dormakaba

Aurora User Guide

Keyscan Aurora 2.0.1.0



Table of Contents

Navigating Aurora	1
User Preferences	5
General User Preferences	5
Person Search Criteria Defaults	5
Default Print Card Template	6
Preferred Sites	6
New Firmware	7
Working Sites	8
Aurora E-Plex Lock Setup	10
E-Plex Service Setup	11
Current E-Plex Services	11
E-Plex Certificate Creation	13
E-Plex Certificate Implementation	14
Verifying Certificates	17
Install E-Plex Services	18
E-Plex Firmware Update	22
E-Plex Quick Guide Reference	23
BEST Offline Lock Integration Setup	25
BEST Guest Credential	31
BEST Room Availability Feature	31
Person Screen	31
Aurora thyssenkrupp Setup	32
Communication Server	32
Adding a thyssenkrupp Panel	32
Group Access Levels	33
Schedule Assignment	33
Mobile Credentials	34
Application Utilities	34
Add Person/Edit Person	34
Keyscan Mobile App	35
KONE Integration Setup	36
How to Register Aurora	38

How to Use the Help	40
How to Log In	41
Back Button / Navigation History	43
Aurora Icons & Symbols	44
Re-organizing Column Data	46
Heading Search Filter	47
What is Access Control?	49
How Access Control Works	51
Basic Site Setup Procedures	52
How Do I...?	54
What is a Site?	56
Site Directory (Site Information Setup)	58
Name & Define a Site	59
Bypass Password Reset Requirement For New Users	62
SMTP Setup - Alarm and Message E-mail	63
Communication Server Setup	64
Corporate ID	66
Logging Level	67
Complex Passwords	68
Auto Delete on Expiry	69
Password Expiry	70
Kaba Integrated Mode	71
Enable Keyscan Credentials for Extended Card Format	73
Allowed Login Attempts	75
Refresh Timer	76
Reason for Disabling Logging	77
Auto Clear Alarms	78
Reduce Photos	79
Hardware Setup	80
Door Control Units	83
Supported Reader Formats	91
About Doors and Readers	97
Configure Door & Reader Parameters	98

Door Setup	99
Reader Assignments	104
Dual Custody Mode	107
Anti-Pass Back	111
Door Status – Manual Overrides	113
Reset Anti-Pass Back	114
Name Auxiliary Outputs	115
Name Inputs - Assign to Outputs	117
Input Status	119
Auxiliary Output Status	120
Introduction to the IOCB1616	121
Operating Modes	122
Example Applications	124
And - Or Conditions - Timers - Schedules	126
Setup IOCB1616 Parameters	127
IOCB1616 Input Status	129
IOCB1616 Output Status	130
Global I/O Overview	131
Setup Global Inputs and Outputs	133
Add an NVR & Specify Settings	135
Configure an Elevator Control Unit	145
Floor Status	151
Replacing a Control Unit	152
Delete a Control Unit	153
E-Plex Door Details	154
First Person In	157
Schedules & Holiday Hours	160
Set Schedule Default Off Times	166
Schedule Examples	167
Master Holidays	170
Holiday Setup	171
Schedule Status	174
Assign Schedules to Doors	175

Assign Schedules for Reader/Keypads	178
Assign Schedules to Auxiliary Outputs	181
Assign Schedules to Elevator Banks/Floors	182
Assign Schedules & Inputs	183
Assign Schedules to IOBC1616 Inputs & Outputs	187
Groups	189
Door Group Access Levels	191
Elevator Group Access Levels	194
E-Plex Group Access Levels	198
BEST Group Access Levels	200
About Alarms and Events	201
Sound Setup	202
Priority Setup	203
Event Setup	204
Assign Devices and Events	207
Response Instructions	209
Actions	211
View Filters	214
Escalations	216
Logging Filter	217
Custom Transaction Names	219
Device Image Setup	220
Default Device Images	222
Device Status Images	225
Alarm Monitoring & Alarm Response	229
Find and Review Past Alarms	232
Email Alarm Notification	234
Alarm Types	235
System Health	237
About People Records	240
About the Edit Person Screen	242
Personal Information	242
Credential Information	244

Site Assignment	245
Optional Fields - Common / Site	246
Site Enrollment	246
Transactions	246
Visits	247
Create a Person's Record	248
Attach a Photo to the Record	252
Image Editor	254
Photo Edit Tutorial	258
Create a Temporary Credential	261
Define Person Types	263
Enable the Middle Name Field	265
Automatically Create PINs	266
Optional Fields - Common & Site	267
Activate/Deactivate Site Optional Fields	270
Records - Multiple Sites	271
Import People Records	272
Export People Records	277
Create Records with a Bizscan Scanner	279
Search for Records	281
Edit/Delete a Record	283
De-activate Credential or Record	284
Cancel & Replace a Lost or Stolen Credential	286
Print Photo Badges	287
Credential Transactions	289
Credential Enrollment Feature	290
Bulk Update Credentials	291
Bulk Update Actions	291
Advanced Filters	292
Bulk Update People	296
Bulk Update Actions	296
Advanced Filters	296
Bulk Print Credentials	300

Block Load Credentials	302
Visits	304
Manage System Users	305
System User Examples	308
System User Types	310
Create a System User Account	311
User Search Directory	313
Edit a System User Account	314
Change a System User's Password	315
Deactivate/Delete System User Accounts	316
Default Keyscan User Account	317
Auto Shutdown Time	318
About the Global Card Template Editor	319
Global Card Template Editor Tools	321
Open - New Buttons	324
Card Properties	325
Database Fields - Placeholders and Labels	327
Colour Selection	329
Template View Selector	330
Supported Barcodes	331
Create a New Card Template	333
Open an Existing Card Template	334
Draw a Rectangle, Ellipse, Triangle - Cards	335
Draw a Free-form Line	336
Draw a Single Line	337
Draw Multiple Angled Lines	338
Insert a Background Image	339
Insert an Image	340
Insert Text	341
Insert a Barcode	342
Insert Person/Credential/Optional Fields from the Database	345
Insert a Personal Photo Frame	346
Move, Rotate or Scale an Object	347

Text Alignment	348
Arrange Objects in Layers	349
Edit or Delete Text	350
Clone a Card Template	351
Delete an Object	352
Save a Global Card Template	353
Delete a Card Template	354
Assigning Card Templates to Specific Sites	355
Active Map Template Editor	357
Map Tools	358
Insert Devices	362
New - Open Buttons	363
Colour Selection	364
Map View Selector	365
Create a New Map	366
Open an Existing Map	367
Import a Floor Plan	368
Draw a Rectangle, Ellipse, Triangle - Maps	369
Draw a Free-form Line	370
Draw a Single Straight Line	371
Draw Angled Multiple Lines	372
Insert an Image	373
Insert Text	374
Insert a Door or Device	375
Move, Rotate or Scale an Object	376
Arrange Objects in Layers	377
Edit or Delete Text	378
Delete an Object	379
Save a Map Template	380
About Visitors & Preliminary Setup	381
Create a Visitor Record	383
Optional Card Scanner	384
Schedule a Visit	386

Cancel a Visitor's Credential	390
Print Visitor Badges	391
Search for Today's Visits	393
About Present3	394
Present3 Modes	395
Using Present3	402
Setup Present3	403
Lockdown - Doors and Elevator Floors	408
Operate the Lockdown	409
Enhanced Lockdown	411
Enhanced Lockdown Setup	411
Manually Revert Enhanced Lockdowns	412
Application Utilities	414
Auto Shutdown Time	416
Gateway Setup	417
E-Plex Gateway Setup	419
Root Certificate	419
E-Plex Server Certificate	419
Gateway Hardware Configuration	420
Extended PIN (7 digit)	422
Reset Status Window Position	423
Transaction Response	424
Door Status - Manual Overrides	427
E-Plex Door Status	431
Reader Status	434
Input Status	436
Auxiliary Output Status	439
IOCB Input Status	442
IOCB Output Status	445
Online Transactions	447
Credential Transaction Photos	449
Floor Status	450
Access Control Unit Card Count	451

Access Control Unit Status	452
Reset Anti-Pass Back	455
Reader Diagnostics	456
Schedule Status	457
Intrusion Zone Status	458
Intrusion Partition Status	459
Intrusion Area Status	461
Software Connections Status	463
Visit Status	464
Person Last Seen Status	466
Gateway Status	467
Access Control Unit Memory Viewer	469
E-Plex Operations	470
About Reports & Summaries	471
People IN/OUT Report	472
Cumulative Hours Report	474
Deleted People Report	477
Door Access Granted Summary Report	479
Door In/Out Summary Report	481
Door Access Summary Report	483
Total People by Hour Report	485
Unused Since Credential Report	487
Active/Expired Credential Report	489
First Usage Report	491
Group Status Report	493
Holiday Reports	495
People Information Reports	498
Visitor Information Report	500
Visit Reports	502
Person Reader Access Report	504
Reader Access Report	506
Group Access Report	508
Global ACU Report	510

People Linked to Active Directory Report 511
Schedule Assignment Report 513
E-Plex Door Access Report 514
E-Plex Battery Level Report 516
BEST Available Guest Credentials Report 518
BEST Available Guest Ranges Report 520
BEST Used Guest Ranges Report 521
BEST Door Access Report 523
BEST Guest Door Access Report 525
Best Door Credential Assignment Report 527
BEST Credential History Report 528
Gateway & Zigbee Information Report 530
Alarm Watch Report and Setup 532
Site Setup Report 535
System Log Report 536
Transactions Reports 539
Introduction 544
System User Account Settings 545
Add an Intrusion Control Unit 546
Communication Setup 548
Enter Master Code & Users 550
Name Intrusion Zones 552
Name Intrusion Partitions / Areas 553
Activate Groups or Credential Holders as Intrusion Users for P3 554
Synchronize Clocks 557
Setup Present3 - Manual Arm/Disarm 558
Intrusion Status - Partitions/Zones 560
Why It’s Important to Manage the Aurora Database 561
Backup Now 564
Schedule Automatic Database Backups 565
Database Maintenance 567
Purge - Transactions and System Log 568
Compress & Re-Index the Database 570

Restore the Database	571
Configure Database Connection Settings	574
Sever Settings XML File	574
Schedule Aurora for Automatic Tasks	575
Keyscan Aurora Agent	577
Disaster Recovery	578
Aurora Output Module	580
Active Directory	583
Keyscan Aurora Milestone Viewer	589
Liability Warning - 26-Bit Wiegand Card Format	592
Waiver of Liability	592

Navigating Aurora

Located near the bottom on all Aurora's screens are seven graphical buttons for rapid access to all the Client software functions. Two mouse actions provide complete navigation to all system menus and commands:

- mouse-over a menu button - a pop-up caption displays the menu button's general function
- click on a menu button - Aurora displays the full list of available menus

Aurora's elegant navigation design lets you easily leap-frog from screen to screen anywhere within the Client software for quick and easy access to all system functions.

Manage People



Manage People

List, search, edit, and delete credential records or visitor records



Add Person

Creates new records for individuals assigned credentials to access system regulated doors and elevator floors; creates visitor records including time, date, status and the contact

Group Access Levels

Assigns groups to doors or elevator floors with specific schedule assignments for regulating access

Import People

Imports external CSV file to populate individual credential record information

Import People

Imports external CSV file to populate individual credential record information

Export People

Exports individual credential record information

Bulk Update Credentials / Bulk Update People

Updates user-selected multiple credential/people records simultaneously

Bulk Print Credentials

Can be used to print several cards at once

Block Load Credentials

Allows entering a group of numerically-sequenced credentials simultaneously

Site



Site Information Setup

Identifies the site

Hardware Setup



Configures site hardware components including control boards, doors, elevators etc.

Schedule Management

Creates schedules for regulating access times, door and elevator auto unlock times, and AI/AO on and off times

Schedule Assignments

Assigns schedules for auto unlock of doors and elevator floors, reader/keypad modes and AI/AO arming/disarming

Group Setup

Creates group names, which credential holders are assigned to, for door and elevator access

Present3 Setup

Assign Optional Fields to Sites

Selects which user-defined optional fields apply to specific sites

Device Image Setup

Inserts photos of system connected devices which are displayed on various interface screens to assist identifying their location

Active Map Template Editor

Creates site floor maps or building plans including the placement of doors, readers, AIs, AOs, CCTV cameras for graphically locating alarm sources

Sound Setup

Imports sound files which can be assigned to priorities and events

Event Priority Setup

Creates a tiered structure for distinguishing alarm level importance

Event Setup

Configures Keyscan's Present3 for credential based toggling of door locks and schedules

Holiday Setup

Assigns holiday schedules to specific calendar dates for statutory holidays, vacation closure or shutdown days or other special days

Assigns specific instructions and actions on designated transactions and alarm events

Digital Video Recorders





Video Device

Calls up Aurora's live video monitoring screen to view system connected DVR cameras

Settings





Manage System User

Create and edit system user accounts to restrict Aurora log-on activity and regulate individual task permissions

Optional Fields Management

Adds user-defined common (universal) and site-specific fields for supplemental credential record information

Manage Master Holidays

Creates a list of master holidays which are common to all sites on multi-site access control systems

Manage Global Card Templates

Create and manage card templates for printing photo ID badges

Application Utilities

Sets SMTP properties for e-mail notification, additional person types, and other system settings

Database Maintenance

Use for backing up site data, programming scheduled backups (critical function), purging older transaction data, and performing other Aurora database tasks

Scheduled Task

Schedules Aurora to automatically run specific transaction reports

Default Device Images

Insert icons or images to replace the system default device icons

Device Status Images

Insert icons or images to replace the system default status images

Custom Transaction Name

Create custom names for system events

Memory Viewer

Control board memory diagnostic tool

Software Registration

Use for registering the Aurora software

Status





Status

Access on-line transactions, door status, input status, output status, anti-pass back reset, schedule status, floor status, panel card count, reader diagnostics, schedule status

Transaction Response

Use to search and view all transactions including alarms that are either new/pending or in the past

Lockdown

Initiates a lockdown at doors or elevator floors connected to selected control units - selected control boards must be configured for lockdown mode

View Active Map



Active Map

Calls up active maps for viewing that were created in the Active Map Template Editor



Reports



People In/Out Report

Produces reports on the in or out status of specified credential holders



Cumulative Hours Report

Formats reports summarizing the cumulative hours credential holders were present based on recorded reader in/out times

Deleted People Report

Lists credential holder records that have been deleted from the Aurora database

Door Access Granted Summary Report

Lists the number of access granted transactions that occurred at each door

Door In/Out Summary Report

Lists the number of access granted transactions at selected in/out readers

Door Access Summary Report

Lists the number of access granted and access denied transactions at selected readers

Total People by Hour Report

Tabulates the access granted transactions at selected readers by the hour

Unused Since Credential Report

Lists individuals whose credentials have been inactive

Active/Expired Credential Report

Lists temporary credentials with a date range that will become active or expire

Group Status Report

Produces reports listing the current status of groups - active or inactive – for one or multiple sites

Holiday Report

Formats a report by site listing dates assigned as holidays during the calendar year

People Information Report

Runs reports with optional levels of details on selected credential holders

Visitor Information Report

Runs reports with optional levels of details on selected visitors

Visit Report

Runs reports on visits and visitors

Person Reader Access Report

Runs reports on individual credential holder’s access levels at each door

Reader Access Report

Formats reports with optional levels of details on group access at reader controlled doors

Group Access Report

The Group Access Report summarizes all predetermined group access levels within a specified site

E-Plex Door Access Report

The E-Plex Door Access Report summarizes group access levels at wireless locks, and, if selected, the schedules for each specified E-Plex door.

Alarm Watch Setup

Reports the in/out status of credentials

Site Setup Report

Produces a report on site hardware, schedule, alarm, system user, access levels, and holiday settings

Important

After the initial setup and whenever changes occur, it is a good idea to run and print a Site Information Report so you have a paper copy of your Keyscan access control system settings

System Log Report

Runs a report listing system log entries

Transaction Report

Formats a user-defined report on all or selective site activity

User Preferences

This component allows the user to set up their preferences. Through User Preferences, the user is able to:

- Choose their preferred language
- Select whether or not People will be automatically enrolled in all sites upon creating a new person
- Turn on/off alarm transaction sounds
- Toggle the Advanced Search on/off
- Provide default values used as search criteria in features that allow the user to search for People
- Indicate which card templates should be used when printing a card based on credential information or visit information
- Select preferred site(s) to work with

General User Preferences

This section allows the user to change general parameters within the software, including:

- Preferred Language - Select the desired language from the drop down box
- User Types Automatically Enrolled in New Sites - Use the drop down box to select which user type(s) will be automatically enrolled when a new site is created
- Enroll New People in All Sites - Select/de-select to toggle whether or not a new person should be enrolled into all sites
- Enroll New Credentials in All Person's Sites - Select/de-select to toggle whether or not new credentials get added to all sites that the user can see/access
- Mute Alarm Transaction Reminder - Select/de-select to enable/disable alarm transaction sounds; only repeating sounds will be muted upon selection (other sounds that do not repeat will always be played)
- Use Advanced Group Access Levels View - Select/de-select to enable/disable the advanced search option as the default view
- Bypass password reset requirement for new users - Select/de-select to enable/disable the password reset requirement

Person Search Criteria Defaults

This section allows the user to manipulate the person search criteria defaults, including:

- Person Type - Select either All Types, Employee or Visitor from the drop down box
- Credential Number - The number entered will change the credential and bath number of a card searched
- Site Name - The site entered will become the default site in a search
- Group Name - The group name entered will become the default in a search
- Optional Field - The default person search criteria will contain the additional information added here
- Active - Select All, Active Only or Inactive Only from the drop down box
- Sort By - Select Given Name, Surname or Type from the drop down box
- Sort Direction - Select between Ascending or Descending from the drop down box to decide the order of importance
- Visit Status - Select an option from the drop down box to determine a visitor's status: Expected, Delayed Arrival, Arrived, Departed or Cancelled
- Today's Visits Only - Select the box in order to keep the default search criteria to the current date only

Default Print Card Template

This section allows the user to set default card templates for both credential holders and visitor credentials. Defaults can be set for both the front and the back of a card. Scroll through the Template and/or Back Template drop down menus to select the desired default.

Preferred Sites

Use the arrow buttons to move a designated site(s) to the list of default search criteria by adding it to the Selected Sites column. The sites selected will be the only sites the user will see when working within the Working Sites menu.

New Firmware

Firmware 9.47 - Aurora 1.0.20.0

As of Aurora Version 1.0.20.0, certain features will require an EPROM Firmware Version 9.47 or higher (applicable ONLY to boards with DIP switches--board revisions PC1097 & PC1156 or higher). To verify your current firmware version, please review the hardware setup of any and all installed units. Please contact our Sales team if you require a firmware upgrade (for an additional cost). If you have any technical questions on these features, feel free to contact the Technical Support team.

New Firmware 9.47 features include:

- The ability to schedule up to 32 Block Holidays per Site; all panels must have the same updated firmware
- Allows the User to arrange Groups for First Person In (FPI) use; individuals must be in valid groups assigned to use FPI
- Allows the User to set the Reset Anti-Pass Back option within Site Information Setup. In this state, credentials may be used at IN or OUT readers with their next reader presentation; choose between one hour time intervals from 12 AM to 6 AM, at which time the Aurora software automatically clears the anti-pass back status
- The ability to add/remove Lockdown access to a credential within the Add Person/Manage People screens:

  Lockdown Access The credential can access the door during a Lockdown based on their assignments and schedules

  No Lockdown Access The credential cannot access the door during a Lockdown

Working Sites

The Working Sites feature allows you to filter what the Aurora software displays according to the site(s) selected. If a site isn't specified, the Aurora software will not apply any filters, which means you will be working with all sites assigned to you as default.

Default Working Sites visible to you on login can be specified through the Preferred Sites setting in the User Preferences menu.

Using the Working Sites Feature

The Working Sites feature can be accessed from any page within the Aurora software; however, you will return to the main screen upon applying changes to your Working Sites.

To access the Working Sites menu, select the triple bar icon  in the top-right corner of the screen. Once there, a list of sites that you are currently working with is displayed with the option to Edit. Select Edit and a list of all the sites associated with your login will be displayed in alphabetical order, with the sites you are currently working with at the top of the list.

The list order can be changed from ascending to descending by selecting the Sites arrow icon; however, items you are currently working with will remain above all other sites. You can also filter the list of sites that you are not currently working with by typing the name of the site into the Site Search field within the Edit Working Sites screen.

In the Edit screen, select/deselect sites to add or remove what you are currently working with. Select Save at the bottom-right of the screen to confirm the change(s), or select Cancel to undo the changes.

The triple bar icon  in the top-right corner of the screen will turn orange if you are not working with all sites, otherwise it will remain white.

Note: The Working Sites menu is not a permanent setting; once logged out, all changes will be lost and will have to be re-entered. You can configure your User Preferences to set up sites that are automatically selected for you when you log in again.

Forced Site Selection Feature

The Forced Site Selection feature changes the work flow in the Aurora client so that users are required to select the site(s) they are working with within the software. This feature prevents the user from working with all of the sites when performing certain tasks. Once the user is finished, they must sign out of the selected site(s) in order to continue with new site(s).

Follow these steps to enable the Forced Site Selection feature:

1. Under the Settings menu, select Application Utilities.
2. Select the Advanced tab at the top of the screen. There, you will see the CMAC Features sub menu on the right of the screen.
3. Select the check box beside CMAC Features and the box beside Use Forced Site Selection.
4. Select the Save button on the bottom right of the screen. Close the software down completely and re-open for the new feature to take effect.

Using Forced Site Selection

Follow these steps to properly utilize the Forced Site Selection feature:

1. Log into the Aurora software client as usual. The screen displays site(s) previously set up in the Working Sites feature, through the Select Sites To Work In menu.
2. Select the appropriate site(s) by either double-clicking on a single site (to select only that site) or select the check box beside each site you wish to work with. Once selected, press the Sign In to Sites button on the bottom-right corner of the screen.
3. If a large list of sites populates the screen, you can filter the results by inputting information in the Custom Site ID, Site Search or Description fields at the top of the screen. You can also sort the results with the Sort By and Sort Direction drop down menus.
4. After selecting the Sign In to Sites button, the selected site(s) are displayed as a banner at the top of the screen in orange. Click the arrow next to the site(s) displayed to view the site's comments.
5. To sign out of the selected Working Sites, click on the triple bar icon ≡ in the top-right corner of the screen. From there, select the Sign Out of Sites button. Signing out of sites will force the screen to return to the Select Sites To Work In menu.

Forced Working Site Selection Feature (Aurora Web)

The forced working site selection feature changes the workflow in the Aurora Web client. It enforces a rule that states that users are required to select the site(s) that they are working with before they can do anything within the Aurora Web application. It forces the user to choose the site(s) that they are working with and prevents them from ever being able to work with all of the sites when performing tasks. Once the user is finished their task with the selected site(s), they must sign out of the site(s) they are currently working with in order to work with new sites.

As of version 1.0.17.0, the forced working site selection feature was only used in the Aurora desktop client. This feature has been added to the Aurora Web client as of version 2.0.2.0, but it must be enabled using the Aurora Desktop client before it is used.

Follow these steps to enable the "Enable Forced Working SItes in Aurora Web" feature:

1. Log in to the Aurora client desktop application.
2. Under the Settings menu, select Application Utilities.
3. Select the Advanced tab at the top of the screen. There, you will see the CMAC Features sub menu on the right of the screen.
4. Select the check box beside CMAC Features and the box beside "Enable Forced Working SItes in Aurora Web".
5. Select the Save button on the bottom right of the screen.
6. Restart the Aurora Web application so that the new feature to take effect.

CMAC Working Sites Options

When CMAC Features are enabled, the following changes are put into effect for each User listed in the table below.

Manager & Administrator	• Can select multiple sites to work with • Able to set User Preferences for their Preferred Working Sites • User's site preferences will be automatically selected in the Forced Working Sites feature upon logging in
User & Visitor	• Unable to select multiple sites • Unable to specify Preferred Working sites as a User Preference

Related Topics

User Preferences

Aurora E-Plex Lock Setup

Follow these steps to properly integrate an E-Plex wireless lock into the Aurora software:

Note: Full E-Plex integration will only become visible after setting up an E-Plex Door Group.

1. Under the Site Management menu, select Hardware Setup. Click on a Site if you already have one made. If not, a Site will have to be established in the Site Information Setup menu.
2. From the drop down menu on the top left of the screen, select E-Plex Door Group.
3. From the drop down menu in the E-Plex Doors sub-screen, select the model of E-Plex wireless lock you wish to add.
4. In the E-Plex Door Details screen, fill out the following fields, where applicable:
    - Name - identifies the door; generally the name should indicate where the door is located
    - Lock Model - identifies the model of E-Plex wireless lock being used
    - Is Wireless - dictates whether or not the lock type is wireless; the box must be checked for E-Plex wireless locks to continue
    - Function Type - assigns Entry, Residential or Privacy function to wireless locks
    - Unlock Time - measures the amount of time, in seconds, that the door remains unlocked for
    - Buzzer Volume - the intensity in which an alarm sounds when the door is help open past the preset unlock time (0 = Off, 3 = Loudest)
    - Tamper Count - dictates how many failed credential reads will trigger a Tamper Lockout
    - Tamper Lockout - the amount of time, in seconds, the lock will sit idle for after the Tamper Count meets the preset threshold of failed credential reads
    - Manual Passage Duration - dictates the amount of time, in hours, a door remains unlocked through a Manual Override on the Status Screen
    - Door Held Open - the time interval, in seconds, that the door may remain open before the system reports a Door Held Open violation
    - Gateway - a pathway number will appear here after the Gateway establishes connection with the Aurora software
    - ZAC - this PIN code is integral into successfully pairing a Gateway to the Aurora software. Select the wrench icon to randomly generate a new PIN code

    Note: To ZAC a lock, enter: ##088# + ZAC Code + #
5. Select Save on the bottom right corner of the screen. The E-Plex Lock Setup is now complete.

Once you've completed setting up your E-Plex Door, you can always reassign the Door to a different E-Plex Door Group. Please refer to "E-Plex Door Details" in the related topics for more information.



Any credential without a PIN will NOT be sent to an E-Plex wireless lock.

Related Topics

E-Plex Door Details

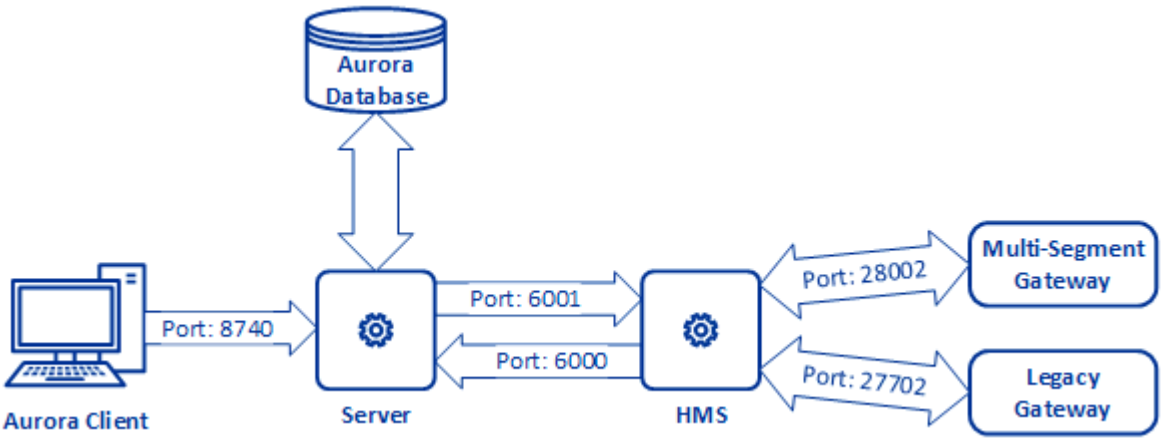
E-Plex Service Setup

Aurora 1.0.20.0 introduces new certificates for enhanced security between the dormakaba HMS and E-Plex Services. This also serves to strengthen secure communications with existing and next generation products with the Aurora software client.

IMPORTANT – As of Aurora 1.0.20.0, all previous E-Plex Services will need to be removed and new E-Plex services will need to be installed to be able to work with Aurora 1.0.20.0 or higher. Please observe the following before continuing:

- This new installation process requires an Administrator level password
- This installation requires Microsoft .NET 4.8 (or higher). The installation program will install, if required. Copies of required files are located in the folder containing the Aurora Software installation files
- Certificate setup is completed on the E-Plex Service server (if different from the database server)
- Certificates are required with Aurora version 1.0.20.0 when using E-Plex products

Example of Complete Setup

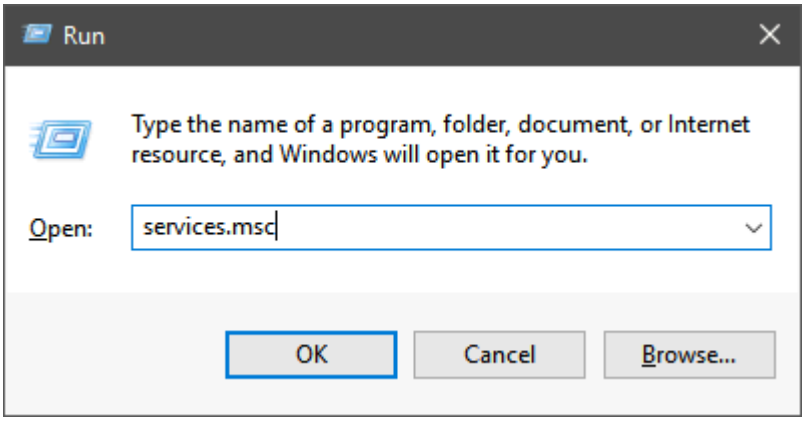


Current E-Plex Services

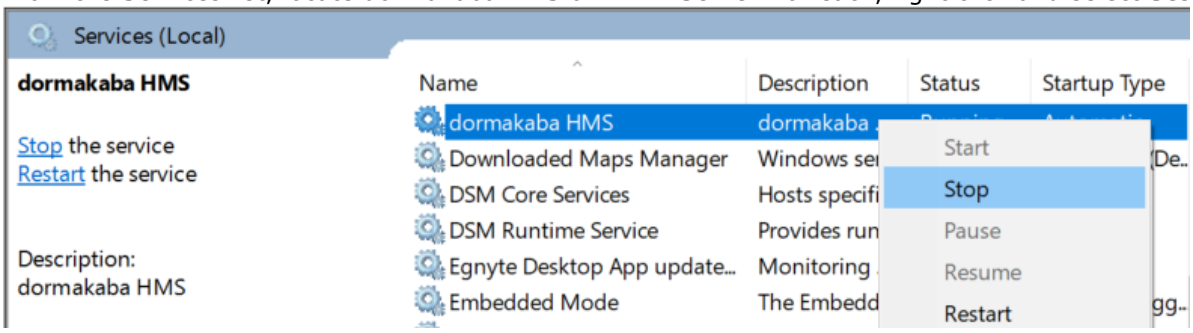
Previously running E-Plex Services must be stopped and uninstalled prior to creating certificates.

Follow these steps to stop and uninstall current E-Plex Services:

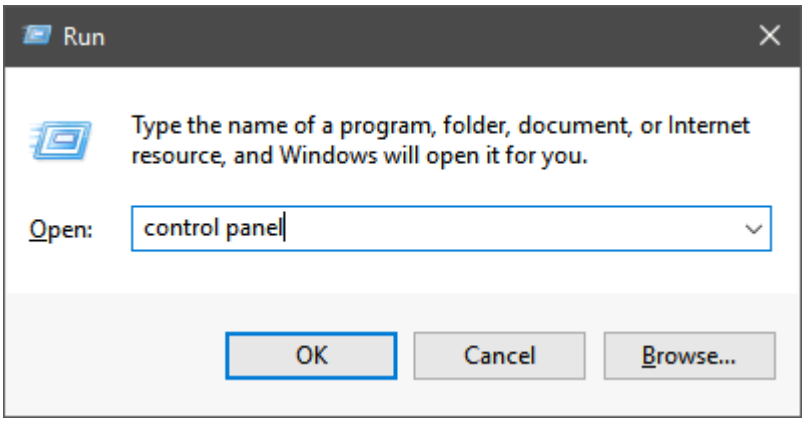
1. Stop existing E-Plex Services by opening a run command (Windows Key + R) and run **services.msc.**

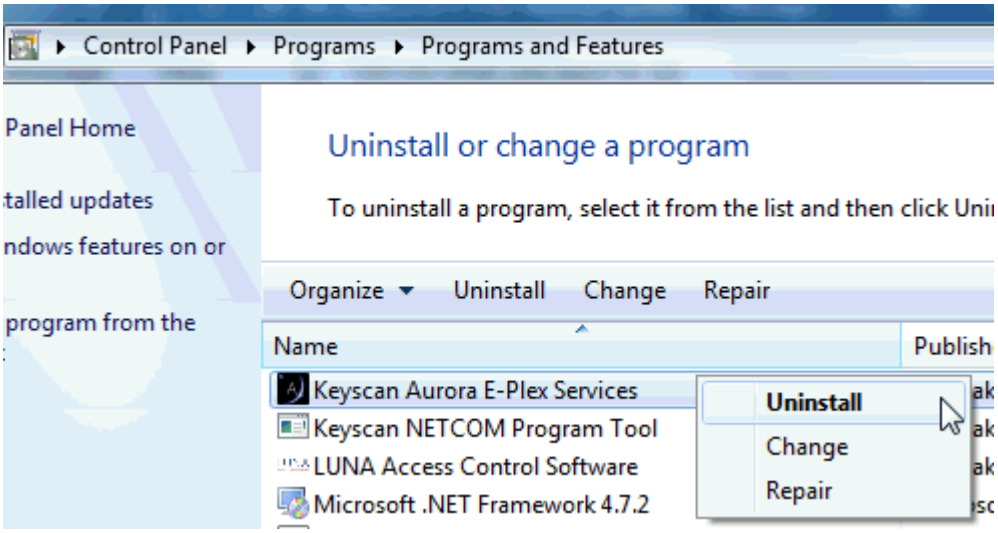


2. From the Services list, locate dormakaba HMS & EPLEX Server. For each, right click and select **Stop**.

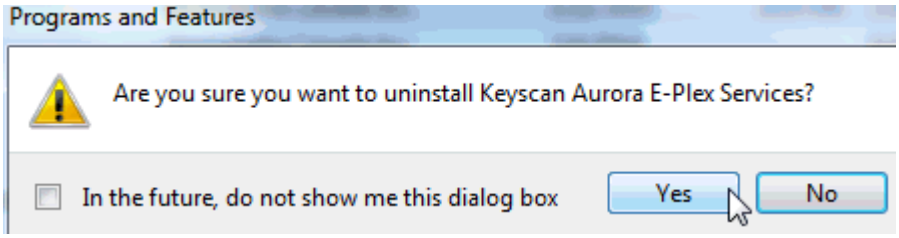


3. To uninstall the existing E-Plex Services, open a run command (Windows Key + R) and run **control panel**. From there, navigate to Programs and Features > Uninstall or change a program. Locate Keyscan Aurora E-Plex Services, right click and select **Uninstall**.





4. Select **Yes**. The Windows Installer will begin uninstalling the E-Plex Services (this may take several minutes). Once uninstalled, the program should no longer appear in the list of programs (detailed in the previous step).



5. Create an Aurora database backup before proceeding.
6. Update the existing Aurora Software to 1.0.20.0 via the Aurora Update Process from: https://www.dormakaba.com/us-en/software-downloads-and-updates. Locate **Download Aurora Software Update (Version 1.0.20.0)** and select the download button.
7. Shut down the Aurora software after upgrading to 1.0.20.0. Right-click the Aurora software icon and select **Run as Administrator**. Start the Aurora software.

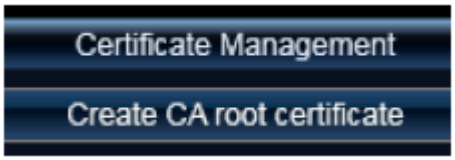
E-Plex Certificate Creation

Public and Private certificates must be created prior to installing new E-Plex Services. Without proper setup, E-Plex Services will not connect to the Aurora database.

> **IMPORTANT:** Running Aurora as admin is required to create certificates. This shouldn't be confused with an Aurora admin user, this is a windows admin user. Prior to creating certificates, ensure you possess Local Administrator privileges. To run Aurora as Administrator, prior to opening the software, right-click on the Aurora .exe file and select "**Run as Administrator**".

Follow these steps to create an E-Plex certificate:

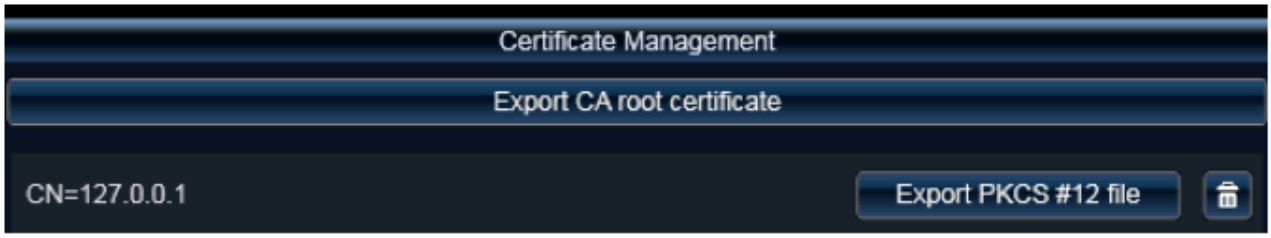
1. Within the Aurora software client, navigate to Application Management > Application Utilities > Security (tab). Select **Create CA root certificate**.



2. At the bottom of the screen, add the server IP (where E-Plex Services are installed) or 127.0.0.1 if the E-Plex service is local to the database PC. Select **Create new certificate**.



3. New information will appear on screen after creating a new certificate. Select **Export CA root certificate**.



4. It is important to choose a safe location when exporting certificates. Select **Browse** to navigate through your computer to the desired (safe) location. Select **Export** when a location is chosen.



5. Next, Select **Export PKCS #12 file**. Follow the same file path chosen in the previous step (Step 4). Input a strong **Import password**; a password is required for adding the private certificate to the Microsoft Console. Select **Export** when a location is chosen.



6. When running Aurora as an Administrator, an **Import Into Store** button will appear next to each certificate the user creates in Certificate Management. When clicked, the certificate will be added to the local PC's certificate store. The icon next to each certificate indicates its current state:

   Green check mark = Found in the local PC's certificate store and it's valid



   Orange Triangle = Found in the local PC's certificate store and it's not valid



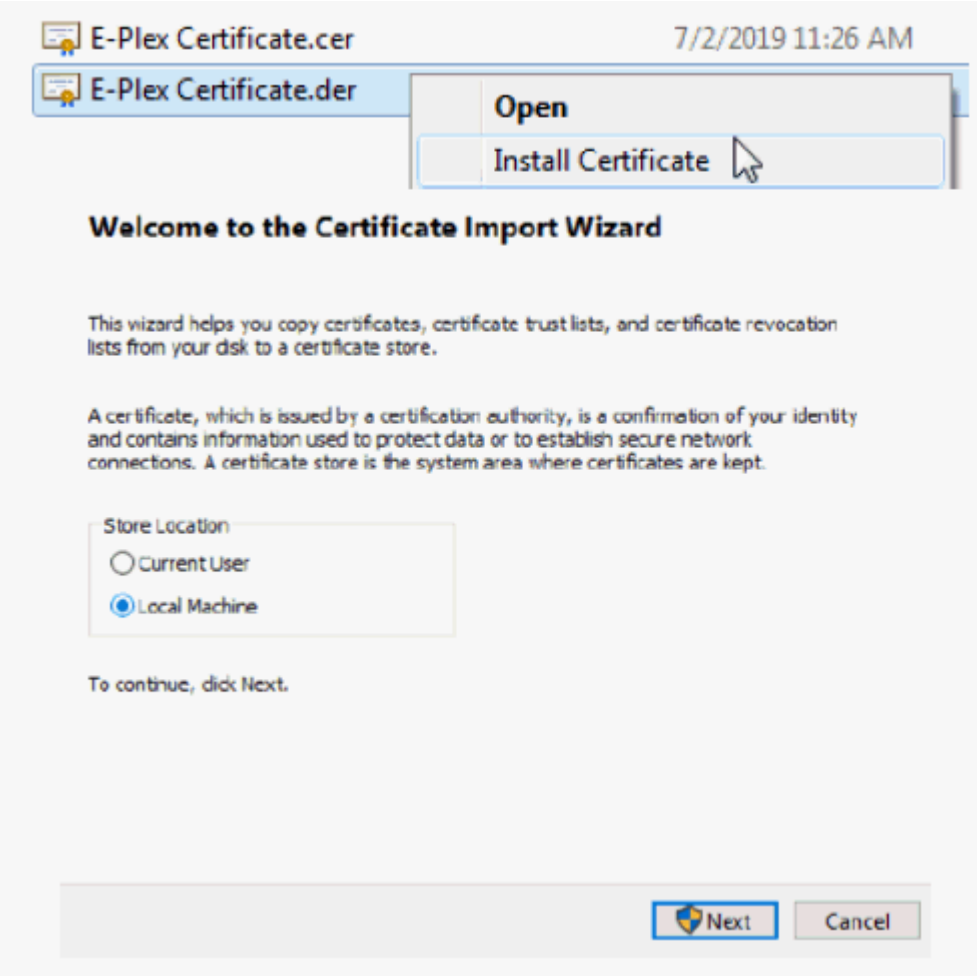
   Red 'X' = Not found in the local PC's certificate store



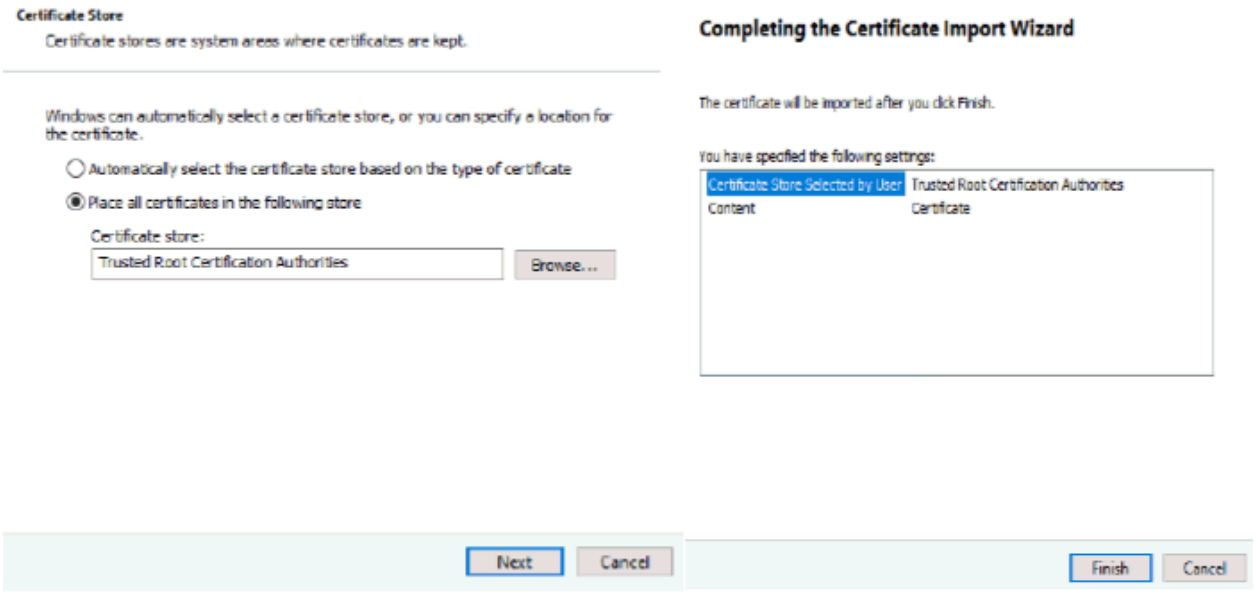
E-Plex Certificate Implementation

*.DER Certificate

1. Open the certificate location (from Step 4 of the previous section) and right click on the *.DER certificate. Select **Install Certificate**. Select **Local Machine** and then **Next**.



2. Assign the certificate to the Trusted Root Certification Authorities Store. Select **Next** and then **Finish**.

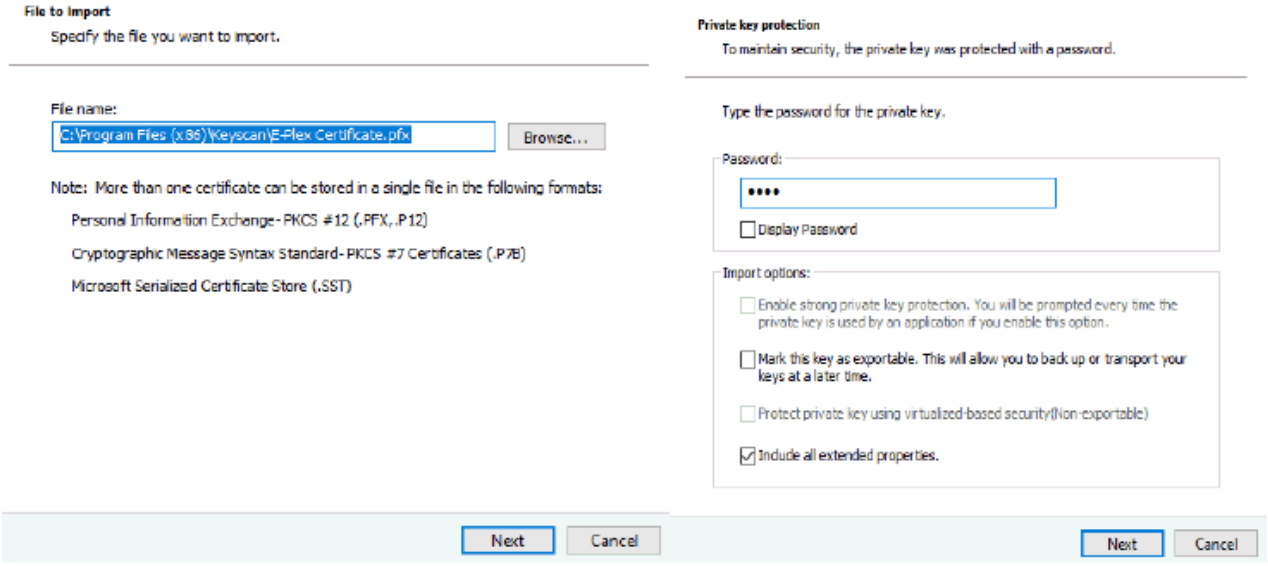


*PFX Certificate

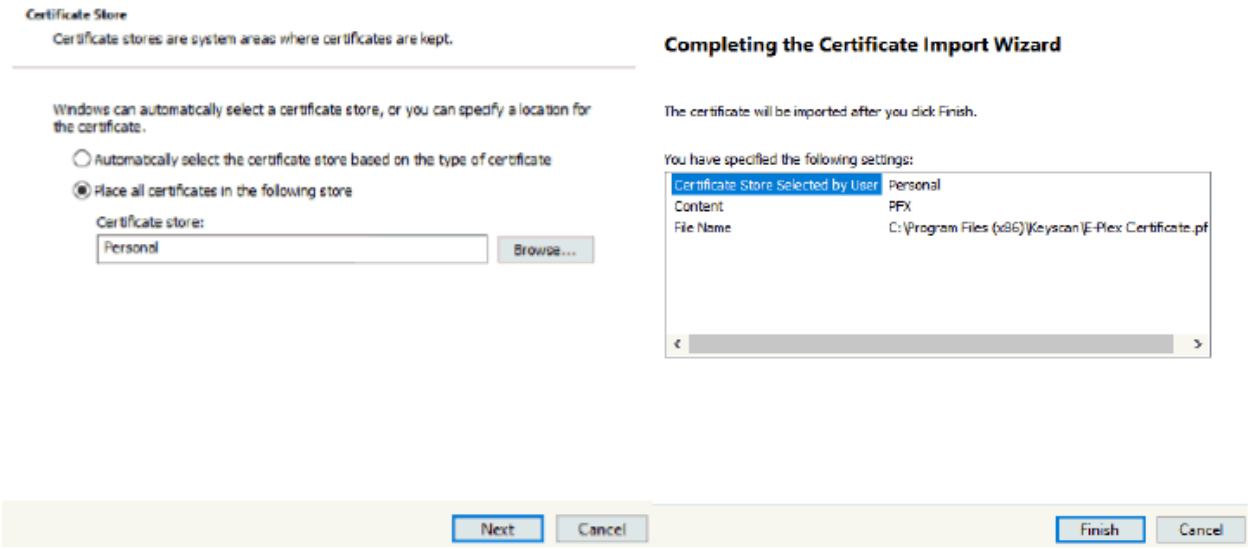
1. Open the certificate location (from Step 5 on Page 2) and right click on the *.PFX certificate. Select **Install PFX**. Select **Local Machine** and then **Next**.



2. Select **Next**. A password prompt will appear, enter the Password from Step 5 on Page 2. Select **Next**.

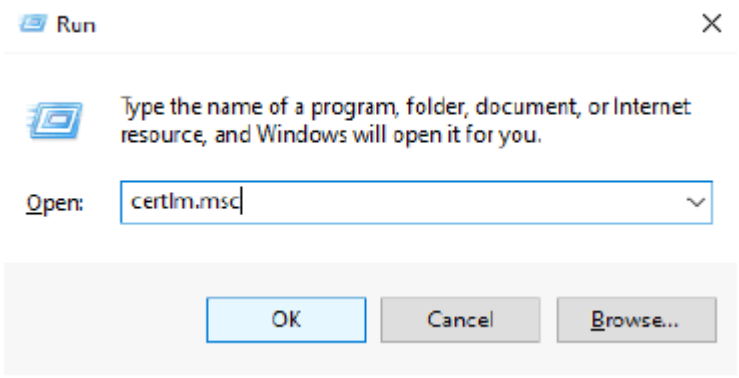


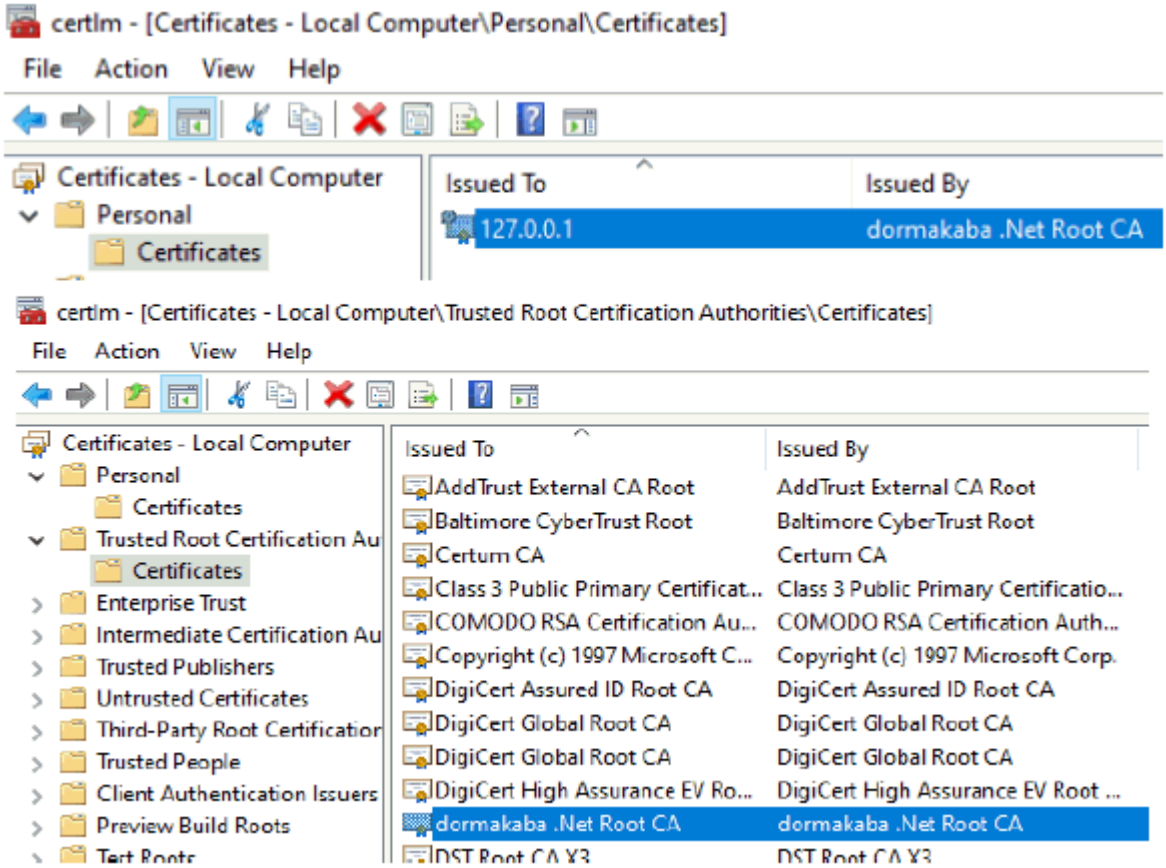
3. Assign the certificate to the Personal Store and select **Next**, then **Finish**.



Verifying Certificates

To verify the certificates, open a run command (Windows Key + R). From the Open dropdown menu, select **certlm.msc** (Windows 10 only). Verify both certificates are present and installed correctly.

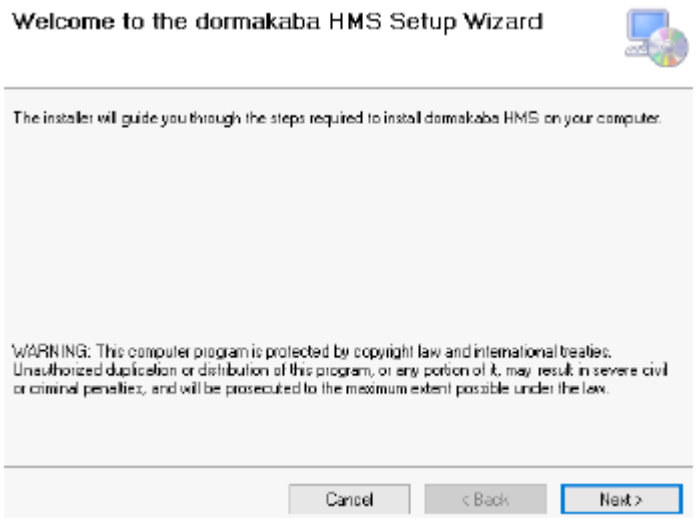




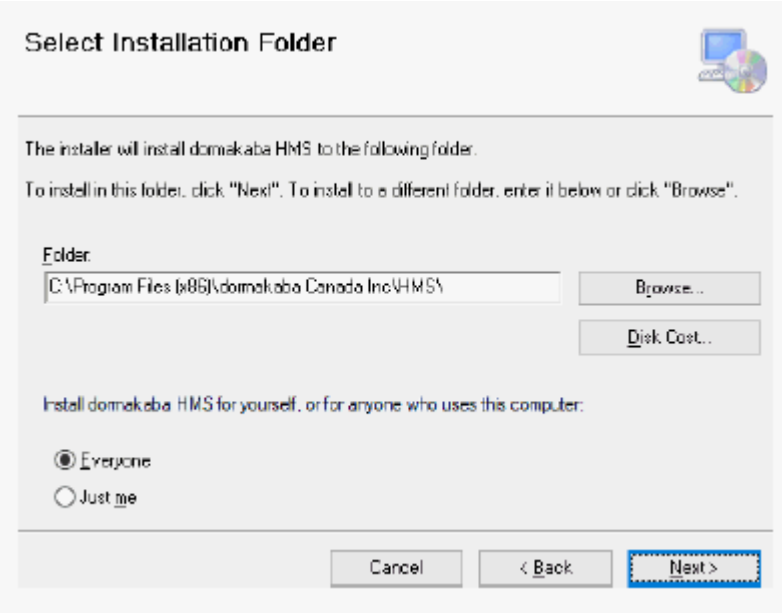
Install E-Plex Services

The final step in this Aurora software update process is to download the new E-Plex Services.

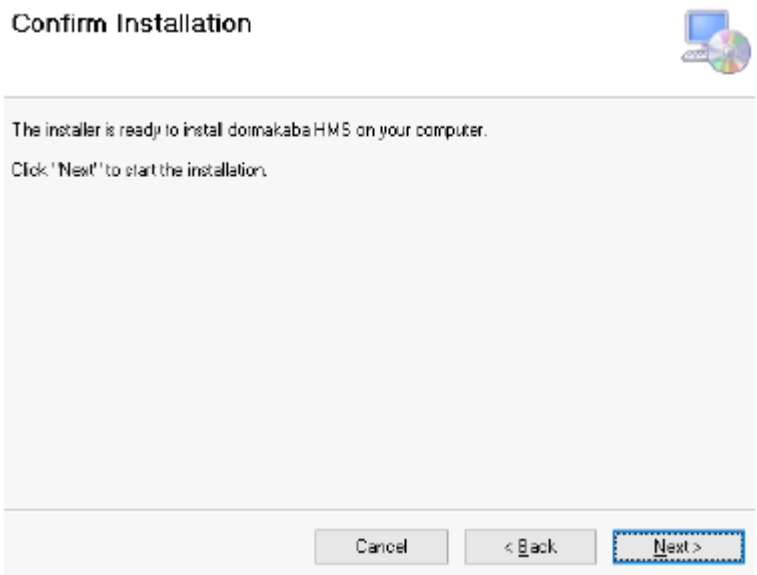
1. From the website, download the two separate installation packages (dormakaba HMS and E-Plex Server).
2. Run the dormakaba HMS Installer.msi file. The Setup Wizard will pop up. Select **Next**.



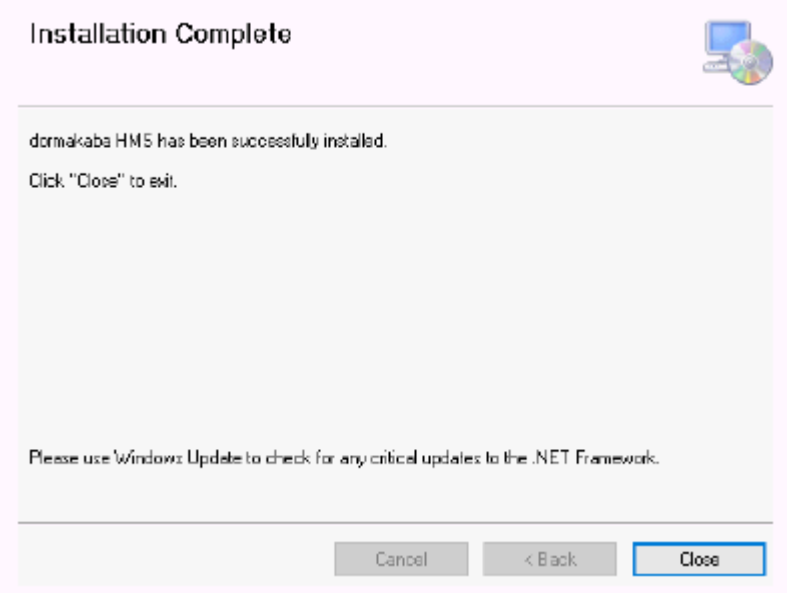
3. Select the destination folder with the **Browse** button. Once a pathway is chosen, select **Next**.



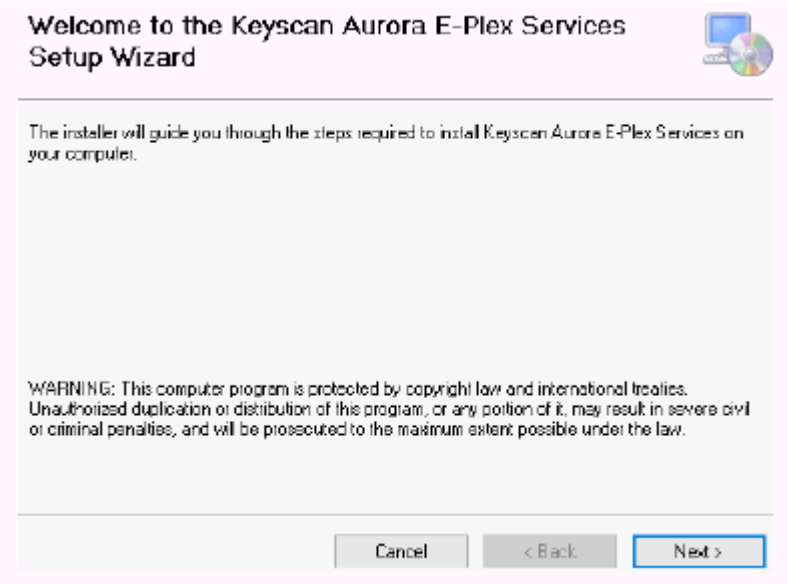
4. Select **Next**.



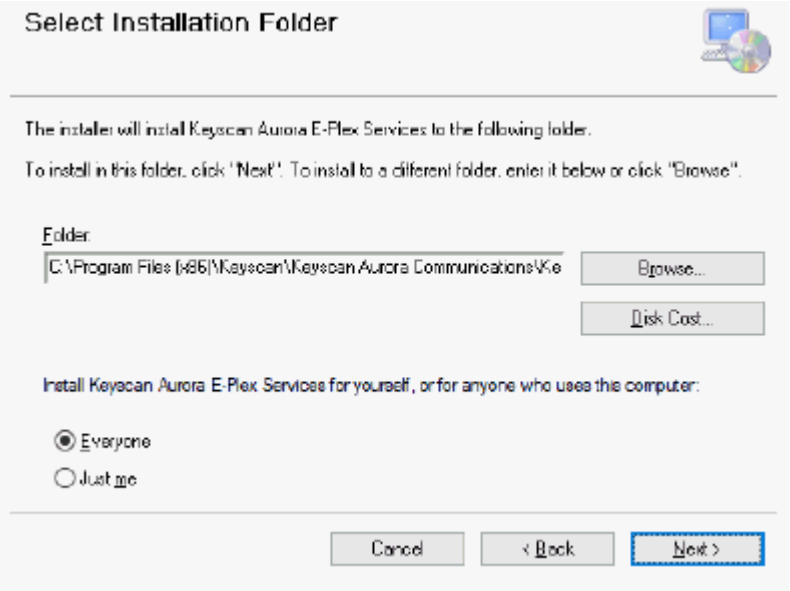
5. Complete the installation by selecting **Close**.



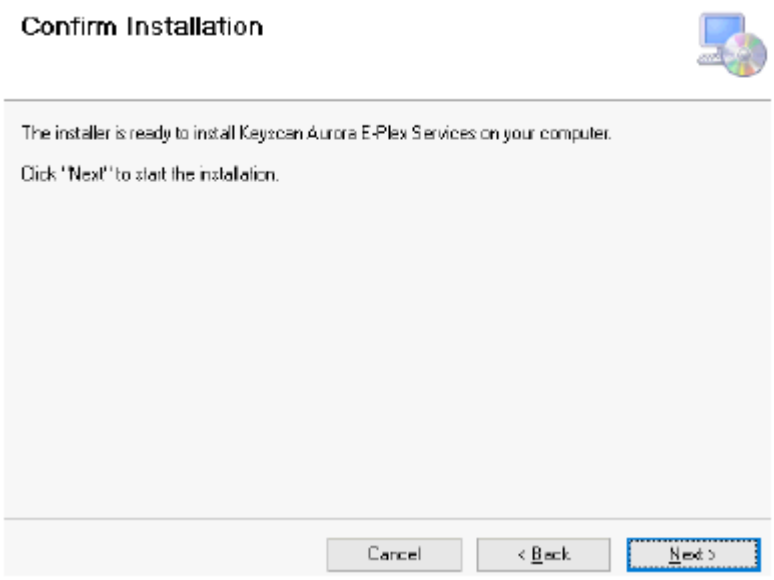
6. Run the E-Plex Server Installer.msi file. The Setup Wizard will pop up. Select **Next**.



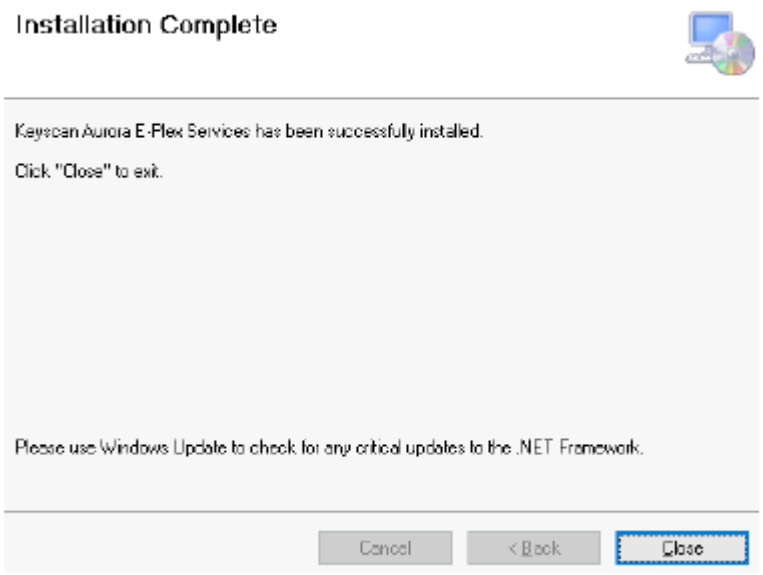
7. Select the **Browse** button to identify the installation folder location. Once a path is chosen, select **Next**.



8. Select **Next** to confirm the installation.



9. Select **Close** to complete the installation.



E-Plex Firmware Update

Updating Aurora with the newest firmware

Follow these steps to properly update the E-Plex firmware within Aurora:

1. Within the Application Management menu, select Application Utilities.
2. Select Pick E-Plex Firmware File.
3. Choose the .xml file provided by your Keyscan representative.
4. Select Save in the lower right-hand side of the screen.
5. Within the System Status and Control menu, select Status.
6. Select Gateway Status under the left-hand list of options.
7. In the Gateway Status sub screen, right click and select Update Firmware.

   Note: The time it takes to complete the firmware update depends on how many locks are present. Times will vary, so please keep your computer running during this process.

E-Plex Quick Guide Reference

The following charts can also be found in Aurora/E-Plex E3600/3700, 5600/5700 Series Quick Reference Guides.

Visual Feedback Message Definitions

Condition	Parameters			
	Green LED	Red LED	Duration	Rate
Valid pushbutton pressed	ON	OFF	1/10 Second	Once
Timeout expired	OFF	ON	1 Second	Once
Valid access credential entered/ presented	ON	OFF	1/10 Second	Once
Access granted	ON	OFF	1/10 Second	1 Second
Access granted (battery low condition)	ON	ON	1/10 Second	1 Second
Access denied	OFF	ON	1 Second	Once
Valid programming entry	ON	OFF	1 Second	Once
Invalid programming entry (including duplicate access credential)	OFF	ON	1 Second	Once
Tamper shutdown beginning	OFF	ON	2 Seconds	Once
Tamper shutdown state	OFF	ON	1 Second	10 Seconds
Tamper shutdown ending	ON	OFF	2 Seconds	Once
Deadbolt/ Thumbturn Privacy Activated	OFF	ON	1 Second	Once
Deadbolt/ Thumturn Privacy De-activated	ON	OFF	1 Second	Once
Hard reset sequence	ON (Alternate)	ON (Alternate)	1/2 Second	Continuously
Hard reset sequence ended successfully	ON	OFF	2 Seconds	Once

Hard reset sequence failed	OFF	ON	2 Seconds	Once

Visual Feedback Message Definitions - Wireless Locks Only

Condition	Parameters			
	Green LED	Red LED	Duration	Rate
Invalid ZAC Entry	OFF	ON	1 Second	Once
ZAC sequence in process	ON	ON	1/2 Second	1 Second
ZAC sequence successful	ON	OFF	1 Second	Once
ZAC sequence failed	OFF	ON	1 Second	Once

Command Reference

Name	Command	Description of Command	Authorization
Factory Reset	099 #	Reset to factory default values, except access PIN length. (Master, Managers, all other users and time/date are retained if already programmed; Users are not reset).	Master
ZAC (Zigbee Access Code)	088 #	Initialize a wireless lock (lock must be in factory default mode).	Master, All Users
Emergency Lockdown	911 #	Put wireless lock(s) in emergency shutdown (lockdown) state.	Master, Manager, Authorized Users
Emergency Passage	811 #	Put wireless lock(s) in emergency evacuation (passage) state.	Master, Manager, Authorized Users
Return to Normal from Emergency	111 #	Put wireless lock(s) back to the normal state from emergency state.	Master, Manager

BEST Offline Lock Integration Setup

BEST G and V series offline locks can be integrated to work with the Aurora software client. In an offline environment, the card (credential) itself is used as the in-between delivery system between the lock and the software. Read and follow the steps outlined below to properly integrate a BEST offline lock with the Aurora software.

Card Formats

Card Formats need to be specified before adding them to a BEST Door Group. Follow these steps to set up BEST card formats:

1. Under the Application Management menu, select BEST Offline Card Formats.
2. From the top-left drop down menu, within the Card Formats sub-menu, select the desired card format to add: Magnetic Stripe Card Format, Standard 26-bit, Corporate 1000 - 35, Corporate 1000 - 48, or Keyscan 36 Bit.
3. Depending on the card format chosen, different options will appear under the Card Format Details sub-menu:
    - **Magnetic Stripe Card Format**
        - Fill in the Name and Facility Code, if your card format uses it, in their respective fields
        - Select the Facility Code, Card Number and Issue Code details by filling in the Length field and selecting the Order from the drop down menu. The Start Address will populate automatically
        - Fill in the Access Control Track in the respective field
        - Select the check box beside Is a Guest Format if applicable, this will change the Start Address automatically
        - Select the Save button on the bottom-right of the screen to finish
    - **Wiegand Card Formats**
        - Fill in the Name and Facility Code in their respective fields
        - Select the Save button on the bottom-right of the screen to finish

    Note: Card Formats can only be edited or deleted if they are not assigned to hardware and there are no credentials in the system using that card format. The card format must be removed from all hardware that it is currently assigned to and delete all credentials of that type from the system in order for it to be edited or deleted.

Schedules

A BEST Schedule needs to be specified to outline specific times BEST Groups and their corresponding credentials are granted access to a specific door. Follow these steps to properly set up a BEST Schedule(s):

1. Under the Site Information menu, select Schedule Management.
2. From the Site drop down menu, located at the top of the screen, choose the applicable Site you wish to add a BEST Schedule to.
3. From the drop down menu, located at the top-left of the screen, scroll through the options and select Add BEST Schedule.
4. Give the schedule a name. To limit confusion, it is advised to add "BEST" into the Schedule Name, since it will only apply to BEST-specific doors.

5. Add blocks of time by clicking and dragging from the start to the end time. To delete a block of time, select the block of time and click the trash (delete) icon located in the top-right corner of the box.
6. Repeat Step 5, if necessary, to input Holiday schedules as well, located at the bottom of the same screen.
7. When complete, select Save located at the bottom-right of the screen to confirm the selection.

Door Group

The next step is to add a BEST Door Group to the software. The Schedules and Card Formats completed in the previous sections will now be added to this group, alongside assigning Doors that this group can access. Follow these steps to properly add a BEST Door Group and Door(s):

Note: The password is a maximum of 21 characters, with no other limitations.

Note: All BEST Door Groups within a single site must have the same regional time zone.

Note: The number and type(s) of permitted card formats depends on the initial door group type.

1. Under the Site Information menu, select Hardware Setup.
2. From the Site drop down menu, located at the top of the screen, choose the applicable Site you wish to add a BEST Door Group to.
3. From the drop down menu, located at the top-left of the screen, scroll through the options and select Add BEST Door Group (G or V, depending on your lock) Series.
4. Provide a Name and Password for the door group, by default the name is 'BEST Door Group' and the password is 'BEST'. To ensure higher security, it is recommended to change the password immediately.
5. From the Regional Time Zone drop down menu, scroll through the options and select your applicable time zone.
6. Select the Doors tab and choose the lock type from the BEST Doors drop down menu. Multiple locks can be added to a single Door Group.
7. Complete the BEST Door Details section on the right-side of the screen by filling in the applicable fields, according to your application and lock type.
8. Select the Schedule Assignment tab. Check the box under the Assigned column that corresponds to the BEST Schedule to be added to the Door Group; an **x** indicates selected.
9. In their corresponding drop down menus, select from the following options under the Schedule ON Mode and Schedule OFF Mode: Locked, Card and Keypad, Card Only, Card or Keypad, Facility Code, First Card Unlock, Unlocked or No Reader Mode Applied.
10. Select the Card Format Assignment tab. From the Card Format column, check the box to select the card format(s) to be used within the BEST Door Group.
11. When complete, select Save located at the bottom-right of the screen to confirm and finalize the BEST Door Group.

Copy Door Settings

By selecting the double door icon beside the BEST Door name, the selected door's configuration can be copied and applied to other doors within the Door Group. This feature can also be used to create new doors with the same configuration. Any new doors created can be added to a current, different or new door group.

Both actions can be used at the same time to ensure that all doors have matching configurations within the Door Group and that the group has the appropriate amount of doors.

On the pop-up window, select the box beside **"Apply Settings to All Doors In Door Group"**, but note you won't be able to create a new door group or add new doors to a different door group.

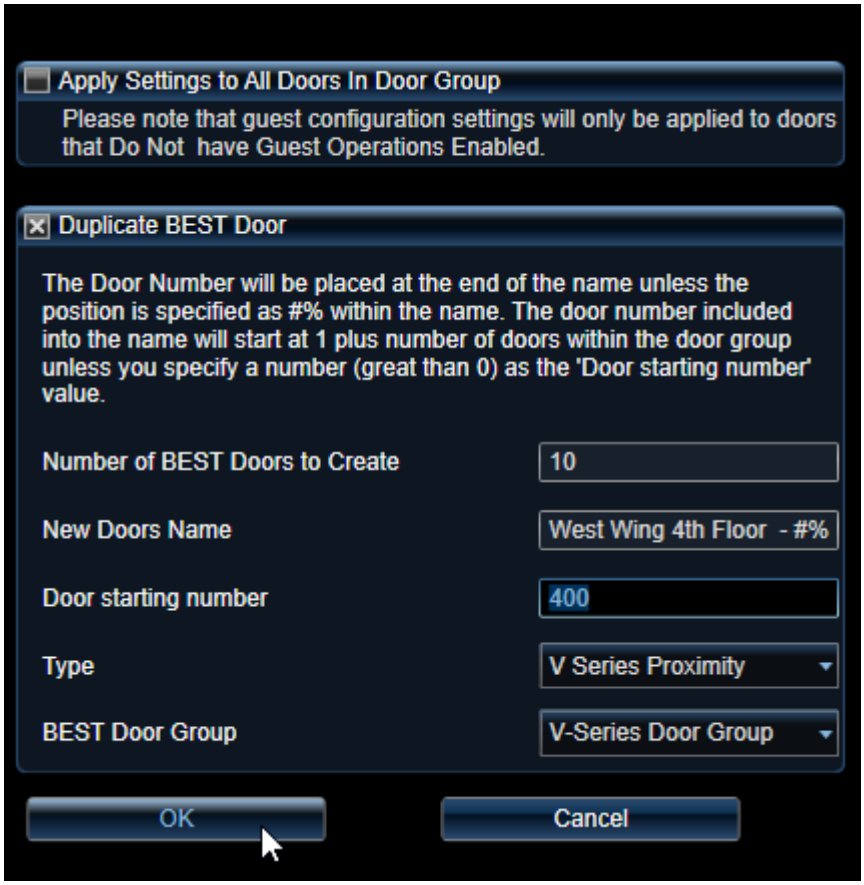
Select the box beside **"Duplicate BEST Door"** to apply the selected door configuration to the number of doors specified. Configure your duplicate BEST door(s) using the fields provided:

- *"Number of Best Doors to create"* - enter the total number of duplicate best doors to create.

- *"New Doors Name"* - the name you enter here will be applied to all newly created doors. Use the characters #% anywhere in the text box to apply numbering to the door names
- *"Door Starting number"* - this is the number that will be applied to the first door created

Use the dropdown menus provided to select the BEST Door "Type" and the "BEST Door Group" o assign them to, then click the "Save" button to create the duplicate BEST doors.

Example) The following will create 10 BEST Doors of type "V Series Proximity" in the "V-Series Door Group". Their names will be as follows: "West Wing 4th Floor - 400", "West Wing 4th Floor - 401", "West Wing 4th Floor - 402", "West Wing 4th Floor - 403", "West Wing 4th Floor - 404", "West Wing 4th Floor - 405", "West Wing 4th Floor - 406", "West Wing 4th Floor - 407", "West Wing 4th Floor - 408", and "West Wing 4th Floor - 409".



Group Access Levels

For a full breakdown of BEST Group Access Levels, read the following section:

BEST Group Access Levels

Adding Individual Credentials

This section assumes you have already created a Person Record. If not, please read the following section:

About the Edit Person Screen

Follow these steps to add an individual credential to a person:

1. Under the Manage People menu, select Manage People. Double-click on the person to be edited.
2. Select Custom Card Format from the Credential Information drop down menu, located at the top-left of the screen.
3. From the pop-up window, scroll through the drop down menu to select the applicable card format. Once chosen, select OK.
4. Enter the card number.

