



eXLent #HMI - Cyber Security Manual

Disclaimer of Liability

ABB BV makes every effort to deliver high quality products & software; this document is
ABB BV does not guarantee that the products/software are free from defects.
Ltd., and may
The software is provided 'as is', and customer use the software at customer's own risk.
part) used
This product/software is designed to be connected to and to communicate information and
consent of ABB
data via one or multiple network interfaces. It is customer's sole responsibility to
condition only
provide and continuously ensure a secure connection between the product and customer
any
network or any other network (as the case may be). Customer shall establish and maintain
copyright and
any appropriate measures (such as but not limited to the installation of firewalls,
copying, use and
application of authentication measures, encryption of data, installation of anti-virus
in which this
programs, establish procedures to scan for malware on a regular basis, etcetera) to
including
protect the product/software, the network, its system and the interface against any kind
of security breaches, unauthorized access, interference, intrusion, leakage and/or theft
of data or information. ABB BV and its affiliates are not liable for damages and/or
losses related to such security breaches, any unauthorized access, interference,
Switzerland Ltd.
intrusion, leakage and/or theft of data or information.
trademark

Special Note

The information contained in
the property of ABB Switzerland
not be reproduced (wholly or in
or disclosed without the prior
Switzerland Ltd. and then on
that this notice is included in
reproduction or disclosure. The
the foregoing restriction on
disclosure extent to all media
information may be embodied
magnetic storage.
Printed in the Netherlands.
Copyright © 2025, ABB
(R) eXLent is an ABB registered

Purpose of this document

This document provides an introduction to cyber security best practices for eXLent #HMI, covering key topics and recommendations for securing your installation and protecting your data.

By implementing these best practices, you can reduce the risk of security breaches, data loss, and system downtime, ensuring the continued safe and reliable operation of your eXLent #HMI system.

Document Conventions

When in this manual a symbol as displayed at the left appears in the text, certain specific operating instructions are given to the user. In such a case, the user is assumed to perform some action, such as the selection of a certain object, or typing on the keyboard.

Important remarks are denoted by this symbol.

Warnings are accompanied by this symbol.

Instruction for use

It is crucial to remember that every aspect of your eXLent #HMI system, from installation and configuration to ongoing maintenance and operation, can have implications for your overall security posture.

As you work through the manual, always keep the principles of cyber security as described in the [eXLent #HMI cyber security manual](#) in mind, applying best practices and taking the necessary precautions to protect your system from potential threats. Maintaining a strong focus on cyber security will help ensure the safety, reliability, and performance of your eXLent #HMI system.

Key Cyber Security Topics

The following topics are covered in this guide:

- 1. Defense in Depth Architecture** : Understand eXLent #HMI's comprehensive multi-layered security strategy and how seven distinct security layers work together to provide robust protection against various attack vectors.
- 2. Security Control Mapping** : Learn how all security controls in eXLent #HMI map to specific defense layers and work together to create a cohesive security architecture with redundant protections.
- 3. Securing Network Communications** : Learn how to configure firewalls and secure network connections to protect eXLent #HMI from unauthorized access and potential attacks.
- 4. System Hardening** : Discover how to strengthen the security of the underlying Windows operating system by disabling unnecessary services, enabling encryption, and implementing strong password policies.
- 5. Strong Passwords for eXLent #HMI Services** : Understand the importance of using strong, randomly generated passwords for all service accounts and sensitive configurations within eXLent #HMI.
- 6. Regular Backups** : Implement a comprehensive backup strategy to ensure the availability and integrity of your eXLent #HMI data in the event of hardware failure, software issues, or malicious attacks.
- 7. Keeping eXLent #HMI Updated** : Keep your eXLent #HMI installation updated to the latest version, taking advantage of important bug fixes, security patches, and new features.
- 8. Verifying the Integrity of Downloads** : Learn how to check the hash of downloaded eXLent #HMI installers to ensure their integrity and authenticity.
- 9. Use Secure Protocols** : Understand the risks of opting for insecure protocols.

By familiarizing yourself with these topics and implementing the recommendations provided in this guide, you can enhance the security of your eXLent #HMI system and protect your organization's valuable data and assets.

Cyber security is an ongoing process, and it is essential to regularly review and update your security practices to stay ahead of evolving threats and maintain the resilience of your systems.

Defense in Depth Architecture

Introduction to Defense in Depth

Defense in depth is a cybersecurity strategy that employs multiple layers of security controls throughout an information system. Rather than relying on a single security measure, this approach creates overlapping defenses that protect against various attack vectors and provide redundancy if one layer fails.

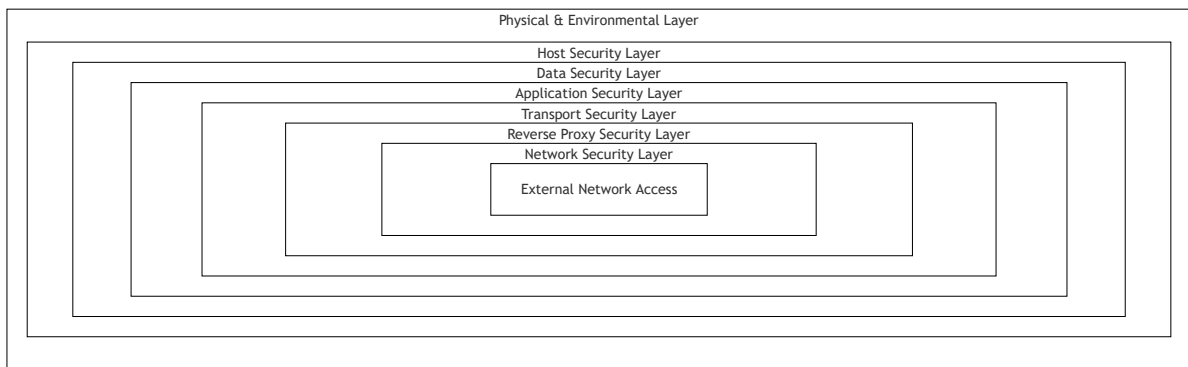
eXLent #HMI implements a comprehensive defense in depth architecture designed specifically for industrial environments where availability, integrity, and confidentiality are critical. This multi-layered approach ensures that even if one security control is compromised, additional layers continue to protect the system and its data.

eXLent #HMI Security Architecture Overview

The eXLent #HMI defense in depth model consists of seven distinct security layers, each providing specific protections and working together to create a robust security posture:

1. **Network Security Layer** - Perimeter defense and network segmentation
2. **Reverse Proxy Security Layer** - Application firewall and traffic filtering
3. **Transport Security Layer** - Encryption and secure communications
4. **Application Security Layer** - Authentication, authorization, and session management
5. **Host Security Layer** - Operating system and service hardening
6. **Data Security Layer** - Data protection at rest and in transit
7. **Physical & Environmental Layer** - Infrastructure and facility security

Security Layer Architecture



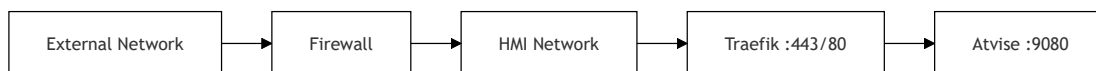
Layer 1: Network Security Layer

The network security layer provides perimeter defense and controls access to eXLent #HMI at the network level.

Security Controls:

- **Windows Defender Firewall:** Restricts inbound connections to essential ports (80, 443, optional Modbus ports)
- **Network Segmentation:** VLANs and network isolation to separate eXLent #HMI from other systems
- **Access Control Lists:** IP-based filtering and connection restrictions
- **Redundancy VPN:** WireGuard VPN for secure primary/secondary server communication

Network Architecture:



Threat Protection:

- Network-based attacks and unauthorized access attempts
- Lateral movement from compromised network segments
- Man-in-the-middle attacks on redundancy communications

Layer 2: Reverse Proxy Security Layer

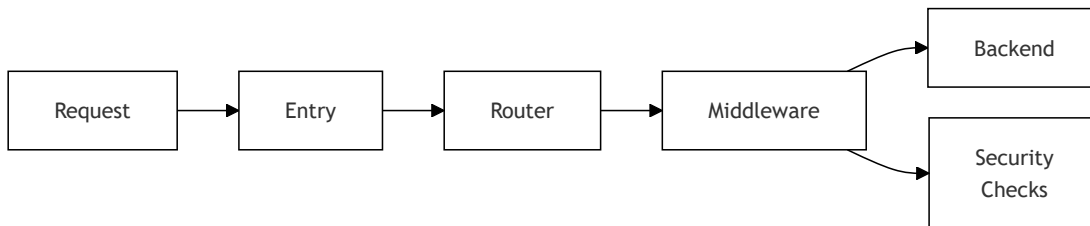
The Traefik reverse proxy acts as an application-level firewall, providing sophisticated traffic filtering and request validation

before requests reach the Atvise web server.

