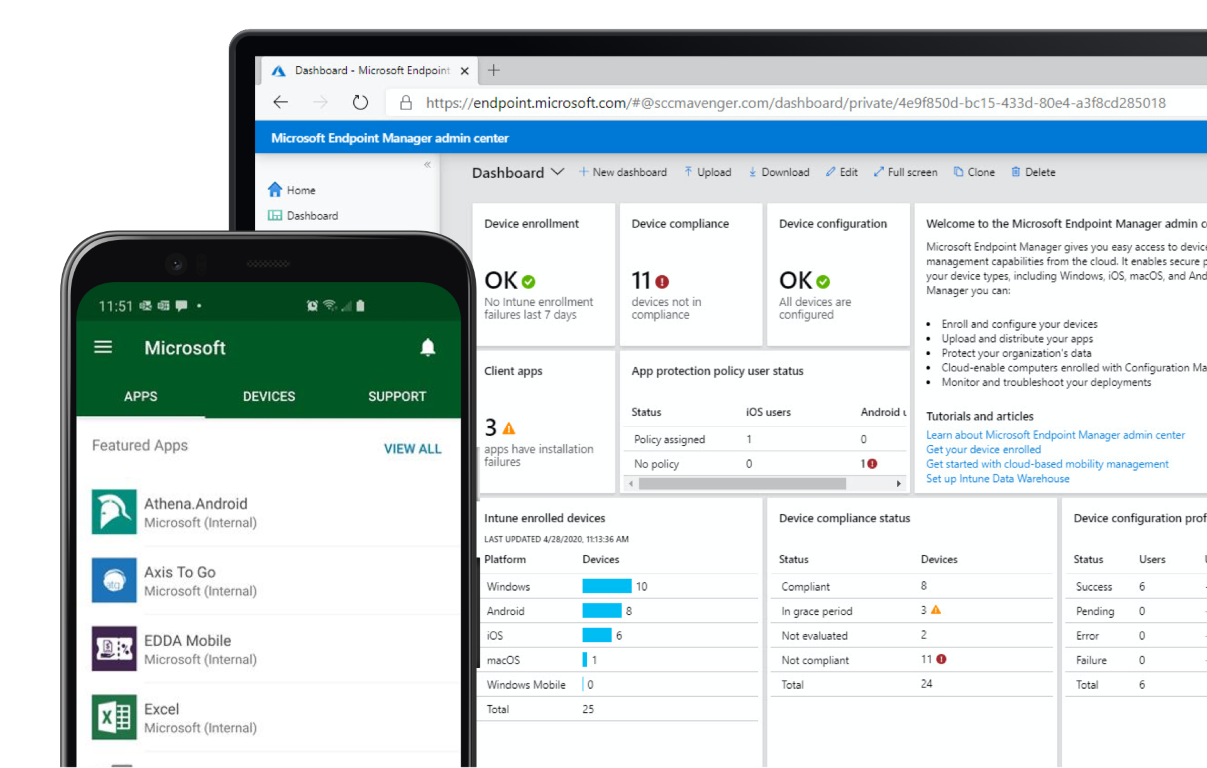
A picture containing drawing

Description automatically generated



Microsoft Endpoint Manager Evaluation Kit

Microsoft Intune | Microsoft Endpoint Configuration Manager

June 28, 2020

Table of Contents

[**1** **Introduction** 2](#_Toc44242936)

[**2** **Lab Setup** 4](#_Toc44242937)

[2.1 On-Premises Environment 4](#_Toc44242938)

[2.2 Cloud Environment 5](#_Toc44242939)

[2.3 On-Premises Environment Post Setup Manual Steps 10](#_Toc44242940)

[**3** **Directory and Network Readiness** 23](#_Toc44242947)

[3.1 Optimize Windows 10 23](#_Toc44242948)

[3.2 Cloud Management Gateway (CMG) & Cloud Distribution Point (CDP) 25](#_Toc44242949)

[3.3 CMPivot for real-time data in Configuration Manager 37](#_Toc44242950)

[3.4 Windows AutoPilot 37](#_Toc44242951)

[3.5 Tenant Attach, Co-Management and Switching Workloads 39](#_Toc44242952)

[3.6 Outlook Mobile App Config and App Protection 44](#_Toc44242953)

[**4 Shaping devices to corporate standards 47**](#_Toc44242954)

[4.1 User File and Settings Migration 47](#_Toc44242956)

[4.2 Security and Compliance 55](#_Toc44242957)

[4.3 Secure and Deploy Business Applications 99](#_Toc44242977)

[4.4 Office and Windows as a Service 136](#_Toc44242987)

1. Introduction

This lab provides guidance on deploying and managing Windows 10 and Microsoft 365 Apps for enterprise using Microsoft Endpoint Manager.

Microsoft Endpoint Manager is the convergence of Microsoft Intune and Microsoft Endpoint Configuration Manager functionality and data—plus new intelligent actions—offering seamless, end-to-end management solution without the complexity of a migration or disruption to productivity. Microsoft Endpoint Manager provides transformative cloud management and security that meets customers where they are and helps them move to the cloud at their own pace.

Services like Microsoft Intune help you manage your Windows 10 devices the same way as you do other mobile devices, all from one place. What makes Microsoft Intune innovative is the native integration with Configuration Manager to co-manage your Windows 10 devices. You can use Configuration Manager to help you in your shift to Windows 10, and then seamlessly add Microsoft Intune management. As a component of Microsoft Endpoint Manager, Configuration Manager becomes the intelligent edge within your organization, connected to the Microsoft 365 intelligent cloud.

This guide helps you understand and evaluate how on-premises management and cloud management come together in a powerful unified platform known as Microsoft Endpoint Manager.

This guide is divided into two sections:

**Directory and Network Readiness**

Cloud connected services in Microsoft 365 Apps for enterprise and new deployment options like Windows Autopilot require Azure Active Directory. Your network and connectivity are also important areas to plan when moving Windows images, apps, drivers and related files to your PCs. Learn how new tools and deployment options reduce and streamline network traffic.

**Related Resources:**

[Intune network configuration requirements and bandwidth](https://docs.microsoft.com/en-us/mem/intune/fundamentals/network-bandwidth-use)

[What is Azure AD Connect?](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect)

**Shaping devices to corporate standards.**

Once you have established your network connections, you can now begin customizing the end-user experience so that devices are ready with minimal set-up required by the end user. This includes:

* **Office and Line of Business App Delivery.** While Windows continues to support MSI-based installations it also now supports newer installations mechanisms, optimized for automated deployment and continuous updates. Microsoft 365 Apps for enterprise and Office 2019 clients use Click-to-Run installation technology. You may want to make a range of UWP apps available, and you may increasingly find yourself deploying third-party apps and in-house developed Line of Business Apps that use the new MSIX-based packaging apps. This step ensures your apps are ready for automated deployments, and that you are set up for success whether your apps deploy using Click-to-Run, MSIX, conventional MSI-based, or are UWP apps deployed from a Microsoft Store from Business you set up.
* **User Files and Settings Migration.** This is a critical step in any PC replacement or refresh cycle: you have to ensure users’ files, data, and settings move successfully and are preserved over the migration. This step covers the options available for manual or automated migrations, including well-known and new options. As in previous upgrades, the User State Migration Tool continues to be a valuable tool to automate this process and it remains an integral part of migrations orchestrated using Configuration Manager or the Microsoft Deployment Toolkit. But moving all this data at migration can be a timing bottleneck for PC replacement due to the physics involved in transferring sometimes hundreds of gigabytes per PC twice – first from the existing desktop, then back down to the new desktop. A new option enabled by OneDrive is Known Folder Move used to sync user documents, pictures, and desktop files at scale, in the cloud, and ahead of deployment.
* **Security and Compliance**. Security and Compliance is an area with a lot upside when moving to Windows 10 and Microsoft 365 Apps for enterprise. It is important you familiarize yourself with the new built-in capabilities and compare that with what you already have. For example, new capabilities in Windows 10 using virtualization-based security can prevent credential theft, protect against browser-based exploits and malicious code execution by isolating core processes and secrets from the operating system. In addition, cloud services like Advanced Threat Protection give you a unified platform for security hardening, post-breach detection, investigation, and response. Advanced Threat Protection can also safeguard you against malicious email attachments, unsafe hyperlinks and more.
* **Windows and Office as a Service.** This represents a major shift in the way you maintain users’ desktop real estate. With this move to Windows 10 and Microsoft 365 Apps for enterprise you can move to managing Windows and Office as a service. In place of a massive shift in technology every few years, you will continually be bringing new capabilities, experiences, and protections to your user. Semi-annual feature updates deliver new capabilities in the Fall and Spring of each year, while monthly cumulative Quality Updates will contain security, reliability, and bug fixes. While you can opt to deploy the Office 2019 client, we strongly recommend moving to Microsoft 365 Apps for enterprise. This follows a similar service plan to Windows so your users get updates to the Office apps on a regular basis too.

**Resources:**

[Using security baselines in your organization](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines)

[Endpoint protection](https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/endpoint-protection)

[Manage endpoint security in Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security)

[Understanding ADMX-backed policies](https://docs.microsoft.com/en-us/windows/client-management/mdm/understanding-admx-backed-policies)

1. Lab Setup

It is important that this section and subsections be performed before proceeding with the lab activities. The following requirements for each environment are needed 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.

* 1. On-Premises Environment

The on-premises environment is configured by using the Windows and Office Deployment Lab Kit, which can be accessed in the [Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-365-modern-desktop-lab-kit) here. Follow the Windows and Office Deployment Lab Kit **Setup Guide** to provision the virtual machines on Hyper-V.

[**Download Lab Environment**](https://www.microsoft.com/en-us/evalcenter/evaluate-lab-kit/)

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

|  |  |
| --- | --- |
| Complete | Task |
|  | One (1) **physical** server or workstation to host the virtual lab environment. The requirements are listed below:   * **Operating System**: Windows Server 2016, 2012 R2, or Windows 10 with Hyper-V installed (recommended to use Windows Server OS) and fully updated. Administrative rights on the host. * **Memory**: Up to 32 GB. * **Disk Space**: At least 300 GB or more. * **Disk Subsystem**: High throughput/speed. * **Ethernet**: Two (2) or more Gb NICs. * **Network Connections**: Internet connection and lab switch. |
|  | One (1) gigabit network lab **switch** with sufficient ports to connect client devices and lab environment. |

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

|  |  |  |
| --- | --- | --- |
| Server Name | Roles & Products | Not Used for this lab |
| HYD-DC1 | Active Directory Domain Controller, DNS, DHCP, Certificate Services |  |
| HYD-MDT1 | Microsoft Deployment Toolkit  Windows 10 2004 ADK  Windows Deployment Services | x |
| HYD-CM1 | Microsoft Endpoint Configuration Manager 2002  Windows Deployment Services  Microsoft Deployment Toolkit  Windows 10 2004 ADK x  Windows Software Update Services  Microsoft SQL Server 2017 |  |
| HYD-APP1 | Microsoft BitLocker Administration and Monitoring  Microsoft SQL Server 2017 |  |
| HYD-GW1 | Remote Access for Internet Connectivity |  |
| HYD-INET1 | Simulated Internet |  |
| HYD-VPN1 | Remote Access for VPN |  |
| HYD-CLIENT1 | Windows 10 2004 Domain Joined |  |
| HYD-CLIENT2 | Windows 10 2004 Domain Joined |  |
| HYD-CLIENT3 | Windows 10 2004 Workgroup |  |
| HYD-CLIENT4 | Windows 10 2004 Workgroup |  |
| HYD-CLIENT 5, 6 | Bare metal (No Installations) |  |
| HYD-CLIENT7 | Windows 7 SP1 Domain Joined x |  |

The table below lists the credentials and access type available in the default implementation:

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

* 1. 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**: It is possible to use an existing trial subscription if the engagement dates are within the evaluation period.  **Note**: An appropriate MSDN subscription could be used to activate the Azure Benefit for 30 days. |

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**   1. Click **Create**.   **Note**: This may take a couple of minutes to complete. |
| Create Azure AD Admin User | 1. Sign out from Azure portal and sign back in again. 2. 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. 3. On the left navigation bar, click **Azure Active Directory**. 4. Click **Users** and then click **+ New user**. 5. 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   1. Select **Auto-generate password** and select **Show Password** and write down the temporary password **<OldLabAdminPassword>**. 2. 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.   1. Click **Create**. |
| Resetting the Password | 1. Logout from Azure Portal. 2. Log in to Azure Portal using **LabAdmin** account. 3. Type in the **<OldLabAdminPassword>** that you wrote down. 4. Type the new password: **<NewLabAdminPassword>**. 5. 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.   1. Click **All services > Subscriptions**. 2. Click **Add** to add a new subscription to the new Azure AD Tenant. 3. If you are eligible for a Free Trial, then click **Free Trial** or select any other offer from the list. 4. Follow the instructions for **Azure – Sign up**. 5. 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 | 1. Open a new tab and navigate to <https://portal.office.com>. 2. Click the **Admin** tile. 3. Click **Billing | Purchase services**. 4. Search for and select **Microsoft 365 E3** and then click **Get free trial**. 5. 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 | 1. Navigate to <https://portal.azure.com>. 2. Sign in with the email address associated with your Azure subscription if required. 3. On the left navigation bar, click **Azure Active Directory**. 4. Click **Users** and then click **+ New user**. 5. 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   1. Select **Auto-generate password** and select **Show Password** and write down the temporary password. 2. Click **Create**. 3. 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 | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://login.microsoftonline.com>. 4. Log in with the user account created **TU1@<AzureDomainName>.onmicrosoft.com** 5. Type in the **temporary password** that you wrote down. 6. Type the New Password: **<newuserpassword>** 7. Confirm the new Password: **<newuserpassword>** 8. Click **Sign in**. 9. Repeat **Steps 38-45** for **TU2@<AzureDomainName>.onmicrosoft.com** 10. Close all browser windows. |
| Create Azure AD Group (Sales) | 1. Open an InPrivate Browser session. 2. Navigate to <https://portal.azure.com> 3. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 5. Click **+ New group**. 6. 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**   1. Click **Create**. |

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 Internet Explorer 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**. |

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 Internet Explorer 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 | 1. Close all browser windows. 2. Open an **InPrivate Browser** session. 3. Navigate to <https://portal.azure.com>. 4. Sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com**. 5. On the left navigation bar, click **Azure Active Directory > Devices > Device settings**. 6. In the **Users may join devices to Azure AD** setting, select **All** if not selected. 7. In the **Users may register their devices with Azure AD** setting, select **All**. 8. 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>   1. Close all browser windows. 2. Open an InPrivate Browser session. 3. Navigate to <https://www.microsoft.com/en-us/windowsforbusiness/windows-atp> and click **Start free trial**. 4. Check the box next to **I accept these terms and conditions** and click **Next**. 5. On the Please enter your details below page, enter your details and click **Submit**. 6. You will get a message stating that the Windows Defender Advanced Threat Protection Team will review your application and contact you via email within 7 business days. Once your application is approved, you will then receive an invitation email with onboarding instructions. 7. Within 7 business days, you will then receive an email to activate your trial and all the onboarding instructions. Click **Activate your trial now**. Download the **setup guide**. The setup guide also contains instructions and links for the attack demo. 8. During activation, click **Sign in**. 9. **Sign in** with **LabAdmin@<AzureDomainName>.onmicrosoft.com** 10. Click **Try now**. 11. Click **Continue**. 12. Close all browser windows. |

* 1. On-Premises Environment Post Setup Manual Steps

Perform once the on-premises environment provisioning is complete.

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 traditional 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.

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.



#### 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 2.3.1.2).

| 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 **Online, persistent connection (recommended)** then click **Next**. 9. In the **Summary** page, click **Next**. 10. In the **Completion** page, click **Close**. |
| Install New Updates (if available) | **Note**: Perform the succeeding steps if there is a newer Configuration Manager build available after 2002. Otherwise, proceed to **2.3.2**.  **Note**: 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**.   **Note:** It will first download the update before it is made Available. If already not downloaded, then select **Configuration Manager 200x** and then click **Download**. Click **OK**.   1. In the **Updates and Servicing** pane, select an **Available** update (**Configuration Manager 200x**) and then click **Install Update Pack**. 2. In the **General** page, select **Ignore any prerequisite check warnings and install this update regardless of missing requirements** and click **Next**. 3. In the **Features** page, select **all** available features then click **Next**. 4. In the **Client Update Options** page, click **Next**. 5. In the **License Terms** page, select **I accept these License Terms** **and Privacy Statement** and click **Next**. 6. In the **Summary** page, click **Next**. 7. In the **Completion** page, click **Close**.   **Note**: The 200x upgrade installation may take up to an hour. |
| Upgrade the Configuration Manager Console and Validate Version Number | 1. In the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. 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 200x**) available.   1. In the **Updates and Servicing** pane, confirm that the update (**Configuration Manager 200x**) is Installed.   **Note:** Install any available hotfixes pertaining to (**Configuration Manager 200x**).   1. After the upgrade, in the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. Validate that the **Version** or **Build Number** was updated (for Configuration Manager 200x). 4. Reboot **CM1** once. |

#### 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 | 1. 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:\**. 2. From the **Start** button, open an **Administrative Command Prompt** and enter **cd /d C:\ServiceConnectionTool**. 3. **Execute** the following command:   **serviceconnectiontool.exe -prepare -usagedatadest .\UsageData.cab** |
| Upload Usage Data and Download Updates from an Internet-connected Remote Computer | 1. **Copy** the folder **C:\ServiceConnectionTool** from **CM1** to the root drive of the computer that has **internet connection**. 2. From the computer that has internet connection, open an **Administrative Command Prompt** and browse to the copied **ServiceConnectionTool** folder. 3. **Execute** the following command:   **md .\UpdatePacks**   1. **Execute** the following command:   **Serviceconnectiontool.exe -connect -usagedatasrc .\UsageData.cab updatepackdest .\UpdatePacks** |
| Import Updates | 1. From the computer that has **internet connection**, copy the **UpdatePacks** folder to **CM1** in the folder **C:\ServiceConnectionTool**. 2. From the **Start** button, open an **Administrative Command Prompt** and enter **cd /d C:\ServiceConnectionTool**. 3. **Execute** the following command:   **serviceconnectiontool.exe -import -updatepacksrc .\UpdatePacks** |
| Force Refresh | 1. In the **Configuration Manager Console**, browse to **Monitoring > System Status >** **Component Status**. 2. In the ribbon, select **Start >** **Configuration Manager Service Manager**. 3. In the **Configuration Manager Service Manager** window, expand **CHQ > Components >** **SMS\_EXECUTIVE**. 4. On the right pane, **right-click** on **SMS\_EXECUTIVE** and select **Stop**. 5. Right-click on **SMS\_EXECUTIVE** and select **Query**. 6. 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 **2.3.2**.   1. In the **Configuration Manager Console**, browse to **Administration > Updates and Servicing**. 2. In the **Updates and Servicing** pane, select the **Configuration Manager 200x** update and then click **Install Update Pack**. 3. In the **General** page, 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 **Summary** page, click **Next**. 8. In the **Completion** page, click **Close**.   **Note**: The 200x upgrade installation may take up to an hour. |
| Upgrade the Configuration Manager Console and Validate Version Number | 1. In the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. 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 200x**) available.   1. In the **Updates and Servicing** pane, confirm that the update (**Configuration Manager 200x**) is Installed.   **Note:** Install any available hotfixes pertaining to (**Configuration Manager 200x**).   1. In the **Configuration Manager Console**, browse to **Administration > Site Configuration >** **Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Properties**. 3. Validate that the **Version** or **Build Number** was updated (for Configuration Manager 200x). 4. Reboot **CM1** once. |

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 | 1. Navigate to **Administration > Hierarchy Configuration >** **Boundaries**. 2. Ensure that the **Default-First-Site-Name** boundary is already created. 3. Navigate to **Administration > Hierarchy Configuration >** **Boundary Groups**. 4. Ensure that the **Corp Boundary Group** is already created. |
| Configure an IP Based Boundary | 1. First, in **DC1**, click **Start > Windows Administrative Tools > Active Directory Sites and Services**. 2. Expand **Sites**, right-click **Subnets** and then click **New Subnet**. 3. In the **Prefix** field, enter **10.0.0.0/24**, select **Default-First-Site-Name** and then click **OK**. 4. Back in **CM1**, navigate to **Administration > Hierarchy Configuration >** **Boundaries**. 5. Right-click **Boundaries** and click **Create Boundary**. 6. 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**. 7. Click the **Boundary Groups** tab and click **Add**. 8. Select **Corp Boundary Group** and click **OK**. 9. Click **Apply** and click **OK**. |
| Configure Boundary Group and DP Group for the DP | 1. Navigate to **Administration | Distribution Points**. 2. Right-click the distribution point and click **Properties**. 3. Click the **Group Relationships** tab and click **Add**. 4. Select **Corp DPs** and click **OK**. 5. Click the **Boundary Groups** tab. 6. Click **Add**. 7. Select **Corp Boundary Group** and click **OK**. 8. Click **Apply** and click **OK**. |
| Configure and Validate the Network Access Account | 1. Navigate to **Administration > Site Configuration >** **Sites**, select the site and click **Settings > Configure Site Components >** **Software Distribution**. 2. 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. 3. Click **Yes** on the prompt. 4. Click the **star** and click **New Account**. 5. 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. 6. Click **Apply** and then click **OK**. |
| Configure and Validate the Client Push Installation | 1. Navigate to **Administration > Site Configuration >** **Sites**. 2. Right-click on the **CHQ** site then select **Client Installation Settings >** **Client Push Installation**. 3. 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. 4. In the **Accounts** tab, Click the **star** button and click **Existing Account**. 5. In the **Select Account** window, select **corp\labadmin** then click **OK.** 6. Review the **Installation Properties** tab. Click **Apply** and then click **OK**. |

Create Test VMs

#### Download MSDN & EVAL ISOs

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the HYPER-V Host.** | |
| Download Windows 10 1909 ISO (MSDN) | 1. Open Internet Explorer and browse to the URL below.   <https://msdn.microsoft.com/subscriptions/securedownloads/>   1. From the website, Sign-in with your MSDN registered account. 2. On the **Search** field, enter **Windows 10**. 3. **Search** for **Windows 10 (business editions), Version 1909 (*Latest Available Update*) (x64) – DVD (English)** and **Download** to C:\. |
| Download Windows 10 2004 ISO (EVAL) | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-in/evalcenter/evaluate-windows-10-enterprise>   1. Select **ISO – Enterprise** and click **Continue**. 2. Fill in all the fields to complete the form and click **Continue** again. 3. Select **64 bit**, select your language and click **Download**. |

#### Build a Windows 10 1909 Client Machine

In the activity, you will build Windows 10 1909 client virtual machine.

