You are here: Welcome

Unison 5.13.0

User Guide

Welcome to Unison 5.13.0 User Guide.

Document Version: 5.13.0.00 (March 2025)

You are here: Document Information

Document Information

Document version 5.13.0.00.

Created March 2025.

Pacom Unison version 5.13.0

Note: Some options, compliance claims or procedures described may not be supported if old versions of device firmware and/or software is used.

Note: This documentation is regularly changed and may have topics that are yet to be completed. Check the Pacom website [www.pacom.com] for updates.

Note, Caution and Warning Conventions

Note: Provides quick tips and information relevant to the procedure or concept presented.

Caution: Indicates information that if not adhered to may result in loss of data or damage to hardware.

Warning: Indicates information that if not adhered to may result in loss of data or damage to hardware, injury or loss of life.

Pacom Support

For product support, go to the Pacom support portal: support.pacom.com.

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.

Copyright Notices

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 terms stated below.

- 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 property of their respective owners. Pacom System 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 following trademarked software is used in the Unison system. For details, refer to the Unison Help.

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)

You are here: Introduction and Licensing

Introduction and Licensing

Pacom Unison integrates the following functionality:

- Access control.
- Intrusion detection.
- Video surveillance.
- Fire and building management.
- Communications and intercom.
- Duress and safety.
- Elevator control.

The user interface includes task related "ribbon bars" to enable the required functionality to be easily accessed.

This documentation contains a topic called "Getting Started". It includes basic operator administration functions as well as how to navigate the system, configure the workspace, and access common functionality. It is recommended to read this section before using the system. The remainder of the user documentation is organized in terms of functionality, for example, using transaction logs, configuring operators and operator groups etc.

License and Version Information

Each installation of Unison requires a license. This contains site information and any license conditions. If the license use has been exceeded, or if there is no valid license registered, Unison will work for 30 days only. Within this period, a valid license must be registered with adequate conditions or delete the portion of the database that exceeds the use. The number of days remaining of this period, can be found under license information.

In order to obtain a license you must contact a Pacom representative and quote the computer signature information shown in the Unison Service Manager and any other information that may be required. Pacom will then provide a license file (*.lic) that is uniquely tagged to your system - this file will not be compatible with any other system for security purposes.

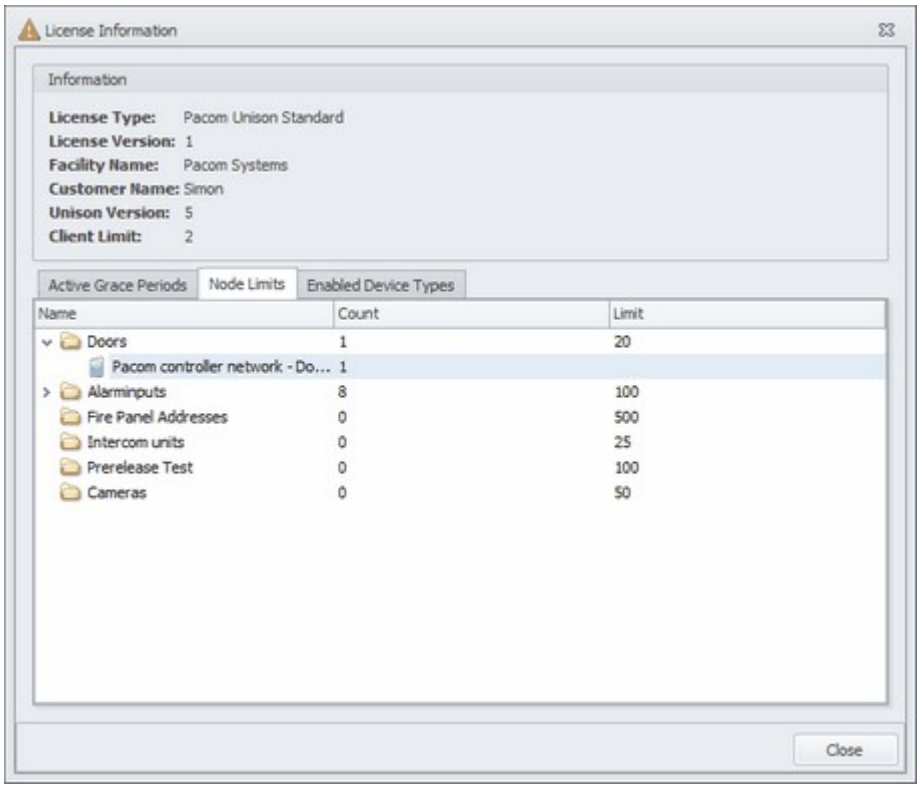
Once the license file is received, it must be loaded into the system for activation:

1. To access the license and version information, click . The About dialog box opens, displaying:

- Version - Software version number (required for technical support).
- This product is licensed to - Registered owner of product license.
- Build - Software compilation reference number (may be required for technical support).
- Framework - Software framework reference number (may be required for technical support).
- License Information - Opens the License Information dialog box.

License Information

1. Click License Info in the About dialog box. The License Information dialog box opens, displaying:



- License Type - Type of license in use.

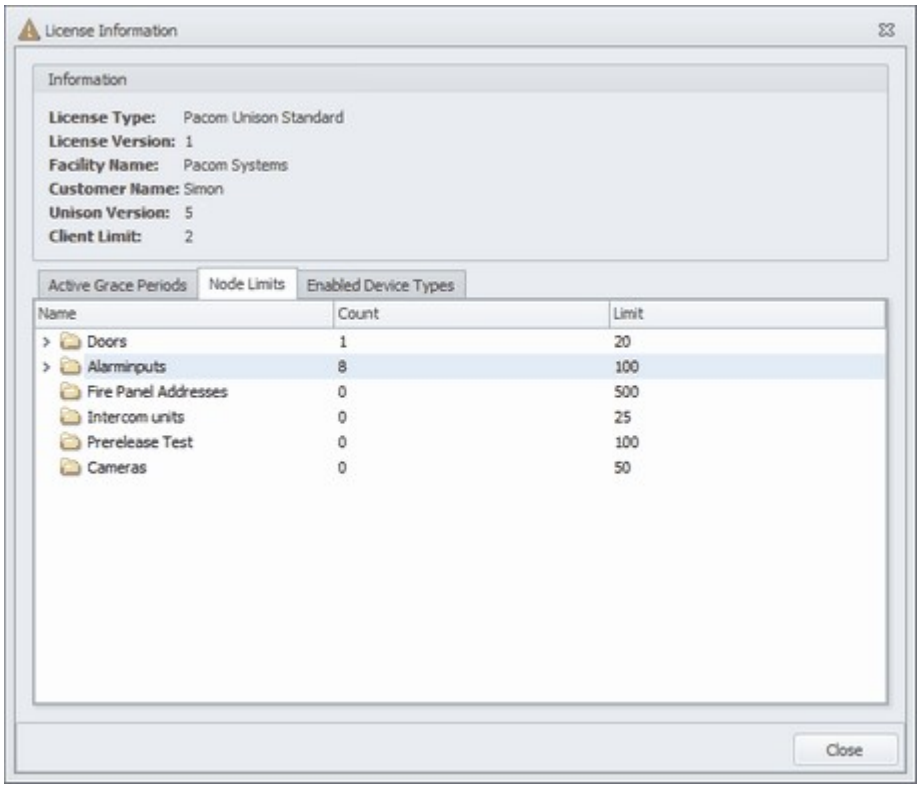
- License Version - Version number of license.
- Facility Name - Name of site which is licensed.
- Customer Name - Name of licensed customer.
- Unison Version - Software version the license covers.
- Client Limit - Maximum number of clients that can be connected at the same time.
- Active Grace Periods - Displays if "grace" periods are in use; that is, temporary use of currently unlicensed features. Lists nodes that are under a grace period and how many grace days remain for each.
- Node Limits - Maximum number of nodes that can be created.
- Enabled Device Types - List of licensed device types that can be connected.

Active Grace Periods

Displays if "grace" periods are in use; that is, temporary use of currently unlicensed features. Lists nodes that are under a grace period and how many grace days remain for each.

Node Limits

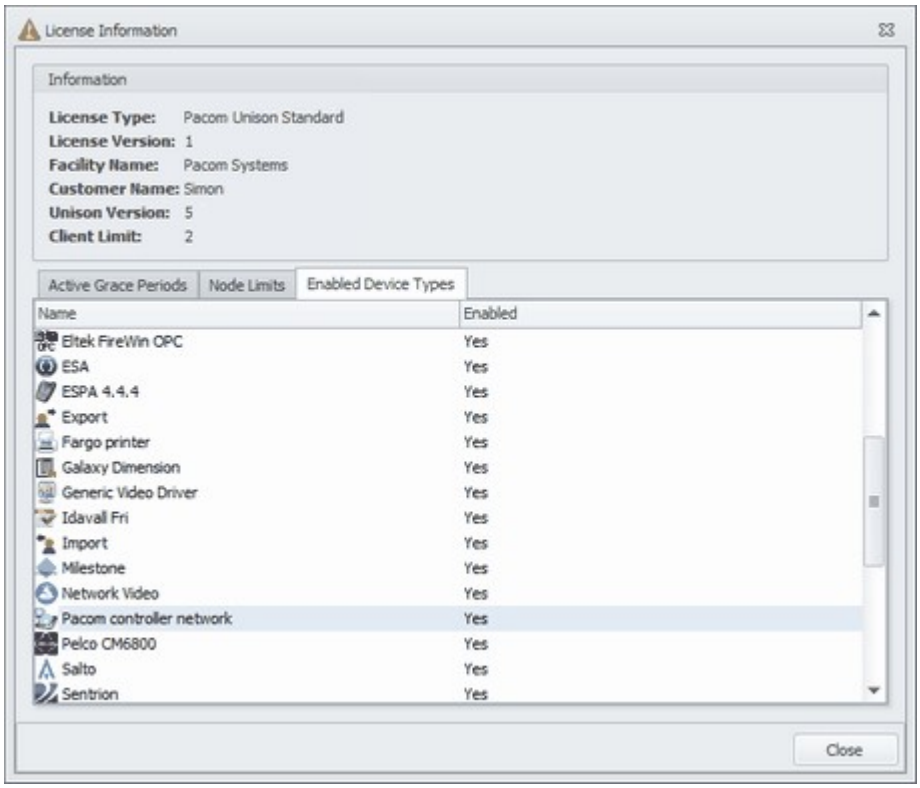
The license determines how many different types of nodes can be created. The information relates to:



- Name - The system device and node type. If the system contains folders for nodes, expand the folder to view nodes.
- Count - Current number of nodes created of this type.
- Limit - Maximum number of nodes the license permits.

Enabled Device Types

The license determines the device types that can be used. The information relates to:



- Name - Device type name.
- Enabled - Yes or No depending on whether or not the device type is licensed.

See Also: Getting Started | Using Unison Service Manager

You are here: Getting Started

Getting Started

The Pacom Unison security management application is designed for security operators and administrators to set up access control and alarm system monitoring and control at a site.

- Access control - Basically means the concept of having authorized users being able to access the premises at set/controlled times and in specific ways. For example, being able to access particular doors on certain days and between certain times. When a user attempts access outside of their allotted access privileges, they are denied access.
- Alarm system monitoring - Basically means to use the system for notifying operators [security personnel using Unison] of alarms, including alarm type and location. The system provides operators with options and functions for responding to alarms. Alarm monitoring is generally based around the concept of controlled access to the premises - if the premises is accessed at an unauthorized time, an alarm is generated. Similarly, the actual security equipment itself is also monitored for tampering, bypassing, hardware failure etc.
- Events - All "events" in the system are recorded in the system database so that an audit trail of system activity is always available. For example, every time a user access a door or an operator sends a command or an alarm occurs or an alarm is responded to. Transaction logs can be easily searched for required data.
- Nodes - All objects in the system, such as devices, card readers, door, users, schedules etc, are referred to as "nodes". All nodes are handled in a similar fashion throughout the system, which makes it less complex to use once the basic techniques for using nodes is understood.

The sub-topics include basic operator administration functions as well as how to navigate the system, configure the workspace, and access common functionality. It is recommended to read this section before using the system. The remainder of the user documentation is organized in terms of functionality, for example, using transaction logs, configuring operators and operator groups etc.

Basic Operator Procedures

Understanding the Workspace

Setting Up the Workspace

Nodes - Defintion and Use

Using Common Functions

Unison Deployment Guide

You are here: Getting Started > Basic Operator Procedures

Basic Operator Procedures

Before using Unison it is important to understand how to access the system and perform basic administrative tasks.

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 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.

- Logging On
- Locking/Unlocking
- Switching Operator
- Exiting
- Changing Operator Password

See Also: Configuring Roles, Operator Groups and Operators | Database and Device Driver Configuration and Management | Getting Started

---

You are here: Getting Started > Understanding the Workspace

Understanding the Workspace

The user interface is task orientated; for example, if card profiles need to be set up, all the necessary information is contained in the Card Profiles view. Each view or panel has a consistent appearance and functionality, making it easy to navigate around the system. This topic describes the main areas of the system, including:

- Common user interface components and terminology.
- Main screen.
- Main screen tabs.
- Panels.
- Views.

- Common User Interface Components and Terminology
- Main Screen Tabs and Panels
- Using Views

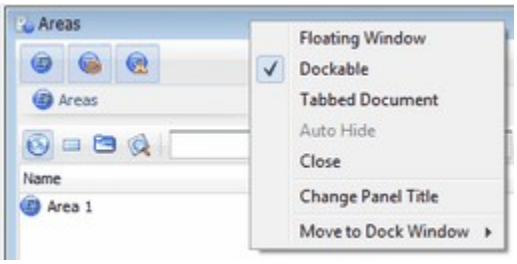
See Also: Configuring Roles, Operator Groups and Operators | Getting Started | Setting Up the Workspace

---

You are here: Getting Started > Setting Up the Workspace

Setting Up the Workspace

Most tasks are performed from the main screen workspace. Workspaces can be configured to display the most often used panels, for easier access. Panels can be docked within the workspace, added as separate windows, or placed as tabbed panels [multiple panels sharing the same workspace area] within the workspace. These settings can be saved when exiting the system so the following time the same user logs on, the same workspace configuration is displayed. Once a panel has been opened, right-click the title bar to display a list of options for workspace configuration.



- Panel and Ribbon Bar Actions
- Docking Windows
- Displaying Date and Time
- Saving Workspace Configuration

See Also: Understanding the Workspace | Getting Started

You are here: Getting Started > Nodes - Defintion and Use

Nodes - Definition and Use

Nodes are a basic object that represent physical items, such as connected pieces of hardware, and "virtual" objects, such as doors, door schedules, operator groups etc. Every object in the system is represented by a type of "node", which generally defines its functions and properties that determine system behavior.

Note: The "system" device contains basic nodes that the system requires. This node cannot be deleted. "Import" and "export" device nodes are virtual objects that are designed for importing/exporting hardware node information. "Test" device nodes are designed to allow simulation of hardware and other functions, such as automated conditions and resultant actions, without actually having the physical device or affecting the actual system. Management of device and node objects is identical, with some exceptions - any differences are noted in the relevant topic.

The system provides a "bulk update" facility that allows you to change certain properties for multiple nodes in a single operation.

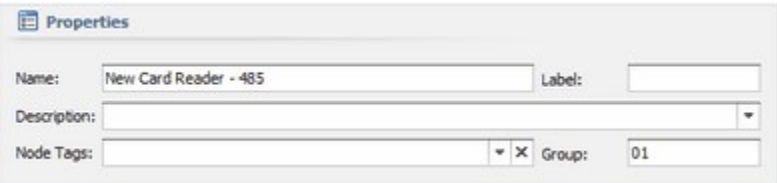
Device Nodes

Devices nodes represent physical hardware in the system. The device node usually corresponds to the applicable properties for managing communications and functions between the system and device, and may have "child" nodes that represent hardware or other functions under control of the device. For example, a Pcom Controller node that has child nodes for areas, card readers, doors etc.

A device has one or more "events" associated with it. Events basically represent a circumstance or occurence that has a value in terms of security, and these events can have a status of either "active" or "inactive". Events are associated with alarm types in order to generate alarms through status change; for example, a fire alarm generated by a smoke detector input that changes state to active. For most device types, nodes can be defined that correspond to hardware or other functionality that is supported by the device.

Node Organization Tools

The system provides a number of properties that are generic for most node types. These properties - "labels", "tags" and "groups" are used for organizing nodes so that they can be easily located in the system. The properties are available in the Properties tab of the applicable node view.



- Labels
- Tags
- Groups
- Folders
- Notes

See Also: Bulk Updating Node Properties | Creating and Commanding Nodes | Using Lists

---

You are here: Getting Started > Using Common Functions

Using Common Functions

There are many functions that are common to different types of nodes, such as using lists - columns, filtering, sorting, searching, selecting and right-click context menu.

- Columns, Sorting and Searching
- Filtering
- Using the Preview Dialog Box

See Also: Getting Started

You are here: Getting Started > Unison Deployment Guide

Unison Deployment Guide

There is a process that can be followed to set up the system for use. In most cases, one or more of each Unison "node"/"object" will be created or connected. For example, intruder and fire alarm inputs, camera system, intercom, access control system components or any other type of sub-system to the Unison system.

Note: When configuring sites, it is usually not required to go through all deployment steps, as most installations have individual or limited requirements. The process below is a guide for deployment of a full system.

For a general approach summary to deploying alarm monitoring and access control functionality using the Unison system, see below.

Alarm Queues 	Create required alarm queues. Alarm queues represent alarms of different types and how they are presented to operators. Alarm queues provide an overview of alarm status, are used to respond to alarms and are easily filtered. For example, fire alarms may have a different queue to intrusion alarms etc. A number of pre-defined alarm queues exist - these can be copied or modified as required [see here]. If required, customize the appearance of the Alarm Queues panel [see here].

Alarm Configuration

Alarm Types 

Create required alarm types. Alarm types represent groupings of similar alarms that can be used for multiple node events, and different nodes within the system, and define the alarm queue that they are represented in. For example, fire, intrusion etc. Alarm types provide common properties that should apply for a group of alarm events, including how operators must respond to alarms, such as through manual tasks and/or automated system response, and response priority (urgency). A number of pre-defined alarm types exist - these can be copied or modified as required [see here]. Configure alarm type behavior and associate them with alarm queues [see here].

Alarm Lists 

Alarm lists are how current alarms and alarm status are presented to operators for response [when not using graphics]. Different highlight colors and list ordering is available to make alarm response tasks simpler. If required, customize the appearance of the Alarm List panel so that alarm status is easily visible - text and background colors etc [see here].

Device Hardware Nodes and Templates  

Create required device nodes. Device nodes represent physical pieces of hardware that are part of the security system and, therefore, are used to send event information to the Unison system for processing and may also, in turn, be under some form of control via the Unison system. The device node usually corresponds to the device driver software [sometimes referred to as "protocol"], which defines communications with the device and its supported events an functions. Devices often have "child" nodes that represent the physical hardware and ancillaries, such as control panels, detectors, card readers, door controllers etc. A device has one or more events associated with it - these events [generally] have a status of "active" or "inactive" that are used for alarm notification. For most device types, nodes can be defined that correspond to attached hardware or other

functionality that is handled by the device [see here].

Device templates are built into the system to provide "standard" configuration that determines events and system behavior for supported devices. These are generally adequate for many installations [see here]. Standard device templates cannot be changed as they are a "system reference" for a device driver, however, you can create copies of standard templates and customize those; for example, to change event behavior etc.

Device/Hardware Configuration

Device Child Nodes

Create required device "child" nodes. Device child nodes usually represent device ancillary hardware and conceptual nodes associated with the device. For example, a Pacom Controller device is likely to have child nodes for doors, card readers, areas etc. There are two ways to define hardware in Unison:

- Scan the connected hardware and automatically create Unison objects for them. Each device node is configured according to its selected device template [see here].
- Manually create nodes for each piece of hardware. Each device object is configured according to its selected device template, however, nodes must be created individually [see here].

Alarm Events

Configure device events that will be treated as alarms, if required or if different behavior to that supplied in the device template is required. Events are associated with alarm types in order to generate alarms through status change; for example, a fire alarm generated by a smoke detector input [state change to active]. Custom event configuration is required only in cases where it is necessary to not follow the device template configuration [see here].

Configure device event "alarm actions", as required. Alarm actions represent commands that, in response to an alarm event, are either

Alarm Event Actions	performed automatically by the system or manually by an operator. For example, to open a door for access, activate an output, activate camera recording or connect an intercom call etc. Actions that apply to alarm events of the same type should be configured by "alarm type" [see here]; that is, the alarm type determines alarm actions. Actions that are specific to one or more alarm events are configured by "node" [see here].
Programming Actions	Configure device event "programming actions", as required. Programming actions represent command actions/tasks performed automatically by the system in connection with an event status change from a device/node. Unlike alarm actions, programmed actions are performed regardless of whether or not the triggering event involves an alarm event. In other words, these actions are not reliant on alarms [see here]. Note: For each hardware device type, there are specific properties available/supported - refer to specific device driver topics for information [see here].
Day Types and Calendars	Configure system "day types", as required. Day types represent access control system operation that is different to normal [see here]. For example, settings to apply on public holidays, half days or during stock-take etc. Configure system "calendars", as required. Calendars are a node type that associates day types and dates [see here].
Door Schedules	Configure "door schedules", as required. Door schedules control the level of security at a door; for example, if it is locked/unlocked, requires access card or PIN verification for entry etc. The security level is time-based over the 24 hours per day and can be applied to all day types and calendars [see here]. Door schedules are applied to doors.

Access Control Configuration

Access Schedules

Configure "access schedules", as required. Access schedules define the times of day and days of the week when users are able to use access control nodes (doors, areas etc). For example, there may be access schedules applicable to technicians, day shift staff, night shift staff etc. Access permission is time-based over the 24 hours per day and can be applied to all day types and calendars [see here]. Access schedules are applied to access groups and directly to users as "personal access" permissions.

Access Groups

Configure "access groups", as required. Access groups are collections of access schedules that define when users have access to doors and areas, and can be applied to multiple users. That is, an access group can be set up to include common doors, areas and associated access schedules that determine when users can enter/exit [see here].

Users

Create "users", as required. Users are authorized and identified persons that are allowed access to the premises, commonly by electronic access card [see here]. Users are assigned access groups and personal access [non-access group based] that determine when, where and how they are capable of accessing the premises [see here].

Site Map Configuration

Site Maps

Create "site map" graphics, as required. Site map graphics are commonly used for providing a visual representation to operators for alarm monitoring and response and access control that provides visual notifications and easily understandable location information etc. Site maps generally contain site floor plan and usually show alarm points, doors etc. Site maps can be generated through importation of CAD drawings [see here] - supported file formats only, or can be created manually [see here].

Configure graphic-node "connections", as required. Graphic-node connections represent interactions between site map graphics and

	Node-Graphic Connections	actual nodes in the system [see here]. When connected, the status of nodes [in alarm etc] is displayed in graphics and provides operators with a "real-time" [automatically updates according to connection status] display for managing and responding to alarms, directly from site maps.
	Roles	Create "roles", as required. Roles are display configurations so that each time an operator logs on to the system or selects a different role when logged on, a pre-defined, fixed [or custom] display can be applied. The idea behind this is to make using the system simpler and more consistent. For example, when setting up an operator group for personnel that will be performing alarm monitoring and response duties, it would be useful to create a suitable role that provides the necessary tools on screen for those operators to easily perform their required task [see here]. Operators can load different roles to immediately apply a workspace suited to the required tasks.
Operator Configuration	Operator Groups	Configure "operator groups", as required. Operator groups define permissions [parts and functionality of the system that operators have] and determine how operators may interact with the system, for example available views, functions, roles etc [see here].
	Operators	Configure Unison "operators", as required. Operators are persons that interact with the system for alarm monitoring and response, access control management, system administration functions etc. Operators have credentials - names and passwords - that the system requires in order to authenticate themselves uniquely to the system and allow them access to it. Operators must be associated with one or more operator groups [see here].

See Also: Configuring Roles, Operator Groups and Operators | Creating and Commanding Nodes | Device Nodes and Drivers | Managing Access Control and Users | Managing Alarms | Users and Access Cards | Using Site Map Graphics

You are here: System Management

System Management

The Unison security management application provides a number of tools for managing and maintaining the system.

- System Node - The "System" node is used for system configuration and "global" node configuration. Many global node types, such as alarm queues and access schedules, can be configured through specific views, however, all are "saved" as child nodes in a tree of sub-folders to the System node.
- Database and Device Driver Management - Managing system servers that define where device drivers run and managing the system databases, including backup functions and using multiple clustered database servers.
- Roles, Operator Groups and Operators - Operators are persons that interact with the system for alarm monitoring and response, access control management, system administration functions etc. Operators must be associated with one or more operator groups, which define permissions [parts and functionality of the system that operators have] and determine how they may interact with the system. Operator groups are also used to determine which graphics, if any, are pre-loaded to the Unison client when an operator logs on. Roles are display configurations so that each time an operator logs on to the system or selects a different role when logged on, a pre-defined, fixed [or custom] display can be applied.
- Functions Drivers - The system applies the concept of "drivers", which are modules within the application that perform specific functions, to several internal features of the system itself.
- Partitions - All "events" in the system are recorded in the system database so that an audit trail of system activity is always available. For example, every time a user access a door or an operator sends a command or an alarm occurs or an alarm is responded to. Transaction logs can be easily searched for required data.
- Task Schedules - A "generic" node that may be used in expressions, restrictions and other types of functions where automated functionality that is controlled by day type and time of day is required.
- Unison Service Manager - A utility driven by the Unison Windows service for controlling device drivers and provides access to various server configuration tools.

Configuring the System

Configuring Roles, Operator Groups and Operators

Managing Clients

Unison Function Drivers

Using Partitions

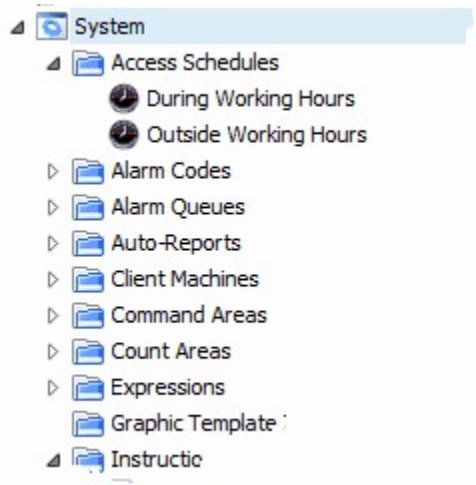
Using Task Schedules

Using Unison Service Manager

Configuring the System

The Unison "System" node is used for system configuration and "global" node configuration. Many global node types, such as alarm queues and access schedules, can be configured through specific views, however, all are "saved" as child nodes in a tree of sub-folders to the system node. The following image is an example of the system device and child node sub-folders.

Note: The system node always exists [it is created automatically] and cannot be removed.



Several other system level settings are available in the System node. These include alarm display, user data fields etc. To access system node settings, click  (Hardware) in the System Configuration ribbon bar to open the view, then click System to display settings in the Properties section.

- System Node - Events and Commands
- Advanced Setup - Configuration
- Alarm - Configuration
- Authentication - Configuration
- Graphics - Configuration
- Keyboard Shortcuts - Configuration
- User - Configuration

See Also: Database and Device Driver Configuration and Management | System Preventative Maintenance Checklist | Using Partitions

Database and Device Driver Configuration and Management

System Preventative Maintenance Advice

You are here: System Management > Configuring the System > Database and Device Driver Configuration and Management

Database and Device Driver Configuration and Management

All data/information in the Unison system is stored in SQL databases. The currently active database is known as the "main" or "primary", and maintains records of all system activity [that is, configuration settings, events, responses, commands, access control etc]. At a pre-determined time, the main database is copied to a "log" database, with the main database being subsequently purged [emptied] of certain data. This is to ensure that system performance is maintained by not allowing the main database to become excessively large, and "load balances" database requirements by splitting records into two databases.

The main and log databases are always available for searching through transaction log views; for example, the All Transactions Log view. Log database archiving is also available for similar database management reasons stated previously. When archived, at a pre-determined time, the log database is copied to an "archive" database, with the log database being subsequently purged [emptied]. Archived databases can be automatically "mounted", which means they are also accessible in transaction log views, however, must be specifically selected. If a log database is not mounted, it will require manual mounting via SQL so it becomes selectable in the Unison system.

- Automatic - The system is set to automatically create backup databases at regular intervals without operator intervention.
- Manual - Backups are created as required by an operator, on demand, issuing a command in the Unison system.

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.

The system supports limiting the overall size of Unison databases ["main", "log" and "archive"], if required. These settings can be used to ensure that hard disk space is never filled completely with event/transaction data. If the limit is reached, the oldest entry is removed from the archive database to make space for the newest entry in the main database. If this continues to the point of the archive database becoming empty [that is, its space is now being used by the main database], then the oldest entry is removed from the log database to make space for the newest entry in the main database. If this continues to the point of the log database becoming empty [that is, its

space is now being used by the main database], then the oldest entry in the main database is removed to make space for the newest entry. If these scenarios eventuate it may indicate that the setting is too low or that database archiving to another storage facility is required. This feature is set via the "System" node.

- Server Clustering Operation Overview
- Device Driver Overview
- Database Server - Management, Configuration and Commands
- Unison [Device] Server - Management, Configuration and Commands
- Replication Target - Management, Configuration and Commands
- Database Management Tools
- Monitoring Server Availability

See Also: Database Replication Driver | Configuring the System | Using Unison Service Manager

---

System Preventative Maintenance Advice

The following recommendations may be used to help verify correct operation of various parts of the Unison system in terms of system databases, database replication [if used], device driver operation and some general configuration requirements. This is provided as a guide only and no recommendation for when and if these checks be made are provided. Each Unison installation and how the system is used, its complexity etc will determine appropriate actions to take, if any.

Databases

- Check available disk space where Unison databases are stored. If available storage space is becoming low take steps to increase it, such as removing data that is no longer required [for example, moving it to another storage facility or deleting], applying the "shrink" command, increasing available storage or archiving etc. Database activities should be performed by an appropriately trained SQL administrator or similar. To check the current size of Unison databases from within Unison, refer to the "database settings" properties in the Unison "System" node.
- Ensure that automated database backups are being created according to schedule, as configured in the "database main server" node.
- Perform a manual database backup and verify that it is created properly. Restore the backed-up database on a separate computer that has Unison installed on it, using the Unison Server wizard, and perform several "spot-checks" against the actual Unison database to ensure that data is being backed-up correctly. In order to access the databases on the separate Unison system, ensure that the SQL Server connection string is correct for the "database main server" node.

- If database replication is in use, temporarily "disconnect" a "database replication server" then makes some changes in the "main server" [for example, creating a "test" node]. Reconnect the replication server and check that the changes made in the main server are visible in the database replication server.

Device Drivers

In general, the following, or similar, tests can be performed on several device drivers used to help verify correct operation. For each device that is being used for "testing, activate "full debug logging" for it [properties for the device node] and open the Unison Debug Monitor application. Use the Unison Debug Monitor display and check that commands are being sent by the system and performed correctly - any errors are displayed in red text - these should noted and rectified.

- Disarm and arm at least one child node of the device [for example, motion detector, area etc] - ensure that the status for the node updates correctly.
- Activate an alarm of some kind and respond to it [acknowledge, reset, close etc] - ensure that the alarm is received in the system and the alarm status updates according to response actions.
- Disarm an alarm input node [for example, a motion detector] and activate an alarm for it - ensure that the alarm is not received into the system. Arm the input node and activate an alarm for it - ensure that the alarm is received into the system.
- For communications devices that may support making and receiving "calls" in the Unison system [for example, some intercom systems], make a call from the third-party system to Unison and answer it - ensure that the call is answered correctly. Make a call from Unison to the third-party system - ensure it is received correctly.

General

- Open a transaction log, perform a search of some kind [that actually does provide some results] and print a report - ensure that the searched for data is included in the report.
- Check for any "blocked"/"disarmed" nodes [for example, alarm inputs] - ensure that all blocked/disarmed nodes that may be listed, should be.
- Check the list of "armed" and "disarmed" area nodes, if applicable - ensure that the alarm system mode for each area is correct.
- Check that all "day types" for schedules [for example, area schedules, door schedules etc] are configured correctly.
- Check that calendars include all "special" days [public holidays etc] and that the correct schedules are applied to them.

See Also: Configuring the System | System Management

You are here: System Management > Configuring Roles, Operator Groups and Operators

Configuring Roles, Operator Groups and Operators

Operators are persons that interact with the system for alarm monitoring and response, access control management, system administration functions etc. Operators have credentials - names and passwords - that the system requires in order to authenticate themselves uniquely to the system and allow them access to it. Operators must be associated with one or more operator groups, which define permissions [parts and functionality of the system that operators have] and determine how they may interact with the system, for example available views, functions, preloaded graphics, roles etc. Some examples of functionality that can be set up for operator groups may be:

- Alarm Operators - Able to acknowledge and respond to alarms; search the alarm logs.
- Access Control Administrators - Able to create and edit users (access card holders).
- System Engineers - Able to access main system functions and configuration, however, may not be able to create or change operators or operator groups.
- System Administrators - Able to access all aspects of the system.

Roles are display configurations so that each time an operator logs on to the system or selects a different role when logged on, a pre-defined, fixed [or custom] display can be applied. The idea behind this is to make using the system simpler and more consistent. For example, when setting up an operator group for personnel that will be performing alarm monitoring and response duties, it would be useful to create a suitable role that provides the necessary tools on screen for those operators to easily perform their required task.

Operator Authentication

Unison supports 3 modes of authentication. When creating and configuring operators, you can map an Active Directory user to an Unison operator.

- Operator Group Management and Configuration
- Operator Management and Configuration
- "Elevated" Permission Control
- Role Management and Configuration

See Also: Configuring the System | Operator Group Permissions | Using Partitions | Setting Up the Workspace | Using Alarm Management Tools

Setting Operator Group Permissions

Configuring Role Settings

Area of Responsibility

You are here: System Management > Configuring Roles, Operator Groups and

Operators > Setting Operator Group Permissions

Setting Operator Group Permissions

Permissions are defined at the operator group level and determine the features and functions available to associated operators - ability to view and to activate functions etc. Permissions enable administrators to completely customize how the system can be interacted with based on roles.

Most objects in the system are defined as nodes; for example, devices, input and outputs, areas, access schedules etc. Nodes can be managed in a number of views and panels, which means that the permission settings can become quite complex. For example, nodes can be displayed in the Nodes panel, Hardware view, Nodes view or in any filtered views that are available for certain node types. The principle of permissions is that separate access settings can be defined for each view. This means that an operator group may not be able to work with a certain type of node in one view, however, may still have access to the same node type from another view.

For example, if an operator group does not have permissions for the Hardware or Nodes views, however, does have permission for the Card Readers view, then associated operators can work on card reader nodes, as (only) nodes of this type are displayed in the Card Reader view. Similarly, if the operator group has permissions for the Hardware or Nodes views, then associated operators can work with card reader nodes, as these views displays nodes of all types.

The items an operator group has permissions for, and the available functions, in different panels is also controlled. For example, being able to view a panel and if allowed to view or access management tools (edit, create etc).

Node panels can be opened with a number of pre-defined filters. The available filters to an operator group is determined by whether or not it has permissions for the corresponding view in the Explorer. For example, if the operator group does not have permissions for the Card Readers view, then card reader filtering will be unavailable as viewing of card readers is unavailable.

Note: If an operator group has permissions for the Nodes view in the Explorer and also to the panel for a node, then operators can open the Node panel using the node as a filter.

See Also: Configuring Roles, Operator Groups and Operators | Using Partitions

You are here: System Management > Configuring Roles, Operator Groups and Operators > Configuring Role Settings

Configuring Role Settings

Global settings for roles can be configured which then apply to all user roles in the system.

- How to set general role functions
- How to set general alarm alert notifications
- How to set general panel features
- How to set what information is displayed in the Alarm Management dialog box

See Also:Configuring Roles, Operator Groups and Operators | Using Partitions

You are here: System Management > Configuring Roles, Operator Groups and Operators > Area of Responsibility

Area of Responsibility

Area of Responsibility enables you to filter alarm lists and graphics based on operators responsibility of specific areas.

Note: It is recommended that you either use Client Sessions or Area of Responsibility, not both.

Set up the operator permissions for the appropriate operator group in the Operator Permissions tab > Panels > Area of Responsibility Sessions.

To set up areas for operators to be responsible for:

1. Make sure that area of responsibility is enabled in System > Advanced Setup.
2. Go to System Administration > Areas of Responsibility.
3. In the Areas of Responsibility view, click Create on the toolbar.
4. Enter the Name of the new area of responsibility and other property details on the Properties tab, Properties section.
5. In the Settings section:

   Select whether you wish to use the default failover where all available operator are able to take over an area to operators who are currently logged on, or manually select specific failover conditions that must be met by an operator

group. Choose 3 failover options which must be met, if any of these are not successful then the default option is chosen.

Tick the Force Monitor checkbox if you wish operators to be forced to monitor alarms and not log off or switch operators until the alarms are actioned. If an area of responsibility is set to force monitor, and if it is unmonitored, a notification is displayed on log off/switch operator or locked.

Tick the Include as a Catch-All checkbox if you wish include a series of conditions that a node must match to be included in the catch-all. It is possible to have more that more catch-all. The catch-all will not hide nodes that are explicitly defined in its conditions, even if they overlap with other area of responsibilities configured in the system. When an area of responsibility is marked as catch all, and a node matches no conditions, this node is displayed in the catch all.

6. In the Conditions section, add expressions to define this area of responsibility.

   These additional expressions are only available to areas of responsibility:

   - Add Node Filter
   - Add Alarm Type
   - Add Alarm State.

   The node filters must be set up and enabled by your administrator in the System > Advanced Settings tab > Area of Responsibility Settings.

7. In the Events tab, there is the additional event for area of responsibility - Unmonitored.

8. Click Save.
9. Once you set up Area of Responsibility, you must restart the Unison client for the changes to take effect.

- How to use the Area of Responsibility Sessions panel
- When issues arise ...

Managing Clients

The Unison system supports the ability to manage Unison client application in terms of being able to track and remotely "block" them. That is, an operator with sufficient permissions is able to send a "block" command to another Unison client. If another operator is using the client at the time, they are logged off automatically and the client is shut down. No operator is able to log on and run the Unison client on that machine

until the client is sent the "unblock" command. This function is an additional security mechanism that is provided to prevent unauthorized use of the system through an active Unison client application.

Caution: If a single Unison client only is available, or if all clients are "blocked", there is no way of again logging into the Unison system. If this occurs, contact Pacom support.

Client machines "ping" the system database at regular intervals, which is how the system determines whether or not the client machine is online [when a ping is sent, an acknowledgment of it is returned, acting as a "heartbeat"]. Each Unison client machine can be classified as "node", which means that they can be used to generate events and to accept commands from the Unison system. For example, to generate an alarm if a computer becomes unavailable, or to send commands to a client to "block" it from interacting with the rest of the system.

Note: Settings for how long the system allows to elapse before considering a client machine to be unavailable are set in the "System" node. • All client computers must be in the same domain as the Unison server.

When the system is set up, a client machine node is automatically created to represent for the Unison client application that is installed with applicable Unison server installations - this is the "default client". That is, if there is a single server, there is a single "default client"; if there are multiple servers, there is still a single "default client", however, commands to it would apply to the client available on each server. Client machines that are used by operators, which are generally not Unison servers, must be added to the client machine list manually.

- Management, Configuration and Commands
- Commands

See Also: Setting Operator Group Permissions

Unison Function Drivers

The Unison system applies the concept of "drivers", which are modules within the application that perform specific functions, including a "web" based data transfer interface for integrating user data with third-party systems, to several internal features of the system itself. This means that the configuration for such features is similar to that for external devices. Drivers include:

- Access Service - HTTP "web" based data trnasfer mechanism for communicating user data between the Unison and third-party systems. For example, receiving user data from a third-party system and, in response, providing access card data and access permissions that are used for encoding access cards which are issued to users.
- Alarm Text - Message decoding service that "reads" messages sent by external hardware. If applicable text is found in messages, alarms nor other events can be configured to be generated in the Unison system as a result.
- Database Replication - A form of Unison system device that is required for "clustering" database servers. That is, a component for Unison installations that utilize several databases for redundancy purposes.
- Export - User data export service. For example, exporting user data from the Unison database into a third-party personnel management system.
- Import - User data import service. For example, importing user data from a third-party personnel management system into the Unison database.
- SMS - Text message service for sending alarm notifications to individuals via their mobile/cell telephone or compatible device in the event of an alarm or other configured event.
- SNMP - "Sniffer" service primarily used by technicians for fault finding external hardware or certain Windows system events that are communicated within the operating system as SNMP "traps" or "WMI" events.
- Test Device - In-built utiltiy that allows "virtual" nodes to be created. These are primarily for simulations etc, where node event activations are fully controlled from within the Unison system.
- WCF Service - HTTP "web" based data trnasfer mechanism for communicating alarm or other events between the Unison and third-party systems. For example, sending alarm event data to a third-party system.
- WCU - A "common alarm protocol" ["CAP"] communications service for alarm message transfer to compatible systems or devices.

See Also: Access Data Service | Alarm Text | Database Replication | Export | Import | SMS | SNMP | Test Device | WCF Service | WCU

Access Service

Alarm Text

Database Replication

Export

Import

SMS

SNMP

Test Device

WCF Service

WCU

You are here: System Management > Unison Function Drivers > Access Service

Access Service

The access service is a generic device driver that handles synchronization of users and access cards with compatible systems as a standard HTTP or HTTPS "web" service. This allows user data to be read from the Unison system by a third-party and, similarly, for third-party systems to provide user information to the Unison system. For example, the Adria Scan visitor management system. The systems connect over a network Ethernet connection.

Note: For detailed protocol and integration information, contact Pacom.

- Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Nodes - Definition and Use

---

You are here: System Management > Unison Function Drivers > Alarm Text

Alarm Text

The alarm text device driver is used to communicate with external hardware that can generate alarms. Alarm nodes are used to read non-encrypted incoming text data from the device and create events if specific text strings are found in it. For example, creating an alarm if the text "alarm" is found.

- Device - Management, Configuration and Commands
- Alarm Node - Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Nodes - Definition and Use

---

You are here: System Management > Unison Function Drivers > Database Replication

Database Replication

Database replication driver nodes are a form of Unison system device that is required for clustering database servers. These "devices" provide the necessary system functionality for replicating databases amongst servers in the cluster. For each database server in the cluster, corresponding "database cluster" nodes are required in the Unison system. These nodes determine where data is replicated amongst database servers, and must exist as child nodes to a Unison database replication device.

Note: The function is available for "Enterprise" versions only.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Database and Device Driver Configuration and Management | Nodes - Definition and Use

---

You are here: System Management > Unison Function Drivers > Export

Export

The export device driver is used for exporting user and access card information. This information can then be imported into another Unison system using the "Unison import device". As a guide, to export user data from one system and import it to another:

1. Create an "Unison export" node on the system to be exported, then send a command to the node to perform the export. The resulting exported data is stored in one or more files.
2. Copy the files or otherwise save them in a location that is accessible to the system that will import them.
3. Create an "Unison import" node on the system to import to that targets the location where the exported files are saved. Send a command to the import node to perform the import.

When export files are created, the naming of them changes depending on:

- If the export is using the "Export All" command, the file is named "FullExport_[date]_[sequence].*". For example, if a full export was carried out for the third time [the "sequence"] on August 24, 2014, the file name is "FullExport_20140824_0003.*".
- If the export is using the "Export" command, the file is named "Export_[date]_[sequence].*". For example, if an export was carried out for the second time [the "sequence"] on January 31, 2014, the file name is "Export_20140131_0002.*".

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Import | Nodes - Definition and Use

---

You are here: System Management > Unison Function Drivers > Import

Import

The import device driver is used for importing user and access card information that has been exported from another Unison system. As a guide, to export user data from one system and import it to another:

1. Create a "Unison export" node on the system to be exported. Set the "device" up to export the required data, then send a command to the node to perform the export. The resulting exported data is stored in one or more files.
2. Copy the files or otherwise save them in a location that is accessible to the system that will import them.
3. Create a "Unison import" node on the system to import to. Set the "device" up to import the required data and functionality and target the location where the exported files are saved. Send a command to the import node to perform the import.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Export | Nodes - Definition and Use

---

You are here: System Management > Unison Function Drivers > SMS

SMS

The SMS device driver enables the system to sends SMS "text" messages to pre-defined contacts via a compatible modem in the event of an alarm. The message format is configurable so that the system automatically creates the content based on event information. Sub-folders to the device node are used for storing member nodes of the SMS system - these are automatically created. The sub-folders are:

- Contact Groups - Groups of SMS contacts to be sent messages simultaneously.
- Contacts - SMS contact nodes, which are mobile/cell telephone information.

Note: Compatible modems are Multitech Systems MTCBA-G2-U GPRS. • If the connected modem uses serial communications and is connected to the system via

Moxa NPort serial-to-IP conversion software, the NPort configuration must have a value of "0" for "delimiter" and "force transit" settings. • If the modem [connected via USB] is unplugged, it is recommended to wait at least five seconds before reconnecting, otherwise an error may occur.

- Device - Management, Configuration and Commands
- Contact - Management, Configuration and Commands
- Contact Group - Management, Configuration and Commands
- Programming Example

See Also: Managing Alarms | Nodes - Definition and Use

You are here: System Management > Unison Function Drivers > SNMP

SNMP

Note: SNMP functionality is primarily for technician use.

The SNMP device driver is capable of receiving SNMP "traps", which are primarily events from hardware devices - these can be used for fault finding or test purposes. 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 if data has been written to the Windows registry etc. The computer that will run 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).

Note: Setting up WMI queries on remote computers is not recommended as different operating system and COM settings may present reliability issues. For detailed information on the above requirements, refer to Windows documentation.

SNMP trap nodes listen for and capture SNMP "trap" events.

Query nodes listen for and capture Windows WMI events.

Note: See http://msdn.microsoft.com/en-us/library/aa384642%28v=VS.85%29.aspx for more information on WMI.

"Ping" nodes (packet Internet network groper) test connections between the system and IP connected devices against a set of acceptable limits. This can be used to determine the "health" of a connection and also to help identify possible connectivity problems. Any device on an IP network can be pinged; for example, an alarm panel device, IP camera, printer etc. If a device is not responding to being pinged, or is

responding outside of acceptable limits, an event is generated and an alarm can be triggered.

Note: The ping function is an additional tool that can be used for fine tuning network connectivity settings, and is recommended for use in troubleshooting where fluctuations or faults in device connectivity are being experienced. For any connected device, if the device is unavailable ("offline") when the system attempts communication, an event is generated. • For alarm events that are generated as a result of device ping settings, messages are shown in the Alarm Management dialog box, Message field that describe the failure. That is, if the ping failed due to timing out or as a result of too many "hops" required to reach the intended destination.

- Device - Management, Configuration and Commands
- SNMP Trap - Management, Configuration and Commands
- WMI Query - Management, Configuration and Commands
- Ping - Management, Configuration and Commands
- Programming Example

See Also: Creating and Commanding Nodes | Nodes - Definition and Use

---

You are here: System Management > Unison Function Drivers > Test Device

Test Device

The Unison system provides a "test" tool that allows creating "virtual" devices and nodes. These nodes can be used to simulate alarms and access control functions, and allow experimental configurations, generating events, testing expressions etc. Test devices support the following sub-folders and child nodes:

- Card Reader - Sub-folder for containing card reader test nodes.
- Door - Sub-folder for containing door test nodes. The nodes support normal door commands.
- Test - Test nodes. The nodes support several commands and can also have "child" test nodes.

Note: The range of functions that can be simulated by test devices may be limited compared to actual hardware and functions.

- Device - Management, Configuration and Commands
- Card Reader Test Node - Management, Configuration and Commands
- Door Test Node - Management, Configuration and Commands
- Test Node - Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Nodes - Definition and Use

WCF Service

A generic open interface "web" service that can be used to access alarms or other events from the Unison system. Similarly, nodes in the Unison system can also be controlled via the WCF service. This means the WCF service is basically an interface for integrating to 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. Whenever the Unison database is changed [for example, users added etc], the WCF service notifies the third-party system to synchronize its database.

Note: The function is available for "Enterprise" versions only.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Nodes - Definition and Use

WCU

The WCU device driver enables the system to integrate with "common alarm protocol" (CAP) compatible devices. In the Unison system, the CAP protocol, which is basically alarm messaging, is enhanced to allow commands to be sent from the Unison system by way of an additional common command protocol (CCP).

Note: The function is available for "Enterprise" versions only.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Nodes - Definition and Use

Using Partitions

Partitions are a way of segmenting aspects of the system to operators, by way of operator group permissions. The idea behind partitions is to "filter" or "channel" aspects of system operation to operator groups; for example:

- Allow specific operators to see specific events, such as alarms or events of a particular type. For example, specifying an alarm type to a partition so that operators with permissions to the partition are presented with alarms of that type; such as intrusion alarms, fire alarms etc.
- Segment parts of an installation so that each partition can be presented as a separate function. For example, specifying a node type to a partition so that operators with permissions to the partition are presented with events, properties etc specifically to nodes of that type; such as doors, elevators etc.
- Segment parts of an installation so that each partition can be presented as a separate site. For example, specifying nodes [devices, doors, areas etc] that are associated by location to a partition so that operators with permissions to the partition are presented with events etc specifically to that site.

Technically, partitions represent portions or segments of the system databases that are used to limit access to node related information, such as transaction information, events etc. That is, if a node is associated with a particular partition, only operators with permissions for that partition are able to view, edit etc. Partitions are created in the Partitions view. The process of partitioning can be summarized as follows:

Partition Configuration	Create Partitions	Create partitions as required. For example, for different clients in a building etc.
	⬇	
	Assign Partitions to Nodes	For each applicable node/object, assign the required partition to it. For example, users, doors, areas etc.
	⬇	
Operator Group Configuration	Create Operator Groups	Create operator groups as required. For example, a group for each partition - operators associated with a group will automatically be restricted to nodes within the associated partition.
	⬇	
	Assign Partitions to Operator Group Permissions	Assign permissions to operator groups as required. Permissions determine which parts of the application and available functions that associated operators can access.
	⬇	
Operator Configuration	Create Operators and Assign to Operator Groups	Create and assign operators to the required operator groups.

- Management, Configuration and Commands
- Assigning Partitions to Nodes/Objects and Operator Groups
- Partition Control and Client Computer Connection Status

See Also: Configuring Roles, Operator Groups and Operators | Configuring the System | Managing Clients

---

You are here: System Management > Using Task Schedules

Using Task Schedules

Task schedules are a "generic" node that may be used in expressions, restrictions and other types of functions where automated functionality that is controlled by day type and time of day is required. Task schedules define "availability"; that is, intervals [start/stop times] during the day for days of the week or day type (according to the calendar). For example, to control when an expression is available to be used, make a condition of the expression to use a task schedule, where the task schedule must be active in order for the expression to run.

- Management, Configuration and Commands

See Also: Calendars and Day Types | Using Expressions to Automate Actions

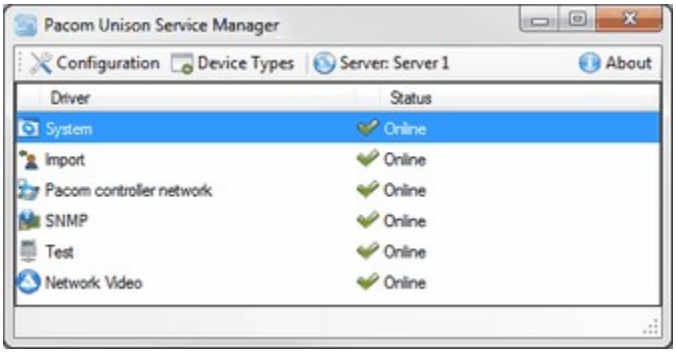
---

You are here: System Management > Using Unison Service Manager

Using Unison Service Manager

The Unison Service Manager is a utility driven by the Unison Windows service for controlling related device drivers and provides access to various server configuration tools. After Unison server installation [any server type], and the "Pacom Unison Server Process" Windows service is running [starts automatically after reboot, or may require manual start if no reboot], the Unison Service Manager becomes available. To open the Unison Service Manager, double-click  in the Windows "system tray", at the bottom-right of the desktop.

Note: Some actions require the Unison Service Manager to be run by an "administrator". To do this, from the Windows Start menu [or equivalent], right-click the Unison Service Manager and select Run as Administrator from the context menu. It may still be necessary to open the application from the "system tray".



If the installation involves multiple device driver servers, 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 device driver server. Normally, there is only one node called "System".

Note: Ensure that not more than one server is associated with a single secondary server. If two or more servers use the same secondary server it is possible that conflicts may arise from several servers attempting to control the same Unison device driver.

- Changing Device Servers
- Loading Licenses
- Registering Devices

See Also: Creating and Commanding Nodes | Database and Device Driver Configuration and Management | Introduction and Licensing | System Management

You are here: Creating and Commanding Nodes

Creating and Commanding Nodes

Nodes are a basic object that represent physical items, such as connected pieces of hardware, and "virtual" objects, such as doors, door schedules, operator groups etc. Every object in the system is represented by a type of "node", which generally defines its functions and properties that determine system behavior.

Note: The "system" device contains basic nodes that the system requires. This node cannot be deleted. "Import" and "export" device nodes are virtual objects that are designed for importing/exporting hardware node information. "Test" device nodes are designed to allow simulation of hardware and other functions, such as automated conditions and resultant actions, without actually having the physical device or affecting the actual system. Management of device and node objects is identical, with some exceptions - any differences are noted in the relevant topic.

The system provides a "bulk update" facility that allows you to change certain properties for multiple nodes in a single operation.

Device Nodes

Devices nodes represent physical hardware in the system. The device node usually corresponds to the applicable properties for managing communications and functions between the system and device, and may have "child" nodes that represent hardware or other functions under control of the device. For example, a Pacom Controller node that has child nodes for areas, card readers, doors etc.

A device has one or more "events" associated with it. Events basically represent a circumstance or occurence that has a value in terms of security, and these events can have a status of either "active" or "inactive". Events are associated with alarm types in order to generate alarms through status change; for example, a fire alarm generated by a smoke detector input that changes state to active. For most device types, nodes can be defined that correspond to hardware or other functionality that is supported by the device.

Note: For device nodes, the system must have the required device drivers installed for correct operation. The device driver is the communications interface between the Unison system and the actual hardware.

- Filtered Node Views
- Management and Configuration

See Also: Areas and Alarm System Control | Bulk Updating Node Properties | Database and Device Driver Configuration and Management | Nodes - Definition and

Use | Using Node Commands | Using Unison Service Manager

Bulk Updating Node Properties

Using Node Commands

Using Expressions to Automate Actions

You are here: Creating and Commanding Nodes > Bulk Updating Node Properties

Bulk Updating Node Properties

The bulk update tool is used for changing some properties for multiple nodes in a single operation. To begin the bulk update process, click (Bulk Update) in any node view toolbar then select the type of property to update. Options may vary depending on the selected node type:

- Properties
  - Node Properties - Change various node data properties.
  - Advanced Properties - Change various node data "advanced" properties.
  - Partition - Change node partition.
  - Folder - Change node folder.
- Events
  - Edit Events from Device Template - Change the device template that the node is using.
  - Edit Individual Events - Change properties for selected event(s) to something other than those set by the device template.
- Actions
  - Add Alarm Actions - Add automated actions based on alarm event status.
  - Add Programming Actions - Add automated actions based on node event status.

Changing Properties
Changing Events
Adding Alarm and Programming Actions

See Also: Creating and Commanding Nodes

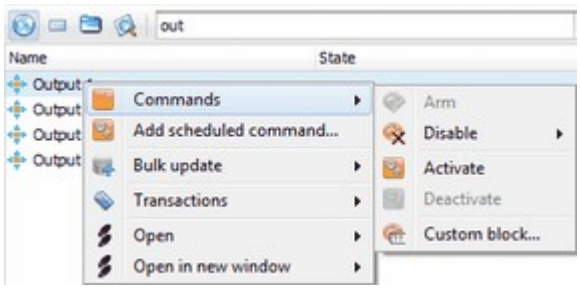
You are here: Creating and Commanding Nodes > Using Node Commands

Using Node Commands

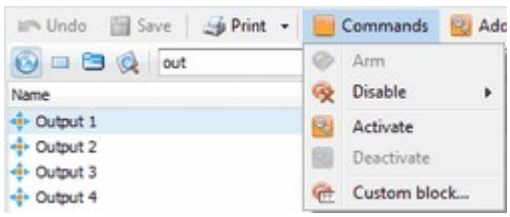
All node types are capable of certain functions that can be performed by way of "commands". The available commands is dependent on the node type, particularly for device nodes, and other factors, such as node arm/disarm status etc. Nodes are displayed in various panels and views, with several methods provided for accessing commands:

Note: Arm/disarm functions are managed through commands. Commands are usually sent from the Nodes panel or from a site map graphics using the Graphics panel. • All commands that occur in the system are logged in the command transaction log. • For specific command information, refer to the topics for specific node types.

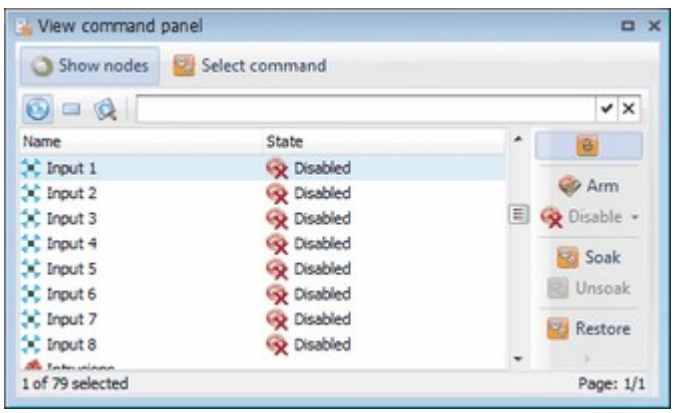
- Right-click - Right-click a node in any list and click Commands in the context menu for available options.



- Toolbars - Select a node then click the (Commands) button for available options.



- Commands panel - Provides access to nodes and commands from a single interface. To open, click (Commands) in the Panels ribbon bar.



Control	Description

X Discard any changes and close the panel or dialog box.

Show Nodes - Displays an Explorer list of nodes. Select a node in the list to send it a command.

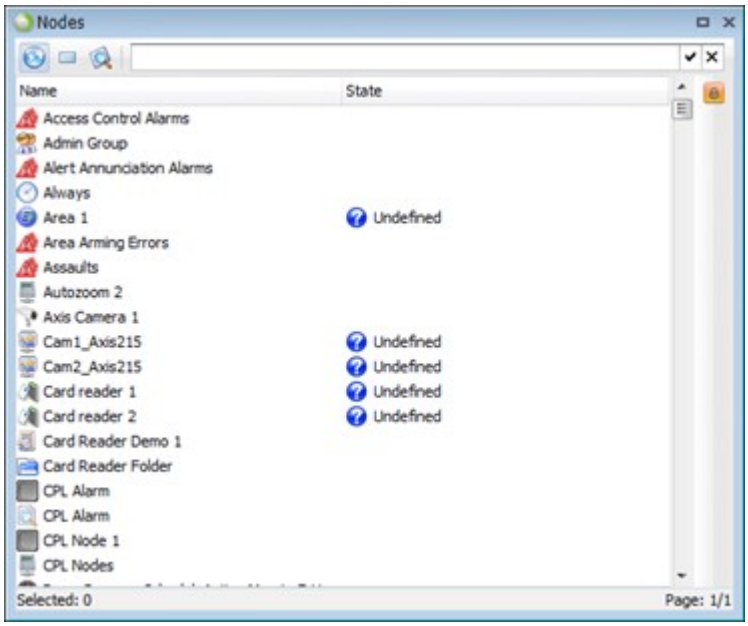
Note: The list is empty until you select a node/command combination using the Command dialog box ( ). • Depending on the node type selected, the list may automatically filter all other nodes. To always display all available node, select

Select Command - Opens the Command dialog box, where you can select the required node and command combination, then click OK to send the command and close the dialog box. The

Show/Hide Commands - Display/hide available commands as part of the / panel. Select a node then click to display commands. Click a command option to perform it. To hide commands, click . Nodes must be listed ( ) for this option to be available.

- Nodes panel - Provides access to all nodes and commands from a single interface.

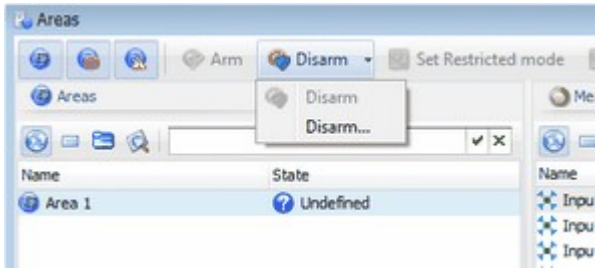
To open, click (Nodes) in the Panels ribbon bar, then select the type of node to display - only this type of node is listed. If you select Nodes, all types of nodes are listed. If several different node types are selected, only commands that are common to all nodes are provided.



Control	Description
X	Discard any changes and close the panel or dialog box.
/	Show/Hide Commands - Display/hide available commands as part of the panel. Select a node then click to display commands. Click a command option to perform it. To hide commands, click .

- Graphics panel - Provides access to nodes that are connected to graphics for alarm response purposes. To open, click (Graphics) in the Panels ribbon bar.

- Buttons - In some panels, commands can be accessed directly through a "command" button - select a node then click the button to display command options.



See Also: Alarm Response/Management | Creating and Commanding Nodes | Using Transaction Logs

---

You are here: Creating and Commanding Nodes > Using Expressions to Automate Actions

Using Expressions to Automate Actions

"Expressions" are used to set node status as a result of other node events; that is, node status is conditional, based on the status of one or more other nodes. Expressions consist of node events and logical "AND" and "OR" operators [also known as Programmable Logic Control (PLC), macros, Boolean algebra or interlocking conditions]. For example, an expression can be created to mean "node A status = X when node C status = Y AND node D status = Y OR node E status = Z".

For example:

Node A = X

when

Node C = Y AND Node D = Y

OR

Node E = Z.

There is no limit to expression complexity, therefore, in principle it is possible to build logical functions that combine events from task schedules and physical input/output (I/O) devices. Expressions can be used as components in other expressions, restrictions or other types of functions where an automated function is required that is controlled by a logical evaluation of nodes. The concept of expressions is based on a series of basic logical functions performed on specified conditions, resulting in an action. Expressions allow very specific conditions to be specified and met, and include the subsequent actions to taken. This provides a high degree of flexibility.

