#CANITPRO CAMP

Windows 10 and Enterprise Mobility

Trial Account Registration

This document will take you through the process of signing up for the trial accounts and subscriptions necessary for completing the Windows 10 EMS Labs.

Overview

You will complete the following objectives.

- Sign up for a Microsoft Account
- Redeem an Azure Pass and sign up for an Azure Trial
- Setup an Office 365 E3 Trial
- Setup a Microsoft Intune Trial
- Add your Tenant Directory to your Azure Subscription

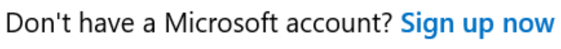
Table 1 outlines the requirements for completing this module.

Table 1. Module requirements

Virtual machines	Physical devices	Subscriptions and accounts
• W10-Client • W10-Edge • W10-IiS	No physical devices are required in this module.	• No subscriptions are required for this lab

Exercise 1: Setup Trials and Accounts

Microsoft Account

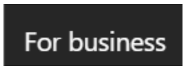
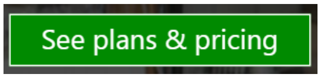
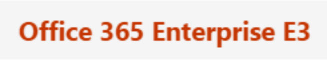
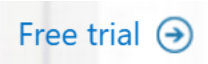
Description	Action
Create a Microsoft Account	1. On the virtual machine W10-W10Client, login using the following credentials. Username: W10User Password: Passw0rd! 2. Launch Internet Explorer by clicking the Start button and typing Internet 3. Launch Edge by clicking the Edge browser icon on the Taskbar It may be necessary to use both Browsers and Private Browser sessions. To Start a Private Session use (CTL+SHIFT+P) 4. Navigate to http://www.outlook.com 5. Click on Sign Up Now  Don't have a Microsoft account? Sign up now 6. Create a new account with a unique ID, for example W10EMCLabs_(your initials)@outlook.com 7. For Password type Passw0rd!012 8. Make a note of your email address and password 9. Fill in the remainder of the required information and then click Create Account 10. On the Welcome to your Inbox, click Continue to Inbox

Description	Action
	11. Keep your browser open and stay logged into your Microsoft Account

Redeem your Azure Pass

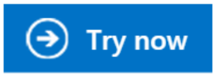
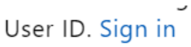
Description	Action
Redeem your Azure Pass. You should have been given an Azure Pass as part of your class attendance pack. The promotional code on the pass should be alpha-numeric.	Open another Tab in your browser and browse to https:// www.windowsazurepass.com 12. Select your country 13. Paste in your promotional code and then click Submit 14. Click Sign In 15. The information for your Outlook Account should pre populate, if it does not then type in the account information from the previous task 16. Click Submit 17. Click Activate 18. Agree to the Terms and Conditions, enter a Phone Number, and click Sign Up 19. Wait for about 1 minute and then click the Click here to Refresh link 20. After the account is provisioned the Microsoft Azure login page will load 21. Enter your password and click Sign In

Sign up for an Office 365 E3 Trial

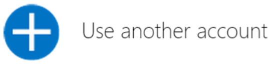
Description	Action
Provision an Office 365 E3 Trial Account. This should be performed on a different machine to the one used for the Microsoft Account and Azure Pass	Using your other Browser or a Private Session, browse to http://office.microsoft.com 22. Click on For business  23. Click on See plans & pricing  24. Click on Office 365 Enterprise E3 from the top navigation pane  25. Click on Free Trial  26. Fill in the required information, set your company to Contoso 27. For the Global Admin account, type Admin 28. For domain name type ContosoXXXXX (replace the X's with letters and/or numbers to make the domain unique) 29. For password type Passw0rd! 30. Make a note of the Global Admin account and password 31. Click Next 32. Type in your mobile phone number and click Text Me 33. Type in the code that is sent to you and click Create my account 34. Make a note of the Office 365 User ID and Sign In page

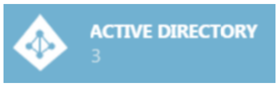
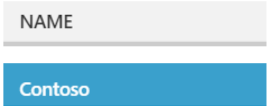
Description	Action
	35. Click You’re ready to go 36. This should log you into the Office 365 Admin Portal 37. Keep your browser open

Setup a Microsoft Intune Trial

Description	Action
Sign Up for a Microsoft Intune Trial	Open another Tab in the browser you have open for the previous task Navigate to http://www.windowsintune.com Click Try now  Click Sign In (This is located at the end of the paragraph directly under Sign Up) User ID. Sign in Your 30 day Intune Trial is automatically provisioned and associated with your Office 365 Tenant Click try now Click continue This will log you into the Intune Account Console You may receive alerts warning of merging accounts and account expiration. Ignore these. Your https://account.manage.microsoft.com login for Intune will use the same credentials as your Office 365 Account

Add your Tenant Directory to your Azure Subscription

Description	Action
Add your tenant directory to your Azure Subscription	Open a third Tab in the browser you have used in the previous two tasks Navigate to https://manage.windowsazure.com The Azure portal will attempt to log you in using the Office 365/Intune credentials so you should receive a "No Subscriptions Found" message Click Sign Out Click Sign In Click Use Another Account  Enter the email address you associated with your Azure Pass, this is the Microsoft Account created in the first task Enter the Azure account password Once Azure loads, Click New Click App Services > Active Directory > Directory > Custom Create From the Directory dropdown menu, Select Use existing directory, check the box I am ready to be signed out now, then click Finish Sign into your Azure Portal using your Office 365 Credentials Click continue Click Sign out now Sign back in with your Azure Credentials

Description	Action
	Click on Active Directory in the Azure Navigation (you may need to scroll down on the left hand side)  You should see the Contoso Directory listed with your Default Directory.  NAME Contoso

Windows 10 and Enterprise Mobility

Deploying Windows 10 using Microsoft Deployment Toolkit

The exercises in this lab guide show how to deploy Windows 10 by using Microsoft Deployment Toolkit (MDT) 2013 Update 1. In the first exercise, you will see how to deploy Windows 10 to new computer. In the second exercise, you will see how to deploy Windows 10 to a device running Windows 7, while retaining the user's settings and data.

Table of Contents

Overview

The exercises in this lab focus on deploying Windows 10 by using MDT to a new computer and refreshing the operating system on an existing device running Windows 7 to Windows 10 by using Lite Touch Installation (LTI). The big takeaway from the exercises in this lab is that you can deploy Windows 10 by using highly automated processes that help minimize the use of IT resources, reduce configuration errors, reduce complexity, and reduce the overall effort required to deploy Windows 10 and apps.

The exercises in this lab include:

- Exercise 1: Deploying Windows 10 to a new device
- Exercise 2: Deploying Windows 10 to an existing device running Windows 7

NOTE: This lab may take longer than 2 hours due to OS deployments in each exercise.

Table 1 lists virtual machines used in this lab.

Table 1. Virtual machines used in this lab

Virtual machine	Description
W10-DC	Domain controller running Windows Server 2012 R2 for the corp.contoso.com Active Directory (AD) domain. Also provides Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services for the virtual machine environment.
W10-CM	Member server in the corp.contoso.com domain running System Center 2012 R2 Configuration Manager Technical Preview and MDT 2013 Update 1.
W10-WIN7	Domain-joined running Windows 7 and Microsoft Office Professional Plus 2013.
W10-BM01	New device with no operating system installed (bare metal).

Exercise 1: Deploying Windows 10 to a new computer

This exercise illustrates how to deploy Windows 10 to a new computer (or "bare metal" deployment) by MDT. In this exercise, you manage MDT deployment shares and the content stored in a deployment share. After you populate the MDT deployment share, you deploy Windows 10 to a new ("bare metal") computer.

In this first exercise, you use the LTI MDT deployment method. You can configure LTI to require a minimal amount of user interaction ("lite touch") or no user interaction ("zero touch") at the time you deploy Windows 10. LTI allows you to control the level of interaction required based on the business and technical requirements of an organization.

LTI has minimal infrastructure requirements, which means that organizations of any size can use it. LTI requires only basic network connectivity and file-sharing capability to perform deployments.

You can perform LTI deployments over the network or by using media that is locally attached to the target computer, such as DVDs or USB drives. This deployment flexibility allows you to manage deployments regardless of the target computer connectivity.

LTI has two primary UIs: the Deployment Workbench and the Deployment Wizard. You use the Deployment Workbench to manage LTI deployment content and deployment configuration settings. You can run the Deployment Wizard optionally at the time of deployment to collect any deployment information that is specific to the target computer.

Overview of the Deployment Workbench

You use the Deployment Workbench to manage MDT deployment shares and the MDT database (MDT DB). A deployment share is a network shared folder that acts as a repository for deployment content, MDT configuration files, and the MDT support files (such as scripts and other software).

The Deployment Workbench uses wizards to create the deployment content in the deployment shares. For each type of content, a wizard is available for importing or creating the content.

The Deployment Workbench performs management tasks by calling the appropriate MDT Windows PowerShell cmdlets. This means you can write Windows PowerShell scripts to help automate the management tasks that you perform in the Deployment Workbench.

CM as CORP\Administrator

Description	**Steps**
Start the Deployment Workbench	1. Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: On the taskbar, click **Deployment Workbench**.

Managing deployment shares

As mentioned, a deployment share is a network shared folder that acts as a repository for deployment content, MDT configuration files, and the MDT support files.

You can create any number of deployment shares. You typically create a new deployment share for each set of desired configuration settings, which are stored in the CustomSettings.ini file, or for different Windows Preinstallation Environment (Windows PE) configurations. Each deployment share has a unique CustomSettings.ini file and unique Windows PE configuration settings.

A deployment share contains built-in subfolders that correspond to the types of deployment content that you can manage. A node in the Deployment Workbench corresponds to each type of content you will manage.

CM as CORP\Administrator

<table>
<tr><th>Description</th><th>Steps</th></tr>
<tr><td>Open the deployment share.</td><td>Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**:
1. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)**.
2. In the console tree, expand MDT Deployment Share (C:\DeploymentShare).</td></tr>
<tr><td colspan="2">Each top-level node has a corresponding folder in the deployment share. For example, there is an Operating Systems node in the Deployment Workbench (and corresponding folder in the deployment share) for managing operating systems and an Applications node in the Deployment Workbench (and corresponding folder in the deployment share) for managing applications.
To better organize deployment content, you can create subfolders beneath the top-level nodes in a deployment share in the Deployment Workbench.</td></tr>
<tr><td>Create a folder in the Operating Systems node in the Deployment Workbench by using the New Folder Wizard.</td><td>3. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Operating Systems**.
4. In the Actions pane, click **New Folder**.
The New Folder Wizard starts.</td></tr>
<tr><td colspan="2">On the **General Settings** page, you specify the name of the folder you want to create. For this example, let's assume you want to create a folder that will contain the 64-bit version of all your operating systems. You enter the appropriate name, and then continue to the next wizard page.</td></tr>
<tr><td>Name the folder **64-Bit Operating Systems**.</td><td>5. On the **General Settings** page, in **Folder name**, type **64-Bit Operating Systems**, and then click **Next**.</td></tr>
<tr><td colspan="2">On the **Summary** page, you can review the configuration settings that were selected while running the wizard. In this case, you see the name of the new folder.</td></tr>
</table>

Description	Steps
No configuration settings need to be changed on this page.	6. On the **Summary** page, click **Next**.
On the **Confirmation** wizard page, you can see the status of the folder-creation process. After you have reviewed the status, you can complete the wizard.	
On the **Confirmation** page, complete the wizard.	7. On the **Confirmation** page, click **Finish**.

