Discovery™ by tecom

Aritech ChallengerPlus and Discovery

Cyber Security Best Practices

and WMS Pro hardening guidelines



ARITECH

Contents

1. Intended audience 2

2. Version Control 2

3. Disclaimer 2

4. Executive Summary 3

5. Additional references 3

6. Quick-Start Checklist: 4

7. General Advice 5

7.1 Key considerations 5

7.2 Access Control 5

7.3 Data security 7

7.4 Networking 8

7.5 System Updates 8

7.6 Support and Maintenance Agreements for WMS Pro 8

7.7 Virtualised or Cloud Instances 9

7.8 Disaster Recovery 9

7.9 Physical Security 9

7.10 UltraSync services 10

8. WMS Pro Installation – Detailed advice 11

8.1 Internet Information Services (IIS) Server hardening 11

8.2 MSSQL server hardening 13

8.3 Windows 10/11 Server Hardening 28

8.4 Wi-Fi/LAN hardening 31

8.5 Web Server Security 33

8.6 ASP.NET and Windows Desktop .NET Core Runtime Patching 34

1. Intended audience

This guide is intended for the following audience:

- Security consultants or architects embedding the product in proposed solutions or specifications
- Product deployment team
- System integrators
- Project Managers
- System Administrators
- Support teams
- Users of the product

2. Version Control

- Version: 1.4
- Last Updated: 13 November 2026

3. Disclaimer

This document is limited to providing general advice and information, and compliance with any and all items within should not be considered as complete prevention against any penetration or manipulation of the installed systems.

Aritech, while maintaining a high standard of engineering with a considered and measurable approach to cyber security, cannot be held responsible for the environment in which the products are installed. As such this document is provided to assist in installation, but the specific requirements and needs of any on site networks, physical hardware, remote access etc. must be considered separately. It is recommended for all installations that cyber security professionals be engaged to assess the complete installation post the implementation of any advice provided in this document.

Aritech does not provide direct support for implementation of any advice contained in this article. For assistance, please engage a cyber security professional.

4. Executive Summary

This guide outlines best practices to secure the Aritech Tecom suite of intrusion and access control systems, including hardware and software. It is intended to reduce vulnerabilities and protect installations from cyber threats by following principles of least privilege, secure communication, access control, and physical protection.

The products mentioned in this guide are:

- **Tecom WMS Pro (base version 3.0)**
  Aritech's software platform for management of on-site physical security
- **Tecom Discovery (base version 1.1)**
  Aritech's physical security hardware platform, containing a web interface for installer programming
- **Tecom ChallengerPlus (base version 10-07)**
  Aritech's physical security hardware platform
- **UltraSync (all versions)**
  Aritech's cloud-based transmissions platform for alarm delivery and remote access
- **CTPlus (base version 3.0)**
  Aritech's programming software for Tecom hardware products

5. Additional references

The information in this document is designed to be implemented using methods described in the following documentation:

5.1 Tecom Discovery installation and quick programming manual

5.2 Tecom Discovery Programming manual

5.3 Tecom Discovery administrator's manual

5.4 Tecom Discovery user's manual

5.5 Tecom WMS Pro installation guide

5.6 Tecom WMS Pro quick start guide

All documentation mentioned above can be downloaded at:

https://support.firesecurityproducts.com.au

Additional information and references can be found within the following:

5.7 Tecom Discovery embedded help, accessed through the product web interface

5.8 Tecom WMS Pro embedded help, accessed through the product web interface

5.9 CTPlus embedded help, accessed through the CTPlus client interface

6. Quick-Start Checklist:

6.1 Change all default credentials

6.2 Enable MFA for all web-based operator access

6.3 Enforce strong password complexity and lockout settings

6.4 Segment network traffic using VLANs

6.5 Apply the latest OS and WMS Pro software patches

6.6 Configure IIS, MSSQL, and Windows security baselines per section 7

6.7 Enable AES encryption between field devices and servers

6.8 Backup data regularly and encrypt backups

6.9 Secure physical access to control panels

6.10 Disable unused services and ports

7. General Advice

This section of the guide is intended to provide general advice on best practices for installation and configuration of Tecom systems.

7.1 Key considerations

7.1.1 Access control

Unauthorised access presents the most prevalent risk to cyber security of information systems. Bad actors gaining access to systems for the purposes of identity theft, system manipulation or interruption to services are events that can cause significant harm.

7.1.2 Sensitive data security

Tecom systems can contain sensitive information such as personal information including names, email addresses, photo identification, license information, address and phone numbers. It is important to consider the type of information that will be held in Tecom systems and secure the system appropriately.

7.1.3 Functional reliability

Ensuring the maximum uptime of Tecom systems helps to prevent against Denial of Service (DoS) attacks, it is recommended that all hardware and software be installed as per their relevant installation manuals to ensure maximum uptime and reliability.

7.1.4 Communications network

Discovery or Challenger panels are designed with physical redundancy and fallback mechanisms. Deploy backup communication infrastructure, such as secondary networks (e.g., satellite links, cellular data, or alternative wired connections. While Tecom hardware does provide a secure RS485 network for communication between devices, it still requires connection to customer network, Wi Fi or consumer 4G LTE network to provide connection to software or other additional services. It is important to consider which connections are most appropriate for the installation environment and remove any unnecessary redundant connections.

7.1.5 Operating environment

Keeping the Windows system up to date is an important step in reducing the risk of cyber vulnerabilities.

7.2 Access Control

7.2.1 When installing WMS Pro, consideration should be made to the authentication of the SQL database. SQL server software is not provided with WMS Pro, it is to be installed and secured by the person installing the database server instance.

7.2.2 Remote connections to the database, database accounts, and required ports should be considered and restricted.

7.2.3 Enforce TLS 1.2 or higher for WMS Pro connections to SQL instances. **For optimal security, it is highly recommended to configure the SQL instances themselves to disable support for TLS 1.0 and 1.1**.

7.2.4 Tecom products ship with default usernames and passwords. It is important to change the following as soon as practicable:

7.2.4.1 **Tecom WMS Pro**
Change the default password for the administrator account on first login (prompted).

7.2.4.2 **CTPlus**
Change the default credentials for the master account to use unique credentials.

7.2.4.3 **Tecom Discovery**
Change the default credentials for the master account to use unique credentials.
Change the default Tecom Master PIN code to a unique code.

7.2.4.4 **ChallengerPlus**
Change the default Tecom Master PIN code to a unique code.

