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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Mobile Device Security: Cloud and Hybrid Builds

Executive Summary

- Adopting mobile devices without the necessary policies and management infrastructure in place increases the opportunities for attackers to breach sensitive enterprise data.
- The National Cybersecurity Center of Excellence (NCCoE) developed an example mobile device and enterprise mobility management solution that organizations can use to reduce the likelihood of a data breach.
- The security characteristics in this guide are informed by guidance and best practices from standards organizations.
- The NCCoE's approach uses commercially available products that can be included alongside your current products in your existing infrastructure.
- The example solution is packaged as a "How To" guide that demonstrates implementation of standards-based, commercially available cybersecurity technologies in the real world. The guide helps organizations utilize technologies to reduce the risk of intrusion via mobile devices, while saving them research and proof of concept costs.

THE CHALLENGE

IT environments have changed drastically because of the increasing popularity of smartphones, tablets, and other highly capable, rapidly maturing mobile devices. These devices have many functional similarities to traditional information technology (IT) systems - including access to a wide range of enterprise applications and data - as well as additional functionality particular to mobile computing. This has greatly expanded the utility and value of mobile devices, enabling employees to do their jobs more effectively and efficiently. Unfortunately, security controls have not kept pace with the security risks that mobile devices can pose, not only in Bring Your Own Device (BYOD) scenarios, but also in corporately owned and personally enabled (COPE) mobile device deployments, where mobile devices are adopted on an ad hoc basis. This gap in protection mechanisms means that data stored on or accessed from mobile devices is at increased risk of being breached.

For example, suppose that an organization has enabled mobile access to its email, calendaring, and contact management services regardless of the origin of the employees' mobile devices (organization-owned and employee-owned, organization-provisioned and employee-provisioned, etc.) If sensitive data is stored on a poorly secured mobile device that is lost or stolen, an attacker may be able to readily gain unauthorized access to that data. Even worse, a mobile device with remote access to sensitive organizational data could be leveraged by an attacker to gain unauthorized access to not only that data, but also any other data that the user is allowed to access from a mobile device.

THE SOLUTION

The NIST cybersecurity practice guide *Mobile Device Security: Cloud and Hybrid Builds* demonstrates how commercially available technologies can meet your organization's needs to secure sensitive enterprise data accessed by and/or stored on employees' mobile devices.

In our lab at the NCCoE, part of the National Institute of Standards and Technology (NIST), we built an environment based on typical mobile devices and an enterprise email, calendaring, and contact management solution.

We demonstrate how security can be supported throughout the mobile device life cycle. This includes how to configure a device to be trusted by the organization, how to maintain adequate separation between the organization's data and the employee's personal data stored on or accessed from the mobile device, and how to handle the deprovisioning of a mobile device that should no longer have enterprise access (e.g., device lost or stolen, employee leaves the company.)

The guide:

- identifies the security characteristics needed to sufficiently reduce the risks from mobile devices storing or accessing sensitive enterprise data
- maps security characteristics to standards and best practices from NIST and other organizations
- describes a detailed example solution, along with instructions for implementers and security engineers on installing, configuring, and integrating the solution into existing IT infrastructures
- selects mobile devices and enterprise mobility management (EMM) systems that meet the identified security characteristics
- provides an example solution that is suitable for organizations of all sizes and evaluates the solution

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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.

BENEFITS

Our example solution has several benefits, including the following:

- reduces risk so that employees are able to access the necessary enterprise data from nearly any location, over any network, using a wide variety of mobile devices
- enables the use of BYOD, COPE, and other mobile devices deployment models, which may provide cost savings and increased flexibility for organizations
- leverages cloud services to secure sensitive corporate data using the latest industry best practices and defense-in-depth security strategy, which may reduce infrastructure costs for organizations
- enables identity federation between an on premise identity store and associated cloud services, which may improve user experience and enhance enterprise security
- enhances visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implements industry standard mobile security controls reducing long term costs and decreasing the risk of vendor lock-in

SHARE YOUR FEEDBACK

You can get the guide at http://nccoe.nist.gov and help improve it by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Or learn more by arranging a demonstration of this example solution by contacting us at mobile-nccoe@nist.gov.

TECHNOLOGY PARTNERS

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partnership (NCEP) partners.

intel®

Lookout

Symantec™

Microsoft

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. As the U.S. national lab for cybersecurity, the NCCoE seeks problems that are applicable to whole sectors, or across sectors. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE
http://nccoe.nist.gov

ARRANGE A DEMONSTRATION
nccoe@nist.gov
240-314-6800

NIST CYBERSECURITY PRACTICE GUIDE

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

Approach, Architecture, and Security Characteristics

for CIOs, CISOs, and Security Managers

Joshua Franklin
Kevin Bowler
Christopher Brown
Sallie Edwards
Neil McNab
Matthew Steele

NIST SPECIAL PUBLICATION 1800-4b

National Institute of Standards and Technology
U.S. Department of Commerce
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-4b

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

Joshua Franklin

National Cybersecurity Center of Excellence
Information Technology Laboratory

Kevin Bowler

Christopher Brown

Neil McNab

Matthew Steele

The MITRE Corporation
McLean, VA

November 2015

U.S. Department of Commerce

Penny Pritzker, Secretary

National Institute of Standards and Technology

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

DISCLAIMER

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

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Contents

List of Figures

List of Tables

1 Summary

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

The NIST 1800-4 series of documents contain:

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

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

1.1 The Challenge

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

1.2 The Solution

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

Our approach to mobile device security includes:

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

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

1.3 Benefits

This proposed solution provides the following value to organizations:

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

1.4 Technology Partners

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

- Intel
- Lookout

- Microsoft
- Symantec

1.5 Feedback

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

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

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

2 How to Use This Guide

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

This guide contains three volumes:

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

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

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

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

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

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

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

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-4c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution that would support the deployment of an ABAC system and the corresponding business processes.[1] Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 4.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

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

3 Introduction

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

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

4 Approach

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

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

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

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

4.1 Audience

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

4.2 Scope

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

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

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

4.3 Assumptions

The following assumptions exist for this project:

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

4.4 Risk Assessment

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

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

4.4.1 Threats

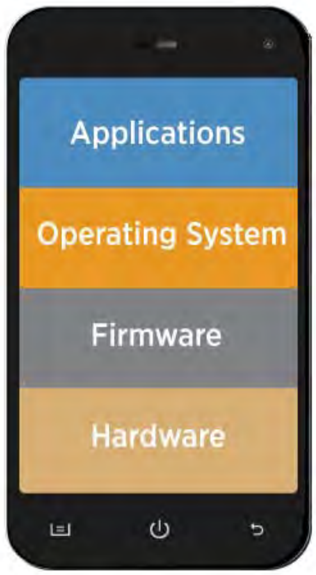
Below are common threats to mobile devices:

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

4.4.2 Vulnerabilities

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

Figure 4.1 Mobile Technology Stack



Note that on mobile devices, the firmware and hardware levels are not as clearly defined as figure 4.1 depicts. Mobile devices with access to a cellular network contain a baseband processor comprising a distinct telephony subsystem used solely for telephony services (e.g., voice calls, texts, data transfer via the cellular network) [22]. This processor and the associated software/firmware on which it operates are separated from the mobile operating system running on the application processor. Furthermore, some mobile devices contain additional security-specific hardware and firmware used to assist with making security decisions and storing important information, such as encryption keys, certificates and credentials [15] [16] [17].

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

4.4.3 Risk

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

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

4.4.4 Security Control Map

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

Table 4.1 Security Control Map

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

Table 4.1 Security Control Map (Continued)

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

Table 4.1 Security Control Map (Continued)

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

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

4.5 Technologies

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

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

Table 4.2 Participating Companies and Contributions Mapped to Controls

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

5 Architecture

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

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

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

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

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

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

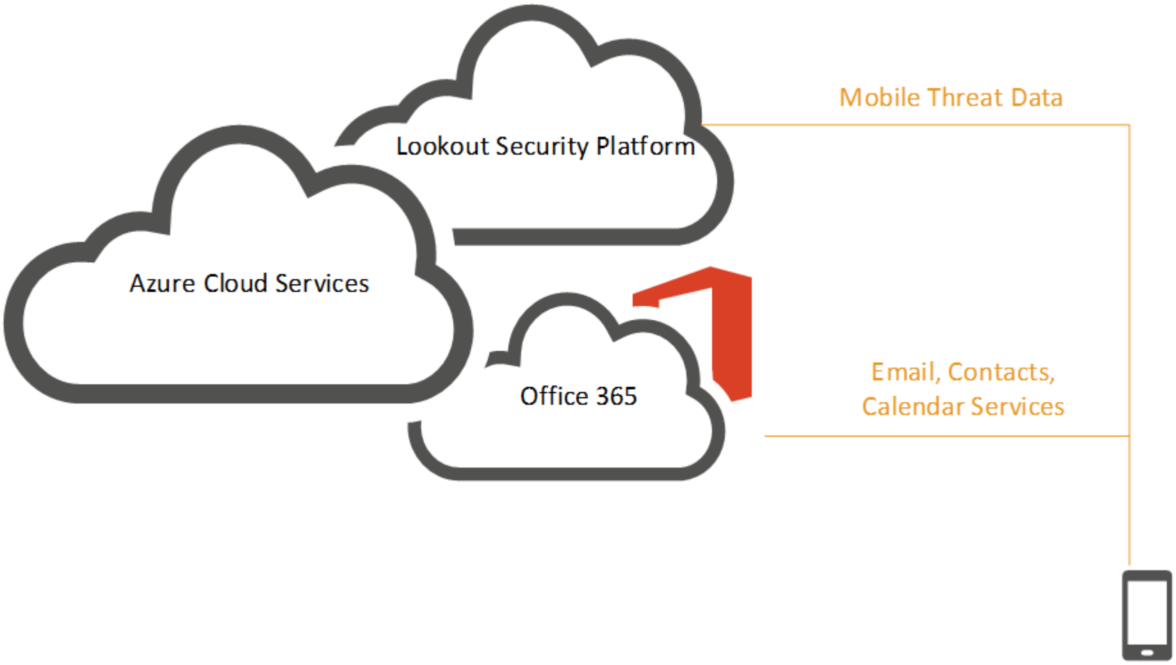
5.1 Cloud Build: Architecture Description

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

This solution can be easily configured and operated as a cloud service to onboard personally or enterprise-owned mobile devices into the EMM. This allows users to access enterprise resources and enterprise managers to push policies to mobile devices. Office 365 allows for a variety of policies to be pushed to the device (detailed in appendix C), but offers a significantly reduced feature set when compared with Microsoft Intune.

Figure 5.1 provides the overall architecture of the cloud build.

Figure 5.1 Cloud Build Architecture



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

5.1.1 Cloud Architecture Benefits

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

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

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

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

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

5.1.2 Cloud Build Security Characteristics

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

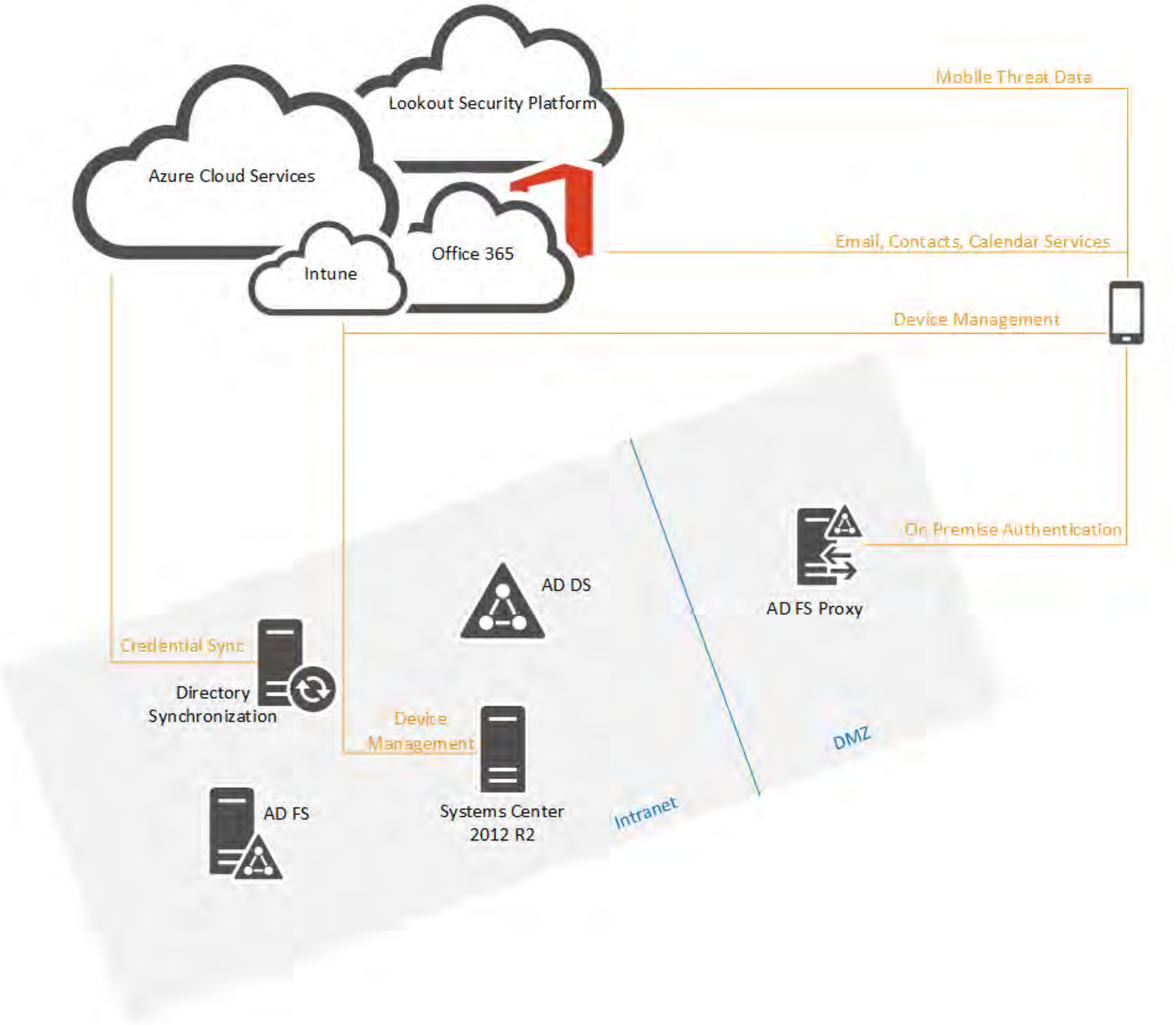
An individual who decides to participate in a managed scenario, must download the Microsoft Community Portal application and input the required information. Then the device is provisioned into the EMM, and the default set of policies listed in appendix C is applied to the device. This includes local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

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

5.2 Hybrid Build: Architecture Description

The hybrid build leverages the same cloud-based services from the cloud build, but integrates them into the network in a different manner. It includes a combination of enterprise assets likely to be present within an organization's existing network, including EMM capabilities, and adds cloud services for MDM. This build might be a starting point for an organization that has significant investment in or dependence on an internal AD server. The cornerstone of the hybrid build is the existing AD server housing user data and associated credentials. Figure 5.2 depicts the high-level hybrid build architecture.

Figure 5.2 Hybrid Build Architecture



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

The hybrid build contains the following elements:

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

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

Additional components not pictured:

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

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

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

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

5.2.1 Hybrid Architecture Benefits

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

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

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

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

5.2.2 Hybrid Build Security Characteristics

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

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

5.3 Security Characteristics and Capabilities

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

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

5.3.1 Default Policies

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

Table 5.1 Default EMM Policy

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

Table 5.1 Default EMM Policy (Continued)

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

Table 5.1 Default EMM Policy (Continued)

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

6 Outcome

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

6.1 The User's Experience

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

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

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

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

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

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

Figure 6.1 Android Workflow

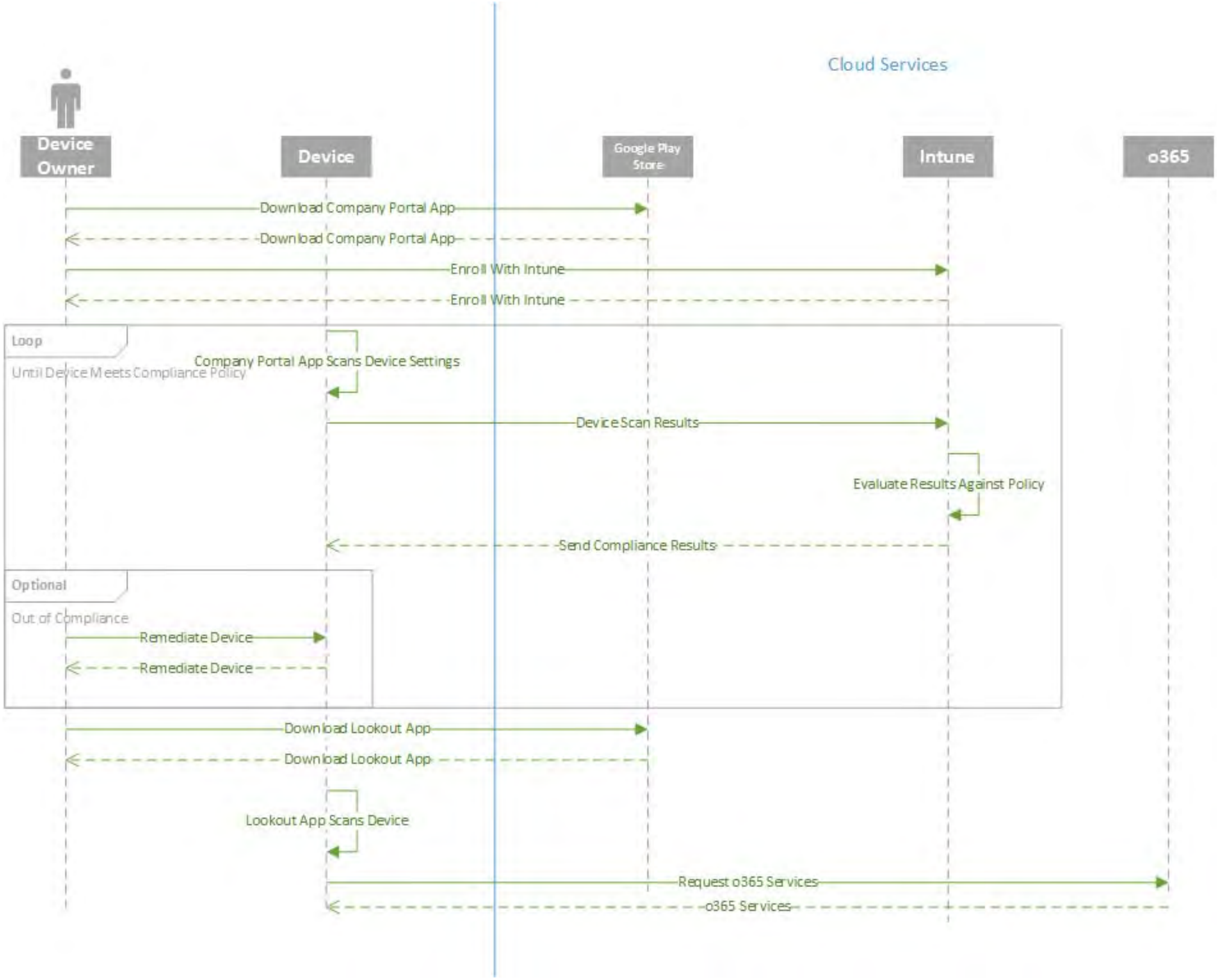


Figure 6.2 iOS Workflow

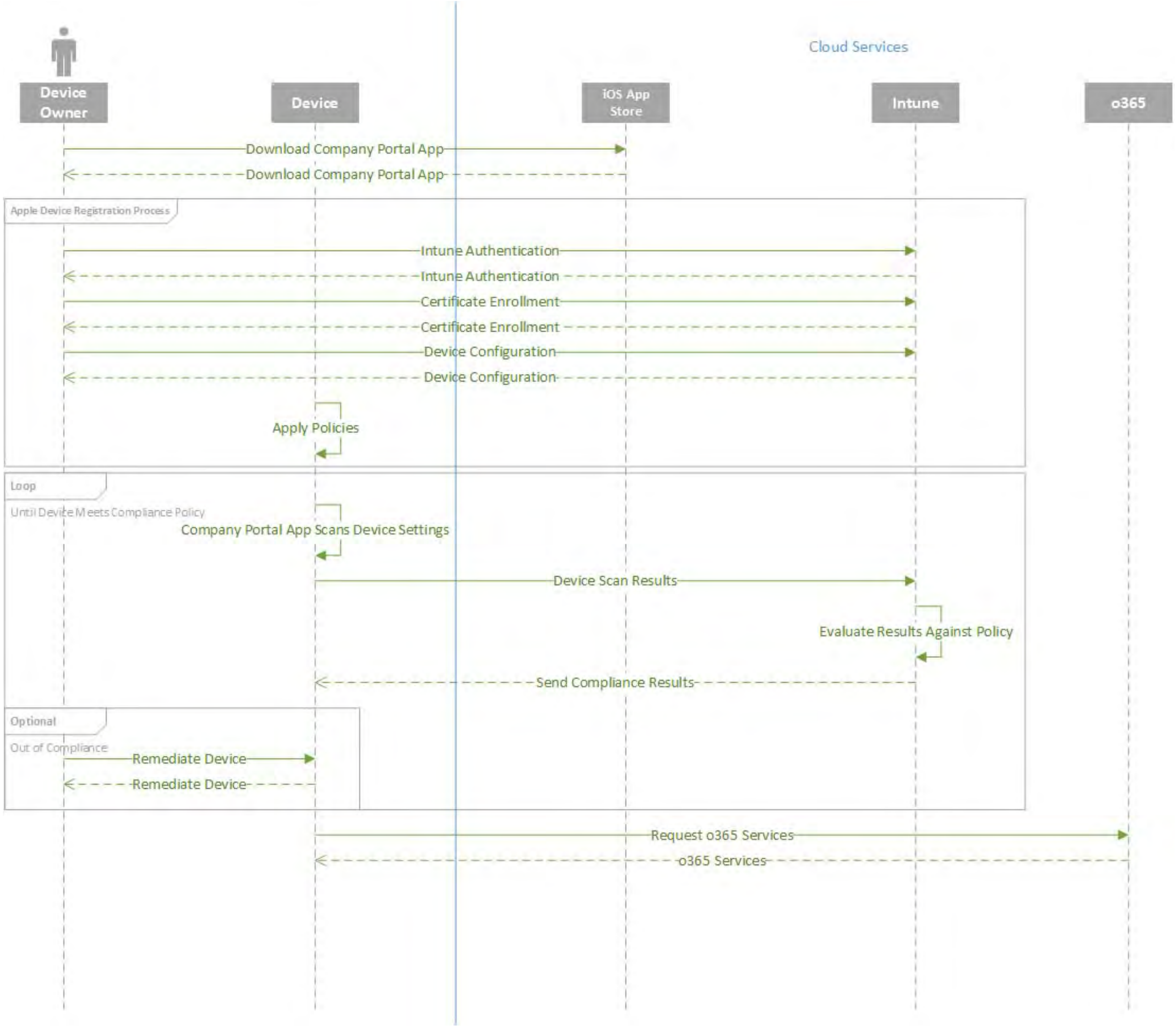
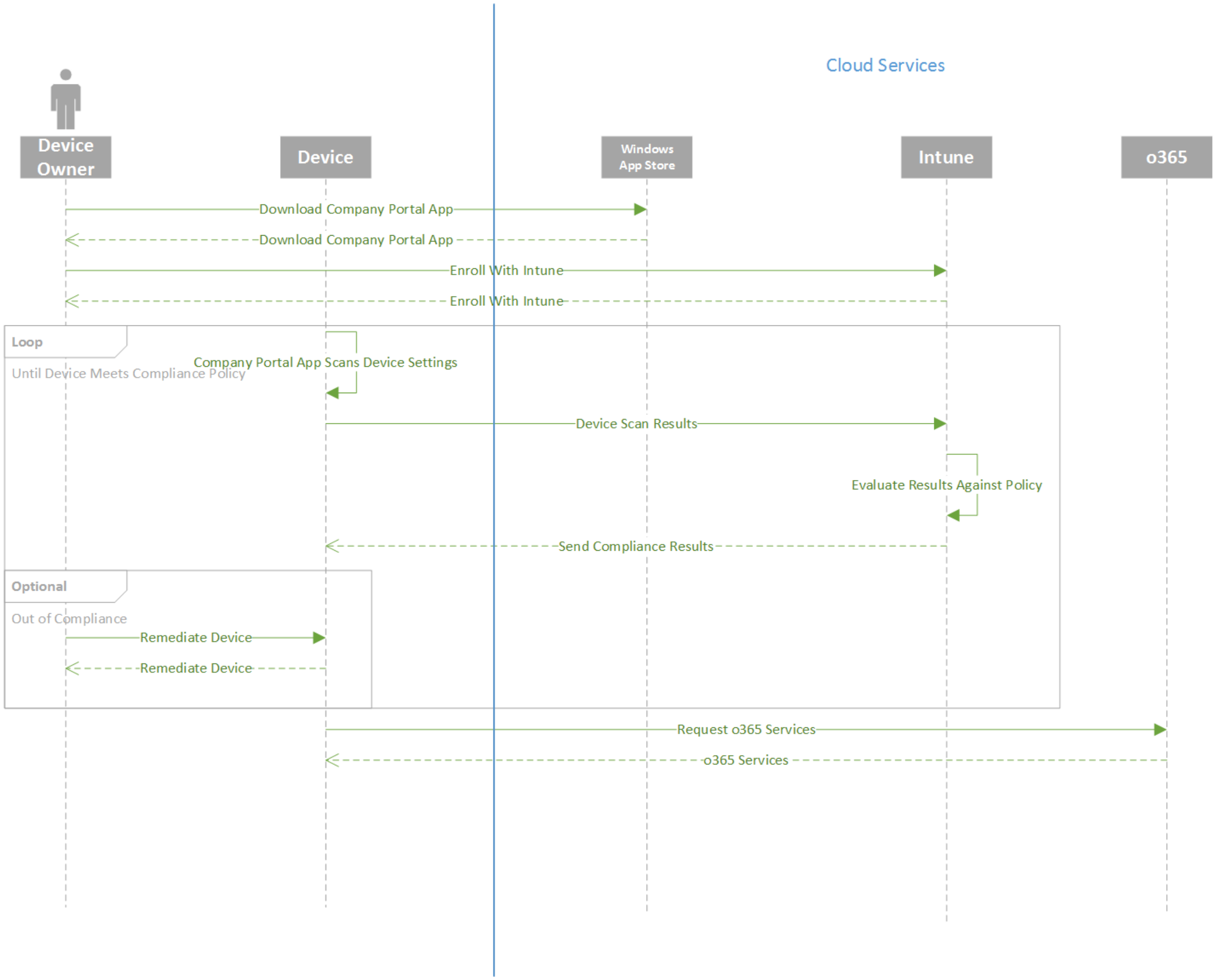


Figure 6.3 Windows Phone Workflow



6.2 The System Administrator’s Experience

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

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

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

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

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

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

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

7 Evaluation

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

7.1 Assumptions and Limitations

This security characteristic evaluation has the following limitations:

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

7.2 Testing

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

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

Table 7.1 Evaluation Objectives

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

Table 7.1 Evaluation Objectives (Continued)

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

Table 7.1 Evaluation Objectives (Continued)

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

7.3 Scenarios and Findings

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

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

7.3.1 Data Protection

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

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

Finally, the Outlook application provides an additional level of encryption. Microsoft protects the Outlook data via AES-128 encryption in cipher block chaining (CBC) mode utilizing Android's cryptography libraries. The iOS application-level encryption was not evaluated, as Microsoft indicated that information is encrypted via the OS cryptographic engine.

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

7.3.2 Data Isolation

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

7.3.3 Device Integrity

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

7.3.4 Monitoring

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

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

Finally, the Lookout MTP service provides monitoring of enrolled devices for malware risks on Android devices. In this build, the administrator periodically reviewed the status of enrolled devices in the enterprise through the MTP web console. More sophisticated notification systems, however, could be developed for larger deployments.

7.3.5 Identity and Authorization

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

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

Access attempts for devices not enrolled produced the following results:

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

7.3.6 Privacy Protection

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

8 Future Build Considerations

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

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

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

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

Some topics of interest for future builds include:

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

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

Appendix A Acronyms

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

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

Appendix B References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix C Security Characteristics and Capabilities

Table C.1 Security Characteristics and Capabilities

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

Table C.1 Security Characteristics and Capabilities (Continued)

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

Table C.1 Security Characteristics and Capabilities (Continued)

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-4c

MOBILE DEVICE SECURITY

Cloud and Hybrid Builds

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

List of Figures

List of Tables

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

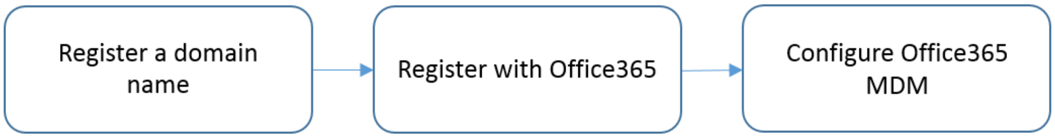
[1] https://www.icann.org/registrar-reports/accredited-list.html
[2] https://developer.apple.com/

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

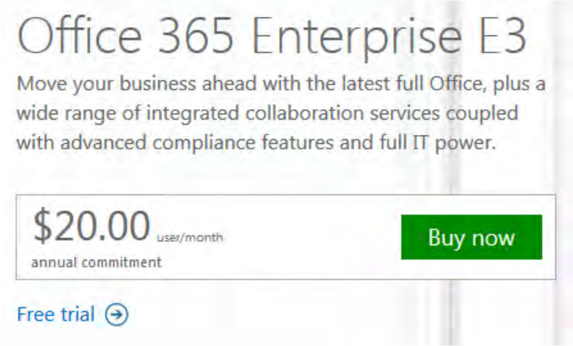


2.1.2 Office 365 Setup

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



Office 365 Enterprise E3

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

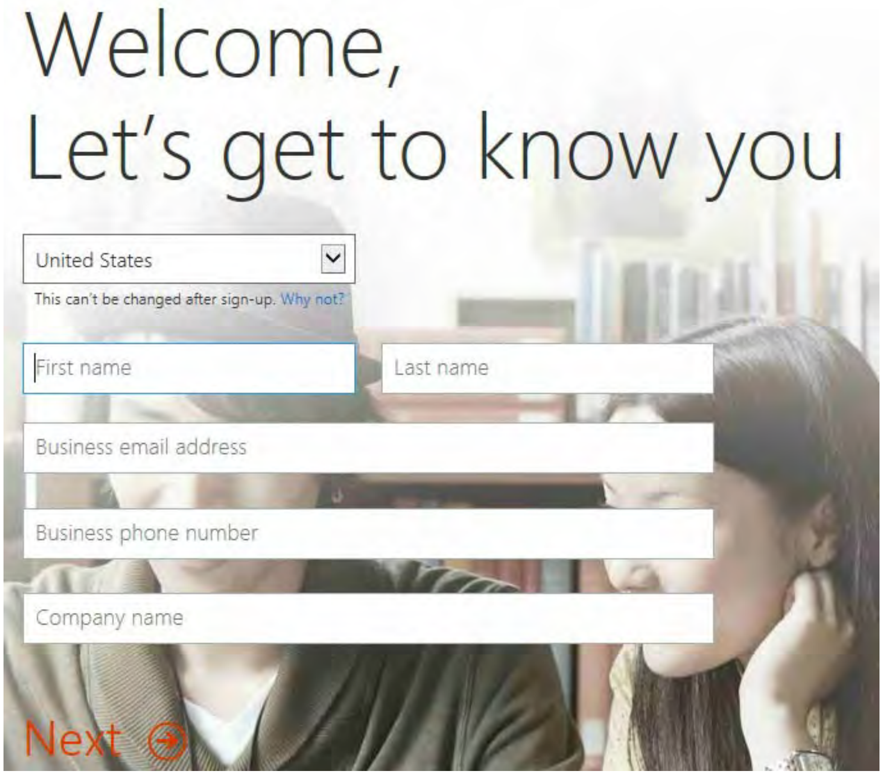
$20.00 user/month

annual commitment

Buy now

Free trial ➔

1. Choose a commitment level.



Welcome,
Let’s get to know you

United States

This can’t be changed after sign-up. Why not?

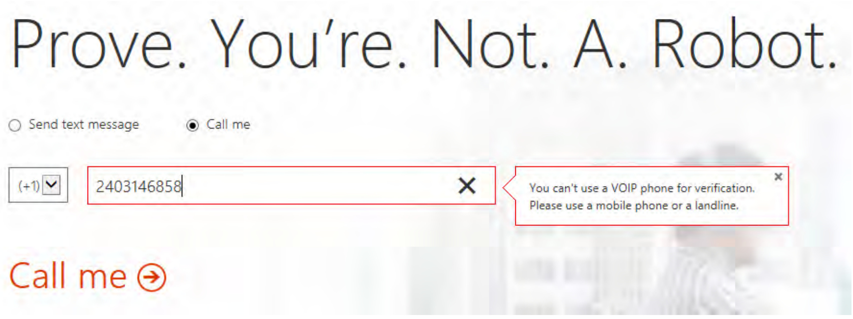
First name

Last name

Business email address

Business phone number

Company name

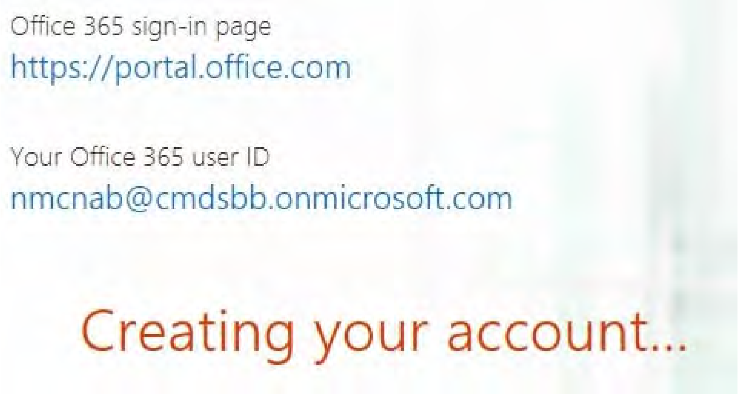


Prove. You’re. Not. A. Robot.

○ Send text message ● Call me

(+1) 2403146858

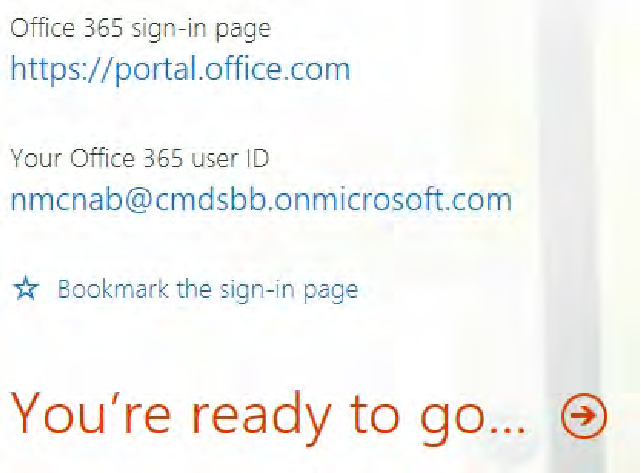
You can’t use a VOIP phone for verification. Please use a mobile phone or a landline.



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

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

Creating your account...



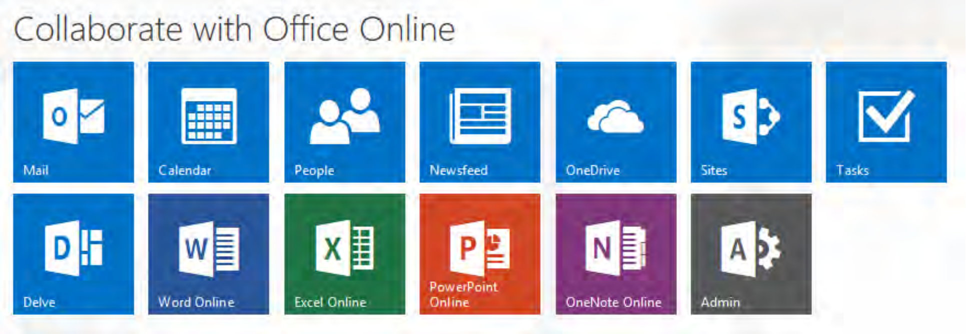
Office 365 sign-in page
https://portal.office.com

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

☆ Bookmark the sign-in page

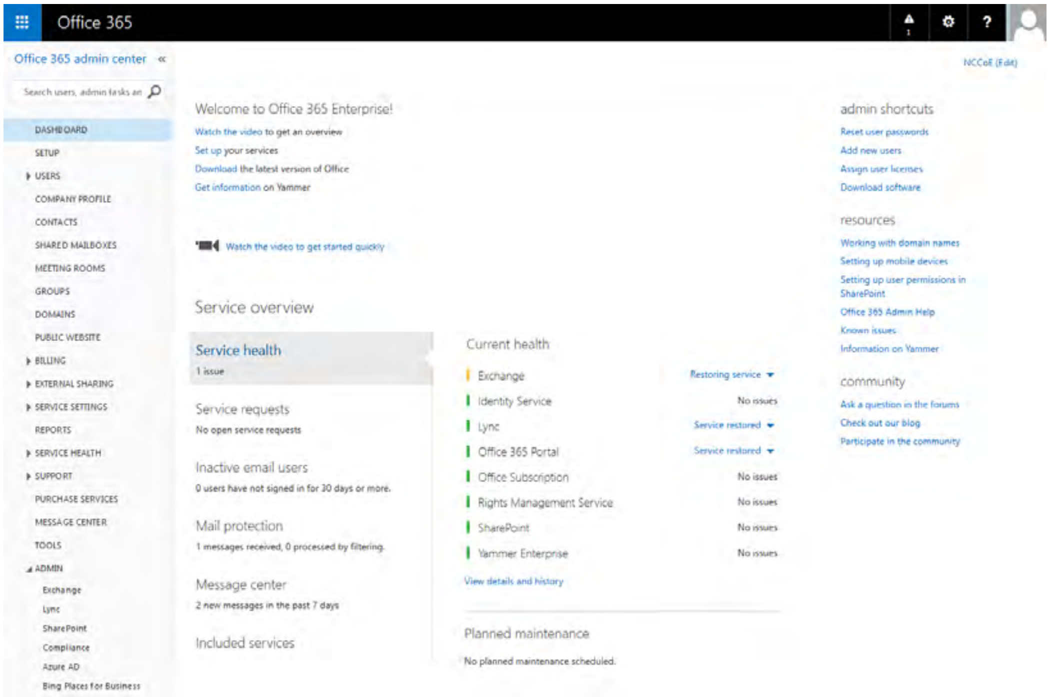
You're ready to go...

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



Collaborate with Office Online

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



Welcome to Office 365 Enterprise!

Watch the video to get an overview
Set up your services
Download the latest version of Office
Get information on Yammer

Watch the video to get started quickly

Service overview

Service health
1 issue

Service requests
No open service requests

Inactive email users
0 users have not signed in for 30 days or more.

Mail protection
1 messages received, 0 processed by filtering.

Message center
2 new messages in the past 7 days

Included services

Current health

Exchange	Restoring service
Identity Service	No issues
Lync	Service restored
Office 365 Portal	Service restored
Office Subscription	No issues
Rights Management Service	No issues
SharePoint	No issues
Yammer Enterprise	No issues

View details and history

Planned maintenance

No planned maintenance scheduled.

admin shortcuts

Reset user passwords
Add new users
Assign user licenses
Download software

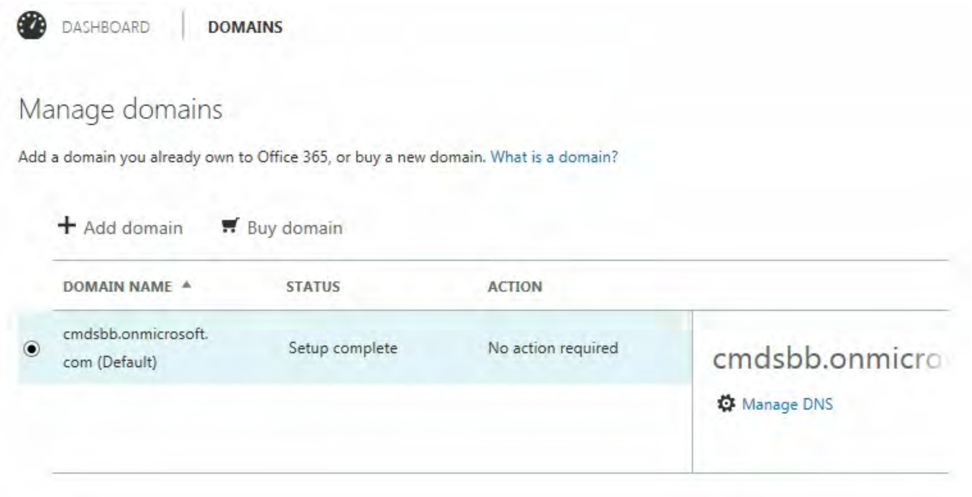
resources

Working with domain names
Setting up mobile devices
Setting up user permissions in SharePoint
Office 365 Admin Help
Known issues
Information on Yammer

community

Ask a question in the forums
Check out our blog
Participate in the community

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



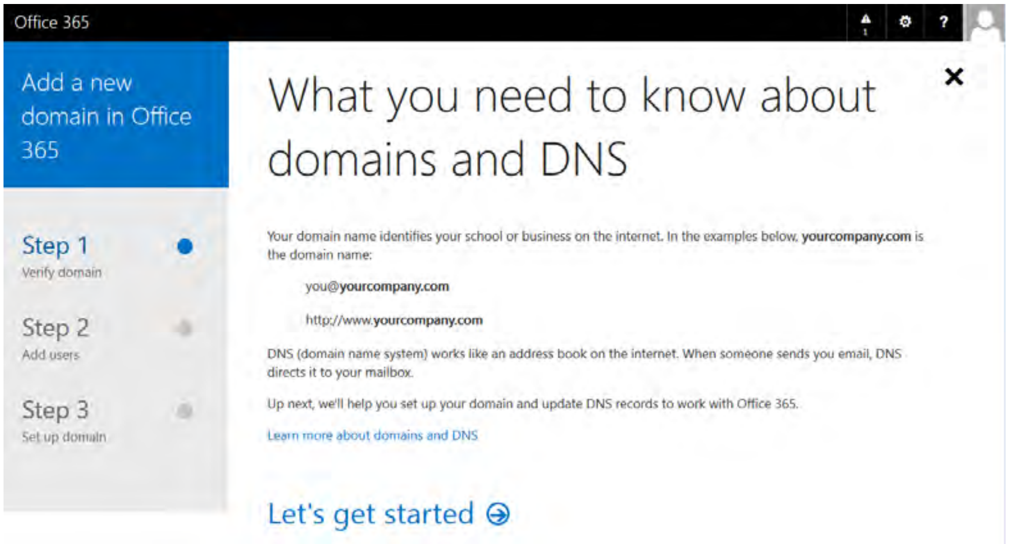
Manage domains

Add a domain you already own to Office 365, or buy a new domain. What is a domain?

	DOMAIN NAME ▲	STATUS	ACTION
●	cmdsbb.onmicrosoft.com (Default)	Setup complete	No action required

cmdsbb.onmicro

5. Choose **Add domain**.



What you need to know about domains and DNS

Your domain name identifies your school or business on the internet. In the examples below, **yourcompany.com** is the domain name:

you@**yourcompany.com**

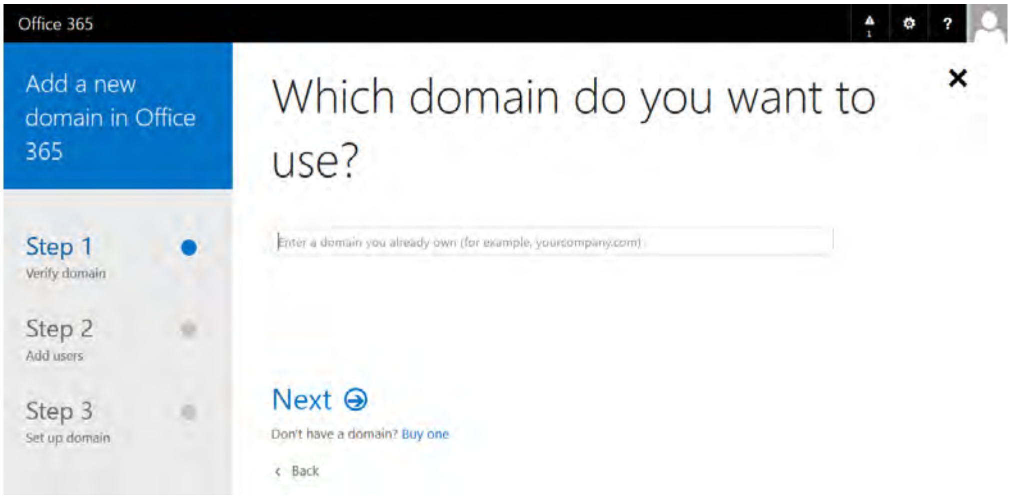
http://www.**yourcompany.com**

DNS (domain name system) works like an address book on the internet. When someone sends you email, DNS directs it to your mailbox.

Up next, we'll help you set up your domain and update DNS records to work with Office 365.

Learn more about domains and DNS

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

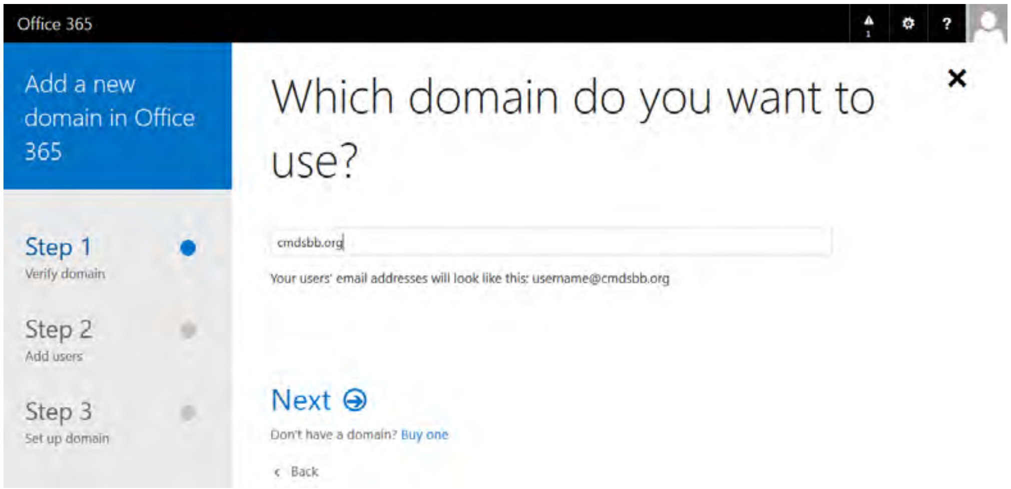


Which domain do you want to use?

Enter a domain you already own (for example, yourcompany.com)

Don't have a domain? Buy one

7. Enter your public domain name.



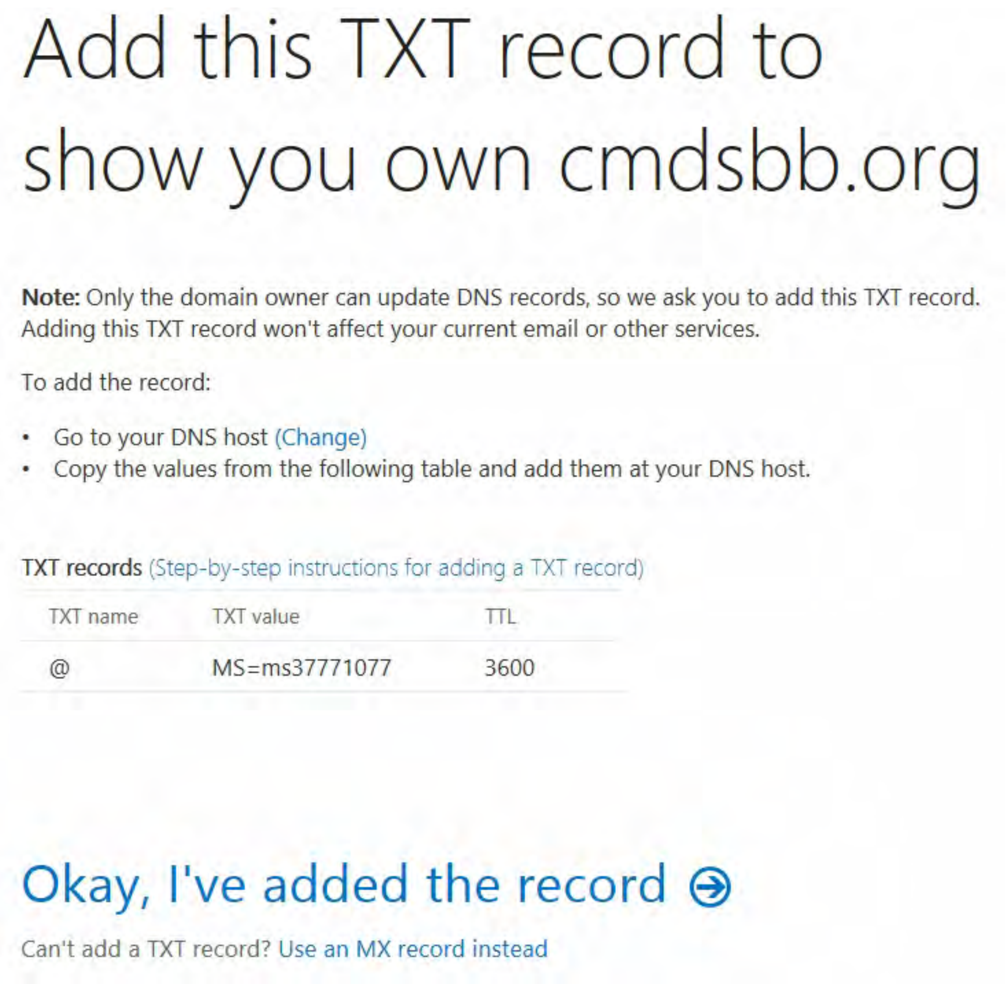
Which domain do you want to use?

cmdsbb.org

Your users' email addresses will look like this: username@cmdsbb.org

Don't have a domain? Buy one

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.

