PACOM

Unison 5.13.0

Hardening Guide

Table of Contents

1. Introduction

Organizations today face an evolving threat landscape that demands robust security measures at every layer of their infrastructure. This guideline aims to provide a practical framework for hardening your Unison installation. By following these recommendations, you can significantly reduce the attack surface of your systems, better protect sensitive data, and ensure continuity of critical services.

The topics covered here are intended for system administrators, security teams, and technical stakeholders responsible for designing, deploying, and maintaining the infrastructure. Whether you are planning a new deployment or strengthening an existing one, this guideline provides practical steps to enhance the security posture of your Unison solution. By implementing these recommendations, you will be better prepared to prevent, detect, and respond to cyber threats while maintaining the performance and availability of your systems.

2. Responsibilities

The customer and/or integrator manages the deployment environment, including operating systems, databases, and network configurations. These components fall outside Pacom's control and are critical to the overall security posture. By securing these areas, the customer/integrator ensures compliance with best practices, protects sensitive data, and minimizes vulnerabilities, aligning the deployment with the organization's unique security requirements.

Customer/Integrator is responsible for secure implementation (configuration, permissions and patching) of:

- Network Segmentation and Firewall policies
- Operating Systems (Microsoft Windows)
- Microsoft SQL Server
- Microsoft Active Directory (if applicable)
- Third-party integrations
- Disaster recovery (backup and restore)
- Certificates/PKI
- Encryption of data in transit and at rest
- Security monitoring (Antivirus/EDR/SOC)
- Post installations activities of Unison to secure its configuration. For example, but not limited to:
  - Change default credentials
  - Securing Driver Setup/Configuration

3. Generic Security Recommendations

Principle of Least Privilege, Identity and Access management (IAM)
Limiting each account or service to the bare minimum privileges required for its role greatly reduces the potential damage if it's compromised. Employ role-based access control (RBAC) to define which tasks belong to which job function and use segregation of duties to ensure no single individual wields excessive influence over critical processes. Regularly audit and adjust permissions to remove unnecessary or outdated access. Restricting administrative credentials and introducing just-in-time (JIT) privilege methods further tightens control, ensuring privileged access is granted sparingly and only when needed. Wherever

feasible, consolidate user identities into a centralized system, ensuring streamlined authentication, consistent policy enforcement, and simpler oversight.

Install Security Patches Promptly
Securing an environment starts with keeping systems up to date. Unpatched servers and applications are often the first targets for attackers, who exploit known vulnerabilities shortly after they're disclosed. To mitigate this risk, implement a structured patch management process that includes testing updates in a staging environment and using automated alerts or vulnerability scanners to track new releases. Regular, timely patching significantly reduces the likelihood of compromise.

Enforce Strong Passwords and Secure Password Storage
Weak or reused passwords are one of the most common pathways for unauthorized access. Encourage the use of long, complex passphrases or implement multi-factor authentication (MFA) to thwart brute-force or credential-stuffing attacks. Providing a reputable password manager to users helps maintain unique, complex credentials and mitigates the temptation to reuse or improperly record them.

Perform Regular, Immutable Backups
Immutable backups are data copies stored in a format that cannot be altered, deleted, or overwritten, even by users with administrative privileges. This ensures the integrity and availability of backup data, protecting it from threats such as ransomware, accidental deletion, or malicious insiders. Common methods to achieve immutability include Write Once, Read Many (WORM) storage, retention locks, and backup solutions with tamper-proof configurations. Immutable backups are a critical component of a robust data protection strategy, ensuring data recovery in the event of a compromise. Regularly perform test restores to ensure that backups are functional and reliable.

Endpoint protection
Combining traditional endpoint protection (e.g., antivirus, firewalls) with Endpoint Detection and Response (EDR) delivers a layered security model. While endpoint protection blocks known threats, EDR continuously monitors devices to identify and respond to more advanced or stealthy attacks. Together, they provide comprehensive coverage, preventing common malware while also detecting and containing sophisticated exploits in real time.