**Note:** The **WIN10-1909** VM, will be used for the following scenarios in this Lab Guide:

* Section 4.4.2 - Servicing Windows 10 with Configuration Manager

| 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. **WIN10-1909**). 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 **2048 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 ISO image as stated in **Steps 1-4** of **Section 2.3.3.1**. 10. On the **Summary** page, review and click **Finish**. 11. 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**). 12. 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 | 1. Once the system has joined the domain, log on to **CM1** virtual machine. 2. Launch the Configuration Manager Console and navigate to **Administration > Hierarchy Configuration >Discovery Methods**. 3. Select **Active Directory System Discovery** and click **Run Full Discovery Now**. Click **Yes** on the prompt. 4. Navigate to **Assets and Compliance >** **Devices** and check if **WIN10-1909** is showing in the list of devices. 5. Right-click on **WIN10-1909** and click on **Install Client** (hold Ctrl and select multiple computers if you want to install on more than one computer). 6. On the Install Configuration Manager Client wizard click on **Next**. 7. Check the box next to **Install the client software from a specified site**, select the Site **CHQ-Contoso Headquarters** and click on **Next**. 8. Click **Next** again. 9. Click on **Close**. 10. After a few minutes, the **WIN10-1909** 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 WIN10-1909 virtual machine.** | |
| Create Checkpoint | 1. Create a virtual machine **checkpoint**. |



#### Build a Windows 10 2004 Client Machine

In the activity, you will build Windows 10 2004 client virtual machine.

**Note:** The **WIN10-2004** VM, will be used for the following scenarios in this Lab Guide:

* Appendix - Desktop Analytics

| 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. **WIN10-2004**). 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 **2048 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 ISO image as stated in **Steps 5-8** of **Section 2.3.3.1**. 10. On the **Summary** page, review and click **Finish**. 11. 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**). 12. 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**. 13. Install the **latest Compatibility/Cumulative Updates**. You must reboot the VM multiple times and check for any remaining updates to be installed until no further updates are required. This step is important for the **Desktop Analytics scenario**. Click **Start > Settings > Update & Security > Check for updates**. |
| **Complete these steps on the CM1 virtual machine.** | |
| Install the Configuration Manager Client | 1. Log on to **CM1** virtual machine. 2. Launch the Configuration Manager Console and navigate to **Administration > Hierarchy Configuration >Discovery Methods**. 3. Select **Active Directory System Discovery** and click **Run Full Discovery Now**. Click **Yes** on the prompt. 4. Navigate to **Assets and Compliance >** **Devices** and check if **WIN10-2004** is showing in the list of devices. 5. Right-click on **WIN10-2004** and click on **Install Client** (hold Ctrl and select multiple computers if you want to install on more than one computer). 6. On the Install Configuration Manager Client wizard click on **Next**. 7. Check the box next to **Install the client software from a specified site**, select the Site **CHQ-Contoso Headquarters** and click on **Next**. 8. Click **Next** again. 9. Click on **Close**. 10. After a few minutes, the **WIN10-2004** 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 WIN10-2004 virtual machine.** | |
| Create Checkpoint | 1. Create a virtual machine **checkpoint**.   **Note:** Repeat **Steps 14-23** above to install the Configuration Manager Client on **HYD-CLIENT1**, **HYD-CLIENT2** and **HYD-CLIENT7**. 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-CLIENT1-7**. Refer to **Step 12** above.  **Note:** For the **Desktop Analytics scenario**, the **Windows Defender Firewall Mode** must be turned off for **Domain networks, Private networks and Guest or public Networks** in the following VMs in the lab - **DC1, CM1, GW1, Windows 10 2004 VM and your Hyper-V Host**. This is to ensure that there are no blocks in the data flow from the lab to Azure. Refer to **Step 12** above. |

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**. 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**. 3. Download **Azure AD Connect** from <https://www.microsoft.com/en-us/download/details.aspx?id=47594> 4. Run **Azure AD Connect** and select **I agree to the license terms and privacy notice** and click **Continue**. Accept the UAC prompt. 5. Select **Use express settings**. 6. In the **Connect to Azure AD** prompt, sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 7. In the **Connect to AD DS** prompt enter the following and click **Next**. USERNAME: **CORP\LabAdmin** PASSWORD: **P@ssw0rd** 8. 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**. 9. 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 done. |
| **Configure Device Sync** | 1. Open **Programs and Features** and uninstall the **Windows Azure Active Directory Module for Windows PowerShell**. Accept the UAC prompt. 2. Open PowerShell as an administrator. Accept the UAC prompt. 3. Run the below cmdlet and accept any prompts. **Note:** Create a directory in **C:\**, example **C:\MSOnline**. Save-Script -Name MSOnline -Path C:\MSOnline\ 4. Run the below cmdlet and accept any prompts. Install-Module -Name MSOnline 5. Locate the name of the **AAD Connector Account** by opening the **Azure AD Connect** and clicking **Configure** and selecting **View current configuration** and then clicking **Next**. Click **Exit**. 6. Run the below cmdlet and at the credential prompt, provide the Azure AD Admin credentials. Import-Module -Name “C:\Program Files\Microsoft Azure Active Directory Connect\ADPrep\ADSyncPrep.psm1”   $aadadmincred = get-credential;  Initialize-ADSyncDomainJoinedComputerSync -AdConnectorAccount <account name> -AzureADCredentials $aadAdminCred; |
| **Confirm Devices are Hybrid Azure AD Joined** | 1. Start Internet Explorer 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**. 4. Select **Devices** > **All devices**. 5. 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:   1. Disable the firewall mode in **DC1** if not done already. 2. Open **Azure AD Connect** and click **Configure**. 3. Select **Configure device options** and click **Next**. 4. Click **Next** again. 5. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 6. Select **Configure Hybrid Azure AD join** and click **Next**. 7. Select **Windows 10 or later domain-joined devices** and click **Next**. 8. Check the box next to **corp.contoso.com** and click **Add**. 9. Sign in with **CORP\LabAdmin** and **P@ssw0rd** and click **OK**. 10. Click **Next**. 11. Click **Configure**. 12. Click **Exit** once done. 13. Open **Azure AD Connect** and click **Configure**. 14. Select **Customize synchronization options** and click **Next**. 15. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 16. Click **Next** again. 17. Click **Next** again. 18. Ensure that **Password hash synchronization** is selected. Also select **Password writeback** and click **Next**. 19. Ensure that **Start the synchronization process when configuration completes** is selected and click **Configure**. Click **Exit** once done. 20. Open **Azure AD Connect** and click **Configure**. 21. Select **Change user sign-in** and click **Next**. 22. Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** and click **Next**. 23. Select **Pass-through authentication** and ensure that **Enable single sign-on** is selected and then click **Next**. 24. Click **Enter credentials** and enter **CORP\LabAdmin** and **P@ssw0rd**. Click **OK**. Click **Next**. 25. Ensure that **Start the synchronization process when configuration completes** is selected and click **Configure**. Click **Exit** once done. 26. 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 10 Enterprise Version 2004 VM** as **labadmin@<AzureDomainName>.onmicrosoft.com** with the password **P@ssw0rd**.  Once the device is Hybrid Azure AD Joined, it would look like this in the Azure Portal:    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>:      **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. |

1. Directory and Network Readiness
   1. Optimize Windows 10

When considering your content distribution strategy for Windows 10, think about enabling a form of peer-to-peer content sharing to reduce bandwidth issues during updates. Windows 10 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 10. Two methods of peer-to-peer content distribution are available in Windows 10.

* [Delivery Optimization](https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization) is a new peer-to-peer distribution method in Windows 10. Windows 10 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](https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache) is a bandwidth optimization technology that is included in some editions of Windows Server 2016 and Windows 10 operating systems, as well as in some editions of Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, and Windows 7.

**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.](https://docs.microsoft.com/sccm/core/plan-design/hierarchy/client-peer-cache)

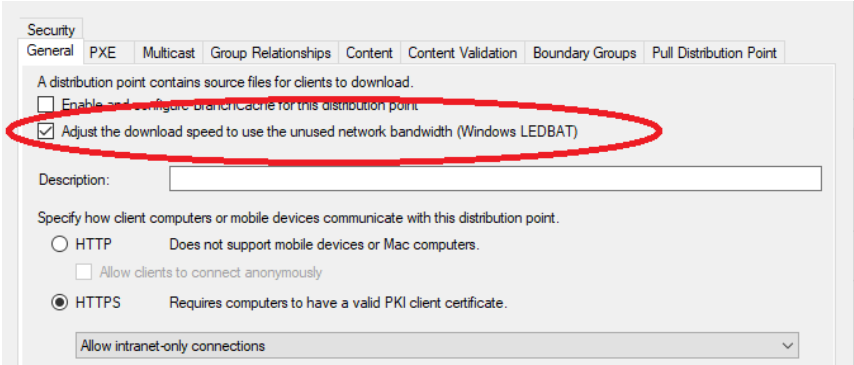
| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps on the DC1 virtual machine.** | | | |
| Configure Delivery Optimization | | 1. Go to **Server Manager>Tools>Active Directory Users and Computers** and right-click **CORP**, then click **New>Organizational Unit**. 2. Create an Organizational Unit, example “**Known Folder**” under **CORP** and add/move the **CLIENT7** 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 configureDelivery Optimization settings. 7. For info, see [**Configure Delivery Optimization for Windows 10 updates**](https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization). | |
| Enable Branch Cache on Client Computers | 1. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 2. 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 “**Branch Cache**” and click **OK**. 3. Right-click the new GPO, example “**Branch Cache**” and click **Edit**. 4. Go to **Computer Configuration\Policies\Administrative Templates\Network**\**BranchCache to configure BranchCache settings.** 5. For info, see [**Branch Cache Client Configuration**](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/dd637820(v=ws.10)). | |

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.

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. 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:

[](https://msdnshared.blob.core.windows.net/media/2018/07/SCCM-LEDBAT.png)

For more information see:

* [Top 10 Networking Features in Windows Server 2019: #9 LEDBAT – Latency Optimized Background Transport](https://blogs.technet.microsoft.com/networking/2018/07/25/ledbat/)
* [Enable distribution points to use network congestion control](https://docs.microsoft.com/en-us/sccm/core/get-started/capabilities-in-technical-preview-1805#enable-distribution-points-to-use-network-congestion-control)
  1. Cloud Management Gateway (CMG) & Cloud Distribution Point (CDP)

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.

A Cloud Distribution Point (CDP) is a Configuration Manager distribution point that is hosted as Platform-as-a-Service (PaaS) in Microsoft Azure. 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 traditional distribution points.

This section provides the steps to install and configure the Cloud Management Gateway (CMG) along with the Cloud Distribution Point (CDP).

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

**Note:** The **Microsoft.ClassicCompute** and **Microsoft.Storage** resource providers must be registered within the Azure subscription. To verify that in the Azure portal, click **All services | search for and click Subscriptions | click the subscription | Resource providers**. If not registered, click **Register** for **Microsoft.ClassicCompute** and **Microsoft.Storage**.

**Note:** For more information, refer to <https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/setup-cloud-management-gateway>

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. |

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. |

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 3.2.1**, in an FQDN format ending with **cloudapp.net**. 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**. |

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. |

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. |

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 Certificate using Group Policy | 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**. 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. |

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. |

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. |

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 **HomePage URL**, specify a URL. By default, this value is **https://ConfigMgrService**. 9. For the **App ID URI**, specify a unique URL. By default, this value is **https://ConfigMgrService**. 10. For the **Secret key validity period**, select either **1 Year** or **2 Years**. By default, this value is **1 Year**. 11. 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. 12. On the Create Server Application window, click **OK**. 13. On the Server App window, select/highlight the app and click **OK**. 14. Back on the App page, click **Browse** next to **Native Client app**. 15. On the Client App window, click **Create**. 16. On the Create Client Application window, provide a friendly name for the app next to **Application Name**. 17. 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. 18. On the Create Client Application window, click **OK**. 19. On the Client App window, select/highlight the app and click **OK**. 20. Back on the App page, click **Next**. 21. 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. 22. On the Discovery page, click **Next**. 23. On the Summary page, review and click **Next**. 24. On the Completion page, click **Close**. |

Set up the CMG along with CDP

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 along with CDP | 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**. 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. 9. Next to **Resource Group**, select **Create new** and specify 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 CDP will be visible from **Administration | Distribution Points**. |

Configure Boundary Group and Distribution Point Group for CDP

This section provides the steps to add the CDP 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 CDP 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 CDP and click **OK** and then click **OK** again. |

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 Certificate Authentication | 1. In the ConfigMgr Console, browse to **Administration | Overview | Site Configuration | Sites**. 2. Right-click the primary site and click **Properties**. 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**. |

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. |

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. |

Configure the Configuration Manager Client Settings for CMG and CDP

This section provides the steps required to configure the ConfigMgr Client Settings for CMG and CDP.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure the Configuration Manager Client Settings for CMG and CDP | 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**. |

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 CDP 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. |

* 1. CMPivot for real-time data in Configuration Manager

Configuration Manager has always provided a large centralized store of device data, which customers use for reporting purposes. The site typically collects this data on a weekly basis. CMPivot is a new in-console utility that now provides access to real-time state of devices in your environment. It immediately runs a query on all currently connected devices in the target collection and returns the results. Then filter and group this data in the tool. By providing real-time data from online clients, you can more quickly answer business questions, troubleshoot issues, and respond to security incidents.

**Note:** Before performing the below steps, ensure that the required client machines (at least **CLIENT1** and **CLIENT2**) in the lab are installed with the latest Configuration Manager client and are turned **ON** and are showing **Active** in **Assets and Compliance > Devices**.

For more information, refer to <https://docs.microsoft.com/en-us/mem/configmgr/core/servers/manage/cmpivot>

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Run CMPivot | 1. In the Configuration Manager Console, navigate to **Assets and Compliance > Device Collections**. 2. Right-click **All Systems** device collection and click **Start CMPivot**. 3. In the **CMPivot (All Systems)** window, click the **Query** tab. 4. Type **OS | summarize dcount( Device ) by Caption** in the query pane and click **Run Query**. 5. Observe the results in the results pane. |

* 1. 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.

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 | 1. Login as the local administrator and 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   1. Change the directory to **C:\Program Files\WindowsPowerShell\Scripts** and run the below command.   **Note:** Ensure that **Windows Remote Management (WS-Management)** service is running on the machine for the script to be executed successfully. .\Get-WindowsAutoPilotInfo.ps1 -ComputerName CLIENT4 –OutputFile C:\Users\Administrator\Desktop\MyComputers.csv   1. Copy the MyComputers.csv file to the computer that will be used for Microsoft Intune setup. 2. Open Command Prompt as an administrator. Accept the UAC prompt if required. 3. Run the following command after changing the directory to **C:\Windows\System32\Sysprep** SYSPREP\Sysprep.exe /OOBE /SHUTDOWN |

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. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to [https://www.portal.azure.com/](https://www.portal.azure.com/en-us/business-store) and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Click **Device enrollment** > **Windows enrollment** > **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 **Microsoft Intune** 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 **Device enrollment** > **Windows enrollment** pane, click **Deployment Profiles** > **+ Create profile**. 13. On the **Basics** tab, in the **Name** box, type **AutoPilot Test Profile** and click **Next**. 14. On the **Out-of-box experience (OOBE)** tab, in the **Deployment mode** dropdown, select **User-Driven**. 15. In the **Join to Azure AD as** dropdown, select **Azure AD joined**. 16. Select **Hide** for the **Microsoft Software License Terms** option. 17. Select **Hide** for the **Privacy Settings** option. 18. Select **Hide** for the **Hide change account options** option. 19. Select **Standard** for the **User account type** option and click **Next**. 20. In the **Assignments** tab, click **+ Select groups to include**, select the **AutoPilot Devices** group just created and click **Select** and then click **Next**. 21. In the **Review + create** tab, click **Create.** 22. Wait for some time for the device to be showing up in **Assigned devices** under **AutoPilot Test Profile**. To speed up the process, click **Sync** and then click **Refresh** in the **Device enrollment** > **Windows enrollment** > **Devices** pane, until you see the device there. 23. Click the **Devices** page, and you should be able to see the **PROFILE STATUS** as **Updating** and then further **Assigned**. Wait for a few moments. 24. Select the device imported and click **Assign user**. 25. 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. |

* 1. Tenant Attach, Co-Management and Switching Workloads

Co-management in Microsoft Endpoint Manager enables you to manage Windows 10 devices using both Configuration Manager and Intune concurrently. It’s an innovative solution that accelerates your modern management strategy, giving you a flexible path to choose the balance of on-premises Method and cloud management that works best for your organization.

After you enable co-management, Configuration Manager continues to manage all workloads. But now you have visibility into all your devices, on-premises as well as cloud managed, in the Microsoft Endpoint Manager administration console. You may take certain remote actions from the cloud on these on-premises managed clients.

When you decide that you are ready, you can have Intune start managing one or more workloads. If for any reason you wish to revert back to Configuration Manager for those workloads, that is an easy switch. You can have Intune manage the following workloads: Compliance policies, Windows Update for Business policies, Resource Access policies, Endpoint Protection and many more.

**Resources:**

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>

Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on an Internet-connected Windows computer.** | |
| Enable Device Management. Set Mobile Device Management Authority (If MDM Authority is not equal to Intune) | **Note**: Before you can enroll mobile devices, you must prepare the Intune service by selecting the appropriate mobile device management authority setting on the Mobile Device Management page of the Administration workspace. The mobile device management authority setting determines whether you manage mobile devices with Intune or Configuration Manager with Intune integration. This guidance assumes Intune is used without Configuration Manager integration so the setting should be set to Microsoft Intune.   1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 4. On the left navigation bar, click **All services > search for and click Intune > Intune**. 5. Select **Device enrollment**. 6. Under Mobile Device Management Authority, select **Intune MDM Authority** and click **Choose**. |
| Configure Auto MDM Enrollment for Intune | 1. Close all browser windows. 2. Start Internet Explorer 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**. |

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.   1. *Summary* – click **Next**, click **Close**. |
| Add a Device to the Collection | 1. In the **Assets & Compliance** workspace, select **Devices** and right-click **CLIENT1**. 2. Select **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 3. Select **Co-managed Devices** and click **OK**. 4. Select **Device Collections**, right-click **Co-managed Devices**, and select **Update Membership**. Click **Yes** on the warning box to continue. |
| Tenant Attach, Co-Management & Switch Workloads | 1. Open the **Configuration Manager Console**, browse to **Administration > Cloud Services > Co-management**. 2. Click **Configure co-management** from the ribbon bar. 3. In the **Co-management Configuration Wizard, Sign In** to Intune using **labadmin@<AzureDomainName>.onmicrosoft.com.** Click **Next** and accept the prompt. 4. On the **Configure upload** page, accept the defaults and click **Next**. 5. On the **Enablement** page, drop-down and select **Pilot** next to **Automatic enrollment in Intune** and then **Browse…** to **Co-managed Devices** collection under **Intune Auto Enrollment**. Click **Next**. 6. On the **Workloads** page, drag the slider for **Compliance policies** and **Windows Update policies** to **Pilot Intune** and click **Next**. 7. On the **Staging** page, **Browse…** to **Co-managed Devices** collection next to **Compliance policies** and **Windows Update Policies** and click **Next**. 8. Click **Next** on the **Summary** page. Click **Close**. |

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=19** 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 10 Device | **Note**: In this example, we will look in Microsoft Intune to see the device details and we can see that it already recognizes Windows 10 as an operating system in Microsoft Intune.   1. Start Internet Explorer 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 > Devices**. 4. Notice that the Windows 10 device (**CLIENT1**) is **Hybrid Azure AD joined**. 5. On the left navigation bar, click **All services > search for and click Intune > Intune**. 6. Select **Devices** > **All devices**. 7. Notice that the Windows 10 device (**CLIENT1**) is **Co-managed**. 8. Click on the Windows 10 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**. |

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 3.2.8)
* 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 Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com.** 4. On the left navigation bar, click **All services > search for and click Intune > Intune**. 5. Select **Device configuration**. 6. Under **Manage**, select **Profiles**. 7. Click **+ Create profile**. 8. Under **Platform**, select **Windows 10 and later** and under **Profile**, select **Trusted certificate**. Click **Create**. 9. Under the **Basics** tab, enter the following and click **Next**:   **Name: Trusted Root Certificate**   1. Under the **Configuration settings** tab, enter the following and click **Next**:   Browse to **C:\Packages** and select the **Client Trusted Root Certificate** created in **Section 3.2.8**  **Destination store: Computer certificate store – Root**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**, select **AutoPilot Devices**, click **Select**.   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, click **Create**. |
| Deploy the Configuration Manager Client | 1. Select **Client apps > Apps > + Add**. 2. Under **App type**, select **Line-of-business app** and click **Select**. 3. Under the **App information** tab, enter the following and click **Next**:   Click **Select app package file** and browse to **C:\Program Files\Microsoft Configuration Manager\bin\i386\ccmsetup.exe**. Click **OK**.  **Publisher: Microsoft**  **Command-line arguments: Enter the command line from the Configuration Manager Console > Administration > Cloud Services > Co-management > Right-click CoMgmtSettingsProd > Properties > Enablement tab > Copy the Command-line arguments from there**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Add group**, select **AutoPilot Devices**, click **Select**.   1. Under the **Review + create** tab, 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 | 1. Start the VM and once OOBE has started, in the **Hi Test User1! Welcome to Microsoft Services** 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 | 1. Go to **Start > Settings**. 2. In the **Settings** app, browse to **Accounts > Access work or school**. 3. 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 | 1. Start Internet Explorer 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 > Devices**. 4. Notice that the Windows 10 device (**CLIENT1**) is **Azure AD joined**. 5. On the left navigation bar, click **All services > search for and click Intune > Intune**. 6. Select **Devices** > **All devices**. 7. Notice that the Windows 10 device (**CLIENT4**) is **Co-managed**. 8. Click on the Windows 10 device (**CLIENT1**). 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 | 1. Revert **HYD-CLIENT4** to the latest checkpoint. |

* 1. Outlook Mobile App Config and App Protection

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. With **MAM without enrollment** (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any [device](https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform), including personal devices in **bring-your-own-device** (BYOD) scenarios. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of [Microsoft Intune protected apps](https://docs.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps) available for public use.

