DAVID NUDELMAN

Twitter: @nudelmanuk

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

Blog: <http://thedesktopteam.com/david>

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>

Microsoft Intune

Enterprise Mobility+Security

Version: Draft v0.01 | Date: November 2018

2018

Table of Contents

[1. Document Change Control Sheet 4](#_Toc529533376)

[1.1. Document History 4](#_Toc529533377)

[2. About the Authors 5](#_Toc529533378)

[2.1. Raphael Perez (Author) 5](#_Toc529533379)

[2.2. David Nudelman (Author) 5](#_Toc529533380)

[3. Introduction 6](#_Toc529533381)

[4. Lab Information 7](#_Toc529533382)

[4.1. Installing a Hyper-V Server 7](#_Toc529533383)

[4.2. Installing Hyper-V role 8](#_Toc529533384)

[4.3. Configure Hyper-V 8](#_Toc529533385)

[4.4. CLASSROOM-WKS0001 9](#_Toc529533386)

[4.5. CLASSROOM-WKS0002 10](#_Toc529533387)

[5. Enterprise Mobility + Security Setup and Initial Configuration 11](#_Toc529533388)

[5.1. Microsoft Intune Trial License 11](#_Toc529533389)

[5.2. Office 365 Enterprise E3 Trial License 11](#_Toc529533390)

[5.3. Enterprise Mobility + Security E5 Trial License 11](#_Toc529533391)

[5.4. Set the Intune Mobile Device Authority 11](#_Toc529533392)

[5.5. Setting up DNS for Enrollment 12](#_Toc529533393)

[5.6. Adding Domains 12](#_Toc529533394)

[6. User Management 14](#_Toc529533395)

[6.1. Adding Users 14](#_Toc529533396)

[6.1.1. Single User 14](#_Toc529533397)

[6.1.2. Multiple User 14](#_Toc529533398)

[6.2. Reseting User Password 15](#_Toc529533399)

[6.3. Deleting Users 15](#_Toc529533400)

[6.4. Recovering Deleted Users 15](#_Toc529533401)

[7. Group Management 16](#_Toc529533402)

[7.1. Creating Group 16](#_Toc529533403)

[7.2. Editting Group Name 16](#_Toc529533404)

[7.3. Converting Dynamic to Assigned Group 17](#_Toc529533405)

[7.4. Converting Assigned to Dynamic Group 17](#_Toc529533406)

[7.5. Adding new members to an Assigned group 17](#_Toc529533407)

[7.6. Group Membership 18](#_Toc529533408)

[8. Device enrolment 19](#_Toc529533409)

[8.1. Enrollment Restrictions 19](#_Toc529533410)

[8.1.1. Default Enrollment Restrictions 19](#_Toc529533411)

[8.1.2. Adding Enrollment Restrictions 19](#_Toc529533412)

[8.1.3. Deleting Enrollment Restrictions 20](#_Toc529533413)

[8.1.4. Assign Enrollment Restrictions 20](#_Toc529533414)

[8.2. Corporate device identifiers 20](#_Toc529533415)

[8.2.1. Adding corporate device identifier 20](#_Toc529533416)

[8.2.2. Deleting corporate device identifier 21](#_Toc529533417)

[8.3. Terms and Conditions 21](#_Toc529533418)

[8.3.1. Create a terms and conditions policy 21](#_Toc529533419)

[8.3.2. Edit a terms and conditions policy 22](#_Toc529533420)

[8.3.3. Deleting a terms and conditions policy 22](#_Toc529533421)

[8.3.4. Assign Terms and conditions policy 22](#_Toc529533422)

[8.4. Company Portal 23](#_Toc529533423)

[8.5. Apple enrollment 23](#_Toc529533424)

[8.6. xxWindows enrollment 24](#_Toc529533425)

[8.6.1. Windows Hello for Business 24](#_Toc529533426)

[8.6.2. CNAME Validation 24](#_Toc529533427)

[8.6.3. Windows Autopilot 24](#_Toc529533428)

[9. xxDevice compliance 25](#_Toc529533429)

[10. xxPolicy 26](#_Toc529533430)

[11. xxEnrolling a Device 27](#_Toc529533431)

[12. xxManaging Windows PC 28](#_Toc529533432)

[13. xxSoftware Policy 29](#_Toc529533433)

[14. xxApplications 30](#_Toc529533434)

[15. xxMobile Management Application 31](#_Toc529533435)

