2017

System Center Configuration Manager

ENTERPRISE MOBILITY+SECURITY E-BOOK

RAPHAEL PEREZ, MICROSOFT MVP IN ENTERPRISE MOBILITY

MVP Profile: https://mvp.microsoft.com/en-us/PublicProfile/4027143

Twitter: @dotraphael

LinkedIn: https://uk.linkedin.com/in/dotraphael

Blog: http://thedesktopteam.com/raphael

Company: http://www.tucandata.com

DAVID NUDELMAN, MICROSOFT MVP IN WINDOWS AND DEVICES FOR IT

MVP Profile: https://mvp.microsoft.com/en-us/PublicProfile/4028355

Twitter: @nudelmanuk

LinkedIn: https://www.linkedin.com/in/dnudelman

Blog: http://thedesktopteam.com/david

Company: http://www.tucandata.com

Version: 1.00 | Date: April 2017

Table of Contents

1. Document Change Control Sheet

1.1. Document History

Date	Author	Version	Change/Reference
April/2017	Raphael Perez David Nudelman	1.00	Initial Release

2. About

2.1. Raphael Perez (Author)

Raphael is a 8 times Microsoft MVP (https://mvp.microsoft.com/en-us/PublicProfile/4027143) with over 20 years of experience in IT, in which 14 years have been dedicated to System Center and Automation.

One of the three MVPs in Enterprise Client Management in the UK, Raphael holds more than 25 Microsoft certifications and is a MCT (Microsoft Certified Trainer). Since 2008, Raphael has been providing Microsoft trainings from basic to advanced levels in several categories.

Throughout his career, Raphael has joined as speaker in well-known events such as TechEd and Gartner Security Risk Management. He also organised community events and lectured around the world, sharing best practices and knowledge within the industry.

Bilingual in English and Portuguese, Raphael has authored diverse articles published in Microsoft's TechEd, served as the editor-in-chief of a magazine focused on System Center in Brazil and wrote two books: "Understanding System Center 2012 SP1 Configuration Manager: The walkthrough book" (https://wp.me/p3ttD0-am and https://wp.me/p3ttD0-8S) and "System Center 2012 R2 Configuration Manager: Automation from Zero to Hero" (https://wp.me/p3ttD0-pd).

He is a Community leader attending physical and virtual meetings and engaging with the community across several forums, twitter (http://twitter.com/dotraphael), LinkedIn (http://www.linkedin.com/in/dotraphael) and his blog (http://www.thedesktopteam.com/).

Raphael is Technical Director at TucanData Ltd (http://www.tucandata.co.uk/), a company that provides extensions to enterprise applications, enhancing reports and data visualisation capabilities as well as consultancy and training services within the United Kingdom and has been working in several different System Center Configuration Manager and OS Deployment projects from small to enterprise environments across the UK.

2.2. David Nudelman (Author)

David has over 15 years of experience in IT Infrastructure strategy, deployment, migration and management. He is a very experienced technical leader that focus on enabling and training his team to achieve more. He holds certifications from Microsoft, Citrix, HP and VMware, and was awarded seven times as Microsoft Most Valuable Professional, due to his outstanding contributions to the Technical Community.

As a conference speaker David has a very informal style of delivering presentations and speeches. Mr. Nudelman presented at key conferences such as TechEd Europe and US, IP Expo, Global Azure Bootcamp, Computer Weekly CW500 and many more. He is a Cloud Activist, encouraging and helping companies to embrace and adopt cloud technologies.

David is a blogger and writer, contributing to communities such as The Desktop Team (www.thedesktopteam.com) and IT Pro Spain (www.itpro.es). He is one of the top 5% contributors to the Microsoft TechNet forums, earning multiple times the “Microsoft Community Contributor” award.

David is the Operations Director at TucanData Ltd (http://www.tucandata.co.uk/), a company that provides extensions to enterprise applications, enhancing reports and data visualisation capabilities as well as consultancy and training services within the United Kingdom.

Find out more about him on Twitter (https://twitter.com/nudelmanuk) or on his personal blog at http://thedesktopteam.com/david

2.3. Niall Brady (Reviewer)

Niall is an Irishman living in Sweden with 3 kids. He blogs about System Center Configuration Manager and Microsoft Intune. He's the guy behind https://www.windows-noob.com.

2.4. Panu Saukko (Reviewer)

Panu from Finland has trained and consulted Microsoft management products about 20 years. He has been MVP for 13 years. His Twitter account is http://tuwitter.com/panusaukko.

3. Introduction

This e-book has been created to provide you with step by step instructions, to improve your understanding of the Enterprise Mobility+Security world with System Center Configuration Manager (SCCM) and Intune. The intended audience of this e-book are technical people that want to learn or improve their understanding of Mobile Device Management (MDM) with SCCM and Intune. Minimum knowledge of the following software and technologies is assumed, including but not limited to Active Directory, SQL Server, Windows, Hyper-V, Mobile Device (iOS, Android, Windows Phone), Mac OS X and Windows Client (i.e. Windows 10). Knowledge of SCCM Current Branch or early versions (including SCCM 2012, SCCM 2007 and SMS 2003) is beneficial.

It's recommended to use this e-book as it has been written because there are dependencies between the chapters.

Please note that the terms System Center Configuration Manager, ConfigMgr, Configuration Manager, CM and SCCM all refer to the same Microsoft product, and the terms are used interchangeably.

4. Lab Information

The Enterprise Mobility+Security lab environment was created using Hyper-V 2016 Virtual Machines connected to its own virtual network, it also has the following hardware (that cannot be emulated on Hyper-V):

- 1x Mac OS X 10.11
- 1x iPhone or iPad
- 1x Windows Phone 8.1

The lab has six (6) virtual machines installed on one (1) Hyper-V host, installed with default configuration, as per following configuration:

Virtual Machine	Hardware	Description	Base OS
HYPER-V	RAM: 24GB Drive 01 (C): 500GB Drive 02 (D): DVD Processor/Core: 4 Network Adapter	Hyper-V Server	Windows Server 2012 R2 IP Address: DHCP
ROUTER01	RAM: 512MB Drive 01: 2GB Processor/Core: 1 Network Adapter Network Adapter	Linux router used to connect VMs to the internet	VyOS 1.1.3 External IP: DHCP Internal IP: 192.168.3.254 Internal Subnet 255.255.255.0 Internal DNS 192.168.3.1
SRV0001	RAM: 2048MB Drive 01 (C): 127GB Drive 02 (D): DVD Processor/Core: 1 Network Adapter	Domain Controller for domain called classroom.intranet (netbios name classroom), DNS, DHCP and Enterprise CA	Windows Server 2012 R2 IP Address: 192.168.3.1 Subnet 255.255.255.0 Default Gateway: 192.168.3.254 DNS 192.168.3.1
SRV0002	RAM: 8192MB Drive 01 (C): 127GB Drive 02 (D): DVD Processor/Core: 2 Network Adapter	Site Server for ConfigMgr	Windows Server 2012 R2 IP Address: 192.168.3.2 Subnet 255.255.255.0 Default Gateway: 192.168.3.254 DNS 192.168.3.1
WKS0001	RAM: 2048MB Drive 01 (C): 127GB Processor/Core: 1 Network Adapter	Windows 10 Enterprise Edition x64 – Workstation	Windows 10 x64 IP Address: DHCP
WKS0003	RAM: 1024MB Drive 01 (C): 127GB Processor/Core: 1	Android 4.4 – Workstation	Android 4.4 IP Address: DHCP

	Network Adapter		
WKS0005	RAM: 2048MB Drive 01 (C): 127GB Processor/Core: 1 Network Adapter	Windows Mobile 10	Windows Phone 10 Emulator IP Address: DHCP

All user accounts have the password set to Pa$$w0rd and the below list explains its utilization:

Account	Objective
CLASSROOM\administrator	Domain admin account
CLASSROOM\admworkstation	Domain user account used to demonstrate RBA settings.
CLASSROOM\sccmadmin	Account with full rights on the SCCM Servers
CLASSROOM\sccmpush	Account used for client push. This account has admin rights on all workstations
CLASSROOM\svc_sccmna	Account used as network account
CLASSROOM\svc_ssrsea	Account used as SSRS execution account
CLASSROOM\svc_sccmjoin	Account used to join computers to the domain
CLASSROOM\User01	Account used to deploy software to
CLASSROOM\User02	Account used to deploy software to

The following table shows the groups created to be used on this training and its objective:

Group	Objective
CLASSROOM\SCCM Admins	Contain all users with Full Access to the SCCM Infrastructure and it is a member of the SCCM Remote Tools
CLASSROOM\Workstation Admins	Contain the Admworkstation user
CLASSROOM\SCCM Remote Tools	Contain users with rights to remote access client machines
CLASSROOM\SCCM Servers	Contain all SCCM Servers

4.1. PowerShell

Automation is a key skill for IT Professionals in today's world and everything can be automated. Within Windows and System Center Configuration Manager this is also true, so I have created some scripts that can help you start creating your lab. The collection of scripts can be downloaded from http://www.tucandata.com/TrainingFiles/TrainingFilesv2.zip.

