Unison 5.11.5

Solutions Guide

Disclaimer

PACOM Systems makes no warranty of any kind with regard to this product, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. PACOM Systems shall not be liable for errors contained herein or for incidental consequential damages in connection with the furnishing, performance, or use of this product. This document contains proprietary information and is protected by copyright. The information contained within this document is subject to change without notice.

The PACOM website (www.pacom.com) contains the latest documentation updates. Some options, compliance claims or procedures described herein may not be supported if old versions of device firmware and/or software are used.

Copyright notices

Compliance and accreditations

PACOM products comply with Advanced Encryption Standard (AES) FIPS 197 (encryption version 1.1).

Underwriters Laboratories Inc. (UL) and Intertek Electrical Testing Laboratories (ETL) are product safety standards/accreditors for North America. Product samples are tested to certain safety requirements, and periodic checks of manufacturers' facilities are carried out.

Software license notice

Your license agreement with PACOM Systems, which is included with this product, specifies the permitted and prohibited uses of the product. It is protected by Australian and international copyright laws and international treaty obligations. Your rights to use the Software are limited by the terms stated below, and your use of the Software indicates your acceptance of these terms. If you do not agree with them, you must return, delete or destroy all copies of the Software. Your rights to use the Software terminate immediately if you violate any of the following terms:

- Any unauthorized duplication or use in whole or in part, in print, or in any other storage and retrieval system is forbidden.
- You may not reverse-engineer, disassemble, decompile, or make any attempt to discover the source code of the Software.
- You may not modify the Software in any way whatsoever.

Trademarks

All trademarks, brand and product names are the property of their respective owners:

- Bouncy Castle (http://www.bouncycastle.org)
- #ziplib (http://www.icsharpcode.net/opensource/sharpziplib/)
- Mono Class Libraries (http://www.mono-project.com)
- NUnit (http://www.nunit.org)

Support

For product support, go to the PACOM (support.pacom.com).

Table of Contents

System Basics

The PACOM Unison software platform helps unify technologies, third-party systems and applications to meet a wide range of security requirements. It is focused on simplicity and usability. Unison:

- centralizes security operations
- provides an intuitive and consistent graphical user interface
- uses an IP [Ethernet] platform for communications
- features a modular / open architecture that enables virtually unlimited expandability.

The Windows-based 'open architecture' means that Unison offers integration with and between various sub-systems from many associated industry manufacturers. These sub-systems can be connected, presented and managed from Unison. The Unison application can be used for:

- alarm monitoring
- access control system management
- video surveillance and CCTV integration
- fire detection and alarm system integration
- incident reporting, access control auditing etc.
- logging system events for auditing and reporting etc.
- card access security badging.

Unison system requirements are listed in the *System Requirements* document updated with each Unison release.

Deployment

PACOM Unison can be deployed on a single server that performs all database and device driver functions, or through multiple servers. Multiple server installations support database server clustering (replication), managing geographically different sites, or to split device driver operation across multiple computers for load balancing.

The ability to interface with different sub-systems enables organizations to preserve existing investments and consolidate them into a modern management platform. Unison architecture ensures that security control panel device drivers can be rapidly developed and the core engine can be enhanced as technologies emerge.

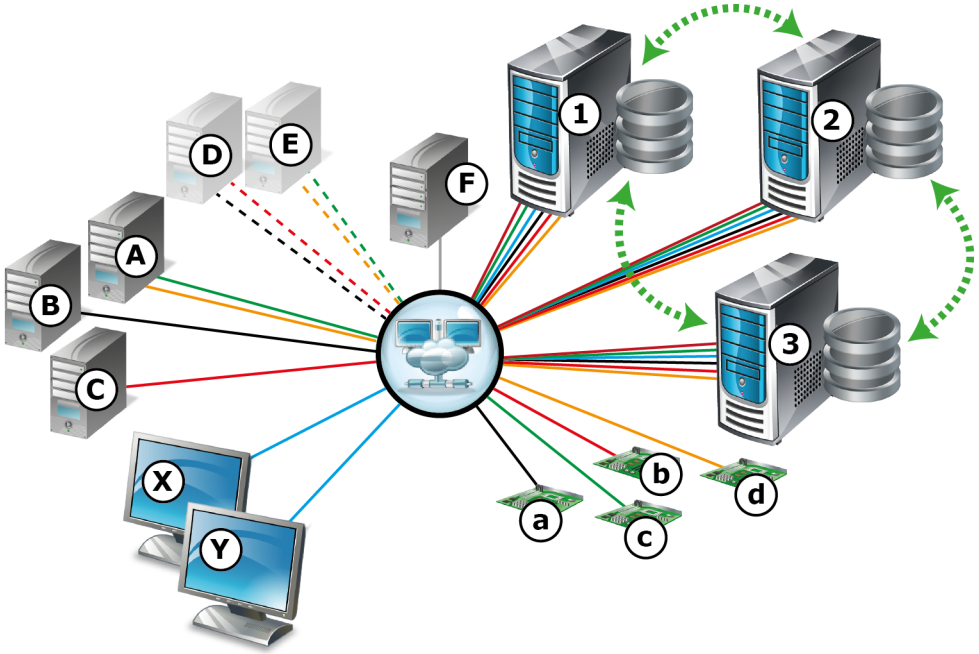
Unison provides control and real-time system status and is a central source for security monitoring and control in campus type (single site, multiple control panel devices) installations; for example, universities, office buildings and hospitals. The Unison system sends and receives messages and alerts from connected security control panel devices; for example, PACOM Controller hardware. The system is database structured and uses a central database as the core, where all operation of the system is derived through information contained within the database. Unison client applications for security operators and system administrators connect to the server over an IP network and are interfaces to the system.