[16. xxPowerShell Scripts 32](#_Toc529533436)

[17. xxConditional Access 33](#_Toc529533437)

[18. xxWindows Information Protection 34](#_Toc529533438)

[19. xxRetire or Wipe Company Device 35](#_Toc529533439)

[20. xxRemote Tasks 36](#_Toc529533440)

[21. xxAlerts 37](#_Toc529533441)

[22. xxUpdate Readiness 38](#_Toc529533442)

[23. Intune roles 39](#_Toc529533443)

[23.1. Adding Custom Role 39](#_Toc529533444)

[23.2. Deleting Custom Role 39](#_Toc529533445)

[23.3. Assigning User rights to a role 39](#_Toc529533446)

[23.4. Removing User rights from a role 39](#_Toc529533447)

[24. xxReporting 41](#_Toc529533448)

[25. xxData Warehouse 42](#_Toc529533449)

[26. xxTroubleshooting 43](#_Toc529533450)

1. Document Change Control Sheet
   1. Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change/Reference |
| November/2018 | Raphael Perez & David Nudelman | Draft 0.01 | Initial Release |

1. About the Authors
   1. Raphael Perez (Author)

Raphael is a 9 times Microsoft MVP (<https://mvp.microsoft.com/en-us/PublicProfile/4027143>) with over 20 years of experience in IT, of which over 14 years have been dedicated to System Center and Automation.

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

Throughout his career, Raphael has participated as a 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/>).

* 1. 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](http://www.thedesktopteam.com)) and IT Pro Spain ([www.itpro.es](http://www.itpro.es)). He is one of the top 5% contributors to the Microsoft TechNet forums, earning multiple times the “Microsoft Community Contributor” award.

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

1. Introduction

The world is in constant change and device management is also changing all the time. Management of devices as we have done in the past may no longer be necessary. To add more complexity, you also need to manage mobile devices, however, users need some mobility and flexibility to perform their day-to-day tasks while you want to keep the data as secure as possible.

Microsoft Intune is the Microsoft solution for this new world. It has lots of capabilities to help both sides, you and your end-users to achieve your goals and this e-book has been created for you to understand all the steps necessary for this management.

The intended audience of this e-book are technical people that want to learn or improve their understanding of Mobile Device Management (MDM) with Intune. Minimum knowledge of the following software and technologies is assumed, including but not limited to Microsoft Azure, Office 365, Windows Server, Hyper-V, Mobile Device (iOS, Android), Mac OS X and Windows Client (i.e. Windows 10).

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

1. Lab Information

The Enterprise Mobility+Security lab environment was created using Hyper-V 2016 Virtual Machines connected to the internet, it also has the following hardware requirements:

* 1x Mac OS X 10.11
* 1x iPhone or iPad or iPod touch
* 1x Android Phone

The lab needs to have access to at least one iOS hardware (iPhone, iPad or iPod touch). It also has a total of three (3) virtual machines, 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 2016  IP Address: DHCP |
| WKS0001 | RAM: 2048MB  Drive 01 (C): 127GB  Processor/Core: 1  Network Adapter | Windows 10 MDM Client | Windows 10 Enterprise Edition version 1803  IP Address: DHCP |
| WKS0002 | RAM: 2048MB  Drive 01 (C): 127GB  Processor/Core: 1  Network Adapter | Windows 10 MDM Client | Windows 10 Enterprise Edition version 1803  IP Address: DHCP |

**Note:** During the lab, you will notice that an internet domain name is required. I have registered clouddemolab.com. I would recommend you registering a test domain, however, any internet domain that you own can be used.

* 1. 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. Create a folder called VM on the C drive |
| 12. Create a folder called ISOs on the C drive |
| 13. Download Windows 10 Enterprise Evaluation x64 from <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise> and save the file the C:\ISOs folder |

* 1. Installing Hyper-V role

To install the Hyper-V Role, perform the following steps on the Hyper-V Server:

|  |
| --- |
| 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 |

* 1. Configure Hyper-V

To configure the Hyper-V, perform the following steps on the Hyper-V Server:

|  |
| --- |
| 01. Open Hyper-V Manager |
| 02. In the Actions pane on the right side of the window, select Virtual Switch Manager |
| 03. Select New virtual switch -> External -> Create Virtual Switch |
| 04. In the Virtual Switch Manager dialog box, under Virtual Switch Properties, type External as the virtual switch name and Under Connection type, select a network adapter that is connected to an Ethernet network that has a DHCP server and Select Allow management operating system to share this network adapter, and then click OK |
| 05. Under Apply Network Changes, click Yes |
| 06. In the Actions pane on the right side of the Windows, Select Hyper-V Settings |
| 07. Select Enhanced Session Mode Policy and select Allow enhanced session mode if not already selected. Click Ok. |

