Unison v5.12.0

Installation 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

Deployment Overview

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

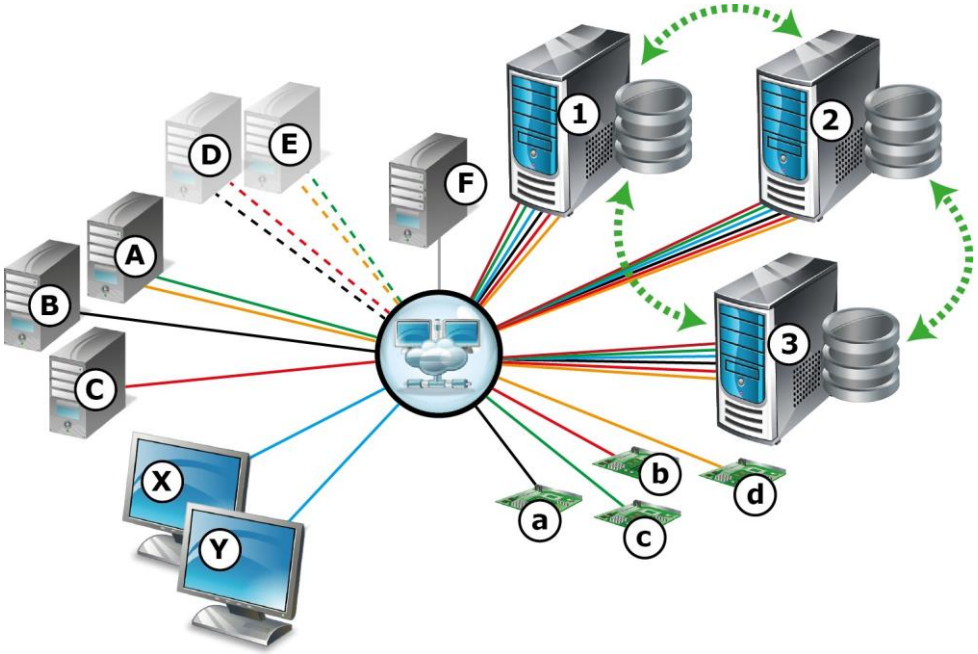
> **Note:** It is important to read and fully understand all relevant sections of this guide in order to correctly install a Unison system. For upgrades from older versions, refer to the appendices for guidelines to changes in system operation between versions and the necessary steps to take in order to successfully upgrade. Similarly, if PACOM Controller hardware is in use, refer to the appendices for information.
> You can upgrade from older Unison system versions and PACOM Unison Controller hardware.

System core components

Component	Description
Unison Server	Used for connection and interfacing between Unison clients, drivers and system databases. All system functionality is centrally controlled via interaction between the Unison database server and databases.
Unison Replication Server	*Optional component* Used for database and system redundancy operations. These are basically replicas of the Unison server that constantly maintain database content synchronization across all replication servers.
Unison Driver Server	*Optional component* Used for running one or more Unison drivers on a physically different server for performance, redundancy or security reasons.
Unison Driver(s)	Used for interfacing with a specific hardware/system or to perform certain type of functionality. Unison drivers, which are self-contained Windows executables, can be run on any Unison Server type as listed above. Each driver component is isolated and runs independently so is not affected by changes in other driver components.
Unison 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.

Example

The following example shows basic connectivity in a replicated database system with redundant driver servers utilizing:



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

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

Prerequisites

Take into consideration the following prerequisites before installing PACOM Unison:

General

- For specific hardware and software requirements, refer to the *System Requirements* document for the specific Unison version to be installed.
- The user performing the installation must have write access to all installation folders. It is recommended that this user has Windows administrator permissions.
- It is recommended that you change the default SQL password to a randomly generated, strong password during any Unison installation or upgrade.

Servers / Communications

- Machines running Unison services must have static IP addresses.
- Hardware devices communicating with Unison must in general have static IP addresses.
- Hardware devices that support serial communications only require Moxa NPort / DIGI PortServer software or equivalent to manage serial-to-TCP data conversion in order to communicate with Unison. Moxa NPort supports traditional virtual COM ports or through TCP Server mode - selection of either is dependent on the driver in question.
- Networks using database replication require a network time protocol (NTP) server to maintain time synchronization between database servers. Time synchronization between servers and the NTP server should occur at least once per hour, which may require configuration (http://support.microsoft.com/kb/816042).

> **Tip:** The time difference between replication servers must never exceed 2 seconds.

Firewalls / Ports

- For each Unison server, open a Windows firewall port for SQL Server database connections according to http://support.microsoft.com/kb/968872.
- For installations using specific hardware, open the port(s) required for the subsystem and ensure that it is not blocked by any type of firewall (Windows, client-side, network, third-party firewalls, etc). Please refer to the Unison Solutions Guide *Appendix – Port Configurations* for a full list of default ports for each supported subsystem.

Windows environments

- For installations using Windows authentication to sign in to the Unison system, ensure that the latest operating system updates are installed on all server and client machines.
- If the Windows environment has the user account control (UAC) feature enabled, UAC related confirmation dialog boxes may display during the Unison installation process.

> **Tip:** Confirmations required through these dialog boxes must be completed within 2 minutes of appearing, otherwise the Unison installer process will be terminated by Windows without any information provided as to why the installer failed.

Database backup and restore

The Unison system provides tools for performing automatic system backups at scheduled times and for restoring from backup 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.

It is recommended that the built-in back-up functions of the Unison system are used. Databases can also be backed up and restored using SQL Server or a 3rd party backup/restore tool if needed.

It is strongly recommended that a backup solution is deployed.

Virtual machines and remote desktop connections

- Virtual machines using VMWare or Hyper-V are supported.
- Remote desktop connections are supported.

Anti-virus software

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

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

- Locking of database files during virus scanning.
- Communications problem during virus scanning of network ports.
- Reduced performance.

Compatibility with embedded web content

Download and install Microsoft Edge Webview2 Runtime on client and server computers before performing a Unison installation or upgrade. This is required if the WebViewControl graphic control is to be used in Unison Graphics.

Windows and SQL Server Requirements

Microsoft Windows and SQL Server must be installed before Unison can be installed. The following must also be installed before installing the SQL Server:

- Windows Installer
- Windows PowerShell
- Microsoft .NET Framework.

During installation the currently installed SQL Server version is validated. If the minimum requirement for the SQL Server version (as listed in the Unison Release Notes) is not met, the Unison installation will not proceed.

The information provided here is a guide only and may alter depending on Microsoft Windows and SQL versions in use - refer to Microsoft documentation for details.

Consider the following ...

- If using the same machine for both the Unison database server and Microsoft SQL Server, for best performance it is recommended that you configure the SQL Server to use approximately half the available system RAM.
- For installations using Unison Enterprise or Unison replication servers, SQL Server Express is not recommended for performance reasons.
- Please bear in mind that access to the servers might also allow access to Unison database information, so make sure to severely limit who has permission to logon to Unison and SQL Server machines. It is also strongly recommended that all servers are physically protected i.e. kept inside a locked server room with limited access.

