AXIS Camera Station.

Microsoft Windows Update Management

January 30, 2023
Rev. 1.0

Contents

Introduction

Microsoft Windows Update Management refers to the process of managing updates and patches for the Windows operating system. This includes scheduling updates, determining which updates are necessary for specific devices, and monitoring the status of updates. By default, on standalone systems, the built-in Windows Update service is used to schedule, download and install updates.

When it comes to Axis Communications Network Video Recorders (NVRs) that run on the Windows operating system, it is important to keep them updated with the latest security patches and bug fixes to ensure that they continue to function optimally and protect against potential security vulnerabilities.

The administrator can configure the Windows Update settings to automatically download and install updates or choose to review and select the updates to be installed before proceeding. It is possible to use the Windows Update service to schedule when the updates will be installed. The administrator also needs to regularly check for updates and make sure that the NVRs are up to date. It is important to test the updates and system to verify that it works as it should and roll back the updates if they would affect the performance of the NVRs negatively.

It is imperative to have a proper change management process in place before deploying updates. This includes testing the updates on a small group of NVRs before deploying them to all the devices. In conjunction, having a rollback plan in case of potential issues and providing proper documentation of the update process should be mandatory. This helps ensure that the updates do not cause any disruption or compatibility issues with the other software and hardware. Additionally, it's also important to have a tested and working backup of the entire system (including the AXIS Camera Station databases) before deploying updates. This helps for quick recovery in case there are any issues with the updates.

Methods for Windows Update management

There are many methods of Windows Update management that can be used, depending on the size, scope and complexity of the network and the specific needs of the organization:

- Manual updates: Manually checking for and installing updates on devices individually. This is often used in small networks with a limited number of devices.

- Windows Server Update Services (WSUS): This is a free Microsoft product that can be used to manage updates for Windows devices. WSUS allows administrators to approve or decline updates and deploy them to groups of devices. Please note that this requires a Microsoft Active Directory Domain controller.

- Microsoft Intune: This is a cloud-based device management solution within the Microsoft ecosystem, which allows administrators to manage updates, security and compliance settings, and device configuration for Windows 10 devices. Intune can be used to deploy updates to groups of devices, monitor the status of updates and create access policies to help ensure that only devices that are compliant with your organization's policies have access to resources. To be able to use Microsoft Intune in combination with AXIS Camera Station, a Hybrid Azure AD joined device is required. AXIS Camera Station currently only supports On-Prem Active Directory.

- Windows Update for Business: This is a service offered by Microsoft which allows administrators to have more control over update processes and reduce the impact of updates on the organization. Updates can be scheduled when to install, choose which ones to install, and control the pace at which feature updates are deployed. Please note that this requires a Microsoft Active Directory Domain controller.

- System Centre Configuration Manager (SCCM): This is an On-Prem device management solution; it is a paid product within the Microsoft ecosystem that provides an advanced way to manage updates and other aspects of device configuration. SCCM can be used to deploy updates to groups of devices, and to monitor the status of updates on the network. Please note this requires an Active Directory Domain controller to be set up for this to function.

- Third-party update management software: There are also third-party update management solutions that can be used to manage updates for Windows devices that are used within distributed systems outside of an Active Directory Domain. These solutions typically offer more advanced features, such as scheduling, rolling back, and testing updates before deploying them to the entire environment.

- Windows Offline updates: Another method for performing Windows updates is by using the Microsoft® Update Catalog. The Windows Microsoft® Update Catalog is a Microsoft website that provides a list of updates and hotfixes for Windows operating systems. To perform an offline update using the Microsoft® Update Catalog, users would first identify the updates that are needed by searching the Microsoft® Update Catalog and then download the updates. It is important to note that the updates must be compatible with the operating system and architecture of the computer, otherwise they will not install correctly. This method is only recommended for advanced users or IT Administrators.