For more information, refer to <https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy>

**Note:** You must have an iOS/iPadOS or Android with a Test User account to perform this scenario.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create an iOS/iPadOS or Android App Protection Policy | 1. Sign in to [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. In Intune portal, choose **Apps > App protection policies**. This selection opens the **App protection policies** details, where you create new policies and edit existing policies. 3. Select **+ Create policy** and select either **iOS/iPadOS** or **Android**. The **Create policy** pane is displayed. 4. On the **Basics** page, add the following values:  * Name: The name of this app protection policy * Description: [Optional] The description of this app protection policy   The **Platform** value is set based on your above choice.   1. Click **Next** to display the **Apps** page. The **Apps** page allows you to choose how you want to apply this policy to apps on different devices. You must add atleast one app.  * Target to apps on all devices types: Use this option to target your policy to apps on devices of any management state. Choose **No** to target apps on specific device types. For information, see [Target app protection policies based on device management state](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#target-app-protection-policies-based-on-device-management-state) * Device types: Use this option to specify whether this policy applies to MDM managed devices or unmanaged devices. For iOS/iPadOS APP policies, select from **Unmanaged** and **Managed** devices. For Android APP policies, select from **Unmanaged**, **Android device administrator**, and **Android Enterprise**. * Public apps: Click **+ Select public apps** to choose the apps to target. * Custom apps: Click **+ Select custom apps** to select custom apps to target based on a Bundle ID.   The app(s) you have selected will appear in the public and custom apps list.   1. Click **Next** to display the **Data protection** page.   This page provides settings for data loss prevention (DLP) controls, including cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps that this app protection policy applies.  **Data protection settings:**   * **iOS/iPadOS data protection**: For information, see [iOS/iPadOS app protection policy settings – Data protection](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#data-protection). * **Android data protection**: For information, see [Android app protection policy settings – Data protection](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#data-protection).  1. Click **Next** to display the **Access requirements** page.   This page provides settings to allow you to configure the PIN and credential requirements that users must meet to access apps in a work context.  **Access requirements settings:**   * **iOS/iPadOS access requirements**: For information, see [iOS/iPadOS app protection policy settings – Access requirements](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#access-requirements). * **Android access requirements**: For information, see [Android app protection policy settings – Access requirements](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#access-requirements).  1. Click **Next** to display the **Conditional launch** page.   This page provides settings to set the sign-in security requirements for your app protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company apps. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for single setting.  **Conditional launch settings:**   * **iOS/iPadOS conditional launch**: For information, see [iOS/iPadOS app protection policy settings – Conditional launch](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios#conditional-launch). * **Android conditional launch**: For information, see [Android app protection policy settings – Conditional launch](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android#conditional-launch).  1. Click **Next** to display the **Assignments** page.   The **Assignments** page allows you to assign the app protection policy to groups of users.   1. Click **Next** to review the values and settings you entered for this app protection policy. 2. When you are done, click **Create** to create the app protection policy in Intune.   **Note:** These policy settings are enforced only when using apps in the work context. When end users use the app to do a personal task, they aren't affected by these policies. Note that when you create a new file it is considered a personal file.   1. End users can download the apps from the App store or Google Play. For more information, see:  * [What to expect when your Android app is managed by app protection policies](https://docs.microsoft.com/en-us/mem/intune/fundamentals/end-user-mam-apps-android) * [What to expect when your iOS/iPadOS app is managed by app protection policies](https://docs.microsoft.com/en-us/mem/intune/fundamentals/end-user-mam-apps-ios) |

1. Shaping devices to corporate standards
2. 1. User File and Settings Migration

User Files and Settings Migration is necessary in PC replacement scenarios and can be accomplished by implementing services like file sync in OneDrive for Business in advance of PC replacement. Leveraging cloud file sync with OneDrive for Business and files on demand can help simplify onboarding onto the new endpoint. In this scenario, we’ll use Group Policy and cloud policy to control OneDrive sync client settings.

**Resources**

[Use Group Policy to control OneDrive sync settings](https://docs.microsoft.com/en-us/onedrive/use-group-policy#OptInNoWizard)

Known Folder File Migration

There are two primary advantages of moving or redirecting Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) to Microsoft OneDrive for the users in your domain:

* Your users can continue using the folders they're familiar with. They don't have to change their daily work habits to save files to OneDrive.
* Saving files to OneDrive backs up your users' data in the cloud and gives them access to their files from any device.

For these reasons, we recommend moving or redirecting known folders to OneDrive if you're an enterprise or large organization. Small or medium businesses may also find this useful, but keep in mind you'll need some experience with Group Policy. For info about the end-user experience, see [Protect your files by saving them to OneDrive](https://support.office.com/article/d61a7930-a6fb-4b95-b28a-6552e77c3057).

#### Modern Method

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create OneDrive Known Folder Move Device Configuration Profiles in Intune | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. Browse to **Device configuration | Profiles | + Create profile** and select the following and click **Create**:   Platform: **Windows 10 and later**  Profile: **Custom**   1. Under **Basics** tab, enter the Name: **PoC OneDrive NGSC** and click **Next**. 2. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **ADMX Ingestion**  Description: **OneDrive for Business admx content**  OMA-URI: **./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/OneDriveNGSC/Policy/OneDriveAdmx**  Data type: **String**  Value: **Original content of the OneDrive.admx file to be copied from %localappdata%\Microsoft\OneDrive\BuildNumber\adm**   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **SilentAccountConfig**  Description: **Silently configure OneDrive using the primary Windows account**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/SilentAccountConfig**  Data type: **String**  Value: **<enabled/>**   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **KFMOptInNoWizard**  Description: **Silently redirect Windows known folders to OneDrive**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/KFMOptInNoWizard**  Data type: **String**  Value: **<enabled/> <data id="KFMOptInNoWizard\_TextBox" value="Insert Your Azure Tenant ID"/> <data id="KFMOptInNoWizard\_Dropdown" value="0"/>**  **Note 1:** For Azure Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box.  **Note 2:** Value of 0 = Don’t display any notification and Value of 1 = Display notification after KFM setup has completed.   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **KFMOptInWithWizard**  Description: **Prompt users to move Windows known folders to OneDrive**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/KFMOptInWithWizard**  Data type: **String**  Value: **<enabled/> <data id="KFMOptInWithWizard\_TextBox" value="Insert Your Azure Tenant ID"/>**  **Note:** For Azure Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box.   1. Under **Configuration settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **KFMBlockOptOut**  Description: **Prevent users from redirecting their Windows known folder to their PC**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/KFMBlockOptOut**  Data type: **String**  Value: **<enabled/>**   1. Under **Configuration Settings** tab, click **Add** and enter the following information for this type of setting and click **Add**:   Name: **FilesOnDemandEnabled**  Description: **Enable OneDrive Files On-Demand**  OMA-URI: **./Device/Vendor/MSFT/Policy/Config/OneDriveNGSC~Policy~OneDriveNGSC/FilesOnDemandEnabled**  Data type: **String**  Value: **<enabled/>**   1. Once done, click **Next** on the **Configuration Settings** tab. 2. Under **Assignments** tab, click **+ Select groups to include | type and select Sales | click Select | Next**. 3. Under **Applicability Rules** tab, click **Next**. 4. Under **Review + create** tab, click **Create**. 5. On the client side, click **Start | Settings**. 6. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 7. Click **Sync** for the Device Configuration Profiles to be deployed. |

#### On-Premises Method

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT7 virtual machine.** | |
| Copy .adml and .admx Files | 1. Create a Microsoft 365 trial subscription and test account per Section 2.2.1 if you haven’t already. 2. Download and install the latest windows version of the [new OneDrive sync client](https://go.microsoft.com/fwlink/p/?linkid=844652). 3. Under **All Programs**, select **Microsoft OneDrive** to open app. 4. When OneDrive starts, enter your test account, or your work or school account, created in Section 2.2.1 (USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com**) and then select **Sign in**. 5. Browse to **%localappdata%\Microsoft\OneDrive\BuildNumber\adm**, to the subfolder for your language as necessary (Where BuildNumber is the number displayed in sync client settings on the About tab.) 6. Copy the **OneDrive.adml** and **OneDrive.admx** files and store it temporarily in **\\DC1\C$**.   The ADM folder in the OneDrive installation directory |
| **Complete these steps on the DC1 virtual machine.** | |
| Paste .adml and .admx Files in Central Store | 1. In File Explorer, go to the **C:\** drive and copy the **OneDrive.adml** and **OneDrive.admx** files. 2. Go to **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions** to your domain's Central Store. 3. Paste the **OneDrive.admx** file in your domain's Central Store and the **OneDrive.adml** file in the appropriate language subfolder (such as **en-US**). **Note:** If you get an “Access Denied” alert when pasting the files, right-click the **Policy Definitions** folder, and then click **Properties>Security>Advanced**. Click the **Permissions** tab, click “**Select principal**” and add “**LabAdmin**” with full permissions. 4. Go to **Server Manager>Tools>Active Directory Users and Computers** and then expand **CORP**. An **Organizational Unit** should have already been created from a previous lab called “**Known Folder**”. 5. Under **Known Folder** ensure that **CLIENT7** and **CLIENT2** exist as done in a previous lab. |
| Configure Group Policy Object | 1. In the Group Policy Management Console, open **Domains>corp.contoso.com>CORP**. 2. Right-click the Organizational Unit, example “**Known Folder**” and click **Create a GPO in this domain, and Link it here**. Name the GPO as “**Known Folder**” and click **OK**. 3. Right-click the new GPO “**Known Folder**” and click **Edit**. 4. Go to **Computer Configuration\Policies\Administrative Templates\OneDrive** and **Enable** the following Known Folder Move policy:[Silently move Windows known folders to OneDrive](https://docs.microsoft.com/en-us/onedrive/use-group-policy#silently-move-windows-known-folders-to-onedrive) 5. Add the **Tenant ID** to Known Folder Move Policy. To find the Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box. 6. Select **Yes** for **Show notification to users after folders have been redirected**. 7. Click **Apply | OK.** For info, see [Link Group Policy objects to Active Directory containers](https://go.microsoft.com/fwlink/?linkid=871796) |
| **Complete these steps on the CLIENT7 AND CLIENT2 virtual machines.** | |
| Confirm Automatic File Transfer | 1. Restart/Start **CLIENT7** and **CLIENT2** to initiate Group Policy and file transfer. 2. Open **CLIENT2** and log into the Microsoft OneDrive app using the same test account as **CLIENT7**. (USER NAME: **TU1@<AzureDomainName>.onmicrosoft.com**). 3. Confirm on **CLIENT2** that you get a notification and in both **CLIENT7** and **CLIENT2**, you see **Documents**, **Pictures** and **Desktop** OneDrive folders synced between the 2 machines. |
| **Complete these steps on the DC1, CLIENT7 AND CLIENT1 virtual machines.** | |
| Move Sample Files from Z Drive to SharePoint Shared Library using SharePoint Migration Tool | 1. Create some **Office Sample Files** and create a folder called **Sample Files** on **CLIENT7**’s desktop and then copy the folder to **DC1**’s **C Drive**. 2. In **DC1**’s **C Drive**, right-click **Sample Files** folder and click **Properties**. 3. Click the **Sharing** tab. 4. Click **Advanced Sharing**. 5. Select **Share this folder** and click **Permissions**. 6. Select **Allow – Full Control** and click **Apply** and **OK**. 7. Click **Apply** and **OK** again. 8. Click the **Security** tab and click **Advanced**. 9. Click **Change permissions** and then click **Add**. 10. Click **Select a principal**, type **Everyone** and then click **Check Names**. Click **OK**. 11. Select **Full control** and then click **OK**. 12. Click **Apply** and **OK**. 13. Click **Close**. 14. Log in to **CLIENT1** as **CORP\LabAdmin**, open **File Explorer** and then click **This PC**. 15. From the top, click **Computer | Map network drive | Map network drive**. 16. Select **Z:** next to **Drive** and next to **Folder** enter **\\DC1\Sample Files**. 17. Click **Finish**. 18. Now open **Internet Explorer** and browse to <http://spmtreleasescus.blob.core.windows.net/install/default.htm> to download and install the **SharePoint Migration Tool**. 19. Select **I agree to the Terms of Service and Privacy Policy** and click **Install**. 20. Click **Run** on the prompt and wait for the download and installation to finish. 21. In the **SharePoint Migration Tool** window, the **Sign in** window will open. 22. **Sign in** as **LabAdmin@<AzureDomainName>.onmicrosoft.com**. Click **Start your first migration**. 23. On the **Where’s your content** window, select **File Share**. 24. On the **Select a source** window, click **Choose Folder** and browse to **This PC > Sample Files (\\DC1) (Z:)**. Click **OK**. 25. Click **Next**. 26. In the **Select a destination** window, enter **https://<AzureDomain>.sharepoint.com/**, click **Next** and wait for the **Select a document library** to populate. 27. Select **Documents** and click **Next**. 28. On the Review migration window, name your migration and review other details and click **Next**. 29. On the **Choose your settings** window, click **Migrate**. 30. Once the migration is finished, click **Save** on the prompt. Click the link to the **Communication site**, sign in with **LabAdmin@<AzureDomainName>.onmicrosoft.com** and you should be able to see the migrated files/data. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Create a Local GPO for Team Library to Sync Automatically and see Results | 1. On **CLIENT1**, Open **Internet Explorer** and browse to **https://<AzureDomain>.sharepoint.com/**. 2. Click **Site contents** and then click **Documents**. You will be able to see the files that have been migrated from the mapped drive. 3. Click **Sync**, click **Allow/Open**, copy and save the **Library ID** and **Sign in** to the OneDrive sync client. 4. Browse to **%localappdata%\Microsoft\OneDrive\BuildNumber\adm**, to the subfolder for your language as necessary (Where BuildNumber is the number displayed in sync client settings on the About tab.) 5. Copy the **OneDrive.adml** to **C:\Windows\PolicyDefinitions\en-US** and **OneDrive.admx** to **C:\Windows\PolicyDefinitions**. 6. Launch **gpedit.msc**. 7. Go to **Computer Configuration\Administrative Templates\OneDrive**. 8. Double-click on **Configure team site libraries to sync automatically**. 9. Select **Enabled** and click **Show…** 10. Under **Value name** enter **Docs** and under **Value** paste the **Library ID** that was saved earlier. Click **OK**. 11. Click **Apply** and **OK**. 12. Go to **Computer Configuration\Administrative Templates\OneDrive** and **Enable** the following Known Folder Move policy:[Silently move Windows known folders to OneDrive](https://docs.microsoft.com/en-us/onedrive/use-group-policy#silently-move-windows-known-folders-to-onedrive) 13. Add the **Tenant ID** to Known Folder Move Policy. To find the Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box. 14. Select **Yes** for **Show notification to users after folders have been redirected**. 15. Click **Apply** and **OK**. 16. Go to **Computer Configuration\Administrative Templates\OneDrive** and **Enable** the policy **Use OneDrive Files On-Demand**. 17. Click **Apply** and **OK**. 18. Run a **gpupdate /force** on **CLIENT1**. 19. Open **File Explorer** and click **<AzureDomain>**. 20. In the **File Explorer**, you will be able to notice the files in the **Communication site - Documents** Shared Library and you will be able to note from the symbol if files are in cloud. |
| **Complete these steps on the CM1 virtual machine.** | |
| Create OneDrive for Business Profile in ConfigMgr for moving Windows Known Folders to OneDrive for Business | 1. Find your Microsoft 365 Tenant ID, log in to Microsoft Azure as the tenant admin. In the Microsoft Azure portal, click **Azure Active Directory**. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box. 2. Ensure that the client has the latest OneDrive sync client. If you have followed the previous steps, clients have the latest version of the OneDrive sync client as it is in Windows 10. 3. In the Configuration Manager Console, browse to **Assets and Compliance | Compliance Settings | OneDrive for Business Profiles**. 4. Click **Create OneDrive for Business Profile** from the ribbon bar. 5. On the General page, enter the **Name** and click **Next**. 6. On the Supported Platforms page, select **Windows 10** and click **Next**. 7. On the Known Folder Move Settings page, **Specify an Office 365 tenant ID** and either select **Prompt users to move Windows known folders to OneDrive** or **Silently move Windows known folders to OneDrive** and you may also select **Show notification to users after folders have been moved** and **Prevent users from redirecting their Windows known folders back to their PC**. Click **Next**. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. 10. To create a Device Collection, right-click **Device Collections** and click **Folder | Create Folder**. Enter **KFM** and click **OK**. 11. Right-click **KFM** and click **Create Device Collection**. 12. Enter the following details and click **Next**:   Name: **KFM**  Limiting collection: **All Desktop and Server Clients**   1. Click **Add Rule | Direct Rule** and click **Next**. 2. Enter **%ClientName%** and click **Next**. 3. Select the client and click **Next**. 4. Click **Next** and then click **Close**. 5. Click **Next** twice and then click **Close**. Ensure that the client is in the **KFM** collection. 6. Now, to deploy the OneDrive for Business Profile, go back to **Assets and Compliance | Compliance Settings | OneDrive for Business Profiles**. 7. Select the profile created earlier and click **Deploy** from the ribbon bar. 8. Click **Browse…** next to **Collection** and select **Device Collections | KFM | KFM**. Click **OK**. 9. Configure the **Alert** and **Schedule** options and click **OK**. Ensure the first deployment happens immediately. 10. In the client, in the **Configuration Manager Properties | Actions** tab. Run the **Machine Policy Retrieval & Evaluation Cycle** and then click **OK**. In the **Configurations** tab, ensure that the **OneDrive for Business Profile** is visible and click **Refresh** and **Evaluate** until it is **Compliant**. |

**Note:** Before proceeding with the labs ahead, make sure to move the **CLIENT1**, **CLIENT2** and **CLIENT7** machines back to the Computers container if they are not in the Computers container:

1. In **DC1**, launch **Active Directory Users and Computers**.
2. Navigate to **corp.contoso.com > CORP > Known Folder**.
3. Select and right-click **CLIENT2** and **CLIENT7** and then click **Move…**
4. In the Move menu, under **corp** select **Computers** and then click **OK**.
   1. Security and Compliance

Endpoint Security is a key value proposition of Microsoft Endpoint Manager. In this module, you will go through Windows 10 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 the Security Module, you will need the vTPM enabled on Client VMs in many scenarios. In order to enable vTPM on Client VMs, the Hyper-V Configuration Version must be at **8.0** in Windows Server 2016 Hyper-V Host for **HYD-CLIENT 1, 2, 3 and 4**. Also, you will notice that **HYD-CLIENT 1, 2, 3 and 4** are **GEN1** VMs. In order to enable vTPM on Client VMs, these **GEN1** VMs need to be converted to **GEN2** VMs.