Security Controls:

- **HTTP Method Filtering:** Blocks dangerous methods (TRACE, TRACK)
- **Path Validation:** Prevents access to system files and hidden directories
- **Rate Limiting:** 100 requests/second average, 600 burst capacity
- **Request Size Limits:** Maximum 200KB request size to prevent DoS attacks
- **WebSocket Connection Limits:** Maximum 20 WebSocket connections per IP
- **Circuit Breakers:** Automatic failure protection when error rates exceed 50%
- **Custom Security Plugins:** Purpose-built security middleware

Request Processing Pipeline:



Threat Protection:

- Application-layer DDoS attacks
- Malformed request exploitation
- Directory traversal and file access attacks
- WebSocket abuse and connection flooding

Layer 3: Transport Security Layer

Ensures all communications are encrypted and authenticated using modern cryptographic standards.

Security Controls:

- **TLS 1.2+ Only:** Minimum TLS version enforcement
- **Strong Cipher Suites:** ECDHE with AES-256-GCM and ChaCha20-Poly1305
- **HTTPS Enforcement:** Automatic HTTP to HTTPS redirection
- **HSTS Headers:** Strict Transport Security with 1-year max-age
- **Certificate Management:** Self-signed or CA-signed certificate support
- **Client Certificates:** Optional mutual TLS authentication

Supported Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Threat Protection:

- Man-in-the-middle attacks
- Eavesdropping and traffic interception
- Protocol downgrade attacks
- Certificate spoofing attacks

Layer 4: Application Security Layer

Provides authentication, authorization, and session management controls within the eXLent #HMI application.

Security Controls:

- **User Authentication:** Username/password with configurable expiration

- **Role-Based Access Control:** Users, groups, and granular permissions
- **Session Management:** Secure session handling with login/logout tracking
- **Content Security Policy:** Comprehensive CSP headers preventing XSS
- **Security Headers:** Complete set of modern browser security headers
- **Input Validation:** Request sanitization and nonce-based protection

Security Headers Applied:

```
Content-Security-Policy: base-uri 'self'; frame-ancestors 'self';
  frame-src 'self'; form-action 'self'; default-src 'self';
  img-src 'self' blob: data:; object-src 'none';
  style-src 'self'; script-src 'self'; worker-src 'self'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Download-Options: noopen
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Referrer-Policy: same-origin
```

Threat Protection:

- Cross-site scripting (XSS) attacks
- Cross-site request forgery (CSRF)
- Session hijacking and fixation
- Clickjacking and frame injection
- Content type confusion attacks

Layer 5: Host Security Layer

Secures the underlying Windows operating system and eXlent #HMI services through hardening and access controls.

Security Controls:

- **Dedicated Service Accounts:** Each service runs under least-privilege accounts
- **BitLocker Encryption:** Full disk encryption for data protection
- **Windows Defender Antivirus:** Real-time malware protection
- **User Account Control:** Privilege escalation protection
- **Service Hardening:** Minimal permissions and unnecessary service disabling
- **Regular Updates:** Automated Windows and eXlent #HMI security patches

Service Account Architecture:

```
exlent-app-server    → Application Server Service
exlent-flowx-opcua  → Flow-X OPCUA Service
exlent-proxy        → Security Proxy Service
exlent-log-reader   → Log Access Service (read-only)
```

Threat Protection:

- Malware and virus infections
- Privilege escalation attacks
- Service exploitation
- Unauthorized system access
- Data theft from unencrypted storage

Layer 6: Data Security Layer

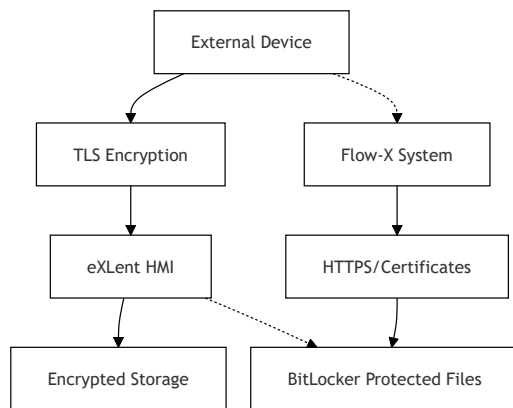
Protects data confidentiality and integrity throughout the system lifecycle.

Security Controls:

- **Encryption at Rest:** BitLocker full disk encryption
- **Encryption in Transit:** TLS for all network communications
- **Secure Backup:** Encrypted backup procedures with access controls
- **Certificate Protection:** Secure storage of TLS and client certificates

- **Configuration Security:** Protected storage of sensitive settings
- **Log Protection:** Secure logging with integrity controls

Data Flow Security:



Threat Protection:

- Data theft and unauthorized access
- Data tampering and corruption
- Information disclosure
- Backup compromise
- Configuration manipulation

Layer 7: Physical & Environmental Layer

Provides foundational security for the physical infrastructure and environment.

Security Controls:

- **Facility Security:** Secure server room access controls
- **Environmental Controls:** Temperature, humidity, and power monitoring
- **Hardware Security:** Secure hardware disposal and TPM utilization
- **Backup Storage:** Offsite secure backup storage
- **Disaster Recovery:** Comprehensive recovery procedures
- **Physical Access:** Restricted access to servers and network equipment

Threat Protection:

- Physical theft and tampering
- Environmental damage
- Unauthorized facility access
- Hardware compromise
- Data recovery attacks

Defense in Depth Effectiveness

The eXLent #HMI defense in depth architecture provides multiple benefits:

Redundant Protection: If one security layer fails, other layers continue to provide protection.

Attack Surface Reduction: Each layer reduces the available attack surface for potential threats.

Detection and Response: Multiple layers provide increased visibility and detection capabilities.

Compliance Support: Layered security supports regulatory compliance requirements.

Adaptability: Individual layers can be updated or enhanced without affecting the entire security posture.

Security Control Interdependencies

The security layers work together with specific interdependencies:

- **Network + Transport:** Firewall rules coordinate with TLS certificate requirements

- **Proxy + Application:** Reverse proxy headers enhance application security policies
- **Host + Data:** BitLocker encryption works with service account access controls
- **All Layers:** Logging and monitoring span across all security layers for comprehensive visibility

Built-in Security Advisory System

The eXLent #HMI installer includes an integrated security advisory system that automatically assesses the security posture of the target system and provides recommendations to strengthen defense in depth implementation.

Security Assessment Features

Drive Encryption Status Check:

- **BitLocker Detection:** Automatically scans for BitLocker encryption on system drives
- **Warning Indicators:** Displays prominent warnings when encryption is not detected
- **Remediation Guidance:** Provides specific recommendations for enabling drive encryption
- **Impact Assessment:** Explains security implications of unencrypted storage

Additional Security Recommendations:

- **Windows Security Features:** Validates Windows Defender, Firewall, and UAC status
- **Network Security:** Checks for proper network segmentation and access controls
- **Service Hardening:** Evaluates service account configurations and permissions
- **Update Status:** Verifies latest security patches and updates are installed
- **Backup Verification:** Confirms backup procedures and encryption status
- **Physical Security:** Reminds about facility and hardware security measures

Integration with Defense Layers

The security advisory system reinforces defense in depth by:

Layer 1 (Network Security):

- Validates firewall configurations and network isolation
- Recommends VPN setup for redundancy communications

Layer 5 (Host Security):

- Enforces BitLocker encryption requirements
- Checks service account security configurations
- Validates Windows security feature status

Layer 6 (Data Security):

- Ensures encryption at rest through BitLocker validation
- Verifies backup encryption procedures
- Confirms certificate protection measures

User Interface Design

Visual Indicators:

- **Warning Status:** Yellow warning indicators for security issues found
- **Completion Status:** Clear visual feedback when security measures are properly configured
- **Progressive Disclosure:** Detailed recommendations organized by security domain

User Experience:

- **Non-blocking:** Security advisory is informational and does not prevent installation
- **Contextual Help:** Provides direct links to relevant manual sections
- **Actionable Guidance:** Specific steps for addressing identified security gaps

Security Assessment Tools

The eXLent #HMI installer includes a comprehensive suite of PowerShell assessment tools designed to validate the effectiveness

of the defense in depth architecture across all security layers.

Comprehensive Assessment Framework

Master Assessment Command:

`Get-ExlentAssessment`

This command executes a complete security assessment covering all defense layers and provides immediate visibility into the system's security posture.

