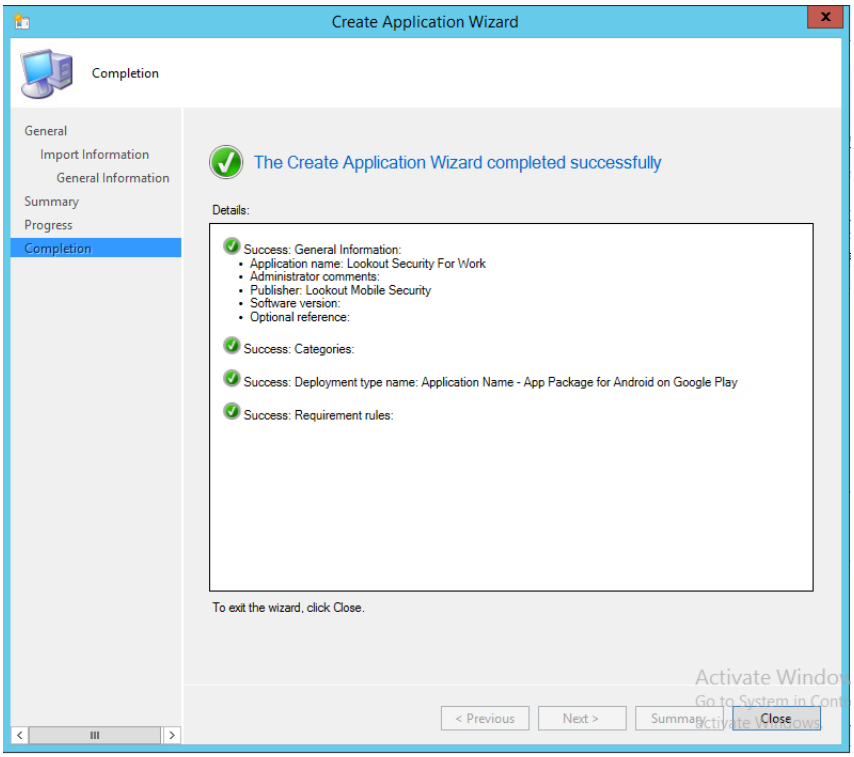
385

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



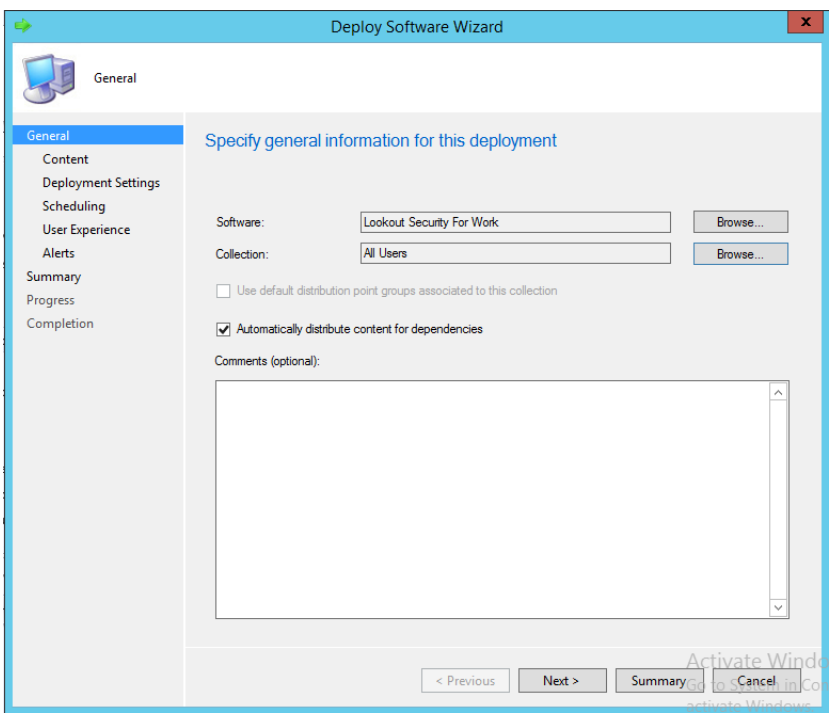
387

388 4. Click **Next**.



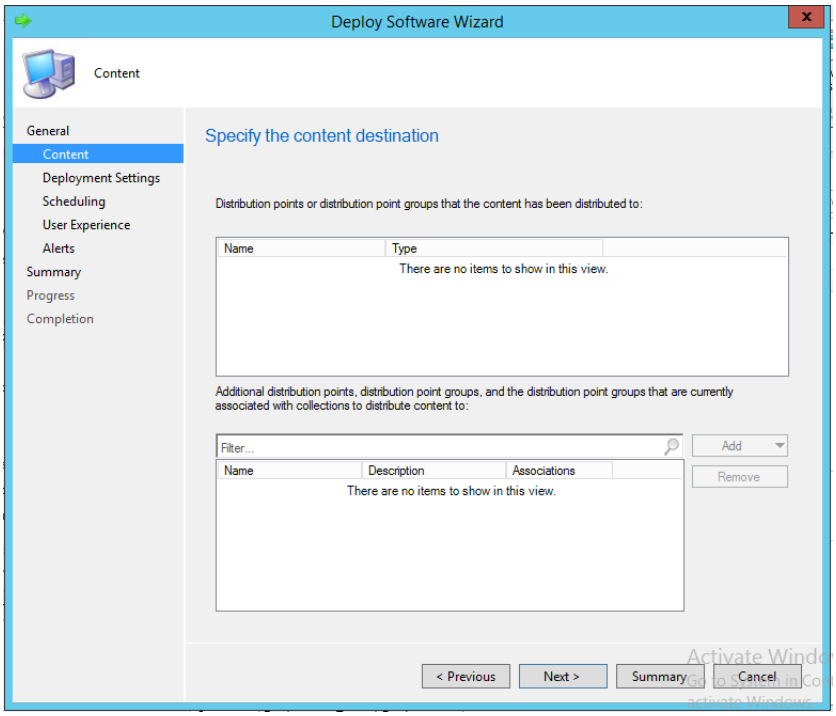
389

390 5. Click **Close**.



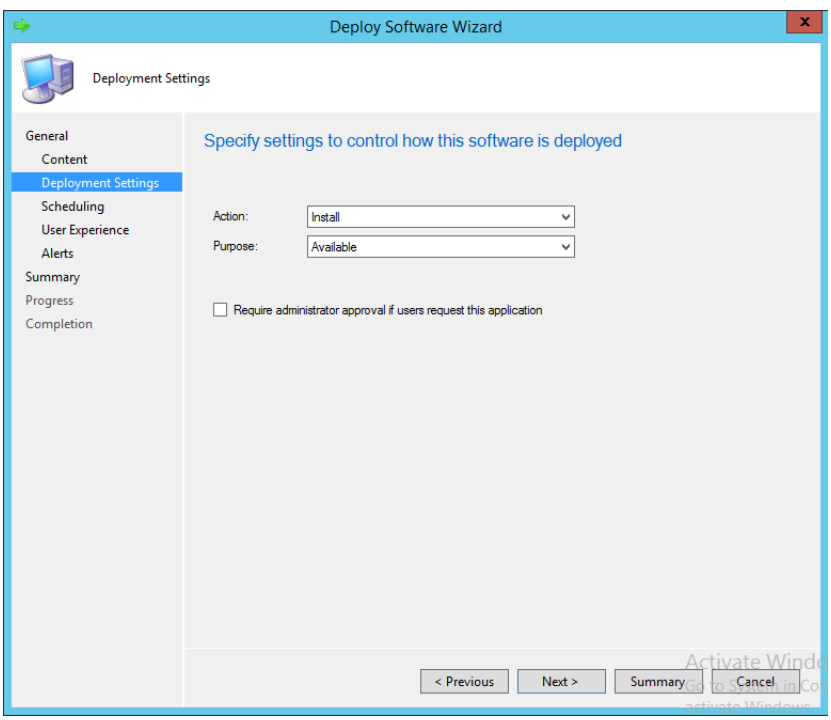
391

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



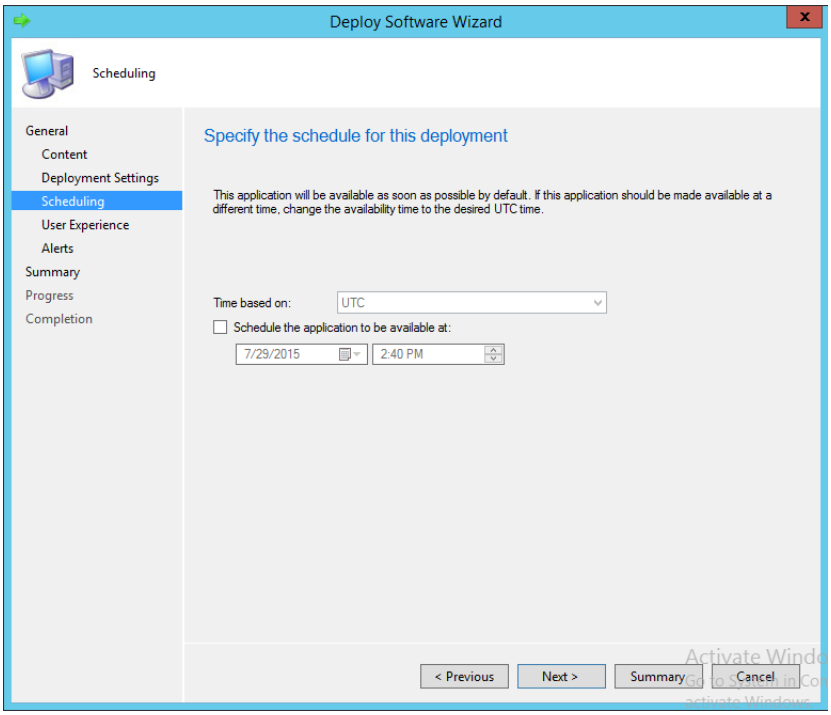
394

395 7. Click **Next**.