Managing operating systems

Next, see how to manage operating systems for LTI deployments. You import and store operating systems in the Operating Systems node and corresponding folder in the deployment share by using the Import Operating System Wizard. You can also use the **Import-MDTOperatingSystem** Windows PowerShell cmdlet to import operating systems.

CM as CORP\Administrator

Description	Steps
You can import different types of operating systems by using the Import Operating System Wizard, such as operating systems from source files (distribution media), captured images of reference computers, or images from Windows Deployment Services (WDS).	
Start the Import Operating System Wizard.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: 8. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Operating Systems**. 9. In the Actions pane, click **Import Operating System**. The Import Operating System Wizard starts.
On the **OS Type** wizard page, you can import different types of operating systems, operating systems from source files (distribution media), captured images of reference	

Description	Steps
computers, or images from WDS. For this exercise, you import Windows 10 from source files, select **Full set of source files**.	
Select **Full set of source files**.	10. On the **OS Type** page, click **Full set of source files**, and then click **Next**.
On the **Source** page, specify the folder to which you copied the entire contents of a Windows 10 DVD.	
In **Source directory**, type **D:\Source$\Windows 10**.	11. On the **Source** page, in **Source directory**, type **D:\Source$\Windows 10**, and then click **Next**.
On the **Destination** page, specify the name of the directory that you should create in the deployment share to contain the files. The wizard defaults to the name of the operating system detected in the source folder. In this case, Windows 10 has already been imported, so change the name to a unique folder name.	
In **Destination directory name**, type **Windows 10 x64 Contoso**.	12. On the **Destination** page, in **Destination directory name**, type **Windows 10 x64 Contoso**, and then click **Next**.
On the **Summary** page, you can review the configuration settings that you selected while running the wizard. In this case, you see the details of the Windows 10 operating system.	
Cancel the wizard because you already imported the Windows 10 operating system. View the properties of the **Windows 10 Enterprise Technical Preview in Windows 10 Enterprise Evaluation x64 install.wim** operating system.	13. On the **Summary** page, click **Cancel**. The **Cancel Wizard** dialog box appears. 14. In the **Cancel Wizard** dialog box, click **Yes**. 15. In the details pane, right-click **Windows 10 Enterprise Technical Preview in Windows 10 Enterprise Evaluation x64 install.wim**, and then click **Properties**.
There is very little to configure in the properties of the operating system. All the information on this property sheet is automatically read from the operating system itself and provided through the Import Operating System Wizard. For example, you can see in	

Description	Steps
the Path and Image file settings where the wizard placed the operating system in the deployment share. In addition to importing and looking at the properties of an operating system, you can perform typical management functions such as copying, pasting, deleting, or renaming. As you saw earlier, you can create a folder structure to help organize operating system images.	
Close the **Windows 10 Enterprise Technical Preview in Windows 10 Enterprise Evaluation x64 install.wim Properties** dialog box by clicking **Cancel**.	16. In the **Windows 10 Enterprise Technical Preview in Windows 10 Enterprise Evaluation x64 install.wim Properties** dialog box, click **Cancel**.

Managing device drivers

Now that you have added an operating system, you need to add device drivers for LTI deployments. You can manage device drivers in the Out-of-Box Drivers node in the Deployment Workbench. You can import a number of devices drivers and organize them by creating the appropriate folder structure in the Deployment Workbench. After you import device drivers, they are stored beneath the Out-of-Box Drivers folder in the deployment share. You import device drivers by using the Import Device Drivers Wizard or the **Import-MDTDriver** Windows PowerShell cmdlet to import device drivers.

CM as CORP\Administrator

Description	Steps
You can import one or more device drivers by specifying the folder in which the device drivers reside. The wizard scans all subfolders beneath this folder for device drivers, so you can create a hierarchy of device drivers, and then the wizard imports all device drivers in the folder hierarchy.	
Start the Import Driver Wizard.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**:

Description	Steps
	17. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Out-of-Box Drivers**. 18. In the Actions pane, click **Import Drivers**. The Import Driver Wizard starts.
On the **Specify Directory** page, you can import one or more device drivers by specifying the folder in which the device drivers reside. The wizard scans all subfolders beneath this folder for device drivers, so you can create a hierarchy of device drivers, and then the wizard imports all device drivers in the folder hierarchy.	
On the **Specify Directory** page, enter the path to the device drivers (D:\Source$\DeviceDrivers).	19. On the **Specify Directory** page, in **Driver source directory**, type **D:\Source$\DeviceDrivers**, and then click **Next**.
On the **Summary** page, you can review the selected configuration settings. In this case, you see the folder that is the root of the folder structure where the device drivers are located.	
Review the configuration settings.	20. On the **Summary** page, click **Next**.
On the **Progress** page, you can monitor and view the device drivers as they are being imported.	
Review the device driver import progress.	21. On the **Progress** page, review the progress.
On the **Confirmation** page, when the import process is complete, you can see the status of the device driver import process.	
Close the Import Device Driver Wizard by clicking **Finish**.	22. On the **Confirmation** page, click **Finish**. 23. In the details pane, right-click **Intel Net w70n501.inf 1.2.5.37**, and then click **Properties**.

Description	Steps
View the properties of the **Intel Net w70n501.inf 1.2.5.37** device driver.	The **Intel Net w70n501.inf 1.2.5.37 Properties** dialog box for the imported device driver opens.
On the **General** tab of the device driver properties, you can type comments about the device driver, select the device driver processor architecture, and enable (or disable) the device driver.	
Review the information on the **General** tab, and then click the **Details** tab.	24. Click the **Details** tab.
On the **Details** tab, you can see all the detailed information about the device driver. All this information was read from the device driver itself or provided when completing the Import Driver Wizard. For example, you can see in the **INF path** setting, in which the wizard placed the device driver in the deployment share.	
Review the information on the **Details** tab, and then click **Cancel**.	25. In the **Intel Net w70n501.inf 1.2.5.37 Properties** dialog box, click **Cancel**.

Managing operating system packages

Next, you manage operating system packages. Operating system packages are most commonly language packs. These language packs are installed with Windows 10 and allow users to select languages that are different from the default language of the operating system. You can manage operating system packages in the Packages node in the Deployment Workbench and they are stored beneath the corresponding Packages folder in the deployment share. You can use the Import OS Packages Wizard or the **Import-MDTPackage** Windows PowerShell cmdlet to import operating system packages.

CM as CORP\Administrator

Description	Steps
You can import one or more operating system packages by specifying the folder in which the operating system packages reside. The wizard scans all subfolders beneath this folder for operating system packages, so you can create a hierarchy of operating system packages, and then the wizard imports all operating system packages in the folder hierarchy.	
Start the Import OS Packages Wizard.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: 26. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Packages**. 27. In the Actions pane, click **Import OS Packages**. The Import OS Packages Wizard starts.
On the **Specify Directory** page, you can import one or more operating system packages by specifying the folder in which the operating system packages reside. The wizard scans all subfolders beneath this folder for operating system packages, so you can create a hierarchy of operating system packages, and then the wizard imports all device drivers in the folder hierarchy.	
On the **Specify Directory** page, enter the path to the device drivers (D:\Source$\Windows 10 Language Packs).	28. On the **Specify Directory** page, in **Package source directory**, type **D:\Source$\Windows 10 Language Packs**, and then click **Next**.
On the **Summary** page, you can review the selected configuration settings. In this case, you see the folder that is the root of the folder structure where the operating system packages are located.	
Review the configuration settings.	29. On the **Summary** page, click **Next**.
On the **Progress** page, you can view and monitor the operating system packages as they are being imported.	

<table>
<tr><th>Description</th><th>Steps</th></tr>
<tr><td>Review the operating system package import progress.</td><td>30. On the <b>Progress</b> page, review the progress.</td></tr>
<tr><td colspan="2">On the <b>Confirmation</b> page, when the import process is complete, you can see the status of the operating system package import process.</td></tr>
<tr><td>Close the Import OS Packages Wizard by clicking <b>Finish</b>.
View the properties of the <b>Microsoft-Windows-Client-LanguagePack-Package fr-FR amd64 10.0.10061.0 Language Pack</b> operating system package.</td><td>31. On the <b>Confirmation</b> page, click <b>Finish</b>.
32. In the details pane, right-click <b>Microsoft-Windows-Client-LanguagePack-Package fr-FR amd64 10.0.10061.0 Language Pack</b>, and then click <b>Properties</b>.
The <b>Microsoft-Windows-Client-LanguagePack-Package fr-FR amd64 10.0.10061.0 Language Pack</b> dialog box for the imported operating system package opens.</td></tr>
<tr><td colspan="2">There is very little that you can configure on the properties of the operating system package. On the <b>General</b> tab, you can type comments about the language pack, enter a user-friendly display name, hide the package in the Deployment Wizard, and enable (or disable) the operating system package.</td></tr>
<tr><td>Close the <b>Microsoft-Windows-Client-LanguagePack-Package fr-FR amd64 10.0.10061.0 Language Pack Properties</b> dialog box by clicking <b>Cancel</b>.</td><td>33. In the <b>Microsoft-Windows-Client-LanguagePack-Package fr-FR amd64 10.0.10061.0 Language Pack Properties</b> dialog box, click <b>Cancel</b>.</td></tr>
</table>

Managing apps

LTI also supports the ability to deploy apps as a part of the deployment process. Think of these apps as being “integrated” with the image, and as deploying immediately following Windows 10 deployment. You manage apps in the Applications node in the Deployment Workbench and stored beneath the Applications folder in the deployment share. As with other nodes, you can create a folder structure to help organize apps. You can use the New Application Wizard or the **Import-MDTApplication** Windows PowerShell cmdlet to create applications.

Apps that LTI manages are designed to be initially deployed with the operating system and not for the ongoing maintenance of the app life cycle. Instead, use System Center 2012 R2 Configuration Manager to provide app management throughout the entire app life cycle.

CM as CORP\Administrator

Description	**Steps**
Apps can contain source files, can be a bundle of two or more other apps, or reference an existing app in a network shared folder. Apps that contain source files can store the source files in the distribution share or on a separate network shared folder. In this exercise, you will create an LTI app for Microsoft Office Professional Plus 2013 by using the Office 2013 source files.	
Start the Import OS Packages Wizard.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: 34. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Applications**. 35. In the Actions pane, click **New Application**. The New Application Wizard starts.
On the **Application Type** page, you select the type of LTI app to create. Apps can contain source files or can be a bundle of two or more other apps. Apps that contain source files can store the source files in the distribution share or on a separate network shared folder. You select to create an app with sources files, which in this case are the source files for Microsoft Office Professional Plus 2013.	
On the **Application Type** page, select the	36. On the **Application Type** page, click **Application with source files**, and then click **Next**.

Description	Steps
Application with source files option.	
On the **Details** page, you can enter details about the app, including who published it, the name of the app, the app version, and the language of the app. The only required information is the app name, so I enter that information and move on to the next wizard page.	
On the **Details** page, type the application name, **Microsoft Office Professional Plus 2013 - x86 (CTR) Demo**.	37. On the **Details** page, in **Application Name**, type **Microsoft Office Professional Plus 2013 - x86 (CTR) Demo**, and then click **Next**.
On the **Source** page, you configure the folder in which the source files reside. Because you selected the **Application with source files** option on the **Application type** wizard page, the wizard will copy the entire contents of this folder to the deployment share.	
Enter the path to the source files for Microsoft Office Professional Plus 2013 (**D:\Source$\OfficeProPlus2013_CTR**).	38. On the **Source** page, in **Source directory**, type **D:\Source$\OfficeProPlus2013_CTR**, and then click **Next**.
On the **Destination** page, you configure the name of the folder in which the app will be stored in the deployment share. As you can see, the folder name defaults to the value entered for **Application name** on the **Details** wizard page.	
Accept the default folder path for the app.	39. On the **Destination** page, click **Next**.