* 1. CLASSROOM-WKS0001

|  |
| --- |
| 01. Open Hyper-V Manager and select the Server on the left pane under Hyper-V Manager |
| 02. In the Actions pane on the right side of the Windows, Select New Virtual Machine |
| 03. On Before You Begin, click Next |
| 04. On Name, Type CLASSROOM-WKS0001 on the name of your Hyper-V virtual machine and C:\VM as location and click Next |
| 05. On Specify Generation, select Generation 2 and click Next |
| 06. On Assign Memory, type 4096 and click Next |
| 07. On Configure Networking, select External and click Next |
| 08. On Connect Virtual Hard Disk, click Next |
| 09. On Installation Options, select Install an operating system from a bootable image file and browse to c:\ISOs and select the 16299.15.170928-1534.rs3\_release\_CLIENTENTERPRISEEVAL\_OEMRET\_x64FRE\_en-gb.iso. Click Ok and then click Next |
| 10. On Completing the new virtual machine Wizard, click Finish. |
| 11. Select the CLASSROOM-WKS0001 virtual machine, In the Actions pane on the right side of the Windows, Select Connect |
| 12. On the Virtual Machine Connection, select Action -> Start |
| 13. On Windows Setup, select the language, time and currency format and keyboard input and click Next |
| 14. On Windows Setup, Click Install now |
| 15. On License terms, Click I accept the license terms and click Next |
| 16. On Which type of installation do you want?, click Custom: Install Windows only (Advanced) |
| 17. On Where do you want to install Windows, click Next  Note: The installation will start and will take around 15-20 minutes |
| 18. On Let’s start with region. Is this correct? Click Yes |
| 19. On Is this the right keyboard layout? Click Yes |
| 20. On Do you want to add a second keyboard layout? Click Skip |
| 21. On Sign in with Microsoft, click Domain join instead |
| 22. On Who’s going to use this PC? Type User01 and click Next |
| 23. On Create a really memorable password, type Pa$$w0rd and click Next |
| 24. On Confirm your password, type Pa$$word again and click Next |
| 25. On Add a hint for your password, type password and click Next |
| 26. On Make Cortana your personal assistant? Click No |
| 27. On Choose privacy settings for your device, click Accept |
| 28. Once connected, click start and then settings |
| 29. On Windows Settings, click System and then About |
| 30. Click Rename this PC |
| 31. On Rename your PC type WKS0001 and click Next and then Restart now |
| 32. Once the computer has been restarted, log on to the computer as User01 and password Pa$$w0rd |

* 1. CLASSROOM-WKS0002

|  |
| --- |
| 01. Open Hyper-V Manager and select the Server on the left pane under Hyper-V Manager |
| 02. In the Actions pane on the right side of the Windows, Select New Virtual Machine |
| 03. On Before You Begin, click Next |
| 04. On Name, Type CLASSROOM-WKS0002 on the name of your Hyper-V virtual machine and C:\VM as location and click Next |
| 05. On Specify Generation, select Generation 2 and click Next |
| 06. On Assign Memory, type 4096 and click Next |
| 07. On Configure Networking, select External and click Next |
| 08. On Connect Virtual Hard Disk, click Next |
| 09. On Installation Options, select Install an operating system from a bootable image file and browse to c:\ISOs and select the 16299.15.170928-1534.rs3\_release\_CLIENTENTERPRISEEVAL\_OEMRET\_x64FRE\_en-gb.iso. Click Ok and then click Next |
| 10. On Completing the new virtual machine Wizard, click Finish. |
| 11. Select the CLASSROOM-WKS0002 virtual machine, In the Actions pane on the right side of the Windows, Select Connect |
| 12. On the Virtual Machine Connection, select Action -> Start |
| 13. On Windows Setup, select the language, time and currency format and keyboard input and click Next |
| 14. On Windows Setup, Click Install now |
| 15. On License terms, Click I accept the license terms and click Next |
| 16. On Which type of installation do you want?, click Custom: Install Windows only (Advanced) |
| 17. On Where do you want to install Windows, click Next  Note: The installation will start and will take around 15-20 minutes |
| 18. On Let’s start with region. Is this correct? Click Yes |
| 19. On Is this the right keyboard layout? Click Yes |
| 20. On Do you want to add a second keyboard layout? Click Skip |
| 21. On Sign in with Microsoft, click Domain join instead |
| 22. On Who’s going to use this PC? Type User02 and click Next |
| 23. On Create a really memorable password, type Pa$$w0rd and click Next |
| 24. On Confirm your password, type Pa$$word again and click Next |
| 25. On Add a hint for your password, type password and click Next |
| 26. On Make Cortana your personal assistant? Click No |
| 27. On Choose privacy settings for your device, click Accept |
| 28. Once connected, click start and then settings |
| 29. On Windows Settings, click System and then About |
| 30. Click Rename this PC |
| 31. On Rename your PC type WKS0002 and click Next and then Restart now |
| 32. Once the computer has been restarted, log on to the computer as User02 and password Pa$$w0rd |