Now, in order to enable vTPM on the Client VMs, perform the following steps:

**Note: (x) = 1, 2, 3 and 4.**

1. In Hyper-V Manager, turn on **HYD-CLIENT(x)** and log in. In **HYD-CLIENT(x)**, open an **elevated command prompt**.
2. Type **cd C:\Windows\System32** and press **Enter**.
3. Now type, **MBR2GPT.EXE /convert /AllowFullOS** and press **Enter**.
4. Once the conversion process completes, **shut down the VM**.
5. In Hyper-V Manager, select **HYD-CLIENT(x)** and click **Delete** under the **Actions** pane on the right.
6. Click **Delete** again on the Delete Selected Virtual Machines dialog box.
7. On the right, under the **Actions** pane, click **New > Virtual Machine…**
8. On the Before You Begin page, click **Next**.
9. On the Specify Name and Location page, for **Name**, enter **HYD-CLIENT(x)** and click **Next**.
10. Now, on the Specify Generation page, select **Generation 2** and click **Next**.
11. On the Assign Memory page, for **Startup memory**, provide a memory of **2GB or more** and click **Next**.
12. On the Configure Networking page, for **Connection**, select **HYD-CorpNet** and click **Next**.
13. On the Connect Virtual Hard Disk page, select **Use an existing virtual hard disk**, **Browse…** to the **SelfService** folder which contains the Lab Kit files and select **HYD-CLIENT(x).VHDx**. Click **Open** and click **Next**.
14. On the Completing the New Virtual Machine Wizard page, click **Finish**.
15. Now select the newly created **HYD-CLIENT(x)** and on the right under the **Actions** pane, click **Settings...**
16. Click **Security** and under **Secure Boot**, ensure that **Enable Secure Boot** is checked.
17. Under **Security**, under **Encryption Support**, check **Enable Trusted Platform Module**.
18. Click **Apply | OK**.
19. **Turn on the VM** to ensure that the VM is turning on and are able to log in and then **shut the VM back down**.
20. These **Steps 1-19** must be performed for **HYD-CLIENT 1, 2, 3 and 4**.

**Note:** In order to avoid hiccups during “Cloud 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.

BitLocker

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

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. 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.



#### 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 Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **BitLockerDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1, TU2**   1. Click **Create**. |
| Configure Windows Bitlocker | 1. On the left navigation bar, click **All services**. 2. Enter “**Intune**” in search. 3. Click on **Intune**. 4. Under **Manage** select “**Device configuration**”. 5. Under **Manage** select “**Profiles**”. 6. Select “**+ Create profile**”. 7. For Platform select “**Windows 10 and later**”. 8. For Profile select “**Endpoint protection**” and click **Create**. 9. Under the **Basics** tab, enter the following and click **Next**:   Name: **Bitlocker Demo**   1. Under the **Configuration settings** tab, 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.   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **BitLockerDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, 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 | 1. Log in to the machine as:   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. After a few minutes of syncing, you will notice that a notification appears **Encryption needed** (at least once) asking you to start encryption. |

#### On-Premises Method

This section describes how to install and configure MBAM server and client components. The server components can be installed using two possible topologies:

* Stand Alone
* Configuration Manager

Both of these installations include the following components: Self-Service Portal, Key Database, Reports Database, Reports, Administration Monitoring Server, Group Policy Template.

To configure MBAM the following tasks need to be performed:

1. Create a GPO to apply MBAM settings to client devices.
2. Test the configuration on a client device.
3. Connect to the Self-Service Portal.

Prerequisites

Perform the following tasks before proceeding.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Download MDOP Group Policy Templates | 1. Open Internet Explorer and browse to the URL below.   https://www.microsoft.com/en-us/download/details.aspx?id=55531   1. Click **Download** and save the **MDOP\_ADMX\_Templates.cab** file to **C:\packages**. 2. On the taskbar, open **File Explorer** and browse to **C:\packages** and create a folder named **MDOPGPO**. |

Create and Deploy MBAM Settings

This activity will guide you through creating and deploying a group policy object that will enforce the configuration of MBAM and BitLocker on the targeted devices.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Create and Deploy MBAM Policies | 1. Start **Command Prompt (Elevated)**. Accept the UAC prompt. 2. On the Command Prompt window, change the working directory to **C:\packages**. 3. On the Command Prompt window, “**manually type**” the following command and press **Enter**.   **expand MDOP\_ADMX\_Templates.cab -F:\* C:\packages\MDOPGPO**   1. Copy all the contents of **C:\packages\MDOPGPO\MBAM2.5SP1** to the Policy Central Store **C:\Windows\SYSVOL\sysvol\corp.contoso.com\Policies\PolicyDefinitions**. 2. Open the **Group Policy Management** console. 3. Navigate to **Group Policy Management / Forest: corp.contoso.com / Domains /** **corp.contoso.com**. 4. Right-click **corp.contoso.com**, then click **Create a GPO in this domain, and Link it here**… 5. In the Name field type **MBAM Client Configuration**, click **OK**. 6. Expand **corp.contoso.com**, right-click on **MBAM Client Configuration** and select **Edit…** 7. Navigate to **Computer Configuration / Policies / Administrative Templates / Windows Components / MDOP MBAM (BitLocker Management)**. 8. Configure the suggested default settings as outlined in the Planning for MBAM 2.0 Group Policy Requirements Guide - <https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v2/planning-for-mbam-20-group-policy-requirements-mbam-2?redirectedfrom=MSDN>. Refer to the screenshot below for the settings.   **Note**: To utilize MBAM on a virtual machine, ensure that Allow BitLocker without a compatible TPM is checked. Ensure that group policies are updated in the **CLIENT2** virtual machine and **APP1** is up and running. |

A screenshot of a social media post

Description automatically generated

Test MBAM Configuration

This activity will guide you through the client experience of MBAM assuming control of BitLocker management.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Install MBAM Agent | 1. Install MBAM client from **\\APP1\C$\packages\Sources\MBAM 2.5 SP1\x64\MBAMClientSetup.exe**. 2. Click **Yes** on the UAC prompt if required. 3. Click **I accept** and click **Next** and complete the installation. |
| Reduce the MBAM Client Startup Delay | 1. From the **Start** screen, find and start **Regedit**. Accept the UAC prompt if required. 2. Navigate to **HKEY\_LOCAL\_MACHINE\Software\Microsoft\MBAM**. 3. Create a DWORD key named **NoStartupDelay**. 4. Set the value of **NoStartupDelay** to **1**. 5. Navigate to **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\FVE\MDOPBitLockerManagement**. 6. Update the value of **ClientWakeupFrequency** to **1**. 7. Update the value of **StatusReportingFrequency** to **1**. |
| MBAM Client | 1. Restart **CLIENT2** to force a full group policy update and **Start/Restart** the **BitLocker Management Client Service** and **Bitlocker Drive Encryption Service** from the **Services** MMC Console. 2. You will notice that a window appears asking you to start encryption in a moment. |

Connect to Self-Service Portal

The following activity may be used to demonstrate the access and use of the Self-Service portal provided by MBAM.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Access the MBAM Self-Service Portal | 1. In Internet Explorer enter the following URL **http://app1.corp.contoso.com/selfservice**, where app1.corp.contoso.com is the path to the MBAM server. 2. When prompted enter user credentials **corp\labadmin** and **P@ssw0rd** and click **OK**. 3. Review the portal. Check the box next to **I have read and understand the above notice** and click **Continue** and then review the next page. |

Windows Defender Antivirus

Windows Defender Antivirus keeps your PC safe with trusted antivirus protection built-in to Windows 10. 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 cloud or on-premises management to configure WDAV.

#### 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 Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **WDAVDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**   1. Click **Create**. |
| Creating an Intune Windows Defender Antivirus Policy | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. 7. Click on “**Device configuration**”. 8. Click on “**Profiles**”. 9. Click **+ Create profile**. 10. In the Platform, select **Windows 10 and later**. 11. In the Profile, select “**Device restrictions**” and click **Create**. 12. Under the **Basics** tab, enter the following information and click **Next**:   Name: **WDAV Demo**   1. Under the **Configuration settings** tab, 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   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select “**WDAVDemo**”   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, 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 | 1. Log in to the machine as:   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Close **Settings**. 9. **Reboot** the machine. 10. Log back in with the same credentials. 11. Click **Start**. 12. 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. |

#### On-Premises Method

Follow the following sections for managing Windows Defender Antivirus through on-premises Method tools.

WDAV

In this section, you will configure 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. Open the **Configuration Manager Console** from the Start Menu. 2. From the Configuration Manager Console, browse to **Administration**. 3. Expand **Site Configuration**. 4. Click on **Servers and Site System Roles**. 5. Right-click on **CM1.corp.contoso.com**. 6. Select **Add Site System Roles**. 7. Click **Next** on the Select a server to use as a site system. 8. Click **Next** on the Specify Internet proxy server. 9. Check **Endpoint Protection point**. 10. Click **OK**. 11. Click **Next**. 12. Select **Basic membership (on Windows 10 and above, the behavior is the same as advanced membership)**. 13. Click **Next**. 14. Click **Next**. 15. Click **Close**. |
| Enable Configuration Manager to Manage Client Endpoint Protection | 1. Click **Administration**. 2. Click on **Client Settings**. 3. Right-click on **Default Client Settings**. 4. Click on **Properties**. 5. Click on **Endpoint Protection**. Click **OK** if a prompt comes. 6. Change **Manage Endpoint Protection client on client computers** to **Yes**. 7. Click on **OK**. |
| Create a Collection | 1. Open the **Configuration Manager Console** from the Start Menu. 2. From the Configuration Manager Console, browse to **Assets and Compliance**. 3. Click on **Devices**. 4. Right-click on **CLIENT1**. 5. Click on **Add Selected Items**. 6. Select **Add Selected Items to New Device Collection**. 7. Enter **WDAV Client1** for the collection name. 8. Limit collection to **All Desktop and Server Clients**. 9. Select **Next**. 10. Select **Next**. 11. Select **Next**. 12. Select **Close**. |
| Create a Custom Antimalware Policy | 1. Open the **Configuration Manager Console** from the Start Menu. 2. From the Configuration Manager Console, browse to **Assets and Compliance**. 3. Expand on **Endpoint Protection**. 4. Click on **Antimalware Policies**. 5. Click on **Create Antimalware Policy**. 6. 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**   1. Click on **OK**. 2. Right-click on **WDAV Demo Policy**. 3. Click **Deploy**. 4. In the right-hand corner, click on **WDAV Client1**. 5. Click **OK**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Check Policy Configuration | 1. Open **Control Panel**. 2. Search for **Configuration Manager**. 3. Open **Configuration Manager**. 4. Click on the **Actions** Tab. 5. Click on **Machine Policy Retrieval & Evaluation Cycle**. 6. Click on **Run Now**. Click **OK**. 7. Wait 3 to 5 minutes then continue. 8. Click **Start**. 9. Type **Windows Security** and click **Windows Security settings**. 10. Under **Protection areas** click **Virus & threat protection**. 11. Under **Virus and threat protection settings**, click **Manage settings**. 12. Notice the This setting is managed by your administrator. |

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.

#### 4.2.3.1 Cloud Management

The following sections cover managing Windows Hello for Business through cloud 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. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. |
|  | 1. Select “**Device enrollment**”. 2. Select “**Windows enrollment**”. 3. Select “**Windows Hello for Business**”. |
|  | 1. Select **Enabled** next to “**Configure Windows Hello for Business**”. 2. Review possible settings. 3. Select **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 | 1. 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.   1. Click “**Set up PIN**”. 2. Click “**Set it up now**”. 3. Select a verification method “**Text message**”. 4. Select a region that is correct for your cell phone. 5. Enter your phone number. 6. Select **Next**.   **Note:** Steps 15-19 are required only when you are setting up for the first time for a user.   1. Retrieve security code from your phone and enter it. 2. Select **Verify**. 3. Enter a new PIN “214359” (or a PIN of your choice, just don’t forget it). 4. Confirm your PIN “214359” and click **OK**. Click **OK** again. Now you will test your new PIN. 5. Sign out. 6. Sign back in using your PIN. |

Credential Guard

In this lab, you will activate Credential Guard.

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 Physical Computer with a Trusted Platform Module (TPM) chip (2.0 recommended), a CPU with VT-x and VT-d capabilities.
* Windows 10 Enterprise running on the Host.
* Local Administrator Account.
* It is recommended that you use a Host for testing purposes. Please do not use your personal machines. Also, the Host must not be domain joined into your company domain, so that there is no compliance or configuration/support issues.



#### Check Credential Guard Requirements

In this exercise, you will:

* Check if the requirements for Credential Guard are fulfilled.
* Manually activate Credential Guard and its dependencies.

| Task | Detailed Steps |
| --- | --- |
| **Complete this activity on the Reference Device 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 * Hyper-V – Second Level Address Translation Extensions = Yes * Hyper-V – Virtualization Enabled in Firmware = Yes * Hyper-V – Data Execution Protection = Yes  1. If any of the above values are not enabled, then boot into your BIOS/UEFI and activate them. 2. 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 | 1. Open **TPM.MSC** and make sure that the TPM is turned on. 2. If TPM is turned off/not visible, make sure that it exists physically and it is enabled in BIOS/UEFI. 3. If the TPM is turned on but not initialized:    1. Create the TPM owner password using **Automatically create the password** option.    2. 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).    3. Click **Initialize**.    4. 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. |
| Enable Required Features | 1. Go to **Control Panel > Programs >** **Turn Windows features on or off**. 2. Check **Hyper-V** and all **sub-options** within it.   **Note:** On a VM, the Hyper-V Hypervisor option might be unselected and greyed out if the host’s processor does not have the required virtualization capabilities.   1. Click **OK**. 2. Restart the computer by clicking **Restart now**.   **Note**: **Hyper-V** supplies the virtualization core. |

#### Cloud Management

Follow the following sections for managing Credential Guard through cloud management tools.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Groups for use with Credential Guard Lab | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. 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 | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. 7. Click on “**Device configuration**”. 8. Click on “**Profiles**”. 9. Click on “**+ Create profile**”. 10. For **Platform**, select **Windows 10 and later**. 11. For **Profile**, select **Custom** and click **Create**. 12. Under the **Basics** tab, enter the following information and click **Next**. |
|  | Name: **Cred Guard Demo**  Description: **Cred Guard Demo**   1. Under the **Configuration settings** tab, Select “**Add**” to add a OMA-URI Setting. 2. Fill out the form and click **Add**:   Name: **Enable VBS**  Description: **Enable VBS**  OMA-URI: **./Vendor/MSFT/Policy/Config/DeviceGuard/EnableVirtualizationBasedSecurity**  Date type: **Integer**  Value: **1**   1. Click **Add** again and fill out the form and click **Add**:   Name: **Enable Configure LsaCfgFlags**  Description: **Enable Configure LsaCfgFlags**  OMA-URI: **./Vendor/MSFT/Policy/Config/DeviceGuard/LsaCfgFlags**  Date type: **Integer**  Value: **1**   1. Click **Add** again and fill out the form and click **Add**:   Name: **Enable Configure Require Platform Security Features**  Description: **Enable Configure Require Platform Security Features**  OMA-URI: **./Vendor/MSFT/Policy/Config/DeviceGuard/RequirePlatformSecurityFeatures**  Date type: **Integer**  Value: **1**   1. Select **Next**. 2. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **CredGuardDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + Create** tab, 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 | 1. Log in to a machine as:   **TU2@<AzureDomainName>.onmicrosoft.com** (You might have to enable MFA for this user on this machine).   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Close **Settings**. 9. **Reboot** the machine. 10. Log back in using the same credentials. 11. Click **Start**. 12. Type and click “**System Information**”. 13. Verify that “**Virtualization-based security is running**”.   **Note:** After the first boot it could be “**Enabled but not running**”.   1. **Reboot** the machine again. 2. Click **Start**. 3. Type and click “**System Information**”. 4. Verify that “**Virtualization-based Security is running**”.   **Note:** It can take up to 3 or more reboots and syncing to see that it is running. |

#### On-Premises Method

Follow the following sections for managing Credential Guard through on-premises Method tools.

#### Configure Virtualization Based Security and Credential Guard

Now that the required features and components are in place, activate the Virtualization Based Security (VBS) 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. Select **Secure Boot** in the **Select Platform Security Level**. 5. Select **Enabled with UEFI lock** in the **Credential Guard Configuration**. 6. Click **Apply** and **OK**. 7. Restart the computer and check “**System Information**” and verify that “**Virtualization-based Security is running**”. |

#### 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.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 virtual machine or a physical machine if your environment does not support nested virtualization.** | |
| Logging | 1. Device Guard policies are logged in Event Viewer at **Applications and Services Logs > Microsoft > Windows > DeviceGuard >** **Operational**. 2. An **event ID 7000** should be logged, which contains the selected settings within the policy (when successfully applied). |
| MSInfo32 | 1. Open **MSINFO32.EXE** (elevated) and confirm that the options are defined as in the following screenshot. |
| Registry | 1. Browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceGuard**. 2. Verify if **EnableVirtualizationBasedSecurity** is set to **1**. 3. Verify if **RequirePlatformSecurityFeatures** is set to **1** (Secure Boot). 4. Browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**. 5. Verify if the **LsaCfgFlags** is set to **1**. |
| Process | 1. Open **Task Manager**. 2. Verify the presence of **Lsalso.exe**. |

Windows Defender Application Guard

Designed for Windows 10 and 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:** Windows Defender Application Guard can only be enabled if the Hardware Requirements are met as stated in <https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-application-guard/reqs-wd-app-guard>

**Note:** 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 SLAT or not, 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.



#### Cloud Management

Follow the following sections for managing Windows Defender Application Guard through modern management tools.

#### Configure Windows Defender Application

In the section below you will be configuring WDAG using modern management.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create Groups for use with WD Application Guard Demo | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **WDAGDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**  7. Click **Create**. |
| Creating an Intune WDAG Policy | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services**. 5. Enter “**Intune**” in search. 6. Click on **Intune**. 7. Click on “**Device configuration**”. 8. Click on “**Profiles**”. 9. Click on “**+ Create profile**”. 10. Under **Platform**, select **Windows 10 and later**. 11. Under **Profile**, select **Endpoint protection** and click **Create**. 12. Under the **Basics** tab, enter the following information and click **Next**:   Name: **WDAG Demo**  Description: **WDAG Demo**   1. Under the **Configuration settings** tab, 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**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **WDAGDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, 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).** | |
| Verify the Policy has been Applied and Working | 1. Log in to a machine as:   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Close **Settings**. Reboot the machine once. 9. Launch **Edge**. 10. Click **New Application Guard window** from the menu. 11. A new window should appear.   **Note:** Notice that in the upper left-hand corner of the window you should see Application Guard and a thin orange line at the top of the windows. This indicates you are running in Application mode.  A screenshot of a cell phone  Description automatically generated   1. Enter the URL **www.bing.com**. 2. Create a new tab. 3. Copy the URL [www.bing.com](http://www.bing.com) to the new tab.   **Note:** Notice that you can do this because it is inside of Application Guard.   1. Open **IE**. 2. Try to copy the URL from WDAG Edge windows to IE.   **Note:** Notice that you cannot copy. This is because WDAG is configured to not allow copy and paste with the OS.   1. Enter the URL of **www.msn.com** in IE. 2. Copy this URL from IE and try and paste it in WDAG Edge window.   **Note:** Notice that you cannot copy. This is because WDAG is configured to not allow copying from the OS to the WDAG Edge windows. |

#### On-Premises Method

Follow the following sections for managing Windows Defender Application Guard through on-premises Method tools.

#### Prerequisites

| 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).** | |
| Install the Feature | 1. Open the **Control Panel**, click **Programs,** and then click **Turn Windows features on or off**. 2. Select the checkbox next to **Windows Defender Application Guard** and then click **OK**. 3. Restart the device. |

#### Configure Group Policy Settings

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the DC1 virtual machine.** | |
| Turn On Windows Defender Application Guard | 1. In the **Group Policy Management** Console, edit the **Default Domain Policy** by going to **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Application Guard**. 2. Double-click **Turn on Windows Defender Application Guard in Enterprise Mode**. 3. Select **Enabled** and click **Apply** and **OK**. |
| Set Up Network Isolation | 1. Go to the **Computer Configuration\Policies\Administrative Templates\Network\Network Isolation\Enterprise resource domains hosted in the cloud**. 2. Select **Enabled** and type **.microsoft.com** into the **Enterprise cloud resources** box. Click **Apply** and **OK**. 3. Go to the **Computer Configuration\Policies\Administrative Templates\Network\Network Isolation\Domains categorized as both work and personal** setting. 4. Select **Enabled** and type **bing.com** into the **Neutral resources** box. Click **Apply** and **OK**. |

#### Validate Windows Defender Application Guard

| 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).** | |
| 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](http://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](http://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. |

Windows Defender Exploit Guard

Windows Defender Exploit Guard (Windows Defender EG) is a new set of host intrusion prevention capabilities for Windows 10, 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 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.

#### Cloud Management

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

#### 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. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **ExploitDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**   1. Click **Create**. | | |
| Configure Windows Defender Exploit Guard | | 1. On the left navigation bar, click **All services**. 2. Enter “**Intune**” in search. 3. Click on **Intune**. 4. Under Manage Select “**Device configuration**”. 5. Under Manage Select “**Profiles**”. 6. Select “**Create profile**”. 7. Under **Platform**, select **Windows 10 and later**. 8. Under **Profile**, select **Windows 10 and later** and click **Create**. 9. Under the **Basics** tab, enter the following information and click **Next**:   Name: **Exploit Protection Demo**   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Expand **Microsoft Defender Exploit Guard** |
|  | | Expand **Controlled folder access**  Folder protection: **Enable**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **ExploitDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, 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 | | 1. Log in to the virtual machine as   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. Open up **Notepad.exe**. 9. Create a simple document. 10. Save it to “**Documents**”.   **Note:** Notice you cannot save to Documents because this is a protected folder. You will get a “**File not found**” message.   1. Press **OK**. |

#### On-Premises Method

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

#### 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 | 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. At the bottom of the **Exploit protection** section, click **Export settings** and then save the configuration file under **Documents**. 4. Copy the file to **DC1** in a shared folder with full permissions. |
| **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**, right-click the **Group Policy Objects** and create a new GPO **WDEG**. 2. Right-click the new Group Policy **WDEG** and 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 > Windows Defender Exploit Guard > Exploit Protection**. 6. Double-click the **Use a common set of exploit protection settings** setting and set the option to **Enabled**. 7. 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 it’s extension and click **Apply | OK**. |

#### 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 > Windows Defender Antivirus > Windows 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**   1. Set the **Value** to **1** and click **OK**. Click **Apply | OK**. 2. 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. |

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](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_language_modes).