System core components

Component	Description
Unison Server	Used for connection and interfacing between Unison clients, device drivers and system databases. All system functionality is centrally controlled via interaction between the Unison database server and databases. All server types include a system data service component that manages the transfer of graphical image data between Unison servers and clients for graphical images / site maps.
Cluster Server	Optional component Used for database and system redundancy operations (also known as database clustering or replication). These are basically replicas of the Unison server that constantly maintain database content synchronization across all cluster servers.
Client Application	Used by system administrators and security operators for interacting with the system, security monitoring and alarm response.
Microsoft SQL Server	Hosts system databases, which store event, user, system and configuration data.
Device Drivers	Used for interfacing with proprietary and third-party hardware / systems. Device drivers, which are self-contained Windows executables, can be run on different computers for load balancing and redundancy purposes. Each driver component uses a `.dll` file to access the Unison database server (and , therefore, the databases). All components are isolated, so are not affected b changes in other components.

Example

The following example shows basic connectivity in a clustered database and redundant device driver system utilizing:



- An initially installed server (**1**) that hosts the system databases (for the sake of the example, this is referred to as the main).
- 2 additional cluster servers (**2**, **3**) that are also active system servers.

  The main and cluster servers make up the clustered server system. In the case of non-availability of server (**1**), clients and device servers switch to the next priority server in the cluster (**2**); if server (**2**) fails, switch to (**3**). Once server (**1**) is available again, it is synchronized with the other servers in the cluster and then takes over again as the main, with the clients and device drivers switching back to it.
- 2 Unison client workstations (**X**, **Y**) can each connect to any applicable server in the cluster (**1**, **2**, **3**).
- 3 device servers (**A**, **B**, **C**) running device drivers that all connect to any applicable server in the cluster - (**A**) for (**c**, **d**); (**B**) for (**a**); (**C**) for (**b**).
- 2 redundant device servers (**D**, **E**) that can be switched to running device drivers if the currently active device server becomes unavailable -
  - if (**A**) fails, (**c**, **d**) switch to (**E**)
  - if (**B**) fails, (**a**) switches to (**D**)
  - if (**C**) fails, (**b**) switches to (**D**).
- A NTP (network time protocol) server (**F**) to maintain time synchronization amongst all servers.

Note: Configuration of third party security systems / devices is performed using relevant tools provided by the vendor. The Unison system provides hardware configuration support for a range of PACOM security devices.

Miscellaneous deployment features

- Silent installation

  The Unison installer is compatible with Microsoft Windows features that support silent upgrades (group policy management and shared network folders).

  Silent upgrades occur in the background on target computers, without displaying messages or requiring user interaction while installing. The installation can be initiated by the Windows user when logging on or when the computer is next restarted.

  This feature can be extended to perform upgrades on multiple computers in multiple locations without having to be physically present at the computer by using `MSI` and `MST` files in a shared network folder. `MST` files are used for non-standard installation; for example, clients and remote server.

  See the Microsoft documentation for instructions (applies to Microsoft operating systems that support silent installation/upgrades only). For more information, see http://msdn.microsoft.com/en-us/library/ms227324%28v=vs.80%29.ASPX.

- Independent initial configuration

  For PACOM Controller hardware, a web server is incorporated that allows initial controller configuration so that an IP connection to a Unison system can be set up without the need for any intermediary software. Accessing the web server is performed by Ethernet connection to the controller either via LAN / WAN or directly to an Ethernet port.

Security and Encryption

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

- Operator passwords are encrypted in the database.

  Optionally, Windows Active Directory single sign-on can be applied.
- One-way password hashes with Salt are used when saving passwords and validating log ins.
- SHA-1 for passwords has been deprecated for SHA-256.
- Connections between the SQL Server and system components supports encryption using SQL Server encryption tools.
- Unison clients can be installed either using a default (hidden) system SQL password or a custom password can be specified during installation.

  If a custom password is used, this must be applied to each Unison client and 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 from a backup.
- SQL database clustering is supported for automated database server redundancy.
- The default administrator user can be replaced.
- System bootstrap configurations are encrypted using machine-based keys.