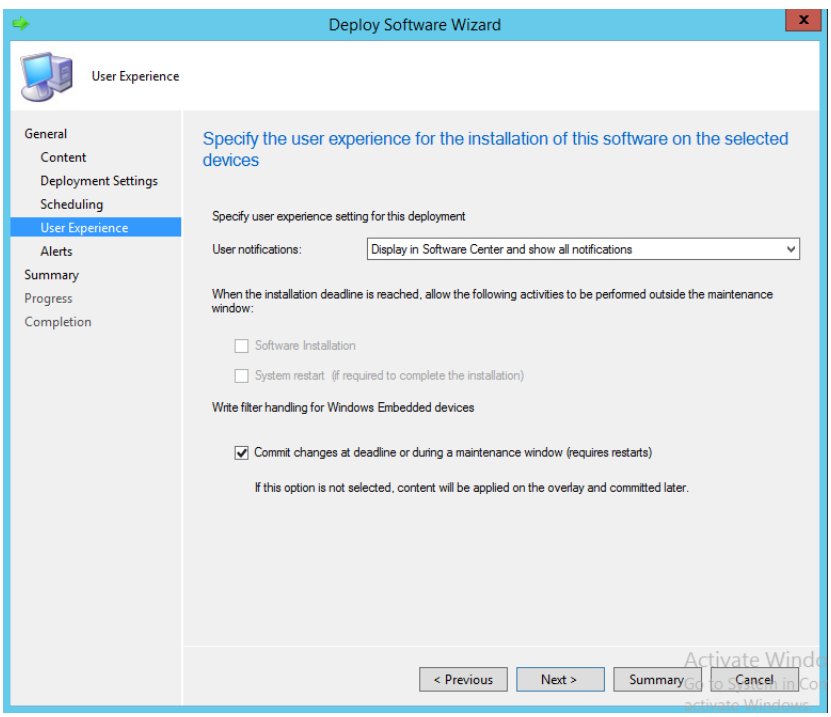
396

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



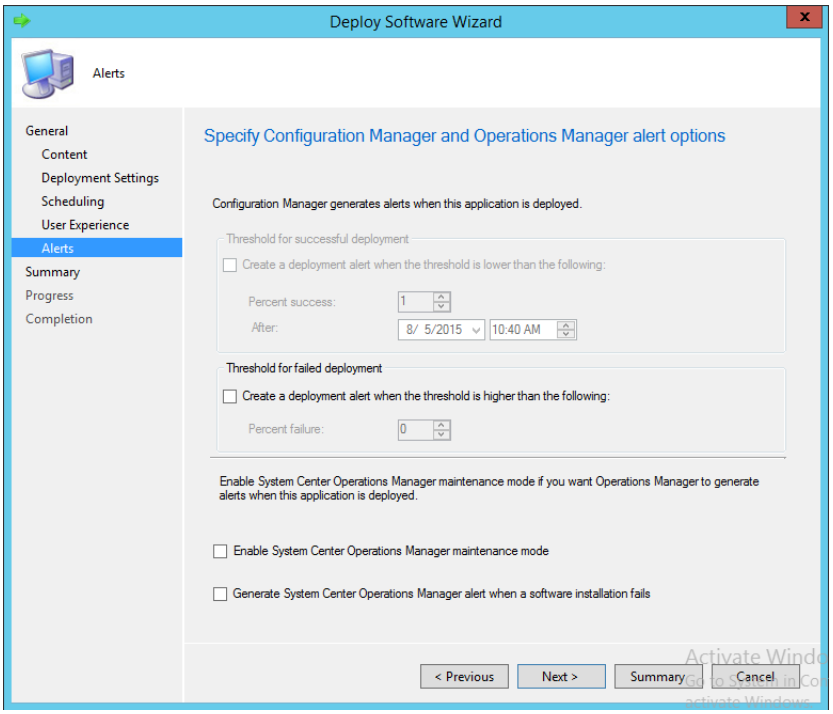
399

400 9. Click **Next**.



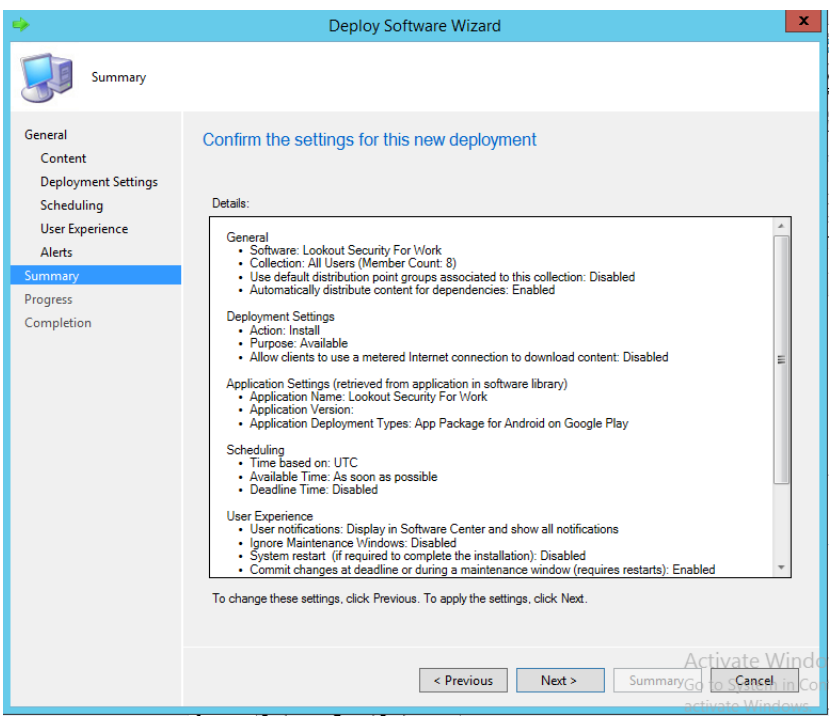
401

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



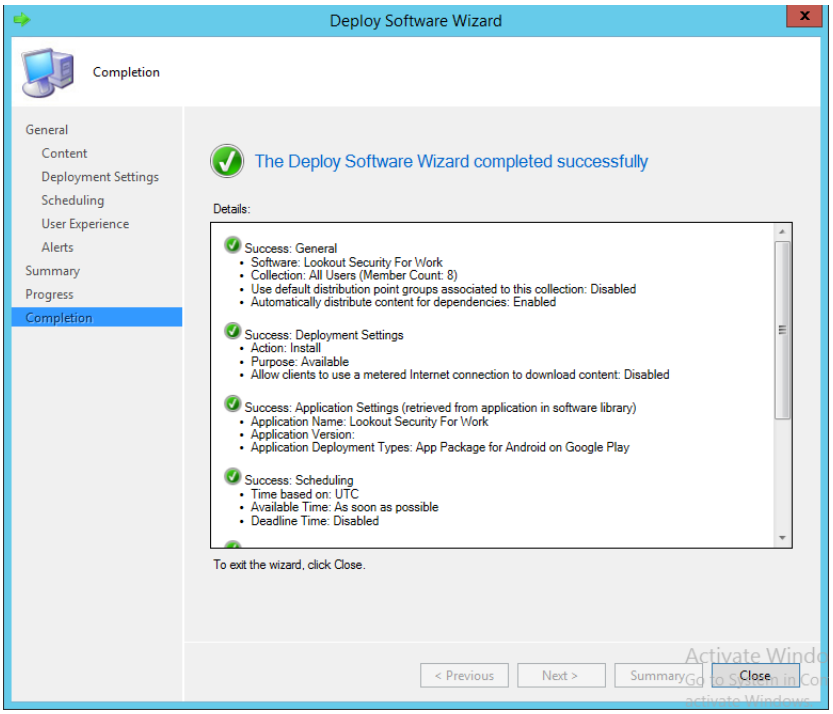
404

405 11. Click **Next**.



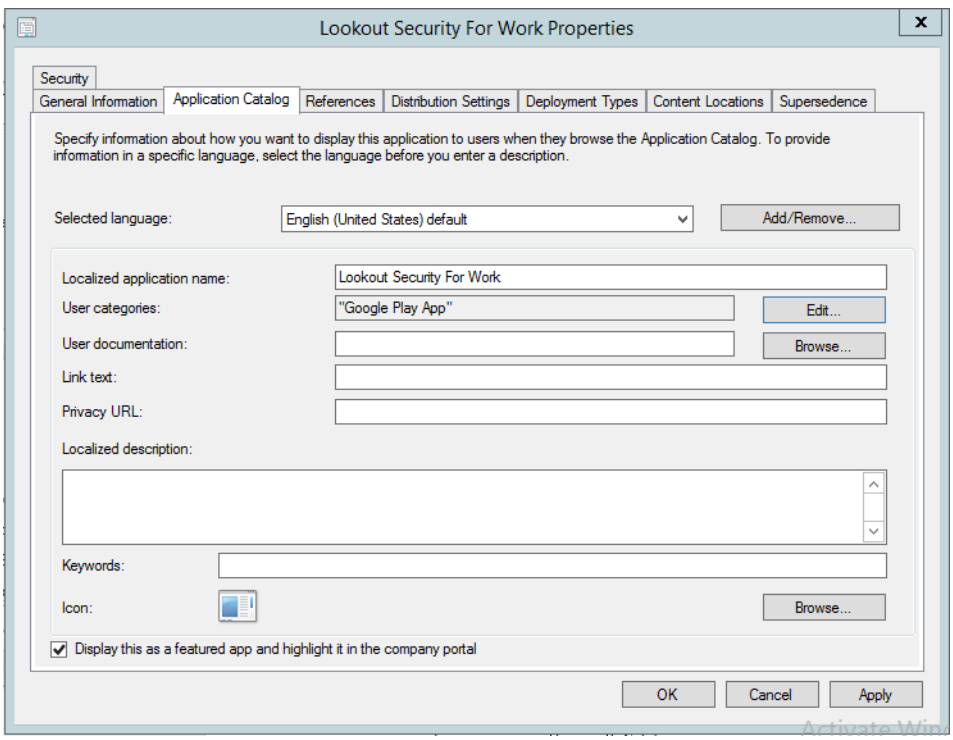
406

407 12. Click **Next**.