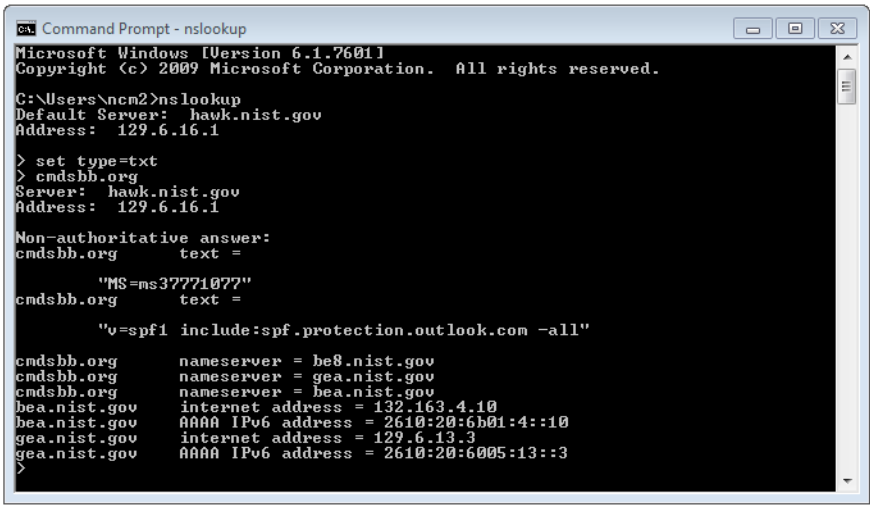
TXT records (Step-by-step instructions for adding a TXT record)

TXT name	TXT value	TTL
@	MS=ms37771077	3600

Okay, I've added the record ➔

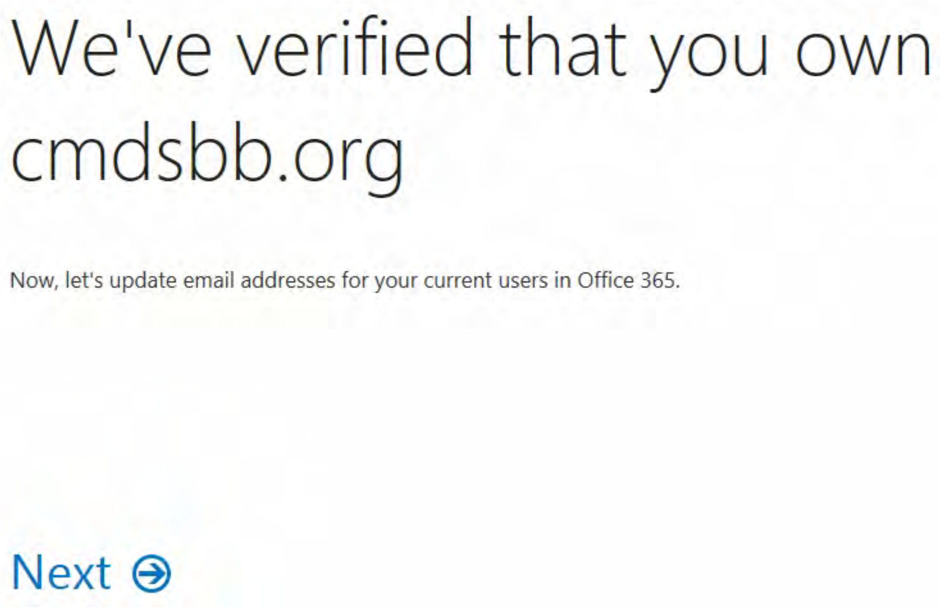
Can't add a TXT record? Use an MX record instead

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



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\ncm2>nslookup
Default Server:  hawk.nist.gov
Address:  129.6.16.1

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

Non-authoritative answer:
cmdsbb.org      text =

        "MS=ms37771077"
cmdsbb.org      text =

        "v=spf1 include:spf.protection.outlook.com -all"

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

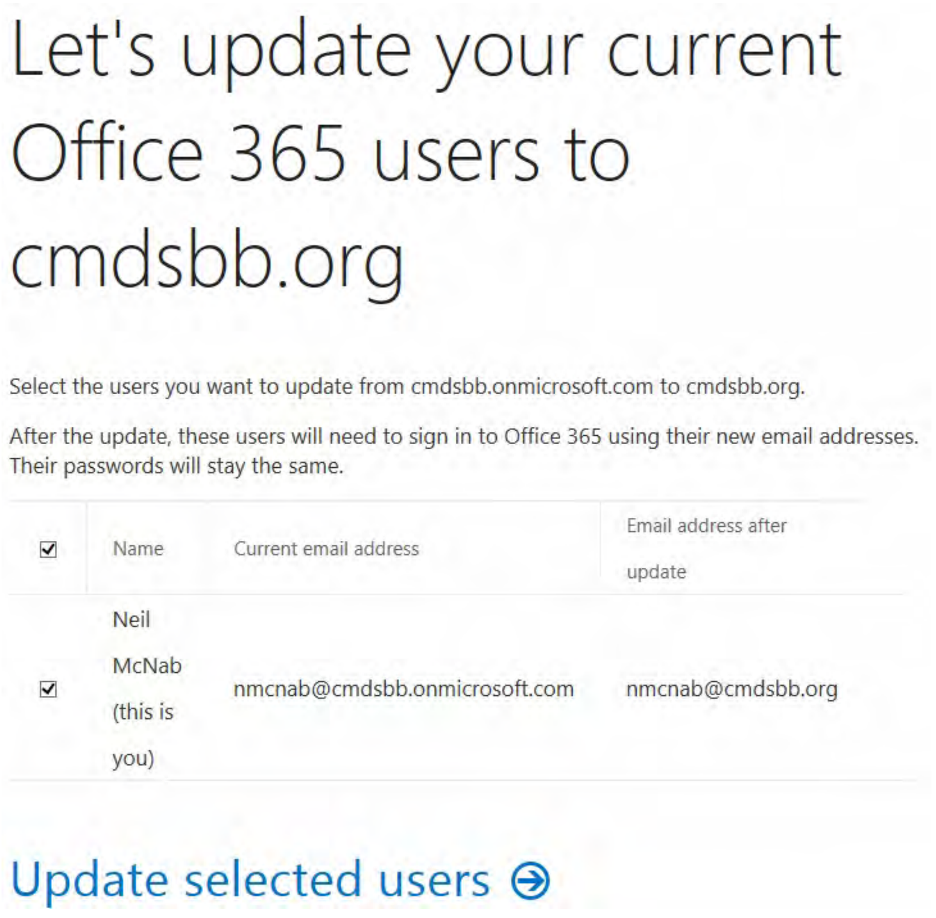
10. Verify the Domain Name Service (DNS) settings. The TXT record should match what was presented in the previous step. Note that it may take several minutes for the record to propagate to the Office 365 DNS servers.



We've verified that you own cmdsbb.org

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

11. Choose **Next**.



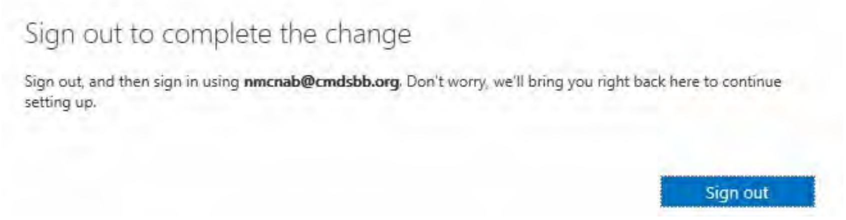
Let's update your current Office 365 users to cmdsbb.org

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

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

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

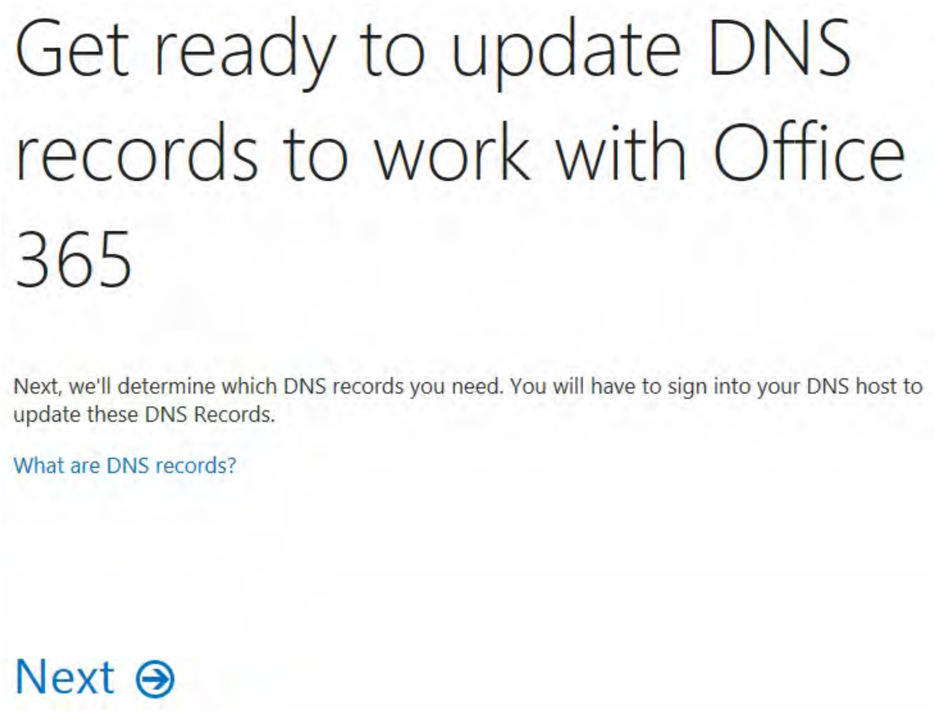
12. Choose **Update selected users**.



Sign out to complete the change

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

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

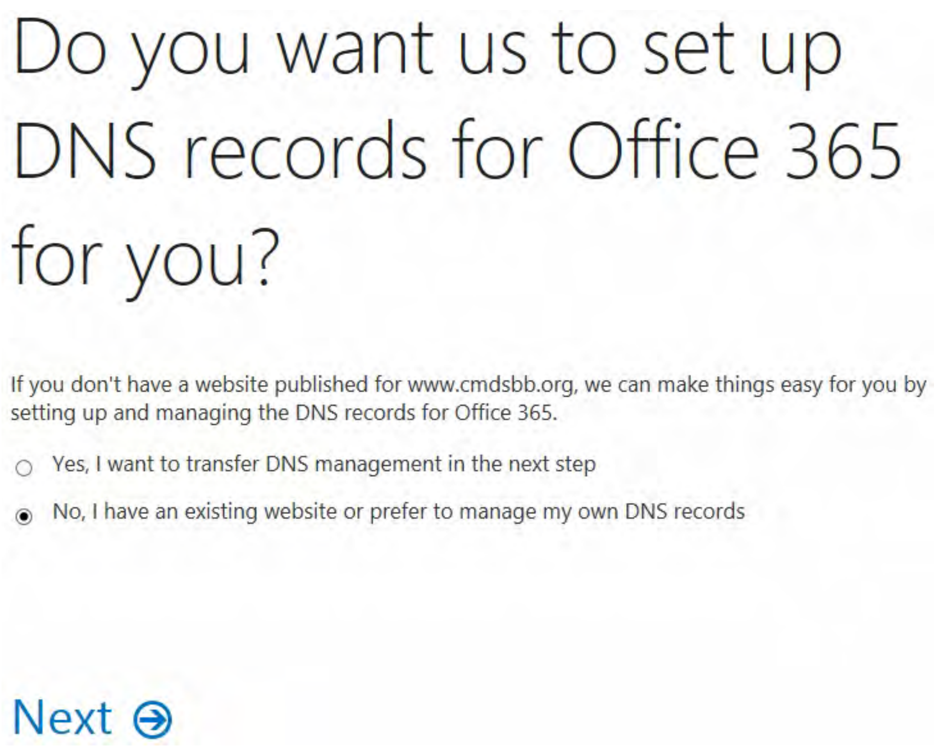


Get ready to update DNS records to work with Office 365

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

What are DNS records?

14. Choose **Next**.



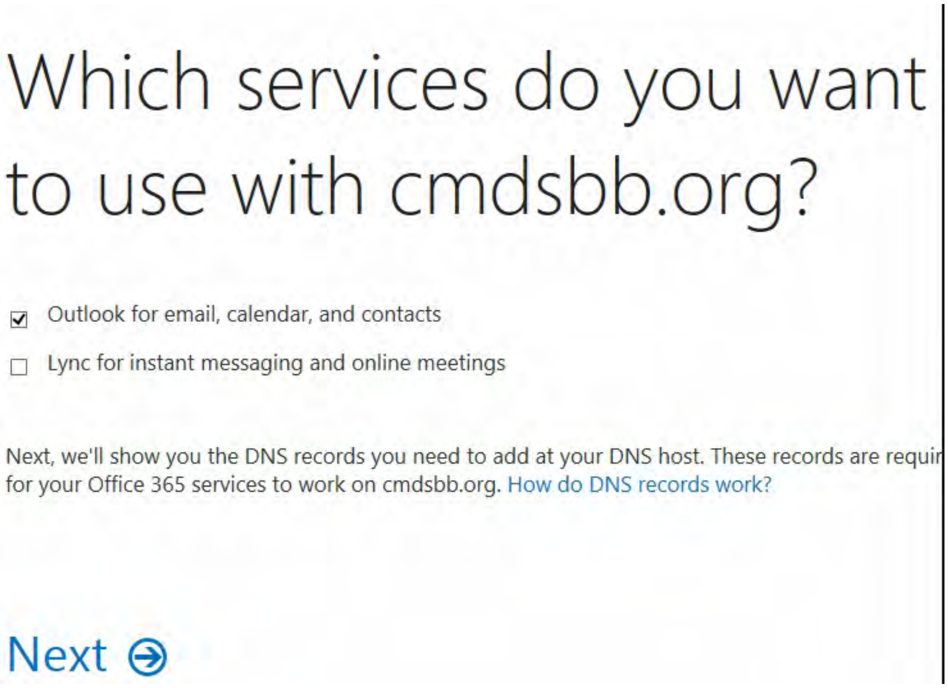
Do you want us to set up DNS records for Office 365 for you?

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

○ Yes, I want to transfer DNS management in the next step

● No, I have an existing website or prefer to manage my own DNS records

15. Choose **Next**.



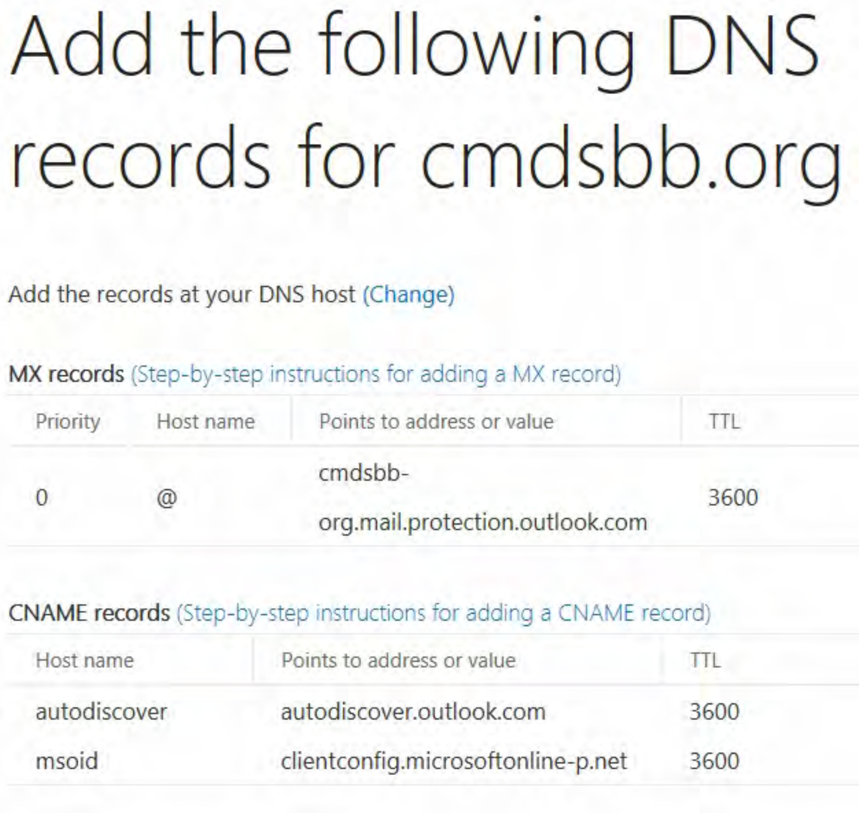
Which services do you want to use with cmdsbb.org?

☑ Outlook for email, calendar, and contacts

□ Lync for instant messaging and online meetings

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

16. Choose **Next**.



Add the following DNS records for cmdsbb.org

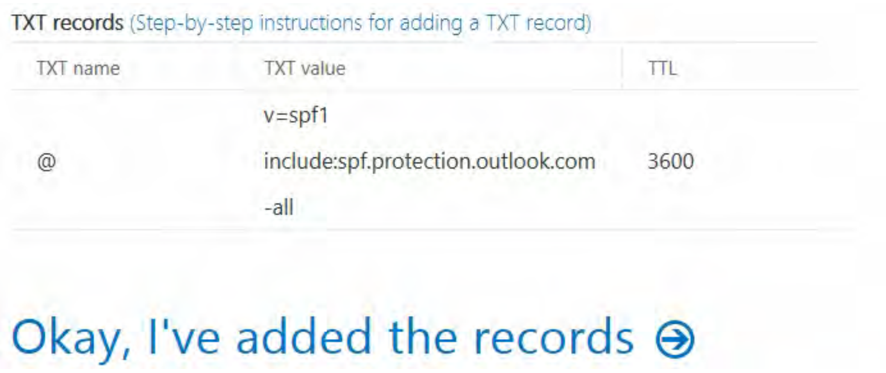
Add the records at your DNS host (Change)

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

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

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

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



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

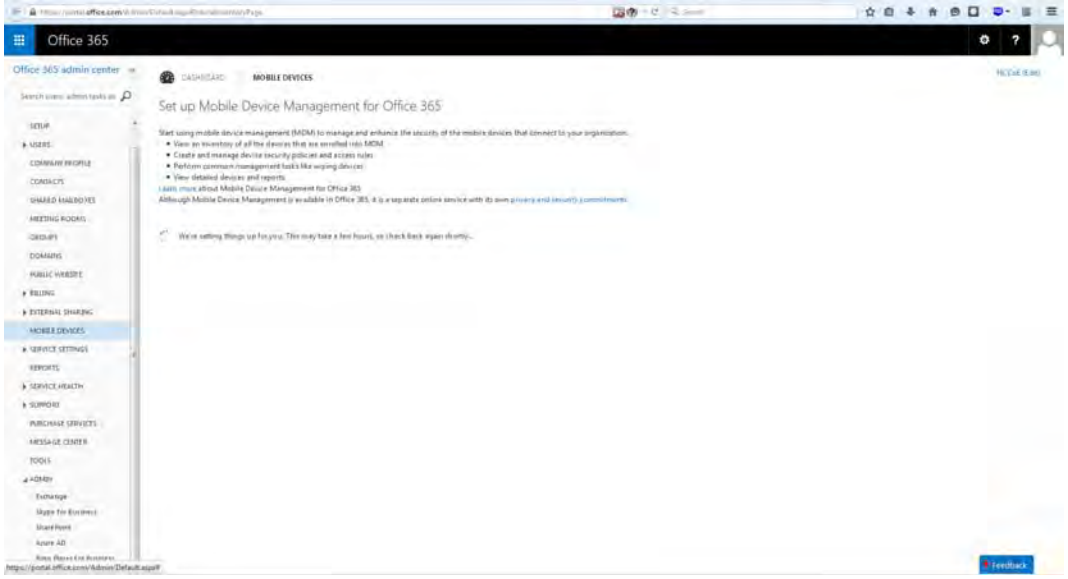
TXT name	TXT value	TTL
@	v=spf1 include:spf.protection.outlook.com -all	3600

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



Set up Mobile Device Management for Office 365

Start using mobile device management (MDM) to manage and enhance the security of the mobile devices that connect to your organization.

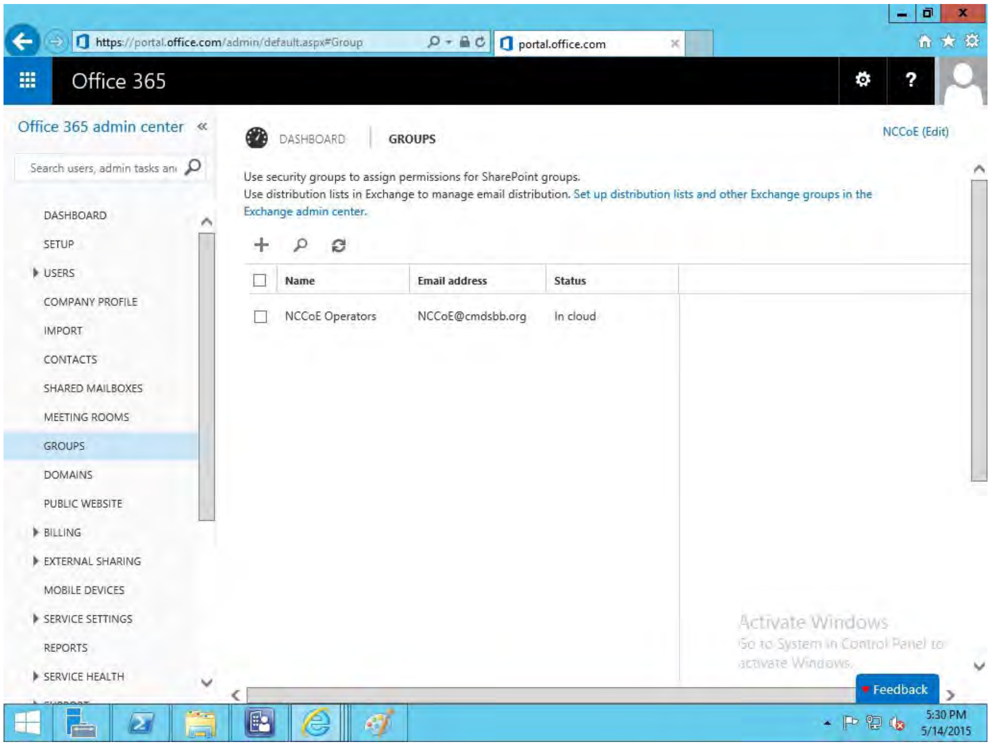
- View an inventory of all the devices that are enrolled into MDM
- Create and manage device security policies and access rules
- Perform common management tasks like wiping devices
- View detailed devices and reports

Learn more about Mobile Device Management for Office 365

Although Mobile Device Management is available in Office 365, it is a separate online service with its own privacy and security commitments.

We're setting things up for you. This may take a few hours, so check back again shortly...

1. Choose **Get Started**.

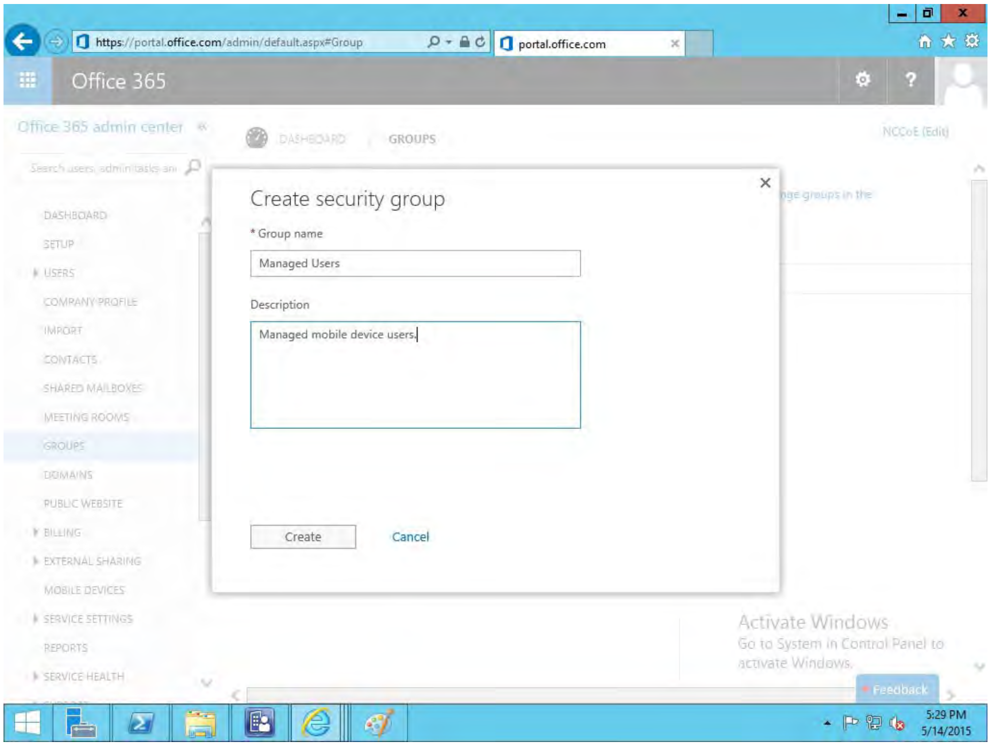


https://portal.office.com/admin/default.aspx#Group

Use security groups to assign permissions for SharePoint groups.
Use distribution lists in Exchange to manage email distribution. Set up distribution lists and other Exchange groups in the Exchange admin center.

Name	Email address	Status
NCCoE Operators	NCCoE@cmdsbb.org	In cloud

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 -> +**.

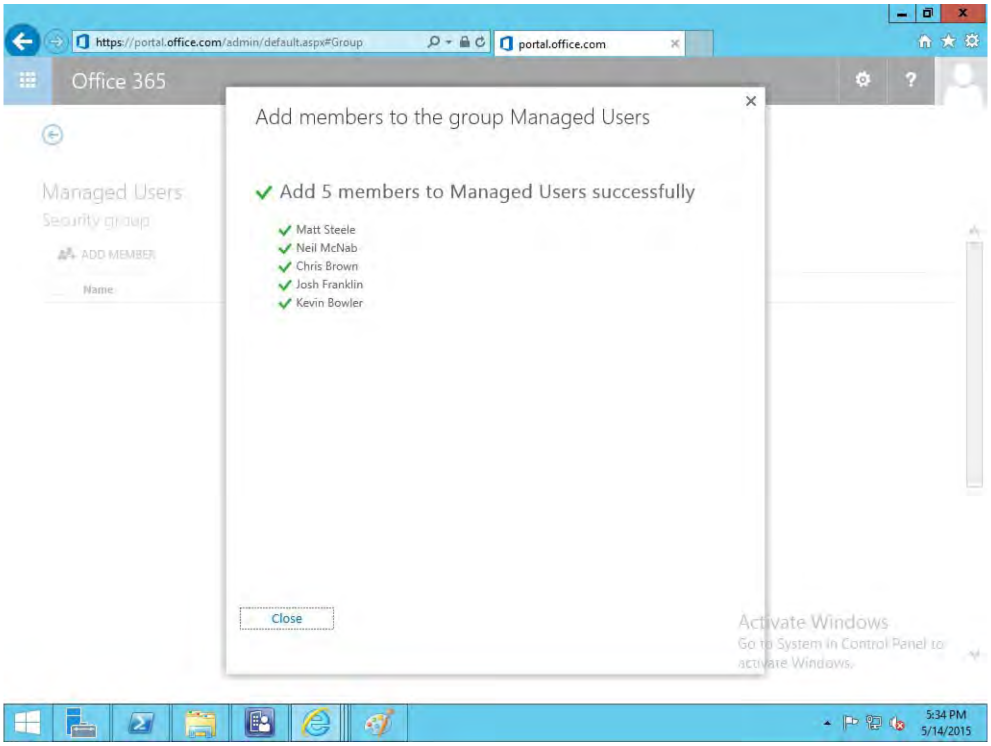


Create security group

* Group name: Managed Users

Description: Managed mobile device users.

3. Add a title and description for the group.

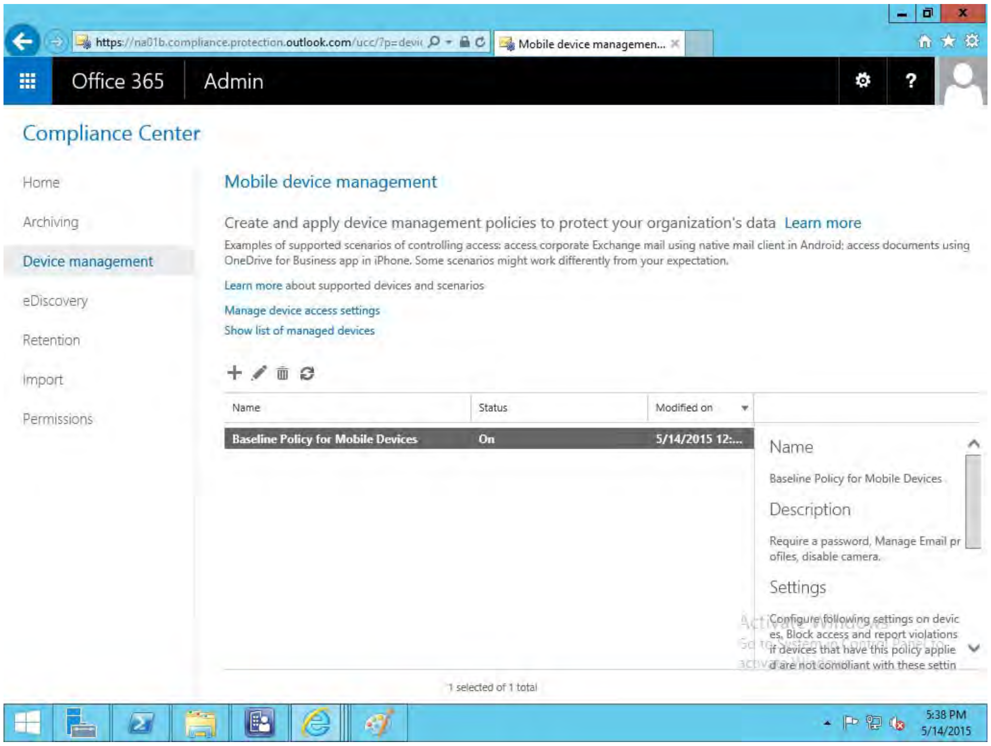


Add members to the group Managed Users

✓ Add 5 members to Managed Users successfully

- ✓ Matt Steele
- ✓ Neil McNab
- ✓ Chris Brown
- ✓ Josh Franklin
- ✓ Kevin Bowler

4. Add members to the group to be managed.



Mobile device management

Create and apply device management policies to protect your organization's data Learn more

Examples of supported scenarios of controlling access: access corporate Exchange mail using native mail client in Android; access documents using OneDrive for Business app in iPhone. Some scenarios might work differently from your expectation.

Learn more about supported devices and scenarios

Manage device access settings

Show list of managed devices

Name	Status	Modified on
Baseline Policy for Mobile Devices	On	5/14/2015 12:...

Name

Baseline Policy for Mobile Devices

Description

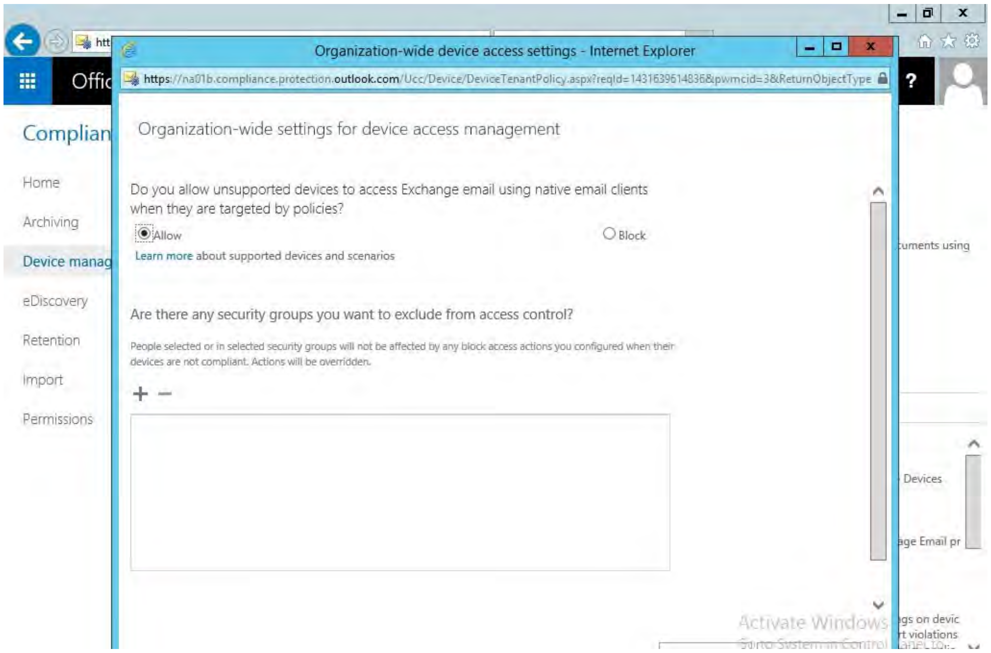
Require a password, Manage Email profiles, disable camera.

Settings

Configure following settings on devices. Block access and report violations if devices that have this policy applied are not compliant with these settin

1 selected of 1 total

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



Organization-wide device access settings - Internet Explorer

https://na01b.compliance.protection.outlook.com/Ucc/Device/DeviceTenantPolicy.aspx?reqId=1431639614836&pwmcid=3&ReturnObjectType

Organization-wide settings for device access management

Do you allow unsupported devices to access Exchange email using native email clients when they are targeted by policies?

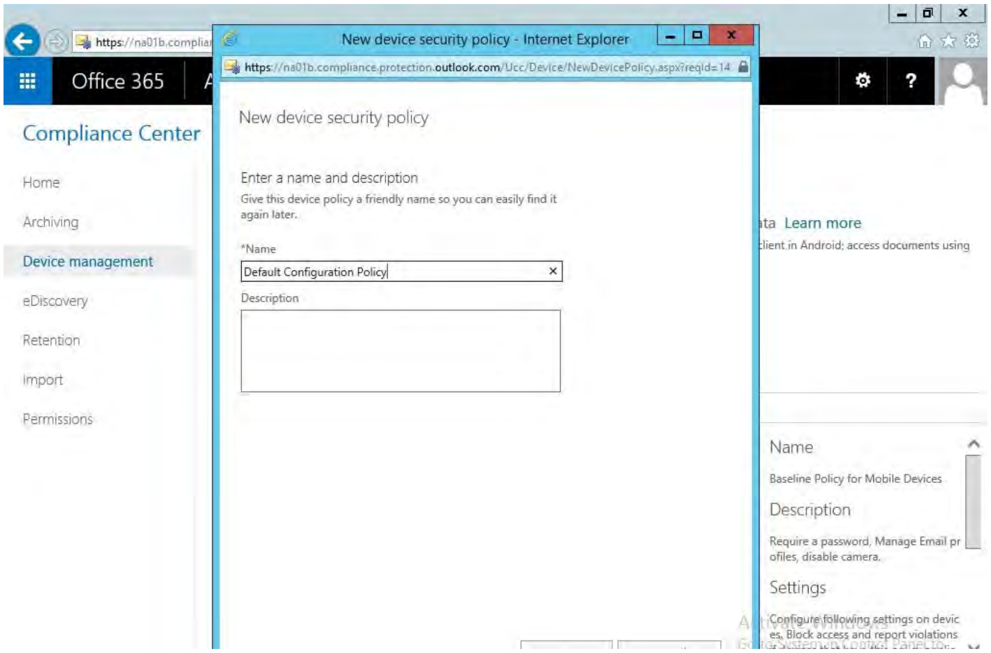
● Allow ○ Block

Learn more about supported devices and scenarios

Are there any security groups you want to exclude from access control?

People selected or in selected security groups will not be affected by any block access actions you configured when their devices are not compliant. Actions will be overridden.

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



New device security policy - Internet Explorer

https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqId=14

New device security policy

Enter a name and description

Give this device policy a friendly name so you can easily find it again later.

*Name

Default Configuration Policy

Description

Name

Baseline Policy for Mobile Devices

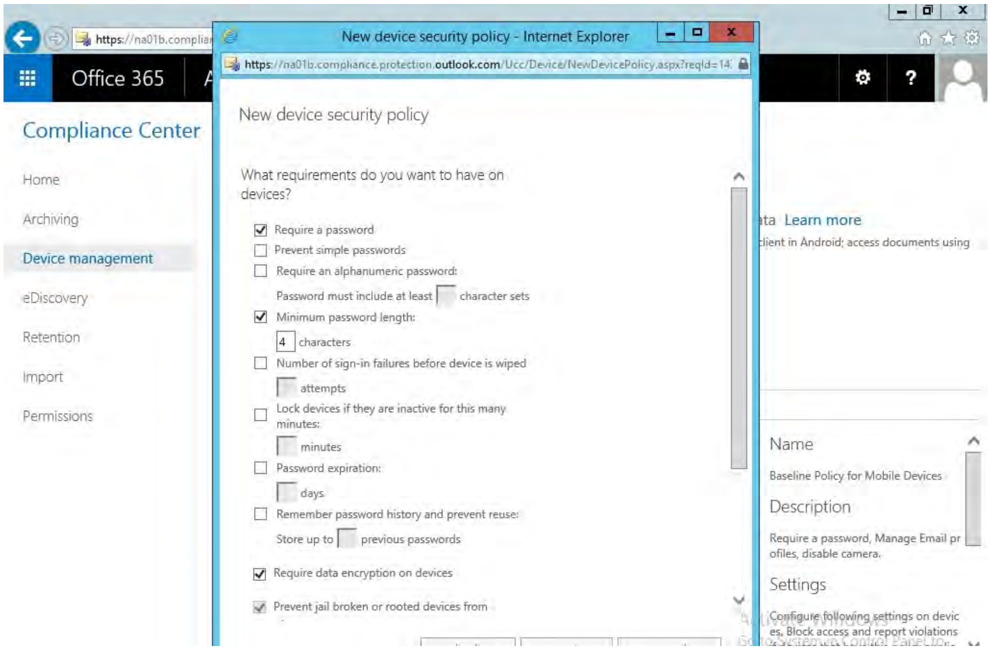
Description

Require a password, Manage Email profiles, disable camera.

Settings

Configure following settings on devices, Block access and report violations

7. Set the name for the device policy.


New device security policy - Internet Explorer
https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqId=14
Office 365
Compliance Center
Home
Archiving
Device management
eDiscovery
Retention
Import
Permissions
Learn more

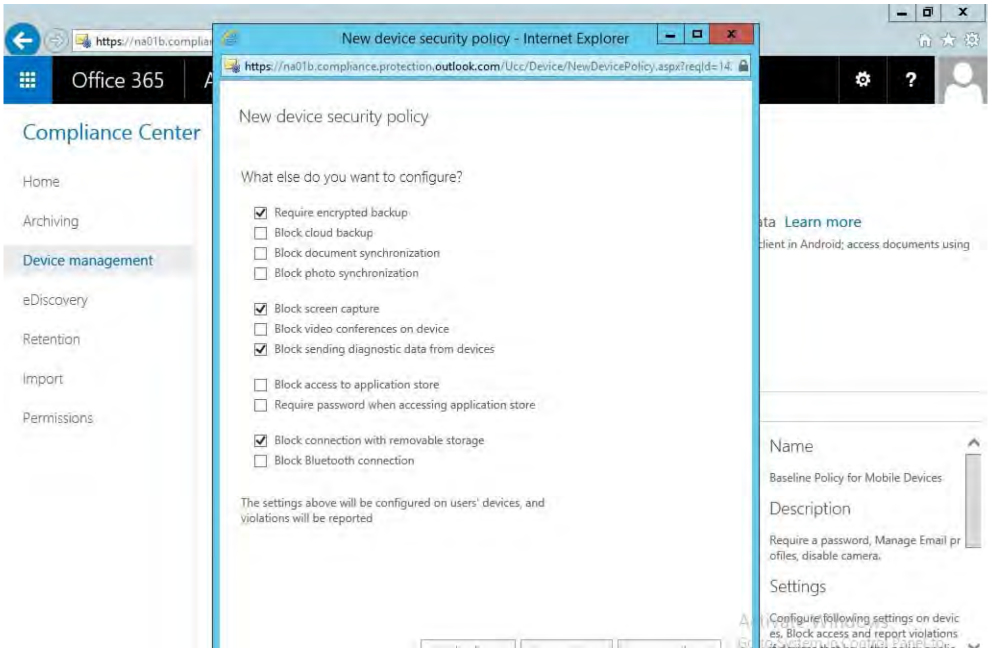
New device security policy

What requirements do you want to have on devices?

☑ Require a password
☐ Prevent simple passwords
☐ Require an alphanumeric password:
Password must include at least ☐ character sets
☑ Minimum password length:
4 characters
☐ Number of sign-in failures before device is wiped
☐ attempts
☐ Lock devices if they are inactive for this many minutes:
☐ minutes
☐ Password expiration:
☐ days
☐ Remember password history and prevent reuse:
Store up to ☐ previous passwords
☑ Require data encryption on devices
☑ Prevent jail broken or rooted devices from

Name
Baseline Policy for Mobile Devices
Description
Require a password, Manage Email profiles, disable camera.
Settings
Configure following settings on devices, Block access and report violations

8. Set rules for the device policy.


New device security policy - Internet Explorer
https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqId=14
Office 365
Compliance Center
Home
Archiving
Device management
eDiscovery
Retention
Import
Permissions
Learn more

New device security policy

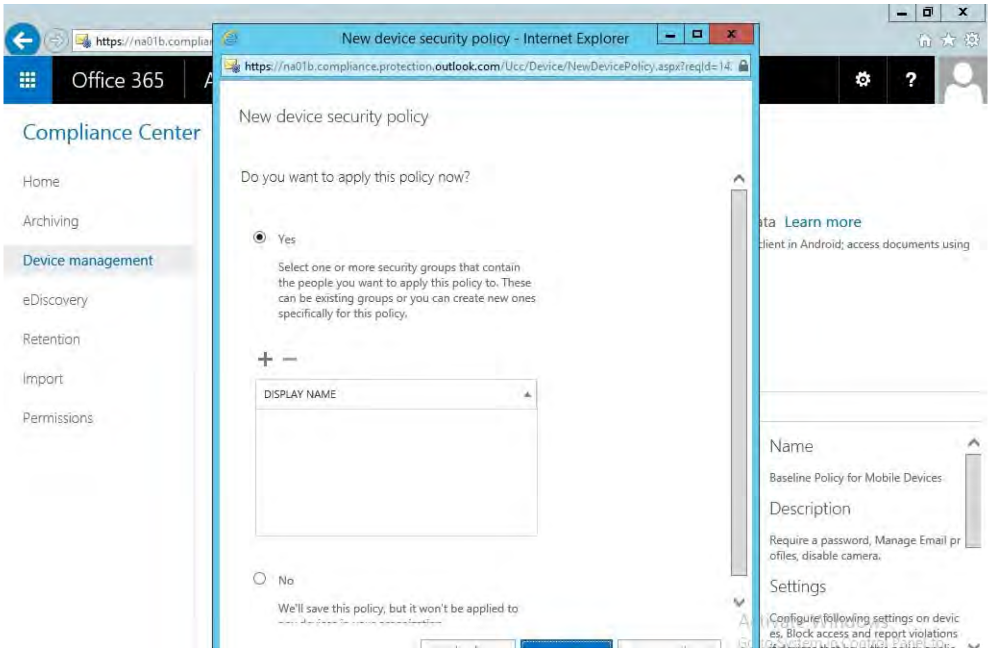
What else do you want to configure?

☑ Require encrypted backup
☐ Block cloud backup
☐ Block document synchronization
☐ Block photo synchronization
☑ Block screen capture
☐ Block video conferences on device
☑ Block sending diagnostic data from devices
☐ Block access to application store
☐ Require password when accessing application store
☑ Block connection with removable storage
☐ Block Bluetooth connection

The settings above will be configured on users' devices, and violations will be reported

Name
Baseline Policy for Mobile Devices
Description
Require a password, Manage Email profiles, disable camera.
Settings
Configure following settings on devices, Block access and report violations

9. Set additional hardware restrictions.



New device security policy - Internet Explorer

https://na01b.compliance.protection.outlook.com/Ucc/Device/NewDevicePolicy.aspx?reqId=14

New device security policy

Do you want to apply this policy now?

● Yes

Select one or more security groups that contain the people you want to apply this policy to. These can be existing groups or you can create new ones specifically for this policy.

+ −

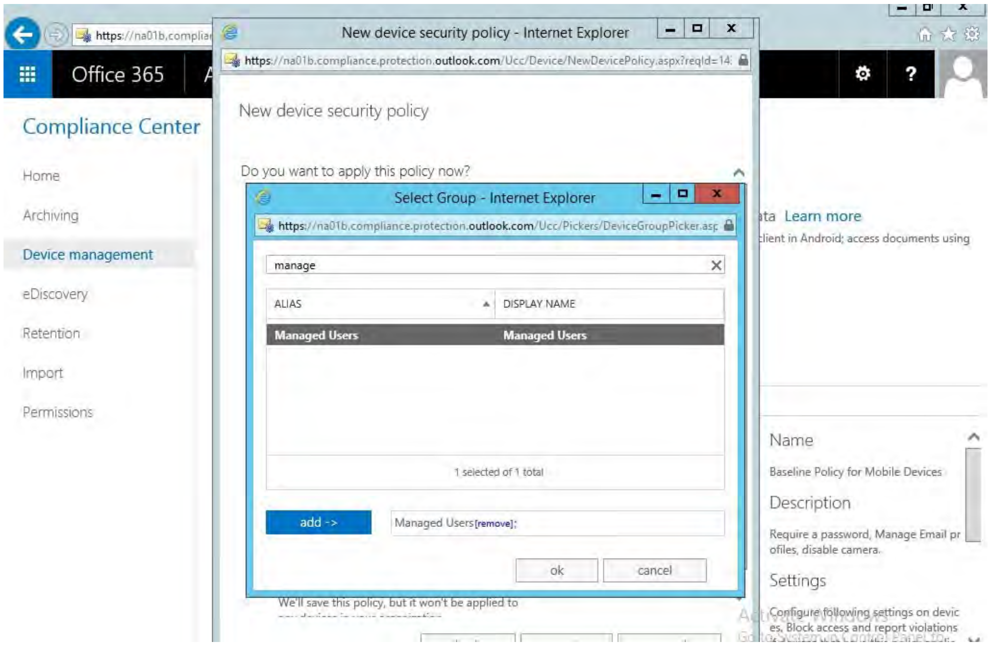
DISPLAY NAME

○ No

We'll save this policy, but it won't be applied to

Office 365
Compliance Center
Home
Archiving
Device management
eDiscovery
Retention
Import
Permissions
Learn more
Name
Baseline Policy for Mobile Devices
Description
Require a password, Manage Email profiles, disable camera.
Settings
Configure following settings on devices, Block access and report violations

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



Select Group - Internet Explorer

https://na01b.compliance.protection.outlook.com/Ucc/Pickers/DeviceGroupPicker.asp

manage

ALIAS	DISPLAY NAME
Managed Users	Managed Users

1 selected of 1 total

add -> Managed Users[remove];

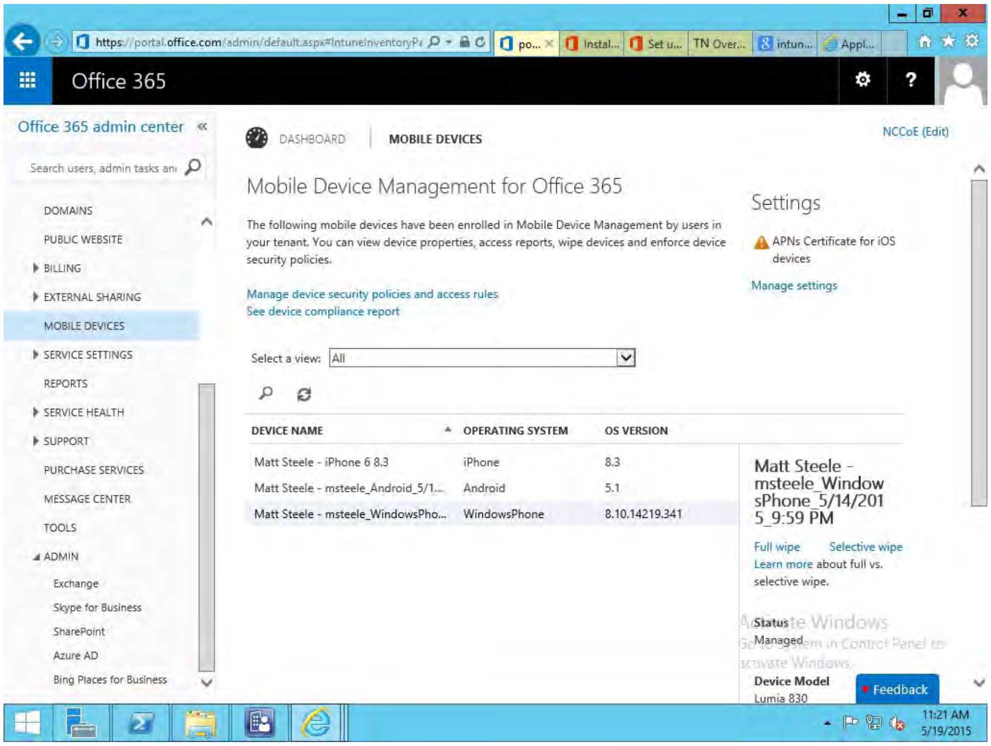
ok cancel

New device security policy - Internet Explorer
New device security policy
Do you want to apply this policy now?
Office 365
Compliance Center
Home
Archiving
Device management
eDiscovery
Retention
Import
Permissions
Learn more
Name
Baseline Policy for Mobile Devices
Description
Require a password, Manage Email profiles, disable camera.
Settings
Configure following settings on devices, Block access and report violations

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

2.1.3.1 Configure Push Certificate for iOS Devices

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



https://portal.office.com/admin/default.aspx#IntuneInventoryPa

Office 365

Office 365 admin center

Search users, admin tasks and

DOMAINS
PUBLIC WEBSITE
BILLING
EXTERNAL SHARING
MOBILE DEVICES
SERVICE SETTINGS
REPORTS
SERVICE HEALTH
SUPPORT
PURCHASE SERVICES
MESSAGE CENTER
TOOLS
ADMIN
Exchange
Skype for Business
SharePoint
Azure AD
Bing Places for Business

DASHBOARD | MOBILE DEVICES

NCCoE (Edit)

Mobile Device Management for Office 365

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

Manage device security policies and access rules
See device compliance report

Settings

⚠ APNs Certificate for iOS devices

Manage settings

Select a view: All

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

Matt Steele - msteele_WindowsPhone_5/14/2015_9:59 PM

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

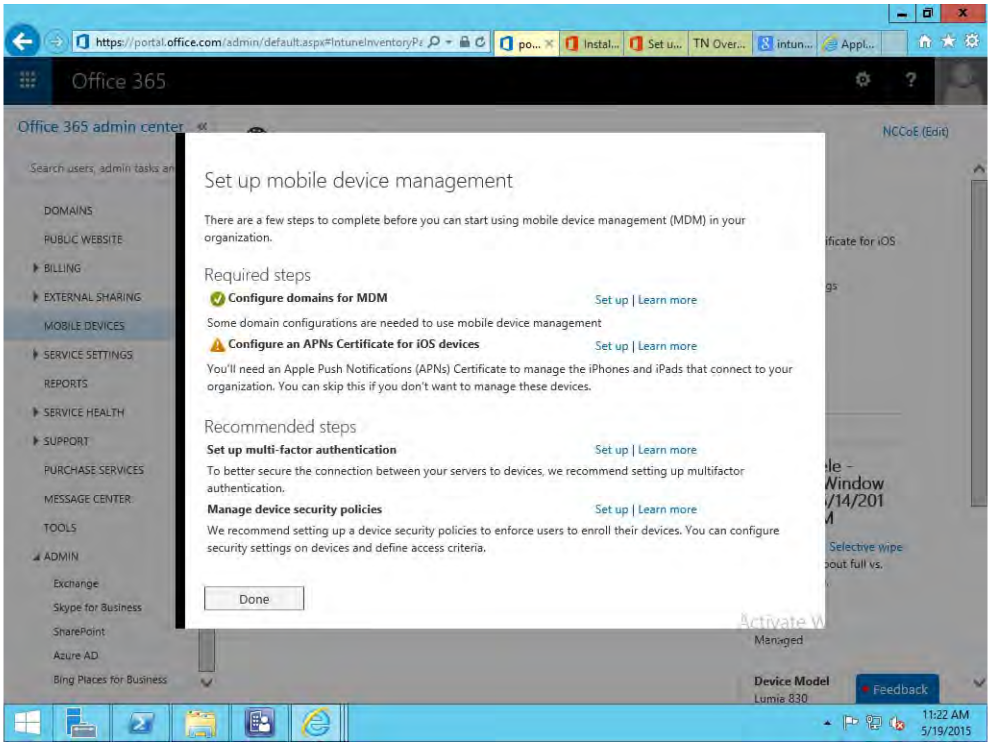
Status
Managed

Device Model
Lumia 830

Feedback

11:21 AM
5/19/2015

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



Set up mobile device management

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

Required steps

✓ **Configure domains for MDM** Set up | Learn more

Some domain configurations are needed to use mobile device management

⚠ **Configure an APNs Certificate for iOS devices** Set up | Learn more

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

Recommended steps

Set up multi-factor authentication Set up | Learn more

To better secure the connection between your servers to devices, we recommend setting up multifactor authentication.