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

Databases

A Unison server stores all transaction logs in 2 databases, the main (primary) and log. The databases can be hosted / located on any computer on the network as long as it is accessible. When the Unison system is installed, it creates a native SQL user (Unison Client) that has public server role and db_ owner privileges to the Unison databases. One SQL Server installation can host a number of Unison databases.

Each server-to-client connection to the database is handled individually. Both Windows and SQL Server authentication modes are supported when connecting to the database. As all information is stored and retrieved from the database, information presented in clients is always current. Additional information from the database may be used for statistics or reporting using the integrated reporting tools. For example, generating attendance reports for payroll purposes. Report templates can be tailored to suit user requirements and corporate images.

Requirements

- For small installations with 10 or less devices, Microsoft SQL Express may be used, however, be aware of its database size limitations.
- For larger systems, Microsoft SQL Server (Standard edition or better) is required.
- For large installations with 100 or more devices, Microsoft SQL Server Enterprise edition may be required.

Note: Unison databases are not compatible with Oracle or other database systems.

Database server clustering (replication) and redundancy operation

Unison v5.4 and later, in conjunction with Microsoft SQL Server 2012 and later, provides tools for performing automatic Unison server and database failover / redundancy operations (without requiring proprietary Microsoft SQL Server failover clustering). That is, in the event of server failure or server communications failure, the system will redirect messages from the previously used server to the next available database cluster server. Several servers can be set up for database clustering / replication, with the database in each one being constantly updated with the latest changes, event and other transactions.

The system supports an internally controlled replicated / clustered server system (that is, not using SQL Server redundancy features, such as SQL clustering). This system incorporates deploying several servers in an active-active configuration, which means all are essentially main servers, with system databases constantly synchronized between all servers. The result is a high-availability, load balancing system with inherent redundancy / failover functions. Servers that are used in a database replication / cluster system are known as a cluster servers. The system also supports failback, which means if the initial database server (that failed) becomes available again, the system switches back to using it. When multiple database servers are used, the system databases are continuously replicated amongst all servers.

Note the following:

- Each database replication server must be installed as a cluster server.
- Each cluster server requires a licensed version of Microsoft SQL Server installed.
- A specific SQL Server account is required for database replication functions. It is recommended to use the same SQL account for each database replication server SQL Server instance. Database replication does not support Windows authentication.
- Each cluster server must synchronize time at least once per hour with a NTP (network time protocol) server. The time difference between cluster servers should never exceed 2 seconds.
- Each cluster server must have a unique global database ID assigned to it, which is the mechanism used for selecting the server to failover to. The main server must have an ID of 1.
- Network bandwidth between cluster servers should be a minimum of 100Mbit/sec (based on a typical system of 200 card readers and 1000 alarm inputs). For larger or busier systems, higher bandwidth availability will improve system performance.

Note: When using clustered database servers, if a failover occurs on the server that a client machine is currently connected to, a notification of server connection loss occurs on the client and the operator is automatically logged off. The client will connect to the next available database (the system data service associated with that database will also be used) and the operator must log on again.
If a higher priority server becomes available again after a failover, client machines are not switched back to it automatically - operators must log off from the currently used server and log on to the required server manually.

Microsoft SQL Server clustering and mirroring

Note: If Microsoft SQL Server database clustering is available, it is recommended to use that for redundancy / failover operation.
The redundancy architecture also provides failover / failback operation for device drivers.

- For increased availability, Unison databases can be hosted in a proprietary SQL Server database cluster. Clustering spreads the databases across a number of servers in the cluster and maintains synchronization between them. If a server in the cluster fails, another one of the cluster servers is automatically switched to. Clustering has been tested with *Microsoft Windows Server Failover Clustering*.

  When clustering, the Unison system should communicate with sub-systems using only TCP/IP in order for failover from one cluster node to another to occur. This means that all sub-systems that normally communicate using RS232 COM ports must be connected via Moxa NPort software in order to connect to cluster nodes using IP.

- Database mirroring has been used successfully, however, is not currently fully tested. PACOM reserves the right to provide support for systems using database mirroring.

  In general, mirroring automatically maintains a replica of databases in another SQL Server database. If the primary database becomes unavailable, the mirrored one can be switched to, however, this requires manual intervention and resetting system components to point to the mirrored SQL Server database.

Backup and restore

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.

> **Note:** Databases can be backed up and restored using SQL Server, however, it is not recommended as the process can be complex (refer to Microsoft SQL Server documentation). It is recommended to use the built-in back-up functions of the Unison system.
> It is strongly recommended that a backup solution is deployed.

Third party system integration

The Unison system supports access user / cardholder database export and import features to third party systems, such as for visitor management and other access control management systems etc. Unison also features a generic open interface web service that allows third party systems to be integrated with the Unison system database. Integration allows the uploading of nodes, applicable node commands, node status, alarms etc to be sent to a third party system, and for commands received from third party systems to be performed in Unison.

