**Module 2 – Upgrading and Updating Windows 11**

**Module Overview**

Most organizations have probably made the move from Windows 7 to Windows 10 sometime in the past seven years. This probably means that your organization, like many others, faces the decision of how best to move from Windows 10 to Windows 11.

If your existing inventory of desktop and laptop devices meet the minimum hardware requirements for Windows 11, you could consider performing an in-place upgrade to Windows 11. If the hardware doesn’t meet these requirements, then you might want to consider performing a migration to Windows 11. During the migration, your users’ settings and data (referred to as user state) are migrated to the a Windows 11 device.

After you’ve installed or upgraded to Windows 11, you’ll need to know how to maintain it. Part of this maintenance includes managing Windows updates. In this module, you’ll learn how to perform upgrades, how to migrate user state, and how to manage Windows 11 updates.

**Objectives**

After completing this module, you will be able to:

* Upgrade to Windows 11
* Migrate user state
* Manage Windows 11 updates

Lesson 1

**Upgrading to Windows 11**

You have two choices when considering an upgrade to Windows 11 from an earlier Windows operating system: perform an in-place upgrade, or migrate. The recommended approach is to perform an in-place upgrade. However, there are numerous reasons why that might not be the best strategy for your organization; and in some cases, an in-place upgrade is not possible. In this lesson, you’ll learn how to choose your upgrade strategy, and how to perform in-place upgrades and migrations.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Identify the supported upgrade paths to Windows 11.
* Compare in-place upgrades with migrations.
* Describe the process for performing an in-place upgrade to Windows 11.
* Describe the process for migrating to Windows 11.

**Supported upgrade paths**

Windows 7 is increasingly dated, and official support ended for this operating system in January 2020. However, many organizations still use Windows 7 on their on-premises computers. So, perhaps the first thing to know is that there’s no direct upgrade path from Windows 7 to Windows 11. In fact, you can only perform an in-place upgrade to Windows 11 from Windows 10.

Users of Windows 8 or Windows 8.1 must also plan for a migration to Windows 11.

If your Windows 7 computers do meet the requirements for Windows 11, and you don’t want to use a migration process, you can consider upgrading to Windows 10 and then upgrading to Windows 11. However, in these situations, a migration probably represents the easiest path to Windows 11.

The following table identifies the direct upgrade paths to Windows 11 that are currently supported. In the table, X indicates that a full in-place upgrade is supported, including user state and installed apps.

|  |  |  |  |
| --- | --- | --- | --- |
| Previous Windows edition | Windows 11 Home | Windows 11 Pro | Windows 11 Enterprise |
| Windows 10 Home | X | X |  |
| Windows 10 Pro |  | X | X |
| Windows 10 Enterprise |  |  | X |

There are some limitations within these broad paths. These include changes in the following:

* **Architecture**. When you want to upgrade from a 32-bit version of Windows 10 to a 64-bit version of Windows 11.
* **Language**. When you want to use a different language in Windows 11 than is being used in Windows 10.
* **Edition**. When you want to downgrade your edition; for example, from Windows 10 Enterprise to Windows 11 Pro.

**Compare in-place upgrades with migrations**

There are two approaches to upgrade to Windows 11. These are:

* **In-place upgrade**. You run setup.exe on the computer running Windows 10 and choose Upgrade.
* **Migration**. There are two methods available:
* **Side-by-side migration**. You migrate your users’ user state from their old computer, running Windows 10, to their new computer running Windows 11.
* **Wipe-and-load migration**. You backup the user state to an external location. You wipe the computer, and apply a Windows 11 image on the computer. Then you restore the user state.

Let’s compare these approaches.