5. If you have engaged the Auto Generate PIN option in the Application Utilities screen, a PIN is automatically inserted in the PIN box. If you have not engaged this option and the person requires a PIN code, you can manually enter a code in the PIN box.
6. As an option, you can use the Description field to make the credential more specific and easy to remember, which is not mandatory to proceed.
7. In the Site Assignment pane, sites are listed on the left. Click in the box to the left of the site the person's credential is authorized for access. The box has an **x** when the site is selected.
8. Select the **v** symbol opposite the site you enabled in the previous step to open the Group Access pane.
9. Select the group or groups the person is assigned to by clicking in the box or boxes to the left. A box has an **x** when selected. Click and drag the scroll bar on the right to access groups not viewable in the pane.
    - You can view a group's access levels, by right clicking when the cursor is positioned over the desired group.
10. Under BEST Lock Features, select Enable Deadbolt Override and/or Enable Door Toggle by clicking the box(es) to the left of the option. A box has an **x** when selected.
11. If you have created and use either common optional fields or site-specific optional fields, select the Optional Fields tab.
12. For Common fields, enter the person’s data in the respective text boxes. Common fields apply to all sites.
13. For Site fields, select the **v** symbol opposite the site and enter the person’s data in the respective text boxes.
14. If required, select the General Info tab to enter any miscellaneous notes or comments about the person.
15. If you have multiple sites and you want the record enrolled at any of those sites but without the credential being valid for access at those sites, select the Site Enrollment tab and select the appropriate sites in the list.
16. Select the Encode Card icon within the BEST Lock Features menu (Card Has Not Been Encoded might be visible beside the icon). The following options will be visible:
    - Card Information to Be Encoded - this section outlines the Card and Track numbers to be encoded onto the card.
    - Encoder Settings - choose the COM Port and Baud Rate through their respective drop down menus. Check the box beside High Coercivity (if applicable); an **x** indicates selected. Select Save Encoder Settings when complete.
17. Prior to encoding a card, ensure the MSR206 Magnetic Stripe Card Reader/Writer is plugged in and functioning properly. For more information, please review the MSR206 Programming Manual.

    Select Encode Card. The Encoding Status window will provide the status, in real time, to the progressing of the card. Upon completion, close the window by selecting the **X** located at the top-right. If the encoding is unsuccessful, or if you want to try again, select either Reset Encoder or Erase Card, depending on your situation.

Block Load Credentials

Follow these steps to add a block of credentials to the Aurora database at once:

1. Under the Manage People menu, select Block Load Credentials.
2. By default, all block loaded credentials will have Given Name set as Block Load and Surname set as Credential.
3. Click on the ▼ symbol opposite Type and select the person type if other than Employee; otherwise, leave the setting on Employee and go to the next step.
4. If the credentials are to be activated immediately leave the Active setting enabled (the box has an **x**) and go to the next step; if you do not want to make the cards active immediately, click in the Active box to the right and disable the setting. The box is blank when disabled.

5. If the credentials require Extended Entry, click in the box to the right. The box has an **x** when enabled. Extended Entry is normally used when doors have electro-mechanical door operators for persons requiring a longer amount of time to access a door. When Extended Entry is enabled, applicable doors follow the Extended Entry Timer and the Extended Entry Door Held Open settings in the hardware Setup screen.
6. Under the Credential Information heading, select Custom Card Format from the Credential Type drop down menu. Next, select the Card Format from the drop down menu.
7. In the Card Range text boxes, enter the lowest credential number in the left box and the highest credential number in the right box. The numbers must be in sequence.
8. If the credentials are being issued on a temporary basis, click in the box to the left of Temporary Options. The box has an **x** when selected.
9. If the card is temporary based on a date range, click on the calendar icon to the right of Valid From.
10. The calendar opens on the current day and month. Do one of the following steps:
    - If the Valid From date is today, select it on the calendar. If applicable, select a time on the right side.
    - If the Valid From date is other than the current day, select the correct start day, or click on the arrows at the top of the calendar and scroll to the desired month and year. Select the day on the calendar. If applicable, select a time on the right side.
11. Click on the calendar icon to the right of Valid To. Do one of the following steps:
    - If the Valid To date is today, select it on the calendar. If applicable, select a time on the right side.
    - If the Valid To date is other than the current day, select the correct end day, or click on the arrows at the top of the calendar and scroll to the desired month and year. Select the day on the calendar. If applicable, select a time on the right side.
12. If the card has a usage restriction, enter the maximum number of times the credential may be used in the Limited # Uses text box. If there is no usage restriction, leave the Limited # Uses blank.
13. Under BEST Card Settings, select Enable Deadbolt Override and/or Enable Door Toggle by clicking the box(es) to the left of the option. A box has an **x** when selected.
14. Under the Site Assignment heading select the first applicable site by clicking in the box to the left of the site name. The box has an **x** when selected. Select the group from the drop down list. You must select at least one group otherwise the credentials will not have a group access level.
15. Click on the Block Load button when you have completed the Block Load Credentials screen.
16. Click on the OK button in the Block Load Complete box.

Exporting/Importing a BEST Database

To export a BEST database, do the following:

1. Under the Site Information menu, select Site Information Setup.
2. Double-click the applicable site you wish to export from.
3. Select Export under the BEST Transport Database section, located at the bottom-right of the screen.
4. When a dialogue window pops up, select where the BEST Database will be saved to. Once a destination is chosen, select OK to continue.
5. Input a Password into the field and select OK. This password will be important later on when Importing a BEST Database, ensure the password is kept in a secure place for future reference. If the password is forgotten, simply repeat steps 1 to 5 over again. A pop up window showing Export Finished will be displayed to complete the process.
6. Select Save located at the bottom-right of the screen.

To import a BEST database, do the following:

1. Under the Site Information menu, select Site Information Setup.

2. Double-click the applicable site you wish to import to.
3. Select Import under the BEST Transport Database section, located at the bottom-right of the screen.
4. When a dialogue window pops up, navigate to the directory housing the BEST Database export file. Once a destination is chosen, select Open to continue.
5. Input the Password entered during the Export phase and select OK. A pop up window showing Import Finished will be displayed to complete the process.
6. Select Save located at the bottom-right of the screen.

BEST Guest Credential

This feature allows a Guest Credential to be added to an available BEST Room. Guest Credentials can be created in the system and assigned to new guests as credentials expire and rooms become available. Settings for credentials are maintained as long as they are not deleted before being reassigned.

If a Guest Credential is deleted before it is reassigned, it becomes available, however Group Access information and other credential-specific details will have to be reconfigured before it is assigned to a Guest.

Note: In order for a Guest Credential to be created and maintained, the system must have G-Series door group(s) with the guest features configured for at least one Guest Door and at least one Guest Card Format.

There are two ways to create a Credential that will grant direct Guest access to an available Room/Door: BEST Room Availability under the Person menu and through the Add Credential feature on the Person screen.

BEST Room Availability Feature

1. Log into Aurora.
2. In the Main Menu, under Person, select BEST Room Availability.
3. On the Guest Room Search screen, select the Site the Guest will be staying.
4. Select the Availability option as the Room State to see available rooms. Select a card that will grant guest access. Use any additional filters to find a specific room/door you are looking for.
5. Select a Card under the Room you want to assign the Person to. This will create a new Person with the Credential selected already assigned to the Person. Provide the Person and Credential information as usual for adding a new Guest to the system.

Person Screen

1. Log into Aurora.
2. In the Main Menu, under Person, select either Add New Person or use the Manage People utility to search for an existing person.
3. In the Credential Information tab, select BEST as the Credential Type to add for the Person.
4. In the Card Format dialogue window, under the Create a Guest Card for a Room tab, select the Site the Guest will be staying.
5. Select the Available option as the Room State to see available rooms. Select a card that will grant guest access. Use any additional filters to find a specific room/door you are looking for.
6. Select a Card number under the Room you want to assign the Person to. This will create a new Person with the Credential you selected already assigned to the Person. This will close the window and return you to the person editing screen. Complete the process providing the Credential and Person information for the Guest.

Aurora thyssenkrupp Setup

Aurora 1.0.21.0 introduces thyssenkrupp virtual elevator integration with the Aurora software client.

Communication Server

The Communication Server allows the ECU to correspond with the Aurora software through a communication service (i.e. where the Communication Server is located).

1. Under the Application Management menu, select Application Utilities.
2. Select the Server Settings tab.
3. Select a Communication Server that will communicate with the CA150-EVTX panel. To add a new Communication Server, select the plus sign **+** on the top- left corner of the Communication Server sub menu. To modify an existing Communication Server, select the appropriate server from the drop-down menu.
4. Input the IP address of the thyssenkrupp server into the thyssenkrupp Host text box.

   Note: The Virtual Elevator Service will not attempt to communicate to any CA150-EVTX panel if this field is empty or if the information is incorrect.
5. Select the Save button.
6. Start the Virtual Elevator Service.

Adding a thyssenkrupp Panel

The next step is to add a CA150-EVTX panel to an Elevator Bank.

1. Under the Site Information menu, select Hardware Setup.
2. Select Virtual Elevators - thyssenkrupp Elevator Integration from the drop-down menu located at the top-left of the screen.
3. Select Yes to adding a CA150-EVTX panel.
4. Select an Elevator Bank associated with the CA150-EVTX panel being added. To add a new Elevator Bank, select the plus sign **+** on the top-left corner of the Elevator Bank sub menu. To modify an existing Elevator Bank, select the appropriate bank from the drop-down menu.
5. Fill out the following fields in the Information sub menu:
   - Name - Input a name for the ECU
   - Serial Number - Enter the ECU serial number, which can be found on the ECU board
   - Password - Input a strong password; the software client will need to be restarted for it to take effect
   - Type - This field will auto-populate with thyssenkrupp Elevator Integration and cannot be changed
   - Status - From the drop-down menu, select between Active, Disable, Inactive and Disaster Recovery
   - Regional Time Zone - Select the applicable Time Zone from the drop-down menu
   - Hardware Notes - Any additional notes, including maintenance notes, etc.
6. Under the Communication sub-menu, enter the IP Address programmed into the ECU. The default IP Address is 192.168.100.254 / 255.255.255.0
7. Select a Communication Server from the drop-down menu.

8. Select the Virtual Elevator Settings tab.
9. From each drop-down menu, select the Kiosk and Location of the Elevator Bank.
10. Select the Save button.

Group Access Levels

Next, Group Access Levels will need to be assigned.

1. Under the Manage People menu, select Group Access Levels.
2. Select the Elevator Group Access tab.
3. Select a Group under the Groups sub menu.
4. From the Access for Group sub menu, select applicable Floors by checking the box beside each. Opposite each Floor, select a Schedule from the drop-down menu. Select between Yes and No from the Destination Front and Destination Rear drop-down menus.

Property	Description
Group	Group that access will be assigned to
Floor	The floor the schedule will be assigned to
Schedule	Schedule assigned to the floor
Destination Front	**Yes** – Access to front when schedule is on **No** – No access to front when schedule is on
Destination Rear	**Yes** – Access to rear when schedule is on **No** – No access to rear when schedule is on

5. Select the Save button.

Schedule Assignment

The final step is to assign an Elevator Bank - Floor a Schedule to determine access.

1. Under the Site Information menu, select Schedule Assignment.
2. Select the Elevator Banks tab.
3. Select applicable Elevator Banks by checking the box beside each. Opposite each Elevator Bank and Floor, select a Schedule from the drop-down menu. Select between Yes and No from the Destination Front On Mode, Destination Front Off Mode, Destination Rear On Mode, and Destination Rear Off Mode drop-down menus.

Property	Description
Elevator Bank	The bank the floor is assigned to
Floor	The floor the schedule will be assigned to
Schedule	Schedule assigned to the floor
Destination Front On Mode	**Yes** – Access to front when schedule is on **No** – No access to front when schedule is on
Destination Front Off Mode	**Yes** – Access to front when schedule is off **No** – No access to front when schedule is off
Destination Rear On Mode	**Yes** – Access to rear when schedule is on **No** – No access to rear when schedule is on
Destination Rear Off Mode	**Yes** – Access to rear when schedule is off **No** – No access to rear when schedule is off

4. Select the Save button.

Mobile Credentials

Keyscan Mobile Credentials are used in conjunction with BLE-enabled wireless locks. The credential itself is hosted on a supported mobile device. Mobile credentials are set up to work with the Aurora software. Follow the steps outlined on this page to properly add a mobile credential to both the Aurora software and assign it to a Person within the company.

Application Utilities

First, an RSA key needs to be created and sent to your Dealer/Installer to order mobile credentials. Follow these steps to properly generate an RSA key and order mobile credentials:

1. Under the Settings menu, select Application Utilities.
2. In the Security tab, select the Create private RSA key button.
3. When a window pops up, select OK. The key begins generating in the background of the Aurora software (the amount of time will vary depending on the PC running the software). You may do other things within the software while the key is being generated in the background. No matter where you are in the software, a pop up window will appear when the key is created. Select OK.

   Note: Once the key is generated, it is recommended that you backup the database. Restoring an old database at this point will render the mobile credential file (the file sent back to you by your Dealer/Installer) useless. See the Related Topics at the bottom of this screen to follow steps to backup the database, under "Backup Now".
4. If you left the Application Utilities screen, return to that menu. Under the Security Tab, select Export public RSA key.
5. Save the file to any place on the PC that's easy to get to for future use. Select Save.
6. Email the newly saved RSA key to your Dealer/Installer to order mobile credentials. Your Dealer/Installer will send you back a Keyscan BLE Mobile Credential file.

   Note: The credential file sent back from your Dealer/Installer will only work with the database that originally created the RSA key. The file will not work with other databases.

Add Person/Edit Person

Next, a mobile credential needs to be assigned to a Person. Whether adding a new Person or editing an existing Person, the process is the same. Follow these steps to properly assign a mobile credential to a Person:

1. Under the Manage People menu, select either Manage People or Add Person (depending on your needs).
2. Under the Credential Information sub menu, select Add Keyscan Mobile Credential from the drop down menu.
3. Click on the Select credential from file button. A window will pop up. Select a Keyscan BLE Mobile Credential file from wherever you saved it (the file sent back to you by your Dealer/Installer). Select Open in the dialogue box.
4. Select the mobile credential that you want to assign to the Person (credentials in gray have already been assigned and cannot be selected again). Press the Select button.
5. The Batch and Card numbers will auto-populate. Assign Group Access and Temporary Options like normal. Select the Save button.
6. Once a mobile credential is assigned to a person, a Bluetooth icon appears beside the Print icon under the Credential Information sub menu. Click the Bluetooth icon button. A pop up window reads: "Select

which method you would like to use to send the registration key to the mobile phone". You can select either Send by email or Display on the screen. Press the Select button.

Note: In order to send the registration key via email, the SMTP settings must first be entered and the person's email must be registered. See the Related Topics at the bottom of this screen to follow steps to setup SMTP settings, under "SMTP Setup".

If you selected Display on screen, a pop up window will appear. The registration key is shown on screen, you can either write down the key or press the Copy button. Otherwise, select Close to exit the window.

Keyscan Mobile App

The final step to activating and using mobile credentials is to launch the Keyscan Mobile App and add a credential to your supported mobile device.

For detailed instructions on how to proceed, please visit: https://www.dormakaba.com/us-en/offering/products/electronic-access-data/high-frequency-readers-credentials/keyscan-mobile-credentials--ka_500239

Related Topics

SMTP Setup

Backup Now

KONE Integration Setup

This section only applies to those using KONE elevator systems. The KONE Communication Service must first be installed and running prior to interfacing with the Aurora software.

Hardware Setup

Follow these steps to properly set up KONE elevator systems within the Aurora software:

Note: Full KONE integration options will only become visible after completing these steps.

1. Under the Site Information menu, select Hardware Setup.
2. On the upper-left drop down menu, select Add KONE People Flow Elevator System Integration.
3. Click on the KONE Settings tab.
4. In the Type sub-field, select the drop down menu to choose between KONE DOP (outside the elevator cab) and KONE COP (inside the elevator cab).
5. In the Kiosk sub-field, select the drop down menu to choose the specific kiosk you wish to view.
6. In the Floor sub-field, select the drop down menu to choose the specific floor you wish to view.
7. In the Disconnected State sub-menu, select the plus sign [+]. Floor Number, Destination Front and Destination Rear will populate the table below. Click through the table to toggle between Yes and No for each field.
8. Once complete, select Save in the bottom-right corner of the screen.

KONE Mask Setup

Individual Masks

Follow these steps to set up individual masks for specific elevator modes and functions:

Note: Setting up individual masks will override any global mask previously set. Skip to the next section if you wish to set a global mask.

1. Under the Site Information menu, select Schedule Assignment.
2. Select Elevator Banks from the upper tab.
3. Destination Front on Mode, Destination Rear On Mode, Destination Front Off Mode and Destination Rear Off Mode are now visible. Click through the table to toggle between Yes and No for each field under these sub-sections.
4. Once complete, select Save in the bottom-right corner of the screen.

Global Mask

Follow these steps to set up a global mask for all elevator modes and functions:

Note: Global masks will be ignored if individual masks were set in the previous section. Remove all individual masks prior to setting up a global mask. Refer to the previous section if you wish to set individual masks.

1. Under the Site Information menu, select KONE Global Mask Setup.
2. Choose between DOP (outside the elevator cab) and COP (inside the elevator cab) in the top-left tab.

3. Under DOP, the Connect Mask and Disconnect Mask will house similar settings: Floor Number, Source Front, Source Rear, Destination Front and Destination Rear. Under COP, the following settings will appear: Floor Number, Destination Front and Destination Rear. Click through each table to toggle between Yes and No for each field.
4. Once complete, select Save in the bottom-right corner of the screen.

Application Utilities

In order to send individual/global masks and floor selections to specific IP addresses, certain parameters need to be set. Under the Settings menu, select Application Utilities. When utilizing KONE integration, the following sub-fields will appear in the Communication Server sub-menu:

- KONE Primary Host
- KONE Primary Port
- KONE Backup Host
- KONR Backup Port

Fill in the applicable fields then select Save in the bottom-right corner of the screen.

How to Register Aurora

You must register your Aurora software to be an authorized user. Only registered users are eligible for updates. You can register using either of the following methods:

- Telephone Registration
- Internet Registration

The procedures for each registration method are outlined below.

To open the Software Registration screen from the Client main screen, select the Settings button > Software Registration.

Trial Period

Keyscan offers a trial period of 30 days to review the software application. During the 30 days you are free to try the basic product; however the application ceases to function at the conclusion of the trial period. You must complete the top six fields under the Customer Contact Information and the Dealer Contact Information headings. These are required fields and must have entries before you can access the Aurora software. After completing the six fields, select the Save button in order to exit the Software Registration screen and view the Aurora software.

Delayed Registration

If you wish to register later, complete the Customer Contact Information and the Dealer Contact Information on the Software Registration screen. The top six fields under the Customer Contact Information and the Dealer Contact Information headings are required fields and must have entries before you can access the Aurora software. After completing the six fields, select the Save button to exit the Software Registration screen. The software must be registered within 30 days of installation.

Telephone Registration

Complete the Customer Contact Information and the Dealer Contact Information on the Software Registration screen. The top six fields under both the Customer Contact Information and the Dealer Contact Information headings are required fields.

Your software package includes a card with a registration serial number for each software module that you purchased. Select the Licenses tab at the top of the Software Registration screen and enter the serial numbers in the applicable License text boxes.

Have your machine key serial number, the registration software license numbers, and your company and dealer information available and call one of the Keyscan numbers listed below. A Keyscan representative will provide you with a corresponding unlock number for each purchased module to complete your registration.

Registration hours are from 9:00 AM to 5:00 PM, Eastern Time, Monday to Friday at the following numbers:

- 1.888.539.7226 - toll free Canada & USA
- + 1.905.430.7226 - elsewhere

Enter the applicable unlock number for each module purchased.

Select the **Register** button.



After entering your unlock serial numbers, ensure you click on the **Register** button before you exit the Software Registration screen.

Internet Registration

The PC you are registering from requires an Internet connection. Please note the Aurora software version number before you begin; it is a required entry when registering the software. The Aurora version is listed on the Client Software Registration screen. Also, you will need to know the Window's operating system running the Aurora software.

Steps

1. Log on to the Aurora Client. The Software Registration screen opens automatically until Aurora is registered.
2. Complete the customer and dealer details. The top 6 fields are mandatory.
3. Click on the Save button.
4. Select the Licenses tab and enter the applicable software licenses.
5. Click on the Save button.
6. Open your web browser and enter http://www.keyscanregistration.ca into the browser's address bar and press Enter on the keyboard.
7. From the Keyscan Registration web page, enter the client and dealer information in the respective fields.
8. Click on the Next >> button.
9. Minimize the Keyscan Registration web page.
10. Return to the Aurora Client and highlight the numbers in the Machine Key field. Right click on the highlighted numbers and select Copy from the pop-up menu.
11. Maximize the Keyscan Registration web page and insert the cursor in the Machine Key Serial Number text box. Right click and select Paste from the pop-up menu.
12. Click in the box below Software Version and select the Aurora version that you are registering.
13. Click in the box below Operating System and select the Windows OS running the Aurora software.
14. Enter the applicable Aurora software licenses in the respective module boxes.
15. Select the Next >> button.
16. Select the Next >> button.
17. From the Review screen ensure that the information you entered is correct. If you have made any mistakes, click on the corresponding Edit link. The cursor changes to a hand symbol when the mouse is positioned over the link. If the information is correct, click on the Register Software button.
18. From the *Thank you for taking the time to register your software* screen, highlight the first Unlock Code, right click and select Copy from the pop-up menu.
19. Maximize the Aurora Client Software Registration screen.
20. Click in the corresponding Unlock text box. Right click and select Paste from the pop-up menu.
21. Repeat for any additional unlock codes remaining in the Keyscan Registration web page *Thank you for taking the time to register your software*.
22. When you have completed entering all the required unlock codes in the Aurora Client Software Registration screen, **click the Register button**.
23. If any modules failed to register, contact Keyscan for registration assistance.
24. To close the Software Registration screen, click on the Back button until you have returned to the main screen.

How to Use the Help

The Aurora help is accessed by pressing the F1 function key on the keyboard.

The help is divided into two screens:

- Left screen - Contents/Search for navigating the help - accessed by clicking on the tab
- Right screen - Topic information, procedures, and links to related topics

Contents

Select the Contents tab for a full list of all the books and topics contained in the Aurora help.

-  double click on a closed book icon to open the list of topics
-  click on the topic icon to open the topic

Search

Select the Search tab to look for all topics that contain the word or phrase.

- Enter a word or phrase in the *Type in the keyword to find:* text box and click on the List Topics button

Procedures

-  indicates instructions, diagrams or explanations - click on the green text to open - to close, click on the green text again

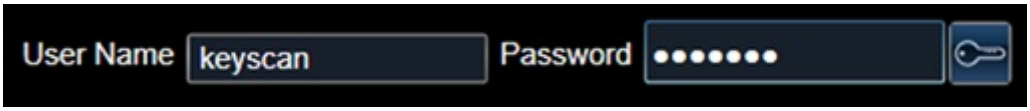
Related Topic Links

-  indicates a link to a related topic - click on the blue text to open the related topic

How to Log In

When Aurora is initially opened, you are presented with the log in screen. Only authorized system users can access Aurora, which safeguards the integrity of your Keyscan access control system.

The log on consists of entering a user name and password as illustrated in the example screen below.



Keyscan Generic Log In Account

When Aurora is first installed, Keyscan provides a default user account Keyscan with a Master designation. This account must be used to initially log in on the Aurora software for the first time to setup and configure your site. The Keyscan account User Name and Password are as follows:

- User Name: Keyscan
- Password: KEYSCAN (upper case characters)

To use the generic Keyscan account for logging on, enter the user name and password as shown above, and then select the key button to the right of the password text box.

You can continue logging on with this generic system user account. However, Keyscan recommends that you create specific system user accounts for each individual with responsibilities for monitoring and managing the access control system. Creating unique system user accounts ensures better security protocols since everyone is regulated by their specific permissions and you can audit user activity in the system log if anything questionable happens.

Note +

For instructions on creating your own specific system user log on accounts, review the information under Manage System Users.

Keyscan recommends that you write down your user name and password and keep it in a safe place.

Language Selection

Aurora is available in one of three language interfaces:

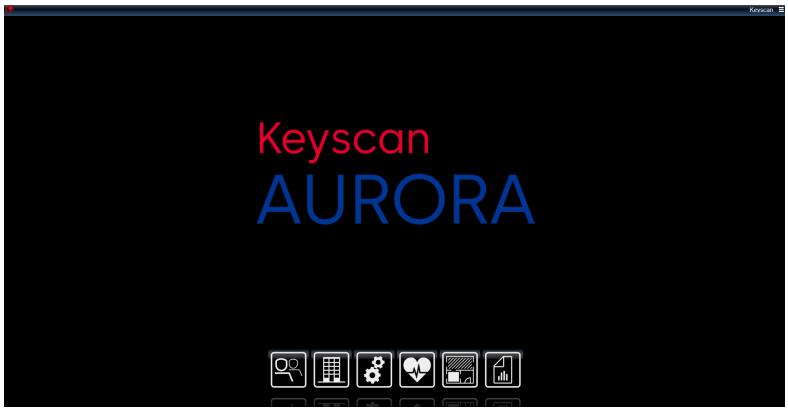
- English
- Français (French)
- Español (Spanish)

To change the Aurora interface to another language, login with your Keyscan user name and password, click on the icon with the three bars in the upper right corner of the Aurora screen. Position the cursor over Switch language, and select the desired language from the fly-out menu. Aurora retains the language preference on subsequent logins for the Keyscan user account. The language preference also applies when logging in on the Aurora WEB Client.

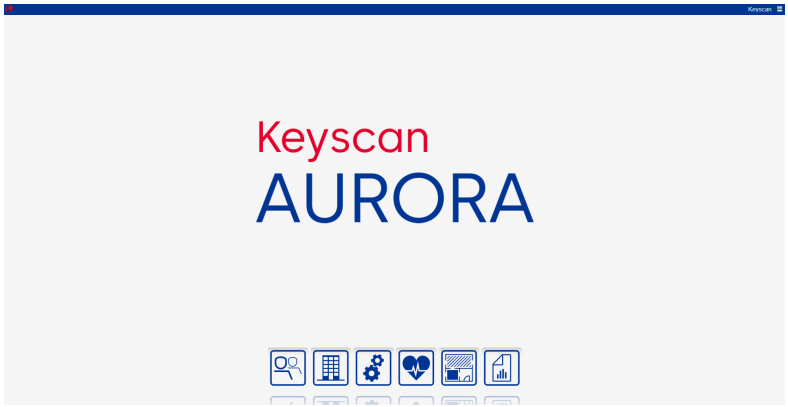
Appearance

The appearance of the Aurora screen can be set to one of the following styles:

- Default - The screens will have the standard black/dark appearance with the menu buttons appearing black with white outlines and images.



- Light Blue - The screens will have a white and blue appearance with the menu buttons appearing white with blue outlines and images.



To change the Appearance of Aurora, login with your Keyscan user name and password, click on the icon with the three bars in the upper right corner of the Aurora screen. Position the cursor over Appearance, and select the desired appearance mode from the fly-out menu. Aurora retains the Appearance preference on subsequent logins for the Keyscan user account. It also applies when logging in on the Aurora WEB Client.

Domain/Local Log In User Name & Password

If your Aurora user account has been configured as domain or local under Login Information, then you are exempted from logging on to Aurora provided you have logged on to Windows with either your domain or local user name and password.

Note domain and local log on are optional features that require the purchase of an Active Directory license.

Procedure

Steps to Log On

1. Open Aurora.
2. Click in the User Name text box and enter your Keyscan user name.
3. Press the tab key.
4. Enter your Keyscan password.
5. Press the logon key button to open Aurora's main interface screen.

Related Topics

Manage System User Accounts

Back Button / Navigation History

Aurora allows you to navigate from one screen to any other screen by merely selecting any function from the menu buttons at the bottom. However you may also use the Back button or the navigation history button for navigation within Aurora as outlined.

Back Button

The Back button acts in a similar manner as on a web browser; each time you select the Back button you are returned to the previously viewed screen.

Navigation History

Aurora keeps track of previously viewed screens during your current login session. Rather than selecting the Back button, which returns you to the previous screen, selecting the Navigation History button  presents a drop down list of the most recently viewed screens. Acting as a shortcut, Aurora returns you directly to the selected interface screen.

Aurora clears the navigation history list of any screens that you viewed after your selection.

Back & Navigation History buttons



Aurora Icons & Symbols

Throughout the Aurora interface screens, you will see the following symbols. Each symbol is explained below.

Symbol	What Is It	How To Use It
	Open Symbol	Indicates hidden settings or commands Position the cursor over the Open symbol and click to reveal
	Close Symbol	Position the cursor over the Close symbol and click to hide the settings or commands
	Selectable Option - Disabled	Clicking in the box alternately selects - has an x - or de-selects - has no x - on each subsequent click
	Selectable Option - Enabled	
	Selectable Option - Partially Enabled	This symbol indicates that only some sub-functions have been enabled
	Non-Selectable Option - Disabled	Non-selectable options are governed by other selectable options or other settings and cannot be manually changed
	Non-Selectable Option - Enabled	
	Drop Down List	Position the cursor over the arrow and click to open the drop down list
	Delete Button	Position the cursor over the delete button to erase the current selection
	Expand	Position the cursor over the + symbol and click to open the hidden fields or content
	Collapse	Position the cursor over the – symbol and click to close the fields or content
	Next	Position the cursor over the > symbol and click to advance to the next record or file
	Previous	Position the cursor over the < symbol to go back to the previous record or file
	Radio Button - Option Selected	Clicking in the radio button alternately selects - has a green dot - or de-selects - has no green dot - on each subsequent click
	Radio Button - Option Not selected	

	Date & Time Selection	Position the cursor over the icon and click to open the calendar and time selector. Use the arrows to scroll back or forward in the calendar
	Date Selection	Position the cursor over the calendar and click to open. Use the arrows to scroll back or forward in the calendar

Re-organizing Column Data

Throughout Aurora, the interface screens that present data input by system users can be re-organized. Clicking on a header changes the order of how the rows in the column are presented on-screen. With successive clicks the heading changes from A to Z / low to high; Z to A / high to low; and then back to the original order.

The illustration below shows a Name heading in which the names would be listed from A to Z.

Column Heading with A - Z selected



The symbols below indicate how the rows of data are organized:

- displays rows alphabetically from A to Z or numerically lowest to highest
- displays rows alphabetically from Z to A or numerically highest to lowest
- No symbol - displays the original list order

Heading Search Filter

Throughout Aurora's interface screens, many of the data field headings have a user-selectable search filter indicated by the search icon as shown in the illustration.

Search Icon on Column Headings



Clicking on the search icon opens the search filter dialog box. Relative to the heading selected, the search filter dialog box displays the following search fields:

- Select All - if enabled, selects all listed entries under the heading
- Select Individual Entries - listed data can be selected individually
- Show rows with value that - select the ▼ symbol opposite Is Equal to open the drop down list of available search filters as outlined below in the table
- aA (Match Case) - select to have search locate entries with matching upper and lower case characters
- And / Or - for a compound search using two search modes with an and / or condition attached to the search - the second or lower search mode must also be engaged for the search
- Filter - select to initiate the search - the search icon changes to yellow indicating the search filter has been applied
- Clear Filter - select to clear the previous search and restore the screen to its original list - the search icon changes to white indicating the search filter has been cleared
- X - closes the search filter dialog box

The following table outlines the search modes with an explanation and an example. The examples are based on performing a search for readers in the Group Access Levels screen. Remember, the search is relative to the entries found under the selected column.

The filters *Is contained in* to *Is not null* do not apply to searches for Aurora headings.

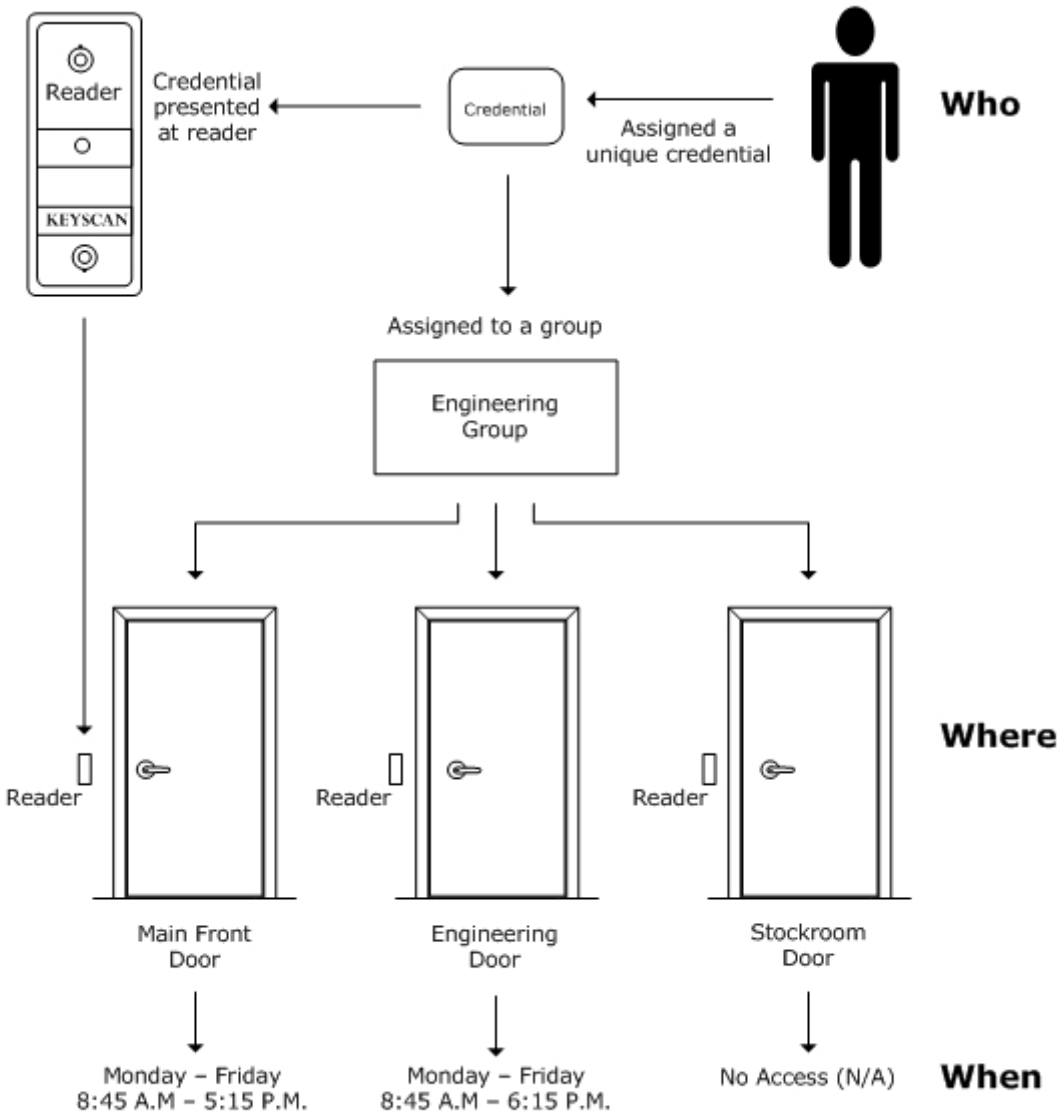
Search Modes	Explanation	Example Search Query
Is equal to	Searches for all the same entries under the heading as specified	Look for reader - Laboratory (In) Select: Is equal to / Enter: Laboratory (In) Lists reader - Laboratory (In)
Is not equal to	Searches for all the entries under the heading that are not as specified	Look for readers other than - Laboratory (In) Select: Is not equal to / Enter: Laboratory (In) Lists readers other than Laboratory (In)
Starts with	Searches for all the same entries under the heading that start with the specified character or value	Look for readers that start with - M Select: Starts with / Enter: M Lists readers that start with - M

Ends with	Searches for all the same entries under the heading that end with the specified character or value	Look for readers ending with the letter - y Select: Ends with / Enter: y Lists readers that end with the letter - y
Contains	Searches for all the same entries under the heading that contain the specified character or value	Look for readers that contain the letter - b Select: Contains / Enter: b Lists readers that contain the letter - b
Does not contain	Searches for all the same entries under the heading that do not contain the specified character or value	Look for readers that do not contain the letter - b Select: Does not contain / Enter: b Lists readers that do not contain the letter - b

What is Access Control?

Electronic access control is based primarily on - WHO, WHERE, and WHEN. Bearing this in mind, an electronic access control system regulates who may access specific doors or other types of entry points, such as parking gates, or elevators at specified times.

Authorized individuals are recognized by a credential, which could be a card, token, biometric characteristic, or personal identification number (PIN). Some older forms of credentials which are still in use include cards with magnetic stripes or bar codes. Acting as a sort of passport, each credential has a unique marker for individual identity. To gain access at a controlled door or entry point, the credential is presented at a reader. Acting like a silent sentry, the access control system grants access or denies access based on programmed settings for the credential. Called a transaction, each instance of attempted access, whether access is granted or denied, is recorded to a dedicated access control database. This database provides a source of records for auditing site activity and security information.



Access granted or access denied based on who – where – when.

Who

In the Aurora software, persons accessing doors or some form of barrier regulated by the access control system represent the who part of the above illustration. Each individual is identified with a personal record including a

unique credential in the Aurora software. Each individual is assigned to a group or possibly multiple groups depending on access requirements. Groups, in turn, are assigned access levels.

Where

When the access control system was installed, your dealer/installer configured the doors with readers and electric locking devices. These doors or entry portals are now under the control of the access control system. The Client software provides full control over where individuals may go based on regulating access to these doors.

When

In the Client software, you establish when groups are permitted access by creating what are called schedules. These schedules - the when part of the illustration - combined with the where and who are the basic elements for controlling access.

Related Topic

How Access Control Works

How Access Control Works

An access control system is an inter-connected group of components that operate as a collective entity.

- access control software - Client, database, communication manager
- server/workstation
- credential - such as proximity card, or tag, PIN, biometric characteristic etc.,
- reader
- electric lock hardware
- door contacts
- access control unit (ACU)

Electronic access control works in a rapid sequence of events between all the components. In the example, we'll use a door as the controlled entry point and breakdown events when someone tries to gain access.

The credential is presented to a reader

The reader, which is positioned near the door, acts as the system's sentinel. To gain access at a controlled door, authorized individuals identify themselves by presenting their credential to the reader. When this happens the reader scans the identity of the credential.

The reader transmits the credential's identity to the control unit

After the reader has scanned the credential, it transmits the credential's unique information to the access control unit (ACU). After receiving the transmitted reader data, the ACU's on-board processor validates whether the credential has authority to access this particular door at this particular time.

The control unit releases the locking device

Once the ACU's on-board processor has validated the identity of the credential, the control unit releases the locking device and the individual can enter. The door automatically re-locks when the door closes.

If the credential was not valid for the door or the time period, which is called a schedule in the access control software, the door would remain locked. The attempted access, however, would be transmitted and recorded to the system database as an "Access Denied" transaction.

Basic Site Setup Procedures

After installing the Aurora software, the next task is to set up your site. This involves entering data on the software screens that are accessed from the menus on the Client's main screen. The hardware components installed at your site and the software features you elect to use ultimately determine which screens you need to complete. In some cases, you may require the assistance of your dealer/installer to configure the access control units, as well as any inputs and outputs connected to external devices. Below are links to the help topics that will instruct you on getting the basic functions of your Keyscan access control system up and running.

Links to Basic Setup Topics

Link	What It Does
Create a Site	Creates a name for the site and describes the site's physical location so as to define the access control system as an entity
Configure Aurora for E-mail	Configures Aurora's SMTP e-mail function for broadcasting event messages, including alarms, to external addresses; requires an IT administrator for mail server protocols
Add the Access Control Units	Identifies the access control units and configures communication settings; may require dealer/assistance (for elevator control units, click on the link below)
Setup Doors and Readers	Identifies and configures the doors and their associated readers connected to the access control units; may require dealer/installer assistance
Setup Elevators	Identifies the elevator control units, names elevator banks and floors and sets other elevator properties
Create Schedules	Creates schedules to govern time periods for access, arming and disarming input devices, such as motion sensors, and regulating when other system connected components are automatically turned on and off
Setup Groups	Create group names and associated properties; individuals issued credentials must be assigned to at least one group for access
Create Access Levels	Creates access levels at all system controlled doors by group assignments
Setup System Users	Creates individual login accounts for persons designated to view and operate the Aurora software; you may also use the generic default Keyscan account
Add Credential Records	Creates records to identify all individuals with their pertinent information for interaction with the access control system
Backup Now	Makes a backup copy of the access control data that has just been entered so the information is saved in a backup file
Schedule Database Backups	Sets a schedule so Aurora automatically backs up all your access control data at regular intervals so the backup database file is constantly kept up-to-date

Supplementary Features

Aurora is a comprehensive access control management software application richly endowed with many supplementary features and tools which are not covered in the topics for a basic setup. After you have completed the basic setup, Keyscan suggests you take some time and review the content outlined in the help and discover all the many gems Aurora has to offer.

Visitor Management

Event Setup

Global Card Template Editor

Are You Unfamiliar with Access Control?

If you are unfamiliar with access control and how it works, before you attempt to set up the system, click on the link below for a basic outline of how access control functions.

What Is Access Control?

How Do I...?

The following is a list of common questions that end-users ask when either setting up or operating their Keyscan access control system. Each question links you with the help topic.

Alarms

... create alarm response instructions?

... respond to an alarm?

Anti-Pass Back

... set anti-pass back at readers?

Credentials

... assign a new credential?

... cancel a lost or stolen credential?

... set a credential for temporary usage?

... find credential records?

... set up optional fields?

... attach a photo to a person's record?

Doors

... see if a door is locked or unlocked?

... momentarily unlock a door?

... set a door to automatically unlock by a schedule?

Elevators

... setup elevators?

Groups

... make a group?

.... assign an access level for a group?

Online Transactions

...view online transactions?

Photo ID Badges

... print photo ID badges?

... make photo ID badge templates?

Reports

... how do I run a report?

Readers

... set readers for monitoring in and out access?...

Schedules

... create a schedule?

System Users

... add a system user?

... delete a system user?

What is a Site?

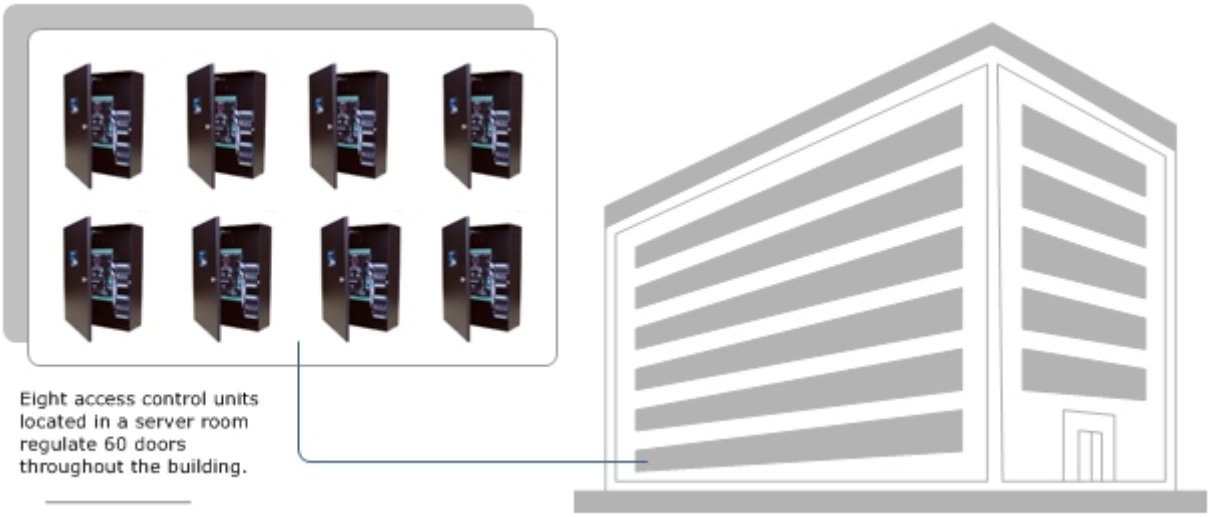
In the Client software, a site is merely a way to identify a group of access control units within a physical location.

With access control there can be many variations: several sites may exist within one building, or one site may include several buildings. It depends on how the access control system is configured for regulating access within your physical structure or structures.

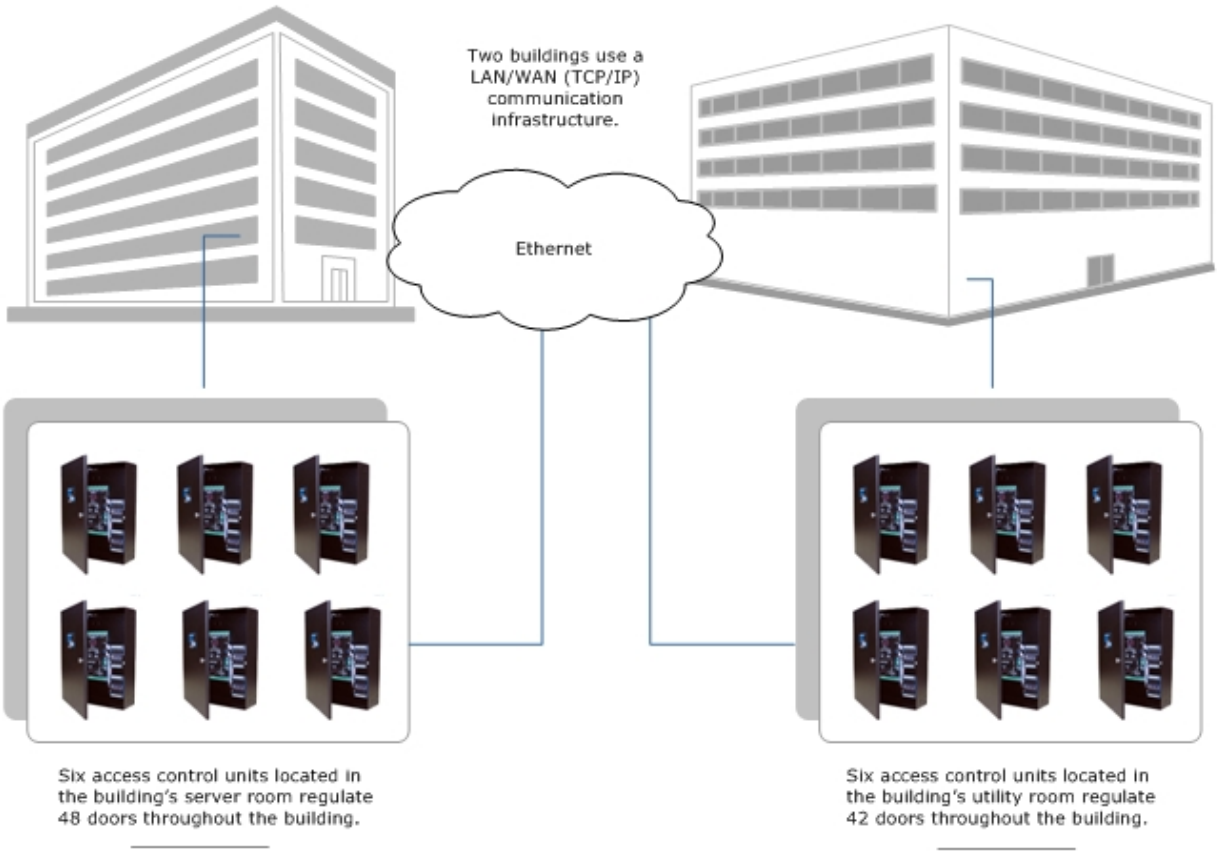
The following three illustrations show different site configurations.

Examples

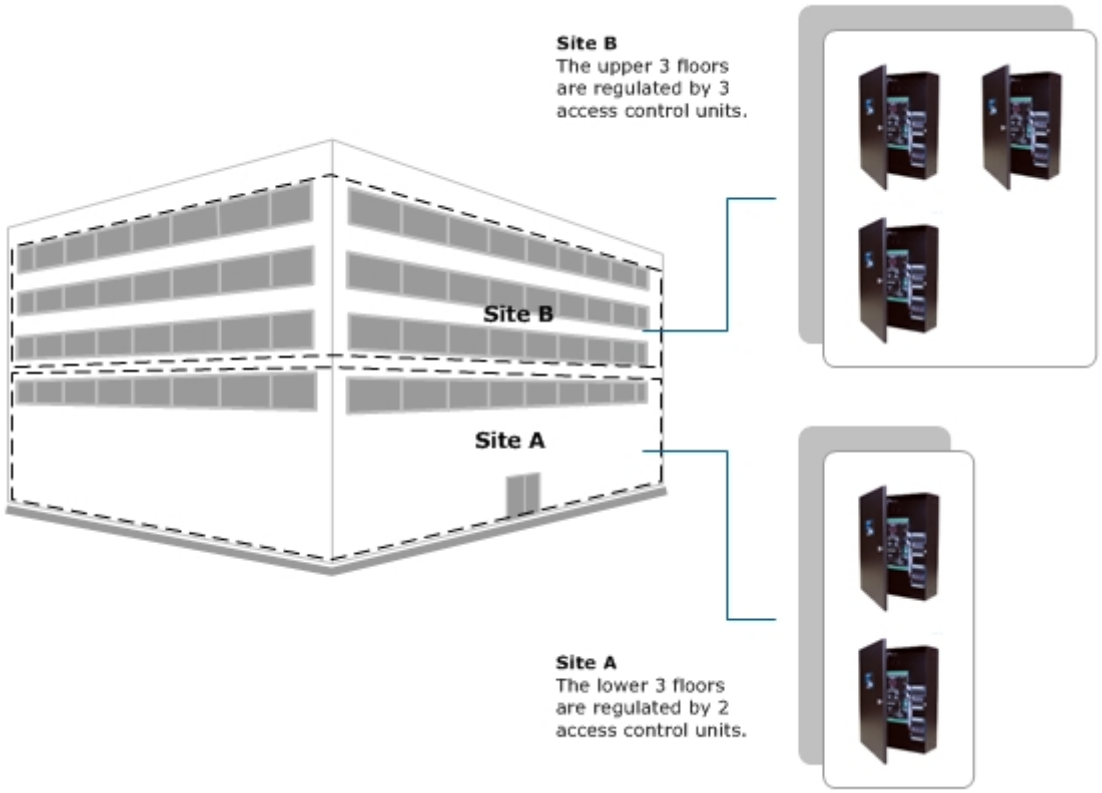
- *One Site - One Building*



- *One Site - Two Buildings*



- *Two Sites - One Building*



Site Directory (Site Information Setup)

When you access the Site Information Setup menu, the first screen to open is the Site Search - Site Setup directory screen. Whether creating a new site or amending information on an existing site, the Site Search - Site Setup directory screen allows performing the following tasks:

- view all sites
- create a new site
- access a specific site to edit site information
- delete a site

Procedures

- To create a new site, select the Add Site button to open the Site Setup screens
- To open an existing site, double click on the site name in the list
- To delete a site, click on the Delete button.

Related Topics

 Name and Define a Site

Name & Define a Site

The Site Information Setup screen identifies a site by name and location. This includes the following fields and switches:

- Name - enter a name that identifies the site such as company name or other description that would be recognized by all system users
- Description/Site Notes - should include details such as an address or other information that is supplementary and supports the site name field
- Default Credential Type - this default credential type will be automatically selected in the Edit Person screen when adding a new credential to that Person for that specified site
- Default Group Access - sets the default access level - no access or 24HR (24 hour access) - for all newly added panels in all applicable schedule related screens until they are manually changed by system users
    - Keyscan recommends that you leave the default schedule set on no access so that all doors, elevators, access levels, and devices are secure until you have reviewed your site and determined schedule assignments
- Reset Anti-Pass Back - in a controlled enter/exit environment where the anti-pass back option is in effect, the access control system maintains an IN or OUT status for all credentials. When anti-pass back is reset, the IN/OUT status is cleared and the credentials may be used at IN or OUT readers on their next reader presentation before they are again governed by the IN/OUT anti-pass back protocol. The Reset Anti-Pass Back option has selectable one hour time intervals from 12 AM to 6 AM at which time the Aurora software automatically clears the anti-pass back status. (Not Set disengages the auto reset option. Aurora also has a manual Reset Anti-pass Back option which is accessed from the Status button.)
- E-Plex Master Credential - to only be used with E-Plex 7900-series of wireless locks. To add a master credential, select the plus sign **+**, fill in the required information and select OK. To delete a master credential, select the trash bin icon.
- E-Plex Master PIN - this PIN number will be used to add E-Plex wireless locks to that specified site. This number must be entered numerically
- Active Directory Agent - enables the Aurora software for integration with MS Active Directory; requires an optional Keyscan Active Directory License (AUR750)
- Enable 90,000 Credential Support - sets the Aurora software for compatibility with M series control boards which have 90k credential capacity (M series control boards are a custom order)
    - once enabled, the Enable 90,000 Credential Support field cannot be de-selected
- Polling Suspended - this function should not be enabled as it stops communication with the access control units; it should only be used by your dealer/installer for troubleshooting or maintenance procedures
- Additional Users Assigned to Site - this enables the user to view and/or edit users responsible for managing a site

Custom Site Unique Identifier

The Aurora software client can be configured to use unique Custom Site Unique Identifiers to help integrators identify sites in Aurora that match sites in other systems. Also, users have an option to indicate whether or not the Custom Site Unique Identifier field is required. Custom Person Unique Identifiers become searchable criteria once configured in the software.

To set up a Custom Site Unique Identifier, first go to Application Utilities under the Application Management menu. Select the Advanced tab and check the box beside Custom Site Unique Identifier. Fill in the Custom Site Identifier Label field and check the box beside Is Required and/or Display In Name (as your needs require). Select the Save button on the bottom-right corner of the screen.

Upon returning to the Site Information Setup screen, the Custom Site Unique Identifier will now appear above the site Name. If Is Required was selected, the Custom Site Unique Identifier becomes a mandatory field and cannot be saved unless filled out.

Site Notes Popup

The Site Notes Popup feature allows the user to supply Site Notes in the Site Information screen. If Site Notes are supplied for a site, and a user is only working with that site, the Site Notes will pop up as soon as they are using the site. To enable this feature, select Application Utilities under the Settings menu. Select the Advanced tab at the top of the screen. There, you will see the CMAC Features sub menu on the right of the screen. Select the check box beside CMAC Features and the box beside Use Site Notes Popup. Select the Save button on the bottom-right of the screen.

Upon returning to the Site Information Setup screen, the Custom Site Notes Popup field will now appear above the Default Group Access. Fill in the Custom Site Notes Popup field and select the Save button. Every time a user is only working with that site, the popup message will appear.

Site Building Image

The Site Information Setup screen allows placing an image of the site building if desired. The image is inserted on the left side of the screen in place of the building silhouette.

On a New Aurora Installation

If you have just installed Aurora, when you first access the Site Information setup directory screen, Aurora has a default Keyscan Site. Keyscan recommends that you simply rename the Keyscan Site to the name of your company or organization. To do this, follow the Modify a Site procedures below by double clicking on the Keyscan Site, change the Name field by selecting the text, press the Delete key and then re-enter the desired name. Set the other fields as explained above.

Site Name Structure

In cases where the access control installation will involve setting up multiple sites, either now or in the future, it is important to use concise and consistent naming conventions for the site names. This will make it easier for other system users logging on the desired site or determine the source of an alarm.

Procedures

Steps to Add a Site

1. From the Client main screen, select the Site Management button > Site Information Setup.
2. From the Site Information Setup screen, select the Add Site button.
3. From the Site Information Setup screen, complete the information required for each applicable field as described above.
4. To add an image of the site building, click on the + symbol below the building silhouette.
5. From the Open dialog box, navigate to the folder with the image.
6. Select the image, and click on the Open button.
7. From the Image Editor, click on the save icon.
    - You can use the Image Editor tools to make alterations to the image. For more about the Image Editor, select the link below Related Topics below.
8. Select the Save button.

Steps to Modify a Site

1. From the Client main screen, select the Site Management button > Site Information Setup.

2. From the Site Information Setup screen, double click on the site you are amending.
3. From the Site Information Setup screen, revise the information in the applicable fields.
4. Select the Save button.

Steps to Delete a Site

Before you can delete a site, your system user account must have permission to delete sites. You cannot be logged in to the site you are attempting to delete. When you delete a site you will erase all site data including credential records.

1. From the Client main screen, select the Site Management button > Site Information Setup.
2. Select the delete icon to the right.
3. From the Delete Site prompt, select the Yes button.

Related Topics

What is a Site?

Site Setup Report

Active Directory

Image Editor

Bypass Password Reset Requirement For New Users

By default, Aurora requires new Users to reset their passwords after initial login. This requirement can be bypassed using either the Application Utilities or User Preferences screens.

Procedure

Steps to Bypass the Password Requirement for New Users

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. On the Application Settings tab, below the User Settings heading, click on the checkbox next to "Bypass password reset requirement for new users" so that an x is visible > [x] this will bypass the password reset requirement.
3. Click on the Save button.
4. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Change a System User's Password

System User Types

User Preferences

SMTP Setup - Alarm and Message E-mail

If you intend to use Aurora's e-mail functions, such as sending alarm messages, the SMTP Setup interface screen must be configured and enabled so as to route Aurora's e-mail through a mail server or exchange server. This task must be performed by the IT department, since settings are based on established mail server protocols.

Procedures

Steps to Setup SMTP

1. From the Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Server Settings tab is selected.
3. Under the SMTP heading, enter the SMTP e-mail server address in the Host text box.
4. Enter the port number in the Port text box.
5. In the Time out (Milliseconds), enter a value (1000 = 1 second) that exceeds the normal amount of time to access the server. If the time to access the server is less than that specified in the time out text box, the Client will abort the request to send the e-mail.
6. In the From text box, enter the sender's address that appears in the From line of the e-mail.
7. If the mail server requires SMTP/TLS enabled, ensure the box to the right of this field has an X. The box has an x when this option is activated.
8. If the mail server requires Use non-default, ensure this function is enabled which is indicated by an x in the box to the right.
9. In the Credential Type, select the appropriate authentication type specified by the Internet Service Provider.
10. In the User Name text box, enter the authorized log in name.
11. In the Password text box, enter the password.
12. Click on the Save button.
    - If you have made any errors, click on the waste bin icon along the SMTP header to clear the fields, and then re-enter the correct settings.
13. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Test Settings

1. After completing the above procedures, to test the SMTP settings, enter a valid e-mail address to receive the test message in the E-mail To text box.
2. Select the Send E-mail button.
3. Verify the e-mail was received; otherwise, check your SMTP settings.

Communication Server Setup

The Communication Server is located in the Application Utilities menu, under the Server Settings tab. The Communication Server allows an ACU/ECU to correspond with the Aurora software through a communication service (i.e. where the Communication Server is located).

Adding or Modifying a Communication Server

To add a new Communication Server, press the plus sign **+** on the top right corner of the Communication Server sub menu. To modify an existing Communication Server, select the appropriate server from the drop down menu. For either application, the transaction fields are the same and are as follows:

- Host - This is the local computer name or IP address of the Communication Server. This name can be changed and specified.
- Listening Port - If using Reverse Networking, this is the port for incoming connections from panels. The port number is auto-populated to a default number, but it can be changed and specified.
- Encryption Type - Choose between AES 128-bit, AES 192-bit, AES 256-bit encryption types. For higher security, we recommend using the AES 256-bit option.
- Encryption Key - Enter an encryption key to be used during communications. Valid characters for the encryption key are as follows: A-F and 0-9.
- Keep Package History - Place an x in this box to keep the server packages for all of the communication panels on this server. This will retain server packages for up to 24 hours, allowing SDK users the ability to check the status of device commands (lock, unlock, pulse, etc.). Server packages that are more than 24 hours old will be deleted daily at 4 am. If this box is unchecked, no package history will be stored.
- Output File Path - Select a file on the PC running the Communication Server to insert transactions into.
- UDP Remote Host - Enter the IP address of the PC listening for the data stream.
- UDP Remote Port - Enter the IP of the port from the UDP Remote Host.
- UDP Local Host - Enter the IP of the PC running the Aurora software.
- UDP Local Port - Enter the IP of the port from the UDP Local Host.
- KONE Primary Host - Enter the IP of the PC running the Aurora software hosting KONE services.
- KONE Primary Port - Enter the IP of the port from the KONE Primary Host.
- KONE Backup Host - Enter the IP of the PC running a backup of the KONE communication service.
- KONE Backup Port - Enter the IP of the port from the KONE backup port.
- thyssenkrup Host - Enter the IP address of the thyssenkrump server

After filling in all the applicable fields, press Save on the bottom right of the screen to complete the Communication Server setup.

Related Topics

- KONE Integration
- UDP Output

CORPORATE ID

If using HID Corporate cards, the corporate ID must be entered in the Application Utilities screen. The ID number is identified on the package of cards. If you do not use HID Corporate cards leave this field blank.

Procedure

Steps to Enroll the HID Corporate ID

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Enter the number in the Corporate ID (Hex) field under Application Settings.
4. Click on the Save Button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Logging Level

The Aurora database captures all system activity including all system user interaction. This includes recording almost everything that a system user does from the time of logging on to the time of logging off. Aurora has a Logging Level function which determines the type of details - basic or enhanced - captured by the system log for system user activity.

- Basic - lists that the system user changed a setting
- Enhanced - lists that a system user changed a setting and the details of the change

Procedure

Steps to Change the Logging Level

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Below the Application Settings heading, click on the symbol to the right of the Logging Level box and select the preferred setting from the drop down list.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Complex Passwords

Aurora's Enforce Complex Password function compels the use of more sophisticated passwords should elevated security be required for system user software access. Complex passwords lessen the chance of an unauthorized individual accessing the Aurora software. In order to institute complex passwords, you must enable the Enforce Complex Passwords function under the Application Settings heading in the Application Utilities screen.

If complex passwords are enabled, then all passwords must conform to the following conventions:

- contain at least one upper case alpha character
- contain at least one lower case alpha character
- contain at least one numeric character from 0 to 9
- contain at least one other character which is a non-alpha or non-numeric character - a space is considered a character
- contain a minimum of 6 characters in the password

You may also specify how many days the password is valid after which it expires and the system user must create a new password to log on. The Password Expiry function is also set under the Application Settings heading in the Application Utilities screen.

Any system user account with a non-complex password created prior to enabling the Enforce Complex Password function will be prompted on the next login to change his or her password which must conform to the complex password format.



Once the Enforce Complex Password has been checked and the Application Utilities screen is saved, you cannot disable the Enforce Complex Password function.

Once the Enforce Complex Password has been checked and the Application Utilities screen is saved, you cannot disable the Enforce Complex Password function.

Enabling the Enforce Complex Passwords function requires a system user account with a Master designation.

Procedure

Steps to Enable Complex Passwords

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Below the Application Settings heading, click in the box to the left of Enforce Complex Passwords. The box has an x when enabled.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

System User Types

Auto Delete on Expiry

The Auto Delete on Expiry function applies to all credentials that have been assigned a temporary date range in the Edit Person screen. This function does not apply to the Limited # Uses temporary option.

The function has the following settings:

- Not Used - the function is disabled
- Remove Credential from Site - the credential cannot be used after the expiry period but is not deleted
- Delete Credential - the credential is deleted from the site where the temporary dates apply
- Delete Person - the person's record is deleted

With the Delete Credential and Delete Person options, if the temporary date is set on an expiration time before midnight, the credential or the person's record are deactivated in the Aurora database and then deleted at midnight by the Aurora Agent.

Procedures

Steps to Set Auto Delete on Expiry

1. From the Client main screen, select the Settings button > Application Utilities.
    - The settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Opposite Auto Delete on Expiry, click on the ▼ symbol and select the desired option from the list.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Create a Temporary Credential

Password Expiry

Aurora has a Password Expiry option in which you may force all Aurora system users to change their passwords after a specified interval has elapsed. When a system user logs in following the expiry period, the Aurora software prompts the individual that his or her current password has expired and it must be changed.

Note +

If you set a password expiry period and no longer require one at a later date, change the setting to Not Used, which disables the function.

The system user account must have a Master designation for setting the Password Expiry function.

Procedure

Steps to Set the Password Expiry Option

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. Below the Application Settings heading, click on the symbol ▼ opposite Password Expiry (days), and select an expiry period from the list.
    - Not Used disables the Password Expiry function
3. Click on the Save button.
4. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Change a System User's Password

System User Types

KABA INTEGRATED MODE

The Kaba Integrated Mode allows configuring the Aurora software and the access control units for integration with Kaba readers, specifically Kaba SR series readers. When enabled, the Kaba Integrated Mode applies to all sites.

Note + This mode should only be enabled if you have Kaba SR series readers connected to the Keyscan access control units.

In conjunction with the Kaba Integrated Mode switch on the Application Settings screen, you must also specify the Kaba Integrated 17-byte reader format, which is reference # S in the Reader Format table.

- Reader formats for CA250B, CA4500B, CA8500B, EC1500B or EC2500B control boards are set from the Hardware Setup > Additional Settings screen as outlined in the procedures below.
- If using a CA150 single door access control unit, the reader format must be set on the control board with DIP switches S2.1 to S2.6. Refer to the CA150 Installation Guide or the Specifications/Settings insert, included with the CA150 control unit, for settings.

Procedures

Steps to Enable Kaba Integrated Mode

1. From the Client main screen, select the Settings button > Application Utilities.
    - The settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Below the Application Settings heading, click on the box to the left of Kaba Integrated Mode. The box has an x when this option is selected.
4. From the Kaba Integrated Mode prompt, ensure you understand that once you save the Application Utilities settings you cannot switch the Kaba Integrated mode off. To continue, click on the Yes button.
5. Click on the Save button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.
7. If you have not previously configured the access control units or specified the Kaba Integrated Mode reader format, from the main screen select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site name in the site directory screen.
8. Do one of the following steps depending the circumstances:
    - If you have not configured the access control units in the Hardware Setup screens, first add the units and complete all the necessary settings including the Kaba Integrated 17- byte reader format which is set in the Additional Settings screen. For assistance, press the F1 key and review the help contents under Hardware Setup & Maintenance.
    - If you only need to set the Kaba Integrated 17-byte reader format for each control unit, ensure the All Hardware tab is selected and double click on the first access control unit; select the Additional Settings tab; click on the symbol on the right of Reader Format and select Ref # S - Kaba Integrated 17-byte from the list.
    - If you have a CA150, you must set the reader format at the control board with the DIP switches S2.1 to S2.6 as outlined in the CA150 Installation Guide.
9. Click on the Save button.
10. Repeat setting the reader format for all other access control units.

11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Reader Formats

Enable Keyscan Credentials for Extended Card Format

Setting the Enable Keyscan Credentials for Extended Card Format allows Keyscan's proprietary 36-bit card format to be integrated with other card configurations, as outlined in the Reader Formats table. See Related Topics Below for more information. The Enable Keyscan Credentials for Extended Card Format setting applies to all sites.

When you activate the Enable Keyscan Credentials for Extended Card Format function, Keyscan 36-bit credentials can be presented at readers for access as well as the credentials that apply to the selected extended card format.

- Reader formats for CA250B, CA4500B, CA8500B, EC1500B or EC2500B control boards are set from the Hardware Setup > Additional Settings screen as outlined in the procedures below.
- If using a CA150 single door access control unit, the reader format must be set on the control board with DIP switches S2.1 to S2.6. Refer to the CA150 Installation Guide for settings.
- Enable Keyscan Credentials for Extended Card Format is a global setting when checked, meaning it is enabled for all sites. When enabling this feature, ensure that all sites are set to the correct extended formats (see Reader Formats).

Procedure

Steps to Enable Keyscan Credentials for Extended Card Format

1. From the Client main screen, select the Settings button > Application Utilities.
    - The settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Below the Application Settings heading, click on the box to the left of Enable Keyscan Credentials for Extended Card Format. The box has an x when this option is selected.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.
6. If you have not previously configured the access control units or set the extended reader format for the access control units, from the main screen select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site name in the site directory screen.
7. Do one of the following steps depending the circumstances:
    - If you have not configured the access control units in the Hardware Setup screens, first add the units and complete all the necessary settings including the reader format which is set from the Additional Settings screen. For assistance, press the F1 key and review the help under Hardware Setup & Maintenance.
    - If you only need to set the reader format for each control unit, ensure the All Hardware tab is selected and double click on the first access control unit; select the Additional Settings tab; click on the symbol on the right of Reader Format and select the extended format ref# B to R from the list.
    - If you have a CA150, you must set the reader format at the control board with the DIP switches S2.1 to S2.6 as outlined in the CA150 Installation Guide.
8. Click on the Save button.

9. Repeat setting the reader format for all other access control units.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Reader Formats

Allowed Login Attempts

Aurora has an Allowed Login Attempts function in the Application Utilities screen that restricts the number of times someone may try logging in. Restricting the number of login attempts precludes an unauthorized person from continually entering random passwords and possibly, by chance, getting one right. Placing a limit on the number of login attempts helps to keep unauthorized persons from hacking the Aurora software and potentially breaching your access control security protocols.

The system user account must have a Master designation for setting the Allowed Login Attempts function.

In the event that someone exceeds the allowed login attempts, Aurora issues a message indicating the software is locked out from any further login attempts for a stated period of time.

Procedure

Steps to Set Allowed Login Attempts

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Below the Application Settings heading, click on the symbol opposite Allowed Login Attempts, and select the number of times a login may be attempted.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Refresh Timer

The Refresh Timer updates, or, as its title implies, refreshes the on-screen data at the specified refresh time. The Refresh Timer range is 5 minutes to 60 minutes.

The purpose of the Refresh Timer is that when multiple system users are logged in concurrently, if a change is made at one Client workstation, all other Aurora Client workstations are updated every 5 to 60 minutes depending on the Refresh Timer setting.

Procedure

Steps to Set the Refresh Timer

1. From the Client main screen, select the Settings button > Application Utilities.
    - If you have multiple sites, the settings in the Application Utilities screen apply to all sites.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Locate the Application Settings heading.
4. In the text box to the right of Refresh Timer (minutes), enter the time in minutes.
    - Refresh Timer range is 5 to 60 minutes
5. Click on the Save Button.
    - When the Refresh Timer value is changed, after you select the Save button, Aurora prompts you with a message that you must restart the Client before the change takes effect. Click on the OK button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.
7. Close the Aurora client and log back on.

Reason for Disabling Logging

The Aurora Client has filters to suppress alarms in the Event Setup > Logging Filter screen. The purpose of the Logging Filter screen is that you may have periods where alarm reporting is not required. An example might be where you have a busy door with a short door held open time and do not want constant door held open alarms. Suppressing the alarm is performed in the Logging Filter screen.

However in the Reason for Disabling Logging, you define the reasons why. The defined reasons are then selectable when an alarm is disabled in the Logging Filter screen.



The Logging Filter should be used with extreme caution. In essence you are suppressing alarm reporting when disabled is selected. Keyscan recommends not using this feature unless you are completely knowledgeable with respect to how your access control system operates.

Procedure

Steps to Define Reasons for Disabling Logging Filter

1. From the Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Advanced tab is selected.
3. Click on the + button to the left of the Reason for Disabling Logging heading.
4. Enter the reason in the text box that opened after selecting the + button.
5. To add another reason, repeat the preceding two steps.
6. When you have completed creating reasons for disabling logging, click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

At a later date if you need to delete a Reason for Disabling Logging, open the Application Utilities screen and click on the trash bin icon on the row of the reason to be discarded.

Related Topic

Event Setup / Logging Filter

Auto Clear Alarms

In Aurora, when an assigned device goes into an alarm condition, it produces an alarm warning with a New status in the Transaction Response screen. Through system user intervention, alarms can be set to Pending for investigation or marked as Completed following the investigation or if an investigation was not warranted.

Aurora's Auto Clear Alarms function automatically changes the status of alarms with new or pending status to completed status after a set time period. This excludes any alarms with associated alarm response instructions. See Auto Clear All Alarms below.

By default, the Auto Clear Alarms function is enabled at seven (7) days. However, this setting may be altered to a lower number of days down to a minimum of two (2) days or disabled with the Not Used setting, which prevents Aurora from automatically changing new or pending alarms after the specified time duration. If Not Used is selected, only operator intervention can change alarms from new or pending to completed regardless of how long ago they occurred.

Auto Clear All Alarms (including alarms with response instructions)

If you elect to use the Auto Clear Alarms and want to include new/pending alarms with response instructions, enable the Auto Clear All Alarms (including alarms with response instructions) setting. This setting is dimmed and unavailable if Auto Clear Alarms is set on Not Used.

Procedure

The Auto Clear Alarms and the Auto Clear All Alarms (including alarms with response instructions) are accessed from the Settings button > Application Utilities. Select the Application Settings tab. To reset the Auto Clear Alarms function, click on the ▼ symbol and select the number of days or Not Used in the box. To enable the Auto Clear All Alarms (including alarms with response instructions), click in the box to the left. The box has an x when enabled.

Related Topics

About Alarms and Events

Response Instructions

Transaction Response

Reduce Photos

Many digital cameras now offer upwards of 20 mega-pixel images. This gives images extremely large dimensions with file sizes of 2 MB or more. If the images of individuals you are inserting in the credential records or system user records have been shot with a digital camera, especially a digital SLR camera, the images will be much larger than required in the photo frame in the Edit Person screen or the Manage System User screen. As these images are stored in the Aurora database, several hundred to several thousand images can occupy a large percentage of the database's overall memory capacity.

The Application Utilities screen has two settings Reduce Photos Over Size and Reduce Photos to Size that automatically reduce the size of imported images of people. An image between 0.25MB to 0.5MB has sufficient detail for both a printed photo badge and an on-screen image.

By default Aurora is defaulted at the following settings

- Reduce Photos Over Size - 0.5 MB
- Reduce Photos To Size - 0.25MB

The two settings above affect importing images in the Image Editor screen or the Import People screen - Photo Name field.

You have the option of altering the settings or disabling them (not recommended).

Procedures

Steps to Change or Disable the Reduce Photos Options

1. From the Aurora main screen, select the Settings button > Application Utilities.
2. Select the ▼ symbol at the right of Reduce Photos Over Size and select one of the file sizes. Any imported image file that exceeds this value is reduced to the specified Reduce Photos to Size value in the next step.
    - To disable the function, select Not Used.
3. Select the ▼ symbol at the right of Reduce Photos To Size and select one of the file sizes. Any imported image file size is reduced to this value.
    - To disable the function, select Not used.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History ▼ down arrow to the right of the Back button.

Note

It is not recommended to disable these settings.

Hardware Setup

With a Keyscan access control system, hardware components must be interfaced with the Aurora software so the two entities - software and hardware - can communicate and operate as an integrated entity. Primary hardware components may be any of the following control boards, wireless locks, NVRs or intrusion panels depending on your particular setup and the licenses purchased from Keyscan.

- Door control units
- Elevator control units
- Wireless locks
- NVRs for CCTV integration
- Intrusion panels for alarm integration



Generally, the dealer/installer completes the Hardware Setup screens. Never make changes to the Hardware Setup screens without first consulting your dealer/installer.

Hardware Setup Screens

The above hardware components must be configured in Aurora's Hardware Setup screens before they are integrated to function within the Keyscan access control system. The Hardware Setup screen is comprised of several sub-screens, each of which is designed to configure specific categories of hardware along with their respective ancillary components. The table below outlines the Hardware Setup screens.

All Hardware

Sub-Screens/Panes	Summary
Access Control Units	lists intrusion control units configured in the software
Elevator Banks	lists elevator banks and assigned EC elevator control units currently configured in the software
Video Devices	lists NVRs currently configured in the software
E-Plex Door Groups	lists E-Plex wireless locks currently configured in the software

Doors

	Setup	Hardware
Information	- Control unit information	1 door control - CA150
	- Communication	2 door control - CA250
	- Additional ACU Settings	4 door control - CA4500
		8 door control - CA8500
		2 door KC Series Control Unit - KC-2A
		4 door KC Series Control Unit - KC-4A
Doors	- Door setup	

	- Dual custody mode - First person in - Reader assignments - Anti-pass back setup	
Auxiliary Outputs	- On name - Off name	OCB-8 For KC Series, Aux Outputs are on panel see here for KC Series Aux Output Naming Conventions (Hardware vs Software)
Inputs	- Name - Output assignment	
IOCB1616	- Input name & timer - Output name & timer - Rules & modes	IOCB1616 input/output board
Global I/O	- Input to output	Global OCB-8 connected to Control 5 on CA4500 or CA8500
Additional Settings	- Output for power failure - Power failure delay - Output for invalid card/ keypad - Output for keypad duress - Hardware settings including reader formats	

Elevators

Sub-Screens/Panes	Setup	Hardware
Information	- Control unit information - Communication - Floor descriptions - Floor timers - Elevator banks	1 cab elevator control - EC1500 2 cabs elevator control - EC2500

Video Device

Sub-Screens/Panes	Setup	Hardware
Video Device	- NVR information - Login credentials	Supported NVRs
Cameras	- Name - Type	

Intrusion

Sub-Screens/Panes	Setup	Hardware
ICU	- Alarm unit information - Communication	Supported intrusion control unit
Zones	- Number & description	
Partition (or Area for DMP)	- Number & name	
Users	- Name - Location - PIN	

Door Groups

Sub-Screens/Panes	Setup	Hardware
E-Plex Door Group	- Door setup - ZAC & Gateway setup	E-Plex series of wireless locks
BEST Door Group	- Information - Doors - Schedule Assignment - Card Format Assignment	BEST G and V Series of offline locks

Auxiliary Output Naming Conventions for KC Series panels (Hardware vs Software)

See chart below to see how the hardware and software names for the Auxiliary Outputs for KC Series boards relate to each other.