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.



#### Cloud Management

| Task | | Detailed Steps |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | | | |
| Create Groups for use with WDAC Demo | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **Azure Active Directory > Groups > All groups**. 2. Click **+ New group**. 3. In the Group pane fill in the following values and click **Select**:   GROUP TYPE: **Security**  GROUP NAME: **WDACDemo**  MEMBERSHIP TYPE: **Assigned**  MEMBERS: **TU1,TU2**   1. Click **Create**. | | |
| Configuring WDAC with Intune | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with   **labadmin@<AzureDomainName>.onmicrosoft.com**.   1. On the left navigation bar, click **All services**. 2. Enter “**Intune**” in search. 3. Click on **Intune**. 4. Click on “**Device configuration**”. 5. Click on “**Profiles**”. 6. Click on “**+ Create profile**”. 7. Under **Platform**, select **Windows 10 and later**. 8. Under **Profile**, select **Endpoint protection** and click **Create**. 9. Under the **Basics** tab, enter the following information and click **Next**: | | |
|  | Name: **WDAC Demo**  Description: **WDAC Demo**   1. Under the **Configuration settings** tab, enter the following information and click **Next**:   Expand **Microsoft Defender Application Control**  Application control code integrity policies: **Enforce**  Trust apps with good reputation: **Enable**   1. Under the **Assignments** tab, enter the following and click **Next**:   Click **+ Select groups to include**  Select **WDACDemo**   1. Under the **Applicability Rules** tab, click **Next**. 2. Under the **Review + create** tab, 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 | 1. Log in to the virtual machine as   **TU2@<AzureDomainName>.onmicrosoft.com**   1. Select **Start**. 2. Select **Settings**. 3. Select **Accounts**. 4. Select **Access work or school**. 5. Select **Connected to <CompanyName> Azure AD**. 6. Click **Info**. 7. Click **Sync** to force a policy update and confirm that the sync was successful. 8. In **DC1**, download **camstudio** from <http://camstudio.org> to **C:\Packages**. 9. Back in **CLIENT3**, copy **camstudio** from **\\DC1\C$\Packages** to the **Desktop**. 10. Try and install the application **camstudio**. 11. The app will be blocked by WDAC when you try and install it. | | |

#### 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.

#### 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/>   1. Click **Download VLC** and save **vlc-3.0.10-win64.exe** to **C:\Packages**. |
| Download CamStudio (Ignore if already downloaded from the previous lab) | 1. Open Internet Explorer and browse to the URL below.   <http://camstudio.org/>   1. Click **Download** and save **camstudio.exe** to **C:\Packages**. |

#### 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 | 1. 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 | 1. 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 already be created and also 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 | 1. Save the file **PoCPolicy.xml** to a network location, example: **\\DC1\C$**. 2. Open the file and review the content without making changes. Open the file **C:\PoCPolicy.xml** with IE. 3. Close the file. |

#### 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 | 1. From the PowerShell window, run the following commands:   **cp C:\PoCPolicy.bin c:\Windows\System32\CodeIntegrity\SIPolicy.p7b**   1. Restart **CLIENT1** and re-log in with the same credentials. |
| Verify Audit Logs | 1. 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. 2. Right-click on the **Start** button and click **Run**. 3. Enter **eventvwr.msc** and click **OK**. 4. In the Event Viewer MMC, browse to **Event Viewer (Local) > Applications and Services Logs > Microsoft > Windows >** **CodeIntegrity >** **Operational**. 5. Browse through the log files especially **Event ID 3076**. |

#### 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.   1. Open the file **C:\AuditPoCPolicy.xml** with IE. 2. Close the file. |
| Merge Golden Policy with Policy from Audit Logs | 1. From the PowerShell window, run the following commands:   **Merge-CIPolicy –OutputFilePath C:\MergedPoCPolicy.xml –PolicyPaths C:\AuditPoCPolicy.xml,C:\PoCPolicy.xml**   1. Open the file **C:\MergedPoCPolicy.xml** with IE. 2. Close the file. |

#### 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**   1. Open the file **C:\MergedPoCPolicy.xml** with IE. 2. Close the file. |
| Convert from XML to Binary File | 1. From the PowerShell window, run the following commands:   **ConvertFrom-CIPolicy C:\MergedPoCPolicy.xml C:\MergedPoCPolicy.bin** |
| Install Compiled Policy | 1. From the PowerShell window, run the following commands:   **cp C:\MergedPoCPolicy.bin c:\Windows\System32\CodeIntegrity\SIPolicy.p7b**   1. Restart **CLIENT1** and re-log in with the same credentials. |
| Install or Launch Your Application(s) | 1. 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 | 1. Right-click on the **Start** button and click **Run**. 2. Enter **eventvwr.msc** and click **OK**. 3. In the Event Viewer MMC, browse to **Event Viewer (Local) > Applications and Services Logs > Microsoft > Windows >** **CodeIntegrity >** **Operational**. 4. Browse through the log files especially **Event ID 3077**. |

#### 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 and the CLIENT2 virtual machines.** | |
| Create Device Guard GPO | 1. 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**. 2. Navigate to **C:\CodeIntegrity**, right-click **CodeIntegrity** folder and click **Properties**. 3. Click the **Sharing** tab and click **Advanced Sharing…** 4. Check the box next to **Share this folder** and click **Permissions**. 5. Ensure **Everyone** is in the list and has been granted **Full Control**. Click **Apply** and click **OK** two times. 6. Click the **Security** tab and ensure that **Everyone** is in the list and has been granted **Full Control**. 7. Click the **Advanced** button and again ensure that **Everyone** is in the list and has been granted **Full Control**. Close all the windows. 8. Now navigate to **C:\CodeIntegrity\SIPolicy.p7b** that has been copied and right-click on the file and click **Properties**. 9. Click the **Security** tab and ensure that **Everyone** is in the list and has been granted **Full Control**. 10. Click the **Advanced** button and again ensure that **Everyone** is in the list and has been granted **Full Control**. Close all the windows.   **Note**: Check to see that everyone has been granted Full Control permissions.   1. Back in the **DC1** VM, in the Active Directory Users and Computers, create an OU called **Devices** (if not already created from the previous labs) and move the **CLIENT2** VM to the **Devices** OU from the default **Computers** container. 2. Open the **Group Policy Management Console**. 3. Right-click on **Group Policy Management > Forest: corp.contoso.com > Domains > corp.contoso.com >** **Group Policy Objects** and select **New**. 4. Under Name, enter **Device Guard Policies** and then click **OK**. 5. Right-click **Devices** OU, click **Link an Existing GPO**… 6. Select **Device Guard Policies** and click **OK**. |
| Deploy Code Integrity Policy and Enable VBS for KCMI | 1. Right-click **Device Guard Policies** and select **Edit**. 2. Browse to **Computer Configuration\Policies\Administrative Templates\System\Device Guard**. 3. Double-click on **Deploy Windows Defender Application Control**. 4. Select **Enabled**. 5. Under Code Integrity Policy file path, enter **\\DC1\CodeIntegrity\SIPolicy.p7b**. 6. Click **Apply** and then **OK**. 7. Double-click on **Turn On Virtualization Based Security**. 8. Select **Enabled**. 9. Under Select Platform Security Level, select **Secure Boot and DMA Protection**. 10. Under Virtualization based Protection of Code Integrity, select **Enabled with UEFI lock**. 11. Click **Apply** and then **OK**. |
| Attempt to Run New Applications that have not installed on the System | 1. Now on the **CLIENT2** VM, run a **gpupdate /force**. 2. Restart **CLIENT2** and re-log in with the same credentials. 3. 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-3.0.10-win64.exe**.   **Note:** In case the CamStudio package is missing in **\\DC1\C$\Packages\camstudio.exe**, re-download it by following **Steps 3-4** of **Section 4.2.7.2**.  **Note:** 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 **Devices** 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. |

Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (Windows Defender ATP) is a security service that enables enterprise customers to detect, investigate, and respond to advanced threats on their networks.

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

* **Endpoint behavioral sensors**: Embedded in Windows 10, 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 (such as the Microsoft Malicious Software Removal Tool, enterprise cloud products (such as Microsoft 365), and online assets (such as Bing and SmartScreen URL reputation), 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 Windows Defender ATP 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 Windows Defender ATP to detect and respond to threats.

**Note:** This lab can only be performed if the customer has already registered and approved for the Microsoft WDATP Preview/Trial program (Section 2.2.3).

#### Onboarding Windows 10 Device

In this activity, you onboard your first Windows 10 client to Windows Defender Advanced Threat Protection.

| 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://securitycenter.windows.com/**](https://securitycenter.windows.com/) 3. **Sign in** to the portal with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. On the Get started page, click **Next**. 5. On the Set up preferences page, select the appropriate data storage location. 6. Select the appropriate data retention policy. 7. Select your appropriate organization size. 8. Keep the preview features on and then click **Next**. 9. Click **Continue** to create a cloud instance. It will start creating your Windows Defender ATP cloud instance. 10. On the Onboard a machine page, under **Deployment method** dropdown, select **Local Script (for up to 10 machines)** and click **Download package**. 11. Click **Save as** and **Save** the package to **C:\**. 12. Click **Start using Microsoft Defender ATP** and click **Proceed anyway**. |
| Execute the Onboarding Package | 1. Navigate to **C:\**, right-click the package and click **Extract All…** 2. Click **Extract**. 3. 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.   1. Close notepad. 2. Right-click the script file and click **Run as administrator**. Press **Y** to confirm and continue. **Press any key to continue**. 3. After 5-10 minutes the machine will be onboarded. 4. In the **Microsoft Defender Security Center**, on the left navigation pane, click **Settings**. 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 | 1. Click the **Start** menu and type **regedit**, right-click and choose **Run as administrator**. 2. Locate the following registry path: **HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection**. 3. 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 | 1. 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**. 2. Open the **Event Viewer (Local) > Windows Logs > Application** log and locate the **Event ID 20** from the source **WDATPOnboarding**. 3. 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. 4. Go to [**https://securitycenter.windows.com/**](https://securitycenter.windows.com/)portal, then choose **Machines list**, on the right locate your machine on the list, its **Health State** should be **Active**. |
| Install Office (If Not Installed) | 1. Go to [**https://portal.office.com**](https://portal.office.com)and **Sign in** as **TU2@<AzureDomainName>.onmicrosoft.com** 2. Click **Install Office 365 > Office 365 apps**. 3. Click **Run**. |

#### 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://securitycenter.windows.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. |

Endpoint Security

As a Security Admin, use the Endpoint security node in Intune to configure device security and to manage security tasks for devices when those devices are at risk. The Endpoint security policies are designed to help you focus on the security of your devices and mitigate risk. The tasks that are available help you identify devices that are at risk, to remediate those devices, and restore them to a compliant or more secure state.

#### Endpoint Security - Security Baselines

Use Intune's security baselines to help you secure and protect your users and devices. Security baselines are pre-configured groups of Windows settings that help you apply a known group of settings and default values that are recommended by the relevant security teams. When you create a security baseline profile in Intune, you're creating a template that consists of multiple *device configuration profiles*.

You deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10 or later. For example, the *MDM Security Baseline* automatically enables BitLocker for removable drives, automatically requires a password to unlock a device, automatically disables basic authentication, and more. When a default value doesn't work for your environment, customize the baseline to apply the settings you need.

Separate baseline types can include the same settings but use different default values for those settings. It's important to understand the defaults in the baselines you choose to use, and to then modify each baseline to fit your organizational needs.

**Note:** Microsoft doesn't recommend using preview versions of security baselines in a production environment. The settings in a preview baseline might change over the course of the preview.

Security baselines can help you to have an end-to-end secure workflow when working with Microsoft 365. Some of the benefits include:

* A security baseline includes the best practices and recommendations on settings that impact security. Intune partners with the same Windows security team that creates group policy security baselines. These recommendations are based on guidance and extensive experience.
* If you're new to Intune, and not sure where to start, then security baselines gives you an advantage. You can quickly create and deploy a secure profile, knowing that you're helping protect your organization's resources and data.
* If you currently use group policy, migrating to Intune for management is much easier with these baselines. These baselines are natively built in to Intune, and include a modern management experience.

[Windows security baselines](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines) is a great resource to learn more about this feature. [Mobile device management](https://docs.microsoft.com/en-us/windows/client-management/mdm/) (MDM) is a great resource about MDM, and what you can do on Windows devices.

For more information, refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

For a full list of Windows MDM security baseline settings for intune, specially the latest baseline in Intune (May 2019), refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-mdm-all?pivots=mdm-may-2019>

**Note:** In order to test some settings of the Security Baseline Profile on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Device Configuration Profiles from the previous labs.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy a Security Baseline Profile | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Endpoint security** > **Security baselines** to view the list of available baselines. 3. Select the baseline you'd like to use, example: **Windows 10 Security Baselines** and then select **+ Create profile**. 4. On the **Basics** tab, specify the following properties:  * **Name**: Enter a name for your security baselines profile. * **Description**: Enter some text that describes what this baseline does. The description is for you to enter any text you want. It's optional, but recommended.   Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab.   1. On the **Configuration settings** tab, view the groups of **Settings** that are available in the baseline you selected. You can expand a group to view the settings in that group, and the default values for those settings in the baseline. For a full list of Windows MDM security baseline settings for intune, specially the latest baseline in Intune (May 2019), refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-mdm-all?pivots=mdm-may-2019>. To find specific settings:  * Select a group to expand and review the available settings. * Use the *Search* bar and specify keywords that filter the view to display only those groups that contain your search criteria.   Each setting in a baseline has a default configuration for that baseline version. Reconfigure the default settings to meet your business needs. Different baselines might contain the same setting, and use different default values for the setting, depending on the intent of the baseline.  Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab.   1. On the **Scope tags** tab, select **+ Select scope tags** to open the *Select tags* pane to assign scope tags to the profile. Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab. 2. On the **Assignments** tab, select **+ Select groups to include** and then assign the baseline to one or more groups. Use **+ Select groups to exclude** to fine-tune the assignment. Select **Next** to go to the next tab. After you advanced to a new tab, you can select the tab name to return to a previously viewed tab. 3. When you're ready to deploy the baseline, advance to the **Review + create** tab and review the details for the baseline. Select **Create** to save and deploy the profile.   As soon as you create the profile, it's pushed to the assigned group and might apply immediately.  **Note:** If you save a profile without first assigning it to groups, you can later edit the profile to do so.   1. After you create a profile, edit it by going to **Endpoint security** > **Security baselines**, select the baseline type that you configured, example: **Windows 10 Security Baselines** and then select **Profiles**. Select the profile from the list of available profiles, and then select **Properties**. You can edit settings from all the available configuration tabs, and select **Review + save** to commit your changes. |

#### Endpoint Security – Device Compliance

Device compliance policies are a key feature when using Intune to protect your organization's resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version. If the device isn't compliant, you can then block access to data and resources using [Conditional Access](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access).

You can also take actions for non-compliance, such as sending a notification email to the user. For an overview of what compliance policies do, and how they're used, see [get started with device compliance](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started).

**Note:** In order to test some settings of the Device Compliance Policies on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Device Compliance Policies from the previous labs.

**Note:** For platforms other than Windows 10, they must be available with a Test User account to perform this scenario.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy Device Compliance Policies | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Devices** > **Compliance policies** > **Policies** > **+ Create Policy**. 3. Select a **Platform** for this policy from the following options:  * *Android device administrator* * *Android Enterprise* * *iOS/iPadOS* * *macOS* * *Windows Phone 8.1* * *Windows 8.1 and later* * *Windows 10 and later*   For *Android Enterprise*, you also select a **Policy type**:   * *Android device owner compliance policy* * *Android work profile compliance policy*   Then, select **Create** to open the **Create policy** configuration window.   1. On the **Basics** tab, specify a **Name** that helps you identify them later. You can also choose to specify a **Description**. Click **Next**. 2. On the **Compliance settings** tab, expand the available categories, and configure settings for your policy. Click **Next**. The following articles describe the settings for each platform:  * [Android device administrator](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android) * [Android Enterprise](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work) * [iOS/iPadOS](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios) * [macOS](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-mac-os) * [Windows Phone 8.1, Windows 8.1 and later](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows-8-1) * [Windows 10 and later](https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows)  1. On the **Locations** tab, you can force compliance based on the location of the device. Choose from existing locations. If you don't have an available location yet, see [Use Locations (network fence)](https://docs.microsoft.com/en-us/mem/intune/protect/use-network-locations) for guidance. Click **Next**.   **Note:** **Locations** are available only for the *Android device administrator* platform.   1. On the **Actions for noncompliance** tab, specify a sequence of actions to apply automatically to devices that don't meet this compliance policy and click **Next**.   You can add multiple actions and configure schedules and additional details for some actions. For example, you might change the schedule of the default action *Mark device noncompliant* to occur after one day. You can then add an action to send an email to the user when the device isn't compliant to warn them of that status. You can also add actions that lock or retire devices that remain noncompliant.  For information about the actions you can configure, see [Add actions for noncompliant devices](https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance), including how to create notification emails to send to your users.  Another example includes the use of Locations where you add at least one location to a compliance policy. In this case, the default action for noncompliance applies when you select at least one location. If the device isn't connected to any of the selected locations, it's considered not compliant. You can configure the schedule to give your users a grace period, such as one day.   1. On the **Scope tags** tab, select tags to help filter policies to specific groups, such as **US-NC IT Team** or **JohnGlenn\_ITDepartment**. After you add the settings, you can also add a scope tag to your compliance policies. Click **Next**.   For information on using scope tags, see [Use scope tags to filter policies](https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags).   1. On the **Assignments** tab, assign the policy to your groups and click **Next**.   Select **+ Select groups to include** and then assign the policy to one or more groups. The policy will apply to these groups when you save the policy after the next step.   1. On the **Review + create** tab, review the settings and select **Create** when ready to save the compliance policy.   The users or devices targeted by your policy are evaluated for compliance when they check in with Intune. |

#### Endpoint Security – Manage Antivirus, Disk Encryption and Firewall

As a security admin, use the security policies from the *Endpoint security* of Intune to configure device security without the overhead of navigating the larger body and range of settings found in device configuration profiles and security baselines.

Each policy type supports one or more profiles. Profiles are where you configure settings and can group settings for different platforms, or for different areas of focus in the larger policy area.

You'll find these policies under Manage in the **Endpoint security** node of the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431).

For more information, refer to - <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-policy>

**Note:** In order to test some settings of the Device Compliance Policies on **CLIENT3** or **CLIENT4** to avoid any conflicts, remove any previous Antivirus, Disk Encryption and Firewall Policies from the previous labs.

**Note:** For platforms other than Windows 10, they must be available with a Test User account to perform this scenario.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy Antivirus, Disk Encryption and Firewall Policies | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Endpoint security** and then select the type of policy you want to configure, and then select **+ Create Policy**. Choose from the following policy types:  * Antivirus * Disk encryption * Firewall  1. Enter the following properties:  * **Platform**: Choose the platform that you're creating policy for. The available options depend on the policy type you selected: * macOS * Windows 10 and later * **Profile**: Choose from the available profiles for the platform you selected. For information about the profiles, see the dedicated sections below for your chosen policy type: * [Antivirus](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-antivirus-policy) * [Disk encryption](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-disk-encryption-policy) * [Firewall](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-firewall-policy)  1. Select **Create**. 2. On the **Basics** page, enter a name and description for the profile, then choose **Next**. 3. On the **Configuration settings** page, expand each group of settings, and configure the settings you want to manage with this profile. When your done configuring settings, select **Next**. 4. On the **Scope tags** page, choose **+ Select scope tags** to open the *Select tags* pane to assign scope tags to the profile. Select **Next** to continue. 5. On the **Assignments** page, select the groups that will receive this profile. Select **Next**. 6. On the **Review + create** page, when you're done, choose **Create**. The new profile is displayed in the list when you select the policy type for the profile you created. |

#### Endpoint Security – Conditional Access

With Intune, enhance Conditional Access in Azure Active Directory by adding mobile device compliance to the access controls. With Intune compliance policy that defines requirements for devices to be compliant, you can use a device's compliance status to either allow or block access to your apps and services. You can do this by creating a Conditional Access policy that uses the setting **Require device to be marked as compliant**.

A Conditional Access policy specifies the app or services you want to protect, the conditions under which the apps or services can be accessed, and the users the policy applies to. Although Conditional Access is an Azure AD premium feature, the Conditional Access node you access from *Intune* is the same node as accessed from *Azure AD*.

**Note:** Before you set up Conditional Access, you'll need to set up Intune device compliance policies to evaluate devices based on whether they meet specific requirements. Refer to **Section 4.2.9.2: Endpoint Security – Device Compliance**.