7.2.5 Enforce strict password complexity requirements. WMS Pro and Discovery both offer built-in enforcement of complex passwords, which should be enabled to the highest level within the system. Installations utilizing Advanced SQL Configuration options during the WMS Pro installation should also ensure that strong passwords are enforced with the WMS Pro SQL database connection.

7.2.6 Operator lockout should be enabled to prevent brute force attacks on operator passwords. Set the number of failed login attempts to accept before locking the account, and the timeout for retry appropriately.

7.2.7 Enable multi-factor authentication where possible. Both WMS Pro and Tecom Discovery offer built-in multi-factor authentication services for operators of the web browser systems. Enabling this feature is critical in ensuring reduced vulnerability to password capture, sharing, or other compromise.

7.2.8 When creating operators or users within Tecom systems, ensure that only the access required for that operator or user is applied. All Tecom systems provide comprehensive controls to facilitate and restrict access only to the components of systems the operator or user requires access to.

Example: Reception desk operator may only require access to the software to add a temporary user for visiting people, their operator permissions in WMS Pro should be set as such and not copied or set as default to higher access. By limiting the permissions of operators, it reduces the risk of the system being manipulated in the event of password compromise or sharing.

7.2.9 All people who have access to any Tecom system should be given unique credentials. Password sharing or PIN code sharing is not advisable and presents a serious security risk. All Tecom systems provide audit logs and reports designed to identify which person/s perform actions within the system. Using password or PIN code sharing renders these reports effectively unusable.

7.2.10 Reserve seats for operator logins where possible. This works to ensure that specific operators are able to log in whenever. This should be utilised for key personnel, such as supervisors, technicians, or managers. This is a feature available natively in the WMS Pro system.

7.2.11 Regularly audit the access to all systems. It is important to ensure any person that should no longer have access is removed. Likewise, if a person changes roles and responsibilities, their access to systems should be immediately changed to reflect this.

7.2.12 Review history logs periodically, looking for failed login attempts, unknown locations, suspicious configuration changes / operator actions or other anomalies. In addition to manual reviews, configure automations in WMS Pro to automatically report on these events to detect and report such events in real-time. Set up email notifications for critical actions or thresholds, such as repeated failed login attempts, and changes to sensitive configurations, to ensure swift detection and response. Set up Cardholder inactivity reminders/auto-void. This feature allows WMS Pro to automatically generate alarms and/or automatically void any persons who have not accessed the physical system (e.g. used their PIN or card) within a configurable number of days.

7.3 Data security

7.3.1 WMS Pro contains potentially sensitive information regarding cardholders and operators of the system. It is advised that all preventative measures outlined in this document are implemented to ensure no personal information is revealed to unintended people.

7.3.2 Carefully consider what information is being stored in WMS Pro and if it is critical to the system application. Any unnecessary information should be removed.

7.3.3 WMS Pro contains the ability to generate reports for the express purpose of auditing events withing the system. Carefully consider who is given access to generate these reports, how they are distributed, and how they are stored to ensure no unauthorised access to sensitive information. WMS Pro provides role-based access control by region and menu access. In WMS Pro, access to certain information can be restricted by region, which can allow an Operator to only see subsets of records (e.g. only see certain Cardholders, devices, access groups, etc.).

7.3.4 Enforce a minimum key length and complexity for all API keys: Require a minimum of 16 characters for the SCP Interface App API key, and 32 characters for all other keys.

7.4 Networking

7.4.1 Consider the use of VPNs where possible. By requiring authentication to a VPN before accessing systems, an extra layer of security is provided against unauthorised access.

7.4.2 Consider segregation of traffic by using VLANs when connecting field devices to software. Also important to consider when using ethernet to connect between Tecom Discovery or ChallengerPlus control panels and their peripherals. This will help to ensure uptime of devices as well as denying access from any public, customer or internal networks to security devices. Specifically, this will help in prevention of DoS, or substitution attacks on WMS Pro software. It is recommended to consult a network engineer to secure the installation in compliance with current industry standard best practices.

7.4.3 Communication between Discovery or ChallengerPlus control panels and the WMS Pro server is secured using AES encryption. This encryption is enforced by default and cannot be disabled, ensuring all data in transit is protected..

7.4.4 Connections between Tecom hardware and WMS Pro or UltraSync are made by TCP, ensuring that communication is handled directly between two known addresses. Ensure only the ports required by the applications in use are opened to allow dataflow between critical points. Consult the relevant documentation for advice on ports in use by default and consider changing from default values.

7.4.5 By default, WMS Pro contains a self-signed certificate to enable HTTPS communications. This can be replaced with a user supplied certificate which has been issued from a trusted Certificate Authority by following the guidelines in the installation manual.

7.4.6 When setting the email gateway for the purpose of sending reports from within the WMS Pro system, ensure the highest levels of security are implemented. WMS Pro supports the use of SSL encryption for these connections. In addition, default credentials should not be used.

7.5 System Updates

7.5.1 Tecom software and hardware are regularly updated with cyber security in mind. It is recommended that all systems be updated to the latest versions as they become available.

7.5.2 Operating system environments should also be maintained and kept updated.

7.6 Support and Maintenance Agreements for WMS Pro

Aritech offers Support and Maintenance Agreements for WMS Pro that should be kept up to date and in place to guarantee access to both the latest versions of software, as well as support for any incidents that may occur.

7.7 Virtualised or Cloud Instances

7.7.1 WMS Pro supports virtualisation in many available platforms. All items in this document remain relevant, and security guides for configuring the specific virtualisation environment should also be followed.

7.7.2 Considerations for virtualised installations:

7.7.2.1 Connections between on-site devices and virtual servers should be secured. Discovery and ChallengerPlus offer built in AES encryption, but additional security such as VPNs should be considered.

7.7.2.2 Access control: consider whitelisting IP addresses that can access the environment, instead of making the environment "publicly available".

7.7.2.3 If installing in Cloud environments, consult an appropriate person to secure the system for both front end access, and communication between the Cloud and onsite devices.

7.8 Disaster Recovery

7.8.1 Ensure regular backups are made of the SQL database and the WMS Pro application.

7.8.2 Ensure backups are held off site and in encrypted locations with restricted access.

7.8.3 Test recovery procedure periodically to ensure they are available when required.

7.8.4 Maintain an incident response plan for security breaches and ensure it is known to relevant persons.

7.9 Physical Security

7.9.1 Tecom hardware should always be installed in appropriate locations:

7.9.1.1 PCBs should be installed in recommended enclosures

7.9.1.2 Enclosures should be installed in locked rooms with logs on access

7.9.1.3 Video security should be deployed for audit purposes

7.9.1.4 All system hardware should be regularly inspected for signs of tampering:

- Scratches or tool marks on enclosures
- Liquids on detection equipment

7.9.1.5 Detection equipment should remain free from obstruction (signage, furniture etc.)

7.9.1.6 Enable tamper detection for all devices and ensure priority alarms are set appropriately in the WMS Pro software. Consult the Tecom installation and programming manuals for further instruction.