Auxiliary Output Naming Conventions (KC-2A, KC-4A)	
Name on Hardware Terminal Block	Name in Software
Aux-Output Op1	Auxiliary Output #1
Aux-Output Op2	Auxiliary Output #2
Aux-Output Op3	Auxiliary Output #3
Aux-Output Op4	Auxiliary Output #4
Dry Mode 1	Auxiliary Output #5
Dry Mode 2	Auxiliary Output #6

Door Control Units

The Hardware Setup screen with the Information tab selected is used to identify the access control units and configure communication settings. If using a serial connection, the baud rate specified on the Information screen must match the baud rate set on the control board.

Door Control Unit Series

Door control units are as follows:

- 2 Door KC Series Control Unit (KC-2A)
- 4 Door KC Series Control Unit (KC-4A)
- 8 Door KC Series Control Unit (KC-8A)
- 1 Door Access Control Unit (CA150)
- 2 Door Access Control Unit (CA250)
- 4 Door Access Control Unit (CA4500)
- 8 Door Access Control Unit (CA8500)
- Allegion AD Wireless Control (CA150WLN)

Information

The Information tab has the following fields for data input (**Note:** fields will vary depending on the Access Control Unit type you choose):

- **Name:** the Aurora software by default names the first door controller Access Control Unit #1 and increments the number by 1 for each control unit added
- **Serial Number:** each control unit has a factory installed serial number marked on the control board and listed on the invoice and packing slip
- **Password:** it is recommended to retain the default password KEYSCAN; if another password is created, be sure to record it
- **MAC Address:** the twelve-digit hexadecimal Media Access Control address. Used for KC Series Control Boards (located on the "UL" label)
- **Device Address:** used by KC Series Control Boards. Can be found on the KC Series Control Board's device web page home screen under "Device Details". **Note:** ensure this matches the value listed on your device's web page.
- **Type:** lists the unit series
- **Status:** indicates the current state of the panel - active, inactive, disabled or disaster recovery
    - **Active:** the panel status must be active to communicate with the software
    - **Inactive:** in the event that the access control unit losses communication, the software automatically sets the unit as inactive
    - **Disabled:** takes an access control unit off-line which is generally for maintenance or troubleshooting by a dealer

    - **Disaster recovery:** is set only in the event that the database has been corrupted or lost without a database backup and data must be retrieved directly from the access control units - see related topics below

- **Regional Time Zone:** select the time zone where the unit is located geographically
- **Hardware Notes:** text field to describe particulars about the control unit such as where it is mounted within the building or site so it can be located for future maintenance and any other important details
- **Communication:**
    - **Serial**
    - **Network**
    - **Reverse Network** (requires a license from dormakaba)

Door Control Unit ID Naming Structure

When adding access control units or elevator control units in the Hardware Setup screen, the Client software assigns the following names to the control units by default as follows:

- Access Control Unit #1
- Access Control Unit #2

You can use the default name format or rename the control units using up to 28 characters. If you elect to rename the control units, employ a format that is consistent and makes sense for other system administrators and service technicians.

Additional Settings

When you add or select a door control unit in the Hardware Setup screen, you will note the Additional Settings tab at the far right. When you select the Additional Settings tab, the screen is divided under two headings for specific control board functions:

- Additional Access Control Unit Settings
- Hardware Settings

The following two sub-headings outline the specific functions.

Additional Access Control Unit Settings

You can assign outputs to the following access control unit conditions and events:

- **Output for Power Failure:** the assigned output is tripped in the event that the access control unit experiences an AC power failure
- **Power Failure Delay:** a time delay - in minutes - before the output is tripped if the control unit experiences an AC power failure
- **Output for Invalid Card/Keypad code:** the assigned output is tripped on either an invalid card presentation or incorrect PIN entry
    - The output is tripped on the sixth (6th) invalid card presentation and remains tripped for ten (10) minutes
- **Output for Keypad Duress:** the assigned output is tripped when a keypad duress code is entered at a connected keypad

Important ! Your installer or service provider should determine the Additional Access Control Unit Settings.

Hardware Settings | DIP Switch (S2) Configured Control Boards and KC Series Boards Only

When adding a KC Series Board, 2 Door Control Unit, 4 Door Control Unit, 8 Door Control Unit, 1 Cab Elevator Control Unit, 2 Cab Elevator Control Unit with a PC1097 or higher printed circuit board, the hardware functions listed below must be set in the Hardware Settings screen. **Note:** Hardware Settings options will vary depending on the Access Control Unit type you choose

- Card Countdown Enabled (J16 on pre-PC1097 circuit boards)
- Lockdown Reader LED Enabled (J18 on pre-PC1097 circuit boards)
- Reader LED (Red/Green Enabled) (J16 on pre-PC1097 circuit boards)
- Extended Entry Relay All Cards Enabled (J16 on pre-PC1097 circuit boards))
- Card Lockout Skip for P3 (J16 on pre-PC1097 circuit boards)
- IOCB Enabled (J16 on pre-PC1097 circuit boards)
- Extended PIN (7 digit) (unavailable on pre-PC1097 circuit boards)
- Callback Timer (unavailable on pre-PC1097 circuit boards)
- End-of-line supervision mode (J18 on pre-PC1097 circuit boards)
- Reader Formats (J3 on pre-PC1097 circuit boards)

The Hardware Settings screen only applies to KC Series Control Boards and PC1097 version or higher control boards with DIP switches.

Do not select or enable any fields in the Hardware Settings screen unless you are adding a KC Series or PC1097 version or later control board. Previous PC109x control board versions are distinguished by jumpers which regulate the above hardware functions from the circuit board.

The control boards must also have Aurora-compatible firmware.

Note + For CA150 and CA150WLN control boards, refer to the installation guides for setting the above functions using the on-board DIP switches. Not all functions are supported on the CA150WLN circuit board.

Card Countdown Enabled

This setting is for the temporary card usage countdown function in the Edit Person screen. Select the box on the left to enable the function.

Lockdown Reader LED Enabled

If the control board is configured for Lockdown Mode, S2 switch # 6 ON, the readers (doors only) can be configured for rapid flashing indicating a lockdown is in effect. To enable Lockdown Reader LED mode, select the box to the left. This mode applies to all readers connected to the door control unit.

- Does not apply to the CA8WL-AL control unit

Reader LED (Red/Green Enabled)

This setting indicates the condition of the door lock/unlock status:

- Red/Green type LED reader - enabled
- Red type LED reader - disabled
- Does not apply to the CA150WLN control unit

Extended Entry Relay - All Cards Enabled

If using HC Accessibility Relays in a capacity that requires all cards enabled, select the box on the left to activate this option. (This option includes all valid cards as opposed to cards set with the Accessibility Feature ON in the Cardholder screen.)

Card Lockout - Skip for P3

When this function is enabled, after P3 is activated, a card is allowed a single presentation for access.

Extended PIN (7 digit)

This function can only be enabled if Extended PIN mode has been activated. For more information, see the Related Topic listed below.

Callback Timer

This function can be configured for panels configured to communicate in Reverse Network Mode. The callback timer allows the user to set the time period when a board using reverse communication will make a call-in attempt. This value is set at 60 seconds by default, but can be set to any value between 10 and 240 seconds.

End of Line Supervision Mode

This sets all auxiliary inputs on the control board to one of the following supervision levels:

- Non-supervised input or digital input
- Single end-of-line supervision
- Double end-of-line supervision

IOCB

When this function is used to enable the use of an IOCB board with the associated access control panel.

Receive Global Lockdown (KC Series panels only)

When this function is enabled, KC series panels will be able to receive lockdown alerts from other panels on the same site (they can be KC series or PC109x boards)

Reader Formats

This sets the control board reader format. Select the Supported Reader Formats link below Related Topics for more information.

Procedures

Steps to Add a New Serial or Network Connected Control Unit (CA150, CA250, CA4500, CA8500, SDAC)

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, select the down arrow on the right side of the Add 8 Door Controller button.
    - By default, Add 8 Door Controller is listed. However, the Add … button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.

3. From the drop down list, select the type of control board you are adding.
4. From the Confirm Hardware Installation prompt, click on the Yes button.
    - If you have selected the wrong control unit series, click on No, and click on the Add …. Button. Remember the Add button lists the last series selected.
5. By default the Client software populates the Name field with Access Control Unit # 1. Each time you add a control unit the # increments by 1. You can leave the default name format (recommended) or change it. If you change it however, Keyscan recommends you retain a consistent naming format for all control units.
6. In the Serial Number text box, enter the access control unit serial number. The serial # is on the packing slip, invoice and the control board.
7. In the Password text box, you can leave the default password of KEYSCAN or if you elect to change it, the password has a maximum of eight characters. If you change the password, be sure to write it down and store it in a safe place. In the event you have to perform a disaster recovery at a later date to retrieve the on-board data, without the password, you cannot communicate with the control board or access the data.
8. Opposite Status, leave the default setting on Active.
9. Click the ▼ symbol on the right side of the Regional Time Zone and select the time zone from the drop down list where the access control unit is located.
10. In the Location text box, enter a brief description where the access control unit is physically located.
11. Opposite the Communication tab, Serial is listed by default, select the ▼ symbol on the right and from the drop down list select the communication mode that is used to communicate with the access control unit and complete the communication mode sub-fields as follows:
    - For a Serial Connection - Specify the Baud Rate of the access control unit, the Communication Port on the PC running the communication service with the serial connection to the access control unit. By default the Client populates the Server field with the name of the local PC. Leave this on the default setting for a single PC/server installation. However if the Keyscan Communication Service is not installed on the local PC/server, enter the name of the PC/server where the Keyscan Communication Service is installed.
    - For a Network Connection - In the Communication Port field, leave the default setting of 3001 unless another network port is used. In the IP Address field, enter the static IP address assigned to the NETCOM device connected at the access control units. By default the Client populates the Server field with the name of the local PC. Leave this on the default setting for a single PC/server installation. However if the Keyscan Communication Service is not installed on the local PC/server, enter the name of the PC/server where the Keyscan Communication Service is installed.
12. If required, set the control board output protocols and hardware settings depending on the configuration and hardware by selecting the Additional Settings tab on the Hardware Setup screen.
13. Select the Save button.
14. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to add a new KC Series Access Control Unit (2 or 4 door)

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, select the down arrow on the right side of the "Add 8 Door Controller" button.
    - By default, Add 8 Door Controller is listed. However, the Add … button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
3. From the drop down list, select the type of control board you are adding.

- 2 Door KC Series Control Unit (KC-2A)
- 4 Door KC Series Control Unit (KC-4A)

4. From the Confirm Hardware Installation prompt, click on the Yes button.
   - If you have selected the wrong control unit series, click on No, and click on the Add …. Button. Remember the Add button lists the last series selected.
5. By default the Client software populates the Name field with Access Control Unit # 1. Each time you add a control unit the # increments by 1. You can leave the default name format (recommended) or change it. If you change it however, dormakaba recommends you retain a consistent naming format for all control units.
6. In the MAC Address text box, enter the access control unit's MAC Address (see the KC Series controller's "UL" label).
7. In the Device Address text box, enter the Device address. The device address for KC Series Control Boards is a pre-set value that can not be changed. It can be found on the KC Series Control Board's device web page home screen under "Device Details". **Note:** ensure this matches the value listed on your device's web page, or communication with the board will be impossible.
8. Opposite Status, leave the default setting on Active.
9. Click the symbol on the right side of the Regional Time Zone and select the time zone from the drop down list where the access control unit is located.
10. Under "Communication" - In the Communication Port field, set your Communications Port to the same port that you used for the "Server Port" and "HB/CTH Port" when you initially set up your KC Series Controller. In the IP Address field, enter the same IP address you used when setting up the KC Series Controller. By default the Client populates the Server field with the name of the local PC. Leave this on the default setting for a single PC/server installation. However if the Keyscan Communication Service is not installed on the local PC/server, enter the name of the PC/server where the Keyscan Communication Service is installed.
11. If required, set the control board output protocols and hardware settings depending on the configuration and hardware by selecting the Additional Settings tab on the Hardware Setup screen.
12. Click the Save button.
13. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to add a new KC Series Access Control Unit (8 door)

1. From the Client main screen, select the Site Management button > Hardware Setup.
   - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, select the down arrow on the right side of the "Add 8 Door Controller" button.
   - By default, Add 8 Door Controller is listed. However, the Add … button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
3. From the drop down list, select the type of control board you are adding.
   - 8 Door KC Series Control Unit (KC-8A)
4. From the Confirm Hardware Installation prompt, click on the Yes button.
   - If you have selected the wrong control unit series, click on No, and click on the Add …. Button. Remember the Add button lists the last series selected.
   - NOTE: After clicking Yes, a new "KC 8 Door Creation" window will pop-up in which you must complete all fields for both KC-8A panels before you can save (described in the following steps).
5. By default the Client software populates the Name field with Access Control Unit # 1. Each time you add a control unit the # increments by 1. You can leave the default name format (recommended) or change

it. If you change it however, dormakaba recommends you retain a consistent naming format for all control units.

6. In the MAC Address text box, enter the access control unit's MAC Address (see the KC Series controller's "UL" label).
7. In the Device Address text box, enter the Device address. The device address for KC Series Control Boards is a pre-set value that can not be changed. It can be found on the KC Series Control Board's device web page home screen under "Device Details". **Note:** ensure this matches the value listed on your device's web page, or communication with the board will be impossible.
8. In the IP Address field, enter the same IP address you used when setting up the KC Series Controller on the KC Series Control Board's device web page.
9. In the Communication Port field, set your Communications Port to the same port that you used for the "Server Port" and "HB/CTH Port" when you initially set up your KC Series Controller on the KC Series Control Board's device web page.
10. Use the Communications Server drop-down to select the name of the computer hosting the Keyscan Communication Service. By default the Client populates the Server field with the name of the local PC. Leave this on the default setting for a single PC/server installation. However if the Keyscan Communication Service is not installed on the local PC/server, select the name of the PC/server where the Keyscan Communication Service is installed.
11. Repeat steps 5 to 10 for "Panel 2".
12. Click the Save button.
13. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Add a New Reverse Network Connected Control Unit

You must have purchased a reverse network license from Keyscan to use this mode of communication and you must have installed the reverse network communication application which is included with the Aurora software installation files.

1. From the Client main screen, select the Site Management button menu > Hardware Setup.
    - If you have multiple sites, select the appropriate site from the Site Search – Hardware Setup directory screen.
2. From the Hardware Setup screen, select the symbol on the right side of the Add 8 Door Controller button.
    - By default, Add 8 Door Controller is listed. However, the Add … button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
3. From the drop down list, select the type of access control unit you are adding.
4. From the Confirm Hardware Installation prompt, click on the Yes button.
    - If you have selected the wrong control unit series, click on No, and click on the Add …. button. Remember the Add button lists the last series selected.
5. By default the Client software populates the Name field with Access Control Unit # 1. Each time you add a control unit the # increments by 1. You can leave the default name format (recommended) or change it. If you change it however, Keyscan recommends you retain a consistent naming format for all control units.
6. In the Serial Number text box, enter the access control unit serial number.
7. In the Password text box, you can leave the default password of KEYSCAN or if you elect to change it, the password has a maximum of eight characters. If you change the password, be sure to write it down and store it in a safe place. In the event you have to perform a disaster recovery at a later date to recover on-board data, without the password, you cannot communicate with the control board or access the data.
8. Opposite Status, leave the default setting on Active.

9. Click the ▼ symbol on the right side of the Regional Time Zone and select the time zone from the drop down list where the access control unit is located.
10. In the Location text box, enter a brief description where the access control unit is physically located.
11. Opposite the Communication heading, select the ▼ symbol on the right and, select Reverse Network from the drop down list.
12. Do one of the following steps:
    - If this is the control board that is designated as the master control board - it is connected to the NETCOM6 and has been programmed with the IP address of the host location, leave the Master Panel Serial # field on Not assigned and go to the next step.
    - If this is a control board other than the master control board on the same communication bus, click on the symbol and select the serial number of the control unit designated as the master.
13. In the Receiver Comms IP text box, enter the IP address of the server/PC which has the Reverse Network Communication installed.
14. If a secondary IP address exists with a connection to the server/PC which has the Reverse Network Communication installed, you can specify the address in the Failure Comms IP text box.
15. Enter the computer name of the server/PC with the Reverse Network Communication if it is other than the unit currently displayed in the Communications Server field.
16. Click on the Save button.
17. To add another access control unit, repeat the above steps.
18. Select the Back button to return to the main screen or the History Navigation button for a previously viewed screen.

Related Topics

- Waiver of Liability
- Configure Door & Reader Parameters
- Extended PIN (7 digit)
- First Person In
- Access Control Unit Replacement
- Delete an Access Control Unit
- Disaster Recovery
- Supported Reader Formats

Supported Reader Formats

The Keyscan access control system and the Aurora software support a range of reader formats other than the Keyscan 36-bit Wiegand proprietary format. Only the dealer/installer should change the reader format setting which is contingent on the type of credential used for the access control system. Reader formats are set in the Hardware Setup >Access Control Unit > Additional Settings screen.

Unless stated otherwise in the CA/EC series table, reader formats apply to PROM version 4.03 or greater. Keyscan does not recommend any 26-bit card formats. 26-bit cards and tags are not secure. Duplicate card numbers exist in this format so a facility is vulnerable to unauthorized access. Also refer to Security Levels below for more about reader/card formats.

All Keyscan control boards and the Aurora software are factory defaulted on Keyscan's 36-bit Wiegand proprietary format.

Keyscan recommends using only one reader format per site.

Reader Formats

The Reader Formats table below reviews not only supported reader formats, but also the security level of each format. Be aware that where Keyscan’s 36-bit proprietary cards share a combined reader format with other manufacturer's cards, the other manufacturer's card binary bits may be truncated to accommodate the joint format. This lessens the overall security, as not all bits are read.

Advantage of Keyscan 36-bit Proprietary Wiegand Format Cards

Keyscan’s 36-bit proprietary Wiegand format cards and tags, which include a manufacturer's code, offer a high level of security. Keyscan tracks all its cards and tags. This ensures that no duplicate cards or tags are sold by Keyscan. When installing or upgrading a Keyscan access control system, we recommend our proprietary Keyscan 36-bit Wiegand format cards and tags, available in 125 kHz or 13.56 MHz formats, for a high level of security.

Waiver of Liability

Installing dealers should have an authorized end-user sign a waiver of liability before enabling 26-bit reader formats/cards. Keyscan has enclosed a Waiver of Liability.

Security Levels

The Reader Formats table below reviews not only supported reader formats, but also the security level of each format. Be aware that where Keyscan's 36-bit proprietary cards share a combined reader format with other manufacturer's cards, the other manufacturer's card binary bits may be truncated to accommodate the joint format. This lessens the overall security, as not all bits are read.

The reader formats in the table have been given one of following security ratings:

- High
- Medium
- Low
- Very Low

Reader formats ranked with medium, low, and very low are NOT recommended. The ratings are based on whether a card's binary bits are truncated and/or the cards are sold by other manufacturers, which Keyscan has no control over.

Keyscan assumes no responsibility for liability for any card format.

Supported Card Formats (KC series boards)

The supported card number formats fall under the following two types:

- Standard Card Number: 3 digit facility code* / 5 digit card number
    - Facility code range: 1 - 255
    - Card number range: 1 - 65535
- Extended Card Number: hexadecimal 0 - 9, A - F or decimal 0 - 9
    - Hexadecimal range: 1 - FFFFFFFFFFFF
    - Decimal range: 1 - 281474976710655

*The facility code may also be referred to as the site code or the batch code.

Reader Format	Security Level	Card Number Format	Notes
Standard 26-bit only	Low	Standard	
HID H10304	Medium	Extended	
HID H10302	Medium	Extended	
Keyscan 36-bit only	High	Standard	
MIFARE - CSN 32-bit only	Low	Extended	Only reads the Card Serial Number sector.
MIFARE - Reverse CSN 32-bit output	Low	Extended	Only reads the Card Serial Number sector.
MIFARE 40-bit CSN (32-bit CSN, 8-bit Checksum)	Low	Extended	Only reads the Card Serial Number sector.
MIFARE Reverse 40-bit (32-bits reverse CSN + 8-bits Checksum)	Low	Extended	Only reads the Card Serial Number sector.
Corporate 1000 - 35	Medium	Extended	
Corporate 1000 - 40	Medium	Extended	
26 to 48 Pass-through Large Card Format	Medium-Low	Extended	
26 to 48 Pass-through Large Card Format (with first and last parity bits dropped)	Medium-Low	Extended	
Keyscan 36-bit only KABA Integrated Credential (17 byte)	High	Extended	Future Support

Supported Card Formats (CA/EC series boards)

The supported card number formats fall under the following two types:

- Standard Card Number: 3 digit facility code* / 5 digit card number

- Facility code range: 1 - 255
- Card number range: 1 - 65535

- Extended Card Number: hexadecimal 0 - 9, A - F or decimal 0 - 9
  - Hexadecimal range: 1 - FFFFFFFFFFFF
  - Decimal range: 1 - 281474976710655

*The facility code may also be referred to as the site code or the batch code.

Ref.#	Reader Format	Security Level	Switch Settings S2.1 - S2.6	Card Number Format	Notes
A	Keyscan 36-bit only	High	0 0 0 0 0 0	Standard	
B	FIPS/TWIC - 75-bit output (48-bit FASC-N, 25-bit expiration date, 2 parity bits)	High	0 0 0 0 0 1	Extended	Legacy support only
C	HID Corporate 1000 - 35-bit output	Medium	1 0 0 0 0 1	Extended	
D	MIFARE - CSN 32-bit output	Low	0 1 0 0 0 1	Extended	Only reads the card serial number sector
E	MIFARE - Reverse CSN 32-bit output	Low	1 1 0 0 0 1	Extended	Only reads the card serial number sector
F	MIFARE - 40-bit CSN (32-bit CSN, 8-bit Checksum)	Low	0 0 1 0 0 1	Extended	Only reads the card serial number sector
G	26 to 48 Pass-through Large Card Format	Medium - Low	1 1 1 1 1 1	Extended	
H	26 to 48 Pass-through Large Card Format (with first and last parity bits dropped)	Medium - Low	0 1 1 1 1 1	Extended	
I	University 1000 - 56-bit	Medium	0 1 1 0 0 1	Extended	Custom order only. Facility code required when ordering
J	MIFARE Reverse 40-bit (32-bits reverse CSN + 8-bits checksum = 40 bits	Low	1 0 1 0 0 1	Extended	Only reads the card serial number sector
K	MLF Indala Format = 16039	Medium	1 1 1 0 0 1	Extended	Custom order only. Letter required from dealer.
L	FIPS/TWIC - 75-bit output (48-bit FASC-N, 25-bit expiration date, 2 parity bits) & Keyscan 36-bit	High	1 0 0 1 0 1	Extended	Legacy support only
M	FIPS/TWIC - 75-bit output (48-bit FASC-N, 25-bit expiration date, 2 parity bits) & Keyscan 36-bit & Mifare	High	0 1 0 1 0 1	Extended	Legacy support only

	- 40-bit CSN (32-bit CSN, 8-bit Checksum)				
N	37-bit H10304 & Keyscan 36-bit	Medium	1 1 0 1 0 1	Extended	Reader PROM 4.04 or higher
O	37-bit H10302 & 35-bit Corporate 1000	Medium	0 0 0 1 0 1	Extended	Reader PROM 4.04 or higher
P*	HID Corporate 1000 48-bit & Keyscan 36-bit	Medium	0 0 1 1 0 1	Extended	Reader PROM 5.05 or higher
Q*	HID Corporate 1000 48-bit, HID Corporate 35-bit, HID H10302 & Keyscan 36-bit	Medium - Low	1 0 1 1 0 1	Extended	Reader PROM 5.05 or higher
R*	HID Corporate 1000 48-bit, HID Corporate 35-bit, HID H10302, Keyscan 36-bit & Standard 26-bit	Low	0 1 1 1 0 1	Extended	Reader PROM 5.05 or higher
S	Kaba Integrated Mode - 17 byte credentials	High	1 0 1 1 1 1	Extended	For Kaba SR series readers Requires System PROM 1.63 or higher Requires Reader PROM 6.00 or higher
*Settings P, Q, and R require "Enable Keyscan Credentials for Extended Card Format" to be applied when using Keyscan credentials					
The reader formats below are NOT recommended.					
1	Standard 26-bit & Keyscan 36-bit	Low	1 0 0 0 0 0	Standard	
2	Legacy Northern 34-bit, Standard 26-bit & Keyscan 36-bit	Low	0 1 0 0 0 0	Standard	
3	Corby 30-bit & Keyscan 36-bit	Medium	1 1 0 0 0 0	Standard	
4	Kantech 32-bit & Keyscan 36-bit	Medium	0 0 1 0 0 0	Standard	
5	DSX 33-bit & Keyscan 36-bit	Medium	1 0 1 0 0 0	Standard	
6	Intercon 32-bit & Keyscan 36-bit	Low	0 1 1 0 0 0	Standard	
7	Legacy Chubb 36-bit (5 & 6 digit cards) & Keyscan 36-bit	Low	1 1 1 0 0 0	Standard	
8	Keyscan 36-bit with zero batch number	Low	0 0 0 1 0 0	Standard - except Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
9	Standard 26-bit & Keyscan 36-bit	Low	1 0 0 1 0 0	Standard - except for 26-bit cards	Enter 0 (zero) for the facility code in the Client software to ignore the FC

				Facility Code = 0	output from the reading device.
10	Northern 34-bit & Keyscan 36-bit	Low	0 1 0 1 0 0	Standard - except for 34-bit cards Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
11	Corby 30-bit & Keyscan 36-bit	Low	1 1 0 1 0 0	Standard - except for 30-bit cards Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
12	Legacy GE 40-bit or Casi-Rusco Ex. Prox-Lite 941-W RDR	Low	0 0 1 1 0 0	Standard	
13	Legacy (37-bit Corp H10302) & Keyscan 36-bit	Low	1 0 1 1 0 0	Standard	
14	Legacy Keyscan England 36-bit with no manufacturer's code check	Low	0 1 1 1 0 0	Standard	Format does not support Keyscan WSSKP-1 Keypad with PIN use.
15	Legacy HID 35-bit & Keyscan 36-bit	Low	1 1 1 1 0 0	Standard - except for HID 35-bit cards - Company ID Code ignored	See Reader Format - Ref # C - preferred option.
16	HID Computrol 34-bit & Keyscan 36-bit	Medium	0 0 0 0 1 0	Standard	
17	Legacy 37-bit (alternate 37 Bit Corp H10304) & Standard 26-bit & Keyscan 36-bit	Low	1 0 0 0 1 0	Standard	
18	Legacy Chubb 36-bit & Keyscan 36-bit	Low	0 1 0 0 1 0	Standard	No parity check on Chubb card.
19	Honeywell 40-bit & Keyscan 36-bit	Medium	1 1 0 0 1 0	Standard	
20	Unassigned		0 0 1 0 1 0	Standard	
21	Unassigned check		1 0 1 0 1 0	Standard	Format does not support Keyscan WSSKP-1 Keypad with PIN use.
22	ITI 29-bit & 26-bit & Keyscan 36-bit	Low	0 1 1 0 1 0	Standard	
23	Legacy 37-bit (37 Bit Corp H10302) & Standard 26-bit & Keyscan 36-bit	Low	1 1 1 0 1 0	Standard	

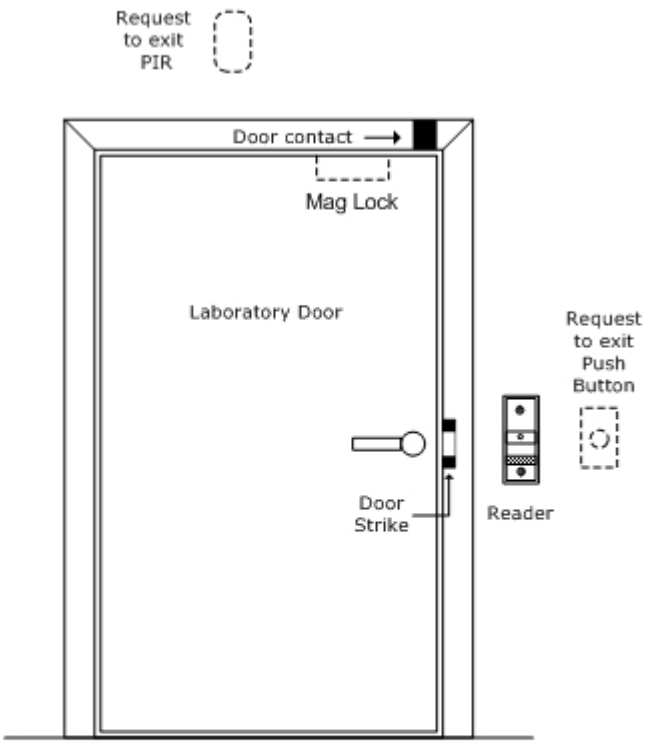
24	Kantech XSF 36-bit IO Prox & Keyscan 36-bit	Low	0 0 0 1 1 0	Standard	
25	CardKey 34-bit & Keyscan 36-bit	Medium	1 0 0 1 1 0	Standard	
26	Keyscan 36-bit & 26-bit with no parity checking format	Low	0 1 0 1 1 0	Standard - except 26-bit no parity check	26-bit format designed for Keri part # SM-2000X
27	Modern 30-bit & 26-bit & Keyscan 36-bit	Low	1 1 0 1 1 0	Standard	
28	Intercon 32-bit & Keyscan 36-bit & Standard 26-bit	Medium	0 0 1 1 1 0	Standard	
29	Indala 27-bit (format 10251) & Keyscan 36-bit	Medium	1 0 1 1 1 0	Standard	
30	Cards between 26-bit & 40-bit read as 26-bit card location with parity check	Very Low	0 1 1 1 1 0	Standard	
31	Legacy Diagnostic Mode - evaluates cards between 26-bit & 40-bit for Keyscan engineers	Display only	1 1 1 1 1 0	Standard	Format ignores card’s stored values at ACU producing access denied for all cards. Format does not support Keyscan WSSKP-1 Keypad with PIN use

About Doors and Readers

Doors regulated and monitored by the access control system are equipped with readers, electric door strikes or magnetic locks, door contacts, and generally request-to-exit (RTE) devices such as motion sensors or push buttons. These devices are all connected to and integrated with the access control unit's control board. In the Aurora software, each door and reader must be configured with user-defined settings for day-to-day operation.

Door Layout

Door Components



Doors/Readers Interface Settings

Doors

Name
- The name of a door, generally identified by its location, gives system user's a reference for assigning and monitoring access and determining the source of alarms within the access control software.

Door Operation Mode
- Contingent on the type of hardware installed at the door, one of six assignable modes must be selected to set the door action and prevent an alarm when someone exits the door.

Relay Unlock Time
- The relay unlock time specifies how long the door strike or mag lock remains unlocked after an "access granted" or on a manual unlock pulse.

Alarm on Forced Entry Output
- An assigned output would trip if the door is forced open.

Accessibility Timer
- If an optional HC output is connected to a electro-mechanical door operator, the accessibility timer specifies how long the HC output is tripped to keep the door open.

Door Held Open/Exit Delay
- When the door is opened on an access granted, this sets the amount of time the door is allowed to remain open before reporting an alarm, or if Present 3 is used this sets the how long to delay a time zone toggle.

Alarm Held Open Timer Output
- An assigned output would trip if the door held open time is exceeded.

Readers

Reader
- Identified by its reader terminal number and its assigned door.

Direction
- Readers monitor the direction the credential holder passes through the door - in or out.

Assigned Door
- The name of the door the reader is mounted by or monitors.

Anti-Pass Back
- Prevents a card from being passed back to another individual to gain entry an requires readers to be configured to enforce this mode.

Configure Door & Reader Parameters

Readers and the door hardware control door access within the Keyscan system. After a door control unit has been enrolled in the Aurora software, selecting the Door tab opens the following interface screens to complete door and reader parameters for each door.

Door & Reader Topic Links

- Door Setup
- Reader Assignments
- Anti-Pass Back
- Dual Custody

Related Topic

- About Doors and Readers

Door Setup

The Doors screen consists of the following fields:

- Name - identifies the door, generally the name should indicate where the door is located
- Operation Mode - identifies how the door operates; see Door Operation Modes below for modes and required hardware
- Relay Unlock Time - the interval the door remains unlocked after a credential has been presented to the reader or has been manually "pulsed" by a system user. (0 = toggles the output state.)
- Alarm on Forced Entry Output - assigns an output that would trip a device such as an alarm or a CCTV camera in the event the door was forced open
- Extended Entry Timer - the time that the HC accessibility output relay trips the door operator; see Accessibility Feature below
- Door Held Open/Exit Delay - the time interval that the door may remain open before the system reports a door held open violation
- Extended Entry Door Held Open - the time interval that the door may remain open before the system reports a door held open violation
- Alarm Held Open Timer Output - allows assigning to an output that would trip a device if the door is held open beyond the Door Held Open/Exit Delay time interval.

First Person In

The First Person In group range can be set up from this screen. To access this option, Select the Doors tab and then the First Person In tab once a Door is selected. Utilize the drop-down menus to select the group ranges. For more information, consult the First Person In section of the Related Topics at the end of this page.

Door Operation Modes

When assigning a door operation mode, you have one of six selectable options depending on the door hardware installed. Door operation modes and the required door hardware and configuration are reviewed below:

- *Unlocks door and shunts door contact*

Lock Options	Door strike or magnetic lock
Door Contact Shunt Control	Reader & RTE button device
RTE Control	Unlocks door and shunts door contact
Door Latch/Strike Plate	Optional
Door Closure*	Re-locks door & resets shunt time
Transactions/Alarms	RTE Door Open/Door Held Open/Alarm Tripped
	Occurrence of a Door Held Open alarm is based on the sum of the Relay Unlock Time and the Door Held Open/ Exit Delay time settings in the Hardware Setup > Doors screen.

- *Shunts door contact only*

Lock Options	Door strike
Door Contact Shunt Control	Reader & RTE motion sensor
RTE Control	Shunts contact
Door Latch/Strike Plate	Required
Door Closure*	Resets shunt time
Transactions/Alarm Events	RTE Door Open/Door Held Open/Alarm Tripped
	Occurrence of a Door Held Open alarm is based on the sum of the Relay Unlock Time and the Door Held Open/ Exit Delay time settings in the Hardware Setup > Doors screen.

- *Free egress door held open alarm only*

Lock Options	Door strike
Door Contact Shunt Control	Reader only (RTE button optional)
RTE Control	Unlocks door & shunts contact
Door Latch/Strike Plate	Required
Door Closure*	Re-locks door & resets shunt time
Transactions/Alarm Events	RTE Door Open/Door Held Open
	Occurrence of a Door Held Open alarm is based on the sum of the Relay Unlock Time and the Door Held Open/ Exit Delay time settings in the Hardware Setup > Doors screen.

- *Unlocks door and shunts door contact (no RTE transaction)*

Lock Options	Door strike or magnetic lock
Door Contact Shunt Control	Reader & RTE button device
RTE Control	Unlocks door & shunts contact
Door Latch/Strike Plate	Optional
Door Closure*	Re-locks door & resets shunt time
Transactions/Alarm Events	Door Held Open/Alarm Tripped
	Occurrence of a Door Held Open alarm is based on the sum of the Relay Unlock Time and the Door Held Open/ Exit Delay time settings in the Hardware Setup > Doors screen.

- *Shunts door contact only (no RTE transaction)*

Lock Options	Door strike
Door Contact Shunt Control	Reader & RTE motion sensor
RTE Control	Shunts contact
Door Latch/Strike Plate	Required
Door Closure*	Resets shunt time
Transactions/Alarm Events	Door Held Open/Alarm Tripped
	Occurrence of a Door Held Open alarm is based on the sum of the Relay Unlock Time and the Door Held Open/ Exit Delay time settings in the Hardware Setup > Doors screen.

- *Unlocks door and shunts door contact - no re-lock (door does not re-lock)*

Lock Options	Door strike or magnetic lock
Door Contact Shunt Control	Reader & RTE button device
RTE Control	Unlocks door & shunts contact
Door Latch/Strike Plate	Optional
Door Closure*	No action
Transactions/Alarm Events	RTE Door Open/Door Held Open/Alarm Tripped
	Occurrence of a Door Held Open alarm is based on the sum of the Relay Unlock Time and the Door Held Open/ Exit Delay time settings in the Hardware Setup > Doors screen.

RTE = Request to Exit / * Prior to Door Relay Unlock Time expiring.

Accessibility Feature

Aurora has an accessibility feature for persons requiring an extended time interval to gain access. In order to use the accessibility feature, the Keyscan system must have OCB-8s configured as HC accessibility output relays which are connected to electro-mechanical door operators. The Extended Entry Timer field sets the amount of time the OCB-8's HC accessibility output relay is energized. If an individual has the Extended Entry function enabled in the Edit Person screen, when that individual presents his or her credential at the door, the HC accessibility relay is tripped and the Extended Entry Timer and the Extended Entry Door Held Open settings are invoked overriding the Relay Unlock Time and Door Held Open/Exit Delay settings.

You may have to consult with your dealer/installer if your access control system is configured to operate with this function.

Pre-alert

Keyscan has a Pre-alert Option, which warns when a door is still open after the ½ interval of the combined Door Relay Unlock Time and the Door Held Open/Exit Delay time. One of the more common uses for the pre-alert option is at doors designated for smoking areas. The pre-alert announces to anyone holding the door open that

if it is not closed shortly, the access control software will report a Door Held Open Alarm. The Pre-alert Option is a hardware feature within the access control board and must be wired either to the reader using the beep conductor or to an external sound device to function. Most readers are equipped with an internal beeper and a conductor for a pre-alert connection to the control board. Additional equipment is required if using an external sound device for this option. Your dealer can assist in determining what is required.

Pre-alert relay trips at the 1/2 interval of the combined times in the Door Relay Unlock Time + the Door Held Open Time/Exit Delay.

Example - Door Relay Unlock Time 5 seconds + Door Held Open Time/Exit Delay 25 seconds = Pre-alert at 15 seconds)



On a request to exit, only the Door Held Open Time/Exit Delay pre-alert time is in effect.

Door Relay Follower

The Hardware Setup - Doors screen has a Door Relay Follower setting that gives you the option of firing a designated HC accessibility relay simultaneously with its corresponding door output relay. When set on Door Relay Follower, the designated HC accessibility output fires on any card presentation or RTE as opposed to just an accessibility card presentation at the assigned door reader. The Door Relay Follower is located in the Extended Entry Door Held Open field at the bottom of the drop down list below 99.

The outputs are powered based on the following software fields:

- Door Output relay - Door Relay Unlock Time (seconds)
- HC Accessibility Output relay - Extended Entry Timer (seconds)

Door Held Open/Exit Delay Time

When the door follower mode is selected, the door held open time is 4 minutes and 15 seconds + the door relay unlock time. The setting expressed in the Door Held Open/Exit Delay time field does not apply.

As an example, if the Door Relay Unlock Time is 20 seconds, the software will not report a Door Held Open alarm for 4 minutes and 35 seconds.

An optional OCB-8 is required for 4-doors CA 4500 control boards and 8-doors CA 8500 control boards. The Door Relay follower also requires firmware version 7.97/8.77 or higher. Refer to the respective technical guide for ribbon cable connections as well as jumper or DIP switch settings.

Procedures

Steps to Configure a Door

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit that is connected to the door you are adding.
3. Select the Doors tab.
4. Select the - Door # xx - you are naming and assigning properties.
5. Enter a name in the Name text box. The name should reflect the door's location for easy reference.
6. A door operation mode must be selected to prevent an alarm event when someone opens a controlled door when exiting. Click on the down arrow to the right of Operation Mode, and select one of the door exit options. Refer to the explanations above for more on door operation modes.

7. Select the ▼ symbol on the right side of the Relay Unlock Time and select a time. The range is 2 to 99 seconds. This is the interval that the door remains unlocked after a credential has been presented to the reader. A setting of zero (0) toggles the output state.
8. Select the ▼ symbol on the right side of the Alarm on Forced Entry Output and select an output. If you are not assigning the door to an alarm output, leave this field set on Not Assigned.
9. The Extended Entry Timer and the Extended Entry Door Held Open fields only require completing if the door is equipped with door operators for extended accessibility time and those door operators have been connected to the proper relays on the Keyscan access control unit. If applicable, click on the ▼ symbol on the right side of the Extended Entry Timer field and select a time that the accessibility output relay will fire the door operator. The range is 2 to 99 seconds. This is an optional feature.
10. Click in the text box of the Door Held Open/Exit Delay field and enter a time. The range is 2 to 65,535 seconds. This is the time interval that the door may remain open before the system reports a door held open violation.
11. If applicable, click on the ▼ symbol on the right side of the Extended Entry Door Held Open field and select a time that the door may remain open before the system reports a door held open violation. The range is 1 to 99 seconds.
12. Click on the down arrow on the right side of the Alarm Held Open Timer Output and select an output. If you are not assigning the door to an output, leave this field set on Not Assigned.
13. Select the Save button.
14. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

If you are setting properties for the reader, leave the Door screen open, select the Reader Assignments link below Related Topics and follow the procedures.

Related Topics

First Person In

Reader Assignments

Anti-Pass Back

Dual Custody

Reader Assignments

The Reader Assignments screen is used to assign the reader various parameters. The Reader Assignments pane consists of the following fields:

- Reader # - indicates the port number the reader is connected to on the control board
- Assigned Door - lists the door the reader is monitoring for access
- Direction - specifies the direction of access the reader monitors In or Out
- Anti-Pass Back - when enabled the reader will not permit successive presentations by the same credential; see Anti-pass back below
- RTE Door Follower - acts as a hold for the exit delay on RTE door operation modes

In addition to the above fields, KC Series Control Units have the following additional fields:

- Protocol - select from one of the available reader communication protocols; Wiegand, OSDP, or Weigand & OSDP.

Anti-Pass Back

Anti-Pass Back prevents one individual from passing his or her credential back to another individual for later use. When anti-pass back is employed in a controlled enter/exit environment, after a credential is presented at an IN reader and enters, the credential must be presented at an OUT reader and exit before the system permits the credential to enter again. A controlled enter/exit environment with anti-pass back requires readers on both sides of the door or in some configuration that monitors and controls in/out activity.

If you are configuring readers with anti-pass back, select the link below Related Topics for more information about the types of anti-pass back modes.

If you are configuring anti-pass back with Executive Access, you must have created door groups before you can set anti-pass back.

RTE Door Follower

If the RTE door follower setting is enabled, the countdown on the Door Held Open/Exit Delay time setting is suspended while the exit push button is depressed. The countdown on the Door Held Open/Exit Delay time setting only commences when the exit push button or similar type exit device is released.

Procedures

Steps to Set Reader Assignments without Anti-Pass Back

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit that is connected to the reader you are configuring.
3. Select the Doors tab.
4. Select the - Door # xx - that is assigned to the reader. This will highlight in yellow the Reader # associated with the corresponding door output.
    - By default door output #1 is assigned to reader port # 1; door output #2 is assigned to reader port # 2 and so on. Unless otherwise configured such as for anti-pass back where two readers may monitor a single door, leave the reader assignments on the default settings.

5. If the highlighted reader is an in reader leave the Direction field set on In. Otherwise click under the Direction column, select the ▼ symbol and set the direction to Out. Generally out is only selected where you are setting up directional readers in a controlled enter/exit environment to enforce anti-pass back or some other form of building control such as time clocks or evacuation.
6. If setting up readers for a KC Series Control Units, use the Protocol drop-down to select one of the available reader communication protocols (Wiegand, OSDP, Wiegand & OSDP).
7. When you have completed setting readers, click on the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Set Reader Assignments with Anti-Pass Back

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit that is connected to the reader you are configuring.
3. Select the Doors tab.
4. Select the - Door # xx - that is assigned to the reader. This will highlight in yellow the Reader # associated with the corresponding door output.
5. By default door output #1 is assigned to reader port # 1; door output #2 is assigned to reader port # 2 and so on. Unless otherwise configured such as for anti-pass back where two readers may monitor a single door, leave the reader assignments on the default settings.
6. If the highlighted reader is an in reader leave the Direction field set on In. Otherwise click under the Direction column, select the ▼ symbol and set the direction to Out. Generally out is only selected where you are setting up directional readers in a controlled enter/exit environment to enforce anti-pass back or some other form of building control such as time clocks or evacuation.
7. On the row with the highlighted reader, under the Anti-Pass Back heading, click in the box to enable the anti-pass back function. The box has an x when enabled.
8. Opposite Anti-Pass Back, click on the ▼ symbol and select the mode from the drop down list. Be sure to select a mode that is applicable to your configuration.
9. If certain door groups are exempted from anti-pass back restrictions, under Executive Access Group Range on the box to the left side click on the ▼ symbol and select either the first door group where a consecutive range of door groups applies or the only door group where a single door group applies.
10. Under Executive Access Group Range, on the box to the right side, click on the ▼ symbol and select either the last door group where a consecutive range of door groups applies or the same door group as selected in the previous step where a single door group applies.
11. If Executive Access Group Range was selected in the preceding step, perform one of the following steps:
    - On a Single ACU configuration - ensure that the box to the left of Global Executive Access is unchecked. Global Executive Access does not apply on a single ACU configuration.
    - On a multiple ACU configuration or multiple communication loop configuration - If different door groups are to have Executive Access at different panels, ensure that Global Executive Access is unchecked so that it is inactive.
    - On a multiple ACU configuration or multiple communication loop configuration - If the same door groups are to have Executive Access at all panels, ensure that Global Executive Access is checked. When checked the field is active.
    - If Timed Anti-pass back was selected as the mode, click on the symbol opposite Minutes and select a time interval in minutes from the drop down list.
12. If setting up readers for a KC Series Control Units, use the Protocol drop-down to select one of the available reader communication protocols (Wiegand, OSDP, Wiegand & OSDP).
13. Repeat the above procedures if setting additional readers.

14. Select the Save button.
15. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

First Person In

Anti-Pass Back Modes

Groups

Dual Custody Mode

Dual custody is a reader mode principally designed for doors leading to high security areas, such as server rooms, inventory rooms, vaults or other areas restricted from general access. Gaining access at an entry point where the reader is configured with dual custody requires successive card presentations by two different individuals using their own credentials. Individuals must be in valid groups assigned to access a dual custody reader.

Dual custody is structured such that you can arbitrarily assign classes of groups to access the reader when the schedule is ON and OFF depending on the level of security required.

Dual custody provides three classes of groups:

- Any Card Range - can be a single group or a contiguous range of groups but only cardholders in the specified groups have access
- Supervisor Range - can be a single group or a contiguous range of groups and would be persons in groups that act in a supervisory capacity over those persons in the any card range groups
- Master Range - are exempt from the dual custody reader protocol; however, individuals in master range groups must present their card twice at the dual custody reader to gain access

Dual custody allows specifying which classes of groups have access when the assigned schedule is ON and OFF:

- Any Two Cards
- One Supervisor and Any Card
- Two Supervisor Cards

Dual Custody Example

As an example, if One Supervisor and Any Card were selected when the schedule is ON, then one individual from a door group in the Supervisor Range and one cardholder from a door group in the Any Card Range would be required to present their cards to gain access; if Two Supervisor Cards were selected when the schedule is OFF, then 2 cardholders from a door group specified in the Supervisor Range would be required to present their cards to gain access.

Dual Custody Groups

Keyscan suggests that you create specific groups for dual custody.



Group assignments for dual custody cannot be higher than group #255. Keyscan recommends that credential holders are not assigned to more than one group in the Edit Person screen for dual custody access. See Credential Holders with Multiple Group Access Assignments below.

User Account

In order to setup dual custody, a system user account must have the following authority level enabled:

- Hardware / Edit Doors

Online Transactions

If you are observing the Online Transaction screen, the following captions indicate dual custody events:

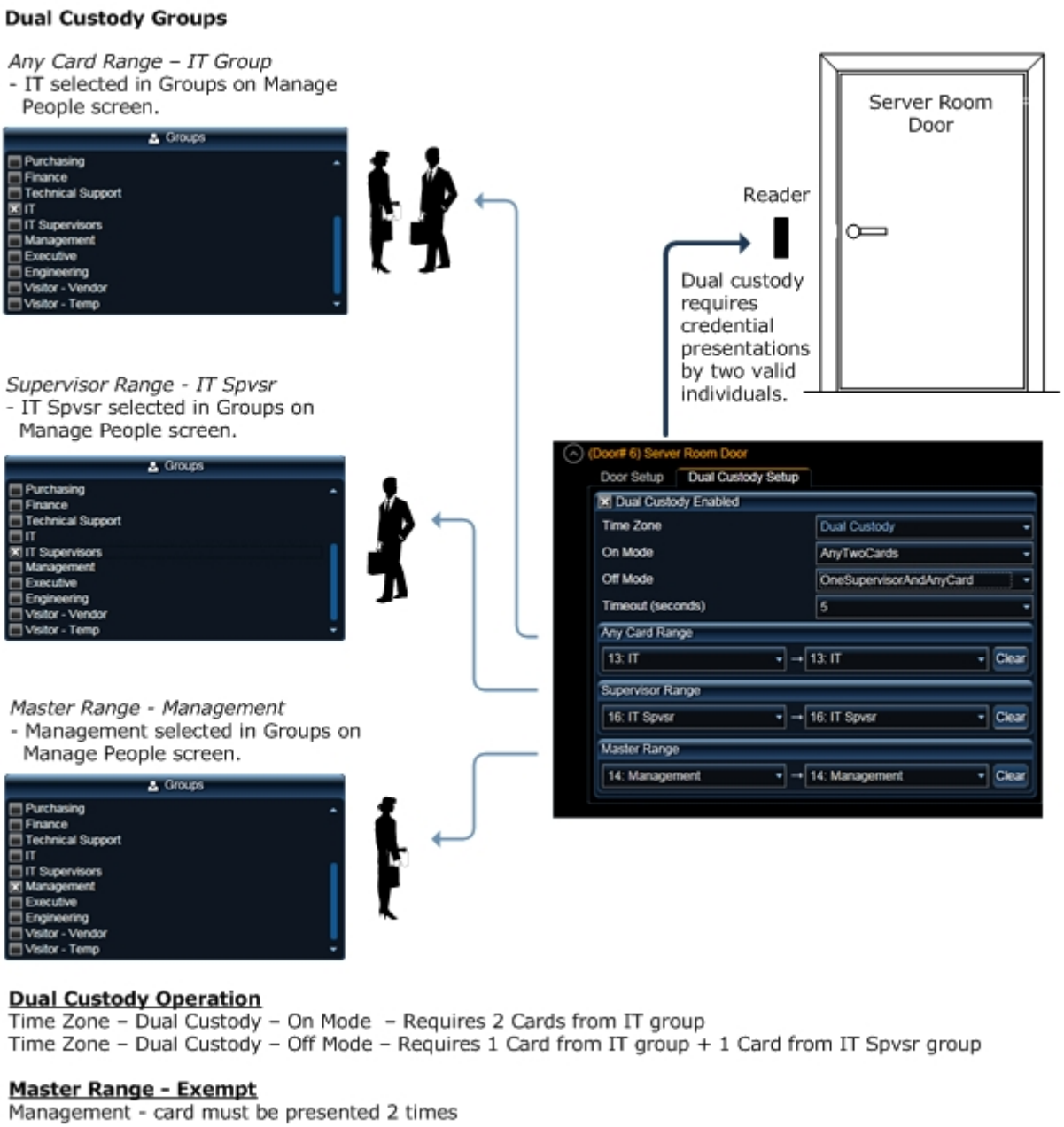
- Access Granted - Dual Custody Waiting - the first valid credential has been presented, the reader is waiting for the second valid credential but the entry point is still locked
- Access Granted - Dual Custody - the second valid credential has been presented and the entry point is unlocked
- Access Denied - Dual Custody Time Out - the second valid presentation did not occur within the specified time out period and the entry point remains locked
- Access Denied - Dual Custody Invalid - the first credential was presented from a door group not assigned to access the dual custody reader and the entry point remains locked
- Access Denied - Dual Custody Mismatch - the first credential presented was from a valid door group, but the second credential was presented from a door group not assigned to access the dual custody reader and the entry point remains locked

Credential Holders with Multiple Group Access Assignments

Please note the following where credential holders have multiple group assignments with valid access at the dual custody reader. In the Edit Person screen, ensure that the group with the lowest group number is, in the Dual Custody Setup screen, either the first group in a range or the only group under the applicable range mode - Any Card Range, Supervisor Range, or Master Range. If the credential holder is assigned to a group with a lower group number than the dual custody group that individual's credential presentation produces either an Access Denied Dual Custody Mismatch or Access Denied Dual Custody Invalid depending on whether it is presented first or second because it is outside the dual custody range. Entry is denied. You can verify the actual group numbers in the Group Setup screen under the Number column.

Illustration of Dual Custody

Example Screens of Dual Custody



Procedures

Steps to Set Dual Custody

Before configuring dual custody, you must have created schedules and groups.

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit connected to the door/reader that you are assigning with dual custody.
3. Select the Doors tab.
4. Select the appropriate door (Door # x) with the reader that you are assigning as a dual custody reader. Selecting the door reveals the Door Setup and Dual Custody Setup sub-menus.
5. Select the Dual Custody Setup tab if it is not currently selected.
6. Click in the box to the left of Dual Custody Enabled. The box has an x when selected.
7. Opposite Schedule, click on the ▼ symbol and select the desired schedule from the drop down list.

8. Opposite On Mode, click on the ▼ symbol and select the desired dual custody mode from the drop down list.
9. Opposite Off Mode, click on the ▼ symbol and select the desired dual custody mode from the drop down list.
    - The Off Mode can also be left on Not Assigned if it is not required.
10. Opposite Timeout, click on the ▼ symbol and select the number of seconds that the two successive card reads must occur within. If the two cards are not presented at the reader within this period, access is denied; the Online Transaction screen indicates Access Denied - Dual Custody Timeout.
11. If you selected Any Two Cards in the On Mode or the Off Mode above, click on the ▼ symbol of the left Any Card Range box and select the first door group in the range.
    - If you did not select Any Two Cards, leave both the left and right boxes blank and go to step 13.
12. Click on the ▼ symbol of the right Any Card Range box and select either the last contiguous group in the range, or if only one group, select the same group as selected in the preceding step.
13. If you selected either One Supervisor and Any Card or Two Supervisor Cards in the On Mode or the Off Mode, then click on the ▼ symbol of the left Supervisor Range box and select the first group in the range.
    - If you did not select either One Supervisor and Any Card or Two Supervisor Cards, leave both the left and right boxes blank and go to step 15.
14. Click on the ▼ symbol of the right Supervisor Range box and select either the last contiguous group in the range, or if only one group, select the same group as selected in the preceding step.
15. If you have groups that require access but are exempt from dual custody mode, click on the ▼ symbol of the left Master Range box, and select the first group in the range.
    - If you are not exempting any groups from dual custody at this reader, leave the Master Range boxes blank and go to step 17.
16. Click on the ▼ symbol of the right Master Range box and select either the last contiguous door group in the range or if only one group is exempt, select the same door group as selected in preceding step.
17. Click on the Save button.
18. To set another reader as a dual custody reader, repeat the preceding steps.
19. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Using Dual Custody

When presenting a credential to a reader that has been assigned with dual custody mode, observe the following procedures. Valid cards may be presented in any order.

1. The first individual in a valid group presents his or her credential at the reader. The reader LED goes off momentarily, then returns to red.
2. The second individual in a valid group presents his or her credential at the reader within the "timeout" period after the first presentation. The LED turns green and the entry point is accessible.
    - If a Dual Custody Timeout occurs, both credentials must be presented again

Related Topics

Groups

Anti-Pass Back

Anti-Pass Back prevents one individual from passing his or her credential back to another individual for later use. When anti-pass back is employed in a controlled enter/exit environment, after a credential is presented at an IN reader and enters, the credential must be presented at an OUT reader and exit before the system permits the credential to enter again. A controlled enter/exit environment with anti-pass back requires readers on both sides of the door or in some configuration that monitors and controls in/out activity.

Hardware Rules

Anti-pass back rules and modes will be governed by the type of communication boards installed:

- CIM Module Communication Loop: anti-pass back applies to the entire CIM communication loop
- CIM/CIM-Link Modules Communication Loops: anti-pass back applies to all configured CIM/CIM-Link communication loops
- CB-485/CPB-10-2 Communication: anti-pass back applies locally to the control board only

Refer to the respective Anti-pass back definitions based on your communication configuration below.

Single ACU or Single Communication Loop Anti-Pass Back Modes

Only one access control unit or multiple access control units on a single communication loop configured with CIM modules are used to control an enter/exit environment with designated in/out readers.

- Hard Anti-Pass Back Mode: With hard mode, a person presents a credential at a designated IN reader. After access is granted at the IN reader, the person must present the credential at an OUT reader. Presenting a credential consecutively at IN readers or OUT readers results in an access denied and generates an Access Denied with Anti-pass back Violation in the Online Transactions
- Hard Anti-Pass Back (Soft Anti-pass back in Communications Failure) Mode: Not applicable for a Single ACU configuration.
- Soft Anti-Pass Back Mode: With soft mode, a person presents a credential at a designated IN reader. After access is granted at the IN reader, the person must present the credential at an OUT reader. Presenting a credential consecutively at IN readers or OUT readers, however, results in an access granted but generates an Access Granted with Anti-pass back Violation in the Online Transactions.
- Timed Anti-Pass Back Mode: Timed anti-pass back mode can be used in a controlled enter/exit environment with IN/OUT readers or where a single reader is designated with anti-pass back.
    - Controlled enter/exit environment with IN/OUT readers: A credential cannot be presented consecutively to IN readers or OUT readers within the specified time otherwise access is denied and an Anti-pass back violation is generated in the Online Transactions. However, when access is granted at the IN reader, and the person presents the credential at the OUT reader, the timer is re-set to zero until the next IN or OUT read.
    - Single reader designated with anti-pass back: A person cannot be presented consecutively at the reader within a specified time limit otherwise access is denied and an Anti-pass back violation is generated in the Online Transactions.

Exemptions

- Executive Access: Executive Access exempts persons in the specified door groups from anti-pass back restrictions. Executive Access can be one door group or a consecutive range of door groups - groups assigned for executive access cannot be higher than group # 255

- Global Executive Access: Global Executive Access is not applicable for a single ACU configuration - for a single communication loop, Global Executive Access applies anti-pass back exemptions universally at all control units for the door group(s) specified under Executive Access

Multiple Communication Loops Anti-Pass Back Modes

Two or more access control communication loops configured with CIM-LINK modules are used to control an enter/exit environment. Integrating multiple communication loops for anti-pass back requires CIM-LINK communication hardware. Consult with your dealer/installer.

- Hard Anti-Pass Back Mode: With hard mode, a person presents a credential at a designated IN reader. After access is granted at the IN reader, the cardholder must present the credential at an OUT reader. Presenting a credential consecutively at IN readers or OUT readers results in an access denied and generates an Access Denied with Anti-pass back Violation in the Online Transactions.

- Hard Anti-Pass Back (Soft Anti-pass back in Communications Failure) Mode: The same as Hard Anti-pass back except that in the case of a communication failure between access control units, anti-pass back goes to soft mode and records violations in the Online Transactions.

- Soft Anti-Pass Back Mode: With soft mode, a person presents a credential at a designated IN reader. After access is granted at the IN reader, the person must present the credential at an OUT reader. Presenting a credential consecutively at IN readers or OUT readers, however, results in an access granted but generates an Access Granted with Anti-pass back Violation in the Online Transactions.

- Timed Anti-Pass Back Mode: Timed anti-pass back mode can be used in a controlled enter/exit environment with IN/OUT readers or where a single reader is designated with anti-pass back. Please note however, it applies only to the assigned access control unit. Timed anti-pass back mode cannot be enforced by multiple access control units.

    - Controlled enter/exit environment with IN/OUT readers: A person cannot be presented consecutively to IN or OUT readers within the specified time otherwise access is denied and an Anti-pass back violation is generated in the Online Transactions. However, when access is granted at the IN reader, and the cardholder presents the credential at the OUT reader, the timer is re-set to zero until the next IN or OUT read.

    - Single reader designated with anti-pass back: a person cannot be presented consecutively at the reader within a specified time limit otherwise access is denied and an Anti-pass back violation is generated in the Online Transactions.

Exemptions

- Executive Access: Executive Access exempts persons assigned to the specified door groups from anti-pass back restrictions and transaction violations. Executive Access can be one door group or a consecutive range of door groups

- Global Executive Access: Global executive access applies anti-pass back exemptions universally at all control units for the door group(s) specified under Executive Access

Related Topics

Configure Door & Reader Parameters

Door Status – Manual Overrides

Click on the link below for the Door Status – Manual Overrides topic.

Door Status – Manual Overrides

Reset Anti-Pass Back

Click on the link below for the Reset Anti-Pass Back topic.

Reset Anti-Pass Back

Name Auxiliary Outputs

The Auxiliary Output screen is used to name auxiliary outputs in both an ON state and an OFF state. Your dealer/installer should determine these names if the access control system uses auxiliary outputs connected to third party devices.

Relay States

The following table shows states for auxiliary outputs.

Device	Relay DIP Switch	Auxiliary Output Status	Possible TZ Status	LED State	Normally Closed Relay State	Normally Open Relay State
Aux Output Relay	Normal		Off			
Aux Output Relay	Normal		On			
Aux Output Relay	Reversed		Off			
Aux Output Relay	Reversed		On			

Legend

LED - On	Relay State Open
LED - Off	Relay State Closed
Auxiliary Output Status - Off	OCB8 Relay DIP Switch - Normal
Auxiliary Output Status - On	OCB8 Relay DIP Switch - Reversed

Procedures

Steps to Name Auxiliary Outputs

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the name of the site you are naming outputs.
2. From the Hardware Setup screen, double click on the control unit with the outputs you are naming.
3. Ensure that the Auxiliary Outputs tab is selected.
4. Under the On Name column, double click on the auxiliary output to be named.
5. Enter a name in the text box for the output when in the on state.
6. Under the Off Name column, double click on the same auxiliary output.
7. Enter a name in the text box for the output when in the off state.
8. Select the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Revise Auxiliary Output Names

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit with the outputs you are naming.
3. Ensure that the Auxiliary Outputs tab is selected.
4. Double click on the auxiliary output name you are revising.
5. Enter the revised name in the text box.
6. Repeat for any other output names you are revising.
7. Select the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Name Inputs - Assign to Outputs

Auxiliary Output Status

Name Inputs - Assign to Outputs

The Auxiliary Inputs screen is used to name an input and assign it to an output.

Generally, the name of the input should be descriptive of the device and location.

The input can also be assigned to an output. As an example, a motion sensor input could be assigned to an output connected to a CCTV system, whereby, if movement was detected, the motion sensor's input trips the output connected with a CCTV system which initiates an NVR to start recording.

Your dealer/installer should determine the input names and output assignments.

Procedures

Steps to Name an Input and Assign to an Output

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit with the inputs you are naming.
3. Ensure that the Inputs tab is selected.
4. Under the Name column, double click on the input to be named.
5. Enter a name for the input.
6. Under the Assigned to Output column, double click on the same input.
7. Select the ▼ symbol to the right and select the output you assigning from the drop down list.
8. Repeat the above procedures to name more inputs and assign to outputs.
9. Select the Save button.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Modify an Input Name

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit with the inputs you are naming.
3. Ensure that the Inputs tab is selected.
4. Under the Name column, double click on the input to be re-named.
5. Enter a new name for the input.
6. Repeat the above procedures to re-name more inputs.
7. Select the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Re-assign an Input to an Output

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit with the inputs you are naming.
3. Ensure that the Inputs tab is selected.
4. Locate the input being re-assigned with another output.

5. Under the Assigned to Output column, double click on the input row.
6. Select the ▼ symbol to the right and select the output from the drop down list.
7. Repeat the above procedures to re-assign inputs to outputs.
8. Select the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Name Auxiliary Outputs

Input Status

Input Status

Click on the link for below for the Input Status topic.

Input Status.

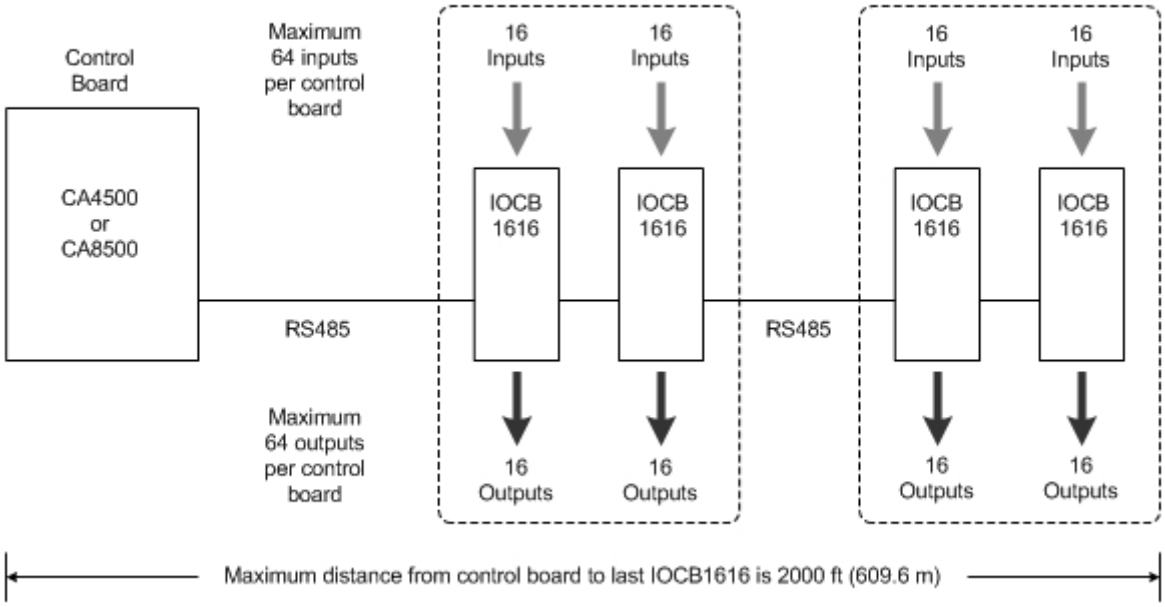
Auxiliary Output Status

Click on the link below for the Auxiliary Output Status topic.

Auxiliary Output Status

Introduction to the IOCB1616

The IOCB1616 is an auxiliary input/output control board with 16 inputs and 16 outputs. Designed for custom applications, the IOCB1616 connects to either a Keyscan 4 door control board or a Keyscan 8 door control board. The board's inputs and outputs connected on the same IOCB network can be used with timers, schedules, or be custom assignable to fit other dealer requirements without the need of a reader. The CA4500 or the CA8500 supports up to 4 (four) IOCB1616 boards for a total of 64 inputs/outputs.



The following lists some real-world examples of how the IOCB1616 can be used:

- Monitor door inputs and use request to exit devices without a reader assignment and trigger a sounder such as a siren or a sound alert.
- Trigger an auxiliary, third-party product such as an alarm panel or a CCTV product that starts a camera recording on a digital input trigger by using an optional output OCB-8 board.
- Monitor parking lot exit gates without readers in which timing is required.
- Use inputs to trigger a third party product by using an optional OCB-8 output control board.
- In sensitive areas where a single PIR motion detector may be triggered by air coolness or heat drafts, the IOCB1616 would allow the installation of two separate PIRs in the same area with conditional AND input programming so that both PIRs must be in alarm before firing an output to prevent false alarms.
- Customize input triggering output with timing for special applications such as switching lights, HVAC, etc.

These are just some of the possible uses.

Note + The IOCB1616 is not compatible with a CA250, CA150 or CA150WLN control boards.

Operating Modes

The IOCB1616 has the following modes that are set from the Client software.

Mode	Output	Input
Delayed Output	If the input remains in alarm past the specified output time, the output is triggered. The output remains triggered until the input is secured or closed.	Alarm immediately
Timed Output	If the input goes into alarm, the output is triggered. The output remains on for the duration of the specified output time.	Alarm immediately
Pulsed Output	If the input goes into alarm, the output is triggered. The output pulses off and on for the specified output time. The output remains triggered until the input is secured or closed.	Alarm immediately
(Input) RTE Mode	When an RTE device triggers, the associated input is shunted. The shunt time is the associated input time. The assigned output is triggered for the duration of the specified output time. When the associated input is closed or secured, all timers are reset.	Alarm immediately sent if the RTE input is not used as a shunt for the associated input. Alarm if input for the door contact is left open after the associated input time has expired.
Delayed Input and Output	If the input is triggered, the alarm is delayed. The input is delayed by the specified input time. The output is triggered at the end of the cumulative input and output times. The output remains triggered until the input is secured or closed.	The input's alarm is delayed until the input timer expires. Then it is sent to the software.
Delayed Input and Timed Output	If the input is triggered, the alarm is delayed. The input is delayed by the specified input time. The output remains on for the duration of the specified output time. The output remains triggered until the input is secured or closed.	The input's alarm is delayed until the input timer expires. Then it is sent to the software.
Delayed Input and Pulsed Output	If the input is triggered, the alarm is delayed. The input is delayed by the specified input time. The output pulses off and on for the specified output time. The output remains triggered until the input is secured or closed.	The input's alarm is delayed until the input timer expires. Then it is sent to the software.
Manual Pulse Control	Client enabled pulse option for an output. (Primarily for use with the active mapping module)	The output is pulsed for the specified output time.

Notes about IOCB1616 Modes

When an Input Schedule Assignment is used, the input remains shunted and does not notify the software regardless of the change of input state when a schedule is turned on.

When an Output Schedule Assignment is used, the output remains in a normal state when the schedule is on regardless of the input trigger.

Restoring associated inputs to normal resets the output state to normal.

The following modes are reserved for global inputs and outputs when used with an IOCB1616:

- Optional I/O Delayed Output
- Optional I/O Timed Output
- Optional I/O Pulsed Output

Example Applications

The following sub-headings outline examples of IOCB1616 modes.

Delayed Output

Example: Freezer Door - Need to know immediately that the freezer door is open and if the door remains open after a specified time an alarm sounds.

Input 1 is defined as the freezer door; Output 1 is defined as the freezer siren. Opening the freezer door trips Input 1 sending an alarm notification to the guard's computer. If the door remains open passed Output 1's specified delay time, the freezer siren is triggered notifying the client that the freezer door has been left open. The siren remains active until the freezer door is closed.

Timed Output

Example: Lights - Turn the lights on in a computer room as soon as motion is detected.

Input 2 is defined as the computer room motion detector; Output 2 is defined as the computer room lights. As soon as motion is detected in the room, Output 2 is triggered and remains active for the duration of Output 2's specified time. If motion is still detected the output remains active until the device does not sense movement.

Pulsed Output

Example: Notification - Warehouse notification when a truck arrives at the shipping dock.

Input 3 is defined as the shipping dock; Output 3 is defined as shipping dock strobe/siren. When a truck arrives at the shipping dock you can manually trigger Input 3 via a push button which will then pulse the strobe/siren for the duration of the specified output time.

Input/RTE Mode

Example: Automated Unlock at Exit Door - Control the exit point of a door without the use of an access control reader.

Input 4 is defined as the side door RTE (Request to Exit); Input 5 is defined as the Door Contact, Output 4 is defined as the door lock hardware. As the person walks towards the door, the RTE device will detect the individual; Output 4 will unlock the door hardware; Input 5 will shunt the door contact for the duration of the specified output time and allow the individual to exit without creating an alarm. (Input 4 must be triggered before Input 5; otherwise Input 5 reports an alarm in the Client software.)

Delayed Input & Delayed Output

Example: Monitoring - Monitor a low security stairwell door.

Input 5 is defined as the stairwell door; Output 5 is defined as the stairwell door strobe. If the stairwell door is opened, the alarm notification to the guard’s computer is delayed by the specified input delay time. Output 5 will not activate the strobe until the end of the cumulative input and output times have expired. The strobe stops when the input is secured.

Delayed Input & Timed Output

Example: Monitoring - Monitor a stairwell door.

Input 6 is defined as the stairwell door; Output 6 is defined as the stairwell door siren. If the stairwell door is opened, the alarm notification to the guard’s computer is delayed by the specified input delay time. Output 6 will not activate until the input time has expired; the siren remains on for the duration of the specified output time. It does not reset until the input is secured.

Delayed Input & Pulsed Output

Example: Monitoring - Monitor a stairwell door.

Input 7 is defined as the stairwell door; Output 7 is defined as the stairwell door siren. If the stairwell door is opened, the alarm notification to the guard’s computer is delayed for the specified input delay time. Output 7 will pulse on and off for the duration of the specified output time. It does not reset until the input is secured.

And - Or Conditions - Timers - Schedules

When assigning two or more inputs to an output, one of the following logic conditions must be specified:

OR

With the OR condition, when multiple inputs are assigned to a common output, any one input fires the output.

AND

With the AND condition, when two multiple points are assigned to any common output, both points need to go to an alarm state to fire the output.

You cannot have more than 2 inputs assigned to an output with an AND condition. You may have multiple sets of 2 inputs that use an AND condition assigned to the same output. An example would be Input 1 AND Input 2 assigned to Output 1 as well as Input 3 AND Input 4 assigned to Output 1.

Input and Output Timers

Input Timer - sets the delay time from the point the input is tripped. The range of time is from 00 seconds to 240 seconds. (00 seconds is no delay.) The Input Timer applies only on Modes 4 to 7.

Output Timer - sets the delay time from the point the output is tripped or the amount of time the output is enabled or activated depending on which of the 7 modes is selected. The range of time is from 00 seconds to 240 seconds. (00 seconds is no delay.)

Schedules to Inputs and Outputs

Input - allows assigning a schedule to enable/disable or arm/disarm the input during the schedule.

Output - allows assigning a schedule to an output to turn it off or on during the schedule.

Setup IOCB1616 Parameters

The following procedures outline how to setup the IOCB1616. Keyscan suggests you review the J17 - IOCB1616 Address Chart in the Hardware section of the IOCB1616 Setup Guide to ensure that the input/output assignments defined in the software match the addresses specified by the J17 jumper setting on the IOCB1616 circuit board.

Ensure that the IOCB1616 setting is enabled in the Hardware Setup > Additional Settings on the control board connected to the IOCB1616 boards.

Procedures

Steps to Create Input Names and Specify Input Timers

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on the control unit that is connected to the IOCB1616 in the All Hardware screen.
3. Select the IOCB1616 tab.
4. Double click on the IOCB Input # 1 or the first input point to be named.
5. In the text box, enter a name or description appropriate for the input point.
6. If applying Delayed Output, Timed Output or Pulsed Output operating mode for this input leave the Input Timer setting as is and go to the next step, otherwise double click on the input row under the Timer column, and select a delay time from the drop down list.
7. Repeat the preceding steps to add additional input points or continue to the next step if you have completed naming inputs.
8. Click on the Save button.
9. To add outputs follow the steps listed under Steps to Create Output Names and Specify Output Timers.

Steps to Create Output Names and Specify Output Timers

1. Select the IOCB Outputs tab.
    - If you are at the Client main screen, select the Site Management button > Hardware Setup > select the site if you have multiple sites > double click on the control unit that is connected to the IOCB1616 in the All Hardware screen > select the IOCB1616 tab > select the IOCB Outputs tab.
2. Double click on the IOCB Output # 1 or the first output to be named.
3. In the text box, enter a name or description appropriate for the output.
4. If you are applying a delay for this output, double click on the output under the Timer column and select a delay time from the drop down list. For no delay select 0 seconds.
5. Repeat the preceding steps to add additional outputs or continue to the next step if you have completed naming outputs.
6. Click on the Save button.
7. To assign inputs to outputs and set modes select the link below and complete the instructions or click on the Back button until you are returned to the main screen.

Steps to Assign Inputs to Outputs and Set Modes

1. Select the Rules tab.
    - If you are at the Client main screen, select the Site Management button > Hardware Setup > select the site if you have multiple sites > double click on the control unit that is connected to the IOCB1616 in the All Hardware screen > select the IOCB1616 tab > select the Rules tab.

2. Click on the row with the first applicable primary input to be assigned to an output. The row is highlighted in blue.
3. On the input row highlighted in blue, double click under the Operator column, and choose the desired operator - AND, OR, or RTE - from the drop down list.
    - If assigning just a single input to a single output, leave the setting on Not Used. If you make an error or need to clear the assignment, select Clear Operator and Secondary Input.
4. Under the Secondary Input column, double click on the highlighted row, and choose the desired secondary input from the drop down list.
    - If you are not assigning a secondary input, leave the field blank.
5. Under the Output column, double click on the highlighted row, and choose the desired output from the drop down list.
6. Under the Mode column, double click on the highlighted row, select the symbol and choose the desired mode from the drop down list.
7. Repeat setting inputs, operators, outputs, and modes. When you have completed assigning inputs to outputs, click on the Save button.
8. If you have additional IOCB1616 boards connected to other access control units, repeat all the above procedures to define and assign the inputs and the outputs; otherwise click on the Back button until you are returned to the main screen or select the Navigation History button for a previously viewed screen.