**Note:** In order to test some settings of the Conditional Access Policies on **CLIENT3** or **CLIENT4** to avoid any conflicts, start their enrollment fresh for them to receive the Device Compliance Policies and for them to be evaluated by the Conditional Access Policies.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Create and Deploy Conditional Access Policies | 1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). 2. Select **Devices** > **Conditional Access** > **Policies** > **+ New policy**. 3. Under **Assignments**, select **Users and groups**. 4. On the **Include** tab, identify the users or groups that this Conditional Access policy applies to. Once you've chosen groups or users to include, use the **Exclude** tab if there are any users, roles, or groups you want to exclude from this policy.  * **All users**: Select this option to apply the policy to all users and groups, including internal and guest users. * **Select users and groups**: Select this option and specify one or more of the following options: * **All guest and external users**: Select this option to include or exclude external guest users (for example, partners, external collaborators) * **Directory roles**: Select one or more Azure AD roles to include or exclude users who are assigned these roles. * **Users and groups**: Select this option to search for and select individual users or groups you want include or exclude.   **Note: Test the policy against a smaller group of users to make sure it works as expected.**   1. Select **Done**. 2. Under **Assignments**, select **Cloud apps or actions**. 3. On the **Include** tab, use available options to identify the apps and services you want to protect with this Conditional Access policy. Then you can use the **Exclude** tab if there are any apps or services you want to exclude from this policy.  * **All cloud apps**: Select this option to apply the policy to all apps.   **Note**: The Microsoft Azure Management app for access to the Azure portal is included in this list. Be sure to use the **Exclude** tab either here or in the **Users and groups** options to make sure you (or the users or groups you designate) will be able to sign in to the Azure portal.   * **Select apps**: Select this option, choose **Select**, and then use the applications list to search for and select the apps or services you want to protect.   When ready, select **Done**.   1. Under **Assignments**, select **Conditions**.  * **Sign-in risk**: Select *Yes* to use Azure AD Identity Protection sign-in risk detection with this policy, and then choose the sign-in risk levels the policy should apply to. * **Device platforms**: On the **Include** tab, identify the device platforms you want to this Conditional Access policy to apply to. Use the **Exclude** tab to exclude platforms from this policy. * **Locations**: On the **Include** tab, specify whether the policy applies to: * Any location * Trusted network locations that are under the control of your IT department * Specific network locations.   Use the **Exclude** tab to exclude network locations from this policy.   * **Client apps**: Select *Yes* to specify if the policy should apply to browser apps, mobile apps, and desktop clients. * **Device state**: The Conditional Access policy will apply to all device states unless you choose Yes and specifically exclude the states Device Hybrid Azure AD joined or Device marked as compliant (or both).   **Note**: If you want to protect both **Modern authentication** clients and **Exchange ActiveSync** clients, create two separate Conditional Access policies, one for each client type. Although Exchange ActiveSync supports modern authentication, the only condition that is supported by Exchange ActiveSync is platform. Other conditions, including multi-factor authentication, are not supported. To effectively protect access to Exchange Online from Exchange ActiveSync, create a Conditional Access policy that specifies the cloud app Microsoft 365 Exchange Online and the client app Exchange ActiveSync with Apply policy only to supported platforms selected.   1. Select **Done**. 2. Under **Access controls**, select **Grant**. Configure what happens based on the conditions you've set up. You can select from the following options:  * **Block access**: The users specified in this policy will be denied access to the apps under the conditions you've specified. * **Grant access**: The users specified in this policy will be granted access, but you can require any of the following further actions: * **Require multi-factor authentication**: The user will need to complete additional security requirements, like a phone call or text. * **Require device to be marked as compliant**: The device must be Intune compliant. If the device is noncompliant, the user will be given the option to enroll the device in Intune. * **Require Hybrid Azure AD joined device**: Devices must be Hybrid Azure AD joined. * **Require approved client app**: The device must use approved client apps. * **For multiple controls**: Select **Require all the selected controls** so that all of the requirements are enforced when a device attempts to access the app.  1. Under **Enable policy**, select **On**. 2. Select **Create**. |

* 1. Secure and Deploy Business Applications

Microsoft 365 Apps Deployment

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)

Further information on the similarities and differences are in the [About Microsoft 365 Apps in the enterprise](https://support.office.com/en-us/article/About-Office-365-ProPlus-in-the-enterprise-9f11214c-911d-4e3c-9993-a566f12b1a68?ui=en-US&rs=en-US&ad=US)

Microsoft 365 Apps can be deployed in 3 scenarios:

* Enterprise Managed
* Locally Managed
* Cloud Managed

Further information on the 3 scenarios are in the [Plan your enterprise deployment of Microsoft 365 Apps](https://support.office.com/en-us/article/Best-practices-Recommended-deployment-scenarios-4d4ff951-ee72-4763-806a-deeb384a369b?ui=en-US&rs=en-US&ad=US)

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

* Current
* Monthly Enterprise
* Semi-Annual Enterprise

Further information on Microsoft 365 Apps Channels are in the [Overview of update channels for Microsoft 365 Apps](https://support.office.com/en-us/article/Overview-of-update-channels-for-Office-365-ProPlus-9ccf0f13-28ff-4975-9bd2-7e4ea2fefef4?ui=en-US&rs=en-US&ad=US)

**Note:** If there are any 32-bit Office versions installed from the previous sections, uninstall them from VM’s that are going to be used in this section, as we are now going to focus on 64-bit Office versions and both 32-bit and 64-bit Office versions have a conflict.

**Note:** For more information on the Office Customization Tool, refer to <https://docs.microsoft.com/en-us/deployoffice/overview-of-the-office-customization-tool-for-click-to-run>



#### 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 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 Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\ODT**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\ODT** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. 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. 2. Open Internet Explorer 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 previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, select **Current Channel** and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. 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**. 8. 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**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\ODT**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Deploy Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\ODT**. 5. Type **setup.exe /configure newconfiguration.xml**. 6. Press Enter. 7. Office will begin the installation. 8. Click **Close**. |
| Update Microsoft 365 Apps | 1. Click **Start**. 2. Select **Word**. 3. Click **Blank document**. 4. Click **File**. 5. Click **Account**. 6. Click **Update Options**. 7. Click **Update Now**.   **Note:** Microsoft 365 Apps will download the updates and apply the updates from the CDN.   1. 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.   1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column record the version number of the current month. 3. Click **File**. 4. Click **Account**. 5. Compare the **Office Updates Version and Build Number** to the version recorded of the current month. 6. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update Channel**, select the **Version** and **Build** that is currently installed. 3. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 6. Save the file to **C:\ODT**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /configure removeaccess.xml**. 9. Press Enter. 10. Office will begin the installation. 11. Click **Close**.   **Note:** The Microsoft Access icon will not be displayed during the installation. |
| Add a Language to Microsoft 365 Apps | 1. 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**.**   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\ODT**. 6. Back in CMD, type **setup.exe /configure addspanish.xml**. 7. Press Enter. 8. Office will begin the installation. 9. Click **Close**. 10. Type **Control Panel** inthe “Type here to search” and press Enter. 11. Click on **Programs**. 12. Click on **Programs and Features**. 13. **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 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 | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\Packages\MC**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\Packages\MC** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. 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. 2. Open Internet Explorer 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 previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options,** select **Local source** and specify the **Source path** as **\\CLIENT2\MC** and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. 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**. 8. 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**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\Packages\MC**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Download Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\Packages\MC**. 5. Type **setup.exe /download newconfiguration.xml**. 6. Press Enter. Office will begin the download. |
| Deploy Microsoft 365 Apps (Offline from a Local Share) | 1. Back in CMD, type **setup.exe /configure newconfiguration.xml**. 2. Press Enter. 3. Office will begin the installation. Click **Close**. |
| Update Microsoft 365 Apps (Offline from a Local Share) | 1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. 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.   1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is for the current month. 3. Under **Update and upgrade**, under **Update and upgrade options**, select **Local source** and specify the **Source path** as **\\CLIENT2\MC**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **update.xml** and click **Export**. 6. Save the file to **C:\Packages\MC**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /download update.xml**. 9. Press Enter. Office will begin the download. 10. Back in CMD, type **setup.exe /configure update.xml**. 11. Press Enter. 12. Office will begin the installation. Click **Close**. 13. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 14. In the **Current Channel** Column, record the version number of the current month. 15. In Word, **File | Account**, compare the **Office Updates Version and Build Number** to the version recorded of the current month. 16. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 7. Back in CMD, type **setup.exe /configure removeaccess.xml**. 8. Press Enter. 9. Office will begin the installation. 10. 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) | 1. 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.   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. Back in CMD, type **setup.exe /download addspanish.xml**. 7. Press Enter. Office will begin the download. 8. Back in CMD, type **setup.exe /configure addspanish.xml**. 9. Office will begin the installation. 10. Click **Close**. 11. Type **Control Panel** inthe “Type here to search” and press Enter. 12. Click on **Programs**. 13. Click on **Programs and Features**. 14. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed. |

#### 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 Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\ODT**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\ODT** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. 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. 2. Open Internet Explorer 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 previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. 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**. 8. 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**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\ODT**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Deploy Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\ODT**. 5. Type **setup.exe /configure newconfiguration.xml**. 6. Press Enter. 7. Office will begin the installation. 8. Click **Close**. |
| Update Microsoft 365 Apps | 1. Click **Start**. 2. Select **Word**. 3. Click **Blank document**. 4. Click **File**. 5. Click **Account**. 6. Click **Update Options**. 7. Click **Update Now**.   **Note:** Microsoft 365 Apps will download the updates and apply the updates from the CDN.   1. 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.   1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column record the version number of the current month. 3. Click **File**. 4. Click **Account**. 5. Compare the **Office Updates Version and Build Number** to the version recorded of the current month. 6. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is currently installed. 3. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 6. Save the file to **C:\ODT**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /configure removeaccess.xml**. 9. Press Enter. 10. Office will begin the installation. 11. Click **Close**.   **Note:** The Microsoft Access icon will not be displayed during the installation. |
| Add a Language to Microsoft 365 Apps | 1. 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**.**   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\ODT**. 6. Back in CMD, type **setup.exe /configure addspanish.xml**. 7. Press Enter. 8. Office will begin the installation. 9. Click **Close**. 10. Type **Control Panel** inthe “Type here to search” and press Enter. 11. Click on **Programs**. 12. Click on **Programs and Features**. 13. **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 | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\Packages\MC**. |
| Extract ODT | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\Packages\MC** and click **OK**. 4. Click **OK** after successful Extraction. |
| Create Installation XML | 1. 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. 2. Open Internet Explorer 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 previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, ensure that **Current Channel** is selected and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options,** select **Local source** and specify the **Source path** as **\\CLIENT4\MC** and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, ensure that **Office Content Delivery Network (CDN)** is selected. 7. 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**. 8. 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**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\Packages\MC**. 14. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings |
| Download Microsoft 365 Apps | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\Packages\MC**. 5. Type **setup.exe /download newconfiguration.xml**. 6. Press Enter. Office will begin the download. |
| Deploy Microsoft 365 Apps (Offline from a Local Share) | 1. Back in CMD, type **setup.exe /configure newconfiguration.xml**. 2. Press Enter. 3. Office will begin the installation. Click **Close**. |
| Update Microsoft 365 Apps (Offline from a Local Share) | 1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. 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.   1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Update channel**, select the **Version** and **Build** that is for the current month. 3. Under **Update and upgrade**, under **Update and upgrade** options, select **Local source** and specify the **Source path** as **\\CLIENT4\MC**. 4. Click **Export** and select **Keep Current Settings** and then click **OK**. 5. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **update.xml** and click **Export**. 6. Save the file to **C:\Packages\MC**. 7. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 8. Back in CMD, type **setup.exe /download update.xml**. 9. Press Enter. Office will begin the download. 10. Back in CMD, type **setup.exe /configure update.xml**. 11. Press Enter. 12. Office will begin the installation. Click **Close**. 13. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 14. In the **Current Channel** Column, record the version number of the current month. 15. In Word, **File | Account**, compare the **Office Updates Version and Build Number** to the version recorded of the current month. 16. Close Word. |
| Remove an Application from Microsoft 365 Apps | 1. Go back to the already opened https://config.office.com/deploymentsettings 2. Under **Products and releases**, under **Apps**, turn OFF the slider for **Access**. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **removeaccess.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. DO NOT CLOSE the already opened https://config.office.com/deploymentsettings 7. Back in CMD, type **setup.exe /configure removeaccess.xml**. 8. Press Enter. 9. Office will begin the installation. 10. 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) | 1. 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.   1. Under **Language**, under **Languages**, select **Spanish (Spain, International Sort)** for additional languages and click **Add/Update**. 2. Under **Installation**, under **Installation options**, ensure that **Fallback to the CDN for missing languages** is selected. 3. Click **Export** and select **Keep Current Settings** and then click **OK**. 4. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **addspanish.xml** and click **Export**. 5. Save the file to **C:\Packages\MC**. 6. Back in CMD, type **setup.exe /download addspanish.xml**. 7. Press Enter. Office will begin the download. 8. Back in CMD, type **setup.exe /configure addspanish.xml** and press Enter. 9. Office will begin the installation. 10. Click **Close**. 11. Type **Control Panel** inthe “Type here to search” and press Enter. 12. Click on **Programs**. 13. Click on **Programs and Features**. 14. **Microsoft 365 Apps** for **English** and **Spanish** will be displayed. |

Enterprise Managed Deployment of Microsoft 365 Apps

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



#### Enterprise Managed Deployment of Microsoft 365 Apps using Configuration Manager

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps on the CM1 virtual machine.** | |
| Create a Share for Microsoft 365 Apps Package and Updates | 1. Open Internet Explorer and browse to the URL below. <https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date> 2. In the **Current Channel** Column, record the version number of the current and previous month. 3. Logon to CM1 as (corp\labadmin). 4. 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 | 1. In the Configuration Manager Console, browse to **Administration | Client Settings**. 2. Double-click on **Default Client Settings**. 3. Select **Software Updates**. 4. For **Enable management of the Office 365 Client Agent**, from the drop-down box select **Yes**. 5. Click **OK**. | |
| Enable and Configure Microsoft 365 Apps Software Updates | 1. Select **Administration**. 2. Expand **Site Configuration**. 3. Select **Sites**. 4. Click **Settings |** **Configure Site Components | Software Update Point**. 5. Under the **Classifications** tab, uncheck all options and only select **Updates**. 6. Under the **Products** tab, uncheck all options and only select **Office 365 Client**.   **Note:** If **Office 365 Client** is not listed, execute a full synchronization of updates and repeat above steps.   1. Under the **Languages** tab, uncheck all options and only select **English**. 2. Click **Apply | OK**. 3. Browse to **Software Library**. 4. Expand **Office 365 Client Management**. 5. Click **Office 365 Updates**. 6. Click **Synchronize Software Updates**. Click **Yes**.   **Note:** Please be patient for the sync to complete, which will take some time. | |
| Create a Folder and a Collection | 1. Browse to **Assets and Compliance | Device Collections**. Right-click **Device Collections** and click **Folder | Create Folder**. 2. Enter a name **Microsoft 365 Apps** and click **OK**. 3. Expand **Device Collections**, right-click **Microsoft 365 Apps** folder and click **Create Device Collection**. 4. Enter a name **Microsoft 365 Apps MC**. Click **Browse**. 5. Under **Device Collections**, select **Root**, select **All Systems** and click **OK**. 6. On the General page, click **Next**. 7. On the Membership Rules page, click **Next**. Click **OK** on the Configuration Manager prompt. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. 10. Browse to **Assets and Compliance | Devices**, right-click on the **CLIENT2** virtual machine, click **Add Selected Items** and then click **Add Selected Items to Existing Device Collection**. 11. Under **Device Collections**, select **Microsoft 365 Apps**, select **Microsoft 365 Apps MC** and click **OK**. 12. Under **Device Collections | Microsoft 365 Apps**, right-click on **Microsoft 365 Apps MC** 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 | 1. Click **Software Library**. 2. Click **Office 365 Client Management** and click **Office 365 Installer**. 3. Specify the following on the Application Settings Page, and click **Next**.   Name: **Microsoft 365 Apps MC**  Content Location: **\\CM1\Packages$\OfficeConfigMan**   1. On the Office Settings page, click **Go to the Office Customization Tool**. 2. On the Deployment settings page, enter the following and click **Next**: 3. Under **Products and releases**, under **Architecture**, select **64-bit**. 4. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 5. 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**. 6. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 7. Under **Installation**, click **Next**. 8. Under **Update and upgrade**, ensure that **Uninstall any MSI versions of Office, including Visio and Project** is turned ON and then click **Next**. 9. 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**. 10. Under **General**, click **Next**. 11. Under **Application preferences**, click **Finish**. 12. Click **Review**, select **Keep Current Settings**, click **OK**, review the details and click **Submit**. 13. On the Deployment page, select **Yes** and click **Next**. 14. On the General page, click **Browse…** next to Collection. 15. Under **Device Collections | Microsoft 365 Apps**, select **Microsoft 365 Apps MC** and click **OK**. 16. Select **Automatically distribute content for dependencies** and click **Next**. 17. On the Content page, click **Add | Distribution Point**. 18. Select **CM1.CORP.CONTOSO.COM** and click **OK**. 19. Click **Next**. 20. On the Deployment Settings page, specify the following and click **Next**.   Action: **Install**  Purpose: **Required**  Other 4 Checkboxes: **Unchecked**   1. On the Scheduling page, select **As soon as possible after the available time** and click **Next**. No other checkboxes to be selected. 2. On the User Experience page, select **Display in Software Center and show all notifications**, check all the **4 checkboxes** below and click **Next**. 3. On the Alerts page, click **Next**. No checkboxes to be selected. 4. On the Summary page, click **Next**. 5. On the Completion page, 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 | 1. In the Configuration Manager Properties, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 2. Select **Application Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 3. After a few minutes, the package will start downloading and installing after a notification. 4. The installation of the package can be validated in the **Programs and Features** once installed. 5. 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 2002 to identify devices with high confidence that are ready to upgrade to Microsoft 365 Apps. 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 **Office 365 ProPlus Upgrade Readiness**. There are few prerequisites that need to be in place.   1. Hardware inventory must be enabled in the client settings. To verify, in the Configuration Manager Console, browse to **Administration | 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 ProPlus Configurations**, **Office add-ins**, **Office document metrics** and **Office VBA scan summary** are selected. 2. 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 [https://docs.microsoft.com/en-us/configmgr/sum/deploy-use/office-365-dashboard#bkmk\_o365\_readiness](https://docs.microsoft.com/en-us/sccm/sum/deploy-use/office-365-dashboard#bkmk_o365_readiness)   1. To access the **Office 365 ProPlus Upgrade Readiness** tile, in the Configuration Manager Console, browse to **Software Library | Office 365 Client Management**. | |
| **Complete these steps on the CM1 virtual machine.** | | |
| Create and Deploy a Microsoft 365 Apps Software Update | 1. Once the sync is complete, browse to **Software Library |** **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**. 2. Enter a name **Microsoft 365 Apps MC Updates** and click **Create**. 3. Browse to **Software Library | Software Updates | Software Update Groups**. Select **Microsoft 365 Apps MC Updates** and click **Deploy** from the ribbon bar. 4. For the Collection, click **Browse…** 5. Under **Device Collections | Microsoft 365 Apps**, select **Microsoft 365 Apps MC** and click **OK**. 6. On the General page, click **Next**. 7. On the Deployment Settings page, specify the following and click **Next**.   Type of deployment: **Required**  Detail level: **Only success and error messages**  No other checkbox to be selected   1. On the Scheduling page, 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   1. On the User Experience page, specify the following and click **Next**.   User notifications: **Display in Software Center and show all notifications**  Under **Deadline behaviour**, check the box next to **Software updates installation**  No other checkbox to be selected   1. On the Alerts page, click **Next**. No checkboxes to be selected. 2. On the Deployment Package page, select **Create a new deployment package** and specify the following and click **Next**.   Name: **Microsoft 365 Apps MC Updates**  Package source: **\\CM1\Packages$\OfficeConfigManUpdates**   1. On the Distribution Points page, click **Add | Distribution Point**. 2. Select **CM1.CORP.CONTOSO.COM** and click **OK**. 3. On the Distribution Points page, click **Next**. 4. On the Download Location page, select **Download software updates from the Internet** and click **Next**. 5. On the Language Selection page, select **English (United States)** for **Office 365 Client Update** and click **Next**. 6. On the Download Settings page, 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**   1. On the Summary page, click **Next**. 2. On the Completion page, 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 | 1. In the Configuration Manager Properties, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 2. Select **Software Updates Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 3. Select **Software Updates Scan Cycle** and click **Run Now**. Click **OK**. 4. 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 **Hardware Inventory Cycle**, **Software Inventory Cycle** and **Software Updates Scan Cycle** on the clients to fasten the process.   1. The installation of the package can be validated in the **Programs and Features**. | |