408

409 13. Click **Close**.



410

411

4 Device Configuration

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

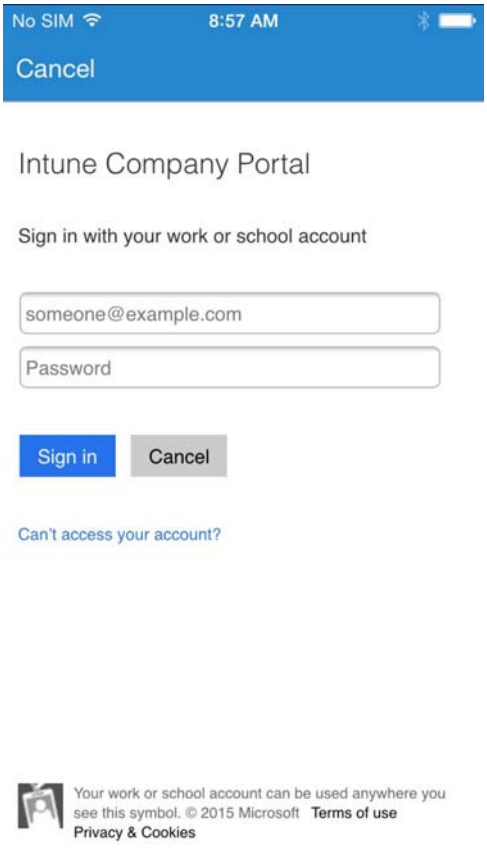
4.1 Device Enrollment with Office 365

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

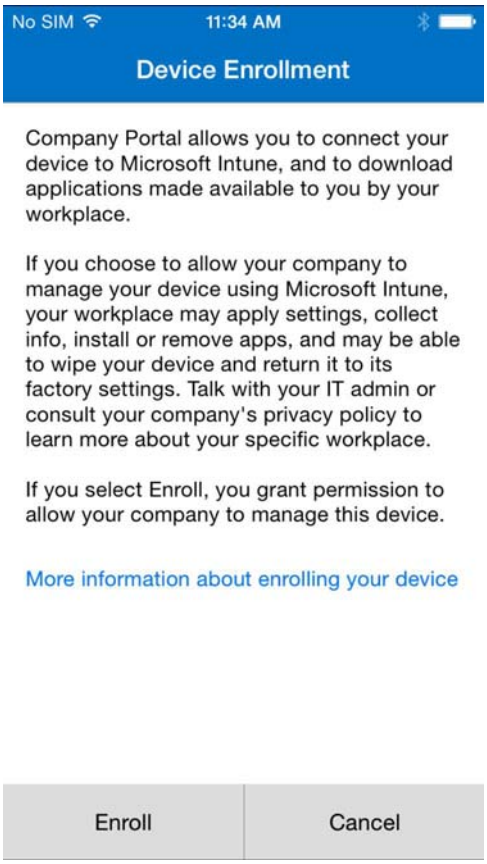
Instruct device owners to download the Company Portal application through the application distribution point of their platform to start the enrollment process.[9] This is not necessary for Windows Phone devices because MDM management through this service is native to the device.

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

4.1.1 iOS

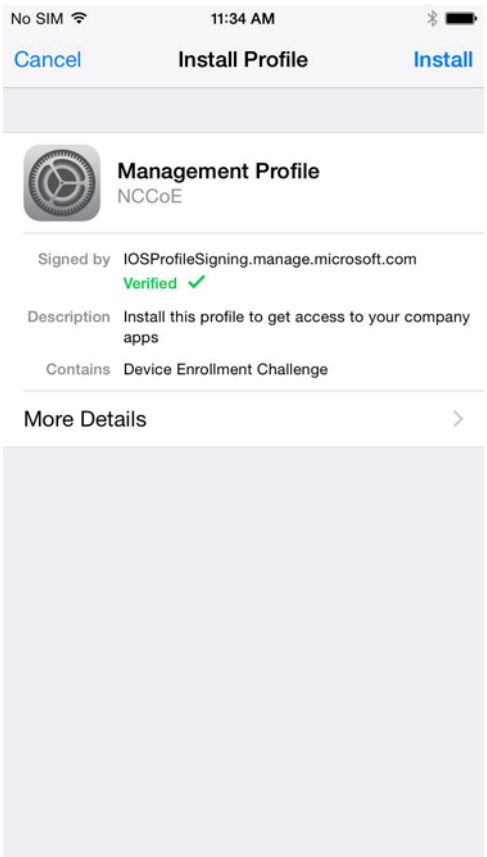


1. Download the company portal application from the App store and log in using Office 365 credentials.

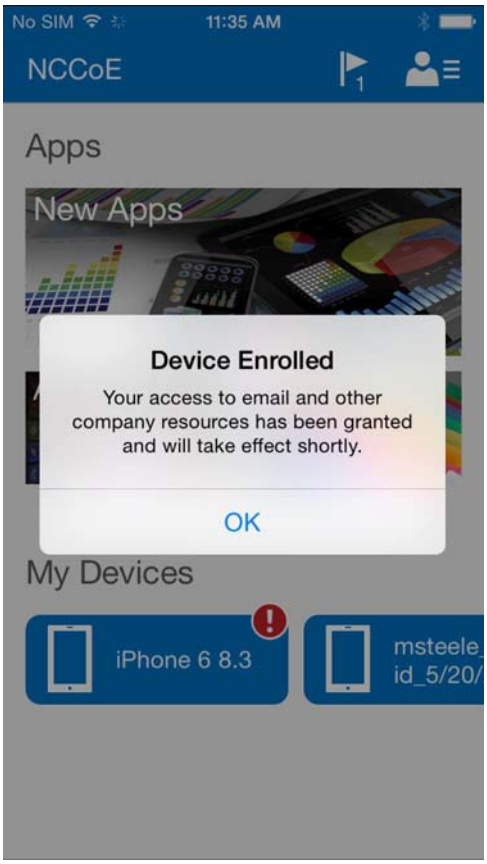


24

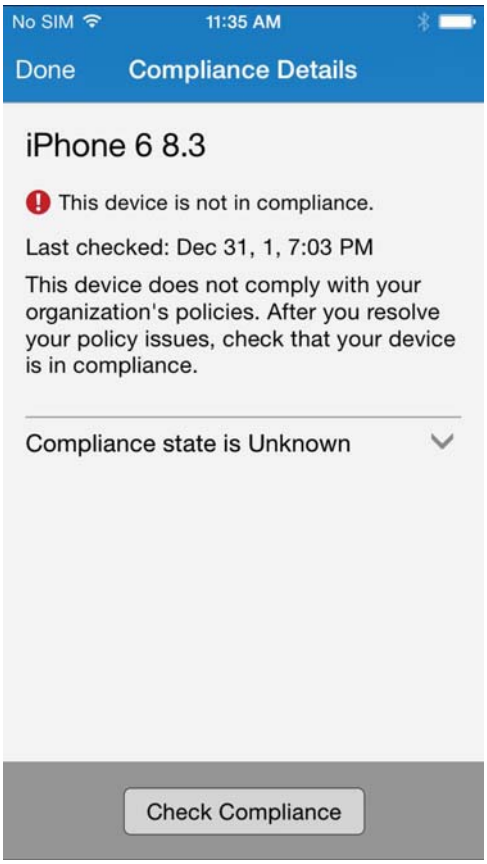
25 2. The user will then be asked to enroll their device and accept the organization's policies.



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

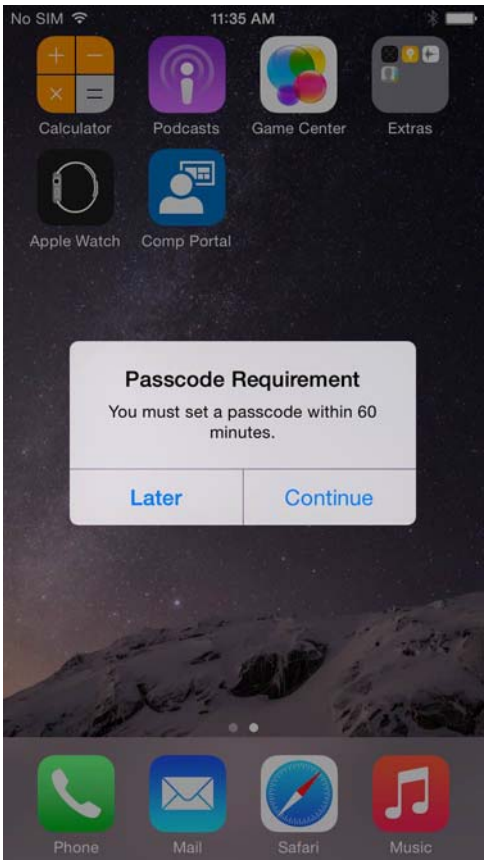


4. Upon accepting the management profile, the device will be enrolled and the user will receive this confirmation message.



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 inthe company portal.