Management and Configuration

See Also: Creating and Commanding Nodes | Nodes - Defintion and Use

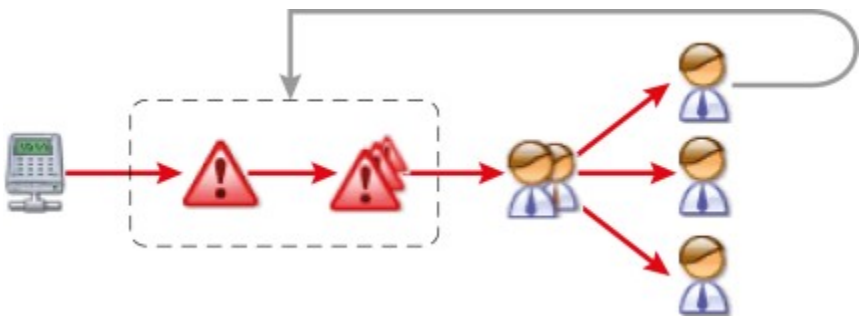
You are here: Managing Alarms

Managing Alarms

Alarm management basically means to use the system for notifying operators [security personnel using Unison] of alarms, including alarm type and location. The system provides operators with options and functions for responding to alarms; for example, by way of site map graphics, alarm lists and alarm queues. Alarm monitoring is generally based around the concept of controlled access to the premises - if the premises is accessed at an unauthorized time, an alarm is generated. Similarly, the actual security equipment itself is also monitored for tampering, bypassing, hardware failure etc.

- Alarm Type - Classifications for different kinds of alarm in order to distinguish it from other kinds of alarms in terms of response type etc; for example, intrusion alarm, hold-up alarm etc.
- Alarm Queue - Used to organize alarms by type into groups of alarms. Using queues makes responding to alarms easier for operators, including to responding to multiple alarms in a single operation.
- Alarm Priority - Used to organize alarms by priority so that operators respond to the highest priority alarms first.

The image below shows the alarm flow where an alarm condition is detected in attached hardware, which signals the system. The alarm is classified by type and then placed in the appropriate queue for operator response. The alarm is sent to operators directly or via operator group, for response. The system reacts accordingly to the operators' response to the alarm.



See Also: Alarm Control Guidelines | Alarm Queues and Types | Alarm Response/Management | Areas and Alarm System Control | Using Alarm Management Tools

Alarm Control Guidelines

Alarm Response/Management

Alarm Control Guidelines

Alarm system control is linked directly with access control in that breaches of security to gain access to a premises are, by design, going to trigger an alarm of some type. Configuration of alarm points is flexible enough to provide a range of behaviors that can be applied when an alarm occurs. Generally, alarms are categorized into alarm groups. Alarm groups require a "priority" setting which controls how the system handles the alarm and the urgency to apply to them.

Sites, and alarm areas within them, can be controlled for alarm system operation using time schedules to determine when disarming and arming can take place. For example, a business may set up time schedules to control the alarm system for normal business working days of Monday to Friday. The alarm system configuration can be set to allow disarming of the alarm from any time after 7AM and for arming of the system from any time after 6PM for weekdays. On Saturday, the business is open for half a day and therefore uses a different time schedule to control alarm system operation. Sundays are set up so that the alarm system is armed from Saturday afternoon until 7AM Monday.

The Pacom alarm system provides numerous features that can be used in various combinations to tailor the behavior or operation of the system. These features provides assistance for reducing false alarms as well as extensive hardware integration, such as with digital video systems, to improve alarm verification and speed up response. As an example of false alarm reduction, areas within a site can be set up to require two consecutive alarms within a period of time in order to "confirm" it as a genuine alarm and, therefore, report it. Also, in response to alarm conditions, an output can be automatically activated, such as lights, video recording etc using highly flexible "expression" [also known as "macro"] programming functions.

The alarm system works in conjunction with Pacom security management applications and hardware [third-party systems are also supported] for alarm and event reporting. These are generally set up and monitored by trained security staff and technicians.

Pacom alarm system hardware is purpose designed to ensure that alarm system and access control operation works in unison and provides features for custom behavior and secure operations. For example, communications between Controllers and alarm monitoring systems can utilize virtually any type of infrastructure available, such as IP

networks, wireless GPRS and dialup communications. Redundancy is inherent in that if one system cannot be used to deliver messages, another will be used and so on. The idea being to ensure that alarms notifications are always received.

Alarm system operation settings are stored in Pacom Controller memory, which allows the hardware to operate independently of the head system. This capability ensures that operation of the system is always maintained even in the event of the site being disconnected from the head system. Each site node has settings to control its operation and use a simple interface. Additional functions, such as management of firmware is also provided to simplify overall system management.

- Areas and Alarm System/Access Control
- Area Access and Alarm System Modes
- Inputs and Outputs - the Basis for Alarm Operation

See Also: Access Control Guidelines | Areas and Alarm System Control | Managing Alarms

---

You are here: Managing Alarms > Alarm Response/Management

Alarm Response/Management

Unison provides generic alarm and sub-system management, which means that all alarms are handled in the same way, regardless of which sub-system sends an alarm. It makes no difference if there is a fire alarm from one type of control panel, or a burglar alarm from another type of control panel. The advantage of this is a single process can be used for managing all alarms. An alarm event has different status conditions during its "life-cycle". Some status transitions happen automatically, some when the status of the alarm input changes, while others happen when they've been processed by an operator. What is relevant for a specific alarm event, and what is required for the alarm event to receive this status, depends partly on connected hardware and partly on system configuration. The alarm event status transitions to be confirmed by an operator and those that are automated can differ and depends on how the alarm is configured. It may therefore differ between different sites, but also between different alarm types within the same site.

The alarm response process comprises six general status transitions. Status transitions always occur in the following order:

New Alarm ▸ **Acknowledge** ▸ Restorable Alarm ▸ **Restore** ▸ Closeable Alarm ▸ **Close**

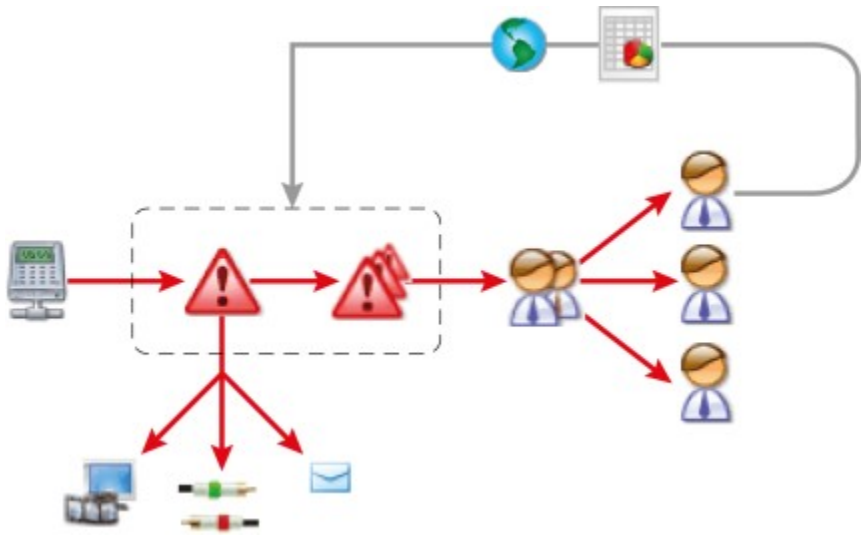
- New Alarm - Alarm event created and displayed via site maps, alarm queue, status bar, alarm alert pop-up etc.

- Acknowledge - Operator informs the system that he/she is aware of alarm [system can also be configured to "acknowledge" automatically].
- Restorable Alarm - Alarm acknowledged and the connected hardware is ready to be restored. This usually occurs when the alarm input returns to its normal position, such as door contacts closed.
- Restore - Operator informs the system that the alarm point is now inactive and can be reset to its normal position, or when the restoration comes from the connected hardware. An example of restoration from the connected hardware is when someone resets the alarm input from an alarm panel [system can also be configured to "restore" automatically].
- Closeable Alarm - Alarm acknowledged and restored and ready to be closed.
- Close - Operator informs the system that the alarm response is complete. When an alarm is closed, it is removed from the Alarm Queues and Alarm List panels and is recorded in the alarm transaction log [system can also be configured to "close" automatically].

Note: Generally, most alarm types are configured to be acknowledged and restored manually by an operator, via the Alarm Management dialog box, and to automatically close once acknowledged and restored. These settings can be automated, if required, using the alarm type configuration. • All alarm event status changes are logged regardless of them being manual or automatic. • Changes of state are accompanied by color changes in various panels and the status bar to make it visually easier for operators to identify alarms on screen.

Additionally to the main alarm interface, the system provides a range of alarm management tools and utilities that can be deployed in alarm management [usually by way of alarm actions], such as auto-email notification, program launchers etc. For example, for an alarm that is considered critical, it is possible to do the following automated actions:

Note: Actions as a result of an alarm or other event can be applied to any node in the system.



In the above scenario, a piece of hardware has an alarm. The alarm is classified by type and alarm queue. As a result of the alarm, alarm actions have been set up to automatically start recording video, activate other inputs and outputs and to send an email. The alarm notification is sent to operators via operator groups and, when an operator responds to the alarm, they create a report and must also go to a web site to report the situation.

- Alarm Response Basics
- Automating Alarm Response Using Actions
- Alarm Response Using Graphics

See Also: Configuring Roles, Operator Groups and Operators | Configuring the System | Creating and Commanding Nodes | Launching External Programs/Documents | Managing Alarms | Using Alarm Management Tools | Using Site Map Graphics

---

You are here: Managing Alarms > Areas and Alarm System Control

Areas and Alarm System Control

Areas are special nodes that are basically "containers" for other hardware based "member" nodes, and enables performing commands on the member nodes by way of the container area. That is, areas represent groups of security and access control devices/nodes that are more easily represented and controlled/commanded as a single object. For example, parts of a building in terms of access control and alarm monitoring.

Note: The concept of areas may not be applicable to all alarm panel hardware.

Certain alarm operation nodes, such as inputs, can be commanded into several states that determine how alarms generated by them are handled by the system [when normal alarm operation is not required]. For example, "isolate", which means that alarms from the node are suppressed in the system although active at the hardware level; and "disarmed", which means that all events (including tamper or false alarms) from the node are ignored by the system. "Alarm commands" are commands usually carried on area nodes that affect all member nodes of the area. For example, to "disarm" an area will automatically disarm the member nodes of the area. If the command is not supported by the sub-system, it is still able to be applied locally within the Unison system, which has no effect on the sub-system. For example, the sub-system may report an alarm as usual, however, the system may be set to ignore the alarm event. When alarm inputs are armed and disarmed, or otherwise commanded, it is important to distinguish whether or not the command is sent to the hardware to be performed, or applies locally in the Unison system only.

Alarm command is usually performed through the Areas panel or directly from a site

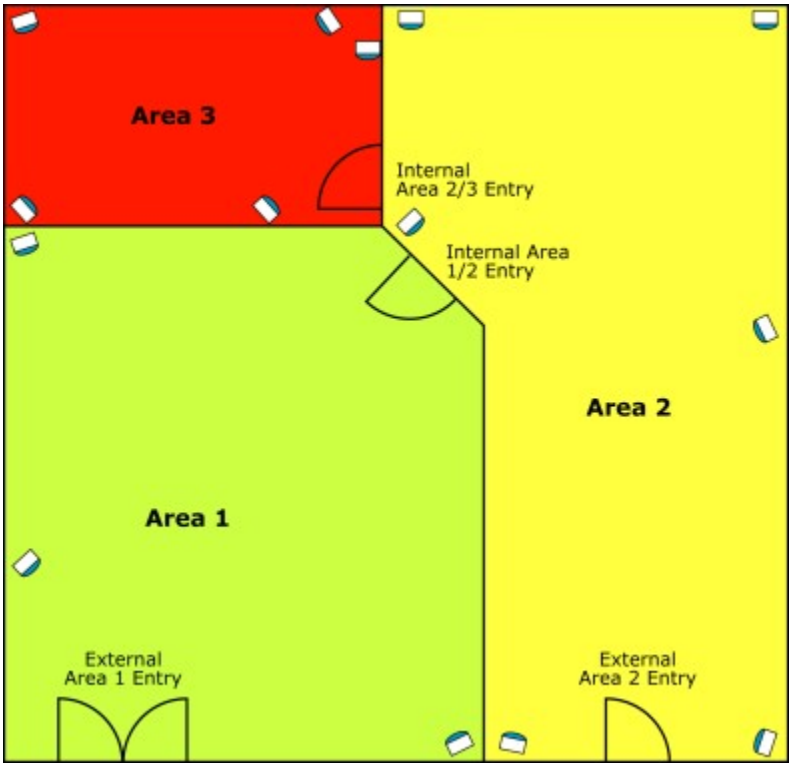
map graphic (Graphics panel). Commands can also be made from anywhere where nodes are listed (Nodes panel, Hardware view etc), where areas can be controlled (that is, multiple alarm nodes) at the same time. You can also command each alarm node individually, known as individual command. In the Areas and Graphics panel the alarm status for areas and member nodes can always be seen.

Example Scenario

Consider a business premises that has a "public" area, "staff" area and "accounts" area. The staff use a different entry to the public. The accounts area is located at the rear of the premises and can only be accessed from the staff area. Areas could be set up as follows:

- Area 1 (green) for the publicly accessible part of the premises. This area operates to access schedules in accordance with normal opening hours for the business and may use different security devices to other parts of the premises, for example, CCTV cameras.
- Area 2 (yellow) for the staff-only accessible part of the premises. This area operates to access schedules that may vary from normal opening hours, so that staff can work outside of normal business hours and requires alarm settings that also vary from the publicly accessible area. It may also employ different security detection devices, for example, motion detectors.
- Area 3 (red) for the accounts area. This area operates to access schedules that may vary from other areas within the premises and allows only authorized staff to access it. It may also use different security detection devices, for example, motion detectors and CCTV cameras.

The following image shows the areas set up for the premises.



As you can see from the example, using multiple areas within a single site make configuration and operation of the system flexible in terms of both access control and alarm system based security.

- Area Access and Alarm System Modes
- Pre-Defined Alarm Commands
- Custom Alarm Disarming
- Area - Management, Configuration and Commands
- Areas Panel
- Alarm Commands from Site Maps and Graphics
- Disarmed Nodes Panel

See Also: Alarm Response/Management | Using Alarm Management Tools

---

You are here: Managing Alarms > Alarm Queues and Types

Alarm Queues and Types

The system must be set up to respond to alarm events. There are three basic "objects" that the system uses for alarm management:

- Alarm Queue - The direct user interface between alarms in the system and operators, providing visual and audible notifications of alarms.
- Alarm Type - A categorization for similar/associated alarms that determines the alarm queue to connect to, alarm priority (urgency) and some system behaviors when responding to alarms of the type, such as automatic acknowledge. Each alarm type is connected to an alarm queue.
- Node - Represent parts of the physical security system (devices, doors, alarm points, card readers etc) that are capable of generating "events", which are basically changes of state. Node events that generate alarms must be connected to an alarm type. Other properties that are connected to the node and determine how an alarm event should behave are:

  - Actions performed automatically when the alarm occurs.
  - Actions an operator should be able to perform manually.
  - How the node should be displayed in a possible graphic image.
  - Other properties, such as arming delay and alarm priority.

This topic contains an overview of the tools used to manage alarms, and how to create and configure alarm management.

- Alarm Queues
- Alarm Types

See Also: Configuring the System | Creating and Commanding Nodes | Managing

Alarms

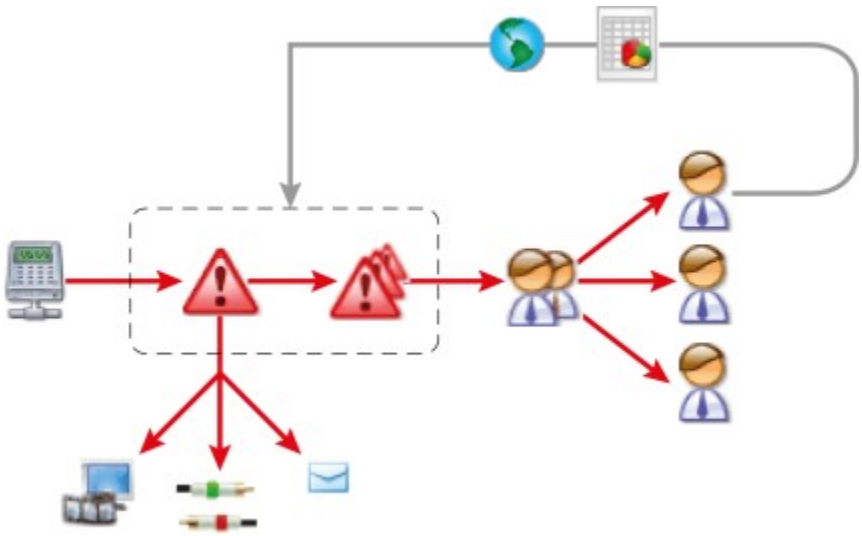
Using Alarm Management Tools

There are three main tools that are used to respond to and manage alarms:

- Alarm Queues panel.
- Alarm List panel.
- Alarm Management dialog box.

Additionally to the main alarm interface, the system provides a range of alarm management tools and utilities that can be deployed in alarm management [usually by way of alarm actions], such as auto-email notification, program launchers etc. For example, for an alarm that is considered critical, it is possible to do the following automated actions:

Note: Actions as a result of an alarm or other event can be applied to any node in the system.



In the above scenario, a piece of hardware has an alarm. The alarm is classified by type and alarm queue. As a result of the alarm, alarm actions have been set up to automatically start recording video, activate other inputs and outputs and to send an email. The alarm notification is sent to operators via operator groups and, when an operator responds to the alarm, they create a report and must also go to a web site to report the situation.

- Alarm Queues Panel
- Alarm List Panel
- Alarm Management Dialog Box

Alarm Alert "Pop-Up"
Alarm Details Panel

See Also: Alarm Code | Alarm Response and Management | Auto-Alarm Report | Auto-Email Notification | Configuring Roles, Operator Groups and Operators | Counter | Frequency | Impulse | Instruction and Web Page | Managing Alarms | Latch | Program Launcher | Step | Action Plans

Alarm Code

Auto-Alarm Report

Auto-Email Notification

Counter

Frequency

Impulse

Instruction and Web Page

Latch

Program Launcher

Step

Alarm Notes

Action Plans

Creating a Shadow Alarm

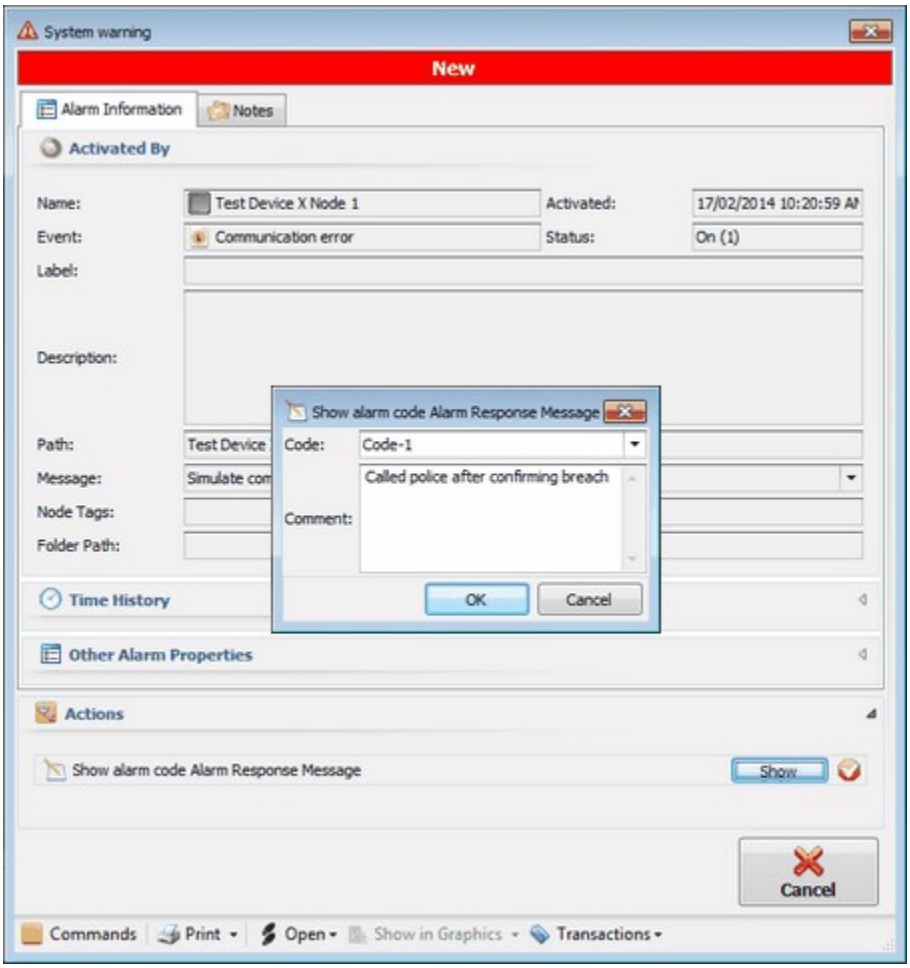
You are here: Managing Alarms > Using Alarm Management Tools > Alarm Code

Alarm Code

"Alarm code" nodes are a form of alarm categorization that is often used to simplify alarm management and response. The concept of alarm codes is basically to provide a "shorthand" or abbreviated label for an alarm of type and applies to several third-party systems; for example, Contact ID. Alarm codes can also be used as a search filter for alarm transactions.

As an example, the following image shows the Alarm Management dialog box for an alarm that has been set up with an action that requires the operator to apply an alarm

code. When the operator clicks Show in the Alarm Management dialog box, a secondary dialog box displays, where the operator can select an alarm code from those configured in the alarm code node properties, and optionally enter some comments regarding the alarm:



Management, Configuration and Commands

See Also: Managing Alarms | Creating and Commanding Nodes | Using Alarm Management Tools | Using Node Commands

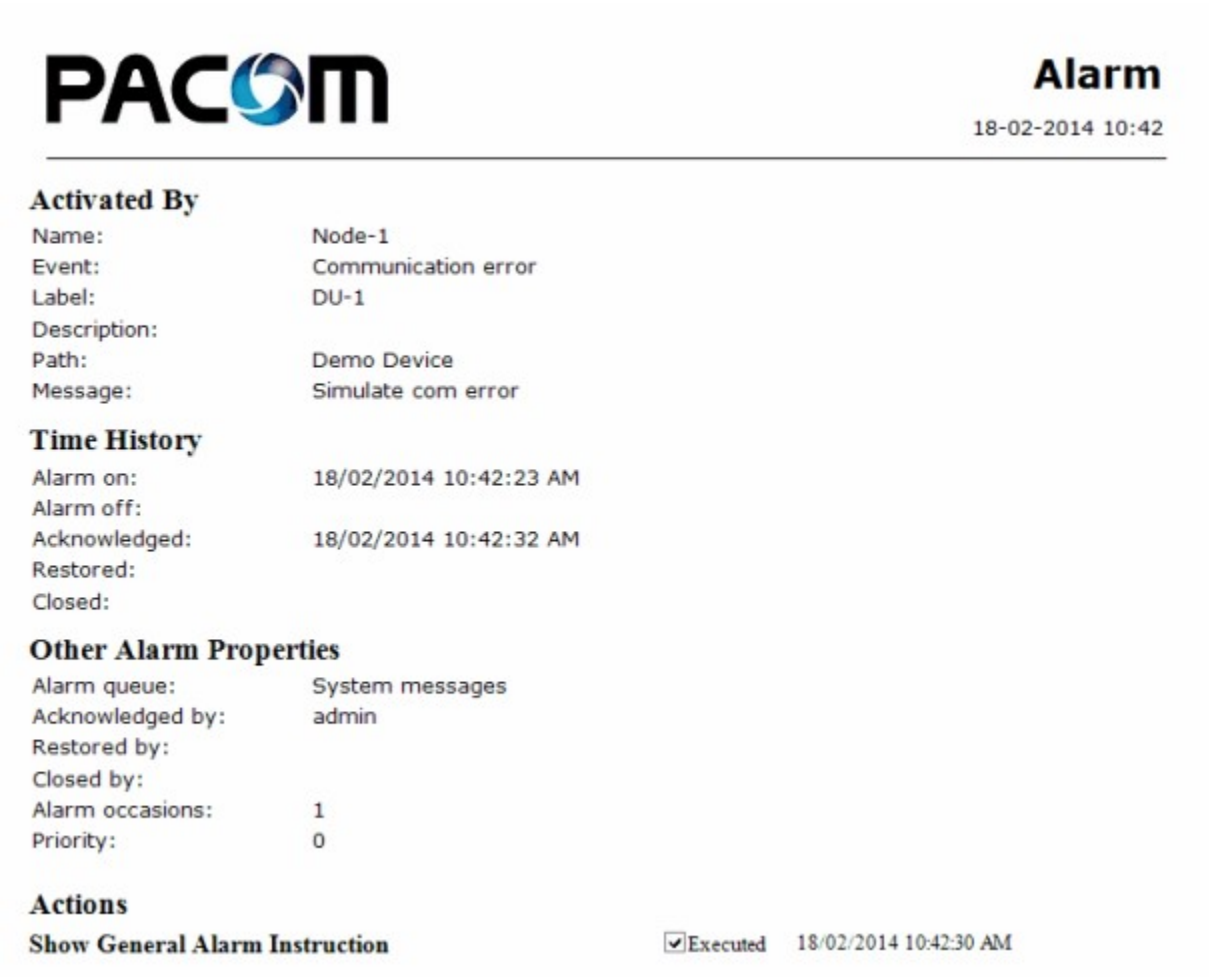
---

You are here: Managing Alarms > Using Alarm Management Tools > Auto-Alarm Report

Auto-Alarm Report

"Auto-report" nodes represent print/electronic document templates for providing alarm related information. The system comes with default alarm report templates (some with and without site maps), that are structured similarly to information displayed in the Alarm Management dialog box.

Note: Commands for alarm auto-report nodes are available only from the Alarm Management dialog box. Alarm reports are not available from transaction logs. • You can also create custom report templates (see Using and Creating Reports).



PACOM

Alarm

18-02-2014 10:42

Activated By

Name:	Node-1
Event:	Communication error
Label:	DU-1
Description:	
Path:	Demo Device
Message:	Simulate com error

Time History

Alarm on:	18/02/2014 10:42:23 AM
Alarm off:	
Acknowledged:	18/02/2014 10:42:32 AM
Restored:	
Closed:	

Other Alarm Properties

Alarm queue:	System messages
Acknowledged by:	admin
Restored by:	
Closed by:	
Alarm occasions:	1
Priority:	0

Actions

Show General Alarm Instruction ☑ Executed 18/02/2014 10:42:30 AM

The above example shows a default "detailed" alarm report that displays most alarm event data. The default "detailed alarm report with graphical image" template has additional parameters:

- Overview Image - Displays the associated overview image for detailed image, where applicable. The detailed image must be associated with an overview image.
- Detailed Image - Displays the graphical image connected to the node. The node with action must be connected to a graphical image.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

You are here: Managing Alarms > Using Alarm Management Tools > Auto-Email

Notification

Auto-Email Notification

"Auto-email notification" nodes are a utility that can be used to automatically send emails from the Unison system to recipients in response to an event. For example, sending email to a technician or IT department in the event of a communications failure etc. This facility can be used to ensure that the correct personnel can be informed of alarms/events with minimal delay or the need for human interaction.

- SMTP Server - Management, Configuration and Commands
- Receiver - Management, Configuration and Commands
- Receiver Group - Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools

---

You are here: Managing Alarms > Using Alarm Management Tools > Counter

Counter

"Counter" nodes represent a counter that increments or decrements on command and when a set number [also set by command] is reached, the node status becomes active ("on"). The idea behind counter nodes is to use them in node actions programming, such as alarm and programming actions, expressions etc, where the changing of state of the counter node acts as a trigger or link for other functionality. For example, setting up an alarm node event to command a counter node, and when a specific value of activations has been reached, the counter node causing another node action based on its own change of state etc.

- Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

---

You are here: Managing Alarms > Using Alarm Management Tools > Frequency

Frequency

"Frequency" nodes represent a changing of state at a regular interval - a timed change between active ("on") and inactive ("off") states. The idea behind frequncy nodes is to

use them in node actions programming, such as alarm and programming actions, expressions etc, where the changing of state of the frequency node acts as a trigger or link for other functionality. For example, setting up an alarm node event to command a frequency node, and the frequency node causing another node action based on its own state changes etc.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

---

You are here: Managing Alarms > Using Alarm Management Tools > Impulse

Impulse

"Impulse" nodes represent an instantaneous signal or "flash" that, when activated and taking on an active state, immediately returns again to a inactive state. That is, an instant toggle between two states. The idea behind impulse nodes is to use them in node actions programming, such as alarm and programming actions, expressions etc, where triggering of the impulse node acts as a trigger or link for other functionality. For example, setting up an alarm node event to command an impulse node, and the impulse node causing another node action based on its own triggering etc.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

---

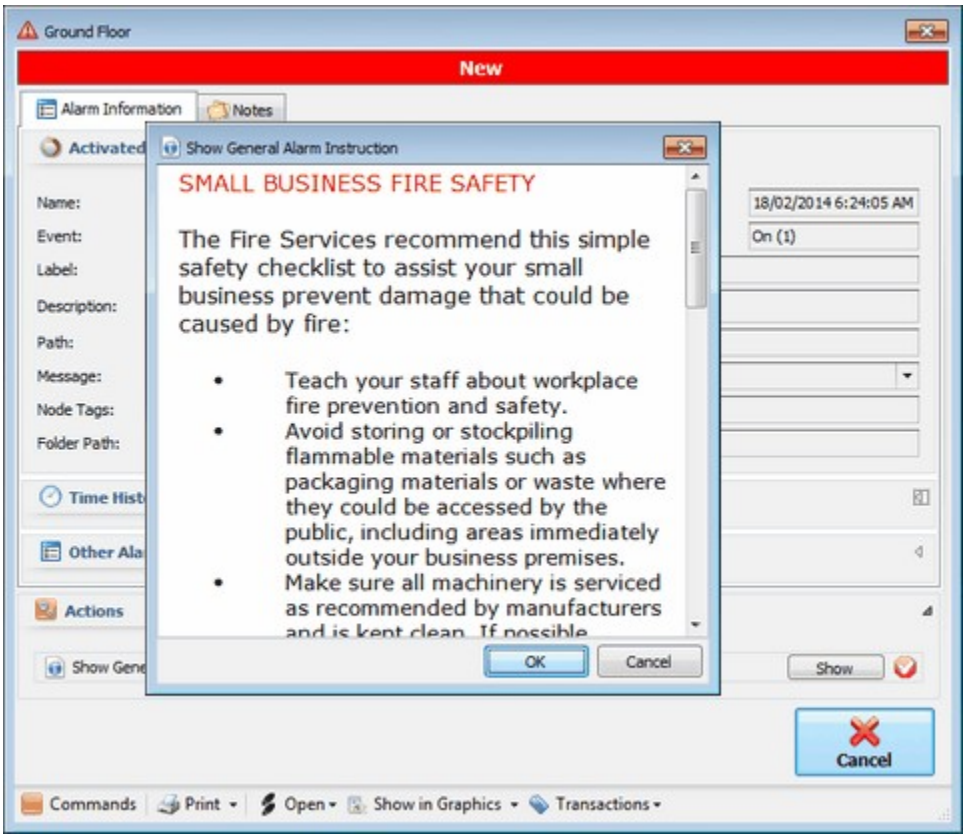
You are here: Managing Alarms > Using Alarm Management Tools > Instruction and Web Page

Instruction and Web Page

"Instruction" nodes represent items of text-based information or web pages (for example, web sites, images, documents etc) that are displayed to operators when responding to alarms through the Alarm Management dialog box.

As an example, the following image shows the Alarm Management dialog box for an alarm that has been set up with an action that requires the operator to display an

instruction. When the operator clicks Show in the Alarm Management dialog box, a secondary dialog box displays, where the operator can view the associated instruction:



Instruction - Management, Configuration and Commands
Web Page - Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

---

You are here: Managing Alarms > Using Alarm Management Tools > Latch

Latch

"Latch" nodes represent a "relay" that alternates state using a common command. That is, if it is currently inactive then is commanded - it takes on the active state and, at the next command activation, it reverts from active to inactive. The idea behind latch nodes is to use them in node actions programming, such as alarm and programming actions, expressions etc, where the changing of state of the latch node acts as a trigger or link for other functionality. For example, setting up an alarm node event to command a latch node, and the latch node causing another node action based on its own state change etc.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

---

You are here: Managing Alarms > Using Alarm Management Tools > Program Launcher

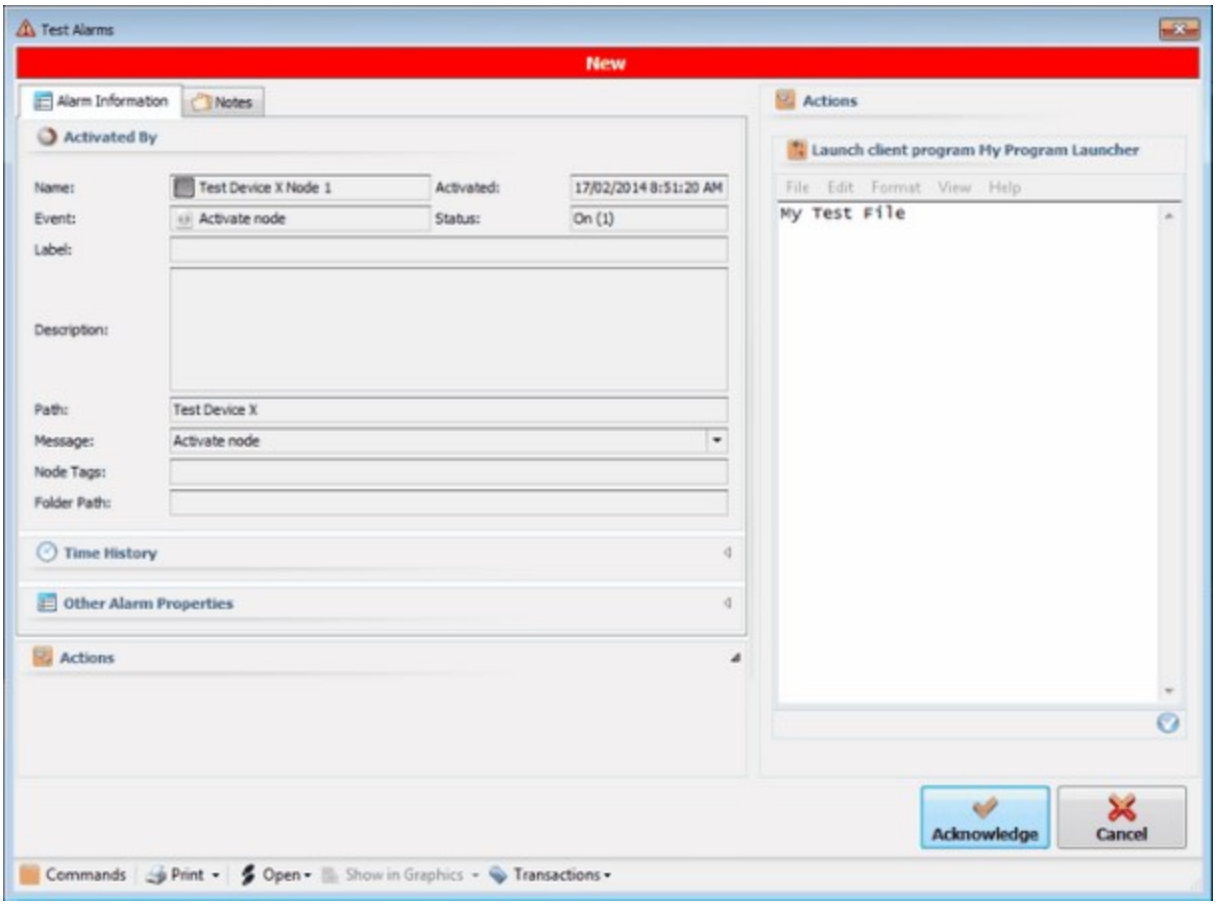
Program Launcher

The "program launcher" node is a feature that allows operators to launch external applications from within the Unison system. It can be used with programs ranging from document viewers to specific applications, and is often used to provide instructions for operators when a specific alarm is triggered [by way of node alarm event action to send a command to the program launcher node to activate it]. This functionality enables the Unison system to be linked to applicable documents etc, and because documents can be referenced from their normal stored locations, the latest version is always used. Programs can be [mostly] launched as integral to the Unison system ("embedded") or in separate windows.

Programs/documents can be launched on either the client machine or server, so there are actually two nodes - "client program launcher" for launching on the client computer [usually manned by an operator], and "server program launcher" for launching on the server computer; for example, a script. Client program launchers are executed on the local client only. This means that the program or command line syntax must be available on the client. That is, requesting an application that is not installed will fail. For server program launchers the same applies, however, the program or command line syntax must be available on the server. For servers, additional settings are available for specifying credentials to run the commands against.

Note: If there are multiple servers being used, the launcher will run on the server currently running the "System" device driver. In cases where multiple servers are being used, the application or file associated with the program launcher needs to be available on all servers.

As an example, the following image shows the Alarm Management dialog box for an alarm that has been set up with an action to launch a program, embedded into the dialog box:



Management, Configuration and Commands

You are here: Managing Alarms > Using Alarm Management Tools > Step

Step

"Step" nodes represent a "switch" that changes to a selected state by command. For each switch, it remains in that state until commanded to the alternate state. The idea behind step nodes is to use them in node actions programming, such as alarm and programming actions, expressions etc, where the changing of state of the step node acts as a trigger or link for other functionality. For example, setting up an alarm node event to change the state of a step node, and the step node causing another node action based on its own state change etc.

Management and Configuration

See Also: Creating and Commanding Nodes | Managing Alarms | Using Alarm Management Tools | Using Node Commands

---

You are here: Managing Alarms > Using Alarm Management Tools > Alarm Notes

Alarm Notes

Comments can be added to specific alarm events so as to register information about actions or incidents relating to an alarm, thereby preserving the transactions. Alarm notes cannot be edited or deleted once they have been created and can be associated with alarms in any state - new, acknowledged, restorable or closable. Unlike notes, alarm notes are specific to alarms whereas notes are general information about a node that can contain images, tables and text.

Alarm notes are date/time stamped and include the name of the operator who created the alarm note thereby preserving information for audit purposes. There is no subject associated with alarm notes. The last comments's timestamp is displayed as Response Changed on the top. Once an alarm note is transferred to the log database or archive no additional comments can be added. The alarm note can also be viewed from the transaction log. Alarm notes are saved to the AlarmNoteLog table of the database.

To add an note to an alarm:

1. Double-click an alarm in the Alarms List.
2. Click the **Alarm Notes** tab.
3. Click **Create Comment**.
4. Enter a comment about the selected alarm.
5. Click **OK**.
6. Click Save.

For example, an operator can add a comment to an alarm note that a guard who was dispatched to check out an alarm in an area. An additional alarm note can be added to report on what the guard found out about the alarm.

You are here: Managing Alarms > Using Alarm Management Tools > Action Plans

Action Plans

You are able to associate an action plan with a specific alarm action so that an operator can follow instructions on what must be done.

1. Go to the Hardware view.
2. Expand the System node.
3. Right-click Action Plans then select Create > Action Plan from the context menu.
4. Click the Properties tab.
5. Enter the property details for the new action plan.

6. In the Settings section, click Add on the toolbar to add a new entry to the table below.
7. Enter the Text for the action plan.
8. Click the checkbox in the Enabled column to activate the action plan.
9. Tick the Comments Required and/or Completion Required checkbox.
10. Repeat from Step 5 to add as many steps to the action plan as needed.
11. Click Save.

Once an action plan has been created, you can associate the action plan with a node by selecting it on the Action tab of the node.

See Also:Alarm Code | Alarm Response and Management | Auto-Alarm Report | Auto-Email Notification | Configuring Roles, Operator Groups and Operators | Counter | Frequency | Impulse | Instruction and Web Page | Managing Alarms | Latch | Program Launcher | Step

---

You are here: Managing Alarms > Using Alarm Management Tools > Creating a Shadow Alarm

Creating a Shadow Alarm

Certain alarms for specific nodes or events can be triggered in 2 different locations, so that 2 different operators are able to view and respond to the event. These are called shadow alarms.

For example, fire or assault alarms for a specific building can be allocated to a second operator group on a separate client.

You are able to create a shadow alarm to allow for operators in 2 different operator groups to be able to action alarms from the same source but with different alarm types.

The primary alarm and the secondary alarm are displayed on different clients and are associated with different operators. If the secondary operator is not logged on, then the alarm event remains in their queue for action when they log on.

With any event that has an associated secondary alarm, both alarms must be acknowledged individually. Only when the primary alarm is closed, can the secondary alarm be closed. The secondary/shadow alarm can only be restored if the original alarm has been restored. The secondary/shadow alarm can only be closed if the original alarm has been closed. An operator with administrator privileges is able to restore or close a shadow alarm regardless of the state of the original alarm.

1. Go to the Hardware view.
2. Select the System node.
3. On the right pane, click the Actions tab.

4. In the Programming Actions section, click Create on the toolbar.
5. Select Create shadow alarm as the Event or Command.
6. Complete the remaining fields for the programming action.
7. Click Save.

The Create shadow alarm command is available from right-clicking the System node and selecting Commands > Create shadow alarm from the context menu.

See Also:Alarm Code | Alarm Response and Management | Auto-Alarm Report | Auto-Email Notification | Configuring Roles, Operator Groups and Operators | Counter | Frequency | Impulse | Instruction and Web Page | Managing Alarms | Latch | Program Launcher | Step

You are here: Managing Access Control and Users

Managing Access Control and Users

Access control basically means the concept of having authorized users being able to access the premises at set/controlled times and in specific ways. For example, being able to access particular doors on certain days and between certain times. When a user attempts access outside of their allotted access privileges, they are denied access. As another example, a user attempts to gain access through a door - the system first checks that the door is available to be accessed via its door schedule; if it is accessible, the system then checks the that the user is able to access the door at that time and during that day via the access schedules and user access privileges; if accessible, users must then validate themselves to the system according to the security level mode set in the door schedule - if all things are acceptable, access is granted. The following types of objects can be created and managed:

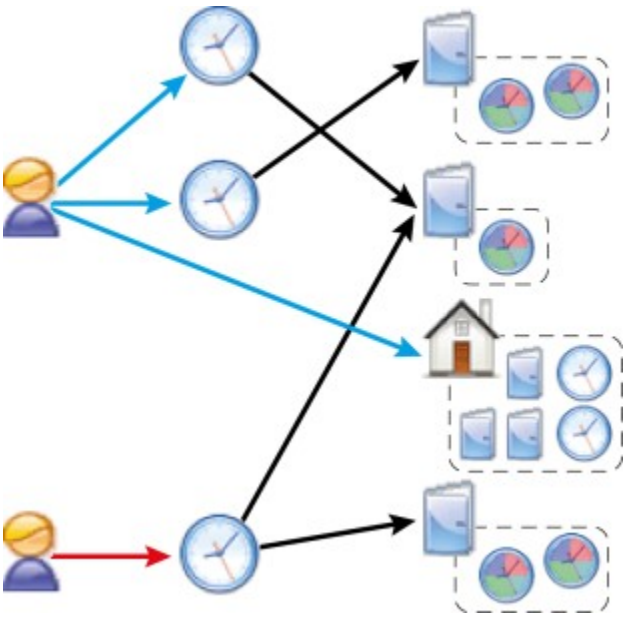
Note: Before setting up access control, all hardware, including doors and associated card readers, should be configured.

-  Day Type - Classifications for days of the week in terms of premises operation and security; for example, normal business days Monday to Friday, half-day business hours on Saturday and closed all day Sunday. For each day type, the security level [door schedule] must be defined.
-  Calendar - Used to identify dates in the year where the normal day type used is to be overridden; for example, on a public holiday.
-  Door Schedule - Settings that determine the required door security levels over a 24 hour period; for example, during a period of the day the door may be locked, unlocked during another period, require users to present a card and enter a PIN during another period etc. Door schedules can be applied to any available day type, and are assigned to one or more doors to automatically provide the physical implementation of security [usually via card readers and keypads connected to the door].
-  Door - Represent physical access controlled doors in the site, including the card readers associated with the door, door control time limits [how long can remain open etc] and door schedules to apply. Doors are connected, together with access schedules, to users' access levels, either individually to a user, or via access groups.
-  Access Schedule - Settings that determine access controlled door availability to users over a 24 hour period; for example, during a period of the day users may be unable to access any doors, and can access doors during another period etc. Access schedules are assigned to one or more users to automatically provide the physical implementation of security. Access schedules are connected, together with door

environments, to users' access capability [which doors can be accessed and when] either individually, or via access groups.

- Access Group - Defines assortments of doors, areas etc that share the same access schedules, and provides a simple method for applying similar access control settings to multiple users.
- User - Persons that are authorized to access the premises through access controlled doors. User information includes personal and access card details as well as actual doors, areas and access groups. Users can also have "personal access" permissions, which are used to assign doors, elevators etc to a user that are not in any access groups that the user has assigned to them.
- Access Card - Defines the information and appearance of user access cards ["layout"] as well as actual access card data format ["profile"] etc.

The image below shows the relationship between each major access control node type; that is, users, access schedules, access groups, doors [and card readers] and door schedules.



See Also: Access Control Guidelines | Access Groups | Access Schedules | Calendars and Day Types | Card Layouts | Card Profiles | Door Schedules | Door and Card Reader Configurations | User Areas | Users and Access Cards

Access Control Guidelines

Access Groups

Access Schedules

Calendars and Day Types

Card Layouts

Access Control Guidelines

Access control allows the security system to control and monitor the movement and location of personnel throughout a site. Access control is accomplished with a combination of Pacom management software, Controller firmware and door controllers (Pacom 1064, 1076 etc). Pacom door controllers (also known as "card reader interfaces" or CRIs) act as the local hardware interface for various types of third-party card reader devices and associated electronic door lock devices.

Note: For information on the installation of Pacom access control hardware, see the Pacom Hardware Installation Guide.

Within any given system the level of access control implementation can vary widely. It can range from a simple system, with a single card reader on the front door for controlling access to the premises during restricted hours of the day, to a fully controlled premises, divided into secured areas by controlled access points using card readers that enable tracking and monitoring of users throughout a premises.

Access to secured areas can be limited to particular users or user types, during certain times, alarm system modes or in various circumstances. User access to secured areas is controlled by assigning a range of options and parameters to the areas themselves, or to individual card readers or users.

Note: A single Controller can support a maximum of 254 "areas", however, up to 32 of them can be used for alarm control (depending on Controller and firmware version) and are sometimes referred to as "alarm areas". All remaining possible areas (up to a maximum of 222 if all alarm areas are being used) are defined in terms of access control only and are sometimes referred to as "access areas". The difference between the two is that alarm areas are able to support alarm devices (for example, motion detectors) and functionality (that is, to apply alarm system modes and generate alarms). • User options are not discussed here, except where they directly effect or are

affected by hardware options or settings.

Pacom security management software support producing reports on any card access transaction data. For example, reports can be made on the number of users passing through a particular door or area, or about individual user activities. The system also dynamically updates access control changes so that operation is always performed using the latest information. For example, changes to individual access cards or access control groups etc are propagated to all sites.

When setting up access control, the means for assigning access control to users should be carefully considered so that the Controller memory usage and user management is as efficient as possible. For example, for access controlled doors, elevators etc that are commonly assigned to users, it is recommended to set this up as an access control "group". This means that a user can be assigned the group and not require being assigned the contents of the group on an individual basis. Using the grouping concepts for access control provided by Pacom management software assists in reducing the time required to set up access control and simplifies managing access control for users.

Standalone Card Readers

Standalone card readers are the more commonly installed method of controlling access. A standalone card reader is where a single card reader is placed at each door and access is controlled on entry only. In some cases a door may use a lock that can be opened from the inside, or an egress button can be connected to the card reader to unlock the door, for exit. Egress buttons may also be installed when there is a door lock that can be opened from the inside. The button is used to mask out the door contacts during the shunt time and prevent a "Forced Door" alarm from being sent when the door is opened. When standalone card readers are used, the system cannot properly monitor users that have entered due to uncontrolled exit, and certain functions that require in/out card readers are not possible.

In/Out Card Readers

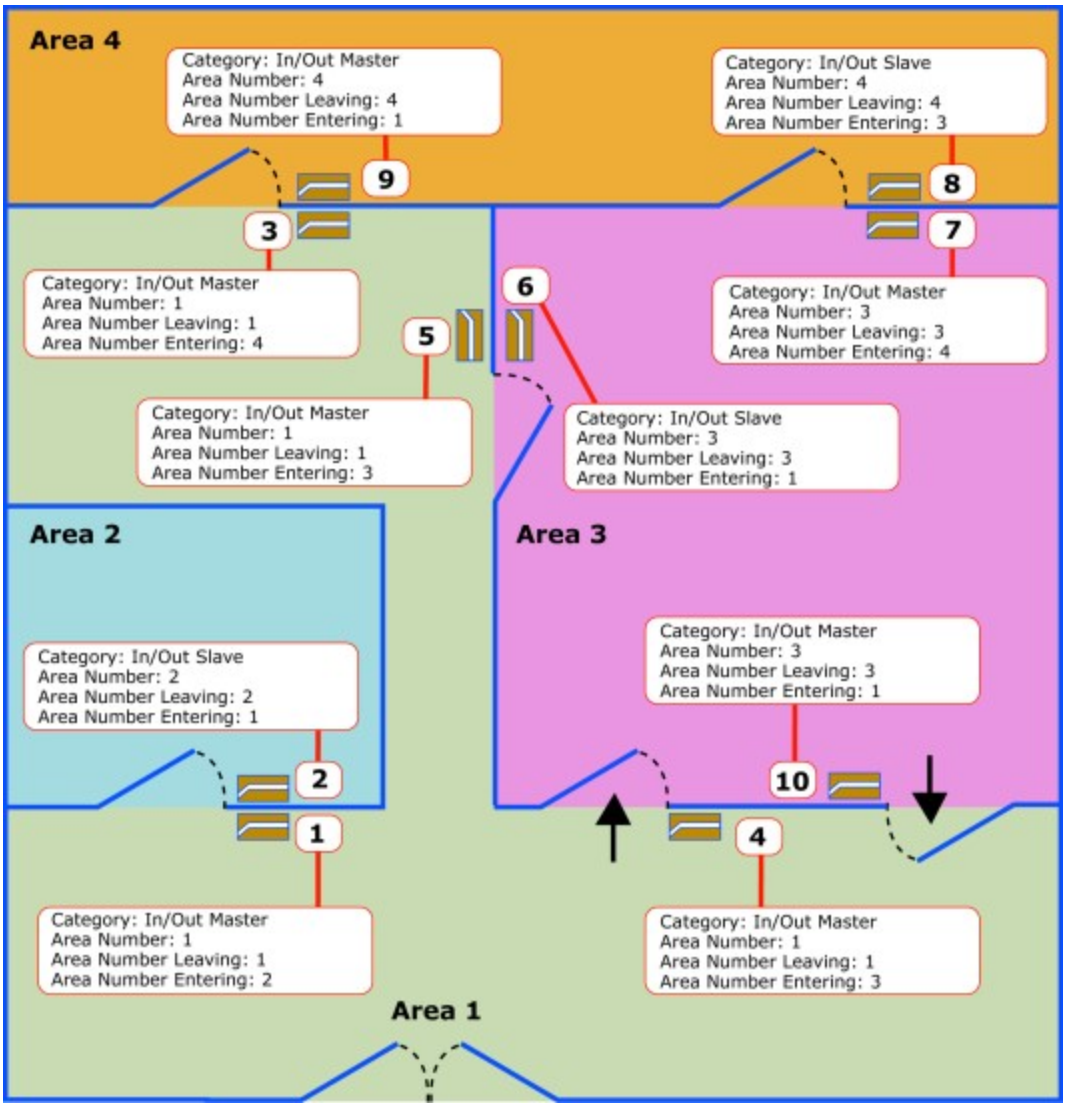
An "in/out" card reader is a pair of card readers mounted on a single access point (usually a door). Each card reader is used to control access in one direction through the access point; that is, one for entry and one for exit. Card readers set up in this configuration allow the system to monitor the entry and exit of users. This enables the system to determine the location and/or the number of users within a site or area, which is often used for safety or emergency/evacuation procedures and for time and attendance records, as in recording when a user entered/exited an area and how long they were in the area. For the system to work, all access points to any secured area must be controlled. The card readers can be connected as:

- Two "main" card readers that have their own door contact inputs (from the same door). The door strike contacts can be connected in parallel to both card readers. Separate one-way doors can also be used with this configuration for high traffic movement. Main card readers connected to the same door do not require consecutive

identification (ID) numbers.
- A "main/ssecondary" pair of card readers, where the door contacts and strike output are connected to the "main". The "secondary" monitors the door contacts of the main and can activate the main card reader strike relay. In this configuration, the secondary card reader must be the next consecutive identification (ID) number from its associated main card reader.

Note: Sending commands to one card reader in an in/out pair does not affect the operation of the other card reader. For example, sending a lock command to the "in" card reader will not lock the associated "out" card reader. • The system keeps track of the area a user is in and, before accepting the new area after a valid read, the system checks that the door has actually been opened. If the door contacts are not connected, the shunt time setting can be set to "0" so that the user is accepted to the new area immediately upon a valid read. • It is possible to set up time and attendance operation for an area using a single card reader. In this configuration, the first card swipe for a particular access card is considered "in", the next swipe is "out", the next "in" and so on.

Each in/out reader is configured using the areas that they are in and control access to. These are the "leaving" and "entering" settings. The "leaving" setting is the same ID number as the area number (the location of the reader). When you assign these parameters, the easiest way to identify the correct area to enter is to draw a diagram of all areas and the locations of card readers within them.



An extension to in/out readers are parking lot readers. The system keeps a count of the entries/exits and compares it with the area profile configuration. For example, when the car park is full, it could trigger an event, such as activating an output to turn on a "Car Park Full" sign or to change modes. You can program the output in the access area profile configuration. As in the above example, a GPO is activated while the count for the area remains at or above the maximum. This output is ignored if the count is set to "0". If the system is only concerned with the number of valid users in the area (car park in this example) and not identities, an input device, such as a push button, can be used to allow egress from the area and command the system to decrement the number of users still present.

Mustering Card Readers

Mustering is a function that is used for safety/evacuation procedures, most often associated with fire or other threats. The idea of mustering is to use one or more card readers that are installed specifically for keeping track of users that have left the building or have moved into a specific area during an emergency.

An example of mustering might be a building where a fire alarm has occurred. In the

case of a fire alarm, access controlled doors unlock so that occupants have direct exit from the building. When access controlled doors are unlocked like this and users can get through without being registered as "out", the system loses track of the whereabouts of them. By using a muster card reader, usually installed in a place that is safe, and having evacuees swipe their cards allows the system to register as having exited the building. In doing so, the system can be used to identify any users still remaining in the building.

Personal Identification Numbers (PINs) and Keypads

Card access can also be combined with PIN (personal identification number) code entry using a keypad device. You can assign users a PIN code in addition to access cards etc. This enables you to set up extra security, for example, swiping a card in conjunction with entering a PIN for access. In addition, you can assign these kinds of functions in accordance with time/door schedules, so that they are valid only during certain times of the day or on certain days. The system can also be programmed to allow PIN entry during certain modes only, or a combination of modes/times/days.

Interlocks

In some instances you may want to ensure that one door is closed before another is opened and vice-versa. For example, if there are two access controlled doors that lead to a high security area, you can interlock them so that no other person can open the first interlocked door whilst the second door is currently open. Once the second door is closed and locked, the first door can be opened again. Interlock doors from their associated reader configuration. Each card reader/door can be interlocked with up to eight others.

Note: When a door is interlocked, it can only be opened through the interlock functionality. That is, it will reject access and unlock commands or egress requests whilst interlocked. • Doors that are interlocked by another door, or are commanded into an interlocked state, will illuminate the red LED on their associated readers.

Anti-Passback

Anti-passback is a function that prevents users from being able to exit or re-enter through the previous door. In effect, anti-passback controls the direction of movement of users through one or more doors. When anti-passback is enabled, the system records the last 16 access cards used, and can optionally do so for a set amount of time. These access cards will not be allowed access again until they are no longer in the stored list, time-out, or are reset by using another card reader. There is also an option for clearing the card reader passback memory in other card readers, if the card is used in a particular reader.

With peer-to-peer communications between Controllers, Pacom access control has the ability for "global anti-passback". This is where the anti-passback can be reset using any card reader, including those connected to other Controllers.

Note: You can assign anti-passback functionality to standalone card readers only. In/out readers do not require anti-passback as they will generate an error if a card is used to attempt entry to the same area twice, without exiting.

Degraded Mode

Under normal operating conditions the Controller performs all access processing. Degraded mode operation is a function built in to Pacom door controllers that stores the last used access card data in on-board memory [non-volatile for some door controllers]. If the door controller becomes disconnected from the Controller and "degraded mode" operation is enabled for it, it will process access cards based on those stored in memory; that is, access cards in memory can be used in degraded mode operation. There are two forms of degraded operation.

- Option 1 - When the door controller first comes online, a "main" card is downloaded to the card reader and stored in non-volatile memory. If the door controller goes offline, the main card is always allowed access.
- Option 2 - As each valid transaction occurs while the door controller is online, the door controller stores a configurable part of the card data (facility code and/or issue number, or whole card number) in non-volatile memory, so that in degraded mode, any card that matches the data can be validated. Up to 256 cards can be stored in a 1064 door controller, and up to 1000 (500 per card reader) in 1076 two-door controllers (these values are based on the 26-bit Wiegand format. Higher bit counts reduce the maximum number), with the door controller checking to ensure that there are no repeated entries.

Duress

The concept behind "duress" is for users, if under threat or other unusual circumstance, to be able to discretely generate an alarm ["duress alarm"] without any obvious signs to an observer. Typically, when a user logs on in duress, all normal functions available to them during "normal" log on are retained. If a duress alarm is generated by accident, the monitoring center should be contacted as soon as possible as duress alarms are treated as an emergency. Different alarm panels may offer various means of generating duress alarms. For example, users entering a specific PIN.

Time Schedules and Calendar Holidays

Time schedules are programmed start and end times that you can apply to various functions in the system. Time schedules are represented in as "nodes"; meaning they can be used any number of times on applicable node types. For example, using time schedules to determine when users can gain access to the premises; when a card reader is locked or unlocked; automatically setting the alarm system mode, etc.

Note: For time schedules that apply to users, these are created and assigned using an access control management tool such as Pacom GMS software.

User Time Schedules

User time schedules define times of the day that users are able to access card readers. That is, if a card reader is available for use, however, it is a time of day that is outside of a user time schedule, then users assigned that time schedule will be denied access through the card reader. Pacom access control management systems [Pacom GMS software] allows for up to 100 user time schedules and up to three access intervals (start time to end time) per day [24 hours] that control when access is available. Each schedule entry has a start and end time for each day of the week (starting at Sunday). Holidays, which represent dates that the system is not to operate as per normal for that particular day of the week, are also programmable.

Calendar Holidays

Generally, there are dates throughout the year where the premises may require different operation to normal in that it requires to be secure instead of a "normal" unsecured or open condition. As an example, consider a work premises that is automatically disarmed on a Wednesday and all card readers and associated doors are unlocked at 09:00 (9AM) until 17:30 (5:30PM). Let us say that Christmas day happens to be on a Wednesday and nobody is required to work - the system would still disarm the premises and unlock card readers and doors as per any "normal" Wednesday, which is not desirable when no-one is there. Calendars provide a means for nominating dates where the alarm and/or access control system [based on card reader operation] is to operate differently. So in this instance, Christmas day (December 25) can be set in the calendar as a "holiday" and nominating an alternate schedule to apply. As each day starts, the system checks the current date and calendars automatically and if the date matches a date in the calendar set as a holiday, it applies the appropriate schedule.

The system provides three different settings that can be applied as "holidays". That is, you can have three different settings that can be applied to dates in the calendar. For example, one setting for holidays that require the premises to be secure for the full day and another for half day closures. Out of the three holiday type options, one ("Holiday 1") is available for alarm system use and all three ("Holiday 1", "Holiday 2" and "Holiday 3") are available for access control use. There are basically two calendar types available - one for the alarm system and one for access control. With alarm control, when a holiday is encountered ("Holiday 1" in the "alarm calendar") all usual alarm operation settings (mode switching, restricted access, etc) are overridden by the holiday time schedule. For example, if an alarm user is normally able to access the alarm system at a time of day that is currently over-ridden, they will not be able to unless they have outside hours access privileges.

Card Reader and Alarm Time Schedules

There is provision for up to 32 card reader time schedule profiles that you can use when selecting output activation, keypad operation, and locking and unlocking card readers. The time schedule determines when the applicable function, action or operation is available. For example, a time schedule that controls when a card reader becomes "unlocked" and, therefore, may be used for access by cardholders. Card reader time schedule profiles cannot be applied to alarm system users or card, only for

card reader related tasks. When setting up card readers, there are options for setting its operation during certain times.

Alarm time schedules are similar to those of card readers, however, operate across the whole site in terms of alarm user access to the alarm system. Common operation generally allows an alarm user to access one or more areas in the premises through a keypad in order to manually disarm the system. The ability of the user to do so is governed by the access settings for the area in question ("staff entry" time, "staff exit" time etc) except when the current date is one set to use the "Holiday 1" time schedule in the alarm calendar. When this occurs, all normal alarm user access settings are over-ridden and the alarm user is denied access until the time schedule passes or the alarm user has outside hours access privileges.

Maximum Users (Cardholders)

User access control is supported by all Pacom Controllers. Controllers store user information in on-board non-volatile memory, so the system can continue operation even if connection to the monitoring center is lost. Controllers have a finite amount of memory and can therefore store a finite number of users. The main factor in determining the best suited Controller for the application is the number of users that it needs to support.

You can expand Pacom Controller memory to increase the number of users supported by adding memory cards to the dedicated slot on the Controller PCB. Memory cards are proprietary Pacom hardware and must be purchased through Pacom.

Note: 1057 revision 5+ and 1058 revision 4+ are required for memory cards. If you place a memory card into an older revision Controller, it will operate, however, using 4MB of the available memory. • For Unison systems, the total number of users that can be stored in a Controller may vary depending on how "personal access" is configured 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, the means for 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.

Maximum Users/Access Cards

Configuration	1057	1058	8001/8002	8003
Standard (no expansion)	9235	1000	9235	1000
With 4MB expansion	32000	10000	N/A	N/A
With 16MB expansion	N/A	N/A	128000	N/A

With 32MB expansion	256000	10000	N/A	N/A
With 64MB expansion	N/A	N/A	256000	N/A
With 1GB SD expansion	N/A	N/A	N/A	500000

See Also: Alarm Control Guidelines | Managing Access Control and Users

---

You are here: Managing Access Control and Users > Access Groups

Access Groups

Access groups are collections of access schedules [and associated days and times per day] that define when users have access to doors and areas, and can be applied to multiple users. That is, an access group can be set up to include common doors, areas and associated access schedules that determine when users can enter/exit.

Management, Configuration and Commands

See Also: Access Schedules | Managing Access Control and Users | Users and Access Cards

---

You are here: Managing Access Control and Users > Access Schedules

Access Schedules

Access schedules define the times of day and days of the week when users are able to use access control nodes (doors, areas, elevators etc). This is in addition to the level of security or more required by the door schedule applicable to the time and day. For example, a user may have access to a door at any time of day and during any day of the week, however, the door schedule may require that during normal business hours Monday to Friday that an access card swipe is adequate security, and on weekends, an access card swipe and PIN entry is required. Access schedules are linked to doors, access groups or to user individual access levels.