Some of the scripts are used to create the entire lab environment using Hyper-V. It is recommended to use PowerShell ISE instead of a normal PowerShell console as it is richer environment. While many PowerShell scripts are expected to run without any user intervention, they have not been created to log or show results easily. Some scripts require you to run few lines at a time as a reboot of the machine may be necessary.

Note: To be able to run the PowerShell scripts, you need to change the PowerShell Execution Policy accordingly. This is necessary because the scripts are not signed.

This can be achieved via an elevated PowerShell console using the commands below:

```
Set-ExecutionPolicy Unrestricted -Force
```

4.2. Installing a Hyper-V Server

Before we start, we need to build a Hyper-V Server that will host our Virtual Environment. To create a Hyper-V Server, perform the following actions:

01. Download Windows Server 2016 Evaluation from Microsoft website https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016 and burn a DVD
02. Insert the Windows Server 2016 DVD-ROM and turn on your computer. After a few minutes, you receive the Windows Server 2016 screen shown. Select the correct Language, Time and Currency Format and Keyboard or input method and Click Next.
03. On the next Install Windows screen, click Install now.
04. On the Select the Operating System you want to install, select Windows Server 2016 Standard Evaluation (Server with a GUI) and click Next.
05. Under License terms, select I accept the license terms and click Next
06. Under Which type of installation do you want? Click Custom: Install Windows only (advanced)
07. Under Where do you want to install Windows? Click Next
08. The Installation will start and it will take some time to complete (15-30 minutes depending on your hardware).
09. Once the installation is completed, On the Settings, you must change the password before logging on for the first time. Once completed, click Finish.
10. Perform a full windows update until there is no other update to be applied
11. Download the Required Scripts from http://www.tucandata.com/TrainingFiles/TrainingFilesv2.zip and extract to c:\

4.3. Installing Hyper-V Role

Perform this task on Hyper-V server logged on as administrator
01. In Server Manager, on the Manage menu, click Add Roles and Features.
02. On the Before you begin page, verify that your destination server and network environment are prepared for the role and feature you want to install. Click Next.
03. On the Select installation type page, select Role-based or feature-based installation and then click Next.
04. On the Select destination server page, select a server from the server pool and then click Next.
05. On the Select server roles page, select Hyper-V.
06. To add the tools that, you use to create and manage virtual machines, click Add Features and click Next.
07. On the Features page, click Next.
08. On the Hyper-V page, click Next
09. On the Create Virtual Switches page, click Next
10. On the Virtual Machine Migration page, click Next
11. On the Default Stores page, click Next
12. On the Confirm installation selections page, select Restart the destination server automatically if required.
13. On the Add Roles and Features Wizard message, click Yes and them Install
14. When the server reboots, open the Server Manager so the installation can finish. Once done, click close

4.4. Downloading Software

Once we have our Hyper-V host configured, it is time to download the required software and create the virtual machines,

Perform this task on Hyper-V server logged on as administrator
01. Open PowerShell (run as administrator) and navigate to C:\Trainingfiles\Scripts
02. Execute .\DownloadSoftware.ps1 **Note:** If anti-virus software has been enabled on the Hyper-V host, it is recommended to add C:\TrainingFiles as an exclusion. Otherwise the anti-virus software will identify the C:\TrainingFiles\Source\Eicar\eicar test file.txt as a Virus. More information can be found at http://www.eicar.org/ **Note:** It is expected to download about 20GB of data.

4.5. Creating Windows Virtual Machines

Perform this task on Hyper-V server logged on as administrator
01. Open PowerShell (run as administrator) and navigate to C:\Trainingfiles\Scripts

02. Execute .\CreateVMs.ps1

4.6. CLASSROOM-ROUTER01

Perform this task on router01 virtual machine
01. Boot Virtual Machine CLASSROOM-ROUTER01
02. Log in using **vyos** as login and password
03. Type **install image** and press enter
04. On Would you like to continue, press enter
05. On Partition, press enter
06. On Install the image on, press enter
07. On Continue, type **Yes** and press enter
08. On How big of a root partition should I create, press enter
09. On What would you like to name this image, press enter
10. On Which one should I copy to sda, press enter
11. On Enter password for user 'vyos', type **Pa$$w0rd** and press enter
12. On Retype password for user 'vyos' type **Pa$$w0rd** and press enter
13. On Which drive should grub modify the boot partition on, press enter
14. Type **poweroff** and press enter
15. On Proceed with poweroff, type **Yes** and press enter
16. Select Media -> DVD Drive -> Eject vyos-1.1.3-amd64.iso and power on the virtual machine
17. Log on with login **vyos** and password **Pa$$w0rd**
18. Type **configure** and press enter
19. Type **set interface ethernet eth0 address dhcp** and press enter
20. Type **set interface ethernet eth0 description 'External'** and press enter
21. Type **set interface ethernet eth1 address 192.168.3.254/24** and press enter
22. Type **set interface ethernet eth1 description 'Internal'** and press enter
23. Type **set system name-server 8.8.8.8** and press enter
24. Type **set system name-server 8.8.4.4** and press enter
25. Type **set system host-name router01** and press enter
26. Type **set nat source rule 100 outbound-interface 'eth0'** and press enter
27. Type **set nat source rule 100 source address '192.168.3.0/24'** and press enter
28. Type **set nat source rule 100 translation address masquerade** and press enter
29. Type **commit** and press enter
30. Type **save** and press enter
31. Type **exit** and press enter
32. Type **show interfaces** and press enter
33. Type **ping www.google.com** and press enter

4.7. CLASSROOM-SRV0001

Perform this task on srv0001 virtual machine. This will be the domain controller.
01. Confirm the Virtual Machine CLASSROOM-ROUTER01 is up and is providing internet connectivity
02. Boot Virtual Machine CLASSROOM-SRV0001

03. Log on as administrator
04. Open PowerShell (run as administrator) and navigate to C:\Trainingfiles\Scripts
05. Type.**\SRV0001.ps1** and press Enter
06. Type **.\SRV0001-01-InstallDC.ps1** and press Enter **Note:** The computer will restart automatically
07. Log on as administrator, Open PowerShell (run as administrator) and navigate to C:\Trainingfiles\Scripts
08. Type **.\SRV0001-02-ConfigureDC.ps1** and press Enter
09. Open Active Directory Users and Computers and navigate to classroom.intranet -> Classroom -> users
10. Click Create a new User
11. On New Object – User • First Name: Device Enrollment Manager • User Logon Name: deviceenrollment • User Logon name (pre-windows 2000): deviceenrollment Click Next
12. On Password: • Password: Pa$$word • User must change password at next logon: disabled • Password never expires: enabled Click Next
13. On Completion, click Finish

4.8. CLASSROOM-SRV0002

Perform this task on srv0002 virtual machine. This will be ConfigMgr site server.
01. Confirm the Virtual Machine CLASSROOM-ROUTER01 is up and is providing internet connectivity
02. Confirm the Virtual Machine CLASSROOM-SRV0001 is up and has been configured as Domain Controller
03. Boot Virtual Machine CLASSROOM-SRV0002
04. Log on as classroom\administrator
05. Open PowerShell (run as administrator) and navigate to C:\Trainingfiles\Scripts
06. Type **.\SRV0002.ps1** and press Enter **Note:** Computer will shutdown