Description	Steps
On the **Command Details** page, you configure the command line that will run to initiate app installation and the working directory for when the command is run. For Office, enter **setup.exe /configure "\\CM\DeploymentShare$\Applications\Microsoft Office Professional Plus 2013 - x86 (CTR) \Contoso_Office_2013_Add_CTR.xml”** as the command line. By default, the working directory name is set to the name of the folder in which the app will be stored in the deployment share.	
Enter the command line for Microsoft Office Professional Plus 2013 (**setup.exe /configure "\\CM\DeploymentShare$ \Applications\Microsoft Office Professional Plus 2013 - x86 (CTR) \Contoso_Office_2013_Add_CTR.xml”**) and accept the default working directory name.	40. On the **Command Details** page, in **Command line**, type **setup.exe /configure "\\CM\DeploymentShare$\Applications\Microsoft Office Professional Plus 2013 - x86 (CTR) \Contoso_Office_2013_Add_CTR.xml”**, and then click **Next**.
On the **Summary** page, you can see the configuration settings that you selected while running the wizard. Because the application-creation process can take a few minutes to finish, cancel the wizard and look at the Office Professional Plus 2013 app that already exists in the deployment share.	
Cancel the wizard and view the properties of the **Microsoft Office Professional Plus 2013 - x86 (CTR)** app in the deployment share.	41. On the **Summary** page, click **Cancel**. The **Cancel Wizard** dialog box appears. 42. In the **Cancel Wizard** dialog box, click **Yes**. 43. In the details pane, right-click **Microsoft Office Professional Plus 2013 - x86 (CTR)**, and then click **Properties**. The **Microsoft Office Professional Plus 2013 - x86 (CTR) Properties** dialog box opens.

<table>
<tr><th>Description</th><th>Steps</th></tr>
<tr><td colspan="2">On the <b>Microsoft Office Professional Plus 2013 - x86 (CTR) Properties</b> dialog box, on the <b>General</b> tab, you can type comments about the app, enter a user-friendly display name, and change other information that you saw in the New Application Wizard.</td></tr>
<tr><td>Click the <b>Details</b> tab.</td><td>44. Click the <b>Details</b> tab.</td></tr>
<tr><td colspan="2">On the <b>Details</b> tab, you can see some of the information you entered in the New Application Wizard. In addition, you can control whether the app requires a computer restart after installation, and you can select specific client platforms for the app.</td></tr>
<tr><td>Click the <b>Dependencies</b> tab.</td><td>45. Click the <b>Dependencies</b> tab.</td></tr>
<tr><td colspan="2">Use the <b>Dependencies</b> tab to add dependencies for this app. These dependencies are other apps that you have previously defined.</td></tr>
<tr><td>Cancel the <b>Microsoft Office Professional Plus 2013 - x86 (CTR) Properties</b> dialog box</td><td>46. In the <b>Microsoft Office Professional Plus 2013 - x86 (CTR) Properties</b> dialog box, click <b>Cancel</b>.</td></tr>
</table>

Managing task sequences

A *task sequence* is a collection of individual steps (called *task sequence steps*) that are in a specific order to perform the deployment. Each task sequence step typically runs an MDT script that performs the task sequence step. You manage task sequences in the Task Sequences node in the Deployment Workbench and they are stored beneath the Task Sequences folder in the deployment share. You can use the New Task Sequence Wizard or the **Import-MDTTaskSequence** Windows PowerShell cmdlet to create task sequences.

CM as CORP\Administrator

Description	Steps
Start the New Task Sequence Wizard.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**:

Description	Steps
	47. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Task Sequences**. 48. In the Actions pane, click **New Task Sequence**. The New Task Sequence Wizard starts.
On the **General Settings** wizard page, you enter information about the task sequence. The *task sequence ID* is a unique ID assigned to the task sequence, and a corresponding folder is created in the deployment share. The *task sequence name* is the user-friendly name for the task sequence that is displayed in the Deployment Wizard at the time of deployment.	
On the **General Settings** page, do the following: • In **Task sequence ID**, type **WIN10DEMO**. • In **Task sequence name**, type **Deploy 64-Bit Version of Windows 10**.	49. On the **General Settings** page, in **Task sequence ID**, type **WIN10DEMO**. 50. In **Task sequence name**, type **Deploy 64-Bit Version of Windows 10**. 51. Click **Next**.
On the **Select Template** page, select the LTI task sequence template you will use to create your task sequence. Task sequence templates are similar to document templates. There are templates for deploying client operating systems, server operating systems, deployments to virtual hard disks, and other scenarios. Because you are deploying a client operating system (Windows 10), accept the default task sequence template.	
Accept the default task sequence template.	52. On the **Select Template** page, click **Next**.
On the **Select OS** page, select the operating system to install. You can select only one operating system for each task sequence. If you want to install multiple operating systems within your organization, you must create a task sequence for each operating system.	

Description	Steps
Select the **Windows 10 Enterprise Technical Preview in Windows 10 Enterprise Evaluation x64 install.wim** operating system.	53. On the **Select OS** page, select **Windows 10 Enterprise Technical Preview in Windows 10 Enterprise Evaluation x64 install.wim**, and then click **Next**.
On the **Specify Product Key** page, you select the product key for the operating system you want deployed. You can elect not to provide a product key at this time, provide a Multiple Activation Key (MAK), or provide a specific product key for this particular operating system. If you select the first option, you can provide the product key at deployment time. If you select the second option, you need to have a key management system and use Microsoft Volume Licensing media. If you select the last option, you can specify a specific product key.	
Accept the default option (do not provide a product key at this time) for the task sequence.	54. On the **Specify Product Key** page, click **Next**.
On the **OS Settings** page, you configure the user name, organization name, and the home page for Internet Explorer.	
In **Full name**, type **Contoso User**, in **Organization**, type **Contoso IT**, and **Internet Explorer Home Page**, type **http://www.contoso.com**.	55. On the **OS Settings** page, in **Full name**, type **Contoso User**. 56. In **Organization**, type **Contoso IT**. 57. In **Internet Explorer Home Page**, type **http://www.contoso.com**. 58. Click **Next**.
On the **Admin Passwords** page, you enter the password for the local Administrator account on the target computers. You can elect to enter a password (the first option) or provide the password in the CustomSettings.ini file or the Deployment Wizard (the second option).	
In **Full name**, type **Contoso User**, in **Organization**, type **Contoso IT**, and **Internet**	59. On the **Admin Passwords** page, in **Administrator Password** and **Please confirm Administrator Password**, type **Passw0rd**, and then click **Next**.

<table>
<tr><th>Description</th><th>Steps</th></tr>
<tr><td><b>Explorer Home Page</b>, type <b>http://www.contoso.com</b>.</td><td></td></tr>
<tr><td colspan="2">On the <b>Summary</b> page, you can review the selected configuration settings. Cancel the wizard as a task sequence already exists in the deployment share to perform the deployment.</td></tr>
<tr><td>Cancel the wizard and view the properties of the <b>Deploy Windows 10 to the target computers</b> task sequence in the deployment share.</td><td>60. On the <b>Summary</b> page, click <b>Cancel</b>.
The <b>Cancel Wizard</b> dialog box appears.
61. In the <b>Cancel Wizard</b> dialog box, click <b>Yes</b>.
62. In the details pane, right-click <b>Deploy Windows 10 to the target computers</b>, and then click <b>Properties</b>.
The <b>Deploy Windows 10 to the target computers Properties</b> dialog box opens.</td></tr>
<tr><td colspan="2">On the <b>Deploy Windows 10 to the target computers Properties</b> dialog box, on the <b>General</b> tab, you can enter comments about the task sequence, specify the client platforms for the task sequence, hide the task sequence in the Deployment Wizard, or enable or disable the task sequence.</td></tr>
<tr><td>Click the <b>OS Info</b> tab.</td><td>63. Click the <b>OS Info</b> tab.</td></tr>
<tr><td colspan="2">On the <b>OS Info</b> tab, you can see information about the operating system we selected during the New Task Sequence Wizard. You can also directly modify the Unattend.xml file for the operating system if you wish to perform highly customized deployments. Normally, the LTI deployment process automatically updates the Unattend.xml file based on configuration settings made in the Deployment Workbench.</td></tr>
<tr><td>Click the <b>Task Sequence</b> tab.</td><td>64. Click the <b>Task Sequence</b> tab.</td></tr>
<tr><td colspan="2">On the <b>Task Sequence</b> tab, you manage the task sequence steps. In most instances, the task sequence created from the LTI task sequence templates requires only minor modification, if any. If you look at the hierarchy of the task sequence, you can see the various deployment phases that are performed, starting with the Initialization phase and</td></tr>
</table>

Description	Steps
ending with State Restore phase. Again, you can fully customize these task sequences if required, but the default configuration typically works fine.	
Navigate to **Install/Install Operating System** in the task sequence hierarchy.	65. In the task sequence hierarchy, navigate to **Install/Install Operating System**.
If you look at one of the task sequence steps, you can see the type of actions a task sequence step performs. In this task sequence, the operating system selected is going to be installed on the target computer by using the **Install Operating System** task sequence step. This task sequence step is configured when the New Task Sequence Wizard is run.	
Navigate to **State Restore/Restore User State** in the task sequence hierarchy.	66. In the task sequence hierarchy, navigate to **State Restore/Restore User State**.
In most cases, a task sequence step ends up running an MDT script. These scripts are used to actually perform the actions that the task sequence step prescribes. As you can see, the **Restore User State** task sequence step actually runs the ZTIUserState.wsf script to restore the user state (if any). Again, you can customize task sequences, but in most instances they require minor or no modifications.	
Cancel the **Deploy Windows 8.1 to the target computers Properties** dialog box.	67. In the **Deploy Windows 8.1 to the target computers Properties** dialog box, click **Cancel**.

Managing deployment configuration settings

Next you need to manage the deployment configuration settings. As previously mentioned, MDT stores the deployment configuration settings in the CustomSettings.ini file or in the MDT DB.

The CustomSettings.ini file contains the deployment configuration settings for a specific deployment share. It has a format that is similar to that of other .ini files. As you use the Deployment Workbench to make changes, some settings in the CustomSettings.ini file are updated accordingly. You can also directly modify the CustomSettings.ini file in the Deployment Workbench or by using any text editor.

You can also use the MDT DB to centrally store deployment configuration settings to be used by any number of distribution shares. As with the CustomSettings.ini file, you can use the Deployment Workbench to manage the MDT DB. You can also use any tools that support Microsoft SQL Server to manage the MDT DB.

CM as CORP\Administrator

Description	Steps
Edit the properties of the **MDT Deployment Share (C:\DeploymentShare)** deployment share.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: 68. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)**. 69. In the Actions pane, click **Properties**. The **MDT Deployment Share (C:\DeploymentShare) Properties** dialog box opens.
On the **General** tab, you can type comments about the task sequence, specify the processor platforms that the deployment share supports, and determine whether the deployment share is enabled for multicast deployments using WDS.	
Review the information on the **Rules** tab.	70. Click the **Rules** tab.
The **Rules** tab has the current configuration settings for the CustomSettings.ini file. You can use this tab to directly modify the CustomSettings.ini file.	
Review the information on the **Rules** tab.	71. Click the **Windows PE** tab.
Use the **Windows PE** tab to manage configuration settings for the Windows PE images generated for the deployment share. The Windows PE images are generated when you run the Update Deployment Share Wizard, which you will see later in this demonstration.	
Select the **Monitoring** tab.	72. Click the **Monitoring** tab.