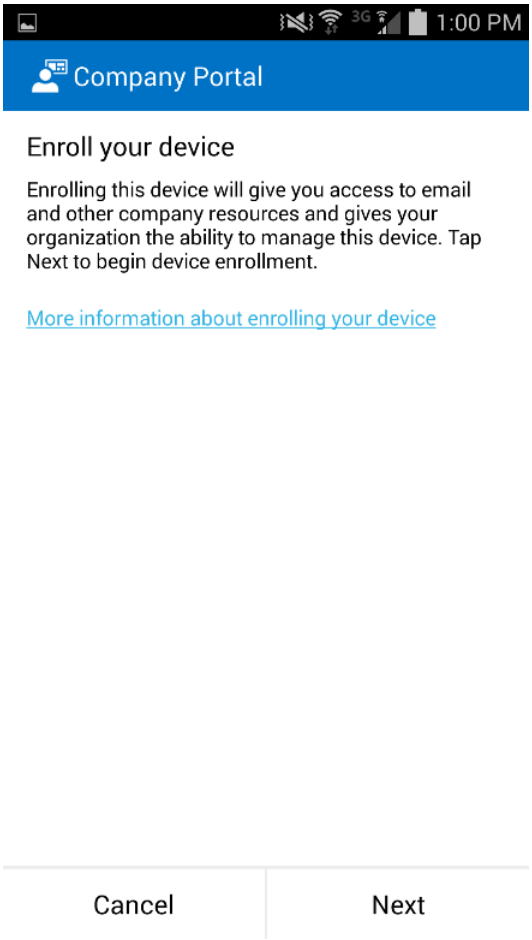
6. The compliance checking process will take a couple of minutes. The user can minimize the application during the compliance checking process.



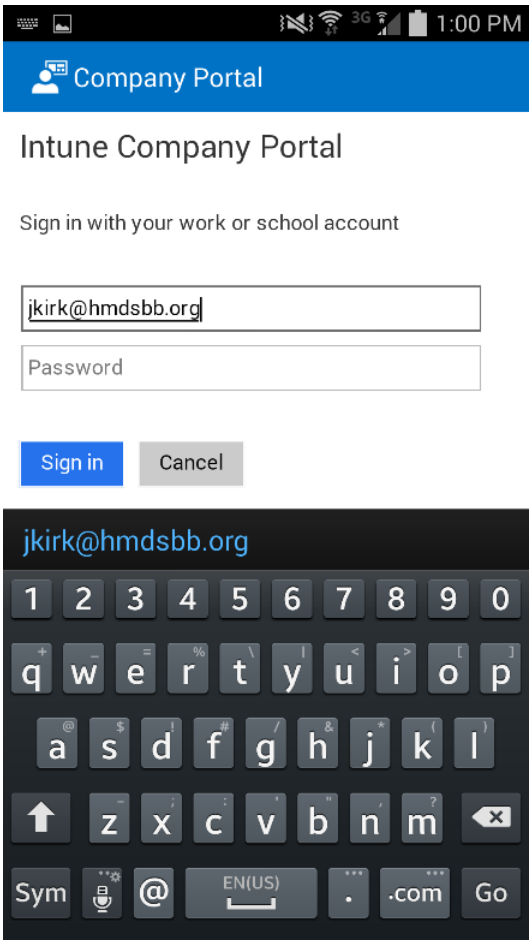
7. Upon minimizing the company portal application during the compliance checking process, the user is presented with the password remediation process, alerting the user to change their password within the hour.

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

4.1.2 Android

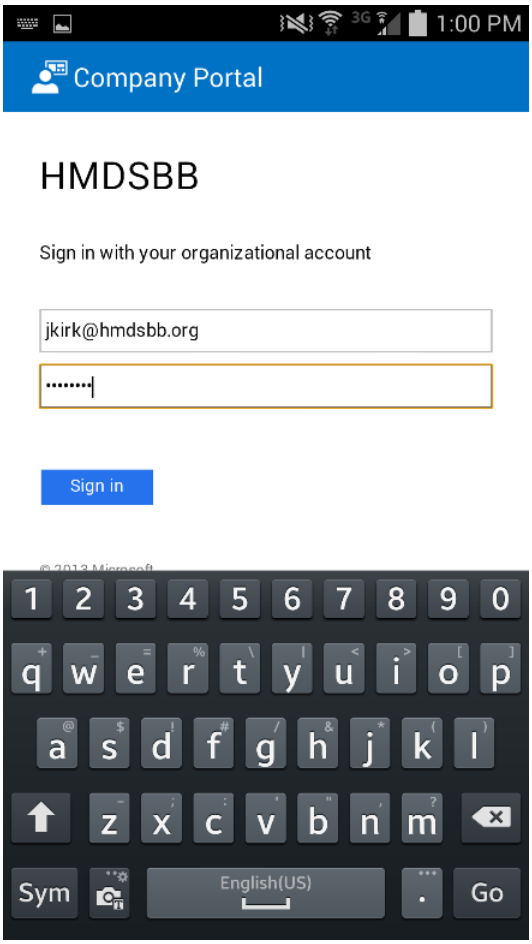


1. After launching the Company Portal, Click **Next**.

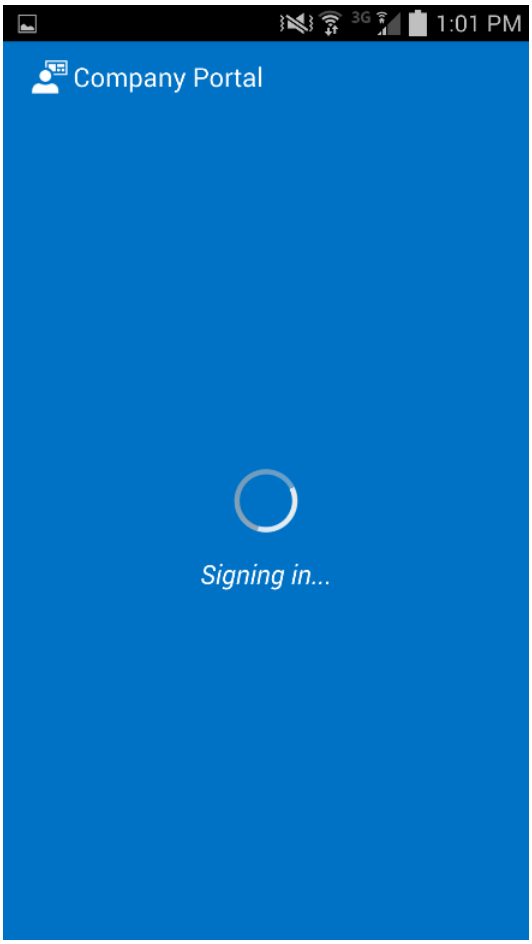


49

50 2. Enter your email address.

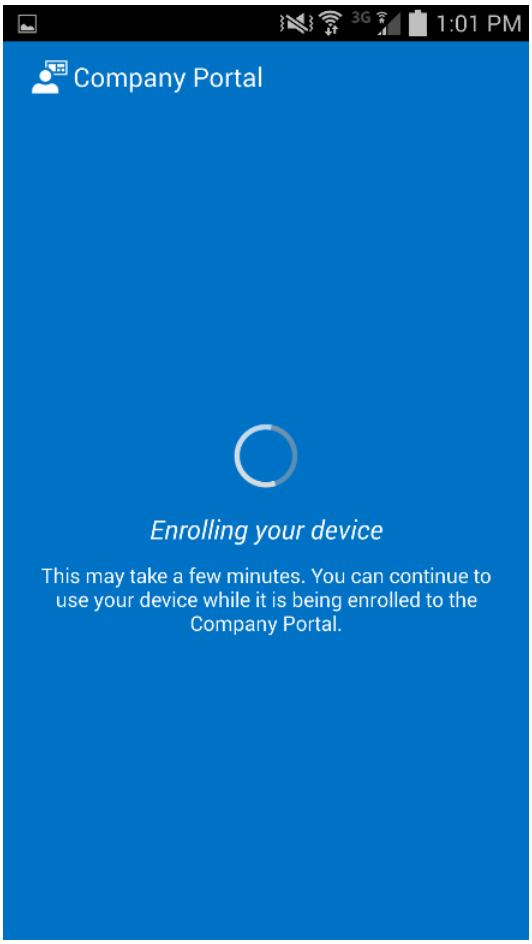


3. If implementing a hybrid architecture, you will be redirected to your enterprise login site to enter your password. Click **Sign In**.

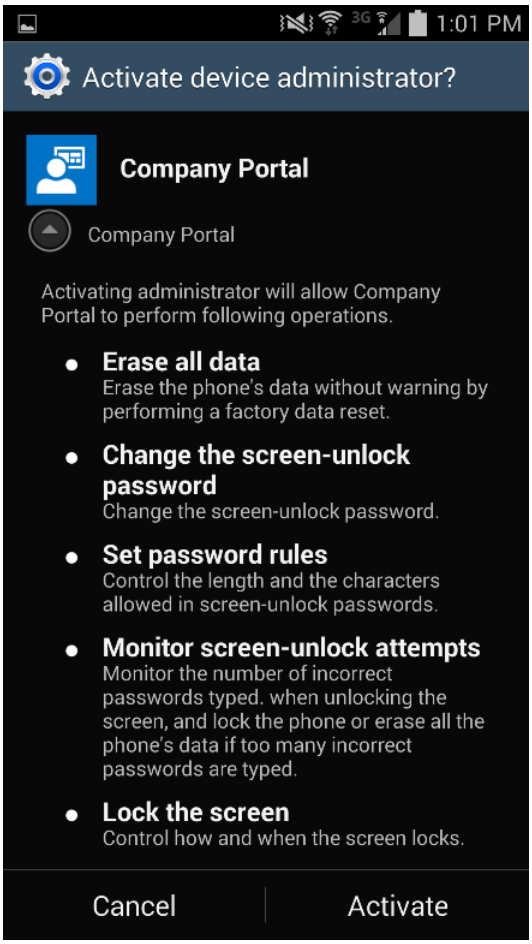


54

55 4. No action required.