Layer-Specific Assessment Tools

Layer 1 (Network Security) Assessment:

- `Get-ActiveFirewallProfile` - Validates Windows Defender Firewall configuration
- `Get-ListeningTCPConnections` - Identifies active network services and potential exposure
- `Get-ListeningUDPConnections` - Analyzes UDP service security posture
- `Get-ExlentPublicPortList` - Evaluates public network service exposure

Layer 2 & 3 (Proxy & Transport Security) Assessment:

- Network connection analysis through TCP/UDP monitoring
- Port exposure evaluation for reverse proxy services
- Certificate validation through service status monitoring

Layer 4 (Application Security) Assessment:

- `Get-ExlentServiceStatus` - Validates service account configurations and security
- `Get-LocalGroupsWithMembers` - Audits user account and group membership
- Service authentication and authorization validation

Layer 5 (Host Security) Assessment:

- `Get-BitLockerStatus` - Comprehensive BitLocker encryption analysis
- `Get-AntiMalwareScanners` - Detects and validates 30+ antivirus solutions
- `Get-InstalledWindowsPatches` - Security update compliance verification
- Service account security validation

Layer 6 (Data Security) Assessment:

- `Get-ExlentFolderPermissions` - File system access control analysis
- BitLocker encryption status for data at rest protection
- Certificate and configuration file security validation

Layer 7 (Physical & Environmental) Assessment:

- Hardware security module (TPM) utilization through BitLocker validation
- Physical access control through service account analysis

Assessment Tool Features

Security-First Design:

- **Administrative Rights Verification:** All tools validate elevated privileges before execution
- **Error Handling:** Comprehensive exception handling with descriptive messages
- **Non-Destructive:** Read-only operations with no system modifications
- **Comprehensive Coverage:** Validates all defense in depth layers

Output Options:

- **Console Display:** Color-coded results for immediate visual assessment
- **JSON Export:** Structured data export for automation and integration
- **Detailed Reporting:** Comprehensive information for security auditing

Anti-Malware Detection Coverage:

The assessment tools detect 30+ antivirus and anti-malware solutions including:

- Windows Defender, Microsoft Security Essentials
- McAfee VirusScan, Sophos Anti-Virus
- Trend Micro, Avast, AVG, Norton Security
- Symantec Endpoint Protection, Kaspersky
- Bitdefender, ESET NOD32, F-Secure
- Panda Security, Webroot SecureAnywhere
- And many enterprise security solutions

Regular Assessment Procedures

Monthly Security Assessment:

Run comprehensive assessment and export results

```
Get-ExlentAssessment -json "monthly-assessment-$(Get-Date -Format 'yyyy-MM').json"
```

Quick Security Check:

Check critical security components

```
Get-BitLockerStatus
```

```
Get-ActiveFirewallProfile
```

```
Get-AntiMalwareScanners
```

```
Get-ExlentServiceStatus
```

Compliance Reporting:

Generate detailed security report for auditing

```
Get-ExlentAssessment -json "compliance-report.json"
```

Monitoring and Maintenance

Continuous monitoring ensures the defense in depth architecture remains effective:

- **Automated Security Assessment:** Regular execution of assessment tools
- **Log Aggregation:** Centralized logging from all security layers
- **Health Monitoring:** Automated checks for security control status using assessment scripts
- **Regular Audits:** Periodic comprehensive assessments using `Get-ExlentAssessment`
- **Update Management:** Coordinated updates across security controls with validation

Security Control Mapping to Defense Layers

Overview

This section maps all eXlent #HMI security controls to their respective defense in depth layers, showing how existing security measures work together to provide comprehensive protection. Each control is categorized by its primary function and layer assignment, with references to detailed implementation guidance elsewhere in this manual.

Layer 1: Network Security Controls

Security Control	Implementation	Manual Reference	Defense Function
Windows Defender Firewall	Inbound rules for ports 80, 443	§ Enable Windows Defender Firewall	Blocks unauthorized network access
Network Segmentation	VLANs and network isolation	§ Implement Network Segmentation	Prevents lateral movement
WireGuard VPN	Encrypted redundancy communication	Installation Manual - Redundancy	Secures inter-server communication
Access Control Lists	IP-based connection filtering	§ Enable Windows Defender Firewall	Restricts source IP addresses

Installation Security Controls

Security Control	Implementation	Manual Reference	Defense Function
Security Advisory System	Built-in installer assessment	§ Defense in Depth - Security Advisory	Validates security posture before installation
Protocol Security Warnings	HTTP insecurity warnings	§ Use Secure Protocols - Installer Warnings	Prevents accidental insecure configuration
Port Conflict Detection	Automatic port availability checking	Installation Manual	Prevents service conflicts and security gaps
Certificate Generation	Automatic TLS certificate creation	Installation Manual	Ensures encrypted communications from start
Service Account Creation	Least-privilege account setup	Installation Manual	Implements security by design
Security Hardening Steps	Automated security configuration	Installation Manual	Applies security best practices automatically

Layer 2: Reverse Proxy Security Controls

Security Control	Implementation	Manual Reference	Defense Function
HTTP Method Filtering	Traefik router rules block TRACE/TRACK	Traefik Configuration	Prevents HTTP verb tampering
Path Validation	Regex patterns block system files	Traefik Configuration	Prevents directory traversal
Rate Limiting	100 req/sec average, 600 burst	Traefik Middleware	Mitigates DoS attacks
Request Size Limits	200KB maximum request size	Custom Traefik Plugin	Prevents large payload attacks
WebSocket Limits	20 connections per IP address	Custom Traefik Plugin	Controls WebSocket abuse
Circuit Breakers	50% error rate threshold	Traefik Middleware	Provides automatic failover
Content Filtering	Static file access restrictions	Traefik Router Rules	Blocks unauthorized file access
Error Handling	Custom error pages and responses	Custom Traefik Plugin	Prevents information disclosure

Layer 3: Transport Security Controls

Security Control	Implementation	Manual Reference	Defense Function
TLS 1.2+ Enforcement	Traefik TLS configuration	§ Use Secure Protocols	Ensures strong encryption
Strong Cipher Suites	ECDHE with AES-256-GCM/ChaCha20	Traefik TLS Options	Provides perfect forward secrecy
HTTPS Redirection	Automatic HTTP to HTTPS redirect	Traefik Middleware	Prevents downgrade attacks
HSTS Headers	1-year Strict-Transport-Security	Traefik Security Headers	Enforces browser HTTPS use
Certificate Management	Self-signed or CA certificates	§ Use Secure Protocols	Enables server authentication
Client Certificates	Optional mutual TLS	§ Use Secure Protocols	Provides client authentication

Security Control	Implementation	Manual Reference	Defense Function
Flow-X Certificates	Custom certificate validation	§ Use Secure Protocols	Secures Flow-X communications

Layer 4: Application Security Controls

Security Control	Implementation	Manual Reference	Defense Function
User Authentication	Username/password with expiration	Administration Manual - Security	Verifies user identity
Role-Based Access Control	Users, groups, permissions	Administration Manual - Security	Enforces authorization
Session Management	Secure session tracking	Custom Traefik Plugin	Prevents session attacks
Content Security Policy	Comprehensive CSP headers	Traefik Security Headers	Prevents XSS attacks
Security Headers	Complete modern header set	Traefik Middleware	Blocks various web attacks
Input Validation	Request sanitization	Custom Traefik Plugins	Prevents injection attacks
Nonce Protection	Dynamic nonce generation	Custom Traefik Plugin	Enhances CSP effectiveness
Login/Logout Logging	Authentication event tracking	Custom Traefik Plugin	Provides audit trails
Authorization Removal	Auth header sanitization	Custom Traefik Plugin	Prevents credential leakage

Layer 5: Host Security Controls

Security Control	Implementation	Manual Reference	Defense Function
Dedicated Service Accounts	Least-privilege Windows accounts	§ Use Least Privilege Principle	Limits service permissions
BitLocker Encryption	Full disk encryption	§ Enable BitLocker Drive Encryption	Protects data at rest
Windows Defender Antivirus	Real-time malware protection	§ Enable Windows Defender Antivirus	Detects malicious software
User Account Control	Privilege escalation protection	§ Configure User Account Control	Prevents unauthorized elevation
Service Hardening	Minimal service permissions	Installation Manual	Reduces attack surface
Security Updates	Regular Windows patching	§ Apply Latest Security Patches	Fixes known vulnerabilities
Unnecessary Service Disabling	Attack surface reduction	§ Disable Unnecessary Services	Eliminates unused attack vectors