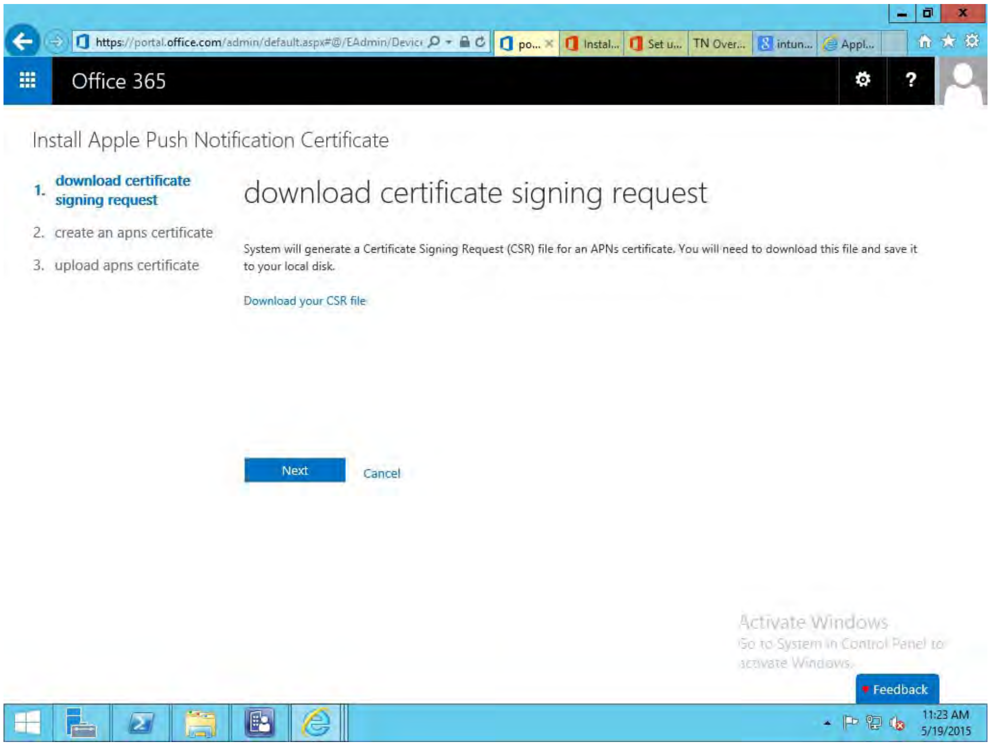
Manage device security policies Set up | Learn more

We recommend setting up a device security policies to enforce users to enroll their devices. You can configure security settings on devices and define access criteria.

Done

11:22 AM
5/19/2015

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



https://portal.office.com/admin/default.aspx#@/EAdmin/Devic
po...
Instal...
Set u...
TN Over...
intun...
Appl...
Office 365
?
Activate Windows
Go to System in Control Panel to activate Windows.
Feedback
11:23 AM
5/19/2015

Install Apple Push Notification Certificate

1. download certificate signing request
2. create an apns certificate
3. upload apns certificate

download certificate signing request

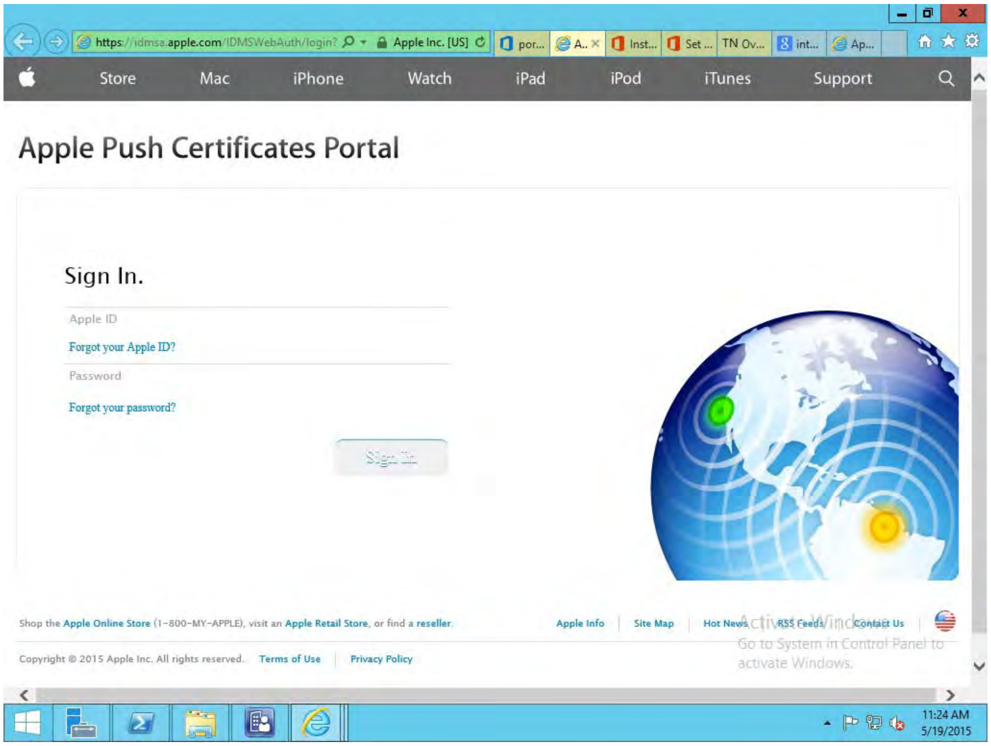
System will generate a Certificate Signing Request (CSR) file for an APNs certificate. You will need to download this file and save it to your local disk.

Download your CSR file

Next Cancel

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.

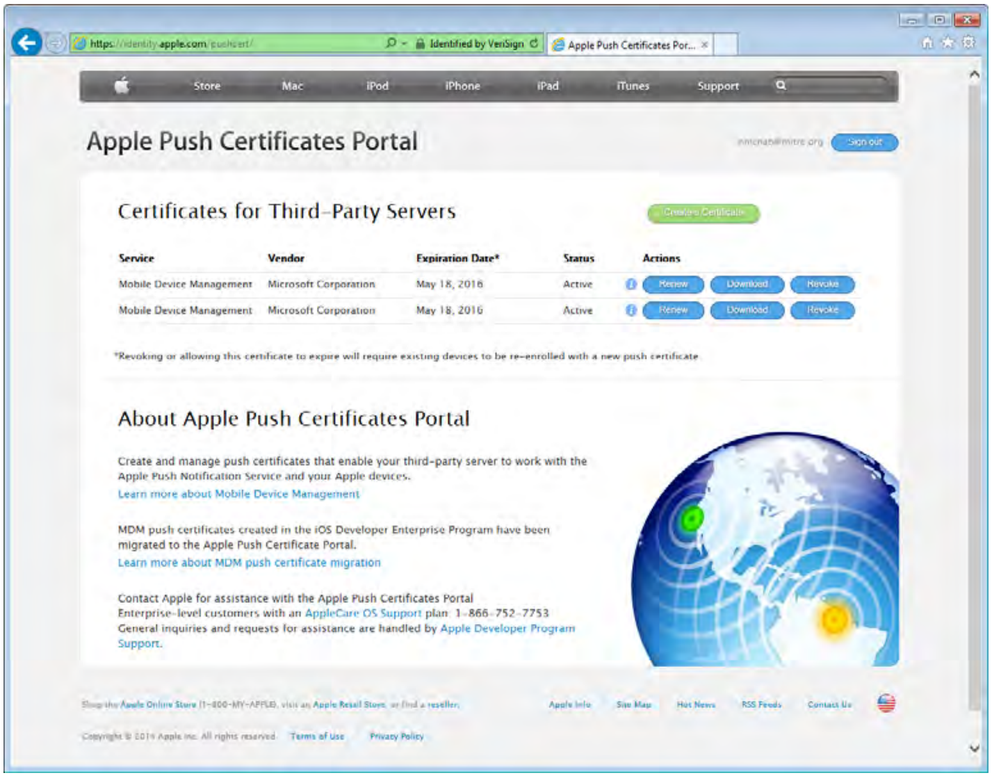


Apple Push Certificates Portal

Sign In.

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Copyright © 2015 Apple Inc. All rights reserved. Terms of Use Privacy Policy



Apple Push Certificates Portal

Certificates for Third-Party Servers

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

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

About Apple Push Certificates Portal

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

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

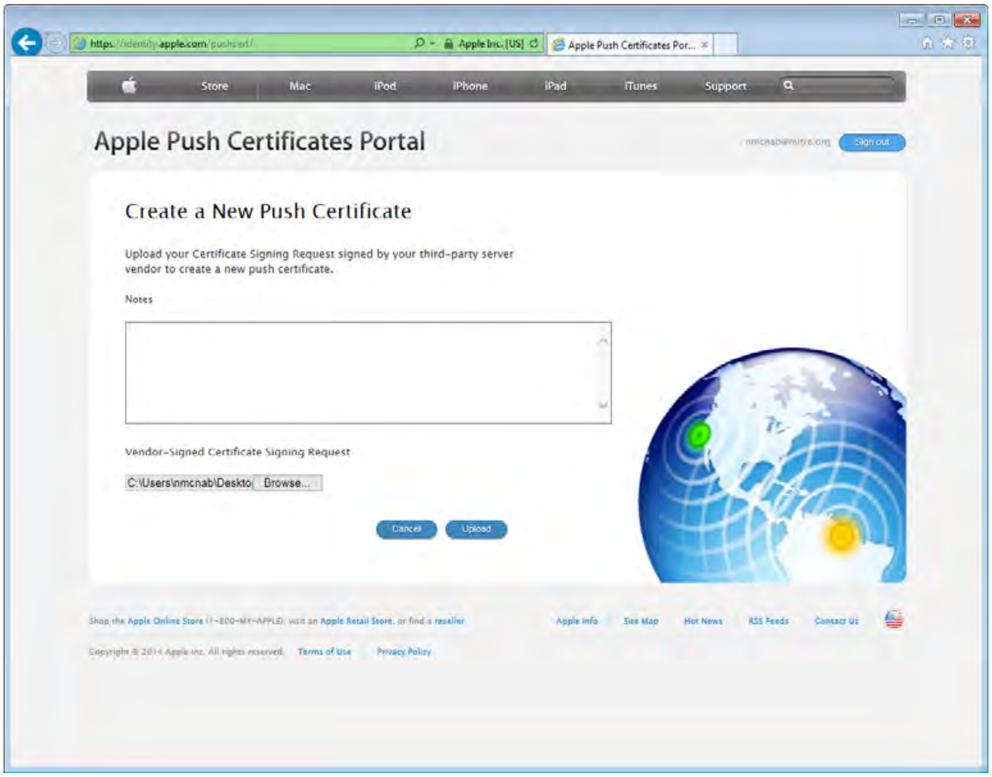
Contact Apple for assistance with the Apple Push Certificates Portal
Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
General inquiries and requests for assistance are handled by Apple Developer Program Support.

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use Privacy Policy

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

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



https://identity.apple.com/pushcert/
Apple Inc. [US]
Apple Push Certificates Por...
Store
Mac
iPod
iPhone
iPad
iTunes
Support
nmcnab@mitre.org
Sign out
Browse...
Cancel
Upload
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.
Apple Info
Site Map
Hot News
RSS Feeds
Contact Us
Copyright © 2014 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy

Apple Push Certificates Portal

Create a New Push Certificate

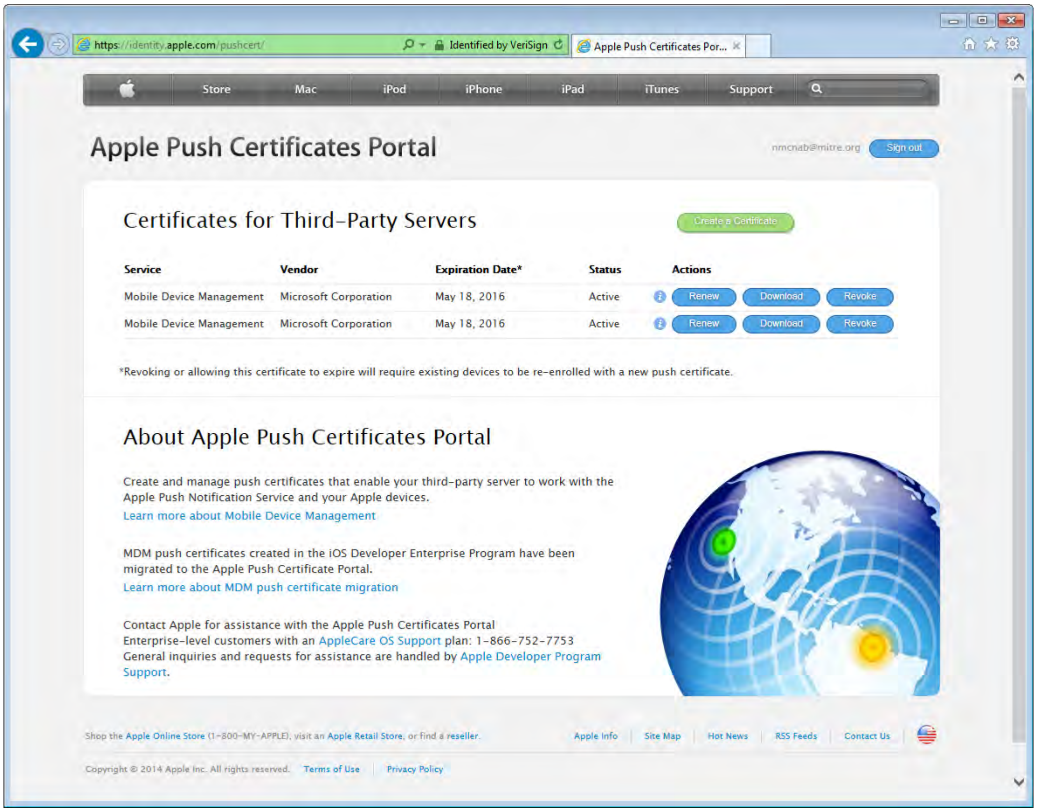
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

C:\Users\nmcnab\Deskto

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.



Apple Push Certificates Portal

Certificates for Third-Party Servers

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

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

About Apple Push Certificates Portal

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

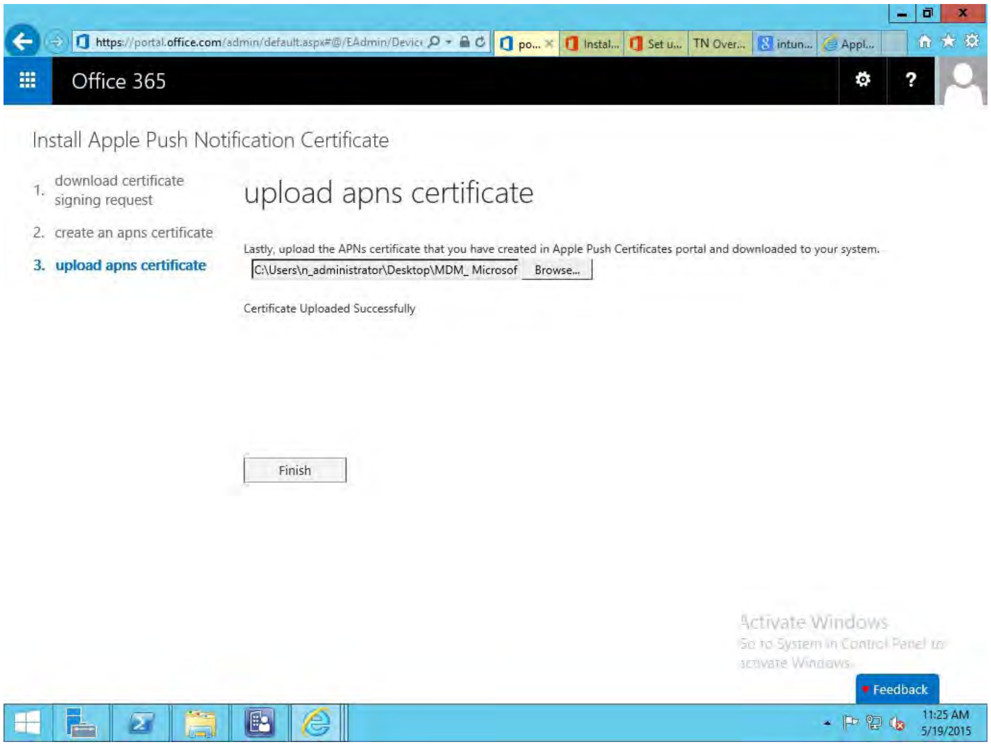
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
Learn more about MDM push certificate migration

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

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use | Privacy Policy



Install Apple Push Notification Certificate

1. download certificate signing request
2. create an apns certificate
3. **upload apns certificate**

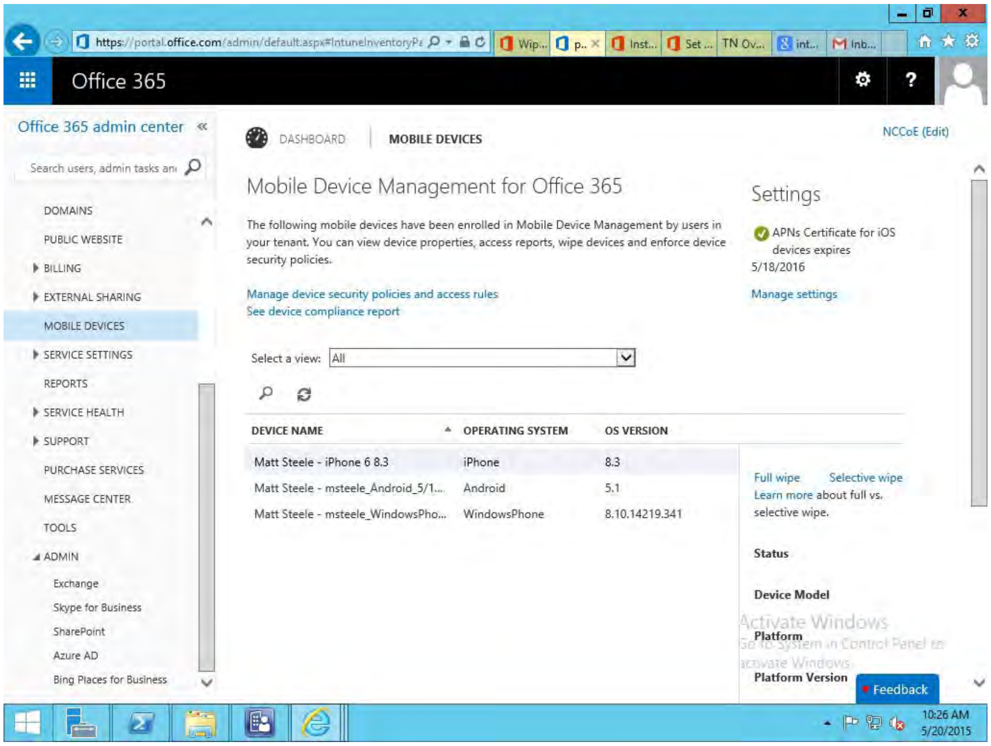
upload apns certificate

Lastly, upload the APNs certificate that you have created in Apple Push Certificates portal and downloaded to your system.

C:\Users\n_administrator\Desktop\MDM_ Microsof

Certificate Uploaded Successfully

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



Mobile Device Management for Office 365

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

Manage device security policies and access rules
See device compliance report

Settings

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

Manage settings

Select a view: All

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

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

Status

Device Model

Platform

Platform Version

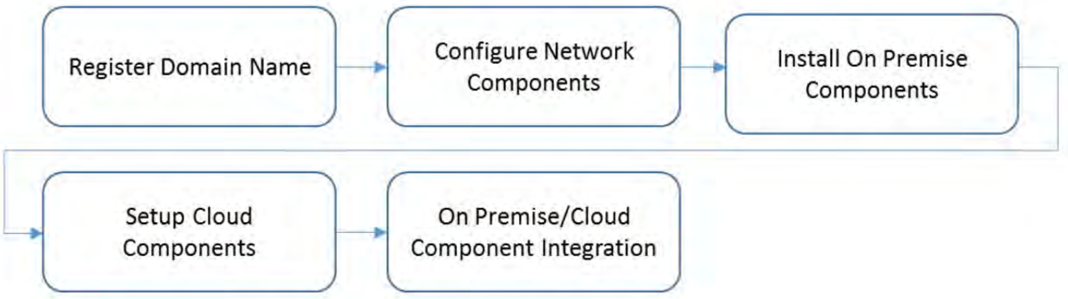
7. Verify that the APN is working correctly; it should have an expiration date listed.

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


Register Domain Name
Configure Network Components
Install On Premise Components
Setup Cloud Components
On Premise/Cloud Component Integration

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.

Figure 3.2 Detailed Architecture

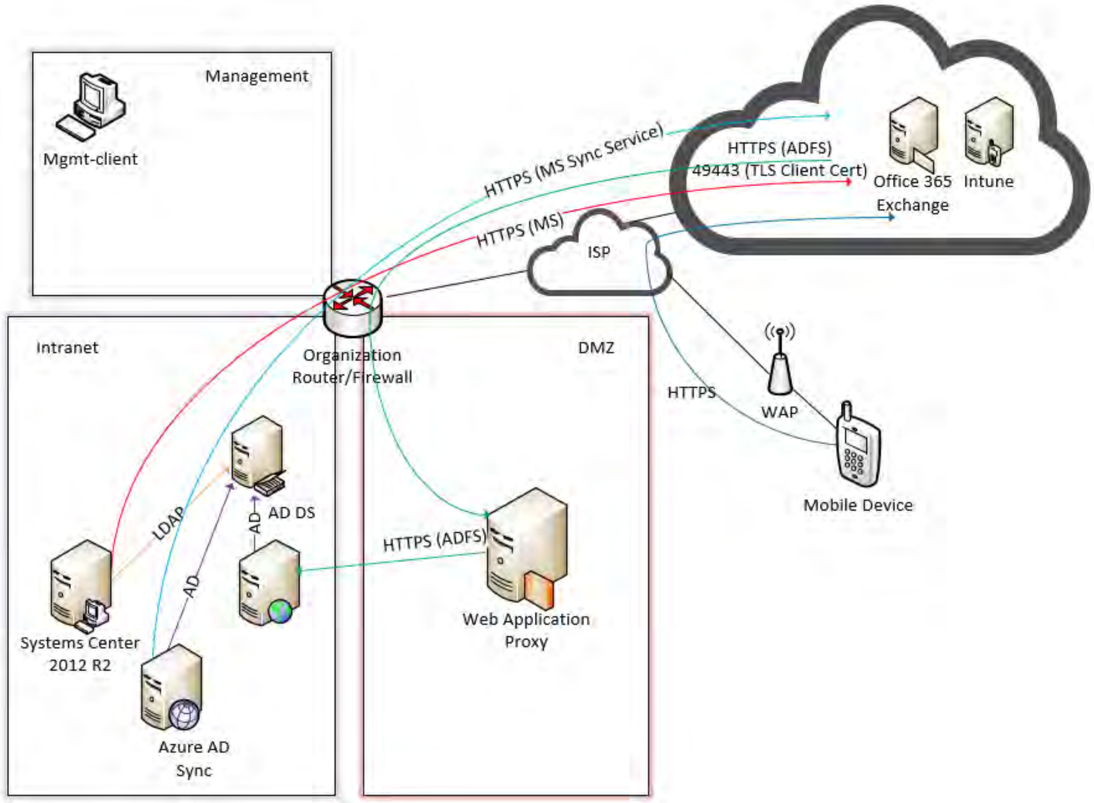
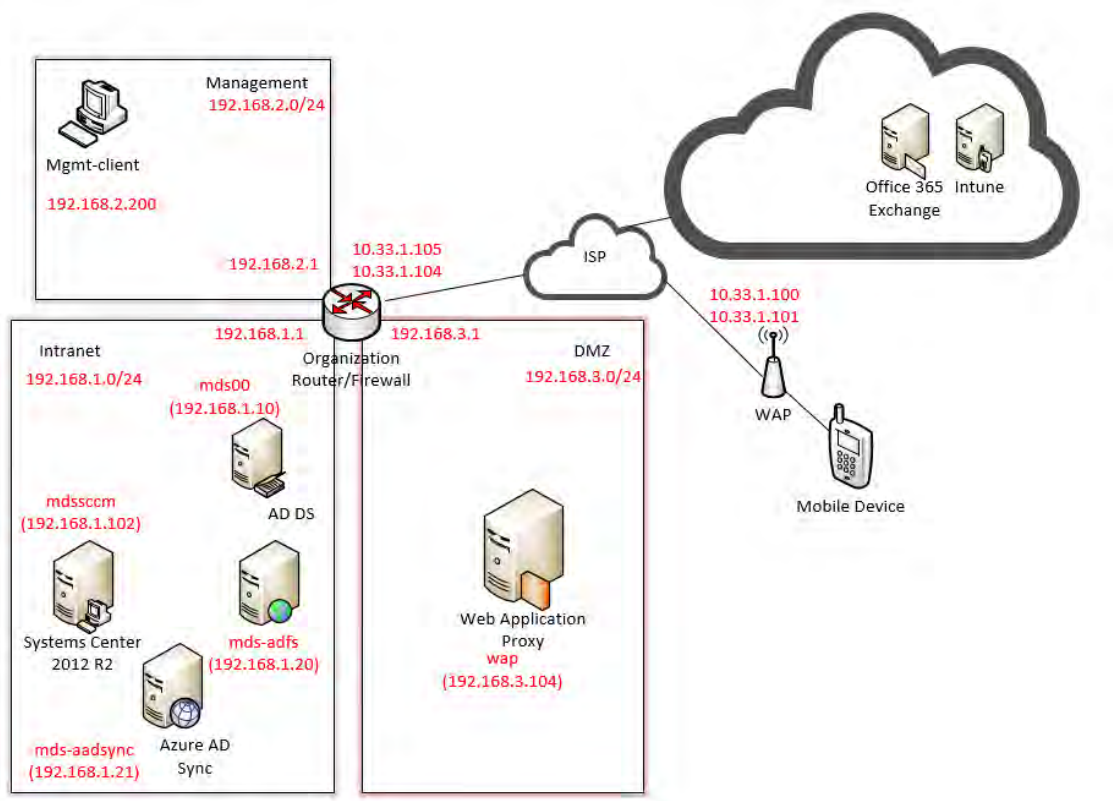


Figure 3.3 Detailed Architecture with IP Addresses



3.2.1 Hybrid Build Components

Table 3.1 lists the components used for this building block.

Table 3.1 Components

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

Table 3.1 Components

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

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

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.

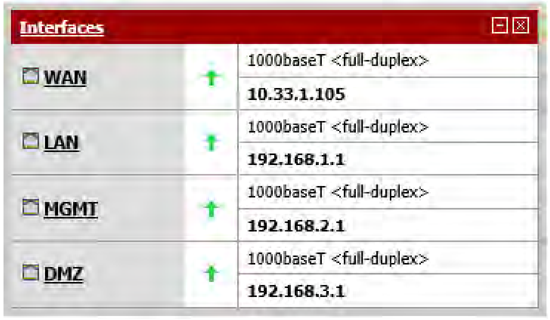
The following screen shots show the final configuration of the PFSense device. Access PFSense through its Web interface. The default screen includes a list of interfaces described as part of the architecture in section 3.2. The individual interfaces are described below with the firewall rules.

[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

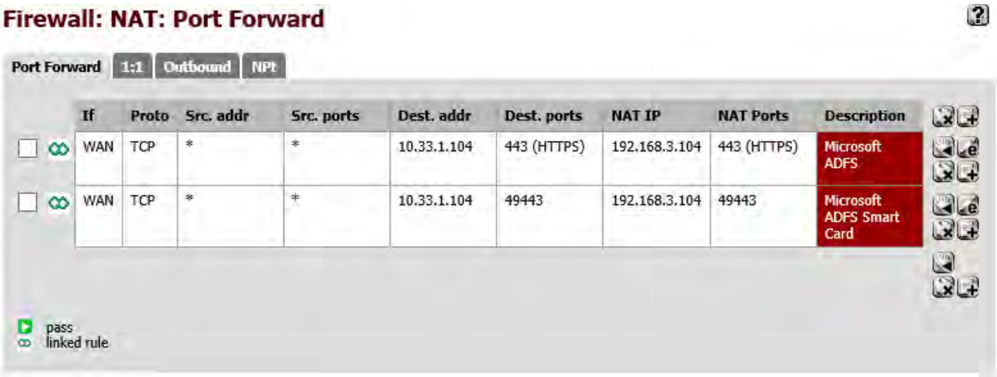
Figure 3.4 List of Configured Interfaces



WAN	↑	1000baseT <full-duplex> 10.33.1.105
LAN	↑	1000baseT <full-duplex> 192.168.1.1
MGMT	↑	1000baseT <full-duplex> 192.168.2.1
DMZ	↑	1000baseT <full-duplex> 192.168.3.1

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

Figure 3.5 WAN



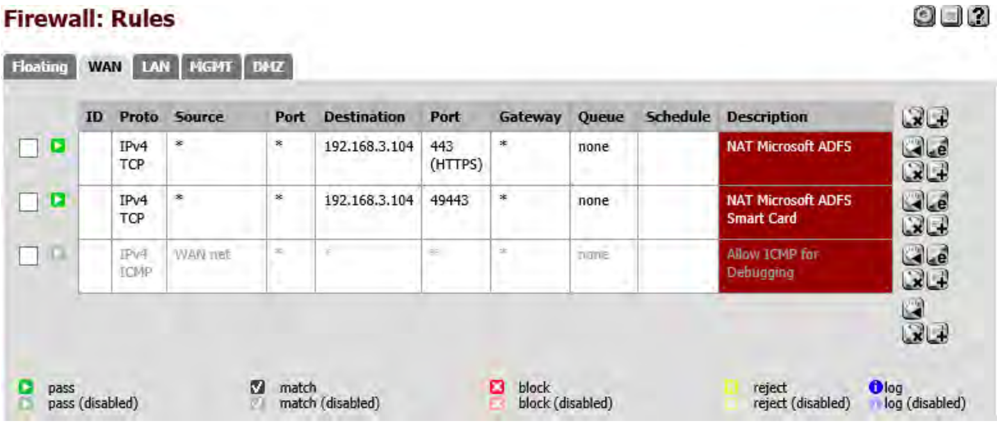
Firewall: NAT: Port Forward

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

🟩 pass
∞ linked rule

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

Figure 3.6 WAN Firewall Rules



Firewall: Rules

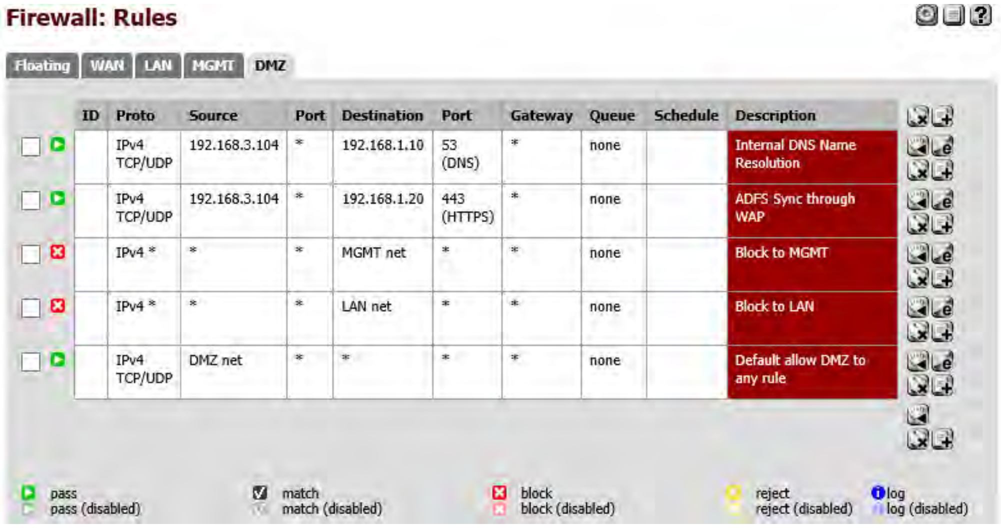
		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
□	🟩		IPv4 TCP	*	*	192.168.3.104	443 (HTTPS)	*	none		NAT Microsoft ADFS
□	🟩		IPv4 TCP	*	*	192.168.3.104	49443	*	none		NAT Microsoft ADFS Smart Card
□			IPv4 ICMP	WAN net	*	*	*	*	none		Allow ICMP for Debugging

🟩 pass ☑ match 🟥 block reject ● log
pass (disabled) match (disabled) block (disabled) reject (disabled) log (disabled)

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

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

Figure 3.7 DMZ Firewall Rules

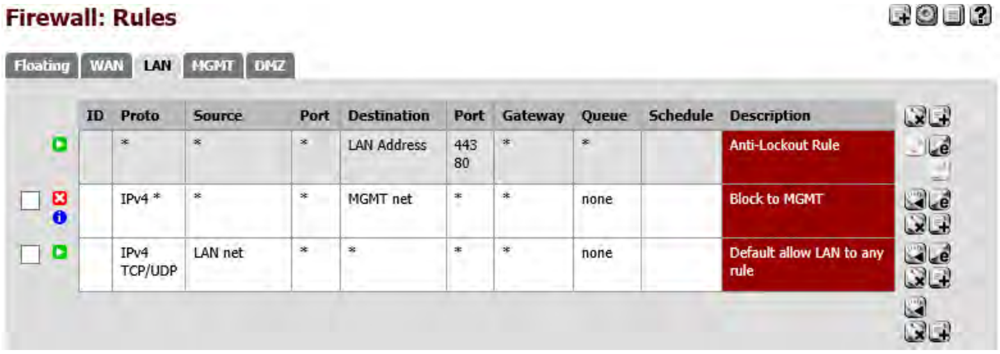


		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
□	🟩		IPv4 TCP/UDP	192.168.3.104	*	192.168.1.10	53 (DNS)	*	none		Internal DNS Name Resolution
□	🟩		IPv4 TCP/UDP	192.168.3.104	*	192.168.1.20	443 (HTTPS)	*	none		ADFS Sync through WAP
□	🟥		IPv4 *	*	*	MGMT net	*	*	none		Block to MGMT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

🟩 pass	☑ match	🟥 block	reject	ℹ log
pass (disabled)	match (disabled)	block (disabled)	reject (disabled)	log (disabled)

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.

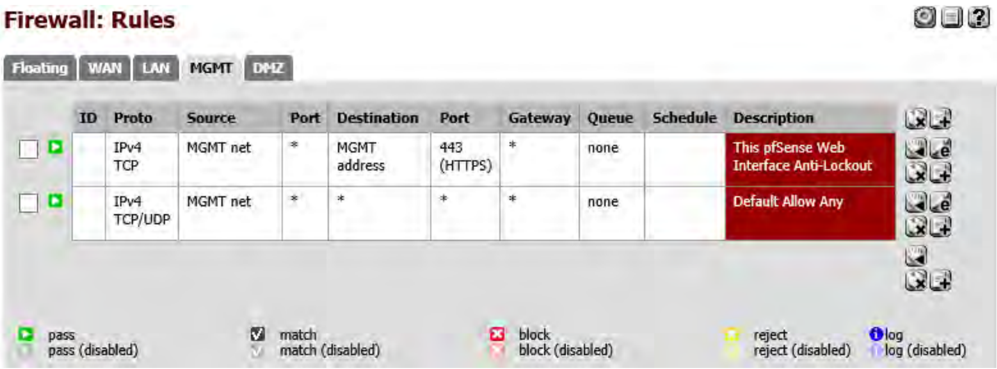
Figure 3.8 LAN Firewall Rules



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

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

Figure 3.9 Management Firewall Rules



Firewall: Rules

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
□		IPv4 TCP	MGMT net	*	MGMT address	443 (HTTPS)	*	none		This pfSense Web Interface Anti-Lockout
□		IPv4 TCP/UDP	MGMT net	*	*	*	*	none		Default Allow Any

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

3.2.3 Enterprise Software Components for Hybrid

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

Table 3.2 Enterprise Software Components

Component	Hostname	IP Address
Active Directory Domain Services	mds00	192.168.1.10
Active Directory Federation Services	mds-adfs	192.168.120
Active Directory Federation Services Proxy	wap	192.168.3.104
Systems Center Configuration Manager	mdssccm	192.168.1.102
Azure Active Directory Sync Services	mds-adsync	192.168.1.21

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

3.2.3.1 Active Directory Domain Services

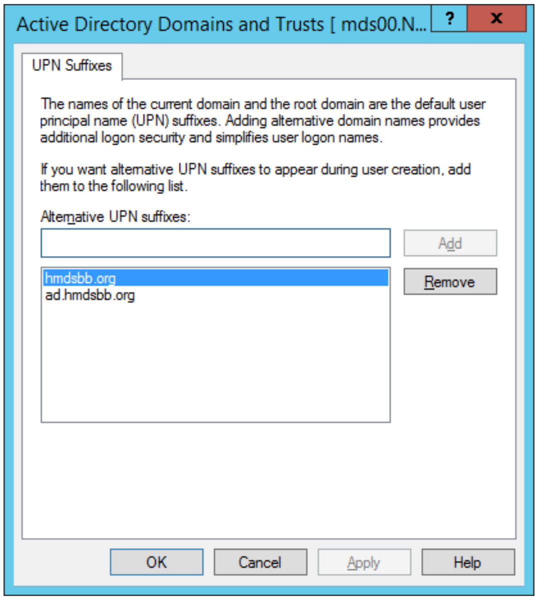
The Active Directory Domain Services (ADDS) instance used in the hybrid build was created using basic configuration settings offered through the Add Roles and Features Wizard. The system was deployed as a new forest with a domain name of nccoe.local. Implementers of this guide who seek more details on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

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

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.



The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

hmdsbb.org
ad.hmdsbb.org

3.2.3.2 Active Directory Federation Service

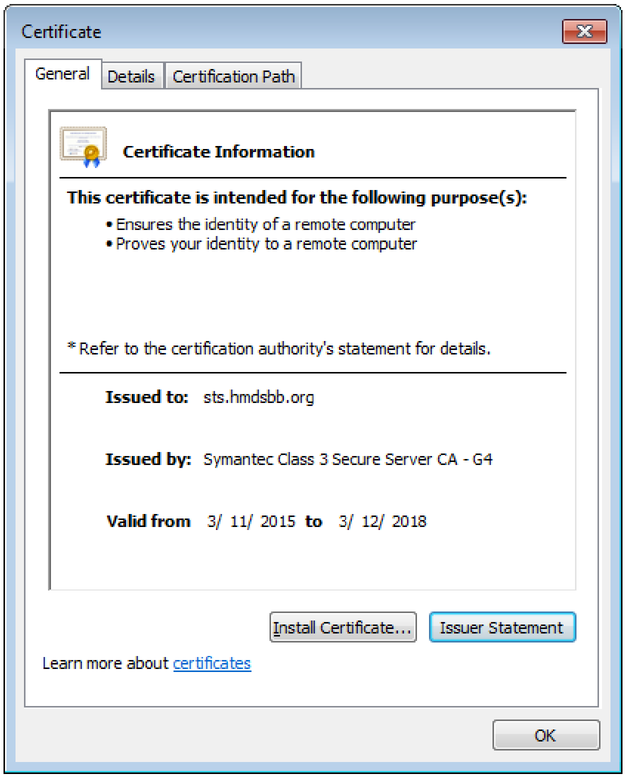
Refer to Microsoft documentation for specific installation instructions for your environment. Consult the following articles as a starting point for installation [6] [7].

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

from Symantec's Secure Site Pro SSL service. Ensure that the provider is able to populate the Subject Alternative Name extension of the certificates used in the implementation.

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



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

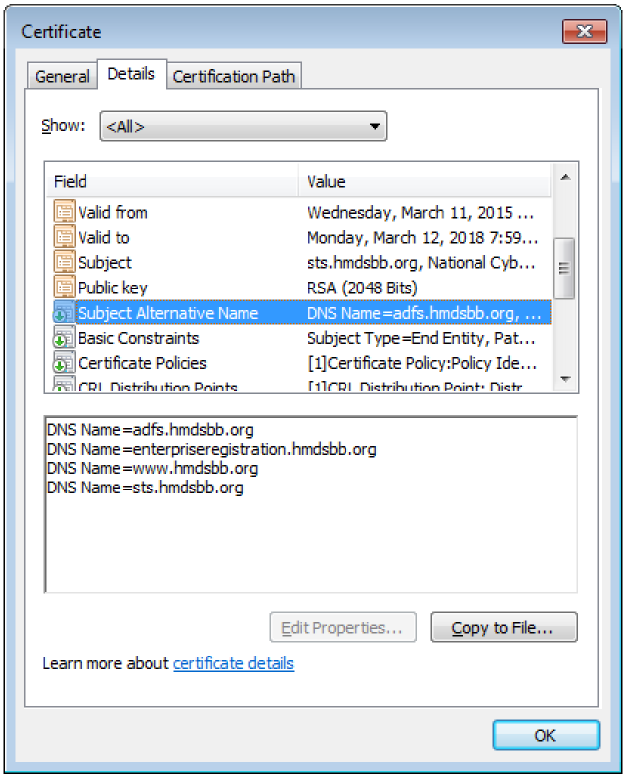
* Refer to the certification authority's statement for details.

Issued to: sts.hmdsbb.org

Issued by: Symantec Class 3 Secure Server CA - G4

Valid from 3/ 11/ 2015 **to** 3/ 12/ 2018

Learn more about certificates



Show: <All>

Field	Value
Valid from	Wednesday, March 11, 2015 ...
Valid to	Monday, March 12, 2018 7:59...
Subject	sts.hmdsbb.org, National Cyb...
Public key	RSA (2048 Bits)
Subject Alternative Name	DNS Name=adfs.hmdsbb.org, ...
Basic Constraints	Subject Type=End Entity, Pat...
Certificate Policies	[1]Certificate Policy:Policy Ide...
CRL Distribution Points	[1]CRL Distribution Point: Distr

```
DNS Name=adfs.hmdsbb.org
DNS Name=enterpriseregistration.hmdsbb.org
DNS Name=www.hmdsbb.org
DNS Name=sts.hmdsbb.org
```

Learn more about certificate details

3.2.3.3 Active Directory Federation Services Proxy

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

3.2.3.4 Systems Center Configuration Manager

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

3.2.3.5 Azure Active Directory Sync Services

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

3.2.4 Cloud Services Instances

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

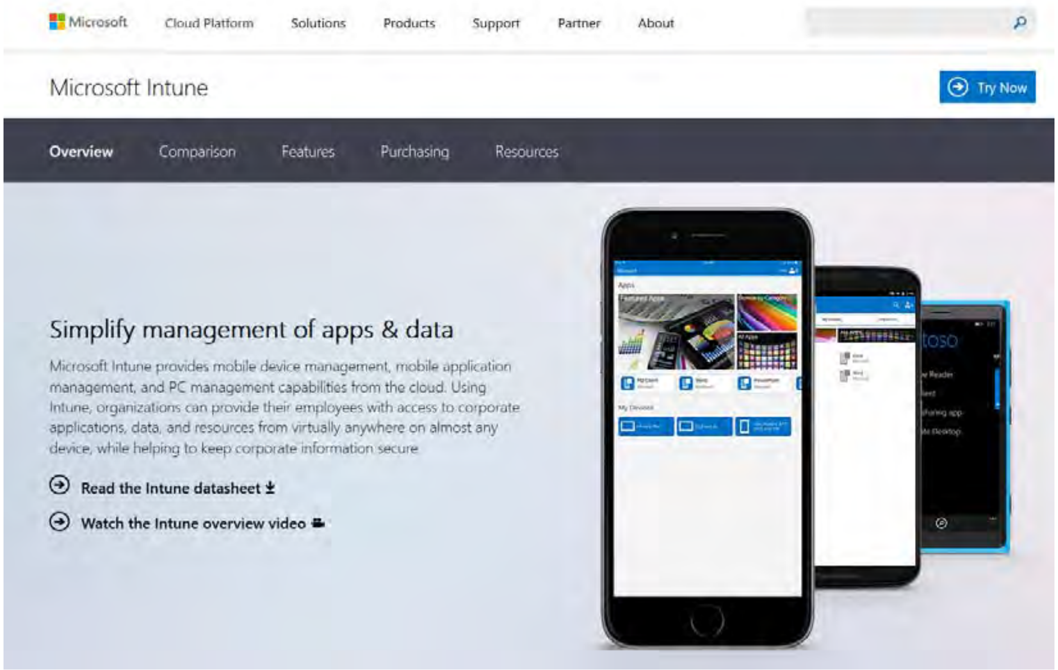
3.2.4.1 Office 365 Setup

The setup of the Office 365 service is the same as previously described for the cloud Office 365 setup. We replaced 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:

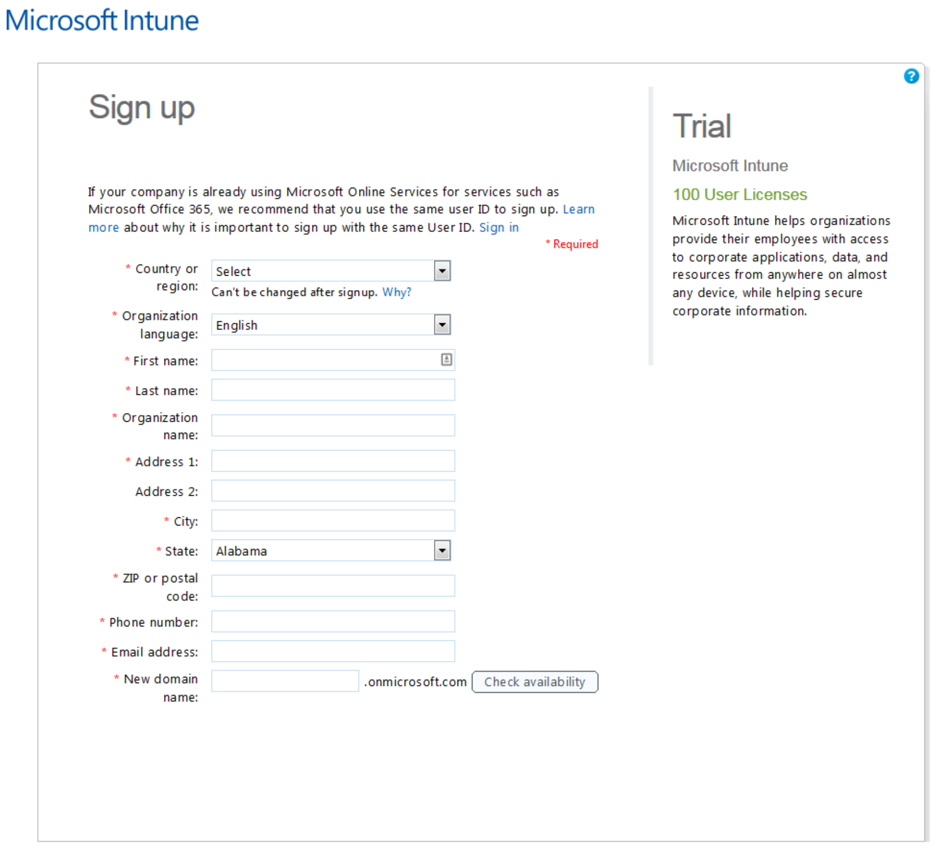
http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/



Simplify management of apps & data

Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

1. Choose **Try now**.



Microsoft Intune

Sign up

If your company is already using Microsoft Online Services for services such as Microsoft Office 365, we recommend that you use the same user ID to sign up. Learn more about why it is important to sign up with the same User ID. Sign in

* Required

* Country or region: Select
Can't be changed after signup. Why?

* Organization language: English

* First name:

* Last name:

* Organization name:

* Address 1:

Address 2:

* City:

* State: Alabama

* ZIP or postal code:

* Phone number:

* Email address:

* New domain name: .onmicrosoft.com

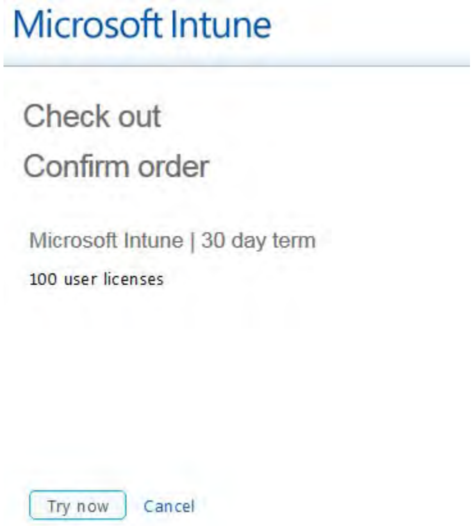
Trial

Microsoft Intune

100 User Licenses

Microsoft Intune helps organizations provide their employees with access to corporate applications, data, and resources from anywhere on almost any device, while helping secure corporate information.

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



Microsoft Intune

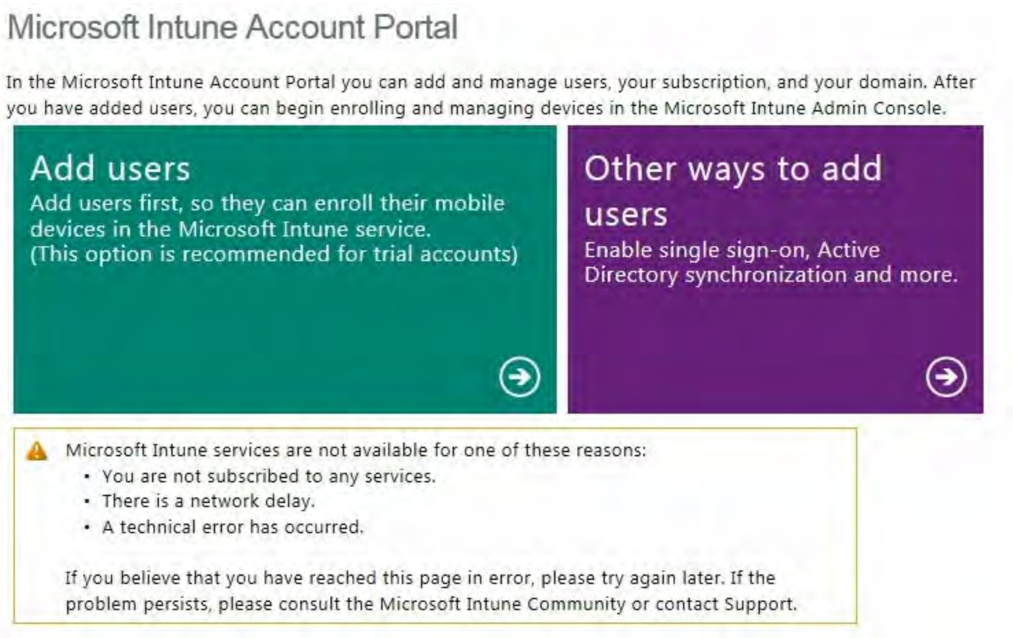
Check out

Confirm order

Microsoft Intune | 30 day term

100 user licenses

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.