Note: When using some third-party device integrations, such as Assa ARX or Traka, access schedule nodes that are compatible with the third-party system may be imported. For users of applicable third-party systems, the required access related nodes must be selected and applied to each user. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access permissions must include one or more Traka "security group" nodes in order to

use the Traka system.

Management, Configuration and Commands

See Also: Creating and Commanding Nodes | Managing Access Control and Users

---

You are here: Managing Access Control and Users > Calendars and Day Types

Calendars and Day Types

The calendar allows you to set "special" days, such as holidays, where the normal access control/alarm system behavior is to be overridden. Access control is normally stipulated through the concept of "day types"; for example, normal business days of Monday to Friday may use a particular day type because the premises is open to staff and customers for normal business activities, and weekend days may use a different day type because the premises is not open for business. Similarly, day types can be created for public holidays or days where special access control/alarm system behavior is required. These day types can be applied to any date of the year through the calendar.

For special day types, corresponding calendar entries can be added to specify the dates that apply the day type. For example, for an example "Public Holiday" day type, the calendar dates may include Easter, Christmas etc. Once special day types have been created, the necessary access times can be specified in the Access Schedules view, and the mode of access can be specified in the Door Schedules view.

Note: If a specific calendar selection is blank (that is, no calendar is selected for the day), then this day applies to all Calendars.

Day Type - Management, Configuration and Commands
Calendar - Management, Configuration and Commands

See Also: Access Schedules | Door Schedules | Managing Access Control and Users

---

You are here: Managing Access Control and Users > Card Layouts

Card Layouts

Card layouts represent the printed design for access cards. The layout may include things such as user photograph and other details, corporate logo, clearance level etc. Card designs can be created based on a pre-defined example layouts, or from an empty

"document". Once a card layout is saved, it can be used to create actual user access cards.

Note: The tools available in the Card Designer are proprietary and designed for multiple purposes [mainly report creation using data extracted from databases]. As a result, some tools or functions may not be considered appropriate to access card design. • For further information on card/report layout tools, refer to www.devexpress.com.

Layouts are based on the concept of "bands". Bands are special containers on the page that define areas of the layout that have certain properties or can hold certain types of objects. As a default, a "page" contains three bands - a band each for top and bottom areas, similar to the "header" and "footer" in a document [called "margins", but not to be confused with actual page margin settings], and a "detail" band that represents the "body" of the document/layout and the one generally used for containing the content or body of information.

- Card Layout Management
- Card Designer - Basic Functionality

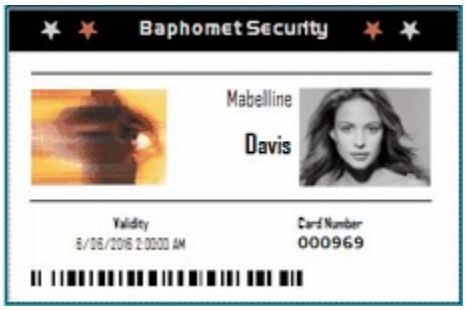
See Also: Card Layout Example | Managing Access Control and Users | Users and Access Cards

Card Layout Example

You are here: Managing Access Control and Users > Card Layouts > Card Layout Example

Card Layout Example

The following example procedure is a guide only and covers the most commonly used information that may be used on access cards. These are adding database fields for user name and photograph, card number and some graphic elements (shapes, images and lines). The following design shall be created:



Note: Many more database related information is available for use than is described in this procedure. However, an understanding of the Unison database structure is

required, which is beyond the scope of this documentation and would likely not be necessary for the majority of access card designs.

The card consists of the labels, shapes, lines, images, bar code, table, and database data for user information.

- Set basic card size and object layout controls:

  - Units of measurement are set to tenths of a millimeter.
  - Card dimensions are set as "550" high x "850" wide, with orientation set to landscape format. Note that settings may automatically be adjusted as the Card Designer uses pixel measurement as its basis.
  - The margins for the "paper" have been set all set to "0" as we want to be able to objects onto the layout that will reach to the very edges of the physical card. Padding is also set to "0".
  - The top and bottom margin bands have been reduced to a height of "0" as we do not require these bands for the access card.

Note: Using the header/footer bands changes the size of the card and its appearance regardless of the page dimension settings.

  - Grid size is set to "10" [1mm], with the snapping mode set to grid snap. These settings means that objects, when being "drawn" and moved, will automatically "snap" to the nearest grid point. The idea behind the grid is to make it easy to size and position objects with relation to common references [the "grid"].

- Create the "title" section:

  - Insert a label (). The label is "snapped to the grid so that its top edge aligns with the top of the card. The left and right edges are adjusted to reach the card edges. The bottom edge of the label is "pulled down" so that it is 10mm high. The label is formatted to be aligned middle-center with a foreground color [the text] of gray and a background color [fill color for the object] of black. The text is added and an appropriate font and size selected.
  - Insert a shape (). The shape is a five-pointed star, in a bounding container of 4mm x 4mm. The shape is rotated internally for the desired orientation and has a foreground set to gray and fill of black. The shape is copied to the clipboard and pasted into the layout three times, creating a total of four identical shapes. The shapes are selected together and aligned to their top edges then positioned horizontally using the grid for symmetrical placement. The two inner shapes are selected and a different fill color applied.

- Create the "body" section:

  - Insert a line (). The line has horizontal direction and a width of "3" and foreground color of black applied. The line is positioned 5 grid spaces below the bottom of the header section, and the end positions adjusted to be 5 grid spaces in

from the left and right edges of the card. The line is copied and pasted, with the second line positioned horizontally the same as the first, and 30 grid spaces below it.

- Insert an image ( ). The image container is selected and sized to 24 grid spaces high x 32 grid spaces wide and positioned so that it is aligned with the left-side end of the lines, and is vertically aligned centrally between the lines. The image URL is set so that the system can place the actual image when creating cards and, because the image is larger than the container object, is set to zoom so that the image scales proportionally to fit the container.
- Insert data fields for user information. Data fields mean that the contained information is inserted from the database for the required user when cards are created. Display the Field List ( ), expand the "Card" > "User" node then click and hold the mouse button down on the "FirstName" field then drag the mouse cursor over the layout and release the mouse button - the data field container is now on the layout. The object label shows the data field that it is associated with. Note the , indicating database derived contents. Do the same for the "LastName" and "Photo" fields. The "Photo" field container is positioned and sized so that it is aligned with the right-side end of the lines and is vertically aligned centrally between the lines also. The sizing is set to zoom so that the image scales proportionally to fit the container and is never distorted. The "FirstName" and "LastName" fields are positioned between the image and "Photo" field containers, one above the other and vertically sized as appropriate. The fields are formatted with font, style and size, and are right-aligned so they appear evenly next to the user photo [a gap of one grid line is between right edge of the fields and the photo field to visually separate them].
- Insert a table ( ). The table defaults to a single row and three columns. Two columns are required - right-click in a table cell and select Delete > Column from the context menu. Two rows are required - right-click in a table cell and select Insert > Row Below from the context menu. The table is now two rows of two columns. Hover the mouse button over the table until displays - click it to select the entire table - editing "handles" display at the corners and center of each edge. The left and right center handles are dragged so that they align with the left and right ends of the lines [the columns automatically adjust with to be equal width]. The height is adjusted using the top handle so that the table takes up 10 grid lines [the table auto-adjusts row height so each row = 5mm high]. With the table still selected, the mouse cursor is hovered over an edge until it becomes a four-pointed arrow - the mouse button is clicked and held then the table moved so that it is 2 grid spaces beneath the lower line. The top-left cell is double-clicked to select its text contents and the text edited to "Validity" as we want to show when the card is due to expire, and the font set. The same is performed on the top-right cell, with the text set to "Card Number" as we want to show that information on the card [these are, in effect, the table column headings]. In the Field List ( ), expand the "User" node then click and hold the mouse button down on the "ValidUntil" field then drag the mouse cursor over the bottom-left cell when displays next to the mouse cursor, release the mouse button - the data field is now contained within the table cell [to remove a data field from a cell, select the table cell, then click to display properties and for Data Binding, select None]. The cell label shows the

data field that it is associated with. Note the , indicating database derived contents. Do the same for the bottom-right cell using the "Card" node, "CardNumber" field. The two lower cells are formatted for font, style and size.

- Insert a bar code ( ). The bar code will be "bound" to the card number data so that the card can be identified using a bar code reader. The bar code container is selected and sized so that it is 5 grid spaces high and the left and right edges are aligned with the left and right ends of the lines, and positioned so its top edge is 2 grid spaces beneath the lower edge of the table. The object is right-clicked and Properties selected from the context menu to display the Properties panel, where its entire range of properties is displayed - the Show Text setting is set to No because we only want to show the bar code and not its alphanumeric version also [already shown in the table], and the Data Bindings > Text > Binding setting is set to Card - CardNumber. Note the , indicating database derived contents.

The layout should look something similar to:

Click (Preview) to show the card with actual data from the database [the database must have the required information in order to create the preview].

See Also: Card Layouts

You are here: Managing Access Control and Users > Card Profiles

Card Profiles

Card profiles represent the settings that are used by card readers for correctly interpreting access card data. Access cards use a variety of data combinations depending on the security required. That is, the more difficult it is to correctly read the access card, the more secure it is from being "skimmed" or "hacked". The system supports creating customizable access card profiles in order to work in conjunction with virtually any type of commercially available access card.

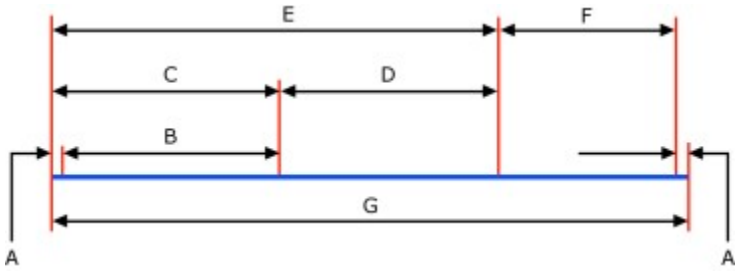
Generally, a card profile determines the length [number of bits] of the access card data, the position and length of the card identification number, facility code and issue or revision number and any parity checks. Card profiles are stored in the system database and are automatically downloaded to Controllers that require them. That is,

when a card reader is set up in a site and a card profile is selected for it, that profile is passed down to the Controller.

The following image show an example card profile for a card reader that outputs 34-bit (G) Wiegand and uses:

- A parity bit on either end of the key data (A).
- A 12-bit facility code (B).
- A 13-bit issue number offset (C).
- A 12-bit issue number (D).
- A 25-bit revision number offset (E).
- A 8-bit revision number (F).

Data field offsets are incremental. Each field offset must include any previous field offsets and lengths.



The system has several pre-defined profiles, such as I/O Prox, Mifare, Standard Magnetic, Wiegand 26-bit and Tagmaster. In certain cases it may be required that some data be static; that is, the same on all cards. Another part on the card may have a unique card number automatically assigned by the system, which is displayed to the operator creating the card. With some card types it may be required to split the data into several fields, for example, card number, system number and version number, which should be entered when cards are created. There is no limit to the number of card profiles that can be created.

Note: When using some third-party device integrations, such as Assa ARX or Traka, access card profiles for users of those systems must have access cards with the correct profile. For users of applicable third-party systems, the required access card profile must be used for encoding user access cards. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access card profile must match that used in the Traka system.

Management, Configuration and Commands

See Also: Managing Access Control and Users

You are here: Managing Access Control and Users > Door Schedules

Door Schedules

Door schedules define the security level mode required to gain access through doors for times of day and days of the week [in addition to the access schedule applicable to the time and day and day types as defined in calendars; for example, public holidays etc]. For example, a user may have access to a door at any time of day and during any day of the week, however, the door schedule security level mode may require that during normal business hours Monday to Friday that an access card swipe is adequate security, however, on weekends, an access card swipe and PIN entry is required. Door schedules are linked to doors.

The available security level mode options provide several options that can be used - from little or no security to more extreme measures, such as user authentication using access card, PIN as well as operator confirmation [perhaps using visual authentication by CCTV].

Note: Depending on which devices are in use, additional sub-types of "door" schedule may be available for use. For example, with some Pacom Controller hardware, specific schedule types for areas, egress buttons, doors etc can be used. This is because various hardware supports different features that are defined by access schedule. For example, the various "modes" that can be used to authenticate users at door, such as PIN before card etc. These additional options become visible when creating access schedules. • When using some third-party device integrations, such as Assa ARX or Traka, door schedule nodes that are compatible with the third-party system may be imported. For users of applicable third-party systems, the required access related nodes must be selected and applied to each user. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access permissions must include one or more Traka "security group" nodes in order to use the Traka system.

Management, Configuration and Commands

See Also: Managing Access Control and Users

You are here: Managing Access Control and Users > Doors and Card Readers

Doors and Card Readers

Doors and card readers are critical nodes/hardware required in an access control system. The two "devices" together create a physical environment where door lock operation can be controlled through card reader data being processed by the system.

Similarly, alarm operation relies on one or more sensors attached to the door/card reader hardware that can detect attempted intrusions.

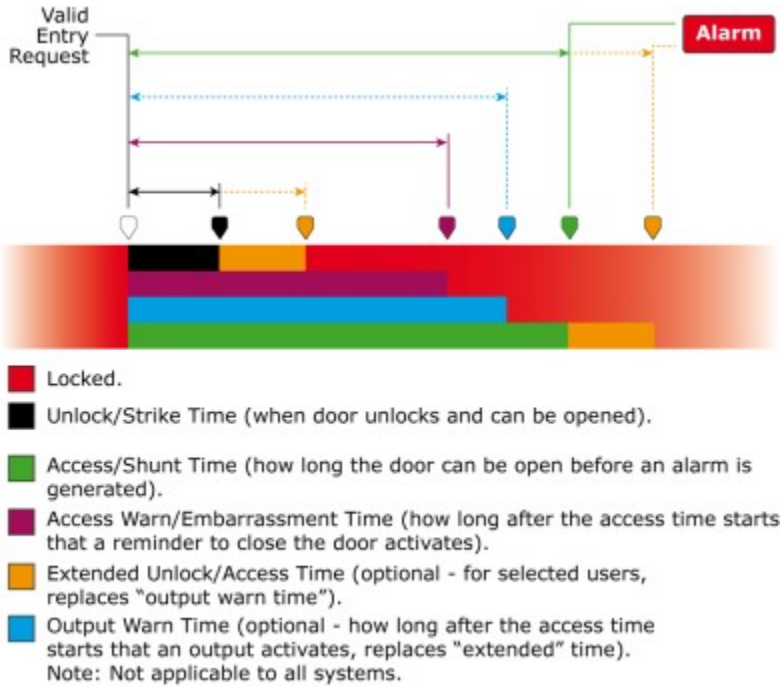
Door Open/Close Sequence

Door operations, which are basically the process of unlocking and locking, are time based. Time must be used to accurately control doors in a secure environment and to determine when the use of a door is abnormal and an alarm should be generated. The following example shows the basic times for access control for a door controlled by a Pacom Controller Network device:

Note: Available settings depend on the connected hardware - refer to topics for specific devices for related door configuration information.

- When the door is available to be unlocked/opened.
- Once unlocked, how long the door can remain unlocked.
- How long the door can remain open in total.
- How long after unlocking and opening that users can be reminded to close the door.

The following image shows the basic door open/close operation.



Door - Management, Configuration and Commands

The Doors view enables managing door configurations.

Note: Due to the system requiring information regarding door and associated hardware for configuration purposes, door nodes must be created using the Hardware view before they can be accessible through the Doors view.

Click  (Doors) in the Access Control Administration ribbon bar to open the Doors view. Once a node has been created, it is listed in the Explorer, with its settings available in the Properties section.

Note: Available settings depend on the connected hardware - refer to topics for specific devices for related door configuration information.

Commands

Commands can be sent by selecting the required door and clicking  (Commands) in the view toolbar. This function can also be accessed by right-clicking the node and selecting Commands from the context menu. The commands available depend on the type of device and associated hardware. For descriptions of events, refer to the relevant device driver information; for example, for doors connected to a Pacom Controller, refer to the "Pacom Controller Network" device driver.

Card Reader - Management, Configuration and Commands

The Card Readers view enables managing card reader configurations.

Note: Due to the system requiring information regarding the actual card reader and associated hardware for configuration purposes, card reader nodes must be created using the Hardware view before they can be accessible through the Card Readers view.

Click  (Card Readers) in the Access Control Administration ribbon bar to open the Card Readers view. Once a node has been created, it is listed in the Explorer, with its settings available in the Properties section.

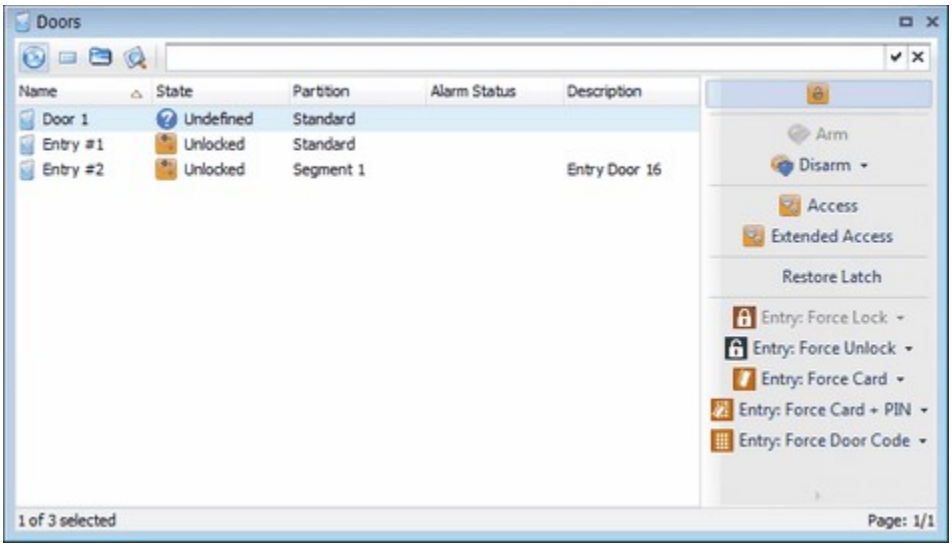
Note: Available settings depend on the connected hardware - refer to topics for specific devices for related card reader configuration information.

Commands

Commands can be sent by selecting the required card reader and clicking  (Commands) in the view toolbar. This function can also be accessed by right-clicking the node and selecting Commands from the context menu. The commands available depend on the type of device and associated hardware. For descriptions of events, refer to the relevant device driver information; for example, for card readers connected to a Pacom Controller, refer to the "Pacom Controller Network" device driver.

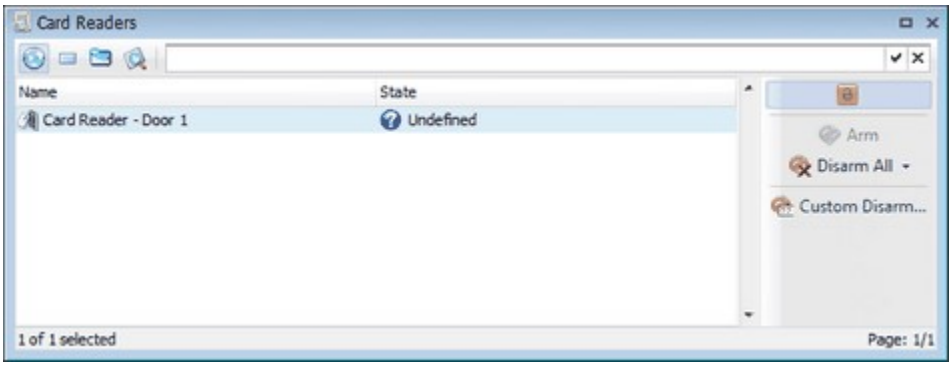
Door - Monitoring

The Doors panel [which is basically a Nodes panel, however, listing door nodes only] enables monitoring door status and events. For example, to view all unlocked doors, etc. Click  (Nodes > Doors) in the Panels ribbon bar to open the Doors panel. Normal node filtering functions and commands for listed nodes are available.



Card Reader - Monitoring

The Card Readers panel [which is basically a Nodes panel, however, listing card reader nodes only] enables monitoring card reader status and events. For example, to view all unlocked card readers, etc. Click  (Nodes > Card Reader) in the Panels ribbon bar to open the Card Readers panel. Normal node filtering functions and commands for listed nodes are available.



See Also: Devices - Driver Configuration | Door Schedules | Managing Access Control and Users

---

You are here: Managing Access Control and Users > User Areas

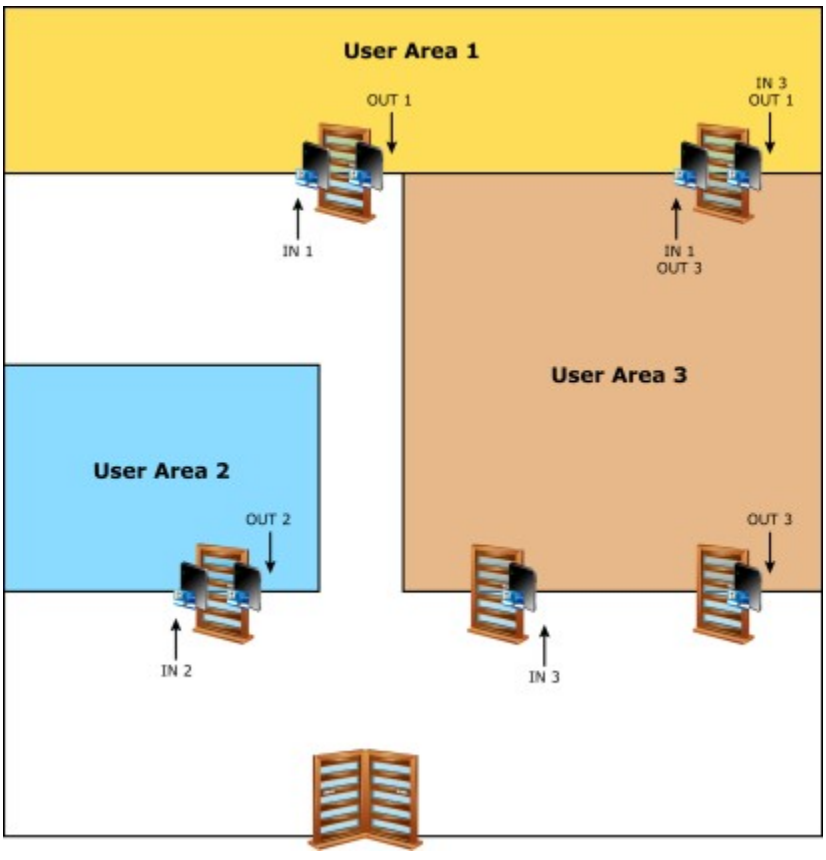
User Areas

User area nodes are used to register the location of users within a premises. That is, the system registers the movements of users in user areas so that it is possible for operators to see the users in any given user area. The system is able to use the count in expressions [also known as "macros"] for automating functions etc. User area door nodes use "in" and "out" card readers to provide the counting mechanism data - the system processes valid access events from "in" card readers to register users entering

the area; similarly, "out" card readers are used for counting users exiting the area. As an example of use, in the event of an emergency that requires evacuation, it will be a simple task to be able to find out the users remaining inside and where they are currently located.

The illustrated example below is a premises that contains three user areas and has a connecting floor area that is not counted [a "public" area that is not access controlled]. In it:

- User area 1 has two doors - one door with "in" and "out" card readers that counts users entering/exiting area 1; one door with "in" and "out" card readers that counts users entering/exiting areas 1 and 3.
- User area 2 has a single door with "in" and "out" card readers that counts users entering/exiting area 2.
- User area 3 has three doors - one door with an "in" card reader that counts users entering area 1; one door with an "out" card reader that counts users exiting area 3; one door with "in" and "out" card readers that counts users entering/exiting areas 1 and 3.



Use the User Areas view to manage user areas [can also be done using the Hardware view, "System" node, User Areas folder] and the User Areas panel for viewing users located in areas.

Management, Configuration and Commands
User Areas Panel

See Also: Creating and Commanding Nodes | Managing Access Control and Users

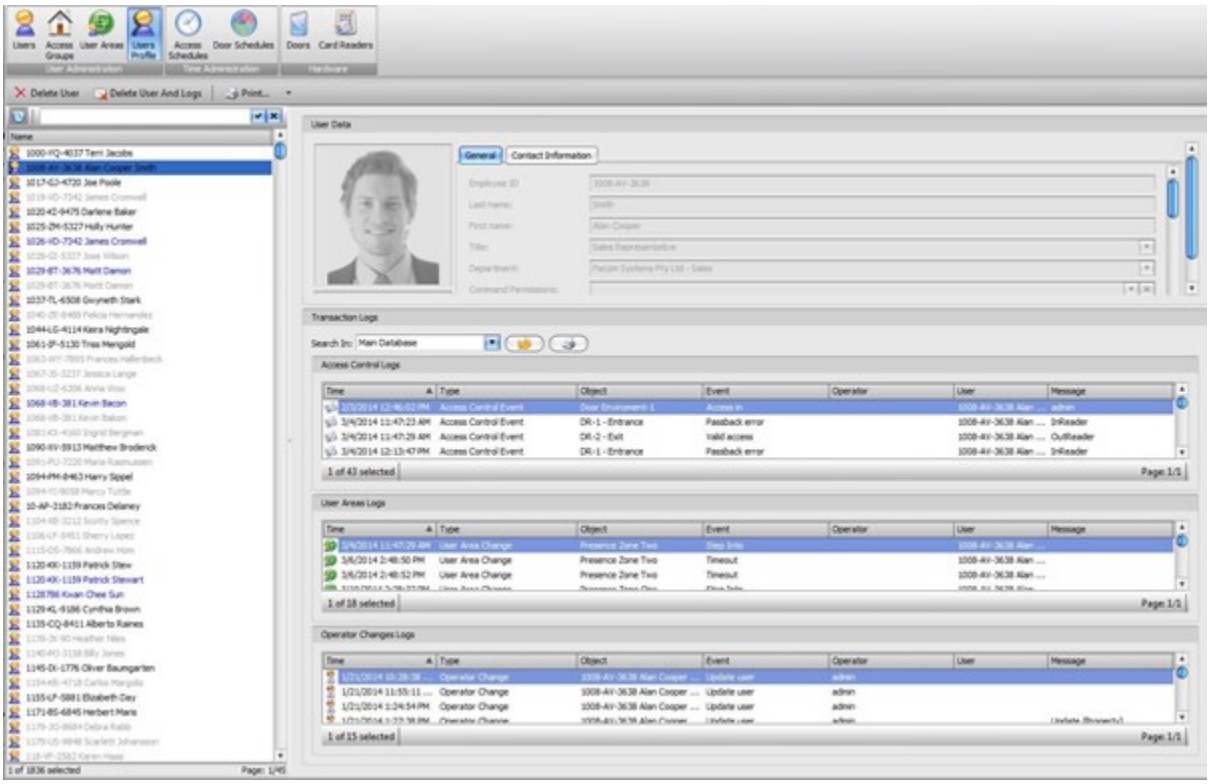
---

You are here: Managing Access Control and Users > Users Profile

Users Profile

The Users Profile view provides operators with a holistic view of users. It provides information on the user, plus all of the transaction logs related to that user. Within the page, operators are able to:

- View stored information on active users, inactive users, and deleted users that still have transaction logs
- Print reports on users and transaction logs
- Delete users
- Delete users and all associated transaction logs.



Management, Configuration and Commands

See Also: Users and Access Cards | Managing Access Control and Users

You are here: Managing Access Control and Users > Users and Access Cards

Users and Access Cards

Users are employees and other persons who use access cards for entry/exit through doors, use elevators etc within the site. When creating users, the following can be configured:

- Access groups with defined access to different doors.
- Personal/individual access.
- Access cards for each user.
- Photos.
- Signatures.

Note: User data, access settings or access card data formats require specific configuration for some device drivers. That is, some settings "normally" used for defining user access are either mandatory or may not be required, or additional settings may apply. Refer to device topics for details. Device drivers that affect user access settings are Assa ARX, Salto and Schindler PORT. • When using some third-party device integrations, such as Assa ARX or Traka, access schedule nodes that are compatible with the third-party system may be imported. For users of applicable third-party systems, the required access related nodes must be selected and applied to each user. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access permissions must include one or more Traka "security group" nodes in order to use the Traka system.

Management and Configuration

See Also: Bulk Updating Users | Configuring the System | Creating and Managing User Access Cards | Managing Access Control and Users | Using Real-Time Transactions Panels | Using Transaction Logs

Bulk Updating Users

Creating and Managing User Access Cards

You are here: Managing Access Control and Users > Users and Access Cards > Bulk Updating Users

Bulk Updating Users

The bulk update tool is used for changing some properties for multiple users in a

single operation. To begin the bulk update process, click (Bulk Update) in the Users view toolbar then select the type of property to update. Options are:

- Properties
  - User Data - Change various user data properties.
  - Partition - Change user partition.
  - Folder - Change user folder.
- Permissions
  - Add Access Group - Add access group(s) to the user's existing access group permissions.
  - Remove Access Group - Remove access group(s) from the user's existing access group permissions.

Changing Properties
Changing Permissions

See Also: Using Partitions | Users and Access Cards

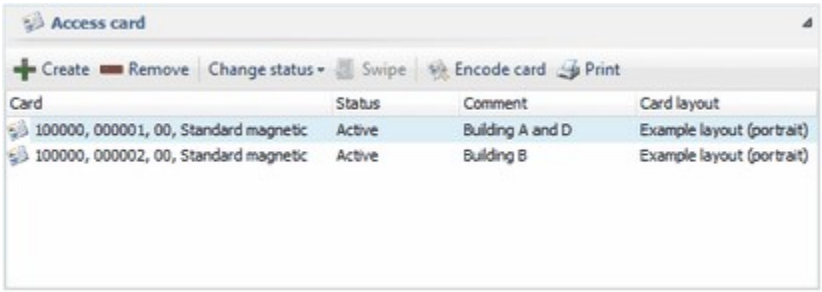
You are here: Managing Access Control and Users > Users and Access Cards > Creating and Managing User Access Cards

Creating and Managing User Access Cards

User access cards are a property of user nodes; that is, they are part of a user entity. Users can have any number of cards associated with them. Access cards can either be created manually and then encoded, or by using a card reader to "enroll" an existing access card. When creating cards manually, card data needs to be entered by operators and then the card is encoded. When creating cards using a card reader, card data is read directly from the card via the card reader and registered in the system.

Note: The visual appearance of printed access cards is controlled by the card layout. The system provides a default layout, however, custom layouts can be created and applied. • Changes to user data are not stored in the database until the user is saved. • When using some third-party device integrations, such as Assa ARX or Traka, access schedule nodes that are compatible with the third-party system may be imported. For users of applicable third-party systems, the required access related nodes must be selected and applied to each user. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access permissions must include one or more Traka "security group" nodes in order to use the Traka system. • For Assa ARX system users, the Unison system does not currently support reading access card data from an ARX card reader when creating users via the Create Card wizard. The access card data must be set manually.

The Users view, Properties tab, Access Card region enables creating/configuring/modifying/deleting user access cards.



Control	Description
Access Card	

Create - Opens the Create Card wizard, Create New Card screen, where you can select the card creation method and begin the creation process.

Select the creation method as required. Click an option to select it:

- Create Card Manually - Requires card number data to be entered manually.
- Read Card from Card Reader - Applies card number data already encoded into the card.

Click Next to move to the next stage of the wizard.

Click here for manual creation instructions.
Click here for creating from a card reader.

Remove - Removes the currently selected access card from the user. That is, the access card exists in the system, however, is not associated with a user.

Sets the access card status in the system. To edit, click ▾ to display available options. Click an option to select it:

Change Status

- Active - Sets the access card for normal use; that is, it can be used for entry/exit etc.
- Blocked - Sets the access card to be denied; that is, it cannot be used for entry/exit. This status is generally assigned to access cards that are not to be used. If an attempt is made to use the access card, the transaction log will show an access denied - card blocked, or similar, message.
- Lost - Sets the access card to be denied; that is, it cannot be used for entry/exit. This status is generally assigned to access cards that are considered temporarily lost. If an attempt is made to use the access card, the transaction log will show an access denied - card lost, or similar, message. This may help trace attempted use of a lost access card.
- Canceled - Sets the access card to be denied; that is, it cannot be used for entry/exit. This status is generally assigned to access cards that are no longer in use. If an attempt is made to use the access card, the transaction log will show an access denied - card canceled, or similar, message. This may help trace attempted use of a canceled access card.


Swipe - Create another access card by reading a card by swiping it against a card reader previously used to read data through the Create Card wizard and opens the Create Card wizard at the Reading Card Data screen. When a card reader is nominated for reading card data, it is saved by the system for creating other access cards. This means that (Create) does not need to be clicked - it is enough to click  (Swipe). This also applies when switching to another user.

Encode - Writes the data for the currently selected access card to a physical card using an encoding device - opens the Create Card wizard at the Choose Card Encoder screen - select an encoding device [for example, a Fargo printer], then click Next. The Card Encoding in Progress screen 
displays, showing the encoding progress; when complete, click Next.

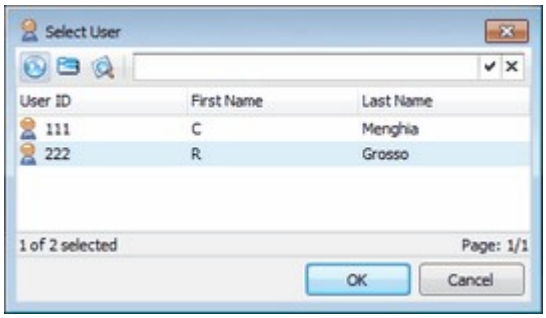
Note: A suitable encoding device must be already installed on the system. • This method is generally used when card data is created initially without being actually encoded to a card or a new card is required for existing card data, such as replacing a faulty access card.

Print - Prints the required card design for the currently selected access card to a suitable print device - opens the Create Card wizard at the Print Card screen - click ... in the Card Layout list to display available layouts (designs). Click an option to select it. A preview of the printed card 
appearance displays in the Preview region. Click Next. A Windows Print dialog box opens, where you can select the required printer, then click OK to proceed.

Note: A suitable print device must be already installed on the system.

Transfer - Opens the Select User dialog box, where you can select a different user to associate with the current access card. Once transferred, the previous user is no longer associated with the access card. This facility simplifies assigning existing access cards between users. For example, if

one user no longer requires a card and another user requires one. Click here for help.



Control	Description
OK	Apply any changes and close the panel or dialog box.
Cancel	Discard any changes and close the panel or dialog box.
User List	Sets the user to transfer the access card to. Click a user to select it.

Access Card Table for Users - Once a card is created for a user, card information is displayed in the table. Some properties can be edited directly from the table.

Note: As per any node, related event transaction information can be accessed by right-clicking the node in the table and selecting Transactions > Access Control from the context menu.

Card	Shows the access card system number [first number], card number [second number], and card data profile. This is for information only and cannot be edited.
Status	Shows the current access card status. To edit, click the field to display options. Click an option to select it.
Comment	Sets additional descriptive text for the access card; for example, for comments or useful information/details, if required. To edit, click the field to display a text entry box; enter the required text [carriage returns can be used] then click OK to apply it.
Card Layout	Shows the current access card layout (design), if any. To edit, click the field then click ... to display options. Click an option to select it. To delete the layout, click X.

See Also: Users and Access Cards

You are here: Managing Access Control and Users > Users and Access Cards

Users and Access Cards

Users are employees and other persons who use access cards for entry/exit through doors, use elevators etc within the site. When creating users, the following can be configured:

- Access groups with defined access to different doors.
- Personal/individual access.
- Access cards for each user.
- Photos.
- Signatures.

Note: User data, access settings or access card data formats require specific configuration for some device drivers. That is, some settings "normally" used for defining user access are either mandatory or may not be required, or additional settings may apply. Refer to device topics for details. Device drivers that affect user access settings are Assa ARX, Salto and Schindler PORT. • When using some third-party device integrations, such as Assa ARX or Traka, access schedule nodes that are compatible with the third-party system may be imported. For users of applicable third-party systems, the required access related nodes must be selected and applied to each user. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access permissions must include one or more Traka "security group" nodes in order to use the Traka system.

Management and Configuration

See Also: Bulk Updating Users | Configuring the System | Creating and Managing User Access Cards | Managing Access Control and Users | Using Real-Time Transactions Panels | Using Transaction Logs

Bulk Updating Users

Creating and Managing User Access Cards

You are here: Managing Access Control and Users > Users and Access Cards > Bulk Updating Users

Bulk Updating Users

The bulk update tool is used for changing some properties for multiple users in a single operation. To begin the bulk update process, click (Bulk Update) in the Users view toolbar then select the type of property to update. Options are:

- Properties
  - User Data - Change various user data properties.
  - Partition - Change user partition.
  - Folder - Change user folder.
- Permissions
  - Add Access Group - Add access group(s) to the user's existing access group permissions.
  - Remove Access Group - Remove access group(s) from the user's existing access group permissions.

Changing Properties
Changing Permissions

See Also: Using Partitions | Users and Access Cards

You are here: Managing Access Control and Users > Users and Access Cards > Creating and Managing User Access Cards

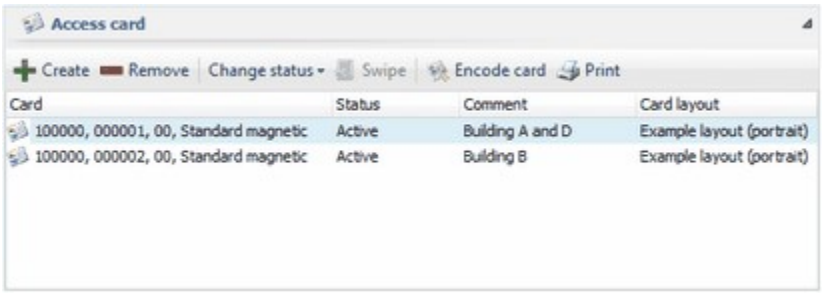
Creating and Managing User Access Cards

User access cards are a property of user nodes; that is, they are part of a user entity. Users can have any number of cards associated with them. Access cards can either be created manually and then encoded, or by using a card reader to "enroll" an existing access card. When creating cards manually, card data needs to be entered by operators and then the card is encoded. When creating cards using a card reader, card data is read directly from the card via the card reader and registered in the system.

Note: The visual appearance of printed access cards is controlled by the card layout. The system provides a default layout, however, custom layouts can be created and applied. • Changes to user data are not stored in the database until the user is saved. • When using some third-party device integrations, such as Assa ARX or Traka, access schedule nodes that are compatible with the third-party system may be imported. For users of applicable third-party systems, the required access related nodes must be selected and applied to each user. For example, if a user is required to have access to assets controlled by a Traka key management system, then the user's access permissions must include one or more Traka "security group" nodes in order to use the Traka system. • For Assa ARX system users, the Unison system does not currently support reading access card data from an ARX card reader when creating users via the

Create Card wizard. The access card data must be set manually.

The Users view, Properties tab, Access Card region enables creating/configuring/modifying/deleting user access cards.



Control	Description
Access Card	

Create - Opens the Create Card wizard, Create New Card screen, where you can select the card creation method and begin the creation process.

Select the creation method as required. Click an option to select it:

- Create Card Manually - Requires card number data to be entered manually.
- Read Card from Card Reader - Applies card number data already encoded into the card.

Click Next to move to the next stage of the wizard.

Click here for manual creation instructions.
Click here for creating from a card reader.

Remove - Removes the currently selected access card from the user. That is, the access card exists in the system, however, is not associated with a user.

Change Status

Sets the access card status in the system. To edit, click ▾ to display available options. Click an option to select it:

- Active - Sets the access card for normal use; that is, it can be used for entry/exit etc.
- Blocked - Sets the access card to be denied; that is, it cannot be used for entry/exit. This status is generally assigned to access cards that are not to be used. If an attempt is made to use the access card, the transaction log will show an access denied - card blocked, or similar, message.
- Lost - Sets the access card to be denied; that is, it cannot be used for entry/exit. This status is generally assigned to access cards that are considered temporarily lost. If an attempt is made to use the access card, the transaction log will show an access denied - card lost, or similar, message. This may help trace attempted use of a lost access card.
- Canceled - Sets the access card to be denied; that is, it cannot be used for entry/exit. This status is generally assigned to access cards that are no longer in use. If an attempt is made to use the access card, the transaction log will show an access denied - card canceled, or similar, message. This may help trace attempted use of a canceled access card.


Swipe - Create another access card by reading a card by swiping it against a card reader previously used to read data through the Create Card wizard and opens the Create Card wizard at the Reading Card Data screen. When a card reader is nominated for reading card data, it is saved by the system for creating other access cards. This means that (Create) does not need to be clicked - it is enough to click  (Swipe). This also applies when switching to another user.

Encode - Writes the data for the currently selected access card to a physical card using an encoding device - opens the Create Card wizard at the Choose Card Encoder screen - select an encoding device [for example, a Fargo printer], then click Next. The Card Encoding in Progress screen displays, showing the encoding progress; when complete, click Next.

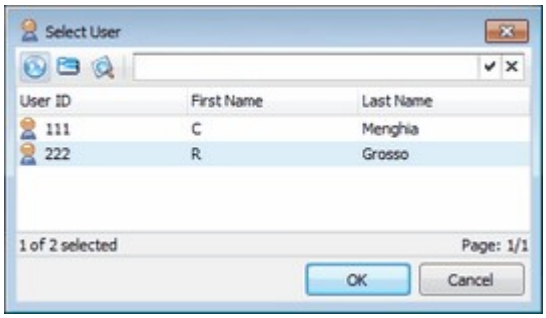
Note: A suitable encoding device must be already installed on the system. • This method is generally used when card data is created initially without being actually encoded to a card or a new card is required for existing card data, such as replacing a faulty access card.

Print - Prints the required card design for the currently selected access card to a suitable print device - opens the Create Card wizard at the Print Card screen - click ... in the Card Layout list to display available layouts (designs). Click an option to select it. A preview of the printed card appearance displays in the Preview region. Click Next. A Windows Print dialog box opens, where you can select the required printer, then click OK to proceed.

Note: A suitable print device must be already installed on the system.

Transfer - Opens the Select User dialog box, where you can select a different user to associate with the current access card. Once transferred,

the previous user is no longer associated with the access card. This facility simplifies assigning existing access cards between users. For example, if one user no longer requires a card and another user requires one. Click here for help.



Control	Description
OK	Apply any changes and close the panel or dialog box.
Cancel	Discard any changes and close the panel or dialog box.
User List	Sets the user to transfer the access card to. Click a user to select it.

Access Card Table for Users - Once a card is created for a user, card information is displayed in the table. Some properties can be edited directly from the table.

Note: As per any node, related event transaction information can be accessed by right-clicking the node in the table and selecting Transactions > Access Control from the context menu.

Card	Shows the access card system number [first number], card number [second number], and card data profile. This is for information only and cannot be edited.
Status	Shows the current access card status. To edit, click the field to display options. Click an option to select it.
Comment	Sets additional descriptive text for the access card; for example, for comments or useful information/details, if required. To edit, click the field to display a text entry box; enter the required text [carriage returns can be used] then click OK to apply it.
Card Layout	Shows the current access card layout (design), if any. To edit, click the field then click ... to display options. Click an option to select it. To delete the layout, click X.

See Also: Users and Access Cards

Using Real-Time Transactions Panels

There are two "real-time" transaction panels that display events as they occur in the system - *Real-Time Access Control Transactions* and *Real-Time Alarm Transactions* panels. This enables operators to monitor events in the system, and respond as required. Queries cannot be created using real-time transaction logs, however, basic filtering can be used within to enable the required transactions only to be displayed.

> **Note**: When a real-time transaction panel is opened, it will initially contain no data. As events/transactions occur, they appear in the panel. If the panel is closed, data being displayed at the time of closure is cleared [not deleted - all transactions and events are recorded in the logs]. • Real-time transaction logs cannot be used to search for historical events. Use transaction logs views to conduct historical searches.

See Also: Creating and Commanding Nodes | Creating Reports | Using Common Functions (Advanced Filtering) | Using Transaction Logs

Using Integrated Video

Video surveillance is useful for both access control and alarm management functions. Depending on the installed devices, camera systems etc, various ways of integrating with the Unison system are available. For example, providing live video footage to operators through the *Alarm Management* dialog box when responding to alarms, or being able to select a camera in a site map and display footage from it as required. The system supports multiple DVR and camera systems.

Most supported video devices are by way of specific device drivers [for example, Milestone] that can be installed as required. The "integrated video" device, however, is used to run the *Integrated Video* application that enables additional DVR/camera support external to the Unison system. The *Integrated Video* application must be installed on each Unison client machine that is to use it, and is activated by the Unison client. Similarly, the *Integrated Video* application "plug-in" for required DVR/NVR/camera systems must also be installed on each Unison client machine. The required settings for which camera to stream video from etc are defined within Unison as "camera" and "view" nodes. These nodes are child nodes to the integrated video device node. Once the *Integrated Video* application is running, operators have a range of controls available, including camera orientation, camera selection etc. More than one instance of the *Integrated Video* application can run simultaneously. For installation instructions, refer to the *Integrated Video* application installer [download it from the Pacom website - www.pacom.com or Pacom FTP site - ftp.pacom.com].

> **Note**: The integrated video device driver does not currently support receiving alarms from DVR/NVR systems. Some video systems are supported with specific device drivers [for example, Milestone] that provide increased functionality, such as alarms etc. With "full" device driver support, additional functions of the Unison system can be used, such as alarm actions. • Sending commands from the Unison system to the DVR/NVR system is not fully supported - each DVR/NVR will have some commands available, but generally not all possible commands as supported by their native management application software. • Previous versions of Unison may have used the "generic video" device driver. The integrated video device driver in the Unison system and the associated *Integrated Video* application replaces the previous generic video device driver. On upgrading, existing generic video nodes are replaced as integrated video nodes so that the system functionality is not disrupted.

The following nodes and parent folders [automatically created] are supported:

- Integrated video device - Provides system functionality for starting and interacting with the Integrated Video application.
- Video - Represents camera hardware managed by the applicable DVR system. Each video node is a connection to a camera that can be commanded to display video. When the "play live video" or "play recorded video" command is sent, the Integrated Video application opens and displays video from the associated camera. Camera hardware and/or associated DVR system may or may not support specific features, such as "PTZ" [pan/tilt/zoom], audio functions etc.
- View - Represents the visual layout [default cameras, multi-camera views etc] for one or more video nodes. That is, a view is a means of accessing multiple video nodes to display simultaneously in a single instance of the *Integrated Video* application as a "grid" of displays. For example, four different cameras displays in a two-column, two-row layout. This is a convenient way of streaming video surveillance; for example, creating views that display video from related cameras so that the progression of actual events are easily followed by operators, or for monitoring entry doors etc. Before creating views, create all required video nodes first.

Device - Management, Configuration and Commands
Video - Management, Configuration and Commands
View - Management, Configuration and Commands
Programming Example
Integrated Video Application - Controls

See Also: Alarm Response/Management | Creating and Commanding Nodes | Nodes - Definition and Use

You are here: Using Site Map Graphics

Using Site Map Graphics

The system has a Graphics Editor for creating and editing graphics, such as "site maps". Site maps are generally floor layouts that operators display using the Graphics panel and use for identifying locations of alarms points, areas, doors etc that are under system management and for indicating node and alarm/event status. In this way, operators have an easily understood, real-time overview of what is happening in a site. The Graphics Editor provides a range of tools for creating shapes etc and can be used to import XAML, DXF or DWG CAD drawings.

Note: The Graphics Editor is not intended to replace a professional drawing tool such as AutoCAD.

Any graphic can be made to be "interactive" with the Unison system. This means showing alarms and other events in site maps, and may be set up so that operators can respond to alarms and events directly from them. For example, you can double-click an unacknowledged alarm on a map to display a new instance of the Alarm Details panel that will automatically close when the alarm is closed.

Graphics support the concept of an "overview", which is a link that can be used to quickly switch between several graphics. For example, a site map of a large building [the "overview"] and several graphics linked to it, each representing a portion of the building with greater detail.

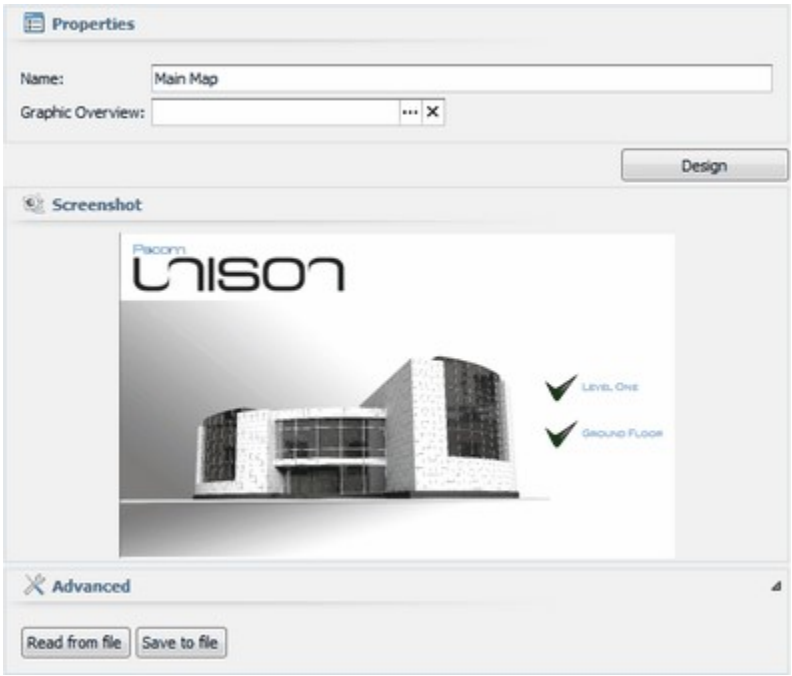
For maximized graphic rendering performance, it is possible to nominate graphic files to be "pre-loaded" into Unison client machines when an operator logs on. This means that accessing the server for graphics is no longer required when the graphic to be displayed; for example, the site map being loaded due to an alarm. This is beneficial for installations that use large size or highly complex site maps. The graphics selected for "pre-loading" is determined by operator group. Any graphics that are used which are not pre-loaded are sent from the Unison server to the required client machine(s) when required.

Note: When site maps are printed using the "alarm report (detailed with site map)" the canvas size determines the overall size of the site map. In other words, empty space around objects is included. This means that a large canvas with a small amount of space used for the graphical content will print "small". When site maps are printed as part of alarm type reports, the site map is automatically scaled to fill as much of the space available for printing the site map. Site map enlargement can also be implemented using the "scale" property for the "graphicalMapLinkControl" report object. Scale values increment by 50% of the "normal" size; that is, "1" [100%], 1.5" [150%], "2" [200%] etc. When site maps are enlarged in this way, the node in

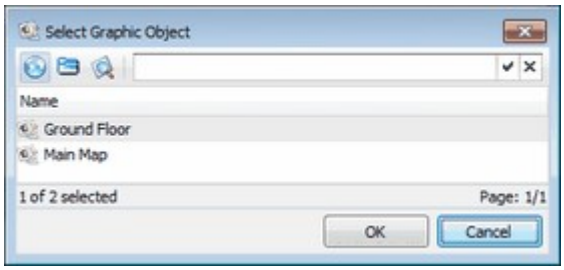
alarm is centered and parts of the site map that are outside the available space are not printed.

Graphics Management

Graphics and site maps are managed in the Graphics view. Click (Graphics) in the System Configuration ribbon bar to open the view. Click (Create) in the view toolbar to create a node. Once a node has been created, it is listed in the Explorer, with its settings available in the Properties section. The Screenshot region displays a preview of the graphic. To open the Graphics Editor, click Design.



Control	Description
Properties - One or more "generic" node properties apply. Click here for help. Additional properties, if any, are listed below.	
Graphic Overview	Sets another graphic node to associate with as the "overview" graphic. To edit, click ... - the Select Graphic Object dialog box opens, where you can select a graphic node.



Control	Description
OK	Apply any changes and close the panel or dialog box.
Cancel	Discard any changes and close the panel or dialog box.

Graphics List	Sets a graphic to be associated as the "overview graphic". A single graphic only can be set. To edit, click an option to select it.

Design	Opens the Graphics Editor with the current image loaded.
Screenshot - **Advanced**	Displays a preview of the graphic as it is currently saved.

Note: Graphics exported from one system and imported into another do not retain node connections.

Read from File	Opens a Windows Open dialog box, where you can navigate to, and select an existing graphic file to save in the Unison system. XAML files only are supported.
Save to File	Opens a Windows Save As dialog box, where you can navigate to a location and set a name to save the current graphic externally to the Unison system. XAML files only are supported.

See Also: Alarm Response/Management | Configuring Roles, Operator Groups and Operators | Graphics Editor

Graphics Editor

Graphic Templates

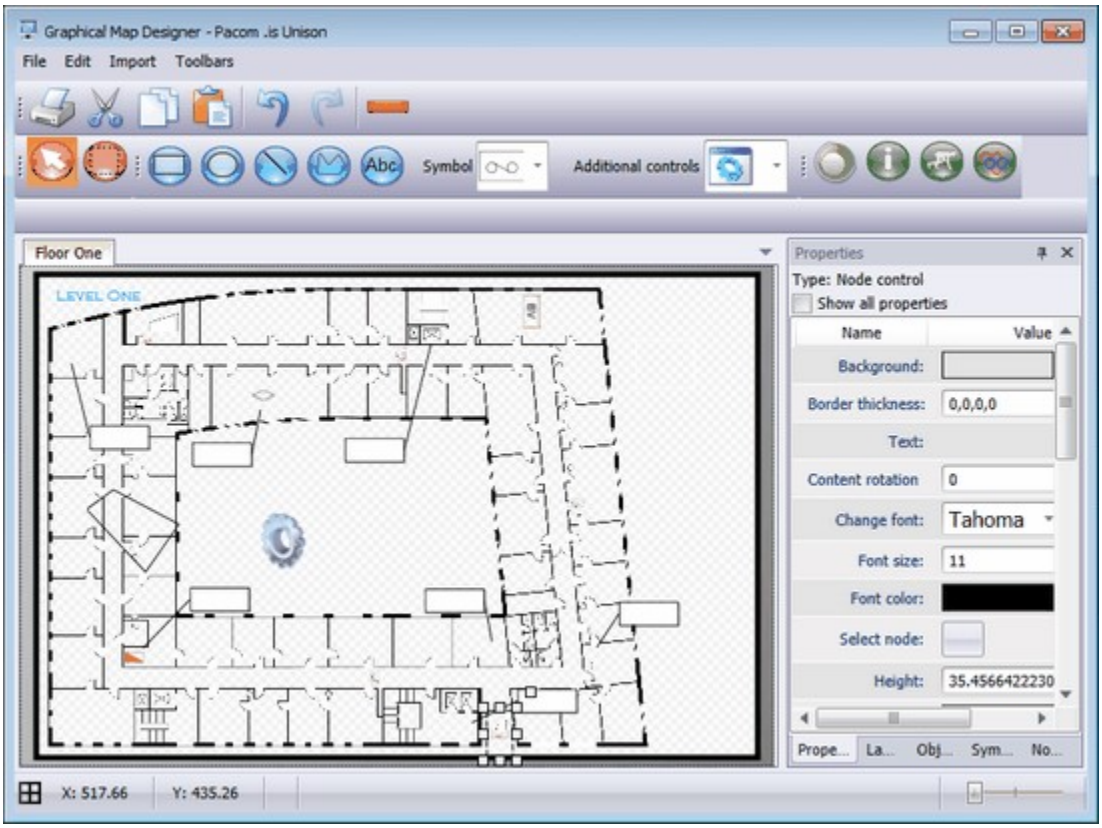
You are here: Using Site Map Graphics > Graphics Editor

Graphics Editor

The Graphics Editor is used for creating and editing site maps and other graphics that are displayed to operators through the Graphics panel. Any changes made to graphics must be saved using the Graphics view. Node "connections" to graphic objects provide additional functionality within the graphic; for example, visual node status and alarm indications, alarm response, area control, multimedia resources, commands etc. Node connections can generally be created using a:

- Symbol - A symbol is a special graphics object that is specifically for a node connection that is not actually part of the graphic.
- Object - Use an existing object in the graphic [shapes, lines etc] as a means for making a node connection.

To open the Graphics Editor, select a graphic in the Graphics view, then click Design in its Properties region.



The Graphics Editor includes the following tools:

- Menu Bar - Provides access to functions and tools using traditional menu selection [File, Edit etc].
- Toolbar - Provides access to [most] functions and tools using "buttons" [ ,  etc].
- Canvas - The "canvas" is the main area of the screen area to view, edit and create graphic content.
- Panels - The panels area is a separate section of the screen that is used to display panels for setting various object and drawing options [Layers, Properties etc].
- Status Bar - Provides access to the following drawing tools:
  - ⊞ - Show Grid Lines - Shows/hide lines in the drawing area for aligning/placing objects. When grid lines are displayed, objects "snap" to them.
  - Coordinates - Displays the mouse cursor position in relation to the top-left corner.
- Magnification and Panning - Use the mouse wheel to change magnification of the canvas ["zoom in/out"]. When zoomed in, use the scroll bars to the bottom and right of the canvas to move the display to different parts of the canvas.
- Object Default Properties - Provides "default" settings that apply to objects automatically when created, such as fills, borders, sizes etc. This enables faster "drawing" time and better consistency. These properties can be overridden at any time using the standard properties for an object.

Drawing Controls and Functions
Panel Functions

See Also: Alarm Response/Management | Importing CAD Drawings and Auto-Connecting Nodes | Site Map Example | Using Site Map Graphics

Importing CAD Drawings and Auto-Connecting Nodes

Site Map Example

You are here: Using Site Map Graphics > Graphics Editor > Importing CAD Drawings and Auto-Connecting Nodes

Importing CAD Drawings and Auto-Connecting Nodes

Computer aided design (CAD) drawings can be imported into Unison and connected to nodes within the system. When importing CAD drawings, the original layers can be included or excluded from the import as required. Standard symbols used in the CAD drawings can also be mapped to node types within the Unison system to automate connection between drawing symbols and existing nodes in the Unison system. The importation process may save time and increase accuracy because site map node connections do not need to be created from scratch etc.

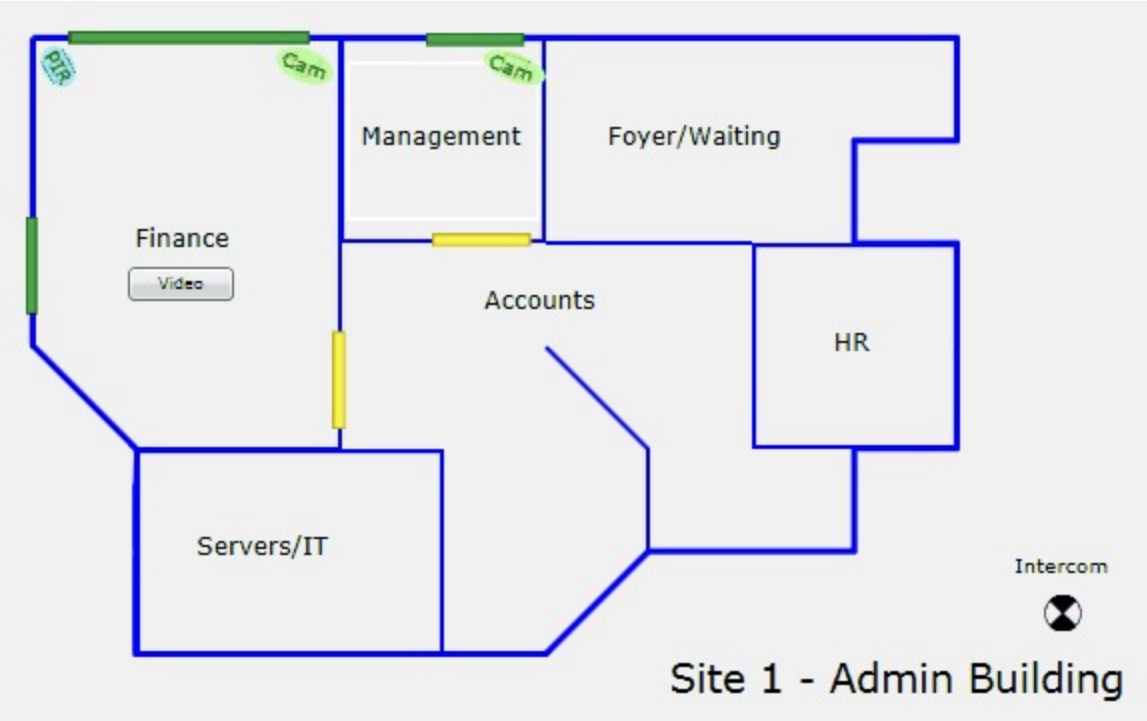
Supported File Formats
CAD Drawing and System Prerequisites for Auto-Node Connection
Importing CAD Drawings

See Also: Graphics Editor

You are here: Using Site Map Graphics > Graphics Editor > Site Map Example

Site Map Example

The following example procedure is a guide only and covers some commonly used site map graphic features. These are adding shapes to create a representation for an area that changes color depending on arm/disarm status, objects linked to nodes for alarm notification via the site map, a command button. The following site map shall be created:



The example includes using the following graphic tools:

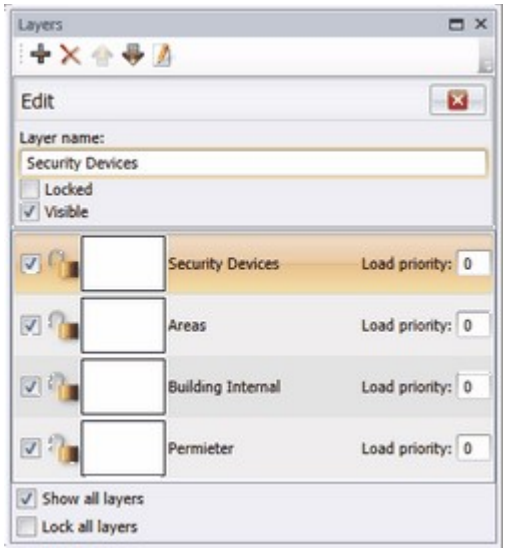
- Rectangles ( ).
- Lines ( ) and poly lines ( ).
- Text ( ).
- Node controls ( ).
- Status indicators ( ).
- Command controls ( ).
- Area controls ( ).

Note: Where areas and nodes are used, these will be assumed to exist in the system so can be connected to. For the purposes of training, simulating the required nodes can be accomplished using a "Test" device, however, the range of alarms, commands etc that can be simulated is limited.