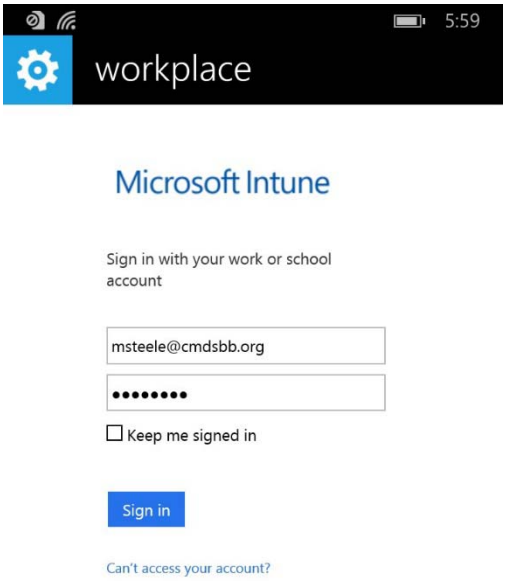
5. No action required.



58

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

4.1.3 Windows Phone 8.1



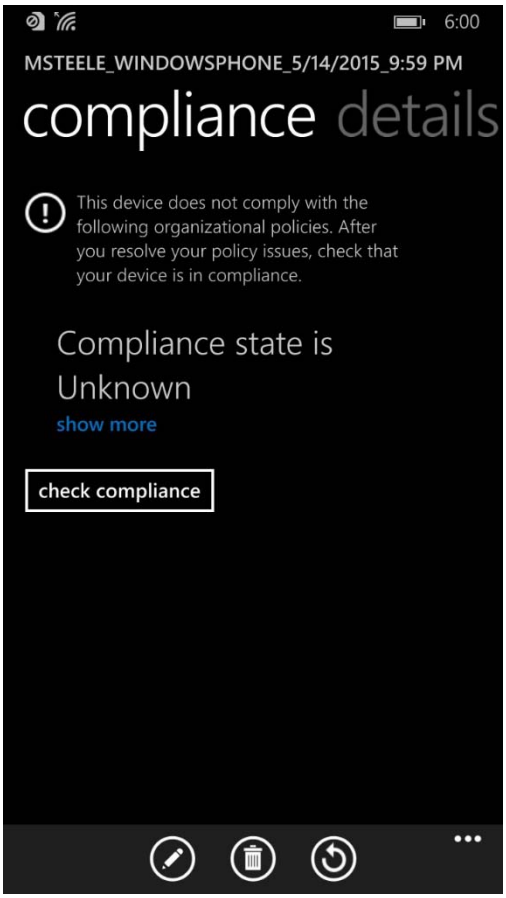
1. First the user must workplace join their device. Navigateto **Settings -> System tab -> Workplace** on Windows Phone 8.1 devices, or **Settings -> System tab -> Company apps** on Windows Phone 8 devices.

65

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

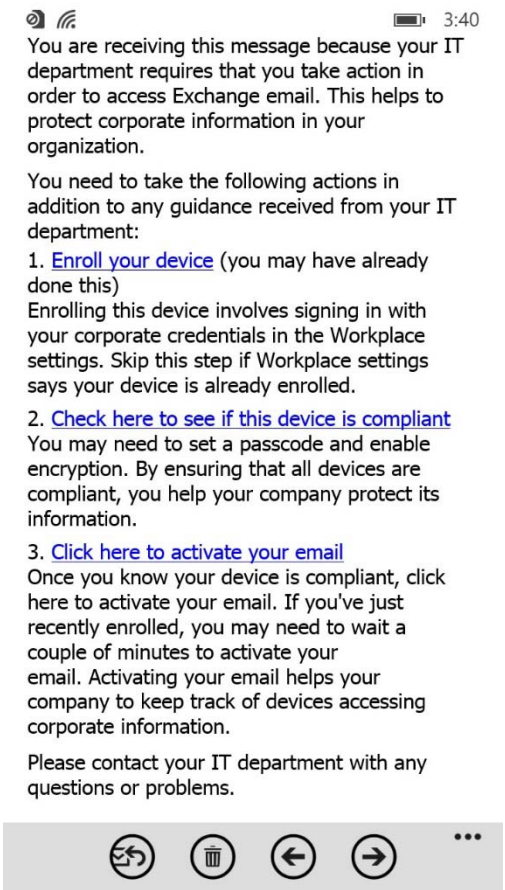
3. After connecting to your company's portal, your device should be able to be managed by Office 365. To do this, download company portal from the App store to finish enrolling your device and receive your organization’s policies.

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

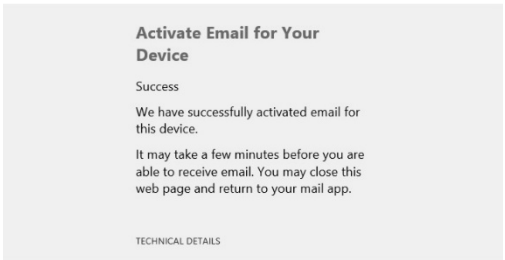


5. After checking the compliance manually (less than 5 minutes), the user's device is fully enrolled and should have the appropriate policies deployed.

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



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



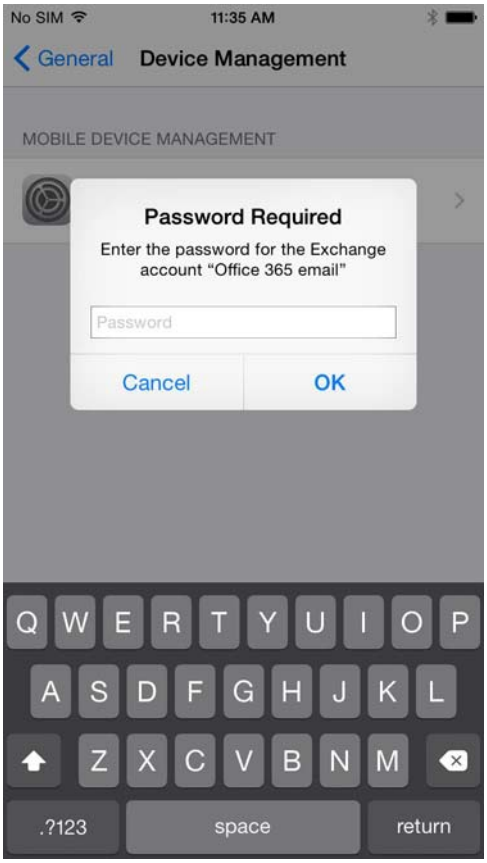
8. The activation link will open a browser, and upon successful activation the user should be directed to this page. At this point the user should have full access to exchange email/contacts/calendar.

4.2 Email Setup

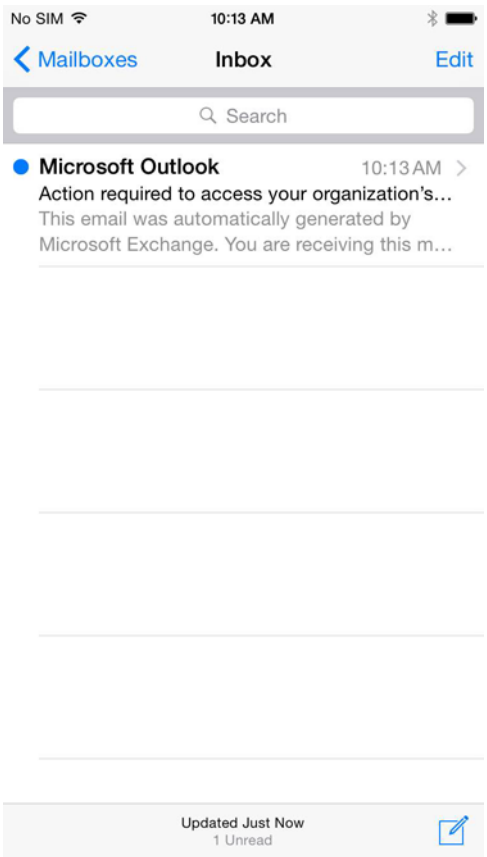
This section steps through the setup of email clients on iOS, Android, and Windows Phone. For iOS and Android, we use the Outlook client from Microsoft in the Play Store. The native email capabilities are used with Windows Phone. Other third-party applications are available, but this guide makes no assumptions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

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

4.2.1 iOS

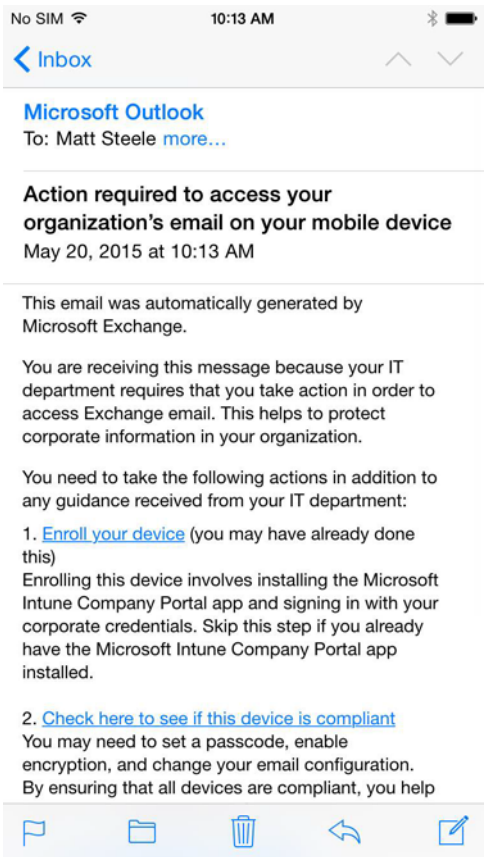


1. When the user first opens the settings application either before/during/after the compliance check, they are prompted for their Office365 password for the exchange profile that is provisioned during the on-boarding process. This is a one-time occurrence.

