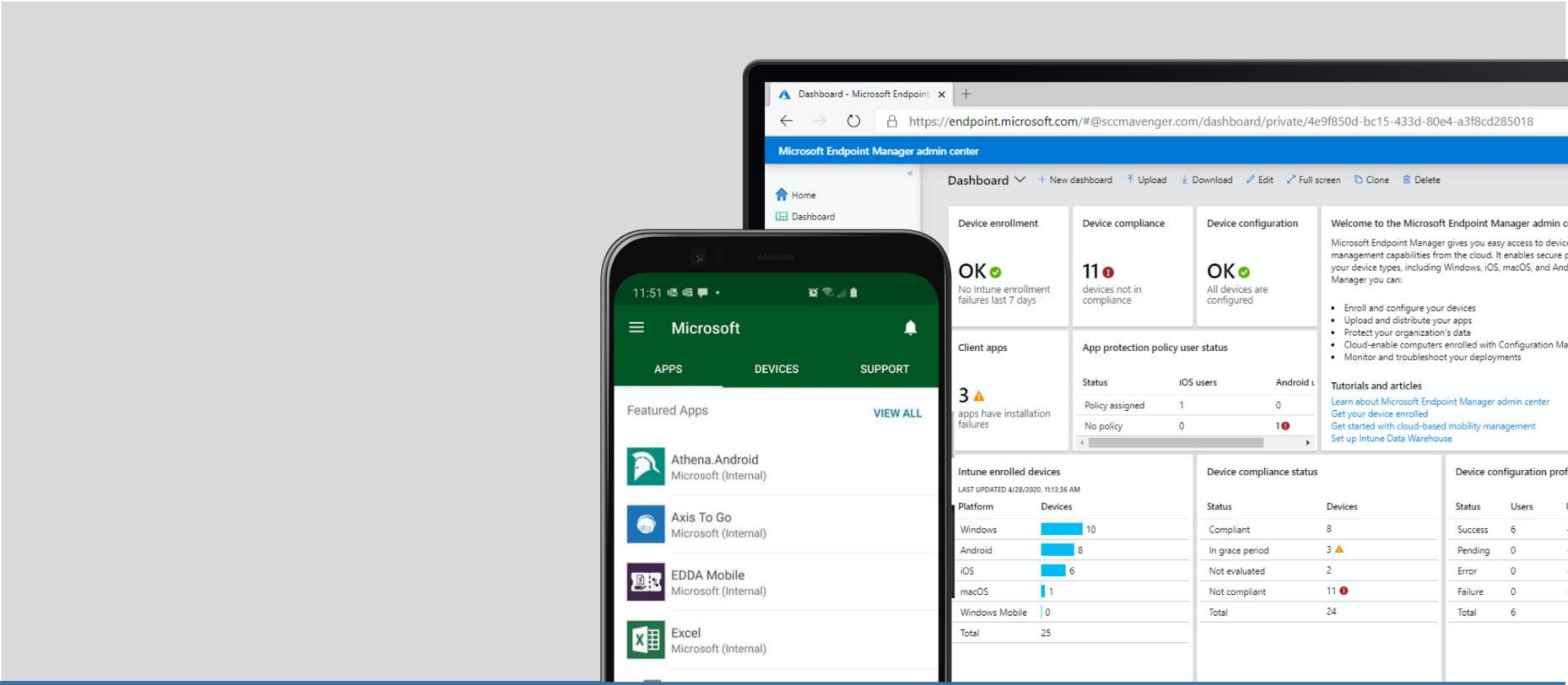


Dashboard - Microsoft Endpoint
https://endpoint.microsoft.com/#@sccmavenger.com/dashboard/private/4e9f850d-bc15-433d-80e4-a3f8cd285018
Microsoft Endpoint Manager admin center
Home
Dashboard
Dashboard
New dashboard
Upload
Download
Edit
Full screen
Clone
Delete
Device enrollment
OK
No Intune enrollment failures last 7 days
Device compliance
11
devices not in compliance
Device configuration
OK
All devices are configured
Client apps
3
apps have installation failures
App protection policy user status
Welcome to the Microsoft Endpoint Manager admin c
Tutorials and articles
Learn about Microsoft Endpoint Manager admin center
Get your device enrolled
Get started with cloud-based mobility management
Set up Intune Data Warehouse
Intune enrolled devices
LAST UPDATED 4/28/2020, 11:13:36 AM
Device compliance status
Device configuration prof
11:51
Microsoft
APPS
DEVICES
SUPPORT
Featured Apps
VIEW ALL
Athena.Android
Microsoft (Internal)
Axis To Go
Microsoft (Internal)
EDDA Mobile
Microsoft (Internal)
Excel
Microsoft (Internal)

Microsoft Endpoint Manager gives you easy access to devic management capabilities from the cloud. It enables secure p your device types, including Windows, iOS, macOS, and And Manager you can:

- Enroll and configure your devices
- Upload and distribute your apps
- Protect your organization's data
- Cloud-enable computers enrolled with Configuration Ma
- Monitor and troubleshoot your deployments

Status	iOS users	Android u
Policy assigned	1	0
No policy	0	1

Platform	Devices
Windows	10
Android	8
iOS	6
macOS	1
Windows Mobile	0
Total	25

Status	Devices
Compliant	8
In grace period	3
Not evaluated	2
Not compliant	11
Total	24

Status	Users
Success	6
Pending	0
Error	0
Failure	0
Total	6

Microsoft Intune and Configuration Manager Evaluation Lab Kit

Microsoft Intune | Microsoft Configuration Manager | Windows 11 | Microsoft 365

Lab Guide

Last Updated: Jan 4, 2023

Table of Contents

1 Introduction

The Microsoft Intune and Configuration Manager Evaluation Lab Kit provides a self-deploying Configuration Manager lab environment that can be integrated a Microsoft Intune trial instance. The lab provides guidance on using this unified platform to deploy and manage Windows 11 and Microsoft 365 Apps for enterprise.

At the end of the lab, you will become familiar with using certain key features of Microsoft Intune and the native integration with Configuration Manager using co-management to manage endpoints in the cloud.

Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints. Intune integrates with other Microsoft products and services that focus on endpoint management, including Configuration Manager for on-premises endpoint management.

You can use Microsoft Intune and Configuration Manager together in a co-management scenario, use tenant attach, or use both. With these options, you get the benefits of the web-based admin center and can use other cloud-based features available in Intune.

This guide is divided into the following eight sections:

1. **Lab Set Up.** This section guides you through the steps required for setting up the on-premises lab environment and joining it to trial versions of Azure and Intune. This will provide you with the full Microsoft 365 infrastructure required to work through all scenarios in the lab.
2. **Plan and prepare infrastructure.** For a successful deployment you must first know what you have. That means taking an inventory of your devices and apps and verifying compatibility. Additionally, this section details how to concurrently manage Windows 11 devices by using both Configuration Manager and Microsoft Intune. Co-management can help you get more out of your existing Configuration Manager deployment by unlocking additional cloud-powered capabilities like conditional access.
3. **Deploying Windows 11.** With everything prepared, the next step is to deploy the OS images. This section will cover deploying Windows 11 using Configuration Manager to both bare metal systems. It also covers Windows 11 deployments using Autopilot.
4. **Servicing Windows 11.** Upgrading to Windows 11, both current and future versions, can be done using Windows Servicing. This section will cover how to use Configuration Manager and Windows Update for Business to upgrade using Windows Servicing.
5. **Managing Windows 11.** This section covers how to manage Windows 11 using Intune. First by enrolling devices, next, configuring Software Updates and other policies that can be enforced using Intune.

6. **Preparing/Deploying Microsoft 365 Apps for enterprise.** Microsoft 365 apps for enterprise is the modern office suite. This section will cover the various ways how Microsoft 365 apps for enterprise can be deployed using Intune, Configuration Manager or local methods. It also covers the different ways to manage and service Microsoft 365 apps for enterprise using each of these tools.
7. **Managing the new Microsoft Edge.** The new Microsoft Edge enhances and extends the browser experience. It runs on Windows, macOS, iOS and Android devices and comes native on Windows 11. This section covers how to deploy the new Microsoft Edge to older versions of Windows 10, how to update it using both Intune and Configuration Manager, and also how to manage policies using both Intune and GPO.
8. **Security and Compliance.** This section covers Windows 11 security capabilities, including BitLocker device encryption, Windows Defender Antivirus and Windows Hello for Business.

Note: The scenarios in this guide were tested using Configuration Manager, Version 2207 and Windows 11, Version 21H2. An updated guide for Windows 11, Version 22H2 and Configuration Manager, Version 2211 will be available soon. This lab guide is not intended to cover all deployment and management tasks and scenarios. For comprehensive guidance, including scenarios that can be tested directly in the lab environment accompanying this lab guide, see: Microsoft 365 documentation.

2 Lab Set Up

It is important that this section be completed after following the steps in the **Lab Set Up Guide** and before proceeding with the lab activities. The following requirements for each environment (on-premises and cloud) to support the labs.

Note: When you are going through the Labs, you might notice that there is repetition of certain steps and conflicts. Therefore, it is recommended that once you are done with a specific lab, reverse the changes made to avoid those conflicts from the VMs and Physical Machines as well as Azure, Intune and Microsoft 365.

2.1 On-Premises Environment

2.1.1 Prerequisites

Listed below are the requirements for the on-premises environment:

Complete	Task
☐	Two (2) **client** devices (one physical and one virtual). • Two (2) devices of the same architecture (64-bit) that can be formatted or do not have a corporate image installed that are compatible with Windows 11 hardware specifications (Windows 11 Specs and System Requirements | Microsoft). These devices will be used for the labs on Windows Autopilot for pre-provisioned deployment (requires a physical device) and Credential Guard.
☐	One (1) **physical** server or workstation to host the virtual lab environment. The requirements are listed below: • **Operating System**: Windows Server 2016/2019/2022, or Windows 10/11 with Hyper-V installed (recommended to use Windows Server OS) and fully updated. Administrative rights on the host. • **Memory**: 16GB RAM (32 GB RAM for optimal performance) • **Disk Space**: At least 150 GB (300 GB for optimal performance) • **Disk Subsystem**: High throughput/speed • **Ethernet**: Two (2) or more Gb NICs. • **Network Connections**: Internet connection and lab switch. • **Applications**: Microsoft Azure PowerShell modules installed (https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-3.8.0).
☐	One (1) gigabit network lab **switch** with sufficient ports to connect client devices and lab environment.

□	Download the latest Windows 11 from MSDN or VLSC.
□	*[OPTIONAL]* Provide the source of any security guidance that is being used with HTML Reports and GPO Backups.

2.1.2 Components

The on-premises environment is configured by using the Windows and Office Deployment Lab Kit, which can be accessed in the Microsoft Evaluation Center here. Follow the Windows and Office **Lab Kit Setup Guide** to provision the virtual machines on Hyper-V.

When setup is complete, the following virtual machines are configured and the deployment lab system is available for use.

Server Name	Roles & Products
HYD-CLIENT1	Windows 11, Version 22H2 Domain Joined
HYD-CLIENT2	Windows 11, Version 22H2 Domain Joined
HYD-CLIENT3	Windows 11, Version 22H2 Workgroup
HYD-CLIENT4	Windows 11, Version 22H2 Workgroup
HYD-CLIENT 5, 6	Bare metal (No Installations)
HYD-CM1	Microsoft Configuration Manager 2211 Windows Deployment Services Windows Assessment and Deployment Kit for Windows 11, Version 22H2 Windows Software Update Services Microsoft SQL Server 2017
HYD-DC1	Active Directory Domain Controller, DNS, DHCP, Certificate Services
HYD-GW1	Remote Access for Internet Connectivity
HYD-INET1	Simulated Internet
HYD-VPN1	Remote Access for VPN

2.1.3 Credentials

The table below lists the credentials and access type available for all servers and clients in the default implementation:

User	Access Type	User Name	Password
Local Administrator	Administrative	Administrator	P@ssw0rd
Domain Administrator	Enterprise Administrator	CORP\LabAdmin	P@ssw0rd

2.2 Cloud Environment

Certain lab scenarios require the cloud environment. Follow the steps below to configure and prepare the required cloud services.

Listed below are the requirements for the cloud environment used for various labs in this guide.

Complete	Task
□	Provide licensed **subscriptions** or sign-up for a trial subscription for the following Microsoft Cloud Services. • **Microsoft Azure**: https://azure.microsoft.com/en-us/free/ • **Enterprise Mobility + Security:** http://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-trial (configured as part of the Lab Setup) • **Windows Defender Advanced Threat Protection:** http://www.microsoft.com/en-us/WindowsForBusiness/windows-atp (configured as part of the Lab Setup) • **Microsoft 365 E3:** Configured as part of the Lab Setup. **Note**: All trial tenants have an evaluation period. These subscriptions/tenants will expire unless they are extended or if the customer purchases the system. **Note**: An appropriate MSDN subscription could be used to activate the Azure Benefit for 30 days.

2.2.1 Set up Azure and Microsoft 365

In this section, you will create an Azure AD and a Microsoft 365 Trial Tenant used for the later lab environment.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Create Azure AD	**Note:** If Azure AD is already present and associated with a Subscription, then skip this section. 1. Open an InPrivate Browser session. 2. Navigate to https://portal.azure.com 3. Sign in with the **email address** associated with your Azure subscription. 4. On the left navigation bar, click **Create a resource** > **Identity** > **Azure Active Directory**. 5. In the Create directory pane fill in the following values: ORGANIZATION NAME: **<CompanyName>** INITIAL DOMAIN NAME: **<AzureDomainName>** COUNTRY OR REGION: **Choose a region** 6. Click **Create**.

Note: This may take a couple of minutes to complete.

Create Azure AD Admin User

7. Sign out from Azure portal and sign back in again.
8. Click your **email address** on the upper right corner and click **Switch directory**. Select **<AzureDomainName>.onmicrosoft.com**. If required, refresh the page for the directory to be visible.
9. On the left navigation bar, click **Azure Active Directory**.
10. Click **Users** and then click **+ New user**.
11. In the New user pane, fill in the following values:
    USER NAME: **<LabAdmin>** (Suggestion: LabAdmin@<AzureDomainName>.onmicrosoft.com)
    NAME: **<Admin Name>**
    FIRST NAME: Enter the first name
    LAST NAME: Enter the last name
12. Select **Auto-generate password** and select **Show Password** and write down the temporary password **<OldLabAdminPassword>**.
13. Click on **User** next to **Roles**, select **Global administrator** and **Desktop Analytics administrator**, then click **Select**.

Note: The Desktop Analytics administrator role is required here for the Desktop Analytics scenario only.

14. Click **Create**.

Resetting the Password

15. Logout from Azure Portal.
16. Log in to Azure Portal using **LabAdmin** account.
17. Type in the **<OldLabAdminPassword>** that you wrote down.
18. Type the new password: **<NewLabAdminPassword>**.
19. Confirm the new password and sign in.

Associate a Subscription with the New Azure AD Tenant

Note: If Azure AD is already present and associated with a Subscription, then skip this section.

20. Click **All services > Subscriptions**.
21. Click **Add** to add a new subscription to the new Azure AD Tenant.
22. If you are eligible for a Free Trial, then click **Free Trial** or select any other offer from the list.
23. Follow the instructions for **Azure – Sign up**.
24. At the end you must be able to see a valid Active Subscription with a Subscription ID in the **All services > Subscriptions** pane.

Subscribe to Microsoft 365 E3 Trial Subscription

25. Open a new tab and navigate to https://portal.office.com.
26. Click the **Admin** tile.
27. Click **Billing | Purchase services**.
28. Search for and select **Microsoft 365 E3** and then click **Get free trial**.

	29. Follow the usual procedure for verification and click **Try now | Continue**. You should now be able to see the subscription under **Billing | Your products**.
Create Azure Test Users	30. Navigate to [https://portal.azure.com.](https://portal.azure.com) 31. Sign in with the email address associated with your Azure subscription if required. 32. On the left navigation bar, click **Azure Active Directory**. 33. Click **Users** and then click **+ New user**. 34. In the New user pane, fill in the following values: USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com** NAME: **Test User1** FIRST NAME: Enter the first name LAST NAME: Enter the last name 35. Select **Auto-generate password** and select **Show Password** and write down the temporary password. 36. Click **Create**. 37. Repeat **Steps 30 – 36** for a second user as follows: USER NAME: **TU2@<AzureDomainName>.onmicrosoft.com** NAME: **Test User2** FIRST NAME: Enter the first name LAST NAME: Enter the last name
Set Password for your New Users using Microsoft 365	38. Close all browser windows. 39. Start Edge InPrivate mode. 40. Navigate to [https://login.microsoftonline.com.](https://login.microsoftonline.com) 41. Log in with the user account created **TU1@<AzureDomainName>.onmicrosoft.com** 42. Type in the **temporary password** that you wrote down. 43. Type the New Password: **<newuserpassword>** 44. Confirm the new Password: **<newuserpassword>** 45. Click **Sign in**. 46. Repeat **Steps 38-45** for **TU2@<AzureDomainName>.onmicrosoft.com** 47. Close all browser windows.
Create Azure AD Group (Sales)	48. Open an InPrivate Browser session. 49. Navigate to https://portal.azure.com 50. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 51. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 52. Click **+ New group**. 53. In the New Group pane fill in the following values: Group type: **Microsoft 365** Group name: **Sales** Membership type: **Assigned** Members: **Test User1** and **Test User2**

	54. Click **Create**.

2.2.2 Set up Enterprise Mobility + Security

In this section, you will create an Intune Trial Tenant that will be used later on in the lab. This tenant will be created using the Azure AD that you created in the previous lab.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Sign Up for a Trial Microsoft Intune Subscription	1. Start a new Edge window in private mode. 2. Navigate to https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-trial and click **Free trial** and then click **Sign in**. 3. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. Click **Try now** to confirm your order. 5. Click **Continue**. 6. On the left navigation bar, click **Billing > Your products** and verify that the **Enterprise Mobility + Security E5 Trial** is **Active**.

2.2.3 Enable and Configure Cloud Services

In the section, you will assign licenses and configure additional cloud services that will be used in the lab environment.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Assign Microsoft 365 E3 and EM+S Licenses	1. Close all browser windows. 2. Start Edge InPrivate mode. 3. Navigate to https://portal.office.com and **Sign in** with **labadmin@<AzureDomainName>.onmicrosoft.com**. Click the **Admin** tile. 4. On the left navigation bar, click **Users > Active users**. 5. Select all **LabAdmin**, **Test User1** and **Test User2** then click the **Manage product licenses** action by clicking the (**…**). Select **Add to existing product license assignments** and click **Next**. 6. Select the appropriate **Location**, enable **Microsoft 365 E3** and **Enterprise Mobility + Security E5**. 7. Ensure all the checkboxes are selected. Ignore the checkboxes which are greyed out or cannot be selected. 8. Click **Add** and then click **Close**. **Note:** Ensure that all the 3 users have all the product licenses assigned.

Enable Device Registration	9. Close all browser windows. 10. Open an **InPrivate Browser** session. 11. Navigate to https://portal.azure.com. 12. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 13. On the left navigation bar, click **Azure Active Directory > Devices > Device settings**. 14. In the **Users may join devices to Azure AD** setting, select **All** if not selected. 15. In the **Users may register their devices with Azure AD** setting, select **All**. **Note:** Enrollment with Microsoft Intune or Mobile Device Management for Office 365 requires Device Registration. If you have configured either of these services, **All** will already be selected and the button will be disabled. 16. Click **Save**.
Enable Windows Defender ATP Trial	**Note**: A trial application should have been started before proceeding with the steps - https://www.microsoft.com/en-us/windowsforbusiness/windows-atp 17. Close all browser windows. 18. Open an InPrivate Browser session. 19. Navigate to https://www.microsoft.com/en-us/windowsforbusiness/windows-atp and click **Start free trial**. 20. On the **Let's get you started** step, sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 21. On the **Check out, confirm your order** page, click **Try now**. 22. Click **Continue**. 23. Close all browser windows.

2.2.4 Configure Azure AD Connect with Device Sync

In this activity, you will configure Azure AD Connect on DC1.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	

Configure Azure AD Connect

1. Click **Start > Windows Administrative Tools > Active Directory Domains and Trusts**. Right-click **Active Directory Domains and Trusts** and click **Properties**. In the **UPN Suffixes** tab, enter **<AzureDomainName>.onmicrosoft.com** and remove **contoso.com**. Click **Add** and click **Apply** and **OK**.
2. Click **Start > Windows Administrative Tools > Active Directory Users and Computers**.
3. Navigate to **corp.contoso.com > Users** and double-click **LabAdmin**. Click the **Account** tab and under **User logon name**, enter **LabAdmin** and in the drop down select **<AzureDomainName>.onmicrosoft.com**. Click **Apply** and **OK**.
4. Download **Azure AD Connect** from https://www.microsoft.com/en-us/download/details.aspx?id=47594
5. Run **Azure AD Connect** and select **I agree to the license terms and privacy notice** and click **Continue**. Accept the UAC prompt.
6. Select **Use express settings**.
7. In the **Connect to Azure AD** prompt, sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**.
8. In the **Connect to AD DS** prompt enter the following and click **Next**.
   USERNAME: **CORP\LabAdmin**
   PASSWORD: **P@ssw0rd**
9. On the **Azure AD sign-in configuration** page, ensure that the UPN suffix added in **Step 1** is listed and then select **Continue without matching all UPN suffixes to verified domains** and click **Next**.
10. On the **Ready to configure** page, keep the checkbox checked next to **Start the synchronization process when configuration completes** and click **Install**. Click **Exit** once synchronization is complete.

Configure Device Sync

11. Open **Apps and Features** and uninstall the **Windows Azure Active Directory Module for Windows PowerShell**. Accept the UAC prompt.
12. Open PowerShell as an administrator. Accept the UAC prompt.
13. Create a directory in **C drive**, example **C:\MSOnline**.
14. Run the below cmdlet and accept any prompts.
    ```
    Save-Script -Name MSOnline -Path C:\MSOnline\
    ```
15. Run the below cmdlet and accept any prompts.
    ```
    Install-Module  -Name MSOnline
    ```
16. Locate the name of the **AAD Connector Account** by opening the **Azure AD Connect** and clicking **Configure** and selecting **View or export current configuration** and then clicking **Next**. Click **Exit**.

Confirm Devices are Hybrid Azure AD Joined

17. Start Edge InPrivate mode.
18. Navigate to https://portal.azure.com and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.**
19. On the left navigation bar, click **Azure Active Directory**.
20. Select **Devices** > **All devices**.

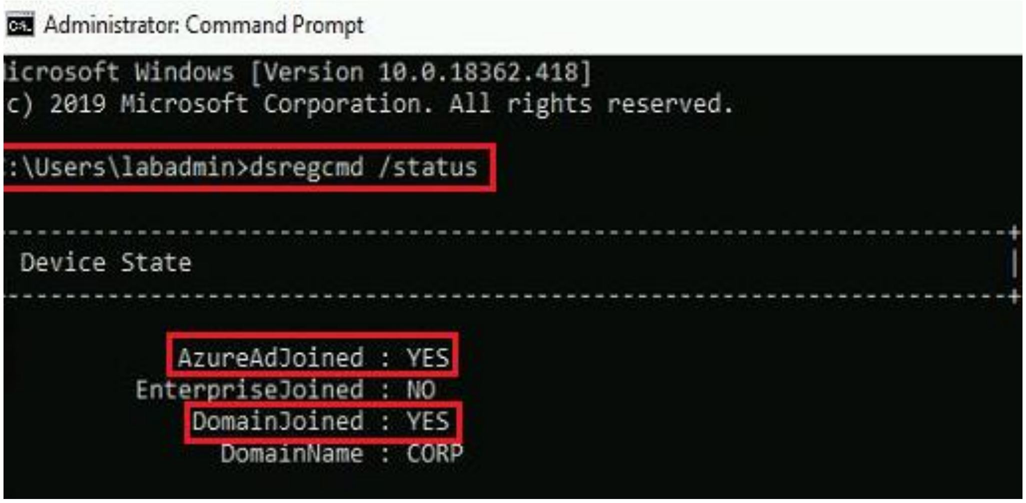
21. Confirm devices are registered to Azure AD.

Note: In case the On-Prem Domain-Joined Clients do not show up in Azure AD, perform the following steps:

22. Disable the firewall mode in **DC1** if not done already.
23. Open **Azure AD Connect** and click **Configure**.
24. Select **Configure device options** and click **Next**.
25. Click **Next** again.
26. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**.
27. Select **Configure Hybrid Azure AD join** and click **Next**.
28. Select **Windows 10 or later domain-joined devices** and click **Next**.
29. Check the box next to **corp.contoso.com** and click **Add**.
30. Sign in with **CORP\LabAdmin** and **P@ssw0rd** and click **OK**.
31. Click **Next**.
32. Click **Configure**.
33. Click **Exit** once done.
34. Open **Azure AD Connect** and click **Configure**.
35. Select **Customize synchronization options** and click **Next**.
36. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**.
37. Click **Next** again.
38. Click **Next** again.
39. Ensure that **Password hash synchronization** is selected. Also select **Password writeback** and click **Next**.
40. Ensure that **Start the synchronization process when configuration completes** is selected and click **Configure**. Click **Exit** once done.
41. Open **Azure AD Connect** and click **Configure**.
42. Select **Change user sign-in** and click **Next**.
43. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**.
44. Select **Pass-through authentication** and ensure that **Enable single sign-on** is selected and then click **Next**.
45. Click **Enter credentials** and enter **CORP\LabAdmin** and **P@ssw0rd**. Click **OK**. Click **Next**.
46. Ensure that **Start the synchronization process when configuration completes** is selected and click **Configure**. Click **Exit** once done.
47. Follow **Steps 16-20** above specially to confirm the On-Prem Domain-Joined Clients show up in Azure AD. Please note, it may take some time (15-30 minutes) for the machines to appear in the console.

Note: Log in to any **Windows 11 Enterprise Version 22H2 VM** as **labadmin@<AzureDomainName>.onmicrosoft.com** with the password **P@ssw0rd**.

On the client side, the **dsregcmd /status** command will give the following results to determine that the device is Hybrid Azure AD Joined. For more information, refer to https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current:



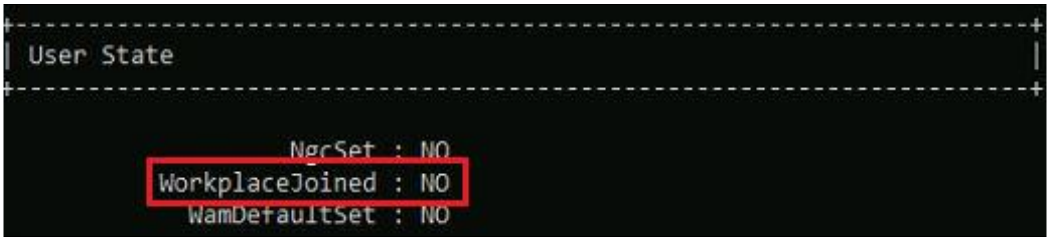
Administrator: Command Prompt

```
icrosoft Windows [Version 10.0.18362.418]
c) 2019 Microsoft Corporation. All rights reserved.

:\Users\labadmin>dsregcmd /status

----------------------------------------------------------------------+
 Device State                                                         |
----------------------------------------------------------------------+

           AzureAdJoined : YES
        EnterpriseJoined : NO
            DomainJoined : YES
              DomainName : CORP
```



```
+----------------------------------------------------------------------+
| User State                                                           |
+----------------------------------------------------------------------+

                  NgcSet : NO
         WorkplaceJoined : NO
           WamDefaultSet : NO
```

Note: If the clients are showing **Pending** under the **Registered** column in the Azure Portal for a long time, to instantly register, run the command **dsregcmd /join** from the client side.

2.3 On-Premises Environment Setup

Perform once the cloud services provisioning is complete.

2.3.1 Servicing Configuration Manager

Configuration Manager uses an in-console service method called Updates and Servicing that makes it easy to locate and then install recommended updates for your Configuration Manager infrastructure. This in-console servicing method is supplemented by out-of-band updates such as hotfixes that are intended for customers who need to resolve issues that might be specific to their environment. These in-console updates replace on-premises update delivery methods.

In this section, you will learn how to use the Configuration Manager console to locate and install updates that provide fixes and new capabilities to your Configuration Manager infrastructure and clients.

2.3.2 Configure as Online Mode

In this activity, you will locate and install Configuration Manager updates from the internet-connected site server. Follow this activity if your environment **has an internet connection** (if not, move to the next activity).

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Enable Service Connection Point (if already not installed)	1. Open the **Configuration Manager Console** from the Start Menu. 2. In the Warning dialog box, click **OK** if it appears. 3. Browse to **Administration > Site Configuration > Servers and Site System Roles**. 4. Select **\\CM1.corp.contoso.com** and verify that the **Service connection point** is listed under **Site System Roles**. 5. If not, add it by right-clicking on **\\CM1.corp.contoso.com** and select **Add Site System Roles**. 6. In the **General** page, click **Next**. 7. In the **Proxy** page, click **Next**. 8. In the **System Role Selection** page, select **Service connection point** and click **Next**. 9. In the **Service Connection Mode** page, select **Online, persistent connection (recommended)** then click **Next**. 10. In the **Summary** page, click **Next**. 11. In the **Completion** page, click **Close**.
Optionally Install New Updates (if available)	Optionally perform the succeeding steps if there is a newer Configuration Manager build available. Otherwise, proceed to **Section** Error! Reference source not found.. **<u>Note</u>**: If the update installation is suspended at "**Downloading**" state for extended period of time, restart the **SMS_EXECUTIVE** (smsexec) service. 1. In the **Configuration Manager Console**, browse to **Administration > Updates and Servicing**. **<u>Note:</u>** It will first download the update before it is made Available. If already not downloaded, then select **Configuration Manager 2xxx** and then click **Download**. Click **OK**. 2. In the **Updates and Servicing** pane, select an **Available** update (**Configuration Manager 2xxx**) and then click **Install Update Pack**. 3. In the **General** page, select **Ignore any prerequisite check warnings and install this update regardless of missing requirements** and click **Next**. 4. In the **Features** page, select **all** available features then click **Next**. 5. In the **Client Update Options** page, click **Next**.

	6. In the **License Terms** page, select **I accept these License Terms and Privacy Statement** and click **Next**. 7. In the **Cloud attach** page, unselect **Enable Microsoft Endpoint Manager admin center** and unselect **Enable automatic client enrollment for co-management** and click **Next**. **Note:** These will be configured in later sections of the lab. 8. In the **Summary** page, click **Next**. 9. In the **Completion** page, click **Close**. **Note**: The 2xxx upgrade installation may take up to an hour.
Upgrade the Configuration Manager Console and Validate Version Number	10. In the **Configuration Manager Console**, browse to **Administration > Site Configuration > Sites**. 11. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 12. In the Warning window, click **OK** to upgrade the Configuration Manager Console. **Note:** At this stage, the Configuration Manager Console will close. The update will be downloaded and installed and the Configuration Manager Console will be reopened. Click **OK** if there are any hotfixes pertaining to (**Configuration Manager 2xxx**) available. 13. In the **Updates and Servicing** pane, confirm that the update (**Configuration Manager 2xxx**) is Installed. **Note:** Install any available hotfixes pertaining to (**Configuration Manager 2xxx**). 14. After the upgrade, in the **Configuration Manager Console**, browse to **Administration > Site Configuration > Sites**. 15. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 16. Validate that the **Version** or **Build Number** was updated (for Configuration Manager 2xxx). 17. Reboot **CM1** once.

2.3.3 Configure as Offline Mode *(OPTIONAL)*

In the activity, you will locate and install Configuration Manager updates from another computer that has internet connection. Follow this section if your environment has **no internet connection**.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Enable Service Connection Point (if already not installed)	1. Open the **Configuration Manager Console** from the Start Menu. 2. In the Warning dialog box, click **OK** if it appears. 3. Browse to **Administration > Site Configuration > Servers and Site System Roles**. 4. Right-click on **\\CM1.corp.contoso.com** and select **Add Site System Roles**.

	5. In the **General** page, click **Next**. 6. In the **Proxy** page, click **Next**. 7. In the **System Role Selection** page, select **Service connection point** and click **Next**. 8. In the **Service Connection Mode** page, select **Offline, on-demand connection** then click **Next**. 9. In the **Summary** page, click **Next**. 10. In the **Completion** page, click **Close**.
Prepare Usage Data	11. Download and extract the EXE from https://www.microsoft.com/en-in/evalcenter/evaluate-system-center-configuration-manager-and-endpoint-protection and copy the folder **ServiceConnectionTool** from **SMSSETUP\Tools** to **C:\**. 12. From the **Start** button, open an **Administrative Command Prompt** and enter **cd /d C:\ServiceConnectionTool**. 13. **Execute** the following command: **serviceconnectiontool.exe -prepare -usagedatadest .\UsageData.cab**
Upload Usage Data and Download Updates from an Internet-connected Remote Computer	14. **Copy** the folder **C:\ServiceConnectionTool** from **CM1** to the root drive of the computer that has **internet connection**. 15. From the computer that has internet connection, open an **Administrative Command Prompt** and browse to the copied **ServiceConnectionTool** folder. 16. **Execute** the following command: **md .\UpdatePacks** 17. **Execute** the following command: **Serviceconnectiontool.exe -connect -usagedatasrc .\UsageData.cab updatepackdest .\UpdatePacks**
Import Updates	18. From the computer that has **internet connection**, copy the **UpdatePacks** folder to **CM1** in the folder **C:\ServiceConnectionTool**. 19. From the **Start** button, open an **Administrative Command Prompt** and enter **cd /d C:\ServiceConnectionTool**. 20. **Execute** the following command: **serviceconnectiontool.exe -import -updatepacksrc .\UpdatePacks**
Force Refresh	21. In the **Configuration Manager Console**, browse to **Monitoring > System Status > Component Status**. 22. In the ribbon, select **Start > Configuration Manager Service Manager**. 23. In the **Configuration Manager Service Manager** window, expand **CHQ > Components > SMS_EXECUTIVE**. 24. On the right pane, **right-click** on **SMS_EXECUTIVE** and select **Stop**. 25. Right-click on **SMS_EXECUTIVE** and select **Query**. 26. Once the **Status** of SMS_EXECUTIVE changes to **Stopped**, **right-click SMS_EXECUTIVE** and select **Start**.

Install New Updates (if available)	**Note**: Perform the succeeding steps if there is a newer Configuration Manager build available after 2002. Otherwise, proceed to section **3.3.2**. 27. In the **Configuration Manager Console**, browse to **Administration > Updates and Servicing**. 28. In the **Updates and Servicing** pane, select the **Configuration Manager 2xxx** update and then click **Install Update Pack**. 29. In the **General** page, click **Next**. 30. In the **Features** page, select **all** available features then click **Next**. 31. In the **Client Update Options** page, click **Next**. 32. In the **License Terms** page, select **I accept these License Terms and Privacy Statement** and click **Next**. 33. In the **Summary** page, click **Next**. 34. In the **Completion** page, click **Close**. **Note**: The 2xxx upgrade installation may take up to an hour.
Upgrade the Configuration Manager Console and Validate Version Number	35. In the **Configuration Manager Console**, browse to **Administration > Site Configuration > Sites**. 36. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 37. In the Warning window, click **OK** to upgrade the Configuration Manager Console. **Note:** At this stage, the Configuration Manager Console will close. The update will be downloaded and installed and the Configuration Manager Console will be reopened. Click **OK** if there are any hotfixes pertaining to (**Configuration Manager 2xxx**) available. 38. In the **Updates and Servicing** pane, confirm that the update (**Configuration Manager 2xxx**) is Installed. **Note:** Install any available hotfixes pertaining to (**Configuration Manager 2xxx**). 39. In the **Configuration Manager Console**, browse to **Administration > Site Configuration > Sites**. 40. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 41. Validate that the **Version** or **Build Number** was updated (for Configuration Manager 2xxx). 42. Reboot **CM1** once.