Device Drivers

Device drivers are the software component of the system that provide the necessary communication protocols and other operations required to correctly interface with specific devices (for example, device events and commands). Device drivers are device-specific executables that can be run across one or more device driver server machines (referred to as a device server in the Unison installer). A single compatible device node may be attached to several device servers to create redundancy operation should the currently used device server become unavailable, and/or for load balancing system resources. An example of load balancing would be a system with several PACOM Controller devices, each with a large number of peripheral hardware attached, and specifying each device to use a different device server. Device server machines require Unison to be installed on them as well as the required device drivers (selectable during installation).

Note: Several system level functions of the Unison system are implemented as devices. For example, the system data service and user import / export functions. The system data service can be configured for redundancy by installing it on separate device servers. It is recommended that only the system data service is run on these servers. It should be noted that this redundancy is only applicable to the same instance of the Unison database. This means that each database cluster server should have its own system data service redundancy device server(s).

For device drivers, in general:

- Any number of different device drivers can be installed and run on each computer, and is basically limited only by the available computer resources.
- If multiple instances of the same device driver are required, each will require its own server - a single computer can run a single instance of a particular device driver.
- Any number of physical devices can connect to a device driver, and is basically limited only by the available computer resources.
- Device driver debug monitoring is available for technician use.

The device driver application programming interface (API) provides a standardized platform for developing device drivers. The core itself is hardware neutral and allows for integrating virtually any kind of hardware. No modifications to the core are required when developing device drivers and new drivers can also be plugged in to previous Unison versions. Certain internal functions of the system are also treated in a similar manner, as device drivers, however, are not actual devices. For example, the user import function.

Automatic configuration

For several supported security control panel device types, Unison is able to read the configuration of the connected third party hardware / system and automatically replicate the component structure of the third party system in Unison. Device templates are also supported, which enable devices of the same type to share common configuration properties by default. Unison device configuration utilities facilitate faster setup of sites and equipment, help standardize configuration thereby reducing the chance for error.

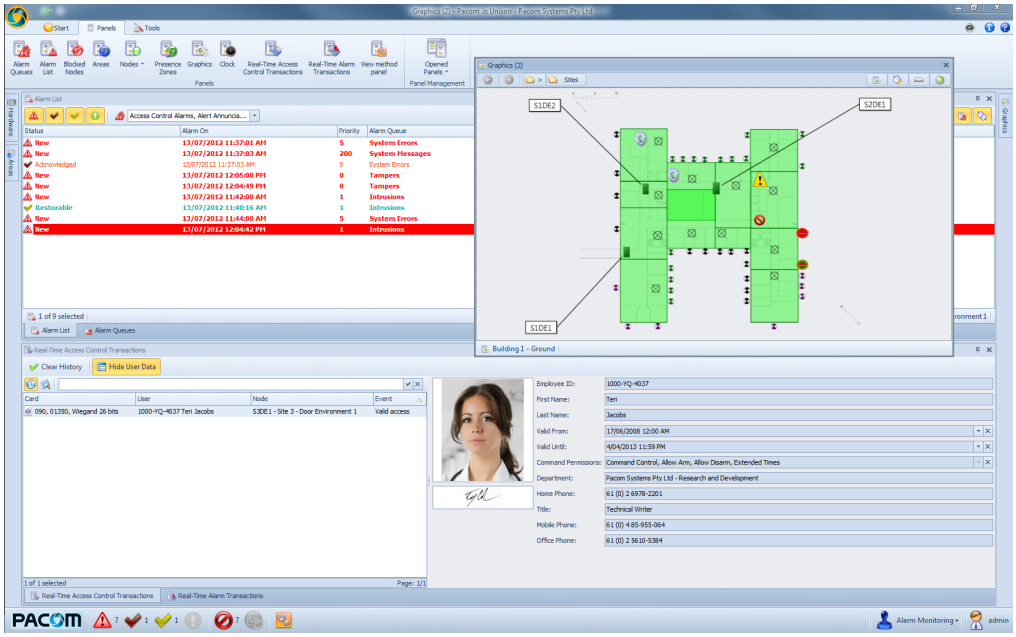
Redundancy operation

The Unison system supports multiple device driver servers that can failover in the event of disruption to device driver server connectivity. This means that if the currently used device driver server becomes unavailable, the next highest priority server will be switched to and so on. The system also supports failback, which means if the initial server (that failed) becomes available again, the system switches back to using it. For each device driver node that has been configured (these nodes control communication / events / commands between the system and connected hardware), each must be set, as required, to use one or more device driver servers, each of which is associated with a database servers and the priority of use.

Unison Client (Workstation)

The Unison client application is used by administrators to set up the system, and for security operators to monitor and respond to security-related situations. Regardless of the connected devices that the client is interacting with, the methods of operation and appearance are presented consistently. Unison uses the concept of roles to specify available system access and functionality to users. Roles and partition, which limit access to system databases, allow the system to be tailored specifically for operators. This means that full control is available over what operators can access within the system and the functionality available to them.