Logging, Monitoring, and Incident Response
Effective logging, monitoring, and incident response practices ensure that security-related data is consistently captured, analyzed, and acted upon. Centralizing logs from both servers and workstations enables correlation and early detection of anomalies—such as repeated login failures or suspicious queries—while configuring alerts provides real-time notifications of potential threats. Additionally, a formal incident response plan clearly defines investigation procedures and team roles, ensuring swift and coordinated action during security events. Establishing a log retention policy aligned with regulatory or business requirements secures older logs and maintains critical evidence for forensic analysis. Leveraging a Security Operations Center (SOC)—whether in-house or outsourced—further enhances real-time monitoring, threat intelligence, and incident handling, thereby strengthening overall security posture.

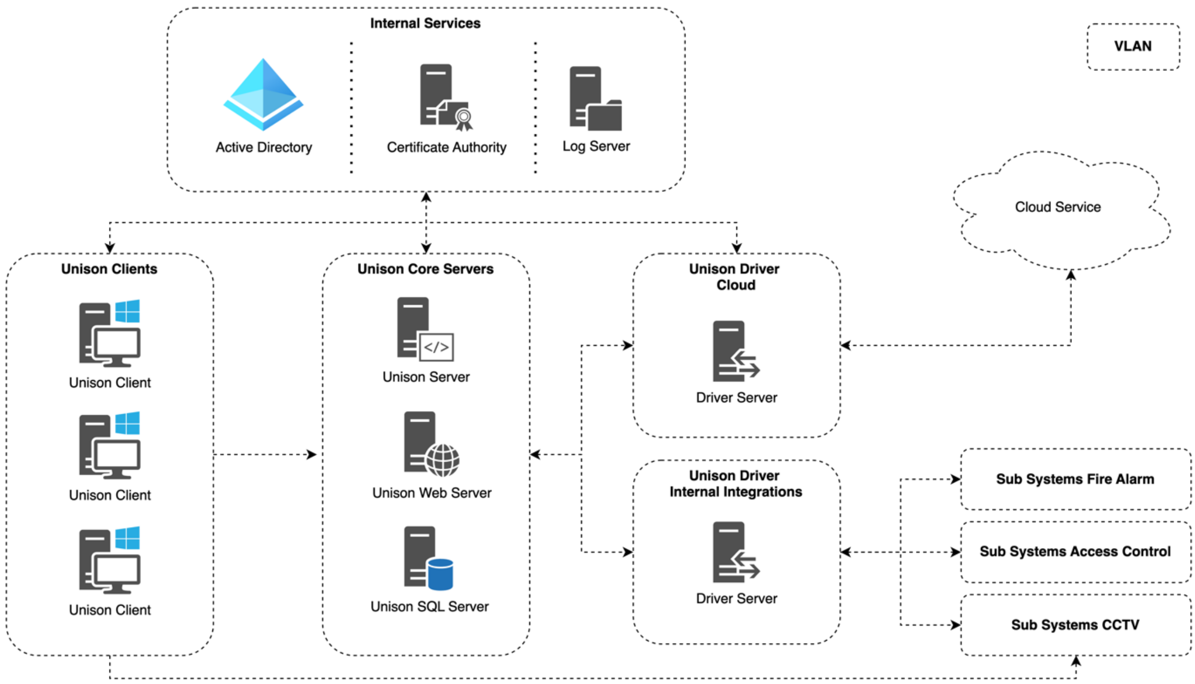
4. Network and Communication Hardening

Network Segmentation and Firewall
Network segmentation and firewalls are essential for enhancing security and protecting critical systems. Implement VLANs or subnets to isolate database servers from client networks, ensuring that sensitive systems are not directly exposed to unnecessary traffic. This separation reduces the risk of unauthorized access and limits potential attack vectors.

Use internal firewalls or network ACLs to restrict traffic between the network segments. Only necessary protocols and ports, such as SQL Server communication on port 1433 or HTTPS on port 443, should be allowed based on the application requirements. All other traffic should be explicitly blocked to minimize the attack surface.

This is especially important for integrations using Unison drivers to connect with third-party systems. Ensure that third-party systems are restricted to accessing only the specific ports required for the integration to function. Additionally, block access to the integration/driver ports for any systems that do not require connectivity, preventing unauthorized access and enhancing security.

Below is an example on how Unison can be segmented into different VLANs. See Appendix A for port configurations.



Encryption in transit

Encryption in Transit protects sensitive data by encrypting it during transmission, preventing interception or unauthorized access. This is critical for safeguarding communications between systems, ensuring data confidentiality and compliance with regulatory requirements.