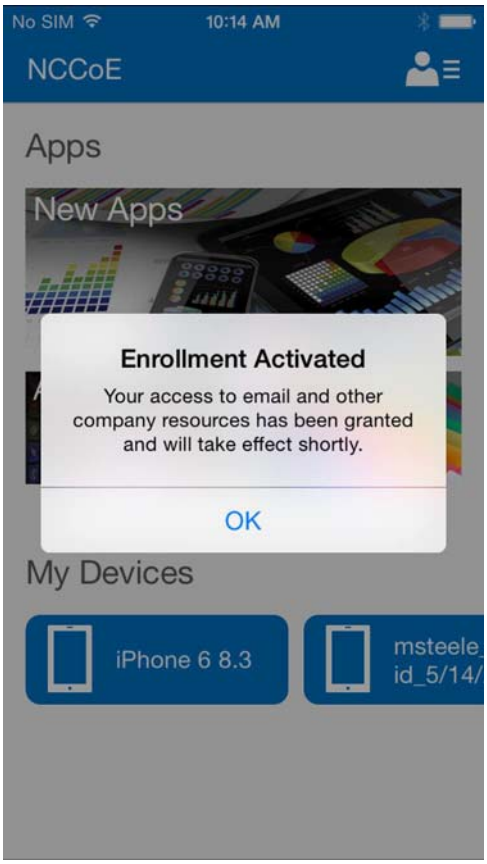


102

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



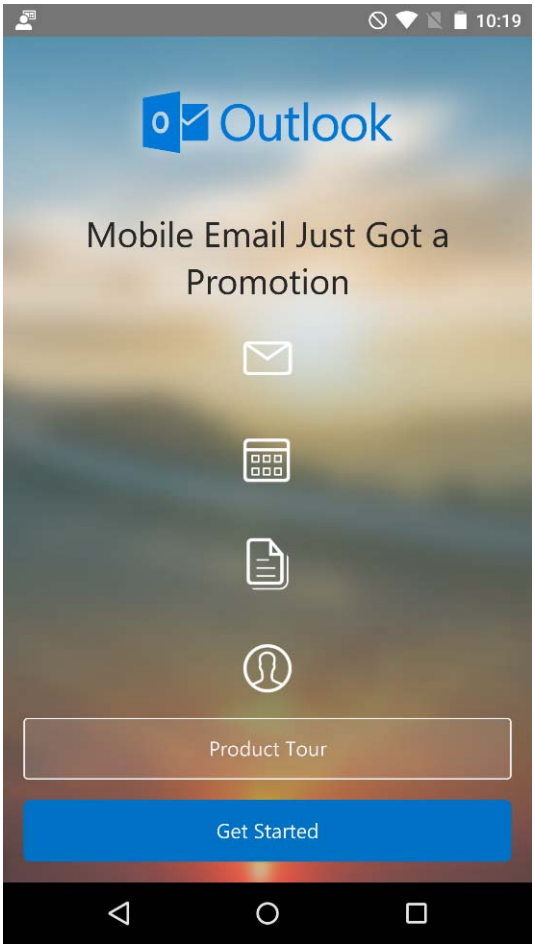
3. To activate their email access, the user will have to tap the link to activate the email and check for compliance.



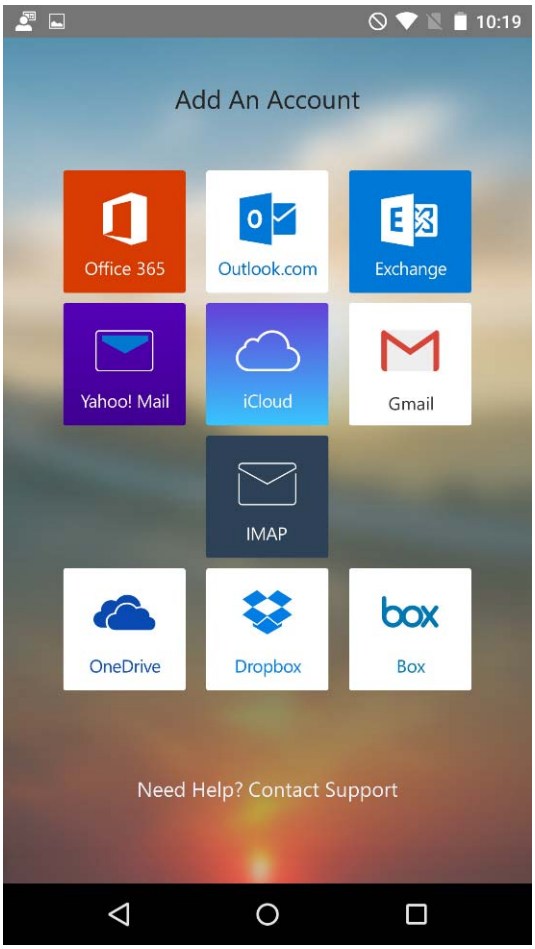
107

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

4.2.2 Android

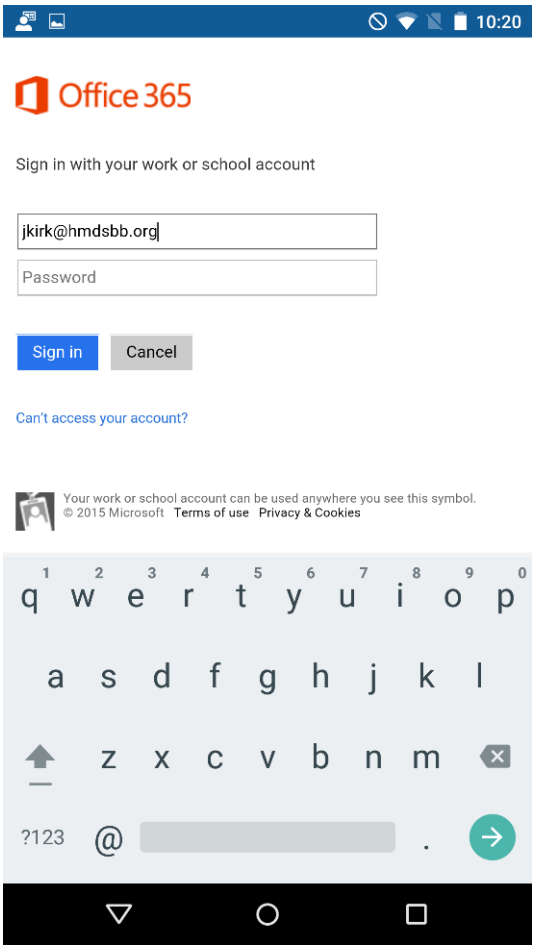


1. Open the Outlook application on your device.



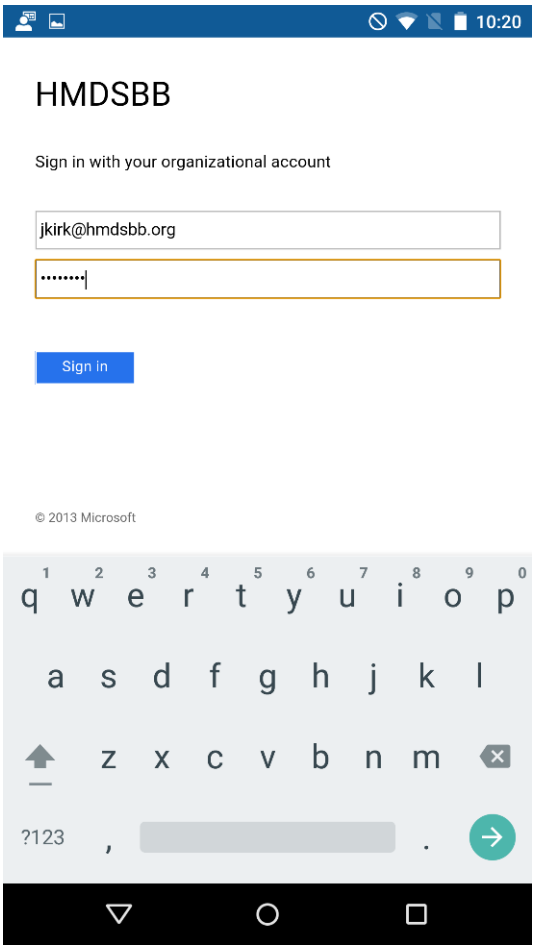
112

113 2. Choose **Office 365**.



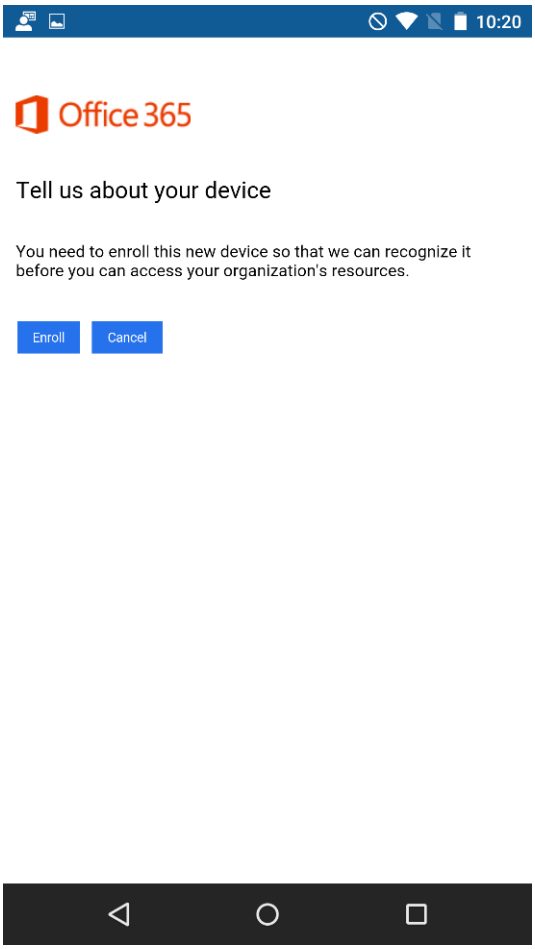
114

115 3. Log in with your enterprise credentials.