#### Enterprise Managed Deployment of Microsoft 365 Apps using Microsoft Intune

| Task | Detailed Steps | |
| --- | --- | --- |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Add Microsoft 365 Apps | 1. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 6. In the Create app pane, under App type, select **Microsoft 365 Apps | Windows 10** and click **Select**. | |
| Configure and Deploy Microsoft 365 Apps | 1. Under **App suite information**, keep the default settings and click **Next**. 2. Under **Configure app suite**, enter/select the following and click **Next**: Leave the rest as default settings: 3. **Select Office apps**: Only select **Excel, OneDrive Desktop, OneNote 2016, Outlook, PowerPoint, Skype for Business,** and **Word** 4. **Update channel**: **Monthly** 5. **Accept the Microsoft Software License Terms on behalf of users**: **Yes** 6. **Languages**: **English** 7. Under **Assignments**, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 8. Under **Review + create**, review the page and click **Create**.   **Note:** This group should have already been created as part of **Section 2.2.1**. | |
| **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.   1. Click **Start | Settings**. 2. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 3. Click **Sync**. 4. The Microsoft 365 Apps will download and install automatically in the background, which can be seen from the **Task Manager**, **Details** tab. 5. The installation of the package can be validated in the **Programs and Features**. | |

Application Deployment and Management with Microsoft Intune



#### 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. Close all browser windows. 2. Start Internet Explorer InPrivate mode. 3. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 4. On the left navigation bar, click **All services > search and click Intune > Intune**. 5. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 6. In the **Create app** pane, under **App type**, select **Line-of-business app** and click **Select**. |
| Configure Line-of-Business App | 1. Under **App information**, click **Select app package file**. 2. 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> 3. Click **OK.** 4. Under **App information**, enter the following information and click **Next**:    1. **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.    2. **Description** - Enter a description for the app. The description is displayed to users in the company portal.    3. **Publisher** - Enter the name of the publisher of the app.    4. **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.    5. **Ignore app version** – Set this to “Yes” only for apps that are automatically updated by the app developer (such as Google Chrome).    6. **Command**-**line** **arguments** - Optionally, enter any command-line arguments that you want to apply to the .msi file when it runs, like /q.    7. **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.    8. **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.    9. **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.    10. **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.    11. **Developer** - Optionally, enter the name of the app developer.    12. **Owner** - Optionally, enter a name for the owner of this app, for example, HR department.    13. **Notes** - Enter any notes you would like to associate with this app.    14. **Logo** - Upload an icon that is associated with the app. The icon is displayed with the app when users browse the company portal. |

#### 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 **Assignments**, click **+ Add group** under **Required**, type **Sales**, select it and click **Select**. Click **Next**. 2. Under **Review + create**, review the page and click **Create**.   **Note:** This group should have already been created as part of **Section 2.2.1**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| User Experience with the Download and Installation of the App on the Client Side | 1. Click **Start | Settings**. 2. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 3. Click **Sync**. 4. The app will download and install automatically in the background. 5. The installation of the app can be validated in the **Programs and Features**. |



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>

#### 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 | 1. Browse to **C:\Packages**. 2. Create a **Folder** by the name **MSTeamsMSI**. 3. 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 | 1. In the Configuration Manager Console, browse to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and click **Create Device Collection**. 3. In the **General** page, enter the following and click **Next**:   Name: **Microsoft Teams MSI**  Click **Browse...**Select **All Systems**. Click **OK**   1. In the **Membership** Rules page, enter the following and click **Next**:   Click **Add Rule > Direct Rule**  Click **Next**  Enter **CLIENT2** and click **Next**  Select **CLIENT2** and click **Next**  Click **Next** and then click **Close**   1. In the **Summary** page, click **Next**. 2. In the **Completion** page, click **Close**. 3. Ensure that **CLIENT2** is in the **Microsoft Teams MSI** collection. |
| Create and Deploy the Microsoft Teams MSI Application | 1. Navigate to **Software Library > Application Management > Applications**. 2. Right-click **Applications** and click **Create Application**. 3. In the **General** page, enter the following and click **Next**:   Location: **\\CM1\Packages$\MSTeamsMSI\Teams\_windows\_x64.msi**   1. In the **Import Information** page, click **Next**. 2. In the **General Information** page, enter the following and click **Next**:   Installation program: **msiexec /i Teams\_windows\_x64.msi OPTIONS="noAutoStart=true" ALLUSERS=1**  Install behavior: **Install for system**   1. In the **Summary** page, click **Next**. 2. In the **Completion** page, click **Close**. 3. Now, right-click **Teams Machine-Wide Installer** and click **Deploy**. 4. In the **General** page, click **Browse...**under **Device Collections**, select **Microsoft Teams MSI** and click **OK**. 5. Click **Next**. 6. In the **Content** page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 7. In the **Deployment Settings** page, select the **Purpose** as **Required** and click **Next**. 8. In the **Scheduling** page, click **Next**. 9. In the **User Experience** page, click **Next**. 10. In the **Alerts** page, click **Next**. 11. In the **Summary** page, click **Next**. 12. In the **Completion** page, click **Close**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Retrieve Policies and Install Teams | 1. Launch the **Configuration Manager Client** applet from **Control Panel > System and Security**. 2. Go to the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 3. As soon as the notification appears click it to launch the **Software Center**. Observe the download and installation. 4. **IMPORTANT: Once the installation has been completed successfully, restart CLIENT2 once and re-login with CORP\LabAdmin.** 5. In a few moments, observe the **Microsoft Teams** icon on the desktop and the same will appear in the **Programs and Features**. |

#### 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 | 1. In the **C:\** drive, create a **Folder** by the name **MSTeamsMSI**. 2. 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 | 1. Start Internet Explorer InPrivate mode. 2. Navigate to <https://portal.azure.com> and sign in with **labadmin@<AzureDomainName>.onmicrosoft.com** 3. On the left navigation bar, click **All services > search and click Intune > Intune**. 4. In the navigation pane select **Client apps** > **Apps**, and click **+ Add**. 5. In the Create app pane, under App type, select **Other | Line-of-business app** and click **Select**. 6. Under the **App information** tab, click **Select app package file**, **browse** to **C:\MSTeamsMSI\ Teams\_windows\_x64.msi**, click **Open**, click **OK**. 7. Under the **App information** tab, enter the following details and click **Next**:  * Publisher: **Microsoft**  1. Under the **Assignments** tab, enter the following details and click **Next**:  * Under **Required**, click **+ Add group** * Type **Sales**, select it and click **Select**  1. Under the **Review + create** tab, 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.   1. Click **Start | Settings**. 2. Click **Accounts | Access work or school | Connected to <Azure Domain> Azure AD | Info**. 3. Click **Sync**. 4. After a moment, a **Teams Installer** folder will be created in **C:\Program Files (x86)**. 5. **IMPORTANT: Restart CLIENT3 once and re-login with TU1 credentials.** 6. 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**. |

Deploy and manage the new Microsoft Edge

The new Microsoft Edge enhances and extends the browser experience. It runs on Windows, macOS, iOS and Android devices. In this section, we will perform the following core scenarios:

* Deploy and Update Edge
* Deploy Edge using Configuration Manager
* Deploy Edge Updates using Configuration Manager
* Configure and Deploy Edge Policies using On-Premises Method
* Deploy Edge using Intune
* Configure and Deploy Edge Policies using Intune
* IE Mode
* Configure and Deploy IE Mode using On-Premises Method
* Configure and Deploy IE Mode using Intune
* Application Guard
* Setup Enterprise New Tab Page
* Configure and Deploy Enterprise New Tab using On-Premises Method
* Configure and Deploy Enterprise New Tab using Intune
* Access Microsoft Edge Legacy after installing the new version of Microsoft Edge (Side-by-Side)

#### Deploy and Update Edge

In this section, we will perform the following scenarios:

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

#### Deploy Edge using Configuration Manager

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

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT1 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 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 | 1. Launch the Configuration Manager console and navigate to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. On the General page, specify the following and click **Next**:   Name: **Edge Clients**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule > Direct Rule**. On the Welcome page click **Next**. On the Search for Resources page, enter **%CLIENT1%** next to Value and click **Next**. On the Select Resources page, select **CLIENT1** and click **Next**. On the Summary page, click **Next**. On the Completion page, click **Close**. 2. Back on the Membership Rules page, click **Next**. 3. On the Summary page, click **Next**. 4. On the Completion page, click **Close**. 5. Ensure that the **Edge Clients** collection has **CLIENT1** in it. |
| Create the Microsoft Edge Application and Deployment | 1. Navigate to **Software Library > Microsoft Edge Management**. 2. Right-click **Microsoft Edge Management** and select **Create Microsoft Edge Application**. 3. In the Application Settings page, specify a Name - **Edge App** and Content Location - **\\CM1\Packages$\Edge** and then click **Next**. 4. In the Specify settings for Microsoft Edge client page, for Channel select **Stable** and select **Specific Version**. In the Specific Version, select the **lowest possible version as we will be updating it later**. Click **Next**.   **Note:** Make a note of the lowest and latest possible versions from the drop-down list.   1. On the Deployment page, select **Yes** and click **Next**. 2. On the General page, select **Edge Clients** next to Collection which comes under the category of **Device Collections** and click **Next**. 3. On the Content page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 4. On the Deployment Settings page, ensure **Install** is selected next to Action and select **Available** next to Purpose. Click **Next**. 5. On the Scheduling page, click **Next**. 6. On the User Experience page, select **Display in Software Center and show all notifications** next to User notifications and click **Next**. 7. On the Alerts page, click **Next**. 8. On the Summary page, click **Next**. 9. On the Completion page, click **Close**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge | 1. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 2. 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. 3. As soon as the notification appears, click on the **notification or launch Software Center**. 4. Select **Edge App** under Applications and click **Install**. 5. Once the installation is completed, notice the **new Microsoft Edge icon on the desktop**. |

#### Deploy Edge Updates using Configuration Manager

| 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 **EdgeUpdates**. |
| Configure Software Update Point | 1. Launch the Configuration Manager console and navigate to **Administration > Site Configuration > Sites**. 2. Right-click the site and select **Configure Site Components > Software Update Point**. 3. Click the **Classifications** tab, **uncheck all the boxes** and only select **Updates**. 4. Click the **Products** tab, **uncheck all the boxes** and only select **Microsoft Edge** under **Windows**. 5. Click the **Languages** tab, ensure and only select **English**. If other languages are selected, deselect them all. Click **Apply** and **OK**. 6. Navigate to **Software Library > Microsoft Edge Management > All Microsoft Edge Updates** and click **Synchronize Software Updates** and click **Yes**.   **Note:** Synchronization can take up to an hour or so.   1. Once the synchronization has completed, refresh the **All Microsoft Edge Updates** to view the metadata. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Refresh Policies | 1. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 2. Click the **Actions** tab and select **all the actions** one by one and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process so that update shows in **Required** state. It could take up to an hour or so for the update to be detected in **Required** state. |
| **Complete these steps on the CM1 virtual machine.** | |
| Configure and Deploy Microsoft Edge Updates | 1. In the **All Microsoft Edge Updates** pane, in order to view the Title of the update, right-click in the **heading panel** and enable **Title**. 2. Sort out the updates based on **Stable**, **Dev** and **Beta** by clicking on the **Title header**. 3. Since you took a note of the lowest and latest possible versions from the drop-down list previously, look for the **latest Stable version** in the list and select both the **x86** and **x64** of that version (Ctrl and select to select multiple versions). 4. From the ribbon bar, click **Deploy**. 5. On the General page, for the Deployment Name, enter **Edge Stable Updates**, for the Collection, select **Edge Clients** and then click **Next**. 6. On the Deployment Settings page, keep the defaults and click **Next**. 7. On the Scheduling page, select **As soon as possible** under Installation deadline and click **Next**. 8. On the User Experience page, keep the defaults and click **Next**. 9. On the Alerts page, keep the defaults and click **Next**. 10. On the Deployment Package page, select **Create a new deployment package**, enter the Name - **Edge Stable Updates**, enter the Package source - **\\CM1\Packages$\EdgeUpdates** and then click **Next**. 11. On the Distribution Points page, click **Add > Distribution Point**, select **CM1.CORP.CONTOSO.COM**, click **OK** and then click **Next**. 12. On the Download Location page, keep the defaults and click **Next**. 13. On the Language Selection page, select **Windows Update** and click **Next**. 14. On the Download Settings page, select **Download software updates from distribution point and install** under Deployment options and then click **Next**. 15. On the Summary page, review and click **Next**. 16. On the Completion page, click **Close**. 17. Navigate to **Software Library > 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. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge Updates | 1. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 2. Click the **Actions** tab and select **all the actions** one by one and click **Run Now** for each. Click **OK** on each prompt. This is only required to trigger the process. 3. As soon as the notification appears, click on the **notification or launch Software Center**. 4. Notice that the update gets **downloaded and installed**. 5. Once the installation is completed, launch **Control Panel > Programs > Programs and Features** and notice that the **Microsoft Edge version has been updated**. |

#### Configure and Deploy 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 Internet Explorer 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.zip** file to the **desktop** and click **Close** and close Internet Explorer. 3. Right-click **MicrosoftEdgePolicyTemplates.zip** and click **Extract All**. 4. Click **Extract**. 5. On the opened folder where the content has been extracted to, navigate to **windows > admx**. 6. 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. 7. 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 | 1. Launch the **Group Policy Management** console and navigate to **Forest: corp.contoso.com > Domains > corp.contoso.com**. 2. Right-click **corp.contoso.com** and click **Create a GPO in this domain, and Link it here...** 3. Specify the Name - **Microsoft Edge Policies** and click **OK**. 4. Right-click **Microsoft Edge Policies** and click **Edit...** 5. Navigate to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Default search provider**. 6. Double-click **Enable the default search provider**, select **Enabled**, click **Apply** and **OK**. 7. Double-click **Default search provider name**, select **Enabled**, under Default search provider name, enter **Google** and then click **Apply** and **OK**. 8. Close all the windows. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Verify Microsoft Edge Policies | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. Launch the new Microsoft Edge and in the address bar type **edge://policy** and press enter. 4. Notice the **2 policies** that have been enabled and configured. The same can be noticed in **HKLM\SOFTWARE\Policies\Microsoft\Edge**. |

#### Deploy Edge using Intune

In this section, we will deploy Edge using Intune, which is the Cloud solution.

| 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 | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **Azure Active Directory** and then click **Groups**. 3. Under All groups, click **+ New group**. 4. 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 | 1. Navigate to <https://devicemanagement.microsoft.com> which is the **Microsoft Endpoint Manager Admin Center** and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. Select **Apps > All apps > + Add**. 3. Under Microsoft Edge, version 77 and later, select **Windows 10** and then click **Select**. 4. On the App information tab, keep all defaults and click **Next**. 5. On the App settings tab, select **Stable** next to Channel. Note the new Logo. Click **Next**. 6. On the Assignments tab, under Required, click **+ Add group**. Select **EdgePoC** and then click **Select**. Click **Next**. 7. On the Review + create tab, click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. 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.** |

#### Configure and Deploy 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://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search for and click Intune**. 3. Click **Device configuration > Profiles**. 4. Click **+ Create profile**. 5. Select the following and click **Create**:   Platform: **Windows 10 and later**  Profile: **Administrative Templates**   1. On the Basics tab, enter **Microsoft Edge Policies** next to **Name** and click **Next**. 2. On the Configuration settings tab, navigate to **Computer Configuration > Microsoft Edge > Default search provider** and click the policy **Enable the default search provider**. Select **Enabled** and click **OK**. 3. Now click the policy - **Default search provider name**. Select **Enabled** and under Default search provider name, enter **Google**. Click **OK**. 4. On the Configuration settings tab. Click **Next**. 5. On the Scopes tags tab, click **Next**. 6. On the Assignments tab, click **Select groups to include**, select **EdgePoC** and click **Select**. Click **Next**. 7. On the Review + create tab, review the settings and click **Create**. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify Microsoft Edge Policies | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. Once the sync has completed, after sometime, launch the new Microsoft Edge and in the address bar type **edge://policy** and press enter. 5. Notice the **2 policies** that have been enabled and configured. The same can be noticed in **HKLM\SOFTWARE\Policies\Microsoft\Edge**. |

#### 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

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

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the APP1 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-clickon **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 | 1. On the taskbar, open **File Explorer** and browse to **C:\Packages\Sources**. 2. Copy the **ContosoLearning** folder to **C:\inetpub\wwwroot**. Accept the prompt. 3. On the Start menu, open **Internet Information Services (IIS) Manager**. 4. Under the **Connections** pane, browse to **APP1 (Corp\LabAdmin) > Sites > Default Web Site > ContosoLearning**. 5. Right-click on **ContosoLearning** and select **Convert to Application**. 6. On the Add Application window, click **OK**. 7. On **ContosoLearning**, under the **Actions** pane select **Advanced Settings.** 8. On the Advanced Settings window, select **Application Pool** and click on the **ellipses (…)**. 9. On the Select Application Pool window, set the **Application pool** to **.NET v2.0** then click **OK**. 10. On the Advanced Settings window, click **OK**. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Pin Internet Explorer on the Taskbar | 1. On the **Start** Menu, search for **Internet Explorer**. 2. Right-click on **Internet Explorer** and select **Pin to taskbar**. |
| Download Enterprise Mode Site List Manager | 1. Open Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49974>   1. From the website, click **Download**. 2. Save **EMIESiteListManager.msi** to **C:\Packages** after creating a folder called **Packages** in **C:\**. |
| Install Enterprise Mode Site List Manager | 1. On the taskbar, open **File Explorer** and browse to **C:\Packages**. 2. Double-click on **EMIESiteListManager.msi**. 3. On the Welcome page, click **Next**. 4. On the End-User License Agreement page, select **I accept the terms in the License Agreement** and then click **Next**. 5. On the Destination Folder page, click **Next**. 6. On the Ready to Install page, click **Install**. Accept the UAC prompt if required. 7. Once complete, click **Finish**. |
| Create a Site List | 1. From the desktop icon, open the **Enterprise Mode Site List Manager**. 2. On the Enterprise Mode Site List Manager for v.2 schema window, click **Add**. 3. On the Add new website window, under **URL** enter **app1/ContosoLearning** and select **IE8 Document Mode** next to **Compat Mode** and then click **Save**. 4. Click on **File >** **Save to XML**. 5. **Save** the file to **\\APP1\EMEI** as **EMEISiteList.xml**. |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure and Deploy IE Mode 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**. 4. Look for the policy - **Configure Internet Explorer integration** and double-click it. 5. Select **Enabled** and under Options, select **Internet Explorer mode**. Click **Apply** and **OK**. 6. Now look for the policy - **Configure the Enterprise Mode Site List** and double-click it. 7. Select **Enabled** and under Options, enter **\\APP1\EMEI\EMEISiteList.xml**. Click **Apply** and **OK**. 8. Close all the windows. |
| **Complete these steps on the CLIENT1 virtual machine.** | |
| Verify IE Mode Policies | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. First launch **IE11** and in the address bar type **http://app1/ContosoLearning** and press enter. 4. Note the warning "**Your browser is not supported by ContosoLearning. Only Internet Explorer is Supported**". 5. Now launch the new **Microsoft Edge** and in the address bar type **http://app1/ContosoLearning** and press enter. 6. 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**. |

#### Configure and Deploy IE Mode using Intune

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the APP1 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 **APP1 (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://APP1/ContosoLearning/EMEISiteList.xml**. |
| **Complete these steps from an Internet-Connected Windows computer.** | |
| Configure and Deploy IE Mode Policies | 1. Navigate to <https://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search for and click Intune**. 3. Click **Device configuration > Profiles**. 4. Click **Microsoft Edge Policies** and click **Properties**. 5. Click **Edit** next to **Configuration settings**. 6. 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**. 7. 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://APP1/ContosoLearning/EMEISiteList.xml** and click **OK**. 8. Click **Review + save** at the bottom and then click **Save** again. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify IE Mode Policies | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. First launch **IE11** and in the address bar type **http://app1/ContosoLearning** and press enter. 5. Note the warning "**Your browser is not supported by ContosoLearning. Only Internet Explorer is Supported**". 6. Once the sync has completed, after sometime, launch the new **Microsoft Edge**. 7. In the address bar type **http://app1/ContosoLearning** and press enter. 8. 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**. |

#### Application Guard

First perform the prerequisites in **Section 4.2 - Security and Compliance (Steps 1-20)**, then perform **Section 4.2.5 - Windows Defender Application Guard**.

#### 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

#### 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 **http://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 **http://www.bing.com** and **http://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 | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. 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**. 4. Now start a **new tab**. Notice that **Microsoft's** website opens up. |

#### 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://portal.azure.com> and Sign in with **labadmin@<AzureDomainName>.onmicrosoft.com**. 2. From the left navigation bar, click **All services > search for and click Intune**. 3. Click **Device configuration > Profiles**. 4. Click **Microsoft Edge Policies** and click **Properties**. 5. Click **Edit** next to **Configuration settings**. 6. 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 **http://www.microsoft.com** and click **OK**. 7. 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**. 8. 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 **http://www.bing.com** and **http://www.google.com** and click **OK**. 9. 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**. 10. Click **Review + save** at the bottom and then click **Save** again. |
| **Complete these steps on the CLIENT3 virtual machine.** | |
| Verify Enterprise New Tab Policies | 1. Click **Start > Settings > Accounts > Access work or school**. 2. Select **Connected to <AzureDomain>'s Azure AD** and click **Info**. 3. Click **Sync**. 4. Once the sync has completed, after sometime, launch the new **Microsoft Edge**. 5. 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**. 6. Now start a **new tab**. Notice that **Microsoft's** website opens up. |

#### Access Microsoft Edge Legacy after installing the new version of Microsoft Edge (Side-by-Side)

In this section, we will access Microsoft Edge Legacy after installing the new version of Microsoft Edge.