SQL Server

The following Microsoft SQL Server settings are specifically required for the Unison system:

- It is generally recommended to install SQL Server as a **default instance**, but named instances are also supported.
- It is recommended that Unison Servers use **SQL Server Authentication** with an SQL Account having the **sysadmin** Server Role.
- If Windows Authentication is used, make sure that:
    - NT AUTHORITY\SYSTEM account (which runs the Unison Server Installer) has **sysadmin** Server Role
    - Windows Users that log on to the Unison Server and starts the Unison Server Manager or runs Unison Server Configuration manually has the **sysadmin** Server Role.
    - The Windows service account that runs *Pacom Unison Server Process* service has the **sysadmin** Server Role (if set to other than NT AUTHORITY\SYSTEM account).
- Make sure that the *SQL Server* service startup type is set to **automatic**.
- Make sure that the Windows service account that runs *SQL Server* service is NT AUTHORITY\SYSTEM.
- Verify that the SQL Server service is running.
- In the SQL Server Configuration Manager, SQL Server Network Configuration, Protocols for MSSQLSERVER settings, enable the **TCP/IP** option.
- If encryption is required, enable the **force encryption** option in the SQL Server network configuration, protocol settings.
- SQL Server Locale Support: English-language version only.

SQL Server Database Roles

The following roles are created and used in the database:

- **UnisonPublic**
  This role is required during the first step of the login. The role has essentially only access to the login procedure. Accounts that are used for client connections should not have any other permissions other that this role in the Unison databases.
- **UnisonLegacy**
  This role is required (in addition to UnisonPublic) for accounts that are using Legacy AD or Legacy Singl Sign-On. This allows the lower security for these authentication methods to be used.
- **UnisonSession**
  The role that is used by the session account. Gives limited permissions to read and change the databases. Please note that the session account is linked to a specific Unison operator, and that some sensitive data is protected against unauthorized changes by the database checking the type of change against the operator's permissions in Unison.

Active Directory & Single Sign-On

If Single Sign-On to Unison clients is to be used, which is recommended from a security perspective, all Unison machines must be part of the same Microsoft Active Directory domain.

With Single Sign-On, logging in to the Unison client will not require a username or password, but instead the client's login to SQL Server determines the current operator, with SQL Server performing the authentication.

A SQL Server account is setup as an Active Directory group (recommended) or identity. SQL Server then looks up which operator in Unison is linked to the connected Windows user and then automatically logs in that operator.

This also require that all Unison clients, when installed, are configured to use a Windows Authenticated connection (Integrated Security) to SQL Server.

Unison Clients running on the Unison server itself does not use Single Sign-On by default but are using the same connection string as the PACOM Unison Server process. If Single Sign-On is required for clients running on the Unison Server, the Unison Client Configuration needs to be run separately after installation.

> **Note:** Since this authentication method is based on which Windows user is logged on to the client machine, this limits the ability to 'switch operator' in the Unison client. Switching to a different operator require the current operator to log out of Windows, and the new operator to log in.

MSDTC

Microsoft Distributed Transaction Coordinator (MSDTC) is not used by Unison.

Windows firewall

The following Microsoft Windows firewall settings are specifically required for Unison servers in order to allow incoming Unison client connections:

- Create an **inbound rule** for the SQL Server Windows service, then:
  - For **port** settings, select the **TCP** and **specific local ports** options.
  - Set the **port number** to **1433**.
  - Enable all **allow connection** options.
  - Enable the appropriate **profile option(s)** (usually Domain).
  - Name it **SQL Server**.

Installation

The installation process uses a step-by-step wizard, with each screen providing various options. The same procedures apply to new installations as well as upgrades.

> **Note:** If using the same machine for both Unison server and SQL Server, it is recommended that you configure SQL Server to use approximately half the available system RAM for best performance.
>
> If upgrading, please refer to the Appendix *Upgrading from Older Versions* regarding specific considerations of the system before proceeding with the upgrade.

Before installing

The following must be installed before installing Unison:

- Microsoft .NET Framework 4.8 on each Unison server and client computer
- SQL Server (see Windows and SQL Server Requirements).

Installation steps

There are three main processes when installing Unison, that must be performed in the following order:

1. Configure Windows and SQL Server.
2. Install Unison servers.
3. Install Unison clients (workstations).

Installation types

There are various installation types that determine the functionality available.

The following options are available from the Setup Type installation screen:

Setup Type Option	Description
Client	Installs a Unison client workstation that is used by operators for security related activities. Client machines require connectivity to a Unison server in order to function. This type of installation is used where multiple Unison client machines are used to connect to a central Unison server.

Setup Type Option	Description
Server	Installs system databases and components as a primary server. A server of this type is mandatory and allows client workstations / secondary servers to interact with the system. When installing a server, a client workstation installation is also included in order to provide a user interface to the system. For standalone systems, where a single computer is used for all system activities (generally used for smaller systems for hosting system databases and drivers, and also being the client workstation), a Unison server installation is all that is required.
Replication Server	Installs a server and databases for use in a replicated server system. This system incorporates deploying several servers in an active-active configuration. This means that all system databases are constantly synchronized between them. The result is a high-availability, load balancing system with inherent redundancy / failover capability.
Driver Server	Installs as a driver server and client application only, without a database. This type of server is for installing and running drivers externally to the Unison server, for driver redundancy operation and/or load balancing system resources. Driver servers require connectivity to a Unison server in order to function. The system supports multiple driver servers.

Configure Windows and SQL Server

The following instructions can be used if you are installing the PACOM Unison server for the first time or upgrading.

Configure Windows

1. Make sure all Unison Servers and Clients are using a Windows version that is supported by Unison. Please refer to the *System Requirements* document for a list of supported Windows versions.
2. Make sure all Windows Servers and Clients are updated with the latest Windows updates.
3. On the Windows Servers, configure the firewall to allow SQL Server remote connections as well as any driver hardware connections that require inbound connections to the Unison Server. See the *Solutions Guide* document for more information of different ports used.
4. If Single Sign-On is used, make sure that all machines are connected to Active Directory and that Windows Accounts are created for each operator that should use Unison.

Configure SQL Server

1. Make sure all Unison Servers are using a SQL Server version that is supported by Unison. Please refer to the *System Requirements* document for a list of supported SQL Server versions.
2. Make sure all SQL Servers are updated with the latest service packs for the installed version.

If only Unison login is used, no further SQL Server accounts need to be created.

In order to use Windows Authentication (Integrated Security) login to SQL Server from Unison Clients (or Clients running on the Unison Server), logins must be created in SQL Server:

How to

SQL Server accounts can be created with Microsoft SQL Server Management Studio (SSMS) which can be download for free from Microsoft. SSMS is typically installed on the Unison server or the SQL Server machine.

1. Start SSMS and connect to the SQL Server which hosts the Unison database.
2. Right-click on Security -> Logins and select **New Login...**
3. Use the Search… button to link the login to an Active Directory group (recommended) or Individual user.
4. Select the group (user) you want to link the account to and click OK.