Note +

When a row of inputs/outputs is either incomplete or has incorrect assignments, it changes to red if a new row is selected. Until you have corrected or completed the current input/output row you cannot assign any other inputs and outputs.

Related Topics

Assign Schedules to IOCB1616 Inputs and Outputs

IOCB1616 Input Status

Click on the link below for the IOCB1616 Input Status topic.

IOCB1616 Input Status

IOCB1616 Output Status

Click on the link below for the IOCB1616 Output Status topic.

IOCB1616 Output Status

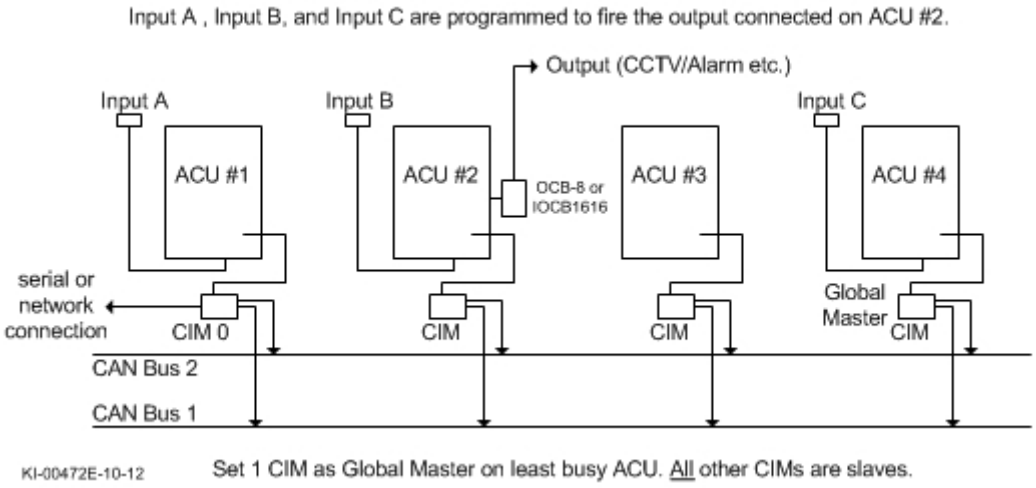
Global I/O Overview

The purpose of using the Global I/O function is to save on cable hardware costs when configuring alarm inputs to fire alarm outputs across multiple access control units where the following communication modes exist:

- single communication loop on CAN Bus 2 with CIM modules
- multiple communication loops on CAN Bus 2 with CIM & CIM-LINK modules

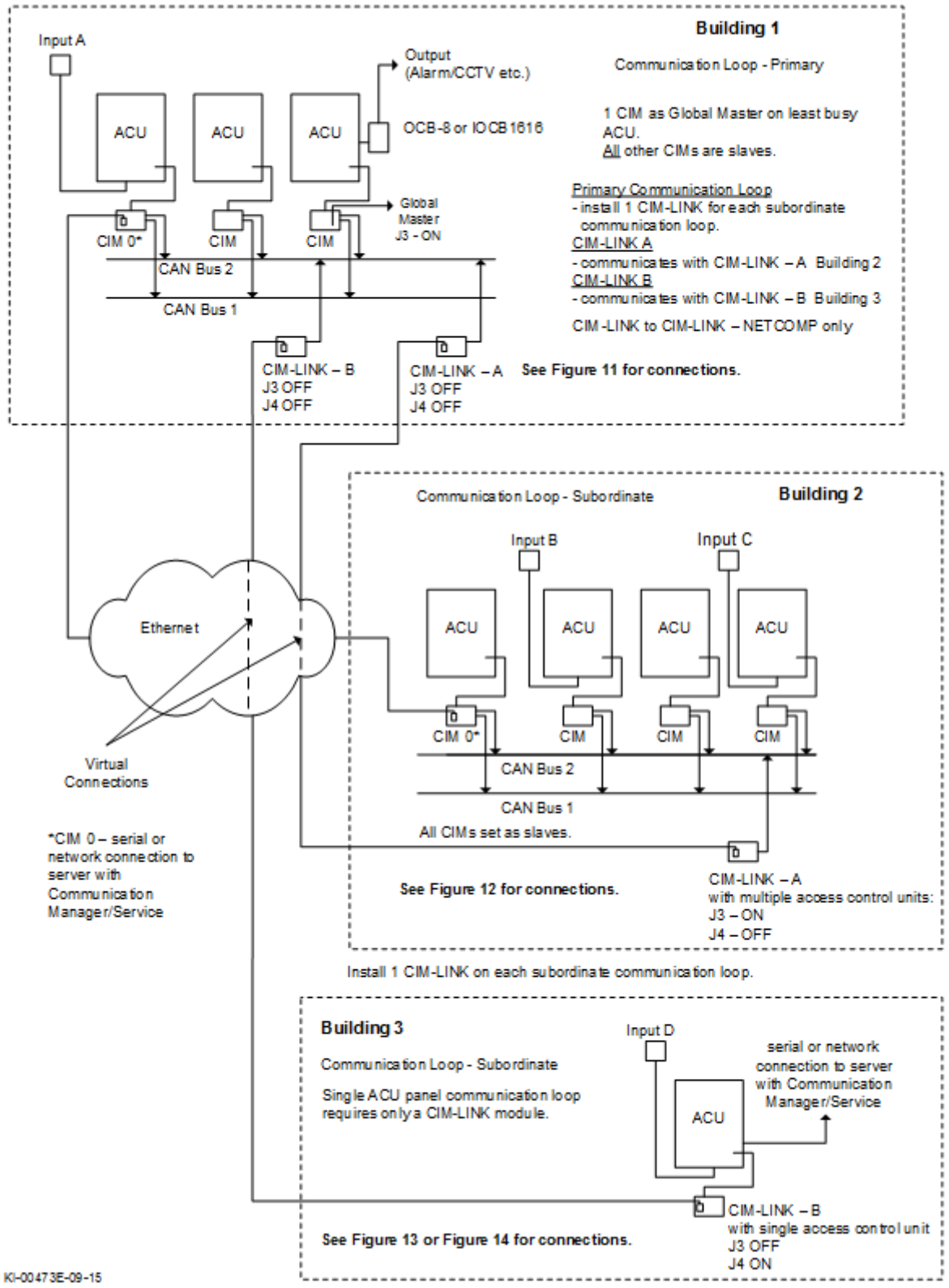
For more information on global inputs and outputs, refer to the Global Inputs and Outputs / Time Zones document on the Aurora Documents folder included with the Aurora Software Installation files.

Global I/Os on a Single CAN Bus Communication Loop



Global I/Os on Multiple Communication Loops Connected with CIM-LINK Modules

Input A, Input B, Input C, and Input D programmed to fire the output in Building 1.



Setup Global Inputs and Outputs

Aurora's Global I/O interface screen allows you to program alarm inputs to trip outputs across multiple access control units where the following communication modes exist.

- single communication loop - CIM modules
- single communication loop - ECM modules (legacy product)
- multiple communication loops - CIM modules & CIM Link modules
- multiple communication loops - ECM modules & GGM modules (legacy products)

When using an OCB-8 for global outputs, the OCB-8 ribbon cable must be connected to Control 5 on either a CA4500 4 door control unit or a CA8500 8 door control unit.

When assigning 2 or more inputs to an output, the Client applies an OR condition. Hence each assigned input will independently trip the output. All input points must be cleared or reset to clear the output.

OCB-8 Global Output Relay #/ Client Relay

- Global IO Relay 1 = AO # 09 in Client software
- Global IO Relay 2 = AO # 10 in Client software
- Global IO Relay 3 = AO # 11 in Client software
- Global IO Relay 4 = AO # 12 in Client software
- Global IO Relay 5 = AO # 13 in Client software
- Global IO Relay 6 = AO # 14 in Client software
- Global IO Relay 7 = AO # 15 in Client software
- Global IO Relay 8 = AO #16 in Client software

Your dealer/installer should setup the Global I/0 input to output assignments. For installers & dealers, refer to the Global I/O & TZ document on the Keyscan Product Documentation Library CD for more information on hardware and CAN Bus requirements and configuration schemes.

Procedures

Steps to Setup Global Inputs and Outputs

1. From the Client main screen, select the Site Setup button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
2. From the Hardware Setup screen, double click on any control unit listed in the All Hardware screen.
3. Click on the Global I/O tab.
4. Opposite Access Control Unit, click on the ▼ symbol to the right and select the access control unit that is connected to the device which will be designated as the input Trigger Device.
5. Click on the + button.
6. Below the Input Trigger heading, click on the row which was just added after you clicked on the + button.
7. Click on the ▼ symbol below Input Trigger, and select the designated triggering input from the drop down list.

8. Below the lower Access Control Unit heading, click on the same row as the Input Trigger above.
9. Click on the ▼ symbol below Access Control Unit, and select the access control unit which is connected to the output device.
10. Below the Output heading, click on the same row.
11. Click on the ▼ symbol below Output, and select the output from the drop down list.
    - OCB-8 global outputs must be connected to Control 5 on the control board.
12. If applicable, to enable either Door Alarm Tripped or Door Held Open alarms, click in the box to the left. This only applies if you are assigning doors as Global Input Triggers and wish to engage either alarm as a triggering mechanism for the output.
    - When enabled the box has an x.
    - When disabled the box is blank.
13. Click on the Save button.
14. To add more input and output assignments, repeat the above steps.
    - You may configure multiple inputs to trip one output.
15. When you have completed assigning inputs and outputs, select the Back button until returned to the main screen or for a previously viewed screen, select the Navigation History ▼ symbol.

Related Topics

Assign Schedules to Inputs

Add an NVR & Specify Settings

NVR integration with Aurora requires the purchase of the video license. Keyscan Aurora supports the following manufacturer's NVRs:

- Avigilon
- Exacq
- Milestone
- i3 International
- Open Eye & Open Eye E-Series
- Salient Systems
- OnSSI
- HikVision

For installing and configuring NVRs, follow the specific instructions for each supported manufacturer's NVR below.

Milestone - Important

For the Aurora Client to activate the cameras connected to the Milestone NVR, set the Camera Shortcut Number in the Milestone software's Camera Properties screen to match the Camera Number in the Aurora Client's Hardware Setup screen. The Camera Shortcut Number may also be described as Shortcut Number or Camera Shortcut depending on the Milestone software version.

OnSSI - Important

In order to integrate the OnSSI CCTV system with Aurora, you must download the C2P Keyscan Bridge Settings software from OnSSi at https://c2p.com/c2p-keyscan-bridge. Select the Download menu and obtain the software and the installation guide.

- To obtain the installation instructions, the Install and Use Guide, select the link below C2P Keyscan Bridge
- To download the C2P Keyscan Bridge Settings software, select the Fully Functional CP2 Bridge 30 Day Demo and follow the prompts



After you have configured the NVR, it is accessed by selecting the Video Integration button on the main screen.

Keyscan Specification CCTV Integration

The Keyscan Specification CCTV Integration setting in the Hardware Setup screen is reserved for NVR applications in which the end-user has arranged directly with an NVR manufacturer to configure the NVR to Keyscan Aurora CCTV specifications. Do not select this CCTV Integration option unless you are aware that your

NVR supplier has configured your NVR with these specifications. For more information contact Keyscan's marketing department at one of the numbers listed below.

- Toll free - Canada or U.S.A.: 1.888.539.7226
- Elsewhere: + 905.430.7226

Procedures

Steps to Add a Milestone NVR

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Install Milestone Viewer Setup

You will require access to your Keyscan Aurora Software Installation files. Install the Milestone Viewer at a server where you currently have a Keyscan Aurora Client installed which will be used for monitoring the Milestone NVR and cameras.

1. Open the folder containing the Aurora Software Installation files.
2. Locate the AuroraInstallation.exe file, right click the file and select Run as Administrator.
3. If you are presented with the User Account Control dialog box, click on the Yes button.
4. From the Aurora Installation screen, select the Integrations and Drivers option.
5. Open the Milestone Keyscan Viewer folder.
6. Locate and double click on the MilestoneKeyscanViewerSetup.exe file.
7. If you are presented with the User Account Control dialog box, click on the Yes button. Wait while the InstallShield Wizard loads.
8. From the Keyscan Aurora Milestone Viewer - Install Shield screen, click on the Next > button and follow the on-screen prompts.
    - You may have to click on the InstallShield Wizard's icon in Windows task bar at the bottom of the screen.

Configure the Milestone NVR in the Aurora Client

1. At the server location with the Aurora Client, and where you installed the MilestoneKeyscanViewerSetup.exe, select the Windows start icon > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora.exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the symbol on the right of the Add 8 Door Controller button, and select Milestone CCTV Integration from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the Milestone NVR you are configuring is on the list of supported Milestone NVRs and click on Yes.
    - If your Milestone NVR is not on the list, select No and call Keyscan to confirm if your model is supported.

6. In the Name text box enter a desired name or description for the Milestone NVR.
7. In the Host text box, enter the following information depending on the type of IP address.
    - Static IP - enter the static IP address assigned to the NVR - example 192.168.100.165
    - Dynamic IP - enter the Unit Name or Domain Name assigned to the NVR
8. Confirm that the port setting in Aurora matches the port setting in the Milestone NVR software. Aurora enters a default setting of 80 in the Port Address field. If another port is specified in the Milestone NVR software, change the Aurora port setting so it is the same in both software applications.
    - The Authentication Type is defaulted to Basic and cannot be changed.
9. Enter the User Name and Password. This must be the same user name and password that is used in the Milestone NVR software.
10. Below the Cameras heading under the Name column, as an option you can name the cameras so they have the same description that is used in the Milestone NVR software for easier reference when viewing cameras in the Aurora software.
11. If you have more or fewer cameras connected than the number of cameras listed on the Hardware Setup screen, insert the cursor in the text box opposite the Cameras heading at the top and enter the number of connected cameras. Then select the Update button.
    - This will re-configure the list to match the actual number of connected cameras.
    - The Type column is not applicable for Milestone regardless of whether the setting is Analog, IP, or Megapixel.
12. Select the Save button.
13. Click on the Back button until you are at the main screen.
14. To verify that you have correctly configured the Milestone NVR, click on the Video Integration button and click on Milestone to open the Aurora Milestone Viewer.

Steps to Add an Avigilon NVR

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Install Avigilon Viewer Setup

You require access to the Keyscan Aurora Software Installation files. Install the Avigilon Viewer at a server/ workstation where you currently have a Keyscan Aurora Client installed which will be used for monitoring the Avigilon NVR and cameras.

1. Open the folder containing the Aurora Software Installation files.
2. Locate the AuroraInstallation.exe file, right click the file and select Run as Administrator.
3. If you are presented with the User Account Control dialog box, click on the Yes button.
4. From the Aurora Installation screen, select the Integrations and Drivers option.
5. Open the Avigilon Keyscan Viewer folder.
6. Locate and double click on the Keyscan Avigilon Viewer Installer file that corresponds to your Avigilon NVR model.
7. If you are presented with the User Account Control dialog box, click on the Yes button. Wait while the InstallShield Wizard loads.
8. From the Keyscan Avigilon Viewer - Install Shield screen, click on the Next > button and follow the on-screen prompts.

Configure the Avigilon NVR in the Aurora Client

1. At the server/workstation location with the Aurora Client, and where you installed the Keyscan Avigilon Viewer, select Windows start > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora .exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the ▼ symbol on the right of the Add 8 Door Controller button, and select Avigilon Control Center from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the Avigilon NVR you are configuring is on the list of supported Avigilon NVRs and click on Yes.
    - If your Avigilon NVR is not on the list, select No and call Keyscan to confirm if your model is supported.
6. In the Name text box enter a desired name or description for the Avigilon NVR.
7. In the Host text box, enter the IP address of the Avigilon NVR. You may have to consult with the network administrator.
8. Confirm that the port setting in Aurora matches the port setting in the Avigilon NVR software. Aurora enters a default setting of 38880 in the Port Address field. If another port is specified in the Avigilon NVR software, change the Aurora port setting so it is the same in both software applications.
9. Enter the User Name and Password. This must be the same user name and password that is used in the Avigilon NVR software.
10. Below the Cameras heading under the Name column, as an option you can name the cameras so they have the same description that is used in the Avigilon NVR software for easier reference.
11. By default 48 cameras are listed on the Hardware Setup screen. If you have more cameras, insert the cursor in the text box opposite the Cameras heading at the top and enter the number of connected cameras to expand the list. Then select the Update button.
    - If you have fewer than 48 cameras connected to the NVR, you can also change the value in the # of cameras box to clear the list of unused cameras. If you change the value, be sure to click on the Update button. This will re-configure the list to match the actual number of connected cameras.
    - The Number column on the left represents the camera's logical ID. When you open the Avigilon Viewer, selecting a camera is determined by the camera's logical ID and not the description in the Name column.
    - The Type column is not applicable regardless of whether the setting is Analog, IP, or Megapixel.
12. Select the Save button.
13. Click on the Back button until you are at the main screen.
14. To verify that you have correctly configured the Avigilon NVR, click on the Video Integration button and click on Avigilon to open the Avigilon Viewer. Enter the Logical ID of a camera and click on OK.

Note

The Avigilon Viewer displays only one camera. However, you may open multiple viewers to monitor different cameras simultaneously. Repeat step 14 above, except enter the Logical ID of a different camera.

 *Steps to Add an Exacq NVR*

Preliminary

You must have installed the Exacq software and configured both the NVR and cameras with all necessary settings so the CCTV system is functioning.

Servers or workstations designated for monitoring the Exacq CCTV system via Aurora must have an Aurora Client and an exacqVision Client installed.

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Obtain Exacq NVR Settings and Camera Names

Before you can configure the Aurora Client, you must obtain the following settings from the Configuration screen in the Exacq Vision Client software:

- the Exacq NVR address exactly as shown under the IP Address column
- the port assigned to the Exacq NVR as listed in the Configuration screen
- the names of the cameras exactly as they are labelled in the Live Cameras screen

You may have to refer to the Exacq NVR documentation.

Configure the Exacq NVR Settings

1. At the server location with the Aurora Client, select the Windows start icon > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora .exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the symbol on the right of the Add 8 Door Controller button, and select Exacq CCTV Integration from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the Exacq NVR you are configuring is on the list of supported Exacq NVRs and click on Yes.
    - If your Exacq NVR is not on the list, select No and call Keyscan to confirm if your model is supported.
6. In the Name text box enter a desired name or description for the Exacq NVR.
7. In the Host text box, enter the IP address of the NVR exactly as it is entered in the exacqVision Client software.
8. Enter the port setting so it is the same as the port listed in the exacqVision Client software.
    - By default, Aurora is set on the default Exacq NVR port setting. Ensure that you enter the correct port if it has been changed in the Exacq software.
9. Bypass the User Name and Password settings. They are not applicable.
10. Below the Cameras heading under the Name column, enter the name of each camera as it is defined on the Live Cameras screen in the exacqVision Client software.
11. By default 24 cameras are listed on the Hardware Setup screen. If you have more cameras, insert the cursor in the text box opposite the Cameras heading at the top and enter the number of connected cameras to expand the list. Then select the Update button.
    - If you have fewer than 24 cameras connected to the NVR, you can also change the value in the # of cameras box to clear the list of unused cameras.

12. Bypass the Type settings. They are not applicable.
13. Select the Save button.
14. Click on the Back button until you are at the main screen.
15. To verify that you have correctly configured the Exacq NVR, click on the Video Integration button and click on Exacq to open the exacqVision Client.

Steps to Add an i3 International NVR

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Servers or workstations designated for monitoring the i3 International CCTV system via Aurora must have an Aurora Client and an i3 International Client installed.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Configure the i3 International NVR Settings

1. At the server location with the Aurora Client, select the Windows start icon > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora .exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the symbol on the right of the Add 8 Door Controller button, and select i3 International CCTV Integration from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the i3 International NVR you are configuring is on the list of supported i3 International NVRs and click on Yes.
    - If your NVR is not on the list, select No and call Keyscan to confirm if your model is supported.
6. In the Name text box enter the same name that is entered in the Video Pilot Client software's Server ID field.
7. In the Host text box, enter the IP address or server name of the i3 International NVR.
8. Leave the Port setting on the default address; if the port address was changed, enter the correct port address.
9. Under the Login Credentials heading, enter the same user name and password that is used to log on to the i3 International NVR.
10. Below the Cameras heading under the Name column, as an option you can name the cameras so they have the same description that is used in the i3's Video Pilot software for easier reference.
    - By default 16 cameras are listed under the Camera heading. If you require more cameras listed, enter the total cameras connected to the I3 NVR in the # text box to the right of Cameras. Click on the Update button. The list is re-populated with the desired number of cameras.
11. Click on the Save Button.
12. Click on the Back button until you are at the main screen.
13. To verify that you have correctly configured the i3 International NVR, click on the Video Integration button and click on i3 International to open the Video Pilot client.

Steps to Add Open Eye & Open Eye E-Series NVR

Preliminary

You must have installed the Open Eye software and configured both the NVR and cameras with all necessary settings so the CCTV system is functioning.

Servers or workstations designated for monitoring the Open Eye CCTV system via Aurora must have an Aurora Client and the Open Eye monitoring software installed.

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Obtain Open Eye NVR Settings

Before you can configure the Aurora Client, you must obtain the following settings from the Configuration screen in the Open Eye software:

- the Open Eye NVR IP address
- the port assigned to the Open Eye NVR
- the Open Eye NVR user name and password

Configure the Open Eye NVR Settings

1. At the server location with the Aurora Client, select the Windows start icon > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora .exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the symbol on the right of the Add 8 Door Controller button, and select Open Eye CCTV Integration or Open Eye E-Series CCTV Integration from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the Open Eye NVR you are configuring is on the list of supported Open Eye NVRs and click on Yes.
    - If your Open Eye NVR is not on the list, select No and call Keyscan to confirm if your model is supported.
6. In the Name text box enter a desired name or description for the Open Eye NVR.
7. In the Host text box, enter the IP address of the NVR exactly as it is entered in the Open Eye software.
8. Enter the port setting so it is the same as the port listed in the Open Eye software.
    - By default, Aurora is set on the default Open Eye NVR port setting of 2000. Ensure that you enter the correct port if it has been changed in the Open Eye software.
9. In the User Name and Password text boxes under Login Credentials, enter the same settings as entered in the Open Eye software.
10. Below the Cameras heading under the Name column, as an option you can name the cameras as they are described in the Open Eye software.
    - Camera #1 in the Aurora Client = Camera #1 in the Open Eye software and so on.

11. By default 16 cameras are listed on the Hardware Setup screen. If you have more or fewer cameras, insert the cursor in the text box opposite the Cameras heading at the top and enter the number of connected cameras to adjust the list. Then select the Update button.
12. Bypass the Type settings. They are not applicable.
13. Select the Save button.
14. Click on the Back button until you are at the main screen.
15. To verify that you have correctly configured the Open Eye NVR, click on the Video Integration button and click on Open Eye to open the Open Eye monitoring software.

Steps to Add a Salient Systems NVR

Preliminary

You must have installed the Salient Systems software and configured both the NVR and cameras with all necessary settings so the CCTV system is functioning.

Servers or workstations designated for monitoring the Salient Systems CCTV system via Aurora must have an Aurora Client and the Salient Systems software installed.

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Obtain Salient Systems NVR Settings

Before you can configure the Aurora Client, you must obtain the following settings from the Salient Systems software:

- the NVR IP address or host name
- the port assigned to the Salient Systems NVR
- the Salient Systems NVR user name and password

Configure the Salient NVR Settings

1. At the server location with the Aurora Client, select the Windows start icon > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora .exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the symbol on the right of the Add 8 Door Controller button, and select Salient Systems CCTV Integration from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the Salient Systems NVR you are configuring is on the list of supported NVRs and click on Yes.
    - If your Salient Systems NVR is not on the list, select No and call Keyscan to confirm if your model is supported.

6. In the Name text box enter a desired name or description for the Salient Systems NVR.
7. In the Host text box, enter the IP address or the host name of the NVR exactly as it is entered in the Salient Systems software.
8. By default, Aurora is set on the default Salient Systems NVR data port setting of 4242. Ensure that you enter the correct port if it has been changed in the Salient Systems software.
9. In the User Name and Password text boxes under Login Credentials, enter the same settings as entered in the Salient Systems software.
10. Below the Cameras heading under the Name column, as an option you can name the cameras as they are described in the Salient Systems software.
    - Camera #1 in the Aurora Client = Camera #1 in the Salient Systems software and so on.
11. By default 16 cameras are listed on the Hardware Setup screen. If you have more or fewer cameras, insert the cursor in the text box opposite the Cameras heading at the top and enter the number of connected cameras to adjust the list. Then select the Update button.
12. Bypass the Type settings. They are not applicable.
13. Select the Save button.
14. Click on the Back button until you are at the main screen.
15. To verify that you have correctly configured the NVR, click on the Video Integration button and click on Salient Systems to open the monitoring software.

Steps to Add an OnSSI NVR

Important Keyscan Default Setting

When configuring the OnSSI CCTV system for integration with Keyscan Aurora, you must complete OnSSI's C2P Bridge Settings screen. For simplified integration, Keyscan recommends using the following default setting in the C2P Bridge Settings screen.

- Enter 127.0.0.1 in the Client field when creating a Dispatch Entry Key for each camera.

The C2P Bridge Settings must be downloaded as noted above. The Bridge Settings software is not included with the NVR.

Preliminary

You must have installed the OnSSI software and configured both the NVR and cameras.

Servers or workstations designated for monitoring the OnSSI CCTV system via Aurora must have an Aurora Client and the OnSSI software installed.

These instructions assume that you have previously installed Keyscan Aurora. If not, first install the Keyscan Aurora software.

Registration

Before you begin the procedures outlined below, register your Keyscan video license. See Software Registration.

Obtain OnSSI NVR Settings

Before you can configure the Aurora Client, you must obtain the following settings from the OnSSI software:

- the OnSSI NVR user name and password
- the dispatch entry key* for each camera

*The dispatch entry key is case sensitive.

Configure the OnSSI NVR Settings

Keyscan recommends that you use the default host and port settings in the Aurora Client's Hardware Setup screen.

1. At the server location with the Aurora Client, select the Windows start icon > All Programs > Keyscan Inc > Keyscan Aurora Client > Launch Aurora.exe.
2. Enter your Keyscan User Name and Password. Click on the key symbol.
3. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site in the Hardware Setup directory screen.
4. From the Hardware Setup screen, click on the ▼ symbol on the right of the Add 8 Door Controller button, and select OnSSI CCTV Integration from the drop down list.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
5. From the Confirm Hardware Installation box, ensure that the OnSSI NVR you are configuring is on the list of supported NVRs and click on Yes.
    - If your OnSSI Systems NVR is not on the list, select No and call Keyscan to confirm if your model is supported.
6. In the Name text box enter a desired name or description for the OnSSI NVR.
7. If you are following Keyscan's recommended settings, leave the Host Address on the default IP address setting.
8. If you are following Keyscan's recommended settings, leave the Port on the default setting. If it has been changed in the OnSSI software, ensure that you enter the correct port .
9. In the User Name and Password text boxes under Login Credentials, enter the same settings as entered in the OnSSI software.
10. Below the Cameras heading under the Name column, enter the camera's Dispatch Entry Key exactly as entered in the C2P Keyscan Bridge Settings screen. The Dispatch Entry Key is case sensitive.
11. Repeat step 10 until you have entered all cameras.
    - By default 16 cameras are listed on the Hardware Setup screen. If you have more or fewer cameras, insert the cursor in the text box opposite the Cameras heading at the top and enter the number of connected cameras to adjust the list. Then select the Update button.
12. Bypass the Type settings. This setting is not applicable.
13. Select the Save button.
14. Click on the Back button until you are at the main screen.
15. To verify that you have correctly configured the NVR, click on the Video Integration button and click on OnSSI to open the monitoring software.

Related Topics

Milestone NVR Viewer

Configure an Elevator Control Unit

The Elevators screen inputs elevator control board settings to interface with the Aurora software so you may establish which credential holders have access to specific floors at specific times within the elevator system. Elevator control units have the following labels in the Client software:

- 40 Floor (1 Cab) = EC1500 elevator control unit
- 16 Floor (2 Cab) = EC2500 elevator control unit

Unit ID Naming Structure

When adding elevator control units in the Elevators / Hardware Setup screen, the Client software assigns the following names to the control units by default as follows:

Elevator Control Units

- Elevator Control Unit #1
- Elevator Control Unit # 2

Each time a unit is added the software increases the unit # by 1. You can elect to use the default names or change the elevator control unit names. If you change the names, Keyscan recommends maintaining a consistent naming format and using descriptions that other system users can understand.

Elevator Screen

The Elevator screen consists of two sub-screens for configuring elevator control units:

- Information
- Elevator Floor Timers

The following two sub-headings review the elevator fields for each respective screen.

Information

- Name - the Aurora software by default names the first elevator controller Elevator Control Unit #1 and increments the number by 1 for each unit added
- Serial Number - each control unit has a factory installed serial number marked on the control board and listed on the invoice and packing slip
- Password - it is recommended to retain the default password KEYSCAN; if another password is created, be sure to record it
- Type - lists the unit series
- Status - indicates the current state of the panel: active, inactive, disabled or disaster recovery
    - Panel status must be active to communicate with the software
- Regional Time Zone - select the time zone where the unit is located geographically
- Hardware Notes - text field to describe where the control unit is mounted within the building or site so it can be located for future maintenance
- Communication - one of three modes: Serial, Network, Reverse Network can be configured for panel communication

- Elevator bank - indicates the elevator bank the elevator cab is assigned to
- Floors - names elevator floors & numbers

Elevator Floor Timers

- Floor Button Selection Time - The floor button selection time is the number of seconds that the authorized elevator floor buttons are active after a valid card is presented to the reader.
- Telephone Entry Interface Floor Button Selection Time - Designed for buildings that have an integrated telephone entry system, the Set Elevator Names screen has a Telephone Interface Floor Button Selection Time field. This field sets the number of seconds that the authorized elevator floor buttons are active after a visitor has been "buzzed in" via the telephone system.

Elevator Banks

In the Client software, schedules and group access are assigned to elevator banks, not individual elevators. Individual elevators are in turn assigned to an elevator bank.

Elevator Bank Names

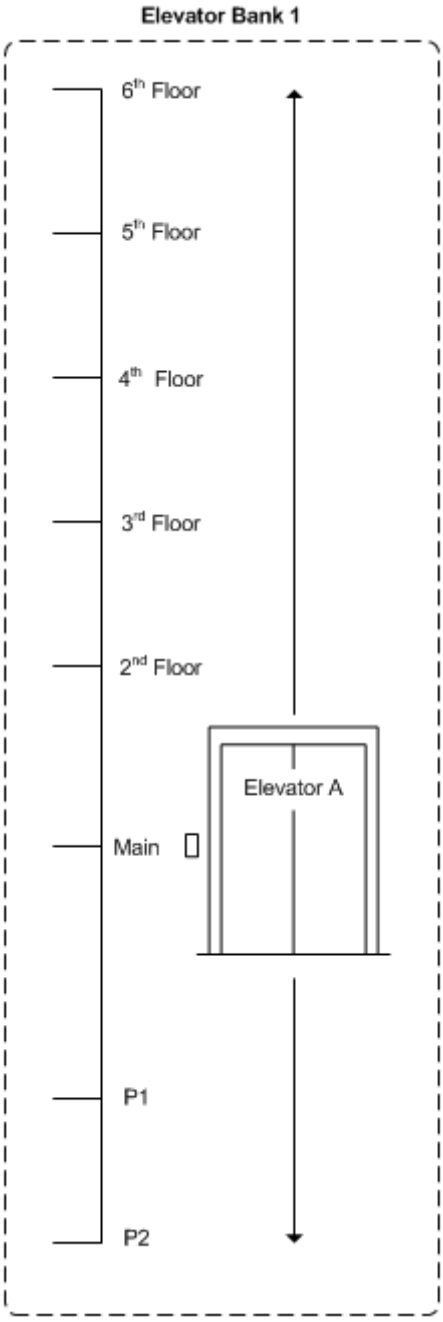
The Client software creates a default Elevator Bank # 1 when the first elevator control unit is added to the site.

After the first elevator control unit has been added, any time another elevator control unit is added to the site, you are prompted with a dialog box. You can create a new elevator bank or assign the elevator to an existing elevator bank. This will depend on how you regulate the elevators based on group access and schedules. See the examples of elevator banks below.

Example of Single Elevator & Elevator Bank

This example shows a basic configuration of 1 elevator in the building. Elevator A is regulated by the schedules, auto unlock floor buttons and group access levels assigned to Elevator Bank 1. Even though there is only 1 elevator it must be assigned to an elevator bank.

Example of Single Elevator Bank



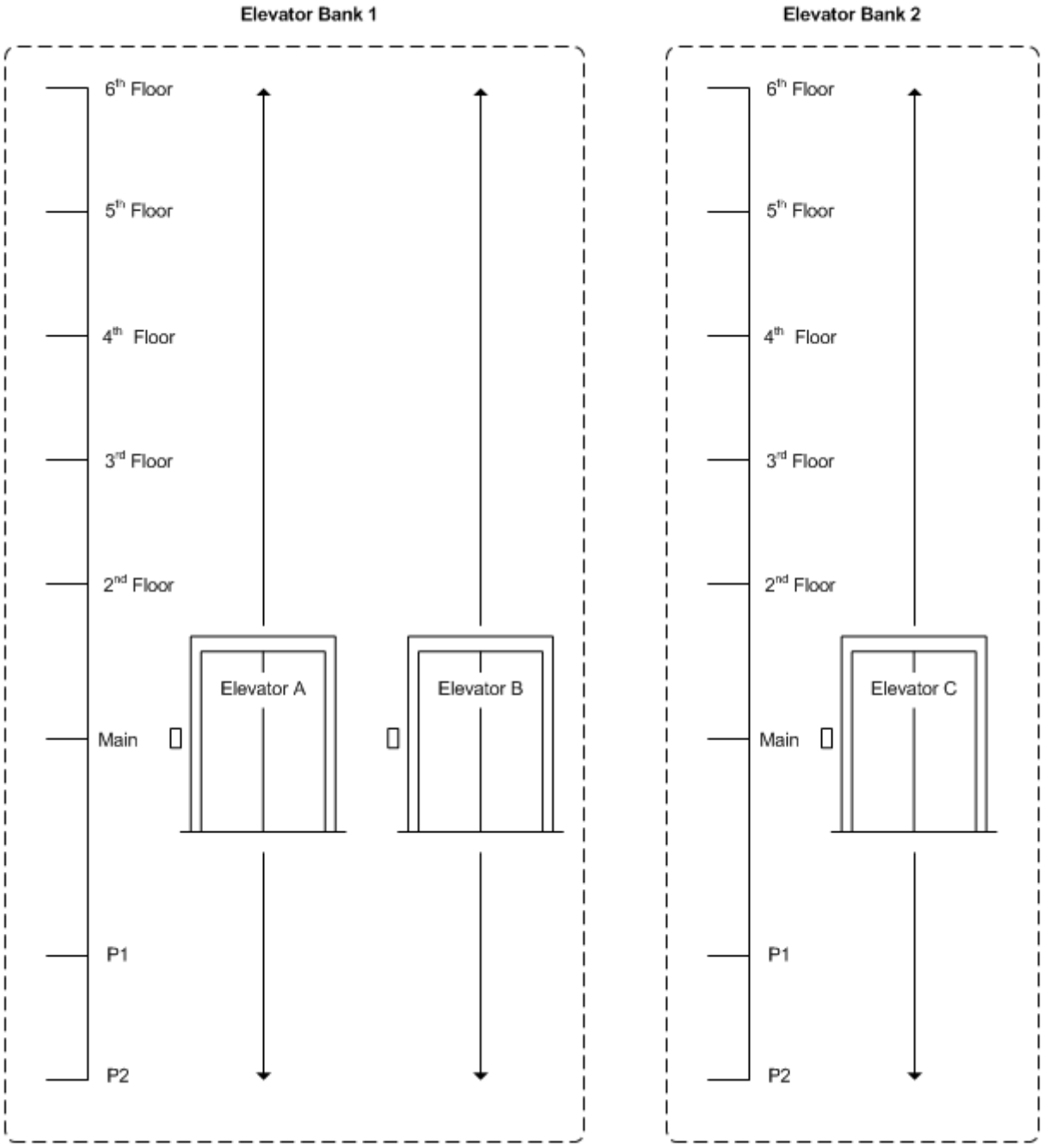
Example of Multiple Elevators & Multiple Elevator Banks

This example shows 3 elevators in the building.

Elevator A and Elevator B are for general use by all valid cardholders. Regulated by the same schedules, auto unlock floor buttons, and elevator group access levels, the elevators are assigned to Elevator Bank 1.

Elevator C is a freight elevator with access restricted to security personnel. Because Elevator C requires different schedules, elevator group access levels, and no auto-unlock floor button assignments, elevator C is assigned to Elevator Bank 2.

Example of Multiple Elevator Banks



Hardware Settings

For information about the Hardware Settings functions in the Elevator Hardware Setup screen, select the link below Related Topics which directs you to the Door Control Units. Refer to the information under the Hardware Settings | DIP Switch (S2) Configured Control Boards Only heading.

Procedures

Steps to Add an Elevator Control Unit

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site listed in the Hardware Setup directory screen.
2. From the Hardware Setup/All Panels screen, select the down arrow on the right side the Add 8 Door Controller button.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.

3. Select the type of elevator control board 40 Floor (EC1500) or 16 Floor (EC2500) you are adding from the drop down list.
    - If you are prompted with the Keyscan Dialog Window to Add an Elevator Bank, you can either select the ▼ symbol to the right of Create New Bank and pick an existing elevator bank that the elevator control board will be assigned to, or you can click on the Create New Bank button and add new elevator bank that the elevator control board will be assigned to.
    - If you are adding an elevator control unit for the first time, by default, the Client creates Elevator Bank # 1 which you can assign to the elevator control unit you are adding.
4. By default the Client software populates the Name field with Elevator Control Unit # 1. Each time you add a control unit the # increments by 1. You can leave the default name format (recommended) or change it. If you change it however, Keyscan recommends you retain a consistent naming format for all elevator control units.
5. In the Serial Number text box, enter the elevator control unit serial number. The serial # is on the packing slip, the invoice, and the ACU circuit board.
6. In the Password text box, you can leave the default password of KEYSCAN or you can change it to a maximum of eight characters. If you change the password, be sure to write it down and store it in a safe place. In the event you have to perform a disaster recovery at a later date to recover on-board data, you cannot communicate with the control board or access the data without the password.
7. Opposite Status, leave the default setting on Active.
8. Click the ▼ symbol on the right side of the Regional Time Zone and select the geographical time zone where the panel is physically situated.
9. In the Location text box, enter a brief description where the ACU is physically located.
10. Opposite the Communication tab, Serial is listed by default, select the ▼ symbol on the right and from the drop down list select the communication mode that is used to communicate with the access control unit as follows:
    - For a Serial Connection: Specify the Baud Rate of the access control unit, the Communication Port on the PC running the communication manager with the serial connection to the access control unit. By default the Client populates the Server field with the name of the local PC. Leave this on the default setting for a single PC/server installation. However if the Keyscan Communication Service is not installed on the local PC/server, enter the name of the PC/server where the Keyscan Communication Service is installed.
    - For a Network Connection: In the Communication Port field, leave the default setting of 3001 unless another network port is used. In the IP Address field, enter the static IP address assigned to the NETCOM device connected at the access control units. By default the Client populates the Server field with the name of the local PC. Leave this on the default setting for a single PC/server installation. However if the Keyscan Communication Service is not installed on the local PC/server, enter the name of the PC/server where the Keyscan Communication Service is installed.
    - For a Reverse Network Connection: In the Communication Port field, leave the default setting of 3001 unless another network port is used. In the Master Panel Serial #, click on the down arrow to the right and select the access control unit that is designated as the reverse network control board. In the Receiver Comms IP text box, enter the IP address of the server/PC which has the Reverse Network Communication installed. If a secondary IP address exists with a connection to the server/PC which has the Reverse Network Communication installed, you can specify the address in the Failure Comms IP text box. Enter the computer name of the server/PC with the Reverse Network Communication if it is other than the unit currently displayed in the Communications Server field.
11. As an option you can name the elevator floors and the floor number. Below the Floors heading under the Name column, double click on Floor # in the table.
12. Enter a name for the floor. The maximum is 34 characters.
13. To change the floor #, double click under the # column for the appropriate floor and enter the number.

- An example might be in cases where the elevator descends to an underground parking garage in a condominium or commercial building and floor numbers have to be altered to reflect a sub-floor number.

14. Select the Elevator Floor Timers tab.
15. Select the ▼ symbol on the right side of the Floor Button Selection Time, and select a value in seconds from the drop down list.
16. If the elevator controller interfaces with a telephone entry system, click on the ▼ symbol on the right side of the Telephone Entry Interface Floor Button Selection Time button, and select a value in seconds from the drop down list.
17. Select the Save button.
18. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Hardware Settings

Floor Status

Click on the link below for the Floor Status topic.

Floor Status

Replacing a Control Unit

These instructions are for installing a replacement access control unit or an elevator control unit that is the same series as the old unit. As an example, you are replacing a 4 door controller - CA4500 with a new 4 door control unit - CA4500.

Procedures

Steps to Re-configure a Replacement Control Unit

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. With the All Hardware tab selected, double click on the control unit you are replacing.
3. Insert the cursor in the Serial Number text box; highlight and delete the existing serial number, and then enter the serial number of the replacement access control unit.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Delete a Control Unit

These instructions apply when you are either deleting an access control unit or elevator control unit from the system or have replaced a unit with a new but different series control unit. These procedures will delete the control unit's data entirely, including all recorded alarm transactions.

Procedures

Steps to Delete a Control Unit

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the site on the Hardware Setup directory screen.
2. With the All Hardware tab selected, select the control unit you are deleting.
3. To the right of the selected control unit for deletion, click on the waste bin (Delete) button.
4. From the Delete Access Control Unit prompt, click on the Yes button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

E-Plex Door Details

The E-Plex Door Details screen consists of the following fields:

- Name - identifies the door; generally the name should indicate where the door is located
- Lock Model - identifies the model of E-Plex wireless lock being used
- Is Wireless - dictates whether or not the lock type is wireless; the box must be checked for E-Plex wireless locks to continue
- Function Type - select one of the three options from the drop down list:

    1. **Entry Lock** - Enables the lock to function normally, with access only being granted with an authorized credential. However, the lock can be put into and taken out of Passage Mode by an authorized operator (e.g. Master User). In Passage Mode, the lock remains unlocked and a credential is not required.

    2. **Residence Lock** - A Residence Lock stays unlocked by default. It can be locked from either the inside via a dead bolt, or from the outside by pressing the # key three times (###), followed by a valid user PIN (Personal Identification Number). The user PIN and entry method depends on your lock type and access credential requirements. When the same or next valid user presents/enters their credential, the lock will open. It will once again stay in unlocked mode until either a dead bolt on the inside is used or by initiating the PIN process from the outside.

    3. **Privacy Lock** - This function enables a lock to have access restricted to certain privileged users. In most cases, only the Master and Manager's credentials will override the privacy function and unlock the door. However, in some cases, with various E-Plex locks and other types of software, privileged users can span beyond Master and Manager.

- Unlock Time - measures the amount of time, in seconds, that the door remains unlocked
- Buzzer Volume - the intensity in which an alarm sounds when the door is held open past the preset unlock time (0 = Off, 3 = Loudest)
- Tamper Count - dictates how many failed credential reads will trigger a Tamper Lockout
- Tamper Lockout - the amount of time, in seconds, the lock will sit idle for after the Tamper Count meets the preset threshold of failed credential reads
- Manual Passage Duration - dictates the amount of time, in hours, a door remains unlocked through a Manual Override on the Status Screen
- Door Held Open - the time interval, in seconds, that the door may remain open before the system reports a Door Held Open violation
- Batteries Last Changed - select the calendar icon and choose the date when the batteries of the E-Plex lock were last changed
- Gateway - a pathway number will appear here after the Gateway establishes connection with the Aurora software

- ZAC - this PIN code is integral into successfully pairing a Gateway to the Aurora software. Select the wrench icon to randomly generate a new PIN code. Click the Default ZAC button to return the code back to it's default setting (10 80 10 80)

E-Plex 7900 Wireless Locks

The following options (including the Default ZAC button listed in the last section above) are only available with E-Plex 7900 series of wireless locks. A ZAC Command Card is required in order to sync an E-Plex 7900 with the Aurora software. Only one wireless lock can utilize the ZAC Command Card at a time.

- Present3 Mode - choose between one of the following: Not Used, Door Toggle, Lockdown and Emergency Passage
- Group Range - determines which group of credentials are able to access the Present3 function detailed above

Each E-Plex 7900 wireless lock requires a pack of Command Cards (sold separately, contact Keyscan for ordering information) to work with the Aurora software. Each pack comes with the following cards (not all cards are listed here):

- Factory - Used as the Master until a Master is programmed into the lock
- Factory Communication - Turns on Communication Mode when the lock is still in Factory Mode
- ZAC - Used to pair an E-Plex 7900 wireless lock with the Aurora software
- Reset to Factory - Resets the lock to Factory Mode. The Factory Master can be used again at this point
- Communication - After using the ZAC Command Card, this card turns on Communication Mode after the lock is programmed

Schedule Assignment

This screen allows you to toggle preset schedules for certain E-Plex doors and presents you with the following options:

- Assigned - check the box beside the schedule you wish to apply to that specific E-Plex door
- Schedule - displays the name of that pre-determined schedule
- Schedule On Mode - dictates how a credential holder can enter an E-Plex door when the schedule is activated. Select between Card Only, Card and Keypad, Card or Keypad, or PIN only



The "Card or Keypad" Schedule On Mode will only work for E-plex 5X00 locks running firmware 3.90 or higher.

- Passage Mode - select one of the four options from the drop down list:

1. **None** - The lock never grants free passage.
2. **Auto** - The lock automatically enters free passage at the start of this schedule and locks back at the end of the schedule automatically.
3. **First Authorized Passage** - The lock goes into free passage, only after a valid "privileged" user opens it with their credential at or after the start of this schedule.
4. **Manual Keypad** - Only the Master or the Manager users can manually set/reset the free passage at the lock keypad between the start and end times of this schedule for Manual Passage mode duration set in the software.

Important ! An E-Plex Schedule must be set up in the Schedule Management menu prior to assigning a schedule to an E-Plex door.

Change Door Group

Once you've completed setting up your E-Plex Door, you can always reassign the Door to a different E-Plex Door Group.

To move an E-Plex Door to a differnt door group, follow the steps below:

Steps to Assign E-Plex Door to a Different E-Plex Door Group

1. From the Client main screen, select the Site Management button > Hardware Setup.
2. If you have multiple sites, double-click the site containing the E-Plex Doors/Groups you want to modify.
3. Click the Door Groups tab on the left side of the screen.
4. Use the drop-down menu on the E-Plex Door Groups sub screen to choose the E-Plex Door Group that contains the E-Plex Door you want to reassign.
5. View the list of E-Plex Doors and locate the one you want to change.
6. To change the E-Plex Door Group, right-click the E-Plex Door you want to change, then click Change Door Group.
7. In The Change Door Group window, use the drop-down list to choose from the list of available Door Groups, then click OK.
8. After clicking OK, the E-Plex Door now belongs to the new door group.

Note: The "Change Door Group" option will not be clickable if the Door Group has changes pending, in which case you must save the changes to the Door Group before proceeding.

Related Topics

Aurora E-Plex Integration Setup

First Person In

First Person In (FPI) is a system safeguard. This function should always be used on exterior doors assigned with a scheduled automatic unlock period. FPI prevents a schedule switching ON regardless of its appointed start time until a valid credential is presented at a designated target reader.

The Importance of FPI

This example illustrates why using FPI is so important. Your front entrance door is programmed to unlock automatically at 9:00 A.M. However, because of heavy traffic, you won't arrive until 9:30 A.M.

- without First Person In, your building is at risk since the front entrance door unlocks automatically at 9:00 A.M. and conceivably no authorized personnel are present
- with First Person In, the front entrance door remains locked as the schedule is prevented from turning ON until someone presents a valid credential to turn on the schedule and unlock the door

Remember, always use First Person In for any exterior doors that are assigned a scheduled auto unlock.

First Person In affects the following elements assigned to the schedule:

- all doors set on auto unlock
- all groups
- all auxiliary input shunt/auxiliary output devices

The Set First Person In screen is used to select target readers that enable the schedule. One or multiple readers/keypads can be selected. Until a valid individual from an authorized door group presents his or her credential to a designated target reader, a schedule designated with first person in remains OFF regardless of its start time.

The First Person In target reader only prevents schedule assignments from starting at the local control unit.

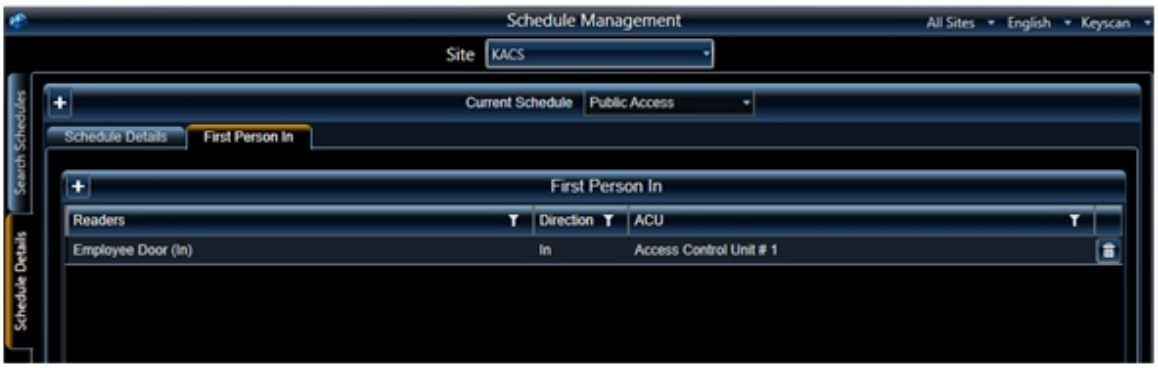
Illustrated Example

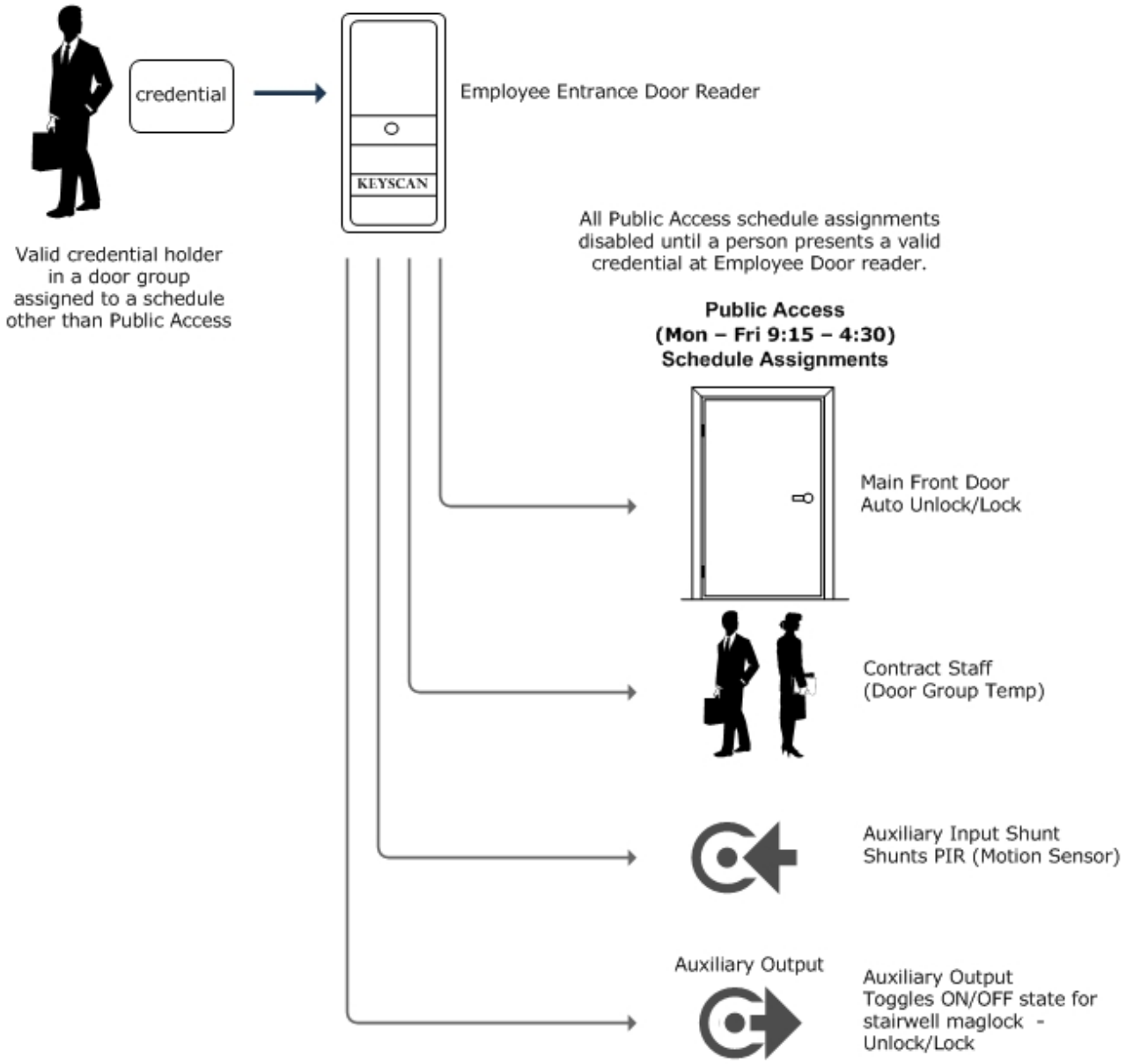
In the example Set First Person In screen below, the Employee Entrance door reader is designated as the target reader. Until a credential from a door group assigned to a schedule other than Public Access Mon - Fri 9:15 AM-4:30 PM is presented at the Employee Door reader, all Public Access schedule assignments remain OFF affecting the following doors, door groups and devices:

- The Main Front Door set to automatically unlock at the start of the Public Access schedule remains locked
- The Contract Staff door group cannot access reader-controlled doors assigned to Public Access.
- The devices remain in their schedule OFF state

Remember, when designating a reader or readers, those readers act as the target readers to enable the schedule specified in the Current Schedule field on the First Person In screen.

View illustrated example





Procedures

Steps to Set First Person In

1. From the Client main screen, select the Site Management button > Schedule Management.
    - If you have multiple sites, double click on the site from the directory screen.
2. From the Schedule Management screen, double click on the schedule that you are applying with First Person In.

- This is the schedule assigned to doors, groups or devices that remains OFF until a valid credential is presented at a target reader with a different schedule assignment.

3. Select the First Person In tab.
4. Click on the + symbol on the First Person In button.
5. From the Readers drop down list, select the desired target reader or readers by clicking in the respective box on the left. The box has an x when selected.
    - If you inadvertently select the wrong reader or readers, either click inside the box to clear the x or click on the Reset button to clear all selected readers.
6. Click on the Add button.
7. Click on the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Assign Schedules to Doors

Schedules & Holiday Hours

The Schedule Management screen allows you to set schedules for doors and elevators. When you create schedules it is important to think in terms of the groups and the times that those groups will access the various doors, access points or elevator floors. Keyscan suggests you pre-plan before you start creating schedules as well as read and understand the conventions and format of schedules.

- Schedules are based on a 24-hour clock
- Schedules are weekly
- The maximum number of user defined schedules that can be assigned to a site is 253*.
- The maximum number of total schedules that can be assigned to a site is 255* (253 user defined + "N/A" + "24HR")
- Total number of time periods (assigned groups/blocks of time within schedules) is 511*
- Range of a schedule is 00:01 to 23:59 (time blocks that fall within these time parameters even if they cross over midnight are highlighted in blue)

The setting of 00:00 in the Keyscan software represents No Time. It does not represent midnight. If either the start time or the end time is assigned 00:00 the following conditions will result:

- If the start time is set to 00:00, the time block does not start*
- If the end time is set to 00:00, the time block does not stop*
- time blocks that either start or end on 00:00 are highlighted in yellow*

Holiday Hours*

The Holiday 1, 2, 3 hours allow creating special 1 day periods for statutory holidays, plant shutdowns, or any other type of occasion where you need alternative time-periods from your regular schedules.

You can create three distinct holiday time periods within each schedule:

- Holiday 1
- Holiday 2
- Holiday 3

Whenever Holiday 1, 2, or 3 is assigned to specific calendar dates in the Holiday Setup screen, they override the schedule on that particular day. Holiday 1, 2 or 3 times are highlighted in green.



Keyscan suggests that you review the full year and consider all groups before creating holiday hours. Whenever possible keep Holiday 1, 2, or 3 hours universal for all schedules in order to avoid creating an unwieldy labyrinth of different holiday times that could become very confusing to manage.

Global Message*

When this function is enabled, indicated by an x, the schedule is designated as a global schedule. To disable click inside the box. The box does not have an x when disabled.

Global Message and global schedules may only be implemented if your site's access control boards are configured with Communication Interlink Modules (CIM). If your site does not use Communication Interlink Modules or designated OCB-8 or IOCB1616 relay boards for global functions, then the Global Message function does not have any effect on the schedule whether it is enabled or disabled.

For more information on global schedules and global inputs and outputs, refer to the Keyscan Documents folder > Global Inputs & Outputs / Schedules included with the Aurora Software Installation files.

Clone Schedule Function

The Schedule Management screen has a function which allows cloning an existing schedule for circumstances where you require duplicating schedule hours for another named schedule. You can also use the cloning tool when creating a new schedule that is similar to an existing schedule and then alter the times. The Clone schedule button can be accessed with either the Search Schedules tab selected or the Schedule Details tab selected.

Schedule Clone Button



E-Plex Schedule

The Schedule Management screen can also add E-Plex schedules for wireless locks. To limit confusion, it is advised to add "E-Plex" into the Schedule Name, since it will only apply to E-Plex-specific doors.



*Does not apply to E-Plex Schedules

It is important to note the following when setting up an E-Plex Schedule:

- Each day must be set for the same timeframe, e.g. Monday to Friday 9a.m. to 5p.m.
- The E-Plex Schedule cannot be set for a period that expands overnight

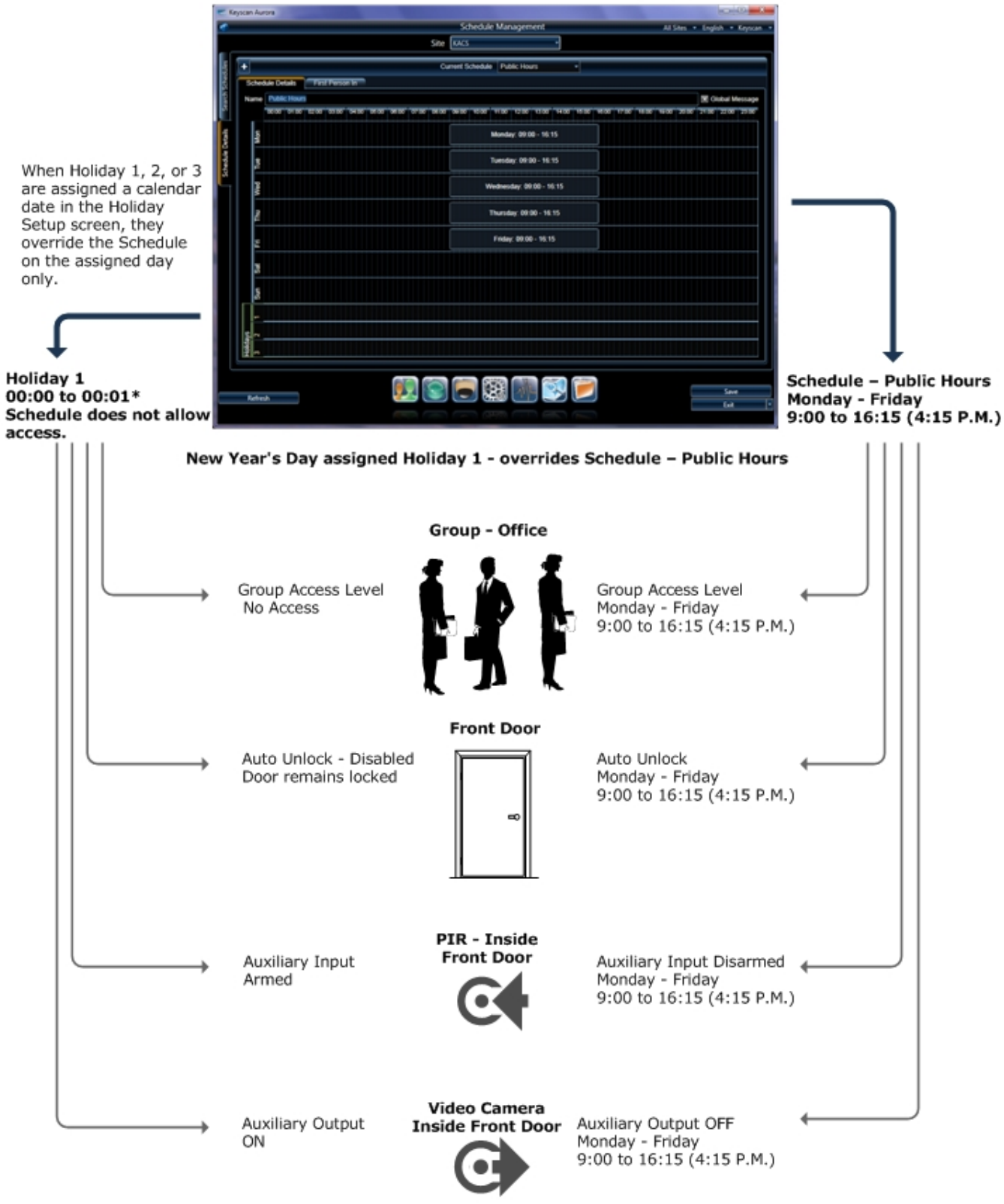
BEST Schedule

The Schedule Management screen can also add BEST schedules for G and V series of offline locks. To limit confusion, it is advised to add "BEST" into the Schedule Name, since it will only apply to BEST-specific doors.

See Also: BEST Offline Lock Integration Setup

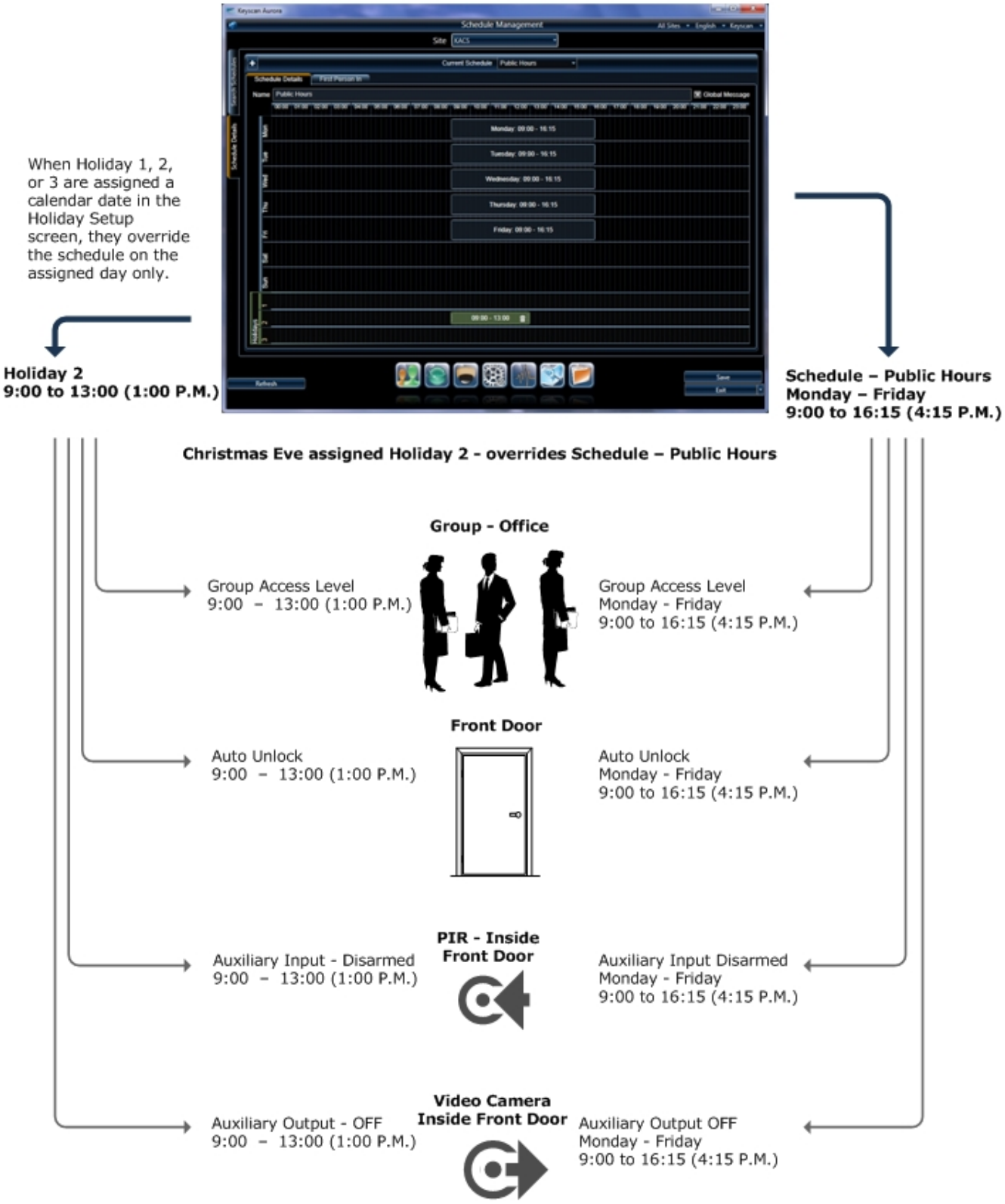
Examples

Holiday Hours - No Access on the Holiday Date



* If Holiday 1, 2, or 3 are set as 00:00 to 00:01, you will not see a block of time in the Schedule Management screen.

Holiday Hours - Shortened Access Times on the Holiday Date



Procedures

Steps to Create a Schedule

1. From the Client main screen, select the Site Management button > Schedule Management.
    - If you have multiple sites, double click on the site in the directory screen.
2. From the Schedule Management screen, select the Add Schedule button.
    - By default, the Client names schedules starting at Schedule # 1 and increments the number by 1 each time a new schedule is created.

3. You can leave schedules on their default Schedule # x name or you can enter a title in the Name text box to better identify the schedule as it relates to its assignments.
4. On the first day that applies to the schedule, position the cursor at the starting time and drag to the end time. The times are blocked in 15 minute intervals.
5. To adjust the start or end time to an interval of less than 15 minutes, position the cursor over the start or end point. The cursor changes to a double horizontal arrow. Click and drag either the start or end time to the exact minute desired. A pop up indicates the setting as you drag the cursor.
    - As an alternative to dragging the cursor for setting the start and end times, double click on the first day of the time zone. From the dialog box in the Start Time and the End Time text boxes, enter the desired times including the AM and PM setting.
6. Repeat either of the above procedures for each day in the week that you are setting start and end times.
    - As an option, right click while the cursor is positioned on the first defined time block and use the copy/paste dialog box to define additional time blocks if the beginning and end times are the same.
    - If you inadvertently add times to a day that you do not wish to have included in the time zone, click somewhere on that day's blue time block and select the waste bin symbol to delete the time block.
7. To set holiday hours for Holiday 1, 2, or 3, position the cursor over the start point and drag to the end point. You can use the same techniques mentioned above to set or refine the holiday hours.
8. When you have completed setting the schedule, click on the Save button.
9. To create another schedule, select the Search Schedules tab.
10. Click on the Add Schedule button and repeat the above procedures; otherwise click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Steps to Clone a Schedule

1. From the Client main screen, select the Site Information button > Schedule Management.
2. Double click on the site in the directory screen.
3. From the Schedule Management screen with the Search Schedules tab selected, select the schedule in the list that you are cloning.
    - To review a schedule's times, click on the + symbol at the left of the schedule name.
4. With the schedule you are cloning highlighted, select the Clone button.
5. Select the applicable Sites by placing an **x** beside each one. Alternatively, input the site name into the Site Search filter above. Selected Sites will remain in the list regardless of the filter.
6. After all potential Sites are chosen, select the OK button. A pop-up window will show how many schedules were cloned and saved to sites successfully.

Steps to Edit a Schedule

1. From the Client main screen, select the Site Management button > Schedule Management.
    - If you have multiple sites, double click on the site on the directory screen.
2. From the Schedule Management screen with the Search Schedule tab selected, double click on the schedule that you are editing from the list.
3. On the first day that you are changing the times, position the cursor over the start or end point. The cursor changes to a double horizontal arrow. Click and drag either the start or end time to the exact minute desired. A pop up indicates the setting as you drag the cursor.

- As an alternative to dragging the cursor to set the start and end times, double click on the first day of the schedule. From the dialog box in the Start Time and the End Time text boxes enter the desired times including the AM and PM setting.

4. Repeat either of the above procedures for each day in the week that you are re-setting the times.
5. To re-set holiday hours for Holiday 1, 2, or 3, position the cursor over the start point or end point and drag to re-set the time.
6. When you have completed re-setting schedules, click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

First Person In

Manage Master Holidays

Holiday Setup

Set Schedule Default Off Times

The Set Schedule Default Off Times is designed as a safeguard for schedules that start with 00:00 and used principally in Present 3 applications. Setting a default off time for the schedule ensures that the schedule has an enforced off time in the event that the door was not locked by user interaction with Present3.

You can set the default off times to a single day, multiple days, Holiday 1, 2, or 3 or all days which includes the three holiday days.

Procedure

Steps to Set Schedule Default Off Times

These instructions assume you have already created the schedule that you are going to set with a default off time.

1. From the Client main screen, select the Site Setup button > Schedule Management.
    - If you have multiple sites, double click on the site on the Site Search-Schedule Management directory screen.
2. From the Schedule Management screen with the Search Schedule tab selected, double click on the schedule that you are going to set with default off times.
3. Select the Set Schedule Default Off Times tab.
4. Click on the ▼ symbol to the right of Create Off Time For: and select the appropriate day, range of days, or holidays from the list.
5. Click In the box to the immediate left of the Add Off Times button, and enter an off time - hh:mm - in hours and minutes.
6. Click on the Add Off Times button.
7. Click on the Save button.
8. The default off times are inserted in the applicable day/holiday boxes.
9. Select the Back button until you are returned to the main screen or the navigation history button to return to a previously opened screen.

Schedule Examples

The table below illustrates examples of schedules that fall within a twenty-four hour clock, overlap midnight, and run continuously over 5 days.

Schedule - Remains within 24 Hour Clock

Example - Monday to Friday 9:00 A.M. to 5:00 P.M.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Start	09:00	09:00	09:00	09:00	09:00	00:00	00:00
End	17:00	17:00	17:00	17:00	17:00	00:00	00:00

View screen with Monday to Friday 9:00 A.M. to 5:00 P.M. schedule settings



Schedule - Overlaps Midnight - 7 Days

Example - Monday to Sunday 5:00 P.M. to 2:00 A.M.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Start	17:00	17:00	17:00	17:00	17:00	17:00	17:00
End	02:00	02:00	02:00	02:00	02:00	02:00	02:00

View screen with Monday to Sunday 5:00 P.M. to 2:00 A.M. schedule settings



Schedule - Overlaps Midnight - 5 Days

Example - Monday to Friday 5:00 P.M. to 2:00 A.M. (Schedule concludes Saturday A.M.)

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Start	17:00	17:00	17:00	17:00	17:00	00:00	00:00
End	00:00	02:00	02:00	02:00	02:00	02:00	00:00

View screen with Monday to Friday 5:00 P.M. to 2:00 A.M. schedule settings



Schedule - Continues Across Multiple Days

Example - Monday to Friday Continuous - TZ concludes at Friday 7:00 P.M. - Resumes Monday 7:00 A.M.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Start	07:00	00:01	00:01	00:01	00:01	00:00	00:00
End	00:00	00:00	00:00	00:00	19:00	00:00	00:00

View screen with a schedule across multiple days



Master Holidays

Intended principally for access control systems with multiple sites, the Master Holidays screen provides the means to create a list of holidays common to all sites. Once created, a master holiday is listed and available on all sites. This reduces the amount of time spent entering holidays common to multiple sites.

Master Holiday dates are specified in one of the following ways:

- Once - such as a special event that does not recur each year
- Annually - such as New Year's Day which recurs on January 1st each year
- Annually Based on Pattern - such as Labor Day which falls on the 1st Monday of September each year

Note + The system user account must have permission to add Holidays in order to access the Master Holidays screen and create master holidays.

Master holidays must be assigned to holiday 1, 2, or 3 in the Holiday Setup screen.

Procedure

Steps to Create a Master Holiday

1. From the Client main screen, select the Settings button > Manage Master Holidays.
2. Select the + symbol beside Master Holidays.
3. Below the Master Holidays heading, click on the Master Holiday # x that was added after you selected the + symbol.
4. Click the cursor inside the Name text box; clear the Master Holiday # x entry, and type the name of the master holiday.
5. Opposite Occurs, select the ▼ symbol and from the drop down list select the way in which the master holiday occurs.
    - Once
    - Annually
    - Annually based on pattern
6. Do one of the following depending on the selection in the preceding step:
    - Once or Annually - Click on the calendar to the right. If the master holiday occurs during a month other than the month currently displayed, use the arrows and scroll the calendar to the desired month. With the calendar on the desired month, select the day when the master holiday occurs.
    - Annually based on pattern - Click on the ▼ symbol to the right of 1st and select the day's occurrence in the month. Click on the ▼ symbol to the right of Monday and select the day of the week. Click on the ▼ symbol to the right of January and select the month.
7. To add another master holiday, select the + symbol beside Master Holidays and repeat the procedures.
8. When you have completed creating master holidays, click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Holiday Setup

The Holiday Setup screen is used for scheduling dates within the year when statutory holidays, facility shutdowns or any other special days occur that require an override to the regular weekly schedules. Holiday dates are specified in one of the following ways:

- Once - such as a special event that does not recur each year
- Annually - such as New Year's Day which recurs on January 1st each year
- Annually Based on Pattern - such as Labour Day which falls on the 1st Monday of September each year

After naming the day and specifying a calendar date, assign it with Holiday Type 1, Holiday Type 2, or Holiday Type 3.

If this holiday schedule is intended to be used with E-Plex locks, then check the box beside Include As E-Plex Holiday. For offline E-Plex locks, the lock will need to be re-programmed with an M-Unit once per year if using Holidays that occur annually or based on annual patterns.

Note +

If this holiday schedule is intended to be used with BEST locks, then check the box beside Include As BEST Holiday. There is a maximum of 8 BEST holidays permitted within a Site. Since BEST locks are offline, they will need to be re-programmed after making a change. If the holiday repeats annually or is based on a pattern, the locks will need to be updated annually for Holidays to be reapplied.

When a holiday is marked to be included as a an E-Plex holiday, the date(s) configured for the holiday defines a period during which users will NOT be granted access to E-Plex doors.

Example - Labour Day

- Name: Labour Day
- Type: 1*
- Occurs: Annually Based on pattern - 1st | Monday | September

* Holiday Type 1 is merely used as an arbitrary example. It could be any of the three holiday types depending on how you have defined them and which type applies. For more details about creating Holiday Types, see the link below Related Topics.

The maximum number of calendar dates that can be assigned a holiday is 64 per site; 32 when using block holidays. Also, a Holiday must start and end within the same month.

Please remember, Holiday Type 1, Holiday Type 2, or Holiday Type 3, override the schedule on that calendar date.

Tip >

At the beginning of each calendar year, we recommend that you review your calendar for annual holidays and update the Holiday Setup screen for the forthcoming year.

Procedures

Holiday procedures include the following sets of instructions:

- adding a holiday at the site level
- assigning holiday 1, 2, or 3 to a master holiday

Master holidays have already been defined in the Manage Master Holidays screen and cannot be altered in the Holiday Setup screen.