4.9. CLASSROOM-WKS0001

Perform this task on wks0001 virtual machine. This will be Windows 10 x64 Enterprise client.
01. Confirm the Virtual Machine CLASSROOM-ROUTER01 is up and is providing internet connectivity
02. Confirm the Virtual Machine CLASSROOM-SRV0001 is up

03. Boot Virtual Machine CLASSROOM-WKS0001
04. Log on as classroom\administrator
05. Open PowerShell (run as administrator)
06. Type **Set-ExecutionPolicy Unrestricted -force** and press Enter
07. Type **\\srv0001\Trainingfiles\Scripts\WKS0001.ps1** and press Enter **Note:** Computer will shutdown

4.10. CLASSROOM-WKS0003

Perform this task on wks0003 virtual machine. This will be Android 4.4 emulator.
01. Confirm the Virtual Machine CLASSROOM-ROUTER01 is up and is providing internet connectivity
02. Boot Virtual Machine CLASSROOM-WKS0003
03. Select Installation – Install Android-x86 to hard disk and press [ENTER]
04. On Choose Partition, select Create Modify partition and press OK
05. On Cfdisk select New and then Primary. Leave the default size.
06. Select write and type Yes
07. Select quit
08. Back to Choose Partition, select sda1 Linux Virtual Disk and then OK
09. On Choose a filesystem, select ext3 and then Ok
10. On the Confirmation to format the disk, select Yes.
11. On the confirmation to install GRUB, select Yes
12. On Question (confirmation to install a read-write system), select Yes
13. When the Congratulations screen appear, select Actions -> Turn off
14. Select Media -> DVD Drive -> Eject android-x86-4.4-r2.iso
15. Select Actions -> Start
16. On the Android, click Ok and Ignore the Bluetooth warning.
17. On the Welcome, select the language and click Next
18. On the Select Wi-Fi, click Skip
19. On the WARNING message, click Skip anyway
20. On Got Google, click No
21. On Make it google, click Not Now
22. On Google & Location, click on the Right arrow
23. On the Date & Time, click Next
24. On This Tablet belongs to… complete with your name and click Next
25. On Google service, click on the Right arrow
26. On Welcome, click Ok
27. On Organise your space, click Ok
28. Drop down the top right of the screen and choose Settings
29. Click Display and then Sleep and select Never time out
30. Drop down the top right of the screen and choose Power off and then click Ok

4.11. CLASSROOM-WKS0005

Perform this task on Hyper-V host. This will be Windows 10 Mobile emulator.
01. Execute EmulatorSetup.exe from C:\TrainingFiles\Source\W10MobileEmulator
02. On Specify Location, click Next
03. On Windows Kits Privacy, click Next
04. On License Agreement, click Next
05. On Select the features you want to install, click Install
06. On Welcome to the Microsoft Emulator – Windows 10.0.14393.0!, click Close and restart computer
07. Confirm the Virtual Machine CLASSROOM-ROUTER01 is up and is providing internet connectivity
08. To Start the CLASSROOM-WKS00005 Virtual Machine, Open Command Prompt as administrator and execute "C:\Program Files (x86)\Microsoft XDE\10.0.14393.0\XDE.exe" /name "CLASSROOM-WKS0005" /vhd "C:\Program Files (x86)\Windows Kits\10\Emulation\Mobile\10.0.14393.0\Flash.vhd" /memsize 2048 /video "1440x2560" /createdifdisk "C:\TrainingFiles\vhdx\CLASSROOM-WKS0005.vhd" /snapshot /fastShutdown

5. SCCM Environment

For this e-book, you must have a SCCM Current Branch environment version 1610 connected to the internet. We have built the lab using the steps and scripts available in our e-book Administering SCCM that is available at https://goo.gl/XnD9Hl

6. Microsoft Intune Setup and Initial Configuration

Computers used in this Lab	ROUTER01 SRV0001
Description	In this chapter, we will be starting the configuration for the intune. We will be setting up a new Intune trial, Adding domain, configuring DNS and Active Directory as well as Assign necessary licenses.

6.1. Microsoft Intune Setup

Perform this task on srv0001 virtual machine logged on as administrator
01. On a browser and navigate to http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/default.aspx and click on the try now button **Note:** In a production environment, I would recommend looking at the EM+S licenses as it adds more benefits for the Management and Security of a device https://www.microsoft.com/en-gb/cloud-platform/enterprise-mobility-security-pricing
02. Fill up the Sign-up form and confirm the creation of the Microsoft Intune Subscription
03. On Don't lose access to your account, click Remind me later
04. The Microsoft Intune subscription has been created and the Microsoft Intune Account Portal should be open
05. A confirmation email from the Microsoft Intune will be sent to email used
06. Click Licenses and confirm that there are 100 licenses that can be used on this trial
07. Click domain and confirm that the onmicrosoft.com domain is already active

6.2. Adding Domains

Perform this task on srv0001 virtual machine logged on as administrator
01. On a browser and navigate to https://portal.office.com
02. Expand Settings and click Domains
03. On Domains, click Add a domain
04. On Specify domain, type your company public test domain name and click next
05. On verify domain, select Add a TXT record (preferred method) under Verify by and make a note of the Text value to be added
06. On your DNS environment, add or change the TXT record with the value required by the Microsoft Intune
07. Once the DNS change has been completed, click verify and you will see that the domain has been added. Click Verify
08. On Set up your online services, select I'll manage my own DNS records and click Next
09. On Update DNS settings make a note of the DNS settings
10. On your DNS environment, add or change the DNS records with the value required by the Microsoft Intune
11. Once the DNS change has been completed, click verify and you will see that the domain has been added. Click Verify

12. On Update DNS Settings, click Finish
13. The list of domains has been updated and the public domain shows Setup complete

6.3. Setting up DNS for Enrollment

Perform this task on srv0001 virtual machine logged on as administrator
01. On your DNS environment, add a CNAME record EnterpriseEnrollment pointing to EnterpriseEnrollment-s.manage.microsoft.com
02. Add a CNAME record enterpriseregistration pointing to enterpriseregistration.windows.net
03. Open a command prompt and type nslookup and press [ENTER]
04. Type EnterpriseEnrollment.<Domain> and press enter, it should have a reply similar to Non-authoritative answer: Name: enterpriseenrollment-s.manage.microsoft.com.nsatc.net Address: 134.170.168.254 Aliases: enterpriseenrollment.<domain> enterpriseregistration.windows.net enterpriseregistration.windows.net.nsatc.net
05. type enterpriseregistration.<domain> and press enter, it should have a reply similar to Non-authoritative answer: Name: prod-a-drs-neu.cloudapp.net Address: 40.69.218.132 Aliases: enterpriseregistration.<domain> EnterpriseEnrollment-s.manage.microsoft.com

6.4. Configuring Active Directory User Principal Name (UPN)

Perform this task on srv0001 virtual machine logged on as administrator
01. Open Active Directory Domains and Trusts
02. Select Active Directory Domains and Trusts and click Properties
03. Under Alternative UPN suffixes, type your Internet DNS suffix and click Add and then OK

6.5. Changing Active Directory Users' UPN

Perform this task on srv0001 virtual machine logged on as administrator
01. Open Active Directory Users and Computers
02. Select Classroom -> Users
03. Select User01 and click Properties
04. On User01 Properties, select account
05. On User logon name, change the @classroom.intranet to the public UPN and click Ok
06. Repeat the process for User02 and deviceenrollment

6.6. Active Directory Synchronization with Azure AD Connect

Perform this task on srv0001 virtual machine logged on as administrator
01. Execute AzureADConnect.msi from \\srv0001\TrainingFiles\Source\ADConnect
02. On Welcome to Azure AD Connect, click I agree to the license terms and privacy notice and click Continue.
03. On Express Settings, click Customize
04. On Install required components, click Install
05. On User sign-in, select Password Synchronization and click Next **Note:** This setting will replicate the password hash to Azaure Active Directory. In a production environment you may want to disable this option and use ADFS instead.
06. On Connect to Azure AD, enter the Account used to create the Intune Subscription and click Next
07. On Connect your directories, under Username type classroom\administrator and under Password type Pa$$word and click Add Directory and then click Next
08. On Azure AD sign-in configuration, select userPrincipalName under User Principal Name and click Next
09. On Domain and OU filtering, select Sync selected domains and OUs and select only classroom.intranet -> classroom -> Users and click Next
10. On Uniquely identifying your users, click Next
11. On Filter users and devices, click Next
12. On Optional features, select Password write-back and click Next
13. On Ready to configure, click Install
14. On Configuration complete, click Exit

6.7. Validating Active Directory Synchronization

Perform this task on srv0001 virtual machine logged on as administrator
01. On a browser and navigate to https://portal.office.com
02. Expand Users and click Active Users
03. On the List of users, confirm User01, User02 and deviceenrollment have been added and the Status shows as Unlicensed.