**In-place upgrade**

This is the easiest method to upgrade to Windows 11, and is recommended. When you perform an in-place upgrade, all apps and user state are retained. The following table describes the advantages and disadvantages of this approach.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Retains user state (user settings, app settings, and data files) without manual intervention | Doesn’t enable you to create a standardized desktop environment. Configuration variations persist. |
| Preserves installed apps, and normally doesn’t require that you reinstall apps | Preserved apps might not work correctly after upgrading from Windows 10, although this is unlikely |
| You don’t need to provide storage space for migrating user state | Legacy settings might cause performance or security issues |
| Provides the least disruptive path for your users from Windows 10 to Windows 11 | Doesn’t support language changes, edition changes, or architecture changes |
| Is relatively simple to perform, and can be automated using Configuration Manager | Is only available from Windows 10 |
| You can rollback the upgrade at any time during and after the upgrade process | Computer must meet the minimum hardware requirements |

If your computers are relatively new, and incorporate features such as an 8th Gen processor, a TPM, and meet the other requirements, then choose to perform in-place upgrades.

**Migration**

If your computers don’t meet the hardware requirements, or are running an unsupported operating system, or you’re attempting to make edition or language changes, consider performing a migration to Windows 11.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Provides you with an opportunity to clean up your existing computers. This can help create a more reliable and secure desktop environment. | You’ll need to plan for user state migration. You’ll also need to plan for app installation. |
| Supports and architecture edition changes. You can install any edition of Windows 11, irrespective of what edition was previously running on your computers. You can also change from 32-bit to 64-bit architectures. | Requires that you reinstall of apps. If these apps are old, you might to verify that you still have access to the installation files. You’ll also to check that app prerequisites can be met on Windows 11. |
| Enables you to take the opportunity to reconfigure low-level hardware settings, such as disk configuration. | Requires available storage space for user state migration. For a large number of migrations, this space could be considerable. |
| Unwanted or malicious legacy software, drivers, and apps don’t migrate. | Depending on the migration option chosen, users can experience some disruption during the process. |

If you opt for migration, then choose between:

* **Side-by-side**. In this scenario, your user has a new computer already installed with Windows 11. You’ll need to configure the device per your organizational requirements, and provision the required apps. Then you can migrate the user state from the legacy device. A key advantage of this approach is that the user experiences less disruption as they can continue working on their old computer until their new computer is ready.
* **Wipe-and-load**. In this scenario, you’ll need to migrate the user state off the computer at the first step. Then you’ll wipe the computer and replace the operating system with an appropriate image of Windows 11. Finally, you’ll restore the user state. This is more disruptive than using side-by-side migrations.

If your computers don’t meet the minimum hardware requirements, you cannot use a wipe-and-load migration.

**The process for performing an in-place upgrade to Windows 11**

Performing an in-place upgrade from Windows 10 is the easiest way to move to Windows 11. The process includes the following high-level steps:

1. Assess readiness for Windows 11
2. Optionally, back up user state
3. Perform the upgrade
4. Verify the upgrade is successful
5. Update Windows 11 with desired Feature updates and required Quality updates

**Assess Readiness**

You must ensure that all your computers meet the minimum hardware requirements for Windows 11. While this is relatively easy on a single computer, if you have hundreds, or even thousands of computers, you’ll need to gather inventory data to make this assessment. You can use Configuration Manager to gather this assessment data from your devices.

You can also use the Microsoft Assessment and Planning Toolkit (MAP) to perform this assessment. Although this tool is aimed more at Windows 10 readiness, you can still use it to gather inventory data that identifies fundamentals such as processor, memory, and disk configurations.

It’s also important to verify that any apps that you’re using in Windows 10 will work in Windows 11. This is likely to be the case, as the architecture for Windows 10 and Windows 11 is broadly similar. However, you can download the Windows Assessment and Deployment Kit (Windows ADK). This kit contains the Compatibility Administrator which you can use to test installed apps.

It's also important to remember to verify that any attached hardware devices are supported in Windows 11. You’ll need to ensure that any device drivers you’ll need are available in Windows 11.

**Back up user state**

This step is optional for an in-place upgrade, but helps protect your user state during the upgrade if anything should go seriously wrong. You can back up the user state to local storage, such as a USB memory stick or external HDD. You can also back up to a network shared folder. Typically, you’ll use a feature like **Back up and Restore (Windows 7)** to perform the backup and, if necessary, the restore.

**Perform the upgrade**

For a small number of computers, you’ll typically run the Windows 11 installation program (setup.exe) to launch the upgrade process. When prompted, select **Upgrade**.