2.3.4 Prepare Configuration Manager (if not already configured)

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure and Validate Discovery Methods	1. Open the **Configuration Manager Console** from the Start Menu. 2. Navigate to **Administration > Hierarchy Configuration > Discovery Methods**. 3. Right-click **Active Directory Forest Discovery** and click **Properties**. 4. Check the box next to **Automatically create Active Directory site boundaries when they are discovered** and uncheck the box next to **Automatically create IP address range boundaries for IP subnets when they are discovered**. 5. Click **Apply** and then click **OK**. 6. Click on **Active Directory Forest Discovery** and select **Run Forest Discovery Now** from the ribbon bar. 7. Click **Yes** on the dialog box. 8. Right-click **Active Directory Group Discovery** and click **Properties**. 9. Double-click the discovery scope already present. 10. Select the option **Specify an account** and click **Set… > New Account**. 11. Enter the User name: **CORP\LabAdmin**, Password: **P@ssw0rd** and Confirm password: **P@ssw0rd**, click **Verify** and test the connection to the Active Directory Data source Path: **LDAP://DC=corp,DC=contoso,DC=com**, click **OK** on the prompt once successful. Click **OK**. Click **OK** again. 12. Click the **Options** tab and select the checkboxes next to **Only discover computers that have logged on to a domain in a given period of time**, **Only discover computers that have updated their computer account password in a given period of time** and **Discover the membership of distribution groups**. 13. Click **Apply** and then click **OK**. 14. Click on **Active Directory Group Discovery** and select **Run Full Discovery Now** from the ribbon bar. 15. Click **Yes** on the dialog box. 16. Right-click **Active Directory System Discovery** and click **Properties**. 17. Double-click the active directory container already present. 18. Check the box next to **Discover objects within Active Directory groups**. 19. Select the option **Specify an account**, click **Set**… > **Existing Account**. 20. In the **Select Account** window, select **corp\labadmin** then click **OK** twice. 21. Click **Apply** and then click **OK**. 22. Click on **Active Directory System Discovery** and select **Run Full Discovery Now** from the ribbon bar. 23. Click **Yes** on the dialog box. 24. Right-click **Active Directory User Discovery** and click **Properties**. 25. Double-click the active directory container already present. 26. Check the box next to **Discover objects within Active Directory groups**. 27. Select the option **Specify an account**, click **Set**… > **Existing Account**.

	28. In the **Select Account** window, select **corp\labadmin** then click **OK** twice. 29. Click **Apply** and then click **OK**. 30. Click on **Active Directory User Discovery** and select **Run Full Discovery Now** from the ribbon bar. 31. Click **Yes** on the dialog box. 32. Ensure that **Heartbeat Discovery** is already **Enabled**.
Configure and Validate Boundaries	33. Navigate to **Administration > Hierarchy Configuration > Boundaries**. 34. Ensure that the **Default-First-Site-Name** boundary is already created. 35. Navigate to **Administration > Hierarchy Configuration > Boundary Groups**. 36. Ensure that the **Corp Boundary Group** is already created.
Configure an IP Based Boundary	37. First, in **DC1**, click **Start > Windows Administrative Tools > Active Directory Sites and Services**. 38. Expand **Sites**, right-click **Subnets** and then click **New Subnet**. 39. In the **Prefix** field, enter **10.0.0.0/24**, select **Default-First-Site-Name** and then click **OK**. 40. Back in **CM1**, navigate to **Administration > Hierarchy Configuration > Boundaries**. 41. Right-click **Boundaries** and click **Create Boundary**. 42. In the **Description** field enter **IP Based Boundary**, for **Type** select **IP subnet**, in the **Network** field enter **10.0.0.0** and in the **Subnet mask** field enter **255.255.255.0**. 43. Click the **Boundary Groups** tab and click **Add**. 44. Select **Corp Boundary Group** and click **OK**. 45. Click **Apply** and click **OK**.
Configure Boundary Group and DP Group for the DP	46. Navigate to **Administration | Distribution Points**. 47. Right-click the distribution point and click **Properties**. 48. Click the **Group Relationships** tab and click **Add**. 49. Select **Corp DPs** and click **OK**. 50. Click the **Boundary Groups** tab. 51. Click **Add**. 52. Select **Corp Boundary Group** and click **OK**. 53. Click **Apply** and click **OK**.
Configure and Validate the Network Access Account	54. Navigate to **Administration > Site Configuration > Sites**, right-click the site and select **Configure Site Components > Software Distribution**. 55. Click the **Network Access Account** tab. You will see a network access account already in the list. Select and click the **cross** button to delete it. 56. Click **Yes** on the prompt. 57. Click the **star** and click **New Account**.

	58. Enter the User name: **CORP\LabAdmin**; Password and Confirm password: **P@ssw0rd**; click **Verify** and in the Network share: enter **\\cm1\SMS_CHQ**; click **Test connection** and click **OK** once successful. Click **OK** again. 59. Click **Apply** and then click **OK**.
Configure and Validate the Client Push Installation	60. Navigate to **Administration > Site Configuration > Sites**. 61. Right-click on the **CHQ** site then select **Client Installation Settings > Client Push Installation**. 62. In the **General** tab, select **Enable automatic site-wide client push installation** and **Allow connection fallback to NTLM**. Ensure that **Servers** and **Workstations** are checked and **Never install the Configuration Manager client on domain controllers unless specified in the Client Push Installation Wizard** is selected. 63. In the **Accounts** tab, Click the **star** button and click **Existing Account**. 64. In the **Select Account** window, select **corp\labadmin** then click **OK.** 65. Review the **Installation Properties** tab. Click **Apply** and then click **OK**.

2.3.5 Create Test VMs

2.3.5.1 Download MSDN ISO

These ISOs will be used to create VMs that will be used in various chapters within the lab.

Note: The trial download of the Windows Enterprise media does not allow an In-Place Upgrade to be performed. To complete this lab, both the Windows 10 Enterprise media and the Windows 11 Enterprise media must be sourced from either MSDN Subscriber Downloads or from the Volume Licensing Site of the customer.

Task	Detailed Steps
Complete these steps on the HYPER-V Host.	
Download Windows 10 21H2 ISO (MSDN)	1. Open Edge and browse to the URL below. https://msdn.microsoft.com/subscriptions/securedownloads/ 2. From the website, Sign-in with your MSDN registered account. 3. On the **Search** field, enter **Windows 10 (business editions), version 21H2**. 4. **Search** for the latest (English) release (updated MMM YYYY) and **Download** to a location that can be accessed by the lab.
Download Windows 11 (latest) ISO (MSDN)	5. Open Edge and browse to the URL below. https://msdn.microsoft.com/subscriptions/securedownloads/ 6. From the website, Sign-in with your MSDN registered account. 7. On the **Search** field, enter **Windows 11 (business editions)**.

	8. **Search** for the latest (English) release (updated MMM YYYY) and **Download** to a location that can be accessed by the lab.

2.3.5.2 Build a Windows 10 21H2 Client Virtual Machine

<u>Note:</u> The **WIN10 (CLIENT7)** VM will be used for the following scenarios in this Lab Guide:

- Section **Error! Reference source not found.** – **Error! Reference source not found.**
- Section **Error! Reference source not found.** - **Error! Reference source not found.**
- Section **Error! Reference source not found.** - **Error! Reference source not found.**

Task	Detailed Steps
Complete these steps on the Hyper-V Host and the New Generation 2 virtual machine.	
Create the Virtual Machine	1. On the Hyper-V Host server, launch **Hyper-V Manager**. 2. Under **Actions**, click **New > Virtual Machine**. 3. On the **Before You Begin** page, click **Next**. 4. On the **Specify Name and Location** page, provide a name (e.g. **CLIENT7**). Based on where you want to store virtual machine files, click **Store the virtual machine in a different location** and **Browse** to that specific location. Click **Next**. 5. On the **Specify Generation** page, select **Generation 2** and click **Next**. 6. On the **Assign Memory** page, provide a Startup memory of **4096 MB** or more and click **Next**. 7. On the **Configure Networking** page, in the Connection drop-down, select **HYD-CorpNet** and click **Next**. 8. On the **Connect Virtual Hard Disk** page, keep the defaults and click **Next**. 9. On the **Installation Options** page, select **Install an operating system from a bootable image file** and **Browse** to the Windows 10 21H2 ISO that was downloaded in **Section** Error! Reference source not found.. 10. On the **Summary** page, review and click **Finish**. 11. Right-click on the name of the new VM (e.g. **CLIENT7**) and select **Settings**. 12. Under the **Hardware** section, click on **Security** and then select **Enable Trusted Platform Module**. 13. Under the **Hardware** section, click on **Processor** and then increase the **Number of virtual processors** to **2**. Click **Apply** and then **OK**. 14. Click **Start** to turn on the VM and proceed with the installation. Join the system to the **corp.contoso.com** domain using the domain administrator credentials (**corp\labadmin**). 15. Log in as **CORP\LabAdmin** and then turn off the **Windows Defender Firewall Mode** for **Domain networks, Private networks and Guest or public networks**. Right-click on the **Start** button, click **Run** and enter **firewall.cpl**. Click **Turn**

	Windows Defender Firewall on or off and then select **Turn off Windows Defender Firewall** for **Domain networks, Private networks and Guest or public networks**. Click **OK**.
Complete these steps on the CM1 virtual machine.	
Install the Configuration Manager Client	16. Once the system has joined the domain, log on to **CM1** virtual machine. 17. Launch the Configuration Manager Console and navigate to **Administration > Overview > Hierarchy Configuration >Discovery Methods**. 18. Select **Active Directory System Discovery** and click **Run Full Discovery Now**. Click **Yes** on the prompt. 19. Navigate to **Assets and Compliance > Overview > Devices** and check if **CLIENT7** is showing in the list of devices. 20. Right-click on **CLIENT7** and click on **Install Client** (hold Ctrl and select multiple computers if you want to install on more than one computer). 21. On the Install Configuration Manager Client wizard click on **Next**. 22. Check the box next to **Install the client software from a specified site**, select the Site **CHQ-Contoso Headquarters** and click on **Next**. 23. Click **Next** again. 24. Click on **Close**. 25. After a few minutes, the **CLIENT7** client will have the client installed and will indicate so in the Configuration Manager console. **Note:** If by any chance the client fails to install, retry the installation.
Complete these steps on the CLIENT7 virtual machine.	
Create Checkpoint	26. Create a virtual machine **checkpoint**. **Note:** Repeat **Steps 14-23** above to install the Configuration Manager Client on **HYD-CLIENT1** and **HYD-CLIENT2**. If by any chance the client fails to install, retry the installation. **Note:** The **Windows Defender Firewall Mode** for **Domain networks, Private networks and Guest or public Networks** must be turned off on **HYD-CLIENT1-4**. Refer to **Step 12** above.

2.3.5.3 Build a Windows 11 22H2 Client Physical Machine

Note: The **WIN11 (CLIENT8)** Physical Machine will be used for the following scenarios in this Lab Guide:

- Section **Error! Reference source not found.** – **Error! Reference source not found.**

In this section, you will provide a physical customer device that meets Windows 11 requirement. The requirements are as follows:

- Customer Provided Devices with Windows 11 pre-installed.

3 Plan and Prepare Infrastructure

3.1 Cloud Management Gateway (CMG)

The Cloud Management Gateway (CMG) provides a simple way to manage Configuration Manager clients on the Internet. By deploying the CMG as a cloud service in Microsoft Azure, you can manage traditional clients that roam on the Internet without additional infrastructure. You also don't need to expose your on-premises infrastructure to the internet.

The CMG creates an Azure storage account, which it uses for its standard operations. By default, the CMG is also content-enabled to provide deployment content to internet-based clients. This service supports the following scenarios:

1) Provide software content to Internet-based clients without additional on-premises infrastructure.
2) Cloud-enable your content distribution system.
3) Reduce the need for on-premises distribution points.

Note: The cloud-based distribution point (CDP) is deprecated. Starting in version 2107, you can't create new CDP instances. To provide content to internet-based devices, enable the CMG to distribute content.

This section provides the steps to install and configure the Cloud Management Gateway (CMG).

Note: Ensure that a trial subscription has been associated with the previously created **<AzureDomainName>.onmicrosoft.com**.

Note: The **Microsoft.KeyVault, Microsoft.Storage, Microsoft.Network** and **Microsoft.Compute** resource providers must be registered within the Azure subscription (required for deploying the CMG to a virtual machine scale set). To verify that in the Azure portal, click **All services | search for and click Subscriptions | click the subscription | Resource providers**. If not registered, click.

Note: For more information, refer to https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/configure-azure-ad#configure-azure-resource-providers

3.1.1 Check for the Globally Unique Name

Before setting up and configuring the CMG server authentication certificate, it is required to know a globally unique name for the service that will be configured in the CMG server authentication certificate. To do so, perform the following steps.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	

Check for the Globally Unique Name	1. Log into the Azure portal using the **labadmin@<AzureDomainName>.onmicrosoft.com** account. 2. Click **Create a resource** from the top left-hand corner. 3. In **Search the Marketplace** search box, type **Cloud Service** and select **Cloud Service** from the search results. 4. Click **Create** in the **Cloud service** blade. 5. In **DNS name**, type a globally unique name and ensure it is available. 6. In **Subscription**, select the appropriate subscription. 7. In **Resource group**, select **Create new** and type in the name of a resource group not already in use. Click **OK**. 8. In **Location**, select the appropriate location which is supported by the subscription. 9. Ensure that there are no errors on the **Cloud service (classic)** blade, take a note of all the details and exit. **Note:** Do not create the cloud service.

3.1.2 Create and Issue the CMG Server Authentication Certificate

After the globally unique name for the service is known, create and issue the CMG server authentication certificate by performing the following steps.

Note: In **DC1**, Active Directory, create a Security Group, example **ConfigMgr Site Servers** and add **CM1** into this Security Group.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Create and Issue the CMG Server Authentication Certificate	1. Launch the **Certification Authority** console. 2. Right-click **Certificate Templates**, and then click **Manage** to load the Certificate Templates console. 3. In the Certificate Templates console, right-click the entry that has **Web Server** in the Template Display Name column, and then click **Duplicate Template**. 4. In the Properties of New Template window, ensure that **Windows Server 2003** is selected under **Certification Authority** and **Windows XP / Server 2003** is selected under **Certificate recipient**. 5. On the **General** tab, enter a template name, example: **CMG Server Authentication Certificate**, to generate the web server certificate for CMG. 6. Click the **Request Handling** tab, and then select **Allow private key to be exported**. 7. Click the **Security** tab, and then remove the **Enroll** permission from the **Enterprise Admins** security group.

	8. Click **Add**, enter the name of the security group, example: **ConfigMgr Site Servers** that contains the computer object of the ConfigMgr site server in the text box, and then click **OK**. 9. Select the **Enroll** permission for the security group, example: **ConfigMgr Site Servers**, and "do not" clear the **Read** permission checkbox. 10. Click **OK**, and then close the Certificate Templates console. 11. Back in the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**. 12. In the Enable Certificate Templates window, select the new template configured, example: **CMG Server Authentication Certificate**, and then click **OK**. Close the Certification Authority console.

3.1.3 Request the CMG Server Authentication Certificate

After the CMG server authentication certificate is created and issued, request this certificate on **CM1** by performing the following steps.

Note: Reboot **CM1** once, so that the server can access the certificate template using the Read and Enroll permissions.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Request the CMG Server Authentication Certificate	1. Right-click **Start**, click **Run**, enter **mmc** and press enter. Accept the UAC prompt. In the empty console, click **File**, and then click **Add/Remove Snap-in**. 2. In the Add or Remove Snap-ins window, select **Certificates** from the list of Available snap-ins, and then click **Add**. 3. In the Certificate snap-in window, select **Computer account**, and then click **Next**. 4. In the Select Computer window, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. 5. In the Add or Remove Snap-ins window, click **OK**. 6. In the console, expand **Certificates (Local Computer)**, and then click **Personal**. 7. Right-click **Certificates**, click **All Tasks**, and then click **Request New Certificate**. 8. On the Before You Begin page, click **Next**. 9. On the Select Certificate Enrollment Policy page, click **Next**. 10. On the Request Certificates page, identify the certificate, example: **CMG Server Authentication Certificate** from the list of available certificates, and then click **More information is required to enroll for this certificate. Click here to configure settings.** 11. In the Certificate Properties window, in the **Subject** tab, for the **Subject name**, select **Common name** as the **Type**. 12. In the **Value** box, specify the globally unique name recorded in **Section** Error! Reference source not found., in an FQDN format ending with

	{AzureRegion}.cloudapp.azure.com. **Note:** Starting in version 2010, if you'll deploy the CMG to a virtual machine scale set, the deployment name is different. With a virtual machine scale set, the service name uses the **cloudapp.azure.com** domain along with the region. For example, Contoso.EastUS.CloudApp.Azure.Com for a deployment in the East US Azure region. 13. Click **Add** and then click **OK** to close the Certificate Properties dialog box. 14. Back in the Request Certificates page, select the certificate, example: **CMG Server Authentication Certificate** from the list of available certificates, and then click **Enroll**. 15. On the Certificates Installation Results page, wait until the certificate is installed, and then click **Finish**. 16. Verify that a new certificate has been created under **Personal | Certificates**.

3.1.4 Export the CMG Server Authentication Certificate

After the CMG server authentication certificate is requested in **CM1**, it needs to be exported by performing the following steps.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Export the CMG Server Authentication Certificate	1. In the Certificates (Local Computer) console, right-click the **certificate** that was just configured and enrolled, click **All Tasks**, and then click **Export**. 2. In the Certificate Export Wizard, click **Next**. 3. On the Export Private Key page, click **Yes, export the private key**, and then click **Next**. 4. On the Export File Format page, ensure that the **Personal Information Exchange - PKCS #12 (.PFX)** option is selected along with the option **Include all certificates in the certification path if possible** and **Enable certificate privacy** and then click **Next**. 5. On the Security page, specify a strong password to protect the exported certificate with its private key, and then click **Next**. 6. On the File to Export page, **Browse** to a suitable location to save the certificate, specify the name of the **PFX** file to be exported, and then click **Save | Next**. 7. To close the wizard, click **Finish** in the Certificate Export Wizard page, and then click **OK** in the confirmation dialog box. 8. Store the file securely and ensure that you can access it from the ConfigMgr console. This certificate will be required during setting up CMG.

3.1.5 Create and Issue the Client Authentication Certificate

To create and issue the client authentication certificate, perform the following steps.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Create and Issue the Client Authentication Certificate	1. Launch the **Certification Authority** console. 2. Right-click **Certificate Templates**, and then click **Manage** to load the Certificate Templates console. 3. In the Certificate Templates console, right-click the entry that has **Workstation Authentication** in the Template Display Name column, and then click **Duplicate Template**. 4. In the Properties of New Template window, ensure that **Windows Server 2003** is selected under **Certification Authority** and **Windows XP / Server 2003** is selected under **Certificate recipient**. 5. On the **General** tab, enter a template name, example: **ConfigMgr Client Authentication Certificate**, to generate the client certificates that will be used on ConfigMgr client computers. 6. Click the **Security** tab, select the **Domain Computers** group, and then select the additional permissions of **Read** and **Autoenroll**. Do not clear **Enroll**. 7. Click **OK**, and then close the Certificate Templates console. 8. Back in the Certification Authority console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**. 9. In the Enable Certificate Templates window, select the new template configured, example: **ConfigMgr Client Authentication Certificate**, and then click **OK**. Close the Certification Authority console.

3.1.6 Configure Autoenrollment of the Client Authentication Certificate using Group Policy

After the client authentication certificate is created and issued, a group policy is configured to autoenroll the client authentication certificate to client computers by performing the following steps.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Configure Autoenrollment of the Client Authentication	1. Click **Start | Windows Administrative Tools | Group Policy Management**. 2. Right-click on the root of the domain, and then click **Create a GPO in this domain, and Link it here**.

Certificate using Group Policy	3. In the New GPO dialog box, enter a name, example: **Client Authentication Certificate Autoenrollment**, and then click **OK**. 4. In the results pane, on the **Linked Group Policy Objects** tab, right-click the new group policy, and click **Edit**. 5. In the Group Policy Management Editor window, navigate to **Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies**. 6. Right-click **Certificate Services Client – Auto-Enrollment** and click **Properties**. 7. For the **Configuration Model**, select **Enabled**, select **Renew expired certificates, update pending certificates, and remove revoked certificates** and select **Update certificates that use certificate templates**. Click **OK**. 8. Close the Group Policy Management Editor and the console.

3.1.7 Automatically Enroll the Client Authentication Certificate and Verify its Installation

After configuring autoenrollment of the client authentication certificate using group policy, to automatically enroll the certificate and verify its installation, perform the following steps.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Automatically Enroll the Client Authentication Certificate and Verify its Installation	1. Reboot **CLIENT1** and run a **gpupdate /force**. Run a **gpupdate /force** on **CM1** as well. 2. Right-click **Start**, click **Run**, enter **mmc** and press enter. Accept the UAC prompt if required. In the empty console, click **File**, and then click **Add/Remove Snap-in**. 3. In the Add or Remove Snap-ins window, select **Certificates** from the list of Available snap-ins, and then click **Add**. 4. In the Certificate snap-in window, select **Computer account**, and then click **Next**. 5. In the Select Computer window, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. 6. In the Add or Remove Snap-ins window, click **OK**. 7. In the console, expand **Certificates (Local Computer) | Personal** and select **Certificates**. 8. In the results pane, confirm that the certificate is present that has **Client Authentication** in the **Intended Purposes** column, and that example: **ConfigMgr Client Authentication Certificate** is in the **Certificate Template** column.

3.1.8 Client Trusted Root Certificate to CMG

The CMG must trust the client authentication certificates. Client trusted root certificate to CMG is required when using client authentication certificate. When clients use Azure AD for authentication, then this certificate is not required. To accomplish this trust, provide the trusted root certificate chain by performing the following steps.

Note: It is not required to configure the other type of certificate called CMG Trusted Root Certificate to Clients in this lab because there is only one Trusted Root Certification Authority. Configuring the Client Trusted Root Certificate to CMG is enough.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Client Trusted Root Certificate to CMG	1. Double-click on the certificate that was just created, issued and auto-enrolled and click the **Certification Path** tab. 2. Select the top-most certificate up the chain and click **View Certificate**. 3. On the new Certificate window, click the **Details** tab and click **Copy to File**. 4. In the Certificate Export Wizard, click **Next**. 5. On the Export File Format page, select **DER encoded binary X.509 (.CER)** and click **Next**. 6. On the File to Export page, **Browse** to a suitable location to save the certificate, specify the name of the **CER** file to be exported, and then click **Save | Next**. 7. To close the wizard, click **Finish** in the Certificate Export Wizard page, and then click **OK** in the confirmation dialog box. 8. Store the file securely. Client trusted root certificate to CMG is required when using client authentication certificate. Ensure that you can access it from the ConfigMgr console. This certificate will also be required during setting up CMG. Close all the windows.

3.1.9 Configure Azure Services

Perform the following steps to configure Azure services in ConfigMgr.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure Azure Services	1. In the ConfigMgr console, navigate to **Administration | Cloud Services | Azure Services**. 2. Right-click **Azure Services** and click **Configure Azure Services**. 3. On the Azure Services page, specify a **Name**, an “optional” **Description**, select **Cloud Management** and click **Next**.

	4. On the App page, ensure **AzurePublicCloud** is selected next to **Azure environment**. 5. Click **Browse** next to **Web app**. 6. On the Server App window, click **Create**. 7. On the Create Server Application window, provide a friendly name for the app next to **Application Name**. 8. For the **Secret key validity period**, select either **1 Year** or **2 Years**. By default, this value is **1 Year**. 9. Click **Sign in** next to **Azure AD Admin Account** and sign in as an Azure administrator (global admin) and subscription admin (owner\contributor) - **labadmin@<AzureDomainName>.onmicrosoft.com**. After successful authentication, the **Azure AD Tenant Name** is displayed. 10. On the Create Server Application window, click **OK**. 11. On the Server App window, select/highlight the app and click **OK**. 12. Back on the App page, click **Browse** next to **Native Client app**. 13. On the Client App window, click **Create**. 14. On the Create Client Application window, provide a friendly name for the app next to **Application Name**. 15. Click **Sign in** next to **Azure AD Admin Account** and sign in as an Azure administrator (global admin) and subscription admin (owner\contributor) - **labadmin@<AzureDomainName>.onmicrosoft.com**. After successful authentication, the **Azure AD Tenant Name** is displayed. 16. On the Create Client Application window, click **OK**. 17. On the Client App window, select/highlight the app and click **OK**. 18. Back on the App page, click **Next**. 19. On the Discovery page, select the checkbox next to **Enable Azure Active Directory User Discovery** and **Enable Azure Active Directory Group Discovery**. Both of them are not requirements for CMG. 20. On the Discovery page, click **Next**. 21. On the Summary page, review and click **Next**. 22. On the Completion page, click **Close**.

3.1.10 Set up the CMG

This section provides the steps required to set up a CMG.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Set up the CMG	1. In the ConfigMgr console, navigate to **Administration | Cloud Services | Cloud Management Gateway**.

2. Right-click **Cloud Management Gateway** and click **Create Cloud Management Gateway**.
3. On the General page, ensure **AzurePublicCloud** is selected next to **Azure environment** and **Virtual machine scale set** is selected for **Please choose how you want to deploy your cloud services**.
4. Click **Sign In** next to **Subscription admin account** and sign in as an Azure administrator (global admin) and subscription admin (owner\contributor) - **labadmin@<AzureDomainName>.onmicrosoft.com**. After successful authentication, the **Subscription ID**, **Azure AD app name** and **Azure AD tenant name** fields are auto-populated with the respective values.
5. On the General page, click **Next**.
6. On the Settings page, click **Browse** next to **Certificate file** and select the CMG server authentication certificate exported earlier.
7. On the Password window prompt, specify the password and click **OK**. The **Service name** and **Deployment name** fields are auto-populated with the respective values.
8. Select the appropriate **Region** from the drop-down list.
   <u>Note:</u> It is important to select the correct region that was used for the FQDN of the certificate that was created.
9. Next to **Resource Group**, select **Create new**, the name should auto-populate, if not enter the name of the resource group.
10. Next to **VM Instance**, enter the number of VMs for CMG. The default value is **1**, but you can scale up to 16 VMs per CMG.
11. Click **Certificates** next to Certificates uploaded to the cloud service.
12. On the Certificates uploaded to the cloud service window, click **Add** and select the client trusted root certificate to CMG exported earlier and click **OK**.
13. By default, the wizard enables the option to **Verify Client Certificate Revocation**. A certificate revocation list (CRL) must be publicly published for this verification to work. If you do not publish a CRL, deselect this option.
14. At the bottom, notice the option **Allow CMG to function as a cloud distribution point and serve content from Azure storage**. This option is enabled by default. Keep it selected.
15. On the Settings page, click **Next**.
16. On the Alerts page, to monitor CMG traffic with a 14-day threshold, select the checkbox next to **Turn on 14-day threshold and alerts for monitoring outbound data transfer** and **Stop this service when the critical threshold is exceeded**. Then, specify the **14-day threshold for outbound data transfer (GB)**, **Percentage of threshold for raising Warning alert** and **Percentage of threshold for raising Critical alert**.
17. Also, select the checkbox next to **Specify storage alert threshold** and then specify the **Storage alert threshold (GB)**, **Generate Warning alert (% of storage alert threshold)** and **Generate Critical alert (% of storage alert threshold)** and then click **Next**.
18. On the Summary page, review and click **Next**.

	19. On the Completion page, click **Close**. 20. At this stage, ConfigMgr starts setting up the service. It will take between 5 to 15 minutes to provision the service completely in Azure. Check the **Status** column for CMG, to determine when the service is **Ready**. 21. The content enabled CMG will be visible from **Administration | Distribution Points**.

3.1.11 Configure Boundary Group and Distribution Point Group for the content enabled CMG

This section provides the steps to add the content enabled CMG to the Boundary Group and the Distribution Point Group.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure Boundary Group and Distribution Point Group for CDP	1. In the ConfigMgr Console, browse to **Administration | Overview | Hierarchy Configuration | Boundary Groups**. Right-click on **Corp Boundary Group** which has the **Default Boundary** and the **IP Based Boundary** as members and click **Properties**. 2. Click the **References** tab and click **Add** under Site system servers. 3. Select the content enabled CMG and click **OK** and then click **OK** again. 4. In the ConfigMgr Console, browse to **Administration | Overview | Distribution Point Groups**. Right-click on the **Corp DPs** distribution point group and click **Properties**. 5. Click the **Members** tab and click **Add**. 6. Select the content enabled CMG and click **OK** and then click **OK** again.

3.1.12 Configure Enhanced HTTP and the Primary Site for Client Certificate Authentication

This section provides the steps to configure Enhanced HTTP and the Primary Site for Client Certificate Authentication.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure Enhanced HTTP and the Primary Site for Client	1. In the ConfigMgr Console, browse to **Administration | Overview | Site Configuration | Sites**. 2. Right-click the primary site and click **Properties**.

Certificate Authentication	3. In the primary site properties window, click the **Communication Security** tab and select the checkboxes next to **Use Configuration Manager-generated certificates for HTTP site systems** and **Use PKI client certificate (client authentication capability) when available**. 4. If you do not publish a CRL, deselect the option for **Clients check the certificate revocation list (CRL) for site systems**. 5. Under **Trusted Root Certification Authorities**, click **Set** and then in the Set Root CA Certificates window, click the **star** button and select the client trusted root certificate to CMG exported earlier. Click **OK**. 6. Click **Apply** and **OK**.

3.1.13 Add the CMG Connection Point

The CMG connection point is the site system role for communicating with CMG. This section provides the steps required to add the CMG connection point on the ConfigMgr site server.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Add the CMG Connection Point	1. In the ConfigMgr console, navigate to **Administration | Site Configuration | Servers and Site System Roles**. 2. Right-click the primary site server where CMG connection point needs to be added and click **Add Site System Roles**. 3. On the General page, click **Next**. 4. On the Proxy page, click **Next**. 5. On the System Role Selection page, select **Cloud management gateway connection point** and click **Next**. 6. On the Cloud management gateway connection point page, select the **Cloud management gateway name** to which the server connects to. The **Region** is auto-populated based on the selected Cloud management gateway name. Click **Next**. 7. On the Summary page, review and click **Next**. 8. On the Completion page, click **Close**. 9. After few minutes, you can check the status of the CMG connection point on the ConfigMgr console, by navigating to **Administration | Cloud Services | Cloud Management Gateway**, where for the selected CMG, the **Connection Status** of the **Connection Point Server Name** shows **Connected** under the **Connection Points** tab.

3.1.14 Configure the Management Point and Software Update Point for CMG Traffic

The management point and the software update point need to be configured to accept CMG traffic. This section provides the steps required to configure the management point and software update point for CMG traffic.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure the Management Point and Software Update Point for CMG Traffic	1. In the ConfigMgr console, navigate to **Administration | Site Configuration**, right-click **Servers and Site System Roles** and select **Management point**. 2. Select the site server which needs to be configured for CMG traffic and right-click **Management point | Properties**. 3. In the **General** tab of the Management point Properties window, under **Client connections**, ensure that **HTTP** is selected. 4. Select the checkbox next to **Allow Configuration Manager cloud management gateway traffic**. 5. Ensure **Allow intranet and Internet connections** is selected automatically. 6. Click **Apply** and **OK**. 7. After few minutes, you can even check the status of the management point endpoints on the ConfigMgr console, by navigating to **Administration | Cloud Services | Cloud Management Gateway**, where for the selected CMG, under **Role Endpoints** tab, you are able to see management point endpoints. 8. Navigate to **Administration | Site Configuration**, right-click **Servers and Site System Roles** and select **Software update point**. 9. Select the site server which needs to be configured for CMG traffic and right-click **Software update point | Properties**. 10. In the Software update point Properties window, select the checkbox next to **Allow Configuration Manager cloud management gateway traffic**. 11. Ensure **Allow Internet and intranet client connections** is selected automatically. 12. Ensure that the checkbox next to **Require SSL communication to the WSUS server** is unchecked and click **Apply** and **OK**. 13. After few minutes, you can even check the status of the software update point endpoints on the ConfigMgr console, by navigating to **Administration | Cloud Services | Cloud Management Gateway**, where for the selected CMG, under **Role Endpoints** tab, you are able to see software update point endpoints.

3.1.15 Configure the Configuration Manager Client Settings for Cloud Services

This section provides the steps required to configure the ConfigMgr Client Settings for Cloud Services.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure the Configuration Manager Client Settings for Cloud Services	1. In the ConfigMgr Console, browse to **Administration | Overview | Client Settings** and double-click on **Default Client Settings**. 2. Click **Cloud Services** and then select **Yes** for **Allow access to cloud distribution point**. Also ensure that **Yes** is selected next to **Enable clients to use a cloud management gateway** and then click **OK**. 3. To verify, from **Assets and Compliance | Overview | Devices**, ensure that the ConfigMgr Client is installed on the clients and are active, example **CLIENT1**. From there, also ensure that the **Resultant Client Settings** show the changes made in the Default Client Settings. Right-click on the client, click **Client Settings | Resultant Client Settings**.

3.1.16 Test a Deployment on a Client on the Internet

In this section, you will create an application, distribute its contents to CDP and deploy the application to CLIENT1, which is simulated to be on the Internet.

Task	Detailed Steps
Complete these steps on the CLIENT1 and CM1 virtual machine.	
Test a Deployment on a Client on the Internet	1. Before making any changes in **CLIENT1**, restart the **SMS Agent Host** service when it is on the Intranet. 2. Now, simulate **CLIENT1** to be on the Internet, by configuring the following registry key - **HKLM\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 1** and restart the **SMS Agent Host** service. 3. On **CLIENT1**, after few minutes, when you open the **ConfigMgr Client Properties**, under the **General** tab, notice that **Client certificate = PKI**, **Connection Type = Always Internet** and the **Network** tab shows the **FQDN of the CMG**. 4. In **CM1**, **download** a sample application, example **XML Notepad** and **create an application** in the ConfigMgr Console. After that **distribute** the application to **CDP** only and **deploy** it on **CLIENT1** as an **Available** deployment. Create a device collection for **CLIENT1**.

	5. On **CLIENT1**, in the **ConfigMgr Client Properties**, **Actions** tab, run **Machine Policy Retrieval and Evaluation Cycle**. 6. On **CLIENT1**, when the notification appears that the software is available for the installation, open the **Software Center**, select the application and install it. The contents of the application will be downloaded from the content enabled CMG to the ConfigMgr client cache and further installed from the ConfigMgr client cache. **Note:** For further labs, change the value of the registry key created in **CLIENT1**, which simulated it being on the Internet - **HKLM\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 0** and then restart the **SMS Agent Host** service.

3.2 Tenant Attach, Co-Management and Switching Workloads

In Configuration Manager, co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Intune. It's a solution that provides a bridge from on-premises to modern cloud management and gives you a path to make the transition using a phased approach.

After you enable co-management, Configuration Manager continues to manage all workloads. When you decide that you are ready, you can have Intune start managing available workloads. You can have Intune manage the following workloads: Compliance policies, Windows Update for Business policies, Resource Access policies, Endpoint Protection and many more.

For more information on Microsoft Endpoint Manager tenant attach: Device sync and device actions, refer to - https://docs.microsoft.com/en-us/mem/configmgr/tenant-attach/device-sync-actions

For more information on Troubleshooting device actions for Configuration Manager devices, refer to - https://docs.microsoft.com/en-us/mem/configmgr/tenant-attach/technical-reference

For more information on How to enable co-management in Configuration Manager, refer to - https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-enable

For more information on How to switch Configuration Manager workloads to Intune, refer to - https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-switch-workloads

3.2.1 Prerequisites

Perform the following tasks before proceeding.