6.8. Assigning a License to a User

Perform this task on srv0001 virtual machine logged on as administrator
01. On a browser and navigate to https://portal.office.com
02. Expand Users and click Active Users
03. On the List of users, select User01
04. On User01, under Product licenses, click Edit
05. On Product licenses, select the Location and under Intune, turn it on and click Save and then click Close twice

06. Repeat the process for the User02 and Deviceenrollment

07. On the List of users, confirm the Status now shows Intune

7. System Center Configuration Manager Configuration

Computers used in this Lab	ROUTER01 SRV0001 SRV0002
Description	In this chapter, we will be starting the integration of SCCM with Intune. We'll be looking at the Collections, Service Connection Point and the Intune Subscription.

7.1. Intune Collection

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Click User Collections and click Create User Collection
03. On General, type Mobile Users under Name and select All Users under Limiting Collection and click Next
04. On Membership Rules, click Add Rule -> Query Rule
05. On Query Rule Properties, under Name type Mobile Users and click Edit Query Statement
06. On Query Statement Properties, click Criteria
07. On Criteria, click Add
08. On Criterion Properties click Select
09. On Select Attribute select: • Attribute class: User Resource • Attribute: UserPrincipalName Click Ok
10. Back on Criterion Properties, change operator to is like and value type %@<your internet DNS Name>. Click Ok three (3) times. **Note:** The Mobile Users query will look similar to the following: select SMS_R_USER.ResourceID,SMS_R_USER.ResourceType,SMS_R_USER.Name,SMS_R_USER.UniqueUserName,SMS_R_USER.WindowsNTDomain from SMS_R_User where SMS_R_User.UserPrincipalName like "%@clouddemolab.com"
11. Back on Membership rules, select Use incremental updates for this collection and click Next **Note:** It is not recommended to have over 250 collections with the Incremental updates enabled
12. On Summary, click Next
13. On Completion, click Close **Note:** Once the collection is created, there is a process to populate it and it may take a while. In this lab, wait 30 seconds or refresh it couple of times until you see Member Count change to 3
14. Select the collection and click Show Members

15. The collection will be expanded under Users and all users that match the query filter will be displayed.

7.2. Service Connection Point

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Site Configuration and click Servers and Site System Roles
03. Select Service Connection Point and click Properties
04. Click Online, persistent connection (recommended) and click Ok

7.3. Adding Microsoft Intune Subscriptions

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Cloud Services and click Microsoft Intune Subscriptions
03. Click Add Microsoft Intune Subscription
04. On Getting Started, click Next
05. On Microsoft Intune Subscription, click Sign In
06. On Set the Mobile Device Management Authority, select I understand that after I complete the sign-in process, the mobile device management authority is permanently set to Configuration Manager and cannot be changed and click Ok
07. On Subscription, sign in with the Account used to create the Intune Subscription and then click Next
08. On General, use the following settings: • Collection: Mobile Users • Company Name: Training Lab • Color scheme for company portal: Red • Configuration Manager site code: 001 • Select the maximum number of devices a user can enroll: 5 Click Next
09. On Specify company contact information, click Next
10. On Company Logo, add a company logo if required and click Next
11. On Device Enrollment Manager, click Next
12. On Multi-Factor Authentication, click Next
13. On Summary, click Next
14. On Completion, click Close
15. Expand Site Configuration -> Servers and Site System Roles
16. Confirm manage.microsoft.com has been added to the list with Count of roles equal to 2
17. In a web browser, navigate to https://manage.microsoft.com
18. Click Admin and then Mobile Device Management
19. Confirm the Mobile Device Management Authority is set to Configuration Manager

8. Enrolling Devices

Computers used in this Lab	ROUTER01 SRV0001 SRV0002 iPod or iPad Mac Book Pro Windows Phone 8.1 WKS0003 WKS0005
Description	In this chapter, we will be lookling at enrolling devices into the SCCM & Intune infrastructure.

8.1. Corporate Devices

8.1.1. Predeclared Devices

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand All Corporate-owned Devices and click Predeclared Devices.
03. Click Create Predeclared Devices
04. On Pre-declared devices, select Manually add IMEI or serial numbers and details and click Next
05. On Manually Entry, type the IMEI, select the Operating System and then click Next
06. On Summary, click Next
07. On Completion, click Close. **Note:** when the device is enrolled to the system, it will automatically be set to Company instead of Personal. If you are not allowing a personal device to be managed, this would not affect any way the management, however, if you are allowing users to bring their own devices (BYOD), this option can be used to, for example, use a selective wipe or not deploying a software to the device

8.1.2. Device Enrollment Manager

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Cloud Services and click Microsoft Intune Subscriptions
03. Select the Microsoft Intune Subscriptions and click Properties
04. Select Device Enrollment Manager and click Add/remove
05. On Device Enrollment Manager, select classroom\deviceenrollment, click Add than Ok twice

8.2. Windows Phone 8.1 and Windows Mobile 10

8.2.1. Allowing Enrollment of Windows Phone 8.1 and Windows Mobile 10

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Cloud Services and click Microsoft Intune Subscriptions
03. Select the Microsoft Intune Subscriptions and click Configure Platforms -> Windows Phone
04. On Microsoft Intune Subscription Properties, select Windows Phone 8.1 and Windows 10 Mobile and click Ok

8.2.2. Enrolling Windows Mobile 8.1 Devices

Perform this task on Windows Phone 8.1 device
01. On the Start Screen, scroll to the All application
02. Open System -> Workplace
03. On Workplace, click Add account
04. On Set up a work or school account, type user01@<your Internet DNS> and click Next
05. On Microsoft Intune, type Pa$$word as password and click Sign in
06. On Account Added, click Done

8.2.3. Enrolling Windows Mobile 10 Devices

Perform this task on wks0005 virtual machine
01. On the Start Screen, scroll to the All Application and select Settings
02. Select Accounts -> Access work or school
03. On Connect to work or school, click Connect
04. On Set up a work or school account, type user01@<your Internet DNS> and click Next
05. On Work or school account, type Pa$$word as password and click Sign in
06. On You're all set, click Done
07. Back on Connect to work or school, click Connect
08. On Set up a work or school account, type user01@<your Internet DNS> and click Next
09. On Microsoft Intune, type Pa$$word as password and click Sign in
10. On You're all set, click Finish

8.3. Android

8.3.1. Allowing Enrollment of Android Devices

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Cloud Services and click Microsoft Intune Subscriptions
03. Select the Microsoft Intune Subscriptions and click Configure Platforms -> Android

04. On Microsoft Intune Subscription Properties, select Enable Android enrollment click Ok

8.3.2. Enrolling Android

Perform this task on wks0003 virtual machine logged on as sccmadmin
01. On the Start Screen, click All applications and Open Play Store
02. Search for Intune Company Portal and click Install and then accept
03. Click Open
04. Click Sign in
05. On Intune Company Portal, use user01@<your DNS Domain> with Pa$$word as password and click sign in
06. On Company Access Setup, click Begin
07. On Why enroll your device, click Continue
08. On We care about your privacy, click Continue
09. On What comes next?, click Enroll
10. On Company Portal, click Activate
11. On Company Access setup, confirm the device has been enrolled properly and click continue and then done