You can also use Configuration Manager to perform the required upgrades. You create a task sequence that performs the upgrade, but that also, if necessary, migrates user state.

The installation program prevents you from selecting the upgrade option if an in-place upgrade is not possible.

To perform an interactive in-place upgrade, use the following procedure:

1. Mount the product DVD.
2. When prompted, run **Setup**. If prompted, at the **User Account Control** prompt, click **Yes**.
3. In the **Windows 11 Setup** wizard, on the **Install Windows 11** page, click **Next**.
4. On the **Applicable notices and license terms** page, click **Accept**.
5. Setup checks for updates and verifies that your computer can run Windows 11.
6. On the **Ready to install** page, review the options. If you want to change the defaults (Install Windows 11, Keep personal files and apps), then click **Change what to keep**. Otherwise, click **Install**.
7. Windows 11 installs, and the computer restarts several times.
8. After a while, your new Windows 11 desktop displays. You might need to sign in depending on your computer’s configuration.

The specific steps in this procedure might vary slightly depending on your particular configuration and circumstances.

**Verify success**

After you’ve completed the upgrade, sign in. Then verify that all apps and hardware devices work as expected. Also verify the presence of user data and both user settings and app settings.

**Update Windows 11**

It’s probable that you’ll need to update Windows 11. As you’ll learn later in this module, Windows 11 receives both Feature and Quality updates on a periodic basis. It’s important to apply these to maintain the security and reliability of your Windows 11 devices. Apply the required updates to your upgraded computers.

**The process for migrating to Windows 11**

If you’ve decided to opt for a migration, then the high-level process is as follows:

1. Optionally, assess readiness for Windows 11
2. Back up user state
3. Optionally, install Windows 11
4. Update Windows 11 with desired Feature updates and required Quality updates
5. Install apps and drivers
6. Restore user state

**Assess Readiness**

This step is not always required. For example, if you have a brand new computer already running Windows 11 to which are migrating, clearly you don’t need to perform an assessment of readiness. Therefore, it’s wipe and load migrations to which this step applies.

**Back up user state**

It’s important that you back up the user state. User state consists of user settings, app settings and user data. Typically, you’ll use USMT (part of Windows ADK) to perform this task. Ensure you have sufficient external storage available. You can use local external storage or network storage. Note that user data resides, by default, in the document Libraries, such as Documents, Pictures, and Videos. If you’re aware that data resides elsewhere, you must ensure that your back up procedure captures this data.

You can create Configuration Manager task sequences that perform all the required steps in a migration.

**Install Windows 11**

This step is only required when you’re performing wipe-and-load migrations. It’s assumed that for side-by-side migrations, you already have a computer running Windows 11. You can install Windows 11 using any of the methods discussed in the previous chapter, including high-touch retail media installations, Microsoft Deployment Toolkit (MDT) deployments, or you can use Configuration Manager.

**Update Windows 11**

As with an in-place upgrade, it’s important that all your computers are up-to-date with the latest Quality updates and any desired Feature updates.

**Install apps and drivers**

You’ll now need to install any required apps, and their dependencies. If your users are using any legacy hardware, you might also need to install the required drivers to support this hardware. You can get a good idea of what drivers you might need during the inventorying process during readiness assessment.

**Restore user state**

The final step in the procedure is to restore the user state. It’s normally a good idea to verify that everything works before allowing your user to use their new Windows 11 device.

**Discussion: Will you upgrade or migrate?**

Lesson 2

**Migrating user state**

Whether you’re migrating or performing an in-place upgrade, it’s likely you’ll need to migrate user state. The primary tool for performing this migration is the user state migration tool. USMT is part of the Windows ADK, which you can download from the Microsoft website. In this lesson, you will learn how to use USMT.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe user state.
* The User State Migration Tool.
* How to migrate user state.

**What is user state?**

User state is the collection of application and user settings, together with user data, that exists on a Windows computer. When planning the migration of user state from one computer to another computer, it’s important that you know where that user state exists.