All the above types of Windows Update management have their own set of advantages and disadvantages, and the best choice is dependent on the specific needs of the organization.

Best practices of managing Windows updates.

When it comes to updating a Windows 10 operating system, there are best practices that should be followed to ensure a smooth and successful update process.

It is important to have a well-planned process in place to ensure that it goes smoothly and that any issues are identified and resolved. The best practices for updating a Windows 10 operating system involve a combination of proactive and reactive approaches that includes backing up important data, checking for known issues, scheduling updates for out-of-hours, validating updates, monitoring the update process, and having a rollback plan.

- **Backup:** Creating a backup of critical data, files, and documents is an important step in preparing for updates. This will ensure that data lost or corrupted during the update process can be easily restored. Keeping your device up to date with the latest security updates and software updates is crucial to protect against potential security vulnerabilities.

- **Known Issues:** Before installing updates, it is important to check the Windows Update history or the Microsoft website for any known issues associated with the update. If there are any issues, it may be best to wait until they have been resolved before proceeding with the update.

- **Scheduling:** Scheduling updates outside of business hours can minimize disruptions to your system. Using Windows Update for Business can provide more control over the process. Administrators can decide when to install updates, choose which to install, and control the pace at which features, or updates are installed. Scheduling the updates outside of business hours will greatly reduce the downtime of critical systems as some windows updates especially feature updates require several system reboots to take effect.

- **Validation:** Before deploying updates to the entire system, it is important to test the updates to ensure they don't negatively impact the system's performance or the applications running on it.

- **Monitoring:** Monitoring the update will help to identify any potential problems and ensure that the update completes successfully.

- **Rollback:** In case of issues, it is important to have a rollback plan in place, this could be something like creating a system image or snapshot before the update, so you can easily revert to the previous state.

By following the above best practices, organizations can ensure that their Windows 10 operating system is kept up to date with the latest security patches and software updates and that the update process is smooth and trouble-free.

Versions of Microsoft Windows installed on AXIS Network Video Recorders

The Network Video Recorders are pre-installed with a Windows 10 operating system as default. To meet the needs of our system, the Network Video Recorders utilize two different versions of Windows 10, namely, the Semi-Annual Channel and the Long-Term Servicing Channel. The below table specifies the branch of Windows 10 used by each Network Video Recorder and workstation.

AXIS Product Series	*Microsoft Windows Version*
Active Products	
AXIS S12	Windows 10 IoT Enterprise LTSC 2021
AXIS S22	Windows 10 IoT Enterprise LTSC 2021
AXIS S21	Windows 10 IoT Enterprise LTSC 2021
AXIS S93	Windows 10 IoT Enterprise LTSC 2021
AXIS S11	Windows 10 IoT Enterprise Semi Annual Channel
Discontinued products	
AXIS S11	Windows 10 IoT Enterprise Semi Annual Channel
AXIS S9002 MKII	Windows 10 IoT Enterprise Semi Annual Channel
AXIS S9101 MKII	Windows 10 IoT Enterprise Semi Annual Channel
AXIS S10 MKII	Windows 10 IoT Enterprise 2015/2016 LTSB
AXIS S9002	Windows 10 IoT Enterprise 2015/2016 LTSB
AXIS S9101	Windows 10 IoT Enterprise 2015/2016 LTSB
AXIS S20	Windows 10 IoT Enterprise 2015/2016 LTSB

AXIS Network Video Recorders default Windows 10 update service configuration.

It is important to note that on the AXIS Network Video Recorders, the default Windows Update configuration is set to notify users of available updates and automatically install them. When the system detects updates that apply to it, the user will be notified of the availability of updates and given the option to download and install them through the Windows Update feature. This ensures that the system stays up to date and secure. To change the Windows Update configuration, please check the AXIS Network video recorder user manual on how to configure the Windows updates.