7.10 UltraSync services

7.10.1 Tecom hardware supports connection to the UltraSync service for various purposes. It is important if this service is not being utilised that it be disabled. Consult the Tecom Discovery or ChallengerPlus manuals for further instruction.

7.10.2 When using the UltraSync service, consider the following at a minimum:

7.10.2.1 UltraSync passcode in the Tecom hardware should be unique for each panel connected.

7.10.2.2 Only users who require connection to the mobile application using this method should be given access, or provided with the UltraSync passcode.

7.10.3 General information about UltraSync:

- Compliant to the NIS2 cyber security directive
- Uses AES encrypted connection between onsite devices and UltraSync Cloud servers.
- Uses encrypted connections between UltraSync Cloud servers and monitoring centres.
- Supports multi-factor authentication for users requiring access to the UltraSync portal.
- All connections made are TCP and are done between known addresses.
- For monitoring connections, the unique identifier known as the SID of the control panel is to be provided to the monitoring centre for provisioning in the UltraSync cloud. This connection is not accessible for any other purpose and contains only the alarm traffic in CID format as transmitted by the Tecom control panel.
- For mobile connections (TecomPlus mobile app), the following is required to establish a connection:
    - Panel unique identified (SID)
    - UltraSync passcode – set in relevant control panel menu
    - User number
    - User PIN code
    - Valid access rights assigned to the user attempting access, governed by the Tecom control panel.



8. WMS Pro Installation – Detailed advice

This section of the guide is intended to provide specific instructions for securing a WMS Pro installation.

8.1 Internet Information Services (IIS) Server hardening

Internet Information Services (IIS) is the default web content presentation server available as an installable option under a Microsoft Windows operating system. An IIS web server accepts and process requests from remote client computers against specific resources served from the server. Upon parsing the requests, the server returns the appropriate response.

The web server provides the primary user and administration interfaces to the WMS Pro software. Vulnerability in the web server could be exploited by an attacker via the web interface to gain unauthorised access. Installation of the WMS Pro software requires a functional IIS server to be installed and configured as a prerequisite.

This section provides generic instructions on reviewing the security configuration of an IIS server. These instructions are developed for IIS 10, but the underlying hardening principles are mostly applicable to earlier versions of IIS releases as well.

8.1.1 Environment setup

The operating system environment should restrict unintended access to the IIS data environment.

8.1.1.1 Storing IIS data on a non-system disk

IIS data should be stored in Virtual Directories mapped to a non-system disk volume. This configuration reduces the risk that high volumes of web traffic or log data will consume space on the system drive, potentially degrading or disrupting core system operations.

Additionally, isolating IIS data from the system disk helps limit the impact of potential web-based malware. If malicious code is uploaded or executed via the web server, storing it on a non-system disk prevents it from residing in system directories that may have elevated execution privileges or implicit trust from the operating system. Such trust relationships could otherwise be exploited during later stages of an attack—for example, to escalate privileges or propagate malware laterally across a network. This risk is conceptually similar to directory traversal attacks, where improperly secured paths are used to gain unintended access to sensitive areas of the file system.

8.1.1.2 Configure application pool identity

Application Pool Identities are the local user accounts used to run the associated IIS worker process - w3wp.exe. Assigning the correct user authority ensures that applications will function properly with the appropriate permissions. These identities can be used in conjunction with ACLs to protect system content. It is recommended that each Application Pool run under a unique identity.

IIS also has built-in least privilege identities for use by Application Pools. It is recommended to configure these default Application Pool Identities based on the least privilege principle. Therefore, it is recommended to assign a unique least privileged principal to each application pool identity.

Moreover, application pools can be run as separate identities to improve isolation across IIS partitions. By default, IIS automatically uses the application pool identity if no anonymous user account is configured for a particular web site. This configuration will greatly reduce the number of accounts needed for websites and simplifies the management of the accounts. It is, therefore, recommended to use the Anonymous User Identity as the default Application Pool Identity.

It is a common practice to set the name of the Application Pool account to be the same as the Application Pool. Application Pool Identities were introduced in Windows Server 2008 SP2. Application Pools should be set to run as Application Pool Identity unless there is an underlying reason for running the application pool using a specified end-user account. One common exception is for running web farms using Kerberos authentication.

In summary, setting Application Pools to use unique least privilege identities such as Application Pool Identity reduces the potential harm should the application become compromised. Additionally, it will also simplify application pool configuration and account management.

Use the following command to set the application identity:

%systemroot%\system32\inetsrv\appcmd set config /section:applicationPools /[name='<apppool name>'].processModel.identityType:ApplicationPoolIdentity

8.1.2 Authentication

Strong authentication and authorisation configurations are necessary to prevent session hijacking and account takeover.

8.1.2.1 Enforce TLS 1.2 or above protection on 'forms authentication'

For Forms-based authentication, which transmits credentials across the network, it is essential to protect this traffic between client and server using robust TLS encryption. Any portion of a site using Forms Authentication **must be encrypted using TLS 1.2 or above, with TLS 1.3 being the preferred and most secure option.** Legacy TLS versions (1.0 and 1.1) are deprecated due to known vulnerabilities and should be disabled. Please that versions of CTPlus prior to 3.0 may not be capable of being installed on a PC locked down to TLS 1.2.

8.2 MSSQL server hardening

The MSSQL Server is an optional component of the operating system and is not automatically patched under the monthly Microsoft Quality Patch update cycles. Unnecessary features should be disabled to reduce the attack surface. Database user accounts, and authentication settings are independent of the underlying operating system environment and must be managed separately.

8.2.1 Maintain up-to-date MSSQL patching

SQL Server patches contain program updates that fix security and product functionality issues found in the software. These patches can be installed with a security update, which is a single patch, or a cumulative update which is a group of patches. The SQL Server version and patch levels should be the most recent and compatible with the organisation's operational needs.