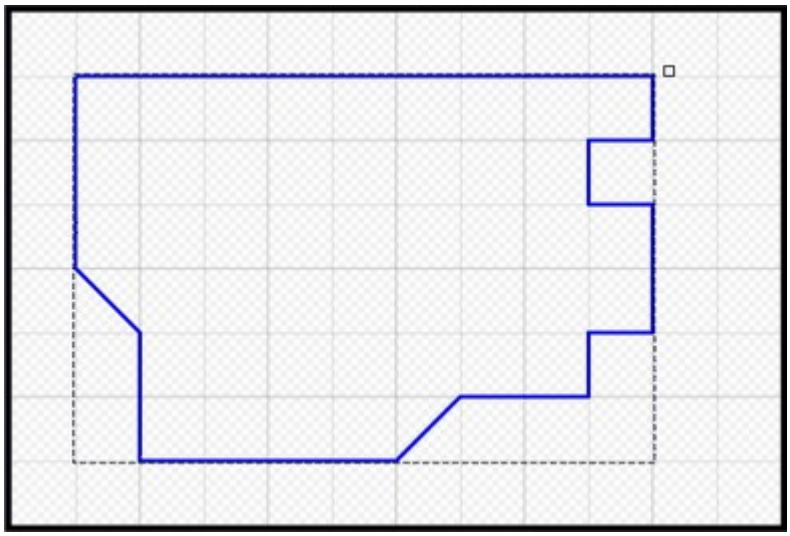
- Create layers - the site map consists of four layers, to separate each major part of the graphic:

  - A layer for the building [site] perimeter.
  - A layer for the building internal layout.
  - A layer for areas inside the building [each "area" represents alarm points and other nodes that are associated].
  - A layer for the security device nodes.

Display the Layers panel and click (Edit) to display layer properties. Click to create each new layer and enter a name for each. Move the layers as required using and , if required, so that the order of layers is similar to:



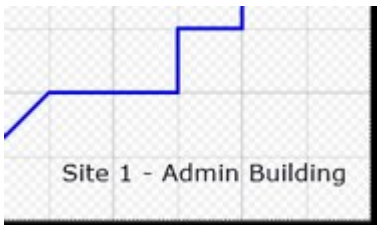
- Create the building perimeter layer content:
  - Turn on grid lines to make positioning objects easier and more accurate - click ⊞. Adjust magnification using the mouse wheel, if required.
  - In the Layers panel, click the required layer so that the objects placed will be on it.
  - Insert a poly line ( ) to represent the outer building walls. Start at a convenient point and click to place the start point of the line. Progressively click to end the current line and begin a new one until you have a design similar to:



Note: If it is necessary to change the size of the "canvas", which is the overall drawing area, open the Objects panel and select the "Root" object - editing "handles" display around the canvas. Click and drag the appropriate handles as required to re-size the canvas. • When site maps are printed using the "alarm report (detailed with site map)" the canvas size determines the overall size of the site map. In other words, empty space around objects is included. This means that a large canvas with a small amount of space used for the graphical content will print "small". When site maps are printed as part of alarm type reports, the site map is automatically scaled to fill as much of the space available for printing the site map. Site map enlargement can also be implemented using the "scale" property for the "graphicalMapLinkControl" report

object. Scale values increment by 50% of the "normal" size; that is, "1" [100%], 1.5" [150%], "2" [200%] etc. When site maps are enlarged in this way, the node in alarm is centered and parts of the site map that are outside the available space are not printed.

- Display the Properties panel and use (Select) to select the object, then set Stroke to blue and Stroke Thickness to "3". This is purely to make the building walls prominent in the graphic.
- Insert text ( ) to create a title for the graphic. Click the graphic to insert a text entry box, select the default text and enter a name for the site; for example, "Site 1 - Admin Building". In the Properties panel, use the Font and Font Size settings to set a suitable font and size. Reposition the text in the graphic as required by clicking and dragging it to the required position, similar to:



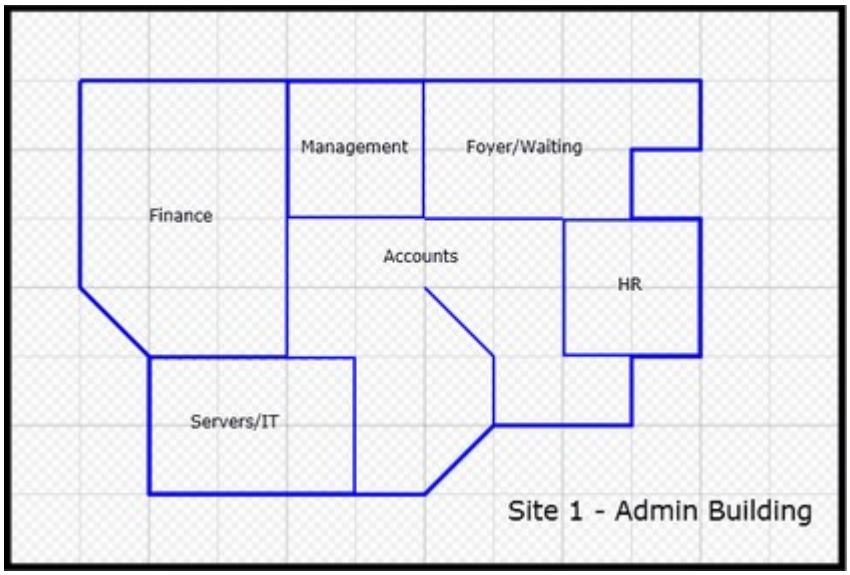
- Use the Layers panel to lock ( ) the layer. This will prevent accidentally selecting objects on the layer.

- Create the building internal layer content:

  - In the Layers panel, click the required layer so that the objects placed will be on it.
  - Insert rectangles ( ) and lines ( ) to represent the internal building walls. Start at a convenient point and click and drag the mouse cursor from the start point to the required end point for each rectangle/line. After inserting an object, you will need to click the required shape tool button again to place the next object. To re-size an object, click (Select) and click the object then use the editing handles to change size.
  - Click (Selection Box) then click and drag the mouse cursor in the graphic so that it passes over all objects as a "marquee". A bounding box is displayed around the selected object [it does not matter if you "marquee" over the perimeter as that layer is locked and objects on it will not be selected].
  - Display the Properties panel and set Stroke to blue and Stroke Thickness to "2".

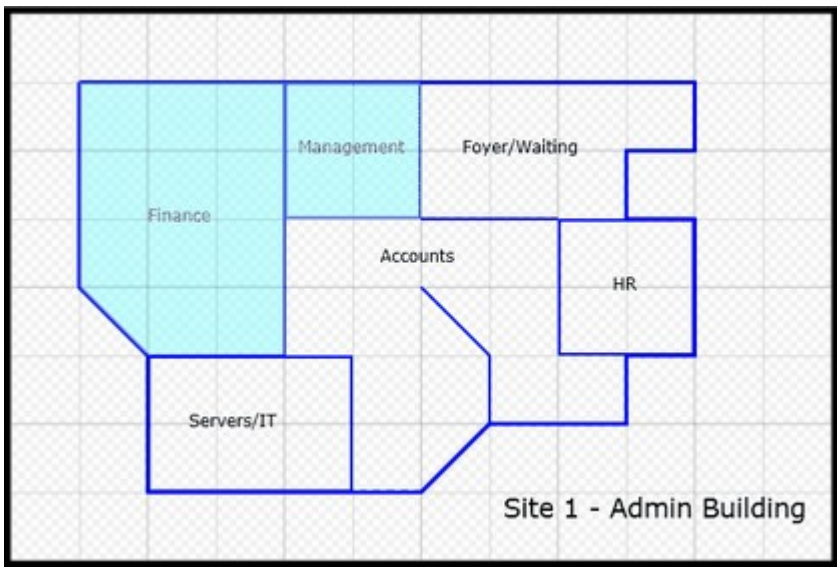
Note: Because objects of different types are selected [rectangle and lines etc], the property values will not display even though they are applied.

- Create text ( ) for a room in the building so that it is easily identifiable to operators. Select the text then use (Copy) and (Paste) to create multiple copies of it on the graphic. Move and edit each piece of text as required, so the graphic is similar to:



- Lock the layer.

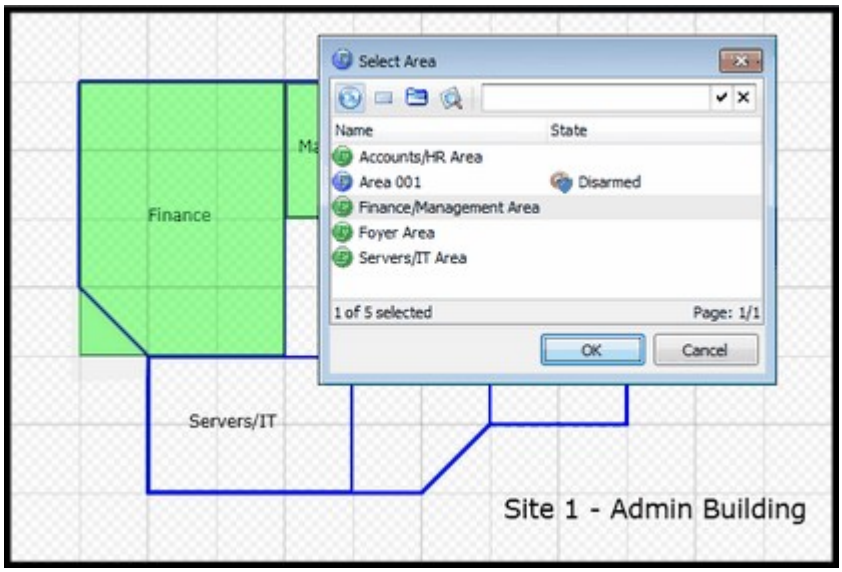
- Create the areas layer content. Areas are special nodes that are basically "containers" for other hardware based "member" nodes, and enables performing commands on the member nodes by way of the container area. In this exercise, a single area will be created for the "Finance" and "Management" rooms, shown in color for reference below:



Note: in this section we will use the "area control" feature, which allows operators to send commands to the area node directly from the graphic. At the time of writing, only rectangular shapes are supported. This can make it somewhat complex when shapes are not specifically rectangular, as in the example. To overcome this, additional steps are required, as described below.

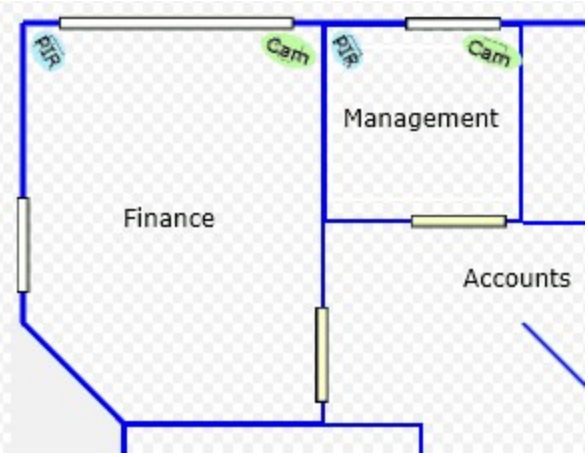
- In the Layers panel, click the required layer so that the objects placed will be on it.
- To create the "area controls" for the "Finance/Management" area, insert an area control ( ) to fit the "Management" room. Once the object is created, the Select

Area dialog box opens - select the required area node and click OK to apply the setting and close the dialog box. Create a second area control to cover the "Finance" room [a corner will sit outside the building perimeter] and set its node to the same area, similar to:

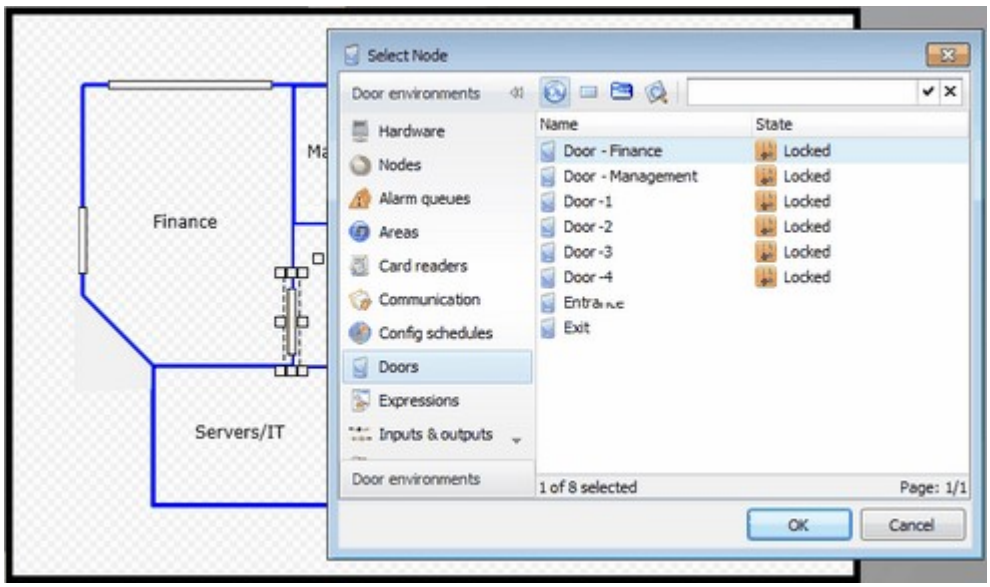


- Display the Properties panel and use (Select) to select the area control objects, then set Background to clear (100% transparent) and Border Thickness to "0,0,0,0". Leave other properties at default values. This is purely to make the area controls "invisible" in the graphic when there are no alarms.
- To "hide" the corner of the "Finance" area that extends beyond the building perimeter, create a poly line to cover the exposed corner and fill it white [or the same color as that of the background as presented in the Graphics panel - this may be affected by the skin/theme of the Unison interface] and have no border. Ensure that the poly line is "on top" of other layer objects - select it, then right-click and select Order > Bring to Front from the context menu.
- Lock the layer.

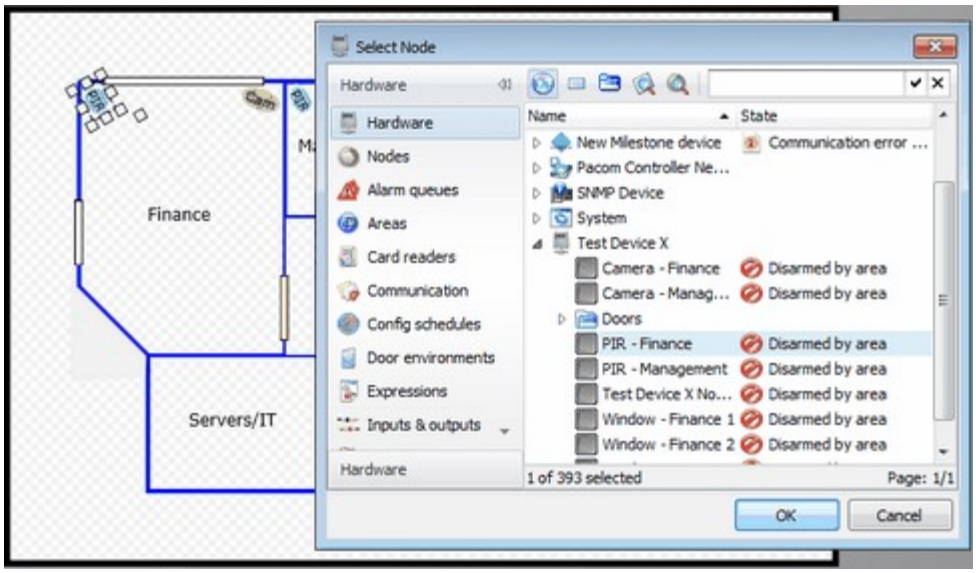
- Create the security devices/alarm point layer content for the previously created area. The security devices and alarm points represent physical devices and alarm switches associated with the area. In this exercise, there will be two doors, three windows, two passive infra-red ("PIR") detectors and two video cameras. The doors and windows are assumed to have contact switches or breakage detectors so will go into "alarm" if opened/broken through when the area is armed - this will be visible to operators viewing the site map. The PIR detectors are motion sensitive and will go into alarm if motion is detected when the area is armed. When in alarm, the PIRs will automatically activate the cameras so that operators have immediate video inside the area to see what is happening at the site. The area will look similar to:



- Insert rectangles ( ) to represent a window and a door [shown in color for clarity]. Turn off grid lines to make placement easier. Copy and paste the objects to create duplicates and place/rotate/size as required [when rotating, press and hold the CTRL key to force rotation in increments].
- Select the "Finance" room "door", then right-click it and select Connect > Node from the context menu - the Select Node dialog box opens. This is the process of associating a graphic object with a node - this creates a "node control" object around the original shape that will indicate alarms to operators viewing the site map. In the dialog box, select the Doors category, then select the required door and click OK. Repeat the process for the other door and for the "windows".

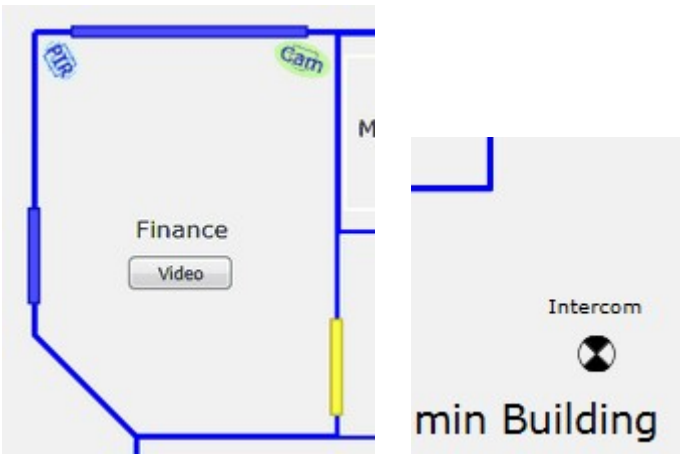


- To create the "PIRs" and "cameras" for the "Finance/Management" area, insert node controls ( ) for each, set the required nodes and apply an appropriate symbol.

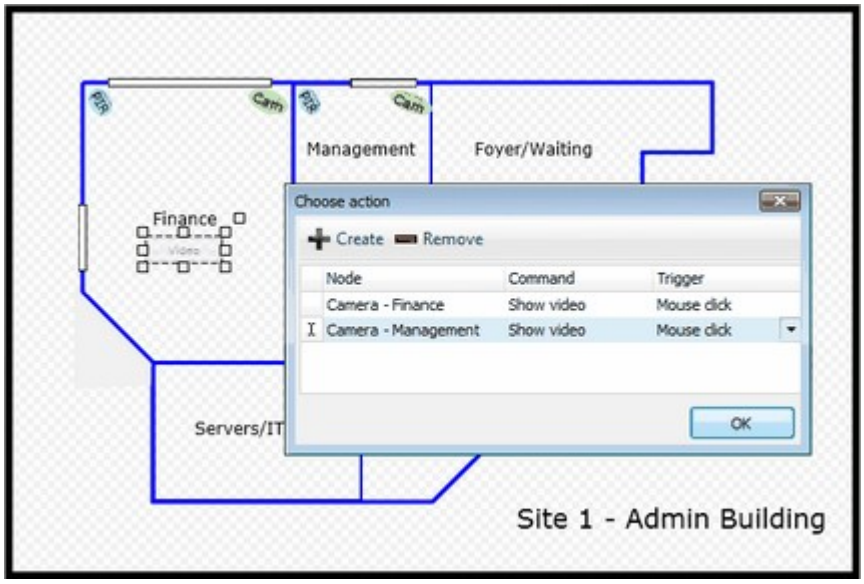


Note: To link the PIRs with associated cameras so that video is shown automatically on alarm, select the required [PIR] input node in the Hardware view and create an alarm action that associates an "Alarm" event, that when active, send a "Show Video" command to the "Camera - Finance" node.

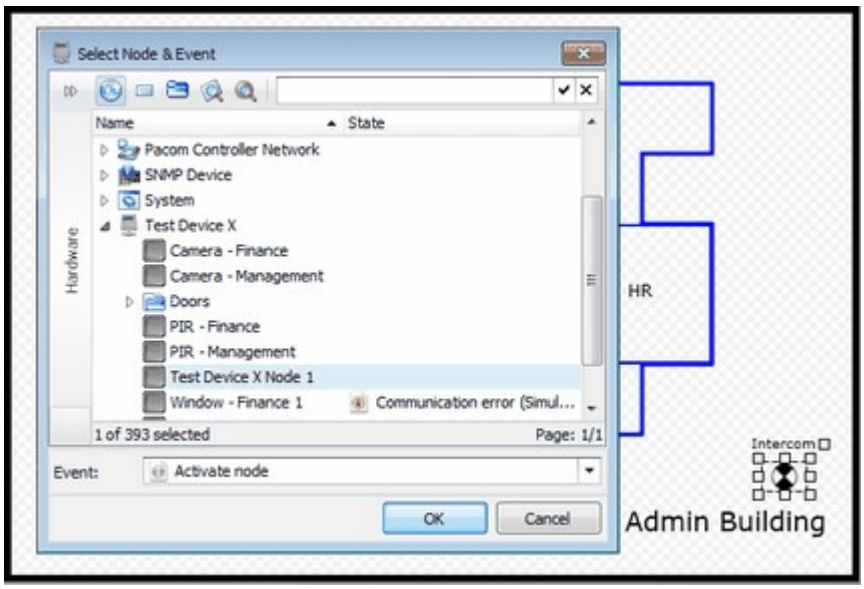
- Additionally to the automated video display on PIR alarm, we can add a button to the graphic that operators can use at any time the area is armed to display video. This may be used for spot checking that the area is secure. We will also include an indicator that graphically shows when a node is active.



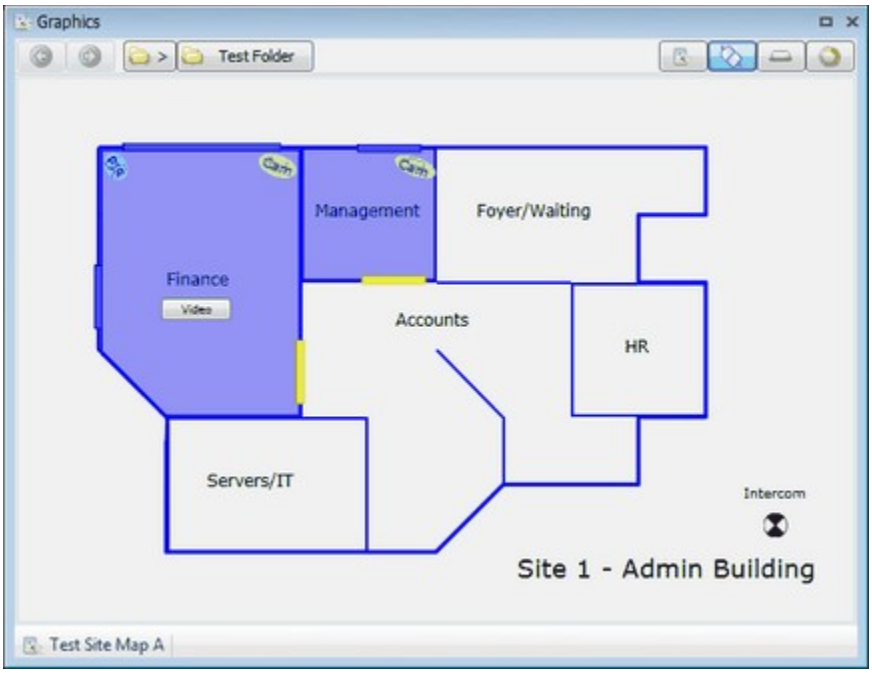
- To create the "button" for the "Finance/Management" area, insert a command control ( ). Once the object is created, the Choose Action dialog box opens - create actions for each camera; select the required camera node and command for each camera and set the trigger to "Mouse Click", then click OK to apply the setting and close the dialog box. Now there is a single button that, when clicked, will display video for each camera in the area.



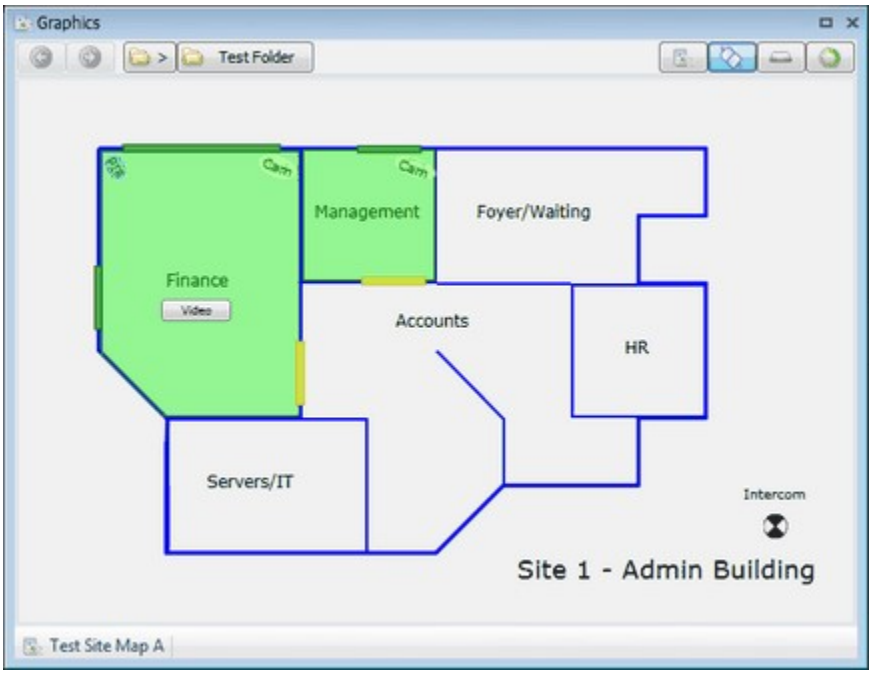
- To create the "intercom indicator", insert a status indicator ( ). Once the object is created, the Select Node and Event dialog box opens; select the required node [in this case it is a node that represents an "intercom"] and event to trigger the status change - in this case "Activate Node" - then click OK to apply the setting and close the dialog box. Ensure that an appropriate symbol and color is applied [use the Properties panel for the object] to ensure an easily visible transition. The text has been added as a separate object so that it can be positioned independently of the status indicator object. Now there is a symbol that, when it associated node becomes active, will change color.



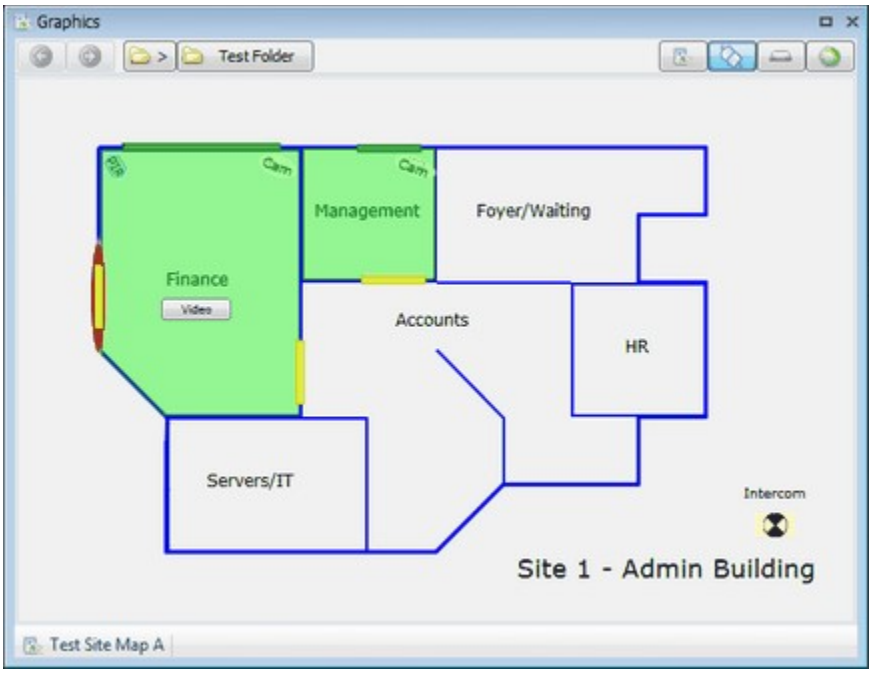
When finished, the graphic should look similar to the following when viewed in the Graphics panel:



Area currently disarmed.



Area currently armed and secure.



Area armed with active alarm [window in "Finance" room] and "intercom" node active.

See Also: Graphics Editor

You are here: Using Site Map Graphics > Graphic Templates

Graphic Templates

Graphic templates are sets of common properties/commands that can be applied to node actions. This is so that it is easier to set up similar or common functionality amongst nodes in site maps. This functionality uses abstract "template nodes" that can be mapped to a real node of the same type at run-time. For example, using a graphic template for using the "show video" command for several actual CCTV camera nodes.

Graphic templates do not exist as actual nodes in the system, however, when a graphic template is applied, an "instance" of it is created as a node. Graphic template instance nodes can be referenced from anywhere in the system in the same way as other node types. Graphical template instances provide the commands required to map, remap and un-map graphic templates to actual nodes; this enables altering the associated "real nodes" by direct command, rather than by having to re-configure the node from scratch.

Graphic templates are not only limited to being displayed in View Command panels [Panels > View Command], but are able to be embedded in other views, such as the Alarm Management dialog box, as part of an event alarm action configuration, and in site map graphics. If an operator does not have access to the View Command or Graphics panels, the graphic template instance can be displayed in the Alarm Management dialog box instead.

As an example, a graphic template that [generically] represents a door bell, door and camera may have the following functions:

- Door bell - Activated by a visitor and creating an "alarm".
- Camera - Activated by the security operator in order to view the visitor.
- Door - Controlled by the security operator in order to allow or deny entry to the visitor.

Graphic template instances can be made of the graphic template, with each one being mapped to actual nodes [door bell, intercom unit, camera etc]. The following image shows an example graphic template that features a "status indication" object for the door bell; a "node control" for the camera [operator must right-click and select Show Video from context menu to view video footage]; two command controls for door unlock and lock operations.

Graphic Templates - Creating
Graphic Template Instance - Creating
Associating Node Alarm Actions

See Also: Creating and Commanding Nodes | Graphics Editor

Using Maps

You can create a diagrammatic presentation of your organization's security system representing buildings, floors, security doors and alarmed points. The map feature in Unison that allows you to do this is based on the ESRI ArcGIS mobile map package. Use the ESRI ArcGIS documentation to set up your map package as this will not be described as part of Unison documentation.

- How to enable the Map feature in Unison
- How to allow operator groups to use the map feature
- How to link Unison nodes to map points
- How to navigate your map

You are here: Managing Reports

Managing Reports

The system comes with a range of pre-defined report layouts that are commonly used in security management; for example, alarms and events. Each node type also has dedicated reports available. In addition to built-in report layouts, you can create custom report layouts. Report layouts may include any available database data, graphics, corporate logo etc. Custom report layouts can be created based on a pre-defined layout, or from an empty "document". Once a report layout is saved, it can be used to create actual reports.

Note: The tools available in the Report Designer are proprietary and designed for multiple purposes [mainly report creation using data extracted from databases]. • For further information on card/report layout tools, refer to www.devexpress.com. • Commands for "Alarm" type reports are available only from the Alarm Management dialog box after being configured as auto-report nodes. Alarm reports are not available from transaction logs. • You can also create customized reports. When creating custom reports, it is recommended to select a "detailed" report that contains the relevant data, export it, then create a new report and import the previously exported report to it. This can then be modified - generally in the form of removing data that is not required, changing font or color etc and replacing the report heading image as required.

Layouts are based on the concept of "bands". Bands are special containers on the page that define areas of the layout that have certain properties or can hold certain types of objects. As a default, a "page" contains three bands - a band each for top and bottom areas, similar to the "header" and "footer" in a document [called "margins", but not to be confused with actual page margin settings], and a "detail" band that represents the "body" of the document/layout and the one generally used for containing the content or body of information.

The report function is designed to be used in conjunction with nodes and transaction logs. That is, to create a report based on nodes, events and statistics stored in the system database. This is achieved using a "report type" [Type setting]; for example, a report type of "operators" makes the report available when working on operator nodes or transactions. It is important to go to the required node or transaction log view and use the transaction log filters to extract the information of interest, then to use the  (Print) function in the view to create the report. Using this method, it is the filter ("query") that defines the information that will be printed. Filters can be saved so that a report can be created at any time, using a pre-defined structure. For example, to create a report that shows users that have used a specific user area over the previous month:

- Open the transaction log view for user areas then set up a filter that defines the interval [previous month], the user area, event type [enter/exit] and other information as required, such as user details etc. The results of the query display in the view - if it is suitable, save the filter with an appropriate name then use the printing tools to create the report.

Pre-Defined Reports
Report Management
Report Designer - Basic Functionality

See Also: Using Common Functions | Using Transaction Logs

Creating Reports

Printing Reports

You are here: Managing Reports > Creating Reports

Creating Reports

Reports are created from events, transactions and statistics that are stored in the system database. This is done by selecting a report type, searching and/or filtering to extract the information of interest, then printing to create the report. It is the filter or query that defines the information that is printed. Filters can be saved so that a report can be created at any time using your pre-defined query.

How to

Examples of creating reports

How to create an operator handling report
How to create an operator station report
How to create an alarm log alarm panel report
How to create an alarm log summarize alarm type report
How to create a blocked nodes report over a period
How to create a blocked nodes report for a specific time

See Also: Managing Reports, Printing Reports

You are here: Managing Reports > Printing Reports

Printing Reports

Once a report type has been selected and the data of interest has been searched and/or filtered, then the report can be created by printing it.

1. Create the report.
2. Click  located on the right-hand side of the Properties section.
3. On the Print dialog box, select the Print Report type from the drop-down list.

   Depending on the selected report type, the available options may vary.

4. Select your print options:

Print option	Description
Print Directly	Prints the report directly to a default printer. You do not have the option to select / change the printer or preview the report.
Print from Setup	Opens a Print dialog box so that you can select a printer and printer options.
Preview	Opens a Preview dialog box displaying the report to be printed and options to format the report, export and email.
Print Selected	Print a report based on one or more selected items in the search results list.
Print All	Print a report based on all available items in the search results list. This option ignores any items that have been selected in the search results list.

5. Click OK.

See Also: Managing Reports, Creating Reports

You are here: Configuring Pacom Hardware

Configuring Pacom Hardware

The system can be used for configuring a range of Pacom Controller hardware over TCP/IP. Pacom Controllers can connect alarm inputs, outputs, card readers, keypads and a number of other devices, and have built-in logic control for defining device/alarm system and access control behavior. This allows custom hardware configuration without the need for intermediary hardware configuration applications. For installation, features, specifications and relevant information on Pacom hardware devices, refer to the hardware installation guide. Supported devices/nodes can be viewed by right clicking on a node and selecting Create from the popup menu. A list of supported devices/nodes will be displayed for you to select from.

Note: In the Hardware view Explorer for Pacom Controllers, the status of "undefined" for Controllers and child nodes is shown whilst configuration updates etc are in progress. After a brief period the actual status is displayed.

Additionally to physical hardware, "virtual" function nodes of a hardware configuration can also be set up, including:

- Area
- Elevator
- Interlock
- Trigger.

Note: Devices are generally treated using multiple node types. The "device" node represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

The Explorer in the Hardware view is different to other views, where devices are presented in a hierarchical tree structure that shows how different nodes are connected to each other. For example, a device node may have child nodes that correspond to attached hardware and/or functionality. These nodes may also have child nodes and so on. Normal list search and filter functions are designed for flat lists, therefore, in the Hardware view an additional search function is included for searching a hierarchical tree structure.

Existing and Pre-Configurations

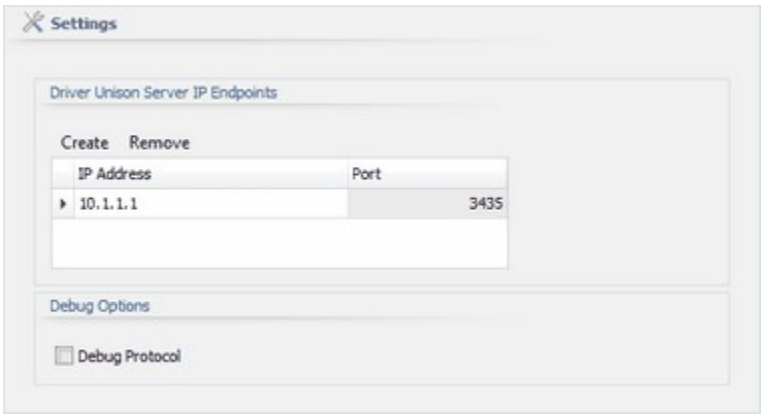
The system supports "migrating" Controllers and existing hardware configurations so that re-configuration is not required. It is also possible to "pre-configure" nodes and functionality before connecting the physical hardware itself, then download the

configuration to the Pacom Controller once it and peripheral devices are connected.

Note: When configuring Pacom hardware, it should be understood that the configuration is at "hardware level" and some concepts in the hardware are designed for other Pacom security management systems [for example, Pacom GMS] and may differ to that of the Unison system. As a result, there are several settings/events/commands that are applicable to scenarios where connected Pacom Controller hardware has been previously used in conjunction with different Pacom security management systems. For "upgrades" such as this, there are settings that are used by Controllers that do not practically exist in the Unison system; for example, "alarm user types" and area "sub-modes". For systems that are not "upgrades" of this nature, these settings/events/commands are not used.

Main Device Node - Management, Configuration and Commands

The Hardware view enables managing Pacom Controller network device nodes. Click (Hardware) in the System Configuration ribbon bar to open the view. Click (Create Device) in the view toolbar to display a list of supported node types, and select Pacom Controller Network. The new device is added to the device tree in the Explorer, with its settings available in the Properties section.



Control	Description

Properties Tab

Properties - One or more "generic" node properties apply. Click here for help. Additional properties, if any, are listed below.

Settings > Protocol Service Options - These settings are for additional device driver servers that the Pacom Controller device hardware can use. That is, they are downloaded to the Controller so that in the event of communications failure, the Controller switches to the next available device driver service.

Add - Add a device driver server, if multiple device driver servers are to be used, for the device driver service to run on, and act as redundancy servers to switch to if a service failure occurs. The order of use of device driver services is first in the table first, and if that fails, second entry in the list and so on. Each driver is added as a row in the table below.

Note: The actual device driver software must be installed on each server.

Remove - Disassociates device driver server node(s) from the device. Select one or more nodes from the table then click - the nodes are no longer associated with the device, however, still exist in the system.

IP Address (Column)	Sets the device Ethernet network IP address. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, click the field and enter a value.
Port (Column)	Specifies the identification number of the device driver server IP port that is being used for communicating with the Pacom Controller (default is "3435"). To edit, double-click the field and enter a value. Note: If multiple instances of the device driver are to be used, each instance must use a unique IP port. IP port settings must also be set in the Pacom Controller.

Settings > Debug Options - Additional debug options specific to Pacom Controller devices. For technician use.

Debug Protocol	Activates communications protocol error logging for device troubleshooting. For technician use only. Click to toggle. ☑ = option enabled.

Settings > Advanced Properties - Generic device node properties apply. Click here for help.

Events Tab - One or more "generic" events may apply. Normal event configuration procedures apply. Click here for help. Additional events, if any, are listed below.

Actions Tab - Lists any event response actions that have been created for the node. Normal node action configuration procedures apply. Click here for help.

Dependencies Tab - Lists any dependencies on the node. Normal node dependency procedures apply. Click here for help.

Scheduled Commands Tab - Lists any scheduled commands that have been created for the node that are yet to be processed.Click here for help.

Notes Tab - Normal note configuration procedures apply.Click here for help.

Commands

Command	Description

One or more "generic" commands may apply. Click here for help. Additional commands, if any, are listed below.

See Also: 8001/8002 Controller | 8003 Controller | Controller Considerations | Configuring Third-Party and Generic Devices| Device Templates | Web Server Controller Configuration Guide

---

You are here: Configuring Pacom Hardware > Hardware Device Nodes

Hardware Device Nodes

Hardware device nodes represent physical hardware connected to the system. Hardware includes Pacom Controllers, which are the fundamental components that provide the interface to the head system. Specific security device peripheral hardware, such as door controllers and keypads, connect to Controllers.

See Also: Controllers | Controller Expansion Cards | Peripheral Devices | Virtual Device Nodes

---

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers

Controllers

Controllers represent Pacom control panel hardware (also referred to as "field controller", "remote terminal unit" or "RTU"). This is the interface between the physical security device hardware (input/output cards, doors, card readers, etc) and the centralized monitoring system. Pacom Controllers are modular in design, allowing you to expand support for the number of card readers, input/output points, areas and cardholders as a system grows in size.

Controllers are designed to monitor, control and maintain security for a site. They are physically located at the site and perform alarm and access control functions. Pacom Controllers have offline capabilities that enables them to apply access control logic independently of the security management or monitoring head system.

Security devices are wired to the Controller, with the Controller and head system communicating using TCP/IP [refer to IT staff for available IP addresses], or a variety of methods, such as, dialup, serial and GPRS.

Communicating with Third-Party Alarm Panels

You can connect alarm panels from other manufacturers so that the messages they generate can be logged and monitored by Site Manager. The Pacom system is able to operate with alarm panels that support industry-standard Contact ID or SIA message formats.

Initial Communications Configuration

Before a Pacom Controller is connected to a Unison system it must first be set up to allow communication between the two. Configuration is carried out with a Pacom "web server" configuration utility, available in Controller firmware 1.10 and later, or using Pacom GMS security management software.

Note: Pacom Controller firmware 1.09 (for 8001/8002 Controllers) or later is required for Unison connections. For organizations currently using older Pacom Controllers (for example, 1057/1058) and looking to upgrade systems to Unison, contact Pacom Systems for assistance with a suitable upgrade path.

Configuration Using "Web Server" Utility

Note: Pacom Controller firmware 1.10 (for 8001/8002 Controllers) or later is required for "web server" utility configuration.

Configuration Using Pacom GMS Software

1. Using Pacom GMS software, open the Port Parameters dialog box for the Controller Ethernet port, and in the Session Level tab specify the following settings:

   - IP Address of Local Node - Set to the required IP address of the Pacom Controller.
   - Subnet Mask of Local Node - Set to the required subnet mask of the Pacom Controller.
   - IP Address of Router - Set to the required IP address of the router, if used.
   - IP Address of Alternate Router - Set to the required IP address of the secondary router, if used.

2. Using Pacom GMS software, open the System Passwords dialog box for a Controller, and set Password 8 to "Pacom" (default setting).
3. Using Pacom GMS software, open the EMCS Parameters dialog box, and specify the following settings:

   - Address Field Valid - Enable this option.
   - Use TCP - Enable this option.
   - Enable Event Reporting - Enable this option.
   - Enable DTP Transfers - Enable this option.
   - Encryption Type - Set to HMAC.
   - Protocol Type - Set to Pacom.
   - Physical Port - Set to the Ethernet port specified in step 1.

- Destination UDP/TCP Port - Set to 3435.
- IP Address - Set to the IP address of the Unison server computer.

4. Download the configuration to the Pacom Controller.

Note: If the Pacom Controller has previously been connected to a Pacom Site manager ("EMCS") system, the following "main key reset" operation must be performed on it:

1. Open the User Defined Commands dialog box.
   • Element Type - Set to Controller.
   • Element No - Set to the Controller identification (ID) number.
   • Function Code - Set to 46.
   • Command Data - Set to 4,0x86.
2. Click Send.

See Also: 8001/8002 Controller | Controller Considerations | Device Templates

Controller Considerations

8001/8002 Controller

8003 Controller

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Controller Considerations

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. Unison is generally limited only by the size of the associated database and/or server resources. The controller is limited by the available on-board memory.

The controller on-board memory can be expanded using memory expansion cards which are available for all PACOM Controllers. When installed, the amount of available access control related data storage increases, provided it is supported by the controller model. 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 to the numbers of each that a controller can store.

There are different controller models that determine some hardware limitations, such

as number of card readers and keypads that can be connected. There also may be model based controller memory management modes that affect limitations on access control 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 any).

Note: Unison supports PACOM 8001 and 8002 Controllers. For organizations currently using older PACOM Controllers, such as, 1057/1058, and looking to upgrade systems to Unison, contact PACOM for assistance with a suitable upgrade path.

Controller Limitations

Note: Some limitations may vary from that of other PACOM security management applications.
• For installations where controller limitations are exceeded there may be other options available, such as using additional controllers and distributing the required data between them.
• Specifications are for standard controllers.
• Some features/functions can be increased by way of expansion cards.
• The total number of users that can be stored in a controller may vary depending on how personal access is configured in Unison and the maximum allowable number of access schedules. 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, the means for 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 details 8001 and 8002 S, M and L Controller model access control limitations:

Feature/Function	Controller		
	S	**M**	**L**
Card Data Size	64-bit	64-bit	64-bit
Calendar Entries	100	100	100 500 with 16MB memory expansion 1,000 with 64MB memory expansion
Users (Cards)	500	2,000	4,000 10,000 with 16MB memory expansion

			256,000 with 64MB memory expansion
			1,000
Offline Events	1,000	1,000	100,00 with 16MB memory expansion
			128,000 with 64MB memory expansion
Access Groups/User	8	8	8
			100
Access Schedules	100	100	500 with 16MB memory expansion
			5,000 with 64MB memory expansion
Intervals/Access Schedule	8	8	8
			200
Door Schedules	200	200	500 with 16MB memory expansion
			2,000 with 64MB memory expansion
			4
Intervals/Door Schedule	4	4	8 with 16MB or 64MB memory expansion
			10
Day Types	10	10	32 with 16MB or 64MB memory expansion
Elevators	16		
Floor Levels	64 Up to 128 with an expansion module.		

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

Hardware/Feature	**Controller**		
	S	**M**	**L**
Inputs	32	128	256
Outputs	8	32	64
Alarm Areas	32	32	32
Card Readers	8	32	64

The following table details the 8002 controller model capacity with the different Unison memory models in terms of access cardholders.

Unison Memory Capacity Model	8002 Controller S	M	L
Small	500	2,000	5,000 300,000 with 64MB memory expansion
Medium	500	2,000	4,000 200,000 with 64MB memory expansion
Large	500	1,000 2,000 with 64MB memory expansion	1,000 64,000 with 64MB memory expansion

See Also: 8001/8002 Controller | Controllers

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > 8001/8002 Controller

8001/8002 Controller

Pacom Controller Device Network nodes represent one or more items of Pacom 8001/8002 Controller hardware, which are used to connect and control inputs and outputs, local keypads, doors etc. Nodes representing actual Controllers can be created and modified in the Pacom Controller Network device root node. Once a Controller node is created, the "initialize" command must be performed to "prepare" the Controller to operate in conjunction with Unison. Choices exist to initialize the Controller and apply the configuration for it that exists in Unison [if available] or existing in the Controller [if available] - this is referred to as the "configuration source". When using the Controller as the "configuration source" it has been previously configured, its current hardware configuration is "read" by the Unison system, with corresponding child nodes automatically created.

Note: The "initialize and "generate" commands perform similar functions. It is recommended to use "initialize" for initial connections as this command also clears the access control database in the Controller and sets it for Unison compatibility. When using "initialize", the Controller may be offline for some amount of time as the access control database is also updated with data from the Unison system. • Whenever a hardware change has been made at the hardware level [via the Controller web configuration interface or some other direct method] after initial connections, it is

recommended to use "generate", as this command performs the hardware configuration upload only. • Hardware configuration complexity may affect node generation time.

Adding a Controller
Commands

See Also: Configuring Pacom Hardware

8001/8002 Properties

8001/8002 Events

8001/8002 Properties

Settings for Pacom 8001/8002 Controllers. The Hardware view enables managing Controller nodes. Click  (Hardware) in the System Configuration ribbon bar to open the view. Click the existing Pacom Controller Network main unit node, then click  (Create) in the view toolbar to display a list of supported node types, and select Controller. The new device is added as a "child" to the main unit node in the Explorer device tree, with its settings available in the Properties section.

Control	Description
Properties Tab	
Properties - One or more "generic" node properties apply. Click here for help. Additional properties, if any, are listed below.	

Settings - Device Information

Settings - Installation

Settings - Areas

Settings - Keypads

Settings - Alarm Users

Settings - Alarms

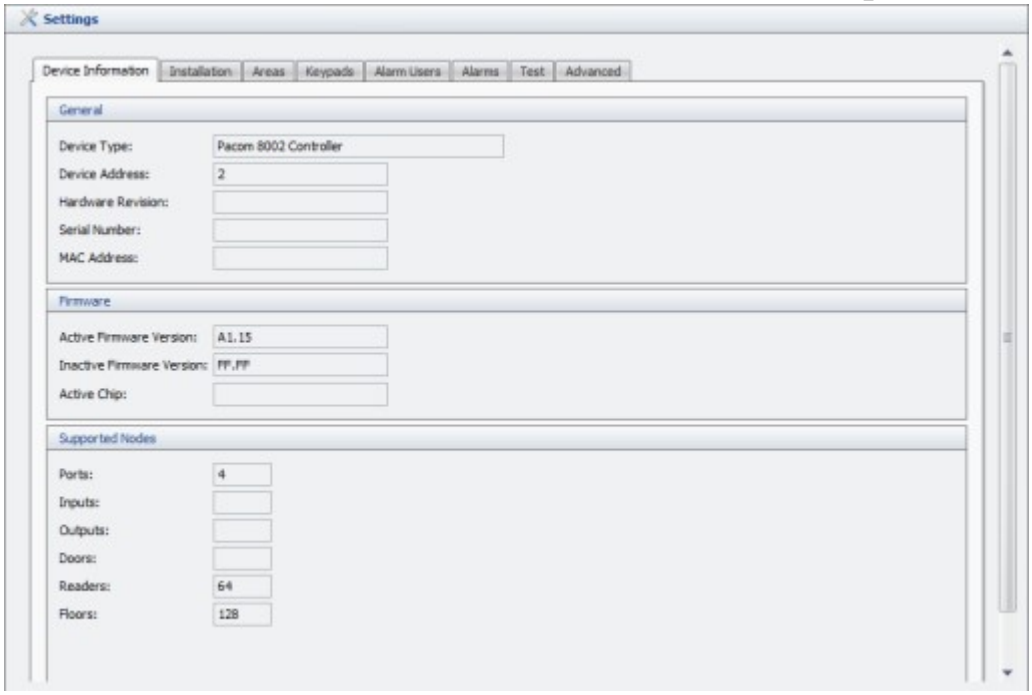
Settings - Test

Settings - Advanced

Settings - Device Information

Device Information settings for Pacom 8001/8002 Controllers.

Control	Description



General

Device Type	Shows the Controller model.
Device Address	Shows the RS485 device address, if applicable.
Hardware Revision	Shows the Controller hardware [printed circuit board] revision number, if available.
Serial Number	Shows the Controller serial number, if available.
MAC Address	Shows the Controller MAC address, if available.

Firmware

Active Firmware Version	Shows the firmware version that the Controller is operating on.
Inactive Firmware Version	Shows the secondary firmware version that is stored in the Controller, if available.
Active Chip	Shows the chip is being used to store the active firmware.

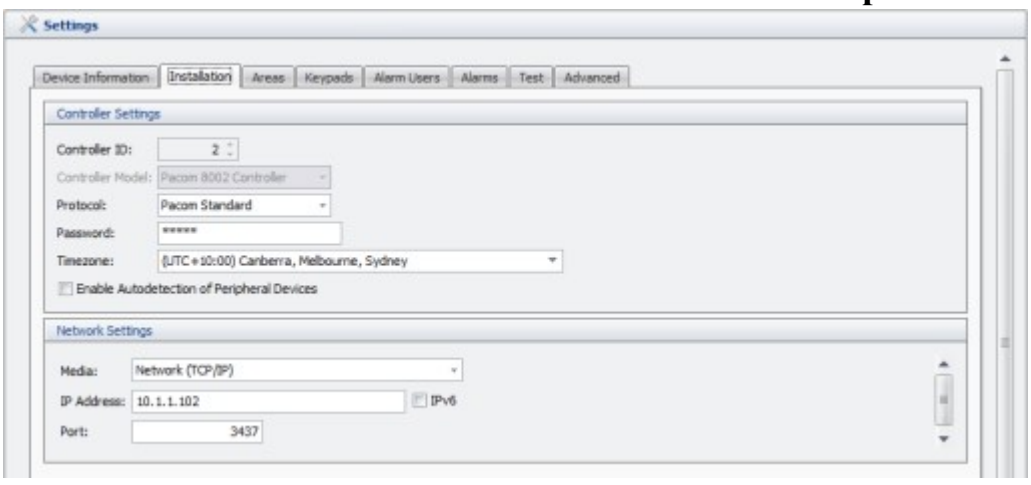
Supported Nodes

Ports	Shows the number of Controller communications ports [Ethernet, RS485 etc] currently configured for use.
Inputs	Shows the total number of inputs that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Outputs	Shows the total number of outputs that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Doors	Shows the total number of doors that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Readers	Shows the total number of card readers that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Floors	Shows the total number of elevator floors that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Installation

Settings - Installation

Installation settings for Pacom 8001/8002 Controllers.

Control	Description
	

Controller Settings

	Shows the Controller identification (ID) number. Each

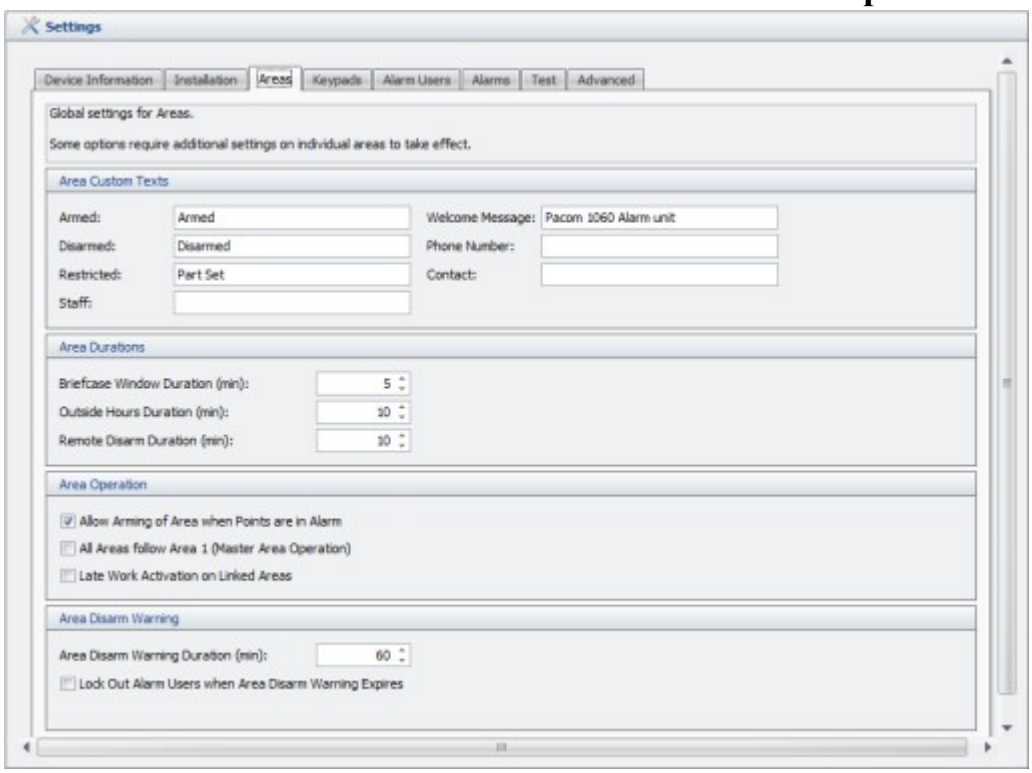
Controller ID	Controller associated with the same "Pacom Controller Network" device must have a unique ID. The ID number for auto-generated nodes cannot be changed.
Controller Model	Sets the Pacom Controller hardware model. To edit, click ▾ for options. Click an option to select it, if required. **Note**: This setting is applicable when setting up Controllers from Unison only, and the actual Controller hardware is to be connected later. That is, the configuration is not being generated from the actual hardware.
Protocol	Sets the protocol used between Unison and the Controller.
Password	Sets the authentication password used to establish communication with the Pacom Controller (default is "Pacom"). To edit, click the field and enter a value. **Note**: The password must correspond to that stored within the Controller password list as "password 8", which is reserved for connection to Unison.
Timezone	Sets the timezone that applies to the Pacom Controller, which is usually determined by geographical location (default is the Unison server timezone). To edit, click ▾ for options. Click an option to select it.
Enable Autodetection of Peripheral Devices	If set, the Controller will automatically autodetect and configure any new peripheral device that is connected on the device loop. Enabling this setting will override the DIP switch setting (DIP 2) for autodetection on the Controller if DIP 2 is OFF, however if DIP switch 2 is ON, autodetection will always be enabled regardless of this setting. Click to toggle. ☑ = option enabled.
Network Settings	
Media	Sets the connection type to use for communications with the Pacom Controller. To edit, click ▾ for options. Click an option to select it (**Network TCP/IP** supported only):
IP Address	Sets the device Ethernet network IP address. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, click the field and enter a value.
IPv6	Determines if the IP address uses version 6 notation [for networks that use "IPv6" addresses]. Click to toggle. ☑ = option enabled. **Note**: IPv6 address notation is not currently supported.
	Specifies the identification number of the Controller device IP port that is being used for communicating with the

Port	system (typically "3435"). To edit, double-click the field and enter a value. **Note**: If multiple instances of the device driver are to be used, each instance must use a unique IP port. IP port settings must also be set in the Pacom Controller.

Settings - Areas

Global settings for Areas. Some options require additional settings on individual areas to take effect.

Control	Description



Controller Settings

Armed	Sets the keypad custom text to display in all Keypads connected to this Controller when an area is armed. Up to 10 characters are allowed for this field. **Note**: This setting also has to be enabled in the individual areas that should use it. See here for more information.
Disarmed	Sets the keypad custom text to display in all Keypads connected to this Controller when an area is disarmed. Up to 10 characters are allowed for this field.

	Note: This setting also has to be enabled in the individual areas that should use it. See here for more information.
Restricted	Sets the keypad custom text to display in all Keypads connected to this Controller when an area is in restricted mode. Up to 10 characters are allowed for this field.
	Note: This setting also has to be enabled in the individual areas that should use it. See here for more information.
Staff	Sets the keypad custom text to display in all Keypads connected to this Controller for staff type alarm users. Up to 8 characters are allowed for this field.
	Note: This setting also has to be enabled in the individual areas that should use it. See here for more information.
Welcome Message	Sets the keypad custom text to display in all Keypads connected to this Controller for welcome message when the keypad is idle. Up to 32 characters are allowed for this field.
	Note: This setting also has to be enabled in the individual areas that should use it. See here for more information.
Phone Number	Sets the keypad custom text to display in all Keypads connected to this Controller for phone number to call to contact the monitoring center for assistance in case of problems during the arming/disarming procedure. Up to 20 characters are allowed for this field.
Contact	Sets the keypad custom text to display in all Keypads connected to this Controller for whom to contact for assistance in case of problems during the arming/disarming procedure. Up to 20 characters are allowed for this field.
Area Durations	
Briefcase Window Duration (min)	The time to use for the Briefcase Window function (if enabled) unless overridden on an individual area. Range is 0 to 255 minutes.
Outside Hours Duration (min)	The time to allow users with Out of Hours access to gain access to areas after the Latest Staff Exit Time setting and before the earliest Staff Entry setting (see Configuring Area Access). If set to 255 allows unlimited access. If set to 0 then no access is allowed. Range is 0 to 255 minutes.
Remote Disarm Duration (min)	The duration for which a Unison operator is allowed to disarm an area. Set to 0 for no restriction on disarming. Range is 0 to 255 minutes.
Area Operation	
Allow Arming of Area when Points are in Alarm	If set, an area that has one or more active alarms can still be manually or automatically armed. Click to toggle. ☑ = option enabled.

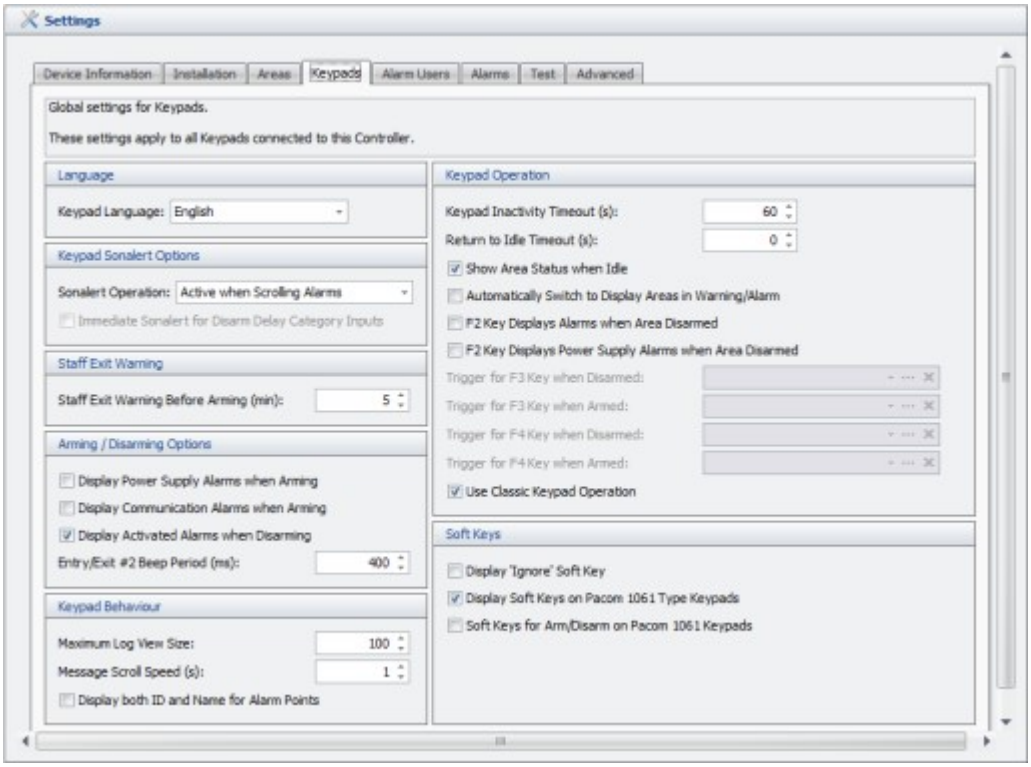
All Areas follow Area 1 (Master Area Operation)	If set, area 1 works as a main area, forcing all other areas on the Controller to follow the mode of area 1. Click to toggle. ☑ = option enabled.
Late Work Activation on Linked Access	If set, late work also applies to all linked areas when an alarm user sets an area for late work. Click to toggle. ☑ = option enabled.
Area Disarm Warning	
Area Disarm Warning Duration (min)	This time used for all areas to define when after the Day Start time (see Configuring Area Access) the system expects the area to be un-set by. This timer is also used to select when Auto Lockout comes into effect. Day lockout prevents users from accessing Day mode after the timer expires if Day mode not entered before day start and open warning timers expire. To enable this, set the Open Warning Time to a non-zero value and enable the Warning Messages option. If the Day Start time is "0" (zero), then Auto Lockout is disabled. Range is 0 to 255 minutes.
Lock Out Alarm Users when Area Disarm Warning Expires	If set, after the Disarm Warning Time expires, the system will prevent alarm users to disarm areas from the keypad. Users will have to contact a Unison operator for the areas to be remotely disarmed. Click to toggle. ☑ = option enabled.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Keypads

Settings - Keypads

Global settings for Keypads. These settings apply to all Keypads connected to this Controller.