Unison clients can be hosted on any computer on the network as long as they can connect to the Unison database server over TCP.



PACOM Controller Considerations

When using PACOM Controllers in conjunction with Unison systems, it is important to note that there are some limitations inherent in controller data storage capability as opposed to the Unison management system. The difference being that the system is generally limited only by the size of the associated database and/or server resources, and at the controller, by the available on-board memory. Memory expansion cards are available for all PACOM Controllers. When installed, the amount of available access control related data storage increases, provided the controller model permits it. This means that although the system is unlimited in the number of cards (users) or other conceptual access control management nodes, such as access schedules and door schedules that can be created; there are limits for each that a controller can store.

There are different controller types that determine some hardware limitations, such as number of card readers and keypads that can be connected. There may also be model based controller memory management modes that affect access control limits for related features, such as total users (cards) supported and card data size. Limitations vary by controller type and model, possibly licensing, and installed memory expansion (if used).

> **Note:** Unison supports PACOM 8000 Series Controllers. For organizations currently using older PACOM Controllers (for example, 1057/1058) and looking to upgrade systems to Unison, contact PACOM for assistance with a suitable upgrade path.

Controller limitations

Some limitations may vary from that of other PACOM security management applications.

For installations where controller limitations have been exceeded, there may be other options available, such as using additional controllers and splitting the required data between them.

Some features / functions can be increased by the use of expansion cards.

The total number of users that can be stored in a controller varies depending on how personal access is configured in Unison and the maximum allowable number of access schedules. This is because each individual personal access permission for each user is treated as an access schedule in the controller memory. For example, if every user had 10 personal access permissions each, the total number of users that can be stored by a controller (with 64MB memory expansion) will be 500 (that is, 5000 access schedules/10 personal access permissions per user).

With regard to controller memory limitations, assigning access control to users should be carefully considered so that the controller memory usage and user management within Unison is as efficient as possible.

The following table lists standard 8001 and 8002 S, M and L Controller access control limitations:

Feature / Function	**Limits**		
	Small	Medium	Large
Card Data Size	64-bit	64-bit	64-bit
Calendar Entries	100	100	100/*500/**1000
Users (Cards)	500	2000	4000/*10000/**256000

Feature / Function	Limits		
Offline Events	1000	1000	1000/*10000/**128000
Access Groups/User	8	8	8
Access Schedules	100	100	100/*500/**5000
Intervals/Access Schedule	8	8	8
Door Schedules	200	200	200/*500/**2000
Intervals/Door Schedule	4	4	4/*8/**8
Day Types	10	10	10/*32/**32

* With 16MB memory expansion.

** With 64MB memory expansion.

The following table lists 8001 and 8002 S, M and L Controller model hardware limitations:

Hardware / Feature	Limits		
	Small	Medium	Large
Inputs	32	128	256
Outputs	8	32	64
Alarm Areas	32	32	32
Card Readers	8	32	64

Anti-virus software

When using anti-virus software on Unison servers, it must be configured correctly in order to not affect Unison stability or performance.

Issues that may arise as a result of incorrect configuration are:

- locking of database files during virus scanning
- communication problems during virus scanning of network ports
- reduced performance.

Bandwidth

Bandwidth represents network data requirements for normal system operations. Due to variances in the available bandwidth or connection speed, the following table provides examples of the length of time taken to perform a range of client-database server operations over a range of available bandwidths.

Operation	Time (seconds) required for available bandwidth				
	500kbps	1Mbps	5Mbps	10Mbps	100Mbps
Start Unison and log on	14	13	13	13	13
Retrieve and list 17000 users	10	3	3	3	3
Move 10 users	1	1	1	1	1
Move 1000 users	7	7	7	7	7
Generate 1000 test nodes	40	40	40	40	40
Operator authorization (check SysAdm)	20	12	12	12	10
Create and open log file with 61200 entries	4	1	1	1	1
Batch update properties of 1000 nodes	8	8	8	8	8
Operator authorization (3 profiles)	34	15	15	15	15
Load Alarm Management dialog box, instructions and 4 images	Time out	85	18	10	4
Load Alarm Management dialog box, instructions and 1 image	34	17	4	3	2
Load Alarm Management dialog box and instructions	1	1	1	1	1

Note: For information relating to data transfer speeds or storage, "b" represents data "bit" values and "B" represents data "byte" values.
Available bandwidth of 10MB per second is regarded as a minimum.

Buffering

Unison uses buffers and caches between device drivers, clients and the database in order to maximize speed and response times and to help balance system loads. Clients use a local buffer that is dynamically updated each second to ensure a minimal time between updates recorded in the system database and for those changes to be reflected in Unison clients.

Graphics are pre-loaded onto the client machine hard disk when operators log on, with selected graphics also cached into RAM. This helps maximize performance for graphics rendering (in other words, reduce the time required to display graphics to operators) and reduce server load in terms of retrieving graphics and sending them to client machine as and when required. To support this functionality, the system data service component is used, which manages the transfer of graphical image data from servers to client machines. The system data service can also use encryption for added security.