Task	Detailed Steps

Prerequisite Sections	**Section** Error! Reference source not found. Error! Reference source not found. **Section** Error! Reference source not found. Error! Reference source not found. **Section** Error! Reference source not found. Error! Reference source not found. **Section** Error! Reference source not found. Error! Reference source not found. **Section** Error! Reference source not found. Error! Reference source not found. **Section** Error! Reference source not found. Error! Reference source not found.
Complete these steps on an Internet-connected Windows computer.	
Configure Auto MDM Enrollment for Intune	1. Start Edge InPrivate mode. 2. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 3. On the left navigation bar, click **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune**. 4. In the **MDM user scope** setting, select **All**. 5. Click **Save**.

3.2.2 Tenant Attach, Co-Management and Switch Workloads

Once co-management is enabled, devices in the Pilot group can automatically enroll into Intune. This requires using a verified domain during the Setup Process of Azure AD Connect.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Create a Device Collection	1. Open the **Configuration Manager Console**, browse to **Assets and Compliance** workspace and select **Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. Input the following information: *General* Name – Enter **Co-managed Devices** Limiting collection – Select **All Desktop and Server Clients** and click **Next**. Select **Use incremental updates for this collection**. Click **Next**. Accept the Warning. 4. *Summary* – click **Next**, click **Close**.
Add a Device to the Collection	5. In the **Assets & Compliance** workspace, select **Devices** and right-click **CLIENT1**. 6. Select **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 7. Select **Co-managed Devices** and click **OK**.

	8. Select **Device Collections**, right-click **Co-managed Devices**, and select **Update Membership**. Click **Yes** on the warning box to continue.
Configure Cloud Attach	9. Browse to **Administration > Cloud Services > Cloud Attach**. 10. Click **Configure Cloud Attach** from the ribbon bar. 11. In the **Cloud Attach Configuration Wizard,** select **AzurePublicCloud** for your environment. 12. Sign into Microsoft Endpoint Manager using **labadmin@<AzureDomainName>.onmicrosoft.com.** Select **Customize settings**, and then click **Next** and accept the prompt. 13. On the **Configure upload** page, accept the defaults and click **Next**. 14. On the **Enablement** page, select **Pilot** next to **Automatic enrollment in Intune.** Under **Intune auto enrollment**., browse and select **Co-managed Devices.** Click **Next.** 15. Click **Next** on the **Summary** page. Click **Close**. 16. Select the newly created **CoMgmtSettingProd** item under **Administration > Cloud Services > Cloud Attach** and click on **Properties** in the ribbon bar. 17. On the **Workloads** tab, drag the slider for **Compliance policies** and **Windows Update policies** to **Pilot Intune**. 18. On the **Staging** tab, next to **Compliance Policies**, browse to **Co-managed Devices.** Scroll down and, next to **Windows Update Policies,** browse to **Co-managed Devices** and click **Apply** and **OK** to initiate configuration.
Perform Device Actions	19. In a browser, navigate to **endpoint.microsoft.com** and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 20. Select **Devices** then **All devices** to see the uploaded devices. You'll see **ConfigMgr** in the **Managed by** column for uploaded devices. **Note:** It may take some time before devices appear. 21. Select a device to load its **Overview** page. 22. Choose any of the following actions: a. **Sync Machine Policy** b. **Sync User Policy** c. **App Evaluation Cycle**
Check device status	23. Navigate back to **Devices>All devices.** Click on a device labeled "Co-Managed" under the "**Managed by**" column. These devices include telemetry generated through Tenant Attach (Intune + ConfigMgr-related items such as App Configurations). 24. On left nav, click **Timeline**. Click **Filter** in top nav and change dates to expand time range by 7-10 days. Click **Apply** to see timeline of device events. Click on an event for details. (To add events, restart the device, add updates, etc.)

3.2.3 Co-Manage Devices with the Configuration Manager Client

For unverified domains, co-management can still be enabled by enrolling the domain-joined device into Intune.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Log in to Client 1	1. Start/restart the VM and log in as **labadmin@<AzureDomainName>.onmicrosoft.com** with password **P@ssw0rd**. 2. Open the **Configuration Manager Client Applet** and under the **Actions** tab, run the **Machine Policy Retrieval & Evaluation Cycle** and then close the applet. Under **C:\Windows\CCM\Logs**, monitor the **CoManagementHandler.log**. At this stage, Co-management will get automatically enabled on the device and will also automatically enroll the device to Intune. 3. After a while, reopen the **Configuration Manager Client Applet** and under the **General** tab, notice the **Co-management capabilities=8211** and **Co-management=Enabled**. 4. Under the **Configurations** tab, **Evaluate** and **Refresh** the following settings to make them **Compliant**: • **CoMgmtSettingsPilotAutoEnroll** • **CoMgmtSettingsPilotCP** • **CoMgmtSettingsPilotWUP** • **CoMgmtSettingsProd**
Complete these steps from an internet-connected Windows computer.	
Check the Windows 11 Device	**Note**: In this example, we will look in Microsoft Intune to see the device details. 5. Start Edge InPrivate mode. 6. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 7. On the left navigation bar, click **Azure Active Directory > Devices > All devices**. 8. Notice that the Windows 11 device (**CLIENT1**) is **Hybrid Azure AD joined**. 9. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 10. Select **Devices** > **All devices**. 11. Notice that the Windows 11 device (**CLIENT1**) is **Co-managed**. 12. Click on the Windows 11 device (**CLIENT1**). Notice the **device actions** like **Sync**. Also, notice the **Co-management** statement, **Configuration Manager agent state**, **Details**, **Last Configuration Manager agent check in time** and **Intune managed workloads**. Notice both the workloads - **Compliance Policy** and **Windows Update for Business**.

3.2.4 Autopilot (Configuration Manager Client Installation from Cloud Management Gateway – CMG)

For devices provisioned using the Autopilot service and for those devices to have the Configuration Manager Client installed from CMG, there are two things that need to be deployed from Intune:

- Client Trusted Root Certificate (Section **Error! Reference source not found.**)
- Configuration Manager Client

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Deploy the Client Trusted Root Certificate	1. Close all browser windows. 2. Start Edge InPrivate mode. 3. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 4. On the left navigation bar, click **Devices > Configuration profiles**. 5. Click **+ Create profile**. 6. Under **Platform**, select **Windows 10 and later,** under **Profile type**, select **Templates**, for the **Template name** select **Trusted certificate**. Click **Create**. 7. Under the **Basics** step, enter the following and click **Next**: **Name: Trusted Root Certificate** 8. Under the **Configuration settings** step, enter the following and click **Next**: Browse to where the **Client Trusted Root Certificate** was saved that was created in **Section** Error! Reference source not found. and select it. **Destination store: Computer certificate store – Root** 9. Under the **Assignments** step, enter the following and click **Next**: Under **Included groups**, click **+ Add groups**, select **Autopilot Devices**, click **Select**. 10. Under the **Applicability Rules** step, click **Next**. 11. Under the **Review + create** step, click **Create**.

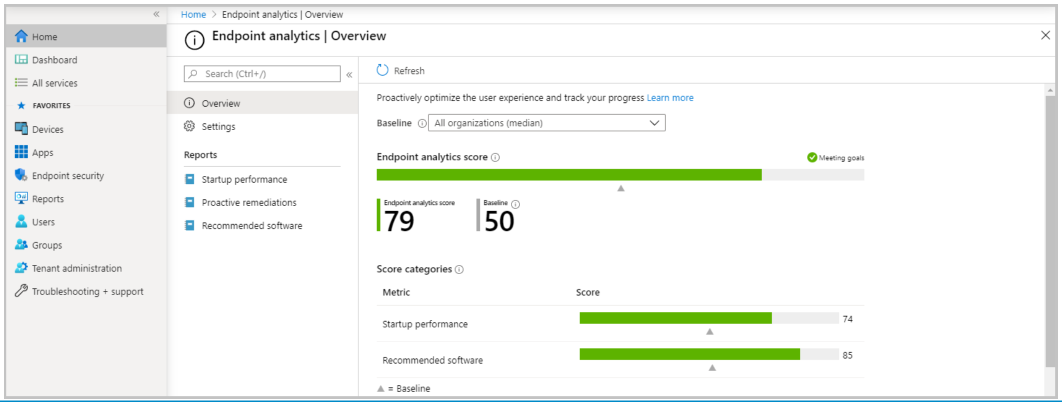
Deploy the Configuration Manager Client	12. On the left navigation bar, select **Apps > All apps > + Add**. 13. Under **App type**, select **Line-of-business app** and click **Select**. 14. Under the **App information** step, enter the following and click **Next**: Click **Select app package file** and browse to **C:\Program Files\Microsoft Configuration Manager\bin\i386\ccmsetup.msi**. Click **OK**. **Publisher: Microsoft** **Command-line arguments: Enter the command line from the Configuration Manager Console > Administration > Cloud Services > Cloud Attach > Right-click CoMgmtSettingsProd > Properties > Enablement tab > Copy the Command-line arguments from there** **Note:** If you did not publish a CRL back in **Section** Error! Reference source not found., then be sure to add the /NoCRLCheck switch within the quotes of the command line 15. Under the **Assignments** step, enter the following and click **Next**: Under **Required**, click **+ Add group**, select **Autopilot Devices**, click **Select**. 16. Under the **Review + create** step, click **Create**. Once the upload is completed, wait for a few minutes for the page to refresh.
Complete these steps from the CLIENT4 virtual machine.	
Perform Azure AD Join	17. Start the VM and once OOBE has started, enter the password for **TU1@<AzureDomainName>.onmicrosoft.com** then click **Next**. 18. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 19. In the **All set!** pane, click **OK**.
Validate Azure AD Join and MDM Enrollment	20. Go to **Start > Settings**. 21. In the **Settings** app, browse to **Accounts > Access work or school**. 22. Confirm that **Connected to <CompanyName>'s Azure AD** is displayed and the **Info** button is displayed as well. Notice the **ConfigMgr Client Setup Bootstrap: EnforcementCompleted message**. If required, click **Sync**. After a while the Configuration Manager Client will be installed from the Cloud Management Gateway.
Complete these steps from an internet-connected Windows computer.	

Validate Azure AD and MDM Enrollment	23. Start Edge InPrivate mode. 24. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 25. On the left navigation bar, click **Azure Active Directory > Devices > All devices**. 26. Notice that the Windows 11 device (**CLIENT4**) is **Azure AD joined**. 27. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 28. Select **Devices** > **All devices**. 29. Notice that the Windows 11 device (**CLIENT4**) is **Co-managed**. 30. Click on the Windows 11 device (**CLIENT4**). Notice the **device actions** like **Sync**. Also, notice the **Co-management** statement, **Configuration Manager agent state**, **Details** and **Last Configuration Manager agent check in time**.
Complete these steps from the HYPER-V Host.	
Revert Virtual Machines	31. Revert **HYD-CLIENT4** to the latest checkpoint.

3.3 Endpoint analytics

Endpoint analytics is part of the Microsoft Productivity Score. These analytics give you insights for measuring how your organization is working and the quality of the experience you're delivering to your users. **Endpoint analytics** aims to improve user productivity and reduce IT support costs by providing insights into the user experience. The insights enable IT to optimize the end-user experience with proactive support and to detect regressions to the user experience by assessing user impact of configuration changes.

Task	Detailed Steps
Complete these steps in browser.	
Onboard in the Endpoint analytics portal	1. Go to https://aka.ms/endpointanalytics 2. Choose from the following options: a. **All cloud-managed devices**: Creates an Intune data collection policy assigned to all Windows 10 1903 or later devices which are either Intune managed or co-managed. b. **Selected devices**: Creates and assigns the policy to devices which you select. c. **I'll choose later**: Doesn't deploy a policy to devices. Proactive remediations can still be used, but any reports that rely on analytics data will be empty. 3. Click **Start**. This will automatically assign a configuration profile to collect boot performance data from all eligible devices. You can change assigned devices later. It may take up to 24 hours for startup performance data to populate from your Intune enrolled devices after they reboot.

Task	Detailed Steps
View the Overview page	Note: You won't see your data immediately. The data needs to be gathered and the results calculated. For startup performance, the device needs to have been restarted at least once. Once your data is ready, you'll notice some information on the **Overview** page, explained in more detail here. 

Proactively optimize the user experience and track your progress Learn more

3.4 Optimize Windows 11 Update Delivery

When considering your content distribution strategy for Windows 11, think about enabling a form of peer-to-peer content sharing to reduce bandwidth issues during updates. Windows 11 offers two peer-to-peer options for update content distribution: Delivery Optimization and BranchCache. These technologies can be used with several of the servicing tools for Windows 11. Two methods of peer-to-peer content distribution are available in Windows 11.

- Delivery Optimization is a new peer-to-peer distribution method in Windows 10 and Windows 11. Windows clients can source content from other devices on their local network that have already downloaded the updates or from peers over the internet. Using the settings available for Delivery Optimization, clients can be configured into groups, allowing organizations to identify devices that are possibly the best candidates to fulfil peer-to-peer requests. Windows Update, Windows Update for Business, and Windows Server Update Services (WSUS) can use Delivery Optimization. Delivery Optimization can significantly reduce the amount of network traffic to external Windows Update sources as well as the time it takes for clients to retrieve the updates.
- BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them.
- **Note:** Configuration Manager has an additional feature called Client Peer Cache that allows peer-to-peer content sharing between clients you use Configuration Manager to manage, in the same Configuration Manager boundary Group. For more information, see Client Peer Cache.

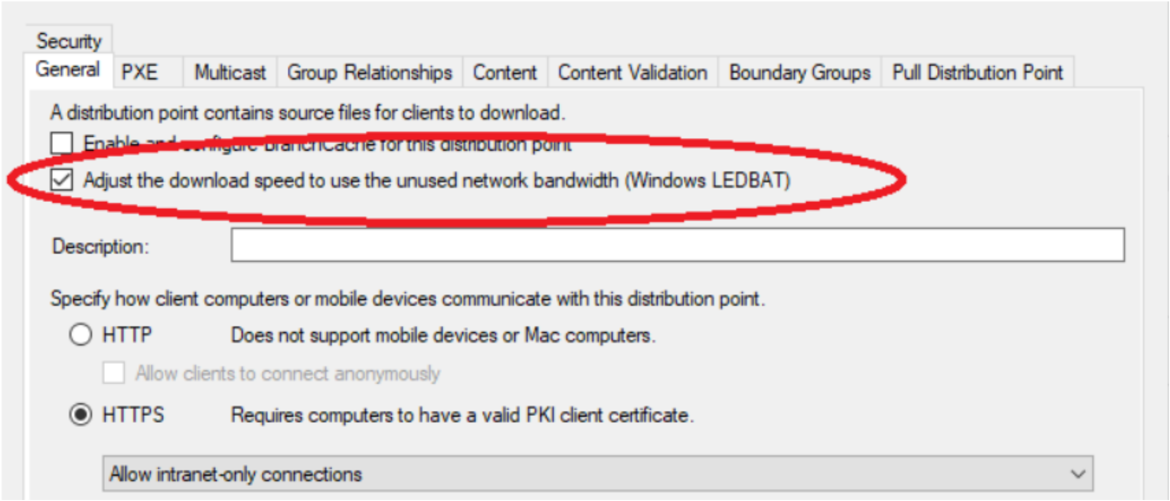
Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Configure Delivery Optimization	1. Go to **Server Manager>Tools>Active Directory Users and Computers** and right-click **CORP**, then click **New>Organizational Unit**. 2. Create an Organizational Unit, example "**Known Folder**" under **CORP** and add/move the **CLIENT1** and **CLIENT2** to this OU. 3. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 4. Right-click the Organizational Unit created "**Known Folder**" and click **Create a GPO in this domain, and Link it here**. Give it a name, example "**Delivery Optimization**" and click **OK**. 5. Right-click the new GPO, example "**Delivery Optimization**" and click **Edit**. 6. Go to **Computer Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization** to configure Delivery Optimization settings. 7. For info, see **Set up Delivery Optimization for Windows client updates** **Note:** At a minimum for this lab, configure **Download Mode** to **Group** (2).
Enable Branch Cache on Client Computers	8. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 9. Right-click the Organizational Unit created "**Known Folder**" and click **Create a GPO in this domain, and Link it here**. Give it a name, example "**BranchCache**" and click **OK**. 10. Right-click the new GPO, example "**BranchCache**" and click **Edit**. 11. Go to **Computer Configuration\Policies\Administrative Templates\Network\BranchCache** to configure BranchCache settings. 12. For info, see **Use Group Policy to Configure Domain Member Client Computers.** **Note:** At a minimum for this lab, configure Turn on BranchCache to Enabled and Set BranchCache Distributed Cache mode to Enabled.

3.4.1 Latency Optimized Background Transport (LEDBAT)

Keeping a network secure is a never-ending job for IT Pros, and doing so requires regularly updating systems to protect against the latest threat vectors. This is one of the most common tasks that an IT Pro must perform. Unfortunately, it can result in dissatisfaction for end-users as the network bandwidth used for the update can compete with interactive tasks that the end-user requires to be productive.

Starting with **Windows Server 2019**, we bring a latency optimized, network congestion control provider called LEDBAT, which stands for Low Extra Delay Background Transfer. LEDBAT is designed to automatically yield bandwidth to users and applications, while consuming the entire bandwidth available when the network is not in use. It's a scavenger protocol – it scavenges whatever network bandwidth is available on the network and uses it. In other words, you can transfer Configuration Manager Packages or Microsoft Updates without interfering with your user's sanity.

LEDBAT can also be enabled on a Configuration Manager distribution point running Windows Server 2019 (or later). Because LEDBAT operates on the sending side, any client regardless of the operating system, will enjoy the benefits that it brings. To enable this in Configuration Manager, check the following option (on the **General** tab of the **Distribution Point Properties**):



A distribution point contains source files for clients to download.

□ Enable and configure BranchCache for this distribution point

☑ Adjust the download speed to use the unused network bandwidth (Windows LEDBAT)

Description:

Specify how client computers or mobile devices communicate with this distribution point.

○ HTTP Does not support mobile devices or Mac computers.

□ Allow clients to connect anonymously

● HTTPS Requires computers to have a valid PKI client certificate.

Allow intranet-only connections

For more information see:

- Announcing: Transport Features and Performance Advancements
- Enable distribution points to use network congestion control

4 Deploying Windows 11

Organizations have traditionally been deploying new versions of Windows through the wipe and load approach using a standard image, Windows Assessment and Deployment Kit, Windows Deployment Services, and Configuration Manager.

We'll also cover modern device deployment. With Windows 11, you can continue to use on-premises OS deployment, but you can also "manage out of the box." Autopilot transforms new devices into fully-configured, fully-managed devices. For existing devices running Windows 10, you can use the robust in-place upgrade process for a fast, reliable move to Windows 11 while automatically preserving all the existing apps, data, and settings.

4.1 OS Deployment Task Sequences in Configuration Manager

4.1.1 Bare Metal

This section describes how to configure Configuration Manager for Bare Metal Operating System Deployment. This is the scenario used to deploy an image to a clean disk, or to reimage a computer where you don't intend to keep any of the data on the disk.

4.1.1.1 Prerequisites

Perform the following tasks before proceeding.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Create Devices OU (if not already created)	1. Logon to **DC1** as a domain administrator (**CORP\LabAdmin**). 2. On the Start screen, open the **Active Directory Users and Computers** MMC. 3. Right-click on **corp.contoso.com** and select **New > Organizational Unit**. You might have to expand **corp.contoso.com**. 4. Under Name, enter **Devices** and then click **OK**.
Complete these steps on the CM1 virtual machine.	
Create Folder and Stage Win11 Install.wim	5. Open **File Explorer** and browse to **C:\Packages**. 6. Create a folder called **W11OSImage** 7. Mount the **Windows 11 ISO** that was downloaded in **Section** Error! Reference source not found. and copy **{driveletter}:\sources\install.wim** to **C:\Packages\W11OSImage**.

	Note: An easy way to do this is to add a DVD Drive to CM1 and insert the ISO from the Hyper-V host.
Enable PXE on the Distribution Point	8. In the **Configuration Manager Console**, navigate to **Administration > Overview > Distribution Points.** 9. Right-click on **CM.CORP.CONTOSO.COM** and select **Properties**. 10. Select the **PXE** tab, enable the following settings and then click **Apply** and **OK** **Enable PXE support for clients**, click **Yes** to the pop-up window **Review Required Ports for PXE** **Allow this distribution point to respond to incoming PXE requests** **Enable unknown computer support**, click **OK** to the pop-up window about unknown computer support Uncheck **Require a password when computers PXE**

4.1.1.2 Create a Bare Metal Task Sequence

In this activity, you will create a task sequence in Configuration Manager to deploy Windows 11 to a bare metal system.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Create and Distribute the Windows 11 OS Image	1. In the **Configuration Manager Console**, navigate to **Software Library > Overview > Operating Systems > Operating System Images**. 2. In the ribbon, click **Add Operating System Image**. 3. On the **Data Source** step, click the **Browse** button and navigate to **\\CM1\Packages$\W11OSImage**, select **install.wim** and click **Open**. 4. Check the box that says **"By checking this box you are agreeing that when applying this image…"**. 5. Check the box that says **"Extract a specific image index from the specified WIM file"** and select **"3 – Windows 10 Enterprise"** from the drop down and click **Next**. Note: The Windows 11 install.wim reads as Windows 10. 6. On the **Pre-cache settings** step, for the **Language** select **English (United States)**, for the **Architecture** select **x64**, and click **Next**. 7. On the **General** step, for the **Name** enter **Windows 11 Enterprise 22H2** and click **Next**. 8. On the **Summary** step, verify the **Details** and click **Next**. 9. On the **Completion** step, verify success and click **Close**. 10. Right-click on the newly created **Windows 11 Enterprise 22H2** Operating System Image and select **Distribute Content**. 11. On the **General** step, click **Next**.

	12. On the **Content Destination** step, click **Add**, select **Distribution Point**, select **CM1.CORP.CONTOSO.COM**, and then click **OK** and **Next**. 13. On the **Summary** step, Confirm the settings and then click **Next**. 14. On the **Completion** step, confirm success and then click **Close**. Ensure that the content is distributed from the **Monitoring > Overview > Distribution Status > Content Status**.
Verify the Boot Image (x64)	15. Navigate to **Software Library > Overview > Operating Systems > Boot Images.** 16. Select the **Boot image (x64)** and ensure that it has been distributed to the local Distribution Point. 17. Right-click on Boot image (x64) and select Properties. 18. On the **Boot image (x64) Properties**, select the **Data Source** tab and verify **Deploy this boot image from the PXE-enabled distribution point** and then click **OK**.
Create the Bare Metal Task Sequence	19. Navigate to **Software Library > Overview > Operating Systems > Task Sequences.** 20. In the ribbon, select **Create Task Sequence**. 21. On the **Create New Task Sequence** step, select **Install an existing image package** and click Next. 22. On the **Task Sequence Information** step, for the **Task sequence name** enter **Windows 11 Enterprise 22H2 Bare Metal**, click the **Browse** button, select **Boot Image (x64) 10.0.22000.1**, and click **OK** and **Next**. 23. On the **Install Windows** step, click the **Browse** button, select **Windows 11 Enterprise 22H2 en-US**, and click **OK**. Unselect **Configure task sequence for use with BitLocker**. Select **Enable the account and specify the local administrator password**, enter **P@ssw0rd** for the password and click **Next**. 24. On the **Configure Network** step, select **Join a domain**, for the **Domain** field click **Browse** and select **corp.contoso.com** and click **OK**. For the **Domain OU** field click **Browse** and select the **Devices** container and click **OK**. For the **Account** field click **Set** and for the **User name** field enter **Corp\LabAdmin** and for the **Password** field enter **P@ssw0rd** and click **OK** and then **Next**. 25. On the **Install Configuration Manager** step, click **Next**. 26. On the **State Migration** step, unselect the follow options and click **Next** **Capture user settings and files** **Capture network settings** **Capture Microsoft Windows settings** 27. On the **Include Updates** step, click **Next**. 28. On the **Install Applications** step, click **Next**. 29. On the **Summary** step, verify the details and click **Next**. 30. On the **Completion** step, verify success and click **Close**.

Deploy the Task Sequence to the Unknown Computers Collection	31. In the results page, select the **Deploy Windows 10 X64** task sequence. 32. On the ribbon click **Deploy**. 33. On the **General** step, next to Collection, click **Browse**… Click **OK** on the notification that appears. 34. In the Select Collection dialog, click the **All Unknown Computers** collection and click **OK**. 35. Click **Next**. 36. On the **Deployment Settings** step, in the **Make available to the following:** drop down list select **Configuration Manager clients, media and PXE**. 37. Click **Next**. 38. On the **Scheduling** step, click **Next**. 39. On the **User Experience** step, click **Next**. 40. On the **Alerts** step, click **Next**. 41. On the **Distribution Points** step, select **Allow clients to use distribution points from the neighbor boundary group** and **Allow clients to use distribution points from the default site boundary group** and click **Next**. 42. On the **Summary** step, review the details and click **Next**. 43. On the **Completion** step, confirm that the wizard completed successfully and click **Close**.

4.1.1.3 Deploy Windows on an Unknown Computer

This activity will initiate and complete the process to deploy Windows 11 through Bare Metal Deployment. At the end of the activity, CLIENT5 will be a Windows 11 client.

Task	Detailed Steps
Complete these steps on the CLIENT5 virtual machine.	
PXE Boot and Commence OSD	1. Power on the **CLIENT5** virtual machine and when prompted, press **Enter** for network service boot to boot from the boot image available from the PXE distribution point. 2. On the Welcome to the Task Sequence Wizard page, click **Next**. 3. On the Select a task sequence to run page, ensure that **Windows 11 Enterprise 21H2 Bare Metal** is selected and click **Next**. 4. The system will now complete the installation of Windows on the virtual machine. Once the deployment is finished, ensure that the deployment status in Configuration Manager shows **Successful** from **Monitoring > Overview > Deployments** as well as the machine has a correct status in Configuration Manager from **Assets and Compliance > Overview > Devices**. Additionally, reboot the client machine once, after the deployment so that the **Configuration Manager Client** shows all the **tabs** and the **Action Tasks** is **fully initialized,** and the **Software Center** is there as well.

Note: The system will be named with a MININT-<random number>.

4.1.2 Upgrade

As an alternative to Windows Servicing, existing computers running Windows 10 can also be upgraded using Windows 11 media. Windows 11 Upgrade leverages the Windows installation program (Setup.exe) to perform an in-place upgrade, which automatically preserves all data, settings, applications, and drivers from the existing operating system version. This requires the least effort, because there is no need for any complex deployment infrastructure.

In this section, you will go through the process of automating the upgrade process through Configuration Manager for enterprise-wide deployments or, optionally, performing manual upgrade for very small-scale scenarios. At the end of the section, the device will be upgraded to Windows 11.

Note: The Trial Download of the Windows Enterprise Media does not allow an In-Place Upgrade to be performed. To complete this lab, Windows Enterprise Media must be sourced from either MSDN Subscriber Downloads or from the Volume Licensing Site of the customer.

4.1.2.1 Prerequisites

Perform the following tasks before proceeding.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Create Folder and Stage Win11 Media	1. Open **File Explorer** then browse to **C:\Packages**. 2. Create a folder called **W11OSUpgradePackage**. 3. Mount the **Windows 11 ISO** that was downloaded in **Section** Error! Reference source not found. and copy the contents to **C:\Packages\W11OSUpgradePackage**. **Note:** An easy way to do this is to add a DVD Drive to CM1 and insert the ISO from the Hyper-V host.

4.1.2.2 Create an In-Place Upgrade Task Sequence

In his activity, you will create a task sequence in Configuration Manager to upgrade Windows 10 systems to Windows 11.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	

Create and Distribute the Windows 11 OS Upgrade Package

1. In the **Configuration Manager Console**, navigate to **Software Library > Overview > Operating Systems > Operating System Upgrade Packages**.
2. In the ribbon, click **Add Operating System Upgrade Package**.
3. On the **Data Source** step, click the **Browse** button and navigate to **\\CM1\Packages$\W11OSUpgradePackage**, and click **Select Folder**.
4. Check the box that says **“By checking this box you are agreeing that when applying this image…”**.
5. Check the box that says **“Extract a specific image index from the specified WIM file”** and select **“3 – Windows 10 Enterprise”** from the drop down and click **Next**.
   Note: The Windows 11 install.wim reads as Windows 10.
6. On the **Pre-cache settings** step, for the **Language** select **English (United States)**, for the **Architecture** select **x64**, and click **Next**.
7. On the **General** step, for the **Name** enter **Windows 11 Enterprise 22H2** and click **Next**.
8. On the **Summary** step, verify the **Details** and click **Next**.
9. On the **Completion** step, verify success and click **Close**.
10. Right-click on the newly created **Windows 11 Enterprise 22H2** Operating System Upgrade Package and select **Distribute Content**.
11. On the **General** step, click **Next**.
12. On the **Content Destination** step, click **Add**, select **Distribution Point**, select **CM1.CORP.CONTOSO.COM**, and then click **OK** and **Next**.
13. On the **Summary** step, Confirm the settings and then click **Next**.
14. On the **Completion** step, confirm success and then click **Close**.
    Ensure that the content is distributed from the **Monitoring > Overview > Distribution Status > Content Status**.

Create an Upgrade Task Sequence

15. Navigate to **Software Library > Overview > Operating Systems > Task Sequences.**
16. In the ribbon, click **Create Task Sequence**.
17. On the **Create New Task Sequence** step, select **Upgrade an operating system from an upgrade package** then click **Next**.
18. On the **Task Sequence Information** step, for **Task sequence name** enter **Windows 11 Enterprise 22H2 Upgrade** then click **Next**.
19. On the **Upgrade the Windows Operating System** step, click **Browse**.
20. On the **Select an Operating System Upgrade Package** window, select **Windows 11 Enterprise 22H2 x64 en-US** and then click **OK**.
21. Verify that in the **Edition index** field it says **Enterprise** and click **Next**.
    Note: The Windows 11 install.wim reads as Windows 10, so it should say 1 – Windows 10 Enterprise.
22. On the **Include Updates** step, click **Next**.
23. On the **Install Applications** step, click **Next**.
24. On the **Summary** step, click **Next**.

	25. On the **Completion** step, verify success and click **Close**.
Create a Collection to Deploy the Task Sequence	26. Browse to **Assets and Compliance** workspace and select **Overview > Device Collections**. 27. Right-click **Device Collections** and select **Create Device Collection**. 28. On the **General** step, enter the following then click **Next**. Name: **Windows 11 In-Place Upgrade** Limiting Collection: **All Desktops and Server Clients** 29. On the **Membership Rules** step, click **Next**. 30. On the warning dialog box, click **OK**. 31. On the **Summary** step, click **Next**. 32. On the **Completion** step, click **Close**.
Add the Windows 10 Device to the Collection	33. In the **Assets & Compliance** workspace, select **Overview > Devices** and right-click **CLIENT8**. 34. Select **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 35. Select **Windows 11 In-Place Upgrade** and click **OK**. 36. Select **Device Collections**, right-click **Windows 11 In-Place Upgrade**, and select **Update Membership**. Click **Yes** on the warning box to continue.
Deploy the Task Sequence	37. Navigate to **Software Library > Overview > Operating Systems > Task Sequences**. 38. Right-click the **Windows 11 Enterprise 22H2 Upgrade** task sequence and select **Deploy**. 39. On the **General** step, next to **Collection**, click **Browse**… Click **OK** on the notification that appears. 40. In the **Select Collection** dialog, click **Windows 11 In-Place Upgrade** collection and click **OK**. 41. On the **Deployment Settings** step, for **Purpose** select **Required**, then click **Next**. 42. On the **Scheduling** step, click **New (**next to Assignment schedule) and select **Assign immediately after this event**. Accept the defaults, click **OK**. Rerun behavior: Set to **Rerun if failed previous attempt**. Then click **Next**. 43. On the **User Experience** step, keep the default settings and click **Next**. 44. On the **Alerts** step, keep the default settings and click **Next**. 45. On the **Distribution Points** ~~page~~ step, select **Allow clients to use distribution points from the neighbor boundary group** and **Allow clients to use distribution points from the default site boundary group** and click **Next**. 46. On the **Summary** step, review the details and click **Next**. 47. On the **Completion** step, confirm that the wizard completed successfully and click **Close**.

4.1.2.3 Upgrade an existing Windows 10 system to Windows 11

This activity will initiate and complete the process to perform an in-place upgrade of a Windows 10 client to Windows 11 using the In-Place Upgrade Task Sequence. At the end of the activity, CLIENT8 will be upgraded to Windows 11.

Task	Detailed Steps
Complete these steps on the CLIENT8 virtual machine.	
Refresh Policy on the Windows 10 Device	48. On the Windows 10 device, logon as **corp\labadmin** and open the **Control Panel**. Select the **Configuration Manager** icon. 49. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now** to force the device to receive updated policy. **Note**: As soon as the deployment is detected, it will start the installation. The In-Place Upgrade Task sequence will now initiate and upgrade the Windows 10 device to Windows 11 without further user intervention.

4.1.3 Manual Upgrade

In this section, you will perform a manual in-place upgrade to Windows 11 on a Customer-Provided device. The requirements are as follows:

- Customer Provided Devices (Reference Devices) with a Corporate Image pre-installed.
- The pre-installed Corporate Image must be Windows 10 and meet the Windows 11 requirements.
- Windows 11 Installation Files.

Task	Detailed Steps
Complete these steps on the Device provided by the Customer.	
Extract Windows 11 Media	1. Extract the files from Windows 11 ISO to a USB drive. The ISO is the downloaded **Windows 11 (business editions), version 21H2 (*Latest Available Update*) (x64) – DVD (English)** from MSDN that was downloaded in **Section** Error! Reference source not found..
Perform Manual In-Place Upgrade	2. Insert the USB drive into the reference device that will be upgraded. 3. Navigate to the drive using Windows Explorer. 4. Start **setup.exe** with elevated rights from the USB drive and accept the UAC prompt. 5. Review any options and compatibility information that is provided. 6. Complete the upgrade. 7. Evaluate the system to ensure that migrated applications and data are retained.

	8. Investigate applications that were installed in the corporate image and note any incompatibilities.

4.2 Windows Autopilot

Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. In this section, you will use the Microsoft Intune to configure Autopilot for pre-configuring devices.

Note: If **CLIENT4** is already existing in **Azure AD** and **Intune** from the previous labs, then remove it from both places and ensure that the device is un-enrolled.

4.2.1 Prerequisites

Perform the following tasks before proceeding.

Task	Detailed Steps
Complete these steps on the HYPER-V Host.	
Create a Checkpoint in Hyper-V (if not already created)	1. Open **Hyper-V Manager**. 2. Right-click on **HYD-CLIENT4** and select **Checkpoint**.
Complete these steps on the CLIENT4 virtual machine.	

Capture Device ID	3. Login as the local administrator and open PowerShell as an administrator. Accept the UAC prompt if required.
	4. Run the below commands and press **Y** and **A** wherever prompted.
	`Install-Script –Name Get-WindowsAutopilotInfo`
	`Set-ExecutionPolicy Unrestricted`
	5. Change the directory to **C:\Program Files\WindowsPowerShell\Scripts** and run the below command.
	`.\Get-WindowsAutopilotInfo.ps1 –OutputFile C:\Users\Administrator\Desktop\MyComputers.csv`
	6. Copy the MyComputers.csv file to the computer that will be used for Microsoft Intune setup.
	7. Open Command Prompt as an administrator. Accept the UAC prompt if required.
	8. Run the following command after changing the directory to **C:\Windows\System32\Sysprep**
	`Sysprep.exe /OOBE /SHUTDOWN`

4.2.2 Setup and Customizations

After you complete the following tasks, you are ready to manage mobile devices and computers.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Customize the Company Portal	1. Click **Azure Active Directory > Company branding > Configure**. 2. Customize the page as per your convenience and then click **Save**. 3. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Tenant administration**. 5. Under **End user experiences**, click on **Customization**. 6. Next to **Settings**, click Edit and customize the page as per your convenience. 7. Click **Review + save** and then click **Save**.
Verify the Company Portal Configuration	8. Close all browser windows. 9. Start Edge InPrivate mode. 10. Navigate to https://portal.manage.microsoft.com and Sign in with **TU1@<AzureDomainName>.onmicrosoft.com**. 11. Review the company portal, browse to **Helpdesk** from the top left-hand corner and confirm that the customizations have been applied.