8.4. iOS and Mac

8.4.1. Creating APNs Certificate Request

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Cloud Services and click Microsoft Intune Subscriptions
03. Click Create APNs certificate request
04. On Request Apple Push Notification Service Certificate Signing Request, type C:\trainingfiles\request.csr and click Download
05. On Subscription, sign in with the Account used to create the Intune Subscription and then click Close
06. Navigate to http://go.microsoft.com/fwlink/?LinkId=264215 and sign in with your apple ID **Note:** It is recommended that you do not use Internet Explorer for this process as it may not work as expected. **Note:** It is recommended creating a new apple ID for the company and never use your personal apple ID when creating the APN. This is because you need to use the same apple ID to renew the APN certificate
07. On Apple Push Certificate Portal, click Create a Certificate
08. On Terms of Use, click I have read and agree to these terms and conditions and click Accept
09. On Create a New Push Certificate, click choose file, select the .csr file that you saved before and click upload
10. On Confirmation, click Download and save the MDM_Microsoft Corporation_Certificate.pem file

8.4.2. Allowing Enrollment of iOS and Mac OS X

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Administration.
02. Expand Cloud Services and click Microsoft Intune Subscriptions
03. Select the Microsoft Intune Subscriptions and click Configure Platforms -> iOS
04. On Microsoft Intune Subscription Properties, select Enable iOS and Mac OS X (MDM) enrollment
05. On APNs certificate, select the .pem file that you saved before and click Ok

8.4.3. Enrolling an iOS Devices

Perform this task on an iOS device
01. On the Start Screen, click All applications and App Store
02. Search for Intune Company Portal and get to Install the App
03. Click Open
04. On Intune Company Portal, use user01@<your DNS Domain> with Pa$$word as password and click sign in
05. On Company Access Setup, click Begin
06. On Why enroll your device, click Continue
07. On We care about your privacy, click Continue
08. On What comes next?, click Enroll
09. On Install Profile, click Install
10. When asked to confirm, click Install
11. On the Warning message, click Install
12. On Remote Management, click Trust
13. On Profile Installed, click Done
14. On Open this page in “Comp Portal”?, click Open
15. On Company Access Setup, confirm the device has been enrolled properly click Continue and then Done

8.4.4. Enrolling Mac OS X Devices

Perform this task on a Mac OS X device
01. In Safari, browse to https://portal.manage.microsoft.com/
02. In Microsoft Intune, use user01@<your DNS Domain> with Pa$$word as password and click sign in
03. Click Tab Here to start enrolling your device
04. Click enroll
05. Click Install
06. On Profiles, click Install
07. On Install Management Profile click Continue
08. On Are you sure you want to install profile Management Profile? Click Install
09. Once the Management profile has been verified, close the Profiles screen

10. Back to Safari, confirm the new device now appears on the List

8.5. Validating Enrollment

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Click Devices and confirm a new device has been added to the user01 **Note:** It may take few minutes to the device to appear on the list of devices.
03. Select one of the new devices and click Properties.
04. Search for Agent Edition **Note:** It will show the Operating System type of the device
05. Search for Client Type **Note:** It will show Mobile
06. Search for MDM Compliance Status **Note:** It will show Compliant
07. Search Device Owner **Note:** It will show Personal or Corporate Click Ok
08. Click Start -> Resource Explorer
09. Expand Hardware -> Device Information
10. Select the device and under Related Objects click Primary User.
11. The collection will be expanded under Users and all primary users of the device will be shown.

9. Policies

Computers used in this Lab	ROUTER01 SRV0001 SRV0002 iPod or iPad Mac Book Pro Windows Phone 8.1 WKS0003 WKS0005
Description	In this chapter, we will be lookling at Policies and settings for the enrolled devices.

9.1. Terms and Conditions

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings and click Terms and Conditions
03. Click Create Terms and Conditions
04. On General, add a name. Click Next
05. On Terms, add a Title, Text for Tems and Text to explain what it means if the user accepts and click Next
06. On Summary, click Next
07. On Completion, click Close
08. Select the created terms and conditions and click Deploy
09. On Deploy Terms and Conditions, select Mobile Users as the User Collection and click Ok **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing **Note:** If you have created and deployed a Terms and Conditions before a user enrolling their devices, they will need to accept it befoce enrolling.

Perform this task on wks0003 virtual machine
01. On the Start Screen, open Company Portal
02. The Terms and Conditions screen will appear. Click Accept

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the Terms and Conditions deployment and click Run Summarization
04. When the Configuration Manager message appears, click OK

Note: The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status

9.2. Updating device policy

This action should happen automatically, however, it does take some time. The following list shows the policy refresh intervals for each platform:

- iOS: Every 6 hours
- Android: Every 8 hours
- Windows Phone: Every 8 hours
- Windows PC: Every 24 hours

In addition to the above list, there are also a set of other intervals that happen if the device has been recently enrolled:

- iOS: Every 15 minutes for 6 hours and then every 6 hours
- Android: Every 3 minutes for 15 minutes then every 15 minutes for 2 hours, and then every 8 hours
- Windows Phone: Every 5 minutes for 15 minutes then every 15 minutes for 2 hours, and then every 8 hours
- Windows PC: Every 3 minutes for 30 minutes, and then every 24 hours

9.3. Configuration Baselines

9.3.1. Creating Configuration Item and Baseline

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings and click Configuration Item
03. Click Create Configuration Item
04. On General, add a name and under settings for device managed without Configuration Manager client, select Windows 8.1 and Windows 10. Click Next **Note:** For Windows Phone 8 select Windows Phone, for iOS select iOS and Mac OSX and for Android select Android and Samsung KNOX
05. On Supported Platforms select Windows 10 only and click Next
06. On Device Settings, select Password and Encryption **Note:** In a production environment, you may want to select other options as well.
07. On Password, select Required under Require password settings on devices and select minimum password length (characters) of 6 and under Password complexity select PIN. Click Next
08. On Encryption, select Storage card encryption and File encryption on device as On and click Next
09. On Platform Applicability, click Next

10. On Summary, click Next
11. On Completion, click Close
12. Expand Compliance Settings and click Configuration Baselines
13. Click Create Configuration Baseline
14. On Create Configuration Baseline, type the name and under configuration data, click Add -> Configuration Item
15. On Add Configuration Items, select the configuration item created previously and click Add. Once done, click Ok twice
16. Select the created baseline and click Deploy
17. On Deploy Configuration Baseline, select Remediate noncompliant rules when supported, allow remediation outside the maintenance window, select All Mobile Devices as the Device Collection and change the simple schedule to run every 1 day and click Ok **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing **Note:** Repeat the process for each device type, Android, Mac OS X and iOS before continuing

9.3.1.1. Windows Mobile 10

Perform this task on wks0005 virtual machine
01. On the Start Screen, scroll to the All Application and select Settings
02. Select Accounts -> Access work or school
03. On Connect to work or school, click Connected to Training Lab MDM and then click Info
04. On Work or school info, click Sync
05. Once the sync has been finished, the policy will be applied and the device will ask you to be compliant by setting up a PIN. Follow the instructions on screen

9.3.1.2. Windows Phone

Perform this task on Windows Phone 8.1 device
01. On the Start Screen, scroll to the All application
02. Open System -> Workplace
03. On Workplace select the workplace and click Sync
04. Once the sync has been finished, the policy will be applied and the device will ask you to be compliant by setting up a password. Follow the instructions on screen

9.3.1.3. iOS

Perform this task on an iOS device
01. On the Start Screen, open Company Portal
02. Under devices, choose the device you are connected
03. Under Device Details, click Sync
04. On the Passcode Requirement, click Continue and Enter the passcode

9.3.1.4. Mac OS X

Perform this task on a Mac OS X device
01. On a Mac OS X, open System Preferences
02. Under System Preferences, click Profiles. The new profile should have been added

9.3.1.5. Android and Samsung KNOX

Perform this task on wks0003 virtual machine
01. On the Start Screen, open Company Portal
02. On the right, click on the 3 dots and then settings
03. Under security policy, click Sync
04. Scroll down the notification window and follow the instructions to secure your device

9.3.2. Monitoring Baseline Deployment

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the Baseline deployment and click Run Summarization **Note:** Before forcing the summarization, wait few minutes (usually it takes up to 5 minutes) for the device to send the information back to the SCCM server
04. When the Configuration Manager message appears, click OK **Note:** The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status **Note:** When using the Windows Phone 10 Emulator an error will occur when trying to set the File encryption on mobile device. You can safely ignore this.