Layer 6: Data Security Controls

Security Control	Implementation	Manual Reference	Defense Function
Encryption at Rest	BitLocker full disk encryption	§ Enable BitLocker Drive Encryption	Protects stored data
Encryption in Transit	TLS for all communications	§ Use Secure Protocols	Protects data transmission
Secure Backup	Regular encrypted backups	§ Implement Regular Backups	Ensures data recovery
Certificate Protection	Secure certificate storage	§ Use Secure Protocols	Protects PKI infrastructure
Configuration Security	Protected configuration files	Installation Manual	Secures system settings
Log Protection	Secure audit logging	Maintenance Manual	Maintains integrity of logs
Access Controls	File system permissions	§ Use Least Privilege Principle	Controls data access

Layer 7: Physical & Environmental Controls

Security Control	Implementation	Manual Reference	Defense Function
Facility Security	Physical access controls	Organization Policy	Prevents unauthorized access
Hardware Security	TPM utilization	§ Enable BitLocker Drive Encryption	Provides hardware-based security
Backup Storage	Offsite backup storage	§ Implement Regular Backups	Protects against physical disasters
Disaster Recovery	Recovery procedures	§ Disaster Recovery Plan	Ensures business continuity
Environmental Controls	Power, cooling, monitoring	Organization Policy	Maintains system availability

Security Control Dependencies

Understanding how security controls depend on each other is crucial for maintaining defense in depth effectiveness:

Critical Dependencies

TLS Certificate Dependencies:

- Network firewall rules (Layer 1) must allow HTTPS traffic
- Certificate files (Layer 6) must be properly protected
- Certificate management (Layer 3) requires update procedures

Service Account Dependencies:

- Host security (Layer 5) creates service accounts
- File permissions (Layer 6) grant appropriate access
- Application security (Layer 4) uses these accounts

Backup Dependencies:

- BitLocker encryption (Layer 5) protects backup data
- Network security (Layer 1) secures backup traffic
- Physical security (Layer 7) protects backup storage

Control Interactions

Rate Limiting + Circuit Breakers:

- Rate limiting (Layer 2) prevents initial overload
- Circuit breakers (Layer 2) provide secondary protection
- Together they create resilient DoS protection

Authentication + Authorization:

- User authentication (Layer 4) verifies identity
- RBAC permissions (Layer 4) control access
- Session management (Layer 4) maintains state
- Service accounts (Layer 5) implement principle

Encryption Layers:

- TLS encryption (Layer 3) protects network traffic
- BitLocker encryption (Layer 5) protects stored data
- Certificate protection (Layer 6) secures key material

Validation and Testing

Each security control should be validated to ensure proper operation within the defense in depth architecture:

Layer Testing Commands

Installation Security Validation:

```
# Verify installer created security configurations
Get-Service | where { $_.Name -like 'exlent-*' } | select Name, Status
Test-Path "$env:ProgramData\ABB\exLent\security-proxy\certificates"
Get-Content "$env:ProgramData\ABB\exLent\security-proxy\dynamic-config\tls.yaml"
```

Network Layer Validation:

```
Get-NetFirewallRule | where { $_.Enabled -eq 'True' -and $_.Direction -eq 'Inbound' }
```

Host Layer Validation:

```
Get-LocalUser | where { $_.Name -like 'exlent-*' }
Get-BitLockerVolume
Get-MpComputerStatus
```

Application Layer Validation:

- Review security headers in browser developer tools
- Verify CSP policy effectiveness
- Test authentication and authorization

Continuous Monitoring

Security Assessment Scripts:

The eXlent #HMI installer includes comprehensive PowerShell assessment tools for security validation:

Core Assessment Tool:

- `Get-ExlentAssessment` - Master script that runs all security assessments
 - Supports console display or JSON export (`-json "filename.json"`)
 - Provides comprehensive system security posture evaluation

Individual Assessment Scripts:

- `Get-ActiveFirewallProfile` - Network layer status and firewall configuration
- `Get-BitLockerStatus` - Data encryption status with drive-specific analysis
- `Get-AntiMalwareScanners` - Host protection status covering 30+ antivirus products
- `Get-ExlentServiceStatus` - Service security status with service account validation
- `Get-ExlentFolderPermissions` - File access controls and permission analysis
- `Get-InstalledWindowsPatches` - Security update compliance verification
- `Get-ListeningTCPConnections` - Network service exposure assessment
- `Get-ListeningUDPConnections` - UDP service security analysis
- `Get-LocalGroupsWithMembers` - User account and group membership audit
- `Get-ExlentPublicPortList` - Public network exposure evaluation

Assessment Tool Usage:

```
# Run comprehensive assessment with console output
Get-ExlentAssessment

# Export comprehensive assessment to JSON
Get-ExlentAssessment -json "security-assessment.json"

# Run individual assessments
Get-BitLockerStatus -DriveLetter "C"
Get-ActiveFirewallProfile
Get-AntiMalwareScanners
```

Assessment Tool Features:

- **Administrative Rights Validation:** All tools verify elevated privileges before execution
- **Comprehensive Coverage:** Covers all seven defense in depth layers
- **JSON Export Capability:** Structured data export for integration with security tools
- **Color-Coded Output:** Visual indication of security status (Green=Good, Red=Issues)
- **Error Handling:** Robust exception handling with descriptive error messages

Log Monitoring:

- Network connection logs
- Authentication event logs
- Error and security logs
- Performance monitoring logs

Maintenance Procedures

Regular Security Reviews:

1. Validate all security controls monthly
2. Review security assessment reports
3. Update security configurations as needed
4. Test disaster recovery procedures quarterly

Update Coordination:

1. Plan updates across all security layers
2. Test updates in non-production environment

3. Coordinate certificate renewals
4. Maintain security control documentation

Incident Response:

1. Activate response procedures at appropriate layer
2. Isolate affected components
3. Implement additional controls as needed
4. Review and strengthen defense layers

Compliance Mapping

The defense in depth architecture supports various compliance requirements:

IEC 62443 Industrial Security:

- Zone and conduit model (Layers 1-2)
- Authentication and authorization (Layer 4)
- Data integrity and confidentiality (Layers 3, 6)
- System hardening (Layer 5)

***## System hardening

This guide provides an extensive overview of hardening a Windows system where eXlent #HMI will be installed. Hardening a system involves implementing security measures to reduce the attack surface and protect the system from potential threats. The steps outlined in this guide apply to Windows 10, Windows 11 and Windows Server 2022.

Applying Latest Security Patches and Updates

Keeping your operating system and installed software updated with the latest security patches is crucial to minimize vulnerabilities and protect your system from potential threats.

Regular updates help fix known security issues, improve performance, and maintain system stability. Here's how to apply updates for each operating system:

Windows 10 and Windows 11

1. **Check for updates manually:** Press **Win + I** to open the Settings app, and then navigate to "Update & Security" > "Windows Update." Click the "Check for updates" button to search for available updates. If any updates are found, install them and restart your system if prompted.
2. **Enable automatic updates:** In the "Windows Update" settings, make sure the "Automatically download updates, even over metered data connections (charges may apply)" option is enabled. This ensures that your system will automatically download and install updates as they become available.

Windows Server 2022

1. **Configure Windows Update:** Open the Server Manager, click on "Local Server" in the left pane, and find the "Windows Update" section. Click on the link next to "Windows Update" to open the Windows Update settings. Here, you can check for updates manually or change the update settings.
2. **Enable automatic updates:** In the Windows Update settings, select "Automatically download updates and install them on the schedule specified below." Choose a schedule that suits your organization's requirements. This ensures that your server automatically downloads and installs updates when they become available.
3. **Use Windows Server Update Services (WSUS):** For centralized management of updates across multiple servers and clients in your organization, consider using Windows Server Update Services (WSUS).

When applying updates, it's essential to test updates in a non-production environment before deploying them to production systems. This helps identify potential issues or conflicts with your specific configuration or applications.

Use Least Privilege Principle

The least privilege principle is a security best practice that involves creating and using user accounts with the minimum necessary permissions for tasks.

This approach reduces the risk of unauthorized access, malware infections, and other security breaches.

The eXlent #HMI installer creates a set of Windows virtual accounts. Those accounts are configured to respect the Least Privilege Principle. Leave those accounts as is to guaranty a minimum attack surface.