4.2.3 Enable Auto MDM Enrollment

In this activity, you will configure automatic MDM enrollment to Intune upon joining Azure AD.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Configure Auto MDM Enrollment for Intune (If not configured)	1. Close all browser windows. 2. Start Edge InPrivate mode. 3. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune**. 5. In the **MDM user scope** setting, select **All**. 6. Click **Save**.

4.2.4 Add an App

In this activity, you will add an app to Intune which will automatically download once the device is enrolled into MDM.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Add an App (If not already done before)	1. Start Edge InPrivate mode. 2. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Apps**. 4. Under **By platform**, select **Windows**. 5. Click **+Add**. 6. In the App type dropdown, select **Line-of-business app** and click **Select**.
Configure App (If not already done before)	7. Under **App information**, click **Select app package file**. 8. On the **App package file** blade, choose the browse button, and select a Windows installation file with the extension **.msi, .appx, or .appxbundle**. A sample msi file can be downloaded from: https://www.7-zip.org/download.html 9. Click **OK.** 10. Under **App information**, enter the following information and click **Next**: a. **Name** - Enter the name of the app as it is displayed in the company portal. Make sure all app names that you use are unique. If the same app name exists twice, only one of the apps is displayed to users in the company portal. b. **Description** - Enter a description for the app. The description is displayed to users in the company portal. c. **Publisher** - Enter the name of the publisher of the app. d. **App install context** – This specifies the install context to be associated with this app. For dual mode apps, select the desired context for this app. For all other apps, this is pre-selected based on the package and cannot be modified. e. **Ignore app version** – Set this to "Yes" only for apps that are automatically updated by the app developer (such as Google Chrome). f. **Command-line arguments** - Optionally, enter any command-line arguments that you want to apply to the .msi file when it runs, like /q. g. **Category** - Select one or more of the built-in app categories, or a category you created. Categorizing apps makes it easier for users to find the app when they browse the company portal.

	h. **Show this as a featured app in the Company Portal** - Display the app prominently on the main page of the company portal when users browse for apps. i. **Information URL** - Optionally, enter the URL of a website that contains information about the app. The URL is displayed to users in the company portal. j. **Privacy URL** - Optionally, enter the URL of a website that contains privacy information for the app. The URL is displayed to users in the company portal. k. **Developer** - Optionally, enter the name of the app developer. l. **Owner** - Optionally, enter a name for the owner of this app, for example, HR department. m. **Notes** - Enter any notes you would like to associate with this app. n. **Logo** - Upload an icon that is associated with the app. The icon is displayed with the app when users browse the company portal.
Deploy App (If not already done before)	11. Under **Assignments**, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 12. Under **Review + create**, review the page and click **Create**. **Note:** This group should have already been created as part of **Section** Error! Reference source not found.**.**

4.2.5 Configure Autopilot

In this activity, you will configure automatic MDM enrollment to Intune upon joining Azure AD.

Note: If **CLIENT4** is already existing in **Azure AD** and **Intune** from the previous labs, then remove it from both places and ensure that the device is un-enrolled.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Configure Autopilot	1. Start **Edge** InPrivate mode. 2. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click on **Devices**. 4. Under **Device enrollment**, click on **Enroll devices**. 5. Under **Windows Autopilot Deployment Program**, click on **Devices**. 6. Click **Import,** and select the **MyComputers.csv** file saved from before and click **Import**. 7. Once imported, to speed up the process, click **Sync** and then click **Refresh** until you see the device. 8. Under the navigation pane, click **Groups > + New group**.

	9. Select **Group type – Security**, **Group name – Autopilot Devices** and **Membership type – Assigned**. 10. Click **Members**, select the machine where the name equals the serial number of the device. Click **Select**. 11. Click **Create**. 12. On the **Devices** > **Enroll devices** pane, click **Deployment Profiles** > **+ Create profile** and select **Windows PC**. 13. On the **Basics** step, in the **Name** box, type **Autopilot Test Profile** and click **Next**. **Note:** Leave the **Convert all targeted device to Autopilot** set to **No**. 14. On the **Out-of-box experience (OOBE)** step, in the **Deployment mode** dropdown, select **User-Driven**. 15. In the **Join to Azure AD as** dropdown, select **Azure AD joined**. 16. For the **Microsoft Software License Terms** option, select **Hide**. 17. For the **Privacy Settings** option, select **Hide**. 18. For the **Hide change account options** option, select **Hide**. 19. For the **User account type** option, select **Standard** and click **Next**. 20. In the **Assignments** step, under **Included groups**, click **+ Add groups**, select the **Autopilot Devices** group just created and click **Select** and then click **Next**. 21. In the **Review + create** step, click **Create.** 22. Wait a few minutes for the device to show up in **Assigned devices** under **Autopilot Test Profile**. 23. Click on **Devices > Enroll devices > Windows Autopilot devices** and you should be able to see the **PROFILE STATUS** as **Updating** and then further **Assigned**. Wait for a few moments.

4.2.6 Autopilot for OOBE

In this activity, you will walk through the experience of self-service Autopilot while in OOBE.

Task	Detailed Steps
Complete these steps from the CLIENT4 virtual machine.	
Perform Azure AD Join	1. Start the VM and once OOBE has started, in the **Let's set things up for your work or school** pane, enter the password for **TU1@<AzureDomainName>.onmicrosoft.com** then click **Next**. 2. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 3. In the **All set!** pane, click **OK**.
Validate Azure AD Join and MDM Enrollment	4. Go to **Start > Settings**. 5. In the **Settings** app, browse to **Accounts > Access work or school**.

	6. Confirm that **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <CompanyName>'s Azure AD** is displayed and the **Info** button is displayed as well.
Complete these steps from an internet-connected Windows computer.	
Validate Azure AD and MDM Enrollment	7. Start Edge InPrivate mode. 8. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 9. On the left navigation bar, click **Azure Active Directory > Users > All users > Test User1**. 10. Click **Devices**. 11. Confirm that the device is listed there and the following settings are configured: JOIN TYPE: **Azure AD joined** MDM: **Microsoft Intune**
Complete these steps from the HYPER-V Host.	
Revert Virtual Machines	12. Revert **HYD-CLIENT4** to the latest checkpoint.

4.2.7 Windows Autopilot for pre-provisioned deployment

Windows Autopilot enables organizations to easily provision new devices – leveraging the preinstalled OEM image and drivers with a simple process that can be performed by the end user to help get their device business-ready.

Windows Autopilot can also provide a pre-provisioned deployment (formerly known as **white glove**) service that enables partners or IT staff to pre-provision a Windows 10 or Windows 11 PC so that it is fully configured and business-ready. From the end user's perspective, the Windows Autopilot user-driven experience is unchanged, but getting their device to a fully provisioned state is faster.

With **Windows Autopilot for pre-provisioned deployment**, the provisioning process is split. The time-consuming portions are performed by IT, partners, or OEMs. The end user simply completes a few necessary settings and policies and they can begin using their device.

Enabled with Microsoft Intune in Windows 10, version 1903 and later, pre-provisioned deployment capabilities build on top of existing Windows Autopilot user-driven scenarios, supporting both the user-driven Azure AD join and Hybrid Azure AD join scenarios.

For more information, refer to https://docs.microsoft.com/en-us/windows/deployment/windows-Autopilot/white-glove

Prerequisites:

1. Windows 10, version 1903 or later, or Windows 11.

2. Windows Pro, Enterprise, or Education editions.
3. An Intune subscription.
4. **Physical devices** that support TPM 2.0 and device attestation; **virtual machines are not supported**. The pre- provisioning process leverages Windows Autopilot self-deploying capabilities, so TPM 2.0 is required. The TPM attestation process also requires access to a set of HTTPS URLs that are unique for each TPM provider. For more information, see the entry for Autopilot self-Deploying mode and Autopilot pre-provisioning in Networking requirements.
5. **Physical devices** with Ethernet connectivity are required to perform pre-provisioning. Wi-Fi connectivity isn't supported because of the requirement to choose a language, locale, and keyboard to make that Wi-Fi connection. Enforcing this requirement in a pre-provisioning process could prevent the user from choosing their own language, locale, and keyboard when they receive the device. For more information, see Using a wireless network connection with Windows Autopilot white glove.

Task	Detailed Steps
Complete these steps on a Physical Machine (CLIENT8) that supports TPM 2.0 and Device Attestation and is installed with Windows 11, version 21H2	

Capture Device ID	1. Open PowerShell as an administrator. Accept the UAC prompt if required.
	2. Run the below commands and press **Y** and **A** wherever prompted.
	`Install-Script –Name Get-WindowsAutopilotInfo`
	`Set-ExecutionPolicy Unrestricted`
	3. Change the directory to **C:\Program Files\WindowsPowerShell\Scripts** and run the below command.
	`.\Get-WindowsAutopilotInfo.ps1 –OutputFile C:\Users\<UserName>\Desktop\MyComputers.csv`
	4. Copy the MyComputers.csv file to the computer that will be used for Microsoft Intune setup.
	5. Open Command Prompt as an administrator. Accept the UAC prompt if required.
	6. Run the following command after changing the directory to **C:\Windows\System32\Sysprep**
	`Sysprep.exe /OOBE /SHUTDOWN`

Complete these steps from an internet-connected Windows computer.	

Configure Autopilot pre-provisioned deployment

7. Start Edge InPrivate mode.
8. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**.
9. On the left navigation bar, click on **Devices**.
10. Under **Device enrollment**, click on **Enroll devices**.
11. Under **Windows Autopilot Deployment Program**, click on **Devices**.
12. Click **Import,** and select the **MyComputers.csv** file saved from before and click **Import**.
13. Once imported, to speed up the process, click **Sync** and then click **Refresh** until you see the device.
14. In the navigation pane, click **Groups > + New group**.
15. Select **Group type – Security**, **Group name – Autopilot pre-provisioned devices** and **Membership type – Assigned**.
16. Under **Members**, click **No members selected** and select the machine where the name equals the serial number of the device. Click **Select**.
17. Click **Create**.
18. In the navigation pane, click **Devices**.
19. Under **Device enrollment**, click on **Enroll devices**.
20. Under **Windows Autopilot Deployment Program**, click on **Deployment Profiles** > **+ Create profile** and select **Windows PC**.
21. On the **Basics** step, in the **Name** box, type **Autopilot preprovisioned deployment test profile** and click **Next**.
    Note: Leave the **Convert all targeted device to Autopilot** set to **No**.
22. On the **Out-of-box experience (OOBE)** tab, in the **Deployment mode** dropdown, select **User-Driven**.
23. In the **Join to Azure AD as** dropdown, select **Azure AD joined**.
24. For the **Microsoft Software License Terms** option, select **Hide**.
25. For the **Privacy Settings** option, select **Hide**.
26. For the **Hide change account options** option, select **Hide**.
27. For the **User account type** option, select **Standard**.
28. For **Allow White Glove OOBE** option, select **Yes**.
29. Click **Next**.
30. In the **Assignments** step, under **Included groups**, click **+ Add groups**, select the **Autopilot pre-provisioned devices** group just created and click **Select** and then click **Next**.
31. In the **Review + create** step, click **Create.**
32. Wait for some time for the device to be showing up in **Assigned devices** under **Autopilot preprovisioned deployment test profile**.
33. Click on **Devices > Enroll devices > Devices**, and you should be able to see the **PROFILE STATUS** as **Updating** and then further **Assigned**. Wait for a few moments.
34. Select the device imported and click **Assign user**.

35. Type in and select **Test User1** or **TU1@<AzureDomainName>.onmicrosoft.com** and click **Select**. Click **Save**. Wait for a moment while the device is assigned to the user.

Complete these steps on a Physical Machine (CLIENT8) that supports TPM 2.0 and Device Attestation and is installed with Windows 11, version 21H2

Technician Flow

1. Start the machine and on the **Let's name your device** screen, click **Skip for now**.
2. On the **Let's set things up for your work or school** screen, press the **Windows key five times** to view an additional options dialog. From that screen, choose the **Pre-provision with Windows Autopilot** option and then click **Next**.
3. On the **Pre-provision with Windows Autopilot** screen, the following information will be displayed about the device:
    a) The **Organization** - **<AzureDomainName>.onmicrosoft.com**
    b) The **Deployment profile** assigned to the device - **Autopilot preprovisioned deployment test profile**
    c) The Assigned user
    d) A QR code containing a unique identifier for the device, useful to look up the device in Intune to make any configuration changes (example: assigning a user, adding the device to any additional groups needed for app or policy targeting).
4. Validate the information displayed. If any changes are needed, make those and then **Refresh** to re-download the updated Autopilot profile details.
5. Click **Next** to begin the provisioning process.
6. Once the pre-provisioning process completes successfully, a message that says **Your device setup is complete** will be displayed with information about the device, including the same details presented previously (Organization, Deployment profile, Assigned user), as well as the elapsed time for the pre-provisioning steps.
7. Click **Reseal** to shut the device down. At that point, the device can be shipped to the end user.

    Note: If the pre-provisioning process fails, a message that says **Something went wrong** will be displayed with information about the device, and a QR code that can be used to review the results. **Diagnostic logs** can be gathered from the device, and then it can be **reset** to start the process over again.

User Flow

8. Start the machine and on the **Let's name your device** screen, click **Skip for now**.
9. On the **Let's set things up for your work or school** screen, enter the password for **TU1@<AzureDomainName>.onmicrosoft.com** then click **Next**.
10. Follow through the prompts for setting up a **PIN** for **Windows Hello**.
11. In the **All set!** pane, click **OK**.

Validate Azure AD Join and MDM Enrollment	12. Go to **Start** > **Settings**. 13. In the **Settings** app, browse to **Accounts** > **Access work or school**. 14. Confirm that **Connected by TU1@<AzureDomainName>.onmicrosoft.com /Connected to <CompanyName>'s Azure AD** is displayed and the **Info** button is displayed as well.
Complete these steps from an internet-connected Windows computer.	
Validate Azure AD and MDM Enrollment	15. Start Edge InPrivate mode. 16. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 17. On the left navigation bar, click **Azure Active Directory** > **Users** > **All users** > **Test User1**. 18. Click **Devices**. 19. Confirm that the device is listed there and the following settings are configured: JOIN TYPE: **Azure AD joined** MDM: **Microsoft Intune**

4.2.8 Autopilot for Existing Devices

Modern desktop management with Windows Autopilot enables you to easily deploy the latest version of Windows 11 to your existing devices. The apps you need for work can be automatically installed. Your work profile is synchronized, so you can resume working right away.

In this section, you will convert a Windows 10 domain-joined computer to Azure Active Directory-joined computer running Windows 11 by using Windows Autopilot.

Note: On **CLIENT7**, revert to the first checkpoint. Ensure it is in a cleaned state with no incompatible software installed. Software that can cause conflicts can be antivirus or firewall software which should be uninstalled if they exist. Also, during applying the checkpoints back and forth, there is a possibility that the VM loses domain trust relationship. In that case, disjoin and then rejoin the VM to the domain. While doing so, ensure that the VM is cleaned up in AD and ConfigMgr and after the domain-join the VM shows active in both AD and ConfigMgr. Also, to avoid any deployments to be triggered from **CM1** from the previous labs, delete those deployments in **CM1**.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Configure Enrollment Status Page	1. Start Edge InPrivate mode. 2. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Devices**. 4. Under **Device enrollment**, click **Enroll devices** > **Enrollment Status Page**.

5. For the **Default** setting, click **All users and all devices** link and then click **Properties**.
6. Click **Edit** next to **Settings**.
7. For the **Show app and profile installation progress** option, select **Yes** and then click **Review + save**.
8. Click **Save**.

Complete these steps on the CLIENT7 virtual machine.

Create the JSON File

9. Launch an elevated **Windows PowerShell** command window.
10. Run the command **Get-ExecutionPolicy**. If the result is **Restricted**, then run the command **Set-ExecutionPolicy Unrestricted** and accept all the prompts.
11. Execute the command - **[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12**.
12. Execute the command - **Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force**.
13. Then execute the command - **Install-Module AzureAD -Force**.
14. Then execute the command - **Install-Module WindowsAutopilotIntune -Force**.
15. Then execute the command - **Import-Module Microsoft.Graph.Intune -Force**.
16. Then execute the command - **Connect-MSGraph**. **Note:** If you get an error (Stack overflow at line:19) for the first time on the form. Click **OK**, close the form, ignore the error and re-execute the command.
17. On the form, log in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Sign in**.
18. Select **Consent on behalf of your organization** and click **Accept**.
19. Now, execute the command - **Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON**.

    Note: This is the data from the Autopilot profile created in the previous section and we are not going to make any changes at this moment to the file, however data can be changed as per the table provided here - https://docs.microsoft.com/en-us/windows/deployment/windows-Autopilot/existing-devices
20. Next, execute the command - **Get-AutopilotProfile | ConvertTo-AutopilotConfigurationJSON | Out-File c:\Windows\AutopilotConfigurationFile.json -Encoding ASCII**.
21. Copy the **AutopilotConfigurationFile.json** to **\\CM1\Packages$\AutopilotConfig** after creating a folder called **AutopilotConfig** on **CM1** under **C:\Packages**.

Complete these steps on the CM1 virtual machine.

Create a Package containing the JSON File	22. In the Configuration Manager Console, browse to **Software Library > Overview > Application Management > Packages**. 23. On the ribbon bar, click **Create Package**. 24. On the **Package** step, enter the following and click **Next**: Name: **Autopilot for Existing Devices Config** This package contains source files: **Selected** Source folder: **\\CM1\Packages$\AutopilotConfig** 25. On the **Program Type** step, select **Do not create a program** and click **Next**. 26. On the **Summary** step, click **Next**. 27. On the **Completion** step, click **Close**.
Create a Target Collection	28. Browse to **Assets and Compliance > Overview > Device Collections**. 29. Right-click **Device Collections** and click **Create Device Collection**. 30. On the **General** step, enter the following and click **Next**. Name: **Autopilot for Existing Devices** Limiting collection: **All Systems** 31. On the **Membership Rules** step, click **Add Rule > Direct Rule** and click **Next** on the **Welcome** step. 32. In the **Search for Resources** step, in the Value, enter **CLIENT7** and then click **Next**. 33. In the **Select Resources** step, select **CLIENT7** and then click **Next**. 34. On the **Summary** step, click **Next**. 35. On the **Completion** step, click **Close**. 36. Back on the **Membership Rules** step, click **Next**. 37. On the **Summary** step, click **Next**. 38. On the **Completion** step, click **Close**. 39. Ensure that the **CLIENT7** machine is present in the **Autopilot for Existing Devices** Collection.
Create an Autopilot for Existing Devices Task Sequence	40. Browse to **Software Library > Overview > Operating Systems > Task Sequences**. 41. Click **Create Task Sequence** from the ribbon bar. 42. On the **Create New Task Sequence** step, select **Deploy Windows Autopilot for existing devices** and click **Next**. 43. On the **Task Sequence Information** step, for the **Task sequence name** enter **Autopilot for Existing Devices**. 44. Click **Browse…**next to **Boot image**, select **Boot image (x64) 10.0.22000.1** and then click **OK** and then click **Next**. 45. On the **Install Windows** step, click **Browse…**next to **Image package**. Select **Windows 11 Enterprise 22H2 en-US** and then click **OK**. The Image index will be auto populated with **1 – Windows 10 Enterprise**. **Note**: The Windows 11 install.wim reads as Windows 10.

	46. On the **Install Windows** step, ensure that **Partition and format the target computer before installing the operating system** is selected and uncheck **Configure task sequence for use with BitLocker**. 47. On the **Install Windows** step, keep the rest as default settings and click **Next**. 48. On the **Install Configuration Manager** step, click **Next**. 49. On the **Include Updates** step, keep the default settings and click **Next**. 50. On the **Install Applications** step, keep the default settings and click **Next**. 51. On the **System Preparation** step, click **Browse…**next to **Package**, select **Autopilot for Existing Devices Config** and then click **OK** and then click **Next**. 52. On the **Summary** step, click **Next**. 53. On the **Completion** step, click **Close**.
Deploy Content to Distribution Point	54. Right-click **Autopilot for Existing Devices** task sequence and click **Distribute Content**. 55. On the **General** step, click **Next**. 56. On the **Content** step, click **Next**. 57. On the **Content Distribution** step, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 58. On the **Summary** step, click **Next**. 59. On the **Completion** step, click **Close**. Ensure that all content has been distributed from the **Monitoring > Overview > Distribution Status > Content Status**.
Deploy the Autopilot for Existing Devices Task Sequence	60. Right-click **Autopilot for Existing Devices** task sequence and click **Deploy**. 61. On the **General** step, click **Browse…** next to **Collection**, click **OK** on the prompt, select **Autopilot for Existing Devices**, click **OK** and then click **Next**. 62. On the **Deployment Settings** step, ensure **Available** is selected next to **Purpose** and **Only Configuration Manager Clients** is selected under **Make available to the following** option and then click **Next**. 63. On the **Scheduling** step, click **Next**. 64. On the **User Experience** step, click **Next**. 65. On the **Alerts** step, click **Next**. 66. On the **Distribution Points** step, select **Download all content locally before starting task sequence**, **Allow clients to use distribution points from the neighbor boundary group**, and **Allow clients to use distribution points from the default site boundary group** and click **Next**. 67. On the **Summary** step, click **Next**. 68. On the **Completion** step, click **Close**.
Complete these steps on the WIN7 virtual machine.	
Execute the Autopilot for	69. Click **Start > Control Panel**. 70. Click **System and Security > Configuration Manager**.

Existing Devices Task Sequence	71. Click the **Actions** tab and then click **Machine Policy Retrieval & Evaluation Cycle**. 72. Click **Run Now** and then click **OK**. 73. Click the notification or open the **Software Center**. 74. Under **Operating Systems** select **Autopilot for Existing Devices** and then click **Install**. 75. Click **Install** again on the prompt. 76. The Task Sequence will download content, reboot, format the drives and install Windows 11. The virtual machine will then proceed to be prepared for Autopilot. Once the task sequence has completed the virtual machine will boot into OOBE and provide an Autopilot experience. 77. Once **OOBE** has started, in the **Is this the right country or region?** screen, select **United States** then click **Yes**. 78. On the **Is this the right keyboard layout or input method?** screen, select **US** then click **Yes**. 79. On the **Want to add a second keyboard layout?** screen, click **Skip**. 80. On the **Please review the License Agreement** screen, click **Accept**. 81. On the **Let's name your device** screen, click **Skip for now**. 82. On the **Let's set things up for your work or school** screen, enter the username: **TU2@<AzureDomainName>.onmicrosoft.com**, then click **Next**. 83. Enter the password for **TU2@<AzureDomainName>.onmicrosoft.com** and then click **Sign in**. 84. Notice the **Setting up your device for work or school** screen. This is coming from the **Enrollment Status Page**. 85. On the **Choose privacy settings for your device** screen, accept the defaults and click **Accept**. 86. On the **Use Windows Hello with your account** screen, click **OK**. 87. Follow through the prompts for setting up a **PIN** for **Windows Hello**. 88. On the **All set!** screen, click **OK**. 89. You will be logged in to the desktop.

5 Servicing Windows 11

Deploying Windows 10 and Windows 11 is simpler than with previous versions of Windows. When migrating from earlier versions of Windows, you can use an easy in-place upgrade process to automatically preserve all apps, settings, and data. Afterwards, deployment of feature updates is equally simple.

5.1 Servicing Windows 11 using Group Policy

In this activity, you will configure Windows Update for Business deferral policies using Group Policy. Before configuring the Windows Update for Business Group Policy settings, consider a deployment strategy for updates and feature updates in your environment. For more guidance, see Walkthrough: use Group Policy to configure Windows Update for Business.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Configure a Deployment Ring	1. Under **Server Manager**, open **Tools>Group Policy Management**. 2. Expand **Forest: corp.contoso.com > Domains > corp.contoso.com**. 3. Right-click **corp.contoso.com** and select **Create a GPO in this domain, and Link it here**. 4. In the **New GPO** dialog box, type **Windows Update for Business – Group 1** for the name of the new GPO and click **OK**. 5. Right-click the **Windows Update for Business – Group 1** GPO, and then click **Edit**. 6. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Update > Defer Windows Update**. 7. Right-click **Select when Feature Updates are received**, and then click **Edit**. 8. In the **Select when Preview Builds and Feature Updates are received** Group Policy setting configuration, **Enable** the policy, and then configure the options – **Select the branch readiness level for the feature updates you want to receive**, **After a feature update is released, defer receiving it for this many days** and **Pause Feature Updates starting**. Click **Apply** and **OK**. 9. Right-click **Select when Quality Updates are received**, and then click **Edit**. 10. In the **Select when Quality Updates are received** Group Policy setting configuration, **Enable** the policy, and then configure the options – **After a quality update is released, defer receiving it for this many days** and **Pause Quality Updates starting**. Click **Apply** and **OK**.

5.2 Servicing Windows 11 with Configuration Manager

Windows 10 delivered a new model for organizations to deploy and upgrade Windows by providing updates to features and capabilities through a continuous process. Windows 11 continues to use this same strategy. Configuration Manager provides a window of the state of Windows in your environment, create servicing plans to form deployment rings and ensure that the Windows 11 machines are kept up to date.

In this section, you will go through how to configure Configuration Manager to support Windows as a Service.

5.2.1 Configure Software Update Point

In this activity, you will configure the Software Update Point to download Windows 11 Servicing Feature Updates.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Configure Software Update Point Site Component	1. Open the **Configuration Manager Console** from the Start Menu. 2. Browse to **Administration > Overview > Site Configuration > Sites**. 3. Right-click on **CHQ – Contoso Headquarters** and select **Configure Site Components > Software Update Point**. 4. For the initial sync, make sure that nothing is selected. On the **Classifications** tab, ensure that everything is unchecked. On the **Products** tab, ensure that everything is unchecked. 5. Browse to **Software Library > Overview > Software Updates > All Software Updates**. 6. In the **Ribbon**, click **Synchronize Software Updates** and click **Yes**. 7. Open **CMTrace.exe** and then open the log file called **wsyncmgr.log** (C:\Program Files\Microsoft Configuration Manager\Logs). Look for the line that says "**Done synchronizing SMS with WSUS Server CM1**". **Note:** This may take up to 20 minutes or more to complete. 8. Browse to **Administration > Overview > Site Configuration > Sites**. 9. Right-click on **CHQ – Contoso Headquarters** and select **Configure Site Components > Software Update Point**. 10. On the **Classifications** tab, select **Security Updates**, **Updates**, and **Upgrades**. 11. On the **Windows 10 Servicing Prerequisite** window, click **OK**. 12. On the **Products** tab, select **Microsoft 365 Apps/Office 2019/Office LTSC**, **Microsoft Edge** (under **Windows**), and **Windows 11**. 13. On the **Languages** tab, verify that only **English** is selected and then click **Apply** and **OK**.

Synchronize Software Update	14. Browse to **Software Library > Overview > Software Updates > All Software Updates**. 15. In the ribbon, click **Synchronize Software Updates** and click **Yes**. **Note**: The synchronization may take up to an hour or more depending on the speed of the internet connection.

5.2.2 Configure Servicing Plan

In this activity, you will configure Servicing Plans in Configuration Manager to form deployment rings and ensure that Windows 11 systems are kept up to date when new builds are released.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Validate that Windows 11 Feature Updates are Available	1. From the **Configuration Manager Console**, browse to **Software Library > Overview > Windows Servicing > All Windows Feature Updates**. 2. On the **Search** bar, type **Upgrade to Windows 11 (business editions) en-us x64** then press **Enter**. 3. Validate that the feature update metadata for **Upgrade to Windows 11 (business editions) en-us x64** is available. **Note:** It can take some time for the **CLIENT7** machine to be detected in Configuration Manager for the **"Required"** update. Run **Machine Policy Retrieval & Evaluation Cycle** and **Software Updates Scan Cycle** on the machine to speed up the process.
Create Servicing Collections	4. From the **Configuration Manager Console**, browse to **Assets and Compliance**. 5. Right-click on **Device Collections** and select **Create Device Collection**. 6. On the **General** step, enter the following then click **Next**. Name: **Windows 11 Servicing Upgrade** Limiting Collection: **All Desktop and Server Clients** 7. On the **Membership Rules** step, click **Next**. 8. On the warning dialog box, click **OK**. 9. On the **Summary** step, click **Next**. 10. On the **Completion** step, click **Close**.
Create a Servicing Plan for Semi-Annual Channel Machines	11. From the **Configuration Manager Console**, browse to **Software Library > Overview > Windows Servicing > Servicing Plans**. 12. On the ribbon, click **Create Servicing Plan**. 13. On the **General** step, enter the following then click **Next**. Name: **Windows 11 Servicing Upgrade**

14. On the **Servicing Plan** step, enter the following then click **Next**.

    Target Collection: **Windows 11 Servicing Upgrade**

15. On the **Deployment Deferral** step, leave the defaults and click **Next**.
16. On the **Upgrades** step, select **Superseded** and click **items to find**.
17. On the **Search Criteria**, select **No** for the **Specify the value to search for** and click **OK**.
18. On the **Upgrades** step, select **Title** and click **items to find**.
19. On the **Search Text** window, in the textbox enter **"Upgrade to Windows 11 (business editions) en-us x64"** (include the quotation marks) then click **Add**.
20. On the **Search Text** window, click **OK**.
21. On the **Upgrades** step, click **Preview**.
22. On the **Preview updates** window, verify that the **Upgrade to Windows 11** feature update is listed then click **Close**.
23. On the **Upgrades** step, click **Next**.
24. On the **Deployment Schedule** step, under **Installation deadline** select **As soon as possible** then click **Next**.
25. On the **User Experience** step, under **User notifications** select **Display in Software Center and show all notifications**, under **Deadline behavior** select **System restart (if necessary)** and then click **Next**.
26. On the **Deployment Package** step, select **Create a new deployment package**, enter the following then click **Next**.

    Name: **Windows 11 Servicing Upgrade**

    Package source: **\\CM1\Packages$\W11ServicingUpgrade**

    <u>Note:</u> Create a folder called **W11ServicingUpgrade** in **C:\Packages**.

27. On the **Distribution Points** step, click **Add > Distribution Point**.
28. On the **Add Distribution Points** window, select **CM1.CORP.CONTOSO.COM** then click **OK**.
29. On the **Distribution Points** step, click **Next**.
30. On the **Download Location** step, click **Next**.
31. On the **Language Selection** step, click **Next**.
32. On the **Summary** step, click **Next**.
33. On the **Completion** step, click **Close**.
    <u>Note:</u> Ensure the option **Download software updates from distribution point and install** is selected **in all cases** in the **Servicing Plan Properties** under **Download Settings** as well as in the **Software Update Group's**, **Deployment Properties** under **Download Settings**.

5.2.3 Service a Windows 10 21H2 Client

In this activity, you will test the servicing plan on a Windows 10 21H2 virtual machine.

Note: The trial download of the Windows Enterprise media does not allow an In-Place Upgrade to be performed. To complete this lab, both the Windows 10 Enterprise media and the Windows 11 Enterprise media must be sourced from either MSDN Subscriber Downloads or from the Volume Licensing Site of the customer.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Move the Test Device to Semi-Annual Channel Collection	1. From the **Configuration Manager Console**, browse to **Assets and Compliance > Overview > Devices**. 2. Right-click on **CLIENT7** and select **Add Selected Items > Add Selected Items to Existing Device Collection**. 3. On the **Select Collection** window, browse to and select **Root > Windows 11 Servicing Upgrade** then click **OK**. 4. Browse to **Assets and Compliance > Overview > Device Collections > Windows 11 Servicing Upgrade**. 5. On the ribbon, click **Collection | Update Membership | Yes** and press **F5**. 6. Verify that the **CLIENT7** machine is shown within the collection.
Force the Servicing Plan to Run	7. Browse to **Software Library > Overview > Windows Servicing > Servicing Plans**. 8. Select **Windows 11 Servicing Upgrade** and from the ribbon click **Run Now**. 9. On the dialog box, click **OK**.
Complete these steps on the CLIENT7 virtual machine.	
Refresh the Client's Policy	10. Logon to **CLIENT7** machine as **corp\labadmin**. 11. Open the **Control Panel**. 12. On the **All Control Panel Items** window, click on **Configuration Manager.** 13. On the **Configuration Manager Properties** window, go to the **Actions** tab. 14. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** then click **Run Now**. 15. On the dialog box, click **OK**. 16. On the **Actions** tab, select **Software Updates Scan Cycle** then click **Run Now**. 17. On the dialog box, click **OK**. 18. On the **Actions** tab, select **Software Updates Deployment Evaluation Cycle** then click **Run Now**. 19. On the dialog box, click **OK**. 20. On the **Configuration Manager Properties** window, click **OK**. 21. A notification will appear after which once the **Software Center** is launched, under the **Installation Status**, the feature update will start **downloading** and **installing** automatically. 22. On the prompt, click **Restart** and then click **Restart** again for a force restart.

23. The upgrade process will continue.
24. Once restarted and logged in, the version of windows will be **Windows 11 Version 21H2 (Build 22000.x)**.

6 Managing Windows 11

6.1 Device Management for Windows 11 using Microsoft Intune

In this lab, you will set up and configure Windows 11 Mobile Device Management (MDM) with Microsoft Intune.

6.1.1 Enroll a Windows 11 Device

This section outlines how to enroll a Windows 11 device into Microsoft Intune for MDM.

Task	Detailed Steps
Complete these steps on the CLIENT3 virtual machine.	
Enroll a Windows 11 Device in Intune	1. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. Click **Enroll only in device management**. 4. The **Setup a work or school account** dialog box will show, asking for your account to enroll the device. 5. Provide the **TU1@<AzureDomainName>.onmicrosoft.com** account and click **Next**. 6. In the **Microsoft Intune Enrollment** page, enter the **password** then click **Sign in**. Click **Got it**. 7. In the **Settings** app, you should see that the device is now connected to the corporate MDM. 8. Select **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <CompanyName> MDM** then click **Info**. 9. Click **Sync** and confirm that the sync was **successful**.
Complete these steps from an internet-connected Windows computer.	
Check Windows 11 Device Enrollment in Microsoft Intune	10. Start Edge InPrivate mode. 11. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 12. On the left navigation bar, select **Devices** > **All devices**. 13. Click on the Windows 11 device that you have enrolled (**CLIENT3**). Observe the information that has been collected about the device in all the tabs. **Note:** It may take up to 15 minutes (or more) for it to show up in the Intune portal.