   Please note that Unison operators that should be able to login to Unison must be members of the selected Active Directory group, and that you must connect each individual Unison operator to an Active Directory user in order to use Single Sign-On for this operator.
5. In the User Mapping page for the login, all Unison databases needs to be ticked (UnisonMain, UnisonLog, UnisonArchive_xxx). For each database, the **UnisonPublic** role must be ticked in addition to the **public** role.

   The role **UnisonLegacy** must be ticked if Legacy AD or Legacy Single Sign-On is to be used (not recommended).

SQL Server Certificates

To use an encrypted connection to SQL Server, a certificate is needed. By default, SQL Server installs a self-signed certificate which is only trusted by itself.

In order for connections to accept self-signed certificates they either need to be added as trusted certificates in Windows on each connecting machine, or the SQL Server connection string needs to contain "TrustServerCertificate=True" (not recommended).

In Unison Server/Client configuration -> Database connection dialog you can switch to Custom Connection to edit the connection string. When you have added or removed the option "TrustServerCertificate=True" (in both Main and Log connections), you can switch back to normal connection again.

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.

> **Note:** If SQL Server Certificates are used, all SQL Server connection strings used must be specified using the server's name and not the IP address.

The following instructions can be used if you are installing the PACOM Unison server for the first time or upgrading.

Obtain the files

3. Download PACOM Unison Installation Files.
4. Click `Unison_Setup_x64.msi` to display the Installation Setup Wizard.

How to install the server

1. On the Installation Setup Wizard, click **Next**.

   Depending on your Windows version and security settings, the User Account Control screen may display. You can verify the software certificate by clicking **Show Information**. If you accept, click **Yes**. Other security warnings may be displayed by Windows depending on network settings, etc.

   What language is used? The display language of the installer is determined by the machine Windows regional settings. If the required regional language is not available, English is used.

   The End-User License Agreement screen displays.

2. Review the license agreement and if acceptable, tick the **I accept the terms in the License Agreement** checkbox.
3. Click **Next** to display the Destination Folder screen.
4. Choose the destination folder for the installation.
   - To accept the default installation folder, do not change anything.
   - To set a different installation folder, click **Change**. The Change Destination Folder screen displays, where you can browse to the required folder. Click **OK** to confirm the change and close the screen.
5. Click **Next** to display the Setup Type screen.
6. Select which type of server to install:

Setup Option	Description
Server	Installs a primary server, databases and the client application.
Replication Server	Installs a server, databases and client application as a member of a replicated server system. When installing a replicated system, the initial server must be installed using the **Server** option (to be a primary server). Subsequent servers must be installed using the **Replication Server** option. This is to ensure that server priority is correctly set and that there is no possible conflict in database identification in a replicated server system.
Driver Server	Installs a driver server and client application only, without a database.

7. Click **Next** to display the Ready to Install Pacom Unison screen.

8. Click **Install**.

   The Installing PACOM Unison screen displays showing progress of the installation.

   The PACOM Unison Server Setup Wizard starts and the Welcome screen displays.

9. Verify that all open programs are closed.
10. Click **Next** to display the Database Connection screen.
11. Enter the database information:

    a. In the **Local Server Connection** section, enter the SQL Server name to use, or click the **Server** drop-down to display the available SQL Server instances.
    NOTE: The drop-down require SQL Server Browsers to be active which are not enabled by default.

    Each database instance is specified as [COMPUTER_NAME]\[INSTANCE_NAME]; for example, "UNISON-SRV\MSSQLSERVER".

    Click the required option to select it. There are also advanced settings for you to use.

    For **Advanced Settings**, see Server and Client "Advanced" Settings.

    > **Note:** It is no longer possible to use localhost, "127.0.0.1", "." or "::1" in the **Local Server Connection**. Use the server name (or Server IP address, if encryption certificates are not used).
    > If restoring a database or upgrading on the same workstation with localhost already set as default, then everything will work as normal. Only when selecting the connection ellipsis on the Hardware-System-Unison Servers-Database Master Server and then clicking **OK** or **Test**, will the pop-up message *Cannot use 'localhost' in connection string* display.

    b. The **Database Status** section shows any applicable database information for the selected SQL Server instance.

    For example, the version of any currently existing Unison database and the database version that will be installed.

    When upgrading, an Advanced option is displayed that allows certain tasks to be carried out on existing databases, such as making back-ups, see Server and Client "Advanced" Settings.

12. Click **Next** to display the Database Installation Path screen.
13. Choose where Unison databases will be located.

    If installing for the first time:

    - To accept the default installation folder, do not change anything.
    - To set different installation folder(s), select **Specify Folders Manually**, then click  next to each database type (Main and Log) to open a Select Folder dialog box, where you can browse to or create the required folder.

      > **Note:** Installing each database file on different physical hard drives may help improve system performance.

    If upgrading to a recent version:

    - Tick the **Backup Databases for Update** checkbox to create a copy of the databases before the update begins.

14. Click **Next** to display the Performing Database Upgrade screen with the progress of the installation.

    After database installation or upgrade, the Set Global Database ID screen displays.

15. The settings are required if a replicated database system is being used; otherwise accept the default **Global Database ID of 1**.

    The initial primary server must have a global database ID value of **1**.

    Subsequent servers in a replicated database system must have differing ID numbers. The installer automatically applies the next available highest priority ID value as it is installed.

16. Click **Next** to display the Configure Unison Client Password screen.

    This sets the password that all Unison clients (workstations) must use in order to access the databases (via the Unison server).

    Select which client authentication modes are accepted by the (SQL) server:

    a. **Unison**
    Username and password is authenticated against username and password stored in the Unison database.

    b. **Single Sign-On**
    Username and password is not required but is determined and authenticated by the client's connection to SQL Server. Note that this option require a SQL Server login linked to a Windows Active Directory group (or identity) to be setup.

    c. **Legacy AD** (Not recommended)
    This option is kept for backwards compatibility but is not recommended since authentication is done by the client.

    d. **Legacy Single Sign-On** (Not recommended)
    This option is kept for backwards compatibility but is not recommended since authentication is done by the client.

    If several options are selected, the client will try them in the following order:
    1) Single Sign-On 2) Legacy Single Sign-On 3) Legacy AD 4) Unison

    > **Note:** If a new database is installed, it is recommended to have the authentication method Unison selected in order to make it possible to login from Client machines to administer Unison Operators and connect them to SSO-accounts. However Unison always allows Unison-authentication for clients connecting with sysadmin permissions in SQL Server, even if this option is not selected in the Server Wizard. This is so basic administration should always be possible, for example from the Client on the Unison server.

    Tick the **Configure SQL Server for Unison Client Access** checkbox to have the installer automatically setup Unison client access to the database.

    If this option is not enabled, client access to the database will require manual configuration (refer to Microsoft SQL Server documentation).