If additional accounts need to be added, please follow these guidelines:

1. **Create standard user accounts:** Whenever possible, create standard user accounts instead of administrator accounts. Standard users have limited privileges, which restricts their ability to make system-wide changes or install unauthorized software. Administrator accounts should only be used when necessary for specific tasks, such as system configuration or software installation.
2. **Limit administrator accounts:** Restrict the number of users with administrative privileges on your system. Having too many administrator accounts increases the risk of unauthorized access and potential security breaches. Assign administrative privileges only to users who require them for their job responsibilities.
3. **Avoid using administrative accounts for daily tasks:** Encourage users with administrative privileges to use a standard user account for daily tasks, such as browsing the internet or checking email. This reduces the risk of inadvertently exposing the system to malware or other threats. Administrative accounts should be reserved for tasks that require elevated privileges.
4. **Implement role-based access control (RBAC):** Use role-based access control to assign permissions based on users' job roles and responsibilities. RBAC helps ensure that users have the appropriate level of access to resources and prevents unauthorized access to sensitive data or systems.
5. **Control access to shared resources:** Restrict access to shared resources, such as files, folders, and network shares, based on the principle of least privilege. Grant read, write, or modify permissions only to users who require them for their job responsibilities.

By following the least privilege principle, you can reduce the attack surface, limit the potential impact of security breaches, and minimize the risk of unauthorized access to your Windows system and eXLent #HMI installation.

Log Access with a Dedicated User

For users requiring access to logs only, create a dedicated Windows account with read permissions restricted to service-specific log directories. Please, avoid assigning administrator privileges for this purpose. Instructions on locating log directories are available in the installation manual.

Enable Windows Defender Firewall

Be cautious when adding, disabling or removing rules, as some rules may be necessary for the proper functioning of your system or applications.

This chapter provides instructions to configure the Windows Firewall for Windows 10, Windows 11 and Windows Server 2022 based on the provided documentation. By following these instructions, you will expose the required ports for the services listed in the table above.

You can configure the firewall using PowerShell or the Command Prompt (CMD).

PowerShell

Open PowerShell as an administrator and execute the following commands to open ports 80 and 443:

```
New-NetFirewallRule -DisplayName "Open Port 80" -Direction Inbound -LocalPort 80 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "Open Port 443" -Direction Inbound -LocalPort 443 -Protocol TCP -Action Allow
```

Command Prompt (CMD)

If the usage of command prompt is preferred above using PowerShell then open the Command Prompt as an administrator and execute the following commands to open ports 80 and 443:

```
netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80
netsh advfirewall firewall add rule name="Open Port 443" dir=in action=allow protocol=TCP localport=443
```

Modbus server

When configuring the Modbus server, it is imperative to adjust the firewall settings to facilitate access. Failure to do so will impede communication with the Modbus servers. Ensure that the TCP servers are appropriately exposed through the designated ports, as outlined in the preceding sections. This step is crucial for seamless operation and uninterrupted connectivity within the network environment.

Please be cautious to take precautionary steps as Modbus is not a secure protocol.

Verifying the Firewall Configuration

To verify that the required ports are open and all other incoming ports are closed, you can review the existing rules in the **Inbound Rules** section of the Windows Defender Firewall with Advanced Security window (for Windows 10 and Windows 11) or by executing the following command in PowerShell or CMD:

PowerShell

```
Get-NetFirewallRule | where { $_.Enabled -eq 'True' -and $_.Direction -eq 'Inbound' -and $_.Action -eq 'Allow' }
```

Command Prompt (CMD)

```
netsh advfirewall firewall show rule name=all
```

Enable Windows Defender Antivirus (or other anti-virus software)

Windows Defender Antivirus is a built-in security feature that provides real-time protection against malware, viruses, and other potential threats. It scans files and applications for malicious content, monitors system activity for suspicious behavior, and automatically removes or quarantines detected threats. Here's how to enable and configure Windows Defender Antivirus to protect your system:

Enable Windows Defender Antivirus

1. Press **Win + I** to open the Settings app.
2. Navigate to "Update & Security" > "Windows Security" (for Windows 10) or "Privacy & security" > "Virus & threat protection" (for Windows 11).
3. Ensure that "Real-time protection" is turned on. If it is turned off, click the toggle to enable it.

Configure Windows Defender Antivirus

1. In the "Virus & threat protection" settings, click on "Virus & threat protection settings" or "Manage settings" (depending on your Windows version).
2. Configure the following settings according to your organization's requirements and security policies:
 - **Cloud-delivered protection:** This setting depends upon if the system is able to connect to the internet. Enable this setting to receive the latest threat definitions and information from the cloud, improving the effectiveness of Windows Defender Antivirus.
 - **Automatic sample submission:** Disable this setting to disallow Windows Defender Antivirus to send samples of suspicious files to Microsoft for analysis.
 - **Tamper protection:** Enable this setting to prevent unauthorized changes to Windows Defender Antivirus settings.
3. Configure the **Exclusions** if necessary, by clicking on "Add or remove exclusions." Add exclusions for specific files, folders, file types, or processes that should not be scanned by Windows Defender Antivirus. Be cautious when adding exclusions, as this may create security vulnerabilities if misused.

Schedule Periodic Scans

1. Open the **Task Scheduler** by searching for "task scheduler" in the Start menu and selecting it from the search results.
2. In the left-hand menu, navigate to "Task Scheduler Library" > "Microsoft" > "Windows" > "Windows Defender."
3. Double-click on "Windows Defender Scheduled Scan" in the center pane.
4. In the "Triggers" tab, click "New..." and configure a schedule for periodic scans according to your organization's requirements. For example, you can set the scan to run daily, weekly, or monthly.

Monitor Scan Results

Regularly review the results of Windows Defender Antivirus scans to detect potential threats and ensure the system's security. To view the scan history, go to the "Virus & threat protection" settings and click on "Protection history" or "Threat history," depending on your Windows version.

By enabling and properly configuring Windows Defender Antivirus, you can protect your Windows system and eXlent #HMI installation from malware, viruses, and other potential threats. Regularly updating the antivirus and monitoring scan results help maintain a secure and stable environment.

Configure User Account Control (UAC)

User Account Control (UAC) is a built-in security feature in Windows that helps prevent unauthorized changes to your system by requiring administrative approval for certain actions. UAC helps protect your system by reducing the attack surface and limiting the potential impact of malware or other threats. Here's how to configure UAC to enhance the security of your eXlent #HMI installation:

Access UAC Settings

1. Press **Win + S** to open the Search menu.
2. Type "uac" in the search bar, and click on "Change User Account Control settings" from the search results.

Configure UAC Settings

In the “User Account Control Settings” window, you’ll find a slider with four different levels of security:

1. **Always notify:** This setting provides the highest level of security, as it notifies you whenever an app or system change requires administrative permissions. You’ll need to provide consent or credentials for any such action. This setting is recommended for users who want maximum security and don’t mind frequent prompts.
2. **Notify me only when apps try to make changes to my computer (default):** This setting is the default for Windows and provides a balanced level of security. You’ll be notified when an app attempts to make changes to your system, but not when you make changes to Windows settings. This setting is suitable for most users.
3. **Notify me only when apps try to make changes to my computer (do not dim my desktop):** This setting is similar to the previous one, but it doesn’t dim the desktop when displaying prompts. This can make the prompts less intrusive but also less secure, as other apps might interfere with the UAC prompts.
4. **Never notify:** This setting disables UAC and provides the least security. It is not recommended, as it leaves your system more vulnerable to unauthorized changes and potential threats.

For a secure eXLent #HMI installation, it’s recommended to use either the “Always notify” or the default setting (“Notify me only when apps try to make changes to my computer”). This ensures that you’ll be alerted when an app or system change requires administrative permissions, helping to prevent unauthorized access and maintain system integrity.

Once you’ve selected the desired UAC setting, click “OK” and restart your system for the changes to take effect. By properly configuring User Account Control, you can enhance the security of your Windows system and protect your eXLent #HMI installation from potential threats.

Enable BitLocker Drive Encryption

BitLocker is a built-in encryption feature in Windows that helps protect your data by encrypting the entire drive. BitLocker uses the Advanced Encryption Standard (AES) algorithm with configurable key lengths to secure your data from unauthorized access, theft, or loss. Here's how to enable BitLocker Drive Encryption on Windows 10, Windows 11 and Windows Server 2022:

Check BitLocker System Requirements

Before enabling BitLocker, make sure your system meets the following requirements:

1. A compatible version of Windows (Windows 10 Pro, Enterprise, or Education; Windows 11 Pro or Enterprise; Windows Server 2022).
2. A Trusted Platform Module (TPM) chip, version 1.2 or later. Some systems without TPM can still use BitLocker with a USB startup key or a password, but it's less secure and less convenient.
3. A BIOS or UEFI firmware that supports Secure Boot and is compatible with TPM.
4. A hard drive with at least two partitions: one for the operating system and another for the BitLocker system files.