6.1.2 Configure Software Updates

In this activity, you will configure and manage **Windows 11 Update Rings** in Intune to form deployment rings and ensure that Windows 11 systems are kept up to date when new builds are released. An update ring includes a group of settings that configures when and how Windows 11 updates get installed. For more details see Manage software updates in Intune.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Create Ring Policy	1. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 2. Select **Devices > Update rings for Windows 10 and later**. 3. Click "**+ Create profile**" to create an Update Ring policy. 4. In the **Basics** step, enter a **Name**, a **Description** (optional), and then click **Next**. 5. In the **Update ring settings** step, enter the following information and then click **Next**: • **Microsoft product updates**: Choose to scan for app updates from Microsoft Update. • **Windows drivers**: Choose to include or exclude Windows Update drivers during updates. • **Quality update deferral period (days)**: Enter the number of days for which quality updates are deferred. You can defer receiving these Quality Updates up to 30 days from their release. • **Feature update deferral period (days)**: Enter the number of days for which Feature Updates are deferred. You can defer receiving Feature Updates up to 365 days from their release. • **Upgrade Windows 10 devices to Latest Windows 11 release**: Set to upgrade eligible Windows 10 devices to latest Windows 11 release. • **Set feature update uninstall period (2 – 60 days)**: Enter the number of days within which Feature Updates can be uninstalled. • **Enable pre-release builds/Select pre-release channel:** Enable pre-release builds if you want devices to be on a Windows Insider channel. • **Automatic update behavior** with **Active hours start** and **Active hours end**: Choose how automatic updates are installed, when to restart or reboot. For details, see Update/AllowAutoUpdate. • **Restart checks**: Enabled by default. When you restart a device, there are some checks that occur, including checking for active users, battery levels, running games, and more. To skip these checks when you restart a device, select **Skip**. • **Option to pause Windows updates:** An option in Windows Update that, when enabled, lets device users pause updates for a certain number of days. • **Option to check for Windows updates:** A button in Windows Update that, when enabled, lets device users check the update service for updates. • **Change notification update level:** Specifies what Windows Update notifications users see.

	• **Use deadline settings** with **Deadline for feature updates**, **Deadline for quality updates**, **Grace period** and **Auto reboot before deadline:** Allow user to use deadline settings.
Assign Ring	6. In the **Assignments** step, under **Included groups**, choose **+ Add groups**, and then choose a group. 7. When finished, choose **Select | Next** to complete the assignment. 8. In the **Review + create** step, click **Create**.
View Update Compliance	7. Select **Devices > Update rings for Windows 10 and later**. You can see information about the status of any update rings you assigned to devices and users. ▪ Select the update ring that was just created. On the **Overview** page, you can see information about the status of the specific deployment ring you assigned to devices and users.
Pause Updates	11. Still on the **Overview** page, click **Pause** on the top menu and then select either **Feature** or **Quality**, then click **OK**.
Uninstall the Latest Software Updates	12. Still on the **Overview** page, click **Uninstall** on the top menu and then select either **Feature** or **Quality**, then click **OK**.

6.1.3 Configure Policy Settings and Policies based on OMA-URI

This section outlines how to configure Policies for Windows 11 in Intune available through the Intune Interface and a Policy through OMA-URI.

Use the Microsoft Intune Windows Phone OMA-URI Policy to deploy OMA-URI (Open Mobile Alliance Uniform Resource Identifier) settings that can be used to control features on Windows Phone Devices. These are standard settings that many mobile device manufacturers use to control device features.

This capability is intended to allow you to deploy Windows 11 Settings that are not configurable with an Intune Policy. For information about the settings you can configure with these Policies, see Configure Security Policy for Mobile Devices in Microsoft Intune.

For help creating OMA-URI Settings for Windows 11 Services, see Configuration service provider reference documentation.

Note: If any of the below policies conflicts with the policies from the previous labs, delete the policies from the previous labs.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	

Create an OMA-URI Policy to Disable Cortana

1. Start Edge InPrivate mode.
2. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**.
3. On the left navigation bar, click **Devices > Configuration profiles > + Create profile**.
4. Under **Platform**, select **Windows 10 and later**.
5. Under **Profile type**, select **Templates**, for **Template name** select **Custom** and click **Create**.
6. Under the **Basics** step, enter the following information and click **Next**:
   In the **Name** field, type **Disable Cortana**.
7. Under the **Configuration settings** step, enter the following information and click **Next**:
   Click **Add**.
   In the **Name** field enter **Disable Cortana**.
   In the **OMA-URI** field enter (Case sensitive and starting with a period):
   ./Vendor/MSFT/Policy/Config/Experience/AllowCortana
   For **Data type** select **Integer**.
   For **Value** enter **0** (0 means the setting is not allowed).
   Click **Save**.
8. Under the **Assignments** step, enter the following information and click **Next**:
   Under **Included groups** click **+ Add groups**.
   Type **Sales** and select it.
   Click **Select**.
9. Under the **Applicability Rules** step, click **Next**.
10. Under the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine.

Confirm the URI Configurations are Applied

11. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**.
12. In the **Settings** app, browse to **Accounts > Access work or school**.
13. Select **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <CompanyName> MDM** then click **Info**.
14. Click **Sync** to force a policy update and confirm that the sync was **successful**.
15. Note that when you click **Start > All apps > Cortana**, it says "**Cortana is disabled. To use Cortana you need to get permission from your administrator**".

Complete these steps from an internet-connected Windows computer.

Configure Windows Defender

16. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**.
17. On the left navigation bar, click **Devices > Configuration profiles > + Create profile**.
18. Under **Platform**, select **Windows 10 and later**.

19. Under **Profile type**, select **Templates**, for **Template name** select **Custom** and click **Create**.
20. Under the **Basics** step, enter the following information and click **Next**:
    In the **Name** field, type **Allow Real Time Protection on Win 11 Desktops**.
21. Under the **Configuration settings** step, enter the following information and click **Next**:
    Click **Add**.
    In the Name field type **Allow Real Time Protection on Win 11 Desktops**.
    In the **OMA-URI** field enter (Case sensitive and starting with a period):
    ./Vendor/MSFT/Policy/Config/Defender/AllowRealtimeMonitoring
    For **Data type** select **Integer**.
    For **Value** enter **1** (1 means the setting is allowed).
    Click **Save**.
22. Under the **Assignments** step, enter the following information and click **Next**:
    Under Included groups, click **+ Add groups**.
    Type **Sales** and select it.
    Click **Select**.
23. Under the **Applicability Rules** step, click **Next**.
24. Under the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine.

Verify Configuration is Applied

25. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**.
26. In the **Settings** app, browse to **Accounts > Access work or school**.
27. Select **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <CompanyName> MDM** then click **Info**.
28. Click **Sync** to force a policy update and confirm that the sync was **successful**.
29. In the **Settings** app, go back to **Privacy & security > Windows Security** and click **Open Windows Security**.
30. In the **Windows Security** app, navigate to **Virus & threat protection** and click **Manage settings** under **Virus & threat protection settings**.
31. Confirm that the **Real-time protection** setting is turned **On** and a message "This setting is managed by your administrator". The ability to turn off this setting will be disabled.

6.2 Dynamic Management with Windows 11

In this lab, you will set up and configure dynamic management policies for Windows 11. For a list of available dynamic management policies, visit: https://docs.microsoft.com/en-us/windows/client-management/mdm/dynamicmanagement-csp.

Note: If any of the below policies conflicts with the policies from the previous labs, delete the policies from the previous labs.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Configure Dynamic Management Policy	1. Close all browser windows. 2. Start Edge InPrivate mode. 3. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Devices > Configuration profiles> + Create profile**. 5. Under **Platform**, select **Windows 10 and later**. 6. Under **Profile type**, select **Templates**, for **Template name** select **Custom** and click **Create**. 7. Under the **Basics** step, enter the following information and click **Next**: In the **Name** field, type **DisableCameraInCorporateNetwork**. 8. Under the **Configuration settings** tab, enter the following information and click **Next**: Click **Add**. In the **Name** field enter **SettingsPack**. In the **OMA-URI** field enter (Case sensitive and starting with a period): **./Vendor/MSFT/DynamicManagement/Contexts/NetworkBased/SettingsPack** For **Data type** select **String**. For **Value** enter **<SyncML>** **<SyncBody>** **<Replace>** **<CmdID>1331</CmdID>** **<Item>** **<Target>** **<LocURI>./Vendor/MSFT/Policy/Config/Camera/AllowCamera</LocURI>** **</Target>** **<Meta>** **<Format xmlns="syncml:metinf">int</Format>** **</Meta>** **<Data>0</Data>** **</Item>** **</Replace>** **<Final/>** **</SyncBody>** **</SyncML>** Click **Save**. Click **Add** again.

In the **Name** field enter **SignalDefinition**.

In the **OMA URI** field enter (Case sensitive and starting with a period):

./Vendor/MSFT/DynamicManagement/Contexts/NetworkBased/SignalDefinition

For **Data type** select **String**.

For **Value** enter

```
<rule schemaVersion="1.0">
  <signal type="ipConfig">
        <ipv4Gateway>10.0.0.254</ipv4Gateway>
  </signal>
</rule>
```

Click **Save**.

Click **Add** again.

In the **Name** field enter **NotificationsEnabled2**.

In the **OMA-URI** field enter (Case sensitive and starting with a period):

./Vendor/MSFT/DynamicManagement/NotificationsEnabled

For **Data type** select **Boolean**.

For **Value** select

True

Click **Save**.

9. Under the **Assignments** step, enter the following information and click **Next**:

   Under **Included groups**, click **+ Add groups.**

   Type **Sales** and select it.

   Click **Select**.
10. Under the **Applicability Rules** step, click **Next**.
11. Under the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine.

Verify Policy is Applied

12. Log in to the virtual machine as **.\Administrator** and go to **Start > Settings**.
13. In the **Settings** app, browse to **Accounts > Access work or school**.
14. Select **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <CompanyName> MDM** then click **Info**.
15. Click **Sync** to force a policy update and confirm that the sync was **successful**.
16. From the **Virtual Machine Connection** window, got to **File > Settings**.
17. In the **Settings** window, under **Network Adapter**, change the **Virtual switch** from **HYD-CorpNet** to **Not connected** and click **OK**.
18. In the **Settings** app, go to **Privacy & security > Camera**.

Note: Camera is currently turned On and unmanaged because the machine is in the internet network.

19. From the **Virtual Machine Connection** window, go to **File > Settings**.
20. In the **Settings** window, under **Network Adapter**, change the **Virtual switch** from **Not connected** to **HYD-CorpNet** and click **OK**.

21. In the **Settings** app, refresh the **Privacy & security > Camera** view.
22. Confirm ***Some of these settings are managed by your organization** is shown.

Note: Camera is turned Off and fully managed because the machine is in the corporate network.

7 Deploying Microsoft 365 Apps for enterprise

Microsoft 365 Apps is the modern client suite with Microsoft 365. The suite is like other versions of Office but there are differences:

- Licensing
- Deployment
- Updates (Channel Management)

For further information, go to About Microsoft 365 Apps in the enterprise

Microsoft 365 Apps can be deployed in 3 scenarios:

- Enterprise Managed
- Locally Managed
- Cloud Managed

For further information, go to Plan your enterprise deployment of Microsoft 365 Apps

Microsoft 365 Apps for enterprise is updated leveraging Channels. The 3 channels are:

- Current
- Monthly Enterprise
- Semi-Annual Enterprise

For further information, go to Overview of update channels for Microsoft 365 Apps.

7.1 Cloud Managed Deployment

In this activity, deploy Microsoft 365 Apps for enterprise from the Content Delivery Network (CDN) using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

Task	Detailed Steps
Complete these steps on the CLIENT2 virtual machine.	
Download Office Deployment Tool	1. Logon as corp\labadmin. 2. On the taskbar, open File Explorer and browse to **C:\** and create a folder named **ODT**. 3. Open Microsoft Edge and browse to the URL below. https://www.microsoft.com/en-us/download/details.aspx?id=49117 4. From the website, click **Download**.

Extract ODT	5. From the **Downloads** directory, double-click to start the extraction of the ODT and accept the UAC prompt if required. 6. Accept the License Terms and click **Continue**. 7. Navigate to **C:\ODT** and click **OK**. 8. Click **OK** after successful Extraction.
Create Installation XML	9. The Sample Configurations for all Office Applications – Current Channel from the https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options can be referenced. 10. Browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 11. In the **Current Channel** Column, record the version number of the previous month. 12. Browse to the URL below. https://config.office.com/deploymentsettings 13. Under **Products and releases**, under **Architecture**, select **64-bit**. 14. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 15. Under **Products and releases**, under **Update channel**, select **Current Channel** and select the **Version** that was recorded earlier and click **Next**. 16. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 17. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 18. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 19. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 20. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 21. Under **General**, click **Next**. 22. Under **Application preferences**, click **Finish**. 23. Click **Export** and select **Keep Current Settings** and then click **OK**. 24. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 25. Save the file to **C:\ODT**. 26. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings
Deploy Microsoft 365 Apps	27. Type **CMD** in the "Type here to search". 28. Right-click **Command Prompt**. 29. Select **Run as administrator**. Accept the UAC prompt if required. 30. Change directory to **C:\ODT**.

	31. Type **setup.exe /configure newconfiguration.xml**. 32. Press Enter. 33. Office will begin the installation. 34. Click **Close**.
Update Microsoft 365 Apps	35. Click **Start**. 36. Select **Word**. 37. Click **Blank document**. 38. Click **File**. 39. Click **Account**. 40. Click **Update Options**. 41. Click **Update Now**. **Note:** Microsoft 365 Apps for enterprise will download the updates and apply the updates from the CDN. 42. Click **Continue** when prompted to close the applications requiring updates. **Note:** Microsoft 365 Apps for enterprise only requires the applications being updated to be closed and will be re-launched once the update is done. 43. Open Microsoft Edge and browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 44. In the **Current Channel** Column record the version number of the current month. 45. Click **File**. 46. Click **Account**. 47. Compare the **Office Updates Version and Build Number** to the version recorded of the current month. 48. Close Word.
Remove an Application from Microsoft 365 Apps	49. Go back to the already opened https://config.office.com/deploymentsettings 50. Under **Products and releases**, under **Update Channel**, select the **Version** and **Build** that is currently installed. 51. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 52. Click **Export** and select **Keep Current Settings** and then click **OK**. 53. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 54. Save the file to **C:\ODT**. 55. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 56. Back in CMD, type **setup.exe /configure removeaccess.xml**. 57. Press Enter. 58. Office will begin the installation. 59. Click **Close**. **Note:** The Microsoft Access icon will not be displayed during the installation.

Add a Language to Microsoft 365 Apps	60. Go back to the already opened https://config.office.com/deploymentsettings **Note:** If creating a Language, set the first language to the client’s culture language. If the first language does not match the client’s culture set, then the chosen language will be the Shell UI language. 61. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 62. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 63. Click **Export** and select **Keep Current Settings** and then click **OK**. 64. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 65. Save the file to **C:\ODT**. 66. Back in CMD, type **setup.exe /configure addspanish.xml**. 67. Press Enter. 68. Office will begin the installation. 69. Click **Close**. 70. Type **Control Panel** in the “Type here to search” and press Enter. 71. Click on **Programs**. 72. Click on **Programs and Features**. 73. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed.

7.2 Locally Managed Deployment

In this activity, you will deploy Microsoft 365 Apps from a local file share using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

Task	Detailed Steps
Complete these steps on the CLIENT2 virtual machine.	
Create a File Share for Microsoft 365 Apps	1. Logon as corp\labadmin. 2. On the taskbar, open File Explorer and browse to **C:\Packages** and create a folder named **MC**. The **Packages** folder must be created in advance in case it is not created. 3. Right-Click on the **MC** folder and select **Give access to**. 4. Select **“Specific people…”**. 5. Select **Everyone** from the drop down. 6. Click **Add**. 7. Set the Permission Level for Everyone to **Read/Write**. 8. Click **Share**. 9. Record the Share Path.

	10. Click **Done**.
Download Office Deployment Tool	11. Open Microsoft Edge and browse to the URL below. https://www.microsoft.com/en-us/download/details.aspx?id=49117 12. From the website, click **Download**.
Extract ODT	13. From the **Downloads** directory, double-click to start the extraction of the ODT and accept the UAC prompt if required. 14. Accept the License Terms and click **Continue**. 15. Navigate to **C:\Packages\MC** and click **OK**. 16. Click **OK** after successful Extraction.
Create Installation XML	17. The Sample Configurations for all Office Applications – Current Channel from the https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options can be referenced. 18. Browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 19. In the **Current Channel** Column, record the version number of the previous month. 20. Browse to the URL below. https://config.office.com/deploymentsettings 21. Under **Products and releases**, under **Architecture**, select **64-bit**. 22. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 23. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 24. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 25. Under **Installation**, under **Installation options,** select **Local source** and specify the **Source path** as **\\CLIENT2\MC** and click **Next**. 26. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 27. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 28. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 29. Under **General**, click **Next**. 30. Under **Application preferences**, click **Finish**. 31. Click **Export** and select **Keep Current Settings** and then click **OK**. 32. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 33. Save the file to **C:\Packages\MC**.

	34. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings
Download Microsoft 365 Apps	35. Type **CMD** in the "Type here to search". 36. Right-click **Command Prompt**. 37. Select **Run as administrator**. Accept the UAC prompt if required. 38. Change directory to **C:\Packages\MC**. 39. Type **setup.exe /download newconfiguration.xml**. 40. Press Enter. Office will begin the download.
Deploy Microsoft 365 Apps (Offline from a Local Share)	41. Back in CMD, type **setup.exe /configure newconfiguration.xml**. 42. Press Enter. 43. Office will begin the installation. Click **Close**.
Update Microsoft 365 Apps (Offline from a Local Share)	44. Open Microsoft Edge and browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 45. In the **Current Channel** Column, record the version number of the current month. **Note:** Unlike Cloud Managed, the monthly build of Microsoft 365 Apps needs to be downloaded to the local file share. 46. Go back to the already opened https://config.office.com/deploymentsettings 47. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is for the current month. 48. Under **Update and upgrade**, under **Update and upgrade options**, select **Local source** and specify the **Source path** as **\\CLIENT2\MC**. 49. Click **Export** and select **Keep Current Settings** and then click **OK**. 50. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **update.xml** and click **Export**. 51. Save the file to **C:\Packages\MC**. 52. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 53. Back in CMD, type **setup.exe /download update.xml**. 54. Press Enter. Office will begin the download. 55. Back in CMD, type **setup.exe /configure update.xml**. 56. Press Enter. 57. Office will begin the installation. Click **Close**. 58. Browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 59. In the **Current Channel** Column, record the version number of the current month. 60. In Word, **File | Account**, compare the **Office Updates Version and Build Number** to the version recorded of the current month. 61. Close Word.

Remove an Application from Microsoft 365 Apps	62. Go back to the already opened https://config.office.com/deploymentsettings 63. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 64. Click **Export** and select **Keep Current Settings** and then click **OK**. 65. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 66. Save the file to **C:\Packages\MC**. 67. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 68. Back in CMD, type **setup.exe /configure removeaccess.xml**. 69. Press Enter. 70. Office will begin the installation. 71. Click **Close**. **Note:** The Microsoft Access icon will not be displayed during the installation.
Add a Language to Microsoft 365 Apps (Offline from a Local Share)	72. Go back to the already opened https://config.office.com/deploymentsettings **Note:** If creating a Language, set the first language to the client's culture language. If the first language does not match the client's culture set, then the chosen language will be the Shell UI language. 73. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 74. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 75. Click **Export** and select **Keep Current Settings** and then click **OK**. 76. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 77. Save the file to **C:\Packages\MC**. 78. Back in CMD, type **setup.exe /download addspanish.xml**. 79. Press Enter. Office will begin the download. 80. Back in CMD, type **setup.exe /configure addspanish.xml**. 81. Office will begin the installation. 82. Click **Close**. 83. Type **Control Panel** in the "Type here to search" and press Enter. 84. Click on **Programs**. 85. Click on **Programs and Features**. 86. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed.

7.3 Microsoft 365 Apps deployment on Non-AD Joined Devices

In this activity, you will deploy Microsoft 365 Apps on a Non-AD Joined Device (**CLIENT4**) using both methods – Cloud Managed and Locally Managed. You will use a combination of Office Customization Tool (OCT) and Office Deployment Tool (ODT) to create the configuration XML and perform activities like deployment of Microsoft 365 Apps, update/upgrade Microsoft 365 Apps, remove an application, add a language and remove prior MSI versions of Microsoft 365 Apps.

Cloud Managed Deployment

In this activity, deploy Microsoft 365 Apps from the Content Delivery Network (CDN) using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365 Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

Task	Detailed Steps
Complete these steps on the CLIENT4 virtual machine.	
Download Office Deployment Tool	1. Logon as .\Administrator. 2. On the taskbar, open File Explorer and browse to **C:\** and create a folder named **ODT**. 3. Open Microsoft Edge and browse to the URL below. https://www.microsoft.com/en-us/download/details.aspx?id=49117 4. From the website, click **Download**.
Extract ODT	5. From the **Downloads** directory, double-click to start the extraction of the ODT and accept the UAC prompt if required. 6. Accept the License Terms and click **Continue**. 7. Navigate to **C:\ODT** and click **OK**. 8. Click **OK** after successful Extraction.
Create Installation XML	9. The Sample Configurations for all Office Applications – Current Channel from the https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options can be referenced. 10. Browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 11. In the **Current Channel** Column, record the version number of the previous month. 12. Browse to the URL below. https://config.office.com/deploymentsettings 13. Under **Products and releases**, under **Architecture**, select **64-bit**. 14. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 15. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 16. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 17. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 18. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected.

	19. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 20. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 21. Under **General**, click **Next**. 22. Under **Application preferences**, click **Finish**. 23. Click **Export** and select **Keep Current Settings** and then click **OK**. 24. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 25. Save the file to **C:\ODT**. 26. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings
Deploy Microsoft 365 Apps	27. Type **CMD** in the "Type here to search". 28. Right-click **Command Prompt**. 29. Select **Run as administrator**. Accept the UAC prompt if required. 30. Change directory to **C:\ODT**. 31. Type **setup.exe /configure newconfiguration.xml**. 32. Press Enter. 33. Office will begin the installation. 34. Click **Close**.
Update Microsoft 365 Apps	35. Click **Start**. 36. Select **Word**. 37. Click **Blank document**. 38. Click **File**. 39. Click **Account**. 40. Click **Update Options**. 41. Click **Update Now**. **Note:** Microsoft 365 Apps will download the updates and apply the updates from the CDN. 42. Click **Continue** when prompted to close the applications requiring updates. **Note:** Microsoft 365 Apps only requires the applications being updated to be closed and will be re-launched once the update is done. 43. Open Microsoft Edge and browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 44. In the **Current Channel** Column record the version number of the current month. 45. Click **File**. 46. Click **Account**.

	47. Compare the **Office Updates Version and Build Number** to the version recorded of the current month. 48. Close Word.
Remove an Application from Microsoft 365 Apps	49. Go back to the already opened https://config.office.com/deploymentsettings 50. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is currently installed. 51. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 52. Click **Export** and select **Keep Current Settings** and then click **OK**. 53. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 54. Save the file to **C:\ODT**. 55. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 56. Back in CMD, type **setup.exe /configure removeaccess.xml**. 57. Press Enter. 58. Office will begin the installation. 59. Click **Close**. **Note:** The Microsoft Access icon will not be displayed during the installation.
Add a Language to Microsoft 365 Apps	60. Go back to the already opened https://config.office.com/deploymentsettings **Note:** If creating a Language, set the first language to the client's culture language. If the first language does not match the client's culture set, then the chosen language will be the Shell UI language**.** 61. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 62. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 63. Click **Export** and select **Keep Current Settings** and then click **OK**. 64. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 65. Save the file to **C:\ODT**. 66. Back in CMD, type **setup.exe /configure addspanish.xml**. 67. Press Enter. 68. Office will begin the installation. 69. Click **Close**. 70. Type **Control Panel** in the "Type here to search" and press Enter. 71. Click on **Programs**. 72. Click on **Programs and Features**. 73. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed.

Locally Managed Deployment

In this activity, you will deploy Microsoft 365 Apps from a local file share using the Office Deployment Tool (ODT), configuration XML, setting Current Channel as the update channel, update Microsoft 365

Apps, remove an application and add a language from an already deployed installation, and remove prior MSI versions of Microsoft 365 Apps.

Task	Detailed Steps
Complete these steps on the CLIENT4 virtual machine.	
Create a File Share for Microsoft 365 Apps	1. Logon as .\Administrator. 2. On the taskbar, open File Explorer and browse to **C:\Packages** and create a folder named **MC**. The **Packages** folder must be created in advance in case it is not created. 3. Right-Click on the **MC** folder and select **Give access to**. 4. Select **"Specific people…"**. 5. Select **Everyone** from the drop down. 6. Click **Add**. 7. Set the Permission Level for Everyone to **Read/Write**. 8. Click **Share**. 9. Record the Share Path. 10. Click **Done**.
Download Office Deployment Tool	11. Open Microsoft Edge and browse to the URL below. https://www.microsoft.com/en-us/download/details.aspx?id=49117 12. From the website, click **Download**.
Extract ODT	13. From the Downloads directory, double-click to start the extraction of the ODT and accept the UAC prompt if required. 14. Accept the License Terms and click **Continue**. 15. Navigate to **C:\Packages\MC** and click **OK**. 16. Click **OK** after successful Extraction.
Create Installation XML	17. The Sample Configurations for all Office Applications – Current Channel from the https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options can be referenced. 18. Browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 19. In the **Current Channel** Column, record the version number of the previous month. 20. Browse to the URL below. https://config.office.com/deploymentsettings 21. Under **Products and releases**, under **Architecture**, select **64-bit**. 22. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 23. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**.

	24. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 25. Under **Installation**, under **Installation options,** select **Local source** and specify the **Source path** as **\\CLIENT4\MC** and click **Next**. 26. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 27. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 28. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 29. Under **General**, click **Next**. 30. Under **Application preferences**, click **Finish**. 31. Click **Export** and select **Keep Current Settings** and then click **OK**. 32. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 33. Save the file to **C:\Packages\MC**. 34. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings
Download Microsoft 365 Apps	35. Type **CMD** in the "Type here to search". 36. Right-click **Command Prompt**. 37. Select **Run as administrator**. Accept the UAC prompt if required. 38. Change directory to **C:\Packages\MC**. 39. Type **setup.exe /download newconfiguration.xml**. 40. Press Enter. Office will begin the download.
Deploy Microsoft 365 Apps (Offline from a Local Share)	41. Back in CMD, type **setup.exe /configure newconfiguration.xml**. 42. Press Enter. 43. Office will begin the installation. Click **Close**.
Update Microsoft 365 Apps (Offline from a Local Share)	44. Open Microsoft Edge and browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 45. In the **Current Channel** Column, record the version number of the current month. **Note:** Unlike Cloud Managed, each month, the monthly build of Microsoft 365 Apps needs to be downloaded to the local file share. 46. Go back to the already opened https://config.office.com/deploymentsettings 47. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is for the current month. 48. Under **Update and upgrade**, under **Update and upgrade** options, select **Local source** and specify the **Source path** as **\\CLIENT4\MC**. 49. Click **Export** and select **Keep Current Settings** and then click **OK**.

	50. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **update.xml** and click **Export**. 51. Save the file to **C:\Packages\MC**. 52. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 53. Back in CMD, type **setup.exe /download update.xml**. 54. Press Enter. Office will begin the download. 55. Back in CMD, type **setup.exe /configure update.xml**. 56. Press Enter. 57. Office will begin the installation. Click **Close**. 58. Open Microsoft Edge and browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 59. In the **Current Channel** Column, record the version number of the current month. 60. In Word, **File | Account**, compare the **Office Updates Version and Build Number** to the version recorded of the current month. 61. Close Word.
Remove an Application from Microsoft 365 Apps	62. Go back to the already opened https://config.office.com/deploymentsettings 63. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 64. Click **Export** and select **Keep Current Settings** and then click **OK**. 65. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 66. Save the file to **C:\Packages\MC**. 67. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 68. Back in CMD, type **setup.exe /configure removeaccess.xml**. 69. Press Enter. 70. Office will begin the installation. 71. Click **Close**. **Note:** The Microsoft Access icon will not be displayed during the installation.
Add a Language to Microsoft 365 Apps (Offline from a Local Share)	72. Go back to the already opened https://config.office.com/deploymentsettings **Note:** If creating a Language, set the first language to the client's culture language. If the first language does not match the client's culture set, then the chosen language will be the Shell UI language. 73. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 74. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 75. Click **Export** and select **Keep Current Settings** and then click **OK**. 76. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 77. Save the file to **C:\Packages\MC**. 78. Back in CMD, type **setup.exe /download addspanish.xml**.

	79. Press Enter. Office will begin the download. 80. Back in CMD, type **setup.exe /configure addspanish.xml** and press Enter. 81. Office will begin the installation. 82. Click **Close**. 83. Type **Control Panel** in the "Type here to search" and press Enter. 84. Click on **Programs**. 85. Click on **Programs and Features**. 86. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed.

7.4 Enterprise Managed Deployment using Configuration Manager

In this activity, you will deploy Microsoft 365 Apps using Configuration Manager and configure updating for Microsoft 365 Apps.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Prerequisites	1. Verify that Error! Reference source not found. **Section** Error! Reference source not found. has been completed and that Microsoft 365 Apps/Office 2019/Office LTSC (under Office) is enabled.
Create a Share for Microsoft 365 Apps Package and Updates	2. Open Microsoft Edge and browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 3. In the **Current Channel** Column, record the version number of the current and previous month. 4. Logon to CM1 as (corp\labadmin). 5. On the taskbar, open File Explorer and browse to **C:\Packages** and create two folders named **OfficeConfigMan** and **OfficeConfigManUpdates**.
Enable Management of Microsoft 365 Apps Client Agent	6. In the Configuration Manager Console, browse to **Administration > Overview > Client Settings**. 7. Double-click on **Default Client Settings**. 8. Select **Software Updates**. 9. For **Enable management of the Office 365 Client Agent**, from the drop-down box select **Yes**. 10. Click **OK**.
Create a Folder and a Collection	11. Browse to **Assets and Compliance > Overview > Device Collections**. Right-click **Device Collections** and click **Folder > Create Folder**. 12. Enter a name **Microsoft 365 Apps** and click **OK**. 13. Expand **Device Collections**, right-click **Microsoft 365 Apps** folder and click **Create Device Collection**. 14. On the **General** step, for the **Name** enter **Microsoft 365 Apps MC**. For the **Limiting collection** field, click **Browse**.

15. Under **Device Collections**, select **Root**, select **All Systems** and click **OK**.
16. Back on the **General** step, click **Next**.
17. On the **Membership Rules** step, click **Next**. Click **OK** on the Configuration Manager prompt.
18. On the **Summary** step, click **Next**.
19. On the **Completion** step, click **Close**.
20. Browse to **Assets and Compliance > Overview > Devices**, right-click on the **CLIENT2** virtual machine, click **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**.
21. Under **Device Collections**, select the **Microsoft 365 Apps** folder, then select the **Microsoft 365 Apps MC** collection and click **OK**.
22. Under **Device Collections > Microsoft 365 Apps**, right-click on the **Microsoft 365 Apps MC** collection and click **Update Membership | Yes** and then refresh once to ensure that the **CLIENT2** virtual machine is a member of this collection.

Create and Deploy a Microsoft 365 Apps Package

23. Browse to **Software Library > Overview > Office 365 Client Management**.
24. Click **Office 365 Installer**.
25. Specify the following on the **Application Settings** step and click **Next**.

    Name: **Microsoft 365 Apps MC**

    Content Location: **\\CM1\Packages$\OfficeConfigMan**
26. On the **Office Settings** step, click **Go to the Office Customization Tool**.
27. On the **Deployment settings** step, enter the following and click **Next**:
    a) Under **Products and releases**, under **Architecture**, select **64-bit**.
    b) Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown.
    c) Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier for the previous month and click **Next**.
    d) Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**.
    e) Under **Installation**, click **Next**.
    f) Under **Update and upgrade**, ensure that **Uninstall any MSI versions of Office, including Visio and Project** is turned ON and then click **Next**.
    g) Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**.
    h) Under **General**, click **Next**.
    i) Under **Application preferences**, click **Finish**.
    j) Click **Review**, select **Keep Current Settings**, click **OK**, review the details and click **Submit**.
28. On the **Deployment** step, select **Yes** and click **Next**.
29. On the **General** step, click **Browse…** next to Collection.
30. Under **Device Collections > Microsoft 365 Apps**, select the **Microsoft 365 Apps MC** collection and click **OK**.

31. Select **Automatically distribute content for dependencies** and click **Next**.
32. On the **Content** step, click **Add > Distribution Point**.
33. Select **CM1.CORP.CONTOSO.COM** and click **OK**.
34. Click **Next**.
35. On the **Deployment Settings** step, specify the following and click **Next**.

    Action: **Install**

    Purpose: **Required**

    Other 4 Checkboxes: **Unchecked**
36. On the **Scheduling** step, select **As soon as possible after the available time** and click **Next**. No other checkboxes to be selected.
37. On the **User Experience** step, select **Display in Software Center and show all notifications**, check all the **4 checkboxes** below and click **Next**.
38. On the **Alerts** step, click **Next**. No checkboxes to be selected.
39. On the **Summary** step, click **Next**.
40. On the **Completion** step, click **Close**. This will download the content to the share specified, create the required Application, Deployment Type and Deployment as well as distribute the content to the Distribution Point.

Complete these steps on the CLIENT2 virtual machine.

Note: Uninstall any existing versions of Microsoft 365 Apps before performing this lab and reboot once.

User Experience with the Download and Installation of Microsoft 365 Apps Package on the Client Side

41. In the Configuration Manager Properties, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**.
42. Select **Application Deployment Evaluation Cycle** and click **Run Now**. Click **OK**.
43. After a few minutes, the package will start downloading and installing after a notification.
44. The installation of the package can be validated in the **Programs and Features** once installed.
45. In the Configuration Manager Properties, **Actions** tab, select **Hardware Inventory Cycle** and click **Run Now**. Click **OK**.

Complete these steps on the CM1 virtual machine.

Microsoft 365 Apps Readiness

You can use Configuration Manager to identify devices with high confidence that are ready to upgrade to Microsoft 365 Apps for enterprise. This integration provides insights into any potential compatibility issues with Office add-ins and macros used in your environment. Then you can use Configuration Manager to deploy Office to ready devices. The existing Microsoft 365 client management dashboard includes a tile called **Microsoft 365 Apps Upgrade Readiness**. There are few prerequisites that need to be in place.

46. Hardware inventory must be enabled in the client settings. To verify, in the Configuration Manager Console, browse to **Administration > Overview > Client Settings**. Double-click on **Default Client Settings** and click **Hardware Inventory**. Ensure that **Enable hardware inventory on clients** is set to **Yes**. Now click **Set Classes** next to **Hardware inventory classes** and ensure **Office 365 Configurations**, **Office add-ins**, **Office document metrics** and **Office VBA scan summary** are selected.
47. The device needs connectivity to the Office content delivery network (CDN) to download an add-in readiness file. If the device can't download this file, the add-ins state is *Needs review*.

For more information, refer to Integration for Microsoft 365 Apps readiness.

48. To access the **Microsoft 365 Apps Upgrade Readiness** tile, in the Configuration Manager Console, browse to **Software Library > Overview > Office 365 Client Management**.

Complete these steps on the CM1 virtual machine.

Create and Deploy a Microsoft 365 Apps Software Update

49. Once the sync is complete, browse to **Software Library > Overview > Office 365 Client Management > Office 365 Updates**. Search for **Current Month Version of Current Channel** with the **x64 architecture**, select and right-click the update and click **Create Software Update Group**.
50. Enter a name **Microsoft 365 Apps MC Updates** and click **Create**.
51. Browse to **Software Library > Overview > Software Updates > Software Update Groups**. Select **Microsoft 365 Apps MC Updates** and click **Deploy** from the ribbon bar.
52. On the **General** step, for the **Collection** field, click **Browse…**
53. Under the **Device Collections > Microsoft 365 Apps** folder, select the **Microsoft 365 Apps MC** collection and click **OK**.
54. Back on the **General** step, click **Next**.
55. On the **Deployment Settings** step, specify the following and click **Next**.

    Type of deployment: **Required**
    Detail level: **Only success and error messages**
    No other checkbox to be selected
56. On the **Scheduling** step, specify the following and click **Next**.