1. Enterprise Mobility + Security Setup and Initial Configuration
   1. Microsoft Intune Trial License

The first step in the device management is to create a Microsoft Intune subscription. Microsoft allows you to have a trial fully functional version for 30 days that allows you to test every single functionality and when it expires, you can opt to buy licenses.

To create a new Microsoft Intune subscription, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <http://www.microsoft.com/intune> and click on the try now button |
| 02. Fill up the Sign-up form and confirm the creation of the Microsoft Intune Subscription |

* 1. Office 365 Enterprise E3 Trial License

The first step you have set up is an Office 365 subscription. This is required to perform the tests that require e-mail and Office applications as well as create the initial Azure Active Directory.

To create a new Office 365 subscription, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://products.office.com/en-gb/business/compare-more-office-365-for-business-plans> and click on the try for free button under the Office 365 Enterprise E3 license type |
| 02. Fill up the Sign-up form and confirm the creation of the Microsoft Intune Subscription |

* 1. Enterprise Mobility + Security E5 Trial License

Once you have set up for Office 365 subscription, you will need to create an Enterprise Mobility + Security E5 subscription. This is required to add Intune and authentication security to our environment, such as Multi-Factor Authentication.

To create a new Enterprise Mobility + Security E5 Trial subscription, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Active Directory |
| 03. Under Active Directory, click Quick Start |
| 04. On Quick Start, click Get a free trial for Azure AD Premium |
| 05. On Activate, under Enterprise Mobility + Security E5, click Free trial |
| 06. On Activate Enterprise Mobility + Security E5 trial, click Activate |

* 1. Set the Intune Mobile Device Authority

Before you can enrol mobile devices, you must prepare the Microsoft Intune service by selecting the appropriate mobile device management authority. The mobile device management authority setting determines whether you manage mobile devices with Intune or System Center Configuration Manager with Intune integration and cannot easily be changed. In case of change, you need to contact support and you may also need to re-enrol all devices already enrolled.

To set the Mobile Device Management Authority, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, select Device Enrollment |
| 04. Under Device Enrollment, Chose MDM Authority, select Intune MDM Authority and click Choose |

* 1. Setting up DNS for Enrollment

Before you can enrol Windows devices, you must prepare the DNS for Mobile Device Enrolment. The process is to create a DNS alias (CNAME) record for EnterpriseEnrollment that points to EnterpriseEnrollment-s.manage.microsoft.com and EnterpriseRegistration that points to EnterpriseRegistration.windows.net, allowing an automatic detection of the servers used by the Enrollment process.

To set the DNS, add a CNAME for record EnterpriseEnrollment and EnterpriseRegistration on your DNS Server on a computer connected to the internet:

|  |
| --- |
| 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: peproxyfeeu02.cloudapp.net  Address: 52.174.26.23  Aliases: enterpriseenrollment.clouddemolab.com  EnterpriseEnrollment-s.manage.microsoft.com  manage-pe.trafficmanager.net |
| 05. type enterpriseregistration.clouddemolab.com and press enter, it should have a reply similar to  Non-authoritative answer:  Name: prod-drs-neu.cloudapp.net  Address: 23.102.20.102  Aliases: enterpriseregistration.clouddemolab.com  EnterpriseRegistration.windows.net  enterpriseregistration.trafficmanager.net |

* 1. Adding Domains

Registering domain allow you to use your company public domain for the enrolment process and users will not need to remember another username.