Enable BitLocker Drive Encryption

Windows 10 and Windows 11

1. Press **Win + X** and select "Windows PowerShell (Admin)" or "Windows Terminal (Admin)" to open an elevated command prompt.
2. Type `manage-bde -status` and press Enter to check if any drives are already encrypted. If not, proceed to the next step.
3. Press **Win + S** to open the Search menu.
4. Type "bitlocker" in the search bar and click on "Manage BitLocker" from the search results.
5. In the "BitLocker Drive Encryption" window, find the drive you want to encrypt and click on "Turn on BitLocker."
6. Choose how you want to unlock the drive at startup: using a TPM, a password, or a USB key. If your system has a TPM, it's recommended to use TPM with a PIN for better security.
7. Follow the prompts to save a recovery key, which can be used to unlock the drive if you forget your password or lose your USB key. You can save the recovery key to a file, print it, or save it to your Microsoft account.
8. Choose the encryption mode: "New encryption mode (best for fixed drives on this device)" or "Compatible mode (best for drives that can be moved from this device)." Select the mode that best suits your needs.
9. Click "Start encrypting" to begin the encryption process. The encryption may take some time, depending on the size of the drive and the speed of your system.

Windows Server 2022

1. Open the "Server Manager" by clicking on the icon in the taskbar or searching for "server manager" in the Start menu.
2. In the "Server Manager" dashboard, click on "Add roles and features."
3. In the "Add Roles and Features Wizard," click "Next" until you reach the "Select features" page.
4. Check the box next to "BitLocker Drive Encryption" and click "Next," then "Install." Wait for the installation to complete and close the wizard.
5. Open an elevated command prompt or PowerShell by right-clicking on the Start button and selecting "Windows PowerShell (Admin)" or "Command Prompt (Admin)."
6. Type `manage-bde -status` and press Enter to check if any drives are already encrypted. If not, proceed to the next step.
7. Type `manage-bde -on C: -RecoveryPassword` to enable BitLocker on the C: drive and generate a recovery password. Replace

Enable BitLocker Drive Encryption on a Virtual Machine

Enabling BitLocker Drive Encryption on a virtual machine (VM) can be slightly different from enabling it on a physical machine. Virtual machines may not have a Trusted Platform Module (TPM) or might require additional configurations in the hypervisor. Here's how to enable BitLocker Drive Encryption on a virtual machine running on popular hypervisors, such as VMware and Hyper-V:

VMware

1. **Enable virtual TPM (vTPM) support** (for VMware vSphere 6.7 or later): In the VMware vSphere Client, right-click the virtual machine and select "Edit Settings." Under the "VM Options" tab, expand "Security" and click "Add TPM." Save your changes.
2. **Power on the virtual machine** and log in to the guest operating system.

3. Follow the previously mentioned steps to enable BitLocker Drive Encryption on Windows 10, Windows 11 or Windows Server 2022.

vTPM is not supported on all VMware products. If your virtual machine doesn't support vTPM, you can use BitLocker without TPM by following the steps mentioned later in this guide.

Hyper-V

1. **Enable virtual TPM (vTPM) support** : In the Hyper-V Manager, right-click the virtual machine and select "Settings." Under the "Security" section, check the box next to "Enable Trusted Platform Module." Save your changes.
2. **Power on the virtual machine** and log in to the guest operating system.
3. Follow the previously mentioned steps to enable BitLocker Drive Encryption on Windows 10, Windows 11 or Windows Server 2022.

BitLocker without TPM

If your virtual machine doesn't support virtual TPM (vTPM) or you're using a hypervisor that doesn't provide vTPM functionality, you can enable BitLocker without TPM by using a password or a USB startup key. Here's how:

1. **Enable the "Require additional authentication at startup" policy** :
 - a. Press **Win + R**, type "gpedit.msc," and press Enter to open the Local Group Policy Editor.
 - b. Navigate to "Computer Configuration" > "Administrative Templates" > "Windows Components" > "BitLocker Drive Encryption" > "Operating System Drives."
 - c. Double-click on "Require additional authentication at startup" and select "Enabled." Ensure that the "Allow BitLocker without a compatible TPM" option is checked. Click "Apply" and "OK."
2. **Enable BitLocker Drive Encryption** : Follow the previously mentioned steps to enable BitLocker Drive Encryption on Windows 10, Windows 11 or Windows Server 2022. When prompted to choose how to unlock the drive at startup, select "Enter a password" or "Insert a USB flash drive."

By following these steps, you can enable BitLocker Drive Encryption on a virtual machine, providing an additional layer of security to protect your data from unauthorized access, theft, or loss.

Implement Network Segmentation and Access Control

Network segmentation and access control are essential security practices that help protect sensitive systems and data by dividing the network into separate segments and restricting access based on user roles and responsibilities. Implementing network segmentation and access control for your eXlent #HMI installation can reduce the attack surface, limit unauthorized access, and minimize the potential impact of security breaches.

1. **Create separate network segments**: Divide your network into separate segments based on different functions, such as eXlent #HMI systems, business applications, and user devices. This helps limit the potential spread of an attack and makes it more difficult for an attacker to gain access to sensitive systems or data.
2. **Use VLANs and firewalls**: Use Virtual Local Area Networks (VLANs) and firewalls to isolate different network segments and enforce security policies. This allows you to control access between segments and restrict communication to only the necessary systems and services.
3. **Implement network access controls**: Apply network access control (NAC) solutions to monitor and control network access based on user roles, device types, and security compliance. NAC solutions can help prevent unauthorized devices from accessing the network and enforce security policies, such as requiring up-to-date antivirus software or operating system patches.

Disable Unnecessary Services and Features

Disabling unnecessary services and features in Windows helps to reduce the attack surface, improve system performance, and free up resources. Here's how to disable unnecessary services and features on Windows 10, Windows 11 and Windows Server 2022:

Identify Unnecessary Services and Features

1. **Research and understand the services and features running on your system**: Before disabling any services or features, it's important to understand their purpose and how they might impact your system or applications. Consult official documentation and consider the specific needs of your environment.
2. **Determine which services and features are not required for your use case**: Based on your research, make a list of services and features that can be safely disabled without impacting the system's functionality or security.

Disable Unnecessary Services

1. Press **Win + R** to open the Run dialog, type "services.msc," and press Enter to open the Services console.
2. In the Services console, scroll through the list of services to find the ones you've identified as unnecessary.

3. Right-click on each service you want to disable, and select “Properties.”
4. In the “Properties” window, change the “Startup type” to “Disabled.” Click “Apply” and “OK.”
5. If the service is currently running, click the “Stop” button to stop the service immediately. Note that stopping some services may cause other dependent services to stop as well.

Disable Unnecessary Features

Windows 10 and Windows 11

1. Press **Win + S** to open the Search menu.
2. Type “windows features” in the search bar and click on “Turn Windows features on or off” from the search results.
3. In the “Windows Features” window, uncheck the boxes next to the features you’ve identified as unnecessary.
4. Click “OK” to apply the changes. You may be prompted to restart your computer for the changes to take effect.

Windows Server 2022

1. Open the “Server Manager” by clicking on the icon in the taskbar or searching for “server manager” in the Start menu.
2. In the “Server Manager” dashboard, click on “Add roles and features.”
3. In the “Add Roles and Features Wizard,” click “Next” until you reach the “Select features” page.
4. Uncheck the boxes next to the features you’ve identified as unnecessary.
5. Click “Next,” then “Remove Features.” Wait for the removal process to complete and close the wizard.

Implement Strong Password Policies

Implementing strong password policies is crucial for protecting user accounts and maintaining the security of your organization's systems and data. A strong password policy enforces the use of complex and unique passwords, making it more difficult for attackers to compromise accounts using methods such as brute-force attacks, dictionary attacks, or credential stuffing.

At ABB, security and data protection are top priorities. Service accounts play a critical role in maintaining this security. These accounts are designed for system use only and cannot be accessed by users directly, eliminating the need for passwords. For non-service accounts, strong, randomly generated passwords are a key component of the security framework.

Randomly Generated Strong Passwords

All passwords used by eXLent #HMI services are strong and created using a random generation process, ensuring the following characteristics:

1. **Length** : The generated passwords are sufficiently long, typically containing at least 16 characters.
2. **Character types** : The generated passwords include a mix of uppercase and lowercase letters, numbers, and special characters, ensuring a high level of complexity and resistance to brute-force and dictionary attacks.
3. **Unpredictability** : By using a random generation process, the passwords are less likely to contain guessable information or follow predictable patterns, making it difficult for attackers to guess or crack them.
4. **Uniqueness** : Each password generated for the eXLent #HMI services is unique, reducing the risk of unauthorized access through the use of shared or reused passwords.