    Time based on: **Client local time**
    Software available time: **As soon as possible**
    Installation deadline: **As soon as possible**

No other checkbox to be selected

57. On the **User Experience** step, specify the following and click **Next**.

    User notifications: **Display in Software Center and show all notifications**

    Under **Deadline behavior**, check the box next to **Software updates installation**

    No other checkbox to be selected

58. On the **Alerts** step, click **Next**. No checkboxes to be selected.
59. On the **Deployment Package** step, select **Create a new deployment package** and specify the following and click **Next**.

    Name: **Microsoft 365 Apps MC Updates**

    Package source: **\\CM1\Packages$\OfficeConfigManUpdates**

60. On the **Distribution Points** step, click **Add > Distribution Point**.
61. Select **CM1.CORP.CONTOSO.COM** and click **OK**.
62. On the **Distribution Points** step, click **Next**.
63. On the **Download Location** step, select **Download software updates from the Internet** and click **Next**.
64. On the **Language Selection** step, select **English (United States)** for **Office 365 Client Update** and click **Next**.
65. On the **Download Settings** step, specify the following and click **Next**.

    Deployment options: **Download software updates from distribution point and install** as well as **Download and install software updates from the distribution points in site default boundary group**

66. On the **Summary** step, click **Next**.
67. On the **Completion** step, click **Close**. This will download the content to the share specified, create the required Deployment Package and Deployment as well as distribute the content to the Distribution Point.

Complete these steps on the CLIENT2 virtual machine.

User Experience with the Download and Installation of Microsoft 365 Apps Software Update on the Client Side

68. In the Configuration Manager Properties, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**.
69. Select **Software Updates Deployment Evaluation Cycle** and click **Run Now**. Click **OK**.
70. Select **Software Updates Scan Cycle** and click **Run Now**. Click **OK**.
71. The software update will start downloading and installing.

Note: It can take some time for the machine to be detected in Configuration Manager for the **"Required"** update. Run the **Software Updates Scan Cycle** on the clients to speed up the process.

72. The installation of the package can be validated in the **Programs and Features**.

7.5 Enterprise Managed Deployment using Microsoft Intune

In this activity, you will deploy Microsoft 365 Apps using Microsoft Intune.

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Add Microsoft 365 Apps	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://endpoint.microsoft.com and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 3. On the left navigation bar, click **Apps > All apps** and click **+ Add**. 4. In the **Select app type** pane, under **App type**, select **Windows 10 and later** under **Microsoft 365 Apps** and click **Select**.
Configure and Deploy Microsoft 365 Apps	5. Under the **App suite information** step, keep the default settings and click **Next**. 6. Under the **Configure app suite** step, enter/select the following and click **Next**: Leave the rest as default settings: a) **Select Office apps**: Only select **Excel, OneNote, Outlook, PowerPoint,** and **Word** b) **Update channel**: **Monthly Enterprise Channel** c) **Accept the Microsoft Software License Terms on behalf of users**: **Yes** d) **Languages**: **English** 7. Under the **Assignments** step, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 8. Under the **Review + create** step, review the page and click **Create**. **Note:** This group should have already been created as part of **Section** Error! Reference source not found..
Complete these steps on the CLIENT3 virtual machine.	
User Experience with the Download and Installation of Microsoft 365 Apps Package on the Client Side	**Note:** Ensure that the **CLIENT3** virtual machine is Azure AD Joined, enrolled into MDM, logged in as a cloud user, example TU1 and **Microsoft 365 Apps** is uninstalled if it is already installed. 9. Click **Start > Settings**. 10. Click **Accounts > Access work or school > Connected by TU1@<Azure Domain>.onmicrosoft.com/Connected to <Azure Domain> Azure AD > Info**. 11. Click **Sync**. 12. The Microsoft 365 Apps will download and install automatically in the background, which can be seen from the **Task Manager**, **Details** tab. 13. The installation of the package can be validated in the **Programs and Features**.

7.6 Servicing Microsoft 365 Apps for enterprise using Configuration Manager

In this section, you will go through how to configure Configuration Manager to support Office updates.

7.6.1 Enable Configuration Manager to receive Microsoft 365 Client Package Notifications

To start, you need to configure Configuration Manager to receive notifications when Microsoft 365 client update packages are available.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Prerequisites	1. Verify that Error! Reference source not found. **Section** Error! Reference source not found. has been completed and that Microsoft 365 Apps/Office 2019/Office LTSC (under Office) is enabled.
Sync Office Updates	2. In the Configuration Manager console under the **Software Library** node, open **Overview > Office 365 Client Management** and right-click **Office 365 Updates** and select **Synchronize Software Updates.** 3. On the **Configuration Manager** dialog box, click **Yes**. **Note:** The synchronization may take 30 minutes or more depending on the speed of the internet connection.

7.6.2 Enable Office COM Objects to Manage Microsoft 365 Client Updates

For Configuration Manager to be able to manage Microsoft 365 client updates, an Office COM object needs to be enabled on the computer where Office is installed. The Office COM object takes commands from Configuration Manager to download and install client updates.

You can enable the Office COM object by using either the Office Deployment Tool or Group Policy.

This lab guide will use Group Policy to enable Office COM Objects. This does the same thing as setting the OfficeMgmtCOM attribute to True in the configuration.xml file used by the Office Deployment Tool. But, with Group Policy, you can apply this setting to multiple computers, an organizational unit (OU), or a domain.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	

Download ADMX Files (If not downloaded before in the previous labs)	1. Download the Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise/Office LTSC 2021/Office 2019/Office 2016 https://www.microsoft.com/download/details.aspx?id=49030 **Note:** Download the appropriate version for the Office architecture you support. In this lab download the x64 version.
Install ADMX Files (If not installed before in the previous labs)	2. Install **admintemplates_x64_<VersionNumber>_en-us.exe** to temporary location. 3. **Copy** the contents of **admx** folder from the temporary location to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. **Note:** If PolicyDefinitions folder doesn't exist you will have to create it and also copy in the latest Windows 11 ADMX files. Download ADMX Templates for Windows 11 October 2021 Update [21H2] from Official Microsoft Download Center **Note:** Version number may change over time.
Enable Microsoft 365 Clients to receive Updates from ConfigMgr	4. Open the Group Policy Management Console. 5. Create a policy called "**Microsoft 365 Client Management**". 6. Edit the "**Policy**". 7. Enable the **Computer Configuration\Policies\Administrative Templates\Microsoft Office 2016 (Machine)\Updates\Management of Microsoft 365 Apps for enterprise** policy setting. 8. Link the GPO to the OU containing the clients. **Note:** Create a temporary OU called **Microsoft 365** and move **CLIENT1** or **CLIENT2** there. Run a **gpupdate /force** on the clients. Remember to move these clients back to the default **Computers** container after the lab is done.

7.6.3 Configure Office Updates

Note: Before deploying Microsoft 365 Updates to CLIENT1 or CLIENT2 VMs from Configuration Manager, ensure that the Configuration Manager Client is installed. For versions released as per channels, refer to https://docs.microsoft.com/en-us/officeupdates/update-history-office365-proplus-by-date

Task	Detailed Steps
Complete these steps on the CLIENT1 or CLIENT2 virtual machine.	
Download Office Deployment Tool	1. Logon as a corp\labadmin. 2. On the taskbar, open File Explorer and browse to **C:\** and create a folder named **ODT**. 3. Open Microsoft Edge and browse to the URL below. https://www.microsoft.com/en-us/download/details.aspx?id=49117

	4. From the website, click **Download**.
Extract ODT	5. From the **Downloads** directory, double-click to start the extraction of the ODT and accept the UAC prompt if required. 6. Accept the License Terms and click **Continue**. 7. Navigate to **C:\ODT** and click **OK**. 8. Click **OK** after successful Extraction.
Create Installation XML	9. The Sample Configurations for all Office Applications – Current Channel from the https://docs.microsoft.com/en-us/deployoffice/configuration-options-for-the-office-2016-deployment-tool can be referenced. 10. Browse to the URL below. https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date 11. In the **Current Channel** Column, record the version number of the previous month. 12. Browse to the URL below. https://config.office.com/deploymentsettings 13. Under **Products and releases**, under **Architecture**, select **64-bit**. 14. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 15. Under **Products and releases**, under **Update channel**, select **Current Channel** and select the **Version** that was recorded earlier and click **Next**. 16. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 17. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 18. Under **Update and upgrade**, under **Update and upgrade options**, select **Microsoft Endpoint Configuration Manager**. 19. Under **Update and upgrade**, under **Upgrade options**, ensure that the slider is turned ON for **Uninstall any MSI versions of Office, including Visio and Project**. Click **Next**. 20. Under **Licensing and activation**, turn ON the slider for **Automatically accept the EULA** and under **Product activation**, ensure that **User based** is selected and click **Next**. 21. Under **General**, click **Next**. 22. Under **Application preferences**, click **Finish**. 23. Click **Export** and select **Keep Current Settings** and then click **OK**. 24. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 25. Save the file to **C:\ODT**.
Deploy Microsoft 365 Apps	26. Type **CMD** in the "Type here to search". 27. Right-click **Command Prompt**. 28. Select **Run as administrator**. Accept the UAC prompt if required. 29. Change directory to **C:\ODT**.

30. Type **setup.exe /configure newconfiguration.xml**.
31. Press Enter.
32. Office will begin the installation.
33. Click **Close**.

Complete these steps on the CM1 virtual machine.

Validate that Microsoft 365 Apps Updates are Available

34. From the **Configuration Manager Console**, browse to **Software Library > Overview > Office 365 Client Management > Office 365 Updates**.
35. Search for the latest **Current Channel Version**. You should be able to see the latest **Current Channel Version** showing in a state of **"Required"** as per https://docs.microsoft.com/en-us/officeupdates/update-history-office365-proplus-by-date?redirectSourcePath=%252fen-us%252farticle%252fae942449-1fca-4484-898b-a933ea23def7

    Note: It can take some time for the **CLIENT1** or **CLIENT2** machines to be detected in Configuration Manager for the **"Required"** update. Run **Machine Policy Retrieval & Evaluation Cycle**, **Software Updates Deployment Evaluation Cycle** and **Software Updates Scan Cycle** on the machines to speed up the process.

Create Servicing Collections

36. From the **Configuration Manager Console**, browse to **Assets and Compliance**.
37. Right-click on **Overview > Device Collections** and select **Folder > Create Folder**.
38. On the **Configuration Manager** window, under **Folder name** enter **Microsoft 365 Apps Updates** then click **OK**.
39. Right-click on the **Microsoft 365 Apps Updates** folder and select **Create Device Collection**.
40. On the **General** step, enter the following then click **Next**.

    Name: **Microsoft 365 Apps Current Channel**

    Limiting Collection: **All Desktop and Server Clients**

41. On the **Membership Rules** step, click **Next**.
42. On the warning dialog box, click **OK**.
43. On the **Summary** step, click **Next**.
44. On the **Completion** step, click **Close**.

Add Devices to Collections

45. Right-click **Microsoft 365 Apps Current Channel** collection and click **Add Resources.**
46. In the **Add Resources to Collection** enter **CLIENT1** or **CLIENT2** in the **Name string contains** field then click **Search**.
47. In the **Search results** box, select **CLIENT1** or **CLIENT2** and click **Add** then **OK**.

48. Browse to **Software Library > Overview > Office 365 Client Management**.
49. Click **Create an ADR**.

Create ADR for Current Channel	General	50. Fill out as defined below and click **Next**: **Name:** Microsoft 365 Apps Updates – Current Channel **Template:** Office 365 Client Updates **Collection:** Microsoft 365 Apps Current Channel
	Deployment Settings	51. Keep defaults and click **Next**.
	Software Updates	52. Fill out as defined below and click **Next**: **Date Released of Revised:** Last 1 month **Product:** Microsoft 365 Apps/Office 2019/Office LTSC **Title:** "Office 365 Client Update...Microsoft 365 Apps Update – Current Channel Quality Update for x64"
	Evaluation Schedule	53. Fill out as defined below and click **Next**: **Run the rule on a schedule:** Selected **Schedule:** Occurs day 15 of every 1 month
	Deployment Schedule	54. Fill out as defined below and click **Next**: **Software available time:** As soon as possible **Installation deadline:** As soon as possible
	User Experience	55. Select **Display in Software Center and show all notifications** and click **Next**.
	Alerts	56. Keep defaults and click **Next**.
	Deployment Package	57. Fill out as defined below and click **Next**: **Create a new deployment package:** Selected **Name:** Microsoft 365 Apps Updates **Package Source:** \\CM1\Packages$\Microsoft365AppsUpdates **<u>Note:</u>** Create the folder beforehand.
	Distribution Point	58. Fill out as defined below and click **Next**: **Distribution Point Group:** Corp DPs
	Download Location	59. Keep defaults and click **Next**.

	Language Selection	60. Keep defaults and click **Next**.
	Download Settings	61. Keep defaults and click **Next**.
	Summary	62. Click **Next**.
	Completion	63. Click **Close**.
Run ADRs		64. Browse to **Software Library** > **Overview** > **Software Updates** > **Automatic Deployment Rules**. 65. Right-click **Microsoft 365 Apps Updates – Current Channel** and click **Run Now**. Click **OK**.
Complete these steps on the CLIENT1 or CLIENT2 virtual machine.		
Apply Updates		66. In the **Configuration Manager Properties**, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 67. Select **Software Updates Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 68. Select **Software Updates Scan Cycle** and click **Run Now**. Click **OK**. 69. The software update will start **Downloading** and **Installing**. The installation of the package can be validated in the **Programs and Features**.

7.6.4 Cloud-Based Policy Management Service for Microsoft 365 Apps for enterprise

The Office cloud policy service helps administrators manage policies for all Microsoft 365 Apps for enterprise users in their organization, from an easy-to-use, Internet-based portal focused on Microsoft 365 Apps management.

Microsoft 365 Apps allows users to access full Office experiences from multiple Windows devices. These may be managed or MDM-enrolled devices but are often also personally owned and unmanaged. Now with the Office cloud policy service, you can define and enforce Office policies without the infrastructure or MDM services traditionally required.

The office cloud policy services allows administrators to define policies for Microsoft 365 Apps and assign these policies to users via Azure Active Directory security groups. Once defined, these office policies are automatically enforced as users sign in and use Microsoft 365 Apps.

- **Build a policy configuration** that includes the policies you want to enforce, configured as needed for your organization's needs. The service is always up to date and includes the latest policies as they are released.

- **Target a group of users** by assigning a policy configuration to a specific AAD security group.
- **Policies automatically enforced** as users sign into Microsoft 365 Apps.

This service compliments Group Policy-based management as another option. Group Policy management enforces policies on Windows PCs joined to an Active Directory domain, while the Office cloud policy service only requires Azure Active Directory sign-in as part of Microsoft 365 Apps.

Office Cloud policy service manages user-based policies for Microsoft 365 Apps. Group Policy can manage both user-based and machine-based policies.

The settings configured as part of Office installation using the Office Customization Tool for Click-to-Run – as well as previous OCT versions – are based on 'preferences', meaning that a user can change them. Office cloud policy service settings are enforced, similar to Group Policy enforcement.

It is not required that the tenant have an Intune subscription. This is a feature of Microsoft 365 Apps and only requires that the tenant have a subscription that includes Microsoft 365 Apps.

This is a feature of Microsoft 365 Apps and only works with the Office apps that are deployed as a part of the Microsoft 365 Apps suite.

It is right now limited to a subset of the user based policies defined in the ADMX templates. All machine based policies are not included.

Only the Global Admin, Security Admin or Desktop Analytics Admin (private preview) roles are allowed access to create or view policy configurations.

For more information on Cloud-Based Policy Management Service for Microsoft 365 Apps, refer to https://techcommunity.microsoft.com/t5/Office-365-Blog/Announcing-the-new-cloud-based-policy-management-service-for/ba-p/310405 and https://docs.microsoft.com/en-us/DeployOffice/overview-office-cloud-policy-service

Prerequisites:

1. At least version 2004 or 2005 of Microsoft 365 Apps installed. In **CLIENT3** or **CLIENT4** ensure that the latest version of Microsoft 365 Apps is installed from https://portal.office.com and **CLIENT3** or **CLIENT4** are Azure Active Directory Joined and enrolled into Intune with the user (**TU1 or Test User1**).
2. User accounts created in or synchronized to Azure Active Directory (AAD). The user (**TU1 or Test User1**) must be signed into Microsoft 365 Apps with an AAD-based account, example: **TU1@<AzureDomainName>.onmicrosoft.com**
3. Security groups created in or synchronized to Azure Active Directory (AAD), with the appropriate users added to those groups. Created as part of this lab.
4. To create a policy configuration, you must be assigned one of the following roles in Azure Active Directory (AAD): Global Administrator, Security Administrator, or Desktop Analytics Administrator. We will be using **LabAdmin@<AzureDomainName>.onmicrosoft.com**, which is a Global Administrator.

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Create a Security Group	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 4. Click **+ New group**. 5. In the Group pane fill in the following values and click **Select**: i. GROUP TYPE: **Security** ii. GROUP NAME: **OCPSDemo** iii. MEMBERSHIP TYPE: **Assigned** **iv.** MEMBERS: **TU1,TU2** 6. Click **Create**.
Create a Policy Configuration	7. Navigate to https://config.office.com/ and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 8. Now under **Customization**, go to **Policy management** and click **Create**. 9. Provide a **Name** - **OCPSDemo** an optional **Description**. 10. Click **Select type** and select **This policy configuration applies to users**. 11. Click **Select group** and search for and select **OCPSDemo**. 12. Click **Configure policies** and search for **Block macros**. 13. Click **Block macros from running in Office files from the Internet** for the **Word** application. 14. Under **Policy type**, select **Microsoft recommended security baseline**. 15. Ensure that under **Configured**, Enabled is the option **selected**. Click **Apply**. 16. Once done, click **Create**.
Complete these steps on the CLIENT3 or CLIENT4 virtual machine.	
User Policy on the Client	17. When a user signs into Office on a device for the first time, a check is immediately made to see if there is a policy configuration that pertains to the user. If the user is a member of an AAD group that is assigned a policy configuration, then the appropriate policy settings are applied.

7.7 Servicing Microsoft 365 Apps for enterprise using Intune

In Intune, you can use Windows 10/11 templates to configure group policy settings. This section shows you how to update Microsoft 365 Apps using an administrative template in Intune.

In this scenario, you create an administrative template in Intune that updates Microsoft 365 Apps on your devices.

For more information on administrative templates, see Windows 10/11 templates to configure group policy settings.

For more information on how to Use Update Channel and Target Version settings to update Microsoft 365 Aps with Microsoft Intune Administrative Templates, refer to - https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-update-office

Note: In order to test Microsoft 365 Apps Updates with Intune, on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Profiles/Policies from the previous labs. Also, install an earlier version of Microsoft 365 Apps.

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Prerequisites	1. Be sure to enable Microsoft 365 Apps Automatic Updates for your Office apps. You can do this using group policy, or the Intune Office 2016 ADMX template.
Set the Update Channel in the Intune Administrative Template	2. In your Intune administrative template, go to the **Update Channel** setting, and enter the channel you want. For example, choose **Current Channel**. 3. Be sure to assign the policy to your Windows 10 devices. To test your policy sooner, you can also sync the policy: • Sync the policy in Intune • Manually sync the policy on the device

7.8 LOB Deployment and Management with Microsoft Intune

7.8.1 Add Windows line-of-business (LOB) apps to Microsoft Intune

Intune supports Windows line-of-business apps (.msi files only).

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Add Line-of-Business App	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Apps > All apps** and click **+ Add**. 4. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 5. In the **Select app type** pane, under **App type**, select **Line-of-business app** under **Other** and click **Select**.

Configure Line-of-Business App	6. On the **App information** step, click **Select app package file**. 7. On the **App package file** pane, choose the browse button, and select a Windows installation file with the extension **.msi, .appx, or .appxbundle**. A sample msi file can be downloaded from: [Download official VLC media player for Windows - VideoLAN]() 8. Click **OK.** 9. Under **App information**, enter the following information and click **Next**: a. **Name** - Enter the name of the app as it is displayed in the company portal. Make sure all app names that you use are unique. If the same app name exists twice, only one of the apps is displayed to users in the company portal. b. **Description** - Enter a description for the app. The description is displayed to users in the company portal. c. **Publisher** - Enter the name of the publisher of the app. d. **App install context** – This specifies the install context to be associated with this app. For dual mode apps, select the desired context for this app. For all other apps, this is pre-selected based on the package and cannot be modified. e. **Ignore app version** – Set this to "Yes" only for apps that are automatically updated by the app developer (such as Google Chrome). f. **Command-line arguments** - Optionally, enter any command-line arguments that you want to apply to the .msi file when it runs, like /q. g. **Category** - Select one or more of the built-in app categories, or a category you created. Categorizing apps makes it easier for users to find the app when they browse the company portal. h. **Show this as a featured app in the Company Portal** - Display the app prominently on the main page of the company portal when users browse for apps. i. **Information URL** - Optionally, enter the URL of a website that contains information about the app. The URL is displayed to users in the company portal. j. **Privacy URL** - Optionally, enter the URL of a website that contains privacy information for the app. The URL is displayed to users in the company portal. k. **Developer** - Optionally, enter the name of the app developer. l. **Owner** - Optionally, enter a name for the owner of this app, for example, HR department. m. **Notes** - Enter any notes you would like to associate with this app. n. **Logo** - Upload an icon that is associated with the app. The icon is displayed with the app when users browse the company portal.

7.8.2 Assign Apps to Groups and Deploy with Microsoft Intune

In the following section, you will assign the Line-of-business app to users and devices.

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Assign and Configure App Assignment	1. Under the **Assignments** step, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 2. Under the **Review + create** step, review the page and click **Create**. **Note:** This group should have already been created as part of **Section** Error! Reference source not found..
Complete these steps on the CLIENT3 virtual machine.	
User Experience with the Download and Installation of the App on the Client Side	3. Click **Start > Settings**. 4. Click **Accounts > Access work or school > Connected by TU1@<Azure Domain>.onmicrosoft.com/Connected to <Azure Domain> Azure AD | Info**. 5. Click **Sync**. 6. The app will download and install automatically in the background. 7. The installation of the app can be validated in the **Programs and Features**.

7.9 Deploy Microsoft Teams

Now Microsoft Teams can be deployed using Configuration Manager as well as Intune using the MSI Installer.

For more information, refer to - https://docs.microsoft.com/en-us/microsoftteams/msi-deployment

7.9.1 Install Microsoft Teams using Configuration Manager

Task	Detailed Steps
Complete these steps on the CLIENT2 virtual machine.	
Uninstall Microsoft 365 Apps from the Previous Labs	1. **Uninstall** any existing versions of **Microsoft 365 Apps** from **Programs and Features**. 2. For **Microsoft Teams** specifically (if exists): • Delete the directory recursively under **%localappdata%\Microsoft\Teams***. • Delete the **HKEY_CURRENT_USER\Software\Microsoft\Office\Teams\PreventInstallationFromMsi** registry value.

Complete these steps on the CM1 virtual machine.	
Create a Folder and Download the Microsoft Teams MSI	3. Browse to **C:\Packages**. 4. Create a **Folder** by the name **MSTeamsMSI**. 5. In the **MSTeamsMSI** Folder, **download** the **Microsoft Teams MSI** from https://teams.microsoft.com/downloads/desktopurl?env=production&plat=windows&arch=x64&managedInstaller=true&download=true
Create a Device Collection and Add the Machine to that Collection	6. In the Configuration Manager Console, browse to **Assets and Compliance > Overview > Device Collections**. 7. Right-click **Device Collections** and click **Create Device Collection**. 8. In the **General** step, enter the following and click **Next**: Name: **Microsoft Teams MSI** Click **Browse…**Select **All Systems**. Click **OK** 9. In the **Membership** Rules page, enter the following and click **Next**: Click **Add Rule > Direct Rule** On the **Welcome** step, Click **Next** On the **Search for Resources** step, for the **Value** field, enter **CLIENT2** and click **Next** On the **Select Resources** step, select **CLIENT2** and click **Next** On the **Summary** step, click **Next** and then click **Close** 10. Back on the **Membership Rules** step, click **Next**. 11. In the **Summary** step, click **Next**. 12. In the **Completion** step, click **Close**. 13. Ensure that **CLIENT2** is in the **Microsoft Teams MSI** collection.

Create and Deploy the Microsoft Teams MSI Application	14. Navigate to **Software Library > Overview > Application Management > Applications**. 15. Right-click **Applications** and click **Create Application**. 16. In the **General** step, enter the following and click **Next**: Location: **\\CM1\Packages$\MSTeamsMSI\Teams_windows_x64.msi** 17. In the **Import Information** step, click **Next**. 18. In the **General Information** step, enter the following and click **Next**: Installation program: **msiexec /i Teams_windows_x64.msi OPTIONS="noAutoStart=true" ALLUSERS=1** Install behavior: **Install for system** 19. In the **Summary** step, click **Next**. 20. In the **Completion** step, click **Close**. 21. Now, right-click **Teams Machine-Wide Installer** and click **Deploy**. 22. In the **General** step, click **Browse…**under **Device Collections**, select **Microsoft Teams MSI** and click **OK** and then click **Next**. 23. In the **Content** step, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 24. In the **Deployment Settings** step, select the **Purpose** as **Required** and click **Next**. 25. In the **Scheduling** step, click **Next**. 26. In the **User Experience** step, click **Next**. 27. In the **Alerts** step, click **Next**. 28. In the **Summary** step, click **Next**. 29. In the **Completion** step, click **Close**.
Complete these steps on the CLIENT2 virtual machine.	
Retrieve Policies and Install Teams	30. Launch the **Configuration Manager Client** applet from **Control Panel > System and Security**. 31. Go to the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 32. As soon as the notification appears click it to launch the **Software Center**. Observe the download and installation. 33. In a few moments, observe the **Teams Machine-Wide Installer** will appear in the **Programs and Features**.

7.9.2 Install Microsoft Teams using Intune

Task	Detailed Steps
Complete these steps on the CLIENT3 virtual machine.	

Uninstall Microsoft 365 Apps from the Previous Labs

1. **Uninstall** any existing versions of **Microsoft 365 Apps** from **Programs and Features**.
2. For **Microsoft Teams** specifically (if exists):
   - Delete the directory recursively under **%localappdata%\Microsoft\Teams***.
   - Delete the **HKEY_CURRENT_USER\Software\Microsoft\Office\Teams\PreventInstallationFromMsi** registry value.

Complete these steps from an Internet-Connected Windows computer.

Create a Folder and Download the Microsoft Teams MSI

3. In the **C:\** drive, create a **Folder** by the name **MSTeamsMSI**.
4. In the **MSTeamsMSI** Folder, **download** the **Microsoft Teams MSI** from https://teams.microsoft.com/downloads/desktopurl?env=production&plat=windows&arch=x64&managedInstaller=true&download=true

Add, Configure and Assign the Microsoft Teams MSI Application

5. Start Microsoft Edge InPrivate mode.
6. Navigate to https://portal.azure.com and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**
7. In the navigation pane click **Apps > All apps** and click **+ Add**.
8. In the **Select app type** pane, under **App type**, select **Other | Line-of-business app** and click **Select**.
9. Under the **App information** step, click **Select app package file**, browse to **C:\MSTeamsMSI\Teams_windows_x64.msi**, click **Open**, click **OK**.
10. Under the **App information** step, enter the following details and click **Next**:
    - Publisher: **Microsoft**
11. Under the **Assignments** step, enter the following details and click **Next**:
    - Under **Required**, click **+ Add group**
    - Type **Sales**, select it and click **Select**
12. Under the **Review + create** step, click **Create**.

Note: Wait for the Teams Machine-Wide Installer to upload.

Complete these steps on the CLIENT3 virtual machine.

User Experience with the Download and Installation of Microsoft Teams on the Client Side	**Note:** Ensure that the **CLIENT3** virtual machine is Azure AD Joined, enrolled into MDM, logged in as a cloud user, example TU1 and **Microsoft 365 Apps** is uninstalled if it is already installed. 13. Click **Start > Settings**. 14. Click **Accounts > Access work or school > Connected by TU2@<Azure Domain>.onmicrosoft.com/Connected to <Azure Domain> Azure AD > Info**. 15. Click **Sync**. 16. After a moment, a **Teams Installer** folder will be created in **C:\Program Files (x86)**. 17. **IMPORTANT: Restart CLIENT3 once and re-login with TU1 credentials.** 18. In a few moments, observe the **Microsoft Teams** icon on the desktop and the same will appear in the **Programs and Features**. Also, notice Microsoft Teams is installed in the user profile in **%localappdata%\Microsoft\Teams***. Microsoft Teams will auto-launch and automatically login as **TU1**.

7.10 Assignment Filters

After you've added an app to Microsoft Intune, you can assign the app to users and devices. You can also create filters to narrow the assignment scope of a policy. For example, use filters to target devices with a specific OS version or a specific manufacturer, or target only personal devices or only organization-owned devices. For more details on using filters when assigning apps in Endpoint Manager, see: Create filters in Microsoft Intune - Azure | Microsoft Docs.

Task	Detailed Steps
Complete these steps on a browser	

Task	Detailed Steps
Create device filters	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://portal.azure.com and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 3. Select **Tenant administration** > **Filters (preview)** > **Try out the filters (preview) feature**. 4. Set **Filters (preview)** to **On**. 5. Select **Tenant administration** > **Filters (preview)** > + **Create**. 6. In **Basics** step, enter the following properties and then click **Next**: ▪ **Filter name**: Enter a descriptive name for the filter. Name your filters so you can easily identify them later. For example, a good filter name is **Windows OS version filter**. ▪ **Description**: Enter a description for the filter. This setting is optional but recommended. ▪ **Platform**: Select your platform. 7. In **Rules** step, create a rule using the **rule builder.** (You can also use the rule syntax.) **Rule builder**: ○ **And/Or**: After you add an expression, you can add to the expression using the and/or options. ○ **Property**: Select a property for your rule, such as device or operating system SKU. ○ **Operator**: Select the operator from the list, such as equals or contains. ○ **Value**: Enter the value in your expression. For example, enter 10.0.22000 for the OS version, or Microsoft for the manufacturer. 8. **Add expression**: After you add the property, operator, and value, select **Add expression.** The expression you created is automatically added to the rule syntax editor. Select **Next**. 9. In **Review + create**, review your settings. When you select **Create**, your changes are saved. The filter is created, and ready to be used. The filter is also shown in the filters list.

Task	Detailed Steps
Assign apps to groups and apply filters.	10. In the navigation bar, select **Apps** > **All apps**. 11. In the **Apps** pane, select the app you want to assign. (e.g. XML Notepad). Select **Properties.** 12. Click **edit** next to **Assignments**. 13. Select **Add group** to add a group of users that you want assigned to the app. Click **Select**. 14. Under **Required**, under the Filter column, click **none**. 15. Under Filters, select the **Exclude filtered devices in assignment**. Select the devices in the group that you want excluded from the app. Click **Select**. 16. To save your changes, select **Review + save** > **Save**. When the device checks in with the Intune service, the properties defined in the filter are evaluated, and determine if the app or policy should be applied.

8 Managing Microsoft Edge

The new, Chromium-based version of Microsoft Edge provides best in class compatibility with extensions and websites. Additionally, this new version provides great support for the latest rendering capabilities, modern web applications, and powerful developer tools across all supported OS platform

In this section, we will perform the following core scenarios:

- Deploy and Update Microsoft Edge
  - ➢ Deploy Microsoft Edge using Configuration Manager
  - ➢ Deploy Microsoft Edge Updates using Configuration Manager
  - ➢ Configure and Deploy Edge Policies using On-Premises Method
  - ➢ Deploy Microsoft Edge using Intune
  - ➢ Configure and Deploy Microsoft Edge Policies using Intune
- IE Mode
  - ➢ Configure and Deploy IE Mode using On-Premises Method
  - ➢ Configure and Deploy IE Mode using Intune
- Setup Enterprise New Tab Page
  - ➢ Configure and Deploy Enterprise New Tab using On-Premises Method
  - ➢ Configure and Deploy Enterprise New Tab using Intune

8.1 Deploy and Update Microsoft Edge

In this section, we will perform the following scenarios:

- Deploy Microsoft Edge using Configuration Manager
- Deploy Microsoft Edge Updates using Configuration Manager
- Configure and Deploy Microsoft Edge Policies using On-Premises Method
- Deploy Edge using Intune or Microsoft Endpoint Manager (MEM)
- Configure and Deploy Edge Policies using Intune

8.1.1 Deploy Edge using Configuration Manager

Note: The new Microsoft Edge is included by default starting with Windows 10 20H2 and later.

In this section, we will deploy Microsoft Edge using Configuration Manager, which is the on-premises Method.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Create a Folder	1. Open **File Explorer** and navigate to **C:\Packages** and create a folder called **Edge**.

Create a Device Collection

2. Launch the Configuration Manager console and navigate to **Assets and Compliance > Overview > Device Collections**.
3. Right-click **Device Collections** and select **Create Device Collection**.
4. On the **General** step, specify the following and click **Next**:
   Name: **Edge Clients**
   Limiting collection: **All Systems**
5. On the Membership Rules page, click **Add Rule > Direct Rule**. On the **Welcome** step click **Next**. On the **Search for Resources** step, enter **%CLIENT1%** next to **Value** and click **Next**. On the **Select Resources** step, select **CLIENT1** and click **Next**. On the **Summary** step, click **Next**. On the **Completion** step, click **Close**.
6. Back on the **Membership Rules** step, click **Next**.
7. On the **Summary** step, click **Next**.
8. On the **Completion** step, click **Close**.
9. Ensure that the **Edge Clients** collection has **CLIENT1** in it.

Create the Microsoft Edge Application and Deployment

10. Navigate to **Software Library > Overview > Microsoft Edge Management**.
11. Right-click **Microsoft Edge Management** and select **Create Microsoft Edge Application**.
12. In the **Application Settings** step, specify a Name - **Edge App** and Content Location - **\\CM1\Packages$\Edge** and then click **Next**.
13. In the **Microsoft Edge Settings** step, for **Channel** select **Stable** and select **Specific Version**. In the **Specific Version** field, select the **lowest possible version as we will be updating it later**. Check **Bypass any machine policies which restrict the execution of PowerShell scripts on the user's device**. Click **Next**.

Note: Make a note of the lowest and latest possible versions from the drop-down list.

14. On the **Deployment** step, select **Yes** and click **Next**.
15. On the **General** step, select **Edge Clients** next to Collection which comes under the category of **Device Collections** and click **Next**.
16. On the **Content** step, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**.
17. On the **Deployment Settings** step, ensure **Install** is selected next to **Action** and select **Available** next to **Purpose**. Click **Next**.
18. On the **Scheduling** step, click **Next**.
19. On the **User Experience** step, select **Display in Software Center and show all notifications** next to **User notifications** and click **Next**.
20. On the **Alerts** step, click **Next**.
21. On the **Summary** step, click **Next**.
22. On the **Completion** step, click **Close**.

Complete these steps on the CLIENT1 virtual machine.

Retrieve Policies and Install Microsoft Edge	23. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 24. Click the **Actions** tab and select **Machine Policy Retrieval & Evaluation Cycle** and **Application Deployment Evaluation Cycle** and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process. 25. As soon as the notification appears, click on the **notification or launch Software Center**. 26. Select **Edge App** under Applications and click **Install**. 27. Once the installation is completed, notice the **new Microsoft Edge icon on the desktop**.