Enter a system specific secure client password and ***make sure to store it in a safe location.*** It is recommended to use the same password across different replication servers to make backup/restore easier.

Is it strongly recommended to NOT use the default password for security reasons.

A client password is always required for SQL Server access regardless of selected client authentication mode.

> **Note:** The system specific client password must be applied when installing the Unison client(s), otherwise they will not be able to access the databases

17. Click **Next** to display the Register/Update Drivers screen.

    This screen lists all supported drivers.

18. Tick the selection box next to each required driver to install it.
    - Newer versions of drivers must be used when available. If you have other drivers that are newer or additional to the displayed items, click **Add Driver** to open a Select Driver dialog box, where you can browse to and select the required driver(s).
    - If you are unsure which drivers will be used, install **all** drivers.
    - When upgrading, if the path for a driver is highlighted red, it means that the installation path is different to that of the existing installation.
    - If required, use the **Driver Language** field to force the drivers to use a specific language independent of the language set for the operating system. That is, properties and displays in Unison for the driver will be in the selected language. Note, however, that not all text or messages in the system may support this. It is not recommended to install drivers in a different languages to what is generally used.
19. Click **Next**.
20. When the installation completes, click **Finish** to close the Unison Server Setup Wizard and return to the Unison installer. Related system Windows services may start at this point.
21. Click **Finish** in the Unison installer to exit.
22. Reboot the computer, if required.
23. After installation, start the PACOM Unison Server Process Windows service.

    It starts automatically after reboot or requires manual start if no reboot.

    When the service is running, Unison Service Manager displays in the Windows system tray, at the bottom-right of the desktop.

    The Unison Service Manager is a tool that allows you to license the system, install and configure drivers and control associated Windows processes.

    To open the Unison Service Manager, double-click the task manager icon .
    - If the installation involves multiple driver servers (for running specific drivers) or integrates with other systems that require assigning the server to a particular system, click **Configuration** to open the Configuration dialog box, then set **Run System** to the applicable driver server. Normally, there is only one node called "System" (see the "System Management" topic in the Unison help for information).

> **Caution:** Do NOT start any Unison client applications for normal system operation (that is, clients that are to be used by operators for normal security purposes) until the system is properly configured.

Installing Driver Servers

The installation procedure for driver servers is similar to that for a Unison server.

How to

1. Click the installer file, `Unison_Setup_x64.msi`, to display the Installation Setup Wizard.
2. Click **Next** on the Welcome screen.

   Depending on your Windows version and security settings, the User Account Control screen may display. You can verify the software certificate by clicking **Show Information**. If you accept, click **Yes**. Other security warnings may be displayed by Windows depending on network settings, etc.

   What language is used? The display language of the installer is determined by the machine Windows regional settings. If the required regional language is not available, English is used.

   The End-User License Agreement screen displays.
3. Review the license agreement and if acceptable, tick the **I accept the terms in the license agreement** checkbox.
4. Click **Next** to display the Destination Folder screen.
5. Choose the destination folder for installation.
   - To accept the default installation folder, do not change anything.
   - To set a different installation folder, click **Change**. The Change Destination Folder screen displays, where you can navigate to the required folder. Click **OK** to confirm the change and close the screen.
6. Click **Next** to display the Setup Type screen.
7. Select to install a **Driver Server**.
8. Click **Next** to display the Unison Client Setup Wizard.
9. Click **Next** to display the Configure Unison Client Connections screen.

   This sets the Unison server and password that the client uses in order to access the system databases.
10. Add a new server to the **Database Server** list.

    Click the three dots (…) on the server and configure the database connection to the Unison database the driver server should connect to.

    Enter the client password for the system as specified in the server installation as the database password.

    Click **Test** to test the connection.

    To add and set up servers:
    - Click **Add** for a new entry to be added to the list. Click **...** for the entry to display connection options - see Server and Client "Advanced" Settings.
    - Click **Move Up** / **Move Down** to adjust the order of the database servers that the client follows for connections in the event of a database failover. That is, connect to the first server in the list, if that is unavailable, connect to the second server and so on.

11. When the installation completes, click **Finish** to close the Unison Client Setup Wizard and return to the Unison installer.
12. Click **Finish** in the Unison installer to exit.
13. Reboot the computer, if required.

The installation procedure for database replication servers is similar to that for a Unison server.

How to

1. Click the installer file, `Unison_Setup_x64.msi`, to display the Installation Setup Wizard.
2. Click **Next**.

   Depending on your Windows version and security settings, the User Account Control screen may display. You can verify the software certificate by clicking **Show Information**. If you accept, click **Yes**. Other security warnings may be displayed by Windows depending on network settings, etc.

   What language is used? The display language of the installer is determined by the machine Windows regional settings. If the required regional language is not available, English is used.

   The End-User License Agreement screen displays.
3. Review the license agreement and if acceptable, tick the **I accept the terms in the license agreement** checkbox, then click .
4. Click **Next** to display the Destination Folder screen.
5. Choose the destination folder for installation.
   - To accept the default installation folder, do not change anything.
   - To set a different installation folder, click **Change**. The Change Destination Folder screen displays, where you can navigate to the required folder. Click **OK** to confirm the change and close the screen.
6. Click **Next** to display the Setup Type screen.
7. Select to install a **Replication Server**.
8. Click **Next** to display the Unison Server Setup Wizard.
9. Click **Next** to display the Database Connection screen.

   This sets the database server that the Pacom Unison Server process uses in order to access the system databases.
10. Select the server using the **Server** list.
11. Click **Next** to display the Database Installation Path screen.
12. Choose where Unison databases will be located.
    a. To accept the default installation folder, do not change anything.
    b. To set different installation folder(s), select **Specify Folders Manually**, then click next to each database type (main and log) to open a Select Folder dialog box, where you can navigate to or create the required folder.

> **Note:** Installing each database file on different physical hard drives may help improve system performance.

If upgrading:

- To a later version, tick the **Backup Databases Before Update** checkbox to create a copy of the databases before the update begins.
- From a non-replicated installation to a replicated database server system and an existing database is detected locally, the Replication Server Upgrade Options screen

displays. This screen provides options for how the database is installed with reference to the primary database:

- Select **Do Not Upgrade Database Now** to leave the database upgrade as a manual process to be done after the server is installed.
- Select **Restore Recent Master Backup** to upgrade using an existing primary database backup. Enter the path to the required database backup file in the **Backup File** field or click  to open a dialog box, then select the database backup file.
- Select **Create New Empty Database** to delete the existing database and create an empty, upgraded database.

13. Click **Next** to display the Performing Database Upgrade screen with the progress of the installation.

    After database installation or upgrade, the Set Global Database ID screen displays.

14. Accept the default global database ID number or use the **New ID** field to set a different value.

    The initial primary server must have a global database ID value of **1**.

    Subsequent servers in a replicated database system must have differing ID numbers. The installer automatically applies the next available highest priority ID value as it is installed.

15. Click **Next** to display the Configure Unison Client Password screen.

    This sets the password that all Unison clients (workstations) must use in order to access the databases (via the Unison server).