Microsoft Intune Account Portal

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

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

Other ways to add users
Enable single sign-on, Active Directory synchronization and more.

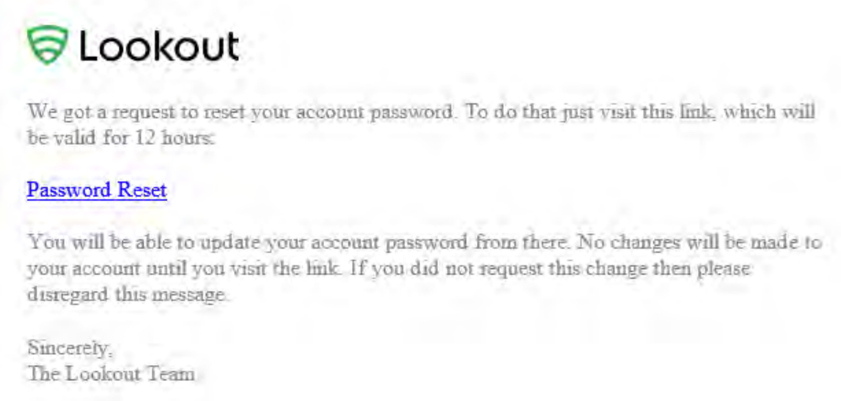
Microsoft Intune services are not available for one of these reasons:
- You are not subscribed to any services.
- There is a network delay.
- A technical error has occurred.

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

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.



Lookout

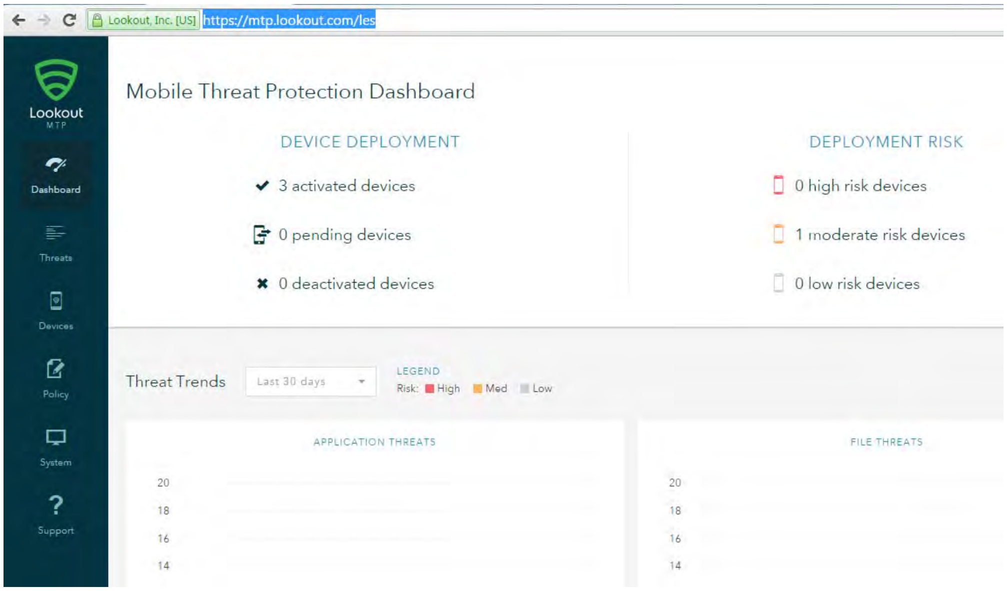
We got a request to reset your account password. To do that just visit this link, which will be valid for 12 hours.

Password Reset

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

Sincerely,
The Lookout Team

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



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

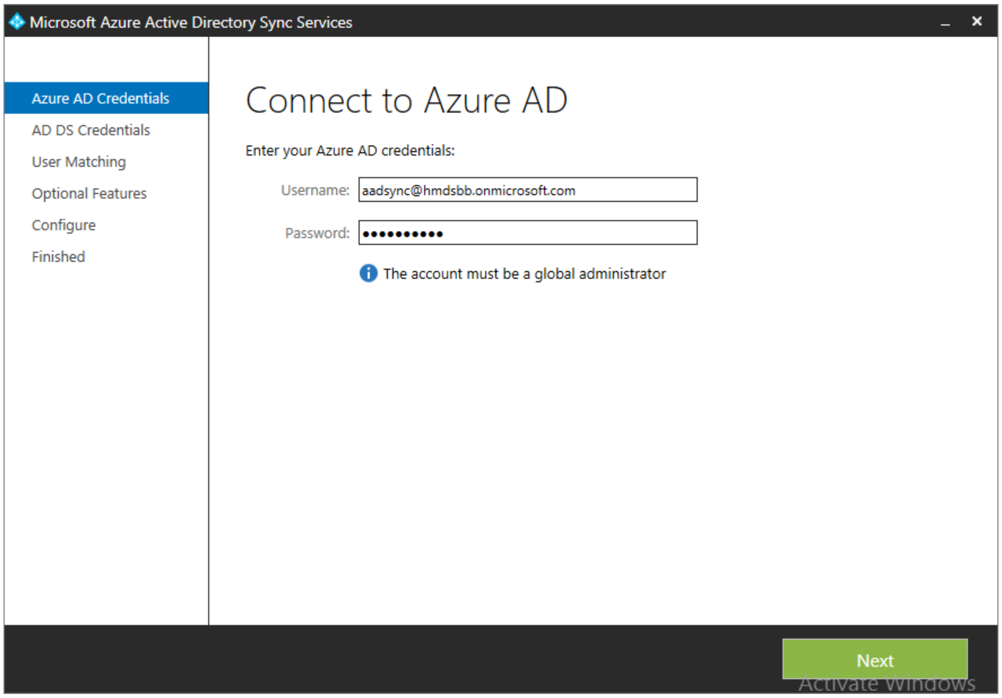
1. In this step, an on-premises ADFS server is integrated with the Office 365 service. The purpose of this integration is to provide identity federation between Office 365 and enterprise authentication service. You should have added your public domain to Office 365as described in section 2.1.2. If not, 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.



Connect to Azure AD

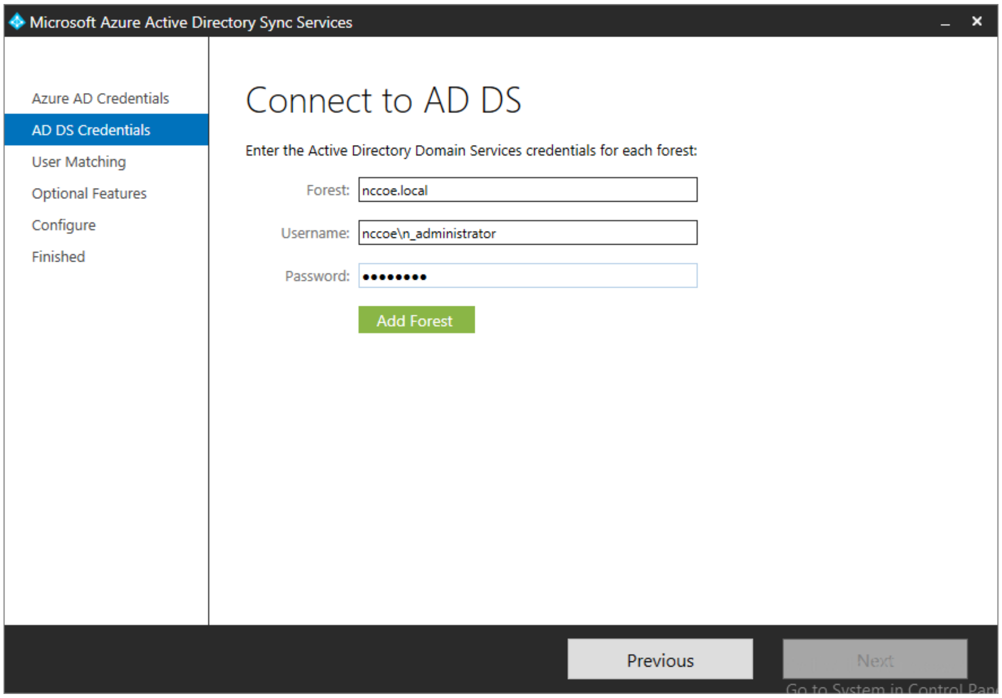
Enter your Azure AD credentials:

Username: aadsync@hmdsbb.onmicrosoft.com

Password: ••••••••••

The account must be a global administrator

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



Connect to AD DS

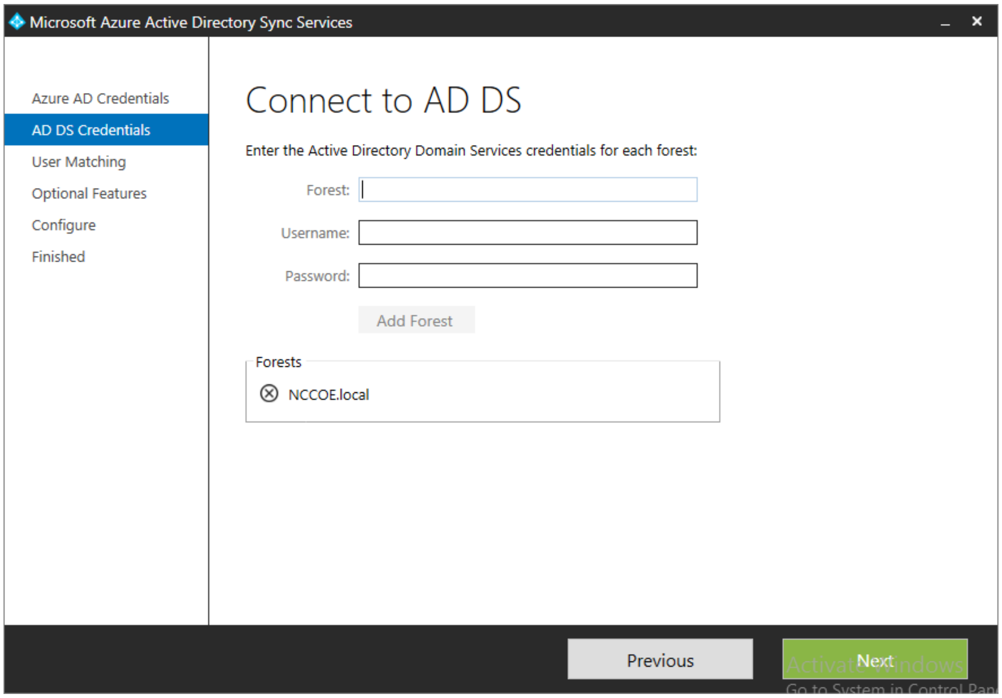
Enter the Active Directory Domain Services credentials for each forest:

Forest: nccoe.local

Username: nccoe\n_administrator

Password: ••••••••

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



Connect to AD DS

Enter the Active Directory Domain Services credentials for each forest:

Forest:

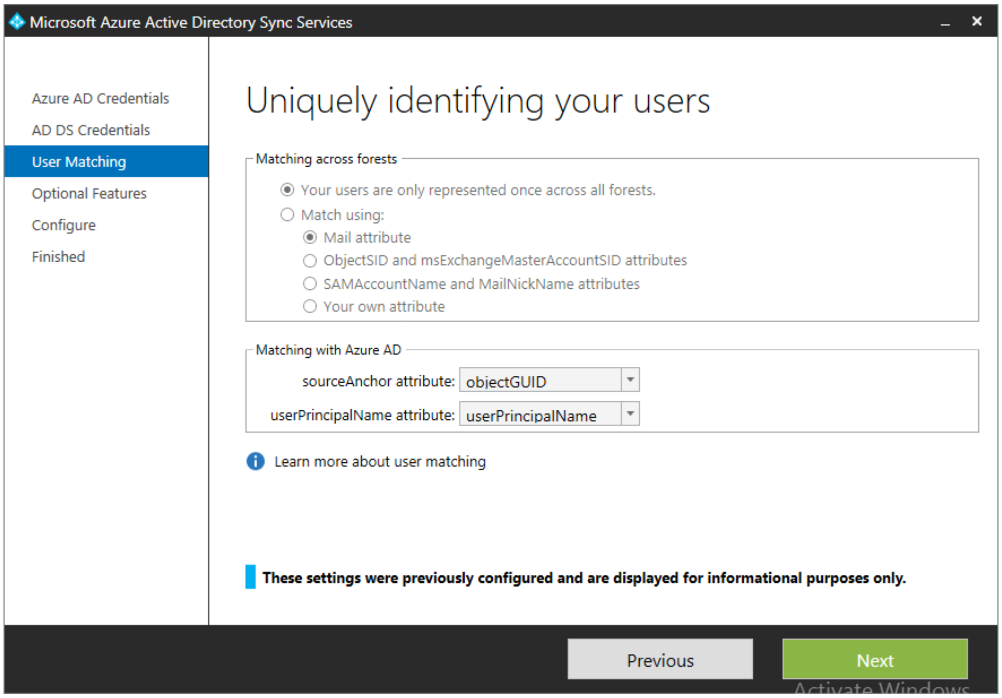
Username:

Password:

Forests

⊗ NCCOE.local

3. Click **Next**.



Uniquely identifying your users

Matching across forests

● Your users are only represented once across all forests.

○ Match using:

● Mail attribute

○ ObjectSID and msExchangeMasterAccountSID attributes

○ SAMAccountName and MailNickName attributes

○ Your own attribute

Matching with Azure AD

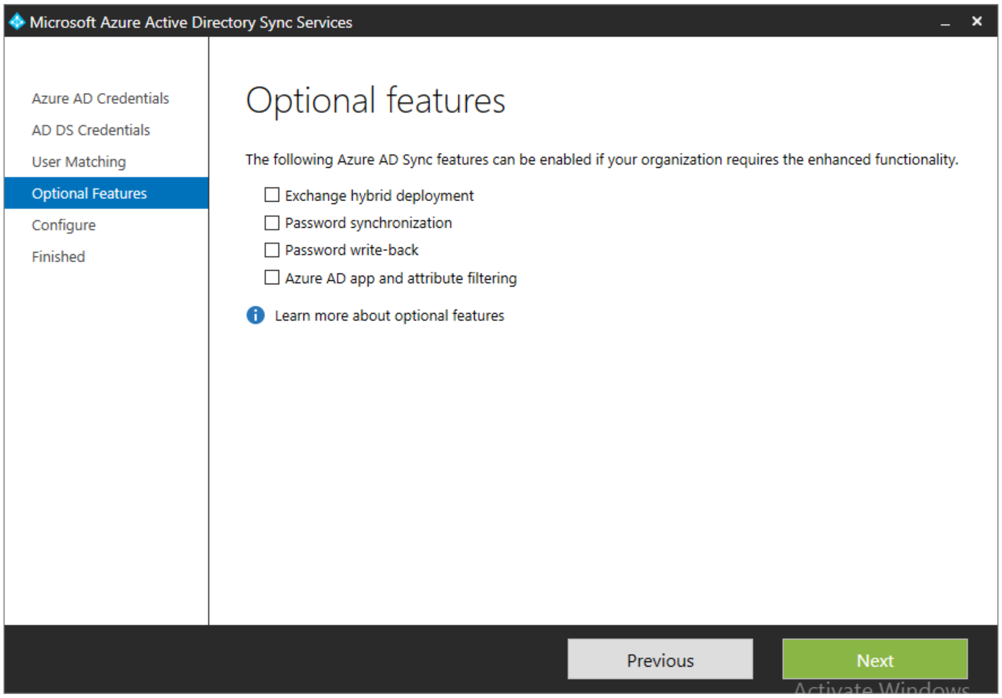
sourceAnchor attribute: objectGUID

userPrincipalName attribute: userPrincipalName

Learn more about user matching

These settings were previously configured and are displayed for informational purposes only.

4. Accept the defaults for uniquely identifying your users.



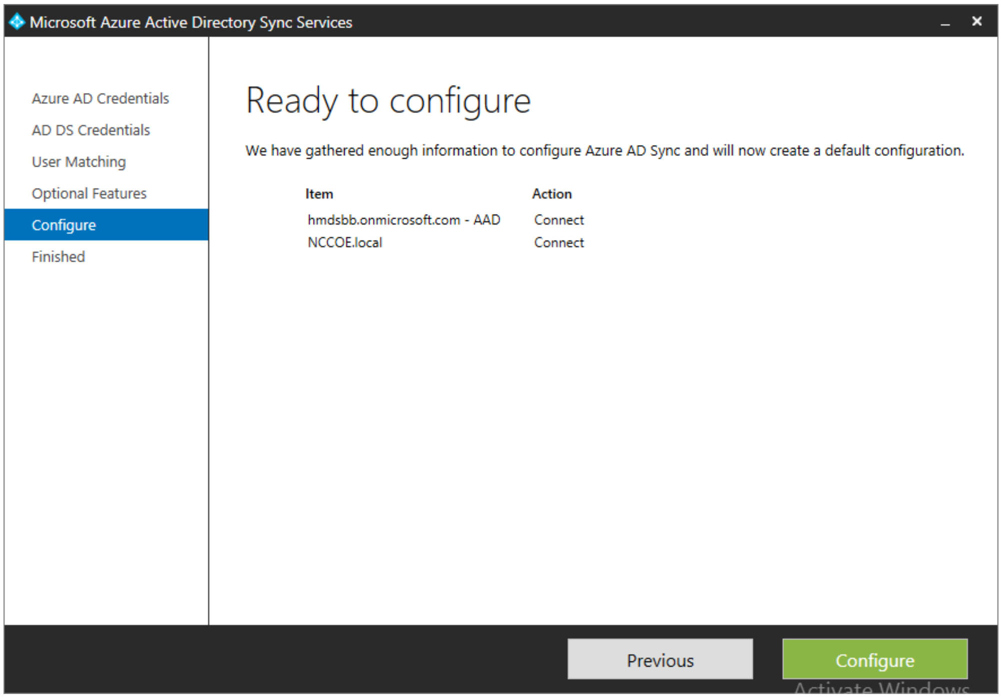
Optional features

The following Azure AD Sync features can be enabled if your organization requires the enhanced functionality.

- □ Exchange hybrid deployment
- □ Password synchronization
- □ Password write-back
- □ Azure AD app and attribute filtering

Learn more about optional features

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

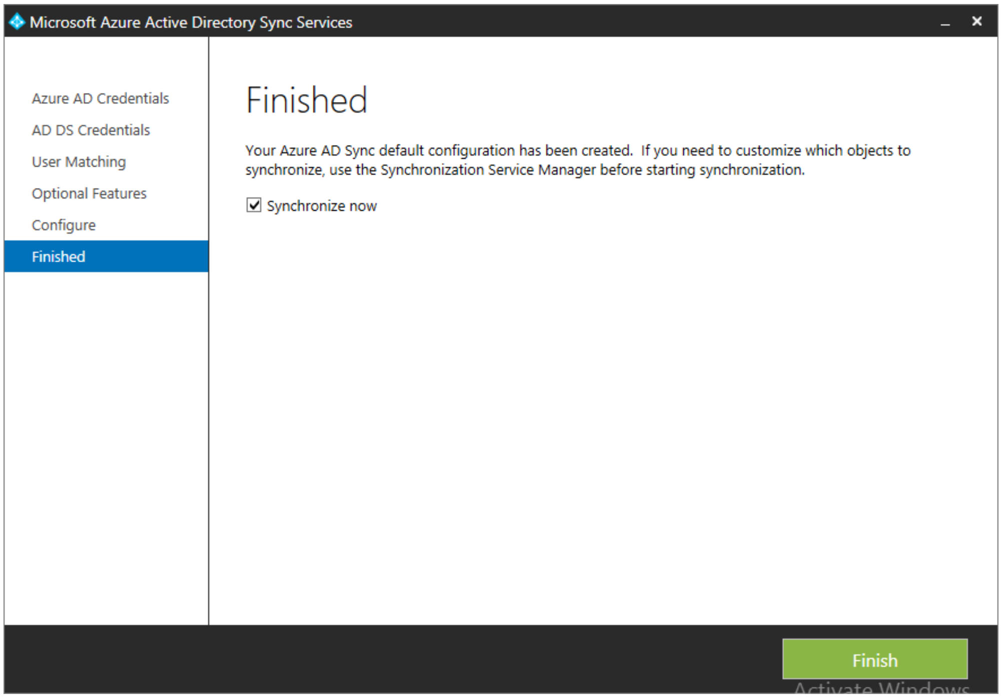


Ready to configure

We have gathered enough information to configure Azure AD Sync and will now create a default configuration.

Item	Action
hmdsbb.onmicrosoft.com - AAD	Connect
NCCOE.local	Connect

6. Click **Configure**.

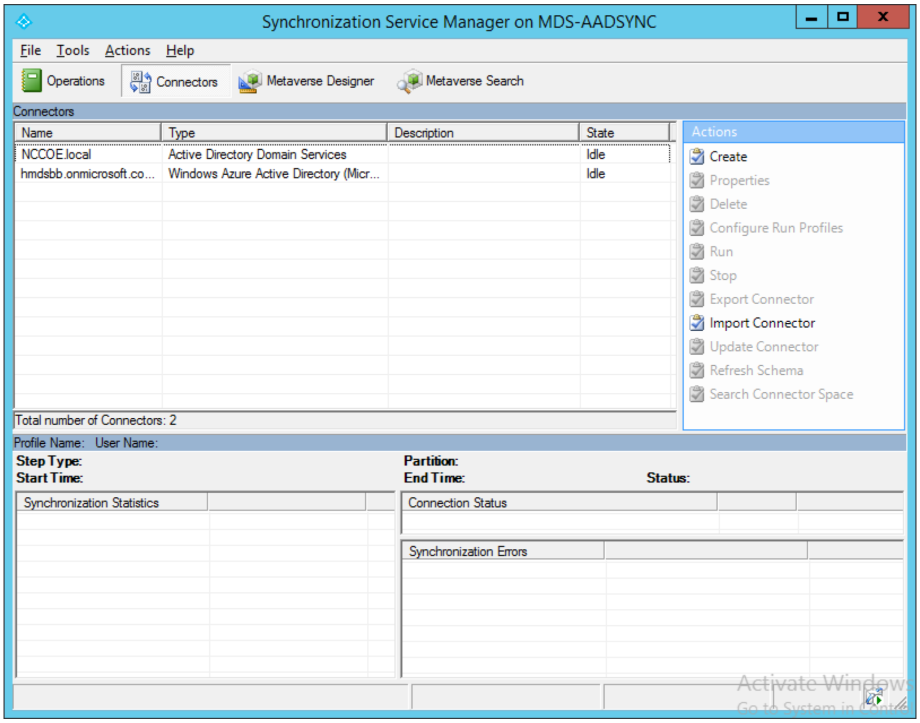


Finished

Your Azure AD Sync default configuration has been created. If you need to customize which objects to synchronize, use the Synchronization Service Manager before starting synchronization.

☑ Synchronize now

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



Name	Type	Description	State
NCCOE.local	Active Directory Domain Services		Idle
hmdsbb.onmicrosoft.co...	Windows Azure Active Directory (Micr...		Idle

Total number of Connectors: 2

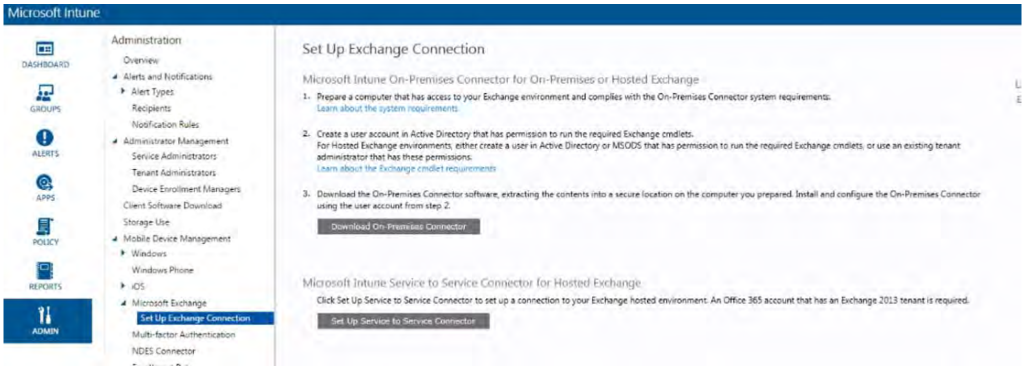
Profile Name: User Name:

Step Type: **Partition:**
Start Time: **End Time:** **Status:**

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

3.2.5.3 Sync Intune with Office 365 Exchange

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



Set Up Exchange Connection

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

1. Prepare a computer that has access to your Exchange environment and complies with the On-Premises Connector system requirements.
   Learn about the system requirements

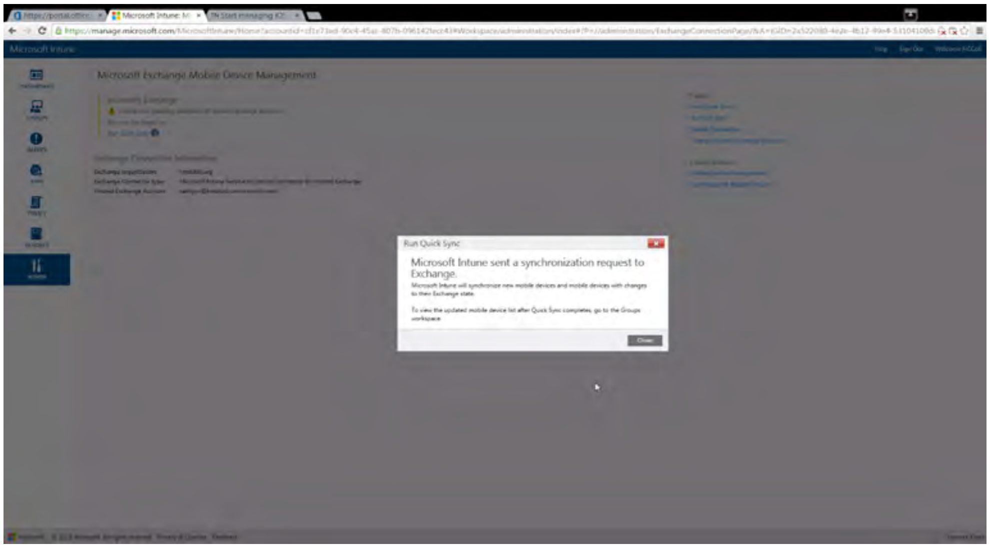
2. Create a user account in Active Directory that has permission to run the required Exchange cmdlets.
   For Hosted Exchange environments, either create a user in Active Directory or MSODS that has permission to run the required Exchange cmdlets, or use an existing tenant administrator that has these permissions.
   Learn about the Exchange cmdlet requirements

3. Download the On-Premises Connector software, extracting the contents into a secure location on the computer you prepared. Install and configure the On-Premises Connector using the user account from step 2.

Microsoft Intune Service to Service Connector for Hosted Exchange

Click Set Up Service to Service Connector to set up a connection to your Exchange hosted environment. An Office 365 account that has an Exchange 2013 tenant is required.

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**.



Run Quick Sync

Microsoft Intune sent a synchronization request to Exchange.

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

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

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

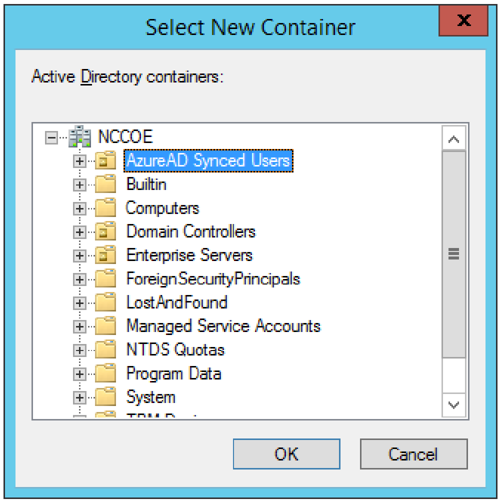
3.2.5.4 Manage Intune with SCCM

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.

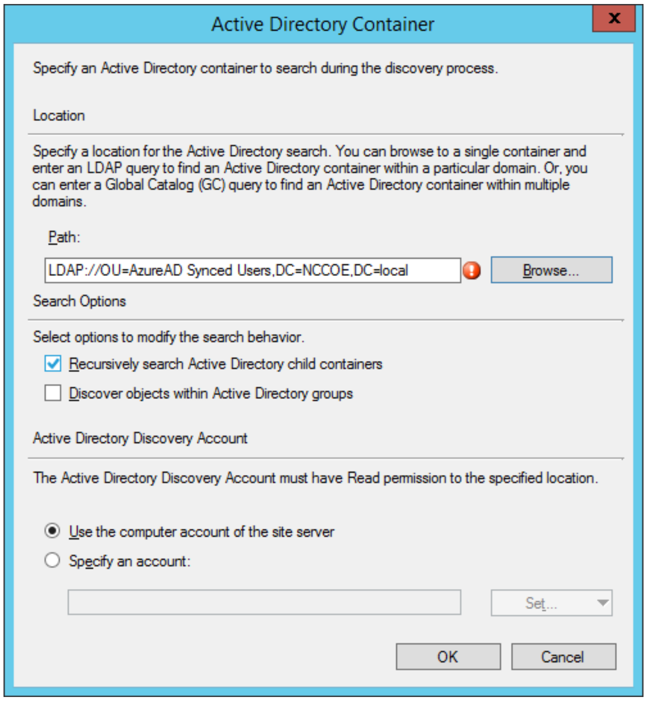
3.2.5.4.1 Configure Active Directory User Discovery

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.



Specify an Active Directory container to search during the discovery process.

Location

Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.

Path: LDAP://OU=AzureAD Synced Users,DC=NCCOE,DC=local

Search Options

Select options to modify the search behavior.

☑ Recursively search Active Directory child containers

□ Discover objects within Active Directory groups

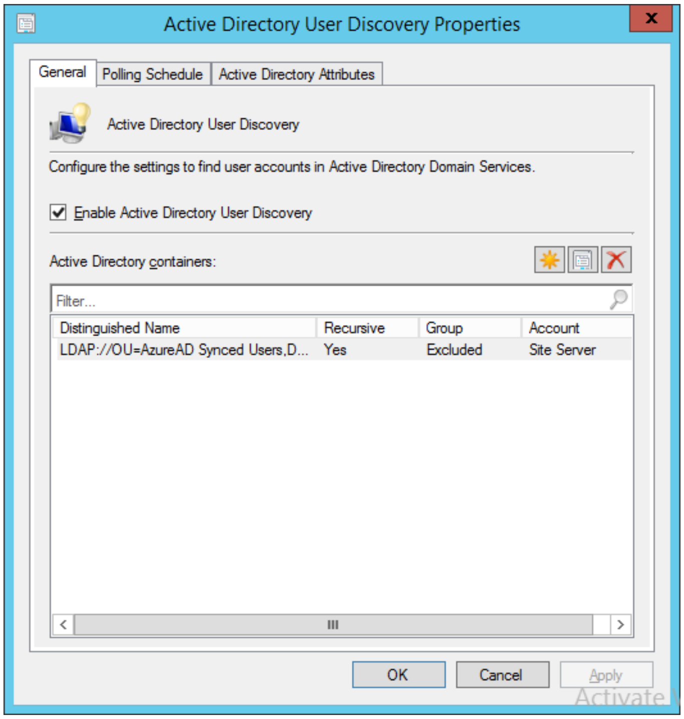
Active Directory Discovery Account

The Active Directory Discovery Account must have Read permission to the specified location.

● Use the computer account of the site server

○ Specify an account:

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



Active Directory User Discovery Properties
General
Polling Schedule
Active Directory Attributes
OK
Cancel
Apply
Activate

Active Directory User Discovery

Configure the settings to find user accounts in Active Directory Domain Services.

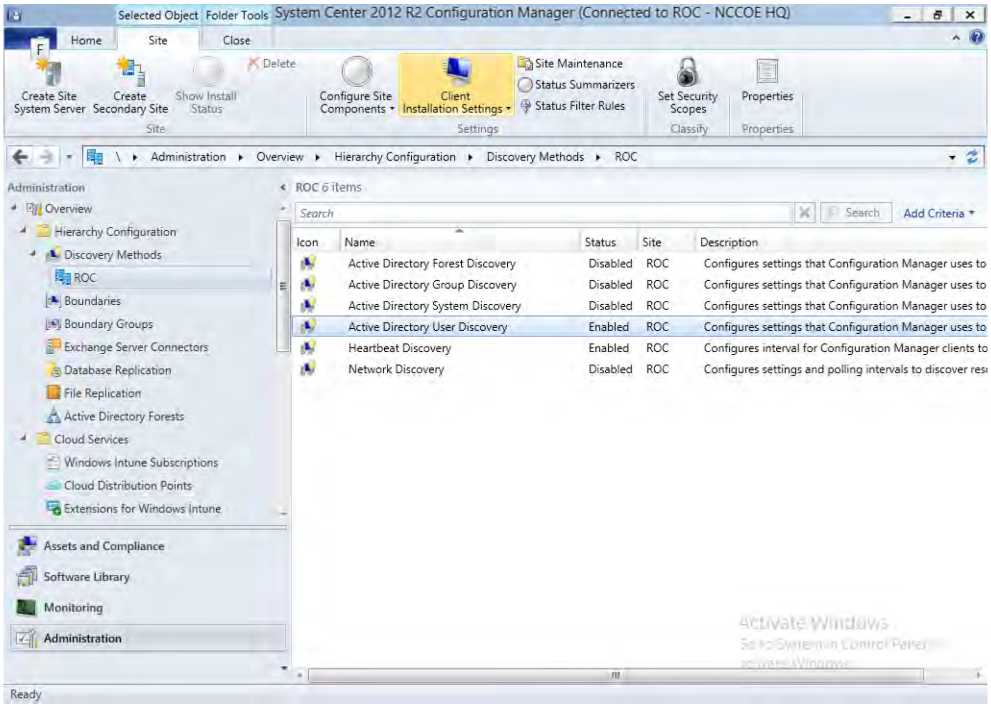
☑ Enable Active Directory User Discovery

Active Directory containers:

Filter...

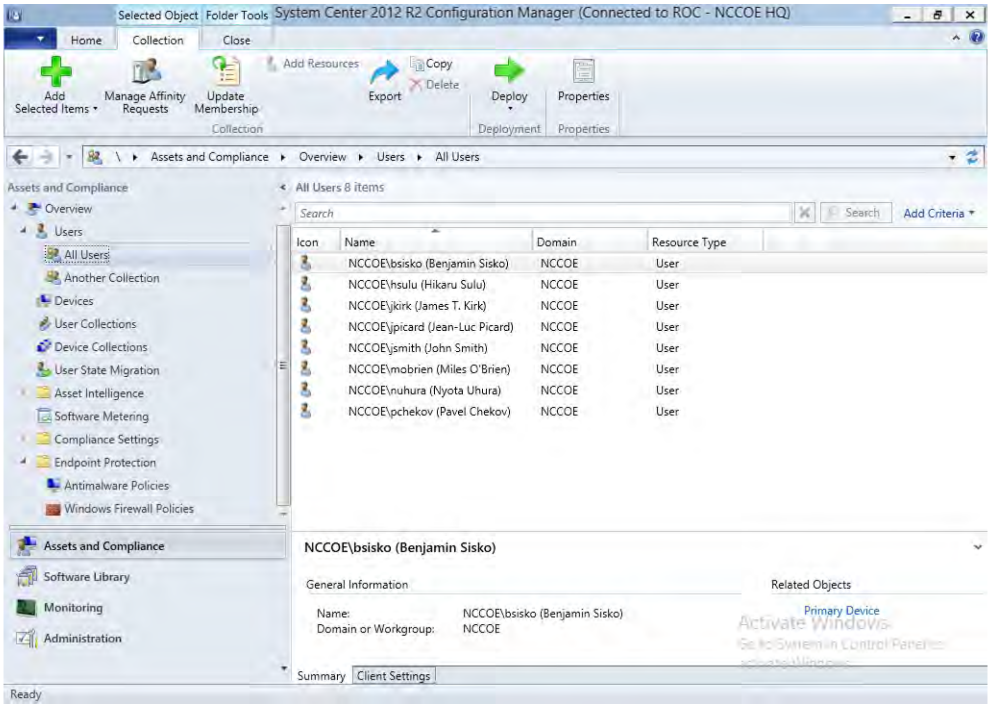
Distinguished Name	Recursive	Group	Account
LDAP://OU=AzureAD Synced Users,D...	Yes	Excluded	Site Server

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



Icon	Name	Status	Site	Description
	Active Directory Forest Discovery	Disabled	ROC	Configures settings that Configuration Manager uses to
	Active Directory Group Discovery	Disabled	ROC	Configures settings that Configuration Manager uses to
	Active Directory System Discovery	Disabled	ROC	Configures settings that Configuration Manager uses to
	Active Directory User Discovery	Enabled	ROC	Configures settings that Configuration Manager uses to
	Heartbeat Discovery	Enabled	ROC	Configures interval for Configuration Manager clients to
	Network Discovery	Disabled	ROC	Configures settings and polling intervals to discover reso

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



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

NCCOE\bsisko (Benjamin Sisko)

General Information

Name: NCCOE\bsisko (Benjamin Sisko)
Domain or Workgroup: NCCOE

Related Objects

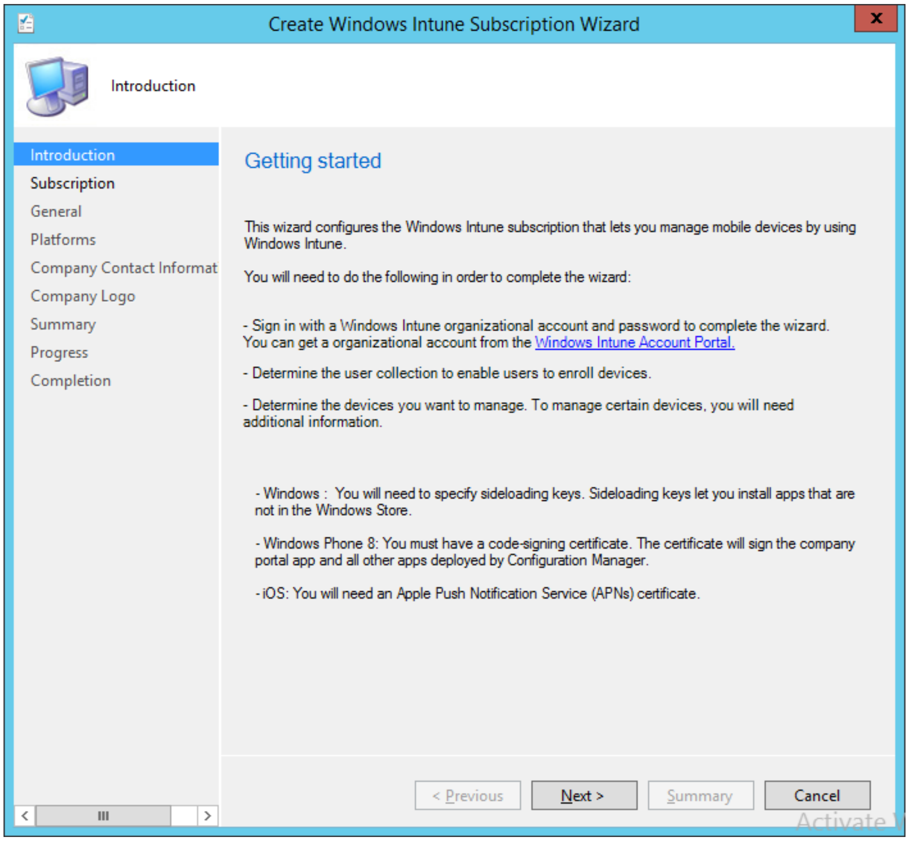
Primary Device

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**.



Getting started

This wizard configures the Windows Intune subscription that lets you manage mobile devices by using Windows Intune.

You will need to do the following in order to complete the wizard:

- Sign in with a Windows Intune organizational account and password to complete the wizard. You can get a organizational account from the Windows Intune Account Portal.

- Determine the user collection to enable users to enroll devices.

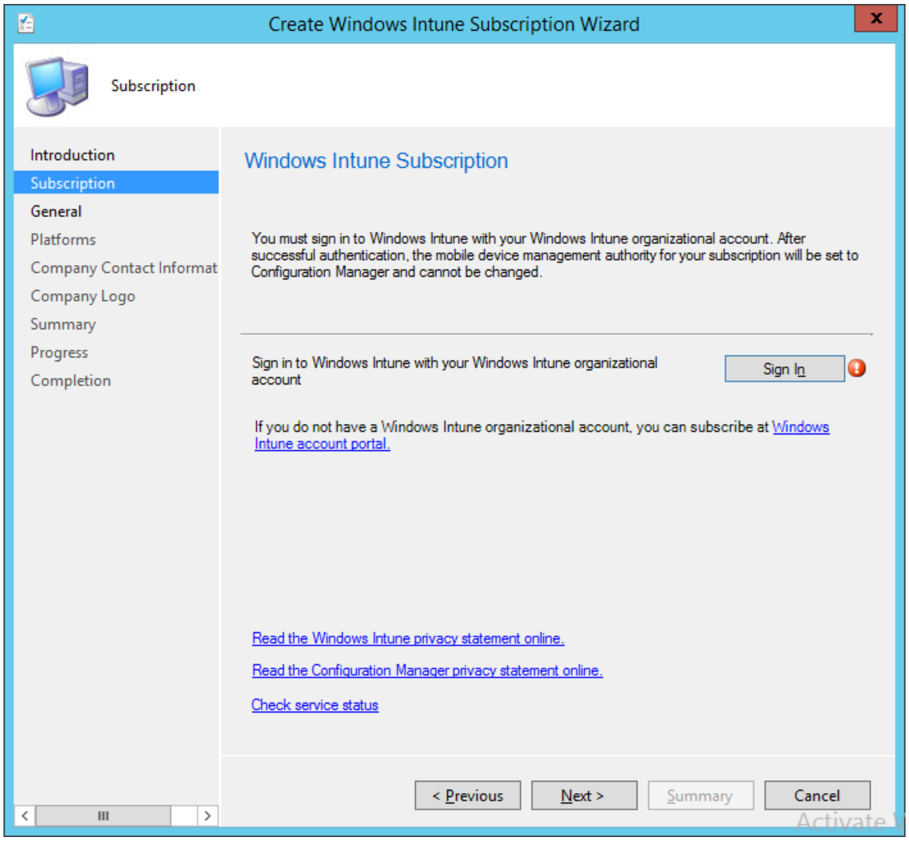
- Determine the devices you want to manage. To manage certain devices, you will need additional information.

- Windows : You will need to specify sideloading keys. Sideloading keys let you install apps that are not in the Windows Store.

- Windows Phone 8: You must have a code-signing certificate. The certificate will sign the company portal app and all other apps deployed by Configuration Manager.

- iOS: You will need an Apple Push Notification Service (APNs) certificate.

2. Click **Next**.



Windows Intune Subscription

You must sign in to Windows Intune with your Windows Intune organizational account. After successful authentication, the mobile device management authority for your subscription will be set to Configuration Manager and cannot be changed.

Sign in to Windows Intune with your Windows Intune organizational account

If you do not have a Windows Intune organizational account, you can subscribe at Windows Intune account portal.

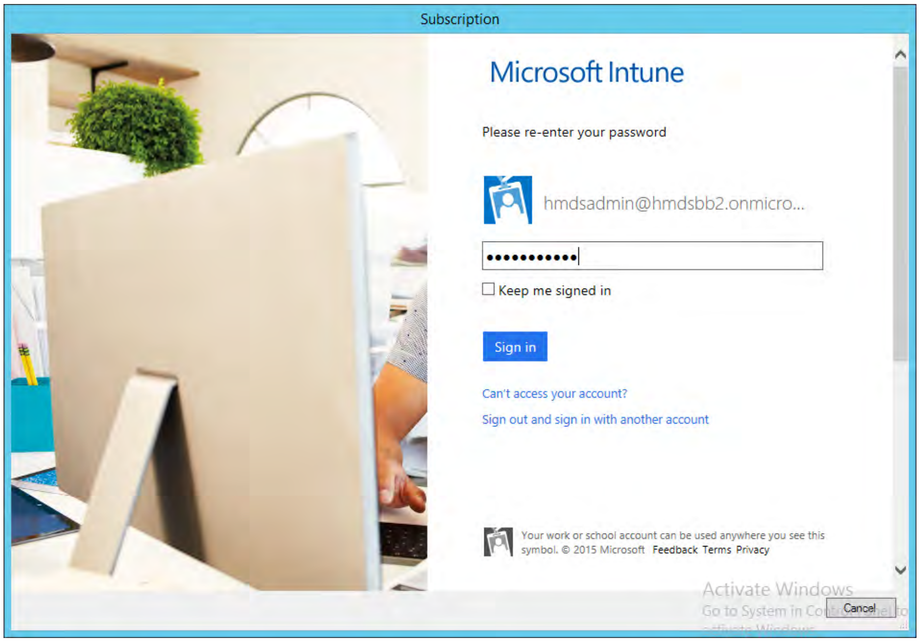
Read the Windows Intune privacy statement online.

Read the Configuration Manager privacy statement online.

Check service status

252

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


Subscription
Microsoft Intune
Sign in
Can't access your account?
Sign out and sign in with another account
Feedback Terms Privacy
Cancel

Please re-enter your password

hmdsadmin@hmdsbb2.onmicro...

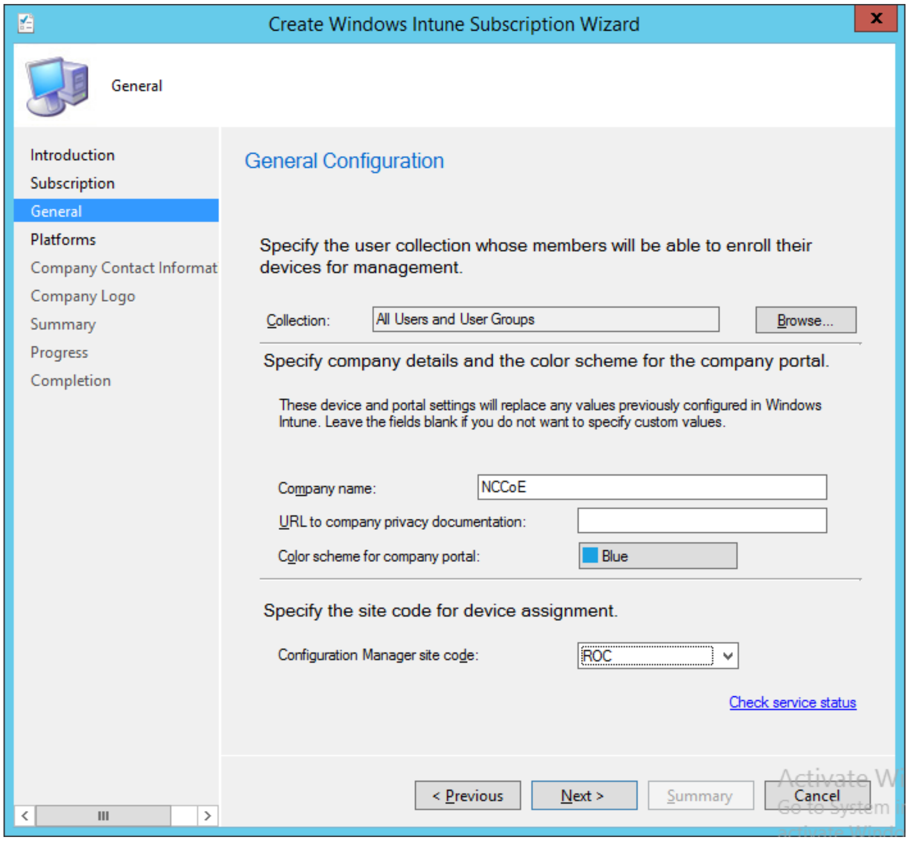
●●●●●●●●●●●

□ Keep me signed in

Your work or school account can be used anywhere you see this symbol. © 2015 Microsoft

254

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



General Configuration

Specify the user collection whose members will be able to enroll their devices for management.

Collection: All Users and User Groups Browse...

Specify company details and the color scheme for the company portal.

These device and portal settings will replace any values previously configured in Windows Intune. Leave the fields blank if you do not want to specify custom values.

Company name: NCCoE

URL to company privacy documentation:

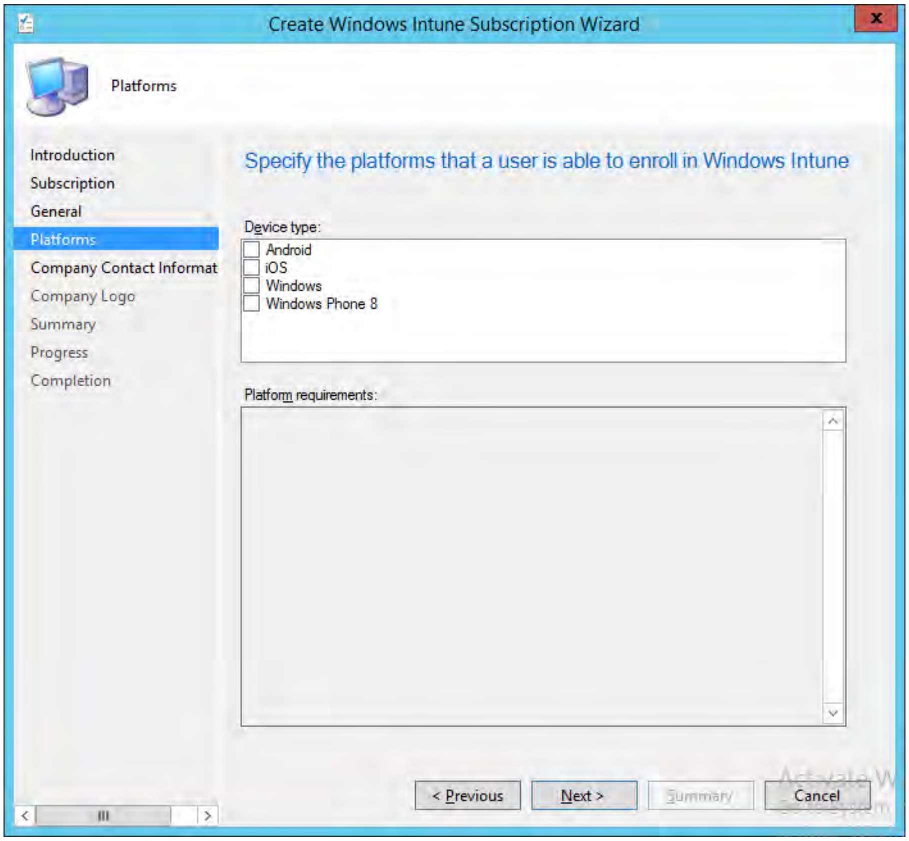
Color scheme for company portal: 🟦 Blue

Specify the site code for device assignment.