8.1.2 Deploy Microsoft Edge Updates using Configuration Manager

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Prerequisites	1. Verify that **Configure Software Update Point Section** Error! Reference source not found. has been completed and that **Microsoft Edge** (under Windows) is enabled.
Create a Folder	2. Open **File Explorer** and navigate to **C:\Packages** and create a folder called **EdgeUpdates**.
Complete these steps on the CLIENT1 virtual machine.	
Refresh Policies	3. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 4. Click the **Actions** tab and run **Machine Policy Retrieval & Evaluation Cycle** followed by **Software Update Scan Cycle**. This is only required to trigger the process so that update shows in **Required** state.
Complete these steps on the CM1 virtual machine.	
Configure and Deploy Microsoft Edge Updates	5. In the console, navigate to **Software Library > Overview > Microsoft Edge Management > All Microsoft Edge Updates**. 6. Sort the updates based on **Stable**, **Dev** and **Beta** by clicking on the **Title header**. 7. Look for the **latest Stable version** in the list and select the version that shows as Required. 8. From the ribbon bar, click **Deploy**. 9. On the **General** step, for the **Deployment Name**, enter **Edge Stable Updates**, for the **Collection**, select **Edge Clients** and then click **Next**. 10. On the **Deployment Settings** step, keep the defaults and click **Next**.

11. On the **Scheduling** step, select **As soon as possible** under **Installation deadline** and click **Next**.
12. On the **User Experience** step, keep the defaults and click **Next**.
13. On the **Alerts** step, keep the defaults and click **Next**.
14. On the **Deployment Package** step, select **Create a new deployment package**, enter the Name - **Edge Stable Updates**, enter the Package source - **\\CM1\Packages$\EdgeUpdates** and then click **Next**.
15. On the **Distribution Points** step, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**.
16. On the **Download Location** step, keep the defaults and click **Next**.
17. On the **Language Selection** step, select **Windows Update** and click **Next**.
18. On the **Download Settings** step, select **Download software updates from distribution point and install** under **Deployment options** and then click **Next**.
19. On the **Summary** step, review and click **Next**.
20. On the **Completion** step, click **Close**.
21. Navigate to **Software Library > Overview > Software Updates > Software Update Groups**, select the **software update group** and click **Run Summarization** few times and click **Refresh** few times from the ribbon bar to ensure that the client machine shows into **non-compliance**, which means that the machine needs one of the updates in the software update group.
    Note: If only one Microsoft Edge Update was selected above, then no Software Update Group will be created. Compliance can be viewed at the Edge Update level.

Complete these steps on the CLIENT1 virtual machine.

Retrieve Policies and Install Microsoft Edge Updates

22. Launch the **Configuration Manager applet** from **Control Panel > System and Security**.
23. Click the **Actions** tab and run **Machine Policy Retrieval & Evaluation Cycle,** followed by **Software Update Scan Cycle,** followed by **Software Updates Deployment Evaluation Cycle**. Click **OK** on each prompt. This is only required to speed up the process.
24. As soon as the notification appears, click on the notification or launch **Software Center**.
25. Notice that the update gets downloaded and installed.
26. Once the installation is completed, launch **Control Panel > Programs > Programs and Features** and notice that the **Microsoft Edge version** has been updated.

8.1.3 Configure and Deploy Microsoft Edge Policies using On-Premises Method

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Download and Install Administrative Templates for Microsoft Edge	1. Open Microsoft Edge and browse to https://aka.ms/EdgeEnterprise to download the administrative templates for Microsoft Edge. Select the **latest Channel/Version and Build**, select the **Platform Windows 64-bit** and then click **GET POLICY FILES**. 2. Click **Accept and download**. Save the **MicrosoftEdgePolicyTemplates.cab** file to the **Downloads** and click **Close**. 3. Open **MicrosoftEdgePolicyTemplates.cab** file and then right-click on **MicrosoftEdgePolicyTemplates.zip** and click **Extract…** and then select a location 4. On the opened folder where the zip file has been extracted to and unzip it, then navigate to **windows > admx**. 5. Scroll down and copy the **msedge.admx** and **msedgeupdate.admx** files to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. Click **Continue** on the prompt. 6. Now, navigate to **windows > admx > en-US** and copy the **msedge.adml** and **msedgeupdate.adml** files to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions\en-US**. Click **Continue** on the prompt.
Configure and Deploy Microsoft Edge Policies	7. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 8. Right-click **corp.contoso.com** and click **Create a GPO in this domain, and Link it here…** 9. Specify the Name - **Microsoft Edge Policies** and click **OK**. 10. Right-click **Microsoft Edge Policies** and click **Edit…** 11. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Default search provider**. 12. Double-click **Enable the default search provider**, select **Enabled**, click **Apply** and **OK**. 13. Double-click **Default search provider name**, select **Enabled**, under Default search provider name, enter **Google** and then click **Apply** and **OK**. 14. Close all the windows.
Complete these steps on the CLIENT1 virtual machine.	
Verify Microsoft Edge Policies	15. Launch an administrative command prompt window. 16. Run the command **gpupdate /force**.

	17. Launch the new Microsoft Edge and in the address bar type **edge://policy** and press enter. 18. Notice the **2 policies** that have been enabled and configured. The same can be noticed in **HKLM\SOFTWARE\Policies\Microsoft\Edge**.

8.1.4 Deploy Microsoft Edge using Intune

Note: The Chromium-based version of Microsoft Edge is included by default starting with Windows 10 20H2 and later.

Task	Detailed Steps
Complete these steps on the CLIENT3 virtual machine.	
Configure Execution Policy	1. Launch an elevated PowerShell window. 2. Run the command **Get-ExecutionPolicy**. If the result is **Restricted**, then run the command **Set-ExecutionPolicy Unrestricted** and accept all the prompts.
Complete these steps from an Internet-Connected Windows computer.	
Create a Security Group	3. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. From the left navigation bar, click **Azure Active Directory** and then click **Groups**. 5. Under All groups, click **+ New group**. 6. Enter the following and then click **Create**: Group type: **Security** Group name: **EdgePoC** Membership type: **Assigned** Members: **CLIENT3**
Create the Microsoft Edge App and Assignment	7. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 8. Select **Apps > All apps > + Add**. 9. Under **Microsoft Edge, version 77 and later**, select **Windows 10 and later** and then click **Select**. 10. On the **App information** step, keep all defaults and click **Next**. 11. On the **App settings** step, select **Stable** next to **Channel**. Note the new Logo. Click **Next**. 12. On the **Assignments** step, under **Required**, click **+ Add group**. Select **EdgePoC** and then click **Select**. Click **Next**. 13. On the **Review + create** step, click **Create**.
Complete these steps on the CLIENT3 virtual machine.	

Retrieve Policies and Install Microsoft Edge	14. Click **Start > Settings > Accounts > Access work or school**. 15. Select **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <AzureDomain>'s Azure AD** and click **Info**. 16. Click **Sync**. 17. In few minutes, notice a **notification** from Intune stating that **Microsoft Edge is being downloaded and installed** and also notice the **new Microsoft Edge icon on the desktop**. **The latest version of Microsoft Edge will be installed from the Stable channel by default.**

8.1.5 Configure and Deploy Microsoft Edge Policies using Intune

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Configure and Deploy Microsoft Edge Policies	1. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **Devices > Configuration profiles**. 3. Click **+ Create profile**. 4. Select the following and click **Create**: Platform: **Windows 10 and later** Profile type: **Templates** Profile: **Administrative Templates** 5. On the **Basics** step, for the **Name** enter **Microsoft Edge Policies** and click **Next**. 6. On the **Configuration settings** step, under **Computer Configuration > Microsoft Edge > Default search provider** click the policy **Enable the default search provider**. Select **Enabled** and click **OK**. 7. Now click the policy - **Default search provider name**. Select **Enabled** and under Default search provider name, enter **Google**. Click **OK**. 8. Back on the **Configuration settings** step. Click **Next**. 9. On the **Scopes tags** step, click **Next**. 10. On the **Assignments** step, under **Included groups**, click **Add groups**, select **EdgePoC** and click **Select**. Click **Next**. 11. On the **Review + create** step, review the settings and click **Create**.
Complete these steps on the CLIENT3 virtual machine.	
Verify Microsoft Edge Policies	12. Click **Start > Settings > Accounts > Access work or school**. 13. Select **Connected by TU1@<AzureDomainName>.onmicrosoft.com / Connected to <AzureDomain>'s Azure AD** and click **Info**. 14. Click **Sync**. 15. Once the sync has completed, after a few minutes, launch the new Microsoft Edge and in the address bar type **edge://policy** and press enter.

	16. Notice the **2 policies** that have been enabled and configured. The same can be noticed in **HKLM\SOFTWARE\Policies\Microsoft\Edge**.

8.2 IE Mode

In this section, we will perform the following scenarios:

- Configure and Deploy IE Mode using On-Premises Method
- Configure and Deploy IE Mode using Intune

8.2.1 Configure and Deploy IE Mode using On-Premises Method

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Create a Shared Folder (EMEI) with Full Permissions	1. Open File Explorer and browse to **C:\**. 2. Create a new folder named **EMEI**. 3. Right-click on **EMEI** and select **Properties**. 4. In the EMEI Properties window, go to the **Sharing** tab. 5. On the Sharing tab, click **Advanced Sharing**. 6. On the Advanced Sharing window, select **Share this folder** then click on **Permissions**. 7. On the Permissions for EMEI window, under **Allow** select **Full Control** then click **Apply** and **OK**. 8. On the Advanced Sharing window, click **Apply** and **OK**. 9. On the EMEI Properties window, click **Close**.
Configure Test Website	10. On the taskbar, open **File Explorer** and browse to **C:\Packages\Sources**. 11. Copy the **ContosoLearning** folder to **C:\inetpub\wwwroot**. Accept the prompt. 12. On the Start menu, open **Internet Information Services (IIS) Manager**. 13. Under the **Connections** pane, browse to **APP1 (Corp\LabAdmin) > Sites > Default Web Site > ContosoLearning**. 14. Right-click on **ContosoLearning** and select **Convert to Application**. 15. On the Add Application window, click **OK**. 16. On **ContosoLearning**, under the **Actions** pane select **Advanced Settings.** 17. On the Advanced Settings window, select **Application Pool** and click on the **ellipses (...)**. 18. On the Select Application Pool window, set the **Application pool** to **.NET v2.0** then click **OK**. 19. On the Advanced Settings window, click **OK**.

Complete these steps on the CLIENT1 virtual machine.

Download Enterprise Mode Site List Manager	20. Open Edge and browse to the URL below. https://www.microsoft.com/en-us/download/details.aspx?id=49974 21. From the website, click **Download**. 22. Save **EMIESiteListManager.msi** to **C:\Packages** after creating a folder called **Packages** in **C:\**.
Install Enterprise Mode Site List Manager	23. On the taskbar, open **File Explorer** and browse to **C:\Packages**. 24. Double-click on **EMIESiteListManager.msi**. 25. On the Welcome page, click **Next**. 26. On the End-User License Agreement page, select **I accept the terms in the License Agreement** and then click **Next**. 27. On the Destination Folder page, click **Next**. 28. On the Ready to Install page, click **Install**. Accept the UAC prompt if required. 29. Once complete, click **Finish**.
Create a Site List	30. From the desktop icon, open the **Enterprise Mode Site List Manager**. 31. On the Enterprise Mode Site List Manager for v.2 schema window, click **Add**. 32. On the Add new website window, under **URL** enter **app1/ContosoLearning** and select **IE8 Document Mode** next to **Compat Mode** and then click **Save**. 33. Click on **File > Save to XML**. 34. **Save** the file to **\\CM1\EMEI** as **EMEISiteList.xml**.

Complete these steps on the DC1 virtual machine.

Configure and Deploy IE Mode Policies	35. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 36. Right-click **Microsoft Edge Policies** and click **Edit…** 37. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge**. 38. Look for the policy - **Configure Internet Explorer integration** and double-click it. 39. Select **Enabled** and under Options, select **Internet Explorer mode**. Click **Apply** and **OK**. 40. Now look for the policy - **Configure the Enterprise Mode Site List** and double-click it. 41. Select **Enabled** and under Options, enter **\\CM1\EMEI\EMEISiteList.xml**. Click **Apply** and **OK**. 42. Close all the windows.

Complete these steps on the CLIENT1 virtual machine.

Verify IE Mode Policies	1. First launch the new **Microsoft Edge** and in the address bar type **http://CM1/ContosoLearning** and press enter.

	2. Note the warning "**Your browser is not supported by ContosoLearning. Only Internet Explorer is Supported**". 3. Close **Microsoft Edge**. 4. Launch an administrative command prompt window. 5. Run the command **gpupdate /force**. 6. Now launch the new **Microsoft Edge** and in the address bar type **http://CM1/ContosoLearning** and press enter. 7. Notice that the new **Microsoft Edge opens the website in Internet Explorer mode**. You can notice an **icon of Internet Explorer in the address bar** on which when you hover you mouse, it displays **Internet Explorer mode**. Also notice that you will **not see the warning**.

8.2.2 Configure and Deploy IE Mode using Intune

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Host the EMEISiteList.xml in Contoso Learning	1. Navigate to **C:\EMEI** and copy the **EMEISiteList.xml** file. 2. Right-click **Start > Run, type inetmgr** and press enter. 3. Navigate to **CM1 (CORP\LabAdmin) > Sites > Default Web Site > Contoso Learning**. 4. Right-click **Contoso Learning** and click **Explore**. 5. Paste the **EMEISiteList.xml** in this location along with the rest of the files. 6. Open **Internet Explorer** and ensure that you are able to access **http://CM1/ContosoLearning/EMEISiteList.xml**.
Complete these steps from an Internet-Connected Windows computer.	
Configure and Deploy IE Mode Policies	7. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 8. From the left navigation bar, click **Devices > Configuration profiles**. 9. Click **Microsoft Edge Policies** and click **Properties**. 10. Click **Edit** next to **Configuration settings**. 11. Navigate to **Computer Configuration > Microsoft Edge** and search for the policy - **Configure Internet Explorer integration** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under Configure Internet Explorer integration, select **Internet Explorer mode** and click **OK**. 12. Now search for the policy - **Configure the Enterprise Mode Site List** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under Configure the Enterprise Mode Site List, enter **http://CM1/ContosoLearning/EMEISiteList.xml** and click **OK**.

	13. Click **Review + save** at the bottom and then click **Save** again.
Complete these steps on the CLIENT3 virtual machine.	
Verify IE Mode Policies	14. First launch the new **Microsoft Edge** and in the address bar type **http://CM1/ContosoLearning** and press enter. 15. Note the warning "**Your browser is not supported by ContosoLearning. Only Internet Explorer is Supported**". 16. Close **Microsoft Edge**. 17. Click **Start > Settings > Accounts > Access work or school**. 18. Select **Connected by TU1@<Azure Domain>.onmicrosoft.com/Connected to <AzureDomain>'s Azure AD** and click **Info**. 19. Click **Sync**. 20. Once the sync has completed, after a few minutes, launch the new **Microsoft Edge** again. 21. In the address bar type **http://CM1/ContosoLearning** and press enter. 22. Notice that the new **Microsoft Edge opens the website in Internet Explorer mode**. You can notice an **icon of Internet Explorer in the address bar** on which when you hover you mouse, it displays **Internet Explorer mode**. Also notice that you will **not see the warning**.

8.3 Setup Enterprise New Tab Page

In this section, we will perform the following scenarios:

- Configure and Deploy Enterprise New Tab using On-Premises Method
- Configure and Deploy Enterprise New Tab using Intune

8.3.1 Configure and Deploy Enterprise New Tab using On-Premises Method

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Configure and Deploy Enterprise New Tab Policies	1. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 2. Right-click **Microsoft Edge Policies** and click **Edit...** 3. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Startup, home page and new tab page**. 4. Look for the policy - **Configure the new tab page URL** and double-click it. 5. Select **Enabled** and under Options, enter **https://www.microsoft.com**. Click **Apply** and **OK**. 6. Now look for the policy - **Action to take on startup** and double-click it.

	7. Select **Enabled** and under Options, under Action to take on startup, select **Open a list of URLs**. Click **Apply** and **OK**. 8. Now look for the policy - **Sites to open when the browser starts** and double-click it. 9. Select **Enabled** and under Options, click **Show...** and enter **https://www.bing.com** and **https://www.google.com** and then click **OK**. Click **Apply** and **OK**. 10. Now look for the policy - **Show Home button on toolbar** and double-click it. 11. Select **Enabled**. Click **Apply** and **OK**. 12. Close all the windows.
Complete these steps on the CLIENT1 virtual machine.	
Verify Enterprise New Tab Policies	13. Launch an administrative command prompt window. 14. Run the command **gpupdate /force**. 15. Now launch the new **Microsoft Edge**. First notice the **home button** at the **toolbar**. Then notice that **Bing** and **Google** websites were opened at the launch of the browser in **2 separate tabs**. 16. Now start a **new tab**. Notice that **Microsoft's** website opens up.

8.3.2 Configure and Deploy Enterprise New Tab using Intune

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Configure and Deploy Enterprise New Tab Policies	1. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **Devices > Configuration profiles**. 3. Click **Microsoft Edge Policies** and click **Properties**. 4. Click **Edit** next to **Configuration settings**. 5. Navigate to **Computer Configuration > Microsoft Edge > Startup, home page and new tab page**. Search for the policy - **Configure the new tab page URL** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under the New tab page URL, enter **https://www.microsoft.com** and click **OK**. 6. Now search for the policy - **Action to take on startup** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under the Action to take on startup, select **Open a list of URLs** and click **OK**. 7. Now search for the policy - **Sites to open when the browser starts** and click the policy from the search results which has the **Setting type Device**. Select **Enabled**, under the Sites to open when the browser starts, enter **https://www.bing.com** and **https://www.google.com** and click **OK**.

8. Now search for the policy - **Show Home button on toolbar** and click the policy from the search results which has the **Setting type Device**. Select **Enabled** and click **OK**.
9. Click **Review + save** at the bottom and then click **Save** again.

Complete these steps on the CLIENT3 virtual machine.

Verify Enterprise New Tab Policies

10. Click **Start > Settings > Accounts > Access work or school**.
11. Select **Connected by TU1@<Azure Domain>.onmicrosoft.com/Connected to <AzureDomain>'s Azure AD** and click **Info**.
12. Click **Sync**.
13. Once the sync has completed, after a few minutes, launch the new **Microsoft Edge**.
14. First notice the **home button** at the **toolbar**. Then notice that **Bing** and **Google** websites were opened at the launch of the browser in **2 separate tabs**.
15. Now start a **new tab**. Notice that **Microsoft's** website opens up.

9 Security and Compliance

In this module, you will go through Windows 11 capabilities that could help organizations be more secure. We will cover the following scenarios:

- BitLocker device encryption
- Windows Defender Antivirus
- Windows Hello for Business
- Windows Defender Credential Guard
- Windows Defender Application Guard
- Windows Defender Exploit Guard
- Windows Defender Application Control
- Windows Defender Advanced Threat Protection

Note: In order to avoid hiccups during "Modern Management" scenarios using Intune, if you have been using **CLIENT3** and **CLIENT4** as Azure AD Joined or Enrolled to MDM Only in other Labs, recommend you to disjoin the machines from Azure AD or Un-enroll the machines from MDM, cleanup these two computer objects from Azure AD and Intune Portals and then re-join them to Azure AD using **TU2@<AzureDomainName>.onmicrosoft.com**. They will get automatically enrolled to Intune as well.

Note: In order to see immediate effects of Intune policies after running a sync, reboot the machine or shut down and then start the machine. It may take few minutes for the policies to be applied on the machine from Intune.

9.1 BitLocker

In this section, we will walk you through setting up BitLocker using modern and on-premises management.

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later (Note: Windows 11 requires TPM version 2.0). The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

On computers that do not have a TPM version 1.2 or later, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation. Starting with Windows 8, you can use an operating system volume password to protect the operating system volume on a computer without

TPM. Both options do not provide the pre-startup system integrity verification offered by BitLocker with a TPM.

In addition to the TPM, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device, such as a USB flash drive, that contains a startup key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is presented.

9.1.1 Cloud Management.

The below section will walk you through setting up BitLocker with Intune.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Create Groups	1. Close all browser windows. 2. Start Edge InPrivate mode. 3. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Groups**. 5. Click **+ New group**. 6. In the Group pane fill in the following values and click **Select**: GROUP TYPE: **Security** GROUP NAME: **BitLockerDemo** MEMBERSHIP TYPE: **Assigned** MEMBERS: **TU1, TU2** 7. Click **Create**.

Configure Windows BitLocker

8. On the left navigation bar, click **Devices > Configuration profiles**.
9. Select "**+ Create profile**".
10. For **Platform** select **Windows 10 and later**.
11. For **Profile type** select **Endpoint protection** and click **Create**.
12. Under the **Basics** step, enter the following and click **Next**:
    Name: **BitLocker Demo**
13. Under the **Configuration settings** step, enter the following and click **Next**:
    Expand **Windows Encryption**
    Encrypt devices: **Require**
    Encrypt storage card (mobile only): **Not configured**
    Warning for other disk encryption: **Not configured**
    Configure encryption methods: **Enable**
    Encryption for operating system drives: **XTS-AES 128-bit**
    Encryption for fixed data-drives: **XTS-AES 128-bit**
    Encryption for removable data-drives: **AES-CBC 128-bit**
    Additional authentication at startup: **Not configured**
    Note: The rest is not going to be configured.
14. Under the **Assignments** step, under **Included groups** enter the following and click **Next**:
    Click **+ Add groups**
    Select **BitLockerDemo**
15. Under the **Applicability Rules** step, click **Next**.
16. Under the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.

Verify the Policy has been Applied and Working

17. Log in to the machine as:
    TU2@<AzureDomainName>.onmicrosoft.com
18. Select **Start**.
19. Select **Settings**.
20. Select **Accounts**.
21. Select **Access work or school**.
22. Select **Connected to <CompanyName> Azure AD**.
23. Click **Info**.
24. Click **Sync** to force a policy update and confirm that the sync was successful.
25. After a few minutes of syncing, you will notice that a notification appears **Encryption needed** (at least once) asking you to start encryption.
    Note: Make sure this is no bootable media in the CD/DVD drive.

9.2 Windows Defender Antivirus

Windows Defender Antivirus keeps your PC safe with trusted antivirus protection built-in to Windows 11. Windows Defender Antivirus delivers comprehensive, ongoing and real-time protection against software threats like viruses, malware and spyware across email, apps, the cloud and the web.

In this section, you can use modern or on-premises management to configure WDAV.

9.2.1 Cloud Management

In this section, you are going to configure Windows defender using Intune.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Create Groups for use with Windows Defender Anti-Virus Lab	1. Close all browser windows. 2. Start Microsoft Edge InPrivate mode. 3. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Groups**. 5. Click **+ New group**. 6. In the Group pane fill in the following values and click **Select**: GROUP TYPE: **Security** GROUP NAME: **WDAVDemo** MEMBERSHIP TYPE: **Assigned** MEMBERS: **TU1,TU2** 7. Click **Create**.
Creating an Intune Windows Defender Antivirus Policy	8. On the left navigation bar, click **Devices > Configuration profiles**. 9. Click **+ Create profile**. 10. For **Platform**, select **Windows 10 and later**. 11. For **Profile type**, select **Templates**. 12. For **Template name**, select **Device restrictions** and click **Create**. 13. Under the **Basics** step, enter the following information and click **Next**: Name: **WDAV Demo** 14. Under the **Configuration settings** step, enter the following information and click **Next**: Expand **Microsoft Defender Antivirus**
	Real-time monitoring: **Enable** Behavior monitoring: **Enable** Network Inspection System (NIS): **Enable** Scan all downloads: **Enable**

Scan scripts loaded in Microsoft web browsers: **Enable**

End-user access to Defender: **Block**

Security intelligence update interval (in hours): **2**

Monitor file and program activity: **Monitor incoming files only**

Days before deleting quarantined malware: **90**

CPU usage limit during a scan: **10**

Scan archive file: **Enable**

Scan incoming mail messages: **Enable**

Scan removable drives during a full scan: **Enable**

Scan files opened from network folders: **Enable**

Cloud-delivered protection: **Enable**

Time extension for file scanning by the cloud: **50**

Prompt users before sample submission: **Always prompt**

Detect potentially unwanted applications: **Enable**

On Access Protection: **Block**

Actions on detected malware threats: **Enable**

Low severity: **Quarantine**

Moderate severity: **Quarantine**

High severity: **Quarantine**

Severe severity: **Quarantine**

Note: No exclusions will be configured

15. Under the **Assignments** step, under **Included groups**, enter the following and click **Next**:

    Click **+ Add groups**

    Select **WDAVDemo**
16. Under the **Applicability Rules** step, click **Next**.
17. Under the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.

Verify the Policy has been Applied and Working	18. Log in to the machine as: **TU2@<AzureDomainName>.onmicrosoft.com** 19. Select **Start**. 20. Select **Settings**. 21. Select **Accounts**. 22. Select **Access work or school**. 23. Select **Connected to <CompanyName> Azure AD**. 24. Click **Info**. 25. Click **Sync** to force a policy update and confirm that the sync was successful. 26. Close **Settings**. 27. **Reboot** the machine. 28. Log back in with the same credentials. 29. Click **Start**. 30. Type and click "**Windows Security settings**". **Note:** Notice that the page for **Virus & threat protection** is not available under **Protection areas** in a few moments because of the policy managing it.

9.2.2 On-premises Method

In this section, you will use Configuration Manager to manage WDAV on clients.

Task	Detailed Steps
Complete these steps on the CM1 virtual machine.	
Add "Endpoint Protection Role" to your Site	1. From the Configuration Manager Console, browse to **Administration**. 2. Expand **Overview > Site Configuration**. 3. Click on **Servers and Site System Roles**. 4. Right-click on **CM1.corp.contoso.com**. 5. Select **Add Site System Roles**. 6. On the **Select a server to use as a site system** step, click **Next**. 7. On the **Specify Internet proxy server** step, click **Next**. 8. On the **Specify roles for this server** step, check **Endpoint Protection point**. 9. On the pop-up window, click **OK** and then click **Next**. 10. On the **Specify Cloud Protection Service membership type** step, select **Basic membership (on Windows 10 and above, the behavior is the same as advanced membership)** click **Next**. 11. On the **Confirm the settings** step, click **Next**. 12. On the **Completion** step, click **Close**.

Enable Configuration Manager to Manage Client Endpoint Protection	13. Under **Administration**, click on **Overview > Client Settings**. 14. Right-click on **Default Client Settings**. 15. Click on **Properties**. 16. Click on **Endpoint Protection**. Click **OK** if a prompted. 17. Change **Manage Endpoint Protection client on client computers** to **Yes**. 18. Click on **OK**.
Create a Collection	19. Browse to **Assets and Compliance**. 20. Click on **Overview > Devices**. 21. Right-click on **CLIENT1**. 22. Click on **Add Selected Items**. 23. Select **Add Selected Items to New Device Collection**. 24. Enter **WDAV Client1** for the collection name. 25. Limit collection to **All Desktop and Server Clients**, click **Next**. 26. On the **Membership Rules** step, click **Next**. 27. On the **Summary** step, click **Next**. 28. On the Completion step, click **Close**.
Create a Custom Antimalware Policy	29. Still under **Assets and Compliance**, expand on **Overview > Endpoint Protection**. 30. Click on **Antimalware Policies**. 31. In the ribbon, click on **Create Antimalware Policy**. 32. Fill out the form: Name: **WDAV Demo Policy** Description: **WDAV Demo Policy** Check the following boxes: **Schedule scans** **Scan settings** **Default actions** **Real-time protection** **Exclusion settings** **Advanced** **Threat overrides** **Cloud Protection Service** **Security Intelligence updates** 33. Click on **OK**. 34. Right-click on **WDAV Demo Policy** and click **Deploy**. 35. On the Select Collection window, select **WDAV Client1** and then click **OK**.
Complete these steps on the CLIENT1 virtual machine.	

Check Policy Configuration	36. Open **Control Panel**. 37. Search for **Configuration Manager**. 38. Open **Configuration Manager**. 39. Click on the **Actions** Tab. 40. Click on **Machine Policy Retrieval & Evaluation Cycle**. 41. Click on **Run Now**. Click **OK**. 42. Wait 3 to 5 minutes then continue. 43. Click **Start**. 44. Type **Windows Security** and click **Windows Security settings**. 45. Under **Protection areas** click **Virus & threat protection**. 46. Under **Virus and threat protection settings**, click **Manage settings**. 47. Notice the *This setting is managed by your administrator*.

9.3 Windows Hello for Business

Windows Hello for Business replaces username and password sign-in to Windows with strong user authentication based on asymmetric key pair.

In this lab, you will find all the information to deploy Windows Hello for Business in a Certificate Trust Model in your on-premises environment.

9.3.1 Cloud Management

The following sections cover managing Windows Hello for Business through modern management tools. In this lab we are going to setup Windows Hello for Business in the Cloud.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Configuring Windows Hello for Business	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Devices > Enroll devices**. 4. Click **Windows Hello for Business**. 5. Next to **Configure Windows Hello for Business**, select **Enabled**. 6. Review the possible settings, then click **Save**.
Complete these steps on the CLIENT4 virtual machine or a physical machine if your environment does not support nested virtualization.	

Setting up your PIN for the First Time

7. Log in for the first time to the virtual machine as: **TU1@<AzureDomainName>.onmicrosoft.com**, assuming it is already Azure AD Joined and Autoenrolled into Intune.
8. Click "**Set up PIN**".
9. Click "**Set it up now**".
10. Select a verification method "**Text message**".
11. Select a region that is correct for your cell phone.
12. Enter your phone number.
13. Select **Next**.

Note: Steps 9-13 are required only when you are setting up for the first time for a user.

14. Retrieve security code from your phone and enter it.
15. Select **Verify**.
16. Enter a new PIN "214359" (or a PIN of your choice, just don't forget it).
17. Confirm your PIN "214359" and click **OK**. Click **OK** again. Now you will test your new PIN.
18. Sign out.
19. Sign back in using your PIN.

9.4 Windows Defender Credential Guard

Introduced in Windows 10 Enterprise and Windows Server 2016, Windows Defender Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Windows Defender Credential Guard prevents these attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

Credential Guard provides an additional layer for protecting secrets, specifically domain user credentials by storing them in a container, secured by the Virtual Secure Mode (VSM), based on Virtualization Based Security (VBS).

These types of containers are separated both from the kernel and the user mode, therefore increasing the difficulty for an attacker, even after compromising the system to steal the credentials directly from Local Security Authority Subsystem (LSASS), for example.

Before working on this lab, you must have:

- A system with a 64-bit CPU and support for VT-x (Intel) or AMD-V
- Trusted Platform Module (TPM) chip is recommended.
- UEFI with Secure Boot
- Windows 10 Enterprise or Windows 11 Enterprise client.
- Local Administrator Account.

- If running on a Hyper-V VM, the Hyper-V host must have an IOMMU and run at least Windows Server 2016 or Windows 10 version 1607. The VM must be Generation 2 with Secure Boot enabled.
- It is recommended that you use a lab system for testing purposes. Please do not use your personal machines. Also, the system must not be domain joined into your company domain, so that there is no compliance or configuration/support issues.

Note: See a full list of requirements and security qualifications in the Windows Defender Credential Guard Requirements (Windows) - Windows security | Microsoft Docs page.

9.4.1 Check Windows Defender Credential Guard Requirements

In this exercise, you will:

- Check if the requirements for Credential Guard are fulfilled.
- Download and run the **Device Guard and Credential Guard hardware readiness tool**.

Task	Detailed Steps
Complete this activity on the lab system provided by the Customer or CLIENT 1-4.	
System Verification	1. Log in as **.\Administrator or the Local Administrator Account** and open **MSINFO32.EXE** (elevated) and check if: ▪ BIOS Mode = UEFI ▪ Secure Boot State = On ▪ A hypervisor has been detected 2. If any of the above values are not enabled, then boot into your BIOS/UEFI and make sure they are configured correctly along with the virtualization settings. 3. Note that if UEFI is in CSM (compatibility) mode, changing it to UEFI Native will require the partition layout to be GPT instead of MBR (requires formatting the hard drive).

TPM Verification

4. Open **TPM.MSC** and make sure that the TPM is turned on.
5. If TPM is turned off/not visible, make sure that it exists physically and it is enabled in BIOS/UEFI.
6. If the TPM is turned on but not initialized:
    a. Create the TPM owner password using **Automatically create the password** option.
    b. In the **Save your TPM owner password**, click **Save the password** and select a location to save the password, and then click **Save** (file is saved as computer_name.tpm).
    c. Click **Initialize**.
    d. After this, the TPM should be ready for use.

Note: The recommended version of TPM is 2.0. Windows might refuse to activate Credential Guard if the computer contains an older TPM version/revision.

Download and run the **Device Guard and Credential Guard hardware readiness tool**

7. Start Microsoft Edge InPrivate mode.
8. Download the Device Guard and Credential Guard hardware readiness tool.
   Note: If the above link does not work, search on the phrase "Device Guard and Credential Guard hardware readiness tool" in order to find the latest version.
9. Extract the downloaded zip file to C:\dgreadiness.
10. Open an elevated PowerShell prompt and change the directory to C:\dgreadiness.
11. Run the following command:
    .\DG_Readiness_Tool_v{x.x}.ps1 -Capable
    Note: If Execution-Policy is not already set to allow running script, then you should manually set it as below and then use the readiness script:
    Set-ExecutionPolicy Unrestricted
12. The first time the readiness tool runs, the system will need to be rebooted in order to enable the driver verification.
13. After the reboot, rerun the following command:
    .\DG_Readiness_Tool_v{x.x}.ps1 -Capable
14. Verify in the Summary output that "Device Guard / Credential Guard can be enabled on this machine." If this is not displayed, then correct any issues before proceeding with this section.
    Note: This tool can also be used to enable, disable and verify Device Guard and Credential Guard. Refer to the ReadMe that is included in the download for more information.

9.4.2 Cloud Management

Follow the following sections for managing Windows Defender Credential Guard using Intune.

Task	Detailed Steps
Complete these steps from an internet-connected Windows computer.	
Create Groups for use with Credential Guard Lab	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 4. Click **+ New group**. 5. In the Group pane fill in the following values: GROUP TYPE: **Security** GROUP NAME: **CredGuardDemo** MEMBERSHIP TYPE: **Assigned** MEMBERS: **TU1,TU2** 7. Click **Select | Create**.
Creating an Intune Credential Guard Policy	8. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 9. On the left navigation bar, click **Devices > Configuration profiles**. 10. Click on "**+ Create profile**". 11. For **Platform**, select **Windows 10 and later**. 12. For **Profile type**, select **Templates**. 13. Search for and select **Endpoint protection** and then click **Create**. 14. On the **Basics** step, enter the following information and click **Next**. Name: **Cred Guard Demo** Description: **Cred Guard Demo** 15. On the **Configuration settings** step, select **Microsoft Defender Credential Guard: Enable without UEFI lock** and click Next. 16. On the **Assignments** step, under **Included groups**, click **Add groups** and select **CredGuardDemo**, then click **Next**. 17. On the **Applicability Rules** step, click **Next**. 18. On the **Review + Create** step, click **Create**.
Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.	
Verify the Policy has been Applied	19. Log in to a machine as: **TU2@<AzureDomainName>.onmicrosoft.com** (You might have to enable MFA for this user on this machine). 29. Select **Start**.

and Working	30. Select **Settings**. 31. Select **Accounts**. 32. Select **Access work or school**. 33. Select **Connected by TU2@<Azure Domain>.onmicrosoft.com/Connected to <Azure Domain> Azure AD**. 34. Click **Info**. 35. Click **Sync** to force a policy update and confirm that the sync was successful. 36. Close **Settings**. 37. **Reboot** the machine. 38. Log back in using the same credentials. 39. Click **Start**. 40. Type and click "**System Information**". 41. Verify that "**Virtualization-based security is running**". **Note:** After the first boot it could be "**Enabled but not running**". 42. **Restart** the computer again. 43. Click **Start** and run "**System Information**". 44. Verify the following: **Virtualization-based Security: Running** **Note:** It can take up to 3 or more reboots and syncing to see that it is running.

9.4.3 On-premises method

Follow the following sections for managing Windows Defender Credential Guard through on-premises management tools.