As part of the planning process for user state migration, you must consider the what elements of user state you want to include in the migration. The following lists describes the elements that make up user state on a typical Windows computer:

* **User accounts**. Each user account is associated with its own collection of user state. You must decide which of the user accounts on a particular computer must be migrated. A typical workstation might include user accounts from the local account database, or indeed from an Active Directory domain.
* **App settings**. Each app will have a collection of settings that relate to it specifically. It’s likely that you’ll want to migrate the settings for all installed apps. However, it’s also possible that you might want to migrate the settings for some apps.
* **Operating-system settings**. Operating-system settings include visual appearance, sound and audio settings, mouse actions, locale settings including time and language, network connectivity settings, email-account settings, fonts, accessibility settings, and much more.
* **Data**. User data can exist in numerous locations. Ideally, your users will be saving their data to file server shared folders, or else using OneDrive or Azure Files to store data online. If this is the case, there should be little actual data to migrate; those locations will be available on the upgraded/migrated computer. However, if your users are storing their data in local libraries (in the C:\Users\%Username% folder), you’ll want to migrate this data. By default, USMT expects user data to exist in this location. However, if your users are storing data elsewhere on their local hard drives, you’ll need to determine where, and adjust the settings in USMT to capture and migrate that data.

Having determined what user state you must migrate, you’re ready to install and configure USMT to perform the migration.

**What is USMT?**

USMT is part of the Windows ADK. It comprises two main elements and a collection of supplemental files. These are:

* **ScanState.exe**. Scans the source computer, collects the user state (data and settings), and then creates a migration store in which to store the user state.
* **LoadState.exe**. Connects to the migration store and migrates the user state from the store to a temporary location on the target computer.
* **Migration .xml files**. Enable you to customize the migration experience by defining the specific apps, users, and data that you want to include in the migration. This is done using a collection of .xml files: MigApp.xml, MigUser.xml, and MigDocs.xml, and also any additional custom .xml files that you create.
* **The MigApp.xml file**. Specify this file when using both ScanState and LoadState. Determines app settings you want to migrate to target computers.
* **The MigUser.xml file**. Specify this file when using both ScanState and LoadState. Determines folders, files, and file types are migrated.
* **The MigDocs.xml file**. Specify this file when using both ScanState and LoadState. Enables you to specify which files and folders are migrated.
* **Custom .xml files**. Create custom files so that you can control the migration for your organization’s needs. For example, you can migrate a specific app or modify the migration defaults using custom .xml files.

**Installing USMT**

To install USMT, use the following procedure:

1. Download and install Windows ADK.
2. When prompted, ensure that you select the User State Migration Tool (USMT) check box. Feel free to install additional components, as required.
3. Complete the installation.

You don’t need to install the Windows ADK, and hence USMT, on each computer that you’re migrating. Instead, install the Windows ADK on an administrative workstation, and then copy the USMT binaries to a shared folder on a file server. Use the following procedure to complete this task:

1. From your administrative workstation, map a network drive to a shared folder on a server that will host the USMT binaries. You’ll need write permissions.
2. Copy the entire contents, including subfolders, of the following folder to the shared folder:

* C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\User State Migration Tool\x86

1. Ensure that the installation team have read-only access to the contents of this shared folder.

Your installation team can then map a network drive to this shared folder, and run the USMT executables from that location.

**How to migrate user state**

The migration is a two-step process. You start on the source computer and use ScanState.exe to capture and store the user state. Next, on the target computer, you use LoadState.exe to retrieve the data and settings from the migration store and apply them.

On the source computer, use the following procedure to complete the user state capture:

1. On a computer called LON-CL3, map a network drive to the shared folder containing the USMT binaries. For example, map drive U to \\LON-SVR1\USMT. You’ll need read permissions to this shared folder.

Make a note of the shared folder that you’ll store the migrated data in. You’ll need Modify permissions to this shared folder. For example: \\LON-SVR2\MigData.