Check the current version and patch level of your SQL Server instances on the MSSQL product page here:

https://learn.microsoft.com/en-us/troubleshoot/sql/releases/download-and-install-latest-updates

It is strongly recommended to test these fixes in the test environments before updating production instances. It should be noted that Cumulative and security updates are not installed by default.

8.2.2 Deploy Single-Function Member Servers configuration if possible

SQL Server software should be installed on a dedicated server, if possible, to minimise the risk of lateral attack by compromised software sharing the host server. Security assurance could be further improved by connecting the database server to a separate subnet allowing access only from authorised hosts through pre-approved network protocols. Database availability will be further increased by expanding from a single database server to an automated failover cluster supporting load balancing.

An important advantage of this design pattern is the reduction of the server's attack surface. By limiting the server's function solely to running SQL Server, the potential vectors for attack are constrained to the operating system, the SQL Server instance itself, and any approved security or operational tooling. To maintain this minimal attack surface, regular audits should be conducted to verify that no additional server roles or unauthorized software have been installed, in accordance with enterprise policy.

8.2.3 Authentication and Authorisation

MSSQL servers support hybrid authentication mode. Hybrid authentication mode supports both SQL user accounts created locally, and user roles mapped to the underlying Windows operating system and enterprise Active Directory. This section provides recommendations to strengthen the authentication process for the MSSQL server.

8.2.3.1 Mandates 'Windows Authentication Mode' for 'Server Authentication' Property.

Windows operating system based authentication provides a more robust authentication mechanism than SQL Server authentication. The windows authentication logs are already monitored by the Security Information and Event Management (SIEM) for intrusion detection and response purposes. Locally created SQL user accounts and login information, on the other hand, is not centrally managed through the enterprise Active Directory and not commonly monitored by SIEM. Adding the log for the locally created SQL user account will add to the processing load licensing cost for the SIEM servers. The practice of creating local SQL users also compels users to maintain separate Active Directory and SQL user accounts, compounding their password management effort. A unified single sign on approach through the 'Windows Authentication Model' reduces user security management workload and improves the integrity of the user management processes.

The following SQL command can be used to check the authentication setting:

SQL>

SELECT SERVERPROPERTY('IsIntegratedSecurityOnly') as [login_mode];

A login_mode of 1 indicates the Server Authentication property is set to Windows Authentication Mode.

A login_mode of 0 indicates mixed mode authentication.

The following SQL command can be used to

SQL>

USE [master]

GO

EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG_DWORD, 1

GO

8.2.3.2 Drop 'Orphaned Users' From SQL Server Databases

A database user for which the corresponding SQL Server login is undefined or is incorrectly defined on a server instance cannot log in to the instance. These user accounts are referred to as orphaned and should be removed to avoid potential misuse of those broken users in any way.

For example, the devastating ransomware attack against the Colonial Pipeline which exploited an unused VPN account is a timely reminder of the risks from the lack of maintenance on stalled accounts.

Audit the database user list using the following T-SQL query in each database to identify orphan users. The query should not return any identified users.

SQL>

USE <database_name>;

GO

EXEC sp_change_users_login @Action='Report';

Identified orphaned user can be revoked using the following T-SQL query in the identified database:

SQL>

USE <database_name>;

GO

DROP USER <username>;

8.2.3.3 Prohibit the use of SQL Authentication in contained databases

Contained databases do not enforce password complexity rules for SQL Authenticated users. The absence of an enforced password policy may increase the likelihood of a weak credential being established in a contained database. While contained databases provide flexibility in relocating databases to different instances and different environments, this must be balanced with the consideration that no password policy mechanism exists for SQL Authenticated users in contained databases.

Regularly audit the existence of contained database using SQL authentication with the following SQL command:

SQL>

SELECT name AS DBUser

FROM sys.database_principals

WHERE name NOT IN ('dbo','Information_Schema','sys','guest') AND type IN ('U','S','G') AND authentication_type = 2;

GO

8.2.4 Using non-default ports for remote database connections

WMS Pro installation provides an advanced SQL configuration. If your SQL server instance has TCP enabled with default port 1433, consider using a non-standard port. Attackers commonly scan for the default port to identify potential database servers to exploit. Changing the port makes it significantly harder for automated scans and unsophisticated attackers to find your database.

8.2.4.1 In SQL Server Configuration Manager, in the console pane, expand SQL Server Network Configuration, expand Protocols for <InstanceName>, and then double-click the TCP/IP protocol.

8.2.4.2 In the TCP/IP Properties dialog box, on the IP Addresses tab, several IP addresses appear in the format IP1, IP2, up to IPAll. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP Address on the computer.

8.2.4.3 Under IPAll, change the TCP Port field from 1433 to a non-standard port or leave the TCP Port field empty and set the TCP Dynamic Ports value to 0 to enable dynamic port assignment and then click OK. When using dynamic TCP ports in SQL Server, the server selects an available port at startup, and clients need to know that port to connect. Since dynamic ports can change after each restart, you do not include the port number directly in the connection string. Instead, you rely on the SQL Server Browser service to resolve the correct port.

Connection String Format (for dynamic TCP port):
Server=hostname\instance_name;Database=YourDatabase;Integrated Security=True;

Requirements:

1. SQL Server Browser service must be running – It listens on UDP port 1434 and tells clients which port the named instance is using.
2. Client must specify the instance name – That's how the browser service knows what to look up.
3. Firewall must allow UDP port 1434 – So the SQL Server Browser can respond to connection requests.

8.2.4.4 In the console pane, click SQL Server Services. In the details pane, right-click SQL Server () and then click Restart, to stop and restart SQL Server. Using a non-default port requires configuring the database server to listen on that port and all client applications that need to connect to the database to specify the non-default port in their connection strings. You need to ensure that the firewall is configured to allow traffic on the non-default port you've chosen.

8.2.5 Disable unnecessary SQL server protocols

Ensure unnecessary SQL server protocols are set to 'Disabled':

SQL Server supports Shared Memory, Named Pipes, and TCP/IP protocols. However, SQL Server should be configured to use the bare minimum required based on the organization's needs. The Database Engine (MSSQL and SQLAgent) services must be stopped and restarted for the changes to take effect.

8.2.6 Restrict network access to the database server

To reduce the attack surface of your system, limit network access to the database server. Potential measures include:

- Configuring firewall rules to allow traffic only for authorized IP addresses and ports
- Using network segmentation to place the database server in a more secure environment

8.2.7 Deployment

8.2.7.1 Disable ad hoc distributed queries

This feature can be used to remotely access and exploit vulnerabilities on remote SQL Server instances and to run unsafe visual basic for application functions.

Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0': Enabling Ad Hoc Distributed Queries allows users to query data and execute statements on external data sources. This functionality should be disabled.

SQL>

EXECUTE sp_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp_configure 'Ad Hoc Distributed Queries', 0;

RECONFIGURE;

GO

EXECUTE sp_configure 'show advanced options', 0;

RECONFIGURE;

Verify that ad hoc distributed queries are disabled:
SQL>

SELECT name, CAST(value as int) as value_configured, CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'Ad Hoc Distributed Queries';

Both value columns must show 0.

8.2.7.2 Disable CLR

CLR Assemblies are DLL files used in an instance of SQL Server to deploy functions, stored procedures, triggers and more that are written in one of the managed languages hosted by the Microsoft .NET Framework common language runtime (CLR). Enabling use of CLR assemblies widens the attack surface of SQL Server and puts It at risk from both inadvertent and malicious assemblies.

Ensure 'CLR Enabled' Server Configuration Option is set to '0':
If CLR assemblies are in use, applications may need to be re architected to eliminate their usage before disabling this setting. Alternatively, some organizations may allow this setting to be enabled 1 for assemblies created with the SAFE permission set, but disallow assemblies created with the riskier UNSAFE and EXTERNAL_ACCESS permission sets. To find user-created assemblies, run the following query in all databases, replacing `<databasename>`_ with each database name:

SQL>

USE [_<database_name>_]

GO

SELECT name AS Assembly_Name, permission_set_desc

FROM sys.assemblies

WHERE is_user_defined = 1;

Verify that CLR is disabled:

SQL>
SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'clr enabled';

Both value columns must show 0 to be compliant.

8.2.7.3 Disable 'Ole Automation Procedures' option

Enabling this option will increase the attack surface of SQL Server and allow users to execute functions in the security context of SQL server.

Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0': The Ole Automation Procedures option controls whether OLE Automation objects can be instantiated within Transact-SQL batches. These are extended stored procedures that allow SQL Server users to execute functions external to SQL Server.
SQL>

EXECUTE sp_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp_configure 'Ole Automation Procedures', 0;

RECONFIGURE;

GO

EXECUTE sp_configure 'show advanced options', 0;

RECONFIGURE;

Verify that 'Ole Automation Procedures' is disabled:

SQL>

SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'Ole Automation Procedures';

Both value columns must show 0 to be compliant.

8.2.7.4 Disable 'Remote Access' option

Functionality can be abused to launch a Denial-of-Service (DoS) attack on remote servers by off-loading query processing to a target.

Ensure 'Remote Access' Server Configuration Option is set to '0': The remote access option controls the execution of local stored procedures on remote servers or remote stored procedures on local server. As per Microsoft this feature will be removed in the next version of Microsoft SQL Server. Do not use this feature in new developments and update applications that are currently using this feature with sp_addlinkedserver.
SQL>

EXECUTE sp_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp_configure 'remote access', 0;

RECONFIGURE;

GO

EXECUTE sp_configure 'show advanced options', 0;

RECONFIGURE;

Verify that 'Remote Access' is disabled:
SQL>

SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'remote access';

Both value columns must show 0.

8.2.7.5 Disable 'sa' login account

Not disabling a SQL server account with sysadmin privileges increases the probability of an attacker executing brute force attacks against a well-known principal.

Ensure the 'sa' Login Account is set to 'Disabled':

The sa account is a widely known and often widely used SQL Server account with sysadmin privileges. This is the original login created during installation and always has the principal_id=1 and sid=0x01.

SQL>

USE [master]

GO

DECLARE @tsql nvarchar(max)

SET @tsql = 'ALTER LOGIN ' + SUSER_NAME(0x01) + ' DISABLE'

EXEC (@tsql)

Use the following syntax to determine if the sa account is disabled. Checking for sid=0x01 ensures that the original sa account is being checked in case it has been renamed per best practices.

Run the following T-SQL command:

SQL>

SELECT name, is_disabled

FROM sys.server_principals

WHERE sid = 0x01

AND is_disabled = 0;

No rows should be returned to be compliant. An is_disabled value of 0 indicates the login is currently enabled and therefore needs remediation.

8.2.7.6 Disable 'xp_cmdshell' option

The xp_cmdshell procedure is commonly used by attackers to read or write data to/from the underlying Operating System of a database server.

Ensure 'xp_cmdshell' Server Configuration Option is set to '0':

The xp_cmdshell option controls whether the xp_cmdshell extended stored procedure can be used by an authenticated SQL Server user to execute operating-system command shell commands and return results as rows within the SQL client.

SQL>

EXECUTE sp_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp_configure 'xp_cmdshell', 0;

RECONFIGURE;

GO

EXECUTE sp_configure 'show advanced options', 0;

RECONFIGURE;

Verify that 'xp_cmdshell' option is disabled:

SQL>

SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'xp_cmdshell';

Both value columns must show 0 to be compliant.

8.2.7.7 Do not grant access to SQL Agent proxies to the 'public' role

Granting access to SQL Agent proxies for the public role would allow all users to utilize the proxy which may have high privileges. This would likely break the principle of least privileges.

Ensure the public role in the msdb database is not granted access to SQL Agent proxies: The public database role contains every user in the msdb database. SQL Agent proxies define a security context in which a job step can run. Before revoking the public role from the proxy, ensure that alternative logins or appropriate user-defined database roles have been added with equivalent permissions. Otherwise, SQL agent job steps dependent upon this access will fail.

1. Ensure the required security principals are explicitly granted access to the proxy (use sp_grant_login_to_proxy).
2. Revoke access to the <*preoxyname*> from the public role.

SQL>

USE [msdb]

GO

EXEC dbo.sp_revoke_login_from_proxy @name = N'public', @proxy_name = N'_<proxyname>_';

Verify that 'public' role does not have access permissions to SQL Agent proxies. Use the following syntax to determine if access to any proxies have been granted to the msdb database's public role.

SQL>

USE [msdb]

GO

SELECT sp.name AS proxyname

FROM dbo.sysproxylogin spl

JOIN sys.database_principals dp

ON dp.sid = spl.sid

JOIN sysproxies sp

ON sp.proxy_id = spl.proxy_id

WHERE principal_id = USER_ID('public');

GO

This query should not return any rows.

8.2.7.8 Disable cross-database ownership chaining across all databases or at the server level

Enabling this option allows a member of the db_owner role in a database to gain access to objects owned by a login in any other database, causing an unnecessary information disclosure.

Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0': The cross db ownership chaining option controls cross-database ownership chaining across all databases at the instance (or server) level.

Run the following T-SQL command:
SQL>

EXECUTE sp_configure 'cross db ownership chaining', 0;

RECONFIGURE;

If required, Cross-database ownership chaining should only be enabled for the specific databases at instance level by using the command ALTER DATABASE_<database_name>_SET DB_CHAINING ON . This database option may not be changed on the master, model, or tempdb system databases.

8.2.7.9 Disable scanning for startup processes

Enforcing this control reduces the threat of an entity leveraging these facilities for malicious purposes.

Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0':

The scan for startup procs option, if enabled, causes SQL Server to scan for and automatically run all stored procedures that are set to execute upon service startup.

Setting scan for startup procedures to 0 will prevent certain audit traces and other commonly used monitoring stored procedures from re-starting on start up. Additionally, replication requires this setting to be enabled (1) and will automatically change this setting if needed.

SQL>

EXECUTE sp_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp_configure 'scan for startup procs', 0;

RECONFIGURE;

GO

EXECUTE sp_configure 'show advanced options', 0;

RECONFIGURE;

Restart the Database Engine.

Verify that scanning for startup processes is disabled:
SQL>

SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'scan for startup procs';

Both value columns must show 0.

8.2.7.10 Use Transparent Data Encryption with Enterprise Databases

The lack of Transparent Data Encryption (TDE) in databases can expose sensitive data to various vulnerabilities. Implementing TDE will decrease the attack surface and is aligned with the defense-in-depth principle.

TDE allows for seamless decryption during access, managed through the database's administrative interface. It protects against network attacks and theft of storage media by ensuring data remains encrypted until accessed by authorized users, enhancing overall security.

Enable TDE for entire tables, columns within a table, and or individual cells within a table when appropriate.

Note: TDE is implemented differently in each enterprise database product. Check the documentation to find out how to implement it in your environment.

8.2.7.11 Disable remote admin connections by default

The Dedicated Administrator Connection (DAC) allows an administrator to access a running server to execute diagnostic functions or Transact-SQL statements, or to troubleshoot problems on the server, even if the server is locked or running in an abnormal state and not responding to a SQL Server Database Engine connection. In a cluster scenario, the administrator may not actually be logged on to the same node that is currently hosting the SQL Server instance and thus is considered "remote". Therefore, this setting should usually be enabled (1) for SQL Server failover clusters; otherwise it should be disabled (0) which is the default.

Ensure 'Remote Admin Connections' Server Configuration Option is set to '0': The remote admin connections option controls whether a client application on a remote computer can use the Dedicated Administrator Connection (DAC).

Note: You can keep this option enabled only for failover clusters in Microsoft SQL Server

SQL>

EXECUTE sp_configure 'remote admin connections', 0;

RECONFIGURE;

Verify that remote admin connections are disabled by default:
SQL>

USE master;

GO

SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'remote admin connections'

AND SERVERPROPERTY('IsClustered') = 0;

If no data is returned, the instance is a cluster and this recommendation is not applicable. If data is returned, then both the value columns must show 0 to be compliant. Note that this option may be enabled only for failover clusters in Microsoft SQL Server.

8.2.7.12 Disable remote admin connections by default

The Dedicated Administrator Connection (DAC) allows an administrator to access a running server to execute diagnostic functions or Transact-SQL statements, or to troubleshoot problems on the server, even if the server is locked or running in an abnormal state and not responding to a SQL Server Database Engine connection. In a cluster scenario, the administrator may not actually be logged on to the same node that is currently hosting the SQL Server instance and thus is considered "remote". Therefore, this setting should usually be enabled (1) for SQL Server failover clusters; otherwise it should be disabled (0) which is the default.

Ensure 'Remote Admin Connections' Server Configuration Option is set to '0': The remote admin connections option controls whether a client application on a remote computer can use the Dedicated Administrator Connection (DAC).

Note: You can keep this option enabled only for failover clusters in Microsoft SQL Server

SQL>

EXECUTE sp_configure 'remote admin connections', 0;

RECONFIGURE;

Verify that remote admin connections are disabled by default:
SQL>

USE master;

GO

SELECT name,

CAST(value as int) as value_configured,

CAST(value_in_use as int) as value_in_use

FROM sys.configurations

WHERE name = 'remote admin connections'

AND SERVERPROPERTY('IsClustered') = 0;

If no data is returned, the instance is a cluster and this recommendation is not applicable. If data is returned, then both the value columns must show 0 to be compliant. Note that this option may be enabled only for failover clusters in Microsoft SQL Server.

8.3 Windows 10/11 Server Hardening

Windows 10 was released in 2015 to replace the aging Windows 7 & 8.1 operating system which was the dominant enterprise desktop platform at the time. By January 2018, Windows 10 surpassed Windows 7 as the most popular version of Windows worldwide. As of August 2022, Windows 10 is estimated to have a 72% share of Windows PCs still, 6.2 times the share of its successor Windows 11 (and 6.0 times that of Windows 7).

Windows 11 offers a number of functional improvements and security enhancements. According to Windows Insider Blog[1], Windows 11 improves security protection by leveraging the Trusted Platform Module (TPM), UEFI Secure Boot features and Virtualisation-based security (VBS). However, the focus of this section is not to explain the details and strengths of these security capability uplifts, but to examine how to utilise these capabilities to harden the protection of the WMS Pro server. Fortunately, the hardening approach between Windows 10 and Windows 11 is essentially identical. The following section summarises some of the key recommendations.

Account Management Policies

Password and lockout are the two primary discretionary hardening options for the protection of user accounts. Microsoft recommends and makes available password-less authentication[2] enablement tools in these operating systems. However, implementing universal password-less authentication across the infrastructure is still not a technical reality today, and likely not anytime soon, as discussed in the post "The Truth about Passwordless Authentication. What it is and how it works"[3]. Passwords will remain a fixture in the authentication system and good cyber hygiene must be enforced through the hardening process. Some of the pragmatic configuration guidelines include:

- Password management hygiene: Enforce password history to 24 or more passwords
- Set maximum password age to 365 or fewer days, but not 0
- Set minimum password age 1 or more days
- Set minimum password length 9-14 or more characters
- Configure and enforce password complexity requirement rule
- Disable store passwords using reversible encryption

Account lock out management:

- Set Account lockout duration to 15 or more minutes
- Set Account lockout threshold to 5 or fewer invalid login attempts but not 0
- Enforce Administrator account lockout
- Configure account lockout reset timeout to 15 minutes or longer