Configuration Manager site code: ROC

Check service status

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



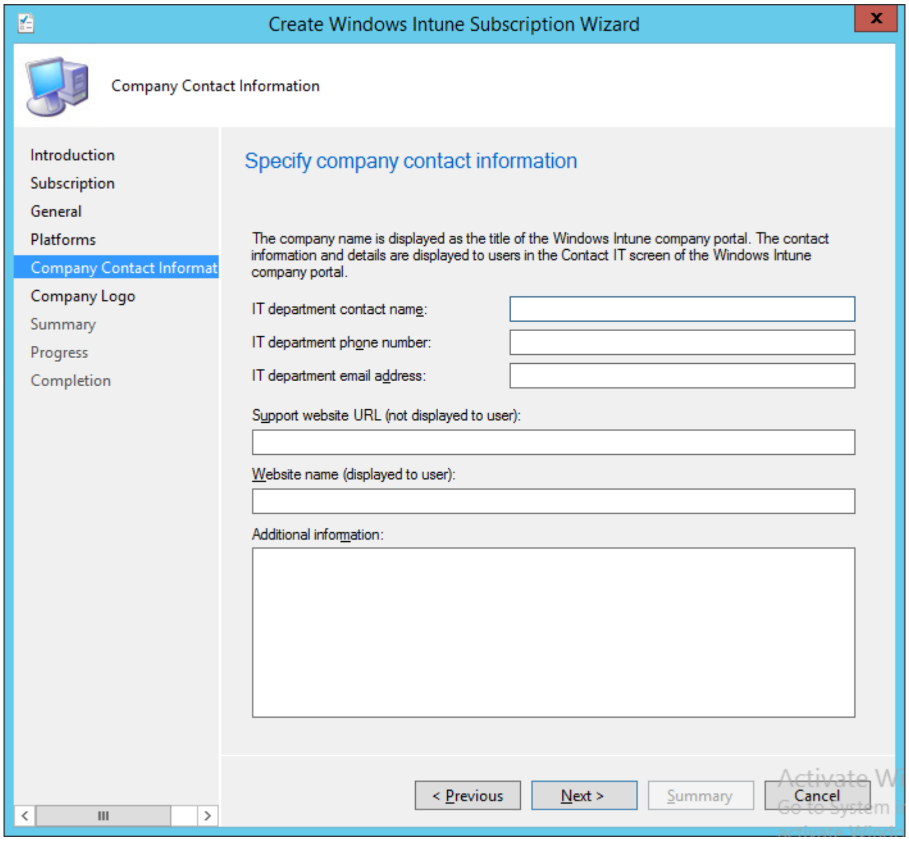
Specify the platforms that a user is able to enroll in Windows Intune

Device type:

□ Android
□ iOS
□ Windows
□ Windows Phone 8

Platform requirements:

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



Specify company contact information

The company name is displayed as the title of the Windows Intune company portal. The contact information and details are displayed to users in the Contact IT screen of the Windows Intune company portal.

IT department contact name:

IT department phone number:

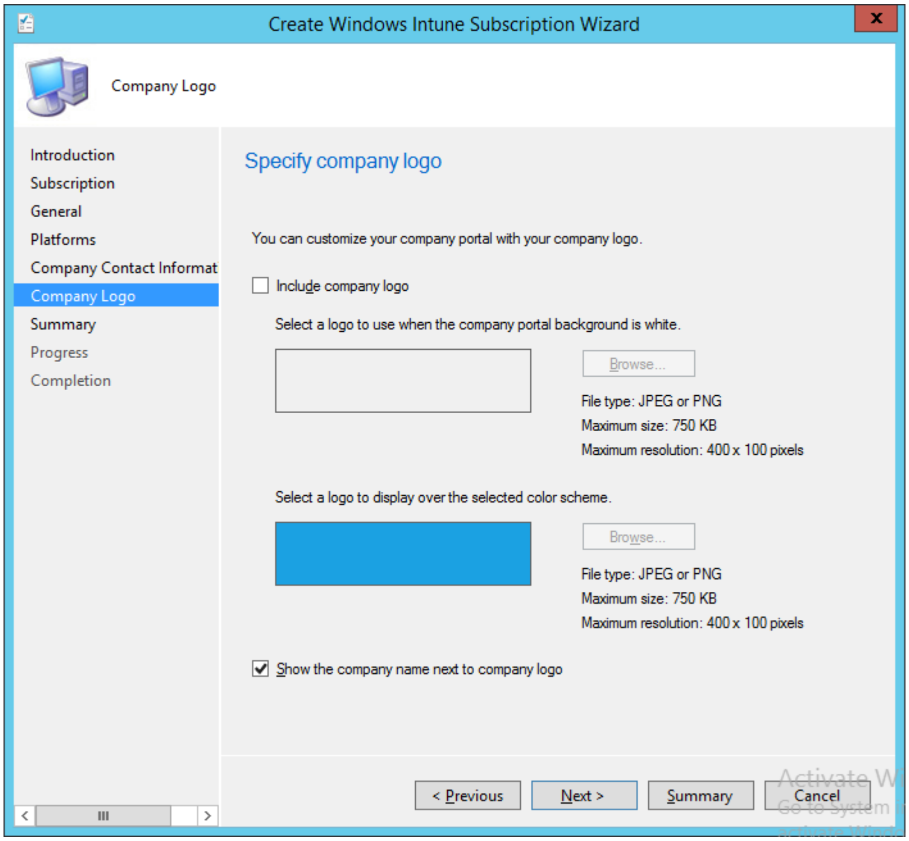
IT department email address:

Support website URL (not displayed to user):

Website name (displayed to user):

Additional information:

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



Specify company logo

You can customize your company portal with your company logo.

□ Include company logo

Select a logo to use when the company portal background is white.

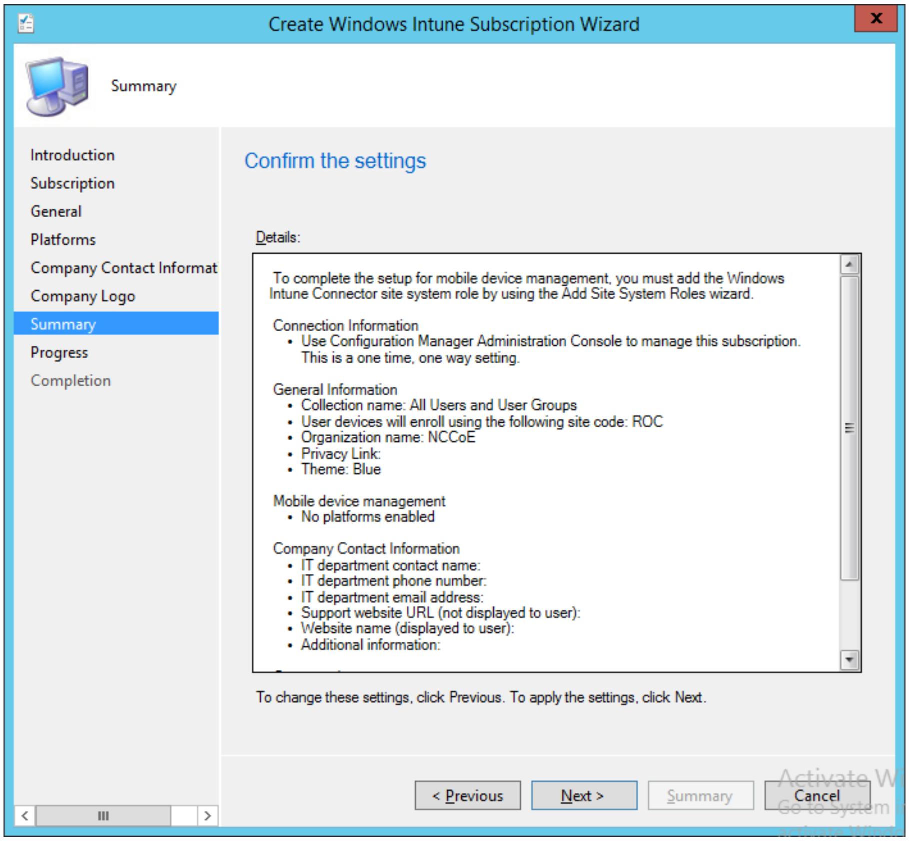
File type: JPEG or PNG
Maximum size: 750 KB
Maximum resolution: 400 x 100 pixels

Select a logo to display over the selected color scheme.

File type: JPEG or PNG
Maximum size: 750 KB
Maximum resolution: 400 x 100 pixels

☑ Show the company name next to company logo

8. Submit an organizational logo, if desired.



Confirm the settings

Details:

To complete the setup for mobile device management, you must add the Windows Intune Connector site system role by using the Add Site System Roles wizard.

Connection Information
- Use Configuration Manager Administration Console to manage this subscription. This is a one time, one way setting.

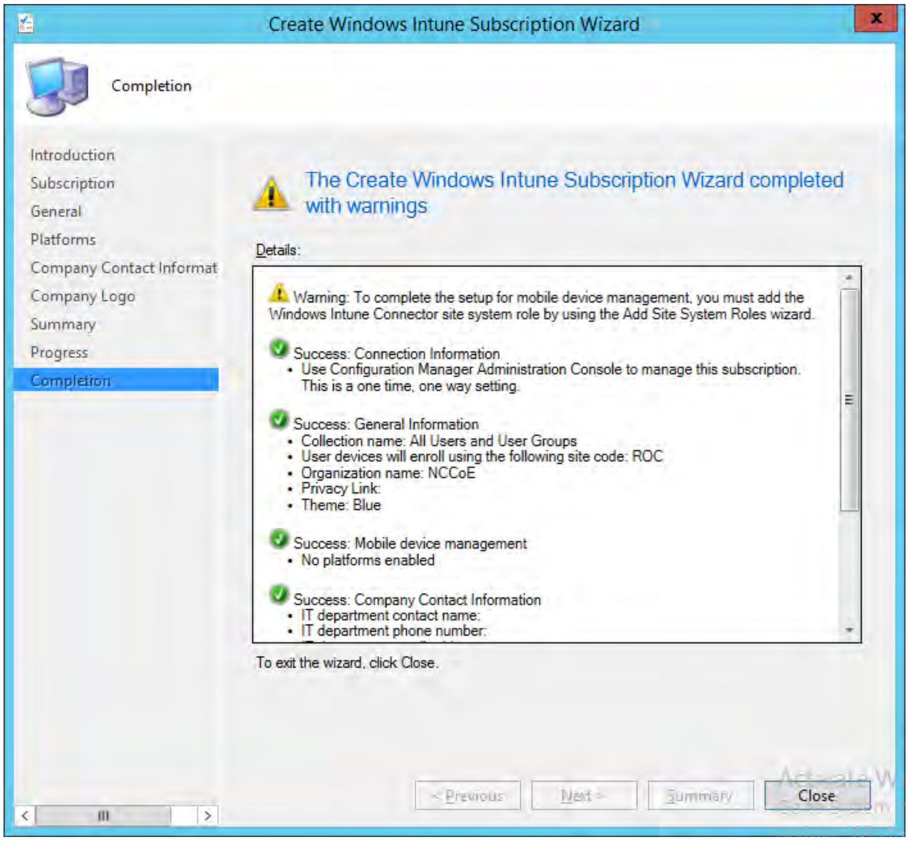
General Information
- Collection name: All Users and User Groups
- User devices will enroll using the following site code: ROC
- Organization name: NCCoE
- Privacy Link:
- Theme: Blue

Mobile device management
- No platforms enabled

Company Contact Information
- IT department contact name:
- IT department phone number:
- IT department email address:
- Support website URL (not displayed to user):
- Website name (displayed to user):
- Additional information:

To change these settings, click Previous. To apply the settings, click Next.

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



The Create Windows Intune Subscription Wizard completed with warnings

Details:

Warning: To complete the setup for mobile device management, you must add the Windows Intune Connector site system role by using the Add Site System Roles wizard.

Success: Connection Information
- Use Configuration Manager Administration Console to manage this subscription. This is a one time, one way setting.

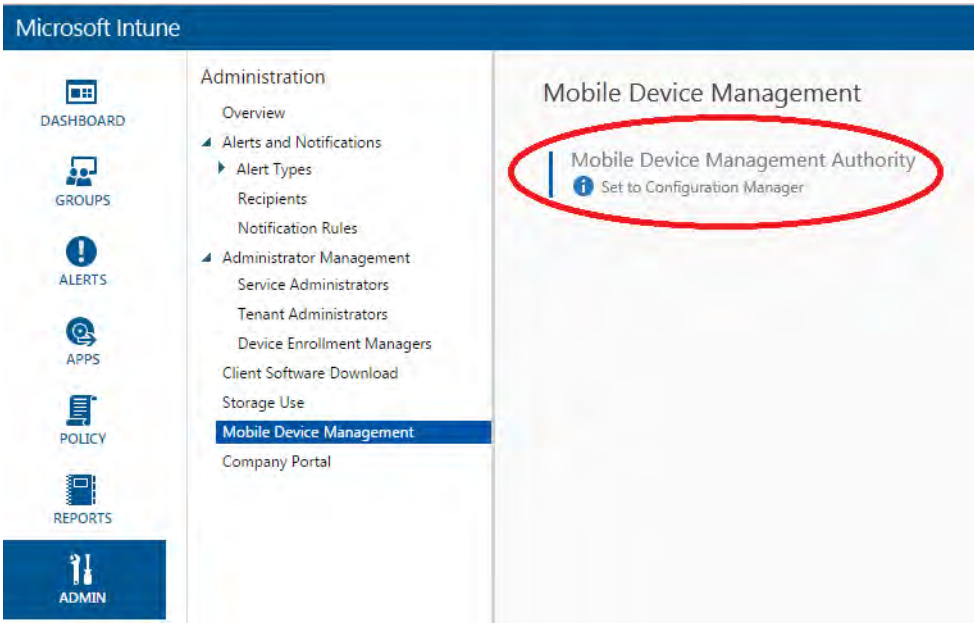
Success: General Information
- Collection name: All Users and User Groups
- User devices will enroll using the following site code: ROC
- Organization name: NCCoE
- Privacy Link:
- Theme: Blue

Success: Mobile device management
- No platforms enabled

Success: Company Contact Information
- IT department contact name:
- IT department phone number:

To exit the wizard, click Close.

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



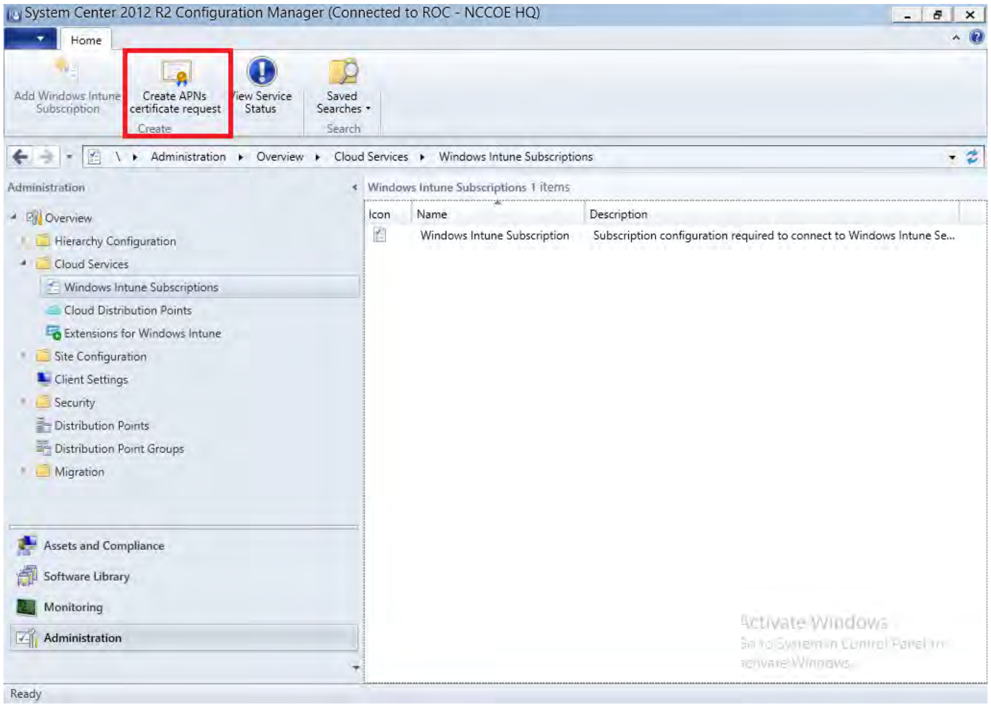
Mobile Device Management

Mobile Device Management Authority
Set to Configuration Manager

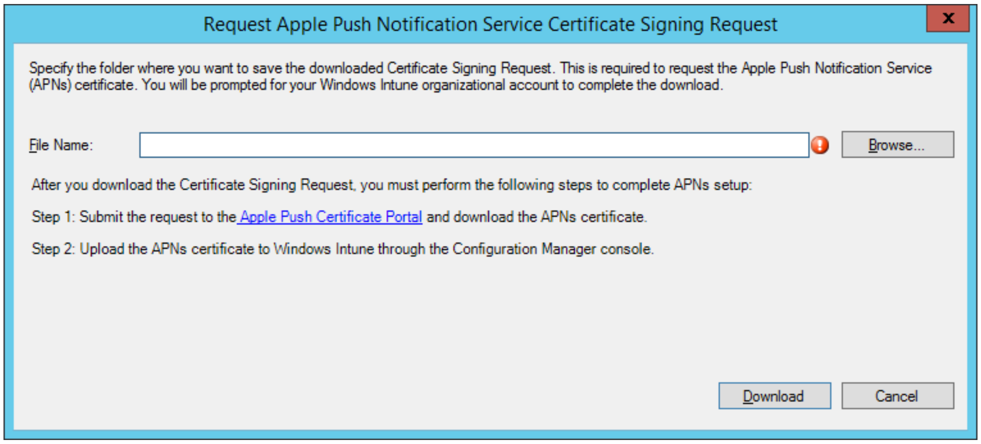
11. The Intune administrative console reflects SCCM management after configuration has been completed.

3.2.5.4.3 Configure Push Certificate for iOS Devices

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


System Center 2012 R2 Configuration Manager (Connected to ROC - NCCOE HQ)
Home
Add Windows Intune Subscription
Create APNs certificate request
View Service Status
Saved Searches
Create
Search
Administration
Overview
Cloud Services
Windows Intune Subscriptions
Administration
Overview
Hierarchy Configuration
Cloud Services
Windows Intune Subscriptions
Cloud Distribution Points
Extensions for Windows Intune
Site Configuration
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Assets and Compliance
Software Library
Monitoring
Administration
Windows Intune Subscriptions 1 items
Icon
Name
Description
Windows Intune Subscription
Subscription configuration required to connect to Windows Intune Se...
Activate Windows
Ready

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



Request Apple Push Notification Service Certificate Signing Request

Specify the folder where you want to save the downloaded Certificate Signing Request. This is required to request the Apple Push Notification Service (APNs) certificate. You will be prompted for your Windows Intune organizational account to complete the download.

File Name:

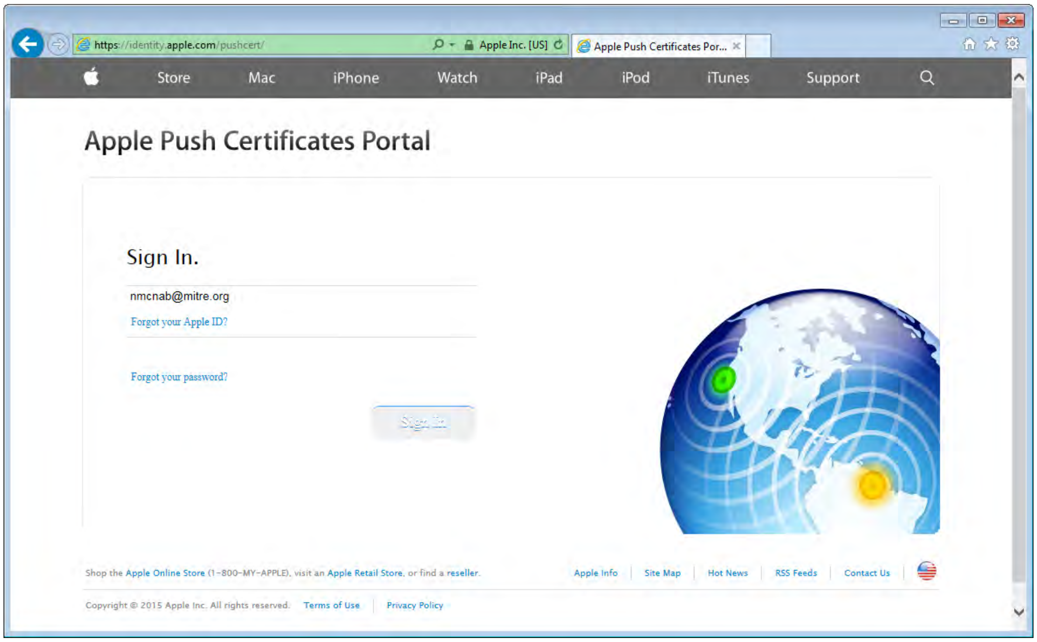
After you download the Certificate Signing Request, you must perform the following steps to complete APNs setup:

Step 1: Submit the request to the Apple Push Certificate Portal and download the APNs certificate.

Step 2: Upload the APNs certificate to Windows Intune through the Configuration Manager console.

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.


https://identity.apple.com/pushcert/
Apple Inc. [US]
Apple Push Certificates Por...
Store
Mac
iPhone
Watch
iPad
iPod
iTunes
Support
Sign In

Apple Push Certificates Portal

Sign In.

nmcnab@mitre.org

Forgot your Apple ID?

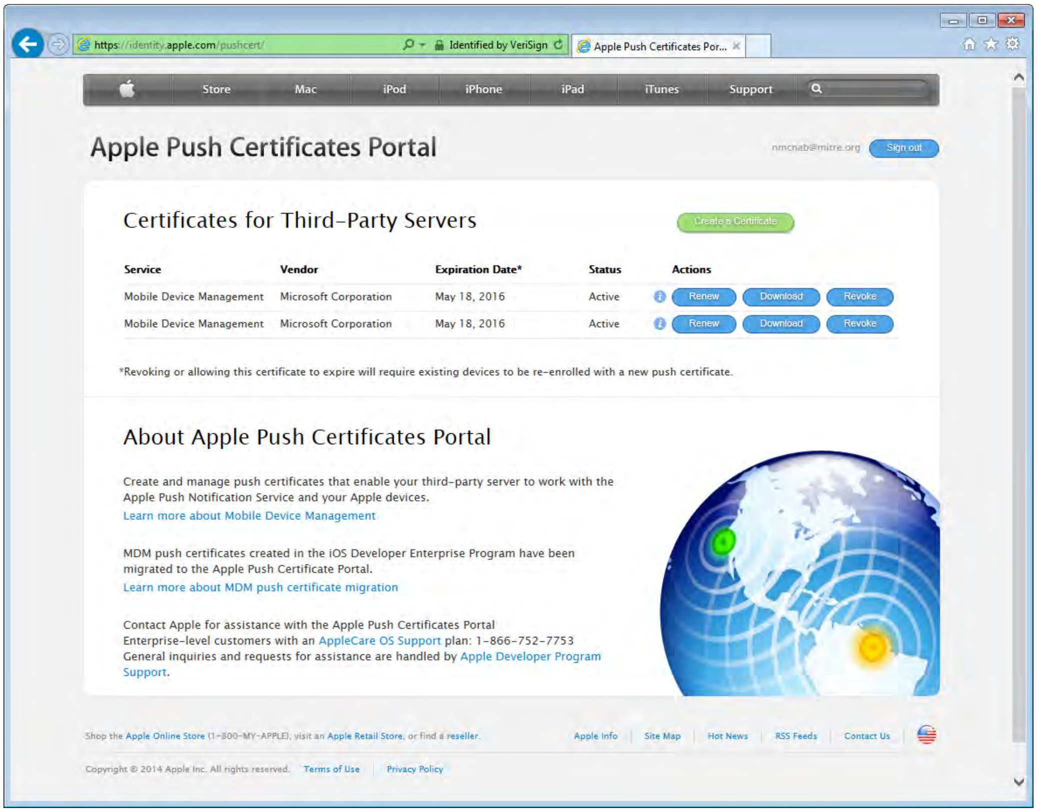
Forgot your password?

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2015 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

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



Apple Push Certificates Portal

nmcnab@mitre.org

Certificates for Third-Party Servers

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

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

About Apple Push Certificates Portal

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

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

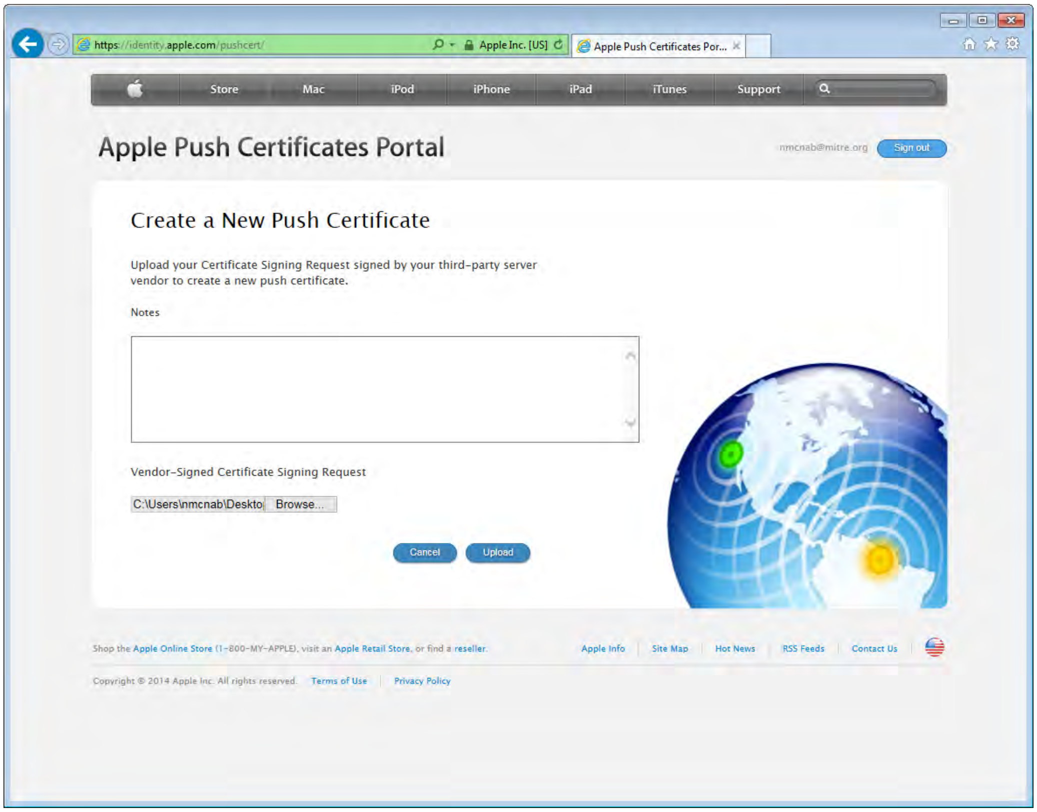
Contact Apple for assistance with the Apple Push Certificates Portal
Enterprise-level customers with an AppleCare OS Support plan: 1-866-752-7753
General inquiries and requests for assistance are handled by Apple Developer Program Support.

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

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



https://identity.apple.com/pushcert/
Apple Inc. [US]
Apple Push Certificates Por...
Store
Mac
iPod
iPhone
iPad
iTunes
Support

Apple Push Certificates Portal

nmcnab@mitre.org

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

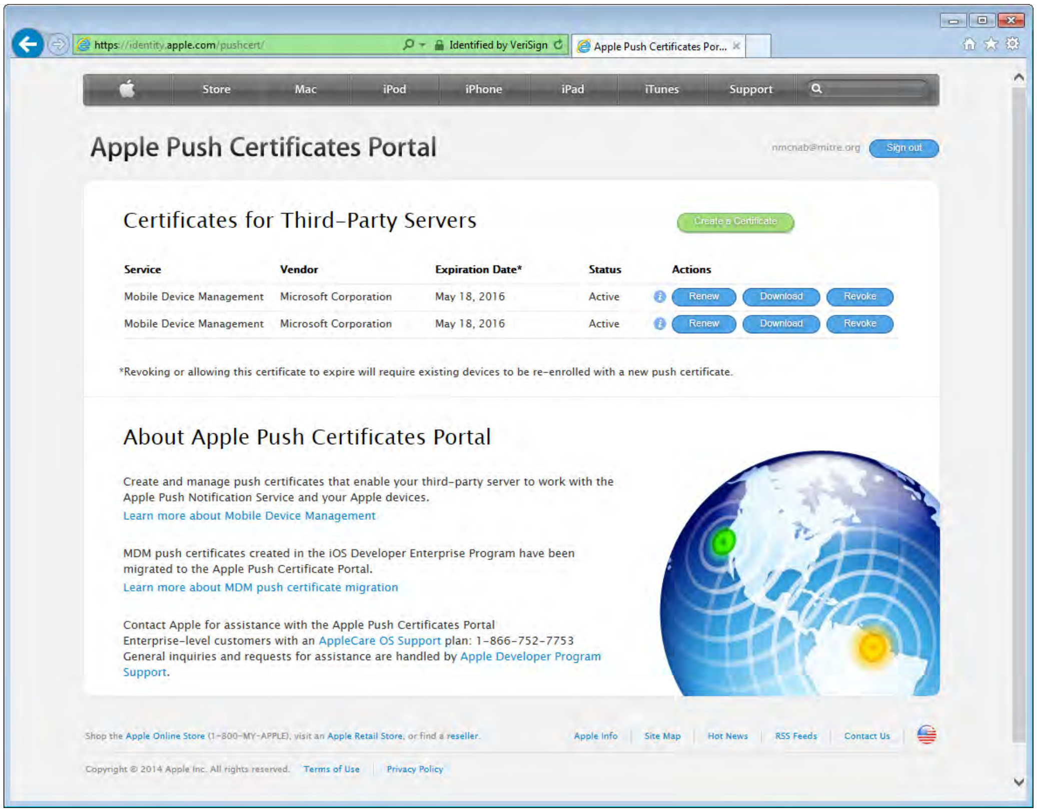
Vendor-Signed Certificate Signing Request

C:\Users\nmcnab\Deskto

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Copyright © 2014 Apple Inc. All rights reserved.

6. 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.



Apple Push Certificates Portal

Certificates for Third-Party Servers

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

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

About Apple Push Certificates Portal

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

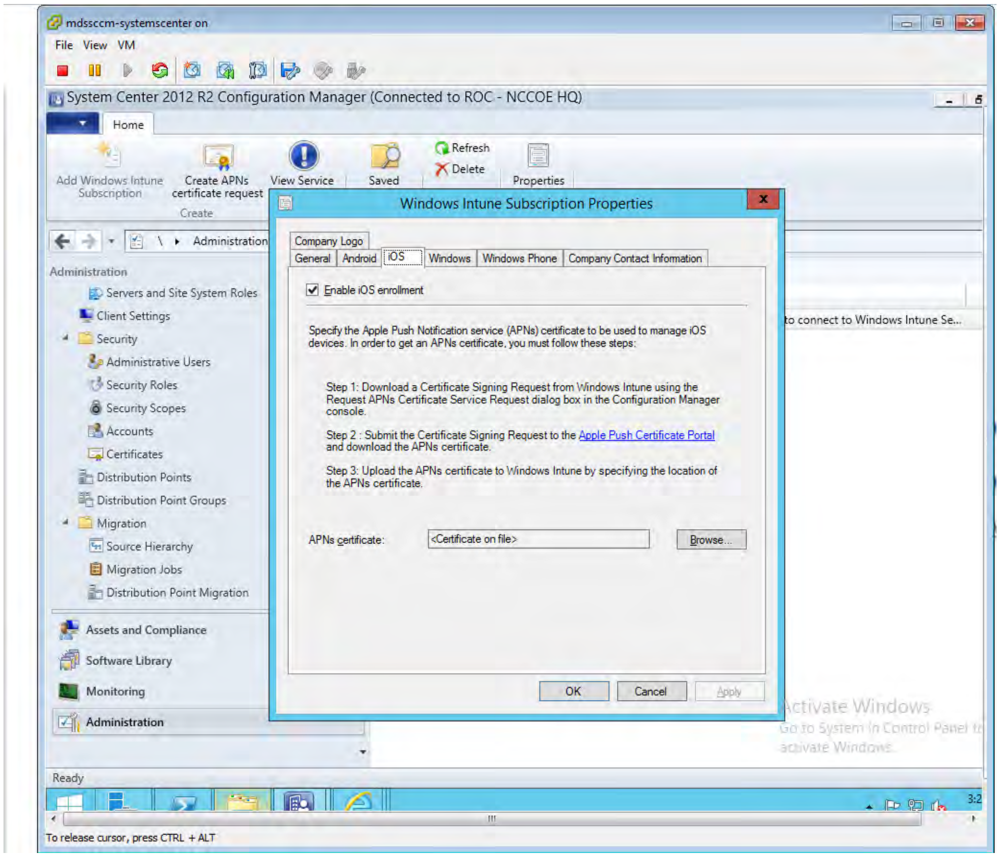
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
Learn more about MDM push certificate migration

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

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller. Apple Info | Site Map | Hot News | RSS Feeds | Contact Us

Copyright © 2014 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

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**.


mdssccm-systemscenter on
File View VM
System Center 2012 R2 Configuration Manager (Connected to ROC - NCCOE HQ)
Home
Add Windows Intune Subscription
Create APNs certificate request
View Service
Saved
Refresh
Delete
Properties
Create
Administration
Servers and Site System Roles
Client Settings
Security
Administrative Users
Security Roles
Security Scopes
Accounts
Certificates
Distribution Points
Distribution Point Groups
Migration
Source Hierarchy
Migration Jobs
Distribution Point Migration
Assets and Compliance
Software Library
Monitoring
Administration
to connect to Windows Intune Se...
Activate Windows
Go to System in Control Panel to activate Windows.
Ready
To release cursor, press CTRL + ALT

Windows Intune Subscription Properties

Company Logo | General | Android | iOS | Windows | Windows Phone | Company Contact Information

☑ Enable iOS enrollment

Specify the Apple Push Notification service (APNs) certificate to be used to manage iOS devices. In order to get an APNs certificate, you must follow these steps:

Step 1: Download a Certificate Signing Request from Windows Intune using the Request APNs Certificate Service Request dialog box in the Configuration Manager console.

Step 2 : Submit the Certificate Signing Request to the Apple Push Certificate Portal and download the APNs certificate.

Step 3: Upload the APNs certificate to Windows Intune by specifying the location of the APNs certificate.

APNs certificate: <Certificate on file> Browse...

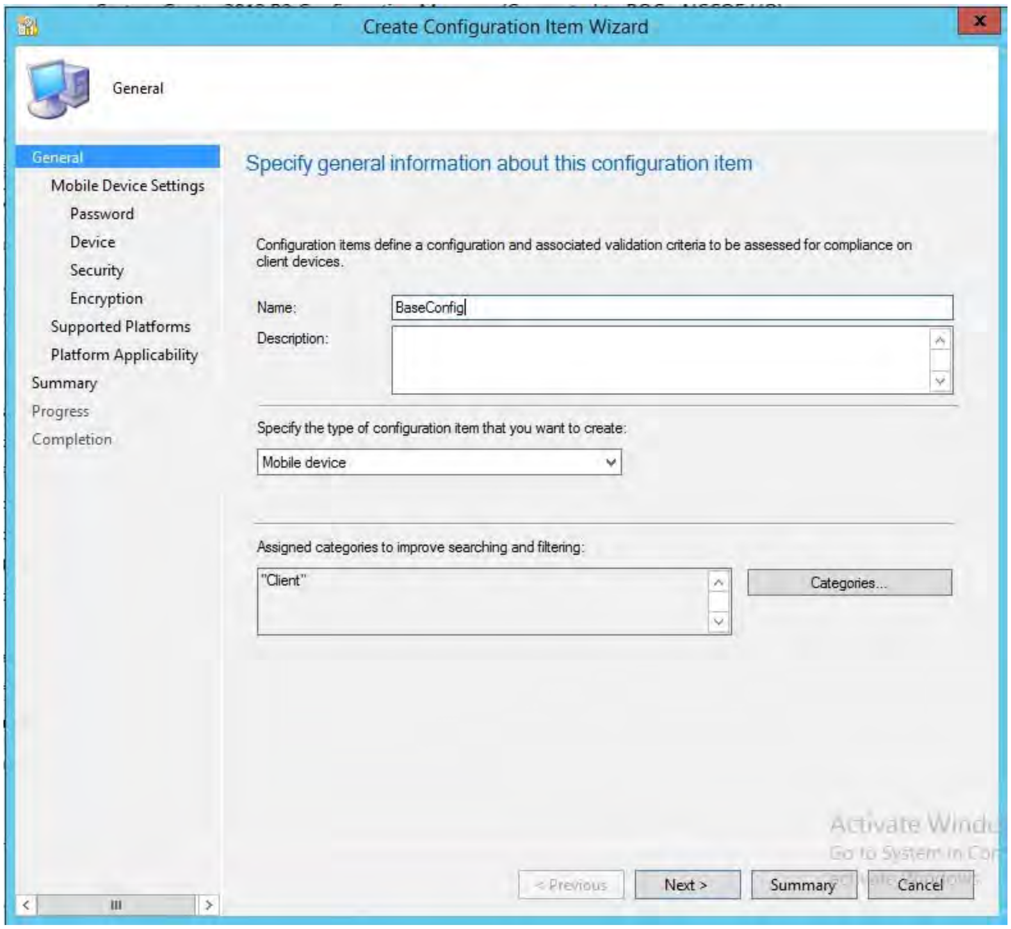
OK Cancel Apply

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.



Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on client devices.

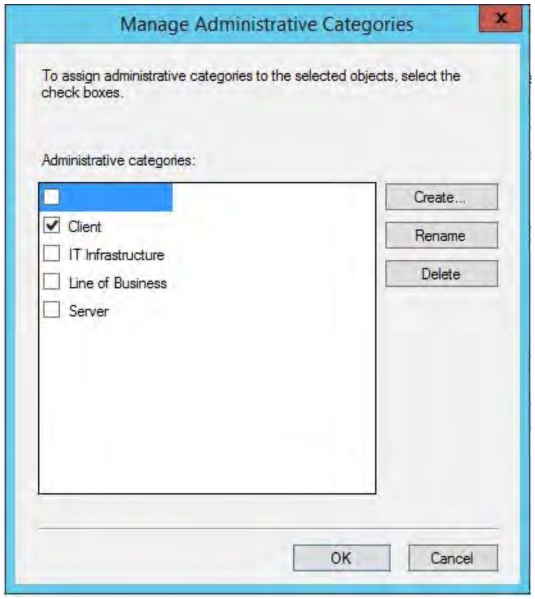
Name: BaseConfig

Description:

Specify the type of configuration item that you want to create: Mobile device

Assigned categories to improve searching and filtering: "Client"

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



To assign administrative categories to the selected objects, select the check boxes.

Administrative categories:

□

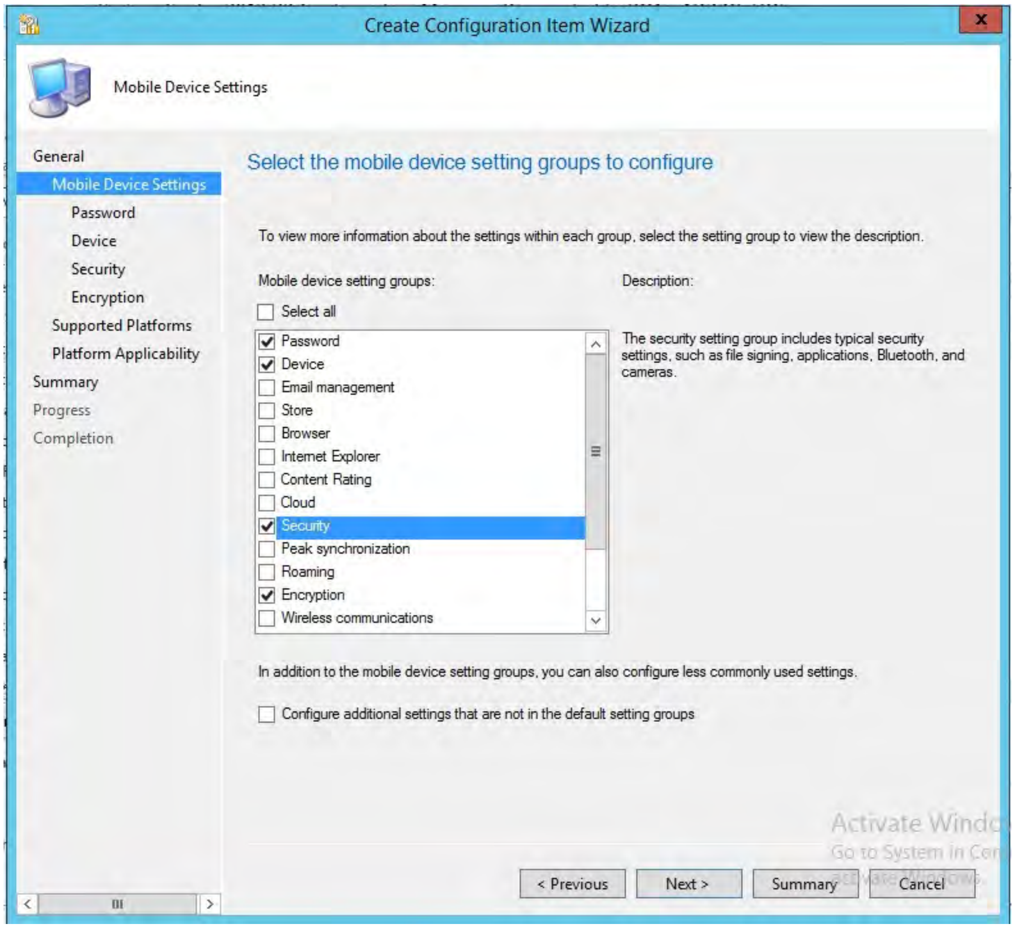
☑ Client

□ IT Infrastructure

□ Line of Business

□ Server

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



Select the mobile device setting groups to configure

To view more information about the settings within each group, select the setting group to view the description.

Mobile device setting groups:

□ Select all

☑ Password
☑ Device
□ Email management
□ Store
□ Browser
□ Internet Explorer
□ Content Rating
□ Cloud
☑ Security
□ Peak synchronization
□ Roaming
☑ Encryption
□ Wireless communications

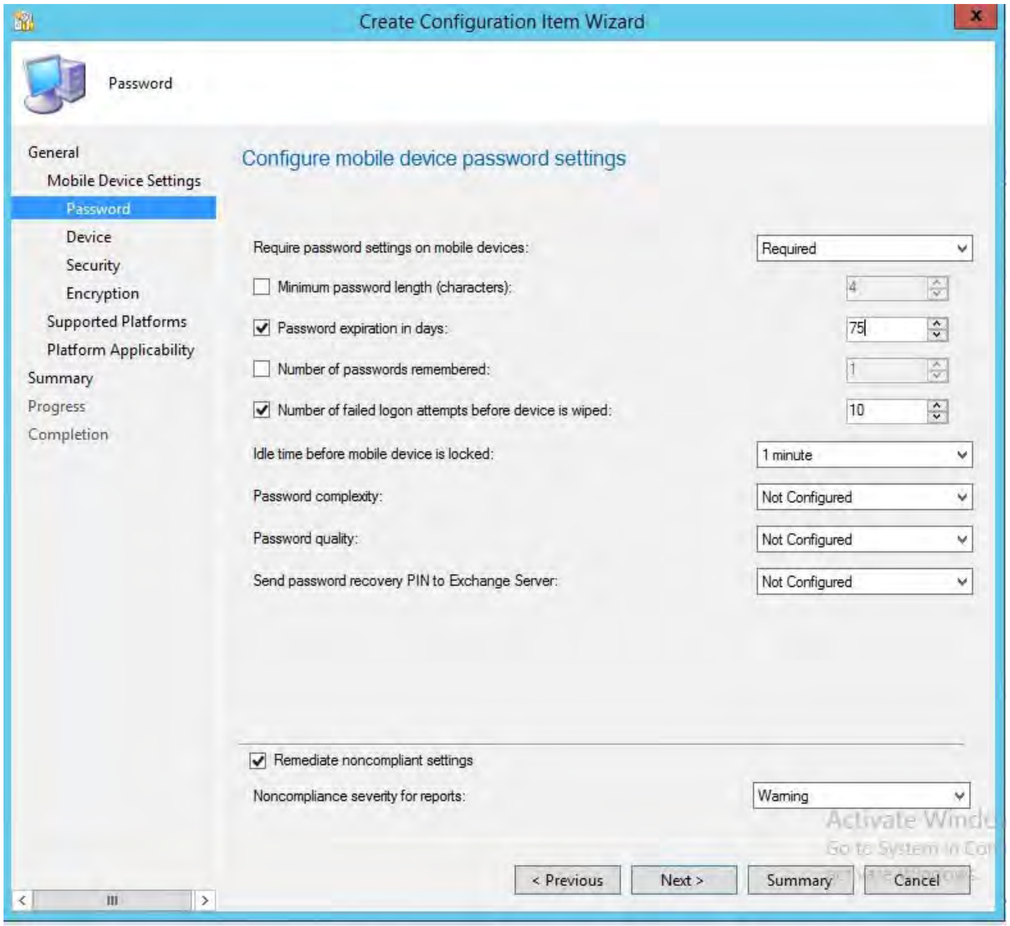
Description:

The security setting group includes typical security settings, such as file signing, applications, Bluetooth, and cameras.

In addition to the mobile device setting groups, you can also configure less commonly used settings.