Computers and distribution

The number of server computers, database clustering / replication, number of client computers, database storage etc depends largely on customer requirements for how the system is to operate and how busy the system is in general terms.

The following guidelines must be considered:

- Computers should meet or exceed the minimum requirements for hardware and software in order to provide the best and most reliable system performance. Specifications are listed in the system requirements and release notes for each Unison version.
- Adequate storage is required for transaction data. Databases should be archived regularly (this is a default Unison feature that can be configured for storage location and archiving frequency).
- If many devices are in use (for example, fire alarm panels), it is recommended to distribute the device drivers over several servers and to set up each device in the system to use particular device servers in order to balance system loads. If commands take excessive amounts of time to be executed by devices, this may be an indication that the system / device drivers are overloaded.
- A network time protocol (NTP) server is required for maintaining synchronization between different aspects of the system (databases, servers, devices, etc.).
- If redundancy is specifically required for the system data service component, it is recommended that each device server used to run a backup system data service has no other device drivers running on it.

  Note: Redundancy is applicable to the system data service associated with a single database instance. This means that redundancy would need to be set up for each individual database in a clustering / replication system.

- If PACOM Controllers are in use, it is recommended to not run more than 10 device nodes per device driver, and not to run more than 10 device instances per device node.

- To gauge system performance and loads, use the Windows Resource Monitor on the Unison server to view which, if any, hardware components are being overloaded by the Unison process and/or device driver executables. If Unison or the device drivers are consistently using large amounts of system resources then load-balancing the system may help better distribute and handle system loads.

Data

Data refers to stored records in the database and log files. The primary database contains the latest log entries. When the limit is reached for how many days of events to store in the primary database, the oldest log entries are moved to the log database. When the log database reaches the limit for how many days of events to store, a copy of the database is created and automatically archived, then the log database is emptied. Archived database file names include, for instance, its creation date.

Sample database sizes are:

- Approximately 1GB for system and event data + image files + site map files + log files.
- Image files are stored in the database in compressed `jpeg` format; approximately 50KB for each image.
- Site map files may vary considerably according to the number of contained security objects and the original AutoCAD drawing (if used).
- Log file entries are approximately 1KB for each event.

Disaster recovery

Unison clients and device 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 clustering as a redundancy for databases.

> **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 devices 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.

Email

Unison supports Simple Mail Transfer Protocol (SMTP). SMTP is a widely supported Internet standard for email transmission across IP networks.

IP addressing

- Computers running Unison servers must have static IP addresses.
- Unison clients support either static or dynamic (DHCP) addressing.
- Controllers should have static IP addresses. They can use dynamic IP addressing (DHCP), however, each time the address is changed, the controller must contact the system to update it with the new address in order to re-establish communication - this requires extra bandwidth.

Operator access management

Operators represent names and passwords that can be used to log on to the system. Operators are connected to operator groups that define permissions which determines how the operator can interact with Unison. The concept of operators and operator groups is very flexible and allows you to define exactly which functions are available to operators. For example, which views they can open, which features are available etc. Unison supports an unlimited number of operator accounts.

- Unison features partitioning, which can be used to define which parts of the system an operator group can view and interact with.

  Partitions represent portions or segments of the database that are used with operator groups to limit access to database objects and related information for relevant operators. That is, if an object is associated with a particular partition, only operators with permissions for that particular partition will be able to view, edit etc. So operators of a particular group may be able to view and edit some (but not all) objects of a certain type.

- Unison permits only authorized operators to administer various aspects of the system, by using permissions.

  Permissions are whether or not a system feature or part of the database is accessible to the operator. For example, an operator being able to view an aspect of the system, or, for example, send commands to a device.

  Permissions apply whenever an operator logs on to the system.

- Unison features operator roles that can be used to control the user interface presented to operators. Various panels and views can be opened and displayed in the Unison application window in a specific way, then saved as a role. Roles can then be assigned to operators. As a result, whenever an operator logs on, a particular role is applied so that the user interface is consistent and the correct components are displayed. For example, operators that are monitor specific alarm types may have a role that shows only part of the system required to view and respond to alarms of a particular type.

  Roles, when used, apply whenever the operator logs on to the system.

- Unison can either allow or prevent operators from changing their own passwords.
- In the operator change log, you can verify which operator carried out a specific operation or caused a change in the database.
- Unison features partitioning, which can be used to define which parts of the system an operator group can view and interact with.

  Partitions represent portions or segments of the database that are used with operator groups to limit access to database objects and related information for relevant operators. That is, if an object is associated with a particular partition, only operators with permissions for that particular partition will be able to view, edit etc. So operators of a particular group may be able to view and edit some (but not all) objects of a certain type.

Ports

All ports used by the system and device drivers can be configured as required. Ports that are being used must be made available for correct operation.

Default ports, where applicable, are listed in the Unison Compatibility Matrix.

See the Appendix for port configurations.