Implement Regular Backups

Implementing regular backups is a critical part of maintaining the integrity and availability of your data, including the data associated with eXLent #HMI. Backups help ensure that you can quickly recover from data loss or corruption caused by hardware failure, software issues, human error, or malicious attacks.

Accessing Data for Backups with a Dedicated User

For users tasked with creating backups, consider creating a dedicated Windows user account with access limited to the data directories of the relevant services. This ensures the user can perform backups without requiring administrative privileges.

To create such a backup user:

1. Set up a new Windows user account.
2. Grant the user read and write permissions to the specific data directories of the services.
3. Avoid granting access to other sensitive system areas or administrative controls.

Refer to the installation manual for details on locating the data directories for each service. This approach ensures backups can be performed securely while maintaining adherence to the principle of least privilege.

Establish a Backup Strategy

1. **Identify critical data and assets** : Determine which data and assets associated with eXLent #HMI are critical to your organization's operations and must be backed up regularly.
2. **Choose a backup schedule** : Establish a backup schedule based on your organization's needs, ensuring that backups are frequent enough to minimize data loss in the event of a failure.
3. **Select backup storage locations** : Choose one or more secure storage locations for your backups. Ideally, use a combination of local and offsite storage to protect against localized disasters or hardware failures.
4. **Implement versioning and retention policies** : Retain multiple versions of your backups and establish retention policies to ensure that older backups are available if needed.
5. **Monitor and maintain backups** : Regularly monitor the backup process to ensure that backups are being created successfully and address any issues that arise.

Perform Regular Backups

1. **Configure your backup software** : Configure your backup software to use the dedicated eXLent #HMI backup user, ensuring that the user has read-only access to the %programdata%\ABB\eXLent directory.
2. **Select the data to be backed up** : Ensure that all critical data associated with eXLent #HMI, including configuration files and databases, are included in the backup process.
3. **Schedule the backups** : Set up a backup schedule that meets your organization's requirements for data protection and recovery.
4. **Test your backups** : Regularly test your backups by restoring data to a separate environment, ensuring that the backup and restore processes are functioning correctly and that the restored data is usable.

By implementing regular backups and using the dedicated eXLent #HMI backup user with read-only access to the %programdata%\ABB\eXLent directory, you can protect your critical data and ensure that you can quickly recover from data loss or corruption. This approach helps maintain the integrity and availability of your eXLent #HMI data and contributes to the overall security and resilience of your organization's systems.

Develop and maintain an incident response plan to handle security incidents effectively. Train employees on the plan and conduct periodic drills to ensure readiness.

Keep eXLent #HMI Updated

Regularly updating eXLent #HMI to the latest version is essential for maintaining the security, stability, and performance of the system.

Updates often include important bug fixes, security patches, and new features that enhance the functionality of the software. By keeping eXLent #HMI updated, you can protect your system from potential vulnerabilities and ensure that you are utilizing the latest improvements and features.

Obtaining the Latest Version of eXLent #HMI

The latest version of eXLent #HMI can be obtained from ABB's library website at the following link: <https://new.abb.com/products/measurement-products/midstream-and-transportation> (<https://new.abb.com/products/measurement-products/midstream-and-transportation>). Visit this link regularly to check for updates and download the latest available version of eXLent #HMI.

Updating eXLent #HMI

Follow these steps to update eXLent #HMI to the latest version:

1. **Download the latest version** : Visit the [ABB website](https://new.abb.com/products/measurement-products/midstream-and-transportation) (<https://new.abb.com/products/measurement-products/midstream-and-transportation>) and download the latest version of eXLent #HMI.
2. **Backup your data** : Before updating, create a backup of your existing eXLent #HMI data, including configuration files and databases, to prevent potential data loss during the update process.
3. **Review the release notes** : Carefully read the release notes provided with the latest version of eXLent #HMI. These notes will provide important information about the changes, bug fixes, and new features included in the update, as well as any potential compatibility issues or required actions.
4. **Install the update** : Follow the installation instructions provided with the latest version of eXLent #HMI to update your system. This may involve running an installer or manually replacing files and folders, depending on the update process.
5. **Test the updated system** : After updating eXLent #HMI, thoroughly test the system to ensure that it is functioning correctly and that there are no issues or conflicts with your existing configuration and data.
6. **Monitor for issues** : Continuously monitor your eXLent #HMI system after updating to identify and resolve any potential issues that may arise.

By keeping eXLent #HMI updated with the latest version, you can maintain the security, stability, and performance of your system while taking advantage of new features and improvements. Regularly visit the [ABB website](https://new.abb.com/products/measurement-products/midstream-and-transportation) (<https://new.abb.com/products/measurement-products/midstream-and-transportation>) to check for updates and ensure that your eXLent #HMI system remains up-to-date and protected against potential vulnerabilities.

Verifying the Integrity of the eXLent #HMI Download

To ensure the integrity and authenticity of the downloaded eXLent #HMI installer, you should verify its hash. Checking the hash ensures that the file has not been tampered with or corrupted during the download process. Typically, the hash is provided as an MD5, SHA-1, or SHA-256 checksum.

Verify the Hash of the Downloaded File

1. **Obtain the official hash** : Visit the [ABB website](https://new.abb.com/products/measurement-products/midstream-and-transportation) (<https://new.abb.com/products/measurement-products/midstream-and-transportation>) or refer to the release notes/documentation provided with the eXLent #HMI installer. Locate and note the official hash for the downloaded file.
2. **Calculate the hash of the downloaded file** : Use a hash calculator tool to generate the hash of the downloaded eXLent #HMI installer. You can use built-in tools on Windows, such as CertUtil (for Windows 10, Windows 11 and Windows Server 2022) or PowerShell, or download a third-party tool.

- **Using CertUtil** : Open Command Prompt and run the following command, replacing `path_to_installer` with the actual path to the downloaded file:

```
CertUtil -hashfile path_to_installer SHA256
```

- **Using PowerShell** : Open PowerShell and run the following command, replacing `path_to_installer` with the actual path to the downloaded file:

```
Get-FileHash -Path path_to_installer -Algorithm SHA256
```

3. **Compare the hashes** : Compare the hash generated in step 2 with the official hash obtained in step 1. If the hashes match, the downloaded file is authentic and has not been tampered with or corrupted. If the hashes do not match, do not proceed with the installation and re-download the file from the official source.

By verifying the hash of the downloaded eXLent #HMI installer, you can ensure the integrity and authenticity of the file, protecting your system from potential security risks associated with tampered or corrupted files. Always check the hash before proceeding

with the installation or update of eXLent #HMI.

Secure Your Data with Secure Protocols

For optimal data security, we strongly recommend you to use secure protocols like HTTPS, which encrypt data and make it harder for attackers to intercept or alter it. Such protocols enhance your data's confidentiality, integrity, and authenticity, making them vital for transmitting sensitive data.

Installer Security Warnings

The eXLent #HMI installer includes built-in security warnings to help prevent the use of insecure protocols:

HTTP Protocol Warning:

- **Automatic Detection:** When HTTP is selected during installation, the installer displays a prominent warning
- **Warning Message:** "It is strongly advised to enable HTTPS" appears immediately when HTTP is selected
- **Visual Indicators:** Warning messages use distinctive styling to ensure visibility
- **Dynamic Updates:** Warnings disappear immediately when switching back to secure protocols

Best Practice Enforcement:

- **Default to HTTPS:** The installer defaults to HTTPS for all new installations
- **User Education:** Clear explanation of security implications when selecting insecure options
- **Non-blocking Guidance:** Warnings inform users without preventing installation, allowing informed decisions

Assessment Tool Integration:

The installer includes comprehensive PowerShell assessment tools that help validate secure protocol implementation:

- **Post-Installation Validation:** Use `Get-ExlentAssessment` to verify HTTPS configuration
- **Network Security Analysis:** `Get-ListeningTCPConnections` confirms secure protocol usage
- **Service Configuration Check:** `Get-ExlentServiceStatus` validates secure service setup

Risks of Insecure Protocols

We advise against using insecure protocols like HTTP due to their inherent risks, but understand they may be necessary at times. Insecure protocols can be used but at own risk.

If you choose to use insecure protocols, be aware of the risks:

- **Data Exposure:** HTTP lacks encryption, allowing attackers to intercept and read your data, particularly sensitive information.
- **Man-in-the-Middle Attacks:** Attackers can intercept, alter, and even inject malicious content into unencrypted communications.
- **Authentication Absence:** Unlike HTTPS, HTTP doesn't authenticate websites, allowing attackers to impersonate sites more easily.