1. Open an elevated command prompt and change to drive U.
2. Run the following command:

* Scanstate \\LON-SVR2\MigData\LON-CL3\ /i:migapp.xml /i:miguser.xml /o

On the destination computer, use the following procedure to complete the user state application:

1. On the target computer, complete the procedures for preparing a target Windows 11 computer including installing any required apps, drivers, and updates.
2. Map a network drive to the shared folder containing the USMT binaries. For example, map drive U to \\LON-SVR1\USMT.
3. Open an elevated command prompt and change to the drive containing the USMT binaries.
4. Run the following command:

* LoadState \\LON-SVR2\MigData\LON-CL3\ /config:config.xml / i:migdocs.xml
* /i:migapp.xml /v:13 /l:load.log

The precise commands entered will vary based on your specific needs and your particular configuration.

**Demonstration: Using USMT**

Lesson 3

**Managing Windows 11 updates**

Prior to Windows 10, significant feature additions and improvements were incorporated into new Windows releases. Thus, the major architectural and security changes introduced by Windows Vista were a significant departure from Windows XP. The introduction of the Microsoft Store, and Modern apps, combined with a touch-centric interface meant that Windows 7 was superseded by Windows 8.

These big changes necessitated upgrade planning. Many organizations were, and are still, reluctant to embark on such upgrades on a frequent basis due to the workload and costs imposed.

With Windows 10, Microsoft introduced a new approach. Rather than releasing a significant upgrade every two or three years, instead, small incremental updates, known as Feature updates, would be released. These would, or rather could, be applied automatically and would install using the in-place upgrade model.

The plan was to mitigate the issues of workload and cost, and increase the uptake of the additional, useful features being introduced. This approach became known as Windows as a Service.

In this lesson, you’ll learn about how Windows 11 updates are managed. You’ll also learn how you can control and manage the application of these updates.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe Windows 11 servicing channels.
* Identify available methods for managing and applying updates.
* Describe Windows Update configuration options.
* Describe the Group Policy Objects available for managing updates.
* Describe Windows Server Update Services.
* Explain how to manage updates with Intune.

**What are the available Servicing Channels?**

There are, broadly speaking, three types of update that Microsoft release. These are:

* **Feature updates**. These updates, as the name suggests, introduce new features.
* **Quality updates**. These updates introduces fixes and corrections.
* **Security updates**. These updates help protect your devices against recently emerging threats.

Microsoft provides you with a high level of control over how these updates are applied to your devices. The first element of this control is the servicing channel. The second element is a deferral value.

**Servicing channels**

Servicing channels determine when your devices receive Feature updates. There are three servicing channels. These are:

* **General Availability Channel**. This is the default channel for all Windows 10 and Windows 11 devices. Features updates are released to this channel annually, in the second half of each year. All Windows client editions are supported in this channel, except Windows 10 and Windows 11 Home editions. Feature updates in this channel have a two year lifecycle from date of general release.
* **Long-Term Servicing Channel**. This channel is designed for low change environments. It is only available on Windows 10 LTSC. This means that rather than configuring a device to use this channel, rather, you license the current version of Windows 10 LTSC. Computers in the LTSC do not usually receive feature updates. This provides a non-changing environment for organizations that require it. Windows 10 LTSC has a five year lifecycle. At the time of writing, there is no Windows 11 LTSC available, but that is expected to change.
* **Insider Program**. The Insider Program is available across all editions of Windows 10 and Windows 11, including Home editions. This channel enables assigned devices to receive Feature updates before they’re released and made generally available. There are three options in this channel:
* **Windows Insider Dev**. For users that want their devices to receive updates well before general release. Devices on this channel receive frequent updates. Due to the early release nature of updates, users must expect that some updates might introduce reliability issues on their devices.
* **Windows Insider Beta**. Devices in this channel receive fewer updates than in the Dev channel. In addition, devices don’t receive the updates quite so early.
* **Windows Insider Release Preview**. This channel probably represents the best option for many IT departments seeking to get to grips with a new update. Devices on this channel receive their updates just prior to general availability. This gives organizations one or two weeks to work with the update before its release.

In Windows 10, the user interface might still reference the term Semi-Annual Channel.

**Deferments**

After you’ve chosen the servicing channel, you must also configure a deferment value for the selected channel. The deferment enables you to control exactly when, after general release, configured devices receive and apply the updates. You can defer:

* Feature updates by up to 365 days.
* Quality updates by up to 30 days.