To add a new domain, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Active Directory |
| 03. Under Active Directory, click Custom domain names |
| 04. Under Custom domain names, click Add custom domain |
| 05. Under Custom name, type the domain and click Add Domain |
| 06. Under Custom domain name, Record type, select TXT record (preferred method) and type note of the Text value to be added |
| 07. On your DNS environment, add or change the TXT record with the value required by the Azure verification process |
| 08. Once the DNS change has been completed, return to Microsoft Azure and click verify to finish the process |
| 09. Navigate to <https://portal.office.com/AdminPortal/> |
| 10. Expand Setup and click Domains |
| 11. Click the domain you have just added and click DNS management. |
| 12. Under choose your online services, select Exchange and Skype for business and click Next |
| 13. Under Update DNS Settings, take notes of the DNS changes necessary to make the Office 365 features functional. |
| 14. On Update DNS settings make note of the necessary changes, return to the Office Admin center and click Verify |
| 15. If everything has been validated successfully, click Finish |

1. User Management
   1. Adding Users

Once the domain has been created and verified, it is time to add users to the Azure Active Directory. Adding users is a necessary step because the Microsoft Cloud Services licensing model is based on users. A single Enterprise Mobility + Security E5 license allows the user to enrol up to 5 devices.

**Note:** Adding users to the Microsoft Intune directory can be achieved manually, as per our example, or via synchronize with an existing on-premises Active Directory Environment via Azure AD Connect (<https://azure.microsoft.com/en-gb/documentation/articles/active-directory-aadconnect/>)

**Note:** The steps are going to be taken from the Office Admin Center portal, however, you can use the Azure Active Directory portal. The reason we are using the Office Admin Center portal is easy to assign licenses and will automatically enable the user to the Office 365 features.

* + 1. Single User

To add a single user, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.office.com/> and click Admin |
| 02. On Admin Center, expand Users and click Active Users |
| 03. On Active Users, click Add User |
| 04. On New User, fill up the details form and select the public domain under username. Make sure you select Intune and Office 365 Enterprise E3 under Product Licenses and click Add |
| 05. Under User was added, take a note of the user’s password. If you want, leave the send password in email and click send email and close, otherwise unselect send password in email and click Close |
| 06. Returning to the Users list, confirm that the new user has been created |

* + 1. Multiple User

To add multiple users, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. Create a text file with extension .csv where the 1st line contain header and the following lines contain the user information  Note: A sample file can be downloaded from <https://portal.office.com/UserManagement/Samples/Import_User_Sample_en.csv> |
| 02. On a browser and navigate to <https://portal.office.com/> and click Admin |
| 03. On Admin Center, expand Users and click Active Users |
| 04. On Active Users, click More -> Import multiple users |
| 05. On Import multiple users, click browse |
| 06. Select the created file, click Open and then verify |
| 07. Once the verification is done, click Next |
| 08. Under Set user options, select Sign-in allowed, confirm the Enterprise Mobility + Security E5 and Office 365 Enterprise are selected under product licenses and click Add |
| 09. On View your results, unselect Email the results files to these people and click Close without sending e-mail |
| 10. Returning to the Users list, confirm that the new user has been created |

* 1. Reseting User Password

Resetting a user’s password is probably the most common task in IT and it can manually be reset.

To reset a user’s password, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.office.com/> and click Admin |
| 02. On Admin Center, expand Users and click Active Users |
| 03. On Active Users, select the user(s) you want to reset the password and click Reset Password |
| 04. On Reset Password, click Reset |
| 05. On Reset Password, uncheck the send email if you don’t want to receive an email and click Close twice |

* 1. Deleting Users

When user leaves the company, you may want to delete its information and reassign its license.

To delete a user, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.office.com/> and click Admin |
| 02. On Admin Center, expand Users and click Active Users |
| 03. On Active Users, select the user(s) you want to delete and click Delete user |
| 04. On Delete user, click Delete |
| 05. On Delete user, click Close |

* 1. Recovering Deleted Users

When you delete a user from Microsoft Intune, the user’s account is deleted and kept in the "recycle bin" for 30 days where it can be recoverable. After 30-days, the account gets deleted permanently.

To recover a deleted user, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.office.com/> and click Admin |
| 02. On Admin Center, expand Users and click Deleted Users |
| 03. On Deleted Users, select the users you want to recover and click Restore |
| 04. On Restore, click Restore |
| 05. On users successfully restored, click Close |

1. Group Management

Groups are logical collections of objects, such as Windows-based computers, Mobile Devices or Users that can be used to apply policies, view reports, etc. You create a group by using the Create Group Wizard. You can explicitly assign membership to a group or you can create rules that will generate a dynamic group membership.