Steps to Add a Site Holiday

1. From the Client main screen, select the Site Management button > Holiday Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. From the Holiday Setup screen opposite Site Holidays, click on the Add Holiday button and select Site Holiday from the drop down list.
3. Below the Holiday Details heading opposite Name, click the cursor inside the Name text box; clear the Site Holiday # x entry, and type the name of the site holiday.
4. Opposite Type, click on the symbol and select either Holiday Type 1, 2, or 3 from the drop down list.
    - The hours specified for Holiday Type 1, 2, or 3 in the Schedule Management screen will override the regular schedule on this holiday date.
5. Opposite Occurs, click on the symbol and from the drop down list select the way in which the site holiday occurs.
    - Once
    - Annually
    - Annually based on pattern
6. Do one of the following depending on the selection in the preceding step:
    - Once or Annually - If the date is other than the current date, click on the calendar to the right. If the holiday occurs during a month other than the month currently displayed, use the arrows and scroll the calendar to the desired month. With the calendar on the desired month, select the day when the master holiday occurs.
    - Annually based on pattern - Click on the symbol to the right of 1st and select the day's occurrence in the month. Click on the symbol to the right of Monday and select the day in the week. Click on the symbol to the right of January and select the month.
7. To add another site holiday, select the Add Holiday button beside Site Holidays and repeat the procedures.
8. When you have completed creating site holidays, click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Assign Holiday 1, 2, or 3 to a Master Holiday

1. From the Client main screen, select the Site Management button > Holiday Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. From the Holiday Setup screen opposite Site Holidays, click on the symbol next to Add Holidays and select the master holiday from the drop down list.
3. Opposite Type, click on the symbol and select either Holiday 1, 2, or 3 from the drop down list.
4. Click on the Save button.
5. To assign Holiday 1, 2, or 3 to another master holiday, repeat the preceding steps; otherwise click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Edit a Site Holiday Date

1. From the Client main screen, select the Site Management button > Holiday Setup.

- If you have multiple sites, double click on the site from the directory screen.

2. From the Holiday Setup screen under the Site Holidays heading, select the site holiday - listed in yellow - you are editing.
3. Under the Holiday Details heading, make the necessary changes.
4. Click on the Save button.
5. To edit another site holiday, repeat the preceding steps.
6. When you have completed editing and saving site holidays, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Change Holiday 1, 2, or 3 Assignments on a Master Holiday

1. From the Client main screen, select the Site Management button > Holiday Setup.
   - If you have multiple sites, double click on the site in the directory screen.
2. From the Holiday Setup screen under the Site Holidays heading, click on the master holiday - listed in green - you are re-assigning with a different holiday type.
3. Below the Holiday Details heading opposite Type, click on the symbol and select either Holiday 1, 2, or 3 from the drop down list.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Delete a Site Holiday Date

1. From the Client main screen, select the Site Management button > Holiday Setup.
   - If you have multiple sites, double click on the site from the directory screen.
2. From the Holiday Setup screen under the Holidays heading, select the site holiday - listed in yellow - you are deleting.
3. On the site holiday that is highlighted in blue, click on the Delete button.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Master Holidays

Schedules and Holiday Hours

Schedule Status

Click on the link below for the Schedule Status topic.

Schedule Status

Assign Schedules to Doors

The Schedule Assignment - Doors function allows programming specified doors to automatically unlock at the start of a schedule and re-lock at the conclusion of the schedule as follows:

- Schedule ON - the door is unlocked
- Schedule OFF - the door is locked

You might use this feature on a front door allowing public access to your lobby or reception area during regular business hours. At the end of business hours, the schedule turns OFF and the door automatically re-locks securing the entry point.

Important ! Keyscan suggests you review First Person In to understand how this function works and how it acts as a building safeguard.

If you do not require doors locking and unlocking automatically on schedules, leave the doors on the default setting of Not Assigned. If the assigned doors are outfitted with E-Plex series wireless locks, then ensure you only assign an E-Plex Schedule to that door.

First Person In

Whenever you assign schedules to automatically unlock doors, especially exterior doors, it is strongly recommended to use the First Person In option. This ensures that a door never automatically unlocks before someone has arrived at the building.

First Person In suspends the schedule's start time and keeps it OFF until a valid credential is presented at a designated target reader. This ensures someone is present and on-site before the schedule turns ON and unlocks the door eliminating a potential security hazard.

As an alternative to assigning a schedule to automatically unlock and lock a door, you can use Present3 to either manually toggle the lock or turn a schedule on or off. See Related Topics below.

Procedure

Steps to Assign Schedules to Doors

1. From the Client main screen, select the Site Management button > Schedule Assignment.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Doors tab is selected.

Single Door

1. Select the door by clicking on the row so it is highlighted in blue. The box to the left has an x, indicting the door is selected.
2. On the row with the door highlighted in blue, click over the Schedule column.
3. Click on the ▼ symbol and select a schedule from the drop down list.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Multiple Doors/Same Schedule Assignment

1. Select the boxes to the left of the access control units/doors that you are programming to automatically unlock and re-lock on the same schedule. The box has an x when a door is selected.
2. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and from the drop down list, select the schedule.

3. Click on the Assign to Selected Doors button.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Remember doors programmed to automatically unlock are not secure during the specified schedule.

Steps to Cancel a Door from Auto Unlocking

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Doors tab is selected.

Single Door

1. Select the door by clicking on the row so it is highlighted in blue. The box to the left has an x, indicating the door is selected.
2. On the row with the door highlighted in blue, click over the Schedule column.
3. Click on the symbol and select Not Assigned from the drop down list.
4. Click on the Save button.
    - If the schedule was on and the door was unlocked when reset to Not Assigned, it must be manually re-locked. Ensure that you continue with steps 5 to 11 to verify all doors are locked.
5. Click on the Back button until you are at the main screen.
6. Click on the Status button > Status.
7. On the left side of the Status screen, double click on Door Status.
8. From the Door Status screen, click on the symbol and select the same site as above, if applicable.
9. Click on the symbol and select the control unit that is connected to the door that you have re-assigned to Not Assigned.
10. Verify the door is locked.
    - Locked doors have a red lock symbol. The door is secure.
    - If the door has a green lock symbol it is currently unlocked. Go to the next step.
11. Right click on the door icon and select Lock from the pop-up menu. The lock symbol changes to red indicating the door is locked.

Multiple Doors/Same Schedule Assignment

1. Select the boxes to the left of the panels/doors that you are cancelling the auto unlock/lock function. The box has an x when a door is selected.
2. Near the bottom of the screen, click on the symbol opposite Schedule and from the drop down list, select Not Assigned.
3. Click on the Assign to Selected Doors button.
4. Click on the Save button.
    - If the schedule was on and the door was unlocked when reset to Not Assigned, it must be manually re-locked. Ensure that you continue with steps 5 to 12 to verify all doors are locked.
5. Click on the Back button until you are at the main screen.
6. Click on the Status button > Status.
7. On the left side of the Status screen, double click on Door Status.
8. From the Door Status screen, click on the symbol and select the same site as above, if applicable.

9. Click on the ▼ symbol and select the control unit that is connected to the doors that you have re-assigned to Not Assigned.
10. Verify the doors are locked.
    - Locked doors have a red lock symbol. The door is secure.
    - Unlocked doors have a green lock symbol. Go to the next step.
11. Click on the Lock All button. The lock symbols change to red indicating the doors are locked.
12. If you changed multiple access control units and/or multiple sites, repeat for each control unit and site.

Related Topics

First Person In

Present3

Assign Schedules for Reader/Keypads

The Schedule Assignment - Readers screen is for setting access modes at doors that have combination readers/keypads, such as Keyscan's K-KPR keypad/proximity reader.

Since a reader requires a credential presentation and a keypad requires a PIN code entry, you can set the reader/keypad's operating modes to a schedule. This provides you with some flexibility so the access mode corresponds with the security required for the door and time.

The three reader/keypad access modes are outlined below:

- Card or Keypad - Either a PIN entry or credential presentation can be used to gain access
- Card Only - Only a credential presentation can be used to gain access
- Card and Keypad - Both a credential presentation and a PIN entry are required to gain access

When the schedule is in ON, one of the following conditions would be in effect:

- If Schedule ON Mode is set to Card or Keypad, an individual can either present his or her credential at the reader or enter his or her PIN code on the keypad to access the door.
- If Schedule ON Mode is set to Card Only, an individual can only present his or her credential at the reader to access the door; the keypad is excluded from use.
- If Schedule ON Mode is set to Card and Reader, an individual must present his or her credential at the reader and enter his or her PIN code on the keypad to access the door.

The same conventions apply for Schedule OFF Mode, whichever card/keypad option is selected.

If your system is connected with any of the following reader/keypads sold by Keyscan please be aware of the following procedure:

- K-KPR
- WSSKP-1
- HID-5355KP
- HID iClass KEYRK40
- Indala PXK 501

Keyscan recommends that when an individual is keying in their PIN code on one of the aforementioned reader/keypads, he or she press the star * key first, and then enter the PIN code. Pressing the star * key clears any previous numbers that may still be stored in the reader/keypad. This procedure eliminates the potential of the keypad misreading a valid PIN entry and denying access. When the system is set to Card and Keypad the card read or PIN entry can be in any order. These reader/keypads should have been purchased through Keyscan so they interface correctly with your Keyscan system. For other reader/keypads not listed above contact Keyscan.

Procedures

Steps to Assign Schedules/Access Modes to Readers/Keypads

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Readers tab is selected.

Single Reader

1. Select the reader by clicking on the row so it is highlighted in blue.
2. With the reader highlighted in blue, click over the Schedule column.
3. Click on the ▼ symbol and select a schedule from the drop down list.
4. Click over the Schedule On Mode column.
5. Click on the ▼ symbol. From the drop down list, select the mode when the schedule is on.
6. Click over the Schedule Off Mode column.
7. Click on the ▼ symbol. From the drop down list, select the mode when the schedule is off.
8. Click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Multiple Doors/Same Schedule Assignment

1. Select the boxes to the left of the access control unit/readers you are assigning schedules/operating modes. These reader/keypads will all operate under the same modes and schedules. The box has an x and the row is highlighted in blue when the reader is selected.
2. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and from the drop down list, select the schedule.
3. Click on the ▼ symbol opposite On Mode and select a mode from the drop down list.
4. Click on the ▼ symbol opposite Off Mode and select a mode from the drop down list.
5. Click on the Assign to Selected Readers button.
6. Click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Change Schedules/Access Modes

1. From the Client main screen, select the Site Management button > Schedule Assignment.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Readers tab is selected.

Single Reader

1. Select the reader by clicking on the row so it is highlighted in blue.
2. With the reader highlighted in blue, click over the Schedule column.
3. Click on the ▼ symbol and select a schedule from the drop down list.
4. Click over the Schedule On Mode column.
5. Click on the ▼ symbol. From the drop down list, select the mode when the schedule is on.
6. Click over the Schedule Off Mode column.
7. Click on the ▼ symbol. From the drop down list, select the mode when the schedule is off.
8. Click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Multiple Doors/Same Schedule Assignment

1. Select the boxes to the left of the panel/readers you are assigning schedules/operating modes. These reader/keypads will all operate under the same modes and schedules. The box has an x and the row is highlighted in blue when the reader is selected.

2. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and from the drop down list, select the schedule.
3. Click on the ▼ symbol opposite On Mode and select a mode from the drop down list.
4. Click on the ▼ symbol opposite Off Mode and select a mode from the drop down list.
5. Click on the Assign to Selected Readers button.
6. Click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Assign Schedules to Auxiliary Outputs

The Schedule Assignments - Auxiliary Outputs screen allows assigning an auxiliary output with a schedule that regulates when the output switches off and on. If you do not use auxiliary outputs, leave this screen on the default settings. You may wish to consult with your dealer or installer.

Procedures

Steps to Assign a Schedule to an Output

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Auxiliary Outputs tab is selected.

Single Output

1. Select the output by clicking on the row so it is highlighted in blue.
2. With the output highlighted in blue, click over the Schedule column.
3. Click on the ▼ symbol and select a schedule from the drop down list.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Multiple Outputs/Same Schedule Assignment

1. Select the boxes to the left of the access control unit/outputs you are assigning to schedules. The box has an x and the row is highlighted in blue when the reader is selected.
2. Click on the ▼ symbol opposite Schedule near the bottom of the screen and from the drop down list, select the schedule.
3. Click on the Assign to Selected Auxiliary Outputs button.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Assign Schedules to Elevator Banks/ Floors

The Schedule Assignment - Elevator Banks screen allows assigning specific floor buttons to automatically unlock at the start of a schedule and re-lock at the conclusion of the schedule.

As an example, your building has four floors. During your regular business hours of 8:30 to 4:30, customer service, located on the second floor, is open to the public. The other floors, however, are restricted to credential holders with valid credentials. Floor 2 would be assigned a schedule starting at 8:30 and ending at 16:30. The other floors would retain their default setting - Not Assigned.

If access to all floors is restricted to valid cardholders, you can bypass this step.

Remember that auto-unlock floor buttons are assigned to an elevator bank.

Procedures

Steps to Assign Schedules to Unlock/Lock Elevator Floor Buttons

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Elevator Banks tab is selected.

Single Floor

1. Select the floor # by clicking on the row so it is highlighted in blue.
2. With the floor # highlighted in blue, click over the Schedule column.
3. Click on the ▼ symbol and select a schedule from the drop down list.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Multiple Floors/Same Time Zone Assignment

1. Select the boxes to the left of the elevator bank/floors you are assigning to schedules. The box has an x and the row is highlighted in blue when the floor is selected.
2. Click on the ▼ symbol opposite Schedule near the bottom of the screen and from the drop down list, select the schedule.
3. Click on the Assign to Selected Floors button.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Assign Schedules & Inputs

The Schedule Assignment - Inputs screen is used when you require a schedule automatically arming and disarming inputs or used when you require inputs to toggle schedules ON or OFF. If you do not use inputs, leave this screen on the default settings. You may wish to consult with your dealer or installer before you make any changes to this screen.

Input Mode

Under the Input Mode field, the two modes are listed below:

- Schedule to Input - the assigned schedule automatically arms & disarms the specified inputs
- Input to Schedule - the assigned auxiliary input toggles the specified schedule on/off

Select the links below Examples to review the two modes.

Schedule & Auxiliary Input States

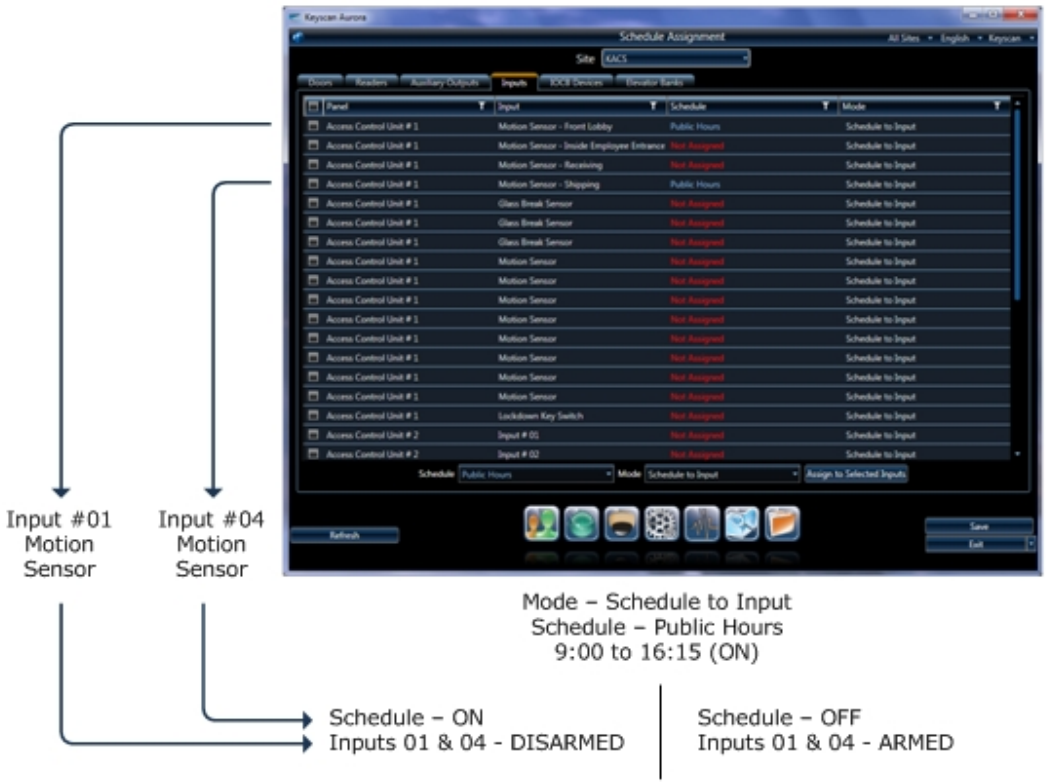
Schedule		AI
ON		Disarmed
OFF		Armed

AI		Schedule
Open		OFF
Closed		ON

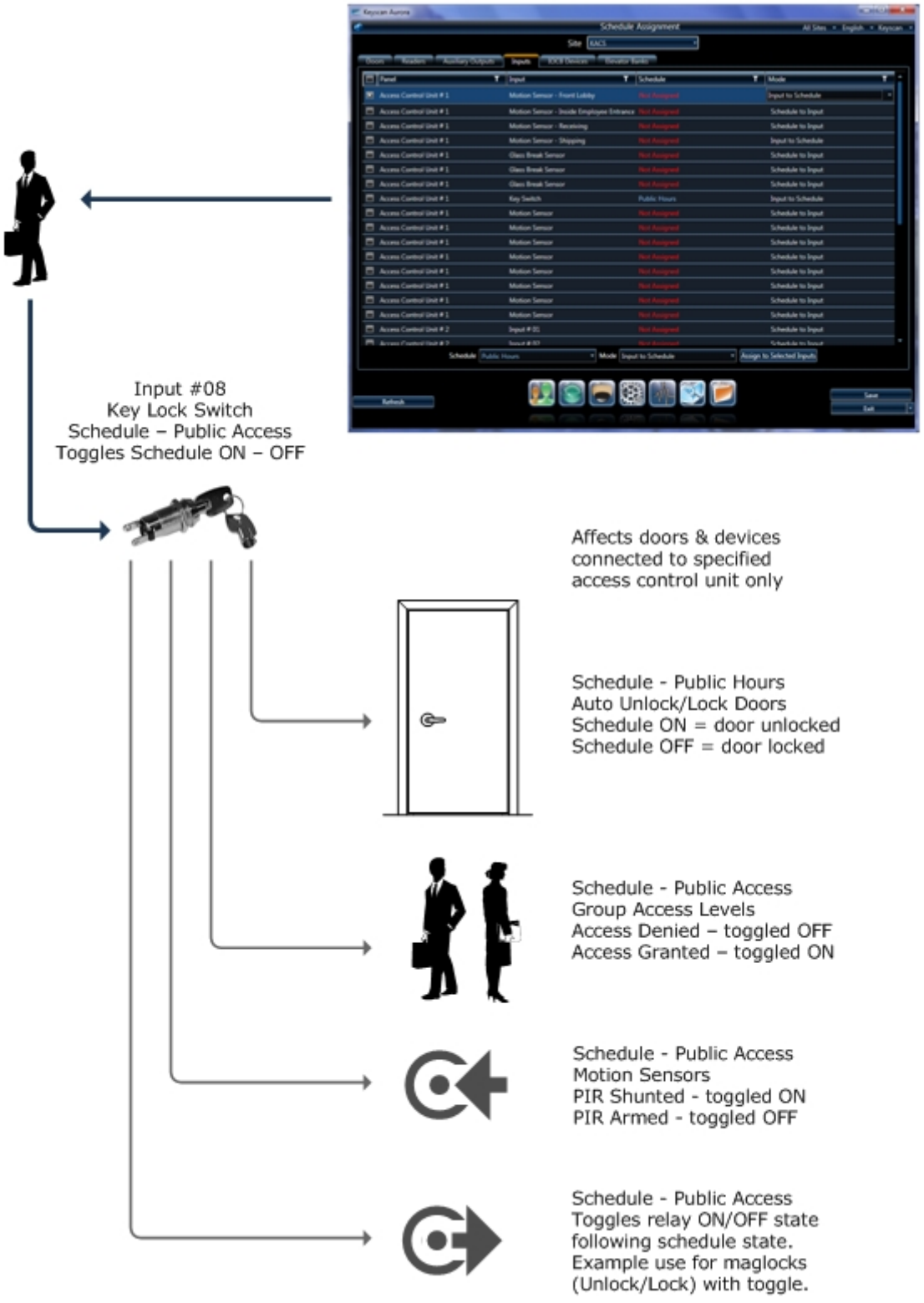
AI = Auxiliary Input

Examples

Schedules Arm & Disarm Inputs



Inputs Toggle Schedules



Procedures

Steps to Assign Schedules/Inputs

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Inputs tab is selected.

Single Input

1. Select the input by clicking on the row so it is highlighted in blue.

2. Along the row with the input highlighted in blue, click over the Schedule column.
3. Click on the ▼ symbol and select a schedule from the drop down list.
4. With the input still highlighted in blue, click over the Mode column.
5. Click on the ▼ symbol and select a mode from the drop down list.
    - Input to Schedule
    - Schedule to Input
6. Click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Multiple Inputs/Same Mode/Same Schedule Assignment

1. Select the boxes to the left of the access control unit/inputs you are assigning to schedules. The box has an x and the row is highlighted in blue when an input is selected.
2. Click on the ▼ symbol opposite Schedule near the bottom of the screen and from the drop down list, select the schedule.
3. Click on the ▼ symbol opposite Mode near the bottom of the screen and from the drop down list, select the mode.
4. Click on the Assign to Selected Inputs button.
5. Click on the Save button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Assign Schedules to IOBC1616 Inputs & Outputs

This screen assigns schedules to IOCB1616 inputs and outputs. IOCB1616 input/output boards are only compatible with 4 door - CA4500 and 8 door - CA 8500 control boards. This screen should only be completed by the dealer installer.

- Schedule On - Input Disarmed
- Schedule Off - Input Armed

If assigning schedules to IOCB inputs and outputs, refer to the IOCB1616 Rules in the Hardware Setup screen.

Procedures

Steps to Assign a Schedule to an IOCB Input

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the Site Search - Schedule Assignment directory screen.
2. Select the IOCB Devices tab.
3. Below the IOCB Inputs heading, click in the box to the left of the access control unit/IOCB Input #. The box has an x when selected.
    - If you are assigning multiple IOCB inputs to the same schedule, click in the box of each applicable input.
4. Click on the ▼ symbol to the right of Schedule, and select the schedule from the drop down list.
5. Click on the Assign to Selected IOCB Devices button.
6. Click on the Save button.
7. Click on the Back button to until you return to the main screen or the navigation history  symbol for a previously viewed screen.

Steps to Assign a Schedule to and IOCB Output

1. From the Client main screen, select the Site Management button > Schedule Assignments.
    - If you have multiple sites, double click on the site from the Site Search - Schedule Assignment directory screen.
2. Select the IOCB Devices tab.
3. Below the IOCB Outputs heading, click in the box to the left of the access control unit/IOCB Output #.
    - If you are assigning multiple IOCB outputs to the same schedule, click in the box of each applicable output. The box has an x when selected.
4. Click on the ▼ symbol to the right of Schedule, and select the schedule from the drop down list.
5. Click on the Assign to Selected IOCB Devices button.
6. Click on the Save button.
7. Click on the Back button to until you return to the main screen or the navigation history symbol  for a previously viewed screen.

Related Topic

IOCB1616 Operating Modes

AND - OR Conditions

GROUPS

In the Aurora software, door and elevator access is determined by groups. Each individual with a credential record is assigned to specific groups. The groups are then assigned access levels for doors and, if your site has elevator control, elevator floors.

Group Setup

Group Setup allows you to name the groups that are given an access level at doors and elevators. Create group names that have the same description as commonly used throughout your company or organization. Groups are listed under the Name field. Unnamed groups appear as Group # 001 to Group # 511.

Group Setup has the following 5 fields:

- Group [Name]
- Active
- Visitor Group
- E-Plex Group
- Intrusion User

Group [Name]

Use to distinguish specific groups. Access at each door or elevator floor is contingent on group access. Each person must be assigned to a group for access.

Active

A group must be active before it is viewable and can be assigned access levels in the Door Groups Access screen and the Elevator Groups Access screen. An active group is listed as Yes under the Active column. An inactive group is listed as No under the Active column.

- Group # 001 to Group # 016 are active by default
- Group # 017 and higher must be manually activated

Intrusion User

The User Intrusion field is used to assign individuals/groups defined in the Intrusion Users screen if the site is integrated with a compatible DSC or DMP intrusion panel. You require an Intrusion license from Keyscan otherwise this field is unavailable.

Visitor Group

Enable this field if you use the visitor management component and the group is designated for visitors.

E-Plex Group

Enable this field if you are using E-Plex series of wireless locks and have already set up an E-Plex Schedule to assign to this group.

Procedures

Steps to Add a Group

1. From the Client main screen, select the Site Management button > Group Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. Under the Group heading, click on the row of the first unassigned group you are naming.
3. Type a group name.
4. Do one of the following under the Active column:
    - For group #1 to group #16, leave the Active field on Yes (enabled).
    - For door group #17 to group #511, the default status is No (Disabled). Double click on the No along the group's row. Click inside the box. The box has an x when this function is enabled. When you click on the next field the status changes to Yes.
5. If this group is to be designated as a visitor group, double click on the No along the group's row under the Visitor Group heading. Click inside the box. The box has an x when this function is enabled. (When you click on the next field the status changes to Yes).
6. If you have intrusion users to be assigned to this group, with the current group row selected, double click over the User Intrusion column, click on the ▼ symbol and select the user/group from the drop down list - requires an Intrusion license.
7. To add another group, repeat the above steps.
8. When you have completed naming groups, click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Edit a Group

1. From the Client main screen, select the Site Management button > Group Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Group Setup tab is selected.
3. Under the appropriate headings, make the required changes.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Copy Groups

This feature copies the Group names and configuration from one site to multiple sites. However, this will overwrite the current settings in the other sites.

1. From the Client main screen, select the Site Information button > Group Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. Select the Copy Groups button to the right of Group Setup. A pop-up window will ask you to save any new changes before proceeding.
3. Select the applicable Sites by placing an **x** beside each one. Alternatively, input the site name into the Site Search filter above. Selected Sites will remain in the list regardless of the filter.
4. After all potential Sites are chosen, select the OK button. The Group Names, Is Active, and Is Visitor properties for those Groups will be copied to the selected Site(s) and applied to the corresponding Group based on the Group Number. Any matching fields will not be touched in this process. If any Site fails to save after this process, the changes to all of the Sites will rollback to what they were prior.

Door Group Access Levels

The Group Access Levels screen consists of the following sub-fields:

- Groups
- Readers
- Schedules

The Door Group Access screen is presented in a column format. It's used to assign each group an access level to the doors controlled by the access control units (ACU) in your system. There are three types of access levels:

- 24 Hour Access - 24HR
- No Access
- Scheduled Access

The Door Group Access screen can be set on Basic View or Advanced View as outlined. To change views, click on the Show Basic View/Show Advanced View button. The button changes description depending on the current view.

Show Basic View/Show Advanced View

The Door Group Access Levels screen can be set on one of the following view modes:

- Show Basic View - lists readers / time zone access for the selected group
- Show Advanced View - lists readers / time zone access for all groups

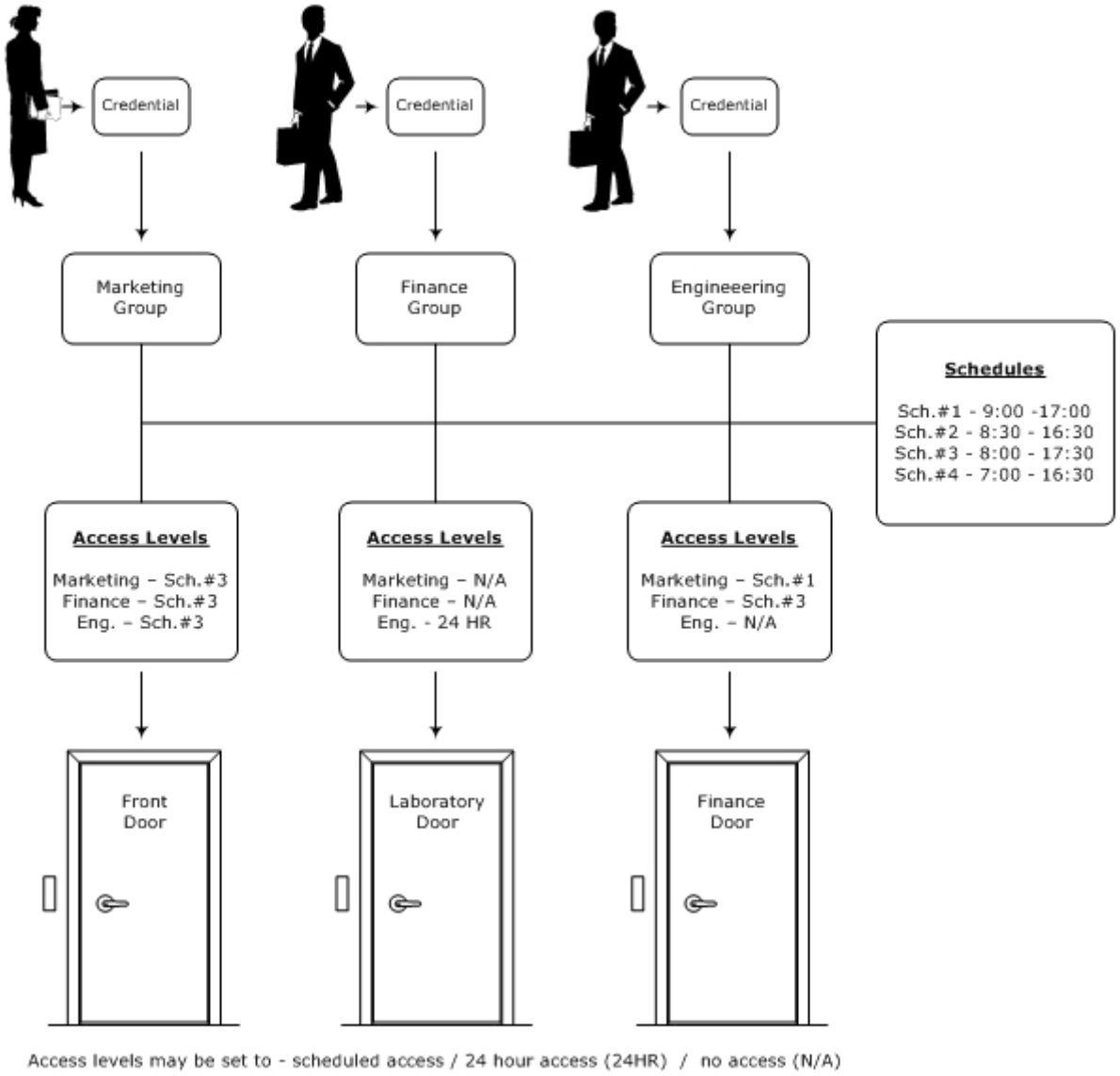


With either view mode, you can re-organize the way groups and access levels are presented by clicking on the column heading. For more information, click on Re-organizing Column Data below Related Topics.

Assign Door Group Access Levels - Example

The following diagram illustrates an example site where there are 3 different door groups Marketing, Finance, and Engineering, and 3 doors that are controlled by an ACU. Door group access levels are summarized above each door. Schedules are listed on the right. You will note that door groups either have 24 hour access, no access, or access limited to the schedule's defined hours.

Illustrated Example



Procedures

Steps to Assign a Door Access Level

Before you can assign door access levels, you must have previously created schedules, groups, and setup control units and identified doors. The instructions are based on working in Show Basic View. After you have set access levels for some of the groups and you are familiar working with the Door Group Access screen, try changing to the Show Advanced View to see which mode is more comfortable and functional based on your personal preference.

1. From the Client main screen, select the Manage People button > Group Access Levels.
    - If you have multiple sites, double click on the site from the directory screen.
2. Ensure that the Door Group Access tab is selected.
3. Near the bottom ensure Show Advanced View is displayed. This indicates you are working in Show Basic View. If the button lists Show Basic View, click on the button to change the screen.

Single Group/Single Reader/Single Access Level

1. Under the Groups heading, click on the group that you are assigning an access level. The group is highlighted in blue.
2. Under the Readers heading, click in the box to the left of the reader that will be assigned a time zone for access. The box has an x when selected.

3. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and select one of the following three options:
    - No Access
    - 24 HR - 24 hour access with no time restrictions
    - User-defined schedule which restricts access to the stated times
4. Click on the Apply button.
5. To assign another group a door access level, repeat the previous steps.
6. When you have completed assigning access levels, click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Single Group/Multiple Readers/Same Access Level

1. Under the Groups heading, click on the group that you are assigning an access level. The group is highlighted in blue when selected.
2. Do one of the following steps:
    - For all readers listed below the Readers column, click in the box to the left of Readers on the column heading. This selects all readers in the list.
    - For select readers, click in the box to the left of the individual readers below the Readers column. When selected the box has an x.
3. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and select one of the following three options:
    - No Access
    - 24 Hr - 24 hour access with no time restrictions
    - User-defined schedule which restricts access to the stated times
4. Click on the Apply button.
5. To assign another group a door access level, repeat the previous steps.
6. When you have completed assigning access levels, click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Edit a Door Access Level

1. From the Client main screen, select the Manage People button > Group Access Levels.
2. If you have multiple sites, double click on the site from the directory screen.
3. Ensure that the Door Group Access tab is selected.
4. Depending on what you are editing, select the appropriate group, reader or schedule and make the required changes.
5. Click on the Save button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

Elevator Group Access Levels

Re-organizing Column Data

Elevator Group Access Levels

The Elevator Group Access Levels screen consists of the following sub-fields:

- Group
- Reader
- Elevator Bank
- Schedule

The Elevator Group Access screen is presented in a column format. It's used to assign each group an access level to the floors controlled by the access control units (ACU) in your system. There are three types of access levels:

- 24 Hour Access - 24HR
- No Access
- Scheduled Access

The Elevator Group Access screen can be set on Basic View or Advanced View as outlined. To change views, click on the Show Basic View/Show Advanced View button. The button changes description depending on the current view.

Show Basic View/Show Advanced View

The Elevator Group Access Levels screen can be set on one of the following view modes:

- Show Basic View - lists readers / access for the selected group
- Show Advanced View - lists readers / access for all groups

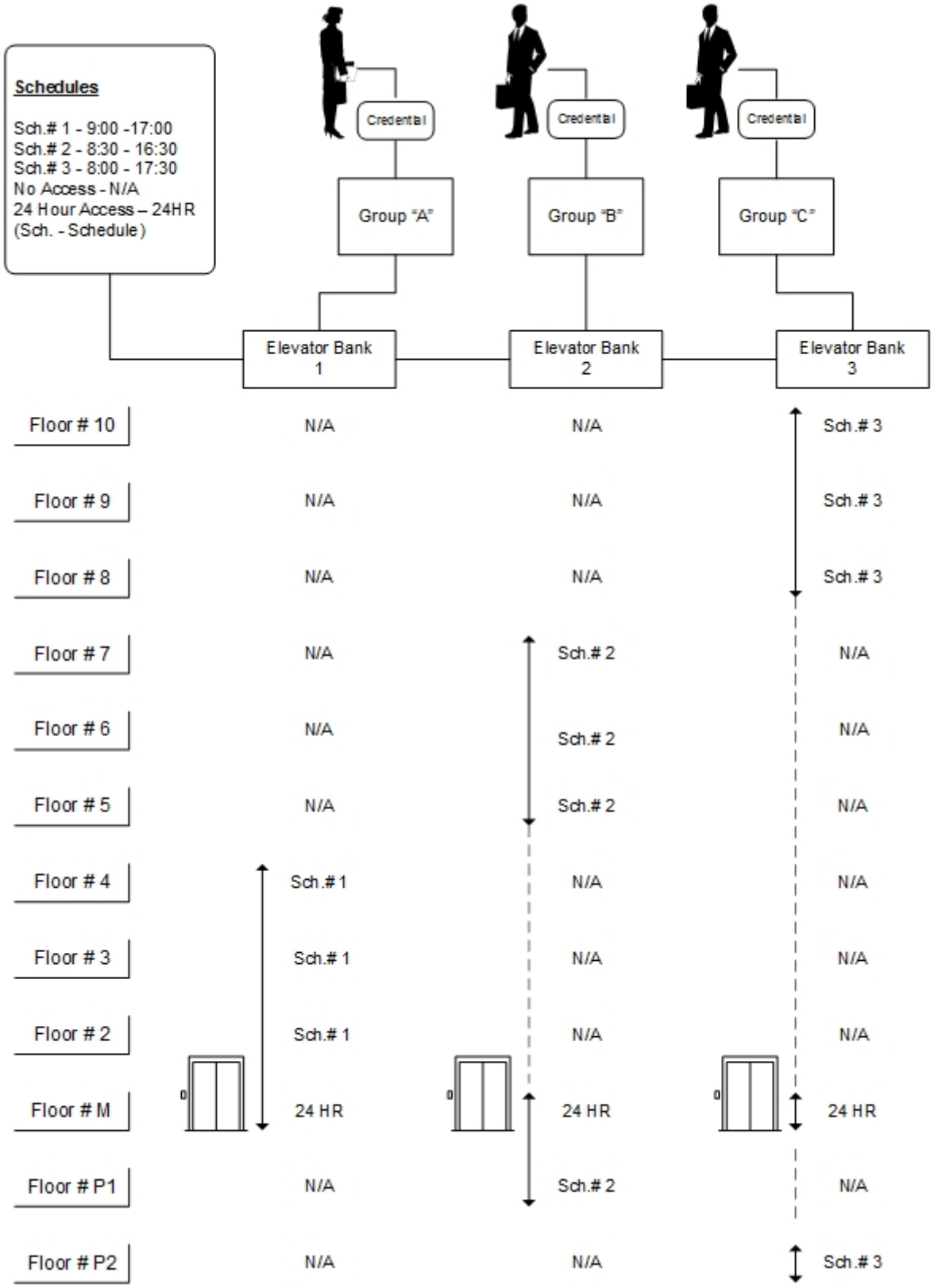


With either view mode, you can re-organize the way groups and access levels are presented by clicking on the column heading. For more information, click on the link below Related Topics.

Example

The following diagram illustrates an example site where there are 3 different groups, and 3 elevator banks in a multiple storey building. Each group has been assigned to a specific elevator bank with access limited to specific floors as summarized below. You will note that groups either have 24 hour access, no access, or limited access based the defined hours of a schedule.

Illustrated Example



Procedures

Steps to Assign an Elevator Access Level

Before you can assign elevator access levels, you must have previously created schedules, groups, and setup control units and identified elevator banks and elevator control units. The instructions are based on working in Show Basic View. After you have set access levels for some of the groups and you are familiar working with the Elevator Group Access Levels screen, try changing to the Show Advanced View to see which mode is more comfortable and functional based on your personal preference.

1. From the Client main screen, select the Manage People button > Group Access Levels.

- If you have multiple sites, double click on the site from the directory screen.

2. Ensure that the Elevator Group Access Levels tab is selected.
3. Click on the ▼ symbol opposite Banks, and select the elevator bank from the drop down list.
4. Near the bottom ensure Show Advanced View is displayed. This indicates you are working in Show Basic View. If the button lists Show Basic View, click on the button to change the screen.

Single Group/Single Floor/Single Access Level

1. Under the Groups heading, click on the group that you are assigning an access level. The group is highlighted in blue.
2. Under the Floor heading, click in the box to the left of the floor # that will be assigned a schedule for access. The box has an x when selected.
3. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and select one of the following three options:
   - No Access
   - 24 HR - 24 hour access with no time restrictions
   - User-defined schedule which restricts access to the stated times
4. Click on the Apply button.
5. To assign another group an elevator floor access level, repeat the previous steps.
6. When you have completed assigning access levels, click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Single Group/Multiple Floors/Same Access Level

1. Under the Groups heading, click on the group that you are assigning an access level. The group is highlighted in blue.
2. Do one of the following steps:
   - For all floors listed below the Floors column, click in the box to the left of Floors on the column heading. This selects all floors in the list.
   - For select floors, click in the box to the left of the individual floors below the Floors column. When selected the box has an x.
3. Near the bottom of the screen, click on the ▼ symbol opposite Schedule and select one of the following three options:
   - No Access
   - 24 HR - 24 hour access with no time restrictions
   - User-defined schedule which restricts access to the stated times
4. Click on the Apply button.
5. To assign another group an elevator floor access level, repeat the previous steps.
6. When you have completed assigning access levels, click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Edit an Elevator Access Level

1. From the Client main screen, select the Manage People button > Group Setup.

- If you have multiple sites, double click on the site from the directory screen.

2. Ensure that the Elevator Group Access Levels tab is selected.
3. Click on the ▼ symbol opposite Banks, and select the elevator bank from the drop down list.
4. Depending on what you are editing, select the appropriate group and elevator floor that require changes.
5. Click on the Save button.
6. Click on the Exit button for the main screen or the history navigation symbol for a previously viewed screen.

Related Topics

Re-organizing Column Data

E-Plex Group Access Levels

The E-Plex Group Access Levels screen consists of the following sub-fields:

- Groups
- E-Plex Door
- Schedule

The E-Plex Group Access screen is presented in a column format. It's used to assign each group an access level to doors controlled by an E-Plex series wireless lock. There are two types of access levels:

- Always
- No Access

The E-Plex Group Access screen can be set on Basic View or Advanced View as outlined. To change views, click on the Show Basic View/Show Advanced View button. The button changes description depending on the current view.

Show Basic View/Show Advanced View

The E-Plex Group Access Levels screen can be set on one of the following view modes:

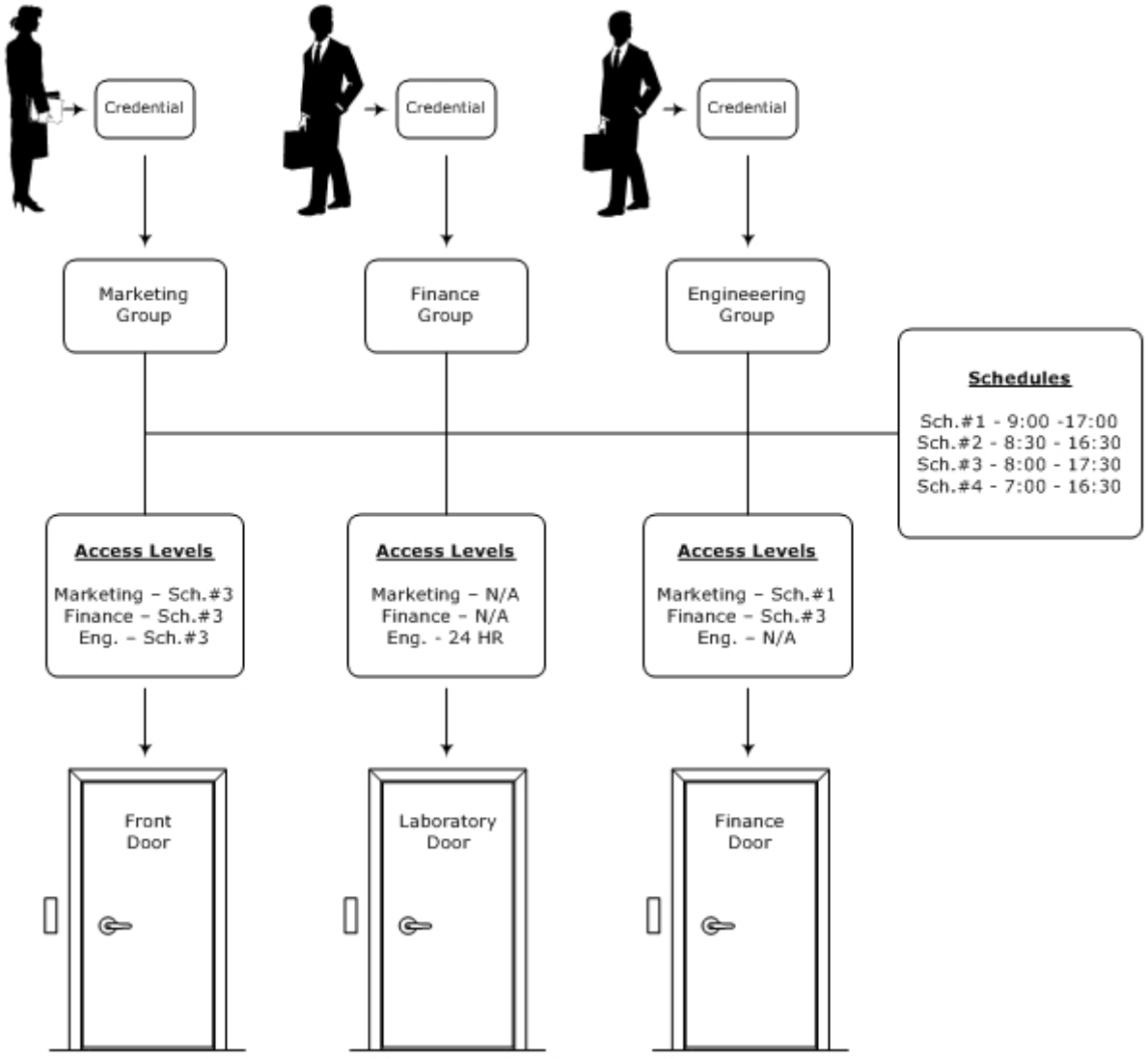
- Show Basic View - lists doors / time zone access for the selected group
- Show Advanced View - lists doors / time zone access for all groups

Tip > With either view mode, you can re-organize the way groups and access levels are presented by clicking on the column heading. For more information, click on Re-organizing Column Data below Related Topics.

Assign Door Group Access Levels - Example

The following diagram illustrates an example site where there are 3 different door groups Marketing, Finance, and Engineering, and 3 doors that are controlled by E-Plex wireless locks. E-Plex Group Access levels are summarized above each door. Schedules are listed on the right. You will note that door groups either have 24 hour access, no access, or access limited to the schedule's defined hours.

Illustrated Example



Access levels may be set to - scheduled access / 24 hour access (24HR) / no access (N/A)

Related Topics

Aurora E-Plex Integration Setup

BEST Group Access Levels

Prior to setting up BEST Group Access Levels, the Card Format(s), Schedule(s) and Door Group(s) must first be outlined. For a list of steps, read the following section:

BEST Offline Lock Integration Setup

Show Basic View/Show Advanced View

The BEST Group Access Levels screen can be set on one of the following view modes:

- Show Basic View - lists doors / schedules for the selected group
- Show Advanced View - lists doors / schedules for all groups

Tip > With either view mode, you can re-organize the way groups and access levels are presented by clicking on the column heading.

Assigning Group Access Levels

Follow these steps to properly assign group access levels to BEST Door Groups:

1. Under the Manage People menu, select Group Access Levels.
2. Select the BEST Group Access Levels tab. From the BEST Door Groups drop down menu, located at the top of the screen, select the applicable door group by scrolling through the options.
3. From the left-hand Group column, select the Group # by single-clicking.
4. From the right-hand Access For Group column, check the box(es) that corresponds to the BEST Door being managed; an **x** indicates selected.
5. Select between No Access, 24HR or your predetermined Schedule from the drop down menu below Schedule. You can also select multiple BEST Doors and select the Schedule for all selected with the drop down menu beside the Apply button.
6. Select Apply located at the bottom-right of the screen to save the current changes.
7. Select Save located at the bottom-right of the screen to confirm all Group Access Level changes.

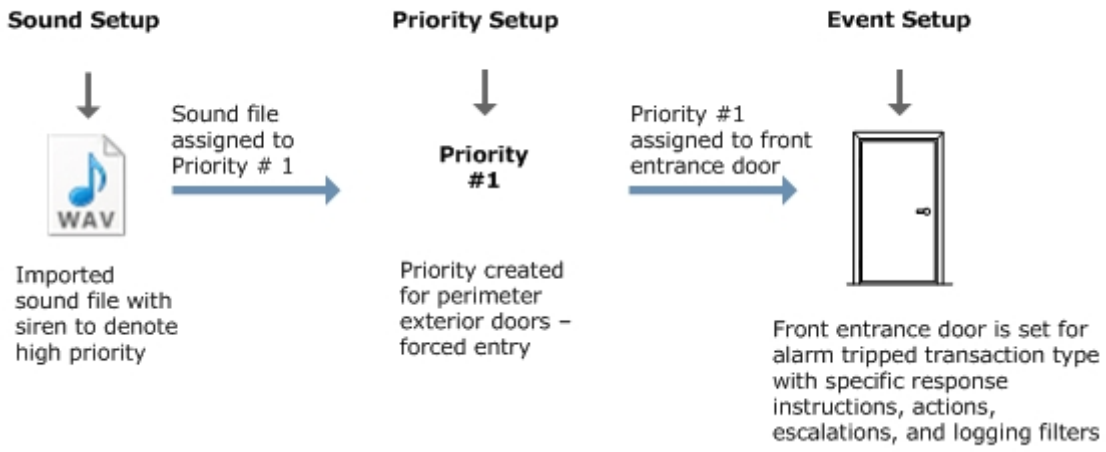
About Alarms and Events

As a Keyscan access control system is designed for regulating access at doors or elevators, it is also designed to keep you apprised of alarms and events. The Sound Setup, Priority Setup and Event Setup interface screens allow customizing and prioritizing alarms and conveying instructions in the event of an alarm.

Events Setup

- Sound Setup - imports sound files that you can attach to an alarm priority
- Priority Setup - creates classes of alarms with sound files for distinguishing the level of alarm importance
- Event Setup - consists of sub-screens for assigning a device to a transaction, response instructions, priority # and other customized properties

Example of How the Sound / Priority / Event Setup Screens Interact



For more on setting up events, click on the link below Related Topics.

Alarms

The Aurora software is designed to warn you of any alarms when a connected sensing device has been tripped or violated. Alarms can be triggered by input devices, door contacts, etc. In the event that an alarm occurs in the Aurora software, they are monitored from the Online Transaction screen and alarm response instructions are accessed from the Transaction Response screen. For more on alarms, click on the links below Related Topics.

Related Topics

- Sound Setup
- Priority Setup
- Event Setup
- Alarm Monitoring & Alarm Response

Sound Setup

Aurora includes sound files or you can import your own sound files that you may assign to priorities. Sound setup is regulated by permissions in your user account.

Procedures

Overview of Sound Setup

- + : allows adding a WAV file to the sounds column
- > : plays the selected WAV file
- X : stops play of the selected WAV file
- Change Sound : inserts a new WAV in place of the current WAV file
- Delete Button : deletes the WAV file from the Sounds column

Steps to Import WAV Sound Files

1. From the Client main screen, select the Site Management button > Sound Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. Select the + button to the left of Sounds on the Sound Setup screen.
3. From the Open dialog box, navigate to the desired folder with the WAV file.
4. Select the WAV file.
5. Select the Open button.
6. To preview the WAV sound file, click on the > button.
7. To stop the sound file, click on the X.
8. Select the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

System User Accounts

Priority Setup

Priority Setup

The Priority Setup screen allows creating a list of named alarm priorities and assigning a sound file to each priority. You can assign a priority with one of the WAV files included with Aurora or assign your own WAV files.

There are no limits on the number of alarm priorities you can create. However, you should keep alarm priorities at a manageable number so that other system users are not overwhelmed or confused at deciphering the importance of the alarm or event.

Priority setup is regulated by permissions in your user account.

Example

As an example, you may wish to create an alarm priority with a loud siren-like WAV file assigned to it. As building security is of the utmost importance, this high-level alarm priority could then be assigned to all building entrance doors in the Event Setup screen. In the event that one of these doors was either forced open or held open beyond its allotted time anyone monitoring the system is warned that this is an alarm of extreme importance as a perimeter door is not secure with the possibility of unauthorized intrusion.

Procedures

Overview of Priority Setup

- Priorities + : adds a priority to the priority list
- Number : the rank of the alarm priority - #1 is the top level
- Name : user defined name of the priority
- Sound : assigns and lists the WAV file assigned to the priority
- Bulk Clearing : when enabled allows using the Clear All in the Alarm screen
- Save : Saves the settings
- Exit : closes the Priority Setup screen
- Refresh : updates the Priority Setup screen

Steps to Create an Alarm Priority

1. From the Client main screen, select the Site Management button > Priority Setup.
    - If you have multiple sites, double click on the site from the directory screen.
2. Select the + button to the right of Priorities on the Priority Setup screen.
3. On the Priority # x just added, double click under the Name column to open the text box.
4. Enter a description for the priority. The description should relate to the priority so other system users will understand its importance and meaning.
5. Under the Sound column click on the row of the priority you are setting up. Click on the ▼ symbol and select the sound file from the drop down list.
6. To enable Bulk Clearing of the priority, click in the box. The box has an x when the function is enabled.
7. Select the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Event Setup

One of Aurora's underlying functions is monitoring and recording all events. Events are user transactions, such as when an individual presents a credential at a reader for accessing a door, or alarm transactions, such as if a door is forced open. As access control is deemed a security system, the Aurora software gives you a range of options for conveying critical information and instructions to other system users monitoring the Keyscan system for alarm transactions or user transactions.

The Event Setup screens are extremely important, especially for perimeter doors, perimeter sensing devices or high security areas. By completing these screens, those persons responsible for overseeing the access control system, such as security personnel, have concise protocols on who to contact or what to do.

Event Setup consists of six sub-screens. Each screen has a specific purpose as briefly reviewed below:

- Assigned Devices and Events - assigns a specific device to a specific transaction type
- Response Instructions - provides fields for conveying instructions, device locations, and contact names for handling alarms
- Actions - allows the selection of action to be taken such as sending an e-mail notification if the transaction occurs
- View Filters - assigns the event a priority level with designated properties
- Escalations - sets alternate response conditions if the event is not acknowledged by a system user for transactions occurring within the last 7 days
- Logging Filter - sets filtering modes

Event Settings Names & Assigning Devices

When adding a new event setting, the Client software creates a named event, Event Settings # 1, by default. Each Time a new event is created, it increments the number by one. However, event setup names can also be user-defined to give them more specific descriptions.

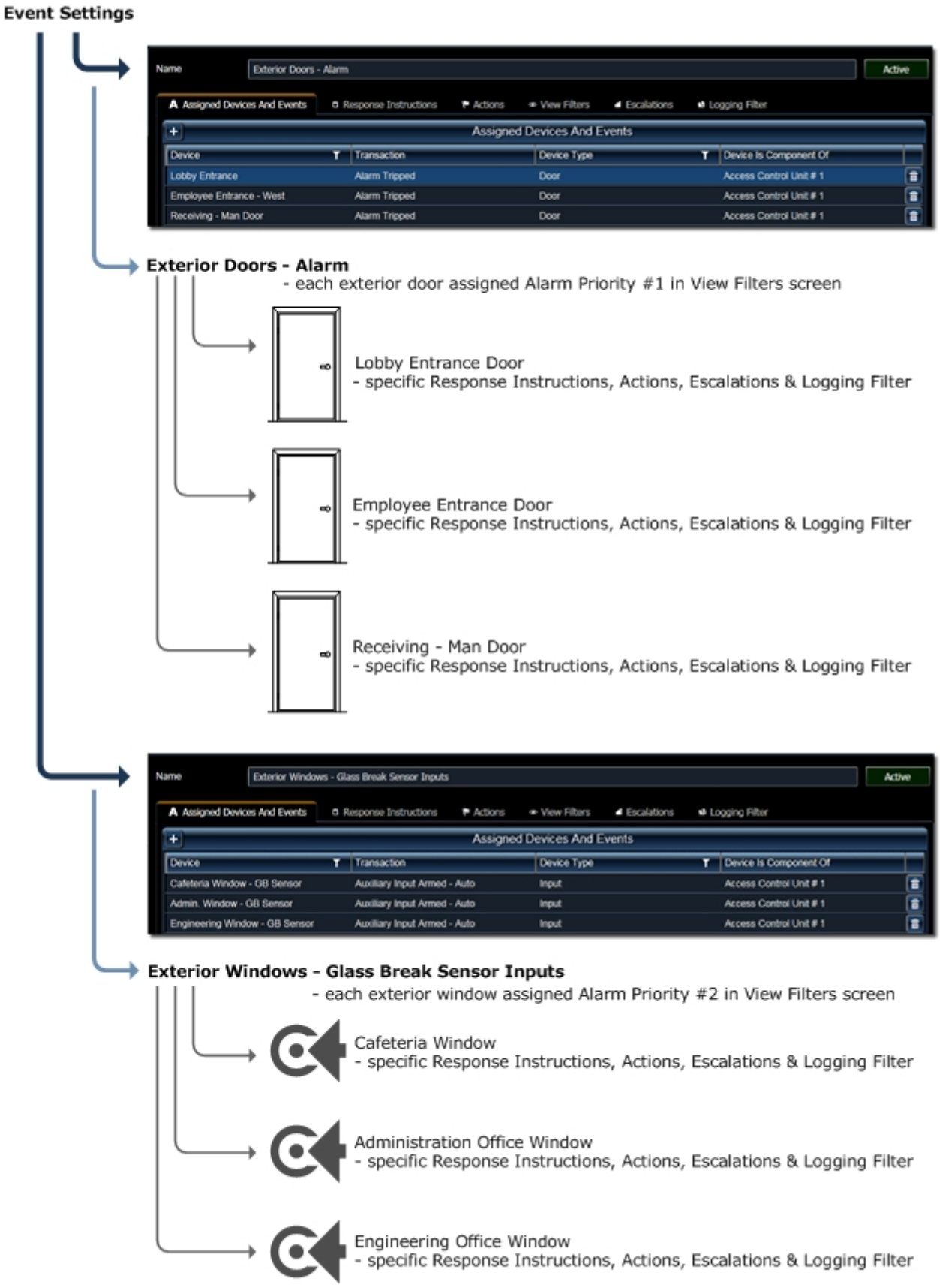
An event setting may contain just a single device assigned to a single transaction type or it may contain multiple devices assigned to multiple transaction types. This will depend on your particular building, types of devices, and security enforcement.

Example of Event Settings Names & Assigning Devices

As an example, a building has three exterior doors: Lobby Entrance, Employee Entrance, and a Receiving Man Door. As these are perimeter doors, they are deemed the most important doors to monitor for a forced entry. We have created an event settings name of Exterior Doors - Alarm. All three doors are placed in this event setting so we can further assign all three doors with Alarm Priority # 1. Each door is assigned to report an Alarm Tripped transaction so that the access control system software reports a potential unauthorized intrusion or break-in.

Also the building has three areas with exterior windows: cafeteria, administration and engineering that have glass-break sensors connected to auxiliary inputs. We have created another event settings name of Exterior Windows - Glass Break Sensor Windows. All three window sensor inputs are placed in this event setting so we can assign all three areas as Alarm Priority # 2. Each input is assigned Auxiliary Input Armed - Auto since they are only armed after business hours.

Illustrated Example



Procedures

Steps for Naming Event Settings

1. From the Client main screen, select the Site Management button > Event Setup.
    - If you have multiple sites, double click on the site from the directory.

2. From the Event Setup screen, select the Add Event Settings Button.
3. Opposite Name near the top of the screen, select the text Event Settings # x in the text box and press the delete key.
4. Enter a name for the event setting.
5. Click on the Save button.
6. For assigning devices/transactions to the event setting, see Assign Devices and Events; otherwise click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Sound Setup

Priority Setup

Assign Devices & Events

Assign Devices and Events

The Assigned Devices and Events screen assigns a transaction event to a named Event Setting for any of the following devices:

- access control unit
- elevator control unit
- wireless lock
- door
- input
- output

Each device has its own specific list of selectable transaction types. Although you can select multiple device/ transaction event assignments for each event setting, Keyscan recommends that you keep your assignments limited to critical devices and transactions.

Note

Once you have assigned a device to a transaction, you cannot edit the assignment. If you either made a mistake or wish to re-assign the device to another transaction, you must delete the assignment by clicking on the Delete button (waste bin icon) to the right and then repeat the procedures.

When a device has been previously assigned a transaction type, it is dimmed, not selectable, and lists the Event Setting # it is currently under.

Procedures

Steps to Assign a Device to an Event

These instructions assume that you have named an event setting. If not, see Event Setup.

1. From the Client main screen, select the Site Management button > Event Setup.
    - If you have multiple sites, double click on the site from the directory.
2. With the All tab selected, below the Names heading, double click on the event setting that you are adding a device and transaction.
3. On the left of the Assigned Devices and Events heading, select the + button.
4. Below the heading Please Select Device(s) and Event(s), click on the ▼ symbol opposite Access Control Unit.
5. Select the unit from the drop down list that is either connected to the device or is to be assigned a transaction directly.
6. Opposite Device, click on the ▼ symbol and select the device from the drop down list. Wait while the software populates the transaction list for the type of device you have selected.
7. Select the desired transaction by clicking in the box to the left. The box has an x when selected. You can assign multiple transactions.
8. Click on the Save button.
9. If you are assigning more devices to transactions, repeat the above procedures.
10. When you have completed assigning devices to transactions, ensure you select the Save button.
11. Do one of the following steps:
    - If you are completing other Event Setup screens, select the desired tab at the top.

- To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Response Instructions

Use the Response Instructions screen to outline critical information and instructions to be followed by system users, such as security personnel, monitoring the Keyscan system whenever the event setting occurs. The Response Instructions screen consists of specifying the following information:

- Instructions - enter specific instructions on what is to be done if the event setting occurs
- Location - enter a description which informs where the device is situated for investigation if the event setting occurs
- Contacts - select individuals from the Manage People list who are responsible for or must be informed of an event setting occurrence
    - Common Optional fields populated with data on the Manage People screen may be added with the contact information
- Emergency Contacts - enter specific emergency contact information such as a security service etc who are contacts other than those specified in the Contacts list
- Maps - specify a map that can be manually opened to identify the location of the event setting (If you specify a map in the Actions screen, the map opens automatically when the Online Transactions screen is open or minimized on the desktop.)

Contacts & Emergency Contacts

With Aurora's Response Instructions screen, please note the difference between contacts and emergency contacts. Contacts are selected from a drop down list of people that you have previously entered in the Edit Person screen. Emergency contact information on the other hand is entered manually in a text box.

Which type you use will depend on your company's or organization's security policies and procedures. In some cases you may have your own internal security personnel who are persons of record in the Aurora software, in which case they would be selected from the Contacts field. In other cases, such as if you contracted an outside security service, you would enter the information in the Emergency Contacts text box. And in other cases you may have both Contacts and Emergency Contacts listed.

In cases where you do not have anyone monitoring the Aurora software, Keyscan recommends that you review assigning an e-mail address to alarm transactions or critical event transactions in the Actions screen so that someone is apprised of a potential security violation or intrusion.



The Contacts list is populated from the Manage People list. You must have existing people records (Edit Person screen) before you can specify contacts in the Response Instructions screen.

Procedures

Steps to Set Response Instructions

1. Do one of the following steps:
    - If you are currently on an Event Setup screen at the desired Event Setting #, select the Response Instructions tab.
    - If you are on the Client main screen, select the Site Management button > Event Setup. If you have multiple sites, double click on the site. Select the desired Event Setting # associated with the response instructions you are creating. Select the Response Instructions tab. Ensure you have assigned devices to transactions for this event setting.
2. Click inside the Instructions text box and enter the instructions to be carried out when the event setting occurs.

3. Click inside the Location text box and enter the location of the device.
4. Click on the Contacts + button.
    - Cancel button - selecting the Cancel button closes the contacts list and cancels your selection.
5. From the drop down list, select the contact. The contact is highlighted in blue when selected.
6. With the contact highlighted, click on the contact's + button.
    - Cancel button - selecting the Cancel button closes the optional fields list, cancels any selection you made and returns you to the contacts list.
7. You have the option of selecting specific common optional fields such as a phone number and extension number or e-mail address to immediately inform the contact of the situation. To select an optional field, click in the box to the left. The box has an x when selected.
    - If you do not want any optional fields added with the contacts name, leave the fields blank and go to the next step.
8. Click on the OK button.
9. To add an additional contact, repeat the preceding 3 steps.
10. To enter emergency contacts, select the Emergency Contact + button.
11. Below the Details column, click in the text box and enter the desired emergency contact information.
12. If more than 1 emergency contact is created per event setting, you can alter the order by clicking and dragging the contact to a higher or lower row position.
    - Each emergency contact added is assigned a number starting at Number 1 and increasing by 1 each time a contact is added.
13. If you have site maps, click on the  symbol to the right of Map and select the map from the drop down list.
14. When you have completed the Response Instructions screen, select the Save button.
15. Do one of the following steps:
    - If you are completing other Event Setup screens, select the desired tab at the top.
    - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topic

 Actions

Actions

The Actions screen allows setting any or all of the following actions for the event setting. Setting some actions will require either optional hardware or optional software module licenses. The following actions can be set for an event setting:

- Command Action - executes a command line when the event setting occurs
    - generally a command line shells out to a third party software application
- E-mail Action - issues an e-mail notice with transaction details to a specified address when the event setting occurs
    - SMTP must be configured and may require Photo and Verification license
- Map Action - opens a user-created map indicating the source of the transaction when the event setting occurs
- Video Action - initiates NVR/Camera operation when the event setting occurs
    - Requires a Video license with NVR and camera integration with the access control system

Procedures

Steps to Assign Actions to Events

These instructions assume that you have named an event setting. If not, see Event Setup.

1. Do one of the following steps:
    - If you are currently on an Event Setup screen at the desired Event Setting #, select the Actions tab.
    - If you are on the Client main screen, select the Site Management button > Event Setup. If you have multiple sites, double click on the site in the directory screen. Select the desired Event Setting #. Select the Actions tab. Ensure you have assigned devices to transactions for this event setting.
2. Click on the ▼ symbol on the Add Action button.
3. From the drop down list, select the type of action you are using for this event setting and follow the appropriate instructions outlined below.

Command Action

The Command Action requires an assigned schedule. If using a schedule other than 24HR, you must create a schedule before you can complete this screen.

1. Select Command Action on the left to open the command action fields.
2. Click inside the Command text box and enter the command line.

   Note: The Command line is a full path to an executable/batch command file. The executable file must be on the computer running the agent.

3. Click on the ▼ symbol opposite Schedule and select a schedule from the drop down list.
4. If the command is in effect while the schedule is on, click in the box to the left of Operates when Schedule is Active. The box has an x when selected.
    - If the command action is to occur when the schedule is off, leave the Operates when Schedule is Active box de-selected.

5. Click on the Save button.
6. Do one of the following steps:
    - If you are completing other actions, select the ▼ symbol on the Add Action button.
    - If you are completing other Event Setup screens, select the desired tab at the top.
    - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

E-mail Action

The SMTP function must be set in the Application Utilities screen to use the E-mail Action. SMTP requires the assistance of IT personnel. E-mail Action requires an assigned schedule. If using a schedule other than 24HR, you must create a schedule before you can complete this screen.

1. You may have to select the v symbol beside E-mail Action on the left to open the e-mail action fields; otherwise go to the next step.
2. Opposite E-mail Address(es), click in the text box and enter the e-mail address of the recipient. If entering more than one e-mail address, separate the addresses with a semicolon (;). The maximum is 255 characters.
    - As an option you can also create an e-mail action for each individual e-mail address.
3. Click on the ▼ symbol opposite Schedule and select a schedule from the drop down list.
4. If the command is in effect while the schedule is on, click in the box to the left of Operates when Schedule is Active. The box has an x when selected.
    - If the command action is to occur when the schedule is off, ensure the Operates when Schedule is Active box is not selected.
5. If the event setting has credential transaction types, such as access granted or access denied modes, to include a photo of the person, select the Include Photo in E-mail option.
    - To limit the Include Photo in E-mail option to specific credential bearers, click on the + opposite People selection. From the list, select the desired individuals by clicking on the > symbol at the right of the name.
6. Click on the Save button.
7. Do one of the following steps:
    - If you are completing other actions, select the ▼ symbol on the Add Action button.
    - If you are completing other Event Setup screens, select the desired tab at the top.
    - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Map Action

Map Action requires an assigned schedule. If using a schedule other than 24HR, you must create a schedule before you can complete this screen.

1. You may have to select the v symbol beside Map Action on the left to open the Map action fields; otherwise go to the next step.
2. Click on the ▼ symbol opposite Map and select a map from the drop down list.
3. Click on the ▼ symbol opposite Schedule and select a schedule from the drop down list.
4. If the command is in effect while the schedule is on, click in the box to the left of Operates when Schedule is Active. The box has an x when selected.

- If the command action is to occur when the schedule is off, leave the Operates when Schedule is Active box de-selected.

5. Click on the Save button.
6. Do one of the following steps:
   - If you are completing other actions, select the ▼ symbol on the Add Action button.
   - If you are completing other Event Setup screens, select the desired tab at the top.
   - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Video Action

Video Action requires an assigned schedule. If using a schedule other than 24HR, you must create a schedule before you can complete this screen.

1. You may have to select the v symbol beside Video Action on the left to open the video action fields.
2. Click on the ▼ symbol opposite Video Device and select a unit from the drop down list.
3. Click on the ▼ symbol opposite Camera and select a camera from the drop down list.
4. Click on the ▼ symbol opposite Schedule and select a schedule from the drop down list.
5. If the command is in effect while the schedule is on, click in the box to the left of Operates when Schedule is Active. The box has an x when selected.
   - If the command action is to occur when the schedule is off, leave the Operates when Schedule is Active box de-selected.
6. Click on the Save button.
7. Do one of the following steps:
   - If you are completing other Event Setup screens, select the desired tab at the top.
   - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

View Filters

The View Filters screen allows assigning an event setting to an alarm priority configured in the Priority Setup screen. You can set the following conditions and properties to a priority.

- Priority - assign the event setting to a pre-defined priority created in the Sound and Priority Setup screen
- Schedule - specify a schedule which governs the period when the priority is in effect
    - 24HR - the priority is always in effect
    - Schedule - the priority is only in effect while the schedule is on
- Sound - assign a sound file to play when the event setting occurs as a priority – see Sound below
- Text Colour - assign the priority to display in selected colour
- Users - assign system users to view and handle priorities

Schedules

You can use existing schedules or create specific schedules for specific priorities depending on your requirements.

Sounds

The View Filters function provides an option of playing a sound file with a priority. This is an optional feature.

If you have assigned a sound file to a priority in the Priority Setup screen, and you also assign a different sound file to the event setting in the View Filters screen, the sound file assigned in the View Filters screen plays once and the sound file assigned in the Priority Setup screen will follow and play repeatedly until the event is put on hold or cleared.

If multiple priorities occur, the sound file assigned to the highest ranking priority will play until it is cleared followed by the next highest ranking priority sound file and so on.

Procedures

Steps to Set View Filters

1. Do one of the following steps:
    - If you are currently on an Event Setup screen at the desired Event Setting #, select the View Filters tab.
    - If you are on the Client main screen, select the Site Management button > Event Setup. If you have multiple sites, double click on the site in the directory screen. Select the desired Event Setting #. Select the View Filters tab. Ensure you have assigned devices to transactions for this event setting.
2. Select the + button to the left of the View Filter heading.
3. Click on the ▼ symbol opposite Priority and select a priority from the drop down list.
4. Click on the ▼ symbol opposite Schedule and select a schedule from the drop down list. The priority is in effect while the schedule is on.
    - If you need to create a specific schedule for this priority, select the Save button, open the Schedule Management screen, create and save the schedule, and then return to the View Filters screen.

5. Click on the ▼ symbol opposite Sound and select a sound from the drop down list. You can also leave this field blank if you assigned a sound in the Priority Setup screen or no sound is required.
6. To display the prioritized event setting in a colour other than the default colour, click on the ▼ symbol opposite Colour and select a colour from the palette.
7. For system users who are to view or handle priorities, click on the Users + button.
8. To select a user or users from the list, click in the box to the left. The box has an x when selected. For any non-selected system users, events will be reported in the normal mode.
9. When you have completed the View Filters screen, select the Save button.
10. Do one of the following steps:
    - If you are completing other Event Setup screens, select the desired tab at the top.
    - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

ESCALATIONS

The Escalations screen can be used as a "failure to respond" by ether firing an output or issuing an e-mail when an assigned device goes into alarm and the alarm has not been cleared within the last 7 days.

If you assign devices to trip outputs in the Escalations screen, ensure that those outputs are available and have not been assigned to either a schedule or an input in the Client software, otherwise you may have a conflict.

If a device goes into alarm either the output will continue to be fired or e-mail messages will continue being transmitted until the alarm is cleared.

Procedures

Steps to Setup Escalations

1. Do one of the following steps:
    - If you are currently on an Event Setup screen at the desired Event Setting #, select the Escalations tab.
    - If you are on the Client main screen, select the Site Management button > Event Setup. If you have multiple sites, double click on the site. Select the desired Event Settings # associated with the escalation you are creating. Select the Escalation tab. Ensure you have assigned devices to transactions and set view filters for this event setting.
2. Select the + button to the left of the Escalations heading.
3. If you are assigning the escalation with a time delay before the output is triggered, click on the ▼ symbol opposite Minutes to wait before output is triggered and select the desired minute delay from the drop down list.
4. Click on the ▼ symbol opposite Auxiliary outputs that will be triggered and select the output or outputs from the drop down list by clicking in the box or boxes to the left. The box has an x when selected.
5. If you are assigning the escalation to issue an e-mail, click on the ▼ symbol opposite Minutes to wait before an e-mail is sent and select the desired minute delay from the drop down list.
6. Click on the ▼ symbol opposite E-mail Address(es) and enter the recipient's e-mail address. If more than one address is entered, separate the addresses with a semicolon (;).
7. Click on the ▼ symbol opposite Schedule and select the desired schedule from the drop down list when the escalation period is in effect.
8. If the escalation is to occur when the schedule is off, ensure the Operates when Schedule is Active box is de-selected.
9. Select the Save button.
10. Do one of the following steps:
    - If you are completing other Event Setup screens, select the desired tab at the top.
    - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Logging Filter

The Logging Filter function gives you the option to filter out events while the priority's schedule is in effect. If this option is used, alarms are only reported in transaction reports or they are completely disabled. The 3 modes are as follows with explanations outlined below.

- Standard
- Record Only
- Disabled

An example application where this function could be applied might be at a busy door with a short door held open time period and you want to suppress Door Held Open Alarms. By selecting one of the modes below, except Standard Mode, any Door Held Open Alarms for that door would not be annunciated in either the online transaction screen or the alarm notification screen.

Standard Mode

This is the default mode that applies to all alarm priorities unless one of the other modes below is selected. Standard Mode annunciates alarm priorities in the Client's Online Transaction screen and, if enabled, the Alarm Notification screen.

Record Only Mode

Record Only mode suppresses an alarm type from being annunciated in the Client's Online Transaction screen. You can control when the mode is in effect with schedule ON and schedule OFF settings. If Record Only mode is selected, the alarm can only be reviewed by running a Transaction Report with the relevant devices, transaction types, and date parameters specified.

Disabled

Disabled mode suppresses the alarm priority from being annunciated in the Client's Online Transactions screen. When disabled is in effect, assigned alarms are not listed in a transaction report.

If disabled is selected, the user must select a reason for disabling the alarm type. Reasons are user-defined in the Application Utilities screen.

Procedures

Steps to Set Logging Filters

1. Do one of the following steps:
    - If you are currently on an Event Setup screen at the desired Event Setting #, select the Logging Filter tab.
    - If you are on the Client main screen, select the Site Management button > Event Setup. If you have multiple sites, double click on the name of the site. Select the desired Event Settings # associated with the logging filter you are creating. Select the Logging Filter tab. Ensure you have assigned devices to transactions and set view filters for this event setting.
2. Click on the ▼ symbol opposite Schedule and select a schedule from the drop down list.
3. In the Schedule On Mode pane opposite Type, click on the ▼ symbol and select the event logging mode from the drop down list.
    - If you selected disabled, opposite Disabled Reason, click on the ▼ symbol and select the disabled reason from the drop down list. Disabled Reasons are user-defined in the Reason for Disabling Logging pane on the Application Utilities screen.

4. In the Schedule Off Mode pane opposite Type, click on the symbol and select the mode from the drop down list.
5. Click on the Save button.
6. Do one of the following steps:
    - If you are completing other Event Setup screens, select the desired tab at the top.
    - To close the Event Setup screens, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

Reason for Disabling Logging

Custom Transaction Names

The Custom Transaction Names screen allows changing the Aurora default transaction descriptions and creating your own custom names.

Example of Custom Transaction Name Change

As an example, if an access control unit lost communication with the software because someone inadvertently unplugged a network cable, the transaction description is Comms Failure in the On-Line Transactions screen. You could change the default name from Comms Failure to something more descriptive such as Communication Failure with Control Unit. In some cases more descriptive transaction names may be more helpful for persons monitoring the system and alerting them to conditions that warrant immediate investigation.

Some event transaction descriptions are used by more than one device type such as alarm tripped which is an alarm event for both doors and inputs. When changing descriptions for events, be sure that you take this into consideration so your renamed event is appropriate where more than one type of device applies.

Procedures

Steps to Create a Custom Transaction Name

1. From the main screen, click on the Settings icon > Custom Transaction Name.
2. From the Custom Transaction Name screen, click on the + button at the left of the Changed Custom Transaction Names heading.
3. Click on the symbol at the right of Device, and select the type of device from the drop down list.
4. Click on the > symbol opposite the event name to be customized.
5. Click on a blank area of the screen.
6. Click on the row just added under the Custom Transaction Name heading.
7. In the text box enter you custom name for the event.
8. Click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Device Image Setup

The Device Image Setup screen allows inserting images of doors, readers, output devices, input devices and IOCB1616 input devices. Images attached to doors / devices displayed on the Device Image Setup screen are shared with and accessible to the Active Map Template Editor and maps.