Deferring the application of updates enables you to test them on a group of computers for which the deferment value is lower. For example, you might:

* Configure most of your devices with a Feature update deferral value of 30 days.
* Configure a group of computers in IT to use the deferment value of 15 days.

This arrangement provides you with:

* 15 days after general release before any updates apply to any of your devices, during which time you can watch for any reported problems in the wider community.
* 15 additional days after application to your subset of IT computers to identify issues specific to your environment before updates are applied to the general population of your devices.

It’s important to remember that although you can defer updates, this is at the cost of the update lifecycle. So, for example, if you choose to defer Windows Feature updates for 365 days, then the lifecycle reduces from two years to one year. This is because the lifecycle is measured from general availability, not your specific application of updates.

**How can you apply updates?**

For small organizations, there’s perhaps little need to worry too much about how updates are applied. But for large organizations, it’s important to understand how you can manage the application of Windows updates.

The available options depend on whether your Windows devices are managed in an on-premises environment or in the cloud.

* **Windows Update**. This Microsoft service is the default servicing model for Windows computers. This online service provides updates to Windows devices, including updates to additional Microsoft products, such as Office, and device driver updates. Using Windows Update gives you little control over the update process, but is automatic and requires little no configuration.
* **Configuration Manager**. You can perform numerous on-premises management tasks in enterprise-level organizations using Configuration Manager, including performing update management. Managing the deployment and application of updates in your organization with Configuration Manager gives you a high degree of control.
* **Windows Update for Business**. Strictly speaking, Windows Update for Business isn’t a service. Rather, it’s a collection of settings, applied either with Intune or with Group Policy, that control the servicing channel, deferments, and related update settings. Windows Update for Business is not available for Windows 11 Home.
* **Windows Server Update Services**. This Windows Server role enables you to apply fine control over the distribution and application of Windows updates.
* **Microsoft Intune**. Intune is an MDM system. You can create Windows Update rings in Intune that are used to apply updates to specific groups of computers in your organization. These update rings define the servicing channel, deferment values for feature and quality updates, and numerous other related settings. Devices must be enrolled in Intune in order receive updates via Intune.

**Configuring Windows Update settings**

You can configure the Windows Update settings for a single computer by using the Settings app. Use the following procedure to access the Windows Update settings:

1. Click **Start**, and then click **Settings**.
2. In Settings, on the navigation menu, select **Windows Update**.
3. From the **Windows Update** pane, you can configure the required settings, as described in the following table.

|  |  |
| --- | --- |
| Setting | Description |
| Check for updates | This button may be labelled differently depending on whether there are updates, and GPO configured options that control how updates are downloaded and installed. For example, if updates are available, the button displays Download now. |
| Pause updates | Enables you to Pause updates for one through five weeks. Any updates being downloaded at the time you select this are abandoned until you resume updates. |
| Update history | Provides access to a list of recently installed updates. These are categorized into Feature Updates, Quality Updates, Driver Updates, Definition Updates, and Other Updates. You can also access a link to **Uninstall updates**. |
| Advanced options | Provides access to a number of options described in the list below, but including Active hours, Optional updates, and Delivery Optimization. |
| Windows Insider Program | If a computer is not enrolled in the program, you can select the Get started button to sign in and select an Insider channel. Depending on settings, and specific scenario, you can also opt out of the Program from here. |

**Advanced options**

You can configure the following Advanced options for Windows Update settings:

* **Receive updates for other Microsoft products**. Enables you to use Windows Update to receive updates for Microsoft Office and other Microsoft apps simultaneously with Windows updates, when available.
* **Get me up to date**. When selected, enables you to bring a computer up to date, forcing restarts as needed to do so.
* **Download updates over metered connections**. If you want to download updates over a metered connection, such as a cellular data plan, select this option. Charges might be incurred.
* **Notify me when a restart is required to finish updating**. This option causes a message to display in the Notifications area if an update requires a restart.
* **Active hours**. These default to 08:00 to 17:00 hours. However, you can specify different values, or request that Windows makes an automatic determination based on your typical activity. This setting controls when restarts are permitted. Typically, restarts won’t occur during your working hours.
* **Optional updates**. Use this setting to review any optional updates, such as driver updates. You can then select those updates as desired.
* **Delivery Optimization**. Windows 11 can receive updates not only from Windows Update, but also via peer sharing to help optimize bandwidth and reduce data charges (where applicable). You can choose to download from:
* Devices on my local network
* Devices on the internet and my local network
* You can also configure additional **Advanced options** to control bandwidth and throttling settings, both in a download and upload context. Finally, you can use the Activity monitor link to review recent download and upload statistics.
* **Recovery**. A shortcut to recovery options.
* **Restart apps**. A shortcut to sign in options. Enables you to control the restart behavior of your apps.
* **Configured update policies**. Displays any settings being enforced on your update policy using Group Policy.

**Using Group Policy to configure Windows updates**

In an on-premises environment, it makes sense to use Group Policy to configure Windows Update settings. You’ll want to ensure that the appropriate Windows Update settings apply to the appropriate groups of computers.

A good approach to take is to create security groups in Active Directory. Then add computer accounts to the appropriate security group. You can then use security filtering to control the application of the Group Policy settings.

For example, to create the settings that control updates for the general population of your computers:

1. Create a group called **Early Release** and add to that group all of the computers that will receive updates prior to general release.
2. Create and link a group policy to the domain object called **Early Release Updates**.
3. Configure it with the appropriate Windows Update settings for the Genpop group. For example, select the Windows Insider Beta channel, and configure 0 for deferments.
4. Finally, use security group filtering to ensure that these update settings only apply to the configured group; in this case **Early Release**.

To be specific, you’ll grant this group both Read and Apply Policy permissions on the GPO, while also removing the Apply Policy permission from the Authenticated Users group.

The next step would be to create additional groups containing appropriate computer objects as members and then repeat the steps described above for each group.

In a Group Policy, under the Computer Configuration node, navigate to Administrative Templates, and select Windows Components. In this folder, there are a number of specific locations for Windows Update related settings. These are:

* **Data Collection and Preview Builds**. These settings control diagnostic and logging data. This data can be used by Configuration Manager and Desktop Analytics to provide useful data and insights about updates in your organization.
* **Delivery Optimization**. These settings are used to control the bandwidth and caching settings that relate to Delivery Optimization.
* **Windows Update**. This parent folder contains four subfolders that host the main settings for Windows Update. The subfolders are:
* **Legacy Policies**. Contains settings that have been used in earlier versions of Windows client.
* **Manage end user experience**. These settings are also present in earlier Windows versions, but still have relevance in some scenarios. For example, the Configure Automatic Updates setting controls how download and installs are handled when updates are pending.
* **Manage updates offered from Windows Server Update Service**. This fairly obviously named folder does exactly what it says: it contains settings that control the WSUS client configuration.
* **Manage updates offered from Windows Update**. Again, the name of the folder identifies its role. These settings control Windows Update for Business. It’s here that you define the Feature Updates, Preview Builds, and Quality Updates deferral values. It’s also here that you opt into the Insider program.

Let’s explore some of the settings in more detail. In the **Manage end user experience** node, you can enable the **Configure Automatic Updates** setting. Doing so allows you to choose between:

* **2 – Notify for download and auto install**. When Windows finds updates that apply to this computer, you are notified. After going to Windows Update, you can download and install any available updates.
* **3 – Auto download and notify for install**. Windows finds updates that apply to the computer and downloads them in the background without notifying the user. After the downloads are complete, you’re notified that they’re ready to install. After going to Windows Update, you can install them. This is the default value.
* **4 – Auto download and schedule the install**. Windows finds applicable updates and downloads them automatically. Windows then uses the configured schedule to install the updates. If you choose this option, you must configure the scheduling settings that display below the **Configure automatic updating** drop down list.
* **5 – Allow local admin to choose setting**. Local administrators can use the Windows Update control panel to select a configuration option of their choice. Local administrators aren’t allowed to disable the configuration for Automatic Updates.
* **7 – Auto Download, Notify to install, Notify to Restart**. This is a Windows Server value only and you can ignore it in Windows 11.