[1] https://blogs.windows.com/windows-insider/2021/08/27/update-on-windows-11-minimum-system-requirements-and-the-pc-health-check-app/

[2] https://www.microsoft.com/en-us/security/business/solutions/passwordless-authentication

[3] https://www.onelogin.com/learn/passwordless-authentication

User Rights Assignment:

- Set 'Access Credential Manager as a trusted caller' to 'No One'
- Set 'Access this computer from the network' to 'Administrators, Remote Desktop Users'
- Set 'Act as part of the operating system' to 'No One'
- Set 'Adjust memory quotas for a process' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'
- Set 'Allow log on locally' to 'Administrators, Users'
- Set 'Allow log on through Remote Desktop Services' to 'Administrators, Remote Desktop Users'
- Set 'Back up files and directories' to 'Administrators'
- Set 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)
- Set 'Change the time zone' to 'Administrators, LOCAL SERVICE, Users'
- Set 'Create a pagefile' to 'Administrators'

8.3.1 Domain security

- Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled'
- Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled'
- Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled'
- Set 'Domain member: Disable machine account password changes' to 'Disabled'
- Set 'Domain member: Maximum machine account password age' to '30 or fewer days, but not 0'
- Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled'
- Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'
- Set 'Interactive logon: Don't display last signed-in' to 'Enabled'
- Set 'Interactive logon: Machine account lockout threshold' to '10 or fewer invalid logon attempts, but not 0'
- Set 'Interactive logon: Machine inactivity limit' to '900 or fewer second(s), but not 0'
- Create 'Interactive logon: Message text for users attempting to log on'
- Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'
- Set 'Interactive logon: Prompt user to change password before expiration' to 'between 5 and 14 days'
- Set 'Interactive logon: Smart card removal behaviour' to 'Lock Workstation' or higher

8.3.2 Microsoft network hardening

- Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'
- Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled' Microsoft doesn't recommend using this group policy setting.
- Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'
- Set 'Microsoft network server: Amount of idle time required before suspending is set to 'Enabled'
- Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'
- Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled'
- Set 'Microsoft network server: Server SPN target name validation level' to 'Accept if provided by client' or higher'
- Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled'
- Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'
- Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'
- Set 'Network access: Do not allow storage of passwords and credentials for network authentication' to 'Enabled'
- Set 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'
- Set 'Network access: Named Pipes that can be accessed anonymously' to 'None'
- Configure 'Network access: Remotely accessible registry paths'
- Configure 'Network access: Remotely accessible registry paths and sub-paths'
- Set 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'
- Set 'Network access: Restrict clients allowed to make remote calls to SAM' to 'Administrators: Remote Access: Allow'
- Set 'Network access: Shares that can be accessed anonymously' to 'None'
- Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves'
- Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'
- Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'
- Set 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' to 'Disabled'
- Set 'Network security: Configure encryption types allowed for Kerberos' to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'
- Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'

- Set 'Network security: Force logoff when logon hours expire' to 'Enabled'
- Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'
- Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' or higher

8.4 Wi-Fi/LAN hardening

The network infrastructure which WMS Pro is connected to could expose the platform to malicious attack or misuse. The hardening instructions in the previous sections enhance the overall cyber hygiene of these platforms. However, software updates or unintended side effects from approved configuration changes can potentially override these security best practices or introduce unexpected behaviour.. Some of these configurations could become incompatible with future platform software releases or changes to business functionality requirements. A Defence In Depth architectural approach where the network environment is hardened in a manner compatible with the platform and application requirements is a strongly recommended and more durable approach.

8.4.1 Defining a secure network

The first and most important step in hardening the network environment is establishing an understanding of the connectivity of the application and platform environments, including maintenance access. Given this understanding, a secure network baseline could then be composed.

For example, the widespread automated malware exploitation in 2023 against vulnerable VMWare ESXi Hypervisor consoles[4] directly exposed to the Internet highlights the lurking danger of oversights in securing privileged remote entry points. The lesson learnt is not exposing these privileged entry points without compelling business or functional reasons. Remote access to the platform and application is often part of the functional requirement, including containing the cost of remote delivery of management and maintenance services. A documented and considered design for remote access is the foundation for defining the secure network.

Place the web application server in a separate DMZ (demilitarised zone) network, isolating it from internal systems.

[4] https://blog.qualys.com/vulnerabilities-threat-research/2023/02/07/ransomware-targets-outdated-vmware-esxi-hypervisors-protect-your-systems-now

8.4.1.1 Asset inventory

No assumption should be made about the completeness of the asset inventory in the targeted network environment. It is common for networks infrastructure to be shared between projects and application environments. The provision and policing of test environments are particularly problematic and often not strongly enforced. A regular active asset-based network discovery scan is strongly recommended to confirm the network environment and to identify the presence of unauthorised devices. Wi-Fi connectivity should be prohibited in the server network unless specifically authorised. Insecure Wi-Fi network is more easily exploited due to the reduction of physical access requirements beyond the radio range of the Wi-Fi network. High gain Wi-Fi antenna is often used to Wi-Fi network at a distance beyond the physical control space associated with the protected network. Therefore, prohibiting the presence of Wi-Fi network connectivity with direct connection to the server network will reduce the operation cost in hardening the Wi-Fi network.

8.4.1.2 Protocol requirement inventory

Equally, an inventory of the approved connectivity patterns expressed in the format of:

Source IP address	Destination IP address	Protocol & Network Port number

is an important artefact in documenting the definition of a secure network. The inventory might identify weak protocols vulnerable to malicious attacks. The granularity of the source/destination IP address specification will also increase the operational cost of securing the network. Narrowing the IP address to a single host might sound like offering maximum protection. But this is a paradox due to the inevitable changes to the network environments necessitating the changes of host IP addresses or even relocation to a different subnet. Tracking these approved access patterns through all the firewall rules and Access Control List is a futile and frustrating experience. These frustrations often encourage the opposite behaviour in over-provisioning the access patterns to cater for these foreshadowed changes. This weakening of the approved connectivity pattern is often not properly risk assessed but for operational convenience with unqualified risk exposure.

Firewall Configuration:

- Only allow necessary inbound/outbound traffic to/from the web server.
- Block all unused ports; ensure HTTPS (port 443) and TCP port 13000 are enabled for web traffic.