9.4. Compliance Policies

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings and click Compliance Policies
03. Click Create Compliance Policy
04. On General, add a name and select Compliance rules for devices managed without the Configuration Manager client. Click Next
05. On Supported Platforms select Windows 10 only and click Next
06. On Rules, click New

07. On Add Rule select Require password settings on mobile devices and click OK
08. Back on the Rules, click Next
09. On Summary, click Next
10. On Completion, click Close
11. Select the created compliance policy and click Deploy
12. On Deploy Compliance Policy, select Mobile Users as the User Collection and click Ok **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing

Perform this task on wks0005 virtual machine
01. On the Start Screen, scroll to the All Application and select Settings
02. Select Accounts -> Access work or school
03. On Connect to work or school, click Connected to Training Lab MDM and then click Info
04. On Work or school info, click Sync
05. Once the sync has been finished, the policy will be applied and the device will ask you to be compliant by setting up a PIN. Follow the screen **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the Compliance Policy deployment and click Run Summarization
04. When the Configuration Manager message appears, click OK **Note:** The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status

10. Company Resources

Computers used in this Lab	ROUTER01 SRV0001 SRV0002 iPod or iPad Mac Book Pro Windows Phone 8.1 WKS0003 WKS0005
Description	In this chapter, we will be lookling at Company resources (E-mail, VPN, Wi-Fi) to be deployed to the enrolled devices.

10.1. E-mail Profiles

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings->Company Resource Access and click Email Profile
03. Click Create Exchange ActiveSync Profile
04. On General, add a name. Click Next
05. On Exchange ActiveSync configure the information for the e-mail profile. Click Next
06. On Synchronization Settings, configure how the ActiveSync profile will be synchronized. Click Next
08. On Supported Platforms, select all the platforms and click Next
09. On Summary, click Next
10. On Completion, click Close
11. Select the E-mail profile created and click Deploy
12. On Deploy Exchange ActiveSync Email Profile select All Mobile Devices device collection and under simple schedule, change to run every 1 days. Click Ok **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing Note: For tests, I would recommend creating an Office 365 Trial account, so you can test all the e-mail functionality and not only confirming the e-mail profile arrived to the device. You can start a new trial from http://go.microsoft.com/fwlink/p/?LinkID=698279&culture=en-GB&country=GB

10.1.1.1. Windows Mobile 10

Perform this task on wks0005 virtual machine
01. On the Start Screen, scroll to the All Application and select Settings
02. Select Accounts -> Access work or school
03. On Connect to work or school, click Connected to Training Lab MDM and then click Info
04. On Work or school info, click Sync
05. On the Start Screen, scroll to the All Application and select Settings
06. Select Accounts -> Email & app accounts, confirm a new account was added

10.1.1.2. Windows Phone

Perform this task on Windows Phone 8.1 device
01. On the Start Screen, scroll to the All application
02. Open System -> Workplace
03. On Workplace select the workplace and click Sync
04. On the Start Screen, scroll to the All application
05. Select email+accounts, confirm a new account was added

10.1.1.3. iOS

Perform this task on an iOS device
01. On the Start Screen, open Company Portal
02. Under devices, choose the device you are connected
03. Under Device Details, click Sync
04. On the Start Screen, open Settings
05. On Settings, click Mail, Contacts, Calendar and confirm a new account was added

10.1.1.4. Android and Samsung KNOX

Perform this task on wks0003 virtual machine
01. On the Start Screen, open Company Portal
02. On the right, click on the 3 dots and then settings
03. Under security policy, click Sync
04. Scroll down the notification window and open Settings
05. On Settings, under Accounts, confirm a new account was added **Note:** The e-mail profile is not available to all version of Android

10.1.2. Monitoring E-mail Profile Deployment

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the E-mail profile deployment and click Run Summarization
04. When the Configuration Manager message appears, click OK **Note:** The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status

10.2. VPN Profiles

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings->Company Resource Access and click VPN Profile
03. Click VPN Profile
04. On General, add a name and select VPN for any supported operating System. Click Next
05. On Configure VPN connection, configure the information for the VPN profile. Click Next
06. On Authentication Method, configure the authentication method to be used with the VPN profile. Click Next.
07. On Proxy settings, Click Next
08. On Automatic VPN, click Next
09. On Supported Platforms, select all the platforms and click Next
10. On Summary, click Next
11. On Completion, click Close
12. Select the VPN profile created and click Deploy
13. On Deploy VPN Profile select All Mobile Devices device collection and under simple schedule, change to run every 1 days. Click Ok **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing

10.2.1.1. Windows Mobile 10

Perform this task on wks0005 virtual machine
01. On the Start Screen, scroll to the All Application and select Settings
02. Select Accounts -> Access work or school
03. On Connect to work or school, click Connected to Training Lab MDM and then click Info
04. On Work or school info, click Sync
05. On the Start Screen, scroll to the All Application and select Settings
06. Select Network & wireless
07. Select VPN, confirm a new VPN profile was added

10.2.1.2. Windows Phone

Perform this task on Windows Phone 8.1 device
01. On the Start Screen, scroll to the All application
02. Open System -> Workplace
03. On Workplace select the workplace and click Sync
04. On the Start Screen, scroll to the All application
05. Select VPN, confirm a new VPN profile was added

10.2.1.3. iOS

Perform this task on an iOS device
01. On the Start Screen, open Company Portal
02. Under devices, choose the device you are connected
03. Under Device Details, click Sync
04. On the Start Screen, open Settings
05. On General, click VPN and confirm a new VPN profile was added

10.2.1.4. Mac OS X

Perform this task on a Mac OS X device
01. On a Mac OS X, open System Preferences
02. Under System Preferences, click Profiles. The new profile should have been added

10.2.1.5. Android and Samsung KNOX

Perform this task on wks0003 virtual machine
01. On the Start Screen, open Company Portal
02. On the right, click on the 3 dots and then settings
03. Under security policy, click Sync
04. Scroll down the notification window and open Settings
05. On Settings, under Wireless & Networks, click More
06. On Wireless & networks, click VPN and confirm the VPN profile was added

10.2.2. Monitoring VPN Profile Deployment

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start the Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the E-mail profile deployment and click Run Summarization
04. When the Configuration Manager message appears, click OK **Note:** The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status

10.3. Wi-Fi Profiles

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start the Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings->Company Resource Access and click Wi-Fi Profile
03. Click Wi-Fi Profile
04. On General, add a name. Click Next
05. On Wi-Fi profile, configure the information for the Wi-Fi profile. Click Next
06. On Security Configuration, configure the information for the Wi-Fi profile. Click Next
07. On Advanced Settings, click Next
08. On Proxy settings, Click Next
09. On Supported Platforms, select all the platforms and click Next
10. On Summary, click Next
11. On Completion, click Close
12. Select the Wi-Fi profile created and click Deploy
13. On Deploy Wi-Fi Profile select All Mobile Devices device collection and under simple schedule, change to run every 1 days. Click Ok **Note:** Once you are finished, wait a few minutes (usually it takes up to 5 minutes) before continuing

10.3.1.1. Windows Mobile 10

Perform this task on wks0005 virtual machine
01. On the Start Screen, scroll to the All Application and select Settings
02. Select Accounts -> Access work or school
03. On Connect to work or school, click Connected to Training Lab MDM and then click Info
04. On Work or school info, click Sync
05. On the Start Screen, scroll to the All Application and select Settings
06. Select Network & wireless
07. Select WiFi
08. Select Manage, confirm a new account was added

10.3.1.2. Windows Phone

Perform this task on Windows Phone 8.1 device
01. On the Start Screen, scroll to the All application
02. Open System -> Workplace
03. On Workplace select the workplace and click Sync
04. On the Start Screen, scroll to the All application
05. Select WiFi
06. Click manage and confirm a new account was added

10.3.1.3. iOS

Perform this task on an iOS device
01. On the Start Screen, open Company Portal
02. Under devices, choose the device you are connected
03. Under Device Details, click Sync
04. On the Start Screen, open Settings
05. On General, click Device Management
06. Select the Device Management and confirm the Contains option has Wi-Fi Network
07. Click on More Details
08. Under WiFi Profile, confirm the Wifi profile created has been deployed

10.3.1.4. Mac OS X

Perform this task on a Mac OS X device
01. On a Mac OS X, open System Preferences
02. Under System Preferences, click Profiles. The new profile should have been added

10.3.1.5. Android and Samsung KNOX

Perform this task on wks0003 virtual machine
01. On the Start Screen, open Company Portal
02. On the right, click on the 3 dots and then settings
03. Under security policy, click Sync
04. Scroll down the notification window and open Settings
05. On Settings, under Wireless & Networks, click Wi-Fi
06. On Wireless & networks, click VPN and confirm the VPN profile was added

10.3.2. Monitoring Wi-Fi Profile Deployment

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the Wi-Fi profile deployment and click Run Summarization
04. When the Configuration Manager message appears, click OK **Note:** The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status

11. Application Deployment

Computers used in this Lab	ROUTER01 SRV0001 SRV0002 iPod or iPad Mac Book Pro Windows Phone 8.1 WKS0003 WKS0005
Description	In this chapter, we will be lookling at deploying applications to enrolled devices as well as securing applications.