Control	Description



Language

Keypad Language Sets the language to use by the keypads connected to this controller.

Keypad Sonalert Options

Sonalert Operation Determines the operation of the Keypad sonalert for all Keypads connected to this Controller.

Immediate Sonalert for Disarm Delay Category Inputs If set, the keypad sonalert will start immediately when a Disarm Delay Category point is activated instead of waiting for the Disarm Warning Timer to expire. Only used if the sonalert operation has the Disarm Delay Category option enabled. Click to toggle. ☑ = option enabled.

Staff Exit Warning

Staff Exit Warning Before Arming (min) The time before the set area exit time that the system sonalerts the keypad to warn the user that the area(s) require to be set within.

Arming/Disarming Options

Display Power Supply Alarms when Arming If set, the keypad will display any power supply warnings when arming. Click to toggle. ☑ = option enabled.

Display Communication Alarms when Arming If set, the keypad will display any communication warnings when arming. Click to toggle. ☑ = option enabled.

Display Activated Alarms when Disarming If set, the keypad will display any alarms that activated during the armed period when the area is being disarmed. NOTE: Alarms that have activated but has then been remotely restored will still be displayed when the area is being disarmed when this option is enabled. Click to

	toggle. ☑ = option enabled.
Entry/Exit #2 Beep Period (ms)	The beep repetition period of the secondary entry/exit time beeper. The number set is the period of the beep repetition in 0.1 sec increments. Valid values are 0.1s-1s.
Keypad Behavior	
Maximum Log View Size	The maximum number of messages that can be viewed on a keypad.
Message Scroll Speed (s)	The length of time that the keypad takes before switching to the next alarm while viewing multiple numbers of alarms that have been set off. If set to 0, the keypad will wait for a manual action to switch to the next alarm (such as pressing enter).
Display both ID and Name for Alarm Points	If set, the keypad displays the ID of inputs, doors etc. in addition to the name. Click to toggle. ☑ = option enabled.
Keypad Operation	
Keypad Inactivity Timeout (s)	The length of time that the keypad waits before sending a keypad inactivity time-out event if a user accesses the system and leaves the keypad without completing the process that they started. Range is 10 to 600 seconds.
Return to Idle Timeout (s)	The length of time that the keypad takes before reverting back to displaying area one (if more than one area is being used) and displaying the welcome message (if configured). This also requires the Return to Idle option being enabled on the keypad. Range is 0 to 255 seconds.
Show Area Status when Idle	If set, the keypad will show the status of the areas when the keypad is idle.
Automatically Switch to Display Areas in Warning/Alarm	If set, the keypad will automatically switch to display any areas that have alarms or warnings (for example, "STAFF EXIT NOW" or sonalert being active). If there are multiple areas with alarms or warnings, the keypad switches between them.
F2 Key Displays Alarms when Area Disarmed	If set, all active alarms can be displayed on a keypad by pressing the F2 key while the area is disarmed and without requiring an alarm user to log on to the keypad.
F2 Key Displays Power Supply Alarms when Area Disarmed	If set, power supply type alarms can be displayed on a keypad by pressing the F2 key while the area is disarmed and without requiring an alarm user to log on to the keypad.
Trigger for F3 Key when Disarmed	Sets the trigger id to activate when the F3 key is pressed on the keypad when the area is disarmed. This require ClassicalKeypadOperation mode to be false. Set to 0 to disable this feature. Range is 0 to 255.
Trigger for F3 Key when Armed	Sets the trigger id to activate when the F3 key is pressed on the keypad when the area is armed. This require ClassicalKeypadOperation mode to be false. Set to 0 to

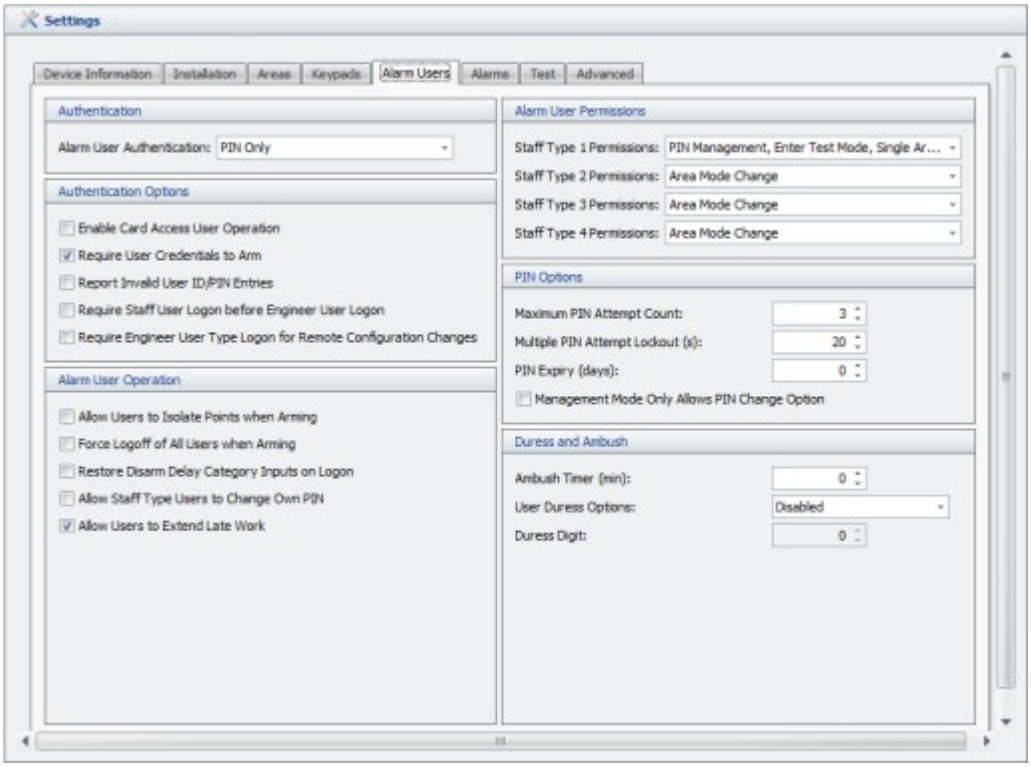
	disable this feature. Range is 0 to 255.
Trigger for F4 Key when Disarmed	Sets the trigger id to activate when the F4 key is pressed on the keypad when the area is disarmed. This require ClassicalKeypadOperation mode to be false. Set to 0 to disable this feature. Range is 0 to 255.
Trigger for F4 Key when Armed	Sets the trigger id to activate when the F4 key is pressed on the keypad when the area is armed. This require ClassicalKeypadOperation mode to be false. Set to 0 to disable this feature. Range is 0 to 255.
Use Classic Keypad Operation	If set, all keypads on this Controller will use classic operation. Click to toggle. ☑ = option enabled.
Soft Keys	
Display 'Ignore' Soft Key	If set, an "Ignore" soft-key option is displayed on all keypads to allow alarm users to be able to accept points being in alarm when arming system. Click to toggle. ☑ = option enabled.
Display Soft Keys on Pacom 1061 Type Keypads	If set, soft-key options are being displayed on a Pacom 1061 type keypad. Click to toggle. ☑ = option enabled.
Soft Keys for Arm/Disarm on Pacom 1061 Keypads	Soft Keys for Arm/Disarm on Pacom 1061 Keypads If set, the soft-keys on a Pacom 1061 keypad functions in the same way as the Disarm (Day) and Arm (Night) keypad keys. Click to toggle. ☑ = option enabled.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Alarm Users

Settings - Alarm Users

Alarm User settings for Pacom 8001/8002 Controllers.

Control	Description



Authentication

Alarm User Authentication Determines the keypad authentication mode for alarm users.

Authentication Options

Enable Card Access User Operation If set, card access users are allowed to operate the keypad as an alarm type user, provided they have sufficient permissions to do so. Click to toggle. ☑ = option enabled.

Require User Credentials to Arm If set, user credentials has to be provided in order to arm areas. Click to toggle. ☑ = option enabled.

Report Invalid User ID/PIN Entries If set, the Controller will report all invalid user ID/PIN combinations entered into a keypad. Click to toggle. ☑ = option enabled.

Require Staff User Logon before Engineer User Logon If set, a staff type alarm user must log on before an engineer type user can log on. The engineer must then enter their user ID and/or PIN within the Keypad Inactivity Timeout setting. If the timer expires and the system has not entered engineering mode, the staff type user must log on again. Click to toggle. ☑ = option enabled.

Require Engineer User Type Logon for Remote Configuration Changes If set, Engineer alarm user type is required to be logged on from the keypad in order to perform configuration changes or do firmware upgrades. Click to toggle. ☑ = option enabled.

Note: This option is required to be set for NFa2p compliance.

Alarm User Operation

Allow Users to Isolate If set, alarm users are allowed to isolate points locally

Points when Arming	using the keypad when arming. Click to toggle. ☑ = option enabled.
Force Logoff of All Users when Arming	If set, the system automatically logs off any other alarm user types from area when the area is armed. Click to toggle. ☑ = option enabled.
Restore Disarm Delay Category Inputs on Logon	If set, the Day Delay alarm count is set back to zero for an area whenever an alarm system user logs on to the keypad and sets or un-sets the area. Click to toggle. ☑ = option enabled.
Allow Staff Type Users to Change Own PIN	If set, alarm users with Staff Type 1 - 4 can change their own PIN at a keypad. If the PIN is successfully changed, this will generate a message to the management system with the new PIN so it can change the user's database record accordingly. Click to toggle. ☑ = option enabled.
Allow Users to Extend Late Work	If set, alarm users are allowed to extend the late work to all day (24h). Click to toggle. ☑ = option enabled.
Alarm User Permissions	
Staff Type 1 Permissions	Determines the alarm user permissions for staff type 1 users.
Staff Type 2 Permissions	Determines the alarm user permissions for staff type 2 users.
Staff Type 3 Permissions	Determines the alarm user permissions for staff type 3 users.
Staff Type 4 Permissions	Determines the alarm user permissions for staff type 4 users.
Pin Options	
Maximum PIN Attempt Count	The maximum number of faulty PIN attempts that can be made before the keypad is locked out. If set to 0, the number of faulty attempts is unlimited. Range is 0 to 15.
Multiple PIN Attempt Lockout (s)	The length of time for which the keypad is locked out after the maximum number of faulty PIN entry attempts is reached. Once the maximum faulty number of attempts is reached, this time will apply for each consecutive try until a valid PIN is entered. **Note**: The first faulty attempt will always trigger a one minute lockout time, this time only applies to any consecutive attempts. Range is 0 to 255 minutes.
PIN Expiry (days)	Sets the number of days before the Alarm user PIN expires and has to be changed. Set to 0 to disable (PIN never expires). Range is 0 to 255 days.
Management Mode Only Allows PIN Change Option	If set, the keypad management menu only allows for PIN change while all other menu options are disabled. Click to toggle. ☑ = option enabled.
Duress and Ambush	

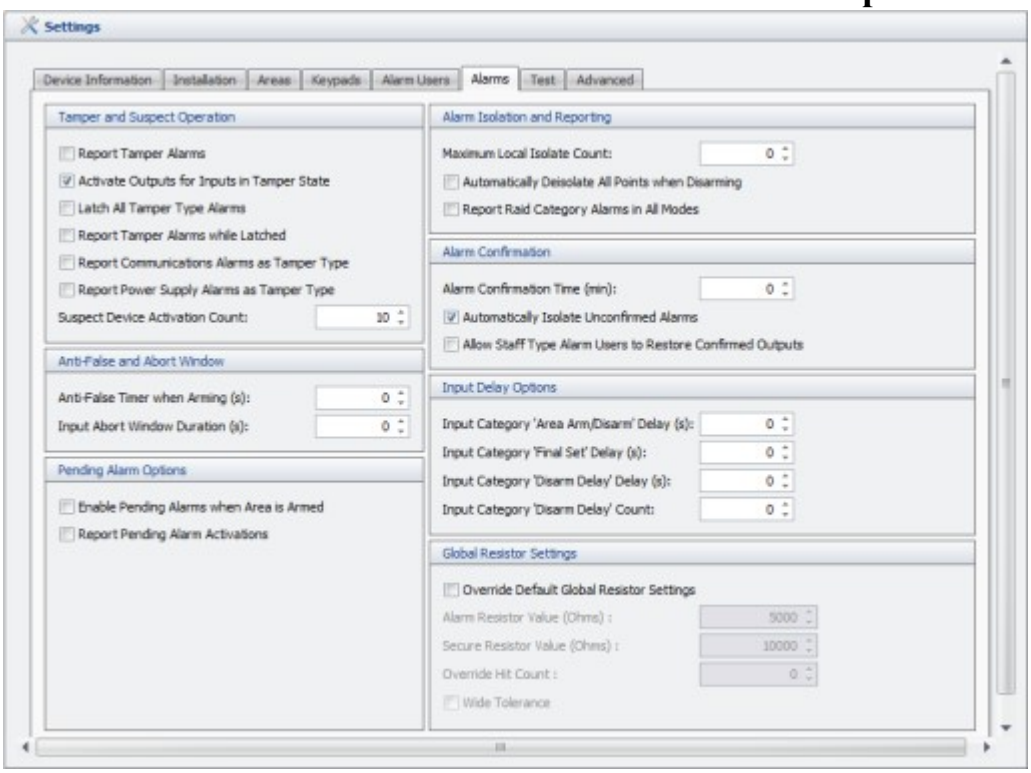
Ambush Timer (min)	The length of time that the user has to disarm the system from the Keypad and press the Enter key before an ambush signal is sent to the monitoring center. Set to 0 to disable. Range is 0 to 255 minutes.
User Duress Options	Specifies the duress options to use when entering PIN codes on an alarm keypad.
Duress Digit	Only used if **User Duress Options** is set to **Specific Last Digit**. Specifies the digit to use as the last digit if this Duress option is used. Range is 0 to 9.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Alarms

Settings - Alarms

Alarm settings for Pacom 8001/8002 Controllers.

Control **Description**



Tamper and Suspect Operation

Report Tamper Alarms	If set, open circuit, short circuit and trouble states are reported as tamper alarms. If unset, these states are reported as normal alarms. Click to toggle. ☑ = option enabled.
Activate Outputs for Inputs in Tamper State	If set, outputs linked to inputs through output macros are activated when inputs goes into a tamper type state (open, short, trouble) as well as a normal alarm state. Click to

	toggle. ☑ = option enabled.
Latch All Tamper Type Alarms	If set, any tamper type alarm is latched when it occurs and has to be manually restored. Click to toggle. = option enabled.
Report Tamper Alarms while Latched	If set, all tamper type alarms will continue to report tamper alarm messages even when latched to allow the system to automatically isolate the point tamper alarm if it exceeds the Suspect Device Activation Counter setting, which generally indicates a fault. Click to toggle. ☑ = option enabled.
Report Communications Alarms as Tamper Type	If set, all communication type alarms (Communication Errors) will be treated as tamper type alarms. Click to toggle. ☑ = option enabled. **Note**: This option is required to be set for EN50131 and NFa2p compliance.
Report Power Supply Alarms as Tamper Type	If set, all power supply type alarms will be treated as tamper type alarms. Click to toggle. ☑ = option enabled. **Note**: This option is required to be set for EN50131 and NFa2p compliance.
Suspect Device Activation Count	The number of times over a 30 second period that if an input or device activates then deactivates, it is reported as faulty and is automatically isolated. Suspect devices must be restored in order to resume normal operation. Range is 0 to 127.
Anti-False and Abort Window	
Anti-False Timer when Arming (s)	The length of time associated with the Anti-False Alarm settings that are added to the Exit Time setting to allow Perimeter or PIR Perimeter points time to settle and restore after an exit. If users are allowed to isolate points locally and a point is still in alarm after the Exit Time and Anti-False Timer have expired, then the point(s) are automatically isolated and a corresponding message is sent to the monitoring center. If users are not allowed to isolate points locally and a point is still in alarm after the Exit Time and Anti-False Timer have expired, then a full alarm is sent to the monitoring center. Range is 0 to 255 seconds.
Input Abort Window Duration (s)	The length of time to allow for a triggered input that has been configured to utilize the abort window to be disarmed before an alarm is generated. Range is 0 to 255 seconds.
Pending Alarm Options	
Enable Pending Alarms when Area is Armed	If set, pending alarms can occur while areas are armed or restricted. If unset, pending alarms only occur while areas are disarmed.
	If set, pending (conditional) alarms will be reported. If

	unset, pending alarms will still occurs, but are not reported.
Report Pending Alarm Activations	The conditions for pending alarms (number of alarm counts and the time period that they must occur within) before reporting takes place is set in the area configuration.
Alarm Isolation and Reporting	
Maximum Local Isolate Count	The maximum number of points that can be isolated from a keypad. If the number is set to 0 (zero), then any number of points can be isolated. Range is 0 to 255.
Automatically Deisolate All Points when Disarming	If set, any isolated points are automatically deisolated when disarming locally using the keypad.
Report Raid Category Alarms in All Modes	If set, inputs with category set to Raid are always reported even in engineering and test mode.
Alarm Confirmation	
Alarm Confirmation Time (min)	The length of time to allow for a point to remain in alarm in order for it to be "confirmed" by another alarm activation within the same alarm area. If the alarm is not confirmed, it is automatically isolated and a message is sent to the monitoring center notifying of the isolation. If the point is restored, the timer continues counting down and, if another point goes into alarm within this time period, then both alarms are reported immediately. Range is 0 to 255 minutes.
Automatically Isolate Unconfirmed Alarms	If set, it allows the system to automatically isolate alarm points that are not confirmed within the Alarm Confirm Time setting. Click to toggle. ☑ = option enabled. **Note**: This option is required to be unset for EN50131 compliance.
Allow Staff Type Alarm Users to Restore Confirmed Outputs	If set, staff alarm type users are allowed to restore latched confirmed outputs. Click to toggle. ☑ = option enabled. **Note**: This option is required to be set for EN50131 grade 3 compliance and unset for grade 2 compliance.
Input Delay Options	
Input Category 'Area Arm/Disarm' Delay (s)	The length of time to allow for any Set/Unset type inputs to fully settle upon activation or deactivation. Range is 0 to 15 seconds.
Input Category 'Final Set' Delay (s)	The length of time to allow for any Final Set type inputs to fully settle upon activation or deactivation. Range is 0 to 15 seconds.
Input Category 'Disarm Delay' Delay (s)	The length of time that applies to any Disarm Delay category point to allow before the system transmits an alarm to the monitoring center and optionally starts the Keypad sonalert. Range is 0 to 3,780 seconds.
	The number of Disarm Delay input category alarms

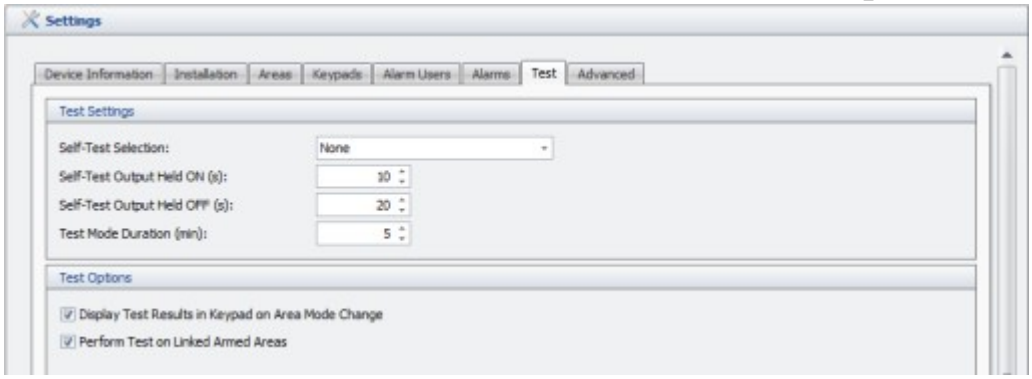
Input Category 'Disarm Delay' Count	allowed in a one disarm period (set to 0 for timer only operation). If this count is reached, then the alarm is sent immediately without delay. Range is 0 to 7.
Global Resistor Settings	
Override Default Global Resistor Settings	If enabled, the **Alarm Resistor Value**, **Secure Resistor Value**, **Override Hit Count** and **Wide Tolerance** properties will be used. If disabled, the default values are used. Click to toggle. ☑ = option enabled.
Alarm Resistor Value (Ohms)	The resistance value when a point is in alarm (in Ohms). Range is 0 to 100,000. Default is 5000.
Secure Resistor Value (Ohms)	The resistance value when a point is in secure (in Ohms). Range is 0 to 25,500. Default is 10,000.
Override Hit Count	The input hit count value. The hit count value is the total number of consecutive measurements with X ms intervals that the same value needs to be measured in order for the input to switch to a different state. A lower value means a more sensitive input, but which may also more easily trigger false alarms based on noise. A higher value means a less sensitive input, but which may also miss to detect a real alarm if it happens very fast. Range is 0 to 16.
Wide Tolerance	Use wider resistor tolerance settings when determining if the point is in trouble state. Click to toggle. ☑ = option enabled.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Test

Settings - Test

Test settings for Pacom 8001/8002 Controllers.

Control	Description



Test Settings

Self-Test Selection	Determines the self-test options for areas.
	The number of seconds an output designated to be a test

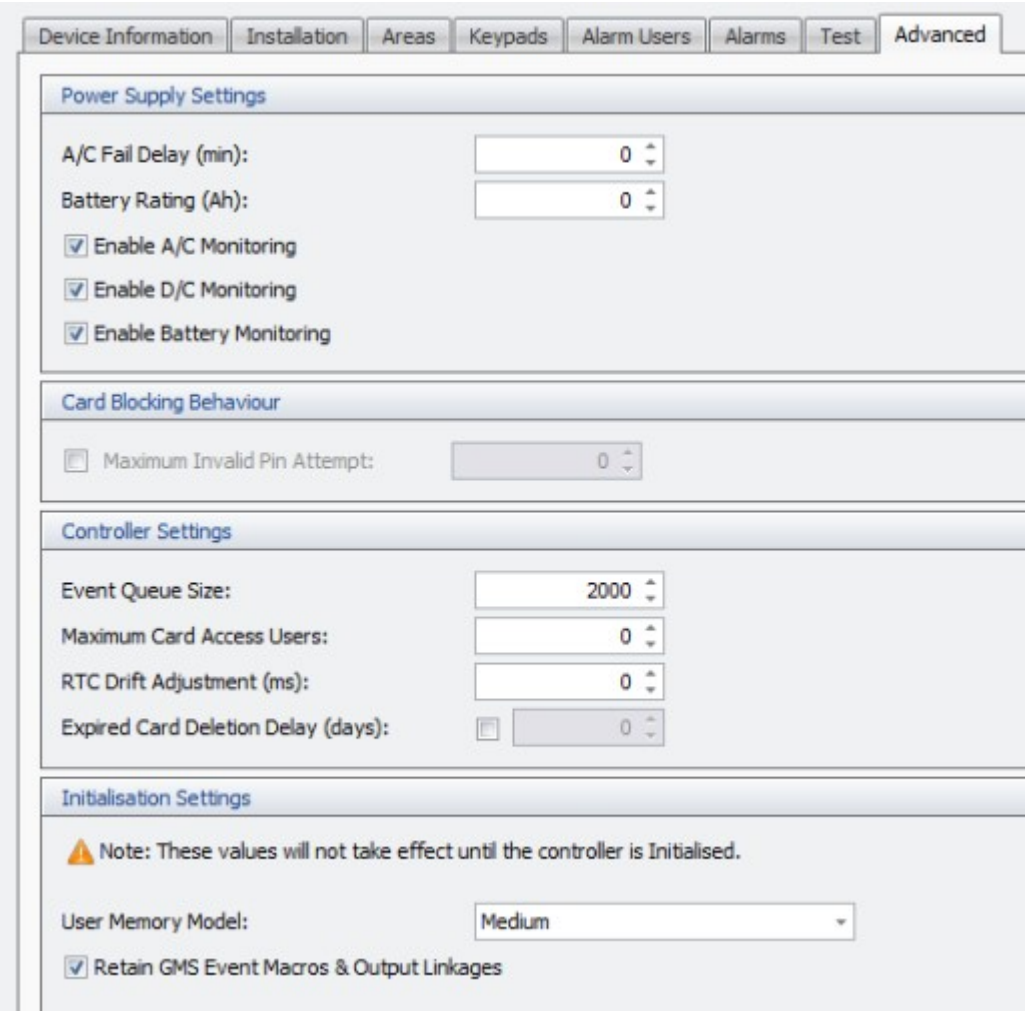
Self-Test Output Held ON (s)	output is held ON when an input point test is performed. Range is 1 to 120 seconds.
Self-Test Output Held OFF (s)	The number of seconds an output designated to be a test output is held OFF after being ON when an input point test is performed. Range is 1 to 120 seconds.
Test Mode Duration (min)	The time to allow systems users to complete Test mode. A warning on the keypad occurs 60 seconds before expiry. A timeout alarm is sent if this time expires and the area returns to being disarmed. Range is 0 to 255 minutes.
Test Options	
Display Test Results in Keypad on Area Mode Change	If set, the keypad displays any failed test results as a result of any selected self-test on mode change options. If any self-test on mode change option is set, the test will be performed in the background in any case but unless this option is enabled, the keypad user will not be made aware of the results, nor prompted for any further action. Click to toggle. ☑ = option enabled.
Perform Test on Linked Armed Areas	If set, the system checks for points in any linked areas when an area is armed if they have seen movement during the day and reports a test failed message for them if they haven't. Click to toggle. ☑ = option enabled. **Note**: This is linked to the input "Self Test while Inactive" option, where points are monitored for activity while the area is disarmed.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Advanced

Settings - Advanced

Advanced settings for Pacom 8001/8002 Controllers.

Control	Description



Power Supply Settings

A/C Fail Delay (min)	Sets a delay time for AC Fail alarms, if required. This is to provide an amount of time after the fault occurs to rectify the problem locally before an alarm is reported to a monitoring center. Range is 0 to 255 minutes.
Battery Rating (Ah)	Used for Pacom 1057 and 1058 type Controllers to set the connected external battery's rating in Ah (Amp-Hours). This is used when doing self-test of the battery to determine its current status. Range is 0 to 9,999.
Enable A/C Monitoring	Used for Pacom 1057 and 1058 type Controllers to enable/disable AC monitoring. Click to toggle. ☑ = option enabled.
Enable D/C Monitoring	Used for Pacom 1057 and 1058 type Controllers to enable/disable DC monitoring. Click to toggle. ☑ = option enabled.
Enable Battery Monitoring	Used for Pacom 1057 and 1058 type Controllers to enable/disable Battery monitoring. Click to toggle. ☑ = option enabled.

Card Blocking Behaviour

Maximum Invalid Pin	Sets the maximum number of attempts allowed for entering a Pin. When the maximum number of attempts is reached,

Attempt	the Controller blocks the card. Click to toggle. ☑ = option enabled. Default value is 0. Range is 0 to 15.
Controller Settings	
Event Queue Size	Total number of events that the Controller is able to store locally. The maximum number of events that can be stored depends on the Controller type and if expansion memory is used or not. This is stored in the Controller as multiples of 1000 events (i.e. a value of 1 is 1000 events). Range is 1000 to 128,000.
Maximum Card Access Users	Total number of card access users that the Controller is able to store locally. The maximum number of cards that can be stored depends on the Controller type and if expansion memory is used or not. This is stored in the Controller as multiples of 1000 users (i.e. a value of 1 is 1000 users), but sent as the raw value. Set to 0 to allow for maximum number of users. Range is 0 to 250,000.
RTC Drift Adjustment (ms)	Sets a drift adjustment value for the real time clock in the Controller. This can be used if the real time clock in the Controller is drifting too much over the course of a day, however this is only relevant when the Controller is offline to Unison otherwise regular time-sets will occur. Set to 0 to allow for the Controller to automatically adjust the time drift based on time set commands. Range is -12,800 to 12,700.
Expired Card Deletion Days (days)	When enabled, sets the number of days the controller will retain an expired card before it is deleted. Range is 0 to 63. Click to toggle. ☑ = option enabled.
Initialisation Settings	
Note: The initialisation settings will not take effect until the controller is initialised.	
User Memory Model	The current user memory model in use by the controller. The following are the possible values: None: Memory model not initialized properly. Small: Allows 64-bit card numbers, 8 access levels. This is the default for the 1058. Medium (default): Allows 64-bit card numbers, 24 access levels. This is the default for the 1057/8001/8002. Large: Allows 256-bit card numbers, 32 access levels.
Retain GMS Event	When enabled, Event Macros and Output Linkages will be deleted in the Controller when a "Full Initialize" command is executed. The Controller will also be prevented from

Macros & Output Linkages	migrating Event Macros and Output Linkages from the old (GMS) format to the new (Unison) format when an "Import" or "Import and Initialize" command is executed (leaving them in GMS format). Click to toggle. ☑ = option enabled.

8002 Events

Control	Description
Events Tab - One or more "generic" events may apply. Normal event configuration procedures apply. Click here for help. Additional events, if any, are listed below.	
Dependencies Tab - Lists any dependencies on the node. Normal node dependency procedures apply. Click here for help.	
Actions Tab - Lists any event response actions that have been created for the node. Normal node action configuration procedures apply. Click here for help.	
Scheduled Commands Tab - Lists any scheduled commands that have been created for the node that are yet to be processed.Click here for help.	
Notes Tab - Normal note configuration procedures apply.Click here for help.	
Alarm Queue Full	Warning - alarm queue at maximum capacity for storing unreported alarms - may create risk of lost alarms.
Auto-Set Devices Fail	Failure - automatic arming failed due to one or more devices being in an alarm state.
Battery Fail	Warning - device backup battery voltage below acceptable levels (normally <10.8VDC).
Battery Missing	Warning - Controller backup battery cannot be detected.
Battery Test Fail	Failure - Controller backup battery failed testing.
Battery Test in Progress	Information - Controller backup battery test started. Event active while test in progress.
Card Database 90% Full	Warning - Controller memory for access control database almost full. Increase available memory.
	Warning - Controller memory

Card Database Full	available to access control data is full. Increase available memory.
Card Deleted	Information - access card removed from Controller access card database.
Communication Path Test Fail	Failure - fault detected during communication path test to head system.
Configuration Changed	Information - device configuration changed.
Configuration Fail	Information - error occurred during configuration download or configuration conflict - configuration not loaded.
Device Isolated on Mode Change	Warning - device connected to Controller "isolated" due to alarm state when alarm area mode changed.
Device Replaced	Device Substitution alarm has been triggered on the device.
Disarm in Hardware	Disarm in Hardware.
EEPROM Error	Warning - error detected in Controller internal memory.
Final Set Fail	Warning - arming of area using "final set" input failed.
Firmware Download	Information - firmware currently downloading to device. Event active as long as download in progress.
Firmware Update Needed	Information - Controller firmware not up-to-date. Firmware Upgrade recommended.
Firmware Version Error	Warning - Controller firmware currently in use is not compatible with Unison software. Firmware upgrade necessary for correct operation.
Fuse Fail	Failure - failure of one or more associated power supply fuses.
General Fail	Warning -
GMS Connected	Information - connection established to Pacom GMS security management software.
	Warning - Controller configuration at hardware level different to

Import Configuration Needed	configuration stored in Unison. Run "Import Configuration" command. Usually occurs after a firmware update or a configuration change was done outside of Unison.
Initialize or Import Initialize needed	Warning - Controller configuration at hardware level different to configuration stored in Unison. Run "initialize" command. Triggered under the following circumstances: • The Controller hardware has been replaced • The controller was defaulted (factory default settings) • Unison was upgraded, an initialize is needed to synchronize the controller & Unison configuration data • The controller has been offline for more than two days (In this case Unison will automatically synchronize the controller) • Unison has failed over to a backup server (In this case Unison will automatically synchronize the controller)
Initializing	Information - Initialize command is running.
Invalid Card Database Version (<5.00)	Warning - Controller restarted using outdated database version, after having run newer version - delete old access card database version.
Key Switch	Alarm - interference with Controller housing key switch detected.
License Grace Status	Information - Controller license grace period expires soon/expired. License-based functions inoperable until properly licensed.
License Invalid	Information - Controller license for one or more functions not valid.

	Update license.
Log On Fail - System Busy	Failure - Controller log on to head system failed due to system being too busy.
Master Key Fail	Failure - authentication between Controller and head system failed due to incorrect main key code.
Master Key Updated	Information - main key for communication between Controller and head system updated.
Memory Card Fault	Failure - Controller memory expansion card failed.
Password Fail	Failure - authentication between Controller and head system failed due to incorrect password.
Power Fail	Failure - failure of (AC) mains power supply to device.
Power Supply Warning	Warning - power to Controller from power supply unit outside acceptable limits.
Rejected Configuration	Warning - configuration not accepted by Controller.
Reporting Fail	Warning - Controller unable to communicate with Unison or Base Station.
Restarted	Information - Controller restarted [switched off then on again].
Secondary Power Fail	Failure - Controller alternative power supply failed.
Temperature Alarm	Warning - Controller power supply temperature outside acceptable levels.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > 8003 Controller

8003 Controller

Pacom Edge Network nodes represent one or more items of Pacom 8003 Controller hardware, which are used to connect and control inputs and outputs, local keypads, doors etc. Nodes representing actual Controllers can be created and modified in the Pacom Edge Network device root node. Once a Controller node is created, the "sync" command must be performed to "prepare" the Controller to operate in conjunction with Unison. Choices exist to sync the Controller and apply the configuration for it

that exists in Unison [if available] or existing in the Controller [if available] - this is referred to as the "configuration source". When using the Controller as the "configuration source" it has been previously configured, its current hardware configuration is "read" by the Unison system, with corresponding child nodes automatically created.

- Adding a Pacom Edge Network node
- Commands

See Also: Configuring Pacom Hardware

8003 Properties

8003 Events

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > 8003 Properties

8003 Properties

Settings for Pacom 8003 Controller are available in the Properties section.

Control	Description
Properties Tab	
Properties - One or more "generic" node properties apply. Click here for help. Additional properties, if any, are listed below.	

Settings - Device Information

Settings - Installation

Settings - Door

Settings - Alarms

Settings - Reporting

Settings - Web Server

Settings - Advanced

Settings - Device Information

Device Information settings for Pacom 8003 Controllers.

Control	Description
General	
Device Type	Shows the Controller model.
Device Address	Shows the RS485 device address, if applicable.
Hardware Revision	Shows the Controller hardware [printed circuit board] revision number, if available.
Serial Number	Shows the Controller serial number, if available.
MAC Address	Shows the Controller MAC address, if available.
Firmware	
Active Firmware Version	Shows the firmware version that the Controller is operating on.
Inactive Firmware Version	Shows the secondary firmware version that is stored in the Controller, if available.
Active Chip	Shows the chip is being used to store the active firmware.
Memory	
Card Capacity (cards)	The maximum number of cards that can be downloaded to the controller.
Card Count	The current number of cards stored in the controller.
Maximum Supported Nodes	
Ports	Shows the number of Controller communications ports [Ethernet, RS485 etc] currently configured for use.
Inputs	Shows the total number of inputs that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Outputs	Shows the total number of outputs that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Doors	Shows the total number of doors that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.
Readers	Shows the total number of card readers that can be managed by the Controller. This is not the number actually in use. The number is dependent on the Controller model or license.

Settings - Installation

Installation settings for Pacom 8003 Controllers.

Control	Description
Controller Settings	
Controller Site ID	ID of the Site this Controller belongs to. This is used when reporting the Site ID to 3rd party monitoring centres or for certain configurations where multiple controllers are set up to work together as a single system. 8003 Controllers only supports SiteId as an integer from 1-9999.
Password	Sets the authentication password used to establish communication with the Pacom Controller (default is "Pacom"). To edit, click the field and enter a value. **Note**: The password must correspond to that stored within the Controller password list as "password 8", which is reserved for connection to Unison.
Timezone	Sets the timezone that applies to the Pacom Controller, which is usually determined by geographical location (default is the Unison server timezone). To edit, click ▾ for options. Click an option to select it.
Auto-Configure Device Loop	If enabled, the Controller will automatically autodetect and configure any new peripheral device that is connected on the device loop. Click to toggle. ☑ = option enabled.
Network Settings	
Media	Sets the connection type to use for communications with the Pacom Controller. To edit, click ▾ for options. Click an option to select it (**Network TCP/IP** supported only):
IP Address	Sets the device Ethernet network IP address. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, click the field and enter a value.
IPv6	Determines if the IP address uses version 6 notation [for networks that use "IPv6" addresses]. Click to toggle. ☑ = option enabled.

Port	Specifies the identification number of the Controller device IP port that is being used for communicating with the system (typically "3435"). To edit, double-click the field and enter a value. **Note**: If multiple instances of the device driver are to be used, each instance must use a unique IP port. IP port settings must also be set in the Pacom Controller.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Door

Settings - Door

Door settings for Pacom 8003 Controllers.

Control	Description
Door Settings	
Enable Strike Input Door 1	Enables the strike input for Door 1. Click to toggle. ☑ = option enabled.
Enable Strike Input Door 2	Enables the strike input for Door 2. Click to toggle. ☑ = option enabled.
Reader Inactivity Timeout (s)	The maximum time between key presses when entering a PIN on an access keypad.
Reader Number of PIN Digits	The number of digits that are present in an access PIN.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Alarms

Settings - Alarms

Alarm settings for Pacom 8003 Controllers.

Control	Description
Latch Alarms	
Latch Offline Alarms	If checked, device offline alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Primary Power	If checked, any primary power source alarms (AC Fail, AC Voltage High / Low) need to be sent a restore command

Source Alarms	from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Secondary Power Source Alarms	If checked, any battery alarms (Battery Fail, Battery Voltage High / Low) need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Battery Charger Fail Alarms	If checked, any battery charger fail alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Fuse Fail Alarms	If checked, any fuse fail alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Internal Battery Low Alarms	If checked, any internal battery alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Temperature Alarms	If checked, any power source temperature alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Reporting Fail Alarms	If checked, any controller connection offline alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Signal Fail Alarms	If checked, any GPRS card "Signal Low / No Network" alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Latch Inovonics Alarms	If checked, any Inovonics specific alarms (Smoke detector cleaning, etc.) need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Tamper	
Latch Tamper Alarms	If checked, tamper alarms need to be sent a restore command from a remote system or be manually restored from a keypad to be restored to normal state after activation.
Tamper Hit Count	The number of consecutive readings required before a tamper event is reported. Default is 3.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > Settings - Reporting

Settings - Reporting

Reporting settings for Pacom 8003 Controllers.

Control	Description
General	
Report Invalid PINs	If enabled, the Controller will report all invalid user ID/PIN combinations entered into a keypad. Click to toggle. ☑ = option enabled.
Report Offline Devices Immediately	If disabled, the controller will give devices approximately 30 seconds to come back online before generating an offline message. Click to toggle. ☑ = option enabled.
Power Fail Reporting Delay (s)	Specified a time to hold off reporting an AC fail condition. If AC mains are restored before this time expires, no event is generated.
SIA Over IP	
Include Timestamp	SIA DC-09 - Include timestamp in any un-encrypted messages. Click to toggle. ☑ = option enabled.
Include MAC Address	SIA DC-09 - Include MAC address in any SIA-DCS / ADM-CID message sent by the controller to CSR. Click to toggle. ☑ = option enabled.
GPRS Data Usage	
Frequency	The frequency in which the GPRS data usage is reset to zero.
Start Date	The day from which the GPRS data usage reporting should start (local time), e.g.: billing cycle start.
Contact ID Settings	
Use Site ID as Account Number	Use the Site ID as the Contact ID / SIA Account Number. Click to toggle. ☑ = option enabled.
Account Number	The Account Number to use if not using the Site ID.
Heartbeat Time	The time of day to send a heartbeat message for CID / SIA connections. The heartbeat will be randomized +/- 30mins.
Heartbeat Interval (s)	The time between heartbeat messages for CID / SIA connections or 0 if not required. If this is non 0, the ContactIdHeartbeatTime is ignored.
Fallback Reporting	
Fallback Reporting Heartbeat Required	Enable this option if a heartbeat is required on non-active connections. Click to toggle. ☑ = option enabled.
Heartbeat Time	The time of day to send a heartbeat message. The heartbeat will be randomized +/- 30mins.
Heartbeat Interval	The time between heartbeat messages or 0 if not required. If this is non 0, the FallbackReportingHeartbeatTime is ignored.

Settings - Web Server

Web Server settings for Pacom 8003 Controllers.

Control	Description
Web Server Settings	
Enable Web Server	Determines whether the web server should be running on the controller or not. Click to toggle. ☑ = option enabled.
Web Server Local Connect Only	Limit the connections to the web server to those that match the local subnet mask. Click to toggle. ☑ = option enabled.
Web Server TCP/IP Port	The IP port number to run the web server on.
Web Server Password	The password to use to secure the web server.
Logging	
Logging Level	Determines the types of error messages that are logged on the controller. To edit, click ▾ for options. Click an option to select it
Debug Log Sub Categories	Determines the types of debug messages that are logged on the controller. This is only applicable if the LoggingLevel is set to Debug. To edit, click ▾ for options. Click an option to select it
Syslog Server Address	The IP address or computer name of the Syslog server.

Settings - Advanced

Advanced settings for Pacom 8003 Controllers.

Control	Description
Advanced Settings	
Compliance Level	The compliance level used for default parameters and ranges. To edit, click ▾ for options. Click an option to select it
Duress Type	The duress type for user PIN: None, IncrementPinBy1, etc. To edit, click ▾ for options. Click an option to select it
Power Supply Type	The type of power supply attached to the controller's power status pin. To edit, click ▾ for options. Click an option to

	select it
Area	
Completion of Arming Required	If checked then when arming area(s) with delay the arming must happen in 2 steps: 1. The arming is initiated from inside the secured premises (e.g. from a keypad) 2. The completion of arming should happen once the user is outside the premises by using one of the following methods: a. Multi badge on a card reader b. Push button switch mounted outside the premises c. Door contact d. Digital key, etc. This should be enabled in order to meet BS 8243 standard's requirements.
De-isolate All Points in Alarm When Disarming	If checked all input points in alarm will be automatically de-isolated when the area/s are disarmed.
Keypad	
Keypad Operational Mode	The keypad state machine implementation kind: Pacom, EN, etc.
Alarm User PIN Length	Get / Set the alarm users mandatory PIN length.
Event Queue Capacity	Event queue capacity - the maximum number of events that is kept in memory and can be browsed from any alarm keypad.
Allow Commands And DTP without Keypad User	If checked, commands and DTP sessions from Pacom .is / Unison will only be accepted when a keypad operator is logged on. Required behaviour for EN.
Suspect Device	
Activate Suspect Device Auto-Latching	If checked, suspect count is active, and auto latching will be activated.
Suspect Device Alarm Count	Suspect device counter is setting number of alarms that a point/device can trigger and after which the point/device auto latches.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controllers > 8003 Events

8003 Events

Control	Description
Events Tab - One or more "generic" events may apply. Normal event configuration procedures apply. Click here for help. Additional events, if any, are listed below. Dependencies Tab - Lists any dependencies on the node. Normal node dependency procedures apply. Click here for help. Actions Tab - Lists any event response actions that have been created for the node. Normal node action configuration procedures apply. Click here for help. Scheduled Commands Tab - Lists any scheduled commands that have been created for the node that are yet to be processed.Click here for help. Notes Tab - Normal note configuration procedures apply.Click here for help.	
Alarm Queue Full	Warning - alarm queue at maximum capacity for storing unreported alarms - may create risk of lost alarms.
Battery Charger Fail	Fault - A device has generated a battery charger fail alarm.
Battery Fail	Fault - device backup battery voltage below acceptable levels (normally <10.8VDC).
Battery Pre-warning Time	Information - A device has generated a battery warning alarm.
Card Database 90% Full	Warning - Controller memory for access control database almost full. Increase available memory.
Card Database Full	Warning - Controller memory available to access control data is full. Increase available memory.
Communication Error	Warning - Communications between the Unison system database or device server and the device is unavailable.
Communication Path Test Fail	Failure - Fault detected during communication path test to head system.
Communication Path Test OK	Communication path test to head system succeeded.
Disarmed	Information - event messages from the device/node are currently being ignored locally in the Unison system. No disarming has taken place externally in the hardware and underlying nodes are not affected [that is, they continue to operate as normal]. Selecting the **Disarm...** option will disarm the

	node to the set time.
Disarmed by Area	Information - the device/node is disarmed by the alarm status [armed/disarmed etc] of the area it is a member of; that is, it is following the parent area status. Areas are "virtual" nodes, defined locally within the system, that are used to control groups of "member" nodes. The status does not affect areas that are defined externally in the hardware.
Disarmed in Hardware	Information - event messages from the device/node are currently not being sent externally from the hardware. That is, for hardware that supports isolating certain functions or events, these have been, in effect, switched "off".
Ethernet Disconnected	The Ethernet cable was disconnected from the controller.
Firmware Download	Information - firmware currently downloading to device. Event active as long as download in progress.
Firmware Update Needed	Information - Controller firmware not up-to-date. Firmware Upgrade recommended.
Internal Battery Fail	Fault - The controller's internal battery / memory backup battery has failed.
Password Fail	Failure - authentication between Controller and head system failed due to incorrect password.
Power Fail	Failure - failure of (AC) mains power supply to device.
Rejected Configuration	Warning - configuration not accepted by Controller.
Reporting Fail - Connection 1	Warning - Controller unable to communicate with Unison or Base Station.
Reporting Fail - Connection 2	Warning - Controller unable to communicate with Unison or Base Station.
Restarted	Information - Controller restarted [switched off then on again].

Sync in progress	Sync Upload or Download command in is progress.
Sync Needed	Controller needs to be synchronized with Unison. This can be done by performing a Sync Download, or performing a Sync Upload followed by a Sync Download.
Tamper	Tamper alarm has been triggered on the device.
Time Changed	The controller date time was updated.

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controller Expansion Cards

Controller Expansion Cards

Note: Some Controller expansion cards detailed below may not be supported.

Pacom Controllers have on-board expansion slots for compatible Pacom expansion cards (also known as "mezzanine" cards). Expansion cards are designed as modular add-on devices for Controllers and some peripheral devices to increase capacity or functionality. For example, to "upgrade" an 8001/8002 Controller to use the GPRS data network, install an 8201 GPRS expansion card. Expansion card configuration is available through Pacom management software. Expansion cards have their own firmware, which is updated when it is plugged into the Controller.

Note: Not all expansion cards are compatible with all Controller expansion slots - see the Pacom Hardware Installation Guide topic for each specific expansion card to see which slots can be used. • Expansion cards draw power from the Controller (the device they are plugged in to). • Memory expansion cards are proprietary hardware and must be purchased through Pacom.

The following tables shows compatibility between Pacom Controller models and peripheral devices that support expansion cards, and available expansion cards.

Expansion Card	1057	1058	8001	8002	8003	1065	8501	8602	8603
1050R-003-UL	☑	☑	☐	☐	☐	☑	☐	☐	☐
1050R-004-UL	☑	☑	☐	☐	☐	☑	☐	☐	☐
1050-201-LL/1050-202*	☑	☑	☐	☐	☐	☐	☐	☐	☐
1057R-203-UL	☑	☑	☐	☐	☐	☐	☐	☐	☐
1057R-207-UL	☑	☑	☐	☐	☐	☐	☐	☐	☐
8201R-001-UL*	☐	☐	☑	☑	☑	☐	☐	☐	☐
8202R-001-UL*	☐	☐	☑	☑	☐	☐	☐	☐	☐

8203R-001-UL	☐	☐	☑	☑	☑	☐	☑	☑	☑
8204R-001-UL	☐	☐	☑	☑	☑	☐	☑	☑	☑
8205R-001-UL	☐	☐	☑	☑	☑	☐	☐	☐	☑
8207R-001-UL	☐	☐	☑	☑	☑	☐	☐	☐	☑
8208R-001	☐	☐	☑	☑	☐	☐	☐	☐	☐
8209R-001-UL*	☐	☐	☑	☑	☑	☐	☐	☐	☐
8220R-001	☐	☐	☐	☐	☑	☐	☑	☐	☑
8403R-001-UL	☐	☐	☑	☑	☐	☐	☐	☐	☐
8404R-001-UL	☐	☐	☐	☐	☑	☐	☐	☐	☑

* One expansion card of type per Controller.

1050R-003-UL 8-Output Card

The 1050R-003-UL is used to increase the number of alarm output points of Pacom 105x Controllers and 1065 I/O cards; providing eight relay controlled outputs.

1050R-004-UL 16-Input Card

The 1050R-004-UL is used to increase the number of alarm input points of Pacom 105x Controllers and 1065 I/O cards; providing 16 supervised alarm inputs. The inputs can report four states:

- Alarm.
- Open circuit.
- Short circuit.
- Trouble/tamper.

The EOL resistance is 10kOhm standard, however, can be altered by physically changing the on-board SIP resistor pack (from 3.3kOhm to 25.4kOhm).

1050-201-LL/1050-202 PSTN Modem Card

The 1050-201-LL/105-202 is a PSTN (public switched telephone network) modem that can be used with Pacom 105x Controllers [generally] for dial-backup communications to a Pacom Base Station, Pacom TransIT and/or for transmission of alarms to central station in Contact ID or SIA formats.

1057R-203-UL RS485 Star Coupler Card

The 1057R-203-UL is used to increase the number of RS485 device lines of Pacom 105x Controllers. It allows "star" connection using up to eight individual device lines and increases the total number of RS485 devices by 32.

Note: Leave all RS485 device lines unterminated.

1057R-207-UL 32MB Memory Card

The 1057R-207-UL is used to expand the on-board data storage capacity of Pacom 105x Controllers. It increases the number of access card data (users/cardholders) and offline event details stored by the Controller. The 1057R-207-UL is battery backed-up to prevent data loss in the case of power failure.

- For 1058R-NC-UL, card capacity increases to 10000 and offline events to 128000.
- For 1057R-001-UL, card capacity increases to 256000 and offline events to 128000.

8201R-001-UL GPRS Modem Card

The 8201R-001-UL is a GPRS (general packet radio service) modem that can be used with Pacom 8001/8002 Controllers for backup communications [generally]. The GPRS system allows data packets to be sent wirelessly to a secure external IP network, thereby allowing commands and other data to be sent.

8202R-001-UL PSTN Modem Card

The 8202R-001-UL is a PSTN (public switched telephone network) modem that can be used with Pacom 8001/8002 Controllers for dial-backup communications to a Pacom Base Station, TransIT and/or for transmission of alarms to central station in Contact ID or SIA formats. It supports "listen-in" operation, where the Controller initiates connection with a Pacom management software operator who can listen to activity going on at the site by way of a microphone connected to the 8202R-001-UL, or through a Contact ID receiver.

8203R-001-UL 4-Output Card

The 8203R-001-UL is used to increase the number of alarm output points of Pacom 8001/8002 Controllers and 8501, 8602 and 8603 devices; providing four relay controlled outputs.

8204R-001-UL 8-Input Card

The 8204R-001-UL is used to increase the number of alarm input points of Pacom 8001/8002 Controllers and 8501, 8602 and 8603 devices; providing eight supervised alarm inputs. All inputs can be configured for analog operation (0 to 8VDC). The inputs can report five states:

- Alarm.
- Open circuit.
- Secure/reset (normal).
- Short circuit.
- Trouble/tamper.

The EOL resistance is 10kOhm standard, however, can be altered by physically changing the on-board SIP resistor pack (from 3.3kOhm to 25.4kOhm) or programmatically through Pacom management software.

8205R-001-UL RS232/RS485 Comms Card

The 8205R-001-UL is used to add an additional RS232 or RS485 device lines to Pacom 8001/8002 Controllers. It can also be used as an interface to third-party systems, such as Inovonics wireless, DVRs and elevator management systems etc.

8207R-001-UL RS485 Star Coupler Card

The 8207R-001-UL is used to increase the number of RS485 device lines of Pacom 8001/8002 Controllers. It allows "star" connection using up to four individual device lines and increases the total number of RS485 devices by 32.

Note: Leave all RS485 device lines unterminated.

8208R-001 S-ART Interface Card

The 8208R-001 is used to connect Serial-Addressable Receiver/Transmitter (S-ART) compatible devices (generally detectors) to Pacom 8001/8002 Controllers. The card has four S-ART interfaces, each of which can have up to 30 devices connected in a daisy-chain fashion, and supports a total of 120 inputs and 60 outputs per card.

S-ART interface is designed specially for security systems for data transmission on a simple cable where it is desired to individually identify each detector on the interface. The cable transmits both DC power to the S-ART and information to/from the S-ART. Communications works on the principle by which an address is sent and the S-ART that recognizes the address then carries out the instruction. The line signal is divided into three levels in order to give a time signal for synchronizing and a data signal containing addresses, instructions etc. Typical signal voltages for the three levels are 15V, 7.5V and 0V.

8209R-001-UL PSTN Modem Card

Pacom 8209R-001-UL is a PSTN (public switched telephone network) modem, that can be used with Pacom 8000 Series Controllers for dial-backup communications to a Pacom Site Manager/"EMCS", Base Station, TransIT and/or for transmission of alarms to central stations in Contact ID or SIA formats. It supports "listen-in" operation, where the Controller initiates connection with a Pacom management software operator who can listen to activity going on at the site by way of a microphone connected to the 8209R-001-UL, or through a Contact ID receiver.

8220R-001 Expansion Card Adaptor

The 8220R-001 enables two expansion card connections using a single expansion card slot on Pacom 8003 Controllers and 8501 and 8603 devices. In this manner, it is possible to increase the available functionality of the Controller/device by it having up to four expansion cards, instead of two.

Note: The 8220R-001 EXP2 slot can accept any Pacom expansion card. The EXP2 slot can accept 8203R-001-UL, 8204R-001-UL or 8208R-001 [input/output functionality] expansion cards only.

8403R-001-UL 64MB Memory Card

The 8403R-001-UL is used to expand the on-board data storage capacity of Pacom 8001R-001-L-UL/8002R-001-L-UL Controllers by 64MB. It increases the number of access card data (users/cardholders) stored by the Controller to 256000/†200000 and offline event details to 128000. The 8403R-001-UL is battery backed-up to prevent data loss in the case of power failure.

† Limitations when using the Pacom Unison security management system.

8404R-001-UL 1GB Micro SD Card

The 8404R-001-UL is an "industrial grade" micro SD memory card used to expand the on-board data storage capacity of Pacom 8003 Controllers and 8603 devices by 1GB. It increases the number of access card data (users/cardholders) stored by the Controller/device to 500000 and offline event details (Controllers only) to 50000.

See Also: 8204 Input Expansion | 8203 Output Expansion

8203 Output Expansion

8204 Input Expansion

8208 S-ART Expansion

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controller Expansion Cards > 8203 Output Expansion

8203 Output Expansion

The 8203 output expansion provides four output connections.

Note: Devices are generally treated using multiple node types. The "device" node represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

Management, Configuration and Commands

See Also: Controller Expansion Cards

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controller Expansion Cards > 8204 Input Expansion

8204 Input Expansion

The 8204 input expansion provides eight input connections.

Note: Devices are generally treated using multiple node types. The "device" node represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

Management, Configuration and Commands

See Also: Controller Expansion Cards

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Controller Expansion Cards > 8208 S-ART Expansion

8208 S-ART Expansion

The Serial-Addressable Receiver/Transmitter (S-ART) interface is designed specially for security systems for data transmission on a simple cable where it is required to individually identify each input on the interface. Communications works on the principle by which an address is sent and the S-ART that recognizes the address then carries out the instruction. S-ART interface is available to 8001/8002 Controllers through Pacom 8208 S-ART interface expansion cards.

S-ART devices may have differing configurations of input and output connections. Each S-ART input in the Pacom system represents a pair of physical inputs on the S-ART device. The two inputs provide combinations to represent normal, alarm, open circuit and short circuit states. If the device does not respond to polling, it is considered in a trouble state. The 8208 has four S-ART interfaces that each support 30 addresses, which includes the physical device plus one input pair and associated output. If there is more than one input pair/output on the device, these will use another address per input pair/output. That is, a single S-ART device with one input pair and one output reserves one address; a single S-ART device with two input pairs and two outputs reserves two addresses.

Note: If an address is being used by more than one S-ART device (address conflict), alarms from them will not be reported. • Due to the 30 device limit per S-ART interface and the logical address blocks of 32 used by the system, the last two

addresses for each block are skipped.

The addresses available per interface are:

Interface 1 - Address 1 to 30.

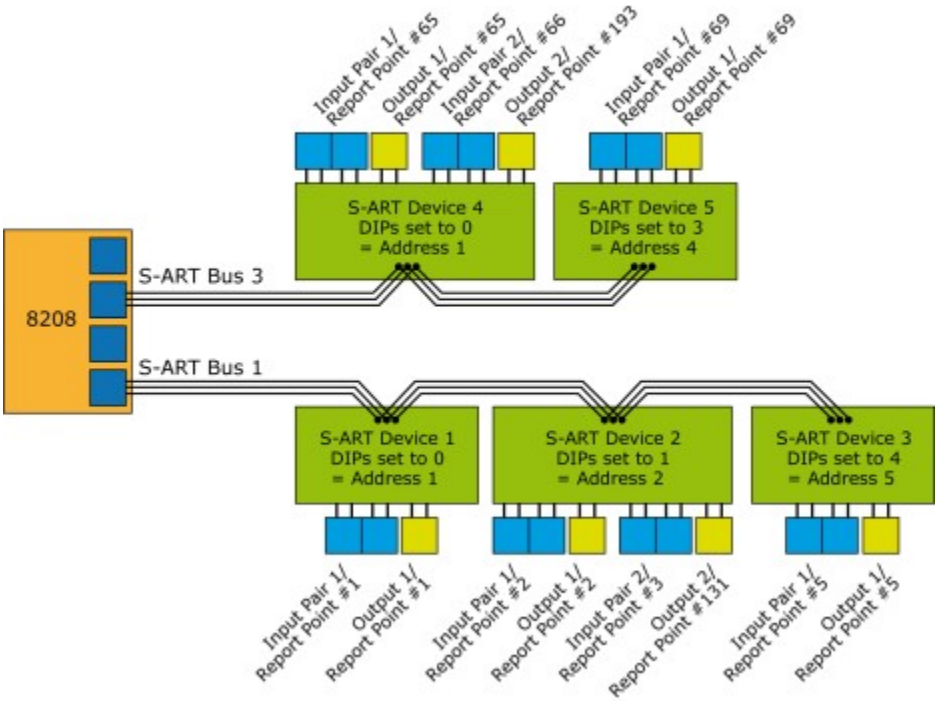
Interface 2 - Address 33 to 62.

Interface 3 - Address 65 to 94.

Interface 4 - Address 97 to 126.

Note: Due to the limit of 256 input and 64 output points that a Controller can support and the possible number of additional input and output points that S-ART interfaces can provide, it is important to map input/output addresses carefully in order to avoid reserving addresses in the Controller that are unused by S-ART devices. • Unused inputs/outputs on S-ART devices still use an address. • For S-ART devices that have more than one output, the additional outputs are reported with an offset of 128 - refer to the diagram below for examples.

Input pairs and output points on each S-ART device are reported in the Pacom system using the 8208 interface number it is connected to and the device address as the basis. For example, if a S-ART device with two input pairs is attached to interface 1 and addressed as "16", the input pairs are reported as "16" and "17". The following example shows a single 8208 with two S-ART interfaces in use (1 and 3), with three S-ART devices on interface 1 and two on interface 3. Observe the reported point numbers based on the interface number and device address.



Note: Devices are generally treated using multiple node types. The "device" node

represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

Management, Configuration and Commands

See Also: Controller Expansion Cards

Peripheral Devices

Note: Some peripheral devices detailed below may not be supported.

Pacom peripheral devices are designed to perform specific security system functions, such as door, elevator and vault control. They are wired to the Controller and have bi-directional communications with it for the purposes of sending events and responding to commands/instructions received from the Controller. Some peripheral devices also further expand system capability by adding input/output points to the system. Pacom peripheral devices communicate with the local Controller using RS485. "Pacom-edge" devices also support Ethernet connectivity to the local Controller.

Note: Most peripheral devices are designed to be mounted in enclosures, which can be supplied as part of the product and also use a variation to the part number quoted in this document. • Not all devices listed in this document may be available in all regions. This is due mainly to compliance and other regulatory requirements.

1064R-002-UL Single Door Controller

The 1064R-002-UL is an interface between the Controller and a single third-party card reader device and door. It has four input and two output connections for door control, card reader LED and buzzer control and alarm reporting. The 1064R-002-UL features on-board memory that can be configured for "degraded mode" operation, in that the device stores details of the last 256 valid access cards and/or facility codes used (based on the 26-bit Wiegand format), enabling it to operate at a limited level if offline to the Controller.

Input/Output (I/O) Operation

Due to the input/output capability, the 1064R-002-UL can also be used as an input/output expansion device when connected to a Pacom Controller - in "I/O" mode, the device supports up to six inputs (4 x EOL monitored and 2 x open collector) and

four outputs.

1064R-EFM-UL Elevator Floor Monitor

The 1064R-EFM-UL is used to indicate to the Controller which floor an elevator car is on. As an elevator passes a floor, a sensor that is attached to an 1064R-EFM-UL input is momentarily shorted, causing the signal. The six inputs of the 1064R-EFM-UL are wired for each floor to provide a sequential binary number, enabling it to monitor up to 64 floors. End of line resistors are not required.

1065R-001-UL 16-Input/4-Output

The 1065R-001-UL is used to increase the number of alarm input/output points of any Pacom Controller; providing 16 supervised alarm inputs and four outputs. The input/output capacity of the 1065R-001-UL can also be increased by installing up to two Pacom 1050R-003-UL (8-Output Controller expansion card)/1050R-004-UL (16-Input Controller expansion card). These cards can be installed in any combination to increase the 1065R-001-UL input/output capacity to either 48 inputs and four outputs/32 inputs and 12 outputs/16 inputs and 20 outputs, depending on configuration.

Multiple 1068R-001-UL cards can be connected to 1065R-001-ULs via 1057R-203-UL RS485 star coupler cards in order to reduce the number of Controller "device configurations" used (total available = 64). In this type of configuration, the 1065R-001-UL acts as a "concentrator" for 1068R-001-UL inputs/outputs.

1065R-EC-UL Elevator Controller

The 1065R-EC-UL is used to control access to the floors serviced by an elevator, where a low-level elevator interface is used. This is carried out by interrupting the wiring between the elevator and its elevator control panel with relays, so that the Pacom system determines whether or not the elevator can be accessed, and may also determine which floors can be selected. Generally, a card reader is installed in the elevator car and when a valid card is swiped, the selection buttons for the floors authorized for that cardholder can be activated. Once a floor selection button is pressed, no other floor can be selected.

The 1065R-EC-UL requires 1050R-003-UL 8-output expansion card(s) in order to have the required number of relays for full control of floor selection. It may also be used without expansion cards, where it will control access to the elevator only, allowing the user to select any floor once their access card is validated. The 1065R-EC-UL also supports "apartment" operation. In this scenario, the person in the apartment can press a button to allow a visitor access to the floor that the apartment is on. When the visitor enters the elevator, only the floor that has granted the access is selectable.