There are 3 types of groups:

* Assigned: members will be assigned manually
* Dynamic User: A query will be created, and the user will be automatically added or removed depending on the result of the query
* Dynamic Device: A query will be created, and the device will be automatically added or removed depending on the result of the query

For more information about creating Azure Groups, refer to <https://docs.microsoft.com/en-gb/azure/active-directory/active-directory-groups-dynamic-membership-azure-portal>

* 1. Creating Group

To create a Group, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click All groups |
| 04. Under User and groups – All groups, click New group |
| 05. Under Group:   * Group Type: Security * Name: All Enabled Users * Membership Type: Dynamic Users * Dynamic user members query: accountEnabled Equals true   Click Create and then click on the X |
| 06. Once back to the Users and Groups – All Groups, click on All Enabled Users group to open its properties |
| 07. Click Members  Note: Allow time for the group to populate. Depending on the size of your tenant, the group may take up to 24 hours for populating for the first time or after a rule change. In our environment it will take about 5 minutes |

* 1. Editting Group Name

To edit an existing Group, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click All groups |
| 04. Under User and groups – All groups, click the Group you want to Edit |
| 05. Click Properties and Change the group Name. Once done, click Save |

* 1. Converting Dynamic to Assigned Group

To convert an existing dynamic group to Assigned, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click All groups |
| 04. Under User and groups – All groups, click the Group you want to Edit |
| 05. Click Properties and Change the Membership type to Assigned and click Yes on the Warning message and then click Save  Note: When you change the group type to assigned, existing members will remain members of the group and the dynamic rule will be deleted |

* 1. Converting Assigned to Dynamic Group

To convert an existing assigned group to Dynamic, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click All groups |
| 04. Under User and groups – All groups, click the Group you want to Edit |
| 05. Click Properties and Change the Membership type to Dynamic User and click Yes on the Warning message and add a Dynamic user members query for accountEnabled Equals true.  Click Save  Note: When you change the group type to Dynamic, existing members may change depending on the membership rule you provided |

* 1. Adding new members to an Assigned group

To add new members to an assigned group, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click All groups |
| 04. Under User and groups – All groups, click the Group you want to Edit |
| 05. Click Members |
| 06. To add new member, click Add members button while to remove an existing member, click the 3 dots at the end of the member name and click remove |

* 1. Group Membership

To visualize a Group Membership, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click All groups |
| 04. Under User and groups – All groups, click the Group you want to view the Membership |
| 05. Under overview, you have a view of how many members the group have. |
| 06. Click Members to see the list of members of the group |

1. Device enrolment

Intune lets the IT admin manage company’s workforce’s devices and apps and how users access company data. To use this mobile device management (MDM), the devices must first be enrolled in the Intune service. When a device is enrolled, it is issued an MDM certificate. This certificate is used to communicate with the Intune service.

* 1. Enrollment Restrictions
     1. Default Enrollment Restrictions

By default, everyone can enrol a maximum of 5 devices of any supported platform. If you want to control the maximum number of devices a user can enrol or limit what platform users can enrol, you need to manage the default Enrollment restrictions.

To configure the Enrollment restrictions, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Enrollment restrictions |
| 04. On Device Enrollment – Enrollment restrictions, click Default under Device Type Restrictions |
| 05. On All Users, click Platform and block any platform you will allow all users to enrol and then click Save |
| 06. Click Platform Configurations and then define the versions allowed (using major.minor.build) and whenever applicable, configure if you will allow personally owned devices to be enrolled. Once you have made the changes, click Save  Note: Intune classifies devices as personally-owned by default. Refer to section Corporate device identifiers |
| 07. On Device Enrollment – Enrollment restrictions, click Default under Device Limit Restrictions |
| 08. On All users, click Device Limit and change the maximum number of devices a user can enrol and click Save  Note: This restriction does not apply to Device enrolment managers |

* + 1. Adding Enrollment Restrictions

Sometimes it is required to have different restrictions per group of users. An example would be when the company only support Android devices, but for Directors, it allows the use of iPhone/iPad devices.

To configure add a new Enrollment restrictions, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Enrollment restrictions |
| 04. On Device Enrollment – Enrollment restrictions, click Create restrictions |
| 05. On Create restriction, type a Name and select the Restriction Type. Once you selected the restriction type you will be able to configure it. |
| 06. Click Create when it is done. |

* + 1. Deleting Enrollment Restrictions

When an Enrollment restriction is no longer required, you may want to delete it.