Public Key Infrastructure (PKI) provides the foundation for secure communication in an enterprise by managing digital certificates and encryption keys. PKI enables:

- **Authentication:** Verifies the identity of systems and users.
- **Data Integrity:** Ensures transmitted data is not altered.
- **Confidentiality:** Secures communication through encryption.

Implementing encryption in transit and PKI minimizes the risk of data breaches, builds trust in digital systems, and aligns with industry security standards.

Ensure communications are protected with strong encryption and establish secure trust (PKI) within the environment.

5. Windows OS Hardening

Unison runs on Microsoft Windows, and ensuring the operating system is properly secured and hardened is a critical step in protecting both the application and the sensitive information it manages. Implementing and maintaining a secure Windows environment not only defends against unauthorized access but also helps maintain system stability and reliability.

Apply Microsoft Security Baseline Policies
Microsoft offers recommended security baselines via its Security Compliance Toolkit and Windows Security Baselines[1]. These baselines include best-practice Group Policy settings that cover password complexity, account lockout thresholds, audit logging, and other key configuration areas. Adopting these baseline policies helps establish a standardized security posture across all Unison-related systems.

Additional protection can be applied if license requirements for Attack Surface Reduction (ASR)[2] is available.

Use and Configure Windows Firewall
A properly configured Windows Firewall[3] is essential for controlling inbound and outbound network traffic. By restricting communication to only the specific ports and protocols used by Unison, you effectively minimize the system's attack surface. Regularly review and update firewall rules as your network environment evolves to maintain optimal protection against external threats.

Enable BitLocker for Data-at-Rest Encryption
Protecting data at rest is paramount, especially if devices are lost or stolen. BitLocker[4] provides full disk encryption, ensuring that only authorized users and systems can access the stored data. By enabling BitLocker on all drives and securely managing the associated encryption keys, organizations can significantly reduce the risk of data breaches stemming from unauthorized physical access.

Minimize Attack Surface and Enforce Least Privilege
Disable or remove any unnecessary Windows services, applications, and features that are not essential for Unison's operation. Ensure that users, service accounts, and administrators only have the privileges required to perform their specific tasks. This approach limits the avenues available for potential attackers and reduces the impact of compromised accounts.

Secure remote administration protocols
Ensure that all remote administration services—such as WinRM, PowerShell remoting, and Remote Desktop Services—are configured in line with Microsoft's best practices. This entails using secure communication protocols and strictly limiting remote administration privileges to only those users who truly require them, thereby reducing potential attack avenues.

Manage local accounts securely
Microsoft LAPS[5] enhances security by automatically managing and rotating local administrator passwords for domain-joined devices. This prevents unauthorized access, mitigates lateral movement during breaches, and eliminates the risks of using shared or default passwords. LAPS ensures compliance with security policies while simplifying password management and reducing administrative overhead.

---

[1] https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines
[2] https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction
[3] https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/
[4] https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
[5] https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview

Secure Windows Clients
For Windows clients running the Unison client, it is recommended to implement either AppLocker[6] or Windows Defender Application Control (WDAC)[7]. These features help prevent attackers who have gained access to a system from executing their own tools by restricting the launch of unauthorized applications, scripts, and DLLs. This approach significantly reduces the risk of malicious activity on compromised endpoints.

6. Microsoft SQL Server

Microsoft SQL Server is a critical component for Unison, managing sensitive data and providing backend services. Properly securing and hardening SQL Server is essential to ensure the confidentiality, integrity, and availability of data, while also reducing the risk of unauthorized access or attacks.

Review Microsoft SQL security best practices[8], most notably:

Reduce the attack surface
To minimize the attack surface, only install Microsoft SQL components that are required by Unison:

- SQL Database Engine

Likewise, only enable IP ports needed for Unison to operate:

- TCP/1433 (default)

Authentication Access
Review accounts that have login permissions to the SQL database. Minimize the number of administrators to reduce the risk of the database being compromised.

Encryption at rest
The most prevalent risks related to encryption for the data stored in the SQL database are loss of storage media (hard drives)/backup media or malicious database administrators. If required by policy or risk assessment, enable database encryption[9]. The following encryption methods are supported by Unison:

- Microsoft BitLocker full disk encryption provides protection for lost hard drives.
- Transparent data encryption (TDE)

> **Note:** Because of Transparent Data Encryption, database backups will also be encrypted. If a backup of the database gets lost or stolen, the culprit will not be able to restore the database without the appropriate certificate, keys and passwords.