Under the **Manage updates offered from Windows Server Update Service** section, there are is an important setting worth calling out. This is:

* **Specify intranet Microsoft update service location**. Enables you to specify an intranet server to host updates from Microsoft Update. Typically this will be a WSUS server. You can then use this update service to automatically update computers on your network.

Finally, in the **Manage updates offered from Windows Update** section, you can configure the Windows Update for Business settings. These control the servicing channel and related settings, and include:

* **Select when Preview Builds and Feature Updates are received**. Enables devices to defer taking the next Feature Update available to your channel for up to 14 days for all the pre-release channels and up to 365 days for the General availability channel. You also have an option to specify a start date for the Pause value for Preview Builds or Features Updates.
* **Select when Quality Updates are received**. Enable this policy to specify when to receive quality updates. You can defer receiving quality updates for up to 30 days
* **Manage preview builds**. Allows you to select the appropriate Insider Program: Dev Channel, Beta Channel, or Release Preview Channel.

**Windows Server Update Services**

While it’s convenient to download updates from Windows Update, for larger organizations, using an internal service to manage and distribute updates is very useful. The Windows Server Update Services (WSUS) role can help. The WSUS role provides centralized management for updates.

In addition to managing updates for Windows client, WSUS can also obtain and manage updates for other Microsoft products, including Windows Server.

Smaller organizations might implement a single instance of a WSUS server, and using the GPO values discussed earlier, point all client computers to that intranet location for their updates.

Larger organizations probably would benefit from deploying multiple WSUS servers. This helps provide for reliability and load balancing.

Without getting into too much detail, after deploying WSUS in your organization, you create computer groups that identify collections of computers that receive updates in a specific way. You can then use the WSUS console to approve and distribute those updates.

**The WSUS update management process**

The WSUS update management process consists of four continual phases. These are:

* **Assess**. Helps you to determine an efficient topology for scaling your WSUS components. If your organization changes, or your needs evolve, you might decide to add new or redistribute existing WSUS servers.
* **Identify**. Enable you to determine whether new updates are relevant to your organization. You can configure WSUS to:
* Retrieve all updates automatically
* Retrieve only specific types of updates
* WSUS can also identify which updates are relevant to which registered computers.
* **Evaluate and plan**. It’s important to determine that updates do not create problems in your organization. For example, you’ll want to ensure that a Quality update doesn’t cause problems with a line of business app. Use this phase to make that ongoing determination.
* **Deploy**. Finally, after you’ve assessed the impact of updates, you can release the updates and make them available to your devices.

**Using Intune to manage Windows updates**

Many organizations now use cloud-based services, either exclusively, or in a hybrid context – with some on-premises apps and resources, and some cloud apps and resources. If you want to manage updates for devices that aren’t joined to your AD DS domain, you might consider using and MDM, like Microsoft Intune.

Windows devices running Windows 11 can be joined to Azure AD and enrolled in Intune for device management. Once enrolled, you can assign Windows Update settings to your devices.

The settings that are applied to a specific device is based on its group membership. Typically, you create a Windows update ring and configure the appropriate settings (servicing channel, deferrals, and related settings). Then you assign the Windows update ring to an Azure AD group. Members of the group use those settings to apply updates. In other words, in a similar way to how you might use GPO security group filtering in an on-premises environment.

**Demonstration: Managing updates**

**Lab: Upgrading and updating Windows 11**

**Question:**In the lab, you performed an interactive upgrade. If you were using new computers, what options might you use to migrate to Windows 11?

**Module Review and Takeaways**

Review Questions

**Question:**Which USMT command is used to collect user state?

**Question:**How often do Feature updates apply to Windows 11?

**Question:**Which update channel enables an organization to avoid receiving Feature updates?

Tools

The following table lists the tools that this module references.

| **Tool** | **How used** | **Where found** |
| --- | --- | --- |
| Loadstate and Scanstate | * Part of USMT, and enables migration of user state | Windows ADK |
| WSUS | * Helps manage updates within your organization | Windows Server role |
| Configuration Manager | * Manages apps, deployments, inventory and much more | N/A |