<table>
<tr><th>Description</th><th>Steps</th></tr>
<tr><td></td><td>73. On the <b>Monitoring</b> tab, observe that the <b>Enable monitoring for this deployment share</b> check box is checked.</td></tr>
<tr><td colspan="2">Use the <b>Monitoring</b> tab to enable monitoring of MDT deployments. You can monitor MDT deployments in the Monitoring node in the Deployment Workbench. If you enable monitoring by selecting the <b>Enable monitoring for this deployment share</b> check box, the CustomSettings.ini file is updated.</td></tr>
<tr><td>Close the <b>MDT Deployment Share (C:\DeploymentShare) Properties</b> dialog box by clicking <b>Cancel</b>.</td><td>74. In the <b>MDT Deployment Share (C:\DeploymentShare) Properties</b> dialog box, click <b>Cancel</b>.</td></tr>
</table>

Creating LTI bootable images

One of the final tasks to complete just prior to Windows 10 deployment is to create the bootable images that then initiate the LTI deployment process. MDT provides a method for creating bootable images that you can then use to create bootable media (such as a DVD or USB drive) or use with WDS. The Deployment Workbench creates both .wim and .iso file formats and stores them in the Boot folder in the deployment share. You can use the Update Deployment Share Wizard in the deployment share in the Deployment Workbench or the **Update-MDTDeploymentShare** Windows PowerShell cmdlet to create these bootable images.

CM as CORP\Administrator

Description	Steps
Start the Update Deployment Share Wizard.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: 75. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)**. 76. In the Actions pane, click **Update Deployment Share**. The Update Deployment Share Wizard starts.
On the **Options** page, you configure the options for updating the deployment share. The first option, **Optimize the boot image updating process**, optimizes the images if any options have been changed. This option invariably takes less time than the other option. You can also select to compress the boot image by selecting the **Compress the boot image contents to recover space used by removed or modified content** check box. The second option, **Completely regenerate the boot images**, generates new boot images. This option takes more time than the first but ensures that the boot images contain the most recent configuration settings.	
No configuration settings need to be changed on the **Options** page.	77. On the **Options** page, click **Next**.
On the **Summary** page, you can review the selected configuration settings. Because updating the deployment share and subsequent generation of the boot images takes a few minutes to finish, cancel the wizard and look at the boot images that were previously generated.	

Description	Steps
On the **Summary** page, cancel the wizard.	78. On the **Summary** page, click **Cancel**. The **Cancel Wizard** dialog box appears. 79. In the **Cancel Wizard** dialog box, click **Yes**. 80. In File Explorer, go to the **C:\DeploymentShare\Boot** folder.
In the **C:\DeploymentShare\Boot** folder, you can see the **LiteTouchPE_x64.iso** and **LiteTouchPE_x64.wim** files (for 64-bit target computers) and the **LiteTouchPE_x86.iso** and **LiteTouchPE_x86.wim** files (for 32-bit target computers). You can use these files to start the LTI deployment process on the target computers by using bootable media (such as a DVD) or by using WDS. In this exercise, you will start the LTI deployment process by using a copy of the LiteTouchPE_x64.iso to start the BM01 virtual machine.	
Close File Explorer.	81. Close File Explorer.

Deploying Windows 10 and Office Professional Plus 2013

After creating the LTI bootable images, you need to determine how to initiate the LTI deployment process. You can use the LTI bootable images to create bootable media (such as a DVD or USB drive) or use them with WDS. For partially automated deployments, the Deployment Wizard starts, you select the appropriate task sequence (which you reviewed saw earlier in this exercise), and then you complete the remaining wizard pages. Based on the task sequence and the deployment configuration settings, only certain wizard pages might be displayed.

For fully automated deployments, the task sequence that will run is configured in the configuration files and is automatically selected. No wizard pages are displayed, and the LTI deployment process continues without requiring user interaction. For fully automated deployments, all configuration settings must be specified in either the CustomSettings.ini file or the MDT DB.

BM01

Description	**Steps**
Start the Deployment Wizard.	Perform the following steps on BM01: 82. Start the virtual machine. The Deployment Wizard starts.
On the **Welcome** page, you can the LTI deployment process or perform other maintenance tasks. For example, you can use tools such as the Microsoft Diagnostics and Recovery Toolset (DaRT) to perform system recovery.	
Click **Run the Deploymen Wizard to install a new Operating System**.	83. On the **Welcome** page, click **Run the Deployment Wizard to install a new Operating System**.
On the **Credentials** page, you configure the credentials that connect to the deployment share. These credentials must allow access to all the files and folders in the deployment share.	
On the **Credentials** page, do the following: • In **User Name**, type **Administrator**. • In **Password**, type **Passw0rd** • In **Domain**, type **CORP**.	84. On the **Credentials** page, in **User Name**, type **Administrator**. 85. In **Password**, type **Passw0rd** 86. In **Domain**, type **CORP**, and then click **OK**.
On the **Task Sequence** page, you select the task sequence that you want to run. This list contains all the task sequences in your deployment share that are not hidden or disabled.	
Select the click **Deploy Windows 10 to the target computers** task sequence.	87. On the **Task Sequence** page, click **Deploy Windows 10 to the target computers**, and then click **Next**.
On the **Computer Details** page, you provide the configuration settings for the computer, the computer name, and whether the computer should join a domain or a workgroup.	

Description	Steps
Use **BM01** for the computer name and join the **corp.contoso.com** domain.	88. On the **Computer Details** page, in **Computer name**, type **BM01**. 89. Click **Join a domain**. 90. In **Domain to join**, type **corp.contoso.com**, and then click **Next**.
The **Move Data and Settings** page allows you to perform an offline migration of user state information by using the offline migration feature in the Windows User State Migration Tool (USMT). There is no user state information to save and restore because this is a new computer (bare metal) deployment.	
No settings need to be configured on this wizard page.	91. On the **Move Data and Settings** page, click **Next**.
On the **User Data (Restore)** page, you can configure the deployment process to restore any user state migration information that might have been captured. There is no user state information to restore because this is a new computer (bare metal) deployment.	
No settings need to be configured on this wizard page.	92. On the **User Data (Restore)** page, click **Next**.
On the **Locale and Time** page, you should provide any configuration settings that relate to locale and the time zone in which the device resides.	
You don't need to configure any settings on this wizard page.	93. On the **Locale and Time** page, click **Next**.
On the **Applications** page, you select the applications that you want to install as a part of the deployment process.	
Select **Microsoft Office Professional Plus 2013 - x86 (CTR)**.	94. On the **Applications** page, select **Microsoft Office Professional Plus 2013 - x86 (CTR)**, and then click **Next**.

<table>
<tr><th>Description</th><th>Steps</th></tr>
<tr><td colspan="2">On the <b>BitLocker</b> page, you configure BitLocker Drive Encryption for the target device. You can’t enable BitLocker virtual machines, so you will not need to configure BitLocker for this exercise. However, you could use MDT to configure BitLocker on your physical devices.</td></tr>
<tr><td>No settings need to be configured on this wizard page.</td><td>95. On the <b>BitLocker</b> page, click <b>Next</b>.</td></tr>
<tr><td colspan="2">On the <b>Ready</b> page, you can see the configuration settings that were selected while running the wizard. Review the details and ensure that the appropriate configuration settings have been made.
After you have reviewed the information that you provided on the previous wizard pages, you are ready to start the automated portion of the deployment process. Again, if you had configured this to be a fully automated deployment, the Deployment Wizard and all these wizard pages would be skipped.</td></tr>
<tr><td>Click <b>Details</b>, review the information, and then click <b>Begin</b>.</td><td>96. On the <b>Ready</b> page, click <b>Details</b>.
97. Review the information, and then click <b>Begin</b>.</td></tr>
<tr><td colspan="2">The deployment process starts, and you can see the progress displayed on the computer. This process will continue unattended until the deployment is complete. Now, see how to use the Monitoring node in the Deployment Workbench to monitor the MDT deployment process.</td></tr>
<tr><td>Navigate to <b>Monitoring</b> node in the Deployment Workbench and view the deployment process for <b>BM01</b>.</td><td>Perform the following steps on W10-CM logged on as <b>CORP\Administrator</b> with the password <b>Passw0rd</b>:
98. In the Deployment Workbench console tree, go to <b>Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Monitoring</b>.
99. In the Actions pane, click <b>Refresh</b>.
100.In the details pane, view the deployment process for <b>BM01</b>.
101.In the details pane, click <b>BM01</b>.
102.In the Actions pane, click <b>Properties</b>.</td></tr>
</table>

Description	Steps
	The **BM01 Properties** dialog box is displayed.
As you monitor the deployment process, you can see the current status of BM01. You can continue to refresh this view and look at updated information about the deployment process. If you want additional information about the deployment process, look at the properties of the entry. Here, you can see detailed monitoring information about the deployment process. You can use this information to determine whether a deployment is stopped and to help troubleshoot deployment problems. You can also remotely connect to the target computer by using Remote Desktop, Virtual Machine Connection, or DaRT Remote Control, depending on the target computer.	
Close the **BM01 Properties** dialog box.	103.In the **BM01 Properties** dialog box, click **OK**.
Note: The deployment process from this point to the beginning of the next section will take approximately 45 minutes. You should continue to Exercise 2 and start the deployment process to WIN7. Then return here to verify the deployment success on BM01.	

Verifying deployment (if time permits)

The entire deployment process takes some time to finish. You can continue to monitor the deployment process from the Deployment Workbench or by viewing the progress on the Deployment Wizard. When the deployment process is complete, the completion status of the Deployment Wizard is displayed on the desktop.

You need to verify that Windows is properly configured by verifying the computer name and the domain to which Windows is joined. You also need to verify that any apps are properly deployed (such as Microsoft Office Professional Plus 2013 that you selected earlier in this exercise).

BM01

Description	Steps
Review the completion status of the Deployment Wizard.	Perform the following steps on BM01:

Description	Steps
	104.On the **Success** page of the Deployment Wizard, review the completion status.
On the **Success** page of the Deployment Wizard, you can see the completion status. If the deployment is successful (which it should be), then there will be no information in the details. If there had been any warnings or errors during the deployment process, they are displayed in the details, which you can use to help troubleshoot the deployment process.	
Close the Deployment Wizard. Sign off as BM01\Administrator. Sign in as CORP\Administrator. Start the Control Panel System applet.	105.On the **Success** page of the Deployment Wizard, click **Finish**. The Deployment Wizard closes. 106.Sign out as BM01\Administrator 107.Sign in as **CORP\Administrator** with the password **Passw0rd**. 108.Press **Win+X**. The task menu is displayed. 109.Click **System**. The Control Panel System applet is displayed.
The Control Panel System applet shows basic information about the Windows installation. In this applet, you can view the computer name and domain membership Windows configuration. You should configure Windows with a computer name of **BM01** and join to the **corp.contoso.com** domain.	
Verify that the computer name is **BM01** and that Windows is joined to the **corp.contoso.com** domain. Close the Control Panel System applet. On the Start menu, open the **Microsoft Office 2013** group of apps.	110.In the System Control Panel applet, under the **Computer name, domain, and workgroup settings** section verify the following: o Computer name is set to **BM01**. o Domain is set to **corp.contoso.com**. 111.Close the Control Panel System applet. 112.On the Start menu, click **All apps**, and then expand **Microsoft Office 2013**. **Note: In this lab,** it can take several minutes before the Start menu is ready. If the Start menu does not open immediately, press the **Windows Key + X**, click

Description	Steps
	Programs and Features, and see that Office 365 ProPlus is installed on the system.
On the Start menu you can see that Microsoft Office Professional Plus 2013 is installed, which confirms that the deployment process successfully installed it.	
	113.Close the Start menu.