Encryption in transit
To protect information transferred over the network, Unison supports encryption of the Microsoft SQL connection but requires some additional setup that is described in ***Application Note UAN-Pacom-0017***.

Vulnerability assessment
To find possible database security issues, it is recommended to perform recurring vulnerability assessments of the database[10].

[6] https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview
[7] https://learn.microsoft.com/en-us/hololens/windows-defender-application-control-wdac
[8] https://learn.microsoft.com/en-us/sql/relational-databases/security/sql-server-security-best-practices
[9] https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/sql-server-encryption
[10] https://learn.microsoft.com/en-us/sql/relational-databases/security/sql-vulnerability-assessment

7. Active Directory

When the Unison solution is deployed on computers joined to an Active Directory domain, it is essential to secure the underlying Active Directory environment in accordance with industry best practices. A single compromise of Active Directory can grant attackers the means to infiltrate the Unison environment as well, underscoring the importance of a robust security posture.

For guidance on hardening Active Directory, refer to the following resources:

- **Microsoft Best Practices for Securing Active Directory**[11]
- **Microsoft Tech Community on AD Hardening**[12]
- **Australian Cyber Security Centre: Detecting and Mitigating Active Directory Compromises**[13]

8. Unison

8.1 Security and Encryption

The following features are available to secure the system and system data:

- Operator passwords are salted and encrypted in the database.
  Optionally, Windows Active Directory account login can be applied.
- Single sign-on ***should be used with caution*** as an attacker that gains control over client can login to Unison without knowing the password of the user.
- Legacy AD/Single sign-on login methods ***should not be used*** since authentication is performed by the client. These methods are available for backwards compatibility with existing systems but may be removed in the future.
- One-way password hashes with Salt are used when saving passwords and validating log ins.
- SHA-256 is used for password hashes.
- Connections between the SQL Server and system components supports encryption using SQL Server encryption tools.
- Unison clients require a system specific database password specified during installation. The database password must be applied to each Unison client and replication server installation.
- All Unison client applications will automatically lock if left idle for a definable period of time. Operator authentication is required to unlock the client application. Operators can manually lock a Unison client at any time. Any system initiated or manual client locks are logged.
- Partition management makes sure that selected parts of the installation are always monitored.
- Client machine management can be configured to create alarms if a client becomes disconnected from the server.
- Unison has in-built tools for automating system database archival (logs) and for restoring backup.
- SQL database clustering is supported for automated database server redundancy.
- System bootstrap configurations are encrypted using machine-based keys.

> **Note:** Unison does not provide protection against denial of service (DOS) attacks.

[11] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
[12] https://techcommunity.microsoft.com/tag/adhardening
[13] https://www.cyber.gov.au/sites/default/files/2024-09/PROTECT-Detecting-and-Mitigating-Active-Directory-Compromises.pdf

8.2 Time synchronization

Time synchronization is essential for maintaining the integrity of all information and for securing access to system resources (for example, programs and data). System clocks must be synchronized by reference to an accurate time source. It is preferable to synchronize Unison server(s) with a Network Time Protocol (NTP) server.

8.3 Logging

Unison does not write any event information into Windows event logs as it has its own logging framework which stores the information in the Unison Database, however Microsoft SQL Server and other .NET components of the system may do this.

8.4 Installation and post-installation Unison hardening

SQL Encryption

It is recommended to install an appropriate certificate in SQL Server that is signed by a trusted Certificate Authority (CA) that all clients and servers accept. See https://learn.microsoft.com/sql/database-engine/configure-windows/manage-certificates for more information about installing a certificate in SQL Server.

If a trusted certificate is installed, "TrustServerCertificate=True" should be removed from all connection strings as this is a security risk.

Change default credentials

After installation, it is important to change the password of the admin account to a secure password. The admin account should only be used when required. Otherwise use operator accounts with lower privileges.

Password policy

The default password policy in Unison is 14 characters. Adjust this according to the organization's password policy.

8.5 Backup, restore and disaster recovery

The Unison system provides tools for performing automatic system backups at scheduled times and for restoring backups for simpler system recovery in the event of system failure. Database archives, known as logs, can be scheduled for creation and the storage location specified.