    Select which client authentication modes are accepted by the (SQL) server to the same options as set on the primary server.

    Tick the **Configure SQL Server for Unison Client Access** checkbox to have the installer automatically setup Unison client access to the database.

    If this option is not enabled, client access to the database will require manual configuration (refer to Microsoft SQL Server documentation).

    Enter the same client password as set during the primary server installation.

16. Click **Next** to display the Register/Update Devices screen.

    This screen lists all supported drivers.

17. Tick the selection box next to each required driver to install it. Install the same set of drivers as installed on the primary server, or if unsure, install all drivers.
18. Click **Next**.
19. When the installation completes, click **Finish** to close the Unison Server Setup Wizard and return to the Unison installer.

    Related system Windows services may start at this point.

20. Click **Finish** in the Unison installer to exit.
21. Reboot the computer, if required.

Note: For Unison clients to connect to system databases, the Windows firewall must be configured to allow correct connection permissions (see Windows & SQL Server Requirements).

How to

1. Click the installer file, `Unison_Setup_x64.msi`, to display the Installation Setup Wizard.
2. Click **Next** on the Welcome screen.

   Depending on your Windows version and security settings, the User Account Control screen may display. You can verify the software certificate by clicking **Show Information**. If you accept, click **Yes**. Other security warnings may be displayed by Windows depending on network settings, etc.

   What language is used? The display language of the installer is determined by the machine Windows regional settings. If the required regional language is not available, English is used.

   The End-User License Agreement screen displays.
3. Review the license agreement and if acceptable, tick the **I accept the terms in the license agreement** checkbox.
4. Click **Next** to display the Destination Folder screen.

   Choose the destination folder for installation.

   - To accept the default installation folder, do not change anything.
   - To set a different installation folder, click **Change**. The Change Current Destination Folder screen displays, where you can browse to the required folder. Click **OK** to confirm the change and close the screen.
5. Click **Next** to display the Setup Type screen.
6. Select to install a **Client**.
7. Click **Next** to display the Ready to Install the Program screen.
8. Click **Install**.

   The Installing PACOM Unison screen displays showing progress of the installation.

   The Unison Client Setup Wizard starts and the Welcome screen displays.
9. Verify that all open programs are closed.
10. Click **Next** to display the Configure Unison Client Connections screen.

    Click **Add** to add a new database server connection.

    Each database instance is specified as `[COMPUTER_NAME]\[INSTANCE_NAME]`; for example, `UNISON-SRV\MSSQLSERVER`.

    Please note that if a SQL Server certificate is being used, the computer name of the database server needs to be used and not the IP address.

    It is also possible to name the connection. The name is then presented in the client's options for database connections. If no name is provided, the name of the database server is shown in the client's database connection options.

The client will automatically test the specified connections in the provided order when logging in, however it is also possible to manually select which connection to use. If a client loses a connection to the database, a failover will occur to the next connection in the order or configuration.

Click the three dots (…) in the database server cell to configure the database connection.

Choose Authentication method:

- **Unison Client Authentication**

  This is the recommended choice if Single Sign-On is not used. This SQL Server account is automatically created during Unison Server installation. No password is required for this choice since the database password is used for the connection.

- **Windows Authentication (Integrated Security)**

  Uses SQL Server Windows Authentication, which means that the Windows user running the Unison client must have permissions to logon to SQL Server. For this to work, the Unison client machine and the SQL Server machine must be part of the same Active Directory.

  It is recommended to use an Active Directory group (as opposed to individual Active Directory users) as SQL Server login. See also *Configure Windows and SQL Server* section in this document.

- **SQL Server Authentication** (not recommended)

  This option requires a SQL Server account setup with the role UnisonPublic in all Unison databases (UnisonMain, UnisonLog, UnisonArchivexxx). The username and password for the account is then specified in the connection string.

  If the Legacy AD or Legacy Single Sign-On options are used (not recommended), the SQL Server account must also have the UnisonLegacy role for all databases in order to allow for client-based authentication.

Once authentication method has been selected, click OK and enter the client password (as specified during the server installation) as the Database Password.

Click **Test** to test the connection.

For **Advanced Settings**, see Server and Client "Advanced" Settings.

> **Note:** The Unson Client supports High DPI but some parts may still look strange depending on which resolution is used. This is being improved with each new version, but if this occur or becomes a problem, High DPI support can be ignored by setting: Unison Client -> Properties - > Compatibility Tab -> Select “Change high DPI settings” then check the “Override high DPI scaling behavior” checkbox and select “System”.

Replicated database servers

For installations that use replicated database servers, it is possible to configure clients to be able to log on to several replicated servers.

a. Click **Add** to insert additional servers into the list.

b. To remove a server so that the client cannot log on to it, select it in the list then click **Remove**.

c. To change the selection order of servers for operators during log on, select a server and click **Move Up** / **Move Down** as required.

d. To access advanced settings for any server in the list, select it, then click **...**, see Server and Client "Advanced" Settings.

e. Enter the client password as specified during the server installation as the Database Password.

11. Click **Next**.
12. When the installation completes, click **Finish** to close the Unison Client Setup Wizard and return to the Unison installer.
13. Click **Finish** in the Unison installer to exit.
14. Reboot the computer, if required.

> **Caution:** Do NOT start any Unison client applications for normal system operation (that is, clients that are to be used by operators for normal security purposes) until the system is properly configured.

Advanced Installation Options

Unison Client Configuration supports a number of command options that can be used in order to automate installation of Unison clients.

- `/SaveConfigPath=c:\path\to\file`
  Used to export configured database connections to an configuration file that can be read by other client installers.
- `/LoadConfigPath=c:\path\to\file`
  Overwrites any currently configured database connections with those from the specified configuration file.
- `/ConfigPassword=xxxxx`
  Specifies a password for the configuration file. If uset, a standard password will be used.
- `/Silent`
  Runs the installer without showing any dialogs. Suitable for scripting of `/LoadConfigPath`.

Please note that the export file contains sensitive data that should be protected and should under no circumstances be left on the client machine after installation.

Advanced Settings

Advanced settings are available for:

Server / Client

> **Note:** Advanced settings should be modified for special reasons only, for example, to encrypt the database connection or split the main and log databases across different computers, etc.

Advanced settings are available from the Advanced Connection Options dialog box.

- For servers:

  Click **Advanced Settings** in the Unison Server Setup Wizard, Database Connection screen, **Local Server Connection** region.

- For clients:

  Click **Advanced Settings** in the Unison Client Setup Wizard, Set Client Logins screen.

The following settings can be configured:

Option	Sub-option	Description
Default Connection		Use the default connection to the database.
	Server	Specifies the computer and instance of SQL Server to connect to.
	Secure Connection	Encrypts the connection to the database.
	Authentication	How to authenticate to the database. Select: • **Unison Client Authentication** Uses the database password to authenticate to SQL Server. • **Windows Authentication** Uses Windows authentication to authenticate to SQL Server. • **SQL Server Authentication** Uses the specified SQL Server account to authenticate to the SQL Server. Username and password must be provided.
Custom Connection		Determines if custom connection strings to connect to SQL Server are used.
	Main	Specify a custom connection string for the main (primary) database.
	Log	Specify a custom connection string for the log database.
Test Connection		Tests connection to database and displays test results.