Exercise 2: Deploying Windows 10 to an existing device running Windows 7 (optional)

The exercise illustrates how to deploy Windows 10 to an existing device running Windows 7 (or "refresh" deployment) by MDT. In this exercise, you will configure MDT to save the user state for existing users in Windows 7. Then, you will configure MDT to restore the saved user state after deploying Windows 10. Finally, you will verify that the user state has been successfully restored in Windows 10.

You will use the LTI MDT deployment method to refresh the device running Windows 7 with Windows 10. As a part of the Windows 10 deployment, you will deploy the apps that are currently running on Windows 7. For example, the Windows 7 device (WIN7) has Microsoft Office Professional Plus 2013 installed. You will install Office Professional Plus 2013 during the Windows 10 deployment to ensure that Office Professional Plus 2013 is available after Windows 10 deployment.

Reviewing the Windows 7 user state

Before you refresh the Windows 7 device with Windows 10, review the existing user data, settings, and apps on the device. Later in this exercise you will configure MDT to perform an offline back up of the user data and settings. You will then configure MDT to restore the same saved user data and settings to Windows 10.

Specifically, you will verify the following on the Windows 7 device:

- Computer name is **WIN7**.
- Windows 7 is joined to the **corp.contoso.com** domain.
- **Office Professional Plus 2013** is installed.
- The **SalesDocument** folder is in the **Documents** folder for the CORP\Mark user and contains the following Microsoft Excel spreadsheets:
  - AverageSellPriceAnalysis.xlsx
  - BreakevenAnalysis.xlsx
  - CustomerProfitabilityAnalysis.xlsx
  - QuarterlySalesReport.xlsx

WIN7 as CORP\Mark

Description	Steps
Start the Control Panel System applet.	1. Perform the following steps on WIN7 signed in as **CORP\Mark** with the password **Passw0rd**: 2. Click Start, right-click **Computer**, and then click **Properties**. 3. The Control Panel System applet is displayed.
The Control Panel System applet shows basic information about the Windows installation. In this applet, you can view the computer name and domain membership Windows configuration. Windows should be configured with a computer name of **WIN7** and be joined to the **corp.contoso.com** domain.	
Verify that the computer name is **WIN7** and that Windows is joined to the **corp.contoso.com** domain. Close the Control Panel System applet. Confirm that the Microsoft Office Professional Plus 2013 icons are on the taskbar.	4. In the System Control Panel applet, under the **Computer name, domain, and workgroup settings** section verify the following: • Computer name is set to **WIN7**. • Domain is set to **corp.contoso.com**. 5. Close the Control Panel System applet. 6. Confirm that the Microsoft Office Professional Plus 2013 icons are on the taskbar.
On the taskbar you can see that the Microsoft Office Professional Plus 2013 icons exist.	
View the **Libraries\Documents\SalesDocument** folder in Windows Explorer.	7. Click **Start**, and then click **Documents**. The Libraries\Documents folder opens in Windows Explorer. 8. In Windows Explorer go to **Libraries\Documents\SalesDocuments**.

Description	Steps
In Windows Explorer, you can see the contents of the **Libraries\Documents\SalesDocuments** folder for the CORP\Mark user. You can see the following Microsoft Excel spreadsheets in the folder: • AverageSellPriceAnalysis.xlsx • BreakevenAnalysis.xlsx • CustomerProfitabilityAnalysis.xlsx • QuarterlySalesReport.xlsx	
Close Windows Explorer	9. Close Windows Explorer.

Reviewing the task sequence

You will use the same task sequence to deploy Windows 10 to the Windows 7 device that you used to deploy Windows 10 to the new device in “Exercise 1: Deploying Windows 10 to a new computer” earlier in this lab. Before you run the task sequence and deploy Windows 10 and Office Professional Plus 2013, review the task sequence to see how the user state information is saved and then later restored.

CM as CORP\Administrator

Description	Steps
View the **State Capture\Capture User State** task sequence step in the click **Deploy Windows 10 to the target computers** task sequence.	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**: 10. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Task Sequences**. 11. In the details pane, click **Deploy Windows 10 to the target computers**. 12. In the Actions pane, click **Properties**. The **Deploy Windows 10 to the target computers Properties** dialog box opens.

Description	Steps
	13. In the **Deploy Windows 10 to the target computers Properties** dialog box, click the **Task Sequence** tab. 14. In the task sequence hierarchy, go to **State Capture\Capture User State**.
On the **Properties** tab of the **Capture User State** task sequence step you can see that the task sequence calls **ZTIUserState.wsf** with the **/capture** parameter. Ultimately, ZTIUserState.wsf calls the savestate.exe tool from the USMT, which is a part of the Windows 10 Assessment and Deployment Kit (ADK). In this task sequence, savestate.exe saves the user state to the local drive. However, you could configure the CustomSettings.ini file or the MDT DB to save the user state to a network shared folder.	
View the **State Restore\Capture User State** task sequence step in the click **Deploy Windows 10 to the target computers** task sequence.	15. In the task sequence hierarchy, go to **State Restore\Restore User State**.
On the **Properties** tab of the **Restore User State** task sequence step, you can see that the task sequence calls **ZTIUserState.wsf** with the **/restore** parameter. For restoring user state, ZTIUserState.wsf calls the loadstate.exe tool from the USMT. In this task sequence, loadstate.exe restores (loads) the user state from the local drive. However, you could configure the CustomSettings.ini file or the MDT DB to load the user state from a network shared folder.	
Close the **Deploy Windows 10 to the target computers Properties** dialog box by clicking **Cancel**.	16. In the **Deploy Windows 10 to the target computers Properties** dialog box, click **Cancel**.

Deploying Windows 10 and Office Professional Plus 2013

Now that you have seen how the task sequence saves and restores user state information, you are ready to run the task sequence on the Windows 7 device to refresh the device with Windows 10 and Office Professional Plus 2013. The task sequence will save the user state information to the local disk on the device and then restore the user state from the local disk. After the user state information is restored, then the task sequence will deploy Office Professional Plus 2013.

WIN7 as CORP\Mark

Description	Steps
On the desktop, double-click **Start Deployment Wizard.**	Perform the following steps on WIN7 signed in as **CORP\Mark** with the password **Passw0rd**: 17. On the desktop, double-click **Start Deployment Wizard**. A command prompt opens and the **User Access Control** dialog box appears. 18. In the **User Access Control** dialog box, click **Yes**. The Deployment Wizard starts.
On the **Task Sequence** page, you select the task sequence that you want to run. This list contains all the task sequences in your deployment share that are not hidden or disabled.	
Select the click **Deploy Windows 10 to the target computers** task sequence.	19. On the **Task Sequence** page, click **Deploy Windows 10 to the target computers**, and then click **Next**.
On the **Computer Details** page, you provide the configuration settings for the computer, the computer name, and whether the computer should join a domain or a workgroup. You will configure the new Windows 10 computer name to be the same as the existing Windows 7 computer name (WIN7).	
Use **WIN7** for the computer name and join the **corp.contoso.com** domain.	20. On the **Computer Details** page, verify that **Computer name**, is set to **WIN7**. 21. Verify that **Join a domain** is selected. 22. Verify that **Domain to join** is set to **corp.contoso.com**. 23. In **User Name**, type **Administrator**.

Description	Steps
	24. In **Password**, type **Passw0rd**. 25. In **Domain**, type **CORP**. 26. Click **Next**.
On the **User Data** page, you specify where you want to save the user state, which includes the user data and settings. You can allow the Deployment Wizard to automatically determine the location, specify a location, or not save any user data and settings.	
You don't need to configure any settings on this wizard page.	27. On the **User Data** page, click **Next**.
On the **Computer Backup** page, you specify where to save a complete backup of the computer. This backup allows you to have a recovery point in the event of a catastrophic failure during the deployment process.	
You don't need to configure any settings on this wizard page.	28. On the **Computer Backup** page, click **Next**.
On the **Locale and Time** page, you should provide any configuration settings that relate to locale and the time zone in which the device resides.	
You don't need to configure any settings on this wizard page.	29. On the **Locale and Time** page, click **Next**.
On the **Applications** page, select the applications that you want to install as a part of the deployment process.	
Select **Microsoft Office Professional Plus 2013 - x86 (CTR)**.	30. On the **Applications** page, select **Microsoft Office Professional Plus 2013 - x86 (CTR)**, and then click **Next**.
On the **BitLocker** page, you configure BitLocker Drive Encryption for the target device. You can't enable BitLocker in virtual machines, so you will not need to configure BitLocker	

Description	Steps
for this exercise. However, you could use MDT to configure BitLocker on your physical devices.	
You don’t need to configure any settings on this wizard page.	31. On the **BitLocker** page, click **Next**.
On the **Credentials** page, you configure the credentials that are used to connect to network shares. These credentials must allow access to all the files and folders in the deployment share.	
On the **Credentials** page, do the following: • In **User Name**, type **Administrator**. • In **Password**, type **Passw0rd** • In **Domain**, type **CORP**.	32. On the **Credentials** page, in **User Name**, type **Administrator**. 33. In **Password**, type **Passw0rd** 34. Verify that **Domain** is set to **CORP**. 35. Click **Next**.
On the **Ready** page, you can see the configuration settings you selected while running the wizard. Review the details and ensure that you made the appropriate configuration settings. After you have reviewed the information that you provided on the previous wizard pages, you are ready to start the automated portion of the deployment process.	
Click **Details**, review the information, and then click **Begin**.	36. On the **Ready** page, click **Details**. 37. Review the information, and then click **Begin**.
The deployment process starts, and you can see the progress displayed on the computer. This process will continue unattended until the deployment is complete. Next, see how to use the Monitoring node in the Deployment Workbench to monitor the MDT deployment process.	
Navigate to **Monitoring** node in the Deployment Workbench	Perform the following steps on W10-CM logged on as **CORP\Administrator** with the password **Passw0rd**:

Description	Steps
and view the deployment process for **WIN7**.	38. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Monitoring**. 39. In the Actions pane, click **Refresh**. 40. In the details pane, view the deployment process for **WIN7**. 41. In the details pane, click **WIN7**. 42. In the Actions pane, click **Properties**. The **WIN7 Properties** dialog box is displayed.
As you monitor the deployment process, you can see the current status of WIN7. You can continue to refresh this view and look at updated information about the deployment process. If you want additional information about the deployment process, look at the properties of the entry. Here, you can see detailed monitoring information about the deployment process. You can use this information to determine whether a deployment is stopped and to help troubleshoot deployment problems. You can also remotely connect to the target computer by using Remote Desktop, Virtual Machine Connection, or DaRT Remote Control, depending on the target computer.	
Close the **WIN7 Properties** dialog box.	43. In the **WIN7 Properties** dialog box, click **OK**.
Note The deployment process from this point to the beginning of the next section will take approximately 60 minutes. You should return to the Verifying Deployment section of Exercise 1 and continue that exercise on BM01 to verify success. When finished with Exercise 1, continue with the Verifying Deployment section of Exercise 2 to verify success on WIN7.	