Assigning an image to the device may assist system users in identifying the device and its location especially if it goes into an alarm state.

You can attach images of the following devices:

- Doors (including E-Plex Doors)
- Readers
- Input Devices such as motion sensors
- Output devices such as CCTV cameras
- IOCB1616 input and output devices
- Elevator Floors
- Video devices
- Intrusion devices*

* Applies to DSC alarm panels with a Keyscan integration license.

Procedures

Steps to Insert an Image

1. From the Client main screen, select the Site Management button > Device Image Setup.
    - If you have multiple sites, double click on the site from the directory.
2. Click on the ▼ symbol opposite Access Control Unit and select the desired control unit from the drop down list if it is not currently displayed.
3. Select the appropriate device tab.
4. Position the cursor over the device icon.
5. When the cursor hovers over the icon, the icon reveals a + symbol. Click on the + symbol.
6. From the Open dialog box, navigate to the folder with the image of the device. Select the image file.
7. Click on the Open button. The image is inserted under the device description on the Device Image setup screen.
8. To insert another image repeat the preceding steps.
9. When you have completed inserting images, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Change a Device Image

1. From the Client main screen, select the Site Management button > Device Image Setup.
    - If you have multiple sites, double click on the site from the directory.

2. Click on the ▼ symbol opposite Access Control Unit and select the desired control unit from the drop down list if it is not currently displayed.
3. Select the appropriate device tab.
4. Position the cursor over the device's current image.
5. When the cursor hovers over the image, the button reveals a + symbol. Click on the + symbol.
6. From the Open dialog box, navigate to the folder with the replacement image of the device. Select the image file.
7. Click on the Open button. The new image is inserted under the device description on the Device Image setup screen.
8. To change another image, repeat the preceding steps.
9. When you have completed inserting images, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Delete a Device Image

1. From the Client main screen, select the Site Management button > Device Image Setup.
    - If you have multiple sites, double click on the site from the directory.
2. Click on the ▼ symbol opposite Access Control Unit and select the desired control unit from the drop down list if it is not currently displayed.
3. Select the appropriate device tab.
4. Position the cursor over the device's current image.
5. When the cursor hovers over the image, the button reveals a + symbol and waste bin symbol. Click on the waste bin symbol.
6. The image is removed.
7. To delete another image, repeat the preceding steps.
8. When you have completed inserting images, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Default Device Images

Aurora uses a set of default icons that represent the devices the system monitors. These icons graphically represent their respective devices in the status widgets screens and may also be inserted on active maps with interactive controls. The following list outlines the devices:

Icon	Device
	Auxiliary Output - represents an assigned auxiliary output connected to devices such as alarm panels, or 3rd party devices regulated by a time zone.
	Door - represents a door or entry point connected to and monitored by the access control unit indicating the status of the door - locked or unlocked.
	Elevator Floor - represents an elevator floor monitored by an elevator control unit with a status of the floor buttons - secured or unsecured.
	Reader Icon - represents a reader on an active map.
	IOCB1616 Input - represents an assigned IOCB1616 input connected to a monitoring or sensing device with a status of normal (on) or disarmed (off).
	Camera Icon - represents a CCTV video camera connected to a camera port on a NVR interfaced with the access control system.
	Auxiliary Input - represents an assigned auxiliary input connected to a monitoring or sensing device with a status of normal (on) or disarmed (off).



IOCB Output - represents an assigned IOCB1616 output connected to devices such as alarm panels, or other 3rd party devices.



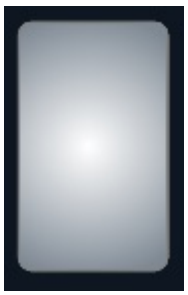
Intrusion Partition - represents a DSC alarm panel intrusion partition. Requires an optional DSC integration license from Keyscan for alarm monitoring from the Client software.



Intrusion Area - represents a DMP alarm panel intrusion area. Requires an optional DMP integration license from Keyscan for alarm monitoring from the Client software.



Intrusion Partition - represents a DSC or DMP alarm panel intrusion zone. Requires an optional DSC integration license from Keyscan for alarm monitoring from the Client software.



Gateway - represents an E-Plex Wireless Gateway.

If desired, you can import your own custom icons to represent any or all of the above listed default image icons in the Default Device Images screen.

Procedure

Steps to Insert a Custom Device Icon

1. From the Client main screen, select the Settings button > Default Device Images.
    - If you have multiple sites, the icons apply to all sites.
2. Position the cursor over the device icon.
3. When the cursor hovers over the icon, the icon reveals a + symbol. Click on the + symbol.
4. From the Open dialog box, navigate to the folder with the custom device icon. Select the image file.
5. Click on the Open button. The image is inserted under the device type.
6. To change another device icon, repeat the preceding steps.
7. When you have completed changing device icon images, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

- Active Map Template Editor
- Auxiliary Output Status
- Doors Status
- Elevator Floor Status
- IOCB Input Status
- IOCB Output Status
- Input Status

Device Status Images

Aurora uses a set of default icons that represent the status of the devices the system monitors. These icons graphically represent the status or state the devices are currently in when viewed in the status widgets screens.

Icon	Device Status
	Shunt - an input is currently disarmed by a manual toggle
	Manual - the device has been manually manipulated by user intervention
	Automatic - the device's state has been set by a time zone or schedule assignment
	Pulse - indicates a system user has pulsed a door or elevator floor button - the door momentarily unlocks for access and then re-locks - an elevator floor button is momentarily unsecured for access and then re-secured Door pulse duration is based on the door relay unlock time setting. Elevator floor pulse duration is based on the floor button selection time setting.
	Door Armed - a door is locked
	Door Disarmed - a door is unlocked
	Timed - a door is currently in a user-initiated timed unlock period or an elevator floor is in a user-initiated timed unlock period (not-secured)



Unknown - the software has not communicated with the device



Armed - an input or output is armed (an output may also be referred to as in its on state)



Disarmed - an input or output is disarmed (an output may also be referred to as in its off state)



Warning - indicates that a door remains open past the door held open time setting following an authorized access



Alarm - the device is currently in an alarm state



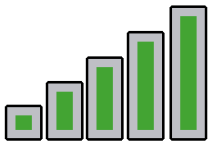
Reader/Keypad - indicates a reader/keypad is currently set on card or keypad mode of operation



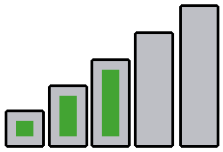
Reader/Keypad - indicates a reader/keypad is currently set on card only mode of operation



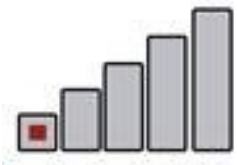
Reader/Keypad - indicates a reader/keypad is currently set on card and keypad mode of operation



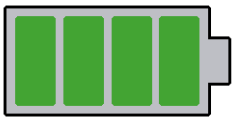
Indicates a Very Good connection between an E-Plex wireless lock and a gateway.



Indicates a Good connection between an E-Plex wireless lock and a gateway.



Indicates an Unacceptable connection between an E-Plex wireless lock and a gateway. Consider moving the Gateway closer to the wireless lock to improve signal strength.



Indicates normal battery life within an E-Plex wireless lock.



Indicates low battery life left within an E-Plex wireless lock. The battery should be replaced soon.



Indicates a dead battery within an E-Plex wireless lock. The battery must be replaced immediately to resume regular operations.

If desired, you can import your own custom icons to represent any or all of the default status icons.

Procedure

Steps to Insert a Custom Status Icon

1. From the Client main screen, select the Settings button > Device Status Images.
    - If you have multiple sites, the icons apply to all sites.
2. Position the cursor over the status icon.

3. When the cursor hovers over the icon, the icon reveals a + symbol. Click on the + symbol.
4. From the Open dialog box, navigate to the folder with the custom status icon. Select the image file.
5. Click on the Open button. The image is inserted under the status type.
6. To change another status icon, repeat the preceding steps.
7. When you have completed changing status icon images, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Alarm Monitoring & Alarm Response

Alarm monitoring and viewing alarm response instructions are performed from the following Aurora screens:

- Alarm Monitoring - Online Transactions screen
- Title Bar (all screens) - System Health Icon
- View Alarm Response Instructions - Transaction Response screen

Refer to the sub-headings below for specific details on each screen.

Alarm Monitoring

For monitoring alarms, use the Online Transaction screen. Alarms are highlighted with a red background so they are readily discernible from all other events within the Online Transaction screen. The Online Transaction screen lists the following alarm information:

- Device - the name of the device as defined in the Hardware setup screen - door, input, output or ACU#
- Transaction - lists the type of alarm
- Date - lists the date and time the alarm occurred dd/mm/yyyy : hh/mm/ss : AM or PM
- Access Control Unit - list the access control unit connected to the device reporting the alarm

Maps - Online Transaction Screen

The Online Transaction screen must be open for maps to display automatically. Maps or floor plans are created in the Active Map Template Editor and must be programmed to open in one of the two Event Setup screens - Response Instructions or Actions.

Comms Failure/Unit Marked Inactive Alarms

The Comms Failure alarm indicates that the access control software has lost communication with a specific access control unit. When this happens the access control software automatically marks the unit inactive and no longer polls it for activity. You should contact your dealer if the alarm is inexplicable and you cannot restore communication with the affected access control units.

Alarm Notice - System Health Icon

The System Health icon positioned in Aurora's upper left corner acts as a barometer of current system conditions. A red icon indicates new or on hold alarm transactions. You can access the Transaction Response screen by clicking on the  red health icon and then selecting the # New or On Hold Transactions text. For more about system health, click on the link below Related Topics.

View Alarm Response Instructions

The Response Instructions screen lists instructions and contacts so anyone monitoring the Client software is aware of the alarm’s source and the action required. The screen has an area where the system user can record any alarm comments indicating the actions taken. From the Response Instructions screen, alarms are completed indicating the alarm has been acknowledged or placed on hold for further investigation.

You must have completed the Response Instructions screen for system controlled doors and devices from the Event Setup function in Site Management menu; otherwise, the Response Instructions in the Transaction Response screen are blank.

Procedures for Responding to an Alarm

Open the Online Transaction Screen for Alarm Monitoring

1. From the Client main screen, select the Status button > Status.
    - If you had a Status screen open previously while logged on, that screen reopens when you access the Status function. To close the screen, select the x at the right of the screen's title bar.
2. From the Status screen, double click on Online Transactions.
3. On the far right side of the Online Transaction title bar, select the ▼ symbol and select the applicable site from the drop down list.
    - The Online Transaction screen lists the last 50 transactions that have occurred. You can retain the last 50 transactions on-screen or, as an option, you can clear all transactions from the screen by selecting the Clear button.
4. All transactions are permanently recorded in the database and can be retrieved and viewed in the Transaction Response screen.
5. As an option, you can reduce the height and width of the Online Transaction screen by placing the cursor on one of the corners of the screen and re-size it so it is less intrusive on the monitor but still visible for monitoring alarms.
6. If an alarm occurs, review the procedures outlined in Respond to an Alarm - Transaction Response Screen below.

Respond to an Alarm - Transaction Response Screen

The instructions conveyed below are intended as a general set of procedures on merely operating the software in the event of an alarm transaction. Be sure to observe and comply with any and all corporate or organizational security protocols.

1. From the Client main screen, select the Status button > Transaction Response.
2. If you have multiple sites, click on the ▼ symbol at the right of Sites, and click on the site in the drop down box.
3. From the Transaction Response screen, ensure that the radio button to the left of New and Pending is selected. The button has a blue dot when selected.
4. Leave the Device Type and Transaction type set on All.
5. Opposite Transaction Category, ensure Alarm is listed; if it is not listed, click on the ▼ symbol at the far right of the box and select Alarm from the list.
6. Click on the Search button.
7. Locate the alarm in the list of transactions.
8. Double click on the on the row of the alarm.
9. From the Response Instructions screen, review the information in the Instructions and Location boxes and if indicated the person or persons to contact.
10. Do one of the following steps:
    - If the alarm requires investigation, select the ▼ symbol opposite Transaction Status and select On Hold from the drop down list, click on Save and then investigate the alarm.
    - If the alarm does not require investigation, select the ▼ symbol opposite Transaction Status and select Completed. Go to the next step.
11. In the Response Comments text box, enter any commentary or action taken if required.
    - If you have Emergency Contacts that were called about the alarm, rather than entering the entire name in the Response Comments box, as an option you could enter Contacted # as a shortcut.
12. Click on the Save button.
13. Click on the x in the upper right corner of the Response Instructions screen to close it.

14. From the Transaction Response screen, if there are Alarm Cleared transactions, select the Set Completed button near the bottom of the screen.
15. Click on the Back button until returned at the main screen or select the history navigation  symbol for a previously viewed screen.

Print an Alarm Transaction Response

1. From the Client main screen, select the Status button > Transaction Response.
    - If you have multiple sites, double click on the site from the Site Search - Transaction Response directory screen.
2. From the Transaction Response screen, do one of the following steps:
    - For a new alarm, select the radio button to the left of New and Pending
    - For a previously completed alarm, select the radio button to the left of Date Range and specify the dates in the To and From fields
3. Click on the Search button.
4. Locate the alarm in the list of transactions.
5. Click on the row of the alarm.
6. From the Response Instructions screen, review the information in the Instructions and Location boxes and if indicated the person or persons to contact.
7. Enter any applicable commentary in the Response Comments. Click on the Save button if you add comments.
8. Click on the Print button.
9. From the Report Viewer screen, click on the printer icon, configure the Print dialog box and select the Print button.
10. From the report screen, click on the x in the upper right corner.
11. From the Response Instructions screen, click on the x in the upper right.
12. If prompted with the Confirm Exit prompt, click on the Yes button.
13. From the Transaction Response screen click on the Back button until returned at the main screen or select the history navigation  symbol for a previously viewed screen.

Related Topics

System Health

Active Map Template Editor

Online Transaction Screen

Transaction Response Screen

Event Setup

Find and Review Past Alarms

The Transaction Response screen is used to view new/pending alarms or search for alarms by a date range. The Transaction Response screen identifies alarms by the following criteria:

- Site - identifies the site location of the alarm
- Access Control Unit - identifies the access control unit that registered the alarm
- Device - identifies the device such as a door
- Person - n/a
- Credential - n/a
- Transaction - identifies the type of the alarm at the source
- Date - lists the Month/Day/Year/Time of the alarm
- Status - New, On Hold, or Completed

From the Transactions Response screen, you can also change the status of all new alarms to complete with the Update All function.

Search Parameters

The Transaction Response screen has the following parameters to narrow or filter the list for a refined search and switches to effect changes:

- New and Pending - lists alarms with a status of new or on hold
- Date Range - specifies to and from dates when searching for alarms
- Device Type - selects a single type of device such as doors or inputs
- Transaction Type - selects a single transaction type such as alarm tripped
- Device Name - specifies the device by its assigned name
- Access Control Unit - specifies a single access control unit
- Search - initiates the search based on the criteria specified above

Procedures

Steps to Search for Past Alarms

1. From the Client main screen, select the Status button > Transaction Response.
    - If you have multiple sites, double click on the site from the Site Search - Transaction Response directory screen.
2. From the Transaction Response screen, ensure that the radio button to the left of Date range is selected. The button has a blue dot when selected.
3. Click on the Date & Time Selection icon to the right of the From box.
4. From the calendar, if the from date is other than the current month displayed, use the arrows to scroll to the desired month/year.
5. Select the day in the calendar.

6. Select the hour in the box on the right of the calendar.
7. Click on the Close button.
    - To change the minutes from the top of the hour 00, select the minutes in the From box and then type the desired minutes.
8. Click on the Date & Time Selection icon to the right of the To box.
9. From the calendar, if the to date is other than the current month displayed, use the arrows to scroll to the desired month/year.
10. Select the day in the calendar.
11. Select the hour in the box on the right of the calendar.
12. Click on the Close button.
    - To change the minutes from the top of the hour 00, select the minutes in the To box and then type the desired minutes.
13. To set specific search criteria, use the Device Type, Transaction Type, Device Name, and Panel fields as desired.
14. Click on the Search button.
15. To view any commentary on a specific alarm, double click on the row of the alarm. Click on the x in the upper right of the Response Instructions screen when you have reviewed the alarm comments.
16. When you have completed searching for alarms, click on the Back button until you are returned to the main screen or select the history navigation  symbol for a previously viewed screen.

Steps to Change the Status of All Alarms from New to Completed

1. From the Client main screen, select the Status button > Transaction Response.
    - If you have multiple sites, double click on the site from the Site Search - Transaction Response directory screen.
2. From the Transaction Response screen, ensure that the radio button to the left of New and Pending is selected. The button has a blue dot when selected.
3. Click on the Update All button and from the drop list select Completed.
4. Click on the Back button until you are returned to the main screen or select the history navigation  symbol for a previously viewed screen.

Related Topics

Alarm Types

Transaction Response Screen

Email Alarm Notification

For setting up email alarm notification, click on the link below.

Event Setup - Actions - Email Action

Alarm Types

The following list identifies the various types of alarms and the cause of the alarm in the Aurora software.

Alarm	Device/Cause of Alarm
ACU Master Comms Failure	Slave CIM/ECM CANBUS 2 communication failure with master CIM/ECM
ACU Master Comms Restore	Slave CIM/ECM CANBUS 2 communication has been restored with master CIM/ECM
Alarm Cleared	Door - a door that was previously forced open has now been closed Auxiliary Input - a monitored auxiliary input point that was previously in an alarm condition has been cleared
Alarm Duress	A person has keyed in *9 preceding their PIN code to indicate some type of problem or emergency
Alarm Tripped	Door - a monitored door was accessed without a valid card presentation (forced open) Auxiliary Input - a monitored auxiliary input point was tripped
Comms Failure	A control unit has lost communication with the access control software
Comms Restored	An access control unit, previously marked as Unit Inactive, has had communications restored and is now active
Door Closed	A door previously in violation of the Door Held Open Time setting has now been closed
Door Held Open	A door was accessed with a valid card but was not closed within the designated Door Held Open Time setting
CIM/ECM/GCM Trouble	A CANBUS communication error
CIM/ECM/GCM Message Trouble	Communication on CANBUS interrupted because of heavy network traffic
Invalid Card/Keypad Code	An invalid card or PIN code has been presented at a reader or keypad more than 5 times
IO Comm Card Failure	IO to ACU communication failure
IO Comm Card Restore	IO to ACU communication has been restored
Reader Communication Failure	System has failed to receive reader communication
Reader Tamper Alarm	Reader tamper switch has been compromised
Reader Restored	Reader has been restored
Power Fail Detect	An access control unit has lost power
Trouble Open	Indicates that a wire has been cut or is broken
Trouble Short	Indicates the wire has a short circuit
Unit Marked Inactive	ACU Model Type - an access control unit that lost communication has now been marked inactive by the access control system

ACU Cover Failed	The control board cover (PC1094 or higher) has been removed or is not completely secured with the mounting screws
ACU Cover OK	The control board cover (PC1094 or higher) has been secured
ACU Tamper Alarm Tripped	The ACU metal enclosure door has been removed or is partially ajar
ACU Tamper Alarm Cleared	The ACU metal enclosure door has been closed and is secure
RTC/SRAM Battery Failed	The on-board 3V lithium battery on the control board is in a weak or exhausted condition indicating it needs replacing. (RTC is the real-time clock and SRAM is the system memory)
RTC/RAM Battery OK	The on-board 3V lithium battery on the control board is OK and has sufficient power
Early Power Failure Alarm Tripped	The voltage to the control board has fallen below approximately 10.5 volts and indicates a power supply problem
Early Power Failure Alarm Cleared	The voltage to the control board is above approximately 10.5 volts and indicates the power supply has been restored

System Health

The Client displays a system health icon in the upper left corner of the Aurora screens. The icon's colour indicates the current state of the access control system as outlined below.

Icon	Heath Condition
	**System Good** A blue health icon indicates the system is good.
	**New or On Hold [Alarm] Transactions** This indicates the number of new or on-hold alarm type transactions detected by the system at sites assigned to the system user. The health icon remains red and the audible alarm continues to sound until the alarm is completed in the Transaction Response screen. Click on the New or On Hold Transaction red text to open the Alarm Response screen for specific alarm instructions and/or to complete the alarms. Click on the red health icon to view the system condition.
	**Database Size** This indicates the system database has reached 9.5 GB*. The communication service has suspended data collection from the access control units. The health icon remains red until the database is purged and reduced to less than 9.5 GB. Click on the Database Size (9.5 GB) red text to open the Database Maintenance screen. First, backup the database; second, purge the database of older transactions and system logs; and last, compress and re-index the database. You should attempt to reduce the database to less than 7.5 GB otherwise you will get a yellow health icon with a database advisory. Keyscan also recommends scheduling automatic database backups, if you have not done so previously. The Keyscan SQL Server 2022 Express database has a 10GB limit. Click on the red health icon to view the system condition.
	**No Scheduled Database Backup** This indicates Aurora has not been scheduled to perform a regularly scheduled database backup. The health icon remains red until a scheduled backup is programmed in the Database Maintenance > Scheduled Backup screen. Clicking on the No scheduled database backup detected message, opens the Database Maintenance screen. To set a backup schedule, recommended, select the Schedule Backup tab, select the Add button and set a database backup schedule. See Related Topics for more information. Click on the red health icon to view the system condition.
	**Inactive Panel(s)** Indicates the number of control units that have experienced a Comms Failure and the Aurora software has marked the units as inactive. Causes may be a power failure at the control board or network/serial connection issues. Click on the # Inactive Access Control Units to open the Site Search/Hardware Setup screens to determine which control units are inactive and require attention. Check network and or serial connections and ensure any reported inactive access control units have power. When the control units are back online with the communication service, the Aurora software automatically creates a Comms Restored alarm transaction and resets the status to Active. Please note that the Comms

Restored transaction should be completed in the Transaction Response screen to restore the system health icon to blue.

Click on the yellow health icon to open the system condition.

Note: If control units have been manually set on Inactive status in the Hardware Setup screen for diagnostics or troubleshooting, the health icon changes to yellow and indicates Inactive Access Control Units.



Communication Service Advisory

The communication service has detected a network IP connection or serial connection with more than 15 access control units on a single communication bus.

Click on the yellow health icon to open the system condition.

Click on the Communication Service Advisory yellow text to open the Site Setup Report screen.

Run a Site Setup Report. Ensure all report options are de-selected except Access Control Units which should have an x in the box to the left. Review the report to see which network connection (same IP addresses) or serial connection (same server name) have more than 15 control units on the same communication bus.

Keyscan recommends that each network IP connection or serial connection not exceed 15 access control units for best system communication efficiencies. If you are experiencing sluggish system performance, you may wish to contact your dealer/installer to re-configure the system architecture by adding more network IP connections or serial connections and balancing the number of access control units so as not to exceed 15 units on each communication bus.

Please note that this is only an advisory and the 15 unit maximum is a general guideline to follow. It is not an indication that the access control system is malfunctioning nor are you required to contact your dealer/ installer.



Database Size

This indicates the system database is now between 7.5 GB and 9.5 GB*. Keyscan recommends reducing the database size.

Click on the yellow health icon to open the system condition.

Click on the Database Size (x GB) yellow text to open the Database Maintenance screen. First, backup the database; second, purge the database of older transactions and system logs; and last, compress and re-index the database. You should attempt to reduce the database to less than 7.5 GB otherwise you will get another yellow health icon with a database advisory. Keyscan also recommends scheduling automatic database backups, if you have not previously done so.



Database Backup is Older Than 7 Days

This indicates that the database has not been backed up in over 7 days. Keyscan recommends that you make an immediate backup copy and then schedule regular backups at least once per week.

Click on the yellow health icon to open the system condition.

Click on the Database backup is older than 7 days text to open the Database Maintenance screen and perform a DB backup.



Software Is Unregistered (# days left)

This indicates the Aurora software has not been registered. After installation of the software Aurora has a thirty day trial period after which it ceases to function unless registered.

Click on the red health icon to open the system condition.

Click on the Software is unregistered text (below the globe icon) to open the Software Registration screen.

---

* Only applies with the Keyscan SQL Server 2022 Express database which has a 10GB limit. If you have a Keyscan Aurora SQL Upgrade license, the Database Size advisories do not apply.

Related Topics

Transaction Response

Database Maintenance

- Site Setup Report
- Software Registration

About People Records

Each person with authorized access to various entry points within your building or facility must be identified in the Client software with a record that includes personal, credential, and site information. Each person must have a unique form of identity - the credential - so he or she is distinguished from all other individuals. When each individual presents his or her credential at a reader, the access control system grants or denies entry based on who the individual is and the programmed access settings. Each time a credential is presented at a reader, the transaction is recorded in the database. By maintaining a database of accurate records, you can keep track of all site activity and know the whereabouts of each individual. And in cases where someone either, leaves, is dismissed, or reports a credential lost or stolen, the record or the credential can be quickly de-activated or deleted nullifying any potential security risk.

Manage People Screens		
Manage People Directory		
		Summary
		lists all persons currently enrolled in the Client software
		waste bin on right deletes person's record
Edit Person		
	Personal Information	**Fields**
		- photo - given name, middle name, surname - type (employee, visitor or user defined) - security level (if enabled) - person active / inactive - extended entry (accessibility)
	Credential Information Tab	- credential type selection & credential information - site & group assignments - temporary options: number of uses or date range - print function for ID badges
	Optional Fields Tab	- common fields - site fields
	General Info Tab	- specific notes or information pertaining to individual

	Site Enrollment Tab	- enable or disable records at specific sites
	Transactions Tab	- lists most recent credential transactions
	Visits Tab	- schedules visits

About the Edit Person Screen

The Edit Person screen is laid out with selectable tabbed sub-screens which furnish you with a wide assortment of data fields for your credential records.

- Personal Information
- Credential Information
- Optional Fields - Common/Site
- General Information
- Site Enrollment
- Transactions
- Visits

This help page presents an overview of the Add Person/Manage People screen. For a full list of topics and procedures on credential records select the Contents pane on the left and open the Manage People & Credential Records.

Personal Information

The personal information fields include given name, middle name and surname as well as the following fields.

Custom Person Unique Identifier

The Aurora software client can be configured to use Custom Person Unique Identifiers to help integrators identify people in Aurora that match people in other systems. To help users understand what a Custom Person Unique Identifier represents, users can provide a custom label for the unique identifier (for example: Student ID). Also, users have an option to indicate whether or not the Custom Person Unique Identifier field is required. Custom Person Unique Identifiers become searchable criteria once configured in the software.

To set up a Custom Person Unique Identifier, first go to Application Utilities under the Application Management menu. Select the Advanced tab and check the box beside Custom Person Unique Identifier. Fill in the Custom Person Identifier Label field and check the box beside Is Required and/or Display In Name (as your needs require). Select the Save button on the bottom-right corner of the screen.

Upon returning to the Edit Person screen, the Custom Person Unique Identifier will now appear above the Person Type. If Is Required was selected, the Custom Person Unique Identifier becomes a mandatory field and cannot be saved unless filled out.

Type

Type is in reference to how the person is categorized. As Aurora includes a visitor management component, the Client has two default types:

- Employee
- Visitor

By categorizing each person by type, you can distinguish individuals for group assignments and group access levels. Assigning individuals as a type allows you to delineate groups of people by category.

Type is also a user-defined field. You can create your own named type categories in the Application Utilities screen. Create types or classes, such as manager, member, guest etc., that assist in identifying individuals and potentially determining access restrictions, permissions, or group assignments.



The Employee and Visitor types cannot be altered or deleted.

Scan DL/Scan BC

The Scan DL and Scan BC buttons are used in conjunction with BIZSCAN or BIZSCAN2 card scanners and require Keyscan's Card Scanning license. The Scan DL and Scan BC functions transpose the names from a business card or an ID card, such as a driver's license, and populate the name fields in the Edit Person screen for enrolling visitors in the Aurora software. For more information, see Optional Card Scanner under Visitor Management.

Person Active/Person Inactive

The active/inactive button enables/disables both the individual’s record and all assigned credentials.

- Active - the individual’s record is active and the assigned credential is valid at all authorized entry points
- Inactive - the individual’s record is de-activated and the assigned credential is disabled from use until the status is changed back to active

As opposed to deleting a record, the Inactive option can be used in cases where an individual may be taking a leave of absence or is off because of an illness but is expected to return later. In cases like this, you can merely set the record on inactive retaining the record in the database, and, upon his or her return, re-activate the individual’s record. While the record is inactive, the person's credential cannot be used. As opposed to deleting the record, setting the person as inactive saves having to re-create the record at a later date.

Clicking on the button alters the state from Active to Inactive or from Inactive to Active.

Extended Entry

The Extended Entry function is for those persons who require a longer period of time when accessing a door. When an individual’s credential is presented with the Extended Entry setting enabled, the reader acknowledges the credential’s Extended Entry status and the access control system invokes the Extended Entry Timer and the Extended Entry Door Held Open settings. These two settings are set in the Hardware Setup screens. Generally the Extended Entry function is used in conjunction with access-control-connected doors that have electro-mechanical door operators.

Refresh

Selecting the Refresh button updates the screen to reflect the current information about the person. The refresh applies more so with multiple Clients to update the screen from the database where changes may have occurred to the record at other stations. The last refresh date and time is displayed below Extended Entry.

Photo Capture

Aurora includes a photo capture option. You can attach an individual’s photo image with his or her record and also include it on a photobadge for additional security measures. There are 2 methods to attach a photo image on the record and on the photobadge:

- use an existing file image
- use a video camera to capture a live image

Credential Information

Keyscan systems are compatible with the following types of credential formats. When adding a person's record, you must know and select the type of format you use. On the left of the Credential Information heading is a button labelled Add Keyscan. When this button is selected it presents a list of supported credential formats. Credentials below are referred to as cards; however, credentials come in various styles including cards, tags, fobs, transmitters etc. What distinguishes each credential format is the type of internal coding/numbering system they use. Each credential format is outlined below.

See "Supported Card Formats" charts on the Reader Formats page for more information on what card/reader types are supported by your panel type.

Keyscan

The Keyscan format uses the 3-digit batch code/5-digit card number format. This is the most common card format used and generally the card number is printed directly on the card. In some cases the batch code* is also printed on the card. If you use Keyscan cards the format would be as follows - xxx - xxxxx - the first 3 digits are the batch code, also referred to as facility code or site code, and the last 5 digits are the card number. If you use cards other than Keyscan cards, refer to the card package or the person who purchased the cards to determine the batch code.

*The batch code may also be referred to as the site code or the facility code.

Corporate 1000

The HID Corporate 1000 card format is controlled by the end-user under its agreement with HID. As such, you may have to contact your card program administrator for more information on card enrollment as there are many variations to the card format. Please note this format is not controlled by Keyscan.

Large Card Decimal/Large Card Hex

The large card format is a general category that includes a number of different formats such as University 1000, FIPS/TWIC, Mifare CSN 32 & 40 and other 3rd party OEM proprietary card formats. You may have to refer to the person who purchased the cards or your dealer if you are not sure which cards you use.

Standard 26-bit

This is a common card format that uses a 5 digit card number. It may or may not use a 3 digit batch code depending on the manufacturer of the card. You may have to consult with your card supplier and/or your dealer and verify if the batch code applies. The batch code may also be referred to as the site code or the facility code.

HID H10304

The HID H10304 is a unique credential format ordering number. This order format can apply to various HID credential products. You may have to consult with the person who purchased the cards or contact your card supplier and/or your dealer if you are not sure whether this format applies.

HID H10302

The HID H10302 is a unique credential format ordering number. This order format only applies to E-Plex wireless locks.

OEM 20 Bit / OEM 24 Bit

These are two 3rd party proprietary card formats that use a batch number and card number. When using these card formats set the Reader Format to H - 26 to 48 Pass-through Large Card Format (first and last parity bits dropped). Reader Formats are specified in the Hardware Setup > Additional Settings screen.

17-byte

This credential type is to be used only with Saflok (Kaba) Integrated Mode.

BEST

To view steps on how to add BEST Credentials to a Person, read the following section:

BEST Offline Lock Integration Setup

Keyscan Smart Mobile

The Keyscan Smart Mobile credential has the same format as the Keyscan Credential, but are designed to be used with the Keyscan Mobile App. Keyscan Mobile credentials allow user to access protected areas using the Keyscan Mobile app and their preferred mobile device by simply presenting their device to the reader or smart lock for authentication. Keyscan Mobile credentials are compatible with Keyscan K-SMART3 readers as well as e-Plex E7900 wireless locks (with the BLE option) and are used as part of a Keyscan Aurora or Keyscan LUNA system. Each Keyscan mobile credential is unique and can only be used once with one mobile device. Since there is no physical card, the Batch and Card Numbers will be provided to the user electronically.

Site Assignment

The Site Assignment screen determines which sites an individual's credential is valid at and his or her group access level assignment and, if applicable, any temporary credential options. In order for the credential to be active for a particular site, even if you have only one site, the site must be selected as indicated by an x in the box to the left of the site name.

Group Access

Each individual must be assigned to a minimum of 1 group. Only groups are assigned access levels at doors, wireless locks or elevators. You can assign the individual the maximum number of groups per site depending on the Aurora software license.

- Standard - maximum of 10 groups per person
- Elite Edition - maximum of 40 groups per person

Groups are created in the Group Setup screen.

View Group Access Levels

You can view the access levels at all doors for a particular group by positioning the cursor over the desired group listed under the Group Access heading in the Edit Person screen. Right click when the cursor is positioned over the desired group.

Temporary Options

In cases where a credential is issued on a short term basis to visitors, temporary staff, or members etc., you can make the credential temporary.

Temporary credentials can be limited by the following parameters:

- date range
- number of uses
- both date range and number of uses, whichever occurs first
- limited to group - applies to Elite Edition licenses only (intended for persons assigned to multiple groups - temporary options only apply to the credential when used for that group's access - all other group assignments are unaffected by the temporary options)

When a date range is assigned, the credential expires 1 minute before midnight on the last valid day.

Clone Function

When assigning an additional credential or replacing a lost or stolen credential, the clone function retains the present group assignments when the new credential is added.

Lockdown Access

This feature gives a credential access to a door during a Lockdown. Under the Site Assignment sub-menu, select the Lockdown Access button:



The credential can access the door during a Lockdown based on their assignments and schedules



The credential cannot access the door during a Lockdown

Note: In order to have lockdown access, Enhanced Lockdown must be registered and firmware version 9.47 or higher installed.

Optional Fields - Common / Site

Common Optional fields and Site fields are used on the Edit Person screen to provide personal details about each individual who is issued a credential for entry to various doors or elevators controlled by the access control system.

Common Fields

The Common fields are user-defined.

The captions in the Common Optional fields apply universally to all personal records at all sites. For steps on creating or editing Common Optional fields, see the procedures below.

Site Fields

The Site fields are user-defined and apply only to the credential records of the current site. You can create any number of Site fields. Site fields may be in text, number, or date formats.

Site Enrollment

When the access control system has multiple sites, you can view at-a-glance the individual's site assignments by selecting the Site Enrollment tab. The Site Enrollment screen also works in conjunction with the site assignments on the Credential Information screen, whereby, you can selectively decide which sites the record is active and which sites the credential is active.

- Site enrollment - the record is active at the site
- Credential Information/Site Assignment - the credential is active at the site

If the site is disabled in the Site Enrollment screen, the credential is automatically disabled in the Credential Information screen.

Sync Function

The sync function updates credential record information at all the control units for the selected site. This is beneficial if you have made changes to the credential record and need them implemented immediately. Otherwise the update may take a few moments before the next automatic communication cycle occurs. To update the panels with the sync function, click on the icon below the Sync heading opposite the desired site.

Transactions

When the Transactions tab is selected, the transactions are listed in the table indicating the device where the credential was presented along with other details including the date and time of the transaction.

- The list of transactions can be updated by pressing the "Refresh" button.
- The "Receive Live Transactions" checkbox can be used to refresh the transactions list automatically every 10 seconds.
- The "Include Credential Not Found Transactions" checkbox will include transactions for credentials that are not enrolled along with the Person's card transaction information. If the user is permitted to create credentials, these records have include a "+" button control that will enroll the credential into the system for the person being viewed.

Note: If the "Receive Live Transactions" feature remains active, any "Credential Not Found" transactions displayed on the screen will be cleared within 10 seconds. When using "Receive Live Transactions", it is recommended that you switch this feature off once the "Credential Not Found" transactions appear.

Visits

The Visits screen is used to schedule visits listing the date of the scheduled visit, the visit status, the name of the visitor and the name of the person visited.

Create a Person's Record

Each person that is assigned a credential for building access is referred to as a credential holder. Creating a record for each person requires completing the Edit Person screen. Each saved record is added in the database. Combined with schedule information and access levels at each door or elevator floor, the access control units regulate when and where the person's assigned credentials are permitted entry.

The Edit Person screen has several optional settings that must be activated or defined elsewhere in the Aurora software as outlined:

- Person’s Middle Name - activated from the Application Utilities screen
- Auto Create a PIN code - activated from the Application Utilities screen
- Common Fields - defined from the Optional Fields Management screen (Site fields are assigned from the Assign Site Optional Fields screen.)

See Related Topics for more information on how to enable these features.

Active Directory License

If operating Aurora with an Active Directory license, the Edit Person screen has the following two fields

- Active Directory Linked
- Active Directory User

For more information, see Active Directory below Related Topics near the bottom of the screen. The above two fields are only visible with an Active Directory license.

Site Enrollment vs. Credential Site Assignment

The Edit Person screen has a site enrollment feature and a site assignment feature. Although they sound similar in name, they each have a distinct purpose.

- Site Enrollment - activates the individual’s record for the selected site
- Credential Site Assignment - activates the credential for the selected site

In certain cases you may only want the record active such as for visitors or where individuals go to other sites but you do not necessarily want his or her credential active for access at all sites. In this case, you would select the sites in the Site Enrollment screen and de-select the site in the Credential Information/Site Assignment screen.

If the site is disabled in the Site Enrollment screen, the credential is automatically disabled in the Credential Information screen.

The Edit Person screen has multiple options that you may or may not require for your records. Also, some functions may not be available, depending on which optional software or hardware you have purchased.



If you are using E-Plex wireless locks that use keypad only (no physical credential) entry, then you must first create a dummy credential in order to create others.

Procedures

Create a Credential Record

1. From the Client main screen, select the Manage People button > Add Person.
2. From the Edit Person screen, click inside the Given Name text box and enter the person’s first name.
3. Click inside the Middle Name field and enter the person’s middle name or initial.
    - The Middle Name field is an optional setting which is enabled from the Applications Utilities screen.
4. Click inside the Surname field, and enter the person’s last name.
5. As an option, you can enter the person's e-mail address. If an e-mail address is specified in this text box it is used in conjunction with the Visitor functions for issuing an e-mail announcing the Arrived, Delayed or Cancelled visit status.
6. By default the Type field is pre-selected as Employee. If this person type applies to the record, go to the next step. To change the Type to another classification, click on the ▼ symbol and select the person type from the drop down list. Employee and Visitor are Aurora default types. You can create other user-defined types in the Application Utilities screen.
7. If the person requires an extended period of time accessing doors, and if you have doors equipped with door operators that are connected to the access control system, click in the box to the left of Extended Entry. The box has an x when the function is enabled. If your system is not connected to door operators for extended accessibility, bypass this step.
8. If you are adding a photo of the person to the record, position the cursor over the silhouette in the upper left corner of the Edit Person screen.
9. Click on the + symbol.
    - On the right of the + symbol is pencil icon. The pencil icon opens the photo editor and allows editing the person's current photo with any of the Image Editor's available tools
10. From the Open file dialog box, navigate to the folder location with the image. Select the image file and then click on the Open button.
11. In the Image Editor screen, click on the Save icon near the bottom.
    - For more about using the tools and functions of the Image Editor, see Related Topics below.
12. Ensure the Credential Information tab is selected.
13. Click on the ▼ symbol to the right of the Add Keyscan Credential button and from the drop down list select the type of card format that is being assigned.
    - If you have previously selected another format during your current login session, the Add button will list the last format chosen.
14. Depending on the format selected, enter the batch number, if applicable, and the card number.
    - The batch code may also be referred to as the site code or the facility code.
15. If you have engaged the Auto Generate PIN option in the Application Utilities screen, a PIN is automatically inserted in the PIN box. If you have not engaged this option and the person requires a PIN code, you can manually enter a code in the PIN box. Generally PIN codes are only required for access at keypads.
16. As an option, you can use the Name field to assign a credential name to the card format if it is other than the Keyscan format. Click inside the Name text box and enter a credential name.
17. In the Site Assignment pane, sites are listed on the left. Click in the box to the left of the site the person's credential is authorized for access. The box has an x when the site is selected.
18. Select the v symbol opposite the site you enabled in the previous step to open the Group Access pane.
19. Select the group or groups the person is assigned to by clicking in the box or boxes to the left. A box has an x when selected. Click and drag the scroll bar on the right to access groups not viewable in the pane.

- You can view a group's access levels, by right clicking when the cursor is positioned over the desired group.

20. If you have multiple sites repeat the preceding 3 steps if the person's credential is authorized for access.
21. If you have created and use either common optional fields or site-specific optional fields, select the Optional Fields tab.
22. For Common fields, enter the person's data in the respective text boxes. Common fields apply to all sites.
23. For Site fields, select the v symbol opposite the site and enter the person's data in the respective text boxes.
24. If required, select the General Info tab to enter any miscellaneous notes or comments about the person.
25. If you have multiple sites and you want the record enrolled at any of those sites but without the credential being valid for access at those sites, select the Site Enrollment tab and select the appropriate sites in the list.
26. Select the Save button to complete the process.

Copy Credential Site Settings

1. If creating a new Person Credential Record, select Add People under Manage People; go through the steps as usual. If using an existing credential, select the Manage People sub menu.
2. Configure the desired settings for the Credential within a Site that the Credential will have access to by assigning it to a Site, selecting the Groups it will belong to for group access, and applying any temporary credential settings.
3. Right-click on the Site that has the desired configuration.
4. Select the Copy Configuration to Other Sites button that appears under the Site Assignment sub menu. A pop-up window will appear with Credential Site Settings to be copied on the left, and available Sites to be copied into on the right.
5. Select the applicable Sites by placing an **x** beside each one. Alternatively, input the site name into the Site Search filter above. Selected Sites will remain in the list regardless of the filter.
6. Under Paste Behavior, use the drop-down menus to decide how Groups, Temporary Options and BEST Lock Features will affect the selected Sites.

   The following general rules apply when copying **Groups** (regardless of paste behaviour):

- Group names must match in both sites, ignoring case sensitivity
- The first Group with a matching name will be used if there are more than one group with the same name existing in the target site
- If the Aurora User is a Visitor Only type, only Visitor type groups will be copied

If **Merge** is selected for **Groups**, the following applies:

- Any Groups already added for the Credential in the Site(s) selected will remain
- Any additional Groups copied will be added for the Credential in the chosen Site(s)
- If a Credential is assigned to more Groups than is permitted, the copying process will fail. Make the appropriate Group changes and try to process again

If **Overwrite** is selected for **Groups**, any Groups already added for the Credential for Site(s) selected will be removed and the ones being copied will be added to the credential instead.

If **Do Nothing** is selected for **Groups**, no Groups will be assigned to the selected sites, to one exception: If Temporary Options are copied and the group applied to the Limited To Group is not assigned to the credential for the site, the credential will then be assigned the group for the site. A window will pop up and give the user a chance to cancel out of the selection.

If **Merge** is selected for **Temporary Options**, the following applies:

- The Valid-From and Valid-To values will be applied to the credential in the selected Site(s) only if there are no values currently set for these fields in the new Site(s)
- The Limited # Uses value will be applied to the credential in the selected Site(s) only if there is no value currently set for the this field in the new Site(s)

If **Overwrite** is selected for **Temporary Options**, all of the settings currently applied for the Temporary Options in the selected Site(s) will be overwritten with the values copied.

If **Do Nothing** is selected for **Temporary Options**, none of the temporary settings will be applied for the Temporary Options in the selected Site(s).

If selecting a Paste Behaviour for BEST Features, please observe the following:

- This feature does not support the **Merge** option
- If **Overwrite** is selected, all settings currently applied to the target site will be overwritten and the values copied
- If **Do Nothing** is selected, none of the settings will be applied to the selected site(s)

7. After all potential Sites are chosen, select OK. The settings are applied to the Credential for each Site selected.
8. Select Save to complete the process.

Related Topics

About the Edit Person Screen

Make a Temporary Credential

Activate the Middle Name Field

Activate the Auto Generate PIN Option

Optional Fields - Common & Site

Add a Visitor Record

Active Directory

Image Editor

Attach a Photo to the Record

There are 2 methods to insert an image on the Edit Person screen:

- from an existing image of the cardholder such as a JPG
- from a live video camera and capture an image of the cardholder (Keyscan USB-CAM)

Keyscan USB Camera (product # USB-CAM)

If you are using Keyscan's USB camera (p/n USB-CAM), ensure that you have installed the drivers that accompanied the device. When you select the + symbol over the image silhouette on the Edit Person screen, the Aurora software will detect the USB camera.

Pencil Icon

You may also edit a person's current on-file image by selecting the pencil icon in the upper left corner of the image silhouette on the Edit person screen.

Deleting an Image

If at a later date you need to delete a person's image, select the waste bin icon on the right side of the image. The icon opens when the cursor is positioned in the upper right area of the person's image. You must select the Save button before exiting the record.

Procedures

Steps to Attach an Image File

These instructions are based on adding an image to an existing record. For adding an image to a new record, see Create a Person's Record.

1. From the Client main screen, select the Manage People button > Manage People.
2. Locate the credential record in the Person Search directory screen.
3. Double click on the credential record in the list.
4. From the Edit Person screen, position the cursor over the silhouette in the upper left corner of the screen.
5. Click on the + symbol.
    - On the right of the + symbol is pencil icon. The pencil icon opens the photo editor and allows editing the person's current photo with any of the Image Editor's available tools
6. From the Open file dialog box, navigate to the folder location with the image. Select the image file and then click on the Open button.
7. In the Image Editor screen, click on the Save icon near the bottom.
    - For more about using the tools and functions of the Image Editor, see Related Topics below.
8. From the Edit Person screen, click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Capture a Live Video Image - Keyscan USB Camera

These instructions are based on inserting a video image on an existing record.

1. From the Client main screen, select the Manage People button > Manage People.
2. Locate the credential record in the Person Search directory screen.
3. Double click on the credential record in the list.

4. From the Edit Person screen, position the cursor over the upper left corner of the silhouette on the Add Person screen.
5. Click on the + symbol.
6. From the Image Editor screen, click on the Start button.
7. Position the person in front of the camera at the desired distance.
8. When the person is suitably posed for the image, click on the Snapshot button.
9. Click on the Save button.
10. From the Edit Person screen, click on the Save button.
    - If the image captured was not satisfactory, position the cursor near the upper right of the silhouette and select the delete button. Repeat the preceding 5 steps.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Image Editor

Reduce Photos

IMAGE EDITOR

The Aurora Image Editor opens automatically when a photo image is imported into the following screens:

- Edit Person
- Manage System User
- Site Information Setup

You may also select the pencil icon, which displays when you position the cursor in the upper left corner over the image silhouette on the Edit Person screen, to edit the person's current on-file image.

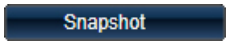
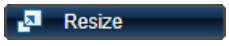
The Image Editor has a suite of tools to perform various photo editing tasks before inserting the image. The tools are outlined in the table below. If you are unfamiliar with basic photo editing software, see the Photo Edit Tutorial below.



When you are inserting an image and no changes are required to the image, just select the Save button on the Image Editor screen.

If you elect to use the Image Editor for amending or enhancing images, Keyscan suggests that you experiment with all the tools so you have a better understanding of how they work and how they affect the image.

Overview of Image Editor Tools

Menu	Tool	Function	How to Use It
Camera			
		Opens the USB camera in Aurora	Click on the Start button to open the USB camera in the Image Editor screen
		Closes the USB camera in Aurora	Click on the Stop button to close or exit from the USB camera
		Acts as the shutter release on the USB camera and inserts the captured image on the Image Editor screen	Click on the Snapshot button to capture the desired still image of the individual which can be edited using any of the tools below
Transform			
		Allows reducing the image size which decreases the file size with the result of conserving space in the Aurora database – See the note on re-sizing images below	Click on the Resize button. Click on the Image Size -pixels - (-) or (+) or the Relative Size - % - (-) or (+) to decrease or increase the image size. The file size is displayed in the right. You should only decrease (-) an image otherwise the image will be distorted. Preserve Aspect Ratio should be left selected (x).

The Start / Stop / Snapshot buttons are only active if Aurora detects the Keyscan USB-CAM camera. If Aurora does not detect the camera, the buttons are dimmed and unavailable.

		Click on Apply. Click on Close.
	Allows increasing the area around the image relative to a selected anchor point	Click on the Canvas Resize button. Select a square in the Image Alignment tool to set where the increased canvas size is applied relative to the image. Example - if the upper left square was selected for the Image Alignment, width would add canvas to the right side and height would add canvas to the bottom. Select a canvas Background color. Click on the Width (-) (+) or the Height (-) (+) adjustments. Click on Apply. Click on Close.
	Rotates the image 90 degrees clockwise	Click on the Rotate 90 button. The image is rotated 90 degrees in a clockwise direction.
	Rotates the image 180 degrees clockwise	Click on the Rotate 180 button. The image is rotated 180 degrees in a clockwise direction.
	Rotates the image 270 degrees counter-clock-wise	Click on the Rotate 270 button. The image is rotated 270 degrees in a counter-clockwise direction.
	Allows placing rounded edges at the corners of the image and adding a border around the image	Click on the Round Corners button. Round corners and borders can be applied together or separately. Round Corners - Click on the Radius arrows or drag the bar to round the edges on the image corners. Select a radius color. Border - Click on the Radius arrows or drag the bar to set the border thickness. Select a radius color. Click on Apply. Click on Close.
	Flips the image horizontally so the left and right sides of the image are reversed	Click the Flip Horizontal button to flip the image horizontally.
	Flips the image vertically so the top and bottom of the image are reversed	Click the Flip Vertical button to flip the image vertically.
	Allows trimming an area out of the image	Do one of the following to crop: Place the cursor over the white crop line and click and drag. Place the cursor over a corner crop square and click and drag. Place the cursor inside the pre-defined crop area and click and drag.

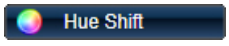
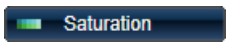
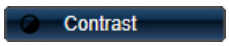
		Click on Apply. Click on Close.
	Allows placing text* on an area within the image * Ensure that the text does not extend beyond the edge of the image otherwise the image is distorted to accommodate the text within the photo frame.	Place the cursor in the text box, click and drag over Your text here … and delete the text. Type the desired text. Keep it within the boundaries of the image. Select a color from the palette. Click on the Font Size arrows or drag the bar to increase or decrease the size of the text. Click on the Horizontal Position arrows or drag the bar to position the text horizontally. Click on the Vertical Position arrows or drag the bar to position the text vertically. Click on the Rotation arrows or drag the bar to rotate the text on the image. Click on Apply. Click on Close.

Note on Re-sizing Images

Many digital cameras now offer upwards of 20 mega-pixel images. This gives images extremely large pixel dimensions with file sizes of 2 MB or more. If the images of individuals you are inserting in the credential records have been shot with a digital camera, especially a digital SLR camera, the images will be much larger than that required in the Manage People screen's photo frame. As these images are stored in the Aurora database, several hundred to several thousand images can occupy a large percentage of the database's overall memory capacity. If you are using images with large pixel dimensions with MB file sizes, try reducing the file size. You may have to experiment in determining how much an image can be reduced without distorting it when inserted in the Edit Person screen's photo frame. Also, bear in mind keeping it to a sufficient size so as not to degrade the image print quality in a photobadge. An image in the 250 Kb to 500 Kb range will probably be sufficient for both a printed photo badge and an on-screen image. The Resize tool continually displays the file size as you increase or decrease the height and width.

The Application Utilities screen has a Reduce Photos Over Size setting (default 0.5 MB) and a Reduce Photos To Size (default 0.25 MB). When you import an image over the 0.5 MB threshold you are prompted if you would like to reduce the photo size or retain the image file size. For more about the Reduce Photos options, see Related Topics below.

Adjust

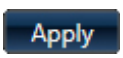
	Allows shifting the color of an image generally to correct or compensate for a color imbalance on the original image	Click on the Hue Shift button. Click on the Hue Shift arrows or drag the bar to scroll through the palette of color hues. Click on Apply. Click on Close.
	Allows changing the strength of the color from 0% (gray) to 100 % (full color saturation)	Click on the Saturation button. Click on the Saturation arrows or drag the bar to adjust the color saturation. Click on Apply. Click on Close.
	Allows changing the brightness and contrast of the image which adjust the luminance and the difference in color and light	Click on the Contrast button. Brightness - Click on the Brightness arrows or drag the bar to image brightness.

	Brightness: black (-1.00) to white (1.00) Contrast: gray (0 %) to saturation (100 %)	Contrast - Click on the Contrast arrows or drag the bar to adjust the image contrast. Click on Apply. Click on Close.
	Allows inverting the color on the image which gives it a the appearance of a film negative	Click on the Invert Colors button.

Effects

	Allows adjusting the sharpness of the image	Click on the Sharpen button. Click on the Sharpen arrows or drag the bar to increase or decrease the image sharpness. Click on Apply. Click on Close.
	Allows blurring the image which has the effect of softening the image focus	Click on the Blur button. Click on the Blur arrows or drag the bar to increase or decrease image blur. Click on Apply. Click on Close.

Common

	Save the image to the Add Person /Manage People screen (The image is saved with any alterations or changes in the Aurora database only. The original source file is not altered.)	Click on the Save button. The Image Editor closes. The image is placed in the photo frame holder on the Add Person / Manage People screen.
	Opens an image in the Image Editor (Use if you have opened the wrong photo image from the Add Person / Manage People screen. The original image is replaced in the Image Editor.)	Click on the Open Folder. Navigate to the folder with the desired image in the Open dialog box. Click on the Open button.
	Undoes the previous actions after the apply button has been selected	Click on the Undo button. Repeat clicking on the button to undo one previous action at a time.
	Redoes the previous actions after the undo button was selected	Click on the Redo button. Click on the button to redo one previous undo at a time.
	Applies the changes to the image and returns to the Image Editor	Click on the Apply button to effect any changes you have made using with the selected tool. When you make changes using a tool and you want to retain those changes to take effect on

		the image, click on the Apply button, then click on the Close button before you select another tool.
Close	Closes the tool and returns to the Image Editor main screen	Closes the tool and returns to the Image Editor main screen. If you have made changes with a tool but do not want the changes to take effect, click on the Close button. You are returned to the Image Editor main screen and the changes are discarded.
Reset	Resets the image and tool to the previous condition after an action was taken with the selected tool	Click on the Reset button to restore the image prior to the last action while working with the tool. If you accidentally click on Apply, you can use the Undo button to reverse the changes.

View Increases or decreases the view of the image in the Image Editor. Click on the arrows or click and drag the slider on the bar to adjust the view in increments. Or, select the symbol opposite Auto and select a view percentage (%) from the drop down list.



Photo Edit Tutorial

Below are two images - an original imported image and the same image after it has been edited in the Image Editor. The original image has too much red and is almost landscape in orientation. The procedures below outline how to correct the color hue and crop the image for a portrait orientation. If you have an image file of an individual, you can follow the steps below and observe the effects the tools have on the image during the tutorial. It is recommended that you use an image with equal height and width dimensions for this exercise. If you position the cursor over an image file in Windows Explorer, the popup window lists the pixel dimensions of the file.

Tutorial

1. From the Client main screen, select the Manage People button > Add Person.
2. From the Add Person screen, position the cursor over the photo frame silhouette to open the + button. Click on the + button.
3. From the Open dialog box, navigate to the folder where the individual's image file is located.
    - Ensure you have either All Files or the matching file format, such as JPEG, PNG etc., listed to view the images in the folder.
4. Select the file.
5. Click on the Open button.
6. The image is loaded in the Image Editors main screen.
7. We'll change the view from Auto to 100%. Click on the ▼ symbol opposite Auto in the lower right corner and select 100% from the drop down list. You can also drag the slider along the bar to increase or decrease the view. Try it. Then set the view to 100% again.
8. The first thing we'll do is correct the color.
9. Select the Hue Shift tool under the Adjust menu.

10. Now we're going to drag the slider along the Hue Shift bar to correct the color for more natural skin tones as shown in the Edited Image below. Try dragging the slider back and forth and observe the effect this tool has on the image color. When you have finished experimenting, drag the slider to the position where the skin tone is at its most natural color
    - If you make a mistake or don't like the change, you can select the Close button and the last change is discarded. You are returned to the Image Editor main screen. If you made several changes, you may have to click on the Undo button.
11. When you are satisfied with the color tones in the image, click on the Apply button.
12. Click on the Close button.
13. Next, select the Crop tool.
14. You will note the outer perimeter of the image is grey with a white marquis surrounding what is now the default cropped area by the Image Editor. However, the default crop area can be altered by clicking and dragging one of the vertical edges left or right or dragging one of the horizontal edges up or down. You can also click and drag one of the corners towards the centre or towards the outer edge.
15. For the cropping exercise, we're going to crop out some of the area on the left and the right of the image to give it a portrait orientation.
16. Position the cursor over the top white line of the default crop area. When the cursor changes to a double arrow, click and drag the line to the top edge of the image. We want to retain all of this detail in the image.
17. Reposition the cursor over the bottom white line of the default crop area and click and drag the line to the bottom edge of the image. We also want to keep all of this detail in the image.
    - You will notice that the pixels dimensions (width x height) change as you drag a line. To achieve a portrait orientation, the height pixels are greater than the horizontal pixels.
18. We will leave the vertical edges as they are. However you can adjust the vertical crop lines depending on your image.
19. When you have completed adjusting the crop lines, click on the Apply button.
20. Click on the Close button. You are returned to the main screen of the Image Editor.
21. Click on the Save button.

The image is loaded in the Edit Person screen. If an individual's image has to be replaced in the Edit Person screen, position the cursor over the upper right corner of the photo image and click on the delete button (waste bin icon) to erase the image from the record and then select the + button on the left side and open and edit the image again.

Any changes you make in the Image Editor do not affect or alter the original source image that you imported.

Original Image	**Edited Image**
	

Related Topics

Reduce Photos

Create a Temporary Credential

Under some circumstances you may have to issue a credential on a short-term basis for visitors, guests, temporary employees, or trades people where access is limited to a certain number of visits or a specified period of time.

The credential can be assigned with one of the following temporary parameters:

- a date range
- a limit on the number of times the credential can be used
- both of the above, whichever occurs first

Temporary cards expire 1 minute before midnight on their expiration date.

Limited to Group

This temporary option is intended for persons with multiple group access assignments. The temporary options only apply to the credential when it is used under the specified group. The temporary options do not apply to any other group access assignments.

When Limited to Group is enabled, note the following for the two temporary options – date range or limited # uses:

- Date Range - the Limited to Group is effective at 12:01 AM on the Valid From date specified in calendar/ time schedule
- Limited # Uses – takes effect immediately after the credential is saved

Please remember that if the temporary options include both a date range or Limited # Uses the Limited to Group assignment expires on the option that occurs first.

The Limited to Group option is only available with an Elite Edition license.

Date Format

The Aurora software uses the date format set in Windows. You can view the date format in the bottom right corner of Windows.

Procedures

Steps to Make a Credential Temporary

1. From the Client main screen, select the Manage People button.
    - To make an existing credential temporary, double click on the name of the person from the Person Search directory.
    - To make an unassigned credential temporary, click on the Add Person button. Complete the personal fields, add the credential information, and specify the group assignment. See Create a Credential Record for more on adding a credential.
2. Ensure that the Credential Information tab is currently selected.
3. If you have more than one site, ensure that the appropriate site is selected in the Site Assignment pane.
4. Click in the box to the left of Temporary Options. The box has an x when it is selected.
5. If the card is temporary based on a date range, click on the calendar icon to the right of Valid From.
6. The calendar opens on the current day and month.

- If the Valid From date is today, select it on the calendar.
- If the Valid From date is other than the current day, select the correct start day, or click on the arrows at the top of the calendar and scroll to the desired month and year. Select the day on the calendar.

Note: For Keyscan ACUs/ECUs, only the hour will be recognized (e.g. 7:15PM and 7:59PM will both be recognized as 7PM).

7. Click on the calendar icon to the right of Valid To.
   - If the Valid To date is today, select it on the calendar.
   - If the Valid To date is other than the current day, select the correct end day, or click on the arrows at the top of the calendar and scroll to the desired month and year. Select the day on the calendar.

   Note: For Keyscan ACUs/ECUs, only the hour will be recognized (e.g. 7:15PM and 7:59PM will both be recognized as 7PM).
8. If the card has a usage restriction, enter the maximum number of times the credential may be used in the Limited # Uses text box. If there is no usage restriction, leave the Limited # Uses blank.
9. If the temporary options only apply to one specific group access assignment, select the ▼ symbol opposite Limited to Group and select the group from the drop down list. Ensure you have reviewed the content under the Limited to Group heading above.
10. Click on the Save button.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Define Person Types

The Edit Person screen has a field called Type. The Client software includes two pre-defined types by default:

- Employee
- Visitor

You can create additional user-defined types as well. Depending on the nature of your access control setup, you may classify individuals such as member, resident etc, that are more applicable in describing person types. Types are created in the Application Utilities screen located in the Settings menu.

Visitor

The Person Type has a Visitor column in which you can designate newly created person types with a non-visitor classification (No) or with a visitor classification (Yes).

You cannot change the visitor status of the two pre-defined Person Types. Employee is set on No; Visitor is set on Yes.

E-Plex Type

The Person Type has an E-Plex Type column where you can designate specific E-Plex door authority to that particular Person. The following User types can be found with their descriptions in the table below.

Manager	• Lock programming/audit rights and 24/7 access; no expiry • Overrides Holidays • Overrides Privacy • Overrides Lockdown ** can be changed if Enhanced Lockdown is registered • Temp settings do not apply
Guest	• Schedule based access with optional privileges • Follows schedules • Follows temp settings • Cannot override Lockdown ** can be changed if Enhanced Lockdown is registered
M-Unit	• 24/7 lock programming/auditing rights only but no access; no expiry • Temp settings do not apply

Procedure

Steps to Create Captions for the Types Field

1. From the Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Click on the + to the left of the Person Type heading.
4. Click in the Person Type # text box that opened, select and delete the Person Type # text.
5. Enter a caption in the text box.
6. By default, a newly created Person Type has Visitor set on No. Do one of the following steps:
    - If the Person Type you have created is not a visitor category, leave the Visitor column set on No.

- If the Person Type you have created is designated as a visitor category, click on No under the Visitor column. Select the ▼ symbol and select Yes.

7. Repeat the above procedures if you are creating more types; otherwise go to the next step.
8. Click on the Save button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Enable the Middle Name Field

By default, only the Given Name and Surname fields are listed on the Edit Person screen. Aurora gives you the option of adding a Middle Name field on the Edit Person screen if it is required.

Procedure

Steps to Add the Middle Name Field

1. From the Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Under the Application Settings heading, click in the box to the right of Enable Middle Name. The box has an x when the function is enabled.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

AUTOMATICALLY CREATE PINS

You can set Aurora to automatically create a personal identification number (PIN) when adding a person's record to the Aurora database. PINs can also be manually entered depending on your site requirements. PINs are used with keypad type readers for gaining access.

Procedure

Steps to Activate the Auto Generate PIN Function

1. From the Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Under the Application Settings heading, click in the box to the right of Auto Generate PIN. The box has an x when the function is enabled.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Optional Fields - Common & Site

The Optional Fields on the Edit Person screen present two categories – Common fields and Site fields – for recording supplementary information about each person. The Common fields and the Site fields are user-defined in the Optional Fields Management screen.

Difference between Common and Site Fields

The primary difference between Common Optional Fields and Site Optional Fields is as follows:

- Common optional fields are listed on all records at all sites
- Site optional fields are available to all records at all sites but can be activated or deactivated for each site

Common Optional Fields

The fields listed under the Common Optional Fields heading are universal to all records at all sites. These fields are user-defined.

Until you create captions in the Optional Fields Management screen, the Common Optional Fields have generic descriptions Optional Field #1 to Optional Field # 12. The fields can be set as one of the following types:

- Text - alpha or numeric characters
    - Use text for phone numbers or other numbers where you will insert dashes - , parenthesis () or periods . or any other characters as part of the number
    - Examples 905-430-7226 (245) or 905.430.7226
- Number - numeric characters
    - Must only be 0 1 2 3 4 5 6 7 8 9
    - Positive or negative values
- Date - localized Windows date format

If you require more than 12 common optional fields, you can add more fields to suit your requirements. There is no limit on the number of common optional fields.

Site Optional Fields

The fields under the Site Optional Fields heading are user-defined. Until you create captions in the Optional Fields Management screen, the Site Optional Fields have generic descriptions Optional Field #1 to Optional Field # 12. The fields can be set as one of the following types:

- Text - alpha or numeric characters
    - Use text for phone numbers or other numbers where you will insert dashes - , parenthesis () or periods . or any other characters as part of the number
    - Examples 905-430-7226 (245) or 905.430.7226
- Number - numeric characters
    - Must only be 0 1 2 3 4 5 6 7 8 9
    - Positive or negative values

If you require more than 12 site optional fields, you can add more fields to suit your requirements. There is no limit on the number of site optional fields.

Site fields are universal to all sites; however, you have the option to selectively enable or disable a site optional field at each site.

Procedures

Steps to Add Common Optional Fields

1. From the Client main screen, select the Settings button > Optional Fields Management.
    - Keyscan suggests that you change the descriptions of the default common Optional Field #1 to common Optional Field # 12 before adding more common optional fields. To do this, go to step 3.
2. From the Optional Fields Management screen, click on the + to the left of Common Optional Fields.
3. Double click in the Optional Field # text box, select and delete the Optional Field # text.
4. Enter a description in the text box.
5. On the same row, double click under the Type column.
6. From the drop down list select the type of data - text, number, or date that will be entered in the common field on a person's record.
    - Remember, for fields such as phone numbers where you are inserting other characters, select text.
7. Repeat the preceding steps for each common field you are re-naming or adding.
8. Click on the Save button.
9. Do one of the following steps:
    - To create site optional fields, see Steps to Create Site Optional Fields.
    - Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Steps to Create Site Optional Fields

1. From the Client main screen, select the Settings button > Optional Fields Management.
    - Keyscan suggests that you change the descriptions of the default site Optional Field #1 to Optional Field # 12 before adding more site optional fields. To do this, go to step 3.
2. From the Optional Fields Management screen, click on the + to the left of Site Optional Fields.
3. Double click in the Site Field # text box that opened, select and delete the Optional Field # text.
4. Enter a description in the text box.
5. On the same row, double click under the Type column.
6. From the drop down list select the type of data - text, number, or date that will be entered in the common field on a person's record.
7. Repeat the preceding steps for each site field you are re-naming or adding.
8. Click on the Save button.
9. Do one of the following steps:
    - To create common optional fields, see Steps to Create Common Optional Fields.
    - Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.



If you have created site optional fields, they may have to be activated/deactivated in the Assign Site Optional Fields screen depending on which site optional fields apply to the site.

Related Topics

Assign Site Optional Fields

Activate/Deactivate Site Optional Fields

Site optional fields are created in the Optional Fields Management screen. However, once the site optional fields are created, you have the option of arbitrarily selecting which fields are available at each site.

Note +

The first 12 site optional fields are listed as Optional Field # 01 - Optional Field #12 until they are named in the Optional Fields Management screen.

If you create additional site optional fields in the Optional Fields Management screen, starting at Optional Field #13, those fields must be activated for the site.

Procedure

Steps to Activate/Deactivate Site Optional Fields

1. From the Client main screen, select the Site Setup button > Assign Optional Fields to Sites.
    - If you have multiple sites, double click on the site from the directory screen.
2. From the Assign Optional Fields to Sites screen, do one of the following depending on whether you are activating or deactivating the optional field for the site
    - Deactivate (the box currently has an x) - click in the box to the right of the optional field under the Assigned column to de-select it. The x is removed when the optional field is de-selected.
    - Activate (the box does not have an x) - click in the box to the right of the optional field under the Assigned column to select it. The box has an x when the optional field is selected.
3. Repeat for each optional site field you are either selecting de-selecting.
4. You can select or de-select all site fields by clicking in the box to the left of the Assigned heading.
5. Select the Save button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

Optional Fields Management

Records - Multiple Sites

When a person is added to the Client, by default that person's credential is enrolled at all sites and the record is enrolled at all sites. In some cases however, you may not want the individual's credential to be valid at all sites, only the record. In this case, you can de-select the applicable sites in the Credential Information screen but retain the record at the desired sites in the Site Enrollment screen.

Example of Site Enrollment

As an example, John Smith is a sales representative working from a regional office and his credential allows him access within that building. Periodically, however, John Smith travels to the head office in another region of the country. When he arrives at the head office his record is accessible but he is issued a temporary visitor's credential.

John Smith's record is as follows:

Credential Information

- enabled for the regional office
- disabled for the head office

Site Enrollment

- enabled for the regional office
- enabled for the head office

Procedures

Steps to Enable Site Enrollment

These procedures only apply if you have multiple sites. This assumes that you have previously created the credential record.

1. From the Client main screen, select the Manage People button > Manage People menu.
2. From the Person Search directory screen, double click on the name of the person in the list.
3. From the Edit person screen, select the Site Enrollment tab.
4. Click in the box to the left of the site to enable site enrollment. The box has an x when enabled.
5. If the credential is to be deactivated at the same site, ensure that you select the Credential Information tab and disable the site. When disabled, the box is blank.
6. Click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Disable Site Enrollment

1. From the Client main screen, select the Manage People button > Manage People menu.
2. From the Manage People directory screen, double click on the name of the person in the list.
3. Select the Site Enrollment tab.
4. Click in the box to the left of the site to disable site enrollment. The box is empty when disabled.
5. This also disables the site in the Credential Information screen.
6. Click on the Save button.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Import People Records

Aurora's Import People function is a time saving utility that lets you share credential and personal information from other external databases. Use the import people function to populate personal, credential, or common optional fields in the Aurora software from data that resides in another external database. In essence, the Import People function works on the basis of tagging the columns of data in the exported database file (CSV) to populate the appropriate Aurora fields.

Example of an Import Application

A company currently has an existing human resources database. This HR database includes information common to the Keyscan database, such as first names, last names, telephone numbers, e-mail addresses etc. Rather than re-enter all that data manually in the Aurora software, the import function allows you to capture the data from the HR database and match it with corresponding fields in the Aurora software. This saves a great deal of time and effort, especially if you are adding or updating hundreds of records.

Import People Requires CSV File Format

The Import People function only imports CSV files. Once you have saved the data in your external database as a CSV file, you open the Import People screen in Aurora, load the CSV file and match the fields with the appropriate Aurora fields.

The Import People function is used to create new credential holder records. Do not import the same CSV file more than one time; otherwise, you will have duplicate records.

Upgrading from System VII or Vantage to Aurora

If you are upgrading from System VII or Vantage, you can use the Export Cardholder Information function in either of those applications to create a CSV file which you can then import into Aurora to create your credential holder records. If your CSV file includes group access levels ensure that System VII/Vantage groups are the same as those created in Aurora with the same numerical assignment as shown in the table below:

System VII/Vantage	Aurora	
Group Description	**Number**	**Group**
001-Administration	1	Administration
002-Engineering	2	Engineering
003-Marketing	3	Marketing
0004-Finance	4	Finance

Please remember that Aurora uses the same groups for both doors and elevators, whereas System VII and Vantage have separate door and elevator groups. You may have to modify the CSV file if your elevator groups are different from your door groups in System VII or Vantage.

Note About Archived Cards in System VII or Vantage

If you have any archived card holder records in System VII or Vantage, amend the ArchivedCard column in your exported CSV file by changing FALSE to TRUE and TRUE to FALSE. Tagging the ArchivedCard column field with the Active field affects either the record or the credential as follows:

- Under the People Match Columns heading = Inactive record
- Under the Credential Match Columns heading = Inactive credential

Import People Conventions

You can choose to import data to populate the person information fields, the credential information fields, and the common optional fields. However, note the following conventions:

- Ensure that you have defined and saved any optional common fields in the Aurora software if you intend to include supplemental data fields for your people/credential records
- If the CSV file has dates and it was created at a different server, ensure that Windows has the same date format on the server with Aurora
- The CSV file must have Surname, Given Name and Person Type columns with populated data in each of the respective columns

Before importing your CSV file, Keyscan suggests that you review it and make any necessary revisions in the spreadsheet. We strongly urge that you have some familiarity with the Aurora Client software before you import the CSV file.

If you are unsure of the type of credentials you are using, select the Credential Information/About the Edit Person Screen link under Related Topics. When you are on the About the Edit Person Screen help screen, scroll down until you see the Credential Information heading. The most common credential used is the Keyscan category which is a card credential with a three digit batch code and a five digit card number - example 014-63385.

Person Types

By default, Aurora has two defined person types, Employee and Visitor. If you have other person types you may import those types. However, you must have defined those person types in the Application Utilities screen before you proceed with the import.

Credentials with Temporary Options

When importing people records in which some or all records have credentials with temporary options, either a date range or limited # uses, the CSV import file must have a designated temporary column. Your designated temporary column must be tagged to the Temporary field under the Credential Match Column in the Import People screen.

On the row of each credential record in which the temporary option applies, enter True under the designated temporary column. You must have representative columns that you can tag to the Valid From and Valid To and/or Limited Uses Fields.

For people records where temporary options do not apply, leave the row under the designated temporary column blank. The following table illustrates examples of temporary options and no temporary options. Remember that when specifying dates the order of the day, month and year must conform to the Windows date format.

Examples	**Import Columns Tagged to Aurora Temporary Options Fields**			
	Temporary	**Valid From**	**Valid To**	**Limited Uses**
People record with Temporary Options - Valid From, Valid To and Limited Uses	True	9/30/2015	10/30/2015	25
People record with Temporary Options - Valid From and Valid To	True	9/30/2015	10/30/2015	
People record with Temporary Options - Limited Uses	True			25
People record with no Temporary Options				

Note - Valid From and Valid To

You may include times with the Valid From and Valid To dates. Use the following convention with a space after the last date character: hh:mm AM or PM - example 9:30 PM. When a time is not specified, the Valid From and Valid To times are defaulted on midnight.

Multiple Credentials

You can import records where individuals have multiple credentials assigned to them. In order to import multiple credentials, the person's credentials must be listed contiguously and have a column with an ID value for each person as shown in the example below. You will note that you do not have to list credential holder information after the first row except the credential number and the matching ID value. In the example below the first person has two assigned credentials and the second person has three assigned credentials.

ID	Surname	Given Name	Person Type	Credential Number
1	Altman	George	Employee	.001-10001
1				.002-10020
2	Smith	Jennifer	Employee	.001-10076
2				.002-12003
2				.003-10024

Multiple Credential Types

You can import multiple credential types in cases where multiple credential formats are used. The formats you use must be supported by Keyscan Aurora and the CSV file must have a column containing the credential types exactly as they are identified in the Aurora software under the Add Keyscan Credential field in the Edit Person screen. The credentials can only be the following types and must be spelled in the CSV column exactly as shown:

- Keyscan
- Corporate 1000 - 35
- Large Card Decimal
- Large Card Hex
- Standard 26-bit
- HID H10304
- OEM 20 bit
- OEM 24 bit
- Corporate 1000 - 48
- HID H10302
- Kaba UID

Importing Images

If importing a large number of records with an individual photo included with each record, Aurora has two default settings in the Application Utilities that reduce any images over 0.5 MB to 0.25 MB. These settings are intended to conserve space in the database while still preserving sufficient image detail for photo badges and the on-screen image in the Edit Person screen or the Manage System User screen. For more about the reduce photos function in the Application Utilities, see Related Topics below.

Procedures

Steps to Import People Records

1. From the Client main screen, select the Manage People button > Import People.
2. From the Import People screen in the upper left under the Sites heading, ensure the applicable sites for the import are selected. The box to the left has an x when the site is selected.
3. Below the File Import heading, select the Browse button and from the Open File dialog screen, navigate to the folder location with the CSV file and select it.
    - Under the Import File Preview, you will see the columns of your CSV file and the first couple of rows. You will tag these column headings with the associated Aurora fields.
4. Click on the Open button.
5. Opposite Default Person Type, click on the ▼ symbol and select In Import File, Employee, Visitor or a user-defined type if other person types have been created.
    - If you have multiple person types in your CSV file, leave the Default Person Type setting on In Import File and assign the CSV column to the Person Type under People Match Columns.
6. Do one of the following steps:
    - If you are importing credentials (card numbers), ensure the box to the left of Import Credentials is selected. Opposite Type, click on the ▼ symbol and select the credential type.
    - If you have multiple credential types in your CSV file, leave the Default Type setting on In Import File.
    - If you are not importing credentials, ensure the box to the left of Import Credentials is de-selected. The box is blank when it is de-selected.
7. Ensure that the People Match Columns fields are visible. To expose the fields, click on the V symbol to the left.
8. Opposite Surname, click on the ▼ symbol and select the field in the CSV file that contains the last names of the people you are importing.
9. Opposite Given Name, click on the ▼ symbol and select the field in the CSV file that contains the first names of the people you are importing.
    - The Surname, Given Name and Person Type fields are required; otherwise you cannot perform the import.
10. Complete the required People Match Columns to tag the Aurora fields with the applicable columns in the CSV file.
11. If you are importing credential information from the CSV file, click on the V symbol to the left of Credential Match Columns. Tag the Aurora headings with the matching CSV columns.
12. If you are importing optional fields from the CSV file, click on the V symbol to the left of Optional Fields Match Columns. Tag the Aurora headings with the matching CSV columns.
    - To blank out an unwanted CSV column, click on ▼ symbol opposite the field and select the blank space at the top of the list.
13. When you have completed tagging the Aurora fields with the applicable columns in the CSV file, click on the Import button.