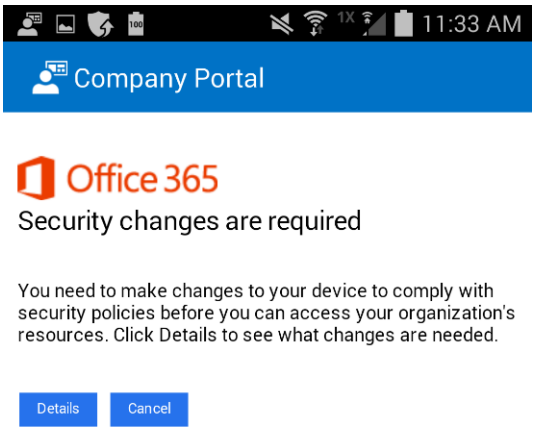
116

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

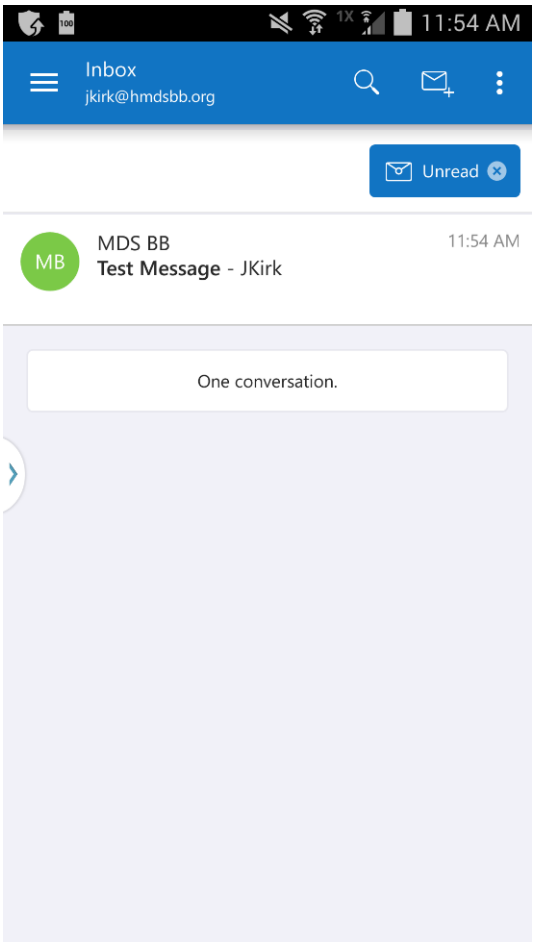


119

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



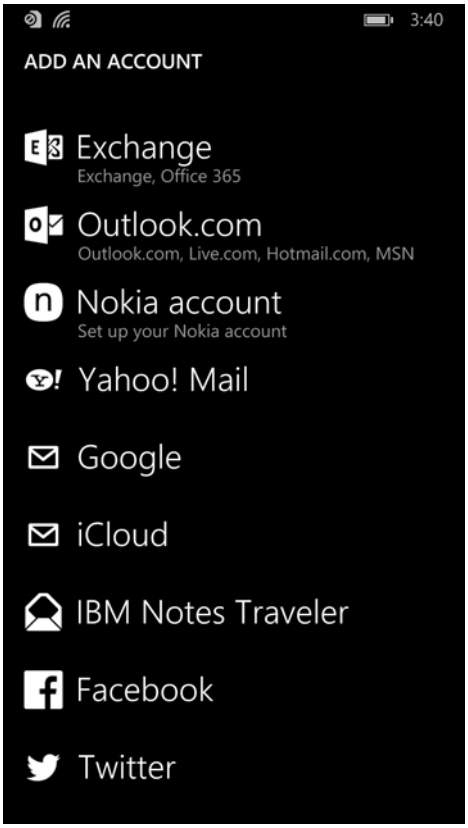
6. A device that is out of compliance with the MDM policy will not have access to Office 365 services. The device owner will be forced to remediate the device.



124

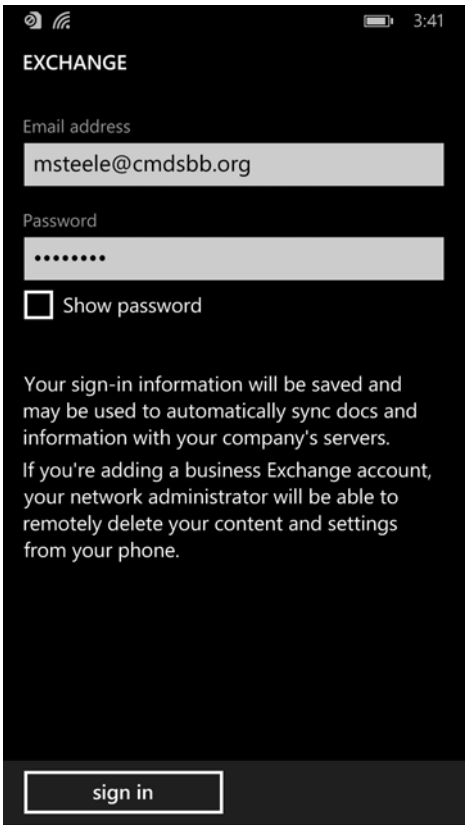
125 7. The device owner will be granted access to Office 365 after the device complies with policy.

126 4.2.3 Windows Phone 8.1



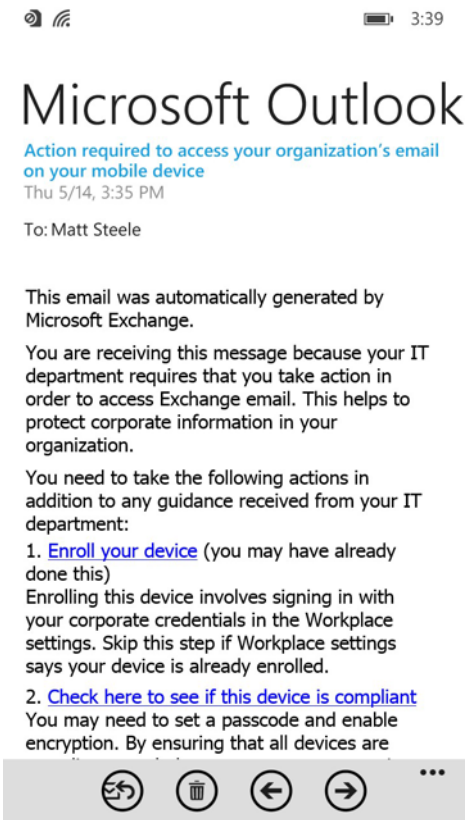
127

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

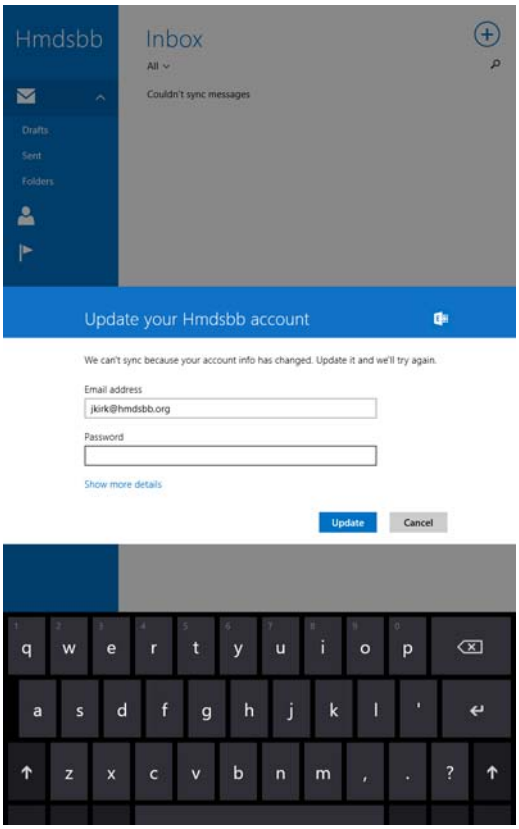
133 2. Log in using your Office365 credentials. The server info should auto-populate.