Mitigating Insecure Protocol Risks

If you must use insecure protocols, reduce the associated risks by:

- **Limiting Sensitive Data Transmission:** Only send non-sensitive data through insecure protocols to lessen the impact of a breach.
- **Adding Extra Security Measures:** Implement additional protections like encryption or digital signatures even with insecure protocols.
- **Keeping Systems Updated:** Regularly apply the latest security patches and updates to mitigate potential vulnerabilities.
- **Monitoring for Threats:** Proactively monitor your systems for unauthorized access or suspicious activities and quickly address any issues.

Client certificates

By default, the web server is configured to only serve via HTTPS. The server will supply a server certificate to the browser in order to identify itself. An additional measure one could take, is the use of so called client certificates. With these certificates, clients identify themselves to the server.

Client certificates are used to control which clients are allowed to connect to the web server.

eXLent #HMI supports the use of client certificates. On server end, one or more public Certificate Authority (CA) certificates need to be stored (see `%ProgramData%\ABB\eXLent\security-proxy\certificates`). Additionally, the server's TLS configuration needs to be extended (see `%ProgramData%\ABB\eXLent\security-proxy\dynamic-config\tls.yaml`):

```

{
  "tls": {
    "options": {
      "default": {
        ...
        "clientAuth": {
          "caFiles": ["%ProgramData%\ABB\eLent\security-proxy\certificates\CA.crt"],
          "clientAuthType": "RequireAndVerifyClientCert"
        }
      }
    }
  }
}

```

All connecting clients should use a private key to create a Certificate Signing Request (CSR) for a client certificate. This CSR needs to be signed by one of the CAs. The resulting certificate/key pair can then be used to connect to the web server. Note that on the Windows operating system, one typically stores these in the **Personal** section of the user certificates store.

Please note that the client certificate feature is turned off by default.

Flow-X certificates

The default mode of communication between eLent #HMI and the Flow-X system utilizes the HTTPS protocol. However, it is important to note that the certificates used in this communication are unlikely to be signed by a globally recognized Certificate Authority (CA). Consequently, it is necessary to perform a manual configuration within the eLent #HMI system to establish trust in these certificates.

To achieve this, it is recommended to place the web certificate or any intermediate trust certificates in the certificate chain directly into the `%ProgramData%\ABB\eLent\flowx-opcua\flowx-certificates` directory. It is essential to adhere to specific constraints when selecting the certificate for this purpose. The chosen certificate should not exceed a file size of 100KB and must be in the .pem format. It is worth noting that if these criteria are not met, eLent #HMI will disregard the certificate.

This procedure ensures the secure and proper functioning of the communication between eLent #HMI and the Flow-X system, even when utilizing certificates signed by a CA that is not globally recognized or self-signed.

Modbus client and Modbus server

Modbus client and Modbus server make use of the modbus protocol, which is not secure by itself. Modbus is unencrypted. In this case, extra measures should be taken to secure the connection. Examples are making sure that the network itself is fully secure, using a VPN, or using SSL tunnel.

Hardening against Denial-Of-Service attacks

Denial-of-Service (DoS) attacks aim to overwhelm systems with traffic or requests, thereby rendering them unavailable for legitimate users. While eXLent #HMI is not an internet-facing product and the chances of direct DoS attacks are relatively low, it is still crucial to implement proper precautions in your infrastructure. This chapter provides guidelines on protecting your eXLent #HMI installation and overall system from potential DoS attacks.

Implement Intrusion Detection Systems (IDS) with Rate Limiting

An Intrusion Detection System (IDS) monitors network traffic for suspicious activities or policy violations and reports them to an administration or security information and event management (SIEM) system. IDS with rate limiting is a valuable tool to prevent potential DoS attacks.

Rate limiting restricts the number of requests a client can make to the system within a specified timeframe. This prevents a single client from consuming all system resources and helps maintain service availability during a DoS attack.

Consider deploying IDS solutions like Cisco Secure Intrusion Detection System, Palo Alto Networks Threat Prevention or other offerings that support rate limiting on your network.

Utilize DoS Protection Systems

Specialized DoS protection systems can be used to detect, mitigate, and report on DoS attacks. These systems typically use a combination of rate limiting, traffic shaping, IP reputation lists, anomaly detection, and other methods to prevent DoS attacks.

Enable Network Firewalls

Firewalls can be configured to limit traffic to services and block specific IP addresses that are generating excessive traffic. In addition to [Windows Defender Firewall](#Enable Windows Defender Firewall), consider using additional network-level firewalls for added security.

Remember, hardening your system against DoS attacks requires an in-depth defense strategy and regular monitoring and updating of the security controls. Regular security audits can help ensure all security measures are working as intended. While you can take numerous steps to prevent DoS attacks, there is no absolute safeguard against them. Therefore, a response plan should be in place to handle an attack if it happens.

Verify the Source of Your License

When obtaining a license for eXLent #HMI, it is crucial to ensure that the license originates from a trusted source. Only licenses that come directly from an official email address from the company ABB should be considered valid. This precaution helps to prevent unauthorized or counterfeit licenses, ensuring the security and integrity of your product usage. Always verify the source before trusting and installing a license for eXLent #HMI.

Disaster Recovery Plan: Recovery from an Installer and the Latest Backup

This section provides a detailed plan to recover from a system failure using the eXLent #HMI installer and the latest backup of your data. Please follow these steps precisely to ensure a successful recovery of your system.

Backup Regularly

The foundation of any disaster recovery plan is regular backups. Ideally, a backup strategy includes creating full system backups daily or weekly, with incremental backups in between. The frequency of backups will depend on the level of activity and the criticality of the data. For details on how to backup eXLent #HMI, refer to the section "[Backup and Recovery](#)."

Pre-Recovery Preparation

Before initiating recovery, ensure that you have the latest version of the eXLent #HMI installer and the most recent backup of your data. You can obtain the latest version of the installer from the ABB library website.

Please verify the integrity of the downloaded installer using the hash verification procedure mentioned in the section "[Verifying the Integrity of the eXLent #HMI Download](#)"

Disaster Recovery Procedure

In case of a disaster situation where eXLent #HMI needs to be recovered, follow these steps:

1. **Isolate the system:** To prevent further damage or data loss, disconnect the affected system from the network. Ensure that the system is stable and ready for recovery.
2. **Clean up:** If necessary, uninstall any corrupted components of the eXLent #HMI system (See section [Uninstallation procedure](#)).
3. **Reinstall eXLent #HMI:** Run the eXLent #HMI installer to install a fresh copy of the system. Be sure to install it in the same environment as the previous installation to ensure compatibility with the backup data. For detailed installation instructions, see the section "[Installation procedure](#)."
4. **Restore the backup:** After the eXLent #HMI system is reinstalled, restore the backup data (See section [Backup and Recovery](#)). Ensure that you restore the data in the correct directories.
5. **Test the system:** Verify that the system is functioning correctly. Check all critical operations and functions to confirm the system is working as expected. This includes user verification, data integrity checks, system performance checks, and more.
6. **Monitor the system:** After recovery, continuously monitor the system to identify any potential issues that may arise.

Remember, every recovery scenario is unique and may require additional steps depending on the complexity of your environment. Always document your recovery process, as it will aid in future disaster recovery planning and execution.

After Recovery

Once you've successfully recovered from a disaster, it's crucial to assess your recovery process, identify any areas for improvement, and update your disaster recovery plan accordingly. Also, ensure that you resume your regular backup schedule to safeguard your system against future disasters.

Reporting Vulnerabilities to ABB

If you discover a security vulnerability in any ABB product or service, including eXLent #HMI:

1. Isolate the affected system if possible.
2. Preserve evidence (screenshots, logs).
3. Notify your organization's IT security team or designated security officer.
4. Visit the ABB Cybersecurity page: <https://global.abb/group/en/technology/cyber-security>
5. Follow the instructions provided on this page for reporting security vulnerabilities.

ABB regularly updates its reporting procedures. Always refer to the official ABB Cybersecurity page for the most current guidelines on reporting vulnerabilities.

Remember to adhere to your organization's specific security policies and incident response procedures.

Monitoring Vulnerabilities of eXLent #MI

Vulnerabilities related to eXLent #HMI will be published on the [ABB Cyber security alerts and notifications](https://global.abb/group/en/technology/cyber-security/alerts-and-notifications) (https://global.abb/group/en/technology/cyber-security/alerts-and-notifications). To stay informed about the latest updates, please check this page regularly.

References

- [abb]: <http://www.abb.com/midstream> (<http://www.abb.com/midstream>)