11.1. Create an Application for Mobile Devices

Perform this task on SRV0002 virtual machine logged on as sccmadmin
01. Start the Configuration Manager Console and Click Software Library.
02. Expand Application Management and click Applications
03. Click Create Application
04. Under Specify settings for this application, use the following: • Type: App Package for Android on Google Play • Location: https://play.google.com/store/apps/details?id=com.microsoft.office.outlook&hl=en_GB Click Next **Note:** For Mobile Device Management, the type of application that can be used are: Windows app package (*.appx, *.appxbundle), Windows app package (in the Windows Store), Microsoft Phone app package *.xap file), Windows Phone app package (in the Windows Phone Store), App package for iOS (*.ipa file), App Package for iOS from App Store, App Package for Android (*.apk file), App Packge for Android on Google Play, Mac OS X, Web Application and Windows Installer through MDM (*.msi)
05. Under Import Information, click Next
06. Under General Information confirm that the Name of the Application has been populated correct and click Next
07. Under Summary, click Next
08. Under The Create Application Wizard completed successfully click Close

11.2. Application Management Policies

Perform this task on SRV0002 virtual machine logged on as sccmadmin
01. Start the Configuration Manager Console and Click Software Library.
02. Expand Application Management -> Application Management Policies
03. Click Create Application Management Policy

04. On General, add a Name and click Next.
05. On Policy Type select the Android as Platform and General as type of policy and click Next. **Note:** The type of policy Managed Browser lets you modify the functionality of the Intune Managed Browser app. This app allows you to manage web browsing experience for users. This includes the sites they can visit and how links to content within the browser are opened.
06. On Android Policy you can configure the individual settings that are applicable to the Android platform and the General policy type selected. Once finished, click Next. **Note:** The options may change depending on the Platform and Policy type selected
10. On Summary, click Next
11. On Completion, click Close

11.3. Deploying Managed Applications

Perform this task on SRV0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Software Library.
02. Expand Application Management and click Applications
03. Select the Application Created previously and click Deploy
04. Under Specify general information for this deployment, click Browse (Collection) and select the Collection you want to deploy. Click Next **Note:** You can deploy to a Device as well as Users. In this example we are using a User Collection – Mobile Users
05. Under Specify the content destination, click Next
06. Under specify settings to control how this software is deployed, click Next **Note:** Action can be Install or Uninstall and Purpose can be Available or Required.
07. Under Specify the schedule for this deployment, click Next
08. Under Specify the user experience for the installation of this software on the selected devices, click Next
09. Under specify Configuration Manager and Operations Manager alert options, click Next
10. Under Application Management, confirm the MAM policy created previously is already selected for the Deployment Type for the Android App and click Next
11. Under Confirm this settings for this new deployment click Next
12. Under the Deploy Software Wizard completed successfully, click Close

11.3.1. Android

Perform this task on wks0003 virtual machine
01. On the Start Screen, open Company Portal
02. On the main screen, the Application should appear. Click on it and then click View in Google Play
03. On the Google Play, click Install and then Accept.

11.3.2. iOS

Perform this task on an iOS device
01. On the Start Screen, open Company Portal
02. Under Apps, click App Apps
03. The Safari Browser will open and the App will be shown under All
04. Click on it and then click Install
05. On App Installation, click Install

11.3.3. Monitoring Application Deployment

Perform this task on SRV0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Monitoring.
02. click Deployments
03. Select the Application deployment and click Run Summarization
04. When the Configuration Manager message appears, click OK **Note:** The Summarization may take some time. Refresh the Deployment couple of times until the time of the summarization changes
05. Click view Status

12. Windows Information Protection

Computers used in this Lab	ROUTER01 SRV0001 SRV0002 WKS0001
Description	In this chapter, we will be lookling at protecting corporate data.

12.1. Client preparation

Perform this task on wks0001 virtual machine logged on as administrator
01. Upgrade the Windows to version 1607 or newer using Windows Update
02. Download and Install an evaluation version of Office Professional Plus 2013 from https://www.microsoft.com/en-gb/evalcenter/evaluate-office-professional-plus-2013

12.2. Create an Data Recovery Agent Certificate

Perform this task on wks0001 virtual machine logged on as administrator
01. Open Command Prompt as Administrator (run as Admin).
02. run **cipher /r:dracert**
03. When prompted, type and confirm a password to help protect your new Personal Information Exchange (.pfx) file.
04. Copy the dracert.cer and dracert.pfx to \\srv0001\TempFiles

12.3. Add a WIP policy

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Expand Compliance Settings and click Configuration Item
03. Click Create Configuration Item
04. On General, add a name and under settings for device managed with Configuration Manager client, select Windows 10. Click Next **Note:** For MDM clients, select device managed without Configuration Manager client and select Windows 8.1 and Windows 10
05. On Supported Platforms select Windows 10 only and click Next
06. On Device Settings, select Windows Information Protection and click Next.
07. On Windows Information Protection, click Add
08. On Add app rule, use the following: • Rule Name: Office 2013 • Enterprise data protection mode: Allow • Rule template: Desktop App • Publisher: O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US

- Product Name: MICROSOFT OFFICE 2013
- Binary Name: *
- Version: *

Click Ok

Note: To find the Publisher and Product Name of a Desktop app, perform the following:

- Open PowerShell
- Get-AppLockerFileInformation -Path "<Path of the EXE file>" | Format-List (i.e. Get-AppLockerFileInformation -Path " c:\Program Files\Microsoft Office\Office15\WINWORD.EXE" | Format-List
- The Publish Name will be the 1st part before the "\", The Product, the 1st part after the "\" and the Binary will be the last part after the last "\". Version is the part after the "," (i.e. **O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US***MICROSOFT OFFICE 2013*\WINWORD.EXE,15.0.4420.1017)

Note: To find the Publisher and Product Name of a Store app, perform the following:

- Navigate to https://go.microsoft.com/fwlink/p/?LinkID=722910
- Search for the App (i.e. Word Mobile)
- Copy the Windows Store link (i.e. https://www.microsoft.com/en-gb/store/p/word-mobile/9wzdncrfjb9s)
- Navigate to https://bspmts.mp.microsoft.com/v1/public/catalog/Retail/Products/xxx/applockerdata (change the xxx to the last part of the Windows Store link – in this case 9wzdncrfjb9s)
- Copy the publisherCertificateName to the Publisher and packageIdentityName to Product Name

Note: If you're running into compatibility issues where your app is incompatible with WIP, but still needs to be used with enterprise data, you can exempt the app from the WIP restrictions. To achieve this, select the Enterprise data protection mode as Exempt. This means that your apps won't include auto-encryption or tagging and won't honour your network restrictions. It also means that your exempted apps might leak.