To delete an Enrollment restriction, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Enrollment restrictions |
| 04. On Device Enrollment – Enrollment restrictions, select the restrictions you want to delete |
| 05. On the restriction overview, click Delete and then Yes |

* + 1. Assign Enrollment Restrictions

When an Enrollment restriction is created, you need to assign it to a group of users so the users can be restricted it instead of the default.

To assign an Enrollment restriction, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Enrollment restrictions |
| 04. On Device Enrollment – Enrollment restrictions, click Assignments |
| 05. On assignment, click + Select groups and select the groups you want. Once done, click Save |

* 1. Corporate device identifiers

Intune classifies devices as personally-owned by default. As an Intune admin, you can identify devices as corporate-owned to refine management and identification. Intune can perform additional management tasks and collect additional information such as the full phone number and an inventory of apps from corporate-owned devices. You can also set device restrictions to block enrolment by devices that aren't corporate-owned.

* + 1. Adding corporate device identifier

To add a corporate identifier, you first need to create a two-column, comma-separated csv file. The first column will be the identifier information (IMEI or serial number) and the second column will contain details about the device. The details column is limited by 128 characters and are for administrative use only.

To add new corporate device identifiers, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. Open notepad |
| 02. Create a new file with the content required and save as .csv file  Note: The list must contain the IMEI or Serial Number. You cannot use Serial Number and IMEI on the same file. In this case, multiple files are required to be created. The file also cannot have more than 5,000 lines.  Note: Some Android devices have multiple IMEI numbers. Intune only reads one IMEI number per enrolled device. If you import an IMEI number but it is not the IMEI inventoried by Intune, the device is classified as a personal device instead of a company-owned device. If you import multiple IMEI numbers for a device, uninventoried numbers display Unknown for enrollment status.  Note: Android Serial numbers are not guaranteed to be unique or present. Check with your device supplier to understand if serial number is a reliable device ID. Serial numbers reported by the device to Intune might not match the displayed ID in the Android Settings/About menus on the device. Verify the type of serial number reported by the device manufacturer. |
| 03. On a browser and navigate to <https://portal.azure.com> |
| 04. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Corporate device identifiers |
| 04. On Device Enrollment – Corporate device identifiers, click Add |
| 05. On Add Identifiers, select the identifier type and browse to the file created in the step 02 and then click Add |

* + 1. Deleting corporate device identifier

Deleting a corporate identifier is sometimes needed. This can be when the device is no longer part of the company because it was recycled or for some other reason.

To delete existing corporate device identifiers, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Corporate device identifiers |
| 04. On Device Enrollment – Corporate device identifiers, select the Identifier that you want to delete and click Delete. On the warning message, click Ok. |

* 1. Terms and Conditions

You can deploy Intune terms and conditions to user groups to explain how enrollment, access to work resources, and using the Company Portal app affect devices and users. Users must accept the terms and conditions before they can use the Company Portal to enroll and access their work.

* + 1. Create a terms and conditions policy

To create a Terms and Conditions Policy, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Terms and conditions |
| 04. On Device Enrollment – Terms and conditions, click Create |
| 05. Create Terms and Conditions, fill up the Display Name, Description, and click Define terms of use |
| 06. On Terms and Conditions, add a Title, Summary of Terms and Terms and conditions and click OK followed by a Create |

* + 1. Edit a terms and conditions policy

To edit a Terms and Conditions Policy, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Terms and conditions |
| 04. On Device Enrollment – Terms and conditions, click the Terms and Conditions you want to edit |
| 05. On the overview, click properties and then Terms and Conditions |
| 06. On Properties – Terms and Conditions, update the Title, Summary of Terms and/or Terms and conditions and decide whether to require users to re-accept updated terms and conditions, select Require users to re-accept, and increment the version number to x. Click ok and then save  Note: As best practices, it is always recommended to select the option to Increase the version number, and require all users to accept the updated terms the next time they open the company Portal |

* + 1. Deleting a terms and conditions policy

To delete a Terms and Conditions Policy, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Terms and conditions |
| 04. On Device Enrollment – Terms and conditions, click the Terms and Conditions you want to delete |
| 05. On the terms and conditions overview, click Delete and then Yes |

* + 1. Assign Terms and conditions policy

To manage the Terms and Conditions Policy deployment, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Terms and conditions |
| 04. On Device Enrollment – Terms and conditions, click the Terms and Conditions you want to assign |
| 04. On Device Enrollment – Terms and conditions, click Assignments |
| 05. On assignment, click select groups to include and select the groups you want. Once done, click Save |

* 1. Company Portal

The Company Portal app helps you search, browse and install apps made available to you by your company, through the Microsoft Intune online service. Apps can be installed without requiring a connection to your corporate network. You can also enroll your personal computers and devices in the service and locate contact information for your IT team.