Database

When upgrading and Unison databases exist, additional database functions are available from the Advanced Options dialog box.

Click **Advanced** in the installer Database Connection screen, **Database Status** section, to:

Option	Description
Back up	Create back-up copies of existing main and log databases.
Benchmark	Measure SQL database performance.
Drop	Deletes the existing main and log databases.
Restore	Import data from backed-up main and log databases.

Authentication (Technical information)

The Unison client login to the Unison database occur in two steps.

In the first step, the client connects to the database with a public account. This account should only have the database role **UnisonPublic** in the database and has very limited access.

UnisonPublic is not allowed to view or change data but can only call the login stored procedures in the database.

The login process checks the following credentials from the client:

- **Unison Authentication**
  Name and password is checked against the Unison database.

- **Single Sign-On**
  No credentials are sent. The login process checks the Windows User of the SQL Connection (Integrated Security / Windows Authentication) and links this to a Unison operator.

- **Legacy AD** (not recommended)
  The Unison client validates name and password against locally connected Active Directory and sends the Active Directory user's identity (SID) to the login process that links this to a Unison operator. Only allowed if the account has the role **UnisonLegacy**.

- **Legacy Single Sign-On** (not recommended)
  Same as Legacy AD, but the Unison client sends the client machine's logged on Windows user's SID instead. Only allowed if the account has the role **UnisonLegacy**.

The login process also verifies that the correct Client Password (Database Password) is sent regardless of the authentication process used.

In step two, the login process creates a session account (UnisonSess-xxx) with extended permissions in the database, however still limited to only necessary client access. The password for this account is generated randomly and is returned to the client upon successful login.

The client then reconnects to the database with this temporary account and the logged-on operator can then continue working, using this session. The session account is removed once the client is closed or if the communication with the client is interrupted.

Licensing

Unison is licensed on a per-module basis for alarm management, access control, video, intercom, elevator, fire alarm panel integration, etc. The total number of Unison clients is also licensed. Furthermore, most modules are also licensed for a limited number of applicable nodes. For example, an access control module includes the ability to manage 10 doors - if management for more than the currently available number of doors is required, packs are purchased to increase the number. Licensing is enforced using a license file provided by PACOM that attaches to unique server information for validation.

After a new installation, Unison will work unlicensed for 30 days. After the 30 day period, a valid license file must be loaded. The license file is based on a computer signature, which is unique to every computer. For example, something similar to `G2D5N2Q97MJAdggRxZ0u8xN3LQc=`. The Unison license file is generated by PACOM and requires that you provide the computer signature in order to generate the license. The license file can be used only with the computer associated with the signature.

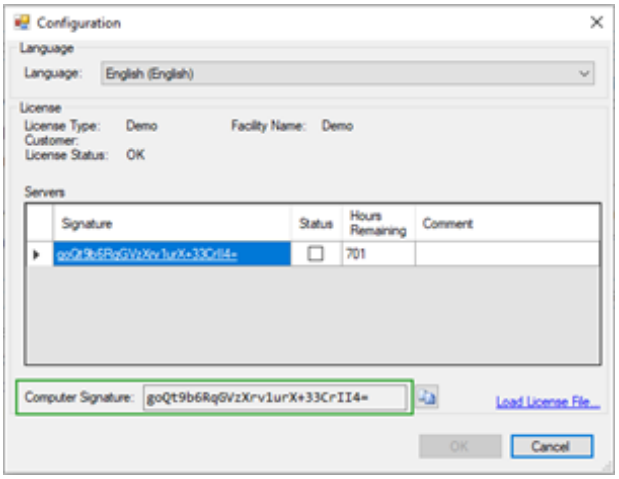
How to access the computer signature

1. Double-click the Unison Service Manager in your System Tray.
2. Click **Configuration**.

   The Configuration dialog box opens.
3. Copy the contents of the **Computer Signature** field and use it when requesting the license.

   Copy the entire signature by using **Copy to Clipboard** next to the **Computer Signature** field.

   > **Note:** For replicated database server installations, the computer signature for the primary server and each replicated server must be provided, so that all servers are properly licensed. System database replication can be carried out only on licensed servers.



4. Once the license file has been created, download it to an accessible network location and then load it into Unison.

Load the license file

1. Click **Load License File** in the Configuration dialog box.
2. Go to and select the license file.

   Details of the facility and license are also displayed in the **License** section of the Configuration dialog box. Any servers that have been set up are displayed in the **Servers** table, along with their status and any grace period hours remaining (if applicable).

Uninstalling

If needed, you can:

Uninstall PACOM Unison

1. Go to the Windows **Control Panel > Programs > Programs and Features**.
2. Select **Pacom Unison**, then click **Uninstall** from the right-click menu or from the toolbar options.

Repair PACOM Unison

1. Go to the Windows **Control Panel > Programs > Programs and Features**.
2. Select **Pacom Unison**, then click **Repair** from the right-click menu or from the toolbar options.

Appendix

There may be instances where you need to:

- upgrade from older versions
- set up the system data service
- set up database replication

or you have issues with 64-bit COM ports.

Upgrading from Older Versions

Over the course of Unison's development, several aspects of the system have changed. In most cases, these changes do not affect how an upgrade is performed, however, for some versions there are some additional tasks that must be performed in order for the system to function as it was prior to the upgrade.

Before upgrading

- All Unison clients should be closed before beginning the server upgrade process.

  This is to prevent client applications from attempting to interact with the Unison database whilst it is being changed (the database is effectively in maintenance mode).

- Terminate the PACOM Unison Server process Windows service on each server prior to starting the upgrade.

System settings or components affected by upgrades

The following information lists the settings or system components that are affected during the Unison upgrade process.

Upgrade path	Affected setting/component	Change/Problem	Description/Solution
previous to 5.4.0 and onwards	System domain, calendar and day type	Node type name change	Node type names changed from "system domain" to "calendar", and previous "calendar" to "day type" to better reflect functionality. Calendar now represents different geographical regions or other distinctions that require variations in dates for public holidays etc. Day type is what is defined in a calendar and is used to reference changes from "normal" access control operation, for example, door operation.
	Device server	Device property change Settings no longer used are erased during upgrade.	The system supports a device server concept to be able to provide redundancy and load balancing of Unison device drivers by allowing them to run on separate machines and for devices to switch between them as required. This design replaces and builds on the previous concept of system domains and calendars, which were used to define where device drivers were running and which one to use. Because of this, the previous system domain and calendar settings are no longer applicable, therefore, it will be necessary to specify the device server for every device in use, with the exception of the system device. The device server setting is in the **Properties > Advanced Properties** section.