□ Configure additional settings that are not in the default setting groups

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



Configure mobile device password settings

Require password settings on mobile devices: Required

□ Minimum password length (characters): 4

☑ Password expiration in days: 75

□ Number of passwords remembered: 1

☑ Number of failed logon attempts before device is wiped: 10

Idle time before mobile device is locked: 1 minute

Password complexity: Not Configured

Password quality: Not Configured

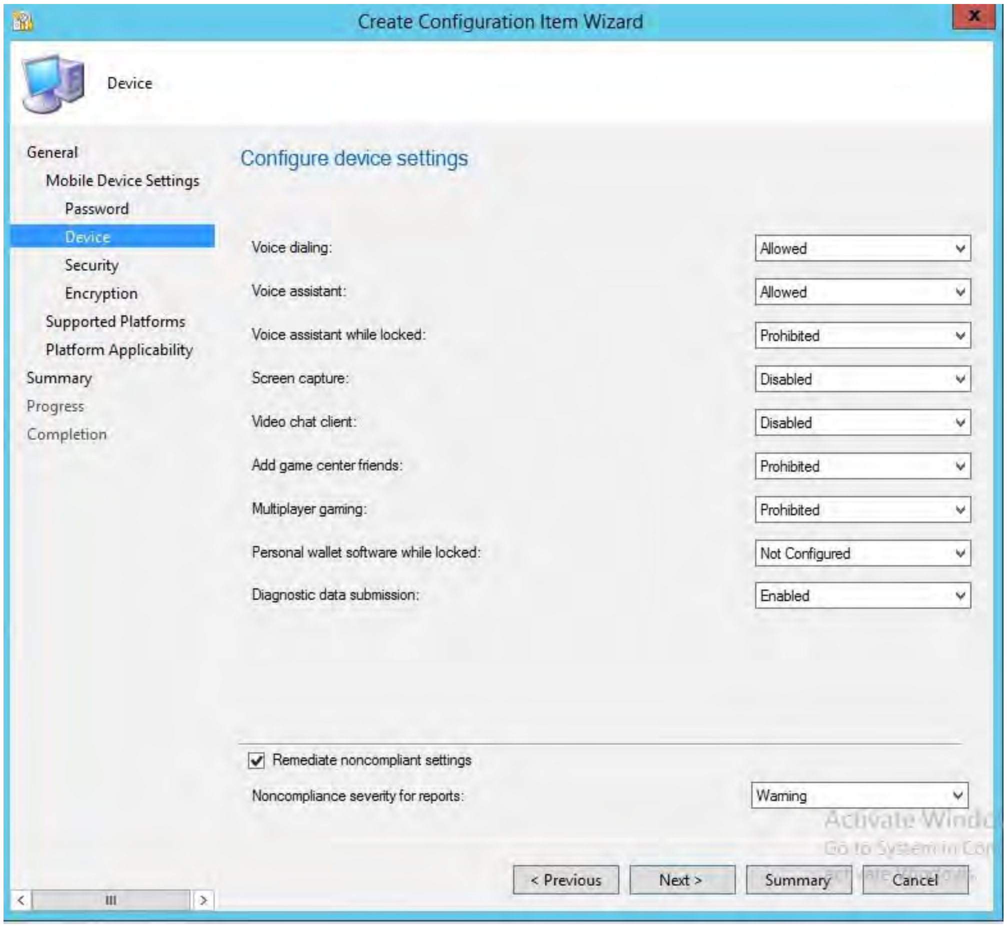
Send password recovery PIN to Exchange Server: Not Configured

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Activate Windo
Go to System in Con

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



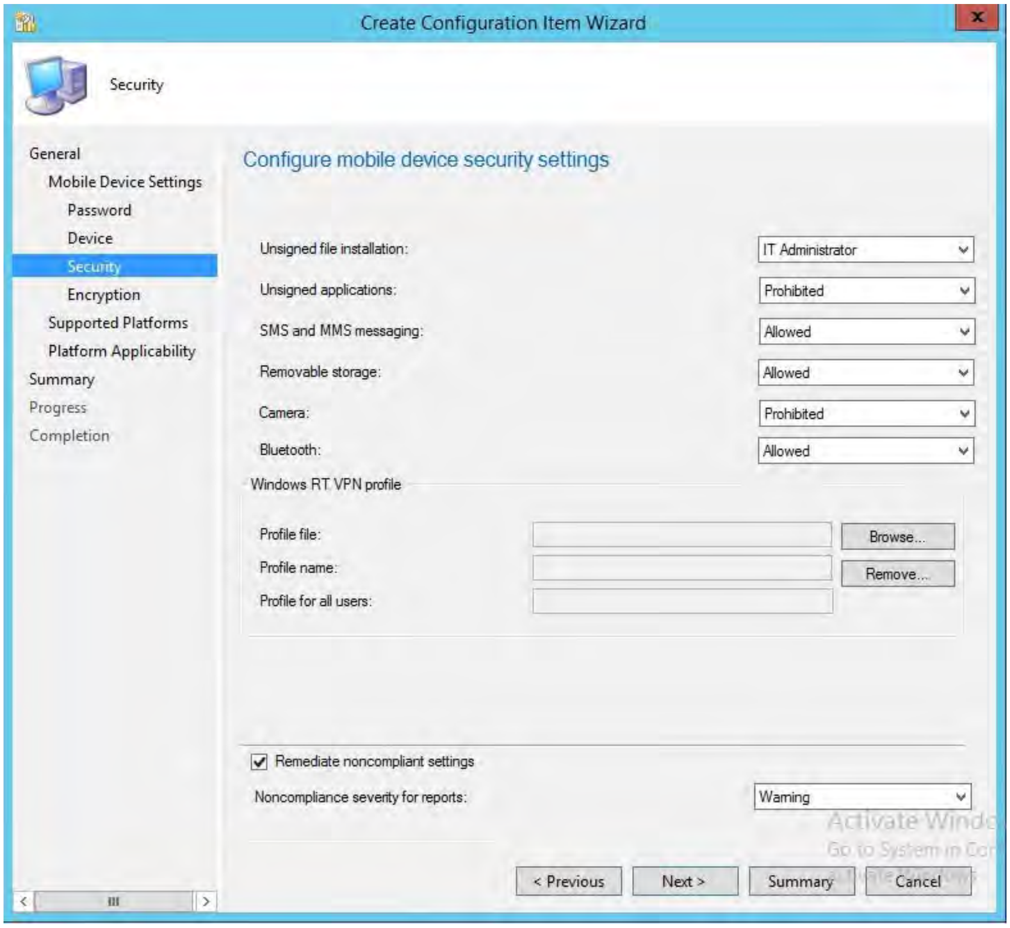
Configure device settings

Voice dialing:	Allowed
Voice assistant:	Allowed
Voice assistant while locked:	Prohibited
Screen capture:	Disabled
Video chat client:	Disabled
Add game center friends:	Prohibited
Multiplayer gaming:	Prohibited
Personal wallet software while locked:	Not Configured
Diagnostic data submission:	Enabled

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

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



Create Configuration Item Wizard

Security

Configure mobile device security settings

Unsigned file installation: IT Administrator

Unsigned applications: Prohibited

SMS and MMS messaging: Allowed

Removable storage: Allowed

Camera: Prohibited

Bluetooth: Allowed

Windows RT VPN profile

Profile file:

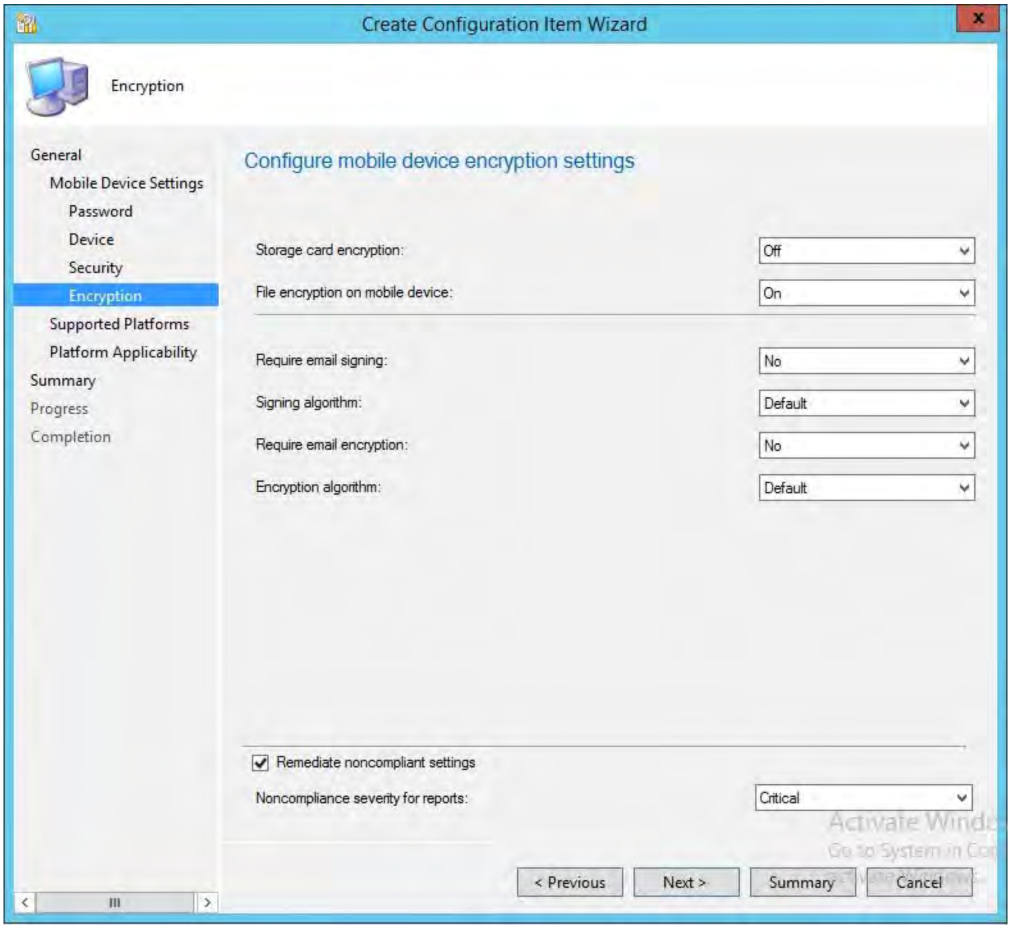
Profile name:

Profile for all users:

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

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



Configure mobile device encryption settings

Storage card encryption: Off

File encryption on mobile device: On

Require email signing: No

Signing algorithm: Default

Require email encryption: No

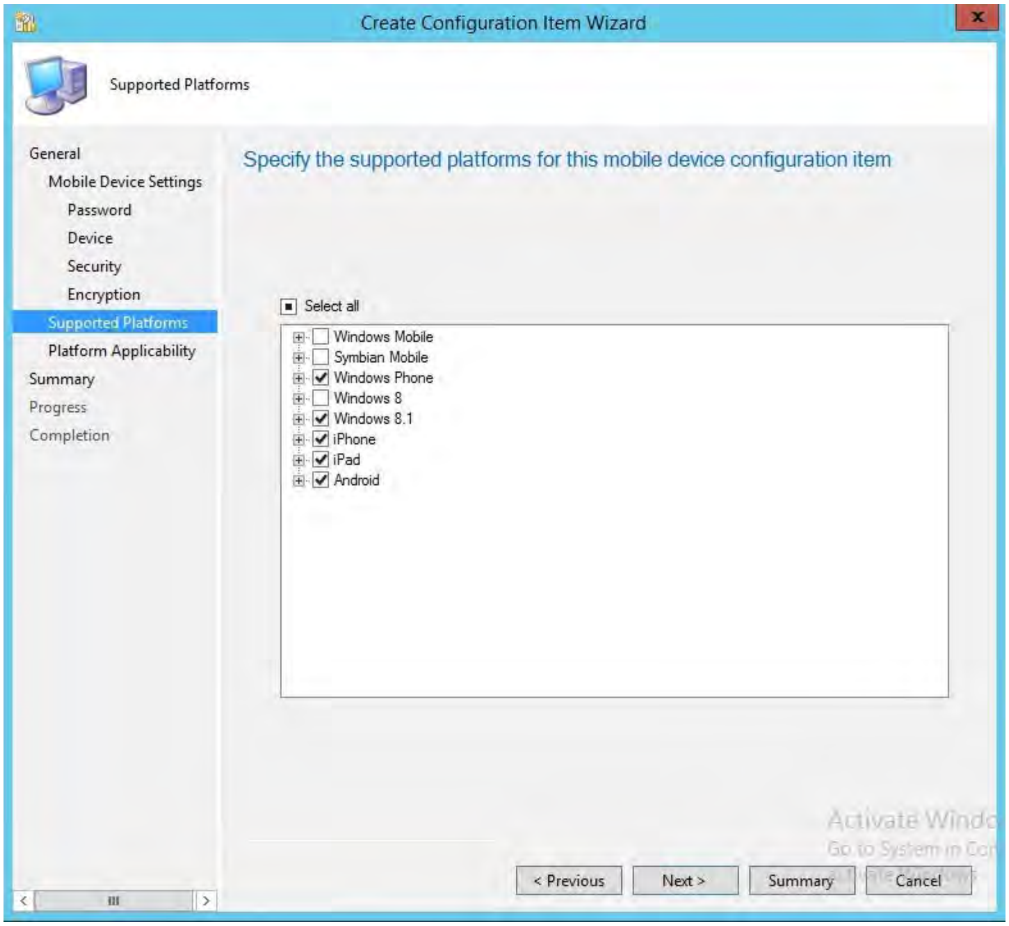
Encryption algorithm: Default

☑ Remediate noncompliant settings

Noncompliance severity for reports: Critical

323

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

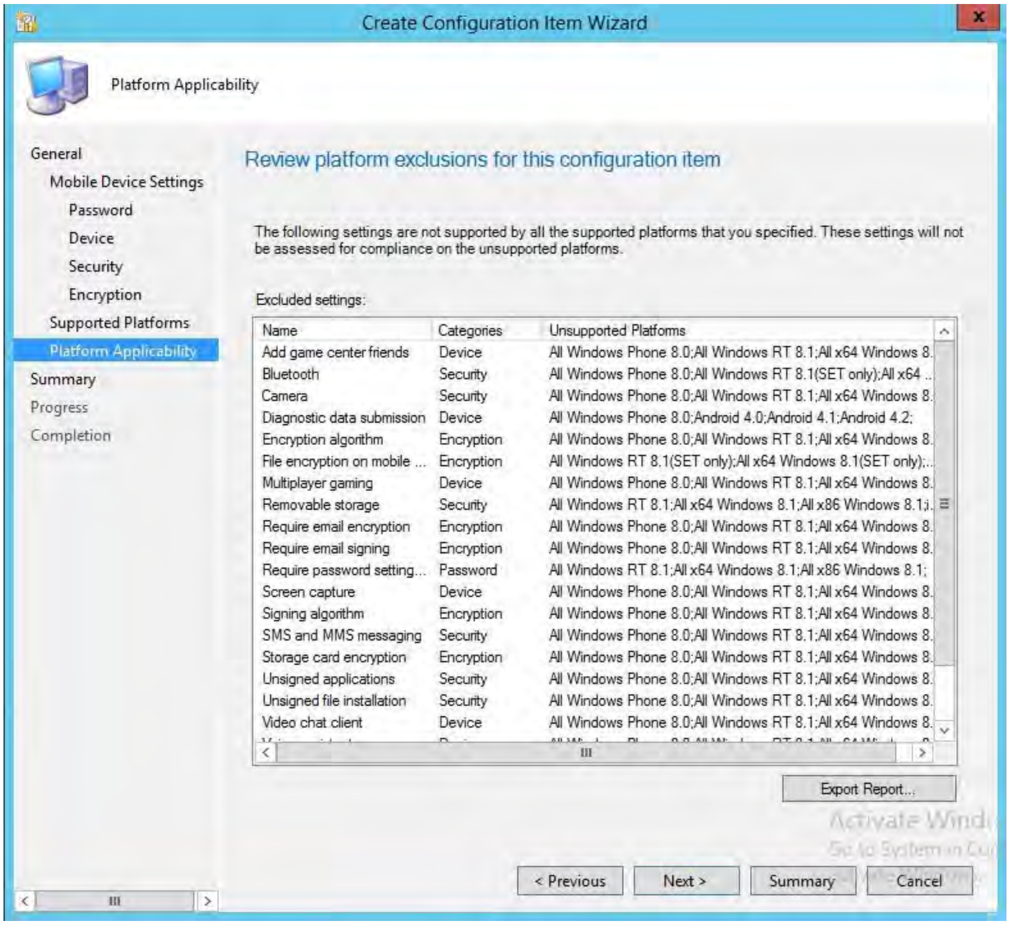


Specify the supported platforms for this mobile device configuration item

■ Select all

- □ Windows Mobile
- □ Symbian Mobile
- ☑ Windows Phone
- □ Windows 8
- ☑ Windows 8.1
- ☑ iPhone
- ☑ iPad
- ☑ Android

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



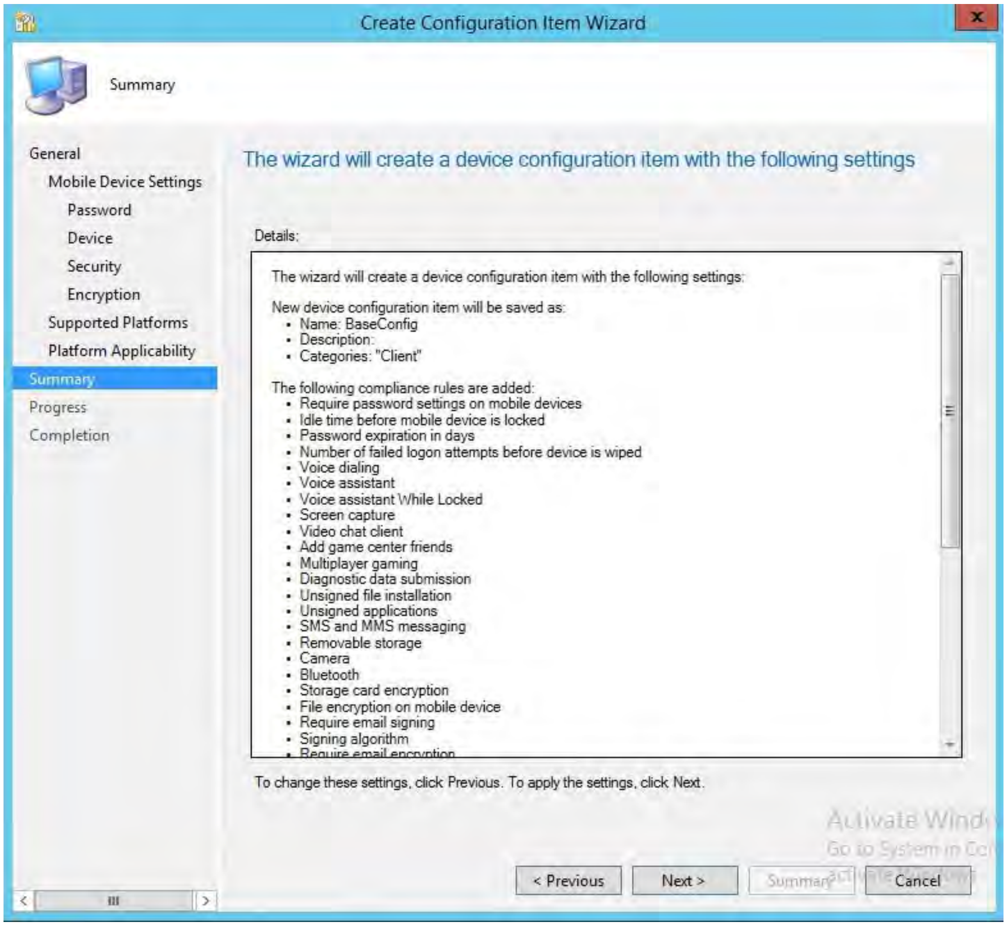
Review platform exclusions for this configuration item

The following settings are not supported by all the supported platforms that you specified. These settings will not be assessed for compliance on the unsupported platforms.

Excluded settings:

Name	Categories	Unsupported Platforms
Add game center friends	Device	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Bluetooth	Security	All Windows Phone 8.0;All Windows RT 8.1(SET only);All x64 ..
Camera	Security	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Diagnostic data submission	Device	All Windows Phone 8.0;Android 4.0;Android 4.1;Android 4.2;
Encryption algorithm	Encryption	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
File encryption on mobile ...	Encryption	All Windows RT 8.1(SET only);All x64 Windows 8.1(SET only);..
Multiplayer gaming	Device	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Removable storage	Security	All Windows RT 8.1;All x64 Windows 8.1;All x86 Windows 8.1;i.
Require email encryption	Encryption	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Require email signing	Encryption	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Require password setting...	Password	All Windows RT 8.1;All x64 Windows 8.1;All x86 Windows 8.1;
Screen capture	Device	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Signing algorithm	Encryption	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
SMS and MMS messaging	Security	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Storage card encryption	Encryption	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Unsigned applications	Security	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Unsigned file installation	Security	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.
Video chat client	Device	All Windows Phone 8.0;All Windows RT 8.1;All x64 Windows 8.

10. Click **Next**.



The wizard will create a device configuration item with the following settings

Details:

The wizard will create a device configuration item with the following settings:

New device configuration item will be saved as:

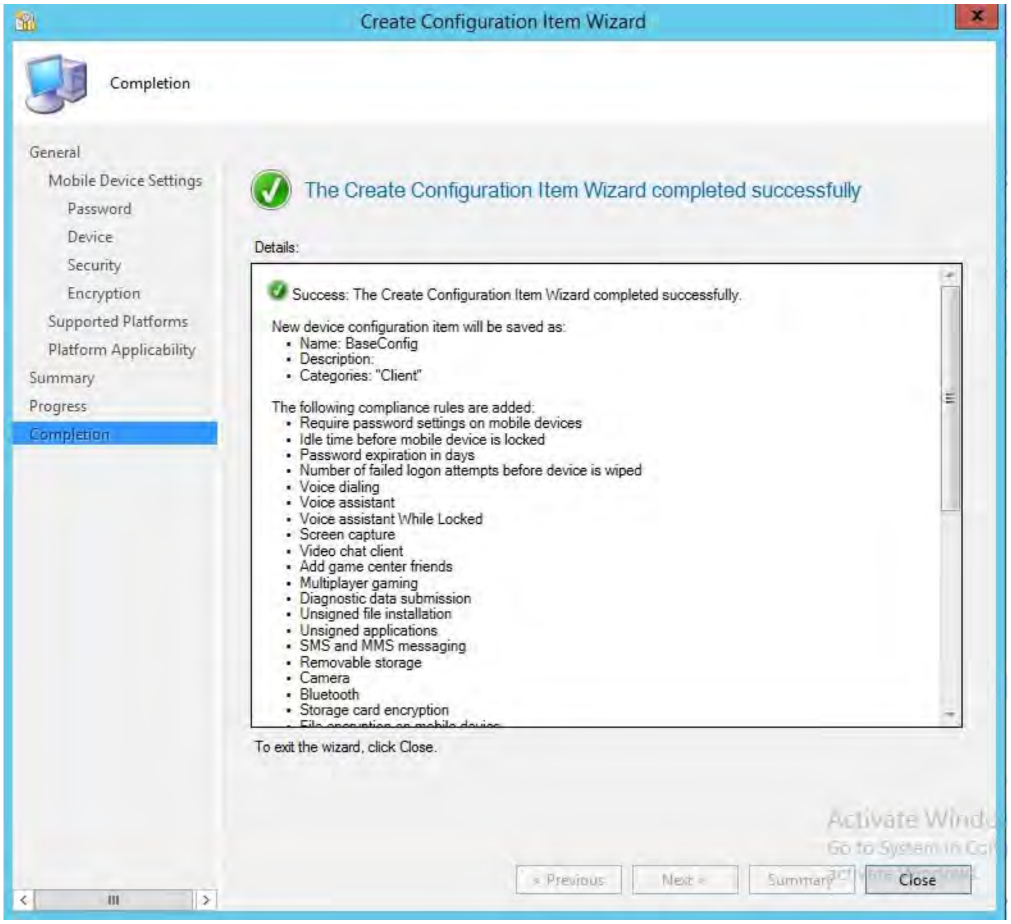
- Name: BaseConfig
- Description:
- Categories: "Client"

The following compliance rules are added:

- Require password settings on mobile devices
- Idle time before mobile device is locked
- Password expiration in days
- Number of failed logon attempts before device is wiped
- Voice dialing
- Voice assistant
- Voice assistant While Locked
- Screen capture
- Video chat client
- Add game center friends
- Multiplayer gaming
- Diagnostic data submission
- Unsigned file installation
- Unsigned applications
- SMS and MMS messaging
- Removable storage
- Camera
- Bluetooth
- Storage card encryption
- File encryption on mobile device
- Require email signing
- Signing algorithm
- Require email encryption

To change these settings, click Previous. To apply the settings, click Next.

11. Click **Next**.



The Create Configuration Item Wizard completed successfully

Details:

Success: The Create Configuration Item Wizard completed successfully.

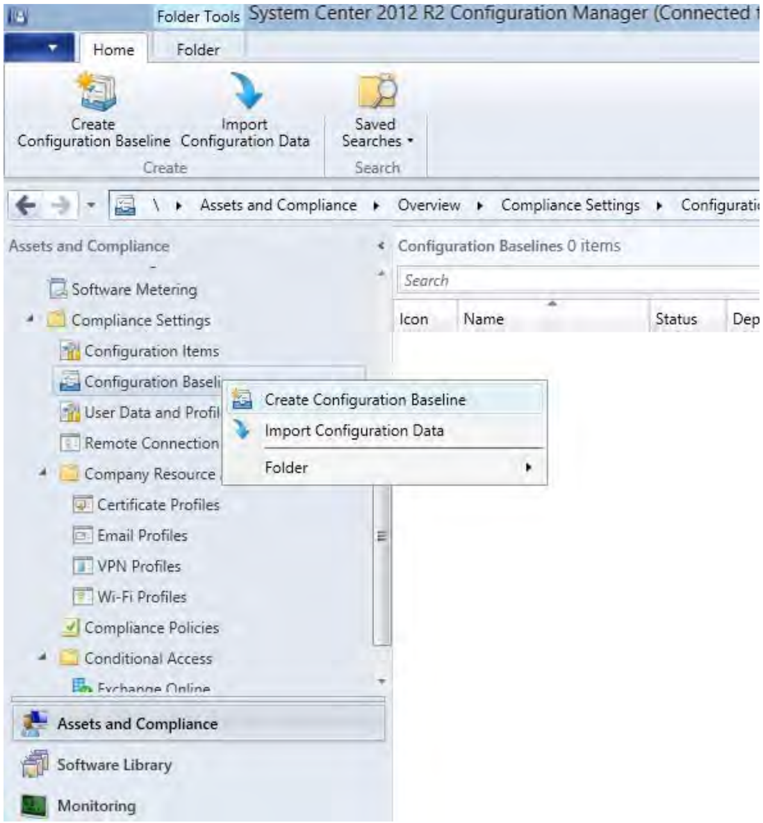
New device configuration item will be saved as:
- Name: BaseConfig
- Description:
- Categories: "Client"

The following compliance rules are added:
- Require password settings on mobile devices
- Idle time before mobile device is locked
- Password expiration in days
- Number of failed logon attempts before device is wiped
- Voice dialing
- Voice assistant
- Voice assistant While Locked
- Screen capture
- Video chat client
- Add game center friends
- Multiplayer gaming
- Diagnostic data submission
- Unsigned file installation
- Unsigned applications
- SMS and MMS messaging
- Removable storage
- Camera
- Bluetooth
- Storage card encryption
- File encryption on mobile device

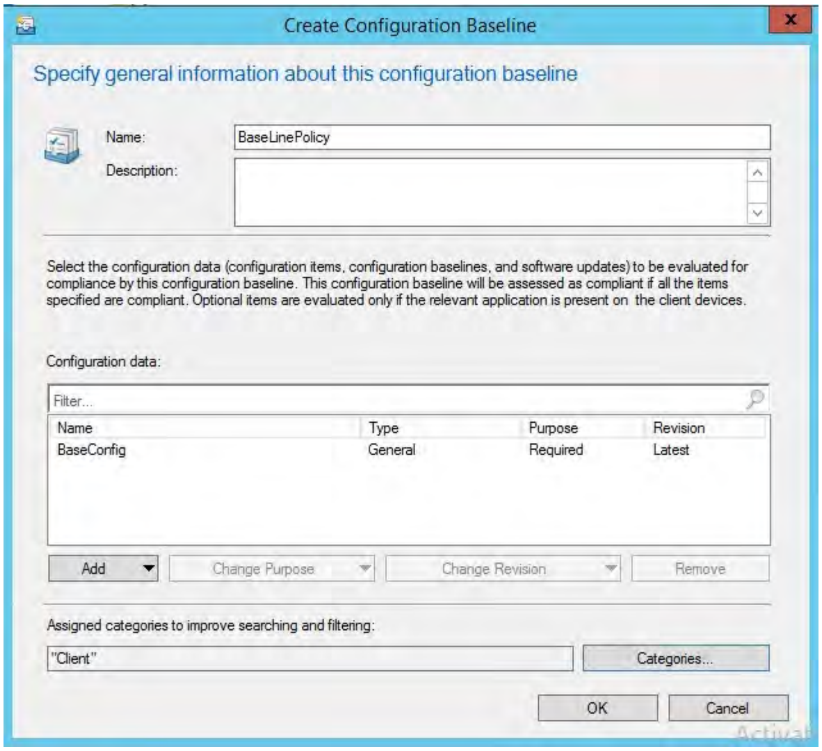
To exit the wizard, click Close.

331

332 12. Click **Close**.



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



Specify general information about this configuration baseline

Name: BaseLinePolicy

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

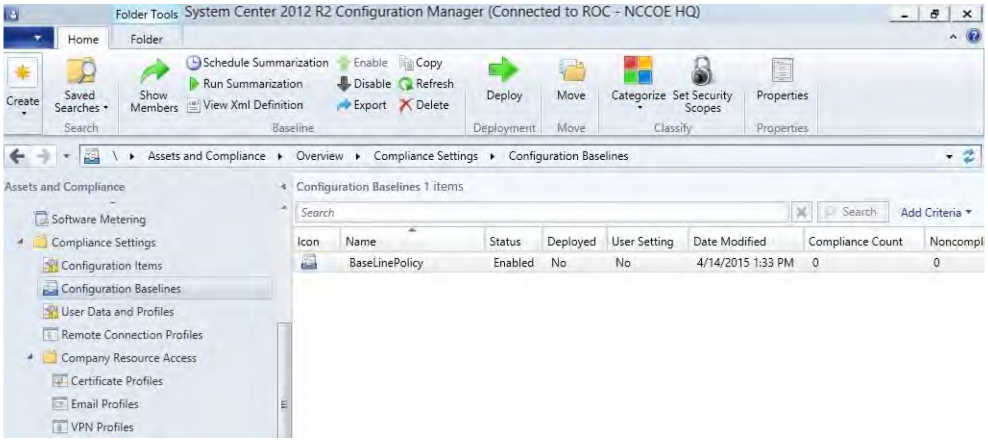
Configuration data:

Name	Type	Purpose	Revision
BaseConfig	General	Required	Latest

Assigned categories to improve searching and filtering:

"Client"

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

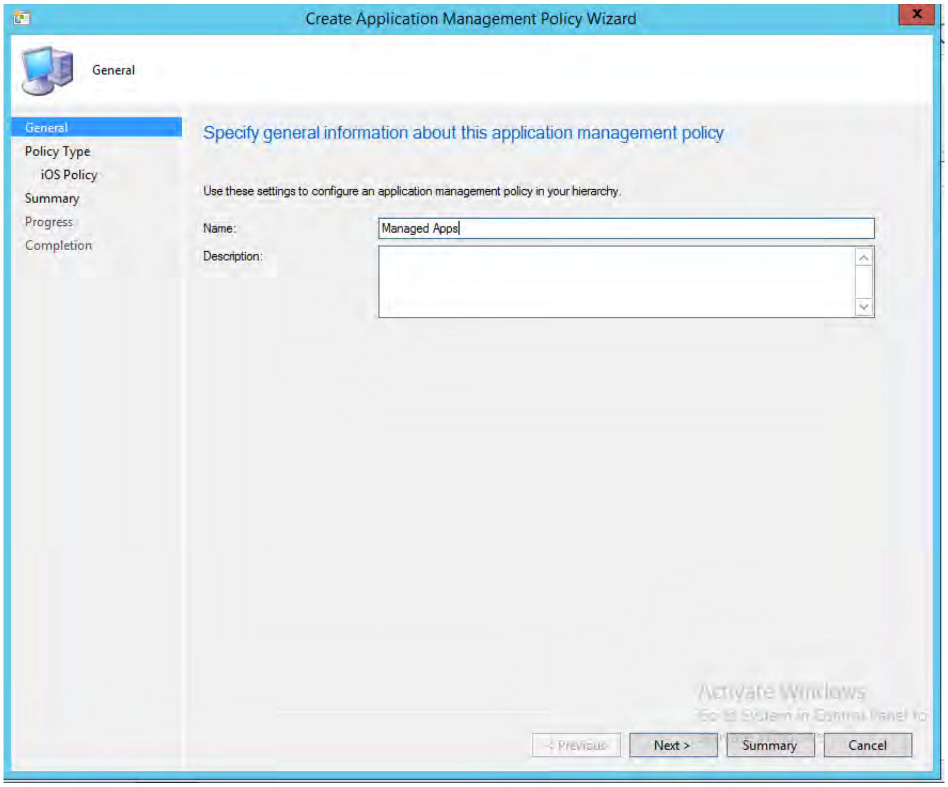


Configuration Baselines 1 items

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompl
	BaseLinePolicy	Enabled	No	No	4/14/2015 1:33 PM	0	0

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.



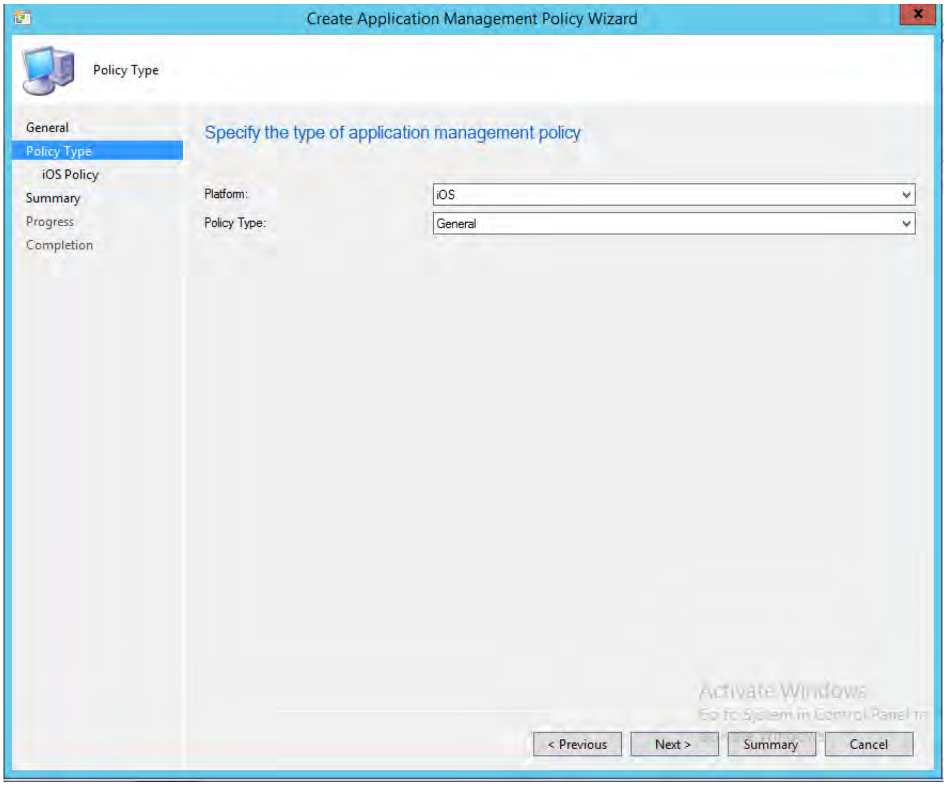
Specify general information about this application management policy

Use these settings to configure an application management policy in your hierarchy.

Name: Managed Apps

Description:

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

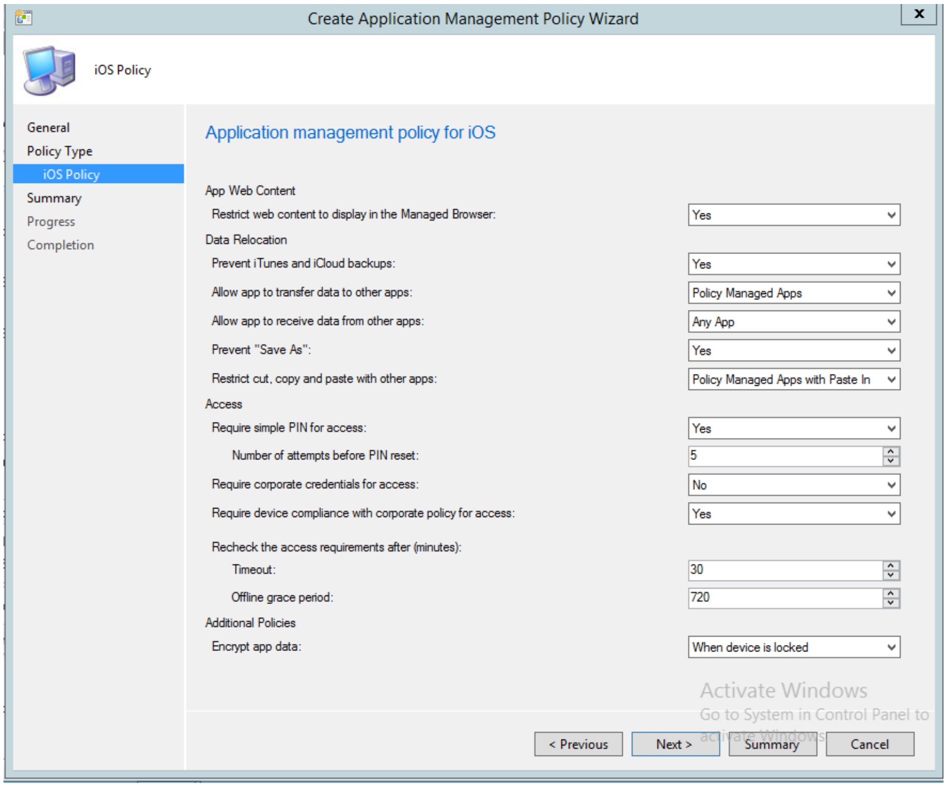


Specify the type of application management policy

Platform: iOS

Policy Type: General

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



Application management policy for iOS

App Web Content

Restrict web content to display in the Managed Browser: Yes

Data Relocation

Prevent iTunes and iCloud backups: Yes

Allow app to transfer data to other apps: Policy Managed Apps

Allow app to receive data from other apps: Any App

Prevent "Save As": Yes

Restrict cut, copy and paste with other apps: Policy Managed Apps with Paste In

Access

Require simple PIN for access: Yes

Number of attempts before PIN reset: 5

Require corporate credentials for access: No

Require device compliance with corporate policy for access: Yes

Recheck the access requirements after (minutes):

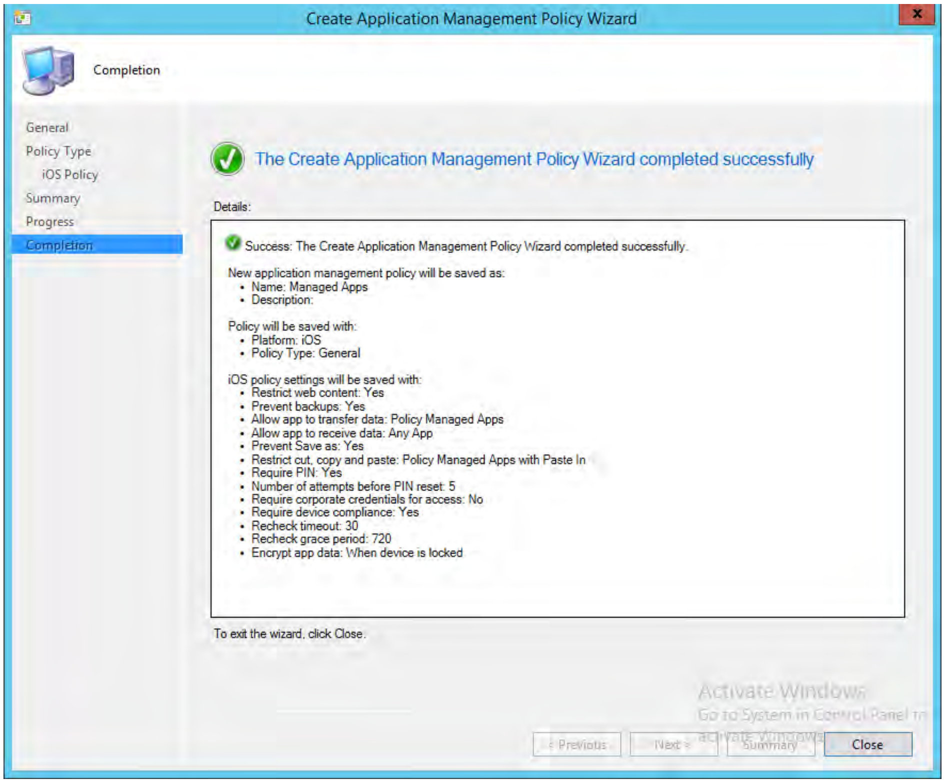
Timeout: 30

Offline grace period: 720

Additional Policies

Encrypt app data: When device is locked

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



The Create Application Management Policy Wizard completed successfully

Details:

Success: The Create Application Management Policy Wizard completed successfully.

New application management policy will be saved as:
- Name: Managed Apps
- Description:

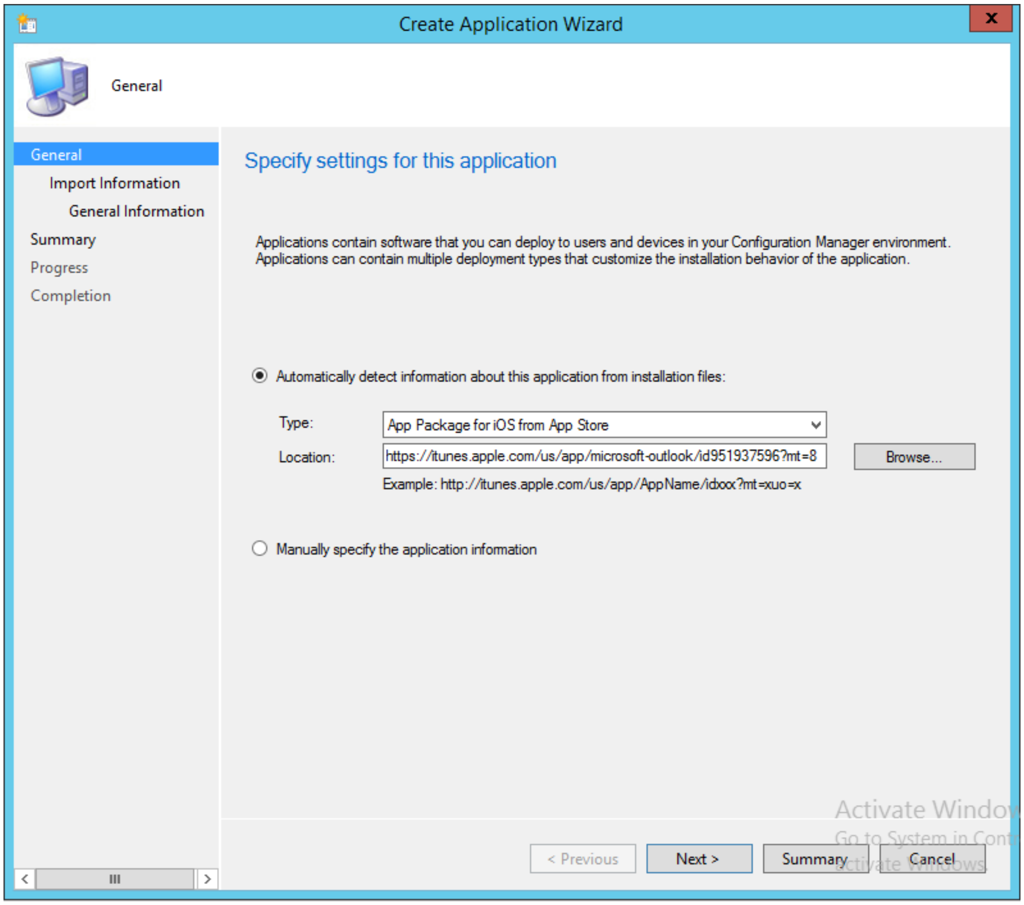
Policy will be saved with:
- Platform: iOS
- Policy Type: General

iOS policy settings will be saved with:
- Restrict web content: Yes
- Prevent backups: Yes
- Allow app to transfer data: Policy Managed Apps
- Allow app to receive data: Any App
- Prevent Save as: Yes
- Restrict cut, copy and paste: Policy Managed Apps with Paste In
- Require PIN: Yes
- Number of attempts before PIN reset: 5
- Require corporate credentials for access: No
- Require device compliance: Yes
- Recheck timeout: 30
- Recheck grace period: 720
- Encrypt app data: When device is locked

To exit the wizard, click Close.

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

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



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

● Automatically detect information about this application from installation files:

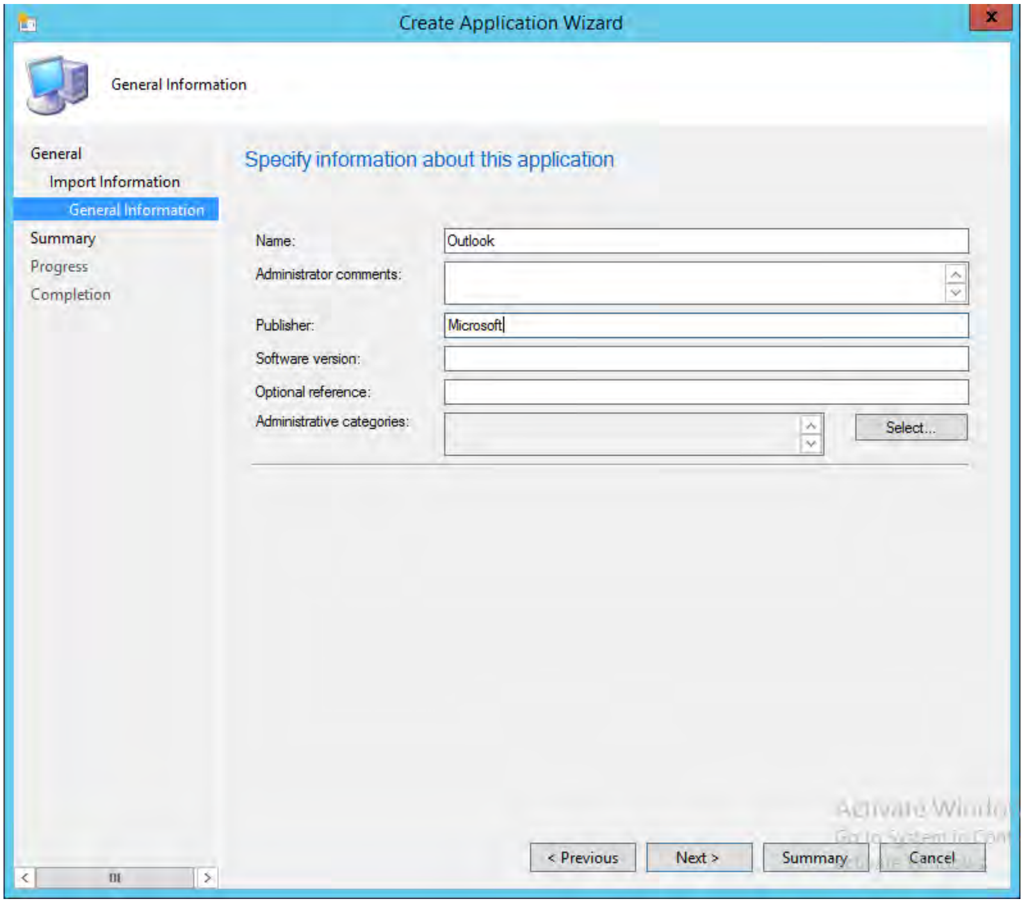
Type: App Package for iOS from App Store

Location: https://itunes.apple.com/us/app/microsoft-outlook/id951937596?mt=8

Example: http://itunes.apple.com/us/app/AppName/idxxx?mt=xuo=x

○ Manually specify the application information

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.



Specify information about this application

Name: Outlook

Administrator comments:

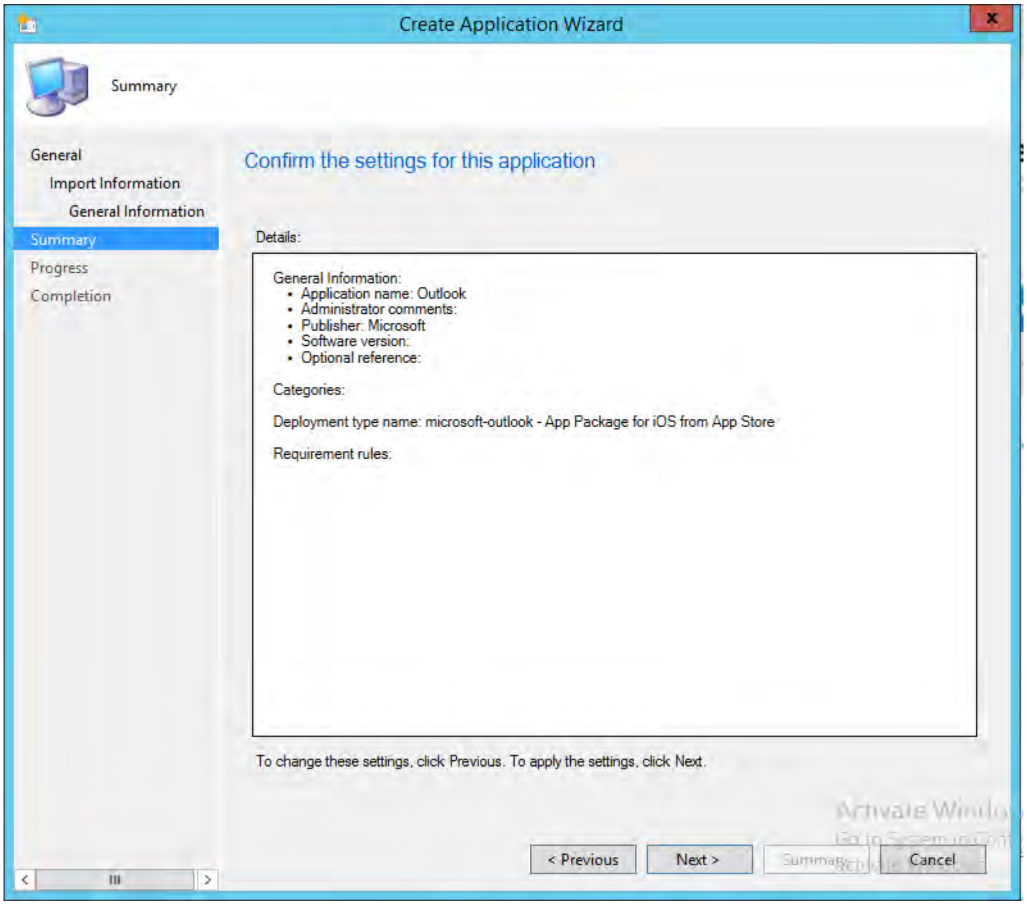
Publisher: Microsoft

Software version:

Optional reference:

Administrative categories:

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



Confirm the settings for this application

Details:

General Information:
- Application name: Outlook
- Administrator comments:
- Publisher: Microsoft
- Software version:
- Optional reference:

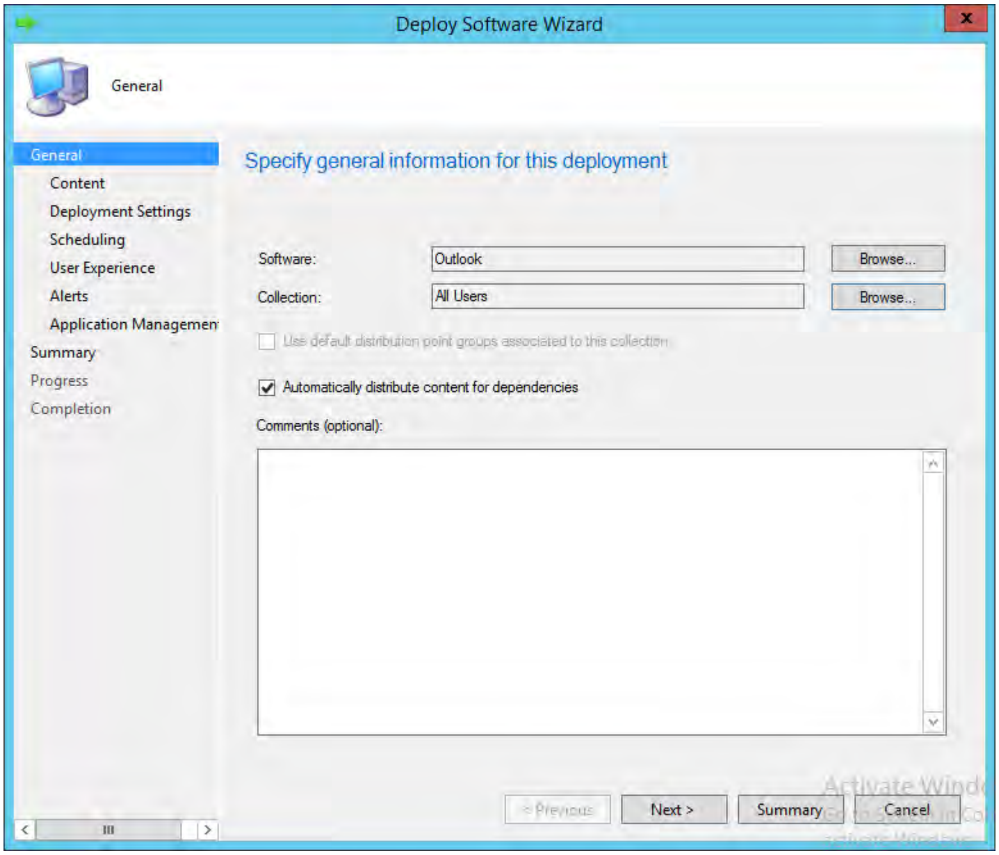
Categories:

Deployment type name: microsoft-outlook - App Package for iOS from App Store

Requirement rules:

To change these settings, click Previous. To apply the settings, click Next.

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



Specify general information for this deployment

Software: Outlook

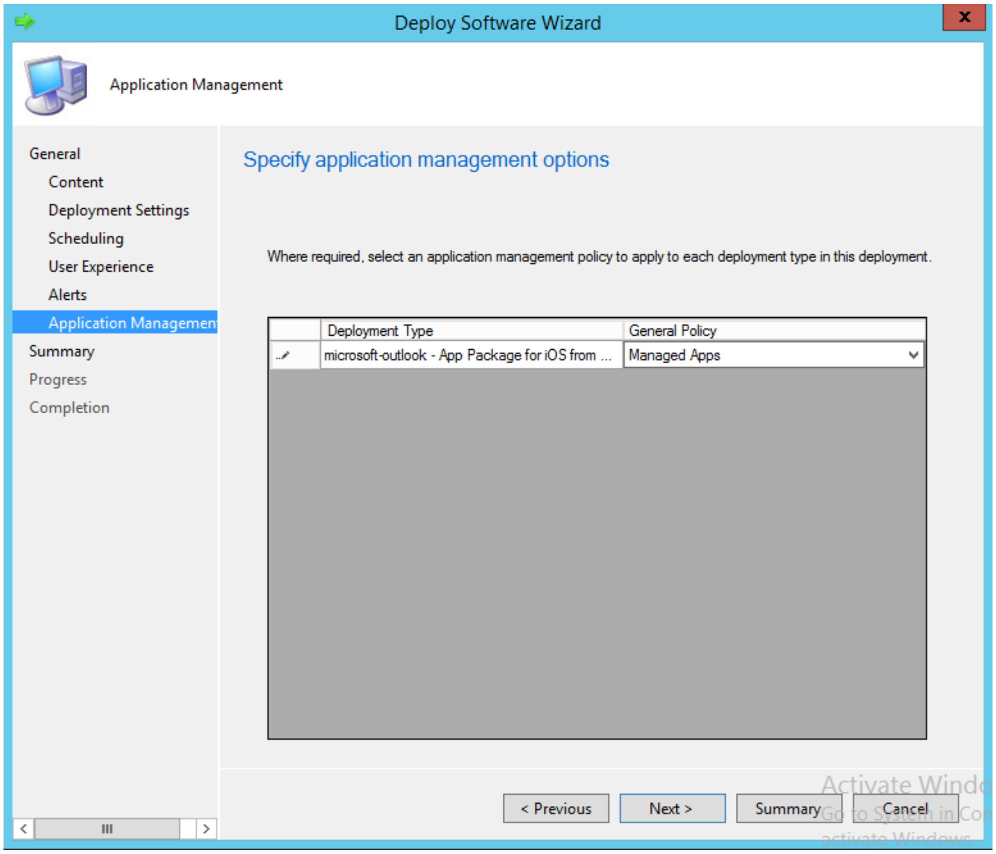
Collection: All Users

□ Use default distribution point groups associated to this collection

☑ Automatically distribute content for dependencies

Comments (optional):

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



Specify application management options

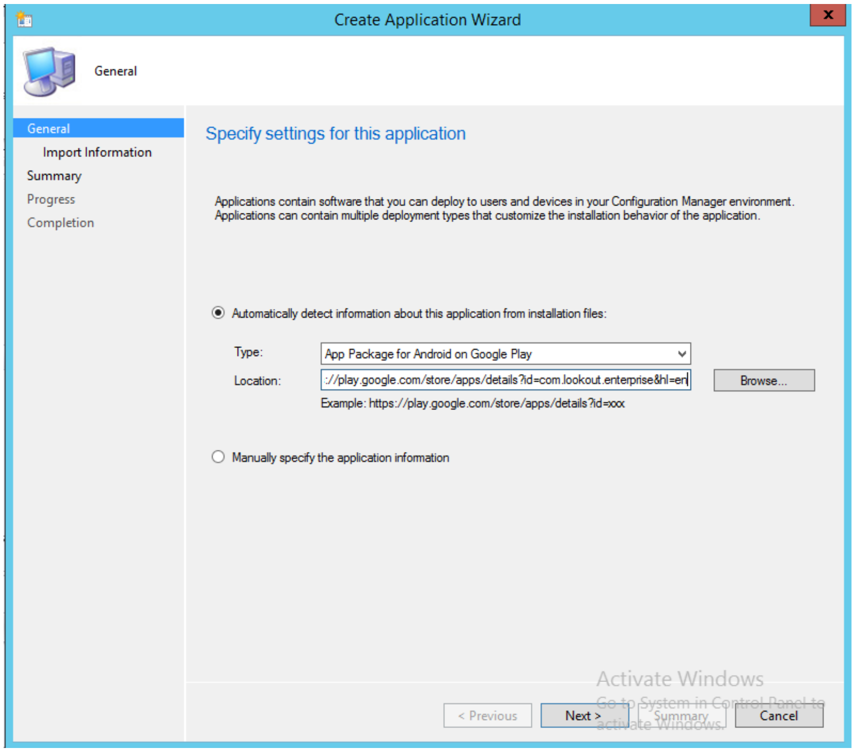
Where required, select an application management policy to apply to each deployment type in this deployment.