SNMP

The Simple Network Management Protocol (SNMP) device driver is capable of receiving SNMP traps, which are primarily events from hardware devices. The SNMP driver uses WMI (Windows Management Instrumentation), which means that there is also supports WMI events; for example, if a process has started, or data has been written to the Windows registry.

The computer running the SNMP device driver must:

- have Windows SNMP and WMI components installed.
- allow anonymous log on for COM ports.
- have firewalls configured to allow SNMP traps (port 162 UDP and TCP).

For detailed information on these requirements, refer to Windows documentation.

> **Note:** Setting up WMI queries on remote computers is not recommended as different operating system and COM settings may present reliability issues.

SSL

Unison supports Secure Sockets Layer (SSL). SSL are cryptographic protocols that provide communication security over IP networks.

Time synchronization

Alarm system management and response is time based, therefore, it is crucial that times between various components of the Unison system are synchronized. It 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.

> **Note:** For clustered database server installations, an NTP server is required.

Upgrading

From time to time, Unison software will be re-released with new features or supported device drivers etc. The upgrade process requires the Unison system to be temporarily shut down and all connections (Unison servers, clients and device drivers) to the Unison databases be terminated before upgrading.

Video integration

- Unison supports messages and commands with video interfaces for viewing live footage, however, it does not store video footage. Some, for example, Bosch VMS 3.01 do support tagging of recorded footage for non-live viewing from within the Unison environment.
- PACOM offers an Integrated Video application that can be installed on Unison client computers, allowing operators to access supported third party video systems for viewing live and historical footage. This application offers several features, including automatically launching from the Unison client, showing multiple simultaneous video displays etc. (available features may depend on the video systems in use).

Virtual machines, terminal services and remote desktop connections

- Unison is designed to work on virtual machines, however, this is not currently fully tested.

  PACOM reserves the right to provide support for systems using virtual computers.

  - Windows terminal services are supported.
  - Unison is designed to work via remote desktop connections, however, this is not currently fully tested

    PACOM reserves the right to provide support for systems using remote desktop connections.

Windows event logging

Unison does not write any event information into Windows event logs, however, the Microsoft SQL and .NET components of the system may do this.

Question	Answer
General system queries	
How many security control panels can be monitored?	Monitoring of security control panel is limited only by server performance and available resources.
Are there options for supporting the system via a remote connection?	Unison is designed to work via remote desktop connections, however, is not currently fully tested. PACOM reserves the right to provide support for systems using remote desktop connections.
Can the alarm and access control functionality be split to allow for a more flexible solution?	Yes Operator group permissions and partitions can be used so that different functionality can be routed to individual operators.
How often should log files be backed up?	Database archive log files should be backed up weekly.
How is the Unison database backed up?	Unison incorporates automated scheduling for database archive log files. SQL Server clustering is supported for automated SQL database redundancy.
How are emails generated? Are there any authentication requirements?	Unison requires an SMTP server for routing emails sent by the system. SMTP server user name and password authentication is supported.
Operators	
Where is operator account and password information stored?	Operator account and password information is stored in the system databases. Passwords are stored in encrypted form.
Can operators change their passwords when required?	Yes, if the associated operator group permissions allow it.
Can passwords be made to expire?	No
Is a minimum password length enforced?	No
Can passwords include a mixture of characters and numerals?	Yes
Can the same password be re-used?	Yes
Can Unison automatically log off unattended clients?	Yes After a configurable period of time, the Unison client will automatically log off if it is not being used.

Question	Answer
Does Unison support Windows single sign-on?	Yes Unison is able to support both native and Windows Active Directory (single sign-on) authentication for operators.
Card access **Note**: Individual PACOM Controller hardware is limited in terms of internally stored access card data. Depending on the controller model and installed memory card, a maximum of 200000 cards is possible.	
How many access cards can be supported?	The number of access cards is only limited by server performance and available resources.
In terms of access control time management, are there any limitations?	Access control time management is only limited by server performance and available resources for conceptual time management nodes, such as access schedules and door schedules.
Software **Note**: Refer to the release notes for the applicable Unison version for system requirements. Later version of Windows include most of the additional applications required. For clustered database server installations, a licensed SQL Server 2012 or later is required on each server.	
Is any additional software required?	The following additional software is required: • Microsoft SQL Server or SQL Server Express (free edition - for use with very small systems only) • Microsoft .NET • Microsoft Windows PowerShell • Microsoft Windows Media Player (for client machines) • Microsoft Installer (for machines hosting SQL) • Moxa NPort as a serial-to-IP interface for devices that support serial communications only.
How are Unison software updates performed?	Releases are available to authorized dealers via the PACOM FTP site.
What development software is Unison written in?	Unison is coded in Microsoft .NET (C#).
Does Unison support AMD processors?	No
What operating systems are supported?	64-bit Microsoft Windows and Windows Server operating systems.
How does Windows service packs and patches affect the system?	At the time of a Unison release, PACOM announces the Windows versions that are officially supported. If there are subsequent Windows release(s), PACOM will not guarantee that Unison will work with these versions until fully test and officially supported.
Which database does Unison use?	SQL Server or SQL Express (free edition - for use with very small systems only).