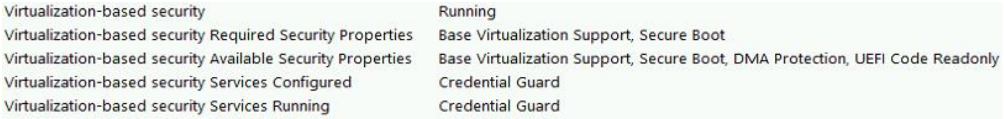
Now that the required features and components are in place, activate the Virtualization Based Security and Credential Guard.

Task	Detailed Steps
Complete these steps on the CLIENT2 virtual machine or a physical machine if your environment does not support nested virtualization.	

System Configuration	1. Log in as **.\Administrator or the Local Administrator Account** and open **gpedit.msc** and accept the UAC prompt if required. 2. Go to **Computer Configuration > Administrative Templates > System > Device Guard**. 3. Edit the **Turn On Virtualization Based Security** policy by selecting **Enabled**. ~~4.~~ For the **Select Platform Security Level** setting, select **Secure Boot**. 5. For the **Credential Guard Configuration** setting, select **Enable without lock**. 6. Click **Apply** and **OK**. 7. Restart the computer and check "**System Information**" and verify the following: **Virtualization-based Security: Running** **Virtualization-based security Services Configured: Credential Guard** **Virtualization-based security Services Running: Credential Guard**

9.4.4 Troubleshoot Credential Guard

After enabling all of the above features and settings, make sure that no errors were logged and all the components are properly configured.

<table>
<tr><th>Task</th><th>Detailed Steps</th></tr>
<tr><td colspan="2"><b>Complete these steps on the CLIENT2 virtual machine or a physical machine if your environment does not support nested virtualization.</b></td></tr>
<tr><td>Logging</td><td>1. Device Guard policies are logged in Event Viewer at <b>Applications and Services Logs > Microsoft > Windows > DeviceGuard > Operational</b>.
2. An <b>Event ID 7000</b> should be logged, which contains the selected settings within the policy (when successfully applied).</td></tr>
<tr><td>MSInfo32</td><td>3. Open <b>MSINFO32.EXE</b> (elevated) and confirm that the options are defined as in the following screenshot.

<table>
<tr><td>Virtualization-based security</td><td>Running</td></tr>
<tr><td>Virtualization-based security Required Security Properties</td><td>Base Virtualization Support, Secure Boot</td></tr>
<tr><td>Virtualization-based security Available Security Properties</td><td>Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly</td></tr>
<tr><td>Virtualization-based security Services Configured</td><td>Credential Guard</td></tr>
<tr><td>Virtualization-based security Services Running</td><td>Credential Guard</td></tr>
</table></td></tr>
<tr><td>Registry</td><td>4. Browse to <b>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard</b>.
5. Verify if <b>EnableVirtualizationBasedSecurity</b> is set to <b>1</b>.
6. Verify if <b>RequirePlatformSecurityFeatures</b> is set to <b>1</b> (Secure Boot).
7. Browse to <b>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa</b>.
8. Verify if the <b>LsaCfgFlags</b> is set to <b>2</b>.</td></tr>
<tr><td>Process</td><td>9. Open <b>Task Manager</b>.
10. Verify the presence of <b>Lsalso.exe</b>.</td></tr>
</table>

9.5 Microsoft Defender Application Guard

Designed for Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and internal networks. Everything not on your list is considered untrusted.

If an employee goes to an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated Hyper-V-enabled container, which is separate from the host operating system. This container isolation means that if the untrusted site turns out to be malicious, the host PC is protected, and the attacker can't get to your enterprise data.

Note: Microsoft Defender Application Guard can only be enabled if the Hardware Requirements are met as stated in System requirements for Microsoft Defender Application Guard - Windows security | Microsoft Docs

Note: Hardware requirements include CPU virtualization extensions. The Logical Processors and Memory on VMs can be increased from Hyper-V Manager. To know if your Hyper-V Host's or Physical Machine's Processor supports extended page tables, also called *Second Level Address Translation (SLAT)*, download and extract CoreInfo from https://docs.microsoft.com/en-us/sysinternals/downloads/coreinfo and run **coreinfo.exe –v**. If it does not support, you will see a dash else you will see an asterisk. The Virtualization Extensions for VBS can be enabled from BIOS or UEFI. When running on a VM, make sure the number of vCPUs is set to 4 (or higher), the RAM is set to 8200 MB so the VM sees a full 8 GB (or higher), and enable nested virtualization on the VM (i.e. Set-VMProcessor -VMName "HYD-CLIENT3" -ExposeVirtualizationExtensions $true)

9.5.1 Cloud Management

Follow the following sections for managing **Error! Unknown document property name.** using Intune.

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Create Groups for use with WD Application Guard Demo	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 4. Click **+ New group**. 5. In the Group pane fill in the following values and click **Select**: GROUP TYPE: **Security** GROUP NAME: **AppGuardDemo** MEMBERSHIP TYPE: **Assigned** MEMBERS: **TU1,TU2** 7. Click **Create**.
Creating an Intune WDAG Policy	8. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 9. On the left navigation bar, click **Devices > Configuration profiles**. 10. Click on "**+ Create profile**". 11. Under **Platform**, select **Windows 10 and later**. 12. For **Profile type**, select **Templates**. 13. Search for and select **Endpoint protection** and then click **Create**. 14. On the **Basics** step, enter the following information and click **Next**: Name: **Application Guard Demo** Description: **Application Guard Demo** 15. On the **Configuration settings** step, enter the following and click **Next**: Expand **Microsoft Defender Application Guard** Application Guard: **Enabled for Edge** Clipboard behavior: **Block copy and paste between PC and browser** External content on enterprise sites: **Not configured** Print from virtual browser: **Allow** Printing type(s): **PDF** Collect logs: **Not configured** Retain user-generated browser data: **Not configured** Graphics acceleration: **Not configured** Download files to host file system: **Not configured** 16. On the **Assignments** step, under **Included groups**, click **Add groups** and select **AppGuardDemo**, then click **Next.**

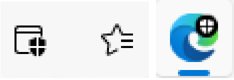
17. On the **Applicability Rules** step, click **Next**.
18. On the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine (if the Hyper-V Host meets all the hardware requirements as stated above) or a physical machine (if the Hyper-V Host meets all the hardware requirements as stated above). NOTE: When running on a VM, make sure the number of vCPUs is set to 4 (or higher), the RAM is set to 8200 MB so the VM sees a full 8 GB (or higher), and enable nested virtualization on the VM (i.e. Set-VMProcessor -VMName "HYD-CLIENT3" -ExposeVirtualizationExtensions $true)

Verify the Policy has been Applied and Working

19. Log in to a machine as:
    TU2@<AzureDomainName>.onmicrosoft.com
20. Select **Start**.
21. Select **Settings**.
22. Select **Accounts**.
23. Select **Access work or school**.
24. Select **Connected by TU2@<Azure Domain>.onmicrosoft.com/Connected to <Azure Domain> Azure AD**.
25. Click **Info**.
26. Click **Sync** to force a policy update and confirm that the sync was successful.
27. Close **Settings**. Reboot the machine once.
28. Launch **Microsoft Edge**.
29. Click **New Application Guard window** from the **...** menu.
30. A new window should appear.

    Note: Notice that a browser icon with a shield will appear next to the favorites button. There will also be a shield on the Edge icon in the task bar. This indicates you are running in Application mode.

31. Enter the URL www.bing.com.
32. Create a new tab.
33. Copy the URL www.bing.com to the new tab.

    Note: Notice that you can do this because it is inside of Application Guard.

34. Try to copy the URL from Application Guard **Edge** window to the non-Application Guard **Edge** window.

    Note: Notice that you cannot copy. This is because Application Guard is configured to not allow copy and paste between the PC and the Application Guard browser.

35. Enter the URL of www.msn.com in the non-Application Guard **Edge** window.
36. Copy this URL from the non-Application Guard **Edge** window and try and paste it in Application Guard **Edge** window.

    Note: Notice that you cannot copy. This is because Application Guard is configured to not allow copy and paste between the PC and the Application Guard browser.

9.5.2 On-premises method

Follow the following sections for managing **Error! Unknown document property name.** using on-premises management tools.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine (if the Hyper-V Host meets all the hardware requirements as stated above) or a physical machine (if the Hyper-V Host meets all the hardware requirements as stated above). NOTE: When running on a VM, make sure the number of vCPUs is set to 4 (or higher), the RAM is set to 8200 MB so the VM sees a full 8 GB (or higher), and enable nested virtualization on the VM (i.e. Set-VMProcessor -VMName "HYD-CLIENT3" -ExposeVirtualizationExtensions $true)	
Install the Feature	1. Logon as a Domain Administrator (**corp\labadmin**). 2. Open the **Control Panel**, click **Programs,** and then click **Turn Windows features on or off**. 3. Select the checkbox next to **Microsoft Defender Application Guard** and then click **OK**. 4. Restart the device.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Download ADMX Files (If not downloaded before in the previous labs)	1. Download the latest Administrative Template files (ADMX/ADML) for Windows 11 [Create and manage Central Store - Windows Client | Microsoft Docs]
Install ADMX Files (If not installed before in the previous labs)	2. Install the downloaded administrative templates to a temporary location. 3. Copy **AppHVSI.admx** and **NetworkIsolation.admx** from the temporary location (**.\PolicyDefinitions)** to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. **Note:** If the PolicyDefinitions folder doesn't exist you will have to create it. If prompted, replace the file in the destination directory. 4. Copy **.\PolicyDefinitions\en-US\AppHVSI.adml** and **.\PolicyDefinitions\en-US\NetworkIsolation.adml** from the temporary location to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions\en-US.** **Note:** If prompted, replace the file in the destination directory.

Turn On Windows Defender Application Guard	5. Open the Group Policy Management Console. 6. Create a policy called "**Microsoft Defender Application Guard**". 7. Edit "**Microsoft Defender Application Guard**". 8. Navigate to **Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard**. 9. Double-click **Turn on Microsoft Defender Application Guard in Managed Mode**. 10. Select **Enabled,** choose **Option 1** and click **Apply** and **OK**.
Set Up Network Isolation	11. Navigate to **Computer Configuration\Policies\Administrative Templates\Network\Network Isolation**. 12. Double-click **Enterprise resource domains hosted in the cloud**. 13. Select **Enabled** and type **.microsoft.com** into the **Enterprise cloud resources** box. Click **Apply** and **OK**. 14. Double-click **Domains categorized as both work and personal** setting. 15. Select **Enabled** and type **bing.com** into the **Neutral resources** box. Click **Apply** and **OK**. 16. Link the GPO to the OU containing the clients. **Note:** Create a temporary OU called **Microsoft Defender Application Guard** and move **CLIENT1** there. Run a **gpupdate /force** on the client. Remember to move this client back to the default **Computers** container after the lab is done.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine (if the Hyper-V Host meets all the hardware requirements as stated above) or a physical machine (if the Hyper-V Host meets all the hardware requirements as stated above). NOTE: When running on a VM, make sure the number of vCPUs is set to 4 (or higher), the RAM is set to 8200 MB so the VM sees a full 8 GB (or higher), and enable nested virtualization on the VM (i.e. Set-VMProcessor -VMName "HYD-CLIENT3" -ExposeVirtualizationExtensions $true)	
Test Application Guard	1. Update the group policies by running **gpupdate /force** from the elevated command prompt. Accept the UAC prompt if required. 2. Start Microsoft Edge and type www.microsoft.com 3. After you submit the URL, Application Guard determines the URL is trusted because it uses the domain you've marked as trusted and shows the site directly on the host PC instead of in Application Guard. 4. In the same Microsoft Edge browser, type any URL that isn't part of your trusted or neutral site lists, example www.msn.com 5. After you submit the URL, Application Guard determines the URL is untrusted and redirects the request to the hardware-isolated environment.

9.6 Windows Defender Exploit Guard

Windows Defender Exploit Guard (Windows Defender EG) is a new set of host intrusion prevention capabilities for Windows 10 and Windows 11, allowing you to manage and reduce the attack surface of apps used by your employees.

There are four features in Windows Defender EG:

- Exploit protection can apply exploit mitigation techniques to apps your organization uses, both individually and to all apps.
- Attack surface reduction rules can reduce the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script- and mail-based malware.
- Network protection extends the malware and social engineering protection offered by Windows Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on your organization's devices.
- Controlled folder access helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware.

9.6.1 Cloud Management

Follow the following sections for managing Windows Defender Exploit Guard through cloud management tools.

9.6.1.1 Exploit Guard Controlled Folders

In this section, we are going to create a group that will be used to assign users an Exploit Guard controlled folder policy. In addition we will configure the policy and test that it works.

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Create Groups	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 4. Click **+ New group**. 5. In the Group pane fill in the following values and click **Select**: GROUP TYPE: **Security** GROUP NAME: **ExploitDemo** MEMBERSHIP TYPE: **Assigned** MEMBERS: **TU1,TU2** 6. Click **Create**.
Configure Windows Defender Exploit Guard	7. Navigate to https://endpoint.microsoft.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 8. On the left navigation bar, click **Devices > Configuration profiles**. 9. Click on "**+ Create profile**". 10. Under **Platform**, select **Windows 10 and later**. 11. For **Profile type**, select **Templates**. 12. Search for and select **Endpoint protection** and then click **Create**. 13. On the **Basics** step, enter the following information and click **Next**: Name: **Exploit Protection Demo** 14. On the **Configuration settings** step, enter the following information and click **Next:** Expand **Microsoft Defender Exploit Guard** Expand **Controlled folder access** Folder protection: **Enable** 15. On the **Assignments** step, under **Included groups**, click **Add groups** and select **ExploitDemo**, then click **Next**. 16. On the **Applicability Rules** step, click **Next**.

	17. On the **Review + create** step, click **Create**.
Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.	
Verify Configuration is Applied	18. Log in to the virtual machine as **TU2@<AzureDomainName>.onmicrosoft.com** 19. Select **Start**. 20. Select **Settings**. 21. Select **Accounts**. 22. Select **Access work or school**. 23. Select **Connected by TU2@<Azure Domain>.onmicrosoft.com/Connected to <Azure Domain> Azure AD**. 24. Click **Info**. 25. Click **Sync** to force a policy update and confirm that the sync was successful. 26. Download the Controlled Folder Access test tool (https://demo.wd.microsoft.com/Content/CFAtool.exe). 27. Run the **CFAtool.exe** located in **C:\Packages and** attempt to create a file in the **Documents** directory by clicking the **Create file** button. **Note:** Notice that no file is created in the **Documents** directory. 28. Open the Event Viewer and navigate to Applications and Services Logs > Microsoft > Windows > Windows Defender > Operational. There will an Event ID 1123, which is a blocked controlled folder access event.

9.6.2 On-premises method

Follow the following sections for managing Windows Defender Exploit Guard through on-premises management tools.

9.6.2.1 Exploit Protection

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	

Configure Program-Level Mitigations	1. Open the **Windows Security** by clicking the shield icon in the taskbar or searching the start menu for **Security**. 2. Click the **App & browser control** tile (or the app icon on the left menu bar) and then the **Exploit protection settings** at the bottom of the screen. 3. Go to the **Program settings** section and click **Add program to customize**. 4. Click on **Add by program name** and type **notepad.exe**. Click **Add**. 5. On the next window, scroll down and on **Disable Win32k system calls**, select **Override system settings** and choose **On**. 6. You will be notified if you need to restart the process or app, or if you need to restart Windows. Click **Apply** and accept the UAC prompt if required. 7. Try to open **notepad.exe**. Notice the error message. Click **OK**.
Create and Export a Configuration File	8. Open the **Windows Security** by clicking the shield icon in the taskbar or searching the start menu for **Security**. 9. Click the **App & browser control** tile (or the app icon on the left menu bar) and then the **Exploit protection settings** at the bottom of the screen. 10. At the bottom of the **Exploit protection** section, click **Export settings** and then save the configuration file under **Documents**. 11. Copy the file to **DC1** in a shared folder with full permissions.
Complete these steps on the DC1 virtual machine.	
Download ADMX Files (If not downloaded before in the previous labs)	12. Download the latest Administrative Template files (ADMX/ADML) for Windows 11 [Create and manage Central Store - Windows Client | Microsoft Docs]()
Install ADMX Files (If not installed before in the previous labs)	13. Install the downloaded administrative templates to a temporary location. 14. Copy **ExploitGuard.admx** and **WindowsDefender.admx** from the temporary location (**.\PolicyDefinitions)** to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. **Note:** If the PolicyDefinitions folder doesn't exist you will have to create it. If prompted, replace the file in the destination directory. 15. Copy **ExploitGuard.adml** and **WindowsDefender.adml** from the temporary location (**.\PolicyDefinitions\en-US)** to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions\en-US.** **Note:** If prompted, replace the file in the destination directory.

Distribute the Configuration File with Group Policy	16. On your Group Policy management machine, open the **Group Policy Management Console**, right-click the **Group Policy Objects** and create a new GPO **WDEG**. 17. Right-click the new Group Policy **WDEG** and click **Edit**. 18. In the **Group Policy Management Editor** go to **Computer Configuration**. 19. Click **Policies** then **Administrative Templates**. 20. Expand the tree to **Windows Components > Microsoft Defender Exploit Guard > Exploit Protection**. 21. Double-click the **Use a common set of exploit protection settings** setting and set the option to **Enabled**. 22. In the **Options** section, enter the location and filename of the Exploit Protection Configuration File that you saved from the previous section in a UNC format including the name of the file and its extension and click **Apply | OK**.

9.6.2.2 Attack Surface Reduction

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Distribute the Configuration File with Group Policy	1. On your Group Policy management machine, open the **Group Policy Management Console**, and right-click the Group Policy Object **WDEG**. 2. Click **Edit**. 3. In the **Group Policy Management Editor** go to **Computer Configuration**. 4. Click **Policies** then **Administrative Templates**. 5. Expand the tree to **Windows Components > Microsoft Defender Antivirus > Microsoft Defender Exploit Guard > Attack Surface Reduction**. 6. Double-click the **Configure Attack Surface Reduction rules** setting and set the option to **Enabled**. Click **Show…** and enter the following rule ID in **Value name: D3E037E1-3EB8-44C8-A917-57927947596D** 7. Set the **Value** to **1** and click **OK**. Click **Apply | OK**. 8. Link the GPO **WDEG** to the root domain. __Note:__ The above rule will block JavaScript or VBScript from launching downloaded executable content as well as block notepad.exe to launch. Do run a **gpupdate /force** on the **CLIENT2** VM.

9.7 Windows Defender Application Control

With thousands of new malicious files created every day, using traditional methods like antivirus solutions—signature-based detection to fight against malware—provides an inadequate defense against new attacks.

In most organizations, information is the most valuable asset, and ensuring that only approved users have access to that information is imperative. However, when a user runs a process, that process has the same level of access to data that the user has. As a result, sensitive information could easily be deleted or transmitted out of the organization if a user knowingly or unknowingly runs malicious software.

Application control can help mitigate these types of security threats by restricting the applications that users are allowed to run and the code that runs in the System Core (kernel). Application control policies can also block unsigned scripts and MSIs, and restrict Windows PowerShell to run in Constrained Language Mode.

Application control is a crucial line of defense for protecting enterprises given today's threat landscape, and it has an inherent advantage over traditional antivirus solutions. Specifically, application control moves away from an application trust model where all applications are assumed trustworthy to one where applications must earn trust in order to run.

9.7.1 Cloud Management

Task	Detailed Steps
Complete these steps from an Internet-Connected Windows computer.	
Create Groups for use with WDAC Demo	1. Start Microsoft Edge InPrivate mode. 2. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 3. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 4. Click **+ New group**. 5. In the Group pane fill in the following values and click **Select**: GROUP TYPE: **Security** GROUP NAME: **WDACDemo** MEMBERSHIP TYPE: **Assigned** MEMBERS: **TU1,TU2** 6. Click **Create**.

Configuring WDAC with Intune

7. Navigate to https://portal.azure.com and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**.
8. On the left navigation bar, click **Devices > Configuration profiles**.
9. Click on "**+ Create profile**".
10. Under **Platform**, select **Windows 10 and later**.
11. For **Profile type**, select **Templates**.
12. Search for and select **Endpoint protection** and then click **Create**.
13. On the **Basics** step, enter the following information and click **Next**:
    Name: **WDAC Demo**
    Description: **WDAC Demo**
14. On the **Configuration settings** step, enter the following information and click **Next**:
    Expand **Microsoft Defender Application Control**
    Application control code integrity policies: **Enforce**
    Trust apps with good reputation: **Enable**
15. On the **Assignments** step, under **Included groups**, click **Add groups** and select **WDACDemo**, then click **Next**:
16. On the **Applicability Rules** step, click **Next**.
17. On the **Review + create** step, click **Create**.

Complete these steps on the CLIENT3 virtual machine or a physical machine if your environment does not support nested virtualization.

Verify Configuration is Applied

18. Log in to the virtual machine as **TU2@<AzureDomainName>.onmicrosoft.com**
19. Select **Start**.
20. Select **Settings**.
21. Select **Accounts**.
22. Select **Access work or school**.
23. Select **Connected to <CompanyName> Azure AD**.
24. Click **Info**.
25. Click **Sync** to force a policy update and confirm that the sync was successful.
26. Download **camstudio** from http://camstudio.org.
27. Try and install the application **camstudio**.
28. The app will be blocked by WDAC when you try and install it.

9.7.2 On-premises method

In this section, you will learn how to Configure and Deploy Code Integrity Policies and Enable Device Guard in an enterprise.

Note: Ignore any errors or warnings from the PowerShell commands below.

9.7.2.1 Prerequisites

Perform the following tasks before proceeding to the succeeding sections.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Download VLC Media Player	1. Open Internet Explorer and browse to the URL below. http://www.videolan.org/vlc/ 2. Click **Download VLC** and save the latest version to **C:\Packages**.
Download CamStudio	3. Open Internet Explorer and browse to the URL below. http://camstudio.org/ 4. Click **Download** and save **camstudio.exe** to **C:\Packages**.

9.7.2.2 Create CI Policy from a Golden System

In this activity, you will go through the steps in creating your first Code Integrity (CI) policy from a “Golden” system.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Open PowerShell	1. Logon as a Domain Administrator (**corp\labadmin**) and from the Start Menu, start an elevated instance of PowerShell.
Create Shadow Copy of System Drive	2. From the PowerShell window, run the following commands: **$s1 = (gwmi -List Win32_ShadowCopy).Create("C:\", "ClientAccessible")** **$s2 = gwmi Win32_ShadowCopy | ? { $_.ID -eq $s1.ShadowID }** **$d = $s2.DeviceObject + "\"** **cmd /c mklink /d C:\scpy "$d"**
Generate a New Policy from Scan	3. From the PowerShell window, run the following commands: **New-CIPolicy -level PcaCertificate -filepath C:\PoCPolicy.xml –scanpath C:\scpy –u** **Note:** It may take around 20-30 minutes and during the process a base policy will be created. If required, increase the memory of the virtual machine for this process to run efficiently. Ignore any errors received after command execution completes.

Explore Policy Configuration	4. Save the file **PoCPolicy.xml** to a network location, example: **\\DC1\C$**. 5. Open the file and review the content without making changes. Open the file **C:\PoCPolicy.xml** with **Windows PowerShell ISE**. 6. Close the file.

9.7.2.3 Configurable Code Integrity – Audit Mode

In this activity, you will create a CI policy and deploy it in audit mode.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Convert from XML to Binary File	1. From the PowerShell window, run the following commands: **ConvertFrom-CIPolicy C:\PoCPolicy.xml C:\PoCPolicy.bin**
Install Complied Policy	2. From the PowerShell window, run the following commands: **cp C:\PoCPolicy.bin c:\Windows\System32\CodeIntegrity\SIPolicy.p7b** 3. Restart **CLIENT1** and re-log in with the same credentials.
Verify Audit Logs	4. Launch the installation package for VLC located at **\\DC1\C$\Packages\vlc-3.0.10-win64.exe** and install the package. The installation will be successful at this point. 5. Right-click on the **Start** button and click **Run**. 6. Enter **eventvwr.msc** and click **OK**. 7. In the Event Viewer MMC, browse to **Event Viewer (Local)** > **Applications and Services Logs** > **Microsoft** > **Windows** > **CodeIntegrity** > **Operational**. 8. Browse through the log files especially **Event ID 3076**.

9.7.2.4 Creating CI Policy from Audit Logs

In this activity, you will go through the steps in creating a Code Integrity (CI) policy from audit log events.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	

Create a CI Policy from Audit Logs	1. From the Start Menu, start an elevated instance of PowerShell. 2. From the PowerShell window, run the following commands: **New-CIPolicy -l PcaCertificate -f C:\AuditPoCPolicy.xml –a –u** **Note**: Ignore any errors received after command execution completes. 3. Open the file **C:\AuditPoCPolicy.xml** with **Windows PowerShell ISE**. 4. Close the file.
Merge Golden Policy with Policy from Audit Logs	5. From the PowerShell window, run the following commands: **Merge-CIPolicy –OutputFilePath C:\MergedPoCPolicy.xml –PolicyPaths C:\AuditPoCPolicy.xml,C:\PoCPolicy.xml** 6. Open the file **C:\MergedPoCPolicy.xml** with **Windows PowerShell ISE**. 7. Close the file.

9.7.2.5 Configurable Code Integrity – Enforce Mode

In this activity, you will deploy and enforce a CI policy to lock down the system.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Disable Audit Mode	1. From the PowerShell window, run the following commands: **Set-RuleOption –option 3 -delete –FilePath C:\MergedPoCPolicy.xml** 2. Open the file **C:\MergedPoCPolicy.xml** with **Windows PowerShell ISE**. 3. Close the file.
Convert from XML to Binary File	4. From the PowerShell window, run the following commands: **ConvertFrom-CIPolicy C:\MergedPoCPolicy.xml C:\MergedPoCPolicy.bin**
Install Compiled Policy	5. From the PowerShell window, run the following commands: **cp C:\MergedPoCPolicy.bin c:\Windows\System32\CodeIntegrity\SIPolicy.p7b** 6. Restart **CLIENT1** and re-log in with the same credentials.
Install or Launch Your Application(s)	7. Launch the installation package for CamStudio or VLC located at **\\DC1\C$\Packages\camstudio.exe** or **\\DC1\C$\Packages\vlc-3.0.10-win64.exe**. The application should not launch at this stage and throw errors, which means it is blocked by code integrity.

Verify Audit Logs	8. Right-click on the **Start** button and click **Run**. 9. Enter **eventvwr.msc** and click **OK**. 10. In the Event Viewer MMC, browse to **Event Viewer (Local) > Applications and Services Logs > Microsoft > Windows > CodeIntegrity > Operational**. 11. Browse through the log files especially **Event ID 3077**.

9.7.2.6 Configure Group Policies

In this activity, you will learn how to configure and deploy group policies to enforce the configuration.

Task	Detailed Steps
Complete these steps on the DC1 virtual machine.	
Download ADMX Files (If not downloaded before in the previous labs)	1. Download the latest Administrative Template files (ADMX/ADML) for Windows 11 [Create and manage Central Store - Windows Client | Microsoft Docs]
Install ADMX Files (If not installed before in the previous labs)	2. Install the downloaded administrative templates to a temporary location. 3. Copy **DeviceGuard.admx** from the temporary location (**.\PolicyDefinitions)** to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. **Note:** If the PolicyDefinitions folder doesn't exist you will have to create it. If prompted, replace the file in the destination directory. 4. Copy **DeviceGuard.adml** from the temporary location (**.\PolicyDefinitions\en-US)** to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions\en-US.** **Note:** If prompted, replace the file in the destination directory.

Create Device Guard GPO	5. Create a folder in the **C:** drive by the name **CodeIntegrity** and in this folder, copy the **SIPolicy.p7b** file created in the previous task from the **CLIENT1** VM. The path of this file in the **CLIENT1** VM is **C:\Windows\System32\CodeIntegrity**. 6. Navigate to **C:\CodeIntegrity**, right-click **CodeIntegrity** folder and click **Properties**. 7. Click the **Sharing** tab and click **Advanced Sharing…** 8. Check the box next to **Share this folder** and click **Permissions**. 9. Ensure **Everyone** is in the list and has been granted **Full Control**. Click **Apply** and click **OK** two times. 10. Click the **Security** tab and ensure that **Everyone** is in the list and has been granted **Full Control**. 11. Click the **Advanced** button and again ensure that **Everyone** is in the list and has been granted **Full Control**. Close all the windows. 12. Now navigate to **C:\CodeIntegrity\SIPolicy.p7b** that has been copied and right-click on the file and click **Properties**. 13. Click the **Security** tab and ensure that **Everyone** is in the list and has been granted **Full Control**. 14. Click the **Advanced** button and again ensure that **Everyone** is in the list and has been granted **Full Control**. Close all the windows. 15. Open **Active Directory Users and Computers**, create an OU called **WDAC** and move the **CLIENT2** VM to the **WDAC OU** from the default **Computers** container. 16. Open the **Group Policy Management Console**. 17. Right-click on **Group Policy Management > Forest: corp.contoso.com > Domains > corp.contoso.com > Group Policy Objects** and select **New**. 18. Under Name, enter **WDAC** and then click **OK**. 19. Right-click **WDAC OU**, click **Link an Existing GPO**… 20. Select **WDAC** and click **OK**.
Deploy Code Integrity Policy and Enable VBS for KCMI	21. Right-click **WDAC** and select **Edit**. 22. Browse to **Computer Configuration\Policies\Administrative Templates\System\Device Guard**. 23. Double-click on **Deploy Windows Defender Application Control**. 24. Select **Enabled**. 25. Under Code Integrity Policy file path, enter **\\DC1\CodeIntegrity\SIPolicy.p7b**. 26. Click **Apply** and then **OK**. 27. Double-click on **Turn On Virtualization Based Security**. 28. Select **Enabled**. 29. Under Select Platform Security Level, select **Secure Boot and DMA Protection**. 30. Under Virtualization based Protection of Code Integrity, select **Enabled without lock**. 31. Click **Apply** and then **OK**.

Attempt to Run New Applications that have not installed on the System	32. Now on the **CLIENT2** VM, run a **gpupdate /force**. 33. Restart **CLIENT2** and re-log in with the same credentials. 34. Verify that any new application installation or new executable is blocked by the Code Integrity Policy, Example: **CamStudio** or **VLC**. The CamStudio package is located at **\\DC1\C$\Packages\camstudio.exe** and the VLC package is located at **\\DC1\C$\Packages\vlc-3.x.xx-win64.exe**. **<u>Note:</u>** Before executing any labs after the Code Integrity Lab in which the **CLIENT1** and **CLIENT2** VMs are going to be used, ensure that they and any other machines have been moved to the default **Computers** container from the **WDAC OU**. Also ensure that there are no other Client VMs in that OU and have been moved to the default **Computers** container. Then in both the VMs, delete the **SIPolicy.p7b** file from **c:\Windows\System32\CodeIntegrity**. Run a **gpupdate /force** and reboot both the VMs. This is to ensure that no activity is blocked by Code Integrity.

9.8 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Defender for Endpoint uses the following combination of technology built into Windows 10 and Windows 11 and Microsoft's robust cloud service:

- **Endpoint behavioral sensors**: Embedded in Windows 10 and Windows 11, these sensors collect and process behavioral signals from the operating system (for example, process, registry, file, and network communications) and sends this sensor data to your private, isolated, cloud instance of Windows Defender ATP.
- **Cloud security analytics**: Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Microsoft 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- **Threat intelligence**: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

In this section, you will learn how to configure and use Microsoft Defender for Endpoint to detect and respond to threats.

<u>Note:</u> This lab can only be performed if the customer has already registered and approved for the Microsoft Defender for Endpoint Trial program (Section **Error! Reference source not found.**).

9.8.1 Onboarding Windows 11 Device

In this activity, you onboard your first Windows 11 client to Microsoft Defender for Endpoint.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Download the Onboarding Package	1. Log in to the device. 2. Navigate to https://security.microsoft.com 3. **Sign in** to the portal with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. On the **Welcome to Microsoft 365 Defender Intro** page, click **Next**. 5. On the **Next steps** page, click **Next**. 6. On the **Give feedback** page, click **Done**. 7. On the Set up preferences page, select the appropriate data storage location. 8. Select the appropriate data retention policy. 9. Select your appropriate organization size. 10. Keep the preview features on and then click **Next**. 11. Click **Continue** to create a cloud instance. It will start creating your Windows Defender ATP cloud instance. 12. On the **Onboarding** page, under **Deployment method** dropdown, select **Local Script (for up to 10 machines)** and click **Download onboarding package**. 13. Click **Save as** and **Save** the package to **C:\**. 14. Click **Start using Microsoft Defender ATP** and click **Proceed anyway**.
Execute the Onboarding Package	15. Navigate to **C:\**, right-click the package and click **Extract All…** 16. Click **Extract**. 17. Navigate to the extracted package, right-click on the script file and click **Edit**. **Note**: Note the registry paths we are writing to. Note the log and the Event ID we are creating in case of successful events using eventcreate. 18. Close notepad. 19. Right-click the script file and click **Run as administrator**. Press **Y** to confirm and continue. **Press any key to continue**. 20. After 5-10 minutes the machine will be onboarded. 21. In the **Microsoft Defender Security Center**, on the left navigation pane, click **Settings > Endpoints**. Scroll down and then under **Machine management**, click **Onboarding**. Scroll down and then under **Run a detection** test, copy the command snippet and run it in an elevated command prompt window. Once successful, the detection test will be marked as **Completed**.

Configure the Sample Collection Setting	22. Click the **Start** menu and type **regedit**, right-click and choose **Run as administrator**. 23. Locate the following registry path: **HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection**. 24. Create a **DWORD** value **AllowSampleCollection** and set it to **1**. **Note**: The machine will file sample collection through the portal for deeper investigation. No samples are collected automatically as this is done by the administrator.
Verify the Deployment Success	25. Check the SENSE service is running, by opening the Command Prompt and running: **sc query sense**. The **STATE** should be **4** and should be **RUNNING**. 26. Open the **Event Viewer (Local) > Windows Logs > Application** log and locate the **Event ID 20** from the source **WDATPOnboarding**. 27. Open the **Event Viewer (Local) > Application and Services Logs > Microsoft > Windows > SENSE > Operational** log. Check for the **Event ID 13** to make sure that the SENSE service has a normal operating process. Connection frequency may vary depending on factors like battery state. 28. Go to **https://security.microsoft.com** portal, under **Endpoints** choose **Device inventory**, on the right locate your machine on the list, its **Health State** should be **Active**.
Install Office (If Not Installed)	29. Go to **https://portal.office.com** and **Sign in** as **TU2@<AzureDomainName>.onmicrosoft.com** 30. Click **Install Office 365 > Office 365 apps**. 31. Click **Run**.

9.8.2 Perform Simulation

In this activity, you will go step-by-step through a typical attack sequence that you will run yourself.

Note: The setup guide also contains instructions and links for the attack demo.

Task	Detailed Steps
Complete these steps on the CLIENT1 virtual machine.	
Follow the Demo Attack Simulation Guidance	1. Click the link to download and open the **RS4_WinATP-Intro-Invoice.docm** word document from the setup guide or https://security.microsoft.com/tutorials **(Scenario 1 - Get simulation file)**. 2. Since the device has Microsoft 365 installed, therefore click **Yes** and **OK** on the Microsoft 365 security prompts if required. 3. Enter the password to open the word document and click **OK**. The password is provided in the setup guide. 4. Click **Enable Editing** and **Enable Content** on the opened word document. 5. Click **OK** on the prompt. 6. A Backdoor will run in a command window. **Press any key to close**. 7. You will now be able to see that an Active alert has been reported to the Windows Defender Advanced Threat Protection by the device. Navigate through the portal for further details on the attack and ways to remediate.