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps on the CLIENT2 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 on the CM1 virtual machine.** | |
| Create a Device Collection | 1. Launch the Configuration Manager console and navigate to **Assets and Compliance > Device Collections**. 2. Right-click **Device Collections** and select **Create Device Collection**. 3. On the General page, specify the following and click **Next**:   Name: **Edge Clients (Side-by-Side)**  Limiting collection: **All Systems**   1. On the Membership Rules page, click **Add Rule > Direct Rule**. On the Welcome page click **Next**. On the Search for Resources page, enter **%CLIENT2%** next to Value and click **Next**. On the Select Resources page, select **CLIENT2** and click **Next**. On the Summary page, click **Next**. On the Completion page, click **Close**. 2. Back on the Membership Rules page, click **Next**. 3. On the Summary page, click **Next**. 4. On the Completion page, click **Close**. 5. Ensure that the **Edge Clients (Side-by-Side)** collection has **CLIENT2** in it. |
| **Complete these steps on the DC1 virtual machine.** | |
| Configure and Deploy the Side-by-Side Browser Experience Policy | 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 Update > Applications**. 4. Look for the policy – **Allow Microsoft Edge Side by Side browser experience** and double-click it. 5. Select **Enabled**. Click **Apply** and **OK**. 6. Close all the windows. |
| **Complete these steps on the CM1 virtual machine.** | |
| Deploy the Microsoft Edge Application previously created to the New Collection | 1. Navigate to **Software Library > Application Management > Applications**. 2. Right-click **Edge App** and click **Deploy**. 3. On the General page, select **Edge Clients (Side-by-Side)** next to Collection which comes under the category of **Device Collections** and click **Next**. 4. On the Content page, click **Next**. 5. On the Deployment Settings page, ensure **Install** is selected next to Action and select **Available** next to Purpose. Click **Next**. 6. On the Scheduling page, click **Next**. 7. On the User Experience page, select **Display in Software Center and show all notifications** next to User notifications and click **Next**. 8. On the Alerts page, click **Next**. 9. On the Summary page, click **Next**. 10. On the Completion page, click **Close**. |
| **Complete these steps on the CLIENT2 virtual machine.** | |
| Retrieve Policies and Install Microsoft Edge (Side-by-Side) | 1. Launch an administrative command prompt window. 2. Run the command **gpupdate /force**. 3. Launch the **Configuration Manager applet** from **Control Panel > System and Security**. 4. 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. 5. As soon as the notification appears, click on the **notification or launch Software Center**. 6. Select **Edge App** under Applications and click **Install**. 7. Once the installation is completed, notice the **new Microsoft Edge icon on the desktop along with the old Microsoft Edge**. |

* 1. Office and Windows as a Service

In this module, you will go through how to manage Windows as a Service (WaaS) and setting up deployment rings using Group Policy.

In the first two sections, we demonstrate how to manage updates using Windows Update for Business. You can use Group Policy or MDM solutions such as Intune to configure the Windows Update for Business settings that control how and when Windows 10 devices are updated. In addition, we take you through the option of using Intune to manage non-domain-joined devices.

We then move to using Configuration Manager to create a servicing plan, including update and deferral policies similar to Windows Update for Business policies above. We also cover servicing Microsoft 365 using Configuration Manager.



Servicing Windows 10 with Microsoft Intune



#### Configure Software Updates

In this activity, you will configure and manage **Windows 10 Update Rings** in Intune to form deployment rings and ensure that Windows 10 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 10 updates get installed. For more details see [Manage software updates in Intune.](https://docs.microsoft.com/en-us/intune/windows-update-for-business-configure)

| Task | Detailed Steps |
| --- | --- |
| **Complete these steps from an internet-connected Windows computer.** | |
| Create Ring Policy | 1. In Intune, navigate to **Software updates > Windows 10 update rings**. Click “**+ Create profile**” to create an Update Ring policy. 2. In the **Basics** tab, enter a **Name**, a **Description** (optional), and then click **Next**. 3. In the **Update ring settings** tab, enter the following information and then click **Next**:    * **Servicing channel**: Set the channel from which the device receives Windows updates.    * **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.    * **Set feature update uninstall period (2 – 60 days): Enter the number of days within which Feature Updates can be uninstalled.**    * **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](https://docs.microsoft.com/windows/client-management/mdm/policy-configuration-service-provider#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**    * **Option to check for Windows updates**    * **Require user approval to dismiss restart notification**    * **Remind user prior to required auto-restart with dismissible reminder (hours)**    * **Remind user prior to required auto-restart with permanent reminder (minutes)**    * **Change notification update level**    * **Use deadline settings** with **Deadline for feature updates**, **Deadline for quality updates**, **Grace period** and **Auto reboot before deadline** |
| Assign Ring | 1. In the **Assignments** tab, choose **+** **Select groups to include**, and then choose a group. 2. When finished, choose **Select | Next** to complete the assignment. 3. In the **Review + create** tab, click **Create**. |
| View Update Compliance | 1. Select **Software updates** > **Overview**. You can see information about the status of any update rings you assigned to devices and users.    * + Select **Software updates > Windows 10 update rings > Select the deployment ring > Overview**. You can see information about the status of the specific deployment ring you assigned to devices and users. |
| Pause Updates | 1. Select **Software updates** > **Windows 10 update rings > Select the deployment ring > Overview**. 2. Choose **Pause**. |
| Uninstall the Latest Software Updates | 1. In Intune, select **Software updates**. 2. Select **Windows 10 update rings > Select the deployment ring > Overview > Uninstall**. |

Servicing Windows 10 with Configuration Manager

Windows 10 delivers a new model for organizations to deploy and upgrade Windows by providing updates to features and capabilities through a continuous process. 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 10 machines are kept up to date.

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

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.









#### Configure Software Update Point

In this activity, you will configure the Software Update Point to download Windows 10 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 > Site Configuration >** **Sites**. 3. Right-click on **CHQ – Contoso Headquarters** and select **Configure Site Components >** **Software Update Point**. 4. On the **Classifications** tab, uncheck **Services Packs** and **Update Rollups** in case they are checked and then keep **Updates** selected (if it is selected from the previous lab) and check **Upgrades**. 5. On the **Windows 10 Servicing Prerequisite** window, click **OK**. 6. On the **Products** tab, uncheck everything and only check **Windows 10, version 1903 and later** and keep **Office 365 Client** selected (if it is selected from the previous lab). 7. On the **Languages** tab, uncheck everything and only check **English** (if not done before) then click **Apply** and **OK**. |
| Synchronize Software Update | 1. From the **Configuration Manager Console**, browse to **Software Library > Software Updates > All Software Updates**. 2. Click **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. |

#### Configure Servicing Plan

In this activity, you will configure Servicing Plans in Configuration Manager to form deployment rings and ensure that Windows 10 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 10 Feature Updates are Available | 1. From the **Configuration Manager Console**, browse to **Software Library > Windows 10 Servicing >** **All Windows 10 Updates**. 2. On the **Search** bar, type **Feature update to Windows 10 (business editions), version 2004, en-us x64** then press **Enter**. 3. Validate that the feature update metadata for **Feature update to Windows 10 (business editions), version 2004, en-us x64** is available and showing in a state of **“Required”**.   **Note:** It can take some time for the **WIN10-1909** machine to be detected in Configuration Manager for the **“Required”** update. Run **Hardware Inventory Cycle**, **Machine Policy Retrieval & Evaluation Cycle**, **Software Inventory Cycle**, **Software Updates Deployment Evaluation Cycle** and **Software Updates Scan Cycle** on the machine to fasten the process. |
| Create Servicing Collections | 1. From the **Configuration Manager Console**, browse to **Assets and Compliance**. 2. Right-click on **Device Collections** and select **Folder >** **Create Folder**. 3. On the **Configuration Manager** window, under **Folder name** enter **Windows 10 Servicing** then click **OK**. 4. From the **Configuration Manager Console**, expand **Device Collections** and right-click on **Windows 10 Servicing**. 5. Select **Create Device Collection**. 6. On the **General** page, enter the following then click **Next**.   Name: **Semi-Annual Channel**  Limiting Collection: **All Desktop and Server Clients**   1. On the **Membership Rules** page, click **Next**. 2. On the warning dialog box, click **OK**. 3. On the **Summary** page, click **Next**. 4. On the **Completion** page, click **Close**. |
| Create a Servicing Plan for Semi-Annual Channel Machines | 1. From the **Configuration Manager Console**, browse to **Software Library > Windows 10 Servicing > Servicing Plans**. 2. On the ribbon, click **Create Servicing Plan**. 3. On the **General** page, enter the following then click **Next**.   Name: **Semi-Annual Channel**   1. On the **Servicing Plan** page, enter the following then click **Next**.   Target Collection: **Semi-Annual Channel** (under Windows 10 Servicing folder)   1. On the **Deployment Ring** page, select **Semi-Annual Channel (Targeted)**, and then click **Next**.   **Note:** As per <https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-Update-for-Business-and-the-retirement-of-SAC-T/ba-p/339523>, **Semi-Annual Channel (Targeted)** has been retired and only **Semi-Annual Channel** will be used BUT at the moment (dated 7th June 2020), you will be able to preview this Feature Update only if you select **Semi-Annual Channel (Targeted)**. By the time you do this lab, you “may” find that you can preview with the selection of **Semi-Annual Channel**.   1. On the **Upgrades** page, select **Title** and click **items to find**. 2. On the **Search Text** window, in the textbox enter **“Feature update to Windows 10 (business editions), version 2004, en-us x64”** (include the quotation marks) then click **Add**. 3. On the **Search Text** window, click **OK**.   **Note:** As per <https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-Update-for-Business-and-the-retirement-of-SAC-T/ba-p/339523>, **Semi-Annual Channel (Targeted)** has been retired and only **Semi-Annual Channel** will be used BUT at the moment (dated 7th June 2020), you will be able to preview this Feature Update only if you select **Semi-Annual Channel (Targeted)**. By the time you do this lab, you “may” find that you can preview with the selection of **Semi-Annual Channel**.   1. On the **Upgrades** page, click **Preview**. 2. On the **Preview updates** window, verify that the **2004** feature update is listed then click **Close**. 3. On the **Upgrades** page, click **Next**. 4. On the **Deployment Schedule** page, under **Installation deadline** select **As soon as possible** then click **Next**. 5. On the **User Experience** page, under **User notifications** select **Display in Software Center and show all notifications**,under **Deadline behavior** select **System restart (if necessary)** and then click **Next**. 6. On the **Deployment Package** page, select **Create a new deployment package**, enter the following then click **Next**.   Name: **Semi-Annual Channel Package**  Package source: **\\CM1\Packages$\SACPackage**  **Note:** Create a folder called **SACPackage** in **C:\Packages**.   1. On the **Distribution Points** page, click **Add >** **Distribution Point**. 2. On the **Add Distribution Points** window, select **CM1.CORP.CONTOSO.COM** then click **OK**. 3. On the **Distribution Points** page, click **Next**. 4. On the **Download Location** page, click **Next**. 5. On the **Language Selection** page, click **Next**. 6. On the **Summary** page, click **Next**. 7. On the **Completion** page, click **Close**. |

#### Service a Windows 10 1909 Client

In this activity, you will test the servicing plan on a Windows 10 1909 virtual machine.

| 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 >** **Devices**. 2. Right-click on **WIN10-1909** and select **Add Selected Items >** **Add Selected Items to Existing Device Collection**. 3. On the **Select Collection** window, browse to and select **Root > Windows 10 Servicing >** **Semi-Annual Channel** then click **OK**. 4. On the **Configuration Manager Console**, browse to **Assets and Compliance > Device Collections > Windows 10 Servicing > Semi-Annual Channel**. 5. On the ribbon, click **Collection |** **Update Membership | Yes** and press **F5**. 6. Verify that the **WIN10-1909** machine is shown within the collection. |
| Force the Servicing Plan to Run | 1. From the **Configuration Manager Console**, browse to **Software Library > Windows 10 Servicing >** **Servicing Plans**. 2. Select **Semi-Annual Channel** and from the ribbon click **Run Now**. 3. On the dialog box, click **OK**. |
| **Complete these steps on the WIN10-1909 virtual machine.** | |
| Refresh the Client’s Policy | 1. Logon to **WIN10-1909** machine as **corp\labadmin**. 2. Open the **Control Panel**. 3. On the **All Control Panel Items** window, click on **Configuration Manager.** 4. On the **Configuration Manager Properties** window, go to the **Actions** tab. 5. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** then click **Run Now**. 6. On the dialog box, click **OK**. 7. On the **Actions** tab, select **Software Updates Scan Cycle** then click **Run Now**. 8. On the dialog box, click **OK**. 9. On the **Actions** tab, select **Software Updates Deployment Evaluation Cycle** then click **Run Now**. 10. On the dialog box, click **OK**. 11. On the **Configuration Manager Properties** window, click **OK**.   **Note:** Ensure that in **CM1**, 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**.   1. 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. 2. On the prompt, click **Restart** and then click **Restart** again for a force restart. 3. The upgrade process will continue. 4. Once restarted and logged in, the version of windows will be **Windows 10 Version 2004 (Build 19041.x)**. |

Servicing Microsoft 365 Apps with Configuration Manager

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

**Note:** This lab can only be performed if the Configuration Manager environment is on Current Branch.

#### 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.** | |
|  | 1. In the Configuration Manager console under the **Administration** node, choose **Site Configuration > Sites**. 2. Right-click on **CHQ – Contoso Headquarters** and select **Configure Site Components > Software Update Point**. 3. In the **Software Update Point Component Properties** dialog box, do the following:    1. On the **Products** tab, under **Office**, select **Office 365 Client** (if not already selected from the previous labs).    2. On the **Classifications** tab, select **Updates** (if not already selected from the previous labs).    3. Click **Apply** and **OK**.   You can have other checkboxes selected in the Products and Classifications tabs. But, **Office 365 Client** and **Updates** need to be selected for Configuration Manager to receive notifications when Microsoft 365 client update packages are available.   1. On the **Software Library** node, open **Office 365 Client Management** and right-click **Office 365 Updates** and select **Synchronize Software Updates.** 2. 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. |

#### 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 Office 2016 Administrative Template files (ADMX/ADML)   <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) | 1. Install **admintemplates\_x64\_<VersionNumber>\_en-us.exe** to temporary location. 2. **Copy** contents of **admx** folder in 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 10 ADMX files.  [Administrative Templates (.admx) for Windows 10 November 2019 Update (1909)](https://www.microsoft.com/en-us/download/100591) (Will have a link to latest ADMX files).  **Note:** Version number may change over time. |
| Enable Microsoft 365 Clients to receive Updates from ConfigMgr | 1. Open the Group Policy Management Console. 2. Create a policy called “**Microsoft 365 Client Management**". 3. Edit the “**Policy**”. 4. Enable the **Computer Configuration\Policies\Administrative Templates\Microsoft Office 2016 (Machine)\Updates\Management of Microsoft 365 Apps for enterprise** policy setting. 5. 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. |

#### 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 Internet Explorer and browse to the URL below.   <https://www.microsoft.com/en-us/download/details.aspx?id=49117>   1. From the website, click **Download**. 2. Save the installer to **C:\ODT**. | | |
| Extract ODT | | 1. Double-click to start the extraction of the ODT and accept the UAC prompt if required. 2. Accept the License Termsand click **Continue**. 3. Navigate to **C:\ODT** and click **OK**. 4. Click **OK** after successful Extraction. | | |
| Create Installation XML | | 1. 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. 2. Open Internet Explorer and browse to the URL below. [https://docs.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date](https://technet.microsoft.com/en-us/library/mt592918.aspx) 3. In the **Current Channel** Column, record the version number of the previous month. 4. Open Internet Explorer and browse to the URL below.   https://config.office.com/deploymentsettings   1. Under **Products and releases**, under **Architecture**, select **64-bit**. 2. Under **Products and releases**, under **Products**, select **Microsoft 365 Apps for enterprise** from the **Office Suites** dropdown. 3. Under **Products and releases**, under **Update channel**, select **Current Channel** and select the **Version** that was recorded earlier and click **Next**. 4. Under **Language**, under **Languages**, select **English (United States)** as the primary language and click **Next**. 5. Under **Installation**, under **Installation options**, ensure that **Office Content Delivery Network (CDN)** is selected and click **Next**. 6. Under **Update and upgrade**, under **Update and upgrade options**, select **Microsoft Endpoint Configuration Manager**. 7. 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**. 8. 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**. 9. Under **General**, click **Next**. 10. Under **Application preferences**, click **Finish**. 11. Click **Export** and select **Keep Current Settings** and then click **OK**. 12. Check the box next to **I accept the terms in the license agreement**, provide the **File Name** as **newconfiguration.xml** and click **Export**. 13. Save the file to **C:\ODT**. | | |
| Deploy Microsoft 365 Apps | | 1. Type **CMD** inthe “Type here to search”. 2. Right-click **Command Prompt**. 3. Select **Run as administrator**. Accept the UAC prompt if required. 4. Change directory to **C:\ODT**. 5. Type **setup.exe /configure newconfiguration.xml**. 6. Press Enter. 7. Office will begin the installation. 8. Click **Close**. | | |
| **Complete these steps on the CM1 virtual machine.** | | | |
| Validate that Microsoft 365 Apps Updates are Available | 1. From the **Configuration Manager Console**, browse to **Software Library > Office 365 Client Management >** **Office 365 Updates**. 2. Search for **the latest MC Version**. You should be able to see **the latest MC 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 **Hardware Inventory Cycle**, **Machine Policy Retrieval & Evaluation Cycle**, **Software Inventory Cycle**, **Software Updates Deployment Evaluation Cycle** and **Software Updates Scan Cycle** on the machines to fasten the process. | | |
| Create Servicing Collections | 1. From the **Configuration Manager Console**, browse to **Assets and Compliance**. 2. Right-click on **Device Collections** and select **Folder >** **Create Folder**. 3. On the **Configuration Manager** window, under **Folder name** enter **Microsoft 365 Apps Updates** then click **OK**. 4. From the **Configuration Manager Console**, expand **Device Collections** and right-click on **Microsoft 365 Apps Updates**. 5. Select **Create Device Collection**. 6. On the **General** page, enter the following then click **Next**.   Name: **Microsoft 365 Apps Current Channel**  Limiting Collection: **All Desktop and Server Clients**   1. On the **Membership Rules** page, click **Next**. 2. On the warning dialog box, click **OK**. 3. On the **Summary** page, click **Next**. 4. On the **Completion** page, click **Close**. | | | | |
| Add Devices to Collections | 1. Right-click **Microsoft 365 Apps Current Channel** collection and click **Add Resources.** 2. In the **Add Resources to Collection** enter **CLIENT1** or **CLIENT2** in the **Name string contains** field then click **Search**. 3. In the **Search results** box, select **CLIENT1** or **CLIENT2** and click **Add** then **OK**. | | | | |
| Create ADR for Current Channel | 1. Browse to **Software Library**. 2. Click on the **Office 365 Client Management** and then click **Create an ADR**. | | | | |
| General Page | | 1. 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 | | 1. Keep defaults and click **Next**. | | |
| Software Updates | | 1. Fill out as defined below and click **Next**:   **Product:** Office 365 Client  **Title:** “Office 365 Client Update…” (Full title of the update) | | |
| Evaluation Schedule | | 1. 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 | | 1. Fill out as defined below and click **Next**:   **Software available time:** As soon as possible  **Installation deadline:** As soon as possible | | |
| User Experience | | 1. Select **Display in Software Center and show all notifications** and click **Next**. | | |
| Alerts | | 1. Keep defaults and click **Next**. | | |
| Deployment Package | | 1. Fill out as defined below and click **Next**:   **Create a new deployment package:** Selected  **Name:** Microsoft 365 Apps Updates  **Package Source:** \\CM1\Packages$\Microsoft365AppsUpdates  **Note:** Create the folder beforehand. | | |
| Distribution Point | | 1. Fill out as defined below and click **Next**:   **Distribution Point Group:** Corp DPs | | |
| Download Location | | 1. Keep defaults and click **Next**. | | |
| Language Selection | | 1. Keep defaults and click **Next**. | | |
| Download Settings | | 1. Keep defaults and click **Next**. | | |
| Summary | | 1. Click **Next**. | | |
| Completion | | 1. Click **Close**. | | |
| Run ADRs | 1. Open **Software Updates\Automatic Deployment Rules**. 2. 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 | 1. In the **Configuration Manager Properties**, **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle** and click **Run Now**. Click **OK**. 2. Select **Software Updates Deployment Evaluation Cycle** and click **Run Now**. Click **OK**. 3. Select **Software Updates Scan Cycle** and click **Run Now**. Click **OK**. 4. The software update will start **Downloading** and **Installing**.   The installation of the package can be validated in the **Programs and Features**. | | | | |

Servicing Microsoft 365 Apps with Intune

In Intune, you can use [Windows 10 templates to configure group policy settings](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows). 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 templates to configure group policy settings](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows).

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](https://docs.microsoft.com/en-us/deployoffice/configure-update-settings-for-office-365-proplus) 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 | 1. In your [Intune administrative template](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows#create-the-template), go to the **Update Channel** setting, and enter the   channel you want. For example, choose **Current Channel**.   1. Be sure to [assign the policy](https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign) to your Windows 10 devices. To test your policy sooner, you   can also sync the policy:   * [Sync the policy in Intune](https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-sync) * [Manually sync the policy on the device](https://docs.microsoft.com/en-us/mem/intune/user-help/sync-your-device-manually-windows#sync-from-settings-app) | | |