Upgrade path	Affected setting/component	Change/Problem	Description/Solution
	Database	New system capability Node types added	The system enables databases to be replicated / mirrored amongst a cluster of servers for the purposes of database redundancy. Nomination and configuration of database cluster services is provided through the normal installation process as described in "Setting Up Database Clustering/Replication" on page 51. Additional configuration of applicable new node types on the Unison server is then required to make database clustering functional - see the Unison user help, *System Management > Configuring the System > Database and Device Driver Configuration and Management* topic.
5.5.0 onwards	Operator log on	New system capability	The system supports Windows authentication / single sign-on. This allows operators to automatically log on to Unison using their Windows credentials.
5.6.0 onwards	Client machine	Node type added	Unison client machines can be added as nodes. This allows client application / machine events to be used when configuring system behavior. For example, creating an alarm if a client machine stops working unexpectedly. Client machine can also be blocked to prevent any operators from logging on, if required.
	Operator groups	New capabilities	Operator groups support defining which client machines can be used and role / skin to apply.

Upgrade path	Affected setting/component	Change/Problem	Description/Solution
5.7.0 onwards	Operating system	32-bit support ended	Unison no longer supports 32-bit operating systems. Ensure that the Windows operating system in use is 64-bit and is compatible with Unison. Refer to the release notes for compatible version information.
	Hardware	Machine specification changes	Ensure that computers being used for running Unison components meet the minimum requirements. Refer to the release notes for minimum computer specifications.
	PACOM Controller hardware	Machine specification changes and limitations	Ensure that computers being used for running PACOM Controller node drivers meet the minimum requirements, and do not exceed the number of device drivers running on a single server. Refer to the release notes for information.
	System Data Service	New system component	Introduced the system data service, which manages data transfer for graphics from server to client through an additional service. Set up the system data service as described in the Unison user help, *System Management > Configuring the System > System Data Service Configuration* topic. **Note**: If system data service communication is encrypted, each Unison client must have the encryption certificate imported into it. This requires a Windows administrator user. Later versions of Unison set up the system data service as part of the normal installation process.

Upgrade path	Affected setting/component	Change/Problem	Description/Solution
	Alarm list	Operator group permission added	Operator groups that require the ability to sort alarm lists will must have the sorting alarms permission enabled. Previously, it was a default feature of any operator group.
	Graphics	New system capability	Graphics now use the System Data Service for transfer from the server to the client. To further improve graphics performance it is now possible to pre-load selected graphics on client machines when operators log on. The graphics are selected on an operator group basis. Any graphics that are not pre-loaded will be downloaded to the client from the server when required.

Upgrade recommendations

Prior to upgrading:

- Ensure that a valid Unison license is available for the version to be installed.

  If a non-valid license is used, Unison will apply the grace period. After the grace period expires, device drivers or other parts of the system will no longer function correctly.

  Apply the license using the Unison Server Manager application after performing the upgrade. See Licensing.

- If database replication is in use, note the global database ID value of each Unison database server in the system before performing the upgrade.

  The database ID value can be checked in the **Properties** tab for each database replicated server node.

- For any third party devices, check the compatibility between the Unison driver and the third party device. This information is available in the release notes and compatibility matrix for the Unison version.

- If any abnormal system behavior is noticed after upgrading, it is recommended that the debugging to file is activated for the applicable driver so that information is available to PACOM Support staff if investigation is required. Ensure that the location where the debug file is saved has adequate space, as these files can become very large.

Upgrade procedure

1. Close all Unison clients.
2. Terminate the PACOM Unison Server process Windows service on all Unison servers.
3. Make sure to back-up the Unison databases as a precaution.
4. Terminate the Unison Service Manager (`PacomIs.ServerManager.exe`) application on all Unison servers if it is running.
5. Upgrade Unison in the normal manner.

   Note the following:

   - Upgrade all server machines before upgrading client machines.
   - If database replication is in use, upgrade each server in the system in the order of its original global database ID value. That is, upgrade the server with database ID **1** first (the primary server), then **2** and so on.
   - If multiple Unison servers are in use as driver servers, upgrade these after upgrading replication servers.
   - Once all server and client machines are upgraded:

     a. Start SQL Server on the database machines if the application was either terminated or the machines shut down.

     b. Start the PACOM Unison Server process Windows service on the database primary server first.

     c. Start each replication server, if applicable.

     d. Start each driver server, if applicable.

     e. Once all servers are operational, Unison client applications can be used as normal.

Roll-back procedure

If it is necessary to roll-back Unison to the previous version:

1. Uninstall Unison.
2. Install the previously running version of Unison in the normal manner.
3. Load the previously backed up databases to Unison.

Upgrading from older versions and using PACOM Controller hardware

As PACOM Controller hardware integration has been phased into Unison since version 5.x, many features supported by PACOM Controllers have been introduced. However, not all settings or concepts have been fully supported. In these cases, Unison GMS or the GMS Config software may have been used to configure controllers for features not supported by Unison at the time. As various Unison and controller firmware releases progress, many settings previously managed by the GMS software are now managed using Unison. Most affected settings are automatically converted and imported into Unison through the **initialize** command, using the existing controller configuration as the source. In cases where these settings are not automatically imported, they must be manually configured in Unison since the original settings configured using GMS are discarded during the initialization process.

Caution: PACOM strongly recommends against using GMS to manage settings after the controller is running using Unison.
Once the following procedure is complete and the Unison-Controller are synchronized, it is highly recommended to perform all controller configuration from the Unison system.

PACOM Controller settings affected by upgrades

The following table describes the settings that either require manual configuration in Unison or are discarded during the Unison upgrade process.

Upgrade Path	Affected Setting	Problem/Change	Solution
5.3.x to 5.4.x	Anti-passback for multiple doors	Settings made using GMS are permanently erased from controller memory.	If anti-passback for multiple doors is required, do NOT upgrade as it is not possible to re-apply the previous settings.
5.4.x to 5.9.0	Controller macros / expressions	Settings made using GMS are permanently erased from controller memory.	It is recommended to make records of any event, card reader or BMS macros / expression configurations in use before migrating to Unison and re-defining them after the migration. In terms of the tools to use to re-define macros/expressions, Unison v5.8 or later should be used. GMS may be used if the Unison version is pre-5.8, however, this is not recommended.
	Reader schedule	The schedule which has egress mode configured in 5.4 is still downloaded to RTU as egress mode but it shows locked mode in Unison.	A user needs to open the reader schedule through the user interface and re-save the schedule again to force an update.