To configure the Company Portal, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Mobile Apps and then Company Portal branding |
| 04. Under Mobile apps – Company Portal branding you can customize how your users will see the Company Portal, like colours, logo, etc. Once you have customized it, click Save |

* 1. Apple enrollment

Before enrolling and managing an iOS device, it is necessary to request and upload an Apple APNs certificate. The Apple APNs certificate is used by the iOS to allow a device management software. This certificate is valid for one year and must be renewed before it expiration, otherwise it will be necessary to re-enroll all already enrolled devices.

To request and upload an Apple APN certificate, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Device Enrollment and then Apple Enrollment |
| 04. Under Device enrolment – Apple enrolment, click Apple MDM Push certificate |
| 05. On Configure MDM Push Certificate, click I agree under I grant Microsoft permission to send both user and device information to Apple. |
| 06. Click Download your CSR and save the IntuneCSR.csr file to your computer  Note: It is recommended not using Microsoft Edge as it may not work as expected |
| 07. On a browser, navigate to <http://go.microsoft.com/fwlink/?LinkId=261984> and log on with an Apple ID.  Note: It is recommended not using Internet Explorer as it may not work as expected |
| 06. On Apple Push Certificate Portal, click Create a Certificate |
| 07. On Terms of Use, click I have read and agree to these terms and conditions and click Accept |
| 08. On Create a New Push Certificate, click choose file, select the IntuneCSR.csr file that you saved before and click upload |
| 09. On Confirmation, click Download and save the MDM\_ Microsoft Corporation\_Certificate.pem file |
| 10. Back to the Microsoft Intune portal, type your apple ID used to create the certificate and import the MDM\_ Microsoft Corporation\_Certificate.pem and Click Upload |
| 11. On Upload an APNs Certificate, click Upload the APNs Certificate |

* 1. xxWindows enrollment
     1. Windows Hello for Business
     2. CNAME Validation
     3. Windows Autopilot

1. xxDevice compliance
2. xxPolicy
3. xxEnrolling a Device

1. xxManaging Windows PC
2. xxSoftware Policy
3. xxApplications

1. xxMobile Management Application
2. xxPowerShell Scripts
3. xxConditional Access
4. xxWindows Information Protection
5. xxRetire or Wipe Company Device
6. xxRemote Tasks
7. xxAlerts
8. xxUpdate Readiness
9. Intune roles

RBAC helps you control who can perform various Intune tasks within your organization, and who those tasks apply to. You can either use the built-in roles that cover some common Intune scenarios, or you can create your own roles.

* 1. Adding Custom Role

To create a Custom role, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Intune roles and then All roles |
| 04. On Intune roles – All roles, click Add Custom |
| 05. On the Add Custom role, type a name for the role and add the required permissions. Once done, click Create |

* 1. Deleting Custom Role

To delete a Custom role, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Intune roles and then All roles |
| 04. On Intune roles – All roles, click on the 3 dots (…) next to the role you want to delete and click Delete. On the warning message, click Ok |

* 1. Assigning User rights to a role

To Assign a User right to a role, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Intune roles and then All roles |
| 04. Select the Role you want to add a user right and then click Assignments |
| 05. Under Assignments, click Assign |
| 06. Under Role assignments, type an Assignment Name and select the groups of administrators under Members (Groups) and what users/devices they can manage under Scope (Groups). Once done, click OK |

* 1. Removing User rights from a role

To remove a User right from a role, perform the following steps on a computer connected to the internet:

|  |
| --- |
| 01. On a browser and navigate to <https://portal.azure.com> |
| 02. Click All Services and select Intune |
| 03. Under Microsoft Intune, click Intune roles and then All roles |
| 04. Select the Role you want to remove a user right and then click Assignments |
| 05. Under Assignments, select the assignment you want to remove |
| 06. On Assignments – Properties, click Delete assignment and then click Ok. |

1. xxReporting
2. xxData Warehouse
3. xxTroubleshooting