Verifying deployment

The entire deployment process takes some time to finish. You can continue to monitor the deployment process from the Deployment Workbench or by viewing the progress on the

Deployment Wizard. When the deployment process is complete, the completion status of the Deployment Wizard is displayed on the desktop.

You need to verify that Windows is properly configured by verifying the computer name and the domain to which Windows is joined. You also need to verify that any apps are properly deployed (such as Microsoft Office Professional Plus 2013 that you selected earlier in this exercise). Finally, you need to verify that the user state has been properly migrated by verifying that the user files and settings have been migrated.

WIN7

Description	Steps
Review the completion status of the Deployment Wizard.	Perform the following steps on WIN7: 44. On the **Success** page of the Deployment Wizard, review the completion status.
On the **Success** page of the Deployment Wizard, you can see the completion status. If the deployment is successful (which it should be), then there will be no information in the details. If there had been any warnings or errors during the deployment process, they are displayed in the details, which you can use to help troubleshoot the deployment process.	
Close the Deployment Wizard. Sign out as WIN7\Administrator. Sign in as CORP\Mark. Start the Control Panel System applet.	45. On the **Success** page of the Deployment Wizard, click **Finish**. The Deployment Wizard closes. 46. Sign out as WIN7\Administrator. 47. Sign in as **CORP\Mark** with the password **Passw0rd**. 48. Press **Win+X**. The task menu is displayed. 49. Click **System**. The Control Panel System applet is displayed.
The Control Panel System applet shows basic information about the Windows installation. In this applet, you can view the computer name and domain membership Windows configuration. Windows should be configured with a computer name of **WIN7** and be joined to the **corp.contoso.com** domain.	

Description	Steps
Verify that the computer name is **WIN7** and that Windows is joined to the **corp.contoso.com** domain. Close the Control Panel System applet. Confirm that the Office Professional Plus 2013 icons are on the taskbar.	50. In the System Control Panel applet, under the **Computer name, domain, and workgroup settings** section verify the following: • Computer name is set to **WIN7**. • Domain is set to **corp.contoso.com**. 51. Close the Control Panel System applet. 52. Confirm that the Office Professional Plus 2013 icons are on the taskbar.
On the taskbar you can see that the Microsoft Office Professional Plus 2013 icons exist.	
View the **Libraries\Documents\SalesDocument** folder in File Explorer.	53. Click Start, and then click **Documents**. The Documents folder opens in Windows Explorer. 54. In File Explorer, go to **Documents\SalesDocuments**.
In File Explorer, you can see the contents of the **Documents\SalesDocuments** folder for the CORP\Mark user. You can see the following Microsoft Excel spreadsheets in the folder: • AverageSellPriceAnalysis.xlsx • BreakevenAnalysis.xlsx • CustomerProfitabilityAnalysis.xlsx • QuarterlySalesReport.xlsx These files were saved as part of the user state in Windows 7 (in the State Capture phase in the task sequence) and then were restored after the Windows 10 deployment (in the State Restore phase).	
Close File Explorer	55. Close File Explorer.

Windows 10 and Enterprise Mobility

Configure a SAAS App from the Gallery

In this Lab you will learn how to configure an App in Azure Active Directory that is acquired from the Gallery in order to make it available to Users

Table of Contents

Overview

This exercise will illustrate how to setup an App in Azure Active Directory and then setup access for users.

You will complete the following objectives.

- Browse a website in the version of Internet Explorer
- View the same website in the Microsoft Edge Browser
- Make a note of the differences and display problems
- Use compatibility mode and enterprise mode to quickly remediate the issues without the need for code.

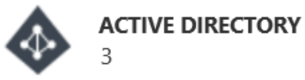
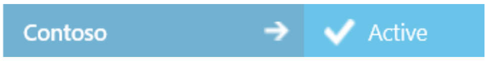
Table 1 outlines the requirements for completing this module.

Table 1. Module requirements

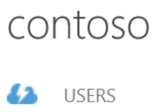
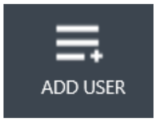
Virtual machines	Physical devices	Subscriptions and accounts
• W10-Client	• No physical devices are required in this module.	• Subscriptions required will have been setup in initial *Trial Account Registration* Exercise

Exercise 1: Configuring an App in Azure Active Directory

Login to Windows Azure

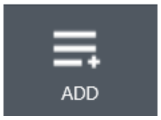
Description	Action
Login to the Azure environment	1. Log in to the W10-W10Client machine using the following credentials Username: W10User Password: Passw0rd! 2. Click on the Edge browser icon on the Taskbar 3. Once the Edge Browser open, ensure it is full screen (maximized)
	4. Navigate to https://manage.windowsazure.com 5. Login using the credentials as they were setup at the beginning of the course 6. Scroll down the list of Services and click on Active Directory  7. Click on Contoso in the list of Directories 

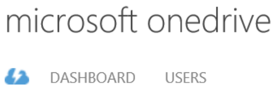
Create a User

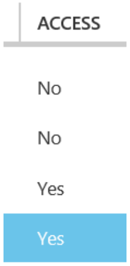
Description	Action
Create a User that will be given access to the App	8. Click on Users  9. Click on Add User  10. Choose New User in your Organization from the dropdown menu 11. Type a Username for your User, for example W10User001 12. Click Next 13. Type a First Name, Last Name and Display Name 14. Ensure User is selected for Role 15. Ensure Multi Factor Authentication remains unchecked 16. Click Next 17. On the Get Temporary Password dialog, click Create 18. Make a note of the Password and click Finished

Description	Action
	19. Open an In Private Browser session (CTL+SHIFT+P) 20. Navigate to https://myapps.microsoft.com 21. Sign in using your User ID and Temporary Password 22. When prompted to update your password, type the old password 23. Type Passw0rd! twice and click on Update password and sign in 24. Once signed in you will notice that there are no apps available

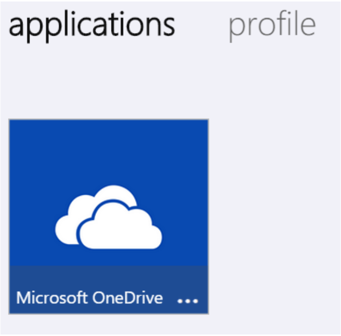
Add an Application and give the user Access

Description	Action
Add an Application from the Galley and give the user access to the Application	Change back to the browser where you are logged in as the Azure Admin 25. In the Contoso Directory environment, click on Applications APPLICATIONS 26. Click on Add  27. Click on Add an application from the gallery

Description	Action
	 Add an application from the gallery 28. In the Search Box, type OneDrive 29. Click Search 30. Click on Microsoft OneDrive and add it to your directory 31. The One Drive configuration page should be displayed  microsoft onedrive 32. Click on Assign accounts 33. Click on (highlight) the user that was created earlier in the lab 34. Click Assign 35. Check the I want to enter Microsoft OneDrive credentials on behalf of the user checkbox 36. Enter the email address and password for the user 37. Click Complete 38. On the OneDrive page under the Access column the user should display the word Yes

Description	Action
	 ACCESS No No Yes Yes

Test that the Application displays for the User

Description	Action
Sign into the User portal and insure the User has access to the Application	39. Open an In Private browser window (CTL+SHIFT+P) 40. Navigate to https://myapps.microsoft.com 41. Login as the user created earlier 42. The Portal should show the application that was made available to the user 

Windows 10 and Enterprise Mobility

Azure AD Join Configuration

Once the user and device are joined to Azure Active Directory Domain there are a number of options that can be configured. In this lab we will look at some of the configuration options available to you when using Azure Active Directory

Table of Contents

Overview

The exercises in this lab will illustrate how to install a custom built Universal App by using PowerShell

You will complete the following objectives.

- Connect to Azure
- Navigate to the Azure AD Configuration
- Enable a specific Group or User to enroll devices
- Enable Multi-Factor Authentication
- Investigate the User Configuration

Table 1 outlines the requirements for completing this module.

Table 1. Module requirements

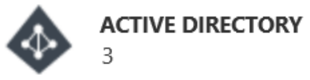
Virtual machines	Physical devices	Subscriptions and accounts
• W10-Client • W10-Edge • W10-IiS	• No physical devices are required in this module.	• As configured in initial *Trial Account Registration* Exercise

Exercise 1: Azure Active Directory Join Configuration

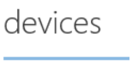
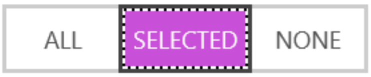
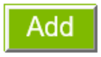
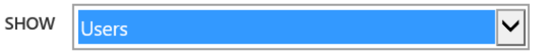
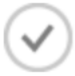
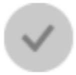
Connect to Azure

Description	Action
Connect to Windows Azure using the Microsoft Account that was setup at the beginning of the course	1. The following steps should be performed on the W10-W10Client virtual machine Username: W10User Password: Passw0rd! 2. Click on the Edge browser on the Taskbar 3. Navigate to manage.windowsazure.com 4. Login with your Microsoft Account

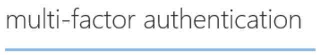
Navigate to the Azure AD Configuration

Description	Action
Navigate to the Azure Active Directory Configuration Environment	5. Once Azure loads, Click on Active Directory  ACTIVE DIRECTORY 3 6. Click on Contoso 7. Click on Configure CONFIGURE 8. You are now in the configuration environment for your Azure Active Directory

Enable a specific Group or User to enroll devices

Description	Action
Enable a specific group and give them the ability to enroll devices	9. In the Configuration window, scroll down to the devices section.  10. Next to the caption - Users may Join devices to Azure AD, Click on Selected  11. Below the Selected button, Click on Add  12. In the Add Members dialog, Click on Users in the Show dropdown menu  13. Click on Finish  14. Highlight an existing user, created earlier that has not been used to join to AAD, and Click Complete 

Enable Multi Factor Authentication

Description	Action
Investigate how to Enable Multi-Factor Authentication to Join a device Azure Active Directory Enable Multi-Factor Authentication for a User	15. Within the Configuration window, under the devices heading, Locate Requires Multi-Factor Auth to Join Devices REQUIRE MULTI-FACTOR AUTH TO JOIN DEVICES 16. Click on Yes 17. A message will appear informing you that other services and setup are required. In the context of this lab we will not be able to setup MFA for device join 18. Click No 19. Scroll up to multi-factor authentication  multi-factor authentication 20. Click on Manage Service Settings Manage service settings 21. A new Tab will open with the MFA configuration page (if prompted for credentials, login with your Microsoft Account) 22. Click on Users users 23. Check the Checkbox next to the user used in the previous task 24. Click Enable 25. Click Enable multi-factor Auth

Description	Action
	26. This user will be prompted for MFA when they login 27. Click Close 28. Switch to the Microsoft Azure Active Directory tab for Contoso

Check the User Configuration

Description	Action
Check the Configuration of the user used in the previous tasks	29. Click on Users 30. Click on the User that has been used earlier for Azure Active Directory Domain Join 31. Click on Devices to check that the Device has been registered during the Join 32. Click on Work Info and scroll down to Authentication Contact Info to see the phone number used for AAD Join. This will be used for future Auth or the user will be prompted for Phone information

Windows 10 and Enterprise Mobility

Create a Provisioning Package

With Windows 10, you can create provisioning packages that let you quickly and efficiently configure a device without having to install a new image.