Unison clients and drivers are dependent on access to the database server in order to interact with the system. It is, therefore, imperative that a database backup and redundancy system be implemented. For example, to set up database replication system for databases.

Note: Databases can also be backed up and restored using SQL Server or a 3rd party solution.
It is however recommended to use the built-in back-up functions of the Unison system for ease of use.

It is strongly recommended that a backup solution is deployed.

Note: It is currently not possible to automate redundancy for the actual Unison database server.
That is, if the Unison database server computer fails, any drivers that are configured to interact with it will not be able to switch to another computer automatically and will need to be re-configured to use the alternate server and restarted.

8.6 Unison Drivers

For Unison Drivers, please refer to the respective driver's integration guide for detailed instructions, hardening & information. Ensure that you follow the specific guidelines in the integration guide to guarantee proper security and configuration of the drivers.

Additionally, please note that each driver creates an additional attack surface. Therefore, do not install drivers that are not in use.

Appendix A - Port Configurations

The following section contains the IP ports usage for Unison and Unison Drivers. Please note that the exact usage will depend on which drivers are installed and how those drivers are configured.

Unison Core Components

Unison - Servers								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	SQL Server	1433	YES	NO	TCP	Allow	Inbound	Unison Server communication with SQL Server.

Unison - Clients								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Client	SQL Server	1433	YES	NO	TCP	Allow	Inbound	Unison Client communication with SQL Server.
Unison Client	Unison Server	8091	NO	NO	UDP	Allow	Inbound	Unison Client debug information (only if the setting is enabled).

NOTE: *Unison Clients might need additional ports open to 3rd party destinations depending on usage. For example, in order to view video from IP Cameras, the Unison Client will need to have outbound access to the IP/Port of the Camera.*

SQL Server								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Client/Server	SQL Server	1433	YES	NO	TCP	Allow	Inbound	Unison Client/Server communication with SQL Server.

Appendix A – Port Configuration

Unison Drivers

NOTE: *The ports listed below are the default ports used for each Unison Device Driver. Some ports are configurable which means the port listed in this table might be changed from its original configuration.*

Unison - Access Service API

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
3rd party system	Unison Server	8000	YES	NO	HTTP	Allow	Inbound	3rd party system communication with Unison Access Service API.
3rd party system	Unison Server	443	YES	YES	HTTPS	Allow	Inbound	3rd party system communication with Unison Access Service API (encrypted).

Unison - Sentrion

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Sentrion S4	7569	YES	NO	TCP	Allow	Inbound	Sentrion S4 communication with Unison Server (unencrypted).
Unison Server	Sentrion S4	7572	YES	NO	TCP	Allow	Inbound	Sentrion S4 communication with Unison Server (unencrypted).
Unison Server	Sentrion S4	7579	YES	YES	TCP	Allow	Inbound	Sentrion S4 communication with Unison Server (encrypted).
Unison Server	Sentrion S4	7582	YES	YES	TCP	Allow	Inbound	Sentrion S4 communication with Unison Server (encrypted).

Appendix A – Port Configuration

Sentrion Manager	Sentrion S4	22	NO	YES	SSH	Allow	Inbound	Sentrion Manager communication with Sentrion S4.
Sentrion S4	Sentrion Manager Debug	8090	NO	NO	UDP	Allow	Outbound, Multicast	Sentrion S4 debug information to Sentrion Manager Debug.
Web Browser	Sentrion S4	443	NO	YES	HTTPS	Allow	Inbound	Web Browser configuration/management of Sentrion S4.

Sentrion S4 (1)	Sentrion S4 (2)	7589	YES	NO	UDP	Allow	Inbound	Sentrion S4 communication between centrals (unencrypted).
Sentrion S4 (2)	Sentrion S4 (1)	7589	YES	NO	UDP	Allow	Inbound	Sentrion S4 communication between centrals (unencrypted).

Sentrion S4 (1)	Sentrion S4 (2)	7589	YES	YES	UDP	Allow	Inbound	Sentrion S4 communication between centrals (encrypted).
Sentrion S4 (2)	Sentrion S4 (1)	7589	YES	YES	UDP	Allow	Inbound	Sentrion S4 communication between centrals (encrypted).