Windows 10 IoT Enterprise Semi Annual Channel

Windows 10 IoT Enterprise Semi-Annual Channel (SAC) is a version of the Windows 10 operating system that is designed for Internet of Things (IoT) devices and other specialized systems that require a balance of stability and the ability to get new features at a faster pace than LTSC versions.

When it comes to Axis Communications Network Video Recorders (NVRs), Windows 10 IoT Enterprise SAC is a suitable option, as it provides a balance between stability and new features. The semi-annual release schedule of this version of Windows 10 means that NVRs running SAC can get new features and capabilities quicker, while still receiving support and security updates. This can be beneficial for organizations that want to take advantage of new features and capabilities, but still require a stable and secure platform for their surveillance applications. SAC releases are supported for 18 months and are intended for organizations that want to take advantage of new features and capabilities as soon as they are available, but still require a stable and secure platform for their surveillance applications.

The SAC) update process provides a greater level of flexibility for organizations when managing updates for their surveillance applications. With the ability to delay the deployment of new features and capabilities for testing and validation, organizations can strike a balance between taking advantage of new features and capabilities and ensuring the stability and security of their systems. This flexibility allows organizations to fully evaluate and validate new updates before deployment, resulting in a more efficient and effective update process.

For further information on the Semi Annual Channel click on the following link. Semi Annual Channel

Windows 10 IoT Enterprise LTSC 2021

Windows 10 IoT Enterprise Long-Term Servicing Channel (LTSC) is a version of the Windows 10 operating system that is specifically designed for Internet of Things (IoT) devices and other specialized systems that require stable and long-term support. This version of Windows 10 is designed for use on embedded devices and other specialized systems, such as industrial automation systems, point-of-sale terminals, medical devices, and digital signs.

When it comes to Axis Communications Network Video Recorders (NVRs) that run on the Windows operating system, Windows 10 IoT Enterprise LTSC is a suitable option because it is designed to provide a stable and secure platform for running surveillance applications. The long-term support of this version of Windows 10 means that NVRs running LTSC can continue to receive security updates and support for a longer period: up to 10 years of mainstream support and 5 years of extended support. This minimizes disruptions to the device's operation and minimizes downtime for these specialized systems.

Additionally, by using Windows 10 IoT Enterprise Long-Term Servicing Channel (LTSC), organizations have a higher level of control over the update process for their Axis Communications Network Video Recorders (NVRs) and other specialized systems. This version of Windows 10 offers the ability for organizations to test and validate updates prior to deployment, allowing them to ensure the updates will not have any negative impact on device performance. This level of control over the update process provides a more stable and secure platform while providing long-term support, which is essential for specialized systems that require minimal disruptions.

By default, the LTSC Windows version does not receive feature updates, but only security and quality updates via the Windows Update service and other services like WSUS. For further information on the LTSC channel, please look at the following: Windows 10 Enterprise LTSC

Conclusion

In conclusion, managing updates for Axis Communications Network Video Recorders (NVRs) is an important task that requires careful planning and execution. Windows 10 IoT Enterprise LTSC and Windows 10 IoT Enterprise SAC are both suitable options for running on NVRs, depending on the specific needs of the organization. Windows 10 IoT Enterprise LTSC provides a stable and secure platform with long-term support and minimal disruptions, while Windows 10 IoT Enterprise SAC provides a balance between stability and new features at a faster pace.

When it comes to update management, it is important to consider the best practices such as creating a backup, checking for known issues, scheduling updates for non-peak hours, testing updates, monitoring the update process, and having a rollback plan in place. Other options such as Windows Server Update Services (WSUS), System Centre Configuration Manager (SCCM) and Microsoft Intune are also available for managing updates on Windows devices.

In addition, organizations should also consider the different types of update management that are available, such as manual updates, third-party update management software and Windows Update for Business, to find the best solution that meets their needs. With the right update management strategy in place, organizations can ensure that their NVRs are kept up to date with the latest security patches and software updates and that the update process is smooth and trouble-free.