	Deployment Type	General Policy
	microsoft-outlook - App Package for iOS from ...	Managed Apps

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.



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

● Automatically detect information about this application from installation files:

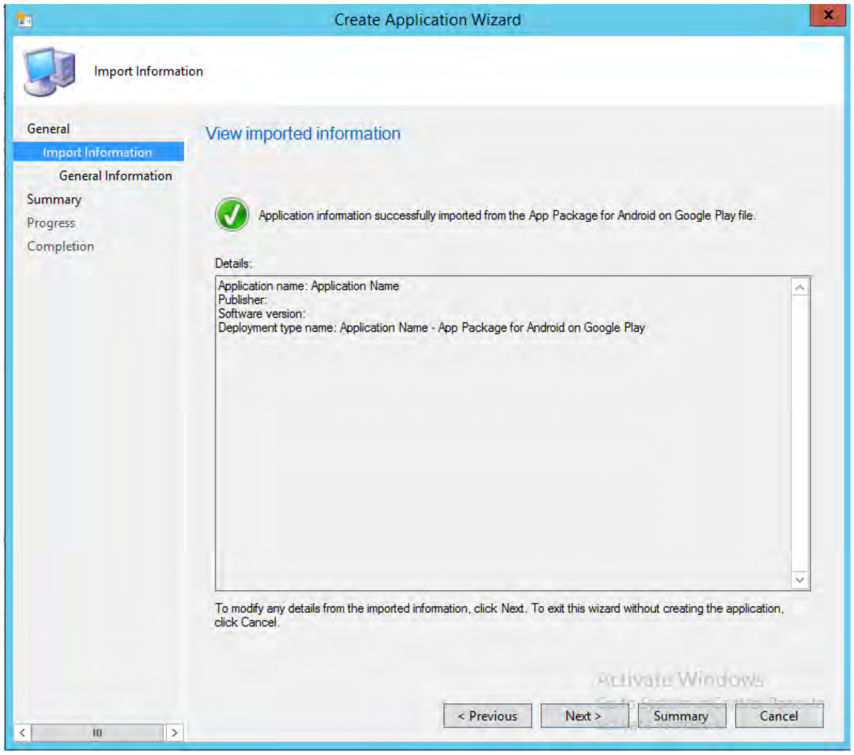
Type: App Package for Android on Google Play

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

Example: https://play.google.com/store/apps/details?id=xxx

○ Manually specify the application information

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.



View imported information

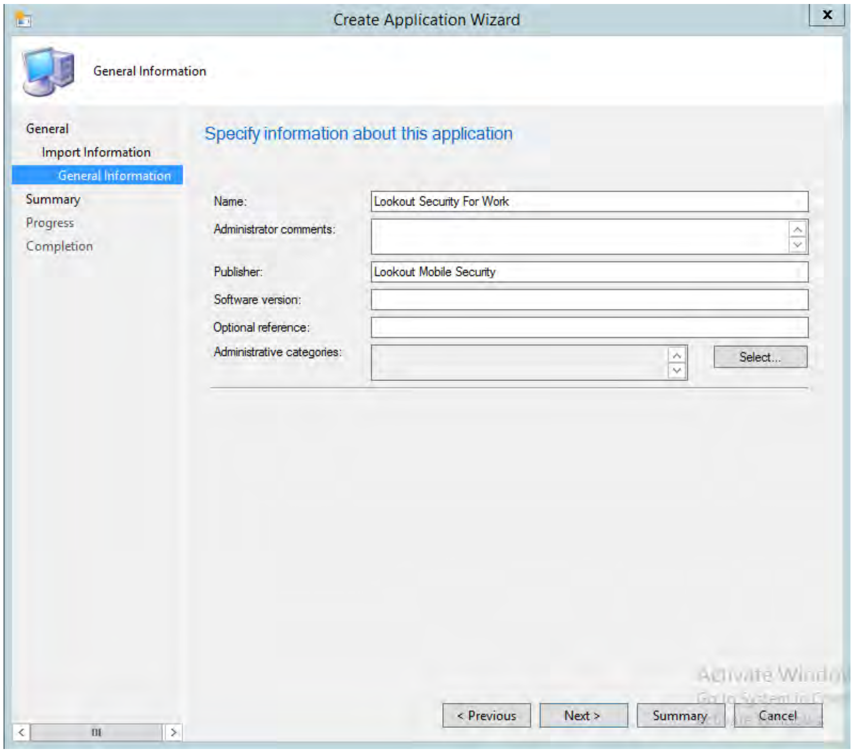
Application information successfully imported from the App Package for Android on Google Play file.

Details:

Application name: Application Name
Publisher:
Software version:
Deployment type name: Application Name - App Package for Android on Google Play

To modify any details from the imported information, click Next. To exit this wizard without creating the application, click Cancel.

2. Click **Next**.



Create Application Wizard

General Information

Specify information about this application

Name: Lookout Security For Work

Administrator comments:

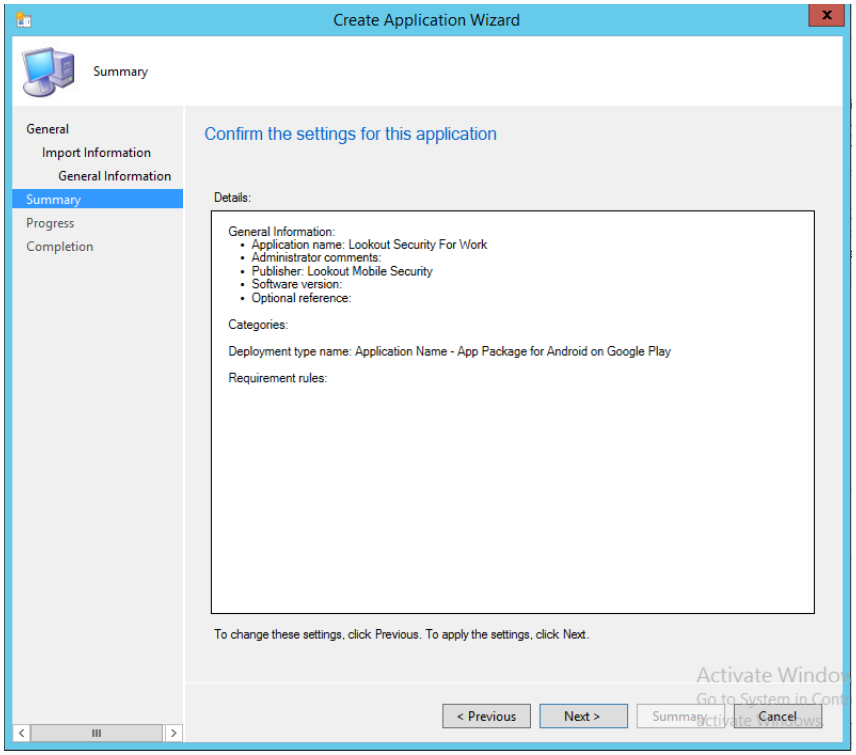
Publisher: Lookout Mobile Security

Software version:

Optional reference:

Administrative categories:

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



Create Application Wizard

Summary

Confirm the settings for this application

Details:

General Information:
- Application name: Lookout Security For Work
- Administrator comments:
- Publisher: Lookout Mobile Security
- Software version:
- Optional reference:

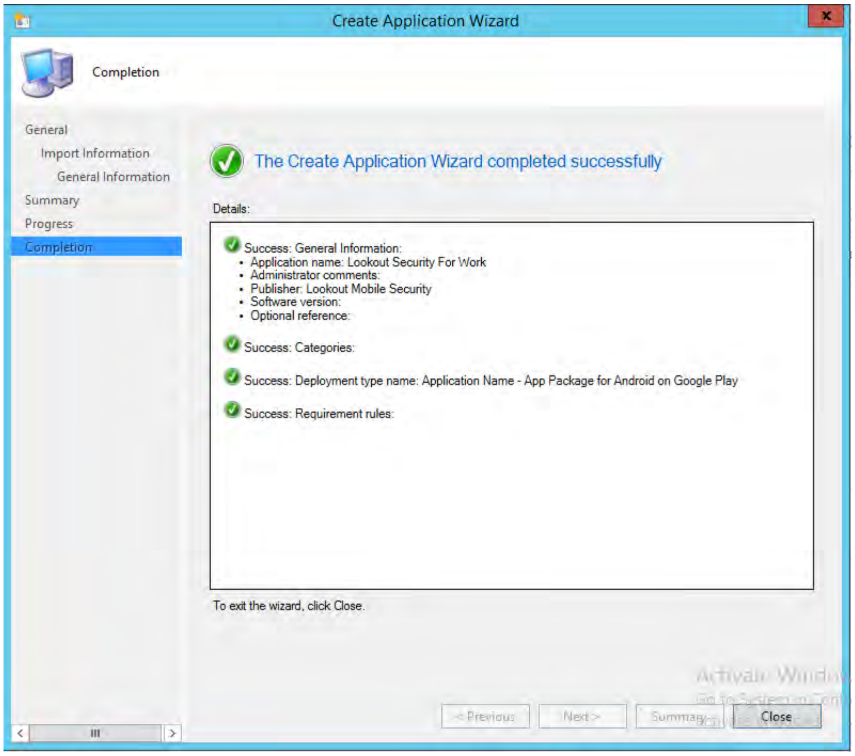
Categories:

Deployment type name: Application Name - App Package for Android on Google Play

Requirement rules:

To change these settings, click Previous. To apply the settings, click Next.

4. Click **Next**.



The Create Application Wizard completed successfully

Details:

Success: General Information:
- Application name: Lookout Security For Work
- Administrator comments:
- Publisher: Lookout Mobile Security
- Software version:
- Optional reference:

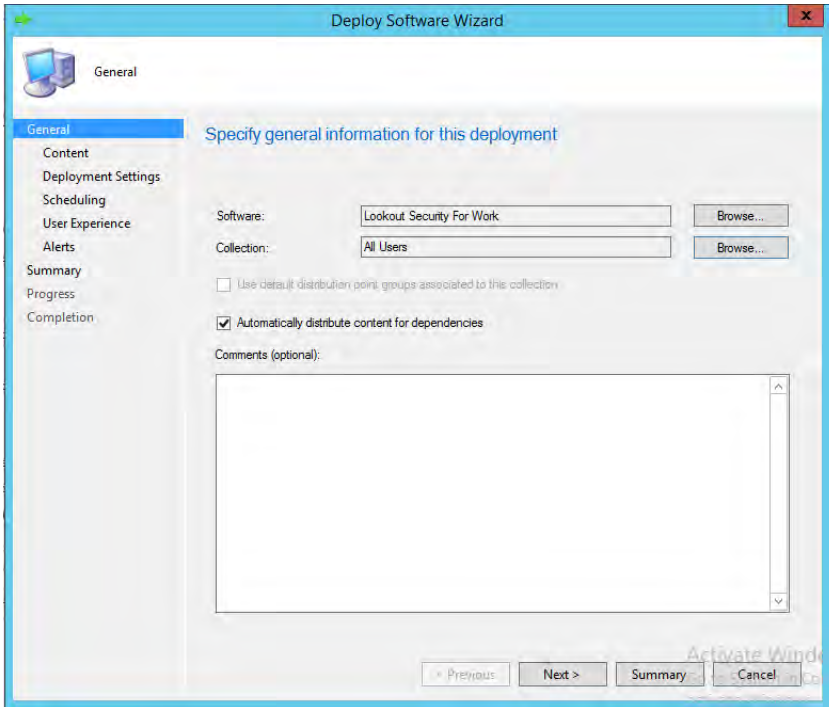
Success: Categories:

Success: Deployment type name: Application Name - App Package for Android on Google Play

Success: Requirement rules:

To exit the wizard, click Close.

5. Click **Close**.



Specify general information for this deployment

Software: Lookout Security For Work

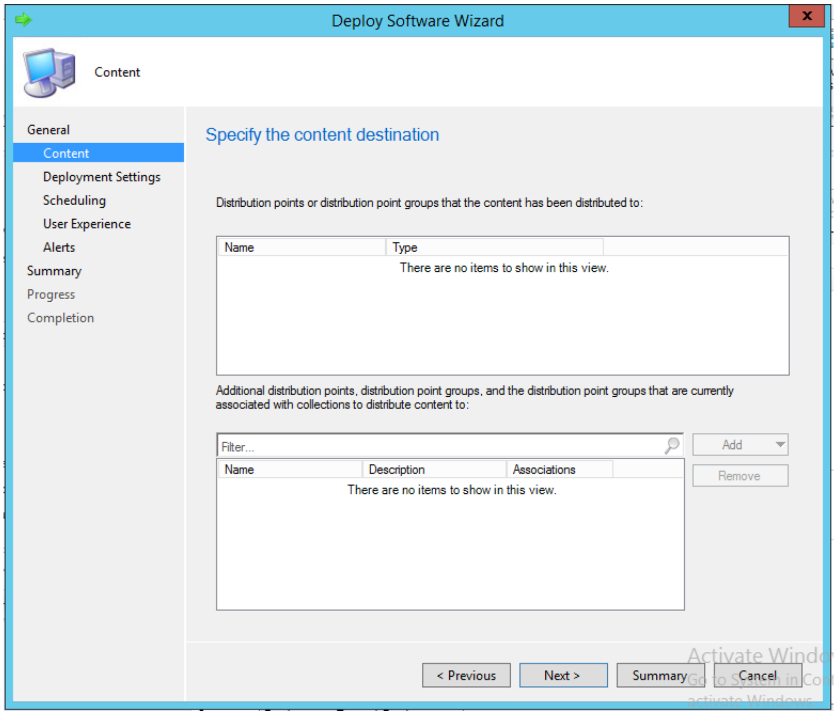
Collection: All Users

□ Use default distribution point groups associated to this collection

☑ Automatically distribute content for dependencies

Comments (optional):

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



Specify the content destination

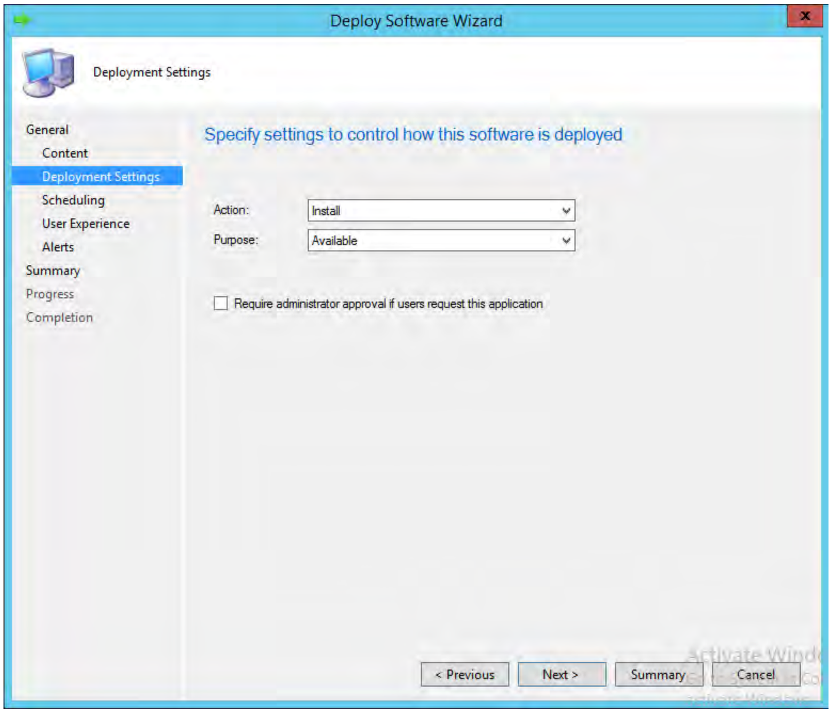
Distribution points or distribution point groups that the content has been distributed to:

There are no items to show in this view.

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

There are no items to show in this view.

7. Click **Next**.



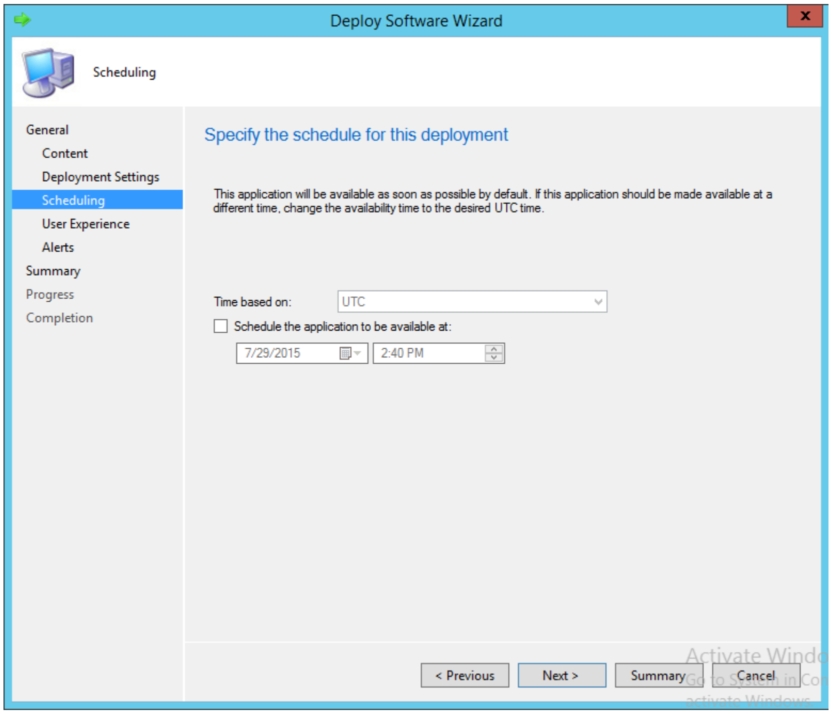
Specify settings to control how this software is deployed

Action: Install

Purpose: Available

☐ Require administrator approval if users request this application

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



Specify the schedule for this deployment

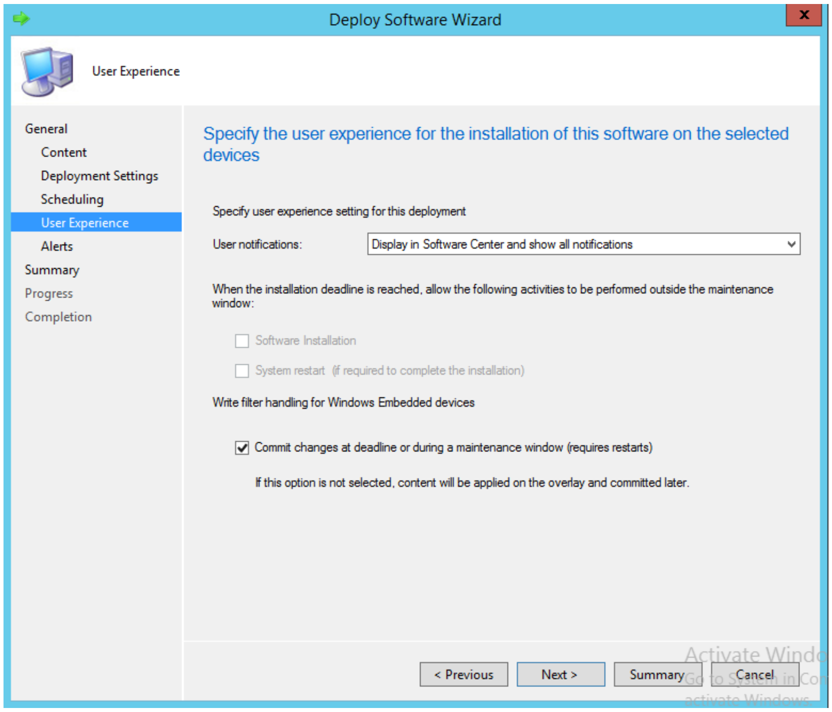
This application will be available as soon as possible by default. If this application should be made available at a different time, change the availability time to the desired UTC time.

Time based on: UTC

□ Schedule the application to be available at:

7/29/2015 2:40 PM

9. Click **Next**.



Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment

User notifications: Display in Software Center and show all notifications

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

□ Software Installation

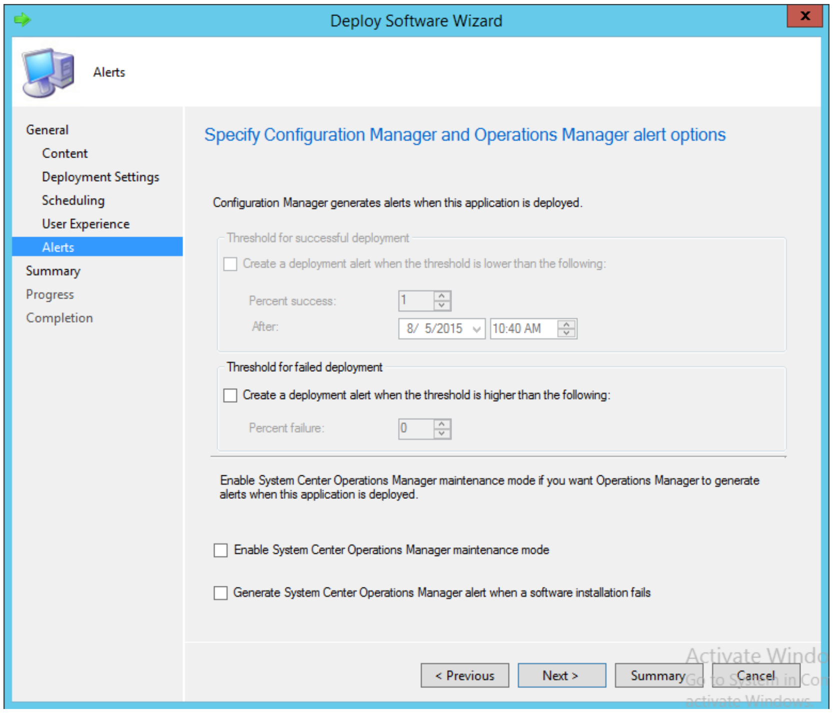
□ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

☑ Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

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



Specify Configuration Manager and Operations Manager alert options

Configuration Manager generates alerts when this application is deployed.

Threshold for successful deployment

☐ Create a deployment alert when the threshold is lower than the following:

Percent success: 1

After: 8/ 5/2015 10:40 AM

Threshold for failed deployment

☐ Create a deployment alert when the threshold is higher than the following:

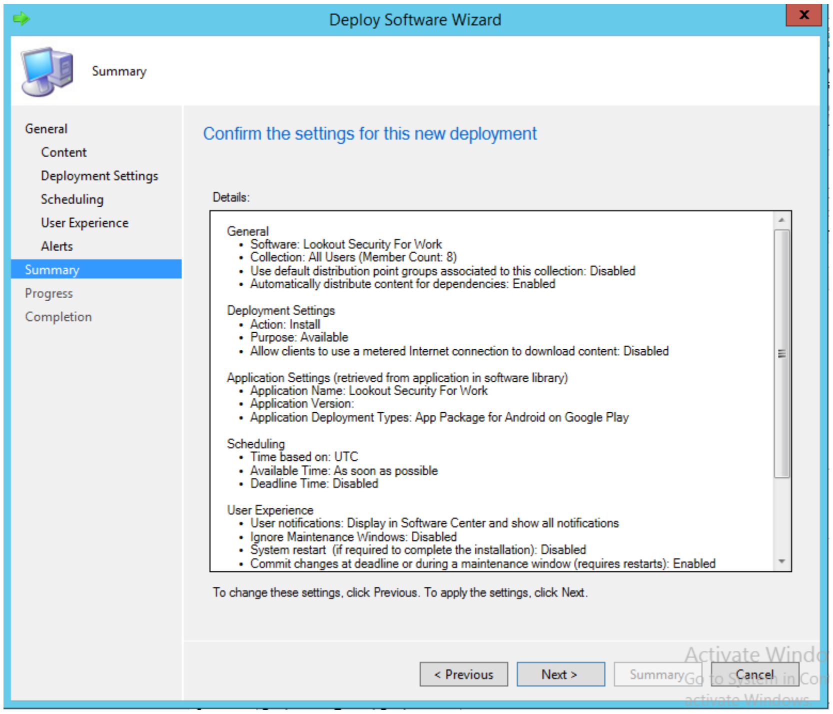
Percent failure: 0

Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.

☐ Enable System Center Operations Manager maintenance mode

☐ Generate System Center Operations Manager alert when a software installation fails

11. Click **Next**.



Confirm the settings for this new deployment

Details:

General
- Software: Lookout Security For Work
- Collection: All Users (Member Count: 8)
- Use default distribution point groups associated to this collection: Disabled
- Automatically distribute content for dependencies: Enabled

Deployment Settings
- Action: Install
- Purpose: Available
- Allow clients to use a metered Internet connection to download content: Disabled

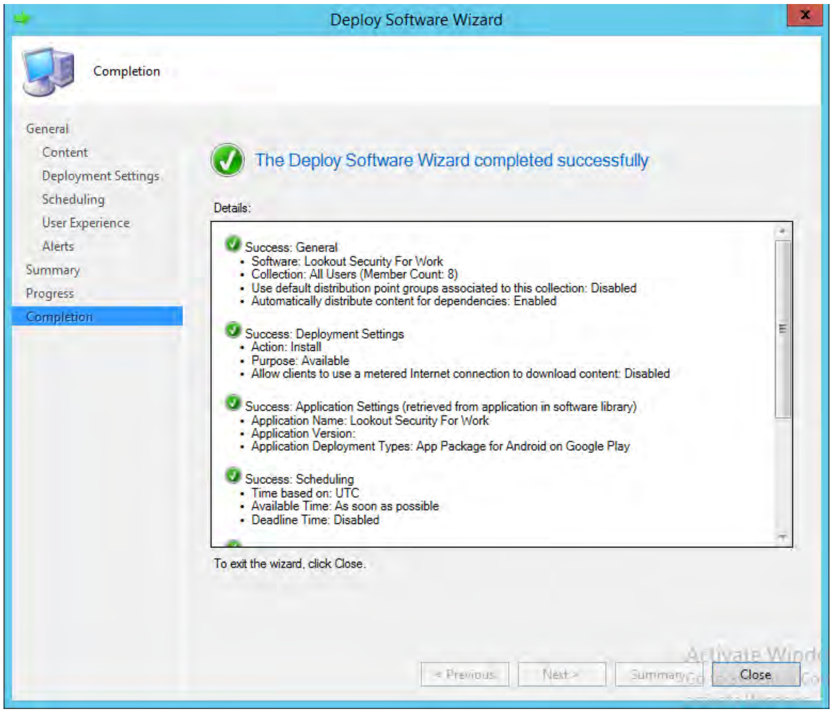
Application Settings (retrieved from application in software library)
- Application Name: Lookout Security For Work
- Application Version:
- Application Deployment Types: App Package for Android on Google Play

Scheduling
- Time based on: UTC
- Available Time: As soon as possible
- Deadline Time: Disabled

User Experience
- User notifications: Display in Software Center and show all notifications
- Ignore Maintenance Windows: Disabled
- System restart (if required to complete the installation): Disabled
- Commit changes at deadline or during a maintenance window (requires restarts): Enabled

To change these settings, click Previous. To apply the settings, click Next.

12. Click **Next**.



The Deploy Software Wizard completed successfully

Details:

Success: General
- Software: Lookout Security For Work
- Collection: All Users (Member Count: 8)
- Use default distribution point groups associated to this collection: Disabled
- Automatically distribute content for dependencies: Enabled

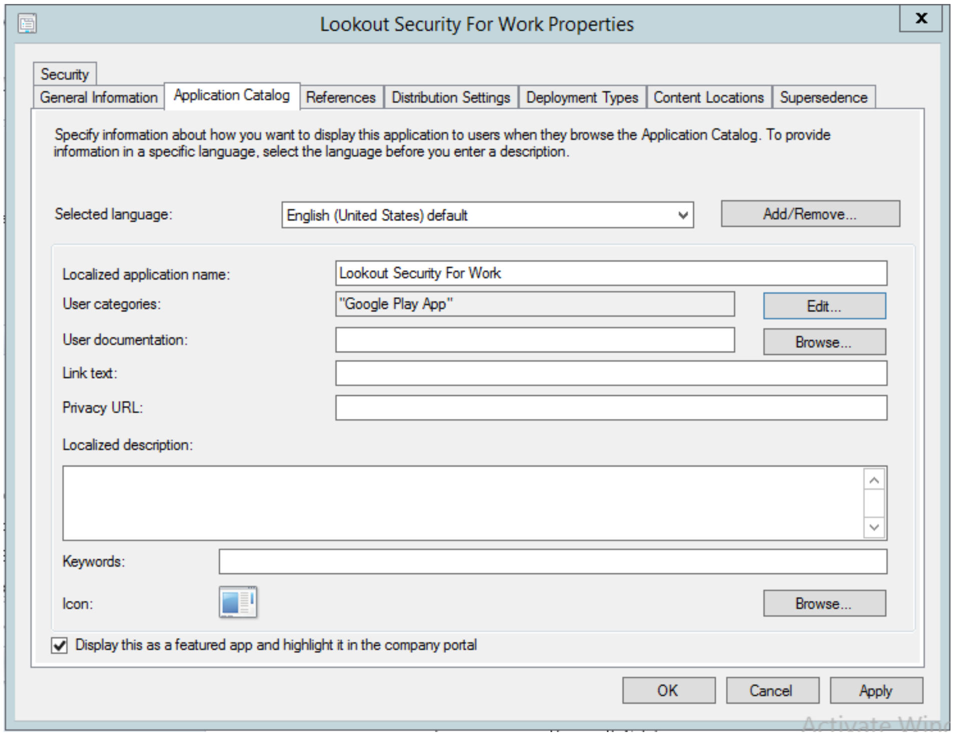
Success: Deployment Settings
- Action: Install
- Purpose: Available
- Allow clients to use a metered Internet connection to download content: Disabled

Success: Application Settings (retrieved from application in software library)
- Application Name: Lookout Security For Work
- Application Version:
- Application Deployment Types: App Package for Android on Google Play

Success: Scheduling
- Time based on: UTC
- Available Time: As soon as possible
- Deadline Time: Disabled

To exit the wizard, click Close.

13. Click **Close**.



Specify information about how you want to display this application to users when they browse the Application Catalog. To provide information in a specific language, select the language before you enter a description.

Selected language: English (United States) default

Localized application name: Lookout Security For Work

User categories: "Google Play App"

User documentation:

Link text:

Privacy URL:

Localized description:

Keywords:

Icon:

☑ Display this as a featured app and highlight it in the company portal

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.

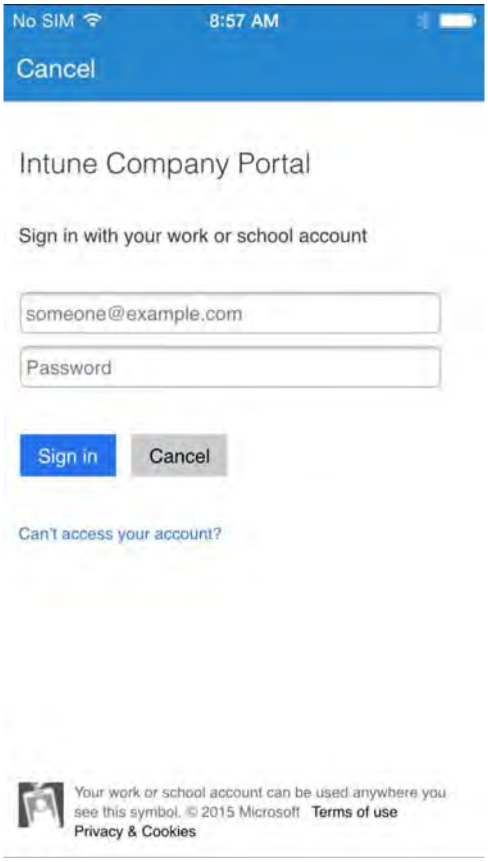
4.1 Device Enrollment with Office 365

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



No SIM 8:57 AM

Cancel

Intune Company Portal

Sign in with your work or school account

someone@example.com

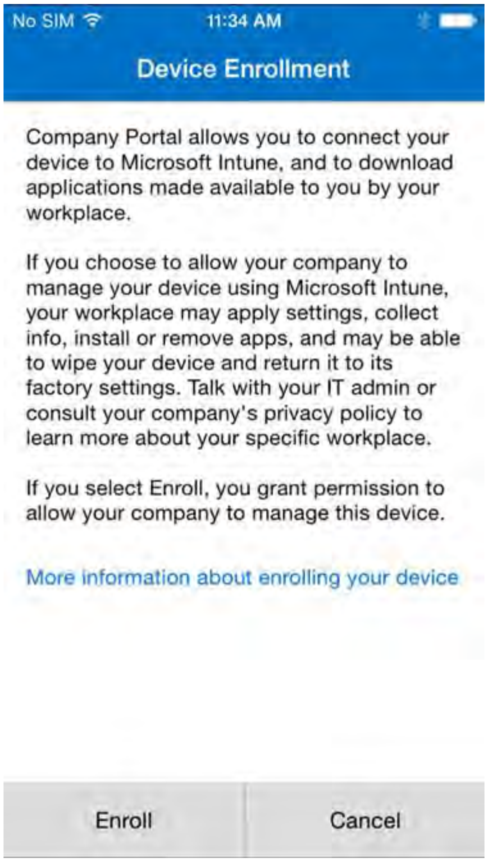
Password

Sign in Cancel

Can't access your account?

Your work or school account can be used anywhere you see this symbol. © 2015 Microsoft Terms of use Privacy & Cookies

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



Device Enrollment

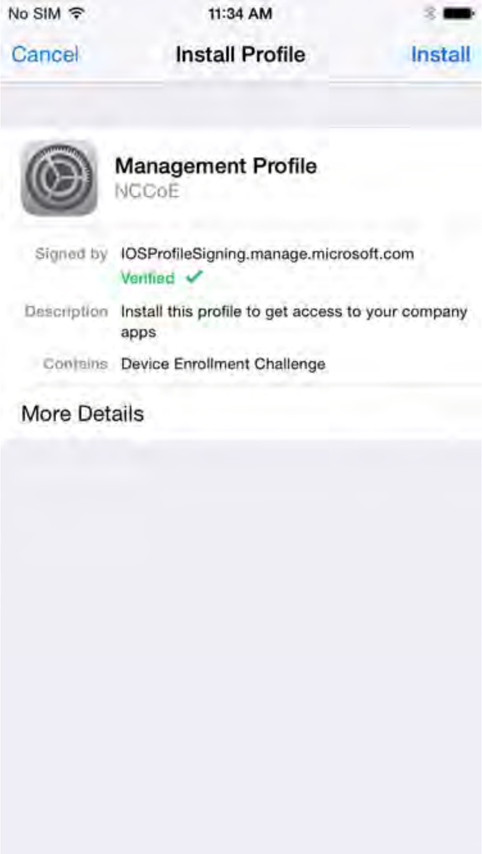
Company Portal allows you to connect your device to Microsoft Intune, and to download applications made available to you by your workplace.

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

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

More information about enrolling your device

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



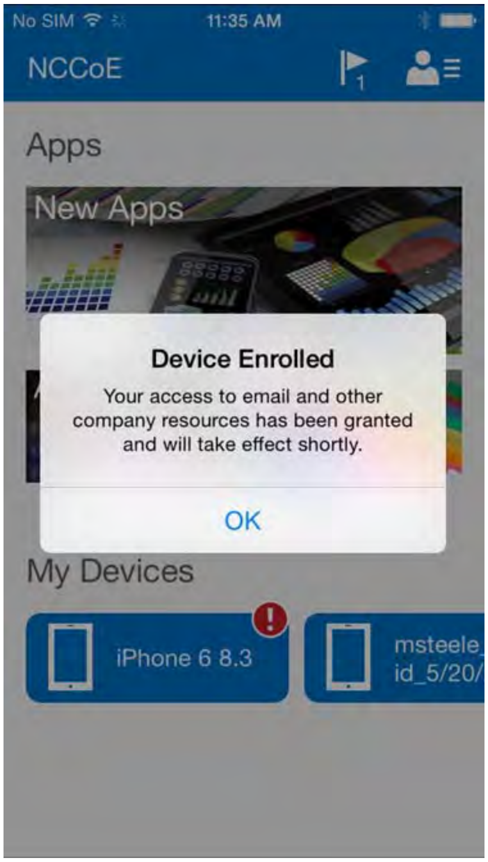
Management Profile
NCCoE

Signed by IOSProfileSigning.manage.microsoft.com
Verified ✓

Description Install this profile to get access to your company apps

Contains Device Enrollment Challenge

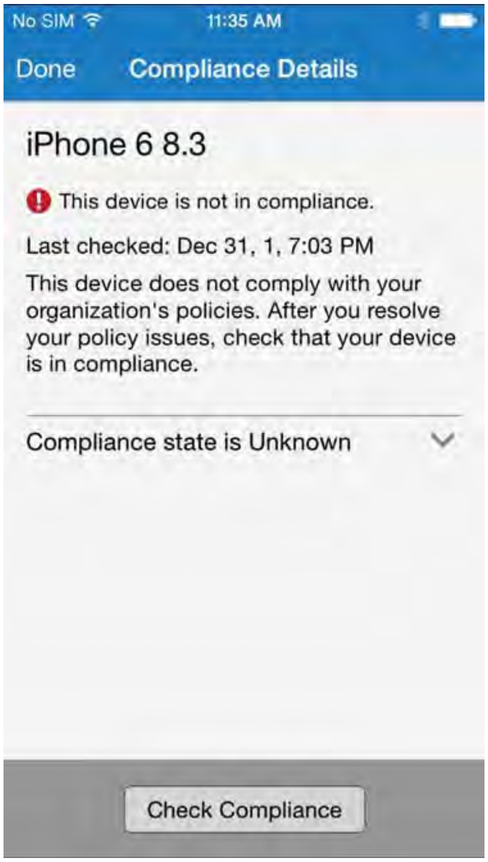
3. Before accepting the management profile, the user can see the specifics of the profile and certificates that are issued.



Device Enrolled

Your access to email and other company resources has been granted and will take effect shortly.

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



iPhone 6 8.3

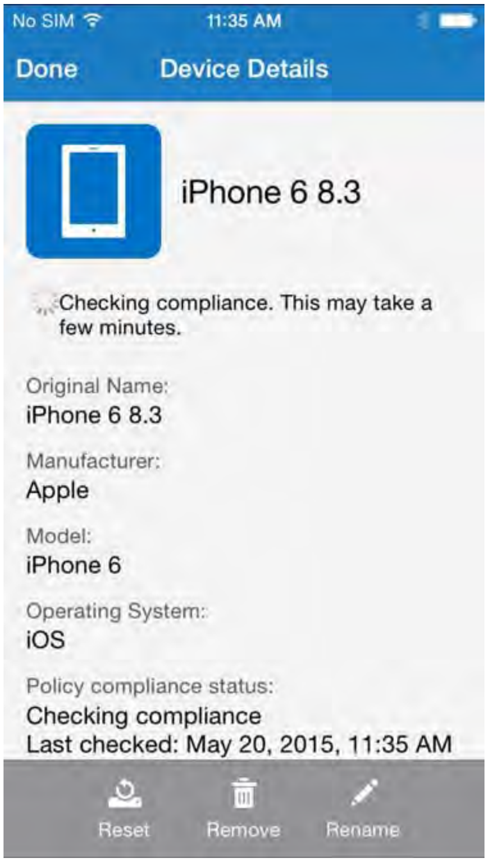
This device is not in compliance.

Last checked: Dec 31, 1, 7:03 PM

This device does not comply with your organization's policies. After you resolve your policy issues, check that your device is in compliance.

Compliance state is Unknown

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.



iPhone 6 8.3

Checking compliance. This may take a few minutes.

Original Name:
iPhone 6 8.3

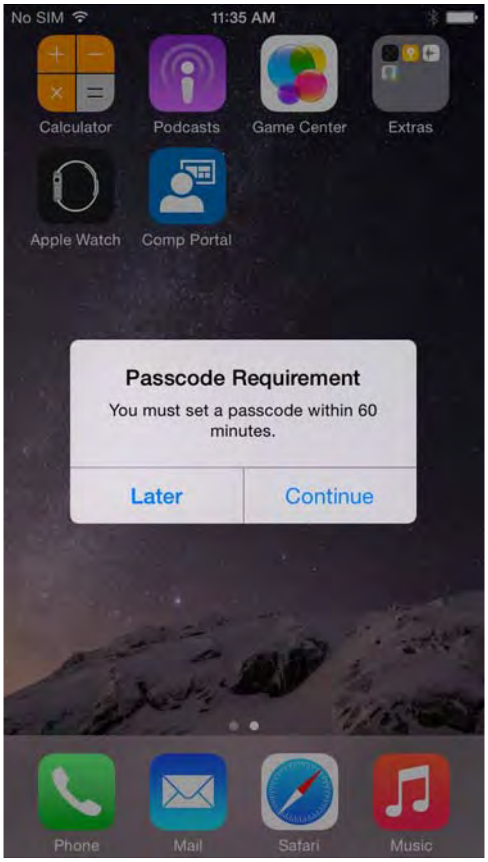
Manufacturer:
Apple

Model:
iPhone 6

Operating System:
iOS

Policy compliance status:
Checking compliance
Last checked: May 20, 2015, 11:35 AM

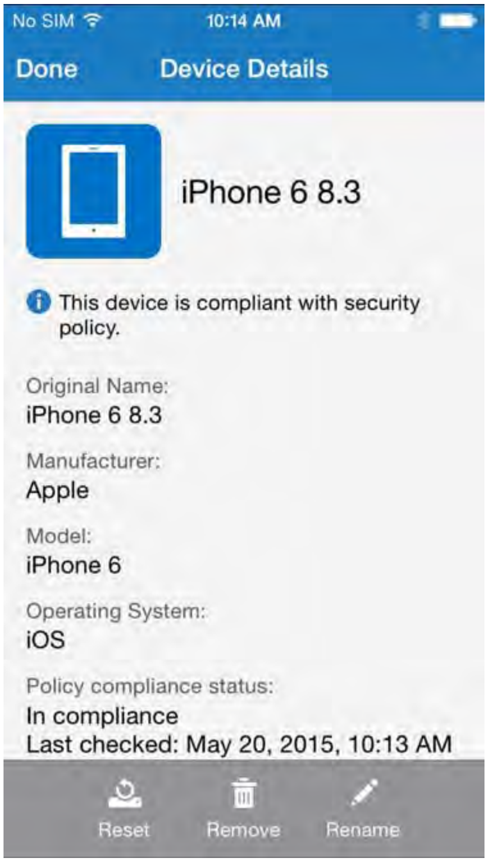
6. The compliance checking process will take a couple of minutes. The user can minimize the application during the compliance checking process.



Passcode Requirement

You must set a passcode within 60 minutes.

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.



iPhone 6 8.3

This device is compliant with security policy.

Original Name:
iPhone 6 8.3

Manufacturer:
Apple

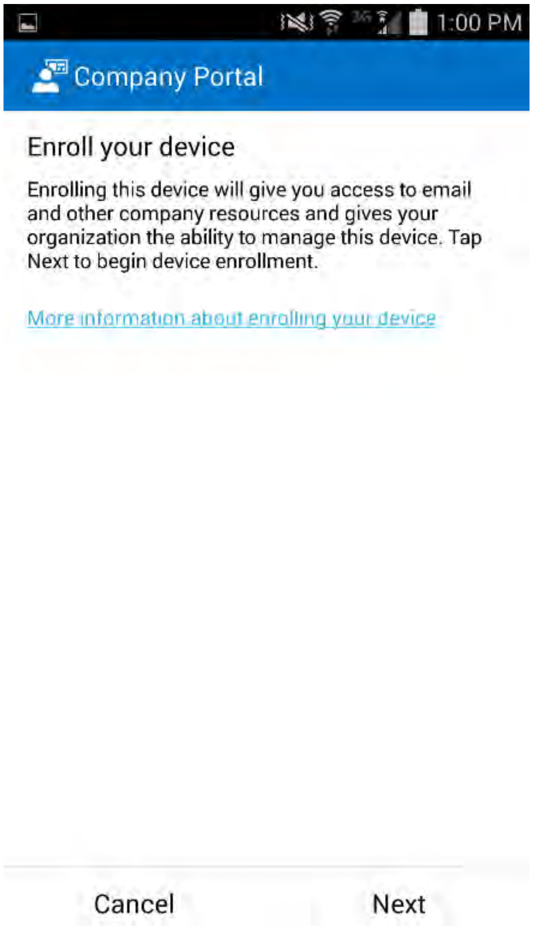
Model:
iPhone 6

Operating System:
iOS

Policy compliance status:
In compliance
Last checked: May 20, 2015, 10:13 AM

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

4.1.2 Android

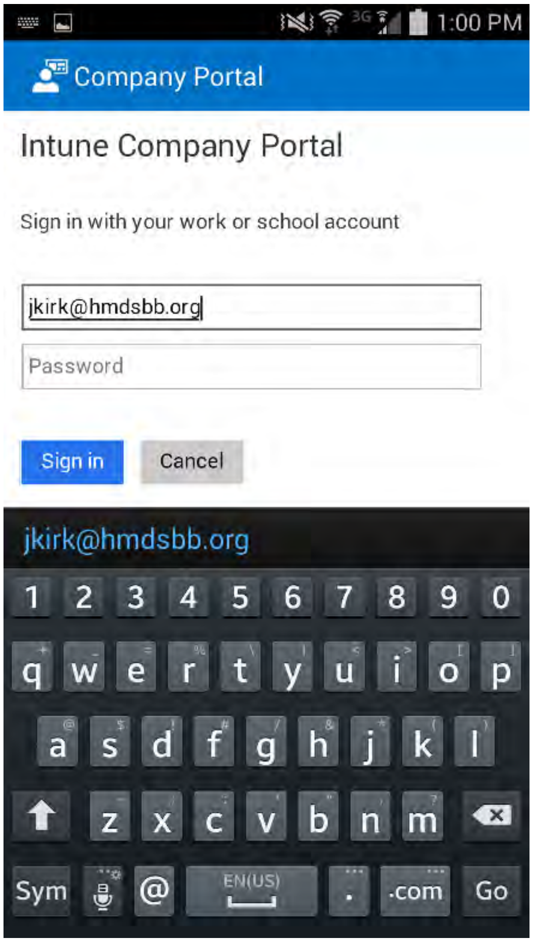


Enroll your device

Enrolling this device will give you access to email and other company resources and gives your organization the ability to manage this device. Tap Next to begin device enrollment.

More information about enrolling your device

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

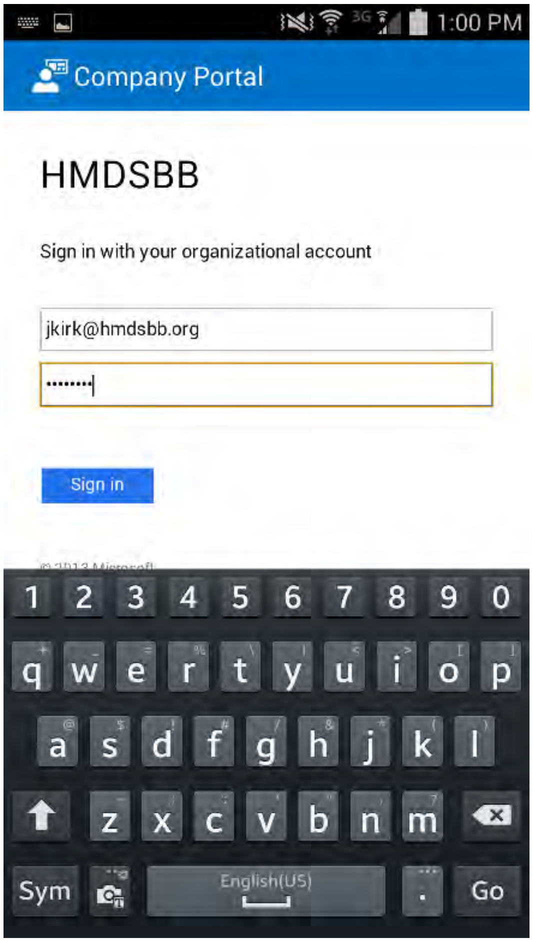


Intune Company Portal

Sign in with your work or school account

jkirk@hmdsbb.org

2. Enter your email address.



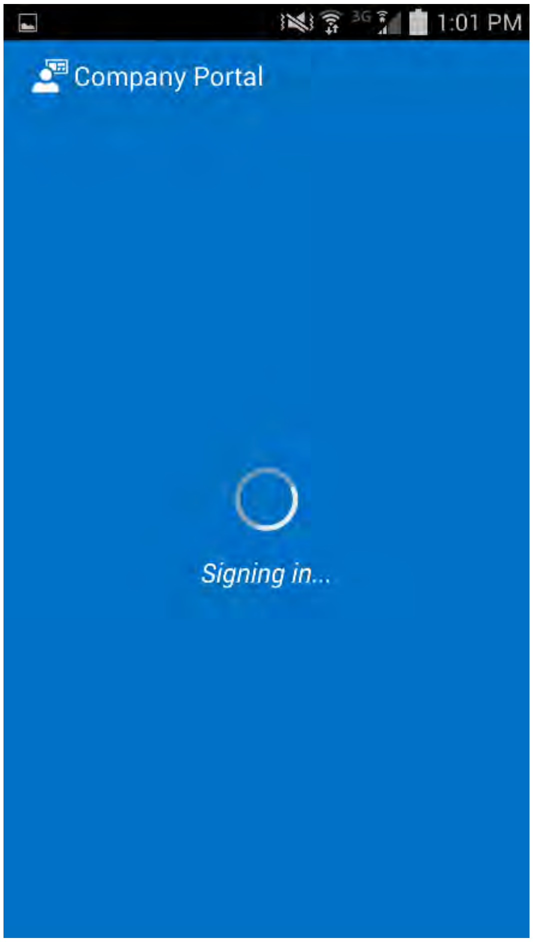
HMDSBB

Sign in with your organizational account

jkirk@hmdsbb.org

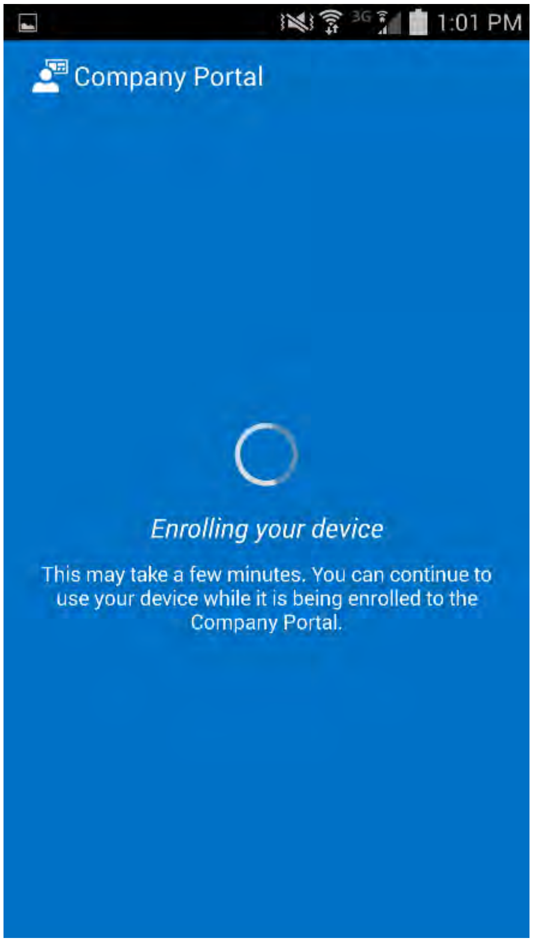
••••••••

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



Signing in...