When connected to a Controller, each 1065R-EC-UL can control access to up to 16 consecutively numbered floors. If an elevator services non-consecutive floors (for

example, floor 1 and floors 20 to 30), although it may be less than 16 floors in total, it may require two 1065R-EC-UL devices - one for each group of 16. A 1058R-xx-UL Controller can control access for up to two elevators. 1057R-001-UL, 8001R-001-x-UL and 8002R-001-x-UL Controllers can control access for up to 16 elevators (all Controllers have a limit of 128 floors per elevator).

1065R-EFM-UL Elevator Floor Monitor

The 1065R-EFM-UL is used to indicate which floor an elevator car is on to the Controller. As an elevator passes a floor, a sensor that is attached to an 1065R-EFM-UL input is momentarily shorted, causing the signal. The 1065R-EFM-UL has 16 inputs, with each input mapped to a specific floor, enabling it to monitor up to 16 floors. The first input should be wired to the lowest floor and each consecutive input to the next consecutive floor. If an elevator skips floors, then the corresponding input should not be wired up. Inputs connected directly to the 1065R-EFM-UL do not require EOL resistors.

Up to two additional 1050R-004-UL 16-Input expansion cards can be fitted to the 1065R-EFM-UL, allowing it to monitor up to 48 floors. Inputs connected to 1050R-004-UL cards require EOL resistors. The 1065R-EFM-UL AC Fail input is used to monitor the elevator "express" mode (that is, skipping the low rise elevator floors) output and report it to the Controller. This input should normally be supplied with 12V, it should be open circuit (or 0V) when the elevator is in express mode.

1068R-001-UL 2-Input/1-Output

The 1068R-001-UL is designed to increase the number of alarm input/output points of any Pacom Controller; providing two supervised alarm inputs and one output. 1068R-001-ULs can also be used to increase the security of remote alarm input devices such as PIRs, door contacts or seismic detectors in that it replaces the standard resistance monitored line to the Controller with an RS485 data link that can be encrypted, if required. It is constantly polled by the Controller and, if a valid response to the poll is not received, the Controller reports an alarm. By connecting detection devices to the security system in this way, the possibility of a device being tampered with or substituted without detection is virtually eliminated. The 1068R-001-UL is small enough to be housed inside the casing of most devices, comes with a universal mounting bracket, and has two inputs to allow monitoring of the device contact and an additional tamper switch.

The inputs support analog data (0 to 5VDC) and can be used to facilitate remote diagnostics via Pacom management software. It is equipped with an output relay that can be used to activate an LED and a buzzer for a seismic detector self-testing or a range of other purposes. The 1068R-001-UL can also be used as an interface for programming Inovonics devices.

Multiple 1068R-001-UL cards can be connected to 1065R-001-ULs via 1057R-203-UL RS485 star coupler cards in order to reduce the number of Controller "device configurations" used. In this type of configuration, the 1065R-001-UL acts as a

"concentrator" for 1068R-001-UL inputs/outputs. For 8001/8002 Controller firmware 1.08 and later, it is possible to use the full range of Controller inputs using 1068R-001-ULs only, which are physically connected to 8207R-001-UL RS485 star coupler expansion cards and are configured as "third-party" devices. In this way, up to 32 1068R-001-ULs can be connected in series on a single 8207R-001-UL RS485 device line.

Note: 1068R-001-UL outputs must be configured as per normal; that is, individual "device configurations" of device type "Pacom 1068". This means it is not possible to accommodate the full 256 inputs and 64 outputs using 1068R-001-UL cards only, as such a configuration requires all device configurations in order to have 64 outputs. That is, for each individual 1068R-001-UL, a device configuration is required for inputs and another device configuration is required for outputs. It is possible to support 63 outputs as there must be at least one device configuration for input definitions using the "third-party" device type. Similarly, if additional "third-party" device configurations are required for inputs, each one reduces the available device configurations by one. A maximum of four 8207R-001-UL RS485 ports can be supported by a single 8001/8002 Controller to provide 256 inputs (64 inputs per RS485 device loop x 4 ports), however, the maximum number of device configurations remaining for outputs is 60. To achieve a total of 64 outputs, it is possible to add a separate output configuration using, for example, a 1065R-001-UL.

1075R-001 PSTN Modem

The 1075R-001 is a PSTN (public switched telephone network) modem that can be connected to a Pacom Base Station CCU (Communications Controller Unit) card, Pacom TransIT or Pacom Controller, generally for providing a backup dialup communications link. It communicates with the connected device using RS232.

1076R-001-UL Two Door Controller

The 1076R-001-UL is an interface between the Controller and up to two third-party card reader devices (each can be a different type as they operate independently) and doors. It has eight input and four output connections for door control, card reader LED and buzzer control and alarm reporting. The 1076R-001-UL features on-board memory that can be configured for "degraded mode" operation, in that the device stores details of the last 1000 valid access cards and/or facility codes used (based on the 26-bit Wiegand format), enabling it to operate at a limited level if offline to the Controller. Additionally to door control inputs/outputs, the 1076R-001-UL has one supervised input and four outputs (two relay and two open collector) that can be configured as general purpose outputs (GPOs).

Input/Output (I/O) Operation

Due to the input/output capability, the 1076R-001-UL can also be used as an input/output expansion device when connected to a Pacom Controller - in "I/O" mode, the device supports up to eight inputs and four outputs.

1076R-IO-UL 8-Input/4-Output

The 1076R-IO-UL is used to increase the number of alarm input/output points of any Pacom Controller; providing eight supervised alarm inputs and four relay controlled outputs.

1076R-VC Vault Controller

The 1076R-VC is designed for connecting certain vault equipment (for example, seismic vibration detectors and vault doors) with Pacom Controllers. Connections to vault equipment are pre-defined and must be wired accordingly for correct operation. When a 1076R-VC is in use, additional configuration settings specific to vault control and operation become available in Pacom management software.

The 1076R-VC also supports the optional PD-DISP-01 vault controller display module. This module provides users with a simple LED display of vault controller status (state of the vault, timers etc).

8501R-001-UL 16-Input/5-Output

The 8501R-001-UL is used to increase the number of alarm input/output points of any Pacom Controller; providing 16 supervised alarm inputs and five outputs (two relay and three open collector). The input resistance is 10kOhm by default, however, can be programmed for any resistance between 1kOhm and 100kOhm. The 8501R-001-UL is a "Pacom-edge" device that communicates with the Controller using Ethernet (TCP/IP) and/or RS485. Ethernet support enables it to connect using existing IP infra-structure. It also features a RS232 serial port for IP/web-based configuration and a USB port.

The input/output capacity of the 8501R-001-UL can also be increased by installing up to two Pacom 8203R-001-UL (output)/8204R-001-UL (input) expansion cards. This can be further increased to four expansion cards by using two 8220R-001 expansion card adaptors.

Note: Future models of this device will feature optional door control operation [one door/two card readers]. When door control is used the number of inputs/outputs is reduced.

8602R-001 8-Input/4-Output/Door Controller

The 8602R-001 is used to increase the number of alarm input/output points of any Pacom Controller; providing eight supervised alarm inputs and four relay controlled outputs, and also can control two card readers/doors. The input resistance is 10kOhm by default, however, can be programmed for any resistance between 1kOhm and 100kOhm.

The input or output capacity of the 8602R-001 can also be increased by installing a single Pacom 8203R-001-UL (output) or 8204R-001-UL (input) expansion card.

8603R-001-UL IP Two Door Controller

The 8603R-001-UL is an interface between the Controller and up to four third-party card reader devices (each can be a different type as they operate independently) and two doors. It has eight input and eight output connections for door control, card reader LED and buzzer control or alarm reporting.

The 8603R-001-UL is a "Pacom-edge" device that communicates with the Controller using Ethernet (TCP/IP) and/or RS485. Ethernet support enables it to connect using existing IP infra-structure. It also features a RS232 serial port for IP/web-based configuration and a USB port. The 8603R-001-UL features on-board memory that can be configured for "degraded mode" operation, in that the device stores details of the last 1000 valid access cards and/or facility codes used (based on the 26-bit Wiegand format), enabling it to operate at a limited level if offline to the Controller.

Input/Output (I/O) Operation

Additionally to door control inputs/outputs, the 8603R-001-UL has eight supervised five-state inputs and eight outputs (two relay and six open collector) that can be configured as alarm inputs/outputs. The input/output capacity of the 8603R-001-UL can also be increased by installing up to two Pacom 8203R-001-UL (output)/8204R-001-UL (input) expansion cards. This can be further increased to four expansion cards by using two 8220R-001 expansion card adaptors.

See Also: Alarm Keypads | Door Controllers | Input/Output Expansion | Third-Party Devices

Alarm Keypads

Door Controllers

Input/Output Expansion

Power Supplies

Third-Party Devices

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > Alarm Keypads

Alarm Keypads

Keypads represent physical security keypads, which communicate directly with the associated Controller, and serve as interfaces to the security system for users. Keypads generally have a text display, numeric keys and other buttons for accessing modes and functions. Keypads can belong to a single area only, however, they can operate across

multiple areas. The number of areas that can be supported is dependent on the keypad and Controller type.

Main Operational Features

Depending on the alarm user operating the keypad and their permissions, the following main keypad functions are available:

- Alarm system operations (arm/disarm, test etc).
- Access control operation (PIN-pad or full access control modes - select keypad models only).
- Program alarm users and some other settings.
- Program basic Controller functionality.

Keypad controller nodes represent the actual keypad hardware. Keypad functionality are properties of the keypad node type.

Note: Devices are generally treated using multiple node types. The "device" node represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

See Also: 1061 Keypad Controller | 8101 Keypad Controller | Keypad | Peripheral Devices

1061 Keypad Controller

8101 Keypad Controller

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > 1061 Keypad Controller

1061 Keypad Controller

The 1061 is a large format keypad with two outputs.

Management, Configuration and Commands

See Also: Alarm Keypads | Keypad

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral

Devices > 8101 Keypad Controller

8101 Keypad Controller

There are several models of 8101 small format keypad, each with differing features in terms of input/output capability.

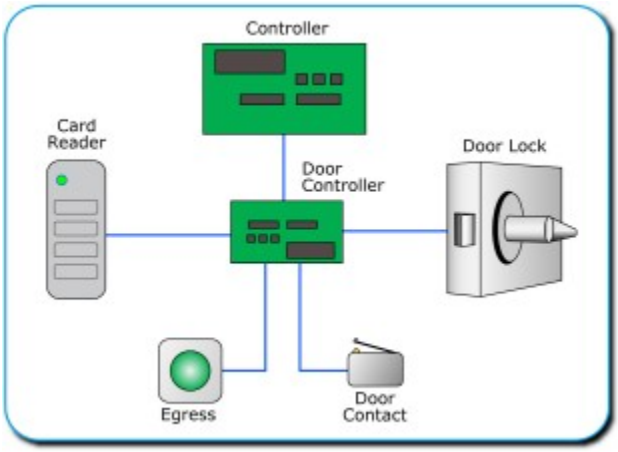
Management, Configuration and Commands

See Also: Alarm Keypads | Keypad

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > Door Controllers

Door Controllers

Door controllers are used to connect card readers and doors for access control functions. Door controller hardware is designed to be the interface between the Controller and a range of access control devices (for example, magnetic stripe card reader or keypad and door locking mechanism) to enable messages and commands to be exchanged between them.



Note: Devices are generally treated using multiple node types. The "device" node represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

See Also: 1064 Door Controller | 1076 Door Controller | 8501 Door Controller | 8601/8602 Door Controller | Peripheral Devices

---

1064 Door Controller

The 1064 supports one door, one card reader, six inputs and four outputs.

Note: The 1064 can also be used as an I/O expansion device.

Management, Configuration and Commands

See Also: Door Controllers | Peripheral Devices

1076 Door Controller

The 1076 supports two doors, two card readers, eight inputs and four outputs.

Management, Configuration and Commands

See Also: Door Controllers | Peripheral Devices

8501 Door Controller

The 8501 supports two doors, four card readers, 16 inputs, four outputs and two 8000-series expansion card slots for increased I/O capability.

Management, Configuration and Commands

See Also: Door Controllers | Peripheral Devices

8601/8602 Door Controller

The 8601/8602 supports two doors, two card readers, eight inputs and four outputs and, for 8602, one expansion card slot for increased I/O capability.

Management, Configuration and Commands

See Also: Door Controllers | Peripheral Devices

Input/Output Expansion

Input/output (I/O) expansion devices serve to expand the input and output connectivity of a Pacom Controller. Pacom I/O cards are designed as additional modules for Pacom Controllers and plug straight in to, or wire directly to, the Controller.

I/O device objects are required by the system as containers for mapping input and output objects. The mapping determines which I/O device port connects to which security equipment (card readers, locks, switches, PIRs, sirens etc) and correspondingly, which Controller. Security equipment is equipped with input and output connections that are linked to functionality. These connections allow signals to be sent between them and the Controller for full interaction. Using I/O cards, you can increase the input and output capacity of the Controller and thus, attach more security equipment to it. This allows the system to grow in accordance with the site security requirements with minimal extra hardware.

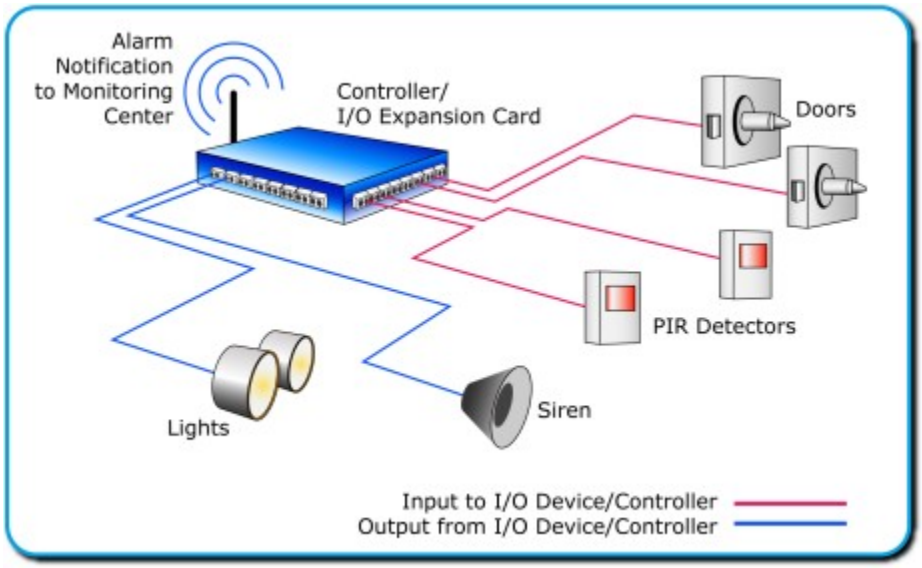
In terms of general connectivity, an output connection from a security device (for

example, a PIR detector) will connect to an input connection on one of the associated Controller I/O devices. Output signals from the Controller will be sent to input connections on the security device through an I/O device output connection.

Note: It is possible to map input/output objects directly to Pacom Controllers that have built-in input/output ports, without an I/O card attached. To do this, you must create a I/O device object using the Controller on-board input/outputs.

Example Scenario

A small office has a simple installation that consists of a Controller, an I/O expansion card, GPRS modem expansion card, PIR motion detectors, door contacts and a siren. The office lights are also wired up to the security system so they can be switched by the Controller. The following diagram shows simplified connectivity of the system, with the I/O expansion card integrated with the Controller.



Imagine that thieves have smashed a window and entered the premises while the alarm system is armed. The doors are wired to the Controller, but because the door contact inputs connected to them remain unaffected by the break-in, do not send any signals. The thieves' motion is detected by the PIR inputs in the office, which send signals to the Controller as they trigger. The Controller receives the signal at an input connection on the I/O expansion card as a security breach. It, in turn, sends an alarm notification wirelessly to the security monitoring center using the GPRS modem and also activates its output connections to operate the siren and turn the lights on.

Various events occur in the example, with each event and system response recorded in the system database. This simple example shows how operation of the system can be customized to automate system responses to security threats. The connectivity between the Controller and the rest of the system is key to providing a high level of system flexibility. The extra connectivity offered by I/O devices attached to the Controller offers scalability for increased security system integration.

Note: Devices are generally treated using multiple node types. The "device" node

represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

See Also: 1064 I/O Expansion | 1065 I/O Expansion | 1076 I/O Expansion | Peripheral Devices

---

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > 1064 I/O Expansion

1064 I/O Expansion

The 1064 in "I/O" expansion mode provides six input and four output connections.

Note: The 1064 can also be used as a door controller device.

Management, Configuration and Commands

See Also: Input/Output Expansion | Peripheral Devices

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > 1065 I/O Expansion

1065 I/O Expansion

The 1065 I/O expansion provides 16 input and four output connections.

Management, Configuration and Commands

See Also: Input/Output Expansion | Peripheral Devices

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > 1068 I/O Expansion

1068 I/O Expansion

The 1068 I/O expansion provides two input and one output connections.

Management, Configuration and Commands

See Also: Input/Output Expansion | Peripheral Devices

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > 1076 I/O Expansion

1076 I/O Expansion

The 1076 I/O expansion provides eight input and four output connections.

Management, Configuration and Commands

See Also: Input/Output Expansion | Peripheral Devices

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > Power Supplies

Power Supplies

Pacom power supplies provides a regulated 12 to 15VDC supply for powering Controllers and peripheral devices and to charge backup batteries. They have a universal AC input range for use anywhere in the world without modification, and feature auto-switching to DC or UPS input if the AC supply fails. When working as a backup battery charger and in conjunction with 8000-series Controllers, they can publish real-time status of backup batteries to the system. With the PD8303R-01-UL, advanced monitoring and configuration options are available. Both power supply types have the following built-in protection features:

- Short circuit/over-voltage/overload protection.

- Battery low (deep discharge prevention) and polarity protection. Battery fuse.
- 100% full load burn-in test.

Backup battery status is detected automatically and requires no configuration. Status pin voltages update within one minute of a change in battery condition (either not present/cut-off, voltage low or voltage OK).

The PD8303R-01-UL has two power outputs and can also power a RS485 device line. It can connect to the Controller as a power supply and/or as a device on the RS485 line.

The 8305R-01-UL has one power output.

Note: When multiple power supplies are in use on the same RS485 device line, each one must be individually earthed.

See Also: 8303 Power Supply | Peripheral Devices

8303 Power Supply

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > 8303 Power Supply

8303 Power Supply

Power supply nodes represent Pacom power supply devices.

Management, Configuration and Commands

See Also: Controllers | Virtual Device Nodes

You are here: Configuring Pacom Hardware > Hardware Device Nodes > Peripheral Devices > Third-Party Devices

Third-Party Devices

Third-party devices are proprietary devices from other manufacturers that are supported by the Pacom system. These devices generally provide extended or specific functionality.

See Also: Assa Abloy Aperio Door Control | Peripheral Devices

---

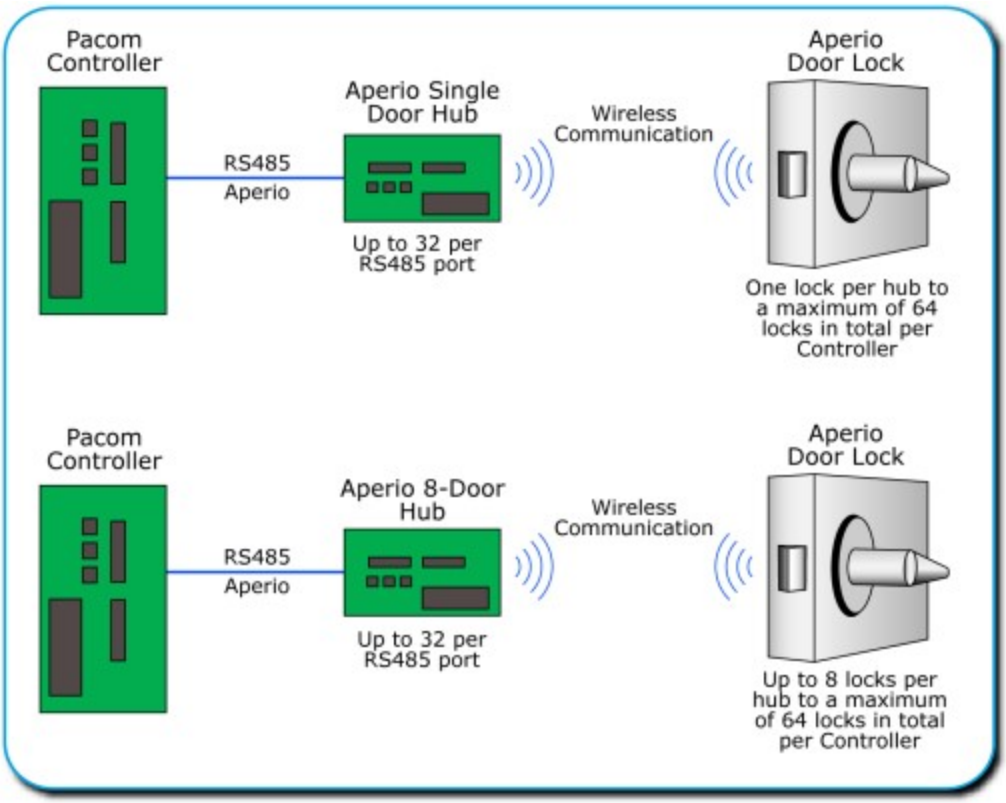
Assa Aperio Door Control

Aperio door hub nodes represent Assa Aperio wireless door locking hardware. The Aperio system uses wireless communications between an Aperio hub (router) and a number of Aperio wireless locks [various models of hub are available, including one-to-one hubs that support a single wireless lock/card reader each, to multi-hubs that can support up to eight wireless lock/card readers each]. When users swipe an access card against the Aperio wireless lock, it sends a signal to the Aperio hub, which then signals the connected Controller. The Controller determines whether or not the access is valid and sends the appropriate signal back to the hub. The hub then signals the lock to either unlock or remain locked as required.

The hub(s) are wired to the Controller for two-way communications using a dedicated RS485 device line. On the Controller, the RS485 can be connected to a RS485 expansion card or to the on-board RS485 port. The system supports up to 64 Aperio wireless locks per Controller using one or more RS485 ports, depending on Aperio hardware and protocol. Aperio "locks" are considered card readers in the Pacom system. To integrate an Aperio system into Unison:

- Ensure the Controller is licensed for Aperio devices in that the "number of OEM readers" supported must cater for the number of Aperio readers to be used.
- Configure a Controller port to use "Aperio protocol" - use the Controller web server configuration utility to set up the required port.
- Perform a "generate" on the Controller to create Aperio nodes, if already set up in the Controller hadrware configuration. If not, create Aperio hub devices manually, as required.
- Create a card reader for each "lock", as required. Link the card readers to an Aperio hub device.
- Set up the required door nodes to use the [Aperio] card readers.
- Create access groups as required, so that users can be granted acess to use Aperio "locks".

Note: For Pacom 8001/8002 Controllers, it is recommended to not connect more than 20 Aperio devices per RS485 device line. Larger numbers of devices may cause delays of several seconds during access card verification. • Aperio 8-door hub variants are no longer supported from Unison 5.7, however, will be created from the Controller "generate" command if the Controller has an existing 8-hub device configured.



Note: Devices are generally treated using multiple node types. The "device" node represents the hardware in terms of other devices, such as by identification and device addressing. Other related nodes are specific to functionality of the device. For example, an I/O device will have a "device" node for the actual hardware, and also multiple "input" and "output" nodes for each input/output function it has.

Management, Configuration and Commands

See Also: Configuring Pacom Hardware | Web Server Controller Configuration Guide

---

Timecon Door Controller

Timecon door controllers support a single door, two card readers, eight inputs and four outputs.

Management, Configuration and Commands

See Also: Door Controllers | Peripheral Devices

You are here: Configuring Pacom Hardware > Virtual Device Nodes

Virtual Device Nodes

Virtual device nodes represent non-physical system components that provide specific functionality in relation to peripheral hardware devices. For example, a "door" node provides the functionality for access control and alarm monitoring by way of door controller, card reader [or other access control interface], and door locking mechanisms. Another example are inputs, which are a functional component of input/output (I/O) devices that, in terms of system functionality, have specific properties.

See Also: Controllers | Controller Expansion Cards | Peripheral Devices | Virtual Device Nodes

Alarm Reporting

Areas

Card Readers

Doors

Elevator

Elevator Floor

Inputs

Interlocks

Keypads

Local Alarm Users

Macros

Networking

Output Macros

Outputs

Ports

Triggers

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Alarm Reporting

Alarm Reporting

Reporting nodes are used to configure alarm reporting connections for a Pacom Controller.

- Alarm Report Settings
- Alarm Report Entry

See Also: Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Areas

Areas

Pacom Controller network area nodes are used to arm and disarm multiple inputs in a single operation, and are generally to manage parts of a building in terms of access control and alarm monitoring.

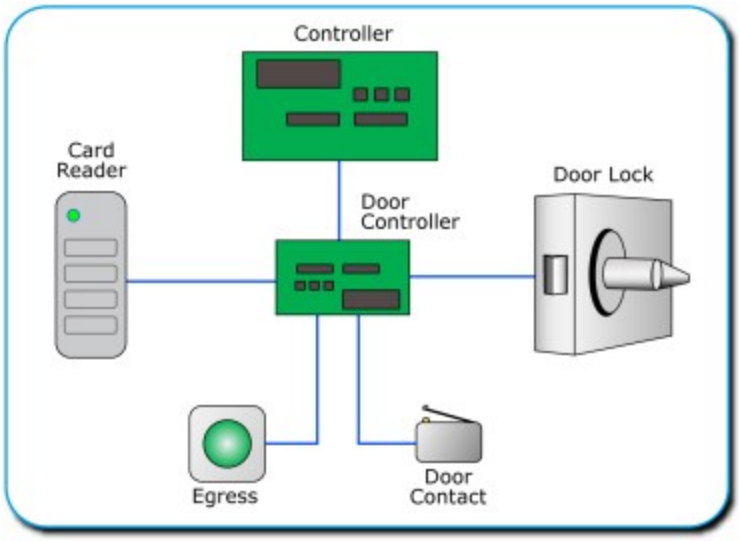
- Management, Configuration and Commands

See Also: Alarm Control Guidelines | Areas and Alarm System Control | Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Card Readers

Card Readers

Card reader nodes represent the functionality of connected access card reader hardware. Card readers are used for passing data from swiped access cards to the system for validation during access control and other related functions. For example, a magnetic stripe card reader controlling the opening of a door. The purpose of access control is to provide only authorized persons with entry/exit. Card readers are directly linked with door controller and door nodes. The following image shows the basic relationship between the hardware controlling a door.



Anti-Passback

Anti-passback is a function that prevents two users gaining access to an area using a single card and also from being able to return through the previous door. In effect, anti-passback controls the direction of movement of users through one or more doors. When you enable anti-passback, the system records the last 16 access cards used on the card reader, and can optionally do so for a set amount of time. These access cards will not be allowed access via the card reader again until they are no longer in the stored list, time-out, or are reset by using another card reader. There is also an option for clearing the card reader passback memory in other card readers, if the card is used in a particular reader.

Management, Configuration and Commands

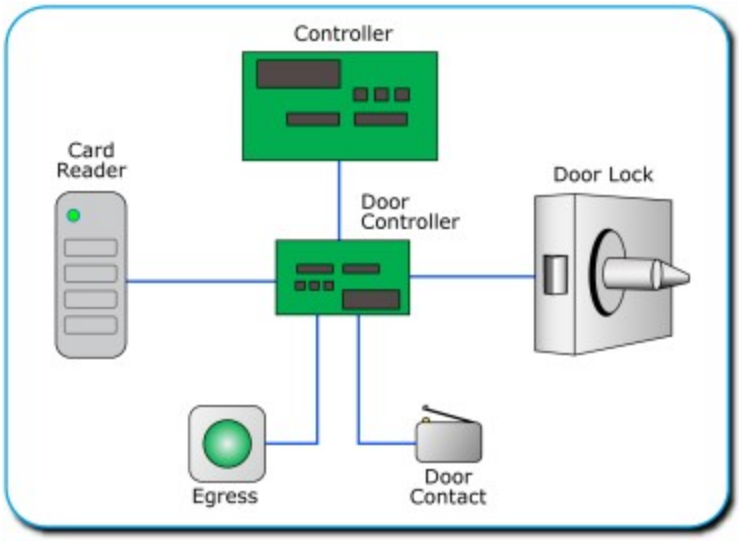
See Also: Access Control Guidelines | Card Profiles | Keypads | Virtual Device Nodes

---

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Doors

Doors

Door nodes represent a door in the site that is locked/unlocked using access control (card reader, keypad, etc). The purpose of access control is to provide only authorized persons with the ability to pass through the door. Doors are linked with card reader and door controller nodes. The following image shows the basic relationship between the hardware controlling a door.



Doors that are managed through an access control system generally consist of the following components (in addition to the physical door itself):

- A locking mechanism that can be actuated electronically. This is often one or more "bolts" (also known as "tongues" or "strikes"), which can be extended or retracted from their housings in order to secure the opening side of the door against the door jam. The bolt is controlled by the "lock output" settings. The bolt can also be monitored for unauthorized movement and can generate "strike" alarm conditions ("lock input" settings).
- A door contact to determine when the door is open or closed ("contact input" settings). This is often a micro-switch or magnetic switch that "closes" (that is; changes position/state) when the door is fully closed. The circuit that the contact is wired to is an "input" that notifies the system of the door being open or closed. The door contact is generally used to generate "door forced" and "door ajar" alarm conditions.
- An egress device (often a button) for doors that are access controlled for exit ("egress" settings). The circuit that the egress is wired to is an "input" that notifies the system of a request to unlock the door. The egress is generally used to generate "door forced" and "door ajar" alarm conditions.

Door Open/Close Sequence
Management, Configuration and Commands

See Also: Access Groups | Card Readers | Virtual Device Nodes

---

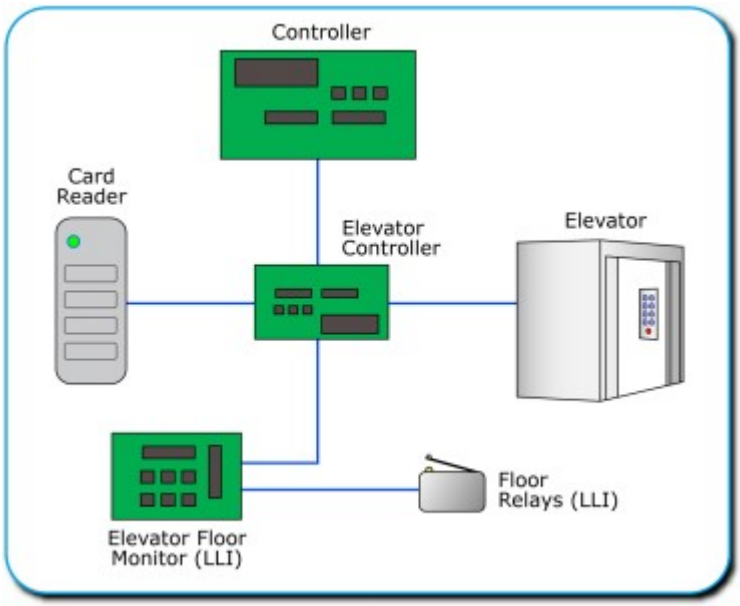
You are here: Configuring Pacom Hardware > Virtual Device Nodes > Elevator

Elevator

Elevator nodes represent elevator (lifts) in a site where the floors that it stops at are managed using access control (card reader, keypad, etc) so that authorized users only can select particular floors. Elevator floors under access control are treated in the same way as doors, where users that have elevator floor nodes in their access groups are able to access those floors. The "elevator" node can be either the elevator control hardware device in a "low level interface" system, or the software driver in a "high level interface" system.

- Low Level Interface (LLI) - These types of elevator systems are hardware based in that the required functionality is provided through the hardware. For elevators, these require elevator floor monitoring devices to notify the system of floor position.

The following image shows the basic relationship between the hardware controlling an elevator in a low-level interface system.



- High Level Interface (HLI) - These types of elevator systems use software based logic control that uses a command-response interface, via communications protocol, to communicate with the device. For elevators, the elevator system is able to notify the system of elevator position, without requiring floor monitoring equipment.

Elevators that are managed through an access control system generally consist of the following components (in addition to the physical elevator itself):

- The elevator itself, which when under access control, is controlled for the floors/levels that can be selected and that the elevator may stop at.
- A card reader to signal to the system an access attempt and the cardholder so that floors that the cardholder may access are selectable. The card reader is operated using time schedules and/or alarm system modes to determine when it is locked/unlocked/active. This allows a single elevator to be used for both access and non-access controlled use of the elevator. It is possible to make particular floors access controlled and others openly accessible.
- An elevator controller device, which provides the signaling to the elevator system

for when to move and which floor to move to. The associated Controller can interface with HLI elevators for floor reporting and elevator floor monitor devices for floor reporting in LLI elevator systems. Several Pacom elevator controller devices are available, each of which is capable of controlling an elevator for a set number of floors. For example, a Pacom 1065 elevator controller can manage a maximum of 16 floors, therefore, an elevator of 32 floors would require two elevator controllers. In cases where access control is required on select floors of an elevator, an elevator controller is required only for the floors being access controlled. For example, an elevator with 100 floors and requiring access control on levels 12, 14 and 50 would require two elevator controllers.

- An elevator floor monitor device for LLI elevators, which is wired to elevator relays that signal when the elevator has reached a floor.

Note: It is possible to use a combination of HLI and LLI on the same elevator. For example, LLI for faster response and floor access, and HLI for elevator status reporting.

Management, Configuration and Commands

See Also: Elevator Floor | Virtual Device Nodes

Elevator Floor

Elevator floor nodes represent elevator (lift) building levels (floors) that can be used for floor selection using access control (card reader, keypad, etc). The purpose of access control is to provide authorized users only with the capability to select particular floors.

Management, Configuration and Commands

See Also: Access Groups | Elevator | Virtual Device Nodes

Inputs

Inputs represent mapping of signals from security devices (card reader, lock, switch,

PIR etc) to the Controller through input/ports on devices that have input/output (I/O) capabilities. These connections can be physically connected digital or analog inputs, or "virtual" inputs, such as a key press on a computer or a CCTV camera alarm. When the associated Controller receives a signal through an input, which often indicates some kind of alarm condition, it responds to it as configured for the input category. The system can be customized to automatically respond to alarms in various ways and, using expressions, can activate outputs or perform virtually any kind of function. Input events are logged in the system database to allow monitoring of events as they occur (in real-time) and to maintain records of all previous events.

- Input Categories and Isolation
- Input State Monitoring
- Management, Configuration and Commands

See Also: Input/Output Expansion | Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Interlocks

Interlock

Interlock nodes represent doors that are connected so that while any one door is open, all others are locked and cannot be opened. Door interlocking is an additional security feature designed to control the passage of users. Interlocks are created manually and you must connect them to the appropriate doors or, for elevator interlocking, elevator floors.

- Management, Configuration and Commands

See Also: Door | Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Keypads

Keypads

Keypad nodes represent keypad functionality. There are several models of Pacom keypad available, each with differing features in terms of display and input/output capability. Keypads have multiple functions such as; alarm user log on/off, area and alarm status display, alarm management, and alarm system mode selection etc.

- Management, Configuration and Commands

See Also: 8101 Keypad Controller | Keypads

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Local Alarm Users

Local Alarm Users

Management, Configuration and Commands

See Also: Alarm Control Guidelines | Areas and Alarm System Control | Virtual Device Nodes

---

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Macros

Macros

The concept of macros is based on a series of basic logical functions performed on specified conditions, resulting in an action. Macros allow you to be very specific with the conditions that need to be met and with the subsequent actions to take, providing you with complete flexibility. These macros are downloaded to the Controller and executed by the Controller. This is different to Unison Expressions that are run from within Unison.

The key functions in macro programming are the AND and OR functions. These can be used in a number of combinations to establish a set of conditions that once met, cause an action or set of actions to be performed.

- The AND function is used to link two conditions that must both be correct before the action is performed or to link multiple actions to be performed.
- The OR function is used to link two conditions so that the action is performed when either condition is correct.

Management, Configuration and Commands

See Also: Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Networking

Networking

Management, Configuration and Commands

See Also: Access Groups | Card Readers | Virtual Device Nodes

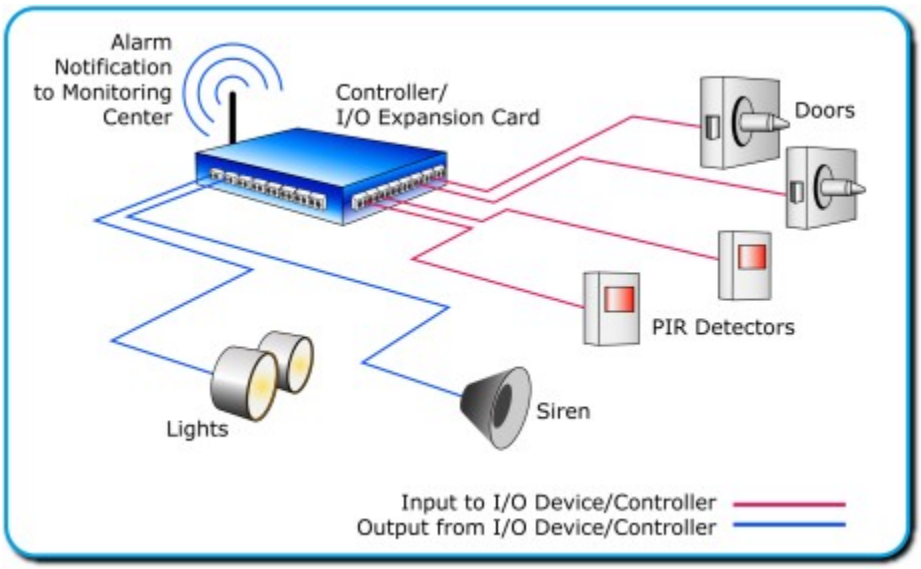
You are here: Configuring Pacom Hardware > Virtual Device Nodes > Output Macros

Output Macros

Output Macros [also known as "expressions"] represent area or Controller conditions that can be used to automate the activation [turning "on"] of one or more outputs. In order for an output to activate, one or more pre-defined conditions must be met, similarly to expressions.

Example Scenario

A small office has a simple installation that consists of a Controller, an I/O expansion card, GPRS modem expansion card, PIR motion detectors, door contacts and a siren. The office lights are also wired up to the security system so they can be switched by the Controller. The following diagram shows simplified connectivity of the system, with the I/O expansion card integrated with the Controller.



Imagine that thieves have smashed a window and entered the premises while the alarm system is armed. The doors are wired to the Controller, but because the door contact inputs connected to them remain unaffected by the break-in, do not send any signals.

The thieves' motion is detected by the PIR inputs in the office, which send signals to the Controller as they trigger. The Controller receives the signal at an input connection on the I/O expansion card as a security breach. It, in turn, sends an alarm notification wirelessly to the security monitoring center using the GPRS modem and also activates its output connections to operate the siren and turn the lights on.

Various events occur in the example, with each event and system response recorded in the system database. This simple example shows how operation of the system can be customized to automate system responses to security threats. The connectivity between the Controller and the rest of the system is key to providing a high level of system flexibility. The extra connectivity offered by I/O devices attached to the Controller offers scalability for increased security system integration.

Management, Configuration and Commands

See Also: Output | Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Outputs

Outputs

Outputs represent mapping of signals to security equipment (sirens, locks, switches, lights, cameras etc) from the Controller through output/ports on devices that have input/output (I/O) capabilities. The system can be set up to activate outputs in response to particular input signals - this is accomplished using output expressions. For example, activating a siren (output) if it a PIR detector (input) goes into an "alarm" state. Output events are logged in the system database to allow monitoring of events as they occur (in real-time) and to maintain records of all previous events.

Management, Configuration and Commands

See Also: Input/Output Expansion | Output Expression | Virtual Device Nodes

---

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Ports

Ports

Port nodes represent the physical communications ports on Pacom Controllers. The available ports for Controller are created automatically, with each associated port node

controlling communications through the physical port. For example, if the Controller is a Pacom 8001 type, there will be [at least] port nodes for RS232, RS485 and Ethernet connections

Management, Configuration and Commands

See Also: Controllers | Virtual Device Nodes

You are here: Configuring Pacom Hardware > Virtual Device Nodes > Triggers

Triggers

Trigger nodes represent "links" that can be used across multiple Controller expressions [for Pacom Controllers] as a method of activation/deactivation. For example, an expression that, when activated, can "activate" a trigger, which in turn through activation/deactivation of the trigger can be used to activate another expression and so on. Trigger nodes have two possible states:

- Activated - An expression or other condition has been reached that causes an associated trigger to become "active". The change of state to active can be used to execute other expression related functions.
- Deactivated - An expression or other condition has been reached that causes an associated trigger to become "inactive". The change of state to inactive can be used to execute other expression related functions.

Management, Configuration and Commands

See Also: Virtual Device Nodes

You are here: Configuring Third-Party and Generic Devices

Configuring Third-Party and Generic Devices

Device nodes, which are generally representative of proprietary third-party hardware and systems, provide the necessary system components for setting up communications between the Unison and third-party systems. Most proprietary third-party devices require specific device driver software modules installed. Device drivers are the software component of the system that provides the necessary communications protocols and other operations required to correctly interface with specific devices. Device templates provide "standard" configurations that determines applicable events and system behavior for devices to make set up easier and to minimize the chance of error. Once a device is created, then its associated hardware or function nodes ["child" nodes] can be created for it.

The Explorer in the Hardware view is different to other views, where devices are presented in a hierarchical tree structure that shows how different nodes are connected to each other. For example, a device node may have child nodes that correspond to attached hardware and/or functionality. These nodes may also have child nodes and so on. Normal list search and filter functions are designed for flat lists, therefore, in the Hardware view an additional search function is included for searching a hierarchical tree structure.

Note: For any third-party devices that have a database that Unison must connect to or extract data from, the database must be compatible with Unison; that is, be a Microsoft

SQL database. • Devices that are used in Nordic countries only are not documented in the English version of the help. These are Contal/Telealarm UC120 (CPU3), TAC5003, TLab C2/C3 and TLab Sentrion. For those devices refer to the Swedish version of the help.

See Also: Creating and Commanding Nodes | Configuring Pacom Hardware | Device Templates

Device Templates

Alarm and Access Control Systems

Communications Systems

Elevator Control Systems

Fire Protection Systems

Intercom Systems

Miscellaneous Devices

Video Systems

Visitor Management Systems

Alarm Receiver

Alarm Sender

You are here: Configuring Third-Party and Generic Devices > Device Templates

Device Templates

Device templates provide "standard" configurations that determines applicable events and system behavior for devices to make set up easier and to minimize the chance of error. Standard templates are provided for each supported device type. Device templates include events such as tamper, alarm, power fail, access denied etc, and relevant alarm types and system behavior, such as whether or not to show alarms to operators via graphics.

Although standard device templates cannot be edited or deleted, a copy of the template can be created. When creating a copy or a new device template, the "child" nodes that are created [where applicable] for the device also inherit the device event configuration. After a node is created, node events can be configured individually - this does not affect the template, as it is applied only when a node is created.

Management and Configuration

See Also: Configuring Third-Party and Generic Devices

You are here: Configuring Third-Party and Generic Devices > Alarm and Access Control Systems

Alarm and Access Control Systems

Assa ARX

Honeywell Galaxy Dimension

Islog Data Writer

Salto

You are here: Configuring Third-Party and Generic Devices > Alarm and Access Control Systems > Assa ARX

Assa ARX

Assa ARX is an "online" access control system, built on industry standards for IP networks and securely connected over TCP/IP. The system supports Internet connectivity and can manage any number of users and doors using proprietary Assa door control hardware. The ARX system also provides integration to other third-party systems. The integration allows the Unison system to record ARX user access control and door events and also provides some door control commands. The following Assa ARX products are supported:

- LCU9016/9017/9101 controllers.
- DAC430 door control unit.
- ARX Server Software 3.0.3 to 3.11.
- ARX Interface Protocol 2.5 and later.

Note: For ARX protocol versions prior to 3.11, user access categories/levels should be imported into Unison from ARX by way of "dummy users" that are associated with the required access levels. Click here for help.

The following node types are supported:

- Assa ARX device - Provides system functionality for the ARX system.
- Assa ARX server - Provides IP connectivity settings to the ARX system server computer. Once a ARX server node is created, its hardware and access control configurations can be "read" by the Unison system, with corresponding child folders/nodes automatically created.
- Access category - Represent user access control permissions in the ARX system. Access category nodes are listed inside an automatically created folder.
- Controller - Represent Assa hardware that connects and controls doors and card readers.
- DAC [door control unit] - Represent Assa Direct Access Category ["DAC"] interface hardware for doors. DAC nodes are listed under each applicable door.
- Door - Represent ARX controlled doors. Door nodes are listed inside folders created automatically under each applicable controller device.
- Reader - Represent ARX controlled access card readers. Card reader nodes are listed under each applicable door.

Integration Functions and Limitations
Integration Requirements

The Unison system supports importing existing Assa ARX hardware and user configurations. When importing, hardware nodes in the Assa system are replicated in the Unison system - this makes device configuration faster and less prone to error. For users, a separate import facility is provided - ARX users are merged into the Unison user database. To import a hardware configuration:

1. Create a "Assa ARX" device in the Unison system. This is the "root" node for the Assa system.
2. Create a "ARX server" child node to the "Assa ARX" device. This node provides a connection to the ARX system.
3. Use the "generate" command on the "ARX server".

Note: If any nodes are deleted from the ARX system after being generated in Unison, they are not automatically removed from Unison during any subsequent node generation process. Unused nodes must be deleted from the Unison system manually.

To import ARX users:

Note: If users are added/edited/removed from the ARX system, it will be necessary to perform the user import process to synchronize the Unison system with ARX. Any changes made to users from the Unison system are automatically synchronized in the ARX system without any additional operator actions required. • The Unison system does not currently support reading access card data from an ARX card reader when creating users via the Create Card wizard. The access card data must be set manually.

1. Use the "user import" command on the "ARX server".

Device - Management, Configuration and Commands
ARX Server - Management, Configuration and Commands
Access Category - Management, Configuration and Commands
Controller - Management, Configuration and Commands
DAC - Management, Configuration and Commands
Door - Management, Configuration and Commands
Reader - Management, Configuration and Commands
Assa ARX User Settings

See Also: Configuring the System | Configuring Third-Party and Generic Devices | Creating and Managing User Access Cards | Device Templates

---

You are here: Configuring Third-Party and Generic Devices > Alarm and Access Control Systems > Honeywell Galaxy Dimension

Honeywell Galaxy Dimension

Honeywell Galaxy Dimension is a fully integrated intrusion monitoring and door control panel, connected over TCP/IP. Honeywell Galaxy Dimension panels can connect alarm inputs, outputs, card readers and a number of other devices. The following node types are supported:

- Honeywell Galaxy Dimension device - Provides system functionality and some "global" settings for the Galaxy Dimension system.
- Central unit - Represent Honeywell Galaxy Dimension hardware that connects and controls inputs and outputs, local keypads, door controllers, card readers etc. Once a central unit node is created, its hardware configuration can be "read" by the Unison system, with corresponding child nodes automatically created.
- Remote input/output ("RIO") - Represent Galaxy alarm panel I/O expansion cards, which are used to connect a collection of inputs and outputs to the central unit. The central unit can be extended with several RIO cards. RIO nodes include:
  - RIO card without its own power supply.
  - RIO card with its own power supply ("Power RIO").
  - RIO card with wireless connection.
- Area/group - Virtual nodes used to group nodes within the Honeywell Galaxy Dimension system. Areas are used to command (arm/disarm etc) input nodes that are associated with an area in a single operation.
- Card reader - Represents access card reader hardware, used for user access control. Card readers may also be used to sending fault and panic event alarms.
- Door controller - Represents door control hardware [lock actuation etc], used for user access control.
- Input - Represents hardware used for alarm detection [door contact sensor etc].
- Keypad - Represents keypad hardware, used for user access control and user alarm

system interaction [arm/disarm areas, reset alarms etc]. The local keypad node type also displays tamper alarms and if a user sends alarms using the keypad etc.
- Output - Represents hardware used for alarm notification or response [sirens, lights etc].

Integration Requirements

The Unison system supports importing existing Honeywell Galaxy Dimension configurations as well as manual configuration. When importing, nodes in the Honeywell system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Create a "Honeywell Galaxy Dimension" device in the Unison system. This is the "root" node for the Honeywell system.
2. Create a "central unit" child node to the "Honeywell Galaxy Dimension" device. This node provides a connection to the central unit.
3. Use the "generate" command on the "central unit".

Device - Management, Configuration and Commands
Central Unit Device - Management, Configuration and Commands
Remote Input/Output (RIO) - Management, Configuration and Commands
Input - Management, Configuration and Commands
Output - Management, Configuration and Commands
Area ("Group") - Management, Configuration and Commands
Keypad - Management, Configuration and Commands
Door Controller - Management, Configuration and Commands
Card Reader - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Alarm and Access Control Systems > Islog Data Writer

Islog Data Writer

Islog Datawriter is an access card encoding platform that supports a variety of "smart-card" micro-chip technology access cards [for example, Mifare Desfire] - these are generally regarded as access card technologies that are not directly supported by Unison. The Unison system can be used to add users and encode access cards using the Islog Datawriter application and appropriate card encoding and printing hardware. It is necessary to install the Islog Datawriter application "plug-in" to the Unison system and also creating compatible "encoding tasks", which can be thought of as a card enrollment reader and profile. To add a person to Islog, create a user node and create an access card using the required Islog encoding task [selected by "card reader"]. The following node types are supported:

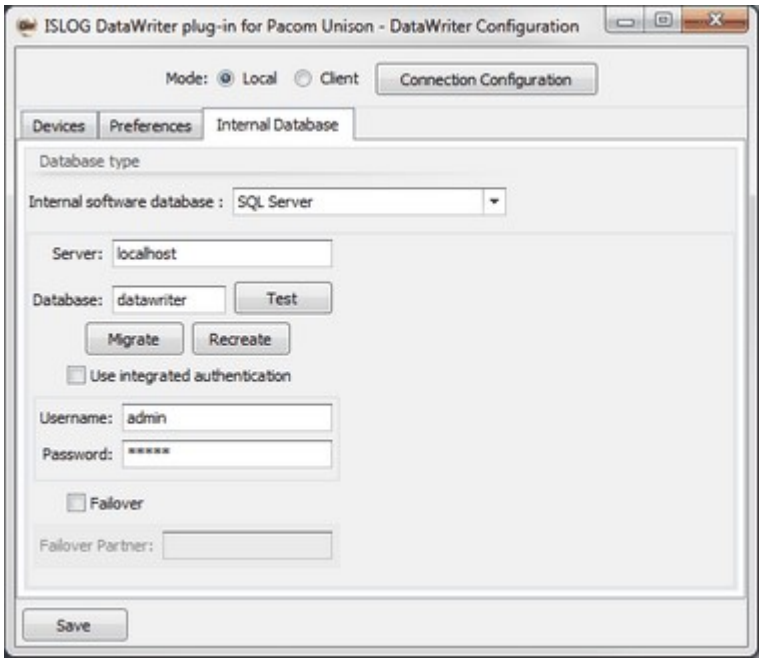
- Islog Datawriter device - Provides system functionality for the Islog Datawriter application, which exists as a separate application to Unison. The node properties allow opening of the Islog Datawriter software for encoding task configuration.
- Islog Datawriter RFID reader - Represents hardware used for encoding access cards and the actual encoding to apply. For example, if two types of encoding is required, two nodes must be created, each with the necessary encoding. The nodes are classified in Unison as "card readers" so they can be selected when creating user access cards.

Integration Functions and Limitations
Integration Requirements

The Unison system requires the Islog Datawriter software to be installed and accessible. To set up the plug-in:

Note: For specific or additional information, refer to the Islog Datawriter application documentation.

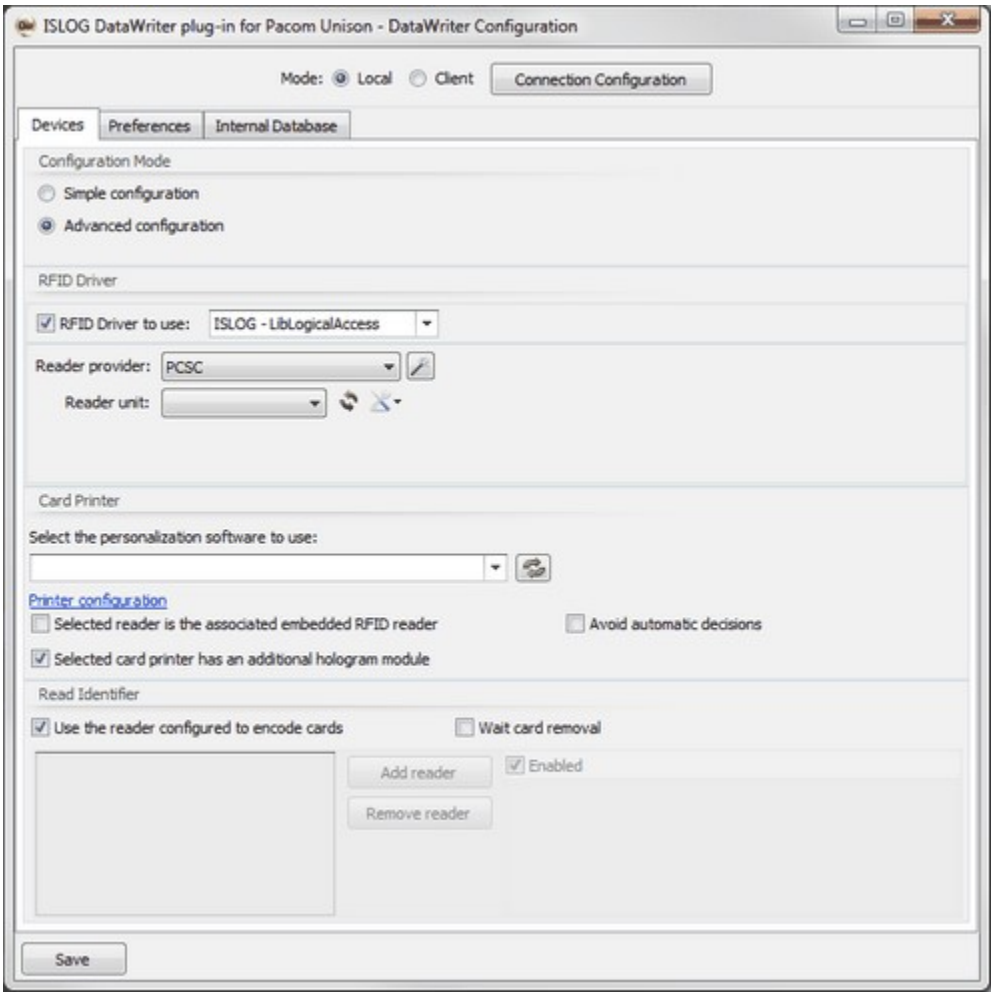
1. Install the Islog Datawriter software and run it. It may be necessary to enter credentials to start the program - enter "admin" for both the User Name and Password settings.
2. In the DataWriter First Use Configuration Wizard, DataWriter Architecture screen, select Standalone.
3. In the DataWriter First Use Configuration Wizard, Configure DataWriter Options screen, select the Internal Database tab, then:



- For the Internal Software Database setting, select SQL Server.
- For the Server setting, enter the computer name or IP address of the machine where SQL Server that Unison uses is running.
- For the Database setting, enter "datawriter".

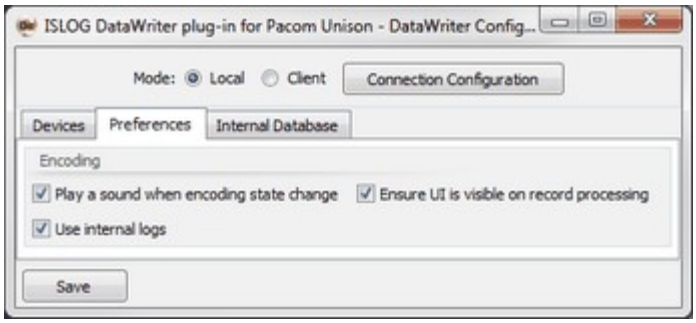
- For the Use Integrated Security option it is recommended to not enable this option and, instead, apply SQL authentication using the User Name and Password fields. This is to prevent a denial of access to the Islog database if a different Unison operator logs on with different Windows credentials.
- Click Recreate. This will install the required Islog database. To verify the database creation and connection, click Test.

4. Select the Devices tab, then:



- Select Advanced Configuration. Additional settings display.
- Ensure that the RFID Driver to Use option is enabled and that ISLOG - LibLogicalAccess is also selected.
- For the Reader Provider setting, select the manufacturer of the encoding device to be used.
- For the Reader Unit setting, select the model of the encoding device to be used.
- Configure any other settings as required, then click Save.

4. Select the Preferences tab and enable options as required.



5. Click Save.
6. Click Finish. The Islog Datawriter application opens.
7. Create a "Islog Datawriter" device in the Unison system. This is the "root" node for the Islog system.
8. Create the required "Islog Datawriter RFID Reader" child nodes to the "Islog Datawriter" device and apply the necessary encoding task to each.

Device - Management, Configuration and Commands
Encoder ["Islog Datawriter RFID Reader"] - Management, Configuration and Commands
Encoding User Access Cards

See Also: Configuring Third-Party and Generic Devices | Creating and Managing User Access Cards | Users and Access Cards

---

You are here: Configuring Third-Party and Generic Devices > Alarm and Access Control Systems > Salto

Salto

Salto is a semi-wireless access control system, connected over TCP/IP. This system is typically used in hospitality for providing guests access to rooms by way of "carriers", such as RFID access cards and keys. The Unison system can be used to add users and access cards to the Salto system. This is achieved by setting up a Salto encoder device as a card reader in the Unison system and also creating a compatible Salto card profile. To add a person to Salto, create a user node and create an access card using the Salto card profile and encoder. The following node types are supported:

- Salto device - Provides system functionality for the Salto system.
- Salto server - Manages connections between Salto devices, hosts access control data and communicates with the Unison system over IP.
- Encoder - Programs access cards with access control data/read access control data. Encoders connect to the server either over IP or USB. When a carrier is encoded, the Salto system requests the user's access level information from the Unison system. This information is written to the card and is valid for a period of time [usually seven days].

- Online door - Provides access control functions and also carrier management, such as adding/deleting carriers etc [also called "wall readers"]. Online doors are wired (Ethernet) devices that connect to the server over TCP/IP.
- Offline door - Provides access control functions. Offline doors are "remote" from other parts of the system and read access control data stored on carriers to grant/deny access [also called "electronic locks"]. Offline reader functionality is set/updated using Salto PPDs [portable programming device].
- PPD - Portable programming device used to set/update functionality [downloaded from the server] in offline readers. Event history is uploaded from offline readers at each use of a PPD, which downloads to the server on connection. Events are also recorded in Unison system transaction logs.
- Area/zone - Virtual nodes used to group nodes within the Salto system.

Integration Requirements

The Unison system supports importing existing Salto configurations as well as manual configuration. When importing, nodes in the Salto system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Create a "Salto" device in the Unison system. This is the "root" node for the Salto system.
2. Create a "Salto server" child node to the "Salto" device. This node provides a connection to the Salto server.
3. Use the "generate" command on the "Salto server".

Device - Management, Configuration and Commands
Salto Server - Management, Configuration and Commands
Area - Management, Configuration and Commands
Encoder - Management, Configuration and Commands
Offline Door - Management, Configuration and Commands
Online Door - Management, Configuration and Commands
Salto Card Profile
Salto Card Exclusion List

See Also: Card Profiles | Configuring Third-Party and Generic Devices | Users and Access Cards

---

You are here: Configuring Third-Party and Generic Devices > Communications Systems

Communications Systems

Ascom Teleprotect

The Ascom Teleprotect system is a paging and personal duress alarm system, where pagers can receive messages and can also initiate and send alarms to the integrated management system. There are two types of pager - "personal alarm units" that support alarm notification and simple messaging; and "personal IM alarm units" that support both alarm notification and interactive messaging. Interactive messages can include options that are displayed along with the message that can be be selected. For example, an option to call an emergency telephone number.

The system consists of hardware [the "server" for OAP], connected over TCP/IP, or DLL files for OAS, that handle the sending and receiving of pager messages, transmitter polling and alarms. The system supports multiple addressable receiver/transmitters called "beacons" that serve as "bridges" between pagers and the rest of the system - several beacons may be used to provide adequate wireless coverage. Beacons are identifiiable so that when a pager alarm is received, the receiving beacon location is used to help locate the pager in alarm. Additionally, fixed message displays, called "corridor message displays", can also be used for general notification. For example, mounted on a wall or ceiling so that any persons passing the display are able to see messages.

Note: The Unison system supports both Ascom OAS and OAP communications protocols.

Pagers can send different alarms:

- Man-down - Indicates that the user is no longer standing depending on the position and angle of the transmitter over a predefined period of time; that is, in some kind of trouble, injured etc.
- Pull-cord - Indicates high priority or emergency alarms when detached from the

transmitter; that is, when the transmitter is forcefully taken from a person.
- Push-button - Two buttons for different alarms. Button one causes the alarm to be transmitted to predefined people. Button two signifies an emergency and activates an emergency alarm.
- Unison-based events - For interactive message capable pagers using OAP, 10 additional "virtual events" are available that can be used as triggers for additional operations within the Unison system. For example, in a particular situation, say an alarm, it is possible to allow pager users to select one of these events as a response to the alarm. The event then can be used by the Unison system in a programming action to trigger some additional function.

The following node types are supported:

- Beacon - Receiver/transmitter device nodes.
- Corridor message display - Fixed visual display device nodes.
- Groups - Groups of pager and/or corridor message display nodes to be sent messages simultaneously.
- Personal alarm unit - Individual pager nodes.

Device - Management, Configuration and Commands
Beacon - Management, Configuration and Commands
Corridor Message Display - Management, Configuration and Commands
Messaging Group - Management, Configuration and Commands
Personal Alarm Unit (Message Pager) - Management, Configuration and Commands
Personal IM Alarm Unit (Interactive Message Pager) - Management, Configuration and Commands
Message Templates for Personal Alarm Units
Programming Example

See Also: Configuring Third-Party and Generic Devices | Device Templates

---

You are here: Configuring Third-Party and Generic Devices > Communications Systems > ESPA 4.4.4 Radio Pager

ESPA 4.4.4 Radio Pager

ESPA (enhanced signaling protocol for alarm processes - "ESPA-X") 4.4.4 is the standard XML-based interface for compatible radio paging systems. Functions include sending messages to pagers and receiving alarms from pagers. This system is often used in health care to provide patients that ability to summon help from care givers. The following node types are supported:

- Alarm node - Represent the matching between messages received from the ESPA controller and events/alarms from pagers in order to create alarm events in the Unison system. Alarm nodes can be used to represent pager functions, such as

specific key presses etc, as well as alarm beacon and alarm receiver nodes.
- Group - Multiple pager nodes to send messages to simultaneously.
- Pager - Individual pager nodes to receive/send messages individually.