Question	Answer
Client workstations	
How does Unison control access to client applications?	Operators must authenticate themselves by operator name and password or with a Windows Active Directory account. These are used when starting Unison and when logging on and logging off. Unison does not restrict access to any other desktop applications.
How many clients can be used?	The number of clients is only limited by server performance and available resources. However, the number of clients that can be connected at the same time is licensed.
Is any data stored on Unison clients?	No All data is stored in the system database.
Does the Unison client application modify the standard desktop or can it be used to administer the client PC?	No
Network and communications	
What port numbers are used by the system?	Default ports are specified for various devices that can connect to the system. All ports may be configured as required. • Unison clients use TCP port 8000 (default). • SQL Server uses TCP port 1433 (default).
Can the system monitor third party equipment?	Yes Device drivers are available for a range of security control panels devices, including PACOM Controllers.
Can the system send commands to devices?	Yes All supported devices have a range of available command and control capability.
What communication ports are used?	Unison requires several TCP ports for normal system operations and may require others depending on the device drivers in use. See Ports.
Can Unison use printers?	Yes Any local or networked printer that is locally configured can be used.
Does the system require static addresses?	• Machines running Unison servers must have static IP addresses. • Unison clients support either static or dynamic (DHCP) addressing. • Controllers should have static IP addresses. They can use dynamic IP addressing (DHCP), however, each time the address is changed, the controller must contact the system to update it with the new address.

Question	Answer
Does the system support redundant components?	Yes The system provides an internally controlled clustered database server architecture (database replication), which has inherent failover/failback functionality. Device drivers can be run on multiple servers for failover / failback operation. **Note**: If SQL database clustering is available, it is recommended to use that for redundancy / failover operation.

Appendix - Port Configurations

Details for configuring Unison ports.

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison - Client								
Unison Client	SQL Server	1433	✓	×	TCP	Allow	Inbound	Client to SQL Server communication
Unison Client	Unison Server	9684	✓	×	HTTP	Allow	Inbound	Client to Unison Server communication (System Data Service)
Unison Client	Unison Server	9684	✓	✓	HTTPS	Allow	Inbound	Client to Unison Server communication (System D
Unison - Server								
Unison Server	SQL Server	1433	✓	×	TCP	Allow	Inbound	Server to SQL Server communication
Unison - Milestone								
Unison Server	Milestone Management Server	80	×	×	HTTP	Allow	Inbound	Unison Server communication with Milestone Management Server (unencrypted). For example, authentication and configuration.
Unison Server	Milestone Management Server	443	×	✓	HTTPS	Allow	Inbound	Unison Server communication with Milestone Management Server (encrypted). For example, authentication and configuration.

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Unison Client	Milestone Management Server	80	×	×	HTTP	Allow	Inbound	Unison Client communication with Milestone Management Server (unencrypted). For example, authentication and configuration.
Unison Client	Milestone Management Server	443	×	✓	HTTPS	Allow	Inbound	Unison Client communication with Milestone Management Server (encrypted). For example, authentication and configuration.
Unison Client	Milestone Recording Server	7563	×	×	TCP	Allow	Inbound	Unison Client communication with Milestone Recording Server. For video and audio streams, PTZ commands.
Unison - Panasonic								
Panasonic EBL Fire Panel	Unison Server	49152	✓	×	TCP	Allow	Inbound / Outbound	Communication between Unison and panel
Unison - Securifire								
Securifire Fire Panel	Unison Server	9006	×	×	TCP	Allow	Inbound / Outbound	Communication between Unison and panel
Unison - Sentrion								
Sentrion S4 Panel	Unison Server	443	×	✓	HTTPS	Allow	Inbound	Web server communication
Sentrion S4 Panel	Unison Server	7569	×	×	TCP	Allow	Inbound	Sentrion protocol (standard)
Sentrion S4 Panel	Unison Server	7572	×	×	TCP	Allow	Inbound	Sentrion protocol (standard)

Source	Destination	Port	Configurable	Encrypted	Service	Action	Direction	Description
Sentrion S4 Panel	Unison Server	7579	×	✓	TCP	Allow	Inbound	Sentrion protocol (encrypted and/or with certificate)
Sentrion S4 Panel	Unison Server	7582	×	✓	TCP	Allow	Inbound	Sentrion protocol (encrypted and/or with certificate)
Sentrion S4 Panel	Unison Server	7589	×	×	UDP	Allow	Inbound / Outbound	Sentrion Manager (configuration)
Sentrion S4 Panel	Unison Server	22	×	✓	SSH	Allow	Inbound	Sentrion Manager (configuration)
Sentrion S4 Panel	Unison Server	8090	×	×	UDP	Allow	Outbound / Multicast	Sentrion Manager debug information