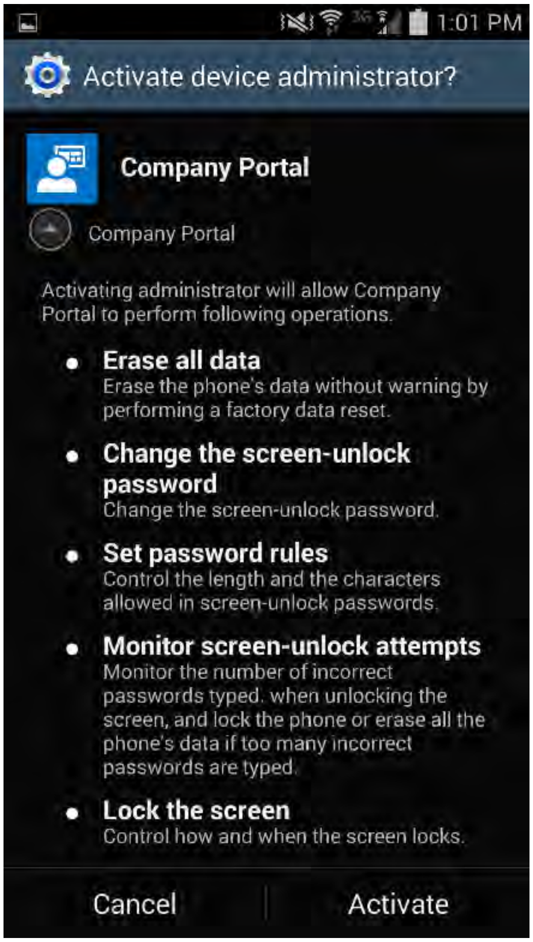
4. No action required.



Enrolling your device

This may take a few minutes. You can continue to use your device while it is being enrolled to the Company Portal.

5. No action required.



Activate device administrator?

Company Portal

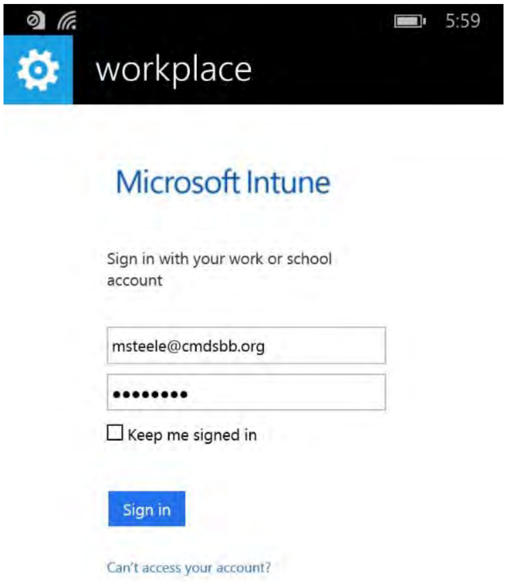
Company Portal

Activating administrator will allow Company Portal to perform following operations.

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.

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

4.1.3 Windows Phone 8.1



Microsoft Intune

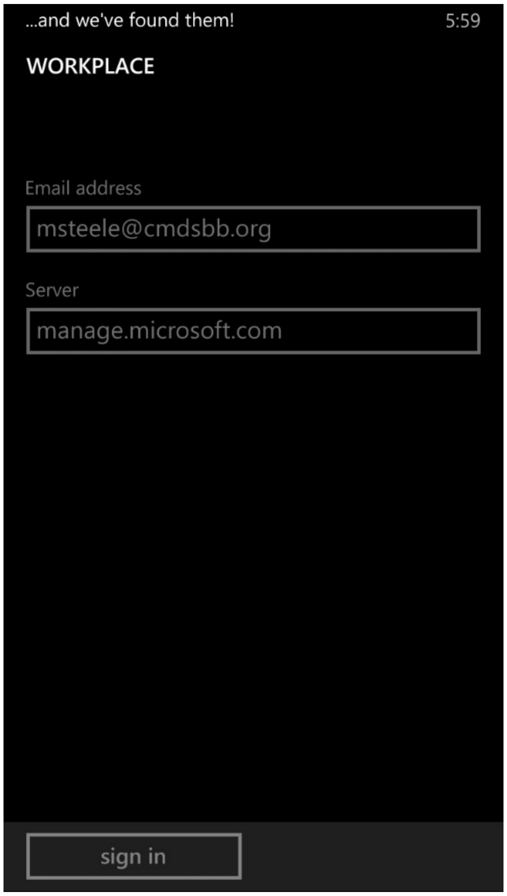
Sign in with your work or school account

msteele@cmdsbb.org

•••••••••

☐ Keep me signed in

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.



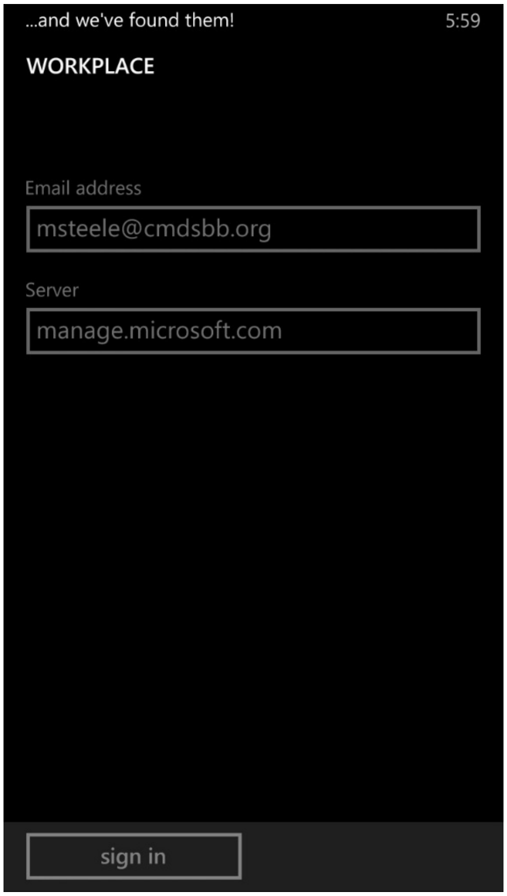
...and we've found them! 5:59

WORKPLACE

Email address: msteele@cmdsbb.org

Server: manage.microsoft.com

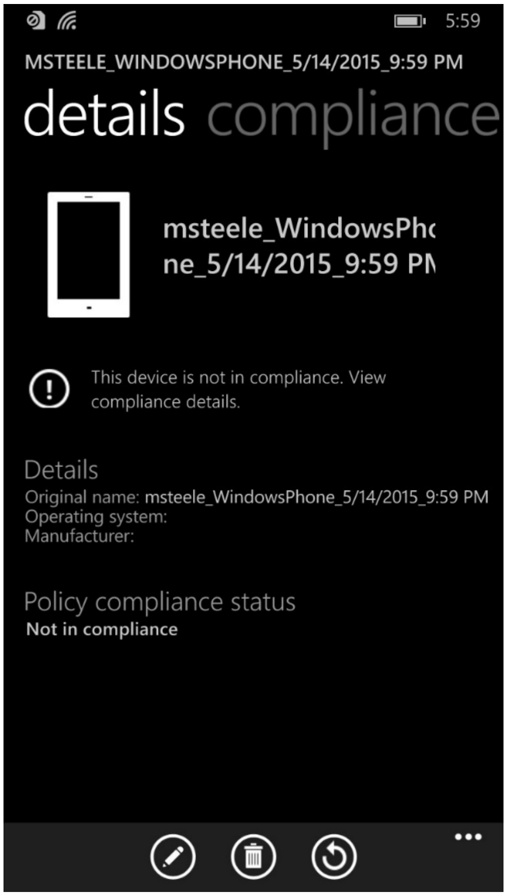
2. The workplace application will attempt to connect to your company's management portal. In our case it did not find the server. We used manage.microsoft.com, the main portal for all Microsoft's Web management for Office365 and Intune.



Email address: msteele@cmdsbb.org

Server: manage.microsoft.com

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.



5:59

MSTEELE_WINDOWSPHONE_5/14/2015_9:59 PM

details compliance

msteele_WindowsPhone_5/14/2015_9:59 PM

This device is not in compliance. View compliance details.

Details

Original name: msteele_WindowsPhone_5/14/2015_9:59 PM

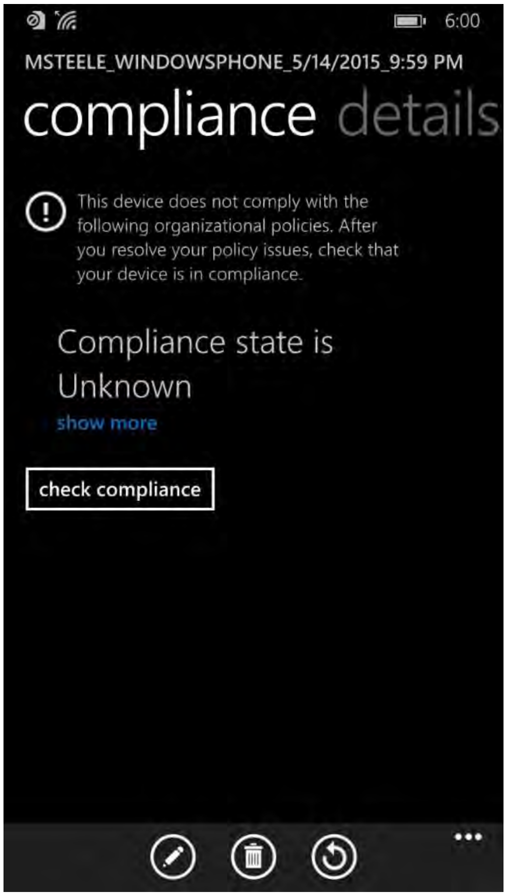
Operating system:

Manufacturer:

Policy compliance status

Not in compliance

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.



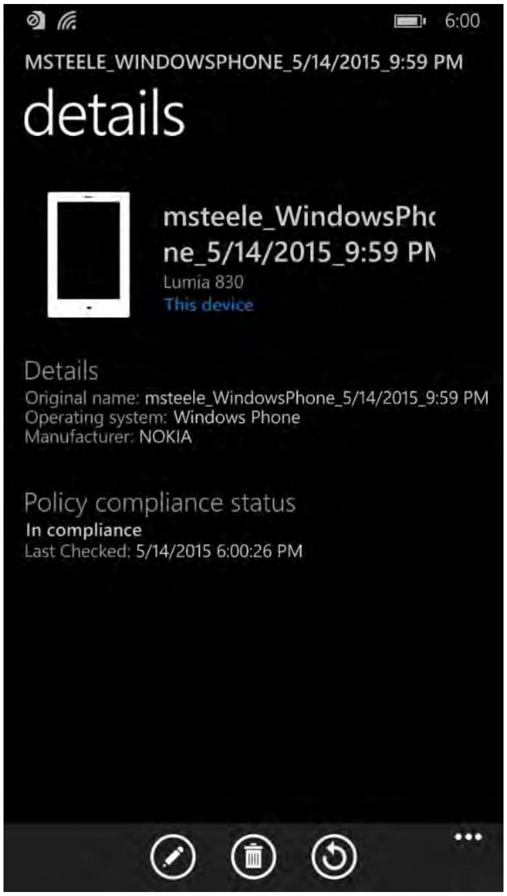
MSTEELE_WINDOWSPHONE_5/14/2015_9:59 PM

compliance details

This device does not comply with the following organizational policies. After you resolve your policy issues, check that your device is in compliance.

Compliance state is Unknown

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



MSTEELE_WINDOWSPHONE_5/14/2015_9:59 PM

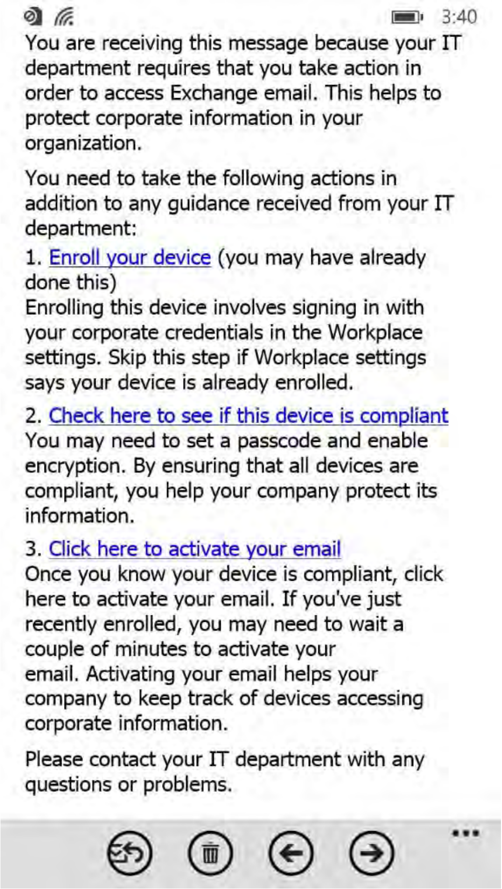
details

msteele_WindowsPhc
ne_5/14/2015_9:59 PI
Lumia 830
This device

Details
Original name: msteele_WindowsPhone_5/14/2015_9:59 PM
Operating system: Windows Phone
Manufacturer: NOKIA

Policy compliance status
In compliance
Last Checked: 5/14/2015 6:00:26 PM

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



3:40

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

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

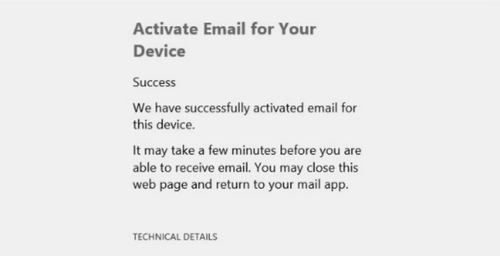
1. Enroll your device (you may have already done this)
Enrolling this device involves signing in with your corporate credentials in the Workplace settings. Skip this step if Workplace settings says your device is already enrolled.

2. Check here to see if this device is compliant
You may need to set a passcode and enable encryption. By ensuring that all devices are compliant, you help your company protect its information.

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

Please contact your IT department with any questions or problems.

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



Activate Email for Your Device

Success

We have successfully activated email for this device.

It may take a few minutes before you are able to receive email. You may close this web page and return to your mail app.

TECHNICAL DETAILS

enterpriseregistration.wi

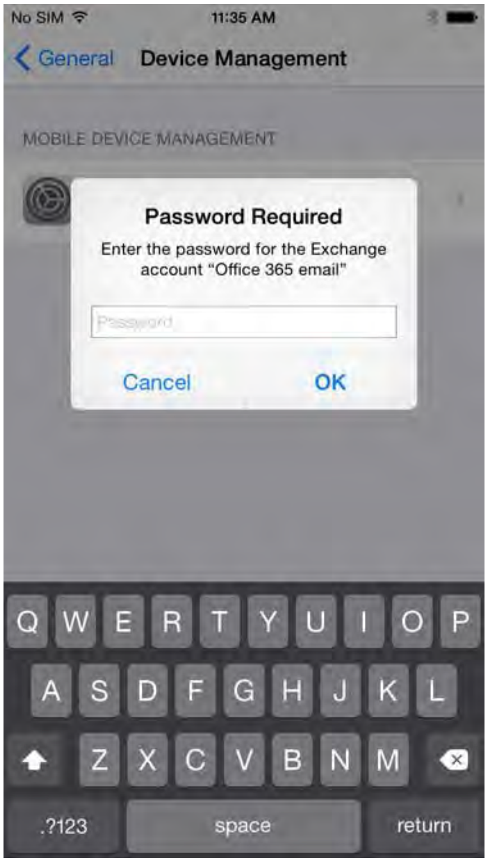
8. The activation link will open a browser, and upon successful activation the user should be directed to this page. At this point the user should have full access to exchange email/contacts/calendar.

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



No SIM 11:35 AM

General Device Management

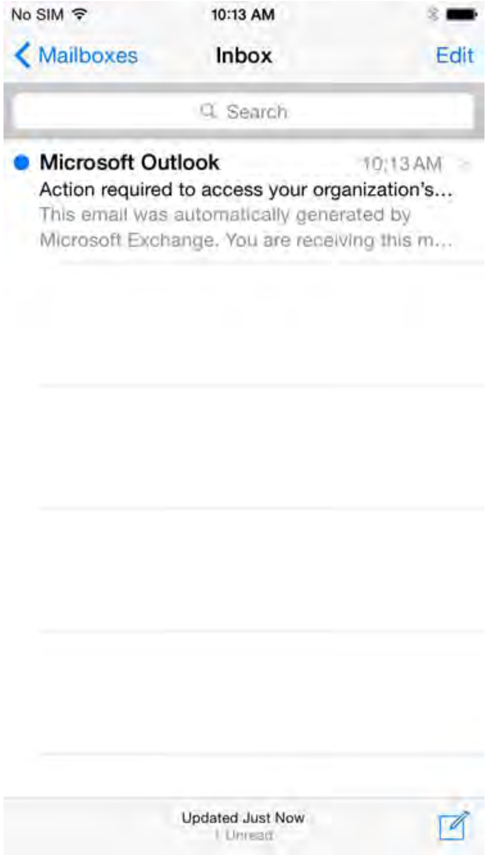
MOBILE DEVICE MANAGEMENT

Password Required

Enter the password for the Exchange account "Office 365 email"

Password

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.



No SIM 10:13 AM

Mailboxes Inbox Edit

Search

Microsoft Outlook 10:13 AM

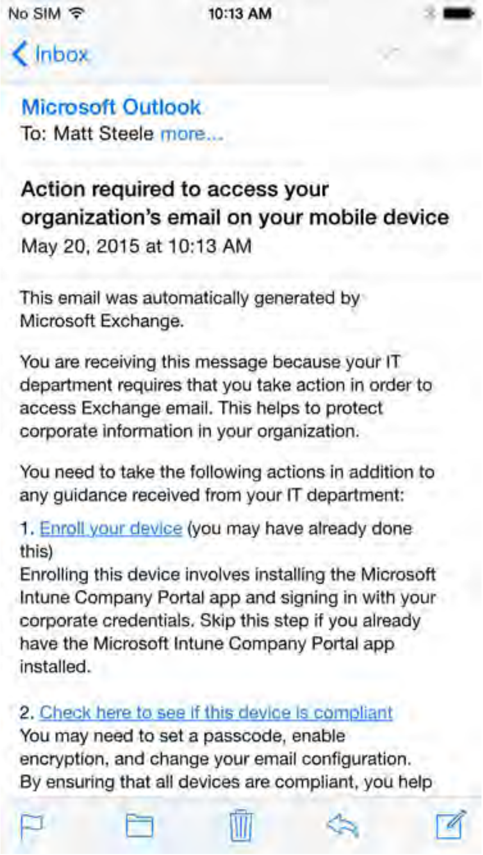
Action required to access your organization's…

This email was automatically generated by Microsoft Exchange. You are receiving this m…

Updated Just Now

1 Unread

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



Microsoft Outlook
To: Matt Steele more...

Action required to access your organization's email on your mobile device
May 20, 2015 at 10:13 AM

This email was automatically generated by Microsoft Exchange.

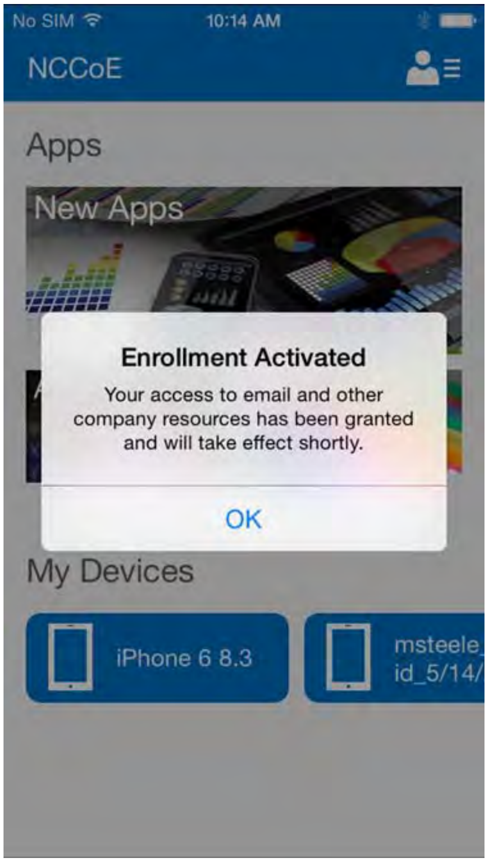
You are receiving this message because your IT department requires that you take action in order to access Exchange email. This helps to protect corporate information in your organization.

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

1. Enroll your device (you may have already done this)
Enrolling this device involves installing the Microsoft Intune Company Portal app and signing in with your corporate credentials. Skip this step if you already have the Microsoft Intune Company Portal app installed.

2. Check here to see if this device is compliant
You may need to set a passcode, enable encryption, and change your email configuration. By ensuring that all devices are compliant, you help

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

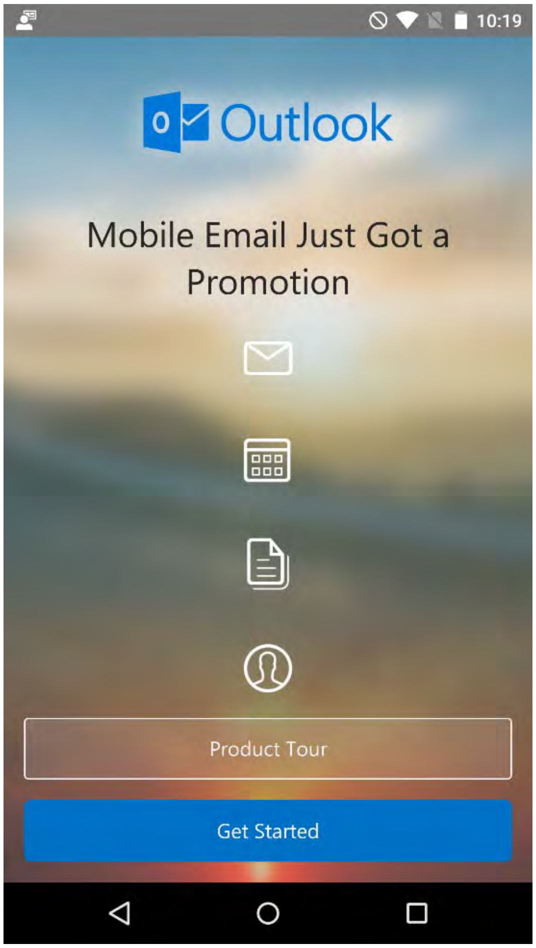


Enrollment Activated

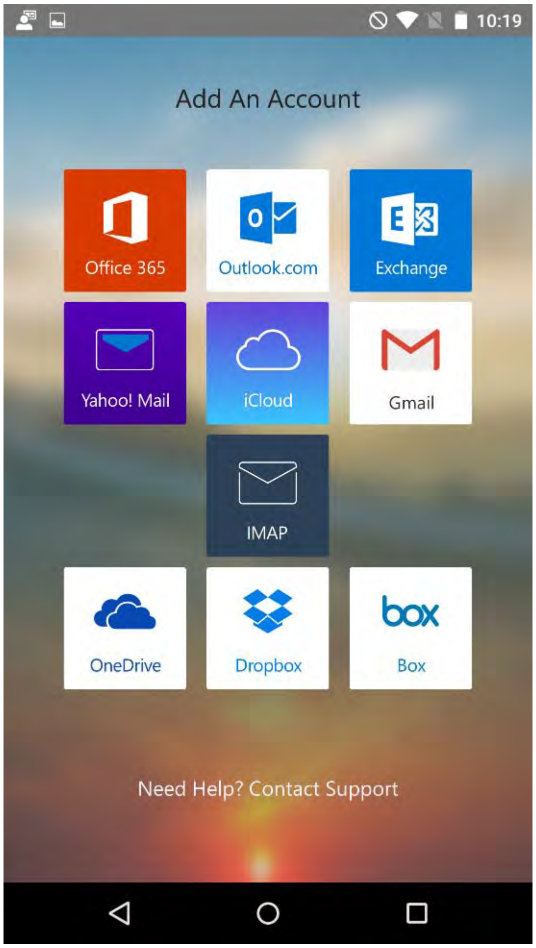
Your access to email and other company resources has been granted and will take effect shortly.

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

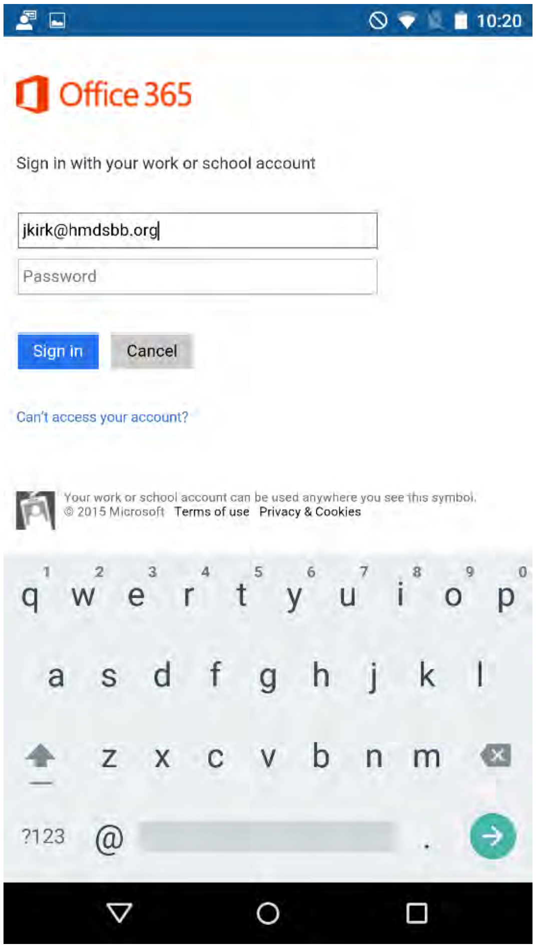
4.2.2 Android



1. Open the Outlook application on your device.



2. Choose **Office 365**.



Office 365

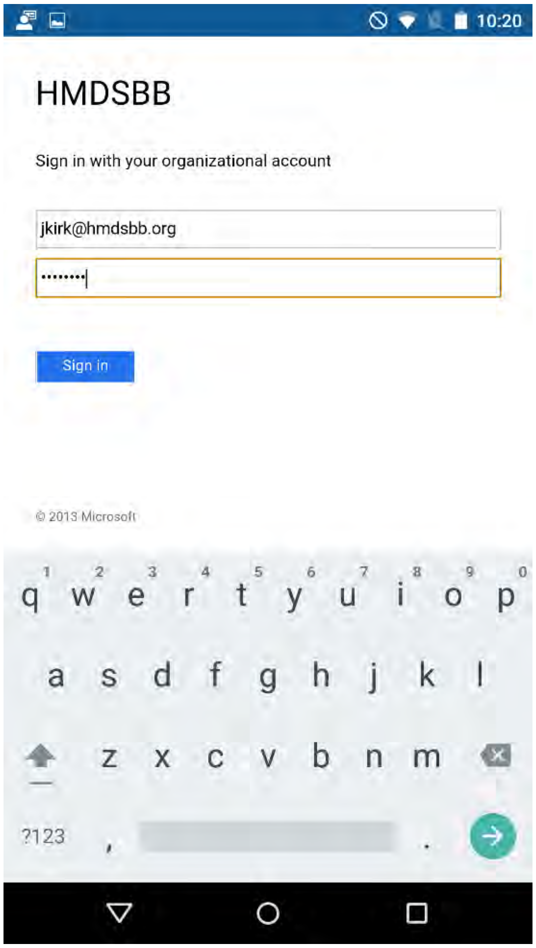
Sign in with your work or school account

jkirk@hmdsbb.org

Password

Your work or school account can be used anywhere you see this symbol.
© 2015 Microsoft Terms of use Privacy & Cookies

3. Log in with your enterprise credentials.



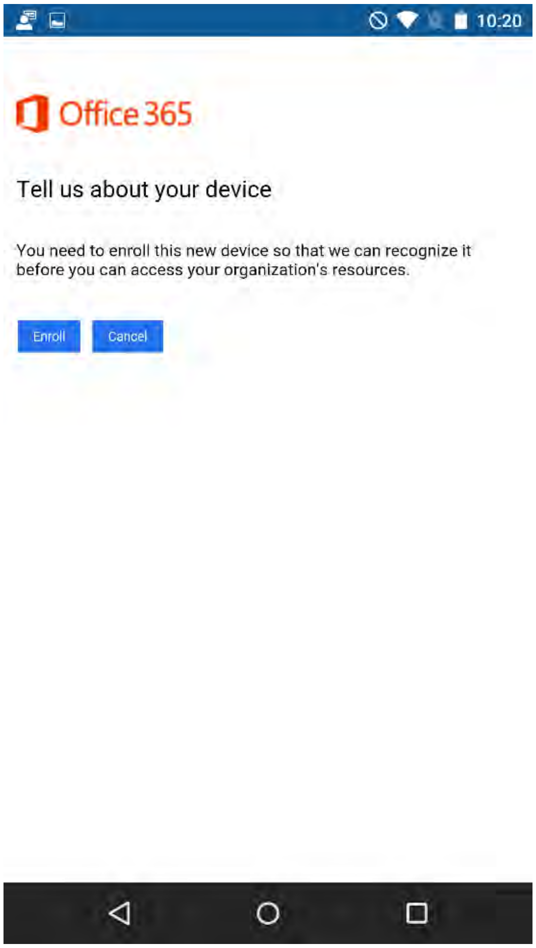
HMDSBB

Sign in with your organizational account

jkirk@hmdsbb.org

••••••••

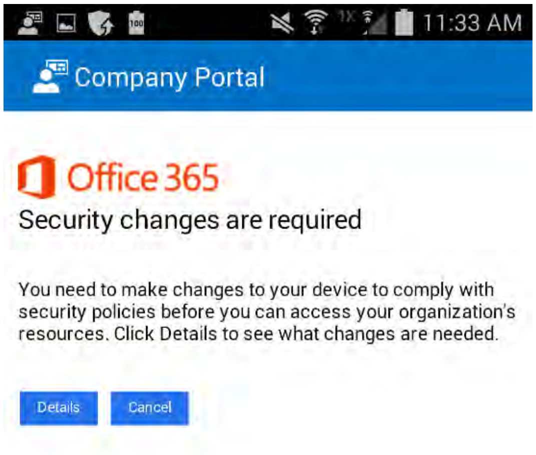
4. Note that if you are using the hybrid build, a single sign-on workflow is initiated. The device owner will be redirected to their local sign-in service.



Tell us about your device

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

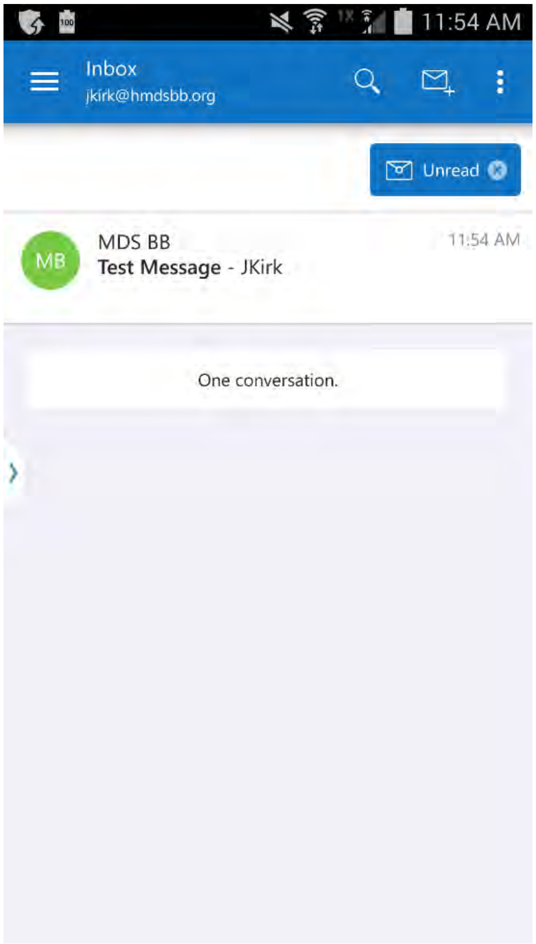
5. If your device has not been enrolled with the MDM, you will be prompted to do so.



Security changes are required

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

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.

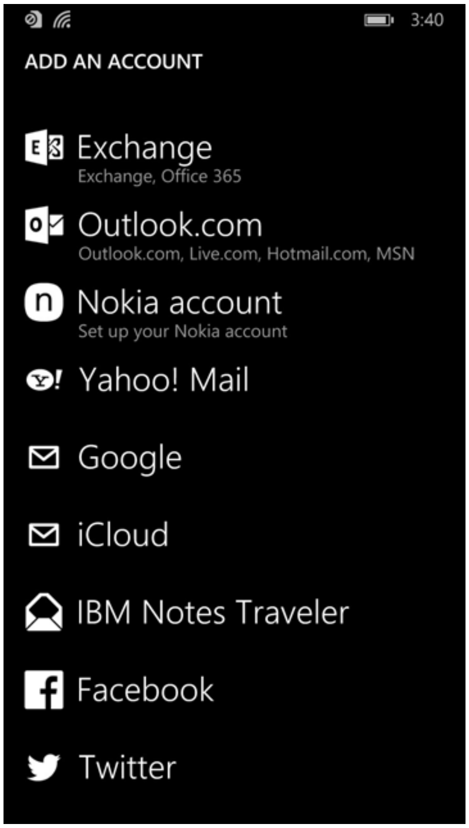


MDS BB 11:54 AM
Test Message - JKirk

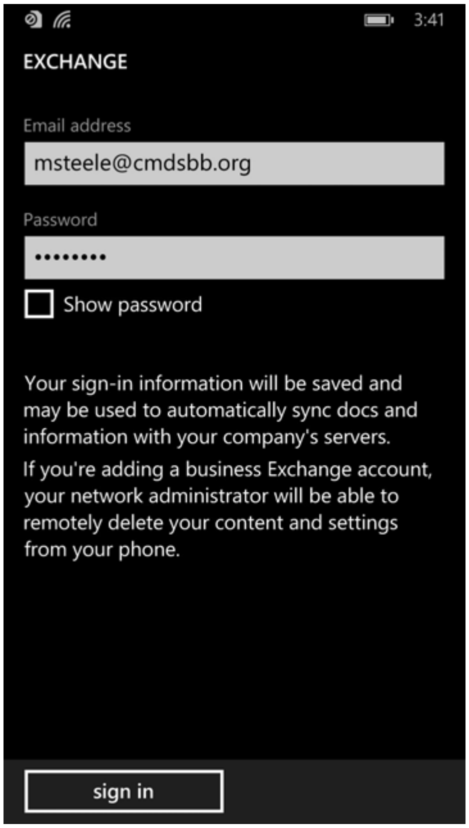
One conversation.

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

4.2.3 Windows Phone 8.1



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



EXCHANGE

Email address

msteele@cmdsbb.org

Password

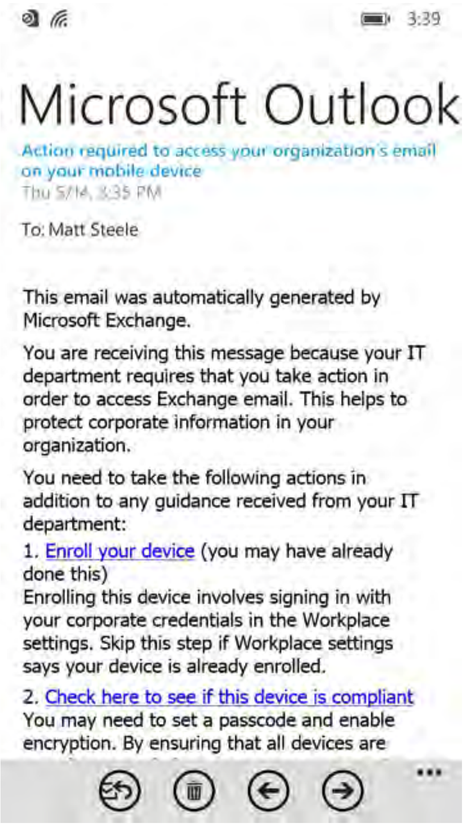
••••••••

□ Show password

Your sign-in information will be saved and may be used to automatically sync docs and information with your company's servers.

If you're adding a business Exchange account, your network administrator will be able to remotely delete your content and settings from your phone.

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



Microsoft Outlook

Action required to access your organization's email on your mobile device

Thu 5/14, 3:35 PM

To: Matt Steele

This email was automatically generated by Microsoft Exchange.

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

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

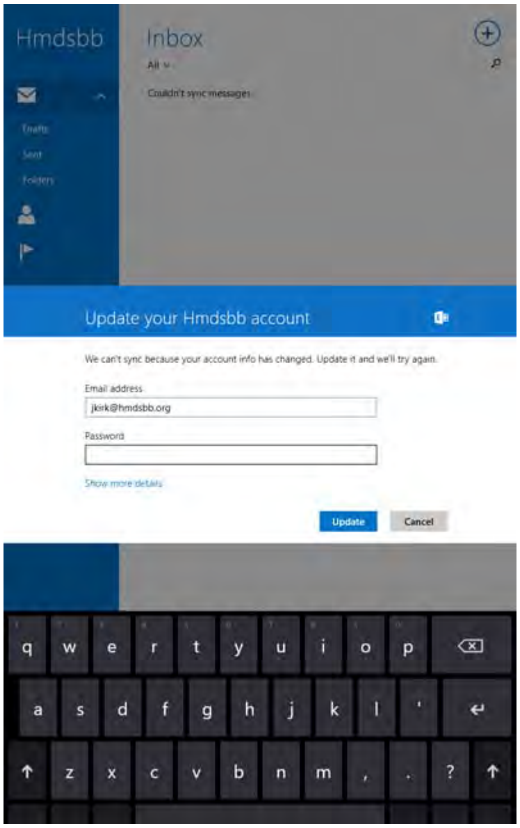
1. Enroll your device (you may have already done this)
Enrolling this device involves signing in with your corporate credentials in the Workplace settings. Skip this step if Workplace settings says your device is already enrolled.

2. Check here to see if this device is compliant
You may need to set a passcode and enable encryption. By ensuring that all devices are

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.



Couldn't sync messages

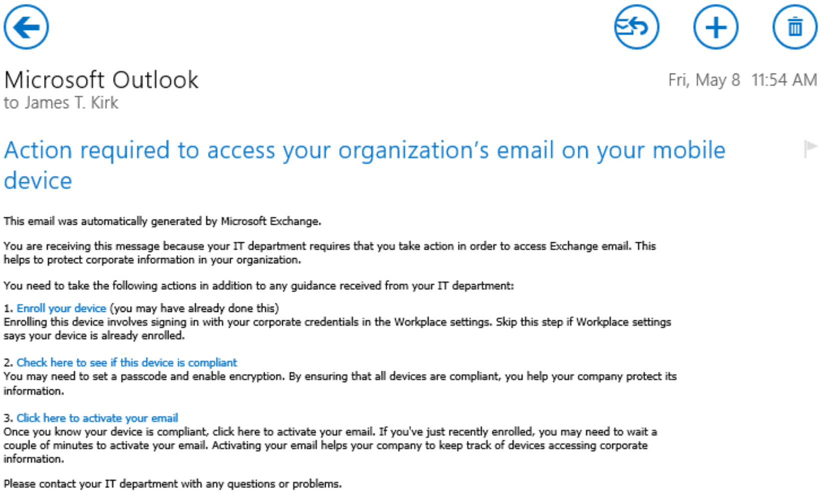
Update your Hmdsbb account

We can't sync because your account info has changed. Update it and we'll try again.

Email address: jkirk@hmdsbb.org

Password

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



Microsoft Outlook
to James T. Kirk

Fri, May 8 11:54 AM

Action required to access your organization's email on your mobile device

This email was automatically generated by Microsoft Exchange.

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

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

1. Enroll your device (you may have already done this)
Enrolling this device involves signing in with your corporate credentials in the Workplace settings. Skip this step if Workplace settings says your device is already enrolled.

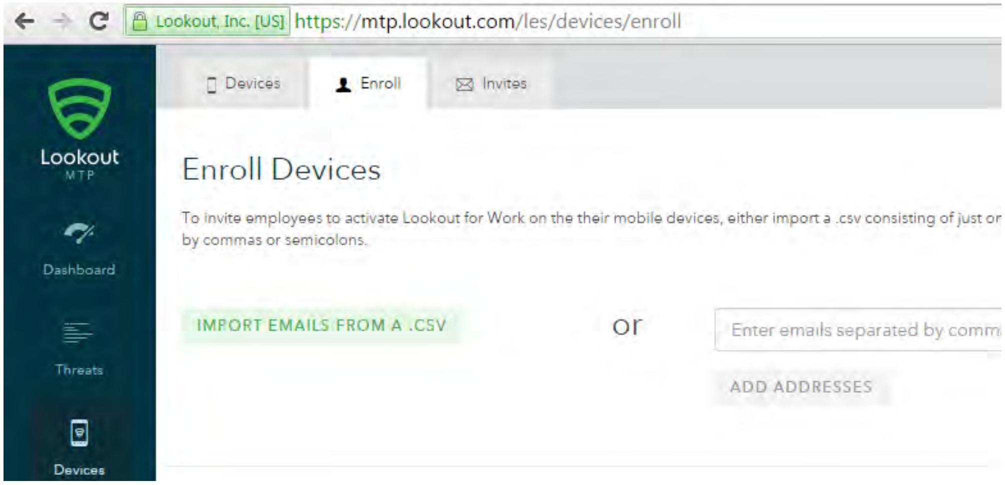
2. Check here to see if this device is compliant
You may need to set a passcode and enable encryption. By ensuring that all devices are compliant, you help your company protect its information.

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

Please contact your IT department with any questions or problems.

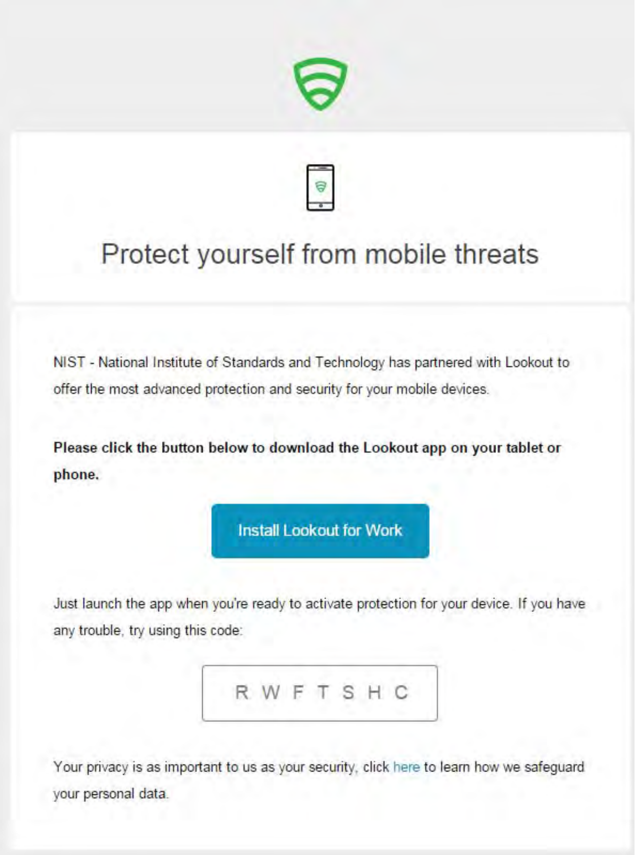
2. Upon connecting to their exchange account, the user should receive an email asking them to activate their email by clicking the link to check compliance.

4.3 Lookout MTP Enrollment



To invite employees to activate Lookout for Work on the their mobile devices, either import a .csv consisting of just or
by commas or semicolons.

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



Protect yourself from mobile threats

NIST - National Institute of Standards and Technology has partnered with Lookout to offer the most advanced protection and security for your mobile devices.

Please click the button below to download the Lookout app on your tablet or phone.

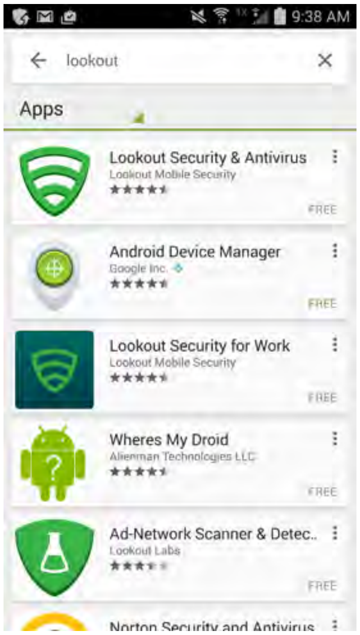
Just launch the app when you're ready to activate protection for your device. If you have any trouble, try using this code:

RWFTSHC

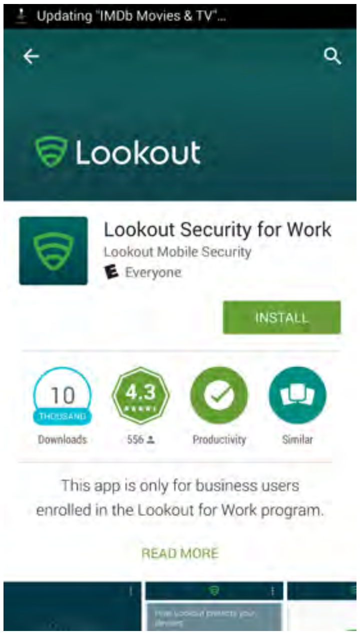
Your privacy is as important to us as your security, click here to learn how we safeguard your personal data.

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

4.3.1 Android

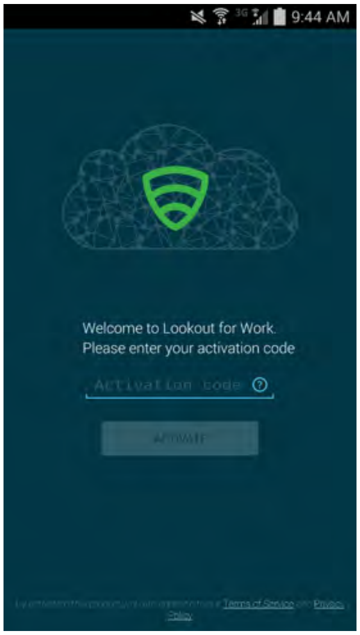


1. Find the MTP application in the Play store by searching **lookout**.



This app is only for business users enrolled in the Lookout for Work program.

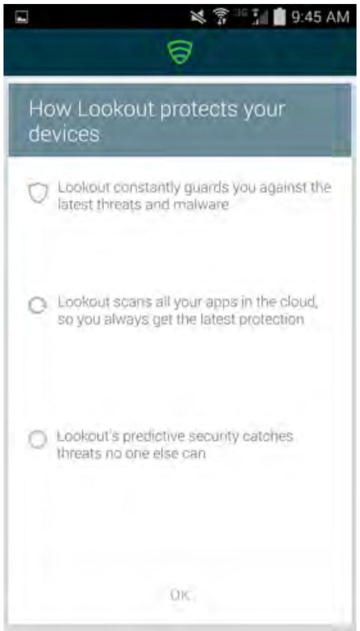
2. Select the **Lookout Security for Work** application and tap **Install**.



Welcome to Lookout for Work.
Please enter your activation code

[illegible] Terms of Service and Privacy Policy

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



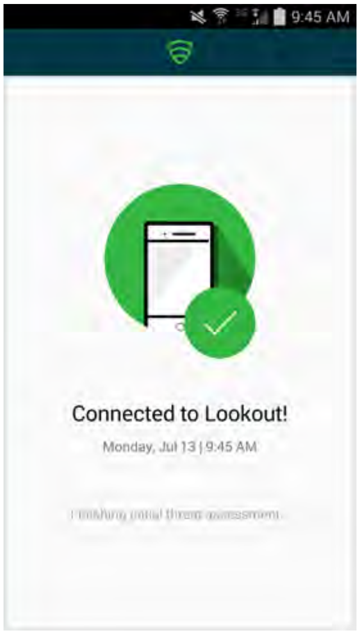
How Lookout protects your devices

Lookout constantly guards you against the latest threats and malware

Lookout scans all your apps in the cloud, so you always get the latest protection

Lookout's predictive security catches threats no one else can

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

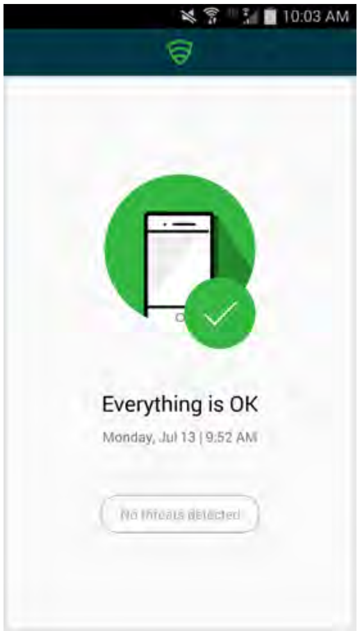


Connected to Lookout!

Monday, Jul 13 | 9:45 AM

Finishing initial threat assessment...

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



Everything is OK

Monday, Jul 13 | 9:52 AM

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

Appendix A Acronyms

2FA	Two-Factor Authentication
AD	Active Directory
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
ADAL	Active Directory Authentication Library
BYOD	Bring Your Own Device
CAG	Consensus Audit Guidelines
CBC	Cipher Block Chaining
CIO	Chief Information Officer
COPE	Corporately Owned and Personally Enabled
COTS	Commercial Off-The-Shelf
CSD	Computer Security Division
CSF	Cybersecurity Framework
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GSA	General Services Administration
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].