Unison - Pacom Controller								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Pacom 800x	3435	YES	NO	TCP	Allow	Inbound	Unison Server communication with Pacom 800x Controller.
Pacom 800x	Unison Server	3435	YES	NO	TCP	Allow	Inbound	Pacom 800x Controller communication with Unison Server.

Unison - Milestone								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description

Unison Server	Milestone Management Server	80	NO	NO	HTTP	Allow	Outbound	Unison Server communication with Milestone Management Server (unencrypted). For example authentication and configuration.
Unison Server	Milestone Recording Server	7563	NO	NO	TCP	Allow	Outbound	Unison Server communication with Milestone Recording Server. For video and audio streams, PTZ commands.
Unison Server	Milestone Event Server	22331	NO	NO	TCP	Allow	Outbound	Unison Server communication with Milestone Event Server for retrieving alarms.
Unison Client	Milestone Management Server	80	NO	NO	HTTP	Allow	Outbound	Unison Client communication with Milestone Management Server (unencrypted). For example authentication and configuration.
Unison Client	Milestone Management Server	443	NO	NO	HTTPS	Allow	Outbound	Unison Client communication with Milestone Management Server (encrypted). For example authentication and configuration.
Unison Client	Milestone Recording Server	7563	NO	NO	TCP	Allow	Outbound	Unison Client communication with Milestone Recording Server. For video and audio streams, PTZ commands.

Unison - Panasonic EBL

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	EBL Fire Panel	49152	YES	NO	TCP	Allow	Outbound	Unison Server communication with Panasonic EBL Fire Panel.

Unison - Securifire

Appendix A – Port Configuration

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Securifire Fire Panel	9006	NO	NO	TCP	Allow	Outbound	Unison Server communication with Securifire Fire Panel.

Unison - Honeywell Galaxy Dimension								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Galaxy Alarm Panel	10001	YES	NO	TCP	Allow	Inbound	Unison Server communication with Galaxy Alarm Panel (MDX Protocol)
Galaxy Alarm Panel	Unison Server	10002	YES	NO	TCP	Allow	Inbound	Galaxy Alarm Panel communication with Unison Server (SIA Protocol)

Unison - Schrack Seconet								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Schrack Fire Panel	11113	YES	NO	TCP	Allow	Outbound	Unison Server communication with Schrack Seconet Fire Panel.

Unison - Assa ARX								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Assa ARX Server	5003	YES	YES	HTTPS	Allow	Outbound	Unison Server communication with Assa ARX Server (encrypted).
Unison Server	Assa ARX Server	5004	YES	YES	HTTP	Allow	Outbound	Unison Server communication with Assa ARX Server (unencrypted).

Unison - Modbus								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Modbus Device	502	YES[1]	NO	TCP	Allow	Outbound	Unison Server communication with Modbus Device.

Unison - Ascom Teleprotect								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description

Appendix A – Port Configuration

Unison Server	Ascom Server - OAS	10072	NO	NO	TCP	Allow	Outbound	Unison Server communication with Ascom Server, OAS Protocol.
Unison Server	Ascom Server - OAP	1322	YES	NO	TCP	Allow	Outbound	Unison Server communication with Ascom Server, OAP Protocol.

Unison - Bosch VMS								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	Bosch VMS Server	5390	YES	NO	TCP	Allow	Outbound	Unison Server communication with Bosch VMS Server.
Unison Server	Bosch VMS Client	5394	YES	NO	TCP	Allow	Outbound	Unison Server communication with Bosch VMS Client.

Unison - SALTO								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	SALTO Server	7667	YES	NO	TCP	Allow	Outbound	Unison Server communication with SALTO Server.
Unison Server (acting as SALTO SHIP Server)	SALTO Server	7668	YES	NO	TCP	Allow	Inbound	SALTO Server communication with Unison Server.

Unison - TrakaWEB								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Server	TrakaWEB Server	10700	YES	NO	HTTP	Allow	Outbound	Unison Server communication with TrakaWEB.
Unison Server	TrakaWEB Server	7852	YES	NO	HTTP	Allow	Inbound	TrakaWEB communication with Unison Server.

Unison - WCF Service								
Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
3rd party system	Unison Server	4242	YES	NO	TCP	Allow	Inbound	3rd Party API communication with Unison Server