Upgrade Path	Affected Setting	Problem/Change	Solution
5.4.1 to 5.5.1	Area schedules	Timezones created using GMS are erased from controller memory.	Recreate the necessary area schedules in Unison, apply them to the required areas and download the configuration to the controllers.
	Egress schedules	Timezones created using GMS are erased from controller memory.	Recreate the necessary egress schedules in Unison, apply them to the required doors and download the configuration to controllers.
	Door schedules	Card+PIN+OP, Card+OP, GIN+OP and Egress+OP modes are no longer used.	Time intervals in existing door schedules that used any of the now unsupported modes are set to "blocked". These intervals will require changing to an applicable door mode that is supported.
	Card reader settings	Card reader settings that are visible and can be configured using GMS that are NOT visible in Unison are erased from controller memory.	Any card reader settings not in Unison are currently not supported. Once a controller is configured to communicate with Unison, it is not possible to configure card readers on that controller using GMS.
5.7.x to 5.9.0	Elevator schedules	Timezones created using GMS are erased from controller memory.	Recreate the necessary elevator schedules in Unison, apply them to the required elevators and download the configuration to controllers.
Pre 5.8.0 to 5.9.0	GMS output linkages (partial)	Simple output linkage configuration is automatically migrated. More complex ones will be wiped out and will need to be manually configured.	Some GMS output linkages need to be manually re-programmed in Unison.
Pre 5.8.0 to 5.9.0	Reader Macros	These macros remain on upgrade and can be programmed through GMS but currently cannot be programmed through Unison.	All GMS reader configurations cannot be programmed through Unison and need to be programmed through GMS.
Pre 5.8.0 to 5.9.0	BMS Macros / Settings	The macros and the settings are wiped out on upgrade and are not supported in this version of Unison.	It is recommended not to use this version of Unison for any site requiring the BMS feature.

Upgrade Path	Affected Setting	Problem/Change	Solution
Pre 5.8.0 to 5.9.0	Timezone macro conditions	These setting are not used on upgrade and need to be manually reconfigured with Unison basic schedule conditions instead.	Manual configuration is required.
Pre 5.8.0 to 5.9.0	Alarm Event Macros	Simple alarm event macros configuration is automatically migrated. More complex ones will be wiped out and will need to be manually configured.	Partial automatic support only. Manual configuration required in complex configurations.
Pre 5.8.0 to 5.9.0	Vaults and Vault Controllers		Not supported in Unison.
Pre 5.8.0 to 5.9.0	People counters		Not supported in Unison.
Pre 5.8.0 to 5.9.0	Ports and Protocols (Partial)	Commonly used protocols are supported. Unsupported protocols to be listed.	Partially supported in Unison.
Pre 5.8.0 to 5.9.0	Alarm User Types (Partial)	For a list of Supported Alarm User Types, refer to the list in the Unison software configuration screens.	Partially supported in Unison.
Pre 5.8.0 to 5.9.0	Message Filters (Partial)	For the list of Supported Message Filters, refer to the list in the Unison software configuration screens.	Partially supported in Unison.
Pre 5.8.0 to 5.9.0	1062 CRI operations	These settings are wiped out and are not supported and cannot be manually configured in Unison.	Not supported in Unison.
Pre 5.8.0 to 5.9.0	Other non-supported GMS configurations	Any settings not explicitly appearing on the supported list are wiped out and cannot be manually configured in Unison. Refer to the help for the list of supported items.	Not supported in Unison.

Upgrade recommendations

Depending on controller configuration prior to upgrade and the functions set using GMS that are discarded from controller memory, then:

- Use GMS to view the settings for each schedule (area, egress, etc) that is used. Note the settings and the areas and doors they are applied to.
- For each controller, use GMS to save the Controller configuration as a template if, and only if the controller has settings, macros, etc that have been set using GMS.

  This step is a safety precaution so that a configuration record is available, if required.

> **Note:** The access card database is not retained as part of the template.

System Data Service

The Unison System Data Service (SDS) has been replaced by a different mechanism from v5.11.5 onwards and is no longer used.

Replication and Redundancy

Unison 5.4 and later, in conjunction with Microsoft SQL Server, provides tools for performing automatic Unison server and database failover / redundancy operations (without requiring proprietary Microsoft 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 server. Several servers can be set up for database replication, with the database in each one being constantly updated with the latest changes, events and other transactions.

This system incorporates deploying several servers in an active-active configuration 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 system are known as replication 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.

When using replicated 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 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.

Take note of ...

- Each database replication server must be installed as a replication server.
- Each replication server requires a licensed version of Microsoft SQL Server installed.

  It is not recommended to use SQL Server Express for replicated database servers or any large system.
- Each replication server must synchronize time at least once per hour with a network time protocol (NTP) server.

  > **Tip:** The time difference between replication servers should never exceed 2 seconds.

- Each replication server must have a unique global database ID assigned to it, which is the mechanism used for selecting the server to failover to.

  The primary server must have an ID of **1**.
- Network bandwidth between replication 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.

Microsoft SQL Server clustering and mirroring

Note: If Microsoft SQL Server database clustering is available, it can be used for redundancy / failover operations.
The redundancy architecture also provides failover / failback operation for 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 TCP/IP only 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.

  Database 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.

You can set up or upgrade an older Unison system to use database server replication.

> **Note:** Network bandwidth between database cluster servers should be a minimum of 100Mbit/sec (based on a typical system of 200 card readers and 1000 alarm points).
> For larger or busier systems, higher bandwidth availability will improve system performance.

How to

1. For upgrades:
   a. Make a backup of the Unison main and log databases from the current system being used.
2. Install the new version of Unison as a server on the primary server.

   Ensure that:
   - A licensed version of Microsoft SQL Server is installed.
   - The global database ID value is **1**.

   The global database ID value is the mechanism used for selecting the server to failover to.
3. Install the new version of Unison as a replication server on all required replication servers.

   Ensure that:
   - A licensed version of Microsoft SQL Server is installed.
   - Each replication server has a unique global database ID value (other than **1**).
4. Restore the previously backed up main and log databases from the primary server.
5. Set up an NTP server on the network and make all Unison server and client machines use it for time synchronization at least once per hour.

   The time difference between database cluster servers should never exceed 2 seconds.
6. Start Unison on the primary server, then:
   a. Create and configure the necessary database replication nodes - database server, Unison server, replication device and replication target, as required.
   b. Configure the driver server(s) for all driver that were available in the Unison database before the upgrade (this is not done automatically) and set up failover / failback as required for each.

> **Note:** DO NOT configure failback for replication nodes.
> DO configure failback for the system driver.

64-Bit Windows COM Ports

A problem with some device drivers has been identified when using 64-bit COM port RS232 communications that may cause the connected device to consistently crash and reboot. The following drivers are known to be affected, however, this may also apply to any device driver that use standard COM port RS232 communications:

- C2 (PacomIs.C2Device.exe)
- UC120 (PacomIs.UC120Device.exe)

How to

To bypass this problem, it is recommended to force the drivers to run in 32-bit mode:

1. Open a command prompt and navigate to the folder where the Unison drivers are installed.

   The default is `C:\Program Files\Pacom Systems\Unison\bin`

2. Enter "Corflags *DriverName* /32BIT+", where *DriverName* is the applicable device driver file.

   For example, "`Corflags PacomIs.C2Device.exe /32BIT+`".

> **Note:** If you use an RS232-to-TCP converter (for example., Moxa NPort or DIGI PortServer) in TCP Server Mode for COM port communication, the drivers do not need run in 32-bit mode.