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

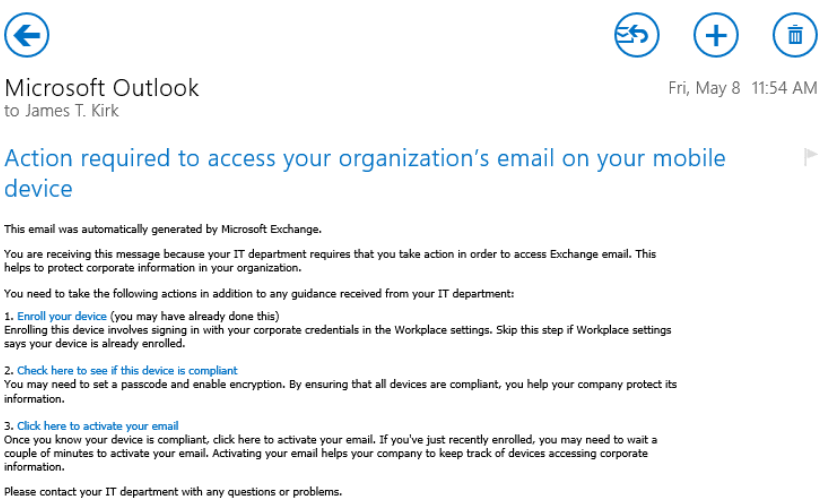
4.2.4 Windows 8.1

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



141

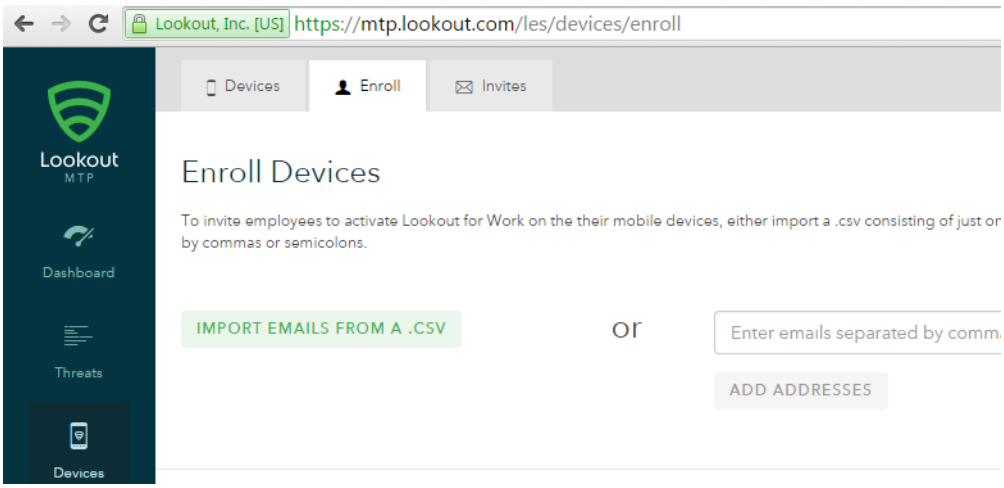
142 1. The user can add their account to the built-in email application by selecting **Exchange**
143 **account** and adding their email@customdomain and password. The email application
144 should be able to pull the settings.



145

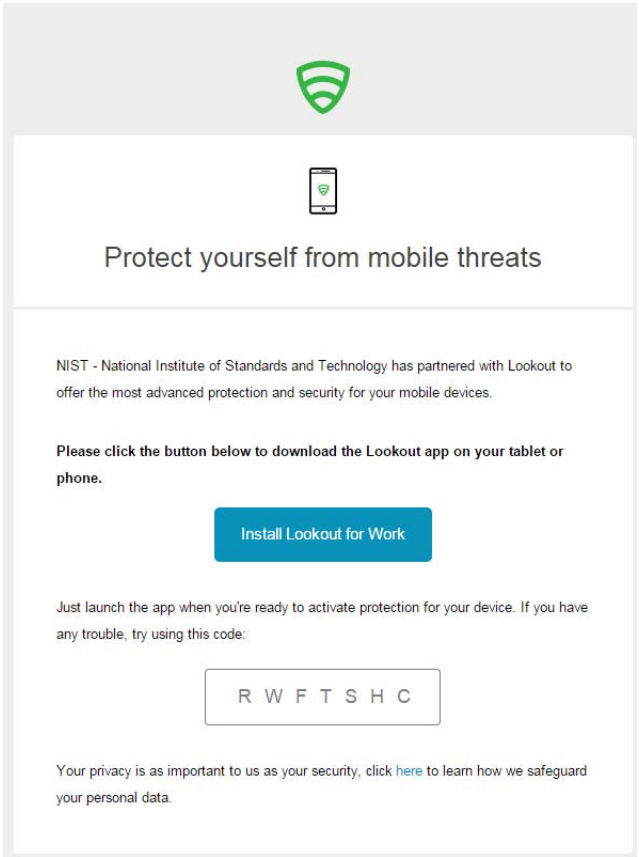
146 2. Upon connecting to their exchange account, the user should receive an email asking them
147 to activate their email by clicking the link to check compliance.

148 4.3 Lookout MTP Enrollment



149

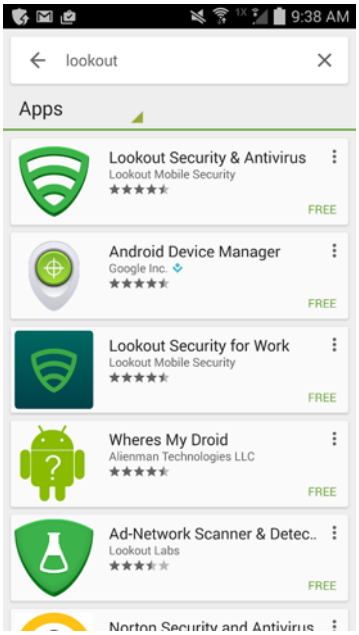
150 1. Open the Lookout MTP administrative console with a browser. Navigate to
151 https://mtp.lookout.com/les/devices/enroll and type the target user's email address into the
152 provided Web field.



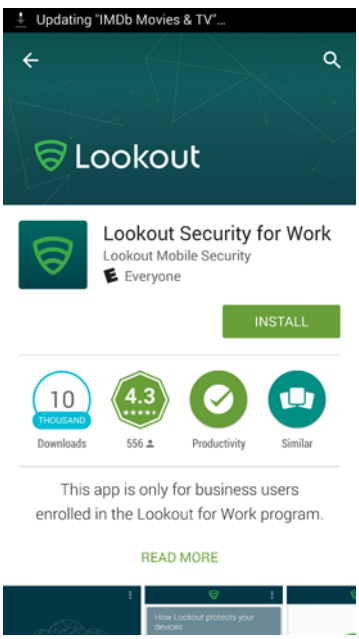
153

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

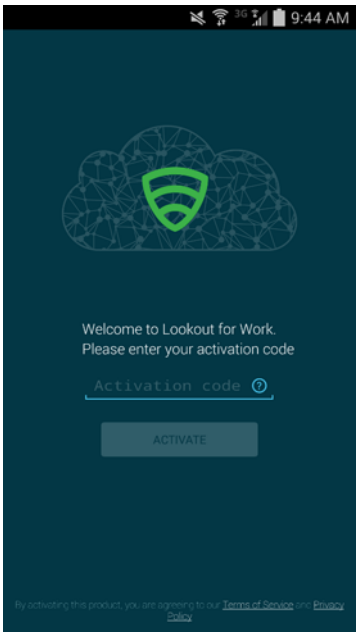
4.3.1 Android



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

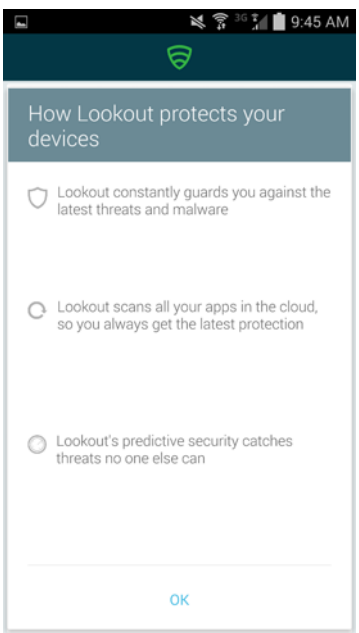


2. Select the **Lookout Security for Work** application and tap **Install**.



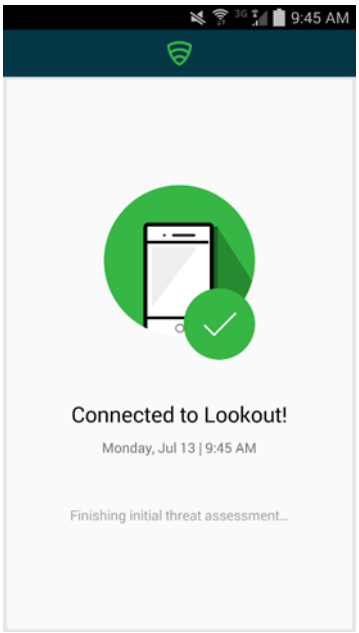
161

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



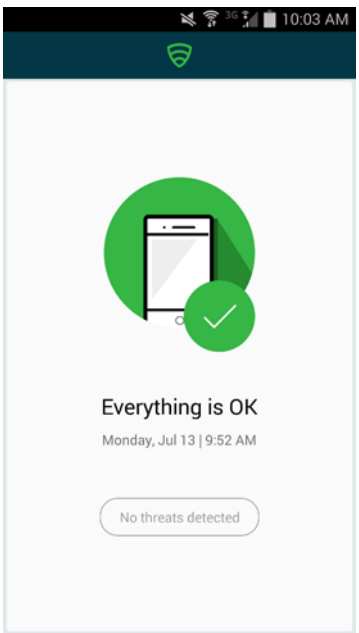
163

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

Appendix A Acronyms

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

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

Appendix B References

[1] IDC, Android and iOS Squeeze the Competition, February 24, 2015. http://www.idc.com/getdoc.jsp?containerId=prUS25450615 [accessed 6/19/2015].

[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].

[3] Microsoft, Understanding Certificate Requirements, November 08, 2011. https://technet.microsoft.com/library/gg476123.aspx [accessed October 14, 2015].

[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].

[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]

[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]

[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].

[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].

[9] Microsoft, Azure Active Directory Sync, July 22, 2015. https://msdn.microsoft.com/en-us/library/azure/dn790204.aspx [accessed October 14, 2015].

[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].