Use the Windows Imaging and Configuration Designer (ICD) to create a provisioning package (.ppkg), which contains customizations that you can include for a particular Windows image. You can either apply the provisioning package to an image or share it as a standalone package that can be applied to a running system using the Provisioning Engine.

Table of Contents

Overview

The exercises in this lab will illustrate how to install a custom built Universal App by using PowerShell

You will complete the following objectives.

- Launch the Image and Configuration Designer
- Create a Provisioning Package
- Deploy the Provisioning Package
- Test the Provisioning Package

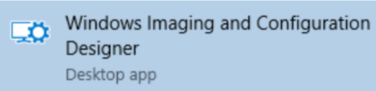
Table 1 outlines the requirements for completing this module.

Table 1. Module requirements

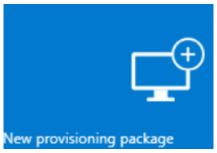
Virtual machines	Physical devices	Subscriptions and accounts
• W10-Client	• No physical devices are required in this module.	• No subscriptions are required for this lab

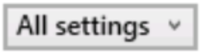
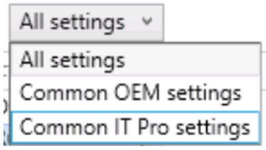
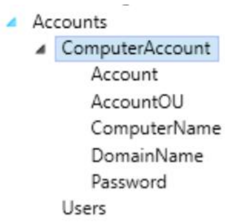
Exercise 1: Create a Provisioning Package using the Windows ICD

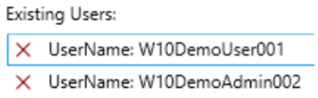
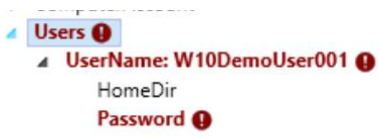
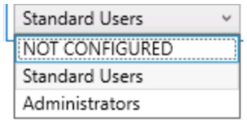
Launch the Image and Configuration Designer

Description	Action
Connect to the Windows 10 virtual machine and then launch the Image and Configuration Designer	1. The following steps should be performed on the W10-W10Client virtual machine 2. Logon using the following credentials Username: W10User Password: Passw0rd! 3. Click on the Start button 4. Type ICD 5. Click on Windows Imaging and Configuration Designer  6. Click Yes 7. When the Windows Imaging and Configuration Designer launches you are ready to create Provisioning Packages

Create a Provisioning Package to Create Users on the Local Machine

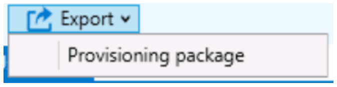
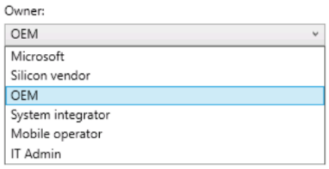
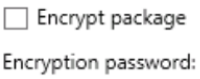
Description	Action
Ensure that Intune is the MDM Authority or setup Intune as the MDM Authority	8. Click on New provisioning package 

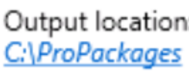
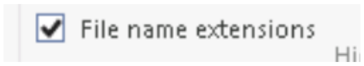
Description	Action
	9. In the New Project dialog, type AddUsers as the Name for your Project 10. Click Browse 11. Navigate to C:\\ 12. Click Make New Folder 13. Type ProPackages as a Name for your folder 14. Click OK 15. Click Next 16. In the Choose which settings to view and configure, click in the Common to all Windows desktop editions radio button 17. Click Next 18. On the Import a Provisioning Package dialog, click Finish 19. Once the Available customizations pane is available, click on All Settings  20. In the dropdown menu, click on Common IT Pro settings  All settings All settings Common OEM settings Common IT Pro settings 21. Expand Runtime Settings 22. Expand Accounts  Accounts ComputerAccount Account AccountOU ComputerName DomainName Password Users 23. Click on Users

Description	Action
	24. In the UserName text box, type W10DemoUser001 25. Click Add 26. In the UserName text box, type W10DemoAdmin002 27. Click Add  Existing Users: UserName: W10DemoUser001 UserName: W10DemoAdmin002 28. Click on UserName: W10DemoUser001 highlighted in Red under the Users node  Users UserName: W10DemoUser001 HomeDir Password 29. Click on Password 30. Type Passw0rd! in the Password text box 31. Click on UserGroup 32. In the UserGroup dropdown menu, click on Standard User  Standard Users NOT CONFIGURED Standard Users Administrators 33. Click on UserName: W10DemoAdmin002 highlighted in Red under the Users node 34. Click on Password 35. Type Passw0rd! in the Password text box 36. Click on UserGroup 37. In the UserGroup dropdown, click on Administrators

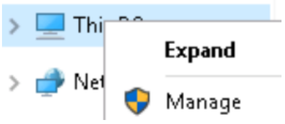
Description	Action
	38. Review your settings in the Selected customizations Pane and notice that settings can be deleted

Deploy the Provisioning Package

Description	Action
Build and Deploy the Provisioning Package	39. Click on Export and then click on Provisioning package  40. In the Describe the Provisioning Package dialog, click on the dropdown menu under Owner and change the value to IT Admin  Owner: OEM Microsoft Silicon vendor OEM System integrator Mobile operator IT Admin 41. Click Next 42. In the Select Security details dialog, uncheck Encrypt package  43. Click Next

Description	Action
	44. Ensure that the Package is saved to the folder created earlier and then click Next 45. On the Build the provisioning package dialog, click Build 46. Click on the link below Output location to open Windows Explorer in the folder where the package is located and then click Finish in the All Done dialog  Output location: C:\ProPackages 47. In the Windows Imaging and Configuration Designer window, click on File > Save 48. Click File > Close project 49. Check that there is an AddUsers project under Recent Projects in the Windows Imaging and Configuration Designer window 50. Minimize the Designer 51. Browse to the folder containing the Provisioning Package 52. Click View and then check the File Name Extensions check box  ☑ File name extensions Hi 53. Copy the AddUsers.ppkg file to the Desktop AddUsers.ppkg

Test the Provisioning Package

Description	Action
Test the package that will add 2 Users. One as an Admin and the other as a Standard User	54. Right-click on This PC and click Manage  55. Expand Local Users and Groups in the Management Window 56. Click on Users 57. Note the Users 58. On the Desktop, double-click on the AddUsers package 59. Click Yes on the User Access Control dialog 60. Click Yes, add it on the Is this package from a source you trust dialog 61. Navigate back to Computer Management 62. Right-click on Users and then click Refresh 63. Right-click on W10DemoAdmin002 and click Properties 64. Click the Member Of tab 65. Ensure that the User is in the Administrators group 66. Repeat for W10DemoUser001 ensuring that the User is a member of Users

#CANITPRO CAMP

Windows 10 and Enterprise Mobility

Create a Password Policy in Windows Intune

Windows Intune allows for the Management of Devices using a Cloud Service. In this lab we will walk through the process of setting a Password Policy using Device Management in Windows Intune.

Table of Contents

Overview

The exercises in this lab will illustrate how to install a custom built Universal App by using PowerShell

You will complete the following objectives.

- Connecting your Device to Windows Intune
- Enabling Microsoft Device Management
- Creating a Password Policy for the Device

Table 1 outlines the requirements for completing this module.

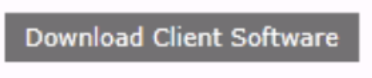
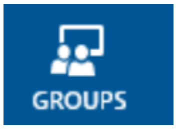
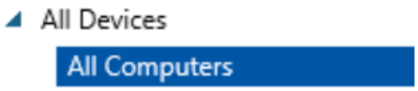
Table 1. Module requirements

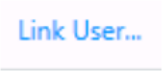
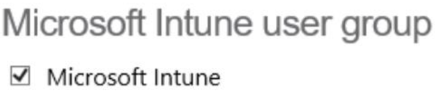
Virtual machines	Physical devices	Subscriptions and accounts
• W10-Client	• No physical devices are required in this module.	• Domain admin account as created in As configured in initial *Trial Account Registration* Exercise

Exercise 1: Create a Password Policy in Windows Intune

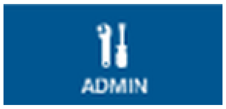
Connect to Windows Intune and Register the Device

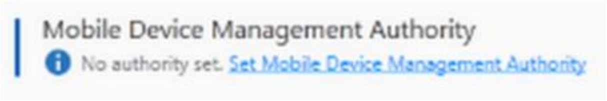
Description	Action
Connect to an Azure Active Directory Joined computer using the credentials of a Domain User	1. The following steps should be performed on the W10-W10Client virtual machine, logged on using your Office 365 Domain Admin credentials 2. Click on the Start button 3. Type Internet Explorer 4. Click on Internet Explorer 5. Navigate to https://account.manage.microsoft.com 6. This will log you into the Windows Intune Portal 7. Right-click on Admin Console and click Open in new tab 8. In the Microsoft Intune Admin Console, click on ADMIN 9. Click on Client Software Download 10. 11. Click on Download Client Software

Description	Action
	 12. Click on Save as 13. Browse to the Desktop 14. Click Save 15. Right-click on the Zip File on the Desktop and click Extract All 16. Accept all the defaults and click Extract 17. In the Folder that opens, double-click on Microsoft_Intune_Setup.exe 18. On the first page of the Wizard, click Next 19. Click Yes in the User Access Control dialog 20. Once the software has installed, click Finish 21. Navigate back to the browser window that has the Windows Intune Console loaded 22. Click on GROUPS  23. Expand All Devices 24. Click on All Computers  25. Click on Devices 26. The computer (WIN10-Client) will be listed

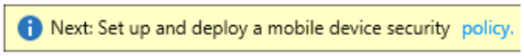
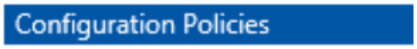
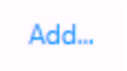
Description	Action
	27. Click on LinkUser  28. In the Link User: Win10-Client1(Computer) dialog, Click on the Admin user 29. Click OK 30. Return to the Account Portal tab 31. Click Users 32. Click on the Name for the Admin account 33. Click in the Microsoft Intune checkbox under Microsoft Intune user group  Microsoft Intune user group ☑ Microsoft Intune 34. Click Save

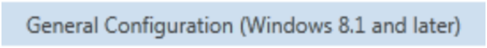
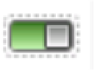
Ensure Intune is the Mobile Device Management Authority

Description	Action
Ensure that Intune is the MDM Authority or setup Intune as the MDM Authority	35. Click ADMIN  36. Click Mobile Device Management 37. If the Window indicates No Authority Set, click Set Mobile Device Management Authority

Description	Action
	 Mobile Device Management Authority No authority set. Set Mobile Device Management Authority 38. In the dialog confirming that you want Intune as the MDM Authority, check the Checkbox and click Yes 39. Intune is now setup as the MDM Authority

Create a Password Policy for the device

Description	Action
Create a Policy for Secure Passwords	40. Click on ADMIN 41. Click on Mobile Device Management 42. Click on the word policy in the sentence Next Set up and deploy a Mobile Device Security Policy  Next: Set up and deploy a mobile device security policy. 43. If not highlighted, click on Configuration Policies  Configuration Policies 44. Click Add  Add... 45. On the Create New Policy dialog, expand Windows

Description	Action
	46. Click on General Configuration Windows 8.1 and later  General Configuration (Windows 8.1 and later) 47. Click Create Policy 48. Type PasswordPolicy for the Name 49. Enter a short description 50. Scroll down and Under Password, click on the Switch for Required Password to Unlock Mobile devices is not Configured  51. Ensure that the value is set to Yes 52. Click on the Switch for Minimum Password Length is not Configured 53. Change the value to 5 54. Click on the Switch for Password Expiration is not configured 55. Change the value to 39 56. Click Save Policy 57. On the Do you want to Deploy this Policy now dialog, Click Yes 58. On the Select the Groups to which you want to Deploy the Policy, Click on All Computers and then Click Add 59. Click OK 60. This policy will now be pushed out to All Computers 61. In the Policy section, Click on Overview and ensure that there are no issues reported

Description	Action
	62. In general a Policy will take around 20 minutes to apply and may require a restart

#CANITPRO CAMP

Windows 10 and Enterprise Mobility

Controlling Updates with Microsoft Intune

Microsoft Intune can help you to secure your managed computers in a number of ways, including the management of software updates that keep your computers up to date by ensuring the latest patches and software updates are quickly installed.