Device - Management, Configuration and Commands
Automatic Node Configuration - COBS Message Server
Alarm Node - Management, Configuration and Commands
Group - Management, Configuration and Commands
Pager - Management, Configuration and Commands
Programming Example
Data Identifiers

See Also: Configuring Third-Party and Generic Devices | Device Templates

---

You are here: Configuring Third-Party and Generic Devices > Communications Systems > Generic OPC

Generic OPC

OPC (object linking and embedding for process control) is a standard communications interface for compatible hardware based process control systems; for example, fire control and building management. The hardware connects to a "server" that handles messages. The Unison system connects to the server over TCP/IP. "OPC-DA Classic" is supported - "DA" is data access provides read/write access to properties of connected hardware. OPC-server software is provided by the hardware manufacturer or other third-party vendor. Functions include receiving messages from the hardware and sending commands to it.

Note: It is recommended to have the OPC server run on the same computer as the Unison device driver in order to avoid additional configuration of users and permissions in Windows. • The generic OPC driver should be used for compatible devices when a specific Unison device driver is not available. For example, Milestone video uses OPC, however, a specific Unison device driver is available that provides deeper integration.

The Unison system supports importing existing OPC object configurations as well as manual configuration. When importing, selected objects in the OPC server are replicated as nodes in the Unison system - this makes device configuration faster and less prone to error. All applicable nodes contained in the OPC system are created when using the command on the root device node. Sub-folders to the parent OPC server node are created if they exist in the OPC system, with applicable nodes contained within them. Sub-folders can also be used for generating nodes, however, nodes are created only for objects contained in corresponding folder in the OPC system. The OPC identification (ID) tag property for automatically generated nodes cannot be edited in the Unison system. Nodes can also be manually created in the

Unison system, however, must map to actual OPC object ID tags. To import a configuration:

1. Create a "Generic OPC" device in the Unison system. This is the "root" node for the OPC server and provides a connection to it.
2. Use the "generate" command on the "Generic OPC" node.

- Device - Management, Configuration and Commands
- Folder - Management, Configuration and Commands
- Input - Management, Configuration and Commands
- Output - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Communications Systems > Modbus

Modbus

Modbus is a generic serial-based protocol designed for bi-directional communications with supporting devices for the purposes of automation; for example, air-conditioning control, fire detection etc. The Unison system supports bi-directional communications with Modbus systems over TCP/IP. With Modbus being based on RS232 serial communications, a Modbus management application that supports TCP/IP connections is required that can be accessible to the Unison Modbus device driver.

Device inputs/outputs [sensors etc] in the Modbus system map to nodes in the Unison system by way of node type and "register" values that represent memory addresses in Modbus devices for reading data [for example, the current value]. The Unison system allows setting of "trigger" events which occur if a pre-defined value is reached in the Modbus system. For example, activate the trigger event if a particular temperature is reached etc. For some nodes, it is possible to set values in the Modbus system by command from the Unison system [that is, they can be "written" to]; other nodes are "read-only". Nodes must be manually created in the Unison system, however, must be correctly mapped to actual Modbus registers. The following node types are supported:

Note: The names for the available Modbus nodes are derived from the Modbus Application Protocol Specification version 1.1B [www.modbus.org]. • Individual device types may or may not support all available register types. • Sub-folders for each registry type are required in order to create nodes.

- Coil - Registers that are considered outputs. Registers of this type can be read and written to.
- Discrete input - Registers that are inputs that can provide a value, as per "analog" inputs. Registers of this type can be read only.

- Holding - Registers that are considered "universal" in that they can be used for inputs, outputs or any kind of data. Registers of this type can be read and written to.
- Input - Registers that are inputs that can be either in an active or inactive state, as per "digital" inputs. Registers of this type can be read only.
- Modbus server - Represents the Modbus application TCP/IP connection.

Understanding Register Addresses

Unison uses Entity Addresses to identify Modbus register numbers.

Note: Modbus register numbers are defined in the Modbus Application Protocol Specification available from www.modbus.com.

In Unison, all Entity Addresses start at register 0. Each data type (Coils, Discreet Inputs, Input Registers, and Holding Registers) are addressed from 0 to 65,535. This allows the Modbus driver to support both standard register ranges (0-9,999) and extended register ranges (0-65,535).

Modbus Standard Register Ranges

Register Type	PLC Address Range	Unison Address Range (Modbus PDU address)	Data Size
Coil Outputs	00000 – 09999	0 – 9,999	1 bit (Read Only)
Digital Inputs	10000 – 19999	0 – 9,999	1 bit (Read Only)
Holding Registers	30000 – 39999	0 – 9,999	16 bit (Read/Write)
Analogue Inputs	40000 – 49999	0 – 9,999	16 bit (Read Only)

Examples

Register Type	PLC Register Number	Unison Register Number
Coil Outputs	00411	411
Digital Inputs	10191	191
Holding Registers	31513	1,513
Analogue Inputs	40000	0

Modbus Extended Register Ranges

Register Type	PLC Address Range	Unison Address Range (Modbus PDU address)	Data Size
Coil Outputs	000000 – 065535	0 – 65,535	1 bit (Read Only)
Digital Inputs	100000 – 165535	0 – 65,535	1 bit (Read Only)
Holding Registers	300000 – 365535	0 – 65,535	16 bit (Read/Write)
Analogue Inputs	400000 – 465535	0 – 65,535	16 bit (Read Only)

Examples

Register Type	PLC Register Number	Unison Register Number

Coil Outputs	000411	411
Digital Inputs	100191	191
Holding Registers	301513	1,513
Analogue Inputs	400000	0

Modbus Data Model Address Ranges

Some PLC's may use the Modbus Data Model (also known as Entity Numbers), which defines register ranges from 1 – 9,999.

Register Type	Modbus Data Model Address Range	Unison Address Range (Modbus PDU address)	Data Size
Coil Outputs	00001 – 09999	0 – 9,998	1 bit (Read Only)
Digital Inputs	10001 – 19999	0 – 9,998	1 bit (Read Only)
Holding Registers	30001 – 39999	0 – 9,998	16 bit (Read/Write)
Analogue Inputs	40001 – 49999	0 – 9,998	16 bit (Read Only)

When the Modbus Data Model is used, it is important to be aware that if a Modbus data register address is X, the Modbus PDU address is X-1. This will affect the Unison register number. It is important to confirm which addressing methodology the Modbus PLC uses in order to monitor the correct register numbers within Unison.

Examples

Register Type	PLC Register Number	Unison Register Number
Coil Outputs	00411	410
Digital Inputs	10191	190
Holding Registers	31513	1,512
Analogue Inputs	40001	0

- Device - Management, Configuration and Commands
- Server - Management, Configuration and Commands
- Folder - Management, Configuration and Commands
- Coil - Management, Configuration and Commands
- Discrete Input - Management, Configuration and Commands
- Holding - Management, Configuration and Commands
- Input - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

Siemens Desigo Insight [BACnet]

BACnet is a standard building management system communications protocol for compatible hardware that defines the various functions and services that devices can be requested to perform. The BACnet protocol represents control equipment as a collection of devices that contain "objects". Objects are uniquely identified by object type and by an instance number, and contain a list of properties. Properties indicate the current state of control equipment; for example, the current temperature value from a thermostat. A BACnet server, connected over TCP/IP, maintains a collection of objects and will respond to BACnet service requests to read and manipulate its objects.

Note: A single Siemens Desigo Insight [BACnet] device only is allowed. • The BACnet integration of the Unison system is currently compatible with the Siemens Desigo Insight 5.1 system only, based on ASHRAE BACnet standards. The Siemens Desigo Insight [BACnet] system is capable of receiving and responding to alarms communicated to it through the Unison system. • The Unison Siemens Desigo Insight BACnet device driver cannot be started until at least one device type has been nominated and a valid notification class is created for it. • If the Unison and Desigo systems exist on different networks, it may take several minutes for communications to initialize. • For device nodes that are sending alarms through the BACnet device, any auto-acknowledge or auto-restore or alarm actions should NOT be set up for alarm types that are being sent to the BACnet device. If additional alarm management work flows are required for such devices, it is recommended to create additional alarm types on the device and to use those for implementing the required alarm management work flow. It is advised not to set up alarm actions that include functionality that is not supported by the Desigo system/work flow. For example, do not apply the "force manual before acknowledge" alarm action status option for alarms being sent to the Desigo system. Auto-close functionality is applied automatically to alarm types sent to the BACnet device. This is because there is no actual "alarm close" function in the Desigo system.

The following node types are supported:

- BACnet device - Provides system functionality for the Siemens Desigo Insight BACnet system.
- Device - Represent device types within the Unison system to be sources of alarms to be sent by Unison through to the Desigo system. When a device type is selected, all instances of that device will pass alarms to the Desigo system. For each device, the child device types required to send alarms must also be selected. For example, areas in a Pacom Controller device.

Note: Device nodes are created using the "add device" command on the Devices folder.

- Notification Class - Represent one or more alarm types to send to the receiving system and a priority to apply to them. Correspondingly, the sending device requires alarm types to be associated with events - these alarm types can be selected here to determine which alarm types are reported to the BACnet system. The priority settings determines how the alarms are displayed to operators in the Desigo system. There are three types of "notification class" available that determine the actions required by operators to respond to the alarm.
- Subscriber - Represent Desigo client applications that are used by operators for monitoring an responding to alarms. These are loaded into the Unison system when the systems connect, however, it may be necessary to restart the Siemens Desigo Insight application in order for the subscribers to load and become visible in the Unison system. Subscriber data is provided for information only and cannot be edited from the Unison system. It is possible to "delete" subscriber nodes from the Unison system. When "deleting", the subscriber is not removed from the Desigo system, however, it is no longer sent alarms from the Unison system. To re-establish a previously deleted subscriber, ensure that the subscriber is exposed to the Unison BACnet device in the Desigo system, then perform a system synchronization [described below].

To synchronize the two systems either after initial set-up or after modification, proceed as follows:

Note: This procedure should be followed when setting up initial communications. It should also be applied after any changes are made to the BACnet device in the Unison system. If the procedure is not followed, synchronization between the two systems will not be correct and unexpected behavior may result; for example, alarms showing in the Desigo system that have no actual information attached to them and also that cannot be acknowledged or restored.

1. Create a device node of type Siemens Desigo Insight, or modify an existing node. Do NOT enable the device (Enabled option = ☐) and do NOT enable sending alarms (Notifications Enabled option = ☐).
2. Add the required device types to expose to the Siemens Desigo system. For each device, select the required node types - alarms from selected node types will be sent to the Desigo system.
3. Create the required "notification class" nodes and select the required alarm types to apply to them.
4. Enable the Siemens Desigo Insight device (Enabled option = ☑) and save the node.
5. In the Siemens Desigo Insight system, perform a "scan" so that the Unison BACnet device is found, then upload it to the "technical view" so that it is recognized as a member of the Desigo BACnet device network.
6. In the Siemens Desigo Insight system, run the "notification wizard" so that the Desigo system is able to receive alarms/events sent by the Unison system.
7. In the Unison system, enable alarm sending for the Siemens Desigo Insight device (Notifications Enabled option = ☑) and save the node.

Device - Management, Configuration and Commands

Device [in "Devices" Folder] - Management, Configuration and Commands
Notification Class - Management, Configuration and Commands
Subscriber - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Elevator Control Systems

Elevator Control Systems

Schindler PORT

You are here: Configuring Third-Party and Generic Devices > Elevator Control Systems > Schindler PORT

Schindler PORT

Schindler PORT is a high-level elevator control system, connected over TCP/IP. This system is typically used in multi-level buildings for providing access to building floors [levels], by way of access card user authentication and proprietary Schindler hardware, using the most efficient elevator. Integration between the Schindler and Unison systems is for the Unison system to provide user and associated access information to the Schindler system. For example, when users are created/deleted/modified, when a user is able to access a floor and which floors can be accessed. The integration is designed so that all user management is carried out in the Unison system and downloaded to the Schindler PORT system. Commands from the Unison system are also performed when received by the Schindler system. For example, to allow access to a floor when an associated area is disarmed or to stop access control on all floors [access control/security over-ride] due to an emergency situation. All access, user and command events are recorded in the Unison database.

Note: When using commands for "all" floors, there may be a latency of around three seconds between sending the command and it being processed for each floor in the Schindler system, with a similar change of security status being displayed in the Unison system. For example, for 10 floors, it may take approximately 30 seconds for the command to complete.

The following node types are supported:

- Schindler device - Provides system functionality for the Schindler PORT system.

- Schindler server - Manages connections between Schindler devices, hosts access control data and communicates with the Unison system over IP.
- Floor - Represents a building level that is controlled by the Schindler system. Floor management is performed in the Schindler system, however, can also be imported or duplicated in Unison. Floor nodes are not a requirement in the Unison system, however, having them allows commands to be sent to specific floors.
- Template - Represents access permissions [days per week and times of day] for one or more floors, that are assigned to users. Template management [create, modify, delete] is performed in the Schindler system and is imported into Unison. Users in the Schindler system must be assigned a single access level template only, therefore, all required floor access for a user must be defined within a suitable template.

Note: The "contents" of access level templates [that is, the floors] is not available for display in the Unison system. • It may be necessary to communicate with administrators of the Schindler system to understand which access level templates to apply to users.

Technician Note: To check template imports, activate the debug logger for the device and use the Unison Debug Monitor application for messages regarding import success/fail. The required format for data exported from the Schindler system is in a *.CSV text file format, where items ["fields"] of data are separated by semi-colon [";"] characters; that is, every data field entry must end with ";". Empty fields must also be defined using semi-colons. It is essential that the correct data items are set up in the Schindler export configuration in order for the data to be correctly interpreted by the Unison system. The template export file requires seven data fields [any additional fields after field 7 are ignored]:

- Field 1 - Ignored.
- Field 2 - Ignored.
- Field 3 - Ignored.
- Field 4 - Template name.
- Field 5 - Ignored.
- Field 6 - Ignored.
- Field 7 - Main group name.

For example, a template with ID "16", name "Main Elevator" and main group name "Building 7" would be written as shown below. In the example, empty fields are shown in **bold-red** and fields containing ignored data are shown in bold-blue for clarity.

16;**;**Template;Main Elevator;**;**Building 7;

Integration Functions and Limitations
Integration Requirements

The Unison system supports importing existing Schindler PORT configurations as well as some limited manual configuration. When importing, nodes in the Schindler system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Create a "Schindler PORT" device in the Unison system. This is the "root" node for the Schindler system.
2. Create a "Schindler server" child node to the "Schindler PORT" device. This node provides a connection to the Schindler server.
3. Use the "import template" command on the "Schindler server" node to import Schindler user access levels.
4. Use the "synchronize users" command on the "Schindler server" node to import users in the Schindler system.

- Device - Management, Configuration and Commands
- Schindler Server - Management, Configuration and Commands
- Floor - Management, Configuration and Commands
- Template - Management, Configuration and Commands
- Schindler PORT User Settings

See Also: Card Profiles | Configuring Third-Party and Generic Devices | Users and Access Cards

---

You are here: Configuring Third-Party and Generic Devices > Fire Protection Systems

Fire Protection Systems

Honeywell Eltek Firewin OPC

Panasonic EBL.NET

Schneider Electric FX NET | Pelco/ESMI ESA

Schrack Seconet Integral IP

Siemens MK8000

You are here: Configuring Third-Party and Generic Devices > Fire Protection Systems > Honeywell Eltek Firewin OPC

Honeywell Eltek Firewin OPC

Honeywell Eltek Firewin is a fire control and building management system that uses OPC [object linking and embedding for process control] for communication. OPC is a standard communications interface for compatible hardware based process control systems. The hardware connects to a Eltek Firewin server that handles messages. The

Unison system connects to the Eltek Firewin server - the Unison device driver must be installed and running on the same computer as the Eltek Firewin server. Functions include receiving messages from the Eltek Firewin system and sending commands to it.

Note: The Eltek Firewin server and Unison Eltek Firewin device driver must run on the same computer. • After upgrading the Unison system to later versions, the Eltek Firewin configuration may be discarded. If this occurs it will be necessary to perform the configuration again. • If any changes are made to the Eltek Firewin system after being imported to the Unison system, it is necessary to re-export the configuration and import it into the Unison system. • Events and commands described in this document are as used in the Eltek Firewin system. Actual functions and meanings may depend on configuration of the Eltek Firewin system or other factors outside of the Unison system. Refer to Eltek Firewin or implementation specific documentation for details.

The following node types are supported:

- Area - Represent groups of equipment that can be controlled by the associated area. This is similar to the generic "area" node in the Unison system. For example, an area enters an alarm state if any of its associated detectors is in alarm. Similarly, all nodes associated with an area can be controlled by a single command to the area. Nodes that are associated with areas are shown in the properties for an area.
- Group - Represent alarm categories for output types.
- Loop - Represent detectors and associated devices, such as fire alarm buttons, that are wired in a loop arrangement [usually a two-wire connection] or require to be associated for management purposes. Loops are continually monitored for connectivity of all associated components. Nodes that are associated with loops are shown as "child" nodes for a loop.
- Unit - Represent physical panel hardware, and show associated nodes in a hierarchical structure.

Integration Requirements

The Unison system supports importing existing Eltek Firewin configurations. When importing, nodes in the Eltek Firewin system are replicated in the Unison system - this makes device configuration faster and less prone to error. Objects in the system are "imported" from a configuration .TXT file and generated automatically in the Unison system as nodes. Sub-folders to the parent device node are created if they exist in the Eltek Firewin system, with applicable nodes contained within them. Identification information for Eltek Firewin objects are applied as names in the Unison system. To import a configuration:

1. Use the Eltek Firewin server application to export the current configuration as a .TXT file.
2. Create a "Eltek Firewin" device in the Unison system. This is the "root" node for the Eltek Firewin system.
3. Use the "generate from file" command on the "Eltek Firewin" node and select the

exported file.

Note: When creating the fxf-file that the Firewin server uses, ensure that numbers are stored as hexadecimal numbers. The format of the fxf file affects the .TXT file that Unison uses.

- Device - Management, Configuration and Commands
- Area - Management, Configuration and Commands
- Group - Management, Configuration and Commands
- Loop and Node - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Fire Protection Systems > Panasonic EBL.NET

Panasonic EBL.NET

The Panasonic EBL.NET is an analog addressable fire alarm system that also supports conventional fire detection equipment. The device driver communicates with the physical device via a "web server" interface, which is normally connected to the first control unit via RS232. The following Panasonic EBL products are supported:

- EBL512 United 2.7.
- EBL512 G3 1.1/2.0/2.1/2.2.x protocols.
- EBL128 control unit hardware.

The following nodes used in the Panasonic EBL.NET system and sub-folders for managing certain nodes are supported. No properties and limited commands only are available for Panasonic EBL.NET node types in the Unison system:

- Control unit - Represent physical panel hardware [also known as "control and indicating equipment" or "CIE"], and show associated nodes in a hierarchical structure. A control unit supports up to 1020 address, of which 512 can be alarm points. An EBL.NET system contains at least one control unit, up to a maximum of 30 connected via TLON network.
- Alarm device - Represent a collection of alarm devices in the EBL.NET system. Alarm devices are used to send non-fault/fire alarms. Alarm device nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.
- Alert annunciation active - Represent a collection of alert annunciation active instances in the EBL.NET system. Alert annunciation active instances are used to assist operators in focusing on more urgent alarms. Alert annunciation active nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.

- Control - Represent a collection of controllable outputs in the EBL.NET system. Control nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.
- Detector/sensor - Represent detector devices that are used to generate fire alarms through smoke and/or heat measurement.
- Display unit/fire brigade panel - Represent display units can be connected to the EBL.NET system, usually via expansion boards. The fire units can be either a fire schedule type, a presentation schedule or a delay schedule. All units have the same events and commands.
- Expansion board - Represent expansion cards that can be attached to EBL.NET control units, for connecting conventional detector loops, fire brigade panel (FBP), outputs etc. All expansion boards are similar regarding events and commands.
- Extinguisher - Represent a collection of extinguishers in the EBL.NET system. Extinguishers are used for fire fighting. Extinguisher nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.
- Fault alarm transmitter - Represent a collection of fault alarm transmitters in the EBL.NET system. Fault alarm transmitters are used to send fault alarms. Fault alarm transmitter nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.
- Fire alarm transmitter - Represent a collection of fire alarm transmitters in the EBL.NET system. Fire alarm transmitters are used to send fire alarms. Fire alarm transmitter nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.
- Interlock - Represent a collection of interlocks in the EBL.NET system. Interlocks are used to define automated output activation if an input is in alarm. Interlock nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.
- Loop - Represent device connections (for example, detectors, inputs, manual call points, outputs etc) from physical connection ports on control unit devices or expansion boards. Loops show associated nodes in a hierarchical tree structure.

Note: For detector devices with multiple alarm points; for example, a single device with separate detectors for smoke and heat built in, separate nodes are created for the device [the "main" node] and each alarm point ["secondary" nodes] so that normal control is available as though each detector component is a separate device. If a fault occurs in the device, it is associated with the main node.

- Control units have four standard loop connections (NMAST).
- Control units can be equipped with expansion boards for up to 8 conventional loop connections (DET8).
- Control units can be equipped with expansion boards for Autronica-loops (BS4).
- On standard loops, address units can be used to connect a conventional loop (3361).

- Input - Represent non-detector devices connected via input/output devices that can provide input signals; for example, fire system water pressure sensor - the different

types of inputs are listed below. Each input has its own events and functions.

- Activated extinguisher
- Activated fault transmitter
- Activated fire ventilation
- Activated key cabinet
- Activated routing equipment
- Alarm devices off/disable areas
- Alarm point
- Alert annunciation acknowledge
- Alert annunciation reset
- Evacuate
- External fault
- External power supply delayed battery fault
- External power supply delayed mains fault
- External time channel
- Extinguisher start
- Extinguisher stop
- Extinguishing alarm
- Extinguishing system fault
- Fault signal external fuses
- Fault signal external power supply
- Fault warning routing equipment fault
- Fire door closing test
- Interlocking
- Key cabinet
- Loss of battery charge to external power supply
- Pre-warning
- Silence alarm
- Technical warning
- Unused

- Input/output device - Represent devices connected to control units via loops that inputs and outputs connect to.
- Interlocking - Represent links between several outputs in the system so that can be controlled simultaneously. Interlocking combinations are defined in the EBL.NET system, however, can be activated/deactivated from the Unison system, if required.
- Manual call point - Represent input devices [buttons etc] that are manually activated by persons to generate a fire alarm.
- Output - Represent fire safety/extinguishing devices connected via input/output devices that can provide output signals; for example, fire fighting mechanisms and emergency escape lighting - there are many different types of outputs. Outputs are managed by control units through logical programming or status conditions. Outputs can be activated/deactivated from the Unison system, if required.
- Section - Represent "virtual" folders as logical groupings of detectors in a control unit to make it easier to present and manage groups of detectors; for example, in different parts of a building. A section can contain 99 detectors and have an identification (ID) number up to "999". Sections are defined in the EBL.NET system.
- Short circuit isolator - Represent devices that are placed in loops to isolate parts of the loop in the event of a short-circuit so that the entire loop does not become disabled.
- Ventilation - Represent a collection of ventilators in the EBL.NET system. Ventilation are used for smoke extraction. Ventilation nodes are generated in the Unison system only when they are associated with the control unit defined in the Unison system.

Integration Requirements

The Unison system supports importing existing Panasonic EBL.NET configurations. When importing, nodes in the Panasonic system are replicated in the Unison system - this makes device configuration faster and less prone to error. Objects in the system are "imported" from a configuration .EBL file and generated automatically in the Unison system as nodes. Sub-folders to the parent device node are created if they exist in the Panasonic system, with applicable nodes contained within them. Identification information for Panasonic objects are applied as names in the Unison system. To import a configuration:

1. Use the Panasonic EBL.NET application to export the current configuration as a .EBL file.
2. Create a "Panasonic EBL.NET" device in the Unison system. This is the "root" node for the Panasonic system.
3. Use the "generate from file" command on the "Panasonic EBL.NET" node and select the exported file.

- Device - Management, Configuration and Commands
- Alarm Device - Management, Configuration and Commands
- Alert Annunciation Active - Management, Configuration and Commands
- Control Unit - Management, Configuration and Commands
- Control - Management, Configuration and Commands
- Detector/Sensor/Manual Call Point - Management, Configuration and Commands
- Extinguisher - Management, Configuration and Commands
- Fault Alarm Transmitter - Management, Configuration and Commands
- Fire Alarm Transmitter - Management, Configuration and Commands
- Fire Brigade Panel - Management, Configuration and Commands
- Input - Management, Configuration and Commands
- Input/Output [I/O] Device - Management, Configuration and Commands
- Interlock - Management, Configuration and Commands
- Interlocking - Management, Configuration and Commands
- Loop Unit - Management, Configuration and Commands
- Output/Short-Circuit Isolator/Siren - Management, Configuration and Commands
- Power Supply - Management, Configuration and Commands
- Section - Management, Configuration and Commands
- Ventilation - Management, Configuration and Commands
- Programming Examples

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Fire Protection Systems > Schneider Electric FX NET | Pelco/ESMI ESA

Schneider Electric FX NET | Pelco/ESMI ESA

The Schneider Electric FX NET [previously Pelco/ESMI ESA] is an addressable fire

alarm system with up to 16 networked client monitoring stations. The device driver is compatible with the MESA1 system, connected serially to the Unison Schneider Electric FX NET device server. The following node types are supported:

- ESA device - Provides system functionality for the Schneider Electric FX NET system.
- Area - Represent logical groups of individual fire detection inputs for alarm reporting and management purposes. For example, all detectors in a particular location could logically be grouped into a single "area". Each area is able to group up to 9999 detectors.
- Detector - Represent individual fire detection inputs associated with a particular loop. Detectors can be automatically generated.
- Loop - Represent detectors and associated devices, such as fire alarm buttons, that are wired in a loop arrangement [usually a two-wire connection] or require to be associated for management purposes. Nodes that are associated with loops are shown as "child" nodes for a loop.
- MESA control unit - Represent control unit hardware that is used for alarm event notifications. Up to four control units can be connected within the one network.
- Unit - Represent hardware for connecting detector loops and managing zones/areas.

Integration Requirements

The Unison system supports importing existing Schneider detector configurations on a per loop basis. When importing, nodes in the Schneider system are replicated in the Unison system - this makes device configuration faster and less prone to error. Identification information for detectors are applied as names in the Unison system. To import loop detector configurations:

1. Create a "ESA" device in the Unison system. This is the "root" node for the Schneider system.
2. Create a "unit" device and child loop nodes in the Unison system. Loop addresses must match those set up in the Schneider system.
3. Use the "generate detectors" command on each loop node.

Device - Management, Configuration and Commands
Area - Management, Configuration and Commands
Detector - Management, Configuration and Commands
Loop - Management, Configuration and Commands
MESA Unit - Management, Configuration and Commands
Unit [ESA] - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Fire Protection Systems > Schrack Seconet Integral IP

Schrack Seconet Integral IP

Schrack Seconet Integral IP is a fire alarm system, connected over TCP/IP. Schrack Seconet Integral IP "control units" can connect inputs, outputs and a number of other devices. There are two types of configuration supported in the Unison system:

- "Simple" configuration - Up to 16 control units. Generally, this configuration is for small installations that have no more than 16 control units.
- "N3" configuration - Up to 1024 control units, split into sub-networks (maximum of 64), each with up to 16 control units. Generally, this configuration is for larger installations that have more than 16 control units.

The following node types are supported:

- Battery - Represent device backup batteries used in Schrack control unit hardware.
- Control unit - Represent physical panel hardware, or "virtual" sub-network in an N3 configuration, and show associated nodes in a hierarchical structure.
- External - Represent "virtual" nodes in the Schrack system that are able to generate events and accept commands.
- Input - Represent non-zone detector devices connected to Schrack hardware that can provide input signals; for example, fire system water pressure sensor.
- Output - Represent fire safety/extinguishing devices connected to Schrack hardware; for example, fire fighting mechanisms and emergency escape lighting.
- Zone - Represent groups of detector equipment, known as "zone detectors", that can be controlled by the associated zone. This is similar to the generic "area" node in the Unison system. For example, a zone enters an alarm state if any of its associated detectors is in alarm. Similarly, all zone detectors associated with a zone can be controlled by a single command to the zone.
- Zone detector - Represent fire detection devices connected to Schrack hardware; for example, smoke detectors. These nodes, when active represent fire alarms.

The Unison system supports importing existing Schrack Seconet configurations as well as manual configuration. When importing, nodes in the Schrack system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

Note: It is highly recommended to configure Schrack systems using an exported .XML configuration file. Multiple configuration files can be imported into a single Schrack server node, if required • If any changes are made to the Schrack system after being imported to the Unison system, it is necessary to re-export the configuration and import it into the Unison system. • Events and commands described in this document are as used in the Schrack system. Actual functions and meanings may depend on configuration of the Schrack system or other factors outside of the Unison system. Refer to Schrack or implementation specific documentation for details.

1. Use the Schrack Seconet IntegralApplicationCenter application to export the

current configuration ["export to OPC server" function. Also, export custom texts - these are used as node names in the Unison system] as one or more .XML files.
2. Create a "Schrack Seconet Integral IP" device in the Unison system. This is the "root" node for the Schrack system.
3. Create a "server" child node to the "Schrack Seconet Integral IP" device. This node provides an IP connection to a control unit.
4. Use the "generate" command on the "server" node and select the exported file(s).

- Device - Management, Configuration and Commands
- Server - Management, Configuration and Commands
- Control Unit - Management, Configuration and Commands
- Battery - Management, Configuration and Commands
- External - Management, Configuration and Commands
- Input - Management, Configuration and Commands
- Output - Management, Configuration and Commands
- Zone - Management, Configuration and Commands
- Zone Detector - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Fire Protection Systems > Siemens MK8000

Siemens MK8000

The Siemens MK8000/Algorex/Sinteso fire detection and alarm system provides various fire alarm warning and response functions. The Unison integration connects to the Siemens system via an OPC (object linking and embedding for process control) server that handles messages between the two systems so that Unison operators are able to monitor aspects of the Siemens system and repond to alarms from it. The following Siemens products are supported:

- MK8000 OPC Server MP4.50.
- Algorex EP7.
- FS20 [Sinteso] hardware with FC2020/FC2040/FC2060/FC2080 controllers.

The following nodes used in the Siemens system and sub-folders for managing certain nodes are supported:

- Siemens MK8000 device - Provides system functionality for the Siemens system.
- NK8222/NK8223 gateway - Provides connections between local and distributed safety and security devices to the CDI network. It provides a first level of centralization and acts as a secure communication partner for the NK8210, MM8000 and MK8000. Nodes include:

- Cerecom Ion - Represents connections between CS6 Guard and control units.
- Clock - Represents NK822x system clock status.
- Digital input - Represents selectable NK822x digital data inputs.
- Digital output - Represents selectable NK822x digital data outputs.
- Ethernet - Represents a virtual Ethernet connection with a management station in an MK8000 or MM8000 project.
- IC2 bus - Represents a bus line for connecting I/O modules and power supplies.
- Line: COM1 - Represents connection status on the COM1 line.
- Power supply - Represents any issues with the power supply, and is managed by a DF8090 device connected tha NK822x, 12C connector.
- Tamper control - Represents NK822x tamper protection status.

- Algorex control unit/terminal - Represent "Algorex" type panel hardware and shows associated nodes in "logical" and "physical" hierarchical tree structures. This device provides events related to the entire CC11 detection system as well as the control unit itself. Logical tree nodes include:

  - Addressable fire detector - Represents a fire detector for automatic alarm detection and individual identification.
  - Alarm transfer equipment: external horn - Represents an output to external devices that receive control activation commands directly from the higher ranking area.
  - Alarm transfer equipment: internal horn - Represents an internal audio output that receives its control activation commands directly from the higher ranking area. Typically, the internal horn is activated simultaneously with the buzzer on the CT11.
  - Alarm transfer equipment: remote transmission channel alarm/fault/other - Represents a remote transmission output for alarms, faults and other outputs that are neither alarms or faults. RT channels receive their control commands directly from the higher ranking area. Typically they are activated in accordance with the Cerberus Alarm Concept (CAC). The CAC prevents unnecessary calling of the fire department for minor incidents.
  - Alarm transfer equipment: RT controller alarm - Represents the "alarm remote transmission delay" within an area.
  - Alarm transfer equipment: RT device - Represents a remote transmission output for alarms, faults and other outputs that are neither alarms or faults. RT channels receive their control commands directly from the higher ranking area. Typically they are activated in accordance with the Cerberus Alarm Concept (CAC). The CAC prevents unnecessary calling of the fire department for minor incidents.
  - Building services section - Represent one or more zones (and in turn, other elements) that monitor or control devices for general services in supervised buildings.
  - Building services zone - Represent a zone that generates (activates) a signal when it detects a state of danger. It evaluates whether a situation should be considered dangerous based on parameters configured for the zone.
  - Digital output - Represent output elements without feedback, activated to control simple external devices such as lamps etc. These elements do not have a feedback input, but can detect an internal fault.

- Fire area - Represent the highest level in the CS11 logical node tree structure and are a grouping for fire sections.
- Fire section - Represent the logical level below "fire area" objects in the CS11 structure and reports the conditions of the associated fire detection zones [inputs].
- Fire zone - Represent the logical level below "fire section" objects in the CS11 structure and are individual fire detection inputs.
- Manual call point - Represent fire alarm equipment that is activated by users; for example, a fire alarm button.
- Manual zone - Represent a zone made up of manual call points.
- Single zone - Represent a zone made up of a single detection element.

Physical tree nodes include:

- Addressable detection line - Represent hardware components that report alarms and faults that, for technical reasons, cannot be reported by detection zones.
- Control panel - Represent hardware components that report any alarms and faults that, for technical reasons, cannot be addressed on the detection zones or detection lines.
- Controller binary/digital I/O - Represent hardware components that report any alarms and faults that, for technical reasons, cannot be addressed on the detection zones or detection lines.
- Digital collective I/O module -
- Power supply - Represent hardware components that report power supply monitoring conditions.
- Transfer record - The transfer record is a representation of a CT11/CK11 connection to the local CK11.

- FS20 control unit/terminal - Represent "FS" type panel hardware and shows associated nodes in "logical" and "physical" hierarchical tree structures. Logical tree nodes include:

  - Alarm control - Represent individual instances of control logic, where each control has dedicated functionality. Control function information should be entered in the description property so that it can be more easily identified.
  - Alarm control group -
  - Alarm intervention verification element [AVC/IC] - Represent elements that andle delays for activating alarm equipment and remote transmission ["RT"] units. The count-down delays for T1 or T2 are displayed when active.
  - Automatic zone - Represent a required element (EN54-2 regulations) that handles raw alarm information coming from one or more detectors. It supports several operating modes influencing the sensitivity of the attached detectors. Different kinds of zones are used according to the required purpose.
  - Alert evacuation sounder channel - Represents an output to external devices that are used as an audible fire warning.
  - Base sounder - Represent "base sounder" functionality of automatic fire detector equipment.
  - Cause and effect group - Represent objects that do not provide any process

information, but are used to separate "causes" from "effects" within the hierarchical tree structure.
- Cause incident [generic] - Represent objects that are used to identify "causes" within the hierarchical tree structure.
- Collective channel - Represent objects that are used exclusively in the "control domain". Specific sensor channels handle the information of different kinds from detection devices and logical inputs report technical alarms coming from other systems. Logical channels are configured as all other elements in the detection tree and then linked to physical channels during commissioning.
- Evacuation control - Represent individual instances of evacuation control logic, where each control has dedicated functionality. Control function information should be entered in the description property so that it can be more easily identified.
- Evacuation control group - Represent objects that are used for organizing different kinds of controls. The four main control groups include alarm, fire, evacuation, and fire extinguishing.
- Evacuation sounder channel - Represent outputs to external devices that are used as an audible evacuation warning.
- Evacuation universal control - Represent individual instances of control logic, where each control has dedicated functionality. Control function information should be entered in the description property so that it can be more easily identified.
- Fire area - Represent control for arming/disarming associated detectors in a single operation, and for identification and organizational purposes.
- Fire control - Represent individual instances of control logic, where each control has dedicated functionality. Control function information should be entered in the description property so that it can be more easily identified.
- Fire control group - Represent objects that are used for organizing different kinds of controls. The four main control groups include alarm, fire, evacuation, and fire extinguishing.
- Fire effect request logical channel - Represnt objects that are a special type of logical channel that models the function of an internal command to another element. It is not linked to a physical channel.
- Fire output - Represent logical channels, used exclusively for the control domain. Inputs are used to trigger controls that in turn activate uutputs or sounders. The configured logical channels are also linked to physical channels.
- Fire section - Represent control for arming/disarming associated detectors in a single operation, and for identification and organizational purposes.

Note: This is an optional structure. The same functions can also be performed at "fire area" level.

- Input channel - Represent objects that are used exclusively in the "logical domain" where specific sensor channels handle the information of different kinds from detection devices. A logical input is used for technical alarms coming from other systems. Logical channels are configured as all other elements in the detection tree and then linked to physical channels during commissioning.

- Manual alarm sub-system zone - Represent objects thar are a required element (EN54-2 regulations) that handles raw alarm information coming from one or more detectors. It supports several operating modes influencing the sensitivity of the attached detectors. Different kinds of zones are used according to the required purpose.
- RT fault control - Represent individual instances of control logic, where each control has dedicated functionality. Control function information should be entered in the description property so that it can be more easily identified.
- RT fire control - Represent individual group entities of control logic, where each control has dedicated functionality. Control function information should be entered in the description property so that it can be more easily identified.
- RT output logical channel - Represent output logical channels are exclusively used in the control domain. Inputs are used to trigger controls that in turn activate outputs or sounders. These configured logical channels are also linked to physical channels.
- Station area - Represent control for arming/disarming associated detectors in a single operation, and for identification and organizational purposes.
- Undefined/undocumented event - Represent events concerning objects that could not be properly identified in the current panel configuration.
- Wired automatic channel - Represent automatic channels are exclusively used in the "logical domain". Specific sensor channels handle the information of different kinds from detection devices and logical inputs report technical alarms coming from other systems. Logical channels are configured as all other elements in the detection tree and then linked to physical channels during commissioning.
- Wired manual channel - Represent manual channels are exclusively used in the "logical domain". Specific sensor channels handle the information of different kinds from detection devices and logical inputs report technical alarms coming from other systems. Logical channels are configured as all other elements in the detection tree and then linked to physical channels during commissioning.

Physical tree nodes include:

- CPU module - Represent CPU hardware modules that can be incorporated with an FS20 host. It can be sub-divided into sub-modules. The CPU module has a specific designation.
- Degrade element sub-module - Represent degraded mode functional components of a module. Generally, sub-modules evaluate faults, however, degrade element sub-modules may also evaluate alarms.
- Ethernet module - Represent Ethernet connection hardware modules that can be incorporated with an FS20 host. It can be subdivided into sub-modules.
- Firmware sub-module - Represent the firmware functional component of a hardware module.
- Floor repeater configuration group - Represent objects that are used for building groups of configuration elements. These elements are visible in BACnet only for building the node tree to configure the panel with. The configuration groups are used for configuration issues, for example, communication.
- Generic configuration element - Represent objects that are mainly used for the

configuration of country-specific operations and to view peripherals. Some process states can also be evaluated as well as some operation modes.

- Generic device - Represent peripheral device hardware on the field bus and consists of physical channels. The evaluation of process relevant information is delegated to the detection or control domain, except the line separator and wireless gateway device.
- I/O module - Represent I/O [input/output] hardware modules that can be incorporated with an FS20 host. It can be subdivided into sub-modules. The I/O module has a specific designation.
- License element sub-module - Represent the license functional components of module used for evaluating faults.
- Network object - Represent some aspects of the communication with other panels. This comprises of requests for opening communications, incorrect certificates, communication faults, and degrades alarms transmitted from another panel.
- P2 module - Represent P2 hardware modules that can be incorporated with an FS20 host. It can be sub-divided into sub-modules.
- P2 element sub-module - Represent a P2 field bus, and is a functional part of a module. Generally, sub-modules evaluate faults, however, some sub-modules may also evaluate alarms.
- Person machine interface - Represent the user interface on Siemens client applications.
- Power supply module - Represent power supply hardware modules that can be incorporated with an FS20 host. It can be subdivided into sub-modules. The power supply module has a specific designation.
- System buzzer - Represent generic configuration elements that are mainly used for the configuration of country-specific operations and to view peripherals. Some process states can also be evaluated as well as some operation modes.

Integration Requirements

The Unison system supports importing existing Siemens Composer projects. When importing, nodes in the Siemens system are replicated in the Unison system - this makes device configuration faster and less prone to error. Objects in the system are "imported" from a configuration .BAK file [which must be created first] and generated automatically in the Unison system as nodes. Sub-folders to the parent device node are created if they exist in the Siemens system, with applicable nodes contained within them. Identification information for Siemens objects are applied as names in the Unison system. To export and import a configuration:

a. Use the Siemens Export Wizard application [usually located in the C:\Program Files (x86)\DMS8000\Utilities\Export Wizard folder] to create the project configuration export:

    a. Select the required Composer application project.
    b. Ensure that all fields are exported.
    c. Set the "character to separate each field" to a semi-colon (";") character.
    d. Enable the "include title line in table" option.

e. Set the "coherence test", if required [this is optional].
f. Export the current configuration as a .BAK file

2. Create a "Siemens MK8000 " device in the Unison system. This is the "root" node for the Siemens system.
3. Use the "generate from file" command on the "Siemens MK8000" node and select the exported file.

- Device - Management, Configuration and Commands
- NK8222/8223 Gateway
- Algorex Control Unit/Terminal - Management, Configuration and Commands
- FS20 Control Unit/Terminal - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Intercom Systems

Intercom Systems

Commend GE 501

Commend GE 200/300/700/800

Stentofon Alphacom

Stentofon Touchline

You are here: Configuring Third-Party and Generic Devices > Intercom Systems > Commend GE 501

Commend GE 501

The Commend GE 501 intercom system is often used by security, business and emergency services. The system enables connections ("calls") to be made between devices, such as intercom units or stations and telephone exchange equipment. The Unison system is able to replicate the configuration of the GE 501 system by "reading" the existing configuration from it ["generate" command on GE 501 "device" node]. The system integration enables alarms from the Unison system to be linked to one or more devices in the GE 501 system to be able to automate calls etc, and also for commands from Unison [for example, making calls from the Unison system] to be processed by GE 501. The following node types are supported:

- Commend GE 501 device - Provides system functionality for the GE 501 intercom system.
- Alias station - Represents a connection between a Commend exchange and intercom station that is made by using a Unison client. Multiple clients can share the same alias station, however, each Unison client can be associated with a single alias station only. For each alias station connection, an intercom station and connecting exchange must be specified. This enables Unison to be used as a method for creating and responding to calls as though it is a "station".
- Exchange - Represents "hubs" that intercom stations connect to in order to make and receive calls to/from other station(s).
- SAM - Represents physical intercom stations that connect to a GE 501 exchange that can be used as a "normal" station and to also answer call requests.
- Station [intercom] - Represents physical telephones that connect to a GE 501 exchange to make and receive calls to/from other stations.

Integration Requirements

The Unison system supports importing existing Commend GE 501 configurations as well as some limited manual configuration. When importing, nodes in the Commend system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Create a "Commend GE 501" device in the Unison system. This is the "root" node for the Commend system and provides a connection to the Commend server.
2. Use the "generate" command on the "Commend GE 501" device.

Device - Management, Configuration and Commands
Alias Station - Management, Configuration and Commands
Exchange - Management, Configuration and Commands
SAM - Management, Configuration and Commands
Station - Management, Configuration and Commands
Programming Example

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Intercom Systems > Commend GE 200/300/700/800

Commend GE 200/300/700/800

Commend GE 200, GE 300, GE 700 and GE 800 are intercom based communications systems often used by security and emergency services personnel. The device driver allows the configuration of connections ("calls") between telephone "station" nodes and telephone "exchange" nodes, that receives and connect calls. The following node types are supported:

- Commend GE 700 device - Provides system functionality for the GE 200/300/700/800 intercom system.
- Alias station - Represents a connection between a Commend controller [exchange] and station that is made by using a Unison client. Multiple clients can share the same alias station, however, each Unison client can be associated with a single alias station only. For each alias station connection, a station and connecting controller must be specified. This enables Unison to be used as a method for creating and responding to calls as though it is a "station". Alias station nodes can also be used for simulating button presses as though by a user of the station device.
- Controller [exchange] - Represents "hubs" that stations (telephones) connect to in order to make and receive calls to/from other station(s).
- Station - Represents physical telephones that connect to a Commend controller [exchange] to make and receive calls to/from other stations. Station nodes can also be used for simulating button presses as though by a user of the station device.

Integration Requirements

Before a Commend controller device is connected to the Unison system it must first be configured correctly. Configuration is performed using Commend Controller Configuration Tool V6 software. This section briefly describes configuration requirements.

Note: For detailed instructions refer to manufacturer documentation.

- It is recommended that the Commend controller is configured so that "line monitoring" (also called "synchronization") for "call requests" is activated. This helps reduce traffic between the controller and the device driver.
- Ensure that each station has the address of another station configured if line faults occur.
- If Commend keyboard shortcuts are used, ensure that the first key in any combination starts with "T". For example, "T+1" to connect a call from station A to station B.

For GE 300 and GE 800 systems:

- The first "data interface" and "TCP/IP" connections must be the connection to Unison. This setting must be an "ICX" type connection.
- A "subscriber control desk" must be configured so that the "IP/RS232-ICX" setting uses the "ICX" connection.
- Set the "idle time" interval between the Commend controller sending messages to notify the Unison system that it is connected and operational. These messages must be sent at least every eight (8) second to avoid communication errors. The idle time is set as part of "data interfaces", "TCP/IP" configuration.

The Unison system supports importing existing Commend GE configurations as well as some limited manual configuration. When importing, nodes in the Commend system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Use the Commend CCT application to export the current configuration as a .CCT file.
2. Create a "Commend GE 700" device in the Unison system. This is the "root" node for the Commend system and provides a connection to the server.
3. Use the "generate" command on the "Commend GE 700" node and select the exported file.

Device - Management, Configuration and Commands
Alias Station - Management, Configuration and Commands
Controller [Exchange] - Management, Configuration and Commands
Station - Management, Configuration and Commands
Programming Example

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Intercom Systems > Stentofon Alphacom

Stentofon Alphacom

The Stentofon Alphacom intercom/telephony system is often used by security, business and emergency services. The system enables connections ("calls") to be made between devices, such as intercom units or stations and telephone exchange equipment. The Unison system is able to replicate the configuration of the Alphacom system by "reading" the existing configuration from it ["generate" command on Alphacom "device" node]. The system integration enables alarms from the Unison system to be linked to one or more devices in the Alphacom system to be able to automate calls etc, and also for commands from Unison [for example, making calls from the Unison system] to be processed by Alphacom. The following node types are supported:

- Stentofon Alphacom device - Provides system functionality for the Alphacom intercom system.
- Alias station - Represents a connection between a Alphacom exchange and intercom station that is made by using a Unison client. Multiple clients can share the same alias station, however, each Unison client can be associated with a single alias station only. For each alias station connection, an intercom station and connecting exchange must be specified. This enables Unison to be used as a method for creating and responding to calls as though it is a "station".
- Exchange - Represents "hubs" that intercom stations connect to in order to make and receive calls to/from other intercom station(s).
- Station [intercom] - Represents physical intercom units that connect to a Alphacom exchange to make and receive calls to/from other stations. Station nodes can also be used for simulating button presses as though by a user of the station device.

Integration Requirements

The Unison system supports importing existing Stentofon Alphacom configurations as well as some limited manual configuration. When importing, nodes in the Stentofon system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Create a "Stentofon Alphacom" device in the Unison system. This is the "root" node for the Alphacom system and provides a connection to the Alphacom server.
2. Use the "generate" command on the "Stentofon Alphacom" device.

Device - Management, Configuration and Commands
Alias Station - Management, Configuration and Commands
Exchange - Management, Configuration and Commands
Station - Management, Configuration and Commands
Programming Example

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Intercom Systems > Stentofon Touchline

Stentofon Touchline

Stentofon Touchline intercom/telephony equipment is often used by security, business and emergency services. The system enables connections ("calls") to be made between devices, such as intercom units or stations and telephone exchange equipment. The Unison system is able to replicate the configuration of the Touchline system by "reading" the existing configuration from it ["generate" command on Touchline "device" node]. The system integration enables alarms from the Unison system to be linked to one or more devices in the Touchline system to be able to automate calls etc, and also for commands from Unison [for example, making calls from the Unison system] to be processed by Touchline. The following node types are supported:

- Stentofon Touchline device - Provides system functionality for the Touchline intercom system.
- Alias station - Represents a connection between a Touchline exchange and intercom station that is made by using a Unison client. Multiple clients can share the same alias station, however, each Unison client can be associated with a single alias station only. For each alias station connection, an intercom station and connecting exchange must be specified. This enables Unison to be used as a method for creating and responding to calls as though it is a "station".
- Exchange - Represents "hubs" that intercom stations connect to in order to make and receive calls to/from other intercom station(s).
- Station [intercom] - Represents physical intercom units that connect to a Touchline

exchange to make and receive calls to/from other stations. Station nodes can also be used for simulating button presses as though by a user of the station device.

Integration Requirements

The Unison system supports importing existing Stentofon Touchline intercom station configurations as well as some limited manual configuration. When importing, nodes in the Stentofon system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

1. Create a "Stentofon Touchline" device in the Unison system. This is the "root" node for the Touchline system and provides a connection to the Touchline server.
2. Create an "exchange" device node. This is a node representing a Touchline exchange device.
3. Use the "generate" command on the "exchange" device.

Device - Management, Configuration and Commands
Alias Station - Management, Configuration and Commands
Exchange - Management, Configuration and Commands
Station - Management, Configuration and Commands
Programming Example

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Miscellaneous Devices

Miscellaneous Devices

HID Fargo Printer

Deister Key Management System

Traka Key Management System

You are here: Configuring Third-Party and Generic Devices > Miscellaneous Devices > HID Fargo Printer

HID Fargo Printer

HID Fargo printers are used for reading, encoding and printing user access cards. The device driver supports data encoding for Mifare Classic 1k, 4k and Ultralight access

card types.

Note: A thorough understanding of the required access card data encoding settings is required.

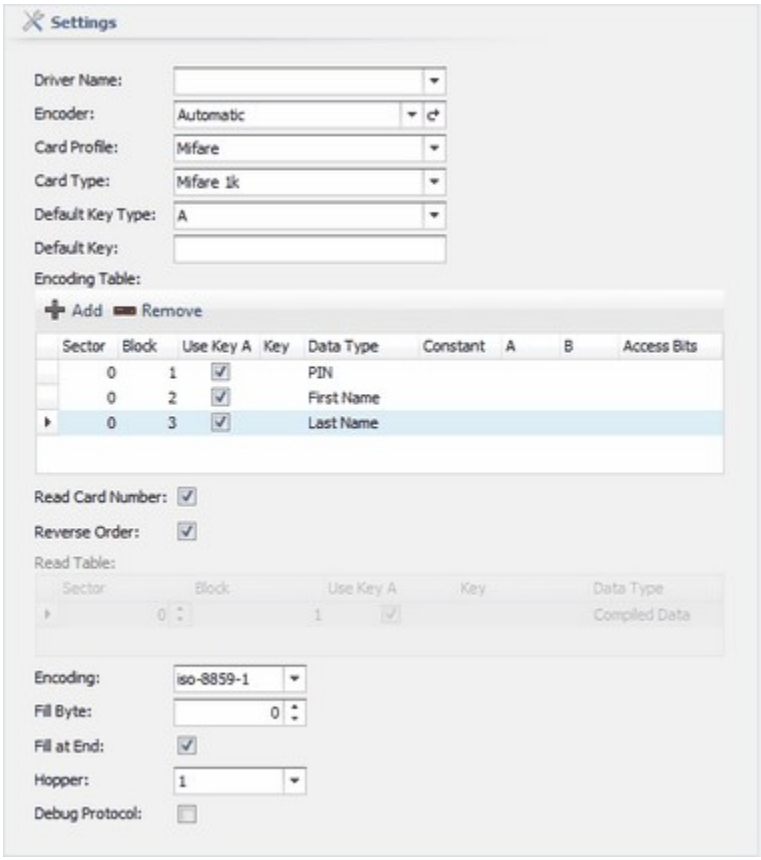
Integration Requirements

The following prerequisites are required before integration:

- Installation of Fargo hardware and software needs to be per manufacturer recommendations.

Device - Management, Configuration and Commands

The Hardware view enables managing Schindler device nodes. Click (Hardware) in the System Configuration ribbon bar to open the view. Click (Create Device) in the view toolbar to display a list of supported node types, and select Fargo Printer. The new device is added to the device tree in the Explorer, with its settings available in the Properties section.



Control	Description
Properties Tab	
Properties - One or more "generic" node properties apply. Click here for help. Additional properties, if any, are listed below.	
Settings	

Driver Name

Sets the Fargo printer driver software, which must be installed on the computer that the printer is connected to. The selected driver must be compatible with the printer. To edit, click ▾ to display options. Click an option to select it:

- Installed printer drivers.

Encoder

Sets the device used to magnetically encode card data, if the printer itself is not capable of encoding. To edit, click ▾ to display options. Click an option to select it:

- Automatic - The printer performs the encoding.
- Available encoders.

Note: When "automatic" is not available, click ↻ to find any available encoders and add them to the selection list.

Card Profile

Sets the card data profile to apply when encoding access cards. The selected profile must be compatible with card readers that the user is expected to use. To edit, click ▾ to display options. Click an option to select it:

- Available card profiles.

Card Type

Sets the physical card type being printed and encoded. The setting must match the actual cards being used. To edit, click ▾ to display options. Click an option to select it:

- Available card types.

Default Key Type

Sets default values to apply to access card data for cards that are pre-programmed to use them, by way of nominating a "default key" - two values are available, classified as "A" and "B". When using a This setting requires the Default Key setting to have a value and is applied before any key that is specified in the Encoding Table settings is used. To edit, click ▾ to display options. Click an option to select it:

- A - Use values defined as "A" as defaults.
- B - Use values defined as "B" as defaults.

Default Key

Determines if pre-programmed default key data (Default Key Type setting) is used. If the default key setting is not applicable, keys set in the Encoding Table are used instead.

Encoding Table - Card data settings that are used when no default key values are specified. Each row defines the data to program for a "sector" in the card data. The printer supports two possible encoding formats that can be applied - these are represented by "key A" and "key B" options.

Note: A thorough understanding of the required access card data encoding settings is required. • The numbering of sectors and blocks start with 0. Block 0 in sector 0 is read-only. Mifare Ultralight has sector 0 only. Mifare 1k and Mifare 4k use a number of sectors, with typically four blocks in each.

	Add - Adds a data configuration to a card data sector. Each sector uses a row in the table below. Delete - Deletes the currently selected card data sector.
Sector (Column)	Sets a portion of available access card data that applicable card readers use. Card data usually consists of several individual data "blocks". To edit, click the field and enter a value or use the arrows to step through numbers.
Block (Column)	Sets a portion of a "sector" that applicable card readers use. To edit, click the field and enter a value or use the arrows to step through numbers.
Use Key A (Column)	Determines which encoding key to apply. Click to toggle. ☑ = key "A" encoding; ☐ = key "B" encoding.
Key (Column)	Sets a hexadecimal number [0 to F] to apply as the actual key data. To edit, click the field and enter a value.
Data Type (Column)	Specifies the data or data format to apply to the block. There are various options, including user information etc [the content may vary depending on the Unison version and how user information has been defined]. To edit, click ▾ to display options. Click an option to select it: • Compiled Data – User data from Unison to be encoded, in compiled form. • Card Number - Card number data. • Static Field - • System Number - Card system number data. • Version Number - Card version number data. • Miscellaneous Number - Card miscellaneous number data. • Constant - Non-specific data with non-variable text value to add for all encoded cards. • New Keys - Keys to encode and read data for the sector. The data is specified in the A and B columns. In addition, the Access Bits value must be specified which determines which data column is used for writing/reading. • User ID - Personal or civic registration number data. • First Name - User first name data. • Last Name - User last name data. • PIN - User access personal identification number (PIN) data. • User Valid From - User validity start date. • User Valid To - User validity end date. • Personnel Category - Personnel or staff category data. • Other data types - User note 1, note 2 etc data.
Constant (Column)	Sets a hexadecimal number [0 to F] to apply as a constant value when Data Type = Constant. To edit, click the field and enter a value.
	Sets a hexadecimal number [0 to F] to apply as either read or write

A (Column)	data [as required] when Data Type = New Keys. The Access Bits value must be specified which determines which data column is used for writing/reading. To edit, click the field and enter a value.
B (Column)	Sets a hexadecimal number [0 to F] to apply as either read or write data [as required] when Data Type = New Keys. The Access Bits value must be specified which determines which data column is used for writing/reading. To edit, click the field and enter a value.
Access Bits (Column)	Sets a hexadecimal number [0 to F] to apply which determines which data column [A and B columns] is used for as either read or write data [as required] when Data Type = New Keys. To edit, click the field and enter a value.
Read Card Number	Determines if the printer should read permanent card number data from the card. Click to toggle. ☑ = option enabled.
Reverse Order	Determines if the printer should encode card number data in reverse order. This option should be enabled only if the card readers in use read card number data in reverse that is, start at the end of the data and read to the left]. Click to toggle. ☑ = option enabled.

Read Table - Determines how card number data is read from specific blocks, if required. That is, card number data is read in a specific way that is non-standard [requires Read Card Number option to be disabled].

Sector (Column)	Sets the portion of access card data to read. To edit, click the field and enter a value or use the arrows to step through numbers.
Block (Column)	Sets the portion of the selected "sector" to read. To edit, click the field and enter a value or use the arrows to step through numbers.
Use Key A (Column)	Determines which encoding key to apply. Click to toggle. ☑ = key A encoding; ☐ = key B encoding.
Key (Column)	Sets a hexadecimal number [0 to F] to apply as the actual key data. To edit, click the field and enter a value.
Data Type (Column)	Specifies the data format to apply. To edit, click ▾ to display options. Click an option to select it: • Compiled Data – Data in compiled form. • Card Number - Card number data.
Encoding	Sets the text encoding to apply to user data; for example, to change the user name to bytes. To edit, click ▾ to display options. Click an option to select it: • Supported encoding formats.
Fill Byte	Sets a substitute number to insert into any "empty" bytes in text data blocks, if required. Data blocks are usually 16 bytes in length. To edit, click the field and enter a value or use the arrows to step through numbers.
	Determines if any fill byte numbers (Fill Byte setting) are added to

Fill at End	the data either after or before the text data, if required. Click to toggle. ☑ = fill byte numbers after text data; ☐ = fill byte numbers before text data.
Hopper	For printers with two card feed mechanisms ["hopper"], the default mechanism can be specified, of required. To edit, click ▾ to display options. Click an option to select it. • 1 - Use hopper "1". • 2 - Use hopper "2".
Debug Protocol	Activates communications protocol error logging for device troubleshooting. For technician use only. Click to toggle. ☑ = option enabled.

Settings > Advanced Properties - Generic device node properties apply. Click here for help.

Events Tab - One or more "generic" events may apply. Normal event configuration procedures apply. Click here for help. Additional events, if any, are listed below.

Authentication Fail	Warning - authentication for encoding or reading cards failed. The key used is probably incorrect.
Encoding Fail	Information - encoding of card failed.
Encode Success	Information - encoding of card successful.
Internal Error	Warning - an internal program error has occurred in the device driver software [providing communications and device functionality]. Send a "restart" command to the device. Contact technical support if the problem persists.
Printer Error	Warning - printer problem detected. The event message contains more information.
Reading Fail	Information - card read failed.
Read Success	Information - card read successful.

Actions Tab - Lists any event response actions that have been created for the node. Normal node action configuration procedures apply. Click here for help.

Dependencies Tab - Lists any dependencies on the node. Normal node dependency procedures apply. Click here for help.

Scheduled Commands Tab - Lists any scheduled commands that have been created for the node that are yet to be processed.Click here for help.

Notes Tab - Normal note configuration procedures apply.Click here for help.

Commands

Command	Description

One or more "generic" commands may apply. Click here for help. Additional commands, if any, are listed below.

Eject	Ejects a card from the printer.
Encode Block	Encodes a single block. Any data can be encoded to the block.

See Also: Card Profiles | Device Templates | Configuring Third-Party and Generic Devices | Users and Access Cards

---

You are here: Configuring Third-Party and Generic Devices > Miscellaneous Devices > Deister Key Management System

Deister proxSafe Key Management System

Deister proxSafe is a key management system, assisting with managing, controlling and monitoring the possession and use of keys by credentialed individuals. Typically, these individuals are granted access to certain keys at certain times/days, and/or for pre-set lengths of time. The individual presents a credential to the key management system (that is, an access card or similar) and is then granted access to keys (attached to keytags/fobs) which have been pre-assigned to them by the administrator. Alarms and reports are generated according to set conditions (for example, keys kept out too long).

The Unison integration "sits on top" of the proxSafe Commander system and maintains synchronization with it. Integrated functionality allows the Unison system to receive alarms/events from proxSafe and for operators to be able to view status for proxSafe nodes [cabinets, fobs etc] and send commands to them, and to manage users in the proxSafe system. The following node types are supported:

- Deister proxSafe Server - Provides system functionality and connection settings for the Deister proxSafe system.
- Terminal -Represents a device that controls one or more cabinets and provides a user interface to support both system control, and user identification.
- Cabinet - Represent Deister key cabinet hardware.
- Key Tag - Represent "assets" in the Deister system that are kept secure in cabinets by means of a fob device. For example, keys, access devices etc. The fob, once placed in the cabinet, is locked in position until a user authorized to remove it does so.
- Key Tag Item- Represent individual "assets" that are associated with a fob.
- Key Tag group - represent one or more Deister access schedules that are associated with fobs and are collectively grouped into a single entity for assigning to user access permissions.

Licensing

Before integration the Unison system must be licensed for access control and an appropriate number of key/assets.

Supported Functions

The Deister - Unison system integration provides the following functions:

- Import and Generate node information and hierarchy
- Users and Card holder management
- Connection status with proxSafe Server
- Events and Alarms Management (Tracing)
- Import valid User from Deister proxSafe to Unison

Card Information

- proxSafe allows one card per user
- Cards with 32-bit or lesser card length and 64-bit Mifare cards are supported
- From Unsion, the first valid card will be considered and added to the proxSafe Server
- A PIN can be associated with a card
- Blocking the card in Unison, will mark the user as invalid in proxSafe

Device - Management, Configuration and Commands
Terminal - Management Configuration and Commands

Cabinet - Management, Configuration and Commands
Key Tag - Management, Configuration and Commands
Key Tag Item- Management, Configuration and Commands
Key Tag Group - Management, Configuration and Commands

See Also: Configuring the System | Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Miscellaneous Devices > Traka Key Management System

Traka Key Management System

Traka is a key/asset management system, connected over TCP/IP. Traka key cabinets are used for security managed assets, such as vehicles, access to doors etc. In effect, access to assets for users is handled as per normal access control nodes in that users are assigned assets [which are known as "fobs"]. Users use their access card etc to access cabinets - only fobs that they are assigned can be taken, with the system generating transactions and events for fob removal, return, late return, missing etc. The Unison integration basically "sits on top" of the Traka system and maintains synchronization with it. Integrated functionality allows the Unison system to receive alarms/events from Traka and for operators to be able to view status for Traka nodes [cabinets, fobs etc] and send commands to them, and to manage users in the Traka system. The following node types are supported:

- Traka device - Provides system functionality and connection settings for the Traka

system.
- Cabinet - Represent Traka key cabinet hardware.
- Fob - Represent "assets" in the Traka system that are kept secure in cabinets by means of a fob device. For example, keys, access devices etc. The fob, once placed in the cabinet, is locked in position until a user authorized to remove it does so.
- Key - Represent individual "assets" that are associated with a fob.
- Security group - represent one or more Traka access schedules that are associated with fobs and are collectively grouped into a single entity for assigning to user access permissions.
- Unassigned fob - represent a fob that exists in the Traka database, however, is not assigned to a cabinet.
- Unassigned key - represent a key that exists in the Traka database, however, is not assigned to a fob.