8.4.1.3 Audit firewall rules and access control list

Armed with an asset and protocol requirement inventory, the organisation should undertake a regular audit of the compliance of the firewall rules and access control list of all devices in the connectivity path. However, the variation in the format of firewall rules and access control lists between different devices could present a logistic challenge to this assurance process. Some security audit tools offer a feature normalising these different device-specific access control specification formats to ease the audit and analysis process. Care and training are needed to understand these normalisation mapping processes, which could give rise to a false sense of assurance.

8.5 Web Server Security

8.5.1 Disable Unused Services:

- Turn off any services or modules not in use (e.g., FTP, WebDAV - Web Distributed Authoring and Versioning).

8.5.2 Secure USB Ports:

Secure USB ports to decrease the threats of enabled ports:

- Set the USB port as a dedicated charging port by default. Ensure that a device plugged in is enumerated as a Dedicated Charging Port (DCP) by default.

Protect USB mounting for upload or download with a console password. That is, change the enumeration mode to Charging Downstream Port (CDP) only after entering the correct password.

8.5.3 Run as a Non-Root User:

- Install and Configure as Admin, Run as Least Privileged User. Limit Administrative Access to the Server.
- After installation and initial configuration, run the web server using a dedicated non-administrative service account. Running as root/admin can expose the entire system to risk if the web server is compromised. A lower-privilege account limits the damage that attackers can do. Use a service account with minimal privileges for the application pool. The default identity (ApplicationPoolIdentity) is sufficient in many cases, but you can create a custom service account with just the permissions needed.
- Separate Administrative Tasks from Daily Operations: Use administrative privileges for management actions (e.g., software updates, configuration changes), but switch to non-admin users for daily web operations. 5
- Use Role-Based Access Control (RBAC): For managing web server settings, configure accounts with specific permissions needed for those tasks, rather than giving full administrative privileges to all users.5
- Elevate Privileges Temporarily: WMS Pro server manager requires administrative privileges for occasional tasks, grant them only when necessary. Use Windows User Account Control (UAC) to elevate privileges as need.
- Privilege Separation for Web Server Processes: Keep processes like worker processes (handling user requests) running as non-admin users, while keeping management processes separate and with necessary privileges. 5
- Restrict File System Access: Ensure the web server service account only has access to necessary directories and files. Deny write access where it's not needed.
- Use widely recommended TLS 1.2 and 1.3. Disable deprecated protocols TLS 1.0 and 1.1. Please note that the earlier versions of CTPlus cannot be installed on a PC locked down to TLS 1.2.

8.6 ASP.NET and Windows Desktop .NET Core Runtime Patching

8.6.1 .NET Version Compatibility

Important! Do not upgrade to a different major version (e.g. .NET 10 → .NET 11) without a corresponding WMS Pro update — major version upgrades require a new WMS Pro release. See the compatibility table below.

WMS Pro Version	.NET Runtime version
3.0-3.2	8.0.x
3.3-4.x	10.0.x

8.6.2 .NET Runtime Patching

WMS Pro uses the Framework-Dependent Deployment (FDD) model, meaning it relies on the Windows Desktop .NET Core and ASP.NET Core runtime installed on the host server. Microsoft releases monthly security patches for the .NET runtime. You should apply these patches regularly to protect against known vulnerabilities.

Check Current Runtime Version
Before patching, confirm the currently installed runtime version:
dotnet --list-runtimes
Look for lines starting with Microsoft.AspNetCore.App, Microsoft.NETCore.App and Microsoft.WindowsDesktop.App. Note the version numbers.
Check the latest available version at:
Download .NET 10.0 (e.g.) | .NET

Patch Procedure

1. Notify Users

Inform operators that WMS Pro will be briefly unavailable. The downtime is typically under 5 minutes.

2. Stop the WMS Pro Application

Open IIS Manager (inetmgr):

1. Expand the server node → Sites
2. Select the WMS Pro site
3. In the Actions panel (right side), click Stop

Then stop the application pool:

1. In IIS Manager → Application Pools
2. Right-click the WMS Pro app pool → Stop

Alternatively, from an elevated command prompt:
%windir%\system32\inetsrv\appcmd stop site /site.name:"WMS Pro"
%windir%\system32\inetsrv\appcmd stop apppool /apppool.name:"WMS Pro"

3. Stop IIS

From an elevated command prompt:
iisreset /stop
Wait for the confirmation message:
Internet services successfully stopped.
Stopping IIS fully releases the runtime DLLs so the installer can replace them without file-lock errors.

4. **Download both installers from** [Download .NET 10.0 (e.g.) | .NET]

Package	Used for
dotnet-hosting-10.0.x-win.exe	IIS ANCM + ASP.NET Core runtime
windowsdesktop-runtime-10.0.x-win-x64.exe	WinForms desktop apps (SCP interface, DB Manager, Migrator)

5. Run both installers as Administrator, in this order:

dotnet-hosting-10.0.x-win.exe first — installs/updates ANCM and the core runtimes
windowsdesktop-runtime-10.0.x-win-x64.exe second — adds Windows Desktop runtime on top
The order matters slightly — the Hosting Bundle should go first since it lays down the shared framework components that windowsdesktop-runtime builds on. When the installer completes, run the following to flush IIS configuration:
net stop was /y
net start w3svc

6. Restart IIS

iisreset /start
Wait for: Internet services successfully restarted.

7. Restart the Application Pool and Site

In IIS Manager:

1. Application Pools → right-click the WMS Pro app pool → Start
2. Sites → select the WMS Pro site → Start

Or from command prompt:
%windir%\system32\inetsrv\appcmd start apppool /apppool.name:"WMS Pro"
%windir%\system32\inetsrv\appcmd start site /site.name:"WMS Pro"

8. Verify

Confirm the new runtime is active:
dotnet --list-runtimes
Open a browser and navigate to the WMS Pro login page to confirm the application is responding.
Check the WMS Pro log for any startup errors:
C:\ProgramData\WMSPro\commslog_<YYYYMMDD>.txt

Recommended Patch Cadence

Trigger	Action
Microsoft Patch Tuesday (second Tuesday of each month)	Check if a new .NET patch has been released
Any .NET CVE rated High or Critical	Patch within 7 days
WMS Pro installer update	Hosting Bundle update may be included — check release notes

Notes

- Installing a newer patch of the same major version (e.g. 10.0.2 → 10.0.12) is non-breaking. WMS Pro does not need to be rebuilt or redeployed.
- The runtime installers are safe to re-run if the same version is already installed — they will detect no change and exit cleanly.
- If WMS Pro is running in embedded mode (comms engine inside the web host process), stopping IIS also stops panel communications. Plan the maintenance window accordingly.