Table of Contents

Overview

The exercises in this lab will illustrate how to install a custom built Universal App by using PowerShell

You will complete the following objectives.

- Log in to Windows Intune
- Create a Policy to Control Updates
- Configure Update Categories and Classifications
- Configure an Automatic Update Approval Rule

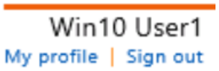
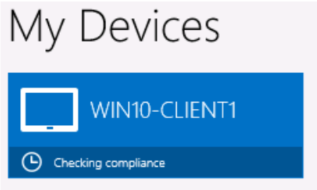
Table 1 outlines the requirements for completing this module.

Table 1. Module requirements

Virtual machines	Physical devices	Subscriptions and accounts
• W10-Client	• No physical devices are required in this module.	• No subscriptions are required for this lab

Exercise 1: Control Updating using Windows Intune

Login to Windows Intune

Description	Action
Connect to Windows Intune using the credentials from the previous lab.	1. The following steps should be performed on the W10-W10Client virtual machine 2. Logon using the credentials that are joined to the Azure Active Directory Domain as per the previous lab. 3. Click on the Start button 4. Type Internet Explorer 5. Click on the Internet Explorer tile 6. Once Internet Explorer launches, navigate to https://account.manage.microsoft.com 7. When Intune signs the User in, Click on Sign Out  8. Click on Use Another Account 9. Sign in using the Admin account setup during the Trials and Subscriptions setup 10. Click on Company Portal 11. Ensure that the Win10-Client1 Device is listed 

Description	Action
	If the device is not listed Click Add Device Click Download Software Click Run Click Next to Start the Setup Wizard Click Finish 12. Return to the original tab and Click on Admin Console Admin Console 13. Click on Policy POLICY

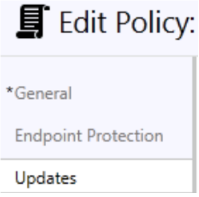
Create a Policy to Control Updates

Description	Action
Create a Policy that will control some of the Update settings available from Microsoft Intune.	14. Click on Add Policy TASKS Add Policy Control features a mobile devices. 15. Expand Computer Management

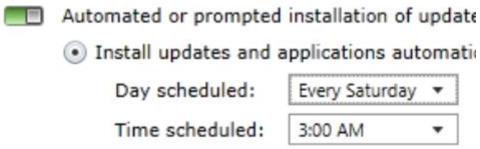
<table>
<tr><th>Description</th><th>Action</th></tr>
<tr><td></td><td>

16. Click on Microsoft Intune Agent Settings

17. Click Create Policy
18. In the Select Groups to which you want to deploy this policy, Click All Computers
19. Click Add
20. Click OK
21. In the Policies list, highlight the Microsoft Intune Agent Settings policy
22. Click Edit
23. Highlight the Name and then Type Update Policy
24. In the pane directly beneath Edit Policy
25. Click Updates



26. In the Update Section
27. Change the Update and application detection frequency to 12 hours
28. Change the Update Schedule to install updates only on weekends



Automated or prompted installation of update

● Install updates and applications automati

Day scheduled: Every Saturday

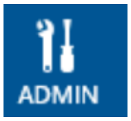
Time scheduled: 3:00 AM

29. Note the remaining settings and leave them as they are currently (default) set

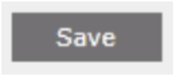
</td></tr>
</table>

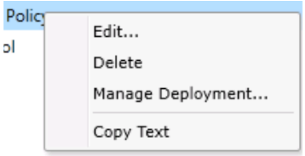
Description	Action
	30. Click Save Policy

Configure Update Categories and Classifications to be made available to Devices

Description	Action
Define the categories and classifications of the updates you want to make available to computers.	31. Click on Admin  32. Click on Updates 33. In the Service Settings: Updates pane, Click on Bing, Visual Studio 2012 and 2013, Microsoft Azure and Microsoft Dynamics CRM 2015 to include them in the products to download updates for 34. Scroll down to Office and uncheck Office, check Office 2010 and 2013 35. In the Update Classification section, Click on Tools

Configure and Automatic Update Approval rule

Description	Action
Create a rule to automatically approve specified types of updates and help reduce your administrative overhead.	36. Scroll down in the Service Settings: Updates pane to Automatic Approval Rules 37. Click New 38. In the Describe the Rule dialog, Type ApprovalRule as the Name 39. Click Next 40. In the Product Categories section, Click Bing 41. Click Next 42. In the Updates Classifications section, Click Critical Updates 43. Click Next 44. In the Deployments section, Click All Computers 45. Click Add 46. Click Next 47. On the Review page, Click Finish 48. In the Service Settings: Updates pane, Click Save  49. Click on Policy 50. Right Click on Update Policy 51. Click on Manage Deployment

Description	Action
	 Policy ol Edit... Delete Manage Deployment... Copy Text 52. In the Select the groups to which you want to deply this policy, All Computers should be listed in Selected Groups 53. Click OK 54. This will push out Updates to devices according to the configuration set in this lab. In the next Lab you will create a Group Policy Object to Manage Servicing Rings in Windows 10

Windows 10 and Enterprise Mobility

Move between Servicing Rings using a Group Policy Object

In the Enterprise, the most common method of configuring Windows Computers is to use Group Policy. Group Policies are settings that are pushed into a computer's registry to configure settings and behaviors that fit the enterprise's operational methodologies. This is one of the advantages of Windows Computers that has been around since Windows NT 4.0 Service Pack 4 and is still the chosen method to manage Windows 10

In this lab, we will use a Group Policy Object (GPO) to move between Service Rings and control how updates are applied or deferred. If you are currently using WSUS or Configuration Manager you can continue to use those technologies and methodologies as you always have.

Microsoft is also introducing Windows Update for Business which is a cloud service designed for End User Devices in businesses and will provide Distribution Rings, Maintenance Windows, Peer to Peer Delivery and all of this will integrate with existing tools like System Center, Orchestrator and Windows Management Instrumentation.

Table of Contents

Overview

The exercises in this lab focus on creating a Group Policy Object that allows the System Administrator to control how updates are applied. Updates in Windows 10 are delivered in an ongoing cadence that offers customers new capabilities as they become available, this is known as Windows as a Service. New security threats, the need for new capabilities and new employee behaviors have started to dictate a different methodology in how systems and computers are managed. In the consumer world there is an acceptance that devices are regularly updated but in a more controlled environment like a hospital or bank updating and system changes need to be controlled and rigidly managed.

Within Microsoft this process is happening in the form of branches. The Engineering team will build out some new functionality and test as a first branch, the changes are then passed on to willing Microsoft users who form the next branch before being passed to the Windows Insider Program branch. At this stage the updates are now being tested by several million users and ready to be passed onto the Current Branch which consists of 100s of millions of users who are generally your pilots and early adopters. This is then passed to Current Branch for Business where organizations can make decisions on how and when they will deploy updates and changes. It is within this branch that you can build your own Rings and do phased deployments into your business or corporate environment. It is possible that the Insider to Current Branch for Business exists within your organization and this is then seen as the pilot, testing and validation which would be similar to the regular update process.

In the addition to the above Windows Enterprise customers with a Volume License Agreement tied to Software Assurance introduces the Long Term Service Branch (LTSB) which mimics the typical method that OS updates are currently handled. Microsoft will release an LTSB version of the OS every 2 to 3 years that integrates the Current Business and Current Branch for Business updates and feature changes and offer it to customers.

For the purposes of this lab the Windows 10 Policy Definitions have been installed on the Domain Controller.

The exercises in this lab include:

- Exercise 1: Windows Update controls in the Settings Menu
- Exercise 2: Create a Group Policy Object to control Update Settings
- Exercise 3: Test the Group Policy Setting

Table 1 lists virtual machines used in this lab.

Table 1. Virtual machines used in this lab

Virtual machine	Description
W10-DC	Domain controller running Windows Server 2012 R2 contoso.com Active Directory (AD) domain. Also provides Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services for the virtual machine environment.
W10-Client	Windows 10 machine under the Management of the Domain Controller
W10-Edge	Virtual Machine configured to provide Internet Access to the virtual machine environment.
W10-Synch	Synchronization Server

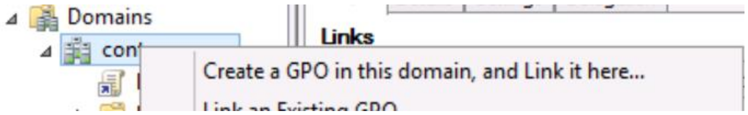
Exercise 1: Create a Group Policy Object to control Service Rings

The Windows Update Settings

Description	Steps
Navigate to the Windows Update Settings Menu	Perform the following steps on W10-Client1 logged on as **Contoso\Administrator** with the password **Passw0rd!**: 1. Click on the **Start Button** 2. Click on **Settings** 3. Click on **Update & security** 4. In the **UPDATE & SECURITY** dialog, Click on **Advanced options** (you may need to scroll down the dialog to find the link) 5. Notice that the current update settings are **Automatic** and the **Defer upgrades** checkbox is currently unchecked.

Configure a Group Policy

Description	Steps
Configure a Group Policy Object that will Defer Upgrades. This will allow you to defer upgrades until the next upgrade period.	Perform the following steps on W10-DC logged on as **Contoso\Administrator** with the password **Passw0rd!**: 6. Minimize the Windows Server Manager dialog 7. Click on the **Start Button** 8. Type **Group Policy** 9. Press **Enter** 10. In the Group Policy Management dialog, Right Click **Contoso.com** under **Domains**

Description	Steps
	11. Click on **Create a GPO in this Domain, and Link it here**  Domains con Links Create a GPO in this domain, and Link it here... Link an Existing GPO 12. In Name, type **WindowsUpdateSettings** 13. Click **OK** 14. Right click **WindowsUpdateSettings** 15. Click **Edit** 16. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update** 17. In the Settings Window, double click on **Defer Upgrade** 18. Click **Enable** 19. Click **Apply** 20. Click **OK** 21. Close the **Group Policy Management Editor**

Test the Group Policy Setting

Description	Steps
Test the Group Policy that was just created.	Perform the following steps on W10-Client logged on as **Contoso\Administrator** with the password **Passw0rd!**: 22. Click on the **Start Button** 23. Type **CMD** 24. Click on **Command Prompt**

Description	Steps
	25. Type **gpupdate /force** and wait for the update to complete 26. Click on the **Start Button** 27. Click **Power** 28. Click **Restart** 29. Log on as **Contoso\Administrator** with the password **Passw0rd!** 30. Click on the **Start Button** 31. Click on **Settings** 32. Click on **Update & security** 33. Click on **Advanced Settings** 34. Notice that the **Defer Upgrades** option is greyed out.