- If you select the Import button and wish to stop the import process, click on the Cancel button.

14. From the Import Complete confirmation box, click on the OK button.
    - If Aurora encountered errors during the import, click on the OK button of the error box. The import is aborted and Aurora opens Windows Notepad with a summary of the errors. Print a copy of the error summary and edit the CSV file with the necessary corrections and repeat the import procedures.

15. Click on the Back button to return to the main screen or the navigation history button to return to a previously opened screen.

Keyscan suggests that you review the records you have just imported. You can access them from the Person Search screen.

Related Topics

About the Edit Person Screen

Reduce Photos

Export People Records

Aurora's Export People function lets you share credential and personal information with other external databases. In essence, the Export People function works on the basis of capturing specific Aurora fields and transposing them in a CSV file which can then be imported into another database.

System User Permission

In order to export people records, a system user account must have either a Master or Administrator designation and it must have the Can Export function selected under the Permissions heading in the Manage System User screen; otherwise, the Export People function is unavailable.

Export File Name

When Aurora exports a credential holder record the file is saved with the following name format:

- Site Name - People Export - Year (yyyy) Month (mm) Day (dd) Hour (hh) Minute (mm).csv

Photos

If you select photos, only the credential holders default photo is exported. You must also specify an export folder location in the Photo Path field when the Photos option is selected. The photos are named on the basis of the Given Name and Surname fields.

Advanced Filters

The following filters can be employed in locating selective records for export:

- Name - lists the records based on the name entered which can be the Given Name or the Surname
    - You can also enter a partial name or just 1 character to list names - example: entering the letter i would list all Given Names and Surnames that have the letter i.
- Optional Field - lists the credentials under the entered common field (data entry, not the optional field description)
- Site - lists the records based on selected site
- Credential Number - lists the records based on the credential entered
- Group Name - lists the records based on the group name entered
- Person Type - lists the credentials based on the Person Type field selected
- Active - lists persons or credentials based on an active status, an inactive status or both (all)

Procedures

Steps to Export People Records

1. From the Client main screen, select the Manage People button > Export People.
2. From the Export People Setup screen below the Export File heading, select the ▼ symbol opposite Site and, if applicable, select the site with the people records you are exporting.
    - You can only export one site per CSV file.
3. To narrow the group of records exported, use the advanced filters if required.
4. Under the People heading, do one of the following steps:

- To include all the listed credential holders, click in the box to the left of Given Name.
- To include just specific credential holders, click in the box to the left of the individual's given name.

5. Ensure that People export columns has the ^ symbol so all the sub-options are visible. Surname and Given Name are selected by default and are mandatory export fields.
6. Do one of the following steps:
   - To select all the people options listed, click in the box to the left of People export columns until it has an x. All the sub-fields are selected.
   - To only include the Surname and Given Name, leave the People export columns unchecked
   - To select only some of the people options, select the boxes to the left of the desired fields. The box has an x when selected.
7. If you selected the Photo option above, click on the Browse button and from the Browse for Folder dialog box, either create a folder by clicking on the Make New folder button or navigate to the desired folder location.
8. Click on the OK button.
9. If you are including credential fields, ensure that the open ^ symbol on the left opposite Credential export columns is selected so all the sub-options are visible. Select the desired options.
10. If you are including common optional fields, ensure that the open ^ symbol on the left opposite Common optional fields export columns is selected so all the sub-options are visible. Select the desired options.
11. If you are including site optional fields, ensure that the open ^ symbol on the left opposite Site optional fields export columns is selected so all the sub-options are visible. Select the desired options.
12. When you have finished selecting fields for the CSV file, click on the Export button.
13. From the Save As dialog box, do one of the following procedures:
    - If you are using the default export file name, navigate to the desired folder location and click on the Save button.
    - If you want to re-name the export file, enter the new file name in the File name text box, navigate to the desired folder location and click on the Save button.
14. From the export confirmation File name on the OK button.
15. To close the Export People Setup screen, click on the Back button until you are at the main screen or for a previously viewed screen, select the Navigation History  down arrow to the right of the Back button.

Create Records with a Bizscan Scanner

You can use Aurora's Scan Driver's License or Scan Business Card functions from the Edit Person screen to create a person's record, whether he or she is an employee, visitor or other user-defined person type. In order to create a record by scanning, you require either Keyscan's Bizscan for business cards or Bizscan2 for driver's licenses and/or business cards.

Business card or driver's license scanning in Aurora requires a Card Scanning License from Keyscan.

Scan Image Only

The Scan Driver's License has a third option - Scan Image Only - which captures an image of the driver's license or business card and adds it in the credential record's photo folder. The Scan Image Only function does not use optical character recognition and does not populate any fields with the information from the driver's license or business card.

Preliminary

Before you can use Aurora's Scan Driver's License or Scan Business Card functions in Aurora, you must have purchased and registered the Card Scanning License and you must have installed the driver which is included in your Aurora Software Installation file folder.

Driver installation instructions for the Bizscan and Bizscan2 are included with the Aurora Software Installation files in the Aurora Documents folder. Review the Document Index to locate the driver installation instructions.

Do not plug in the scanner's USB cable until you are instructed to do so in the driver installation procedures.



If you have upgraded from System VII or Vantage and previously used a Bizscan or Bizscan2, you must install the drivers included with the Aurora Software Installation files. Older drivers from System VII or Vantage will not function in Aurora.

Procedures

Steps to Scan a Business Card

1. From the Client main screen, select the Manage People button > Add Person.
2. Place the business card horizontally, face-down with the top of the card entering the scanner first. Ensure the card is to the right edge of the scanner's feed tray.
3. From the Edit Person screen, select the ▼ symbol on the right of Scan Driver's License and select Scan Business Card from the drop down list.
    - If you have not scanned a card yet, you will be prompted to insert the calibration paper. Follow the on-screen prompts.
4. After the business card has been scanned, complete any remaining fields in the Edit Person screen.
5. The Edit Person screen also captures an image of the business card which you can save along with the record. If you want to delete the card image, click on the Waste Bin icon over the upper right corner of the card image.
6. Select the Save button.
7. Click on the Back button until returned to the main screen or the ▼ navigation history button to return to a previously opened screen.

Steps to Scan a Driver's License or ID Card

1. From the Client main screen, select the Manage People button > Add Person.
2. Place the driver's license horizontally, face-down with the top of the license entering the scanner first. Ensure the license is to the right edge of the scanner's feed tray.

3. From the Edit Person screen, select the ▼ symbol on the right of Scan Driver's License and select Scan Driver's License from the drop down list.
    - If you have not scanned a license yet, you will be prompted to insert the calibration paper. Follow the on-screen prompts.
4. After the business card has been scanned, complete any remaining fields in the Edit Person screen.
5. The Edit Person screen also captures an image of the driver’s license which you can save along with the record. If you want to delete the license image, click on the Waste Bin icon over the upper right corner of the license image.
6. Select the Save button.
7. Click on the Back button until returned to the main screen or the ▼ navigation history button to return to a previously opened screen.

Search for Records

The Person Search screen acts as the directory for accessing all records and conducting user-defined searches to locate specific records for editing, deleting or other tasks.

People Record Presentation

Each record on the Person Search - Manage People screen presents the individual's information as follows:



Sort By

You can re-organize how records are presented on screen by clicking on the ▼ symbol to the right of Sort By to open the drop down list and selecting one of the following options:

- Given Name
- Surname
- Type

Advanced Filter

The advanced filter in the Person Search directory screen offers the following fields which can be used individually or in any combination for locating records.

- Name - searches for records based on Given Name, Middle Name (if enabled) and Surname
- Group Name - searches for records based on access level assignments
- Site Name - searches for records based on site enrollment
- Credential Number - searches for records based on Batch Number or Card Number
- Optional Field - searches for records based on optional field
- Person Type - searches for records based on type assigned
- Active - searches for either records or credentials with an inactive status, active status or both (all)
- Today's Visits Only - searches for records based on visits scheduled for today's date
- Visit Status - searches for records with the selected visit status
- Expires Between - searches for records with credentials assigned a temporary date range which expire within the period specified

To open the advanced filters, click on Advanced Filter.

Search Filter Parameters

In the search field boxes, you can enter the full name or number or just a segment of the alpha or numeric characters right down to one alpha or numeric character. The more characters and the more fields specified, the more refined the search.

Refresh

Selecting the Refresh button updates the screen to reflect the current people list. The refresh applies more so with multiple Clients to update the list from the database where changes may have occurred at other stations. The last refresh date and time is displayed at the bottom of the list view.

Examples

- If you wanted to list all cardholders whose name contains the letter M, type M in the Name field.
- If you had IT and Security group names, and you entered IT in the Group Name filter, the search result would list both groups since they both contain IT.
- If you were searching for a particular person by name, specify the given name, middle name (if enabled) and the surname in the Name search filter box.

Refine Searches %

In the Advanced Filter, to refine the people search even further, use the **%** symbol to isolate certain names. For instance, searching **Jose** will bring up everyone with **Jose** in their name, whether it's their first, last or even middle name. To refine, by searching **Jose%Olazabal** a person with only those names will appear in the search. You can also search for middle names to refine even further, for instance **Jos%Mar%Ol** will bring up J**ose Maria Olazabal**.

Procedures

Steps to Perform a Records Search

1. From the Client main screen, select the Manage People button > Manage People menu.
2. From the Person Search directory screen, click on (v) Advanced Filter to open the search filters.
3. Enter the search parameters in desired search filter boxes.
    - You will note that as you continue entering characters the in the respective boxes the Person Search screen instantly refines the results.
4. Continue to enter characters in the search filters until you have located the desired record or records.
5. To perform another search, you must place the cursor inside each search filter that was used and delete the text and then conduct another search.
6. When you have completed searching for records, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Edit/Delete a Credential Record

Edit/Delete a Record

You can edit or delete individual records from the database.

The Person Search directory gives you access to all the records to edit or delete. You can either scroll through all listed records or use the search operators in locating specific records; then select the specific record you are either editing or deleting.

Procedures

Edit a Person's Record

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory, scroll through the list of credential records or use the search operators to locate the desired record.
3. Double click on the record.
4. From the Edit Person screen, select the relevant tabs along the top and edit the desired information.
5. Select the Save button.
6. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Delete a Person's Record

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, scroll through the list of records or use the Advanced Filter search operators to locate the desired record.
    - Important - once you select the waste bin button in the next step, the person's record is permanently deleted.
3. Select the waste bin button along the row of the record that you are deleting.
4. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Search for Credential Records

Deleted People Report

De-activate Credential or Record

Aurora provides you with an option of de-activating either an individual's record or a credential. De-activating a record or a credential are options that can be used when you wish to maintain the record in the database rather than deleting the record or the credential permanently so the data doesn't have to be re-entered at a later date.

As noted below, when a person is marked as inactive the credential cannot be used at any site while it is set as inactive, whereas, credential inactive is credential and site specific. Credential Active/Inactive only apples in cases where the individual has been issued two or more credentials.

- Person Active - the person and his or her credentials have access to all valid sites
- Person Inactive - the person and his or her credentials cannot access any valid sites
- Credential Active - the selected credential has access at all valid sites
- Credential Inactive - the selected credential does not have access at specified sites

Note: When a Person becomes Inactive, so do their credential(s). When a Person becomes Active again, all previously Active credentials will also re-activate. Any credentials marked Inactive prior will remain Inactive when the Person is re-activated.

Procedures

Steps to De-activate a Person's Record

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, locate the credential record by either scrolling through the list or using the search operators.
3. Double click on the record.
4. From the Edit Person screen, select the Person Active button below the individual's personal information on the left side of the Edit Person screen.
    - The status changes to Person Inactive.
5. Select the Save button.
6. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to De-activate a Credential

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, locate the credential record by either scrolling through the list or using the search operators.
3. Double click on the record.
4. From the Edit Person screen, ensure the Credential Information tab is selected.
5. Below the Groups & Temporary Options panes, click on the < > arrows until the credential being de-activated is listed.
6. Select the Credential Active button below the Temporary Options pane.
    - The status changes to Credential Inactive.
7. Select the Save button.
8. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Re-activate a Person's Record

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, locate the credential record by either scrolling through the list or using the search operators.
3. Double click on the record.
4. From the Edit Person screen, select the Person Inactive button below the individual's personal information on the left side of the screen.
    - The status changes to Person Active.
5. Select the Save button.
6. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Re-activate a Credential

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, locate the credential record by either scrolling through the list or using the search operators.
3. Double click on the record.
4. From the Edit Person screen, ensure the Credential Information tab is selected.
5. Below the Groups & Temporary Options panes, click on the < > arrows until the credential being activated is listed.
6. Select the Credential Inactive button below the Temporary Options pane.
    - The status changes to Credential Active.
7. Select the Save button.
8. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

Bulk Update Credentials

Records - Multiple Sites

Cancel & Replace a Lost or Stolen Credential

In the event a person reports a lost or stolen credential and issue a new credential, open the person's record and add the new credential, delete the old credential number, and save the record. The old credential is neutralized and no longer usable if someone tries gaining access with it. If the credential is returned at a later date, it can be re-assigned to another individual.

Ensure the Auto Update function is enabled - the box has an X - on the Site Information Setup screen.

Procedure

Steps to Replace a Credential

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, locate the credential record by either scrolling through the list or using the search operators.
3. Double click on the record.
4. From the Edit Person screen, ensure the Credential Information tab is selected.
5. Below the Groups pane, click on the ▼ symbol to the right of the Clone button.
    - Selecting the Clone button will preserve the person's current group assignments.
6. Select the format of the replacement credential you are issuing.
7. Enter the credential's number in the Card Number field, and if a batch code applies, enter the number in the Batch field.
    - The batch code may also be referred to as the facility or site code.
8. Below the Groups & Temporary Options panes, click on the ▼ symbol between the < > arrows and select the lost or stolen credential number.
9. On the Credential Information title bar near the top, click on the waste bin button to delete the old credential from the database.
10. Select the Save button.
11. To exit, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Print Photo Badges

If you have created photo badge templates with the Manage Global Card Templates editor and have a card printer connected, you can print badges from the Edit Person screen.

You cannot change the badge's portrait or landscape orientation in the Print Badge screen; the template's orientation is based on how it was designed in the Manage Global Card Templates editor.

Hide Image/Change Image

The Print Badge screen has a Hide Image/Change Image function if the photo badge template is designed with the credential holder image placeholder. The Hide Image function is designed for masking out the grey silhouette when there is no available image for the credential holder. The Change Image function allows substituting an alternate image, if the selected credential holder has more than one image on file.

The Hide Image/Change Image is accessed by right-clicking on either the credential holder's image or the grey silhouette place holder after the template has been selected and loaded in the Print Credential screen.

Card Type

Aurora allows creating three different card types - global, site or visit. The procedures below outline the steps for printing global or site card type templates only. For printing visit card type templates, select the link Print Visitor Photo Badges below Related Topics. For more information about card types, click on the Card Properties link below Related Topics.

Procedures

Steps to Print a Photo Badge

These instructions assume that you have previously created the person's record and you are printing a photo badge with a Card Type of either global or site.

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, scroll through the list of records or use the search operators to locate the desired record.
3. Double click on the record.
4. From the Edit Person screen, ensure the Credential Information tab is selected.
5. Select the print icon button on the Credential Information heading.
6. From the Print Credential dialog box, click on the ▼ symbol to the right of Template and select the desired template file from the drop down list. The dialog box opens a preview image of the template.
7. To use the Hide Image/Change Image function, position the cursor over the grey silhouette or the person's photograph, right click and select the desired option.
    - Hide Image - click on Hide Image. The image is removed from the template.
    - Change Image - click in the box that is to the upper left of the desired image. The Box has an x when selected. Click on the OK button.
8. If the photo badge uses a back side template, click on the ▼ symbol to the right of Back Template and select the desired template file from the drop down list.
9. Click on the OK button.
10. From the Print dialog window, click on the badge printer from the list under Select Printer.
    - If the card printer is not displayed, select the Find Printer button and browse for the card printer. Then select it when it is listed.
11. Click on the Print button.

12. To return to the Person Search directory, select the navigation history  symbol and select Person Search from the list, or click on the Back button until you reach the main screen.

Related Topics

- Manage Global Card Templates
- Print Visitor Photo Badges
- Card Properties

Credential Transactions

The Edit Person screen has a tab titled Transactions. When the tab is selected, the Transaction window lists where and when the credential was used. Transactions are listed in descending order with the most recent transaction at the top of the list. Transactions are retained for the past 45 days. Transaction details are presented in columns from right to left as follows:

- Site name
- Access control unit
- Device
- Credential
- Type
- Date

Modes of Viewing Transactions

You use one of two modes for viewing transactions:

- Receive Live Transactions - if this option is enabled, the box has an x, the transaction screen is automatically updated as each transaction occurs
- Refresh - the transaction screen is only updated with the latest transactions after clicking on the Refresh button, the date and time of the last refresh is posted above the Refresh button

When the Receive Live Transactions is enabled, the Refresh option is unavailable.

Include Credential Not Found Transactions

This option is used as an alternate method of credential enrollment. Select Credential Enrollment Feature below Related Topics for more details about this function.

Related Topics

Credential Enrollment Feature

Credential Enrollment Feature

The Credential Enrollment feature is a convenient method in determining a card number where one of the following circumstances applies:

- For an unknown card format, usually with more than 5 digits, in which the system re-creates a new card number compatible with Keyscan
- As above, except that a large number of cards have to be enrolled
- Where the number has worn off and is no longer visible on the card
- Enrolling cards that use a large card format
- Corporate 1000 cards with multiple Corporate ID numbers per site

The Credential Enrollment requires the use of a reader.

The Credential Enrollment Feature uses the Include Credential Not Found Transactions function in the Transactions sub-screen of the Edit Person screen.

Procedure

Steps to Use the Card Enrollment Method

1. From the Client main screen, select the Manage People button > Add Person.
2. From Add Person screen, select the Transactions tab.
3. Click in the box to the left of Receive Live Transactions to enable this feature. The box has an x when this function is enabled.
4. Click in the box to the left of Include Credential Not Found Transactions to enable this feature. The box has an x when this function is enabled.
5. Present the card at a conveniently located reader.
6. The card transaction is listed as Accessed Denied - Card Not In ACU.
7. Right click on the transaction and from the pop-up screen, select Add Credential.
    - The credential number is inserted in the card number field in its large card number format regardless of the type card.
8. Complete the relevant cardholder fields.
9. Click on the Save button when you have completed entering the information.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Bulk Update Credentials

The Bulk Update Credentials screen simultaneously updates multiple credentials which all share a common change.

- Activate or deactivate credentials
- Delete credentials
- Add or remove group access
- Edit or clear temporary options
- Add or remove lockdown access

As opposed to opening individual credentials, using the Bulk Update Credentials screen is more efficient and saves time when making the same change for a group of credentials.

Examples

As an example, you may have a group of temporary workers. Some will return at a later date; some will not return at all:

- Individuals returning - those individuals will have their credential(s) deactivated, which retains the person record, but the credential cannot be used until re-activation
- Individuals not returning - those individuals will have their credential(s) deleted

Bulk Update Actions

The Bulk Update Credentials screen presents several selectable actions. The table below outlines what each Bulk Update Action does.

Bulk Update Action	Notes
Activate	Activate a credential.
Deactivate	Deactivate a credential so it can be re-activated at a later date.
Delete	Permanently delete a credential so it can never be used again.
Add group access	Add various group access levels to a specified credential on a selected site.
Remove group access	Remove various group access levels from a specified credential on a selected site.
Edit temporary options	Change what is recorded within temporary options on selected sites.
Clear temporary options	Remove what is recorded within temporary options on selected sites.
Add Lockdown Access	Add lockdown access to a specified credential.

Remove Lockdown Access	Remove lockdown access from a specified credential.

Advanced Filters

The following filters can narrow the search:

- Credential Number - filters by credential number
    - If using the Keyscan credential format, entering just the batch code and the first three digits that precede the hyphen will list all records assigned with the specified batch code, also referred to as a site code or facility code
- Description - filters credentials based on the credential description entered
- Site - filters credentials based on the option selected: All Sites (based on the user's site permissions), No site or a specific site
- Person - filters credentials based on the name entered which can be the Given Name, Middle Name or the Surname
- Group Name - filters credentials based on the group name entered
- Credential Type - select the applicable credential type from the drop-down menu, the list will be filtered with those credentials
- Active - filters credentials based on active status, inactive status or both (all)
- Expires Between - filters credentials that expire before, between or after the selected dates
- Unused Since - filters credentials that haven't been used since the date specified
- Person Type - lists the credential based on Person Type field selected
- Optional Field - additional information can be entered here for person search criteria

You can use one or multiple filters to refine credentials.

Procedures

Steps to Perform a Bulk Activate Update

1. From the Client main screen, select Manage People > Bulk Update Credentials.
2. The Bulk Update Credentials screen shows all credentials the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol and choose Activate from the drop-down menu.
4. Do one of the following steps for Credentials Upload:
    - All - All credentials will be uploaded, regardless of which credentials are chosen
    - Single - Only updated credentials will be uploaded; a credential is selected when the box beside it has an **x**
5. Select Update.
6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt - Select OK.
8. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Deactivate Update

1. From the Client main screen, select Manage People > Bulk Update Credentials.
2. The Bulk Update Credentials screen shows all credentials the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol and choose Deactivate from the drop-down menu.
4. Do one of the following steps for Credentials Upload:
    - All - All credentials will be uploaded, regardless of which credentials are chosen
    - Single - Only updated credentials will be uploaded; a credential is selected when the box beside it has an **x**
5. Select Update.
6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt - Select OK.
8. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Delete Update

1. From the Client main screen, select Manage People > Bulk Update Credentials.
2. The Bulk Update Credentials screen shows all credentials the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol and choose Delete from the drop-down menu.
4. Do one of the following steps for Credentials Upload:
    - All - All credentials will be uploaded, regardless of which credentials are chosen
    - Single - Only updated credentials will be uploaded; a credential is selected when the box beside it has an **x**
5. Select Update.
6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt - Select OK.
8. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Add or Remove Group Access Update

1. From the Client main screen, select Manage People > Bulk Update Credentials.
2. The Bulk Update Credentials screen shows all credentials the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol. From the drop-down list, select the one of the following:
    - Add group access
    - Remove group access
4. On the right of the Site heading, select the ▼ symbol and choose an applicable site.
5. Select Group(s) to add/remove access to. A Group is selected when the box beside it has an **x**.
6. Do one of the following steps:
    - All - All credentials will be uploaded, regardless of which credentials are chosen
    - Single - Only updated credentials will be uploaded; a credential is selected when the box beside it has an **x**

7. Select Update.
8. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
9. From the Bulk update finished prompt - Select OK.
10. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform an Edit or Clear Temporary Options Update

1. From the Client main screen, select Manage People > Bulk Update Credentials.
2. The Bulk Update Credentials screen shows all credentials the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the symbol. From the drop-down list, select the one of the following:
   - Edit temporary options - select if you are changing or adding information to temporary options
   - Clear temporary options - select if you are removing information from temporary options
4. Under the Site heading, select the site(s) that apply for the temporary options you are updating.
   - If at any point you inadvertently make a mistake in the Action window, select Clear, which will cancel all your current selections
5. If you are editing temporary options, fill in the necessary fields (Valid From, Valid To, and/or Limited # of Uses).
6. Do one of the following steps for Credentials Upload:
   - All - All credentials will be uploaded, regardless of which credentials are chosen
   - Single - Only updated credentials will be uploaded; a credential is selected when the box beside it has an **x**
7. Select Update.
8. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
9. From the Bulk update finished prompt - Select OK.
10. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Add or Remove Lockdown Access Update

1. From the Client main screen, select Manage People > Bulk Update Credentials.
2. The Bulk Update Credentials screen shows all credentials the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the symbol. From the drop-down list, select the one of the following:
   - Add Lockdown Access
   - Remove Lockdown Access
4. Do one of the following steps:
   - All - All credentials will be uploaded, regardless of which credentials are chosen
   - Single - Only updated credentials will be uploaded; a credential is selected when the box beside it has an **x**
5. Select Update.

6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt - Select OK.
8. Select Back until you return to the main screen or choose  Navigation History for a previously viewed screen.

Bulk Update People

The Bulk Update People screen simultaneously updates multiple people records which all share a common change.

- Activate or deactivate people records
- Delete people records
- Edit or clear content in optional fields
- Add or remove people records from a site

As opposed to opening individual people records, using the Bulk Update People screen is more efficient and saves time when making the same change for a group of records.

Examples

As an example, you may have a group of temporary workers. Some will return at a later date; some will not return at all.

- Individuals returning - those individuals will have their record deactivated, which retains the record, but the credential cannot be used until re-activation
- Individuals not returning - those individuals will have their records deleted

Bulk Update Actions

The Bulk Update Person screen presents several selectable options. The table below outlines what each Bulk Update Action does.

Bulk Update Action	Notes
Activate	Activate a person record.
Deactivate	Deactivate a person record so it can be re-activated at a later date.
Delete	Permanently delete a person record so it can never be used again.
Edit optional fields	Change what is recorded within the Optional Fields.
Clear optional fields	Remove what is recorded within the Optional Fields.
Add people to site	Add a person record to a specified site.
Remove people from site	Remove a person record from a specified site.

Advanced Filters

The following filters can narrow the search:

- Name - filters records based on the name entered, including Given Names, Middle Names and Surnames
- Group Name - filters records based on the group name entered

- Site - filters records based on the option selected: All Sites (based on user's site permissions), No site or a specific site
- Credential Number - filters records based on the credential entered
    - If using the Keyscan credential format, entering just the batch code and the first three digits that precede the hyphen will list all records assigned with the specified batch code, also referred to as a site code or facility code
- Optional Field - filters records under the entered common field (data entry, not the optional field description)
- Person Type - filters records based on the Person Type field selected
- Active - filters people based on active status, inactive status or both (all)
- People without Credentials - filters the search to people who do not possess a credential but have a person record
- Show photos - displays an image of the person in the list if records have image files attached

You can use one or multiple filters to refine people records.

Procedures

Steps to Perform a Bulk Activate Update

1. From the Client main screen, select Manage People > Bulk Update People.
2. The Bulk Update People screen shows all people records the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol and choose Activate from the drop-down menu.
4. Do one of the following steps:
    - All - All records will be uploaded, regardless of which records are chosen
    - Single - Only updated records will be uploaded; a record is selected when the box beside it has an **x**
5. Select Update.
6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt, select OK.
8. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Deactivate Update

1. From the Client main screen, select Manage People > Bulk Update People.
2. The Bulk Update People screen shows all people records the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol and choose Deactivate from the drop-down menu.
4. Do one of the following steps:
    - All - All records will be uploaded, regardless of which records are chosen
    - Single - Only updated records will be uploaded; a record is selected when the box beside it has an **x**
5. Select Update.

6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt, select OK.
8. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Delete Update

1. From the Client main screen, select Manage People > Bulk Update People.
2. The Bulk Update People screen shows all people records the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the symbol and choose Delete from the drop-down menu.
4. Do one of the following steps:
    - All - All records will be uploaded, regardless of which records are chosen
    - Single - Only updated records will be uploaded; a record is selected when the box beside it has an **x**
5. Select Update.
6. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
7. From the Bulk update finished prompt, select OK.
8. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform an Edit or Clear Optional Fields Update

1. From the Client main screen, select Manage People > Bulk Update People.
2. The Bulk Update People screen shows all people records the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the symbol. From the drop-down list, select the one of the following:
    - Edit optional fields - select if you are changing or adding information to optional fields
    - Clear optional fields - select if you are deleting the information from optional fields
4. Under the Site heading, select the site(s) that apply for the optional fields you are updating.
    - If at any point you inadvertently make a mistake in the Action window, select Clear, which will cancel all your current selections
5. Select either Common Optional Fields or the site name depending on whether you are updating a common optional field or a site-specific optional field.
6. If you are editing or clearing optional fields, select either Common Optional Fields and/or the site name. For each, select the Optional Field and fill out the text box beside it. An Optional Field is selected with an **x** beside it.
7. Do one of the following steps:
    - All - All records will be uploaded, regardless of which records are chosen
    - Single - Only updated records will be uploaded; a record is selected when the box beside it has an **x**
8. Select Update.
9. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
10. From the Bulk update finished prompt, select OK.
11. Select Back until you return to the main screen or choose Navigation History for a previously viewed screen.

Steps to Perform a Bulk Add or Remove People Update

1. From the Client main screen, select Manage People > Bulk Update People.
2. The Bulk Update People screen shows all people records the user has access to. To refine the list further, fill in the applicable field(s) under the Advanced Filter.
3. At the right of Action, select the ▼ symbol. From the drop-down list, select the one of the following:
    - Add people to site - select if you are adding people to the applicable site
    - Remove people from site - select if you are removing people from the applicable site
4. Under the Site heading, select the site that applies:
    - If at any point you inadvertently make a mistake in the Action window, select Clear, which will cancel all your current selections
5. Do one of the following steps:
    - All - All records will be uploaded, regardless of which records are chosen
    - Single - Only updated records will be uploaded; a record is selected when the box beside it has an **x**
6. Select Update.
7. From the Bulk Update prompt - Do you want to proceed with these updates? Select Yes.
8. From the Bulk update finished prompt, select OK.
9. Select Back until you return to the main screen or choose  Navigation History for a previously viewed screen.

Bulk Print Credentials

The Bulk Print Credentials feature is used to print several cards at once. Before using this feature, a Card Template must first be added to the system.

Note: Although the Bulk Print Credentials feature can be used with each of the three card template types (Global, Site, and Visit), some visit-specific fields, such as arrival and departure times, will not work with Bulk Print and will therefore appear blank when printed. In addition, visits cannot be selected in bulk operations. For this reason, bulk printing using the Visit card template type might be undesirable.

Procedure

Steps to Bulk Print Credentials

1. Fill in the Advanced Filters at the top of the screen to search for the credentials you would like to print. The results of filtering will be applied to the credentials listed under the Credentials sub menu. Available filters are as follows:
    - **Credential Number**
    - **Active**
    - **Person**
    - **Description**
    - **Group Name**
    - **Site**
    - **Credential Type**
2. Choose credentials to be printed and select the **>** icon to move them to the Credentials to Print sub menu. Alternatively, move credentials back with the **<** icon.
3. Ensure items in the Credentials to Print sub menu are in the same order that your printer will print. For example, if you are printing cards 001-0001, 001-0002, and 001-0003, ensure your printer's card hoper is ordered so that card 001-0001 will be printed first, followed by 001-0002, and finally 001-0003. (Cards will print in order on screen, not necessarily in sequential order). This way, the proper card holder's details will be printed on the card. You can re-order credentials by using the **^** and **v** icons beside each card number or by dragging selected items to the correct spot (you can drag multiple selected items and when you drop them they will appear as a group).
4. Select the Template you would like to print on the front for the credentials selected. If your printer supports back printing, you can also select a Back Template.
5. Select the Print Batch Size from the drop-down menu. We recommend starting with a batch size of 1 to ensure the printer is in proper working order for the first print and increase the batch size once you are happy with the results. This function supports a batch size of up to 50 cards at a time.
6. Click Print to proceed.
7. Choose the applicable card printer from the pop-up menu. Don't worry, you will have a chance to confirm your cards on the next screen before printing begins.
8. In the Bulk Print Batch screen, confirm the order that you are printing matches the order of cards in your printer's hopper so that the item listed at the top is printed first and the items following are ordered

properly. If everything matches, select OK to print the batch. Once that batch is printed, confirm the order of the next batch and select OK to continue. Repeat this process until all cards are successfully printed.

Note: Periodically clean your printer between batches for the best printing results and to adhere to the cleaning rules that maintain your printer's warranty.

Related Topics

Create a New Card Template

Block Load Credentials

The Block Load Credentials screen lets you quickly enter a group of credentials for immediate use without having to enter names or other personal information for individual credential holders. This is a fast method to enter cards; however, the disadvantage is that you have no records identifying the names of credential holders or the assigned credential.

You can only use the Bulk Load Credentials option for Keyscan, Keyscan Smart Mobile, and BEST type credentials; the credentials must all have the same batch number and the credential numbers must be in sequence. The batch number may also be referred to as the site code or the facility code.

You cannot use the Block Load Credentials function for any other credential type.

Credentials entered in the Block Load Credentials screen are identified in the Edit Person screen as - Given Name - Block Load, Surname - Credential (batch # and credential number #)

To view steps on how to block load BEST Credentials, please read the following section:

BEST Offline Lock Integration Setup

Procedures

Steps to Block Load Credentials

1. From the Aurora main screen, select the Manage People button > Block Load Credentials.
    - By default all block loaded credentials will have Given Name set as Block Load and Surname set as Credential.
2. Click on the ▼ symbol opposite Type and select the person type if other than Employee; otherwise, leave the setting on Employee and go to the next step.
3. If the credentials are to be activated immediately leave the Active setting enabled (the box has an x) and go to the next step; if you do not want to make the cards active immediately, click in the Active box to the right and disable the setting. The box is blank when disabled.
4. If the credentials require Extended Entry, click in the box to the right. The box has an x when enabled. Extended Entry is normally used when doors have electro-mechanical door operators for persons requiring a longer amount of time to access a door. When Extended Entry is enabled, applicable doors follow the Extended Entry Timer and the Extended Entry Door Held Open settings in the hardware Setup screen.
5. Below the Credential Information heading in the Batch Number field, enter the batch number of the credentials. You can only enter one batch number.
6. In the Card Range text boxes, enter the lowest credential number in the left box and the highest credential number in the right box. The numbers must be in sequence.
7. If the credentials are being issued on a temporary basis, click in the box to the left of Temporary Options. The box has an x when selected.
8. If the card is temporary based on a date range, click on the calendar icon to the right of Valid From.
9. The calendar opens on the current day and month. Do one of the following steps:
    - If the Valid From date is today, select it on the calendar. If applicable, select a time on the right side.
    - If the Valid From date is other than the current day, select the correct start day, or click on the arrows at the top of the calendar and scroll to the desired month and year. Select the day on the calendar. If applicable, select a time on the right side.
10. Click on the calendar icon to the right of Valid To. Do one of the following steps:
    - If the Valid To date is today, select it on the calendar. If applicable, select a time on the right side.

- If the Valid To date is other than the current day, select the correct end day, or click on the arrows at the top of the calendar and scroll to the desired month and year. Select the day on the calendar. If applicable, select a time on the right side.

11. If the card has a usage restriction, enter the maximum number of times the credential may be used in the Limited # Uses text box. If there is no usage restriction, leave the Limited # Uses blank.
12. Under the Site Assignment heading select the first applicable site by clicking in the box to the left of the site name. The box has an x when selected. Select the group from the drop down list. You must select at least one group otherwise the credentials will not have a group access level.
13. For additional site assignments, repeat the above procedure.
14. Click on the Block Load button when you have completed the Block Load Credentials screen.
15. Click on the OK button in the Block Load Complete box.
16. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Visits

Click on the link below for more about the Visits function in Aurora.

About Visitors and Preliminary Setup

Manage System Users

The Manage System User screen is for creating individual log in accounts so you may regulate who can access the Aurora software. Creating and maintaining individual system user accounts protects the integrity of the access control system by preventing unauthorized software access.

The Manage System User screen gives you broad flexibility. How you set individual user accounts greatly depends on the nature of your organization, the levels of security required, and individual responsibilities.

From within the Manage System User screen, you identify the individual, assign a unique log in User Name and Password, and specify permissions.

This help topic provides a general overview on the Manage System User screen. For specific instructions on performing system user account tasks, see Related Topics below or the list of topics under System User Management in the Contents pane at the left.

Generic Keyscan System User Account

Aurora includes a generic Keyscan system user account allowing you to log in to Aurora after it is installed so you can set up your site in the Aurora software and get your access control system functioning. See Related Topics below.

Login Authentication Type

When configuring system user accounts in Aurora, you can set the account for one of the following log in Authentication Types depending on your network environment and Keyscan licenses:

- Keyscan - user must login with a specific Aurora user name and password
- Domain - Aurora uses Windows network domain user name and password*
- Local - Aurora uses Windows local network user name and password*

*Domain log in and local log in require the purchase of the optional Active Directory license from Keyscan.

The three sub-headings below explain the different types of log in methods.

Keyscan Log In

When this option is selected, the system user account must be given a user name and password specifically for logging in to Aurora. When the system user logs in, he or she must enter his or her Aurora system user name and password to open Aurora. The user name must be unique to all other system users.

The first time the user logs in to Aurora, the person will be prompted to create a new password.

Domain Log In

When this option is selected, Aurora uses the assigned Windows user account for log in authentication. Once the system user has logged in to the PC with his or her Windows user name and password on a network domain, he or she can open Aurora directly, by-passing the Aurora log in screen. The PC must be on a network domain to use this log in type.

Local Log In

The same as Domain Logon, except the PC is on a local network.



Whenever Domain or Local is used as a log in type, always be sure to lock the PC while it is unattended; otherwise, anyone can open Aurora and potentially make unauthorized changes to the software settings and compromise your access control system security.

User Information / User Type

Each individual who has an account to access the Aurora software is considered a system user. There are, however, four User Type designations.

- Master
- Administrator
- User
- Visitor Only User

See related topics below for a link to the table outlining the main differences.

Active/Inactive Status

System user accounts are either in an active state or inactive state.

Active Status

The Active status allows the system user to log in to the Aurora software and perform tasks within his or her assigned permissions. By default, when a system user account is created it is set on Active status.

Inactive Status

The Inactive status retains the system user account in the database, but the account is frozen and the individual cannot log in or access the system software while set on the Inactive status.

Cloning a User Type

Select the double arrow **<->** under User Information in order to clone a user's type, permissions and site configurations into a new user/credential.

Sites

System user accounts may be assigned to access multiple sites provided the site is enabled under the Sites heading.

Permissions

After setting the User Type, you can then arbitrarily select specific permissions depending on the individual's responsibilities for operating the Aurora access control management software. Permissions may be further defined by selecting any of the following four sub-permissions:

- View - may only view data/records within the selected function
- Add - may add new data/records within the selected function
- Edit - may alter existing data/records within the selected function
- Delete - may delete data/records within the selected function

You can select one or a combination of the above sub-permissions when assigning the permission to the system user's Aurora log in account.

Example

As an example, if only View was selected under the People and Credentials categories, the log in account would be restricted to looking at people records and credentials accessed from the Manage People menu. The log in account would be unable to create a new record, alter an existing record, or delete a record.

Related Topics

- How to Log On
- System User Types
- Default Keyscan System User Account
- Create a System User Account

System User Examples

Below are two examples of system user accounts. The first example outlines one site with three system user accounts. The second example outlines two sites with four system user accounts. In both examples, all system user accounts have specific permissions related to their overall access control system responsibilities.

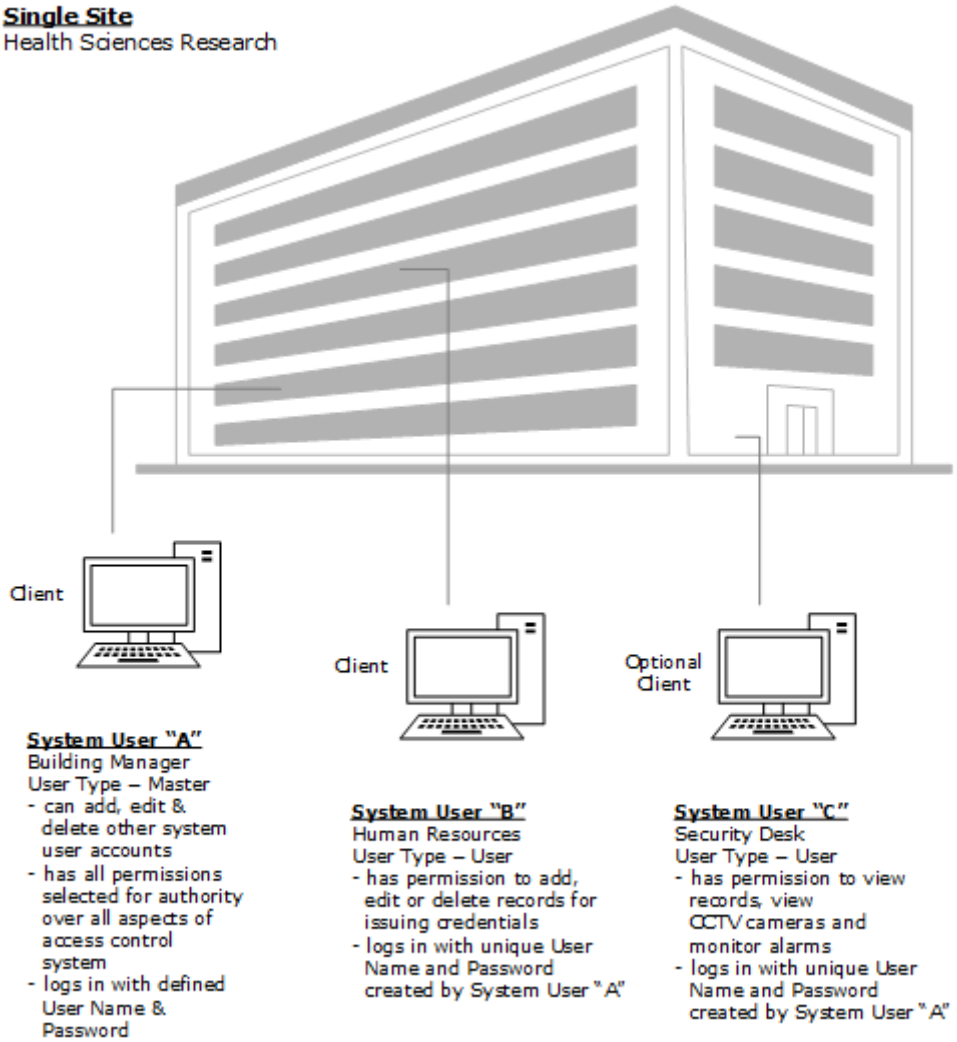
One Site

System User A has a Master account designation. This person is responsible for operating and maintaining the entire access control system.

System User B is in Human Resources and has permission to add, edit, or delete credential records and issue credentials.

System User C works at the security desk. This person has permission to view credential records and view CCTV cameras.

One Site with 3 System User Accounts



Two Sites

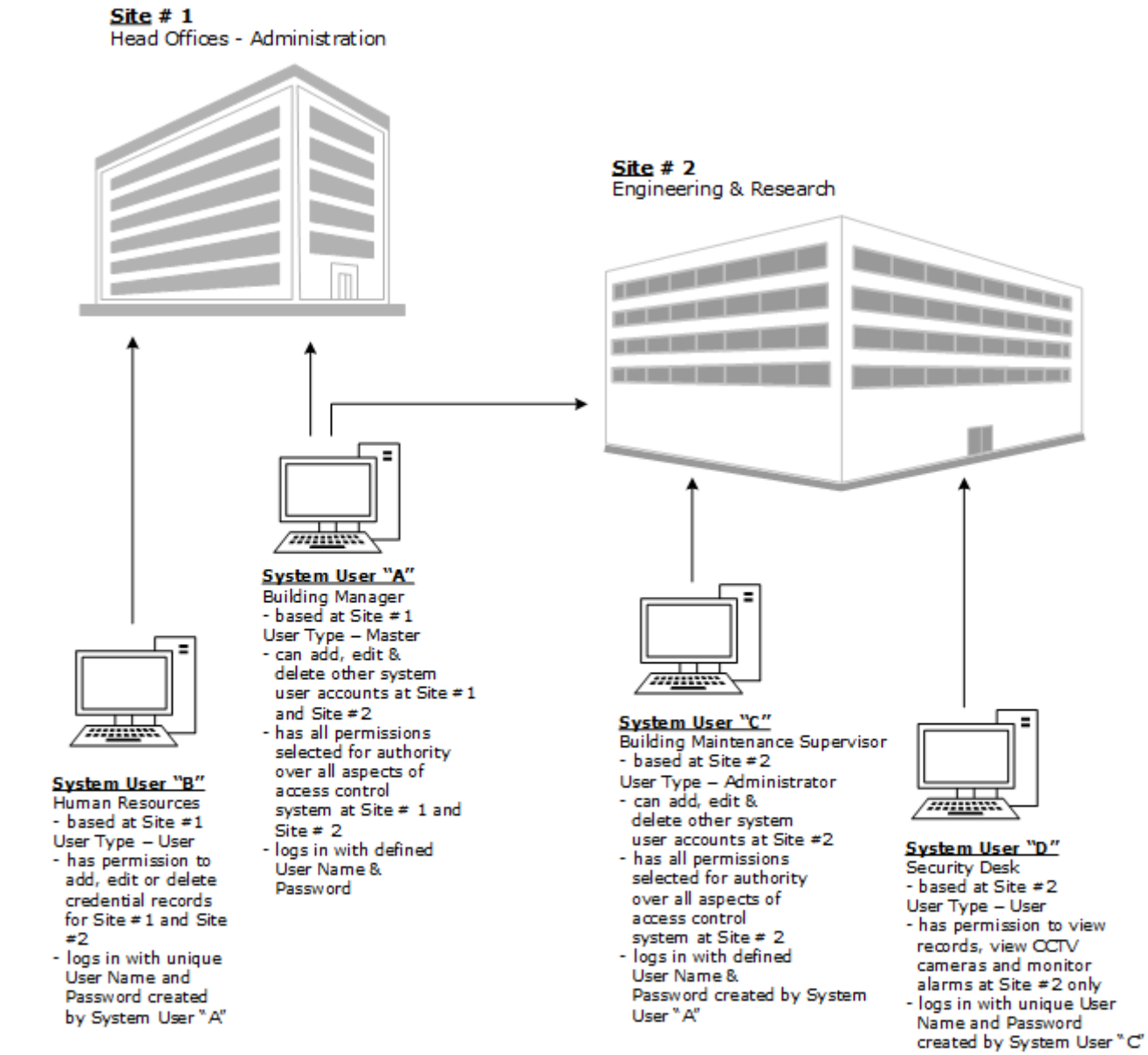
System User A has a Master account designation. This person is responsible for operating and maintaining the entire access control system for both site #1 - the head office/administration building and site #2 - the engineering and research building.

System User B is designated as a User account. System User B is in Human Resources and has permission to add, edit, or delete credential records and issue credentials at Site #1 and Site #2.

System User C has an Administrator account designation. This person is responsible for site #2.

System User D is designated as a User account and is responsible for security at site #2.

Two Sites with 4 System User Accounts



System User Types

Each individual who has a log in account to access the Aurora software is considered a system user. There are, however, four system user designations. The following highlights the functional differences between those four designations.

System User Types / Default Permissions			
Master includes all Administrator functions plus:	**Administrator** includes all User functions plus:	**User**	**Visitor Only User**
Add / delete sites Application utilities - Person types - Application settings - Communication servers - SMTP settings - Disable logging reasons Database maintenance - Backup - Restore - Compress - Re-index - Purge - Export daily counts Scheduled Tasks - Database backup only Software registration Default device images Device status images Custom transaction names Site setup report* Memory viewer Clear packets* Master holidays* Optional field management*	Manage users* - Reset user passwords - Change user passwords System log report* Export people* Import people* Block Load Credentials* Assign optional fields to sites* Schedule tasks - reports only Full panel upload* View / edit PINs* Site setup report*	Permissions are discretionary based on designated user responsibilities Excluded from administrator and master permissions	Restricted by the following rules: 1) may only select the Visitor option under the Type field in the Add Person and Edit Person screens (applies to any Person Type with a Visitor - Yes status in the Application Utilities screen, as well) 2) may only assign a credential to a group in the in the Add Person and Edit Person screens that has a Visitor Group - Yes designation in the Group Setup screen providing the relevant Credentials permissions are set as well 3) has 2 optional sub permissions to restrict viewing and/or editing visitor types only Permissions are discretionary based on designated user responsibilities Excluded from administrator and master permissions
* Only unlocks the permission - must be manually selected or the associated category must be selected under the Permissions heading before it is enabled **Note:** An Administrator cannot change a Master User.			

Create a System User Account

A system user can be assigned with a Master, Administrator, User or Visitor Only User designation depending on the desired range of functionality.

You must have 1 system user that has a Master designation. This can be the same person for all sites or several persons depending on the structure of your organization. On a multiple site configuration, only a Master designation can create or assign system user accounts to another site.

Domain and Local log in require the purchase of an Active Directory license.

If you are using complex passwords, be sure the password complies with the required character conventions. See Related Topics below.

Procedures

Steps to Create a User Account

1. From the Client main screen, select the Settings button > Manage System User.
2. On the User Search directory screen, select the Add User button.
3. Below Log in Information, select the ▼ symbol opposite Authentication Type and choose one of the following options depending on your license and network configuration:
    - Keyscan - click inside the User Name text box, enter a name, press the Tab key, enter a password in the Password text box, press the Tab key and re-enter the password. Passwords are case sensitive and have no maximum. Passwords may consist of alpha, numeric or special characters.
    - Domain - select ▼ symbol opposite User Name and select the name of the person from the network domain drop down list.
    - Local - select ▼ symbol opposite User Name and select the name of the person/PC name on the local network drop down list.
4. Below User Information, click inside the Given Name text box and enter the user's first name.
5. Click inside the Surname Name text box and enter the user's last name.
6. Enter the user's e-mail address.
7. Opposite User Type, click on the ▼ symbol and select the designated User Type for this individual.
    - Unless the system user account is not being activated immediately, leave it set on Active; otherwise click on the Active button to change the status to Inactive.
8. Below Sites, if you have more than one site, select the sites the user will have permission to access.
9. To insert the system user's photo, move the cursor over the silhouette in the upper left and click on the + button.
10. Navigate to the file folder with the image and select the file.
11. Click on the Open button.
12. From the Image Editor, click on the save icon.
13. Below Permissions, select the desired permissions depending on the range of functions to be performed. When selected the box has an x.
    - ▶ indicates the permission has sub-levels of permissions; click on the symbol to list the sub-levels of permissions
    - As an option, you can use the Quick Permissions buttons to set a desired range or type of permissions

14. Select the Save button.
15. To create another system user account, click on the Back button and then click on the Add User button on the User Search screen.
16. When you have completed creating system user accounts, click on the Back button until you are returned at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

If the Authentication Type selected is Domain or Local, the system user may have to log off and log back on Windows in order to access the Client software.

When the system user log's on Aurora for the first time, he or she will be prompted to enter a new password.

Related Topics

- Manage System Users
- System User Types
- Complex Passwords
- Image Editor
- Edit a User Account
- Change a System User's Password
- De-activate/Delete a System User Account
- Enforce Complex Passwords

User Search Directory

The User Search directory screen lists all system user accounts. Use this screen to not only search for system users, but also to access user accounts for adding, editing, activating/de-activating, or deleting system users.

Depending on your account's permissions, you may be prohibited from performing some of the above mentioned procedures or viewing accounts at certain sites.

Procedures

Overview of User Search Directory

- Add User - select to open the Manage System User screen and create a new system user account
- Refresh - select to update the User Search directory
- List of User Accounts
    - User Name - lists the user name the individual enters when logging on to Aurora
    - Given Name - lists the system user's first name
    - Surname - lists the system user's last name
    - E-mail - lists the person's e-mail address
    - User Type - lists the system user's designated User Type – Master, Administrator, User or Visitor Only User
    - Delete button - erases the system user account from the database preventing the individual for accessing the Aurora software
    - Show Photos - displays a system user photo if inserted on the system user account
    - Back - returns to the previously viewed screen

Edit a System User Account

Periodically, you may have to amend a system user account, such as altering permissions, changing the Authentication Type or making other changes. Follow the instructions below.

Procedures

Steps to Edit a User Account

1. From the Client main screen, select the Settings button > Manage System User.
2. From the User Search directory, locate and select the system user account you are editing.
3. From the System User Account screen, make the necessary changes.
4. Select the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Change a System User's Password

From time to time, you may have to change a system user's password or you may enforce password changes after a certain period of time as a security protocol. Changing passwords does not apply if the system user's account is set on Local or Domain under the Authentication Type field.

Reset a Forgotten Password

In the event a system user has forgotten his or her password, follow the steps Reset a Forgotten Password outlined under procedures. The steps differ from the Change the System User's Password procedures.

Procedures

Change the System User's Password

1. From the Client main screen, select the Settings button > Manage System User.
2. From the User Search directory, locate and double click on the system user account.
3. Below Login Information, click on the Force Change Password button.
4. Select the Save button.
5. Select the Back button until you reach the main screen.
6. Opposite the logged on account name in the upper right of the Aurora main screen, click on the symbol and select Log Off.
7. From Aurora's Log In screen, enter the Keyscan user name of the account whose password was reset.
8. Press the Tab key.
9. Enter the current password.
10. Press the Tab key.
11. Enter the new password.
12. Select the key button.

Reset a Forgotten Password

1. From the Client main screen, select the Settings button > Manage System User.
2. From the User Search directory, locate and double click on the system user account.
3. Below Login Information, click on the Change Forgotten Password button.
4. In the Password text box, enter the new password.
5. In the Re-Enter Password, enter the same password as in step 4.
6. Click on the Save button.
7. Click on the Back button until you are returned to the main screen or the Navigation History  symbol for a previously viewed screen.

Related Topic

Enforce Complex Passwords

Deactivate/Delete System User Accounts

Periodically, you may find that you have to either delete the account of a system user who has perhaps left your organization or been assigned other responsibilities or de-activate the account of a system user who has taken an extended vacation or a leave of absence.

- Deleting the system user permanently removes the account from the database.
- De-activating the system user account sets the status to Inactive, and retains the account in the database. The system user cannot log in while his or her account is inactive.

Follow the appropriate procedures below depending on whether you are de-activating or deleting the system user's account.

Procedures

Steps to Delete a User Account

1. From the Client main screen, select the Settings button > Manage System User.
2. From the User Search directory, locate the system user account.
3. Click on the Delete (waste bin) button.
4. Click on the Yes button in the Delete User confirmation box.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to De-activate a User Account

1. From the Client main screen, select the Application Settings button > Manage System User.
2. From the User Search directory, locate and double click on the system user account.
3. Below User Information, click on the Active button. The button changes to Inactive.
4. Click on the Save button.
5. Click on the Exit button or the navigation history symbol.

Note +

To restore the user account to active status, follow the Steps to De-activate a User Account. When the Inactive button is selected it changes back to Active.

Default Keyscan User Account

When Aurora is first installed, Keyscan provides a default user account Keyscan with a Master designation. The User Name and Password are as follows:

- User Name - Keyscan
- Password - KEYSCAN (upper case characters)

To use the generic Keyscan account for logging in, enter the user name and password as shown above, and then select the button with the key symbol at the right of the password text box.

You can continue logging in with the Keyscan generic system user account. However, Keyscan recommends that you create specific system user accounts for each individual who will have responsibilities for monitoring and managing the access control system. Creating unique system user accounts ensures better security protocols since everyone is regulated by their specific permissions and you can audit user activity in the system log if anything questionable happens.

Once you have created your own user accounts and use them to log in, Keyscan suggests de-activating the generic Keyscan account after you have become familiar with the Aurora software.

See Deactivate/Delete System User Accounts for procedures.

Auto Shutdown Time

The Auto Shutdown Time function automatically closes the software and logs the User out completely after a specified amount of time. The Auto Shutdown Time will trigger when the computer sits idle for the time, in minutes, specified in the User Settings in the Aurora software client.

Note: Any unsaved data will be lost if the Auto Shutdown Time triggers. The User will be forced to re-launch the application and re-enter their login credentials.

Procedure

Steps to Set Auto Shutdown Time

1. From the Client main screen, select the Settings button > Application Utilities.
    - The settings in the Application Utilities screen apply to all sites
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Under the User Settings sub-menu, fill in the Auto Shutdown Time field with the desired time in minutes (between 1 - 999). Inputting a value of 0 (set by default) will render the feature inactive.
4. Select the Save button.

About the Global Card Template Editor

The Global Card Template Editor designs templates for printing photo ID badges or access credentials. The editor offers a full complement of tools and features for professionally designed ID badges:

- Insert graphics such as company logos
- Draw objects with line and shape tools
- Insert database fields including given name, surname
- Insert the individual’s on-file photo image
- Insert bar codes from a full range of industry-standard formats
- Edit and modify text with custom attributes
- Insert a background photo or texture
- Assign card templates to specific sites

Design a Card Template Tutorial

Included with the Aurora Software Installation files in the Aurora Documents folder is a PDF version of a tutorial on designing a basic card template for photo ID badges or access credentials. The tutorial takes you through the steps of creating a basic template and shows you how to use various tools.

A Note to System VII Users

If you have upgraded from System VII to Aurora, the Global Card Template Editor is accessed directly within the Client module from the Settings menu.

Manage Global Card Template Editor screen with a Card Template



Related Topics

Global Card Template Editor Tools

Global Card Template Editor Tools

The global card template editor has two tool sets: text tools and background tools. Each set of tools is accessible by selecting the desired tab - Text or Background - under the Tools heading. The functions of the text and background tools are outlined in the table.

About the Select Tool

The global card template editor text and background tool sets each have a select tool. Each select tool can only select an object for editing, re-sizing, moving, or deleting from its respective tool set.

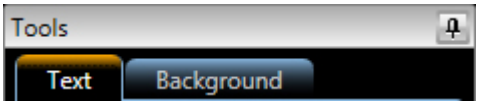
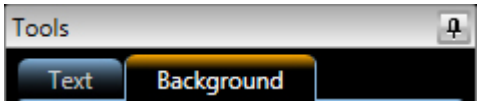
- The text select tool can only select objects on the template created by a text tool
- The background select tool can only select objects on the template created by a background tool

About the Snap and Grid Tools

The snap and grid tools operate in the same fashion as a switch - click on either one to turn it on, click on it again to turn it off.

- Snap or Grid - Off - dark blue
- Snap or Grid - On - light blue

The functions of the text and background tools are outlined in the table.

Tools - Text / Background	
	
Text Select by clicking on the Text tab. All the associated text tools are accessible for creating and editing text on the template work area.	**Background** Select by clicking on the Background tab. All the associated background tools are accessible for drawing shapes and inserting images or barcodes on the template work area.
 **Text Select Tool** Use to select a text-related object such as a text box, placeholder, or label currently on the card template.	 **Background Select Tool** Use to select a background-related object, such as a photo, shape, or line currently on the card template.
 **Text Editor Tool** Inserts a text box for adding text on the card template.	 **Import Background Tool** Use to import an image which the template editor scales to the full size of the background. Use this tool if inserting a floor plan or map created in another application such as Visio or similar drawing application.
 **Horizontal Alignment - Left** Left aligns the text in the selected text box.	 **Fill Background Tool** Use to paint the entire background with the colour displayed in Color 1 palette box.



Horizontal Alignment - Centre

Centre aligns the text in the selected text box.



Horizontal Alignment - Right

Right aligns the text in the selected text box.



Vertical Alignment - Top

Aligns the text to the top of the selected text box.



Vertical Alignment - Middle

Aligns the text to the middle of the selected text box.



Vertical Alignment - Bottom

Aligns the text to the bottom of the selected text box.



Color 1

Indicates the current colour selection for text. Click on the box to open the palette and select an alternate colour.



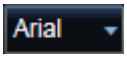
Color 2 Text Tool

Not applicable as a text tool.



Font Size Tool

Indicates the current font size selection for inserting text. Click on the ▼ symbol to open the drop down box and select an alternate font size.



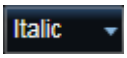
Font Tool

Indicates the current font selection. To change fonts, click on the ▼ symbol and select an available font from the drop down box.



Font Weight Tool

Indicates the current font weight selection. To change the font weight, click on the ▼ symbol and select an available font weight from the drop down box.



Font Style Tool

Indicates the current font style selection. To change the font style, click on the ▼ symbol and select an available font style from the drop down box.



Delete Background Tool

Use to delete the current background.



Rectangle Tool

Use to draw a rectangle or square.



Ellipse Tool

Use to draw an ellipse or circle.



Triangle Tool

Use to draw a triangle.



Free-form Line Tool

Use to draw a line free-hand.



Line Tool

Use to draw a straight line.



Multi-line Tool

Use to draw multiple straight connecting lines.



Add Photo Tool

Imports an image for placement on the template.



Personal Photo Frame Tool

Use to frame an area on the template where the person's photo is inserted on his or her credential or badge.



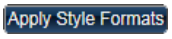
Bar Code Tool

Inserts a bar code on the template.



Color 1 Tool

Indicates the current colour selection for a line or the border of a rectangle, ellipse or triangle. Click on the box to open the palette and select an alternate colour.



Apply Style Formats

Selecting the Apply Style Formats button after any changes are made to the font properties resets the defaults to those currently selected. The Apply Style Formats is dimmed and unavailable until any of the font properties are altered.



Color 2 Tool

Indicates the current colour selection for the fill of a rectangle, ellipse or triangle. Click on the box to open the palette and select an alternate colour.



Grid Tool

Lays out a grid over the work area for aligning text and objects on the card template.



Line Thickness Tool

Indicates the current line thickness or border thickness of a rectangle, ellipse or triangle. Click on the ▼ symbol to open the drop down box and select an alternate line thickness.



Snap Tool

Positions the selected text box or object at intersecting grid lines.



Grid Tool

Lays out a grid over the work area for aligning text and objects on the card template.



Snap Tool

Positions the selected text box or object at intersecting grid lines.

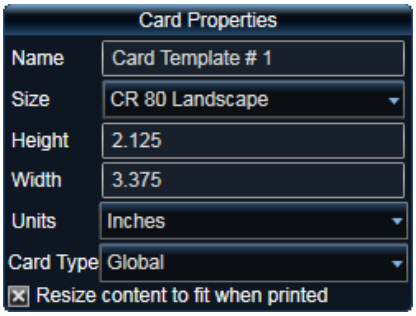
Open - New Buttons

The following outlines the open, new, save, undo and redo functions in the Manage Global Card Templates editor. These functions are always visible regardless of the type of tools selected.

Button	Name and Function
	**Open Card Template** Select to open an existing card template.
	**New Badge Template** Select to create a new card template. See Card Properties.
	**Clone Current Card Template** Select to make a duplicate of the template currently open in the template editor.
	**Undo** Select to delete the last action or actions on the template work area.
	**Redo** Select to recover the last action or actions if the Undo button was previously selected.
	Note on undo and redo - only applies to actions that have occurred after the last save.

Card Properties

Use the card properties fields when creating a new template as outlined.



Name

Identifies the name of the template file. For a new template file, click in the text box and enter a file name for the card template.

Size

Indicates the card size CR-80 or CR-79 in landscape or portrait orientation or Custom. See About CR-80 & CR-79 or Custom Size below.

Height

Indicates the height dimension in inches of the template.

Width

Indicates the width in inches of the template.

Units

Displays the card dimensions in: inches, millimeters, or centimeters.

Card Type

Determines the type of template - global, site or visit - see Card Type below for more information.

Re-size Content

Pre-selected by default to keep placeholder fields within the confines of the card when printed.

Landscape or Portrait Orientation

To configure the card template for landscape of portrait orientation, follow this general guideline:

- Landscape - enter the longer card dimension in the Width text box
- Portrait - enter the longer dimension in the Height text box

About CR-80 & CR-79

CR-80 and CR-79 are industry-standard card sizes with the following dimensions:

- CR-80 - 3.375" x 2.125"
- CR-79 - 3.303" x 2.051"

If you have purchased printable proximity cards or photo badge cards from Keyscan, use the CR-80 dimensions. If you have purchased your cards from elsewhere either measure the cards or consult with the distributor.

The PVC adhesive-back cards sold by Keyscan are CR-79 and are designed to be affixed to a CR-80 proximity card. As the CR-79 is slightly smaller, the edge of the adhesive back card is recessed making it extremely difficult to peel off the proximity card.

Custom Size

If using a card size other than CR-80 and CR-79, select the Custom option for the Size field and enter the dimensions of the card template in the height and width boxes. Be sure you specify the correct units - inches, millimeters or centimeters.

Card Type

The card type allows designing card templates as global templates, site templates or visit templates. Selecting the Card Type: Global, Site or Visits, determines which of the database fields are available for insertion on the template as listed below.

The three card type options provide you with additional latitude in designing templates. Which card type selected will depend on the information you require printed on the photo badge. As an example if you issue visitors with photo badges, selecting the Visits card type allows inserting specific fields related to visit details. You may have to experiment with the three card types to view the differences and determine which card types work for your particular template applications.

Global

- Person Field Placeholders & Labels
- Credential Field Placeholders & Labels
- [Common] Optional Field Placeholders & Labels

Site

- Person Field Placeholders & Labels
- Credential Field Placeholders & Labels
- [Common] Optional Field Placeholders & Labels
- Site Optional Fields Placeholders & Labels

Visit

- Person Field Placeholders & Labels
- [Common] Optional Field Placeholders & Labels
- Site Optional Fields Placeholders & Labels
- Visit Placeholders & Labels
    - Arrival Time/Departure Time

The card type selected also affects where the card template is accessed from when printing a photo badge. Select the Print Photo Badges link below Related Topics for more information.

Related Topics

Common Fields - Optional & Site

Print Photo Badges

Database Fields - Placeholders and Labels

The text tool set includes a list of database fields. These are the same database fields used on the Edit Person screen. You specify which of these fields you want included on the photo badges or access cards by inserting them on the template. When the template is loaded for printing in the Add Person screen, each person's specific information is printed on the photo badge or access card.

When inserting database fields, you have the option of selecting either placeholders or labels. The difference is explained below.

Placeholders

Selecting a database placeholder inserts only the data entry for the specified field when the card is printed. If the field is blank in the credential record the field will not be printed on the card.

Labels

Selecting a label inserts a text box with the label name on the template. You can use the label to identify fields on the template and add the corresponding placeholder to the right as shown in the lower row in the table below, or use it as a text box to insert text on the template.

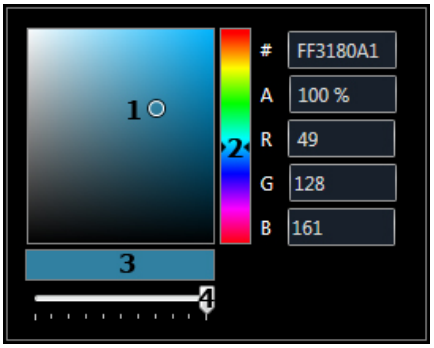
Database Fields	Specific Fields
	**Person Fields - Placeholders or labels** Given Name Surname Middle Name (if enabled) **Credential Fields - Placeholders or Labels** Card Number Description **Optional Field - Placeholders or Labels** User defined fields
Sample Template with <<Placeholders>>	**Template Loaded in Add Person Screen**
	
Sample Template with Labels & <<Placeholders>>	**Template Loaded in Add Person Screen**


KEYSCAN
ACCESS CONTROL SYSTEMS
A Member of the Kaba Group
Given Name <<Given Name>>
Surname <<Surname>>
Department <<Department>>
901 Burns St. E., Whitby, Ontario L1N 0E6
KEYSCAN
ACCESS CONTROL SYSTEMS
AURORA


KEYSCAN
ACCESS CONTROL SYSTEMS
A Member of the Kaba Group
Given Name Elizabeth
Surname Schumann
Department Finance
901 Burns St. E., Whitby, Ontario L1N 0E6

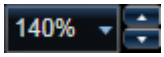
Colour Selection

When Color 1 or Color 2 are selected on the applicable text or background layers, the colour palette opens and you can adjust or change the colour, hue or transparency of the object or text inserted on the template work area.

Colour Palette	Colour, Hue, Transparency Selection
	1 - Circle indicates current hue selection - To change the hue, click and drag the circle to the desired hue 2 - Colour palette with > < arrows indicating current colour selection - To change colour, click and drag the arrows to the desired colour 3 - Opacity indicator 4 - Transparency/opacity slide - To change transparency, click and drag opacity/transparency slide left or right to desired setting # - indicates the hexadecimal color value - the first two characters represent the opacity value and the last six characters represent color value A - indicates the color's opacity percentage (%). R, G, B - indicates the red, green and blue values for the selected color

Template View Selector

The global card template editor allows zooming in or out to enlarge or shrink the view of the template.



% - indicates the current template magnification

Click on the symbol to the immediate right of the magnification % to open a drop down list for a range of selectable views - 20% to 200%.

Clicking on the up or down arrows to the far right increase (up) or decrease (down) in increments of 20% each time an arrow is clicked.

Supported Barcodes

Keyscan supports the following barcode types in the Manage Global Card Templates editor if you employ barcodes for access control or other non-access control functions. If you are using barcodes for access control with EZ Barcode or BR7 barcode readers, refer to the MISC-BRC Barcode Interface document on the Keyscan Product Documentation Library CD for supported barcode types. For non-access control applications, refer to the scanner manufacturer's literature for supported barcode types. When selecting a barcode in the Manage Global Card Template editor you must specify the barcode type currently in use. You cannot arbitrarily select any barcode.

The Manage Global Card Templates editor supports the following barcodes:

- Code 11
- Code 128
- 128A
- 128B
- 128C
- 25 Interleaved (Interleaved 2 of 5)
- 25 Standard
- Code 39
- Code 39 Extended
- Coda Bar
- EAN13
- EAN8
- MSI
- PDF417
- Postnet
- QR
- UPC-A
- UPC-E
- UPC Supplement 2
- UPC Supplement 5

This list is subject to change without notice. Refer to the drop down list for supported barcode types in the Barcode Setup screen which is accessed by selecting the Barcode button in manage global card templates editor.

Related Topics

Insert a Barcode

Create a New Card Template

Procedure

Steps to Create a New Card Template

1. From the Client main screen, select the Settings button > Manage Global Card Templates.
2. From the Manage Global Card Templates screen, click on the New Card Template  button near the bottom. When you mouse over the button a pop-up displays New Card Template.
3. Below Card Properties, click inside the Name text box and enter a name for the badge template.
4. Opposite Size, click on the ▼ symbol to the right and select the card type and orientation - landscape or portrait.
    - To create a template for a card size other than CR79 or CR80, select Custom and enter the applicable dimensions of the card template in the Height and Width boxes.
5. Opposite Units, to display the template in unit measurements other than the type currently listed, click on the ▼ symbol to the right and select the desired option.
6. Opposite Card Type, Global is the default setting. If the template requires site optional or visitor database fields, click on the ▼ symbol to the right and select the desired option.
    - The selection of Card Type affects which of the Aurora database fields are available for insertion on the card template. For more information, select the link Card Properties below Related Topics.
7. Select the Save button. The badge template is saved to the Keyscan database.

Related Topic

Card Properties

Open an Existing Card Template

Procedure

Steps to Open an Existing Card Template

1. From the Client main screen, select the Settings button > Manage Global Card Templates.
2. From the Manage Global Card Templates screen, click on the open card template  button in the lower area of the tools screen.
3. From the pop up list, select the template to open.

Draw a Rectangle, Ellipse, Triangle - Cards

If you are unfamiliar with drawing objects, experiment with the draw tools on the template work area until you have a better grasp of how they function. After you have drawn several objects, select the object and press the Delete key to remove it.

Procedure

Steps to Draw a Background Object - rectangle, ellipse, triangle

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select one: the rectangle tool , the ellipse tool , or the triangle tool .
    - All three tools behave in the same manner by clicking and dragging.
3. Position the cursor over the desired area on the template work area.
4. Click and drag in a top to bottom, left to right motion until the object reaches the desired size and then release the pointing device or mouse.
5. The object is currently selected as indicated by the blue marquis surrounding it.
6. While it is selected you can change the line thickness, line colour and the fill colour as follows:
    - Line thickness - select the ▼ symbol opposite the line thickness tool and select an option from the drop down list.
    - Line color - select Color 1 and change the color or hue by adjusting the palette settings.
    - Fill color - select Color 2 and change the fill color or hue by adjusting the palette settings.

For more information about moving, rotating or scaling an object, select the link below.

Related Topics

Move, Rotate, or Scale an Object

Draw a Free-form Line

Procedure

Steps to Draw a Free-form Line

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the free-form line tool (pencil) .
3. Position the cursor over the desired area of the template work area.
4. Click and drag to create the line.
5. You can change the line thickness or line colour. First click on the select tool, then select the line on the template work area. While it is selected, do either of the following steps:
    - Line thickness - select the ▼ symbol opposite the line thickness tool and select an option from the drop down list.
    - Line color - select Color 1 and change the color or hue by adjusting the palette settings

Draw a Single Line

Procedure

Steps to Draw a Single Line

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the line tool .
3. Position the cursor at the desired spot on the template work area where the line is to start.
4. Click and drag to create the straight line.
5. You can change the line thickness or line colour. First click on the select tool, then select the line on the template work area. While it is selected, do either of the following steps:
    - Line thickness - select the ▼ symbol opposite the line thickness tool and select an option from the drop down list.
    - Line color - select Color 1 and change the color or hue by adjusting the palette settings

Draw Multiple Angled Lines

Procedure

Steps to Draw a Multiple Angled Line

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the multi-line tool .
3. Position the cursor at the desired spot on the template work area where the line is to start.
4. Click and drag to create the first line segment.
5. Release the mouse or pointing device while positioned at the end of the line segment, then click the mouse or pointing device and draw the next line segment. Repeat using the same technique until the continuous multiple angled lines have been drawn.
6. You can change the line thickness or line colour. First click on the select tool, then select the line on the template work area. While it is selected, do either of the following steps:
    - Line thickness - select the ▼ symbol opposite the line thickness tool and select an option from the drop down list.
    - Line color - select Color 1 and change the color or hue by adjusting the palette settings

Insert a Background Image

These instructions are when you are placing an image on the template that will cover the entire background of the card template. The Manage Global Card Template editor will scale the image to fit the dimensions of the template. You may find that you have to crop or re-size the image in a photo editor.

Procedures

Steps to Insert a Background Image

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the background image tool  below Background Fill.
3. From the Open dialog box, navigate to the folder location with the image file you are importing to the global card template editor.
4. Select the file.
5. Click on the Open button.

Note: A transparent GIF image does not support background transparency and will result in a black background.

Insert an Image

These instructions are when you are placing an image on the template such as a logo that will only cover a portion of the template. You may have to re-size the image in a photo editor to obtain the desired results when inserting an image on the template.

This function is not for inserting images of credential holders. See Related Topics below and select Insert a Personal Photo Frame

Procedures

Steps to Insert an Image

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the add photo  tool.
3. From the Open dialog box, navigate to the folder location with the image file you are importing to the global card template editor.
4. Select the file.
5. Click on the Open button.

For more information about moving an image (object), select the link below.

Related Topics

Insert a Personal Photo Frame

Move, Rotate, or Scale an Object

Insert Text

Procedure

Steps to Insert Text

1. Ensure the Text tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the text editor tool .
3. Position the cursor over the desired area on the template work area.
4. Click and drag in a top to bottom, left to right motion to create a text box until it is the desired size. Then release the pointing device or mouse.
5. With the text box selected as indicated by the blue marquis surrounding it, insert the cursor in the text box in front of the word Label, click and drag so Label is highlighted.
6. Press the Delete key to clear the text box.
7. Enter the text.
    - Tip - you can use the text alignment tools to reposition the fields within the box.
8. While it is selected you can change the text color or font properties as follows:
    - Text Color - select Color 1 and change the color or hue by adjusting the palette settings.
    - Font Size - select the font size tool and select the desired setting.
    - Font - click on the ▼ symbol to the left of the displayed font and select a font from the drop down list
    - Font Weight - click on the ▼ symbol to the left of the displayed font weight and select a weight option from the drop down list
    - Font Style - click on the ▼ symbol to the left of the displayed font style and select a style option from the drop down list
9. Click the cursor outside the text box to close it.

Related Topic

Text Alignment

Insert a Barcode

The global card template editor gives you the option of placing barcodes on photo ID badges or access cards. You select the type of barcode in the Barcode Setup screen and assign it one or more common optional fields. The barcode is then populated with the data from the selected common optional fields on the photo ID badges or access cards for authentication when credential holders present their ID badges or access cards at barcode readers or scanners.

If the assigned common optional fields are blank on any credential holder's record, a barcode will not be printed on the actual photo ID badge or access card. As an option, you can create a specific common optional field called Barcode and implement your own barcode identification numbering system.

As barcodes come in many variations and specifications, Keyscan can only provide some general guidelines when inserting barcodes on photo ID badges or access cards. Refer to your barcode literature for specific details concerning size requirements, maximum distance from the edge of the card for scanning and any other specifications.

Barcode Types, Size, and Data Detail

Supported barcode types include linear barcodes, made up of lines and spaces of varying widths, and matrix barcodes, made from a rectangular grid of cells.