Integration Functions and Limitations
Integration Requirements

The Unison system supports importing existing Traka hardware and user configurations. When importing, nodes in the Traka system are replicated in the Unison system - this makes device configuration faster and less prone to error. To import a configuration:

Note: It is recommended to create all users of the Traka system from the Unison system.

1. Create a "Traka" device in the Unison system. This is the "root" node for the Traka system and provides a connection to the Traka database.
2. As a precaution, backup the existing Traka database.
3. Use the "synchronize hardware configuration" command on the "Traka" device node to create device and access nodes in Unison.

Device - Management, Configuration and Commands
Cabinet - Management, Configuration and Commands
Fob - Management, Configuration and Commands
Key - Management, Configuration and Commands
Security Group - Management, Configuration and Commands

See Also: Configuring the System | Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Video Systems

Video Systems

Bosch VMS

Bosch VMS is a software based video management system ["VMS"] that provides video surveillance functions. The Bosch system supports several security features, such as camera on alarm, camera manipulation, motion detection via camera etc. The Unison system is able to replicate the configuration of the Bosch system by "reading" the existing configuration from it ["generate" command on Bosch VMS "device" node]. The system integration enables alarms from the Bosch system to be transferred to the Unison system and also for commands from Unison [for example, layout activation] to be processed by Bosch VMS. Alarms from Bosch that are acknowledged within the Unison system become acknowledged in the Bosch system also. The following Bosch VMS products are supported:

Note: The Bosch VMS supersedes the "Vidos" system.

- VMS 2.0 to 4.5.5. These version require a "patch" to be installed that will make the Unison device driver compatible.

Compatibility

- VMS 5.5.5.

Note: Any changes made in the Bosch system require running the "generate" command in the Unison system again in order to synchronize it.

The following node types are supported:

- Bosch VMS device - Provides system functionality for the Bosch system.
- Alias client - Represents a connection between a Unison client application and a Bosch VMS client application running on a specific computer. This enables computers running Unison client applications and computers running Bosch VMS

client applications to be "paired" so that if a Unison operator sends a command to the "alias", the command is performed on the associated Bosch VMS client; for example, to display video.

- Alias monitor - Represents a connection to a Bosch VMS video display monitor. This enables computers running Unison client applications and Bosch VMS video display monitors to be "paired" so that the required computers are near one another for easy operator access. For example, if the Unison operator requires viewing video on the Bosch VMS video display monitor, the required monitor is nearby.
- Camera [dome] - Represents camera hardware that supports positional changes etc managed by the Bosch system. Dome camera configuration in the Bosch system is replicated when nodes are generated.
- Camera [fixed position] - Represents camera hardware managed by the Bosch system. Camera configuration in the Bosch system is replicated when nodes are generated.
- Client - Represents a Bosch VMS client application running on a specific computer. This enables Bosch VMS clients to be "paired" with Unison clients as "alias clients".
- Decoder - Represent Bosch hardware that receives video data from cameras, decodes it to analog format and sends it to an associated monitor.
- Input [physical] - Represents physical alarm inputs in the Bosch system; for example, panic buttons. Input configuration in the Bosch system is replicated when nodes are generated.
- Input [virtual] - Represents virtual alarm inputs in the Bosch system; for example, an event configured to be treated as an alarm in the same way as a physical input. Input configuration in the Bosch system is replicated when nodes are generated. Virtual inputs can also be manually activated/deactivated.
- Monitor - Represents video data decoding and video display hardware in the Bosch system. A single monitor device can have multiple display panes/frames within, for simultaneously displaying video from multiple cameras. Monitor configuration in the Bosch system is replicated when nodes are generated - the monitor node is always defined with a "logical identification number" of "1".
- Monitor [analog] - Represents video display frames within a monitor device and have "logical identification numbers" other than "1". Analog monitor nodes must be manually replicated in the Unison system, with the "logical identification numbers" as defined in the Bosch system.
- Output - Represents external devices that are connected to camera hardware as an additional output; for example, lights. This is applicable to camera hardware that supports outputs.

Monitor [Analog] - Management, Configuration and Commands
Output - Management, Configuration and Commands
Programming Example
Adding a camera to a BVMS panel

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Video Systems > Indigovision

Indigovision

Indigovision is a software based video management system ["VMS"] that provides video surveillance functions. The Indigovision system supports several security features, such as video fault etc. The Unison system is able to replicate part of the configuration of the Indigovision system by "reading" the existing configuration from it ["generate" command on Indigovision "device" node]. The system integration enables alarms from the Indigovision system to be transferred to the Unison system and also for commands from Unison [for example, viewing live video in the Unison system, arming/disarming zones etc] to be processed by Indigovision. Alarms from Indigovision that are acknowledged within the Unison system become acknowledged in the Indigovision system also. The following Indigovision products are supported:

- Indigovision Binding Kit 2.8.1.
- Indigovision Control Center 12.0.

Note: Any changes made in the Indigovision system require running the "generate" command in the Unison system again in order to synchronize it.

The following node types are supported:

- Indigovision device - Provides system functionality for the Indigovision video system.
- Camera - Represents camera hardware managed by the Indigovision system. Camera hardware may or may not support specific features, such as "PTZ" [pan/tilt/zoom] etc - manual camera configuration is required as the Indigovision system does not support providing camera data to the Unison system.
- Detector - Represents "virtual" alarm inputs defined in the Indigovision system for individual cameras. For example, motion detection, network fault etc. Th Unison system receives alarm and other applicable events from detectors. Detector data is retrieved from the Indigovision system - these nodes cannot be created manually. Indigovision zone nodes also display in the Inputs and Outputs panel, which provides operators monitoring detectors/inputs/outputs managed by Indigovision the same interface as for "normal" inputs and outputs defined in the Unions system.
- Zone - Represents groups of detectors that can be controlled as a single entity. For

example, disarming a zone disarms all member detectors associated with the zone. Zone data is retrieved from the Indigovision system - these nodes cannot be created manually. Indigovision zone nodes also display in the Areas panel, which provides operators monitoring zones/areas managed by Indigovision the same interface as for "normal" areas defined in the Unions system.

- Integration Requirements
- Device - Management, Configuration and Commands
- Camera - Management, Configuration and Commands
- Detector - Management, Configuration and Commands
- Zone - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices | Using Integrated Video

---

Network Video

The network video device driver supports two kinds of protocols and other operations required to communicate with the following video devices:

- Axis brand-specific VAPIX.
- ONVIF (Open Network Video Interface Forum).

Note: Audio streaming using ONVIF is currently not supported by the Unison system. For correct video playback in Unison, audio must be disabled in the host ONVIF system "RSTP" settings.

Both protocols are based on TCP/IP and can handle pan/tilt/zoom (PTZ) functions, however, there is no support for events via VAPIX. ONVIF is an open interface that enables you to combine several different types of ONVIF compatible cameras from different manufacturers.

- Integration Requirements
- Device - Management, Configuration and Commands
- Programming Example

See Also: Axis Camera | Configuring Third-Party and Generic Devices | Device Templates | Jupiter Video Wall | ONVIF Camera

Axis Camera

Jupiter Video Wall

ONVIF Camera

You are here: Configuring Third-Party and Generic Devices > Video Systems > Network Video > Axis Camera

Axis Camera

Axis is a proprietary camera manufacturer that can be used an alternative to ONVIF cameras for the Unison Network Video device. Axis cameras do not provide events to the Unison system.

Note: It is possible to have a mix of cameras using different VAPIX versions in the same system. • VAPIX 2 cameras allow a maximum of 100 simultaneous connections. For example, if 101 Unison clients are all attempting to display video for the same camera, the 101st client will not be able to connect to the camera until another client drops its connection.

- Integration Requirements
- Camera - Management, Configuration and Commands

See Also: Configuring Third-Party and Generic Devices | Device Templates | Network Video

---

You are here: Configuring Third-Party and Generic Devices > Video Systems > Network Video > Jupiter Video Wall

Jupiter Video Wall

Jupiter video walls can be operated from within Unison, and are part of the Network Video device. The Jupiter video wall system contains display wall processors for command and control applications. It is designed to provide a real-time, collaborative work environment for monitoring, response, dispatch, coordination, process management, recording and escalation - from incident detection to resolution.

Once a wall node has been configured, Unison attempts to connect to it. The Events tab is activated also. Unison attempts to connect to every single wall node created in the system when it is launched. So it is not necessary to repeat this process in order to connect to a wall every time Unison is started. The following node types are supported:

- Wall device - Provides system functionality for the Jupiter video wall system.

- Layout - Represents a "matrix" consisting of one or more "windows". When a layout is displayed in the Jupiter system, its associated windows are displayed. When a layout is created, it is automatically set as the active layout. One wall can display one layout.
- Window - Represents a video source and display size definitions to apply when its associated "layout" is displayed in the Jupiter system.

Integration Requirements
Device - Management, Configuration and Commands
Layout - Management, Configuration and Commands
Window - Management, Configuration and Commands

See Also: Configuring Third-Party and Generic Devices | Device Templates | Network Video | ONVIF Camera

---

You are here: Configuring Third-Party and Generic Devices > Video Systems > Network Video > ONVIF Camera

ONVIF Camera

ONVIF compliant cameras are used to provide video to the Unison system, support a range of standard events, and are also compatible with some functions of the Jupiter video wall system. ONVIF is a standard that several camera manufacturers comply with, making the actual camera make/model irrelevant. When ONVIF cameras are being used, a "ONVIF service" is installed on the network and used to manage connections between cameras and third-party systems, such as Unison.

Note: Audio streaming using ONVIF is currently not supported by the Unison system. For correct video playback in Unison, audio must be disabled in the host ONVIF service "RSTP" settings. • The Unison system supports configuring ONVIF camera nodes either by way of the Camera Configuration Wizard dialog box.

Integration Requirements
Camera - Management, Configuration and Commands

See Also: Configuring Third-Party and Generic Devices | Device Templates | Jupiter Video Wall | Network Video

---

You are here: Configuring Third-Party and Generic Devices > Video Systems > Milestone

Milestone

Milestone is a software based video management system ["VMS"] that provides video surveillance functions. The Unison system is able to replicate the configuration of the Milestone system by "reading" the existing configuration from it ["generate" command on Milestone "device" node]. The system integration enables alarms from the Unison system to be linked to one or more cameras connected to the Milestone VMS for display on Milestone client applications, and also for commands from Unison [for example, viewing live video in the Unison system] to be processed by Milestone. Video from the Milestone system can also be viewed using the Pacom Integrated Video application. The following Milestone products are supported:

- XProtect Corporate 5.0c/2014 7.0b.
- XProtect Enterprise 8.0c/2014 8.0b.
- XProtect Expert 2014 7.0b.

Note: Any changes made in the Milestone system require running the "generate" command in the Unison system again in order to synchronize it.

The following node types are supported:

- Milestone device - Provides system functionality for the Milestone video system.
- Alias monitor - Represents a connection between a Unison client application and a Milestone client application running on a specific computer. This enables computers running Unison client applications and computers running Milestone client applications to be "paired" so that if a Unison operator sends a command to the "alias", the command is performed on the associated Milestone client; for example, to display video.
- Alias user-defined event - Represents a method of using the Unison system to activate one or more user-defined events on a Milestone client running on a specific computer. For example, in the event of an alarm for a node, activate the alias user-defined event, which in turn activates a user-defined event in the Milestone client. It can also be used to send video from a specific camera or camera group to the user-defined event ["send video" command] - in effect, substituting the cameras defined in the Milestone user-defined event.
- Camera - Represents camera hardware managed by the Milestone system. Camera hardware may or may not support specific features, such as "PTZ" [pan/tilt/zoom], additional inputs etc - camera configuration in the Milestone system is replicated when camera nodes are generated.
- Camera group - Represents the visual layout [default cameras, multi-camera views etc] for Milestone client application displays, such as "Smart Wall". Camera groups can be applied automatically as an action in response to an alarm so that video from each camera is displayed to Milestone operators. The cameras specified for camera groups are configured in the Milestone system. "Virtual" camera groups can be created in the Unison system that specify cameras externally to those configured in the Milestone system by way of "alias user-defined events".
- Input - Represents external devices that are connected to camera hardware as an

additional input; for example, a panic button. This is applicable to camera hardware that supports inputs.
- Monitor - Represents "matrix" displays as defined in the Milestone system. A matrix is pre-defined view [video displayed from one or more cameras] shown to operators of Milestone client applications.
- Output - Represents external devices that are connected to camera hardware as an additional output; for example, lights. This is applicable to camera hardware that supports outputs.
- User-defined event - Represents rule-based "events" as defined in the Milestone system. This is a similar concept to expressions. For example, the Milestone system is set up to create an event based on some other circumstance [for example, a camera detecting motion] that is used to automatically send video from pre-defined cameras to Milestone client applications.

Integration Requirements
Device - Management, Configuration and Commands
Alias Monitor - Management, Configuration and Commands
Alias User-Defined Event - Management, Configuration and Commands
Camera - Management, Configuration and Commands
Camera Group - Management, Configuration and Commands
Input - Management, Configuration and Commands
Monitor - Management, Configuration and Commands
Output - Management, Configuration and Commands
User-Defined Event - Management, Configuration and Commands

See Also: Configuring Third-Party and Generic Devices | Device Templates | Using Integrated Video

---

You are here: Configuring Third-Party and Generic Devices > Video Systems > Mirasys

Mirasys

Mirasys is a software based video management system ["VMS"] that provides video surveillance functions. The Mirasys system supports several security features, such as camera on alarm, camera manipulation, motion detection via camera etc. The Unison system is able to replicate the configuration of the Mirasys system by "reading" the existing configuration from it ["generate" command on Mirasys "gateway" node]. The system integration enables alarms from the Mirasys system to be transferred to the Unison system and also for commands from Unison [for example, layout activation] to be processed by Mirasys. Alarms from Mirasys that are acknowledged within the Unison system become acknowledged in the Mirasys system also. The following Mirasys products are supported:

Note: The Mirasys system integration is for alarm transfer between Mirasys and the

Unison systems only. It is not for streaming video between the two systems - viewing of video is performed using the Mirasys Spotter application.

- System Manager Enterprise 7.2.1.
- Workstation Enterprise 7.2.1.
- Spotter Enterprise 7.2.1
- DVMS Gateway Service 7.2.1.130.
- SDK 5.10.5.0.

Note: Supported DVMS Gateway service, Spotter clients and SDK must be installed on site prior to setting up the Unison Mirasys device. • The Mirasys system must be configured for a Unison connection before setting up the device in Unison. That is, to have the necessary connection and authentication details available. • Any changes made in the Mirasys system, such as adding or removing cameras, are updated in the Unison Explorer hardware display when the display is refreshed [to refresh, close and re-open the display or browse away and then back again]. Changes made to names or profile IDs in the Mirasys system require running the "generate" command in the Unison system again in order to synchronize it.

The following node types are supported:

- Mirasys device - Provides system functionality for the Mirasys video system.
- Camera - Represents camera hardware managed by the Mirasys system. Camera hardware may or may not support specific features, such as "PTZ" [pan/tilt/zoom], additional inputs etc - camera configuration in the Mirasys system is replicated when camera nodes are generated. PTZ [pan/tilt/zoom] settings for individual cameras, if supported by the camera and configured in the Mirasys system, are stored with camera nodes and can be applied as commands. Presets can be used to position and zoom cameras automatically as an action in response to an alarm.
- Digital input - Represents external devices that are connected to camera hardware as an additional input; for example, a panic button. This is applicable to camera hardware that supports inputs.
- Digital output - Represents external devices that are connected to camera hardware as an additional output; for example, a light. This is applicable to camera hardware that supports outputs.
- Gateway - Represents the Mirasys system server and authentication details for accessing it. All Mirasys internal operations are performed by the Gateway service.
- Layout - Represents the visual layout [default cameras, multi-camera views etc] for Mirasys operators using the Spotter application. Layouts can be applied on Spotter applications automatically as an action in response to an alarm.
- Profile - Represents access settings to a Mirasys Gateway service [the Mirasys application]. After generating nodes in the Unison system, the node [folder] representing this is named as it is in the Mirasys system.
- Spotter - Represents Mirasys operator applications. This is generally a viewing platform for operators [view video streamed from attached cameras] and for monitoring and response.

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Video Systems > Pelco Video Matrix

Pelco Video Matrix

Pelco Video Matrix is a self contained analog video controller that features multiple camera inputs and monitor outputs. The device driver is compatible with CM6800 and CM9700 switchers and "Genex multiplexer" hardware and enables the Unison system to be used for controlling the Pelco equipment. For example, switching cameras, adjusting camera zoom etc. Viewing video from the Pelco hardware is by way of monitors connected to it. It is not possible to view video from the Pelco system within Unison. In addition to video (monitor/camera), internal/external inputs and outputs are also supported. The following node types are supported:

- Pelco device - Represents Pelco CM6800/9700 hardware and provides system functionality for the Pelco video system.
- Camera - Represents camera hardware managed by the Pelco system. Camera hardware may or may not support specific features, such as "PTZ" [pan/tilt/zoom], additional inputs etc.
- External input - Represents third-party inputs that, when active, are [generally] used for activating video display from one or more cameras.
- Genex multiplexer - Represents Pelco Genex multiplexer hardware which is used for displaying video from multiple cameras simultaneously and provides additional features for managing and controlling displays.
- Internal input - Represents inputs on the Pelco device that, when active, are [generally] used for activating video display from one or more cameras. Internal inputs are direct connections to the device from input sources; for example, motion detectors.
- Monitor - Represents physical monitor (video display) devices that are used for displaying video.
- Monitor alias - Represents a connection to a Pelco client application running on one or more specific computers, that is used specifically by the Unison system. One or

more monitors is also specified that determines how video is displayed and for which cameras. This enables Unison to be used as a method for commanding video to be sent to Pelco clients. That is, the monitor connection is not necessarily part of the Pelco configuration.

- Output - Represents external devices that are connected to camera hardware as an additional output; for example, lights. This is applicable to camera hardware that supports outputs.

Integration Requirements
Device - Management, Configuration and Commands
Camera - Management, Configuration and Commands
External Input - Management, Configuration and Commands
Genex Multiplexer - Management, Configuration and Commands
Internal Input - Management, Configuration and Commands
Monitor - Management, Configuration and Commands
Monitor Alias - Management, Configuration and Commands
Output - Management, Configuration and Commands

See Also: Device Templates | Configuring Third-Party and Generic Devices

---

You are here: Configuring Third-Party and Generic Devices > Visitor Management Systems

Visitor Management Systems

Adria Scan Virtual Border

You are here: Configuring Third-Party and Generic Devices > Visitor Management Systems > Adria Scan Virtual Border

Adria Scan Virtual Border

Adria Scan Virtual Border is a visitor management system that Unison can be integrated into. That is, the Unison system is an external device and the driver for it is in the Adria Scan system. Communications between the two systems is accomplished through the Unison "access service" device driver, which supports standard HTTP "web" communications.

The result of this integration is that the details for temporary users in the Adria Scan system [generally classified as "visitors" or "contractors"], such as name, photograph, access level and validity dates etc, are provided by the Adria Scan system and

recorded in the Unison system database for the duration of the user's visit. Once the user's visit is over, by way of end validity date or handing back their access card, and is processed in the Adria Scan system, the access card/PIN data is removed from the user record in the Unison database. The access card data/PIN previously allocated then becomes available to assign to another user. Unison can be used to trace archived access transactions for visitors processed using Adria Scan by way of access card numbers.

When setting up Unison for an Adria Scan Virtual Border integration, the following is required:

Note: The specific details for the required custom user data fields are defined by Adria Scan. Th two systems must use the same data type and other values for the custom fields so that the required data is read correctly.

- In the Unison "system" device, create a custom user data field to categorize the user as an "employee" or not an employee, which means either a "contractor" or "visitor".
- In the Unison "system" device, create a custom user data field for the user image file data.
- In the Unison "access service" device settings, "user data field" list, add the custom data fields created above.
- The Adria Scan system must be set up to use the Unison access service on the applicable computer and port as configured in the Unison system.

See Also: Access Service | Configuring the System

You are here: Configuring Third-Party and Generic Devices > Alarm Receiver

Alarm Receiver

The Alarm Receiver device is designed to receive alarm events from any Alarm Receiving Station (Receiver) that supports sending Contact ID or SIA events using a Sur-Gard Protocol. Unison then links the event to an alarm so operators can identify, respond and manage the situation appropriately.

Alarms are received from a receiver, and Unison then matches the Account ID to a Site node, the Zone/Device ID to a Device node, and an Event code to an Event node. If an alarm is associated with that particular event, then an operator will be required to manage the alarm (Acknowledge, Restore, and Close).

There are five types of Nodes supported in the Alarm Receive Driver:

- Receiver – Alarm Sending Stations that will relay alarm messages to Unison. The currently supported Sur-Gard protocols are S for SIA, and 5 and Q for Contact ID

- Site – Nodes that represent a specific site/location. Each Site node has a specific Account ID.
- Device – Nodes that represent end-points. They can be physical devices like elevators or doors, zones, users, or relays. Device nodes are child nodes of Site nodes.
- Event – Child nodes that represent an individual SIA or CID event code. An example could be a “BA” event (usually BA = Burglary Alarm). Event nodes can be configured to toggle on then off briefly, or be stateful (on until reset). Event nodes are child nodes of Device nodes.
- Device Template – These nodes are the same as Device nodes and have Template Events as child nodes. The Device Template is used as a way for administrators to pre-configure devices with different event nodes. The template can then be imported as a device, to minimize the effort involved during setup.

Alarm Sender

The Alarm Sender driver allows Unison to send alarm events to remote monitoring centres. Unison supports sending SIA and Contact ID alarm events using TCP/IP or UDP/IP. Additionally, Unison supports relaying SIA alarms using the IRIS Touch dialler.

You are here: Appendices

Appendices

This section includes the following topics that may be useful to administators and technicians:

- Unison system architecture.
- Unison software installation.
- Pacom Integrated Video application third-party "plug-in" installation instructions.
- Pacom Controller hardware configuration using its "web server".
- Pacom hardware information and installation instructions.

Web Server Controller Configuration Guide

Regular Expressions (Regex)

General Data Protection Regulation (GDPR) Support Advice

GDPR Automatic Deletion

You are here: Appendices > Web Server Controller Configuration Guide

Web Server Controller Configuration Guide

Pacom Controller firmware version 1.10 onwards for 8001/8002 types and version 5.10 onwards for 105x types have an in-built "web server" to enable initial commissioning to a head system [for example, Pacom Unison] and some testing capabilities without the need for intermediary software. "Commissioning" means to apply necessary firmware, set Controller identification (ID) number, IP address of the head system for connection etc.

Note: Controllers must be set to factory defaults in order to allow initial "web server" connection. • Controllers must have the correct firmware in order to have "web server" capability. • 8003 type Controllers have a different web server that can be used for initial configuration - refer to the web server help system for information.

Connect a computer to the Controller using an Ethernet connection. If connecting directly, use a cross-over Ethernet cable. If connecting with a hub between computer and Controller, use normal Ethernet cables.

Open a web browser [Mozilla Firefox, Microsoft Internet Explorer etc] on the computer and enter "10.1.1.1". The log on screen displays.

In the Logon ID field, enter "1".

In the Password field, enter "Pacom".

The "home" screen displays. Basic Controller information displays including serial number, firmware and memory details. All web server feature can be accessed from this screen.

To exit the web server configuration, click Log Off at any time.

Firmware Management

Note: For firmware upgrades, the required firmware must be available through a TFTP server. • If required, click to open the Pacom website, where you can download the latest firmware.

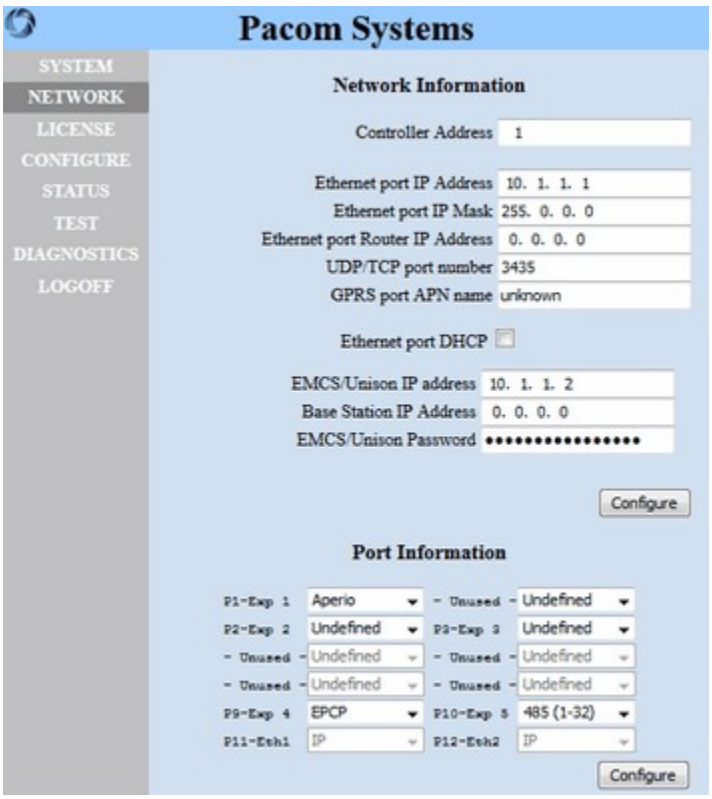
In the home screen, click System. Firmware management controls display. Click Update Firmware.

Control	Description
TFTP Server IP Address	Sets the required TFTP server network IP address. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, double-click a segment and enter a value.
Run in Chip 1	Command the Controller to restart using the firmware stored in microprocessor ("chip") 1.

Run in Chip 2	Command the Controller to restart using the firmware stored in microprocessor ("chip") 2.
Start Download	Download firmware from the TFTP server [TFTP Server IP Address setting] to the Controller. The firmware will be stored in whichever microprocessor ("chip") is currently not being used - once new firmware is loaded, restart the Controller using the "chip" with the new firmware. When downloading, download status displays with controls for aborting (exit) the download.

Network Configuration

In the home screen, click Network. Network/IT management controls display.



Control	Description
Controller Address	Sets the identification (ID) number of the Controller to apply when connecting to the head system. Each Controller in a system requires a unique ID. To edit, double-click the field and enter a value.
Ethernet Port IP Address	Sets the IP address for the Controller Ethernet port [some Controller models have several Ethernet ports that can be configured]. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, double-click a segment and enter a value. Note: The IP address must conform to network requirements in

	order for the Controller to be contactable.
Ethernet Port IP Mask	Sets the subnet mask to apply to the Controller IP address. The subnet mask determines which of the IP address segments are variable. For example, a subnet mask of "255.255.0.0" means that the first two segments are fixed and the second two are variable [between "0" and "255"]. To edit, double-click a segment and enter a value. Note: The subnet mask must conform to network requirements in order for the Controller to be contactable.
Ethernet Port Router IP Address	Sets the IP address of a gateway router, if applicable. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, double-click a segment and enter a value.
GPRS Port APN Name	Sets the access point name ["APN"] that is the gateway between the Controller GPRS [wireless data] card and another computer network, if applicable. To edit, double-click the field and enter a value. Note: The APN entry must conform to wireless network requirements in order for connection to be possible.
Ethernet Port DHCP	Determines if the Controller IP address, subnet mask and router IP address are assigned by a network DHCP server. When enabled, the Ethernet Port IP Address, Ethernet Port IP Mask and Ethernet Port Router IP Address settings are disabled. If not yet allocated, "0.0.0.0" is displayed. Note: Connections to the head system may not be available until network information is assigned by the DHCP server.
EMCS/Unison IP Address	Sets the default IP address for the Controller to connect to - for Unison systems, the device driver server; for Site Manager/"EMCS" systems, the Protocol Service server, if applicable. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, double-click a segment and enter a value.
Base Station IP Address	Sets the Pacom Base Station hardware IP address for the Controller to connect to, if applicable. When entering an "IPv4" address [four segments with up to three decimals each], use period (".") characters to identify when one address segment ends and the next one starts; for example, "10.1.60.131". To edit, double-click a segment and enter a value.
EMCS/Unison Password	Sets the password used to authenticate the Controller to a Unison or Site Manager/"EMCS" system, if applicable. To edit, double-click the field and enter a value.

Configure Downloads current settings to the Controller and reboots the Ethernet port so that the settings take effect. After reboot, it will be necessary to log on tot he Controller again.

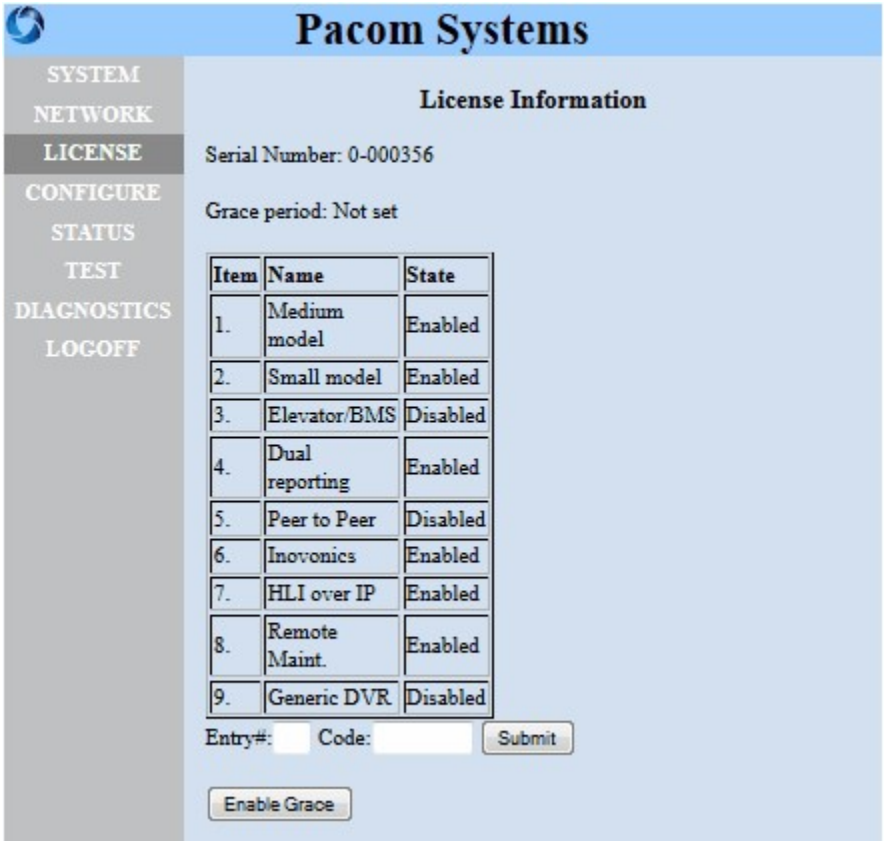
Port Information - Settings for selecting the protocol to apply to available ports on the Controller and applicable expansion cards. Any ports that are not used are marked as "unused".

Port Sets the communications protocol to apply to the selected port. To edit, click for options. Click an option to select it:

- 485 (1-32) - Standard RS485 for addresses 1 to 32.
- 485 (33-64) - Standard RS485 for addresses 33 to 64.
- 485 (65-96) - Standard RS485 for addresses 65 to 96.
- Aperio - For compatible Assa Aperio access control devices.
- Dialup - For compatible PSTN modem devices.
- Elevator HLI - For compatible high-level interface elevator systems/devices.
- EPCP - Proprietary "enhanced" Pacom protocol for compatible systems, such as Pacom GMS.
- Generic DVR - For compatible digital video recorder/network video recorder systems/devices.
- GP Driver - General purpose IP [Ethernet] protocol for compatible devices.
- Inovonics - For compatible Inovonics devices.
- IP - Standard Ethernet protocol for compatible systems/devices.
- Likon - For compatible Likon video systems/devices.
- Modbus - For compatible Modbus systems/devices.
- Pager - For compatible paging systems/devices.
- Printer - For compatible print devices.
- Timecon - For compatible Timecon systems/devices.
- Undefined - No protocol applied - port not used.
- Unknown - Port already configured, however, not to a recognized protocol [in this list].
- Wyreless - For compatible IR Schlage Wyreless systems/devices.

License Configuration

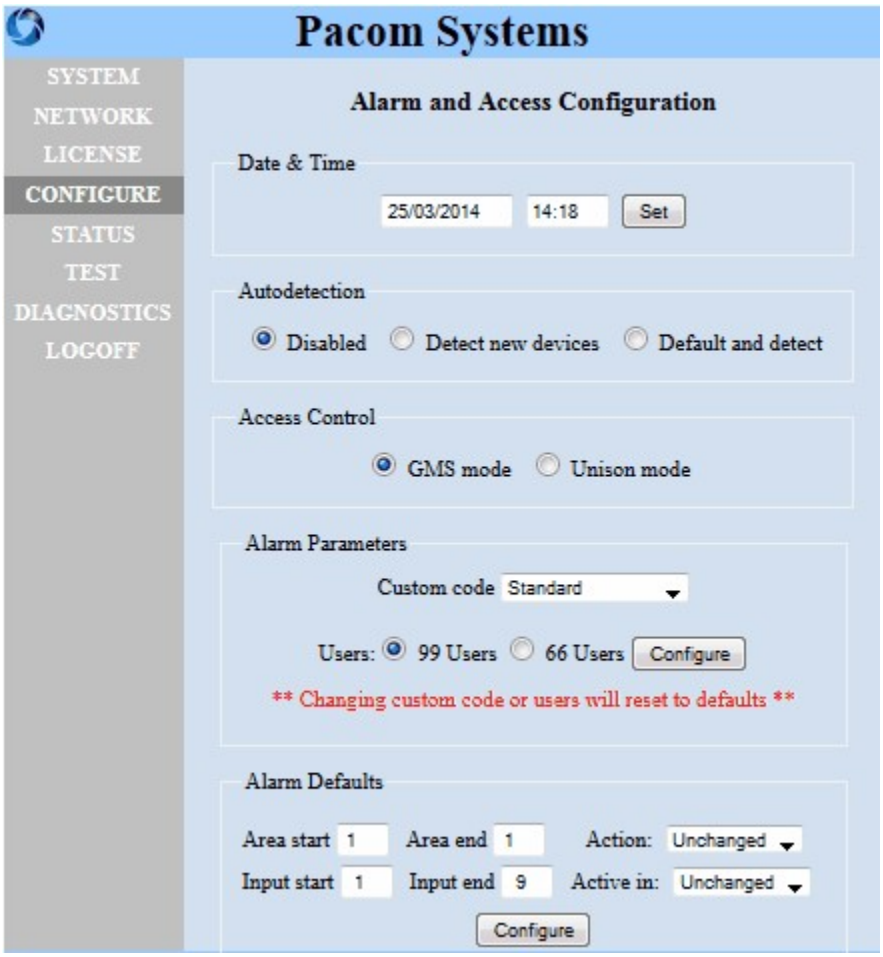
In the home screen, click License. Licensed feature management controls display.



Control	Description
Serial Number	Shows the serial number of the Controller. The serial number is used for tracking licensed features.
Grace Period	Shows if the grace period is in use or not. Pacom offers a 14 day "grace" period, during which unlicensed features will be functional. Once the grace period expires, the feature(s) are disabled until properly licensed. When in use, the remaining days of the grace period are displayed.
Features Table	Shows the current license status for available features [that must be licensed to use]. The table may vary depending on the Controller type. • Item - Numerical identifier for the adjacent feature. • Name - Name of feature/feature set. • State - Shows whether or not the Controller is currently licensed to use the adjacent feature.
Entry#	Sets the feature "item" number to license. For example, enter "6" to license Inovonics features. To edit, click the field and enter a value.
Code	Sets the eight-digit activation code for the feature license. To license a feature, a valid activation code must be received from Pacom. To edit, click the field and enter a value.
Submit	Send the activation code and associated feature entry to the Controller for license update.
Enable Grace	Activates the 14 day grace period.

Alarm System and Access Control Configuration

In the home screen, click Configure. Alarm system and access control management controls display.



Control	Description
Date and Time	
Date Setting	Sets the date to apply in the Controller. To edit, double-click a segment [year, month etc] and enter a value.
Time Setting	Sets the time [in 24-hour format] to apply in the Controller. To edit, double-click a segment [hour, minute] and enter a value.
Set	Apply the current date and time settings to the Controller.

Auto-Detection - Pacom Controllers [from firmware 5.00 (for 1057/1058)/1.02 (for 8001/8002)] are capable of auto-detecting RS485 connected devices. The basic device configuration is uploaded to the head system when the Controller detects devices.

Disabled	Prevents the Controller from detecting any connected devices. Click to apply. ◉ = Option applied.
Detect New Devices	Sets the Controller to reboot the RS485 device line and check expansion slots and detect and upload only "new" devices. That is, currently known devices are ignored, and newly detected devices are uploaded. Click to apply. ◉ = Option applied.
	Sets the Controller to reboot the RS485 device line and check expansion

Default and Detect	slots and detect and upload all devices. That is, currently known devices and newly detected devices are uploaded. Click to apply. = Option applied.

Access Control - Sets the Controller internal access control database [users, access card data, access schedules etc] to be compatible with either Pacom GMS or Unison security management platforms.

GMS Mode	Sets the Controller to manage access control data to be compatible with the GMS security management platform. Click to apply. = Option applied.
Unison Mode	Sets the Controller to manage access control data to be compatible with the Unison security management platform. Click to apply. = Option applied.

Alarm Parameters

Note: Changing any setting in this section will reboot the Controller and reset other Controller settings to default values.

Custom Code

Sets a predefined Controller configuration (apart from the Standard option). These configurations are designed to aid compliance with a range of operational standards for different regions or applications of the system. Many parameters set by the predefined Controller configurations remain editable, therefore, it is advisable to note which settings are affected. To edit, click for options. Click an option to select it:

Note: The following settings are required for compliance with the associated standard. For compliant installations, apply the required predefined Controller configuration (where applicable) and check that all settings are correct to ensure the installation is compliant. • Refer to Pacom management software help for details [not applicable to Pacom Unison].

- Bank Config.
- CP-01.
- EN 50131 Grade 2.
- EN 50131 Grade 3.
- Standard - No predefined configuration.
- UK Banking - BS8243.

Users

Set the total allowable number of alarm users [either 66 or 99, which also controls the available maximum alarm system log on PIN length between a maximum of eight or four digits, respectively] for Controllers. To edit, click an option to apply it. = Option applied.

- 99 Users - Allows up to 99 alarm user identities and a maximum alarm user PIN length of four digits.
- 66 Users - Allows up to 66 alarm user identities and a maximum alarm user PIN length of eight digits.

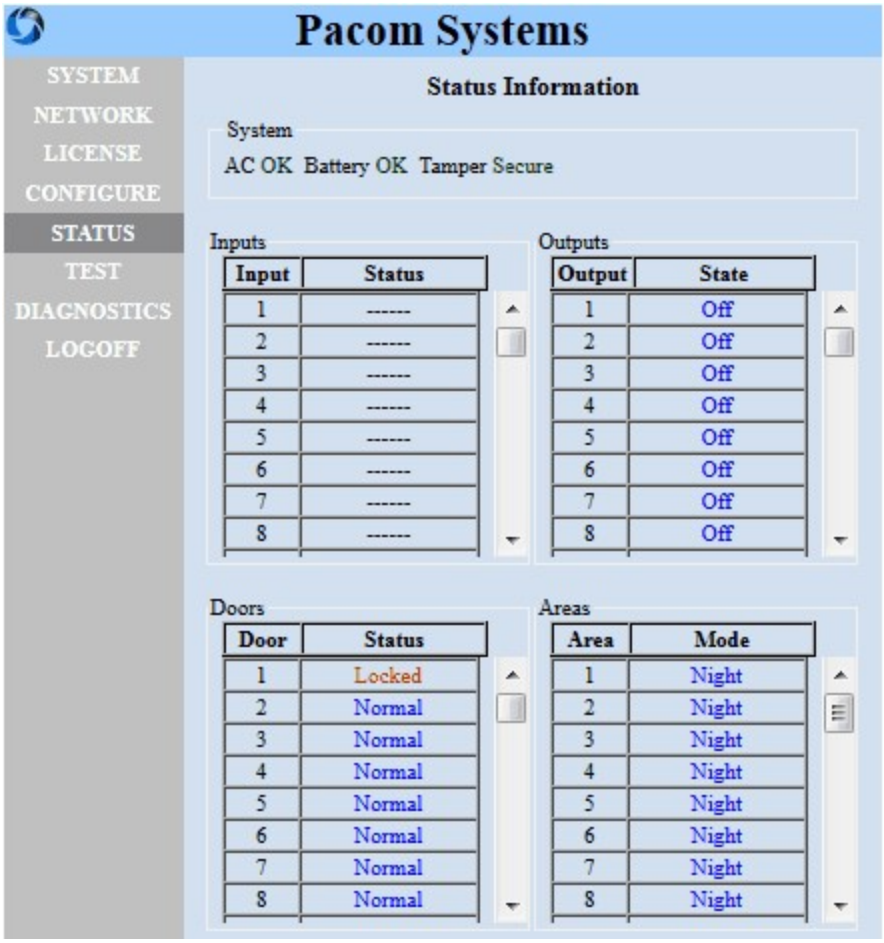
Configure Apply the current settings to the Controller.

Alarm Defaults

Area Start	Sets the first alarm area identification (ID) number to pre-configure in the Controller, if required. By default, a Controller will have a single area defined [area 1]. Depending on Controller type, the number of alarm areas that can be supported may vary. To edit, double-click the field and enter a value.
Area End	Sets the last alarm area identification (ID) number to pre-configure in the Controller, if required. By default, a Controller will have a single area defined [area 1]. Depending on Controller type, the number of alarm areas that can be supported may vary. To edit, double-click the field and enter a value.
Action	Sets the alarm system mode that inputs are operational [that is, are capable of generating alarms]. To edit, click ▾ for options. Click an option to select it: • Disable - Remove from configuration. • Enable - Add to configuration. • Unchanged - No specific setting applied.
Input Start	Sets the first input identification (ID) number to pre-configure in the Controller, if required. To edit, double-click the field and enter a value.
Input End	Sets the last input identification (ID) number to pre-configure in the Controller, if required. To edit, double-click the field and enter a value.
Active In	Sets the alarm system mode that inputs are operational [that is, are capable of generating alarms]. To edit, click ▾ for options. Click an option to select it: • 24Hour - Always operational regardless of alarm system mode. • Day Mode - Operational in Disarm/Day mode only. • Disabled - Not operational regardless of alarm system mode. • Night Mode - Operational in Arm/Night mode only. • Unchanged - No specific setting applied.
Configure	Apply the current settings to the Controller.

Viewing Hardware Status

In the home screen, click Status. Status for inputs, outputs and doors connected to the Controller display as well as alarm areas.



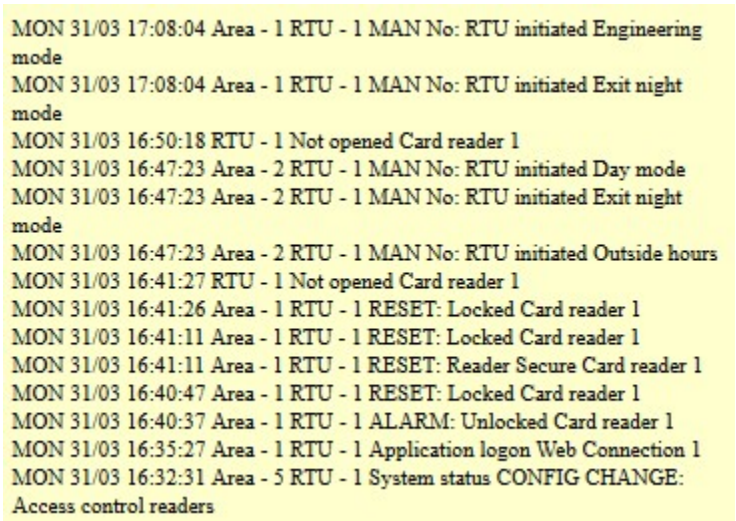
Testing and Diagnostics

In the home screen, click Test. Test command controls applicable to doors, inputs, outputs and areas display. Use the Status display to view the result of test commands.

Control	Description
ID	Sets the identification (ID) number of the node/object to apply the test command to. To edit, click the field and enter a value.
	Sets the command to apply to the selected node/object. To edit, click ▾ for options. Click an option to select it: • Area Reset - Sets the selected alarm area to change mode according to alarm system settings. • Day Mode - Sets the selected alarm area to Disarm/Day mode regardless of alarm system settings. • Door Access - Sets the selected door for a single access [unlock for a period of time then lock again]. • Door Lock - Sets the selected door to a locked state - no access available.

Command	• Door Unlock - Sets the selected door to an unlocked state - free access available. • Door Secure - Sets the selected door to its normal state [usually determined by its alarm area settings]. • Eng Mode - Sets the selected alarm area to Engineer mode regardless of alarm system settings. • Input Deisolate - Sets the selected currently disarmed/isolated input so that alarm events from it are responded to by the head system. • Input Isolate - Sets the selected input so that alarm events from it are ignored by the head system. • Night Mode - Sets the selected alarm area to Arm/Night mode regardless of alarm system settings. • Output Off - Sets the selected currently active ("on") output to an inactive ("off") state. • Output On - Sets the selected currently inactive ("off") output to an active ("on") state.
Send	Sends the selected command to the Controller.

To view transactions for test commands for diagnostics/testing purposes, click Diagnostics in the home screen.



You are here: Appendices > Regular Expressions (Regex)

Regular Expressions (Regex)

A full explanation of regular expression ["regex"] is beyond the scope of this documentation, only some brief notes and examples are provided here for reference. Regular expressions are used to find specific text in a larger body of text. For example, to locate a specific word, such as "alarm" and, as a result, perform some kind of action. The following regular expression syntax is supported:

Simple Expressions

The most basic search is to search for a specified word. For example, "cde" when compared to "abcdef" matches "cde".

Square Brackets

Square brackets ("[" and "]") can be used when looking for words with alternative spellings:

- "Eri[ck]son" matches both "Ericson" and "Erikson".

A range of characters can be specified between square brackets:

- "[a-z]" matches all letters between "a" and "z".
- "[2-5]" matches numbers 2, 3, 4 and 5.

Full Stop

Full stop (".") matches any character. For example, "a.b" matches "aab", "acb", "a7b", "a?b" etc.

Backslash

Backslash ("\") can be used to enter special characters:

- "\d" matches a number.
- "\s" matches a single space.
- "\w" matches a letter, a number or "_".

Backslashes can also be used to find exact characters:

- "\[" matches "[".
- "a\.b" matches "a.b", but not "a?b".

Vertical Bar

Vertical bar ("|") or pipe is used for alternative matches. For example, "a|b" matches both "a" and "b".

Brackets

Brackets ("(" and ")") are used to group letters together into individual search entities. For example, "(ab)|(cd)" matches both "ab" and "cd".

Repetitions

Special characters are used for handling character/word recurrences:

- Question mark ("?") matches none or one instance only.
  - "a?" matches "" or "a".

- Asterisk ("*") matches from zero to any number of consecutive instances:
  - "a*" matches "", "a", "aa" etc.
- Plus ("+") matches from one instance to any number of consecutive instances:
  - "a+" matches "a", "aa", "aaa", etc.
- Parentheses ("{" and "}") match a specific number of consecutive instances:
  - "a{3}" matches "aaa".
  - "a{3,4}" matches "aaa" or "aaaa".
  - "a{3,}" matches "aaa", "aaaa", "aaaaa" etc.

Further Examples

A simple expression for finding IP addresses can be "(\d{1,3}\.){3}\d{1,3}". The expression finds 1 to 3 numbers followed by a full stop - this must recur three times. After the last full stop another 1 to 3 numbers is required. This expression would also match "999.999.999.999", which is not a valid IP address. A more advanced expression for IP addresses is "((25[0-5]|2[0-4]\d|1\d\d|[1-9]\d|\d)[.]){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]\d|\d)".

To match an email address, "\w+@\w+\.\w{2,4}" can be used. It finds any amount of consecutive characters followed by an @ symbol, then any number of consecutive characters followed by a full stop and then 2 to 4 consecutive characters.

Examples using the following strings as examples for testing regex syntax:

String 1 - Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)

String 2 - Mozilla/4.75 [en] (X11;U;Linux2.2.16-22 i586)

Syntax	Result
Simple Matching - Literal character testing. Spaces are included and all characters are case-sensitive when searching.	
m	String 1 - compatible String 2 - no match
a/4	String 1 - Mozilla/4.0 String 2 - Mozilla/4.75
5 [	String 1 - no match String 2 - Mozilla/4.75 [en]
le	String 1 - compatible String 2 - no match

Brackets and Ranges - "Metacharacters" used to define lists and ranges to test for:

[] : Square brackets - Test for one character position once and once only. For example, "[12]" means test for "1", and if not found, test for "2". Charcters on either side of the

brackets are added to the test.

- : Dash, inside square brackets - "Range separator" to define a range. For example, "[0-2]" means test for "0", and if not found, test for "1", and if not found, test for "2". Another example, "[0-9A-C]" means test for "0" to "9" and "A" to "C" (but not "a" to "c").

^ : Caret, inside square brackets - Negates the expression. For example, "[^Ff]" means test for anything except "F" or "f". Another example, "[^a-z]" means tst for anything except lower case "a" to "z".

in[du]	String 1 - Windows String 2 - Linux
x[0-9A-Z]	String 1 - no match String 2 - Linux2
[^A-M]in	String 1 - Windows String 2 - no match

Positioning/Anchors - "Metacharacters" used to define where tested characters must appear in searched data:

^ : Caret, outside left of square brackets - Start of string. For example, "^[T]" means test for "T" as the first character in the string.^ (caret, outside square brackets) - Start of string. For example, "^[T]" means test for "T" as the first character in the string. square brackets) - Start of string. For example, "^[T]" means test for "T" as the first character in the string.

$: Dollar, outside right of square brackets - End of string. For example, "[z]$" means test for "z" as the last character in the string.

. : Period - Any character(s) in this position. For example, "duc." means test for "duc" with any characters after it.

^[A-Z]	String 1 - Mozilla String 2 - Mozilla
[a-z]\)$	String 1 - DigiExt) Note that "\" is an "escape character" so that ")" is treated as a literal. String 2 - no match
.in	String 1 - Windows String 2 - Linux

Quantifiers - "Metacharacters" used to define the number of times tested character must appear in searched data:

? : Question mark - Preceding character occurs 0 or 1 time only. For example, "colou?r" finds "color" as "u" appears zero times, and "colour" as "u" appears one time.

* : Asterisk - Preceding character occurs 0 or more times. For example, "tre*" finds "trog" as "e" appears zero times, and "tread" as "e" appears one time, and "tree" as "e" appears more than one time.

+ : Plus - Preceding character occurs 1 or more times. For example, "tre+" does not find "trog" as "e" appears zero times, but finds "tread" as "e" appears one time, and "tree" as "e" appears more than one time.

{n} : Braces, with required value - Preceding character or character range occurs exactly n times. For example, "e{2}" finds all strings containing "ee".

{n,m} : Braces, with required minimum and maximum values separated by comma (",") - Preceding character or character range occurs exactly n times, but not more than m times. For example, "ba{2,3}" finds "baab", "baaab", but not "bab" or "baaaab".

{n,} : Braces, with required minimum value followed by comma (",") - Preceding character or character range occurs at least n times. For example, "ba{2,}" finds "baab", "baaab", "baaaab", but not "bab".

W*in	String 1 - Windows String 2 - Linux
[xX][0-9]{2}	String 1 - no match String 2 - X11

Special Metacharacters - "Metacharacters" that imply special functions:

\ : Backslash - Following character is to be treated as a "literal" and not part of the regular expression. For example, "4\.[0-2]" means treat "." as part of the test, resulting in matches for "4.0", "4.1" and "4.2".

(n) : Parenthesis, with content n. Combines regular expressions together in a nested fashion. This can be used for using expressions within other expressions, where the result of nested expressions are applied to the containing expression. For example, "^([A-C]in)" means find any strings where the first three characters are "Ain", "Bin" or "Cin".

n|m : Pipe, with content either side, n and m. Find values on left side or right side but not both. If left side is found, the right side is not tested; if the left side is not found, the right side is tested. For example, "gr(a|e)y" will find "gray" or "grey".

You are here: Appendices > General Data Protection Regulation (GDPR) Support Advice

General Data Protection Regulation (GDPR) Support Advice

The General Data Protection Regulation (GDPR) aims to protect all EU citizens from

privacy and data breaches. It seeks to give individuals control of how an organization uses their personal data and introduces hefty penalties for any organization that fails to comply with the rules.

Personal data includes any information related to a natural person that can be used to directly or indirectly identify that person. Organizations complying with the GDPR need policies and procedures to manage any personal data they collect and store.

PACOM Systems is aware of its legal and regulatory responsibilities under the applicable privacy laws and the new GDPR. We are fully committed to protecting the privacy and confidentiality of our customers in compliance with the new rules.

Disclaimer

The information in this document is for information purposes only. The intent is to help you understand how Unison stores and processes personal data.

PACOM Systems does not have any access to the data your organization chooses to store when they implement Unison. It is the sole responsibility of your organization to establish clear and transparent processes and policies so that they comply with GDPR requirements. These may include:

- Getting express consent from data subjects (employees, visitors, contractors, etc) to store details about them including access information, video and/or images.
- Determining minimum retention periods for data storage is required to support security, legal and individual requirements. This should be disclosed to all data subjects.
- Displaying signs to let data subjects know that they are being filmed, photographed, or otherwise tracked when within company premises.
- Determining what personal information is to be kept for identification purposes.
- Determining what types of security and secure infrastructure that the company will use.

How Unison supports your organization’s GDPR Compliance

Know your data

One of the key aspects of GDPR compliance is to know what personal data you collect and store. Unison has been designed to include data protection concepts which include limit data collection, retention and accessibility.

Personal data is stored in Unison as a means to identify cardholders. The personal data that is recorded for a cardholder is determined by your organization’s policies. As a minimum, a User ID must be entered for each cardholder. This User ID is used throughout Unison to monitor cardholders and ensure the access control rules configured in your system are implemented.

Data security

All information recorded by Unison is stored securely in Microsoft SQL Server databases which feature industry-leading security measures and privacy policies for safeguarding data and reducing risks. SQL Server provides controls for managing database access and authorization and a powerful set of built-in capabilities that safeguard data and identify when a data breach occurs.

Unison relies on SQL Server for the encryption and security, and the available functionality is dependent on the version of SQL Server:

- For transparent data encryption, supported from SQL Server 2008+
- For backup encryption support, supported from SQL Server 2014+
- Separation of duties, supported from SQL 2014+
- Unison 5.9.0 also introduces full support for SQL Server 2016, which enables additional security aspects:
  - Encryption at rest and in motion
  - Dynamic Data Masking and Row Level Security

  Further information on SQL Server and the features that help with GDPR compliance can be obtained from Microsoft.

Unison supports full transport encryption to ensure that data transmitted between the controllers, servers and clients is secure. Operator roles and permissions are core to the software and are used to control who can access the data held by Unison.

The right to be forgotten

Unison (v5.8.6 and later) includes a number of features that support your organization's compliance with the GDPR right to be forgotten:

- Automatic Transaction Log management – any transaction logs held within the system are automatically deleted when they are older than a specified (configurable) number of days.
- Automatic Driver Log Management – If your Unison installation is set to save driver log data to disk, they can be set to be deleted when they are older than a specified (configurable) number of days.
- Automatic User Management – Users can be automatically deleted from Unison under three different conditions:
  1. User Validity: If a user's "Valid To" date has expired, and the number of days since expiry is more than the limit, the user will be deleted.
  2. Card Validity: If a user does not have any active access cards for longer than a specified number of days, the user will be deleted.
  3. Permissions: If a user has permissions and those permissions have expired for longer than a specified number of days, the user will be deleted.

See Configuring the System section on Data Privacy configuration for more information on these settings.

Note: With Automatic User Management, the operator has the option to whitelist

(exclude) the user from automatic deletion. Each condition can be set differently, with a different number of days before automatic deletion takes effect.

Unison v5.9.0 introduced a new feature, Manual User Management. This allows you to manually deletion of individual user logs (for example: access control, alarms, events). This supports identifying and deleting logs where the user itself has been deleted. See Users Profile for information relating to Manual User Management.

Right of access to data

One of the GDPR requirements is that users can request a copy of any personal data held by your organization. Unison v5.9.0 introduced a new feature, User Transaction Printing, which provides you with the ability to print user records. See Users Profile for information relating to User Transaction Printing.

Right to restriction of processing

Unison v5.9.0 includes additional features that can be used should one of your data subjects exercise the GDPR right to restriction of processing. This allows you to store the personal data, but that is all. These features are:

- Ability to control operator views/permissions
- Full audit tracking for operator changes.

See Configuring Roles, Operator Groups and Operators for related information.

Additional protection and security information

Unison also contains a number of features that your organization can use to help secure your system and system data, including:

- Operator passwords are encrypted in the database. Optionally, Windows Active Directory "single sign-on" can be applied.
- Connections between SQL Server and system components support encryption using SQL Server encryption tools.
- Unison clients can be installed either using a default [hidden] system SQL password or a custom password that is 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; requiring operator authentication to unlock. Operators can manually lock a Unison client at any time. Any system initiated or manual client locks are logged.
- Partition management that can help ensure 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.
- In-built tools for automating system database archival ["logs"] and for restoration

from backup.
- SQL database clustering is supported for automated database server redundancy.

You are here: Appendices > GDPR Automatic Deletion

GDPR Automatic Deletion

Introduction

The enactment of GDPR in the EU on May 25 2018 signifies a codification of data privacy and data protection schemas. It not only protects the rights of the individual to see the data collected about them, and to have data deleted when it no longer is required by the organization, but it also protects against accidental (or deliberate) data loss. Further, there may be additional laws or regulations dictating the minimum period of time that data must be retained for irrespective of whether an individual has requested the data to be removed.

GDPR defines a Personal Data Breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”

In context, GDPR Chapter 4 Article 32 paragraph 2 specifies that for the controller and processor “… account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.”

It is important for organizations to understand their obligations for GDPR compliance in both the deletion AND protection aspects and have clearly defined policies and procedures to demonstrate how they will comply with the regulations and laws. Software applications, such PACOM Unison only help facilitate the organization’s policy, but if it is incorrectly used, it is the organization and not the developers of the software that would be liable for any breach.

PACOM Unison provides operators with the ability to automatically delete user records and transaction data based on specified criteria, and also manually delete records and data for individuals (or collection of individuals). Manual data deletion is not an issue, because an operator is making a conscious decision to delete a user, and must follow a number of steps in order to delete the records for that user.

However, with any automatic deletion functionality, there is an inherent risk of accidental data loss because the software relies on operator-defined “validation criteria”, and processes user records against that validation criteria without regard to what the data is. The user record could be a temporary contractor that has left the organization, or it could be a senior manager who is on long-term leave.

Given that there are steep penalties for breaches of GDPR, consideration must be made on which is the easier breach to rectify, bearing in mind that each breach of GDPR requires rectification within 72 hours.

- Breach 1: Accidentally retaining users because the user is currently set to be "excluded" from automatic deletion.
- Breach 2: Accidentally deleting users because of an automatic process that removes users based on specific criteria;

With Breach 1, the operator can simply select the individual (or individuals) concerned and delete the user record. They can then bulk-update users that they want to include for future automatic deletion. Deletion of individual (or multiple) users can take seconds. Bulk-updating users can also take a short amount of time. Rectification of Breach 1 should take less than a minute or two. In fact, it will take less time to rectify than it will to report.

With Breach 2, the operator must identify the details of the individual (or individuals) that were accidentally deleted. They will need to gather:

- All of the user details including employee number
- Specific details on which facilities and assets that the user had access to, and what times of the day/week they had such access
- Any additional "personal access" information that may pertain to that user
- What access cards the user had (including potentially lost or blocked card details too)

Rectifying an individual user may take up to a day to collect and validate information. Lost cards would be almost impossible to recover because the card numbers would not easily be recoverable.

Rectifying a large number of users would take days or longer to resolve.

Safeguards

There are four safeguards to help protect operators against accidental data deletion:

1. For PACOM Unison version 5.9.0, By default, ALL users are excluded from automatic deletion.
    - An operator (with appropriate permissions) must explicitly add a user (or users) for deletion
    - To revert to pre-5.9.0 behavior, an operator simply needs to select all users and do a "Bulk Update" to "Include for automatic deletion" for all users.
2. Permissions for automatic deletion
    - In 5.8.6, Only the administrator was able to access the automatic deletion function
    - In 5.9.0, full operator permissions have been added, which allow "view" and "edit" permissions for the automatic deletion.
3. There is a warning in the Automatic deletion section that warns operators that

data will be permanently deleted if the function is enabled

4. The operator must enable the functions that they want to use – first enabling the feature, then enabling the separate criteria. Each step requires action on the part of the operator.

Steps to Activate Automatic User Management

1. Administrator or operator (with appropriate permissions) needs to go to the User Privacy section of the Unison (Explorer > System Configuration > System > Settings > Data Privacy).
2. If the operator wants to enable automatic deletion of users, they will need to "Enable Invalid User Management".
3. Next, they need to specify which criteria they want to validate against:
   a. User is Invalid for x number of days,
   b. No Active Cards for y number of days, or
   c. No Valid Permissions for z number of days.

   They also need to specify the number of days between validation checks, and the time of day that the validation check occurs.

4. Once the appropriate options are selected and set correctly, the operator simply clicks on "Save". At this stage, NO user records will be deleted automatically.
5. Next the operator will go to the users section of Unison (Access Control Administration > Users)
6. They must explicitly "include" the user (or users) for automatic deletion.
   a. For individual users, the operator can select a user, and enable the "Include for automatic deletion" option.
   b. For multiple users, the operator selects the users they want to include, then do a "Bulk Update" of the "Include for automatic deletion" option.

At the end of these steps, any user that has been included for automatic deletion, AND meet one or more validation criteria will be automatically deleted during the next validation check. Remember, user records that are automatic deleted are permanently deleted. There is no option to undo a user deletion.

Conclusion

PACOM Unison helps operators prevent against accidental deletion through a number of safeguards including requiring operators to explicitly opt users into automatic deletion.

If a user is excluded from automatic deletion, the user (and user logs) can still be manually deleted

Accidental data loss can still occur if operators have incorrectly changed settings, but it is an express change that the operator must do to allow automatic deletion. That change is logged for audit purposes.