09. Back on Windows Information Protection, select Override as protection level.

Note: The WIP Protection level can be:

- Block - WIP looks for inappropriate data sharing practices and stops the employee from completing the action. This can include sharing info across non-enterprise-protected apps in addition to sharing enterprise data between other people and devices outside of your enterprise.
- Override: WIP looks for inappropriate data sharing, warning employees if they do something deemed potentially unsafe. However, this management mode lets the employee override the policy and share the data, logging the action to your audit log, accessible through the Reporting CSP.
- Silent: WIP runs silently, logging inappropriate data sharing, without blocking anything that would've been prompted for employee interaction while in Override mode. Unallowed actions,

like apps inappropriately trying to access a network resource or WIP-protected data, are still blocked. • Off (not recommended): WIP is turned off and doesn't help to protect or audit your data. After you turn off WIP, an attempt is made to decrypt any closed WIP-tagged files on the locally attached drives.
10. On Windows Information Protection, define your Corporate identify as follow: • classroom.intranet
11. On Windows Information Protection, Corporate network definition, click Add
12. On Add or Edit corporate network definition, select as follow: • Name: Classroom.Intranet Domain • Network Element: Network Domain Names * • Enterprise Network Domain Names definition: classroom.intranet Click Ok
13. On Add or Edit corporate network definition, select as follow: • Name: Internal IP Address • Network Element: Enterprise IPv4 Ranges * • IPv4 Address range definition: 192.168.3.1-192.168.3.254 Click Ok
14. On Enterprise IP Ranges list as authoritative (do not auto-detect), set to Yes
15. On Show the enterprise data protection icon overlay on your allowed apps that are EDP-unaware in the Windows Start menu, and on corporate file icons in the File Explorer, set to Yes
16. On Upload a DRA (Data Recovery Agent) certificate to allow recovery of encrypted data (required), browse and navigate to \\srv0001\TempFiles. Select the dracert.cer file. Click Ok and then click Next
17. On Show the "Personal" option from the "File ownership" menus in the Windows File Explorer and the Windows Save As dialogs set to Yes
18. On Platform Applicability, click Next
19. On Summary, click Next
20. On Completion, click Close
21. Expand Compliance Settings and click Configuration Baselines
22. Click Create Configuration Baseline
23. On Create Configuration Baseline, type the name and under configuration data, click Add -> Configuration Item
24. On Add Configuration Items, select the configuration item created previously and click Add. Once done, click Ok twice

12.4. Deploy the WIP policy

Perform this task on srv0002 virtual machine logged on as sccmadmin
01. Select the created baseline and click Deploy
02. On Deploy Configuration Baseline, select Remediate noncompliant rules when supported, allow remediation outside the maintenance window, select Windows 10 Workstations as the Device Collection and change the simple schedule to run every 1 day and click Ok

Perform this task on wks0001 virtual machine logged on as user01
01. Open the Configuration Manager Properties
02. Change to the Actions Tab, select Machine Policy Retrieval & Evaluation Cycle and click Run now **Note:** Using this option will force the client to connect to the server and update its settings. By default, this happen every 60 minutes and can be changed under Client Settings -> Client Policy -> Client policy polling interval (minutes)
03. Under Machine Policy Retrieval & Evaluation Cycle click Ok **Note:** Depending on the SCCM environment, the user policy retrieval & evaluation cycle can take few minutes
04. Change to Configurations tab. **Note:** It may be necessary to click the refresh button
05. Select the WIP Baseline created before and click evaluate. **Note:** After a few seconds, the baseline compliance state should change to Compliant
06. Open Microsoft Word 2013. On the top right of the screen, you will see a new icon saying the App is now a managed app
07. Create a new document and save it on the desktop. Once done, close Microsoft Word 2013 **Note:** When saving the document, a new icon next to the file name will show what type of document it is.
08. Open Command Prompt
09. Type cipher /c <file name> **Note:** If the file has been encrypted, you will see an output similar to: C:\Users\user01>cipher /c Desktop\test2.docx Listing C:\Users\user01\Desktop\ New files added to this directory will not be encrypted. E test2.docx Compatibility Level: Enterprise Protected Enterprise protected by: classroom.intranet Recovery Certificates: Administrator(Administrator@CLASSROOM) Certificate thumbprint: 1F2C AB38 A7D0 B5D3 8A3E 833A 35AE 9009 06F7 6D54

Key Information: Algorithm: AES Key Length: 256 Key Entropy: 256
10. Open WordPad and Open the created doc. The access to the file will be denied
11. On the Windows Explorer, right click the file -> File ownership and click Personal
12. Try to open the file again on the WordPad. This time, the access will be allowed.

13. Remote Tasks

Computers used in this Lab	ROUTER01 SRV0001 SRV0002 iPod or iPad Mac Book Pro Windows Phone 8.1 WKS0003 WKS0005
Description	In this chapter, we will be lookling at remote tasks for securing a device, like Remote Lock, Reset Passcode and Retire/Wipe a enrolled device.

13.1. Remote Lock

Perform this task on an iOS device
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Select Devices and select the device you want to remote lock
03. Select Remote Device Actions -> Remote Lock
04. When the Configuration Manager message appears, click Yes

13.2. Reset Passcode

Perform this task on an iOS device
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Select Devices and select the device you want to remote lock
03. Select Remote Device Actions -> Reset Passcode
04. When the Configuration Manager message appears, click Yes
05. Select Remote Device Actions -> View Passcode **Note:** The new passcode will be available once SCCM receives the information back from Intune, and it takes up to 5 minutes

13.3. Retire/Wipe

Perform this task on an iOS device
01. Start Configuration Manager Console and Click Assets and Compliance.
02. Select Devices and select the device you want to remote lock
03. Select Remote Device Actions -> Retire/Wipe
04. On Retire from Configuration Manager, select: • Wipe company content and retire the mobile device from Configuration Manager: if you want to remove only the company data and leave the user data intact

- Wipe the mobile device and retire it from Configuration Manager: if you want to remove all content and reset the device to the its factory settings

Once you made the choice, click Ok

Note: It may take up to couple of minutes for the device to be wiped. If you selected the option to wipe the device, all the information will be removed and the device will be reset to factory settings

05. When the Configuration Manager message appears, click Yes

14. Appendix A – Tools

14.1. DataExplorer

Data Explorer is a data visualization platform which helps enterprises to streamline the access control and management of strategic business information.

By displaying key metrics and indicators in one single screen, the software interface can be tailored and expandable to support particular objectives and needs.

More info at: http://www.tucandata.com

14.2. HealthCheck Toolkit

The Healthcheck tool supports you to analyse the health conditions of the Configuration Manager in an easy and practical manner.

Through the software, users can assess the status of the Configuration Manager's performance, latest updates, disk space, client data and other key indicators.

More info at: http://www.rflsystems.co.uk/software/healthcheck-toolkit/

14.3. CM12Automation

Configuration Manager 2012 Automation is a PowerShell project to help perform the basic implementation of a CM12 infrastructure.

More info at: http://cm12automation.codeplex.com/

14.4. ConfigMgrRegistrationRequest

ConfigMgrRegistrationRequest allows you to simulate a client using SCCM Client SDK.

More info at: https://configmgrregistratio.codeplex.com/

14.5. SCCM Client Center

The tool is designed for IT Professionals to troubleshoot SMS/SCCM Client related issues. The SCCM Client Center provides a quick and easy overview of client settings, including running services and SCCM settings in a good easy to use, user interface.

More info at: https://sourceforge.net/projects/smsclictr/

14.6. Mark Cochrane RegkeytoMof 3.3a

RegKeytoMof is used to quickly create custom Hardware Inventory entries formatted correctly for the sms_def.mof and configuration.mof files, when the target is Registry keys.

More info at: http://www.enhansoft.com/blog/how-to-use-regkeytomof

Download at: http://mnscug.org/images/Sherry/RegKeyToMOFv33a.zip

14.7. RuckZuck

Software package manager, a quick way to install and update your Software.

More info at: http://ruckzuck.tools/

15. Appendix B – Unmissable Sites

Site Address	Comments
http://www.tucandata.com	3rd Party tools and Consultancy
http://www.rflsystems.co.uk	3rd Party tools and Consultancy
http://www.thedesktopteam.com	MVP Raphael Perez and MVP David Nudelman
http://blog.colemberg.ch	MVP Mirko Colemberg
http://www.dekeukelaere.com http://www.scug.be/tim	MVP Tim De Keukelaere
http://www.ronnipedersen.com	MVP Ronni Pedersen
http://sccm.biz	MVP Nicolai Henriksen
http://Stevethompsonmvp.wordpress.com	MVP Steve Thompson
https://rzander.azurewebsites.net/	MVP Roger Zander
http://sms-hints-tricks.blogspot.com/	MVP Matthew Hudson
http://faqshop.com/	MVP Cliff Hobbs