Linear Barcode Example	Matrix Barcode Example
	

When you are inserting a barcode on the template, you will have to be aware of the barcode's specifications with respect to its size and in some cases color. As an example, the matrix barcode on the right - Barcode QR - is defaulted to black and the color cannot be changed. Some barcodes must be sized to within certain tolerances. You may require a sample printed barcode for sizing requirements when inserting a barcode on the template.

As you can assign multiple optional fields to the barcode, depending on how much data is in the assigned Common Optional fields, you could inadvertently extend the barcode beyond the dimensions of the template, in which case you will not be unable to open the template for printing credentials or ID badges in the Edit Person screen. When assigning common optional fields, Keyscan suggests limiting the number of fields and choosing fields that authenticate each individual with a unique identity. As suggested above, you can create an optional barcode field and implement your own barcode identification numbering system.

Bar Code Measurements

When completing the Bar Code Setup screen, you must specify the exact size of the barcode as measured from an actual printed bar code in use. Measure the width from the outer edges of the left and right bars. Measure the height as follows depending on the bar code configuration:

- the top of the bars to the bottom of the bars
- the top of the bars to the bottom of the alpha or numeric characters

WARNING! Do not stretch, shrink, or scale the barcode when it is inserted on the template work area. The width of each bar represents a specific value. Altering the dimensions of the barcode will distort the bars and may cause an improper read when a card is scanned.



Checksum

Checksum, which may also be referred to as check digit, is the number on the far right of the barcode. The checksum verifies the information on the barcode is correct. Some codes require a checksum, which is indicated by the barcode manufacturer.

Barcode Security for Access Control Applications

If using linear barcodes for access control applications, Keyscan recommends placing a background color under the barcode to act as a mask and prevent photocopying, thereby reducing potential security problems. Keyscan suggests creating a background color with the following red, green and blue (RGB) values which still allows infrared scanning but prevents the barcode from being photocopied.

- Red - R = 10
- Green - G = 0
- Blue - B = 0

The barcode must be black with the following RGB values Red = 0, Green = 0, Blue = 0 for the background color to prevent photocopying.

Procedure

Steps to Insert a Barcode

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select Color 1, and choose a color for the barcode.
    - If implementing a background color to mask the barcode, ensure that the barcode color selected is black by dragging the circle on the color selector to the bottom right corner. Black has the following RGB values Red = 0, Green = 0, Blue = 0.
3. Select the Barcode tool 

.
4. Position the cursor over the area where you are inserting the barcode. Click and drag in a top to bottom, left to right motion to create a marquis representing the approximate size for the barcode. Release the mouse or pointing device.
5. From the Barcode Setup screen, click on the ▼ symbol and select the type of barcode from the list of supported barcodes.
    - Remember, you cannot arbitrarily pick any barcode. You must select the barcode in use and it must be sized within the barcode's tolerance and at a position on the template that will allow the reader to scan the barcode.
6. If you selected "Barcode QR" as the Barcode type, click on the ▼ symbol and select an appropriate QR Barcode version.

Note: Aurora currently supports versions 1 to 40. Research is recommended to best choose a barcode version that suits your needs. This will depend on how much data you intend to include in the barcode and the physical size you would like the barcode to be on their card template

7. If the text in the barcode is to remain out of sight on the actual badge, click in the box to the left of Hide Bar Code Text.
8. If the barcode requires a checksum or check digit, click in the box to the left of Embed Checksum Within Barcode. Checking this option will include the checksum value when the barcode lines are generated.
9. If the text for the checksum should be visible, click in the box to the left of Display Checksum.

   Note: The Display Checksum option only shows the checksum value. For the value to physically be within the barcode itself, the Embed Checksum Within Barcode option must be selected.

9. Under Optional Fields, click in the box to the left of the optional field or fields used as the identifying properties of the barcode.

   Alternatively, select Site Optional Fields instead of Common Optional Fields to make each optional field site-specific within the barcode. This feature can only be used with Site or Visit card types.

10. Opposite Units, select the ▼ symbol and select the barcode unit of measurement: inches, centimeters or millimeters.
11. Enter the height.
12. Enter the width.
13. Click on the OK button.
14. The template editor inserts the barcode pre-selected on the template work area. If required, you can re-position it by locating the mouse or pointing device over the barcode, the cursor changes to four arrows, and dragging it to the desired area on the template.

Steps to Place a Security Mask on the Barcode

These steps are based on creating and placing the mask immediately following the insertion of a barcode. The barcode must be black with the following RGB values - Red = 0, Green = 0, Blue = 0.

Note: While the barcode itself must have the above RGB values, the field behind it can be any colour. However, some credential types do not support colouration behind the barcode. Double-check the credential type before adding colour.

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select Color 1.
3. Either drag the circle in the color selector to the lower right corner until the R, G and B boxes have the following values:
   - Red (R)=10, Green (G)=0, Blue (B)=0
   - When you drag the circle on the color selector you will notice the RGB values change.
4. Ensure that the color is at full opacity, A is at 100%; otherwise drag the transparency slide to the far right until A is at 100%.
5. Select Color 2 and repeat the preceding two steps.
6. Click on the rectangle tool.
7. Position the cursor at the upper left corner of the bar code and click and drag to the lower right corner of the barcode so that it is now completely masked.
8. With the rectangle still selected, right click and select Move Back so the rectangle is on the layer below the barcode.

Insert Person/Credential/Optional Fields from the Database

The person, credential, and optional fields have a placeholder option and a labels option when inserting a database field on the template:

- Placeholder - when selected, the data entered on the person's record is inserted on the photo badge
    - Example Placeholder Surname: Smith
- Labels - when selected, the field label followed by the data entered on the person's record is inserted on the photo badge
    - Example Label Surname: Surname Smith

Procedures

Steps to Insert a Database Field

1. Ensure the Text tab is selected on the Tools screen. It has a yellow highlight when selected.
2. To open either the person, credential or optional field placeholders or the field labels, click on the v symbol to the left of the field category.
3. Select the desired database field; it is highlighted with a blue marquis.
4. Click and drag the database field from the Tools screen to the card template work area. Position it in the desired location on the template.
5. To extend the width of the box, position the cursor over one of the corners, click and drag it to the desired size.
    - Tip - you can use the text alignment tools to reposition the fields within the box.
6. While the database field is selected you can change the text colour or font size as follows:
    - Text Color - select Color 1 and change the color or hue by adjusting the palette settings.
    - Font Size - select the font size tool and select the desired setting.
7. Click the cursor outside the text box to close it.

Related Topic

Database Fields - Placeholders vs Labels

Insert a Personal Photo Frame

This procedure creates a placeholder on the template for the actual on-file image of the credential holder when a photo badge is printed. This is the same image displayed on the Edit Person screen

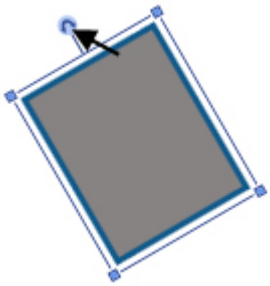
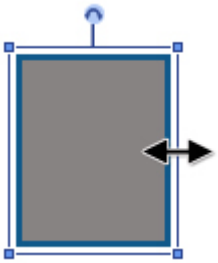
Procedure

Steps to Insert a Personal Photo Frame

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Select the personal photo frame tool.
3. Position the cursor over the desired area on the template work area.
4. Click the mouse. The photo frame is inserted on the template.
5. Click and drag in a top to bottom, left to right motion until the photo frame is the desired size and then release the pointing device or mouse.
6. With the photo frame still selected, drag it to the desired position on the photo badge template.
7. To de-select the photo frame, click the mouse with the cursor positioned on the template but off the photo frame.

Move, Rotate or Scale an Object

Objects which include text boxes, or background shapes can be manipulated on the template work area. Depending on where the cursor is positioned on a selected object it changes to indicate which of the three tasks can be performed as shown in the table.

Rotate an Object	Move an Object	Scale an Object
		
Place the cursor over the circle at the top of the selected object, click and rotate object.	Move the cursor over the selected object. It changes to a four-point cursor as shown above. Click and drag the object to the desired position on the template work area.	Position the cursor at the edge of the object anywhere on the blue marquis or one of the four bounding boxes at the corners. Click and drag in the direction of the arrows and scale the object to the desired size. When scaling an image it is recommended to drag from one of the 4 corners to retain its aspect ratio.

Text Alignment

The text alignment tools can align text within text boxes created by the text tool or the database person, credential, or optional field tools. Ensure that the text box is selected, before selecting one of the text alignment tools.

Text Alignment Tools

Horizontal Alignment - Left / Center / Right



Vertical Alignment - Top / Middle / Bottom



Arrange Objects in Layers

The global card template editor composes object in layers. Each object introduced to the template is, in effect, layered above the preceding object. Objects are text boxes, database fields, images, photo placeholders and drawn objects such as circles, squares etc. Re-arranging objects can be especially important where some objects overlap. The editor has the following two commands that allow you to re-arrange how objects are layered on the template.

- Bring Forward - pulls an object forward one layer on the template
    - Right click on the selected object, click on Bring Forward
- Move Back - pushes an object back one layer on the template
    - Right click on the selected object, click on Move Back

Try drawing three or four different color rectangles with each rectangle partially overlapping the others to see how objects are layered. Select different rectangles and experiment with the bring forward and move back commands.

Edit or Delete Text

Procedure

Steps to Edit or Delete Text

1. Ensure the Text tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Click on the select text tool.
3. Position the cursor over the text you are editing or deleting on the template work area and click the mouse or pointing device.
4. The text box is now selected.
    - To edit the text, with the text box selected as indicated by the blue marquis surrounding it, click the cursor inside the text box and edit the text. Then click outside the text box.
    - To delete the text box, with the text box selected as indicated by the blue marquis surrounding it, press the Delete key on the keyboard.

Clone a Card Template

The global card template editor has a card clone function. This function is useful when you have already created a template and you intend to create additional but similar templates. Selecting the clone tool creates a duplicate of the template currently open; however, the editor adds the suffix - Copy (1) to the current template file. You can then re-name the file, make the desired changes to the new template and save it.

Procedure

Steps to Clone a Template

1. Open the template you intend to clone.
2. Click on the clone button .
3. Under Card Properties enter a template name in the Name box.
4. Make the desired changes to the template.
5. Click on the Save button.
6. Click on the Back button until returned to the main screen or the navigation history  button for a previously viewed screen.

Delete an Object

Procedure

Steps to Delete an Object

1. Ensure the Background tab is selected on the Tools screen. It has a yellow highlight when selected.
2. Click on the select tool.
3. Position the cursor over the object you are deleting on the template work area and click the mouse or pointing device.
4. With the object selected, press the Delete key on the keyboard.

Save a Global Card Template

Procedure

Steps to Save a Global Card Template

1. From the Manage Global Card Template editor screen, click inside the Card Properties - Name box and enter a file name for the card template.
2. Select the Save button. The template is saved to the Keyscan database.
    - If you do not enter a name before saving, the card editor creates a file name Global Card Template #.

Delete a Card Template

Procedures

Delete a Card Template

These procedures are based on opening the desired template for deletion.

1. From the Manage Global Card Templates editor screen, select the Open Card Template  icon.
2. Select the card template that you are deleting.
3. In the upper right corner of the template editor, click on the Delete  icon.
4. From the Card Templates dialog box - Please confirm deletion of the card template [File Name], click on the Yes button.

Assigning Card Templates to Specific Sites

Sometimes, it might be desirable to create a unique design for a card template that you only want used for cards belonging to a specific site. It is for this reason that the Global Card Template Editor has a Sites property associated with each card template.



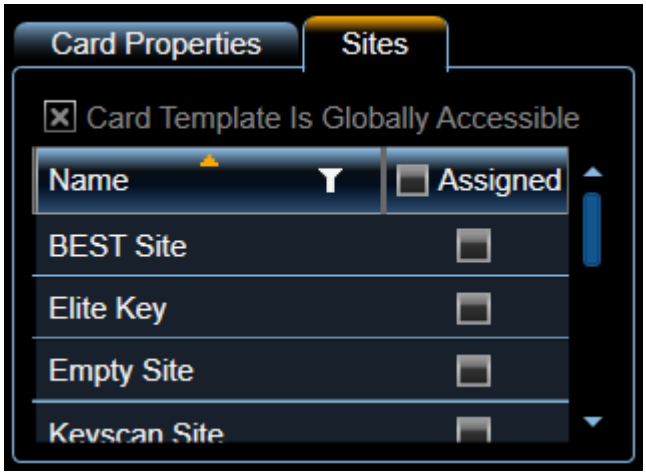
Global Card Templates

A card template will be globally accessible under the following conditions:

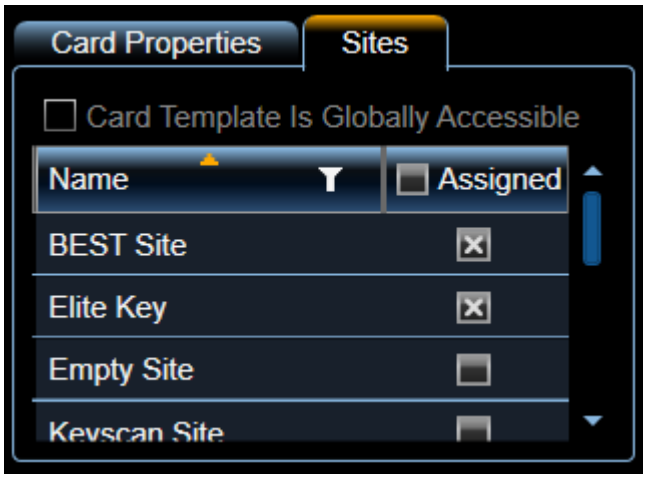
- when the card template is not assigned to any sites
- when the card template is assigned to all sites in the system

Site Assignment

When you first create a new card template, the template is set to Global by default, as indicated by the checkbox that appears next to the phrase "Card Template Is Globally Accessible". This means that the card template can be used for printing cards/credentials belonging to all sites.



To restrict the use of the card template to one or more sites, simply click the corresponding checkbox next to any of the sites that appear in the list of sites. When selecting one or more sites, notice that "Card Template Is Globally Accessible" is automatically deselected.



For the example in the image above, note that this card template is only assigned to two sites; Best Site and Elite Key. This means that when printing a card/photo badge, this particular template can only be used for people with credentials in these sites only.

Note: the global state of a card template should not be confused with the global Card Template Type as defined under Card Properties. All types of card templates (global, site, and visitor) can be assigned to sites. This feature is not restricted to "Site" card template types.

Related Topics

- Manage Global Card Templates
- Card Properties
- Global Card Template Editor Tools
- Print Photo Badges

Active Map Template Editor

The Active Map Template Editor allows you to create maps of your sites, which can be viewed by system operators. In the event an alarm is triggered, the operator can pinpoint the exact location in order to investigate the cause of the alarm. Draw original maps or import floor plans. In both cases, you can insert icons representing doors, readers, and supervised and auxiliary inputs connected to various types of intrusion devices. Maps are saved as MAP files.

The Active Map Template Editor help is divided into 2 sections:

- map overview
- creating maps using the tools

Active Map Template Editor Screen with a Map



Related Topic

Map Tools

Map Tools

The Active Map Template Editor has three tool sets:

- Text tools
- Devices
- Background tools

Each set of tools is accessible by selecting the desired tab - Text, Device or Background - under the Tools heading. Map tools are accessible by selecting the respective tab. The three map tool categories are outlined in the table as follows:

About the Select Tool

The Active Map Template Editor Text, Devices, and Background tool sets each have a Select tool. Each Select tool can only select an object for editing, re-sizing, moving, or deleting from its respective tool set.

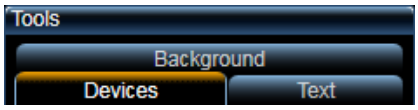
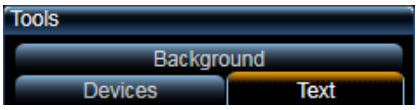
- The Text Select tool can only select objects on the template created by a text tool
- The Devices Select tool can only select objects on the template inserted by a devices tool
- The Background Select tool can only select objects on the template created by a background tool

About the Snap and Grid Tools

The snap and grid tools operate in the same fashion as a switch - click on either one to turn it on, click on it again to turn it off.

- Snap or Grid - Off - the button is dark blue
- Snap or Grid - On - the button is light blue

The three map tool categories are outlined in the table as follows:

Map Tools - Devices - Text - Background		
		
Devices Select by clicking on the tab. All the associated device tools are accessible for inserting and placing system connected devices on the map.	**Text** Select by clicking on the tab. All the associated text tools are accessible for creating and editing text on the template work area.	**Background** Select by clicking on the tab. All the associated background tools are accessible for drawing shapes and inserting images on the map.
 **Select Device Tool** Select a device on the map when the Device layer is active.	 **Select Text Tool** Selects a text box previously inserted when the Text layer is active.	 **Select Background Tool** Use to select an object inserted on the background layer.



Map Link Tool

Inserts a link to another map.



Text Editor Tool

Inserts text on the map template.



Import Background Tool

Use to import an image which the template editor scales to the full size of the background. Use this tool if inserting a floor plan or map created in another application such as Visio or similar drawing application.



Color 1

Not applicable for Devices.



Color 1 Text Tool

Indicates the current colour selection for text. Click on the box to open the palette and select an alternate colour.



Fill Background Tool

Use to paint the entire background in the colour displayed in Color 1 palette box.



Color 2

Not applicable for Devices.



Color 2 Text Tool

Not applicable on Text Layer.



Delete Background Tool

Use to delete the current background.



Line Thickness

Not applicable for Devices.



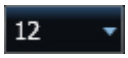
Font Size Tool

Indicates the current font size selection for inserting text. Click on the ▼ to open the drop down box and select an alternate font size.



Rectangle Tool

Use to draw a rectangle or square.



Font Size Tool

Indicates the current font size selection. Click on the ▼ symbol to open the drop down box and select an alternate font size.



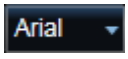
Font Tool

Indicates the current font selection. To change fonts, click on the ▼ symbol and select an available font from the drop down box.



Ellipse Tool

Use to draw an ellipse or circle.



Font Tool

Indicates the current font selection. To change fonts, click on the ▼ symbol and select an available font from the drop down box.



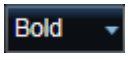
Font Weight Tool

Indicates the current font weight selection. To change the font weight, click on the ▼ symbol and select an available font weight from the drop down box.



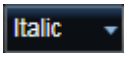
Triangle Tool

Use to draw a triangle.



Font Weight Tool

Indicates the current font weight selection. To change the font weight, click on the ▼ symbol and select an



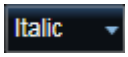
Font Style Tool

Indicates the current font style selection. To change the font style, click on the ▼ symbol and select an



Free-form Line Tool

Use to draw a line free-hand.

available font weight from the drop down box.	available font style from the drop down box.	
 **Font Style Tool** Indicates the current font style selection. To change the font style, click on the ▼ symbol and select an available font style from the drop down box.	 **Apply Style Formats** Clicking the Apply Style Formats button alters the font style (font, color, etc.) for any text currently selected on the map so that they match the chosen settings in the Tools menu.	 **Line Tool** Use to draw a straight line.
 **Apply Style Formats** Clicking the Apply Style Formats button alters the font style (font, color, etc.) for the text of any objects currently selected on the map so that they match the chosen settings in the Tools menu.	 **Grid Tool** Lays out a grid over the work area for aligning devices, text and objects on the map template.	 **Multi-line Tool** Use to draw multiple straight connecting lines.
 **Grid Tool** Lays out a grid over the work area for aligning devices, text and objects on the map template.	 **Snap Tool** Positions the selected text box at intersecting grid lines.	 **Import Image Tool** Imports an image in its original dimensions for placement on the map.
 **Snap Tool** Positions the selected device at intersecting grid lines.		 **Color 1 Tool** Indicates the current colour selection for a line or the border of a rectangle, ellipse or triangle. Click on the box to open the palette and select an alternate colour.
Note on Inserting Devices When a device is inserted on the map work area, a text box with the device's assigned name is included with the icon. You can use the device font property tools to alter the text or you can delete the text.		 **Color 2 Tool** Indicates the current colour selection for the fill of a rectangle, ellipse or triangle. Click on the box to open the palette and select an alternate colour.
		 **Line Thickness Tool** Indicates the current line thickness or border thickness of a rectangle, ellipse or triangle. Click on the ▼ symbol to open the drop down box and select an alternate thickness.

		 **Grid Tool** Lays out a grid over the work area for aligning devices, text and objects on the map template.
		 **Snap Tool** Positions the selected background object at intersecting grid lines.

Insert Devices

Devices that can be inserted on a map include the following items.

- Doors (including E-Plex Doors)
- Readers
- Auxiliary Outputs
- Inputs
- IOCB Outputs
- IOCB Inputs
- (Elevator) Banks
- Intrusion Partitions
- Intrusion Zones
- Cameras

If any of the above devices had images attached in the Device Image Setup screen, the image, rather than an icon, is inserted on the map.

Note on Inserting Devices

When a device is inserted on the map work area, a text box with the device's assigned name is included with the icon. You can use the device font property tools to alter the text or you can delete the text.

Related Topic

Insert a Door or Device

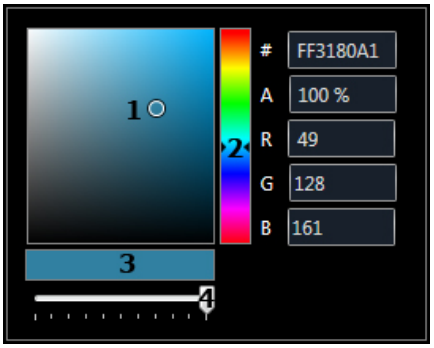
New - Open Buttons

The following outlines the Open, New, Save, Undo and Redo functions on the Active Map Template Editor. These functions are always visible regardless of the type of tools selected.

Button	Name and Function
	**Open Map Template** Select to open an existing map template.
	**New Map Template** Select to create a new map template.
	**Undo** Select to delete the last action or actions on the template work area.
	**Redo** Select to recover the last action or actions if the Undo button was previously selected.
	Note on undo and redo - only applies to actions that have occurred after the last save.

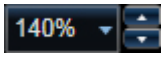
Colour Selection

When Color 1 or Color 2 are selected on the applicable Text or Background tools, the colour palette opens and you can adjust or change the colour, hue or transparency of the object or text inserted on the template work area.

Colour Palette	Colour, Hue, Transparency Selection
	1 - Circle indicates current hue selection - To change the hue, click and drag the circle to the desired hue 2 - Colour palette with > < arrows indicating current colour selection - To change colour, click and drag the arrows to desired colour 3 - Opacity indicator 4 - Transparency/opacity slide - To change transparency, click and drag opacity/transparency slide left or right to desired setting # - the indicates the hexadecimal colour value - the first two characters represent the opacity value and the last six characters represent the colour value A - indicates the colour's opacity percentage (%). R, G, B - indicates the red, green and blue values for the selected colour

Map View Selector

The Active Map Template Editor allows zooming in or out to enlarge or shrink the view of the template.



% - indicates the current template magnification

Click on the symbol ▼ to the immediate right of the magnification % to open a drop down list for a range of selectable views - 20% to 200%.

Clicking on the up or down arrows to the far right increase (up) or decrease (down) in increments of 20% each time an arrow is clicked.

Create a New Map

Procedure

Steps to Create a New Map

1. From the Client main screen, select the Site Management button > Active Map Template Editor.
    - If you have multiple sites, double click on the name of the site for which you are creating a new map.
2. Click on the New Map  button near the bottom below the Tools menu.
3. Under the Map Properties heading, click inside the Map Name text box and enter a file name for the map.
    - By default, the Active Map Template Editor creates a file name Map # 1 and increments the number by 1 each time a new map is created. You can retain the default map file name, however it may not be sufficiently descriptive for other system users.
4. Select the save button. The map template is saved to the Keyscan database.

Open an Existing Map

Procedure

Steps to Open an Existing Map

1. From the Client main screen, select the button with the building icon > Active Map Template Editor.
    - If you have multiple sites, double click on the name of the site for which you are creating a new map.
2. From the Active Map Template Editor screen, click on the Open Map  icon in the lower area of the Tools screen.
3. From the Active Maps pop up list, select the template.

Import a Floor Plan

The Active Map Template Editor has the capability of importing floor plan drawings created in other 3rd party software which have been saved in graphic file formats such as JPEG, PNG, GIF or BMP. The template editor will scale larger imported drawings to fit within the work area.

Procedure

Steps to Import a Floor Plan

1. From the Active Map Template Editor screen, ensure the Background tab is selected on the Tools screen.
2. Select the Import Background icon  under Background Fill.
3. From the Open dialog box, navigate to the folder location with the floor map file you are importing.
    - You may have to set the Open dialog box to All Files opposite File name to view all files in the folder.
4. Select the file.
5. Click on the Open button.

Note: A transparent GIF image does not support background transparency and will result in a black background.



To clear a floor plan drawing from the template, select the Delete Background tool .

Draw a Rectangle, Ellipse, Triangle - Maps

Procedures

Steps to Draw an Object - rectangle, ellipse, triangle

1. Ensure the Background tab is selected on the Tools screen.
2. Select one: the Rectangle Tool , the Ellipse Tool , or the Triangle Tool .
    - All three tools behave in the same manner by clicking and dragging.
3. Position the cursor over the desired area on the template work area.
4. Click and drag in a top to bottom, left to right motion until the object is the desired size and release the pointing device or mouse.
5. The object is currently selected as indicated by the blue marquis surrounding it.
6. While it is selected you can change the line thickness, line colour and the fill colour as follows:
    - Line Thickness - select the ▼ symbol opposite the Line Thickness tool and select an option from the drop down list.
    - Line Colour - select Color 1 and change the colour or hue by adjusting the palette settings.
    - Fill Colour - select Color 2 and change the fill colour or hue by adjusting the palette settings.

More information about moving, rotating or scaling an object, select the link below.

Related Topics

Move, Rotate, or Scale an Object

Draw a Free-form Line

Procedures

Steps to Draw a Free-form Line

1. Ensure the Background tab is selected on the Tools screen.
2. Select the Free-form Line tool (pencil) .
3. Position the cursor over the desired area of the template work area.
4. Click and drag to create the line.
5. You can change the line thickness or line colour. First click on the Select tool, then select the line on the template work area. While it is selected, do either of the following steps:
    - Line Thickness - select the ▼ symbol opposite the Line Thickness tool and select an option from the drop down list.
    - Line Colour - select Color 1 and change the colour or hue by adjusting the palette settings

Draw a Single Straight Line

Procedures

Steps to Draw a Single Straight Line

1. Ensure the Background tab is selected on the Tools screen.
2. Select the Line tool .
3. Position the cursor at the desired spot on the template work area where the line is to start.
4. Click and drag to create the straight line.
5. You can change the line thickness or line colour. First click on the Select tool, then select the line on the template work area. While it is selected, do either of the following steps:
    - Line Thickness - select the ▼ symbol opposite the Line Thickness tool and select an option from the drop down list.
    - Line Colour - select Color 1 and change the colour or hue by adjusting the palette settings

Draw Angled Multiple Lines

Procedures

Steps to Draw Angled Multiple Lines

1. Ensure the Background tab is selected on the Tools screen.
2. Select the Multi-line tool .
3. Position the cursor at the desired spot on the template work area where the line is to start.
4. Click and drag to create the first line segment.
5. Release the mouse or pointing device while positioned at the end of the line segment, then click the mouse or pointing device and draw the next line segment. Repeat using the same technique until the contiguous angled lines have been drawn.
6. You can change the line thickness or line colour. First click on the Select tool, then select the line on the template work area. While it is selected, do either of the following steps:
    - Line Thickness - select the ▼ symbol opposite the Line Thickness tool and select an option from the drop down list.
    - Line Colour - select Color 1 and change the colour or hue by adjusting the palette settings

Insert an Image

Procedure

Steps to Insert an Image

1. Ensure the Background tab is selected on the Tools screen.
2. Select the Import Image tool .
3. From the Open dialog box, navigate to the folder location with the image file you are importing to the Active Map Template Editor.
    - You may have to set the Open dialog box to All Files opposite File name to view all files in the folder.
4. Select the file.
5. Click on the Open button.

For more information about moving an image (object), select the link below.

Note: A transparent GIF image does not support background transparency and will result in a black background.

Related Topics

Move, Rotate, or Scale an Object

Insert Text

Procedures

Steps to Insert Text

1. Ensure the Text tab is selected on the Tools screen.
2. Select the Text Editor Tool .
3. Position the cursor over the desired area on the template work area.
4. Click and drag in a top to bottom, left to right motion to create a text box until it is the desired size and then release the pointing device or mouse.
5. With the text box selected as indicated by the blue marquis surrounding it, insert the cursor in the text box in front of the word Label, click and drag so Label is highlighted.
6. Press the Delete key to clear the text box.
7. Enter the text.
8. While it is selected you can change the text colour or font properties as follows:
    - Text Colour - select Color 1 and change the colour or hue by adjusting the palette settings.
    - Font Size - select the Font Size tool and select the desired setting.
    - Font Weight - select the Weight tool and specify a style
    - Font - select the Font tool and specify the desired font
9. Click the cursor outside the text box to de-select it.

Insert a Door or Device

Procedures

Steps to Insert a Door or Device on the Map

1. Ensure the Devices tab is selected on the Tools screen.
2. On the Tools screen, click on the device category.
3. Click on the applicable control unit.
4. Select the device.
5. Click and drag the icon from the Tool screen on to the template in the desired map location.
    - You will note that a text box with the device's name accompanies the device icon. You can leave the text box, edit the text in the text box or delete the text box.

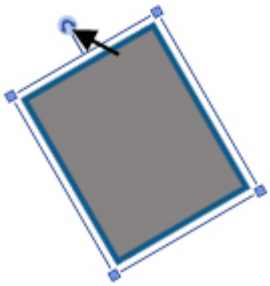
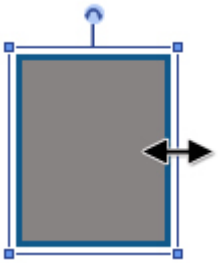
For more information about moving, rotating or scaling an object, select the link below.

Related Topics

Move, Rotate or Scale an Object

Move, Rotate or Scale an Object

Objects which include text boxes, device icons, or background shapes can be manipulated on the template work area. Depending on where the cursor is positioned on a selected object it changes to indicate which of the three tasks can be performed as shown in the table.

Rotate an Object	Move an Object	Scale an Object
		
Place the cursor over the circle at the top of the selected object, click and rotate object.	Move the cursor over the selected object. It changes to a four-point cursor as shown above. Click and drag the object to the desired position on the template work area.	Position the cursor at the edge of the object anywhere on the blue marquis or one of the four bounding boxes at the corners. Click and drag in the direction of the arrows and scale the object to the desired size. When scaling an image it is recommended to drag from one of the 4 corners to retain its aspect ratio.

Arrange Objects in Layers

The active map template editor composes object in layers. Each object introduced to the template is, in effect, layered above the preceding object. Objects are text boxes, images, drawn objects such as circles, squares etc. Re-arranging objects can be especially important where some objects overlap. The editor has the following two commands that allow you to re-arrange how objects are layered on the template.

- Bring Forward - pulls an object forward one layer on the template
    - Right click on the selected object, click on Bring Forward
- Move Back - pushes an object back one layer on the template
    - Right click on the selected object, click on Move Back

Try drawing three or four different color rectangles with each rectangle partially overlapping the others to see how objects are layered. Select different rectangles and experiment with the bring forward and move back commands.

Edit or Delete Text

Procedure

Steps to Edit or Delete Text

1. Ensure the Text tab is selected on the Tools screen.
2. Click on the Select Text tool .
3. Position the cursor on the template work area over the text you are editing or deleting and click the mouse or pointing device.
4. The text box is now selected as indicated by the blue marquis surrounding it.
    - To edit text, click the cursor inside the text box and edit the text. Then click outside the text box to de-select it.
    - To delete the text box, with the text box selected as indicated by the blue marquis surrounding it, press the Delete key on the keyboard.

Delete an Object

Procedure

Steps to Delete an Object

1. Depending on the type of object you are deleting, a Device object or a Background object, ensure the correct tab is selected on the Tools screen.
2. Click on the Select tool .
3. Position the cursor on the template work area over the object you are deleting and click the mouse or pointing device.
4. With the object selected, press the Delete key on the keyboard.

Save a Map Template

Procedures

Steps to Save a Map Template

1. From the Active Map Template Editor screen under the Map Properties heading, click inside the Map Name text box and enter a name for the map.
2. Select the Save button. The map template is a saved to the Keyscan database.

About Visitors & Preliminary Setup

The Visits tab on the Edit Person screen opens Aurora's visitor management component for systematically scheduling, monitoring, and recording all visitors coming to your premises. The Visits function keeps a complete history of all visitor activity, tracks arrival and departure times, who the visitor met and retains each visitor's information on hand for subsequent visits. You can issue credentials so visitors may gain entry at authorized doors or elevator floors controlled by the access control system.

See Schedules, Groups and Access Levels below if you intend to issue credentials to your visitors.

System User Account

The system user account requires the following people permissions depending on the level of responsibility for using the visits function:

- View People - user is restricted to viewing a person's record and cannot add or make changes*
- Add People - user can add a record
- Edit People - user can edit a record

*If View People is selected as a permission, the system user can still schedule a visit or update the visit status provided that the Add Visits and Edit Visits permissions are enabled. See Visits below.

The system user account may also require enabling Person Photos and, if issuing visitors with credentials, enabling the Credentials sub-permissions.

Visitor Only User

For restricting a system user to only enrolling and scheduling visitors, select Visitor Only User in the User Type field on the Manage System User screen. The Visitor Only User function limits access to visitor type people records. Visitor types can be identified in the Application Utilities screen under the Person Type heading with a Visit - Yes status.

The following two permissions can further restrict the Visitor Only User function:

- View Visitor Types Only - the system user is restricted to viewing visitor types
- Edit Visitor Types Only - the system user is restricted to editing visitor types

The above two permissions can only be enabled when the User Type is set on Visitor Only User.

For more on configuring a system user account, select the link below Related Topics.

Visits

Anyone, such as a receptionist or administrative assistant, responsible for scheduling visits must have the Visits permissions enabled in his or her system user account. The Visits permission has 3 sub-fields for controlling the level of user interactions:

- View Visits - user is restricted to viewing a visitor record and cannot add or make changes
- Add Visits - user can schedule a visit and update the visit status
- Edit Visits - user can edit the visit status

When assigning Add Visits or Edit Visits permissions, the View Visits permission must be enabled otherwise the Visits tab is unavailable in the Edit Person screen.

Schedules, Groups & Access Levels

If you intend issuing credentials for autonomous visitor access at system regulated doors or elevator floors, Keyscan recommends that you create specific schedules, groups and door group access levels and/or elevator group access levels for maintaining better site controls and isolating visitors from your other groups.

Group Setup

When creating visitor groups in the Group Setup screen, ensure the following field is enabled:

- Visitor Group

This identifies the group as a specific visitor group.

Optional Card Scanner

If you have an optional business card scanner you may have to calibrate it before you can start scanning. Select the link below Related Topics for more about scanning business cards or ID cards such as driver licenses.

Related Topics

- System User Accounts
- Schedules
- Groups
- Door Group Access Levels
- Elevator Group Access Levels
- Optional Card Scanner
- Visit Status Widget

Create a Visitor Record

Visitor records are created in the Edit Person screen. After you have entered and saved a record, the visitor's information is retained in the Keyscan database which is easily accessed when scheduling visits. When a new visitor record is created, the First Name and Last Name fields are required entries. The Client software will not save the record unless those two fields are completed.

Procedure

Steps to Create a Visitor Record

1. From the Client main screen, select the Manage People button > Add Person.
2. From the Add Person screen, enter the person’s first name in the Given Name text box.
3. If the Middle Name field is enabled in the Applications Utilities screen enter the person’s middle name if required.
4. Enter the person’s last name in the Surname text box.
5. Click on the ▼ symbol to the right of Type and select Visitor or a user-defined visitor category from the drop down list.
    - You can create user-defined visitor categories under Person Type in the Application Utilities screen.
6. If you have a USB camera connected for capturing images, go to the next step; if you do not require attaching an image to the visitor record go to step 12.
7. To attach the visitor’s photo to his or her record, move the cursor over the silhouette in the upper left and click on the + symbol.
8. From the Image Editor screen, click on the Start button.
9. Position the person in front of the camera at the desired distance.
10. When the person is suitably posed for the image, click on the Snapshot button.
11. From the Image Editor screen, click on the Save button.
12. If any of the Optional Fields or General Information applies, select those tabs at the top and complete the necessary details.
13. Select the Save button.
14. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Scan a Visitor Record

Schedule a Visit

Optional Card Scanner

Aurora can be interfaced with a card scanner to enroll visitors from either an ID card, such as a driver's license, or from a business card. This function requires an optional Card Scanning license from Keyscan and either a BIZSCAN2 scanner for business cards and ID cards, or a BIZSCAN scanner for business cards.

When you scan a card the names are captured by the scanner and transferred to the Edit Person screen. A graphic image of the card is also stored with the visitor record.

Calibrate the Card Scanner

The card scanner must be calibrated before you can start scanning. You require the calibration paper to complete these procedures. Calibrating the scanner is performed from the Application Utilities screen. Before you can calibrate the scanner you must have installed the drivers as outlined on the BIZSCAN Driver and Software Installation Guide that accompanied the device.

Card Scanner Cleaning

Periodically and depending on how frequently the card scanner is used, its internal scanning apparatus requires cleaning with the special cleaning paper included with the scanner. See the procedures below. Cleaning the scanner is performed from the Application Utilities screen.

Procedures

Steps to Calibrate the Scanner

Before you start, ensure that you have the special calibration paper that was included with the scanner. It has the large black bar with two arrows.

1. From the main screen, select the Settings button > Application Utilities.
2. Insert the calibration paper into the scanner in the direction of the arrows. The scanner will pull the edge of the calibration paper into the slot and stop.
3. Below the Application Settings heading, select the Calibrate Scanner button.
4. Wait until the calibration is completed.
5. From the Scanner calibrated successfully confirmation box, click on the OK button.
6. Select the Back button until you are returned to the main screen or select the Navigation History symbol for a previously viewed screen.

Steps to Scan a Business Card

1. From the main screen, select the Manage People button > Add Person.
2. Place the visitor's business card horizontally, face-down with the top of the card entering the scanner first. Ensure the card is to the right edge of the scanner's feed tray. You should feel a slight tug on the card as the scanner pulls the edge of the card in.
3. From the Edit Person screen, click on the Scan BC button.
4. Wait for the scan to finish. The scanner will eject the card when the scan is completed.
    - The information from the card is now inserted in the appropriate visitor name fields.
5. Complete any remaining fields on the Edit Person screen.
6. Click on the Save button.
7. To scan another business card, repeat steps 2 - 6, or, click on the Back button until you are returned to the main screen.

Steps to Scan an ID Card (Driver's License)

1. From the main screen, select the Manage People button > Add Person.

2. Place the visitor's ID card horizontally, face-down with the top of the card entering the scanner first. Ensure the card is to the right edge of the scanner's feed tray. You should feel a slight tug on the card as the scanner pulls the edge of the card in.
3. From the Edit Person screen, click on the Scan DL button.
4. Wait for the scan to finish. The scanner will eject the card when the scan is completed.
    - The information from the card is now inserted in the appropriate visitor name fields.
5. Complete the remaining fields on the Edit Person screen.
6. Click on the Save button.
7. To scan another card, repeat steps 2 - 6, or, click on the Back button until you are returned to the main screen.

Steps to Clean the Scanner

Before you start, ensure that you have the special cleaning paper that was included with the scanner. It has a grainy textured feel.

1. From the main screen, select the Settings button > Application Utilities.
2. Insert the cleaning paper into the scanner in the direction of the arrows. The scanner will pull the edge of the paper into the slot and stop.
3. Below the Application Settings heading, select the Clean Scanner button.
4. Wait until the cleaning is completed.
5. From the Scanner cleaned successfully confirmation box, click on the OK button.
6. Select the Back button until you are returned to the main screen or select the Navigation History symbol for a previously viewed screen.

Schedule a Visit

Scheduling a visit is performed from the Edit Person screen with the Visitors tab selected. Scheduled visits are saved to the database creating a history for each individual visitor.

Visits can be scheduled in advance and marked as expected or upon the visitor's arrival and marked as arrived. Upon leaving record the visitor as departed, thus preserving a time line of the visit in the database.

Schedule a Visit - From an Employee Record or a Visitor Record

Visits may be scheduled from an employee record or a visitor record.

If issuing a credential to a visitor, the credential must be issued from the visitor record.

Status

A visit can be changed to any of the following states and accurately reflect the current status of the visit appointment. Visit status is listed below the Status heading.

- Expected - the visitor has a scheduled visit or appointment
- Delayed Arrival - the visitor has been delayed past the scheduled visit or appointment time but is still expected
- Arrived - the visitor has arrived and is currently in the building or is on site
- Departed - the visitor has left the building or the site
- Cancelled - the visit or appointment has been cancelled

E-mail Notification

Persons who are listed as Attendees for a scheduled visit and have an e-mail address specified in the Edit Person screen's E-mail field receive a notification when the Quick Action button is used to update a visit status for one of the following conditions:

- Arrived
- Delayed
- Cancelled

Issuing Credentials to Visitors

If you issue cards that allow visitors independent entry to access controlled doors and/or elevators, the Credential Information fields are used for assigning the credential and setting any temporary usage/date options after you have created a visitor record in the Edit Person screen.

If you have credentials that are re-issued to visitors, those credentials must be deleted at the end of a visit before they can be re-assigned. Deleting the credential is also a security precaution. See Related Topics below for more on cancelling a visitor’s credential.

Procedures

Steps to Schedule the Appointment in the Future

These instructions are based on scheduling an appointment from a visitor record. If scheduling an appointment from an employee record, perform the procedure in the same manner.

1. From the Client main screen, select the Manage People button > Manage People.

2. From the Manage People screen, locate the name of the visitor.
3. Double click on the visitor.
4. Select the Visits tab if it is not currently highlighted.
5. Click on the Add Visit button.
    - The Status indicates Expected, the Arrival Time is set at the current time and the Departure Time is set at 1 hour later than the current time.
6. On the highlighted visit below the Arrival Time column, click so the date & time selection icon opens.
7. Click on the date & time selection icon to open the calendar/time screen.
8. On the calendar side, use the arrows to scroll to the desired month if necessary.
9. Select the day in the calendar.
10. On the time side of the screen, select the arrival time.
    - If the appointment does not start at the top of the hour, click on the Close button and then click and drag over the arrival minutes and type the correct minutes for the arrival time.
11. Click on the Close button on the calendar/time screen.
12. Ensure the row with the visit is still highlighted.
13. Click on the visit row under the Departure Time column.
14. Set the departure time using the same techniques above.
15. Click on the Close button on the calendar/time screen.
16. Below the Visit Details heading, click on the Attendees + button.
    - Attendees will include the visitors and the persons or contacts with whom the visitors are meeting.
17. Scroll down until you locate the first attendee and click on the > button or the attendee's name.
    - If you select the wrong attendee, click on the Remove button and repeat the previous two steps.
18. Repeat the previous two steps until you have listed all persons scheduled to attend the appointment.
19. Click on the Save button.
20. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Record the Appointment without a Credential - Visitor Has Arrived

These instructions assume you have previously created a visitor record.

1. From the Client main screen, select the Manage People button > Manage People.
2. From the Manage People screen, locate the name of the visitor.
3. Double click on the visitor.
4. Select the Visits tab if it is not currently highlighted.
5. Click on the Add Visit button.
    - The Status indicates Expected, the Arrival Time is set at the current time and the Departure Time is set at 1 hour later than the current time. Ensure the row with the visit is still selected.
6. Below Quick Action, click on Arrived.
    - The Status changes from Expected to Arrived.
7. If you need to alter the departure time go to the next step, otherwise go to step 12.
8. Click on the visit below the Departure Time column so the date & time selection icon opens.
9. On the time side of the screen, select the departure time.

- If the appointment does not end at the top of the hour, click on the Close button, and then click and drag over the minutes and type the correct minutes for the departure time.

10. Click on the Close button on the calendar/time screen.
11. Below the Visit Details heading, click on the Attendees + button.
    - Attendees will include the visitors and the persons or contacts with whom the visitors are meeting.
12. Scroll down until you locate the first attendee and click on the > button or the attendee's name.
    - If you select the wrong attendee, click on the Remove button and repeat the previous two steps.
13. Repeat the previous two steps until you have listed all persons scheduled to attend the appointment.
14. Click on the Save button.
15. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Steps to Schedule a Visit and Issue a Credential - Visitor Has Arrived

These procedures assume you are recording the appointment/visit and issuing a credential when the visitor arrives on site. If you have already scheduled the appointment/visit and just need to issue a temporary credential, refer to Create a Temporary Credential under Manage People and Credential Records.

1. From the Client main screen, select the Manage People button > Manage People.
2. From the Manage People screen, locate the name of the visitor.
3. Double click on the visitor.
4. Ensure that the Credential Information tab is currently selected.
5. Click on the  symbol to the right of the Add Keyscan button and from the drop down list select the type of card format.
    - The button will list the last credential type selected if you do not use the Keyscan 3 digit batch - 5 digit number card format.
6. Depending on the format selected, enter the batch number if applicable and the card number.
7. Select the v symbol opposite the applicable site to open the Groups pane.
    - If you have multiple sites, you may wish to de-select sites the visitor is not authorized to access. Sites are listed in the Site Assignment pane on the left.
8. Select the group or groups the visitor is assigned to by clicking in the box or boxes to the left. A box has an x when selected. Click and drag the scroll bar on the right to access groups not viewable in the pane.
9. Click in the box to the left of Temporary Options. The box has an x when it is selected.
10. If the card is temporary based on a date range, click on the calendar icon to the right of Valid From.
11. The calendar opens on the current day and month. Select the time on the right and click on the Close button.
12. Click on the calendar icon to the right of Valid To.
13. The calendar opens on the current day and month. Select a time on the right and click on the Close button.
14. If the card has a usage restriction, enter the maximum number of times the credential may be used in the Limited # Uses text box. If there is no usage restriction, leave the Limited # Uses blank.
15. Select the Visits tab.
16. Click on the Add New Visit button.
    - The Status indicates Expected, the Arrival Time is set at the current time and the Departure Time is set at 1 hour later than the current time.
17. Ensure the row with the visit is still selected.

18. Below Quick Action, click on Arrived.
19. The Status changes from Expected to Arrived.
20. If you need to alter the departure time go to the next step, otherwise go to step 27.
21. Click on the same row below the Departure Time column so the date & time selection icon opens.
22. On the time side of the screen, select the departure time.
    - If the appointment does not end at the top of the hour, click on the Close button and then click and drag to select the departure minutes in the visit row and type the minutes to complete setting the departure time.
23. Click on the Close button on the calendar/time screen.
24. Below the Visit Details heading, click on the Attendees + button.
    - Attendees will include the visitors and the persons or contacts with whom the visitors are meeting.
25. Scroll down until you locate the first attendee and click on the > button or the attendee's name.
    - If you select the wrong attendee, click on the Remove button and repeat the previous two steps.
26. Repeat the previous two steps until you have listed all persons scheduled to attend the appointment.
27. Click on the Save button.
28. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Cancel a Visitor's Credential

Visitor Information Report

Visit Report

Cancel a Visitor's Credential

If you issue temporary access credentials to visitors, at the conclusion of the visit when the credential is returned, before it can be re-issued to another visitor, it must first be deleted from the database. Deleting the card is also a security precaution which takes the access credential out of circulation.

Procedures

Steps to Cancel a Visitor's Credential

1. Retrieve the visitors credential.
2. From the Client main screen, select the Manage People button > Manage People.
3. From the Manage People screen, locate the name of the visitor.
4. Double click on the row with visitor record.
5. Click on the Credential Information tab if it is not currently selected.
6. Click on the waste bin icon on the right side of the Credential Information heading to delete the credential and take it out of circulation.
7. Click on the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Print Visitor Badges

You can print and assign photo badges if you have created photo badge templates with the Manage Global Card Templates editor and have a card printer. As Aurora's card template editor allows the creation of multiple card types - global, site or visit - you will need to know the template's card type when printing, as outlined below.

Card Types

Depending on the template's card type, note the following when printing photo badges.

Card Type - Visit

Card templates assigned with Card Type - Visit are accessed from the following two interface locations:

- Edit Person > Visit tab > click on the printer icon beside the visitor below the Attendees heading
- Status > Visit Status > click on the printer icon beside the visitor below the Attendees heading

Card Type - Global or Site

Card templates assigned with Card Type - Global or Site are accessed from the following interface location:

- Edit Person > Credential tab > click on the printer icon to the left of the Credential Information heading

Hide Image/Change Image

The Print Badge screen has a Hide Image/Change Image function if the photo badge template is designed with the credential holder image placeholder. The Hide Image function is designed for masking out the grey silhouette when there is no available image for the credential holder. The Change Image function allows substituting an alternate image, if the selected credential holder has more than one image on file.

The Hide Image/Change Image is accessed by right-clicking on either the credential holder's image or the grey silhouette place holder after the template has been selected and loaded in the Print Credential screen.

Note +

You cannot change the badge's orientation from Portrait or Landscape in the Print Badge screen; the template's orientation is based on how it was designed in the Manage Global Card Templates editor.

Procedure

Steps to Print a Photo Badge

These steps assume you have previously created visitor's record and have scheduled an appointment.

1. From the main screen, select the Manage People button > Manage People.
2. From the Person Search directory screen, scroll through the list of records or use the search operators to locate the desired record.
3. Double click on the record.
4. From the Edit Person screen, perform one of the following steps depending on the credential's card type:
    - Card Type - Visit: select the Visit tab and below the Attendees heading click on the printer icon opposite the visitor - only templates assigned with Card Type - Visit are viewable in the next step
    - Card Type - Global or Site: select the Credential Information tab and click on the printer icon at the left of the Credential Information heading - only templates assigned with Card Type - Global or Site are viewable in the next step

5. From the Print Credential dialog box, click on the ▼ symbol to the right of Template and select the desired template file from the drop down list. The dialog box opens a preview image of the template.
6. To use the Hide Image/Change Image function, position the cursor over the grey silhouette or the person's photograph, right click and select the desired option.
    - Hide Image - click on Hide Image. The image is removed from the template.
    - Change Image - click in the box that is to the upper left of the desired image. The Box has an x when selected. Click on the OK button.
7. If you have a template for the reverse side of the card, click on the ▼ symbol to the right of Back Template and select the desired template file from the drop down list. The dialog box opens a preview image of the template.
8. Click on the OK button.
9. From the Print dialog window, click on the badge printer from the list under Select Printer.
    - If the card printer is not displayed, select the Find Printer button and browse for the card printer. Then select it when it is listed.
10. Click on the Print button.
11. To return to the Person Search directory, select the navigation history  symbol and select Person Search from the list, or click on the Back button until you reach the main screen.

Related Topics

Card Properties

Search for Today's Visits

The Client has a "today's visits only" function on the Person Search screen that you can employ when you need a summary of scheduled visit appointments for today. You can use this function to list visitors with a scheduled appointment or list employees who have a scheduled appointment with a visitor. Please note that the instructions refer to the two default person types of employee and visitor. If you have created more person types in the Application Utilities screen, you would use the desired person type in your search for today's visits.

Procedure

Steps to List Today's Scheduled Visits

1. From the Client main screen, select the Manage People button > Manage People.
2. From the Person Search screen, click in the box to the right of Today's Visits Only. The box has an x when the function is enabled.
3. Opposite Person Type, click on the ▼ symbol to the far right and select Visitor from the list.
    - If you select employee, the search will list all employees who have a scheduled appointment with a visitor.
4. Opposite Visit Status, click on the ▼ symbol to the far right and select one of the visit options from the list.
5. The search will list the scheduled visits for today.

Related Topics

Schedule a Visit

Define Person Types

About Present3

Present3 is an Aurora credential utility. When an authorized credential is presented three successive times at a selected reader, Present3 can either toggle a door lock or toggle a schedule depending on the assigned mode.

With this added flexibility, Present3 gives you an optional control mechanism using a credential rather than sitting at a Client module server to effect the change. Use Present3 for any of the following applications:

- lock and unlock doors such as school classrooms or condominium recreational facilities etc.
- arm and disarm various Keyscan points connected to devices such as motion sensors
- lock out other credential holders to prevent false alarms
- implement a supervisory override to keep staff out
- control devices such as lights or HVAC etc.
- arm/disarm intrusion panel partitions or areas (requires optional Intrusion license and supported intrusion panel hardware and interface modules)

Related Topics

Present3 Modes

Using Present3

Setting Up Present3

PRESENT3 MODES

Present3 has five modes of operation, which are outlined under the following sub-headings. Only credential holders in the selected groups at the assigned reader can toggle the door lock or the schedule. Present3 is also referred to as P3.

Door Toggle

- toggles specified door's lock state - locked or unlocked

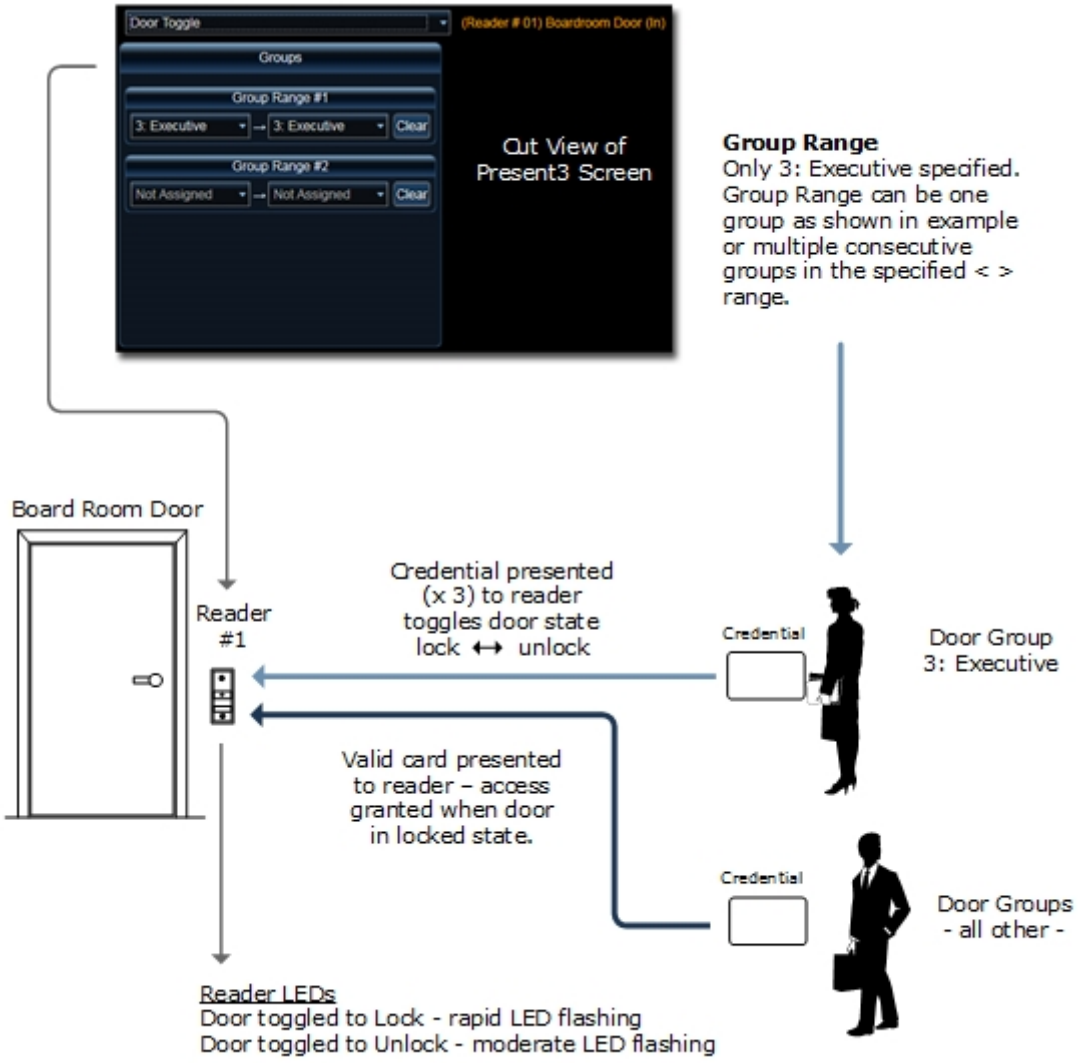
Change of State

- Lock - immediate on P3 at target reader
- Unlock - immediate on P3 at target reader

Affects

Only credential holders in selected door groups can toggle the door lock. Valid cardholders in other door groups may still access the door with a "single card presentation" when the door has been toggled to its locked state.

Example of Door Toggle



Schedule with Card Lockout

- toggles specified schedules - ON or OFF

Change of State

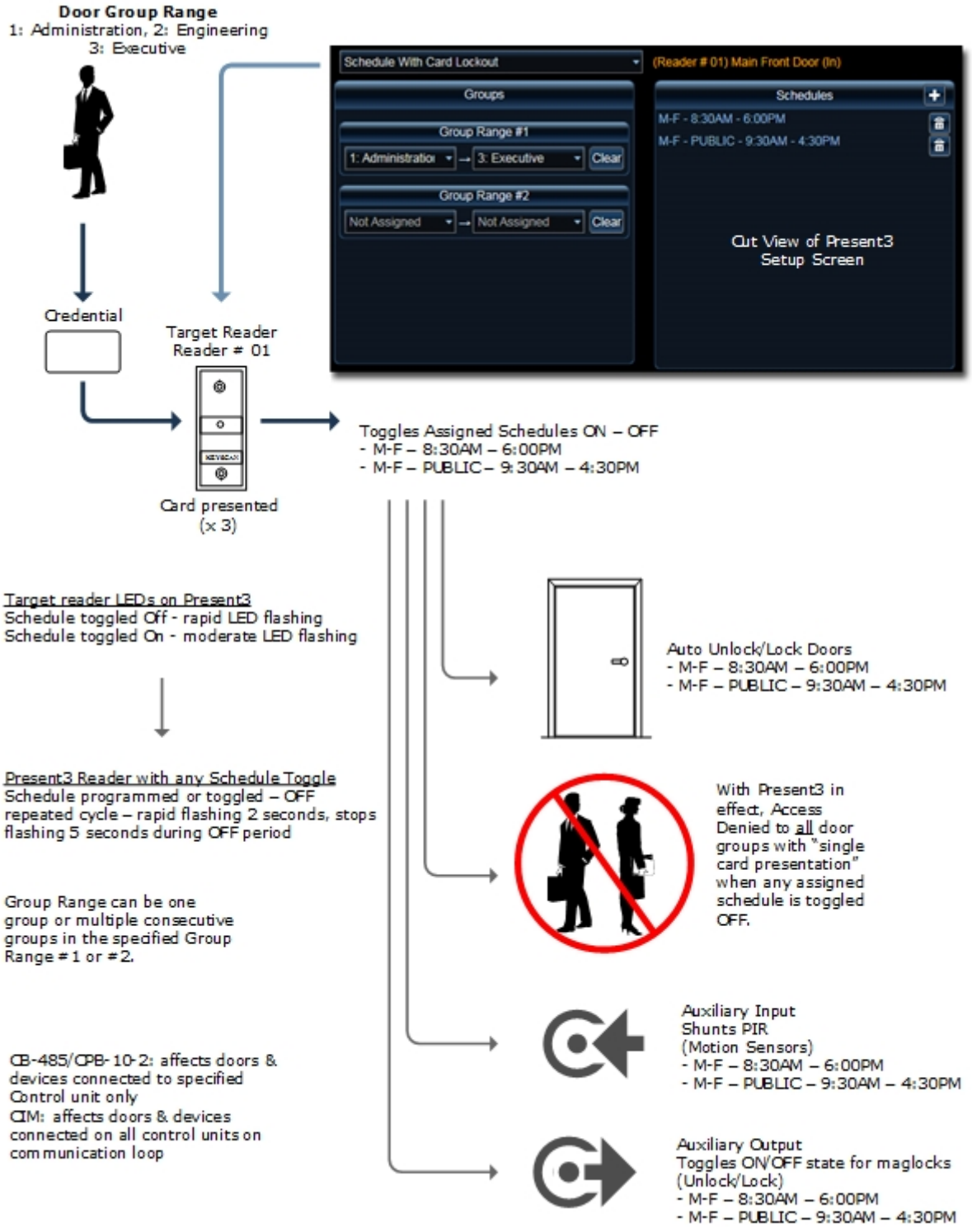
- Schedule to ON - immediate on P3 at reader
- Schedule to OFF - immediate on P3 at reader

Affects

Only credential holders in the selected groups at specified target reader can affect a Schedule with Card Lockout. This mode affects door group access, doors set on auto unlock/lock, and auxiliary input/shunt and auxiliary output devices that are controlled by the selected schedules.

While Present 3 is in effect and the schedules specified under Schedule Assignment in the Present3 Setup screen are toggled OFF, all credential holders in all door groups are denied access with a "single card presentation".

Example of Schedule with Card Lockout



Schedule with Card Lockout and Exit Delay

- toggles specified schedules - ON or OFF

Change of State

- Schedule to ON - immediate on P3 at target reader
- Schedule to OFF - occurs after # of seconds specified in the Door Held Open Time / Exit Delay field has elapsed on P3 at target reader

To cancel a schedule from turning OFF once initiating P3, repeat P3 within the Exit Delay time.

Affects

Only credential holders in selected door groups at a specified target reader can affect a Schedule with Card Lockout and Exit Delay. This mode affects door group access, doors set on auto unlock/lock, and auxiliary input/ shunt and auxiliary output devices that are controlled by the selected schedules.

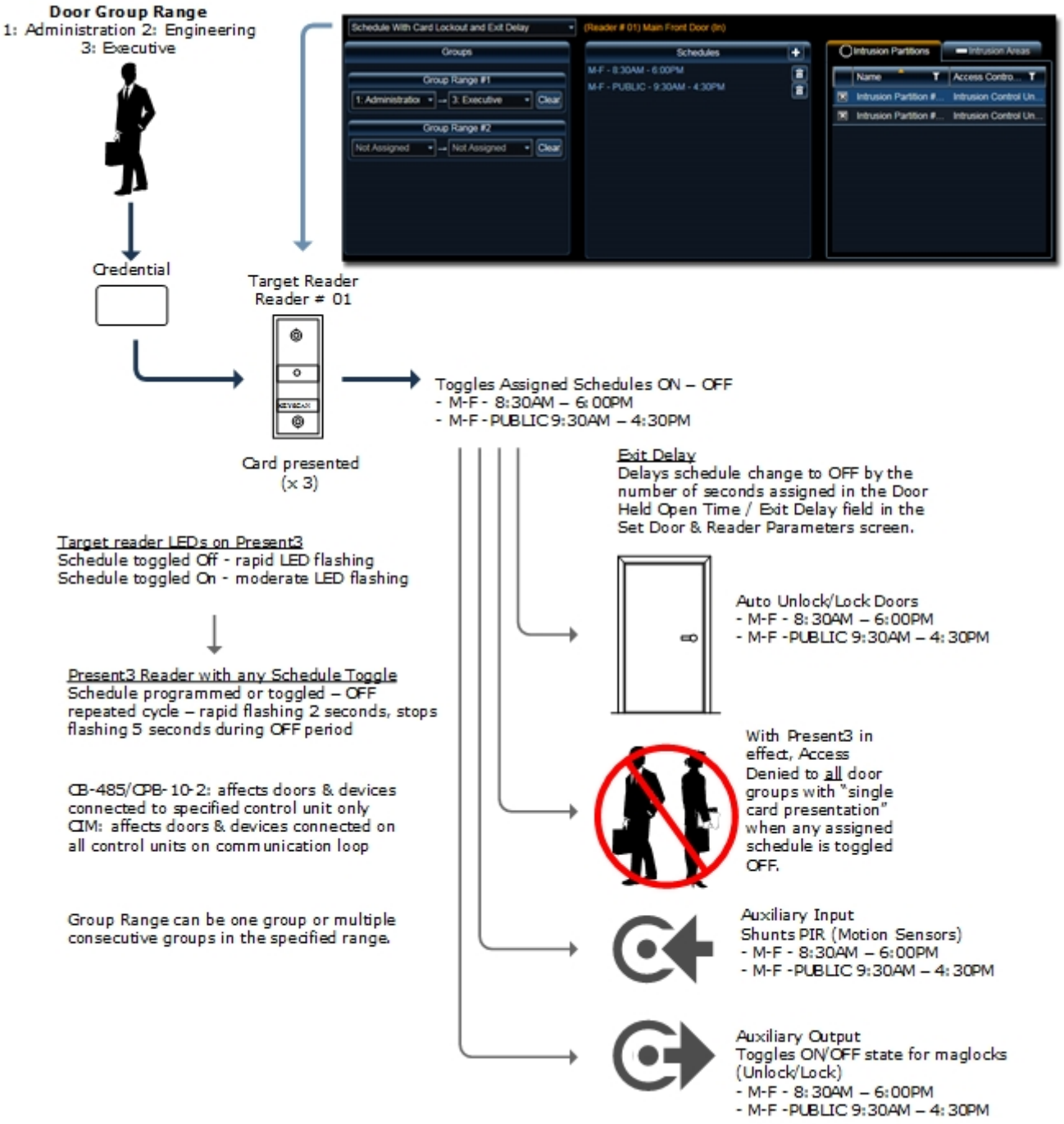
The Door Held Open Time / Exit Delay field is set in the Hardware Setup > Doors screen. The exit delay can be from 1 - 99 seconds. This mode can be cancelled to stop the schedule from being toggled off after the initial P3 credential presentation. To cancel this mode, repeat presenting the card 3 times within the Exit Delay time.

While Present 3 is in effect and the schedules specified under Schedule Assignment are toggled OFF, all credential holders in all door groups are denied access with a "single card presentation".

Alarm Panel Intrusion Integration

This mode is also used in conjunction with alarm panel integration for arming and disarming intrusion partitions or intrusion areas. The exit delay only applies a delay in toggling the schedule change of state for Keyscan points. It does not apply a delay in arming and disarming the partitions or areas. In addition, a schedule change of state does not toggle a partition or area.

Example of Schedule with Card Lockout and Exit Delay



Schedule without Card Lockout

- toggles specified schedules - ON or OFF

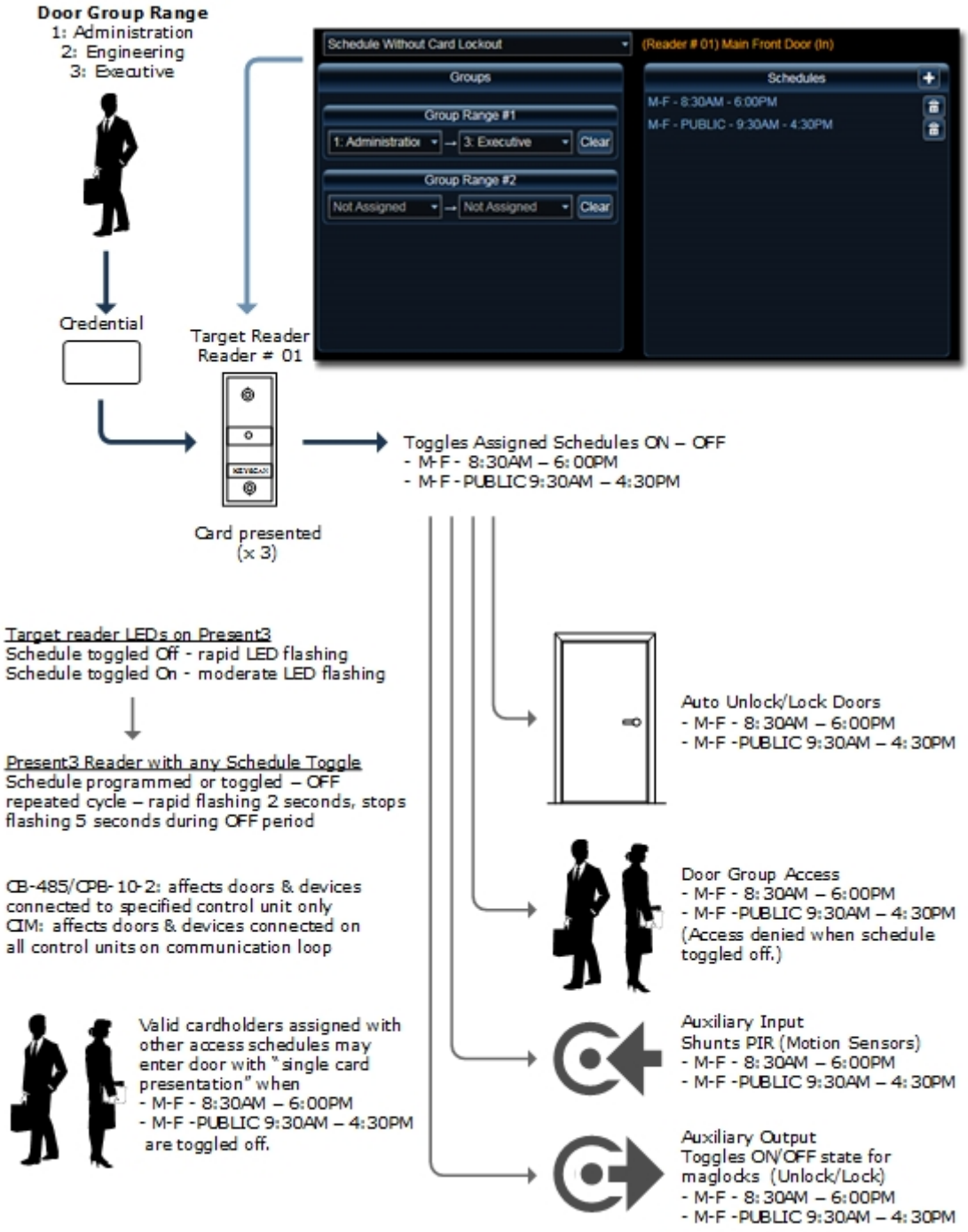
Change of State

- Schedule to ON - immediate
- Schedule to OFF - immediate

Affects

Only credential holders in selected door groups at a specified target reader can affect a Schedule without Card Lockout. This mode affects door group access, doors set on auto unlock/lock, and auxiliary input/shunt and auxiliary output devices that are controlled by the selected schedules.

Example of Schedule without Card Lockout



Schedule with Card Lockout and Enter/Exit Delay

- toggles specified schedules - ON or OFF

Change of State

- Schedule to ON - occurs after # of seconds specified in the Door Held Open Time / Exit Delay field has elapsed

- Schedule to OFF - occurs after # of seconds specified in the Door Held Open Time / Exit Delay field has elapsed

Affects

Only credential holders in selected door groups at a specified target reader can affect the Schedule with Card Lockout, Exit & Entry Delay. This mode affects door group access, doors set on auto unlock/lock, and auxiliary input/shunt and auxiliary output devices that are controlled by the selected schedules.

The Door Held Open Time / Exit Delay field is set in the Hardware Setup > Doors screen. The exit delay can be from 1 - 99 seconds. This mode can be cancelled to stop the schedule from being toggled off after the initial P3 credential presentation. To cancel this mode, repeat presenting the credential 3 times within the Door Held Open Time / Exit Delay time.

While Present3 is in effect and the schedules specified under Schedule Assignment in the Present3 Setup screen are toggled OFF, all credential holders in all door groups are denied access with a "single card presentation".

Intrusion Control Unit Integration

This mode is also used in conjunction with alarm panel integration for arming and disarming partitions or areas. The enter & exit delays only apply a delay in toggling the schedule change of state for Keyscan points. This mode does not apply a delay in arming and disarming the partitions or areas. Also a schedule change of state does not toggle a partition or area.

Not Used

Not Used clears the previous Present3 mode for the selected reader.

Using Present3

Credential holders in groups assigned to use Present3, just as its name implies, present their credential 3 times in succession at a designated target reader. Each successive credential presentation must occur within 1.5 seconds of the preceding credential presentation. When using the door toggle mode or one of the schedule toggle modes, the reader's LED flashes as listed below indicating that the door or schedule is being toggled:

- Door toggled to lock - rapid LED flashing
- Door toggled to unlock - moderate LED flashing
- Schedule toggled OFF - rapid LED flashing
- Schedule toggled ON - moderate LED flashing

The Online Transactions screen displays the relevant details whenever a door or schedule has been toggled.

SETUP PRESENT3

Present3 has five modes of operation. Instructions to setup each mode are listed below under Procedures.

Present3 is based on group assignments. One or a consecutive range of groups can be selected. Present3 usage is regulated by the door group access, either 24 hours or the schedule hours.

Note +

Group assignments for Present3 cannot be higher than group #255.

Avoid using keypads, biometric readers or keypad/proximity readers configured for either Card or Keypad or Card and Keypad modes when assigning a target reader for Present3. These types of readers or reader modes may not transmit the credential data to the ACU within the required time frame for enacting P3.

Credential Holders with Multiple Group Access Assignments

Where credential holders have multiple group assignments with valid access at the Present3 target reader, note the following rule. The group with the lowest group number in the Edit Person screen must be either the first P3 group in a range or the only P3 group in the Present3 Setup screen. You can verify the actual group numbers under the Number column in the Group Setup screen. Refer to the example below.

Example

As an example, a credential holder has three group access assignments - Group #1, Group #2 and Group #3. All three groups have valid access at the assigned Present3 target reader. If the Present3 Group Assignment was Group #2 or higher, be it a single group or a consecutive range of groups, this credential holder would not be able to initiate Present3 as Group #1 would trigger an access granted or access denied depending on the assigned schedule. In this example Group #1 must be in the Present3 Group Assignment. This example uses the default group names. If you have renamed your groups, the group number is identified under the Number heading in the Group Setup screen.

Keyscan strongly recommends not using the First Person In function with Present3.

Procedures

Steps to Setup Door Toggle Mode

1. From the Client main screen, select the Site Management button > Present3 Setup.
    - If you have multiple sites, double click on the desired site in the Site Search - Present3 Setup directory screen.
2. If the correct control unit is currently displayed near the top of the screen go to the next step; otherwise click on the ▼ symbol to the right of the control unit currently displayed and select the desired unit from the drop down list.
3. Opposite the reader you are going to assign for toggling the door lock off and on, click on the ▼ symbol to the left of the (Reader # x) and select Door Toggle from the drop down list.
4. Below Groups, click on the ▼ symbol in the left box under Group Range # 1 and from the drop down list, select the first group that can toggle the door lock using Present 3.
5. Click on the ▼ symbol in the right box under Group Range # 1 and select either the same group chosen in the preceding step if only one group is to use the door toggle mode or select the group that is the last group in the range of groups to use the door toggle mode.
    - If you inadvertently select the wrong groups, click on the Clear button and repeat the step.
6. To create a second range of groups, repeat the preceding two steps using the Group Range #2 boxes; otherwise go to the next step.
7. Click on the Save button.

8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Setup Schedule with Card Lockout

1. From the Client main screen, select the Site Management button > Present3 Setup.
    - If you have multiple sites, double click on the desired site in the Site Search - Present3 Setup directory screen.
2. If the correct control unit is currently displayed near the top of the screen go to the next step; otherwise click on the symbol to the right of the control unit currently displayed and select the desired unit from the drop down list.
3. Opposite the reader you are going to assign as the target reader for toggling the schedule with card lockout, click on the symbol to the left of the reader # and select Schedule with Card Lockout.
4. Under Groups, click on the symbol in the left box below Group Range # 1 and from the drop down list, select the first group that can toggle the schedules with Present 3.
5. Click on the symbol in the right box below Group Range # 1 and select either the same group chosen in the preceding step if only one group is to use Present3 or select the group that is the last group in the range of groups to use Present3.
    - If you inadvertently select the wrong groups, click on the Clear button and repeat the step.
6. To create a second range of groups, repeat the preceding two steps using the Group Range #2 boxes; otherwise go to the next step.
7. At the right of Schedules, click on the + symbol.
8. From the Schedules pop-up window, click on the < symbol opposite the schedule to toggle on and off.
    - If you select the wrong schedule, click on the delete button (waste bin icon).
9. To add more schedules, repeat the above two steps.
10. Click on the Save button.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Setup Schedule with Card Lockout and Exit Delay

1. From the Client main screen, select the Site Management button > Present3 Setup.
    - If you have multiple sites, double click on the desired site in the Site Search - Present3 Setup directory screen.
2. If the correct control unit is currently displayed near the top of the screen go to the next step; otherwise click on the symbol to the right of the control unit currently displayed and select the desired unit from the drop down list.
3. Opposite the reader you are going to assign as the target reader for toggling the schedules with card lockout, click on the symbol to the left of the reader # and select Schedule with Card Lockout and Exit Delay.
4. Under Groups, click on the symbol in the left box below Group Range # 1 and from the drop down list, select the first group that can toggle the schedules with Present 3.
5. Click on the symbol in the right box below Group Range # 1 and select either the same group chosen in the preceding step if only one group is to use Present3 or select the group that is the last group in the range of groups to use Present3.
    - If you inadvertently select the wrong groups, click on the Clear button and repeat the step.
6. To create a second range of groups, repeat the preceding two steps using the Group Range #2 boxes; otherwise go to the next step.
7. Under Schedules, click on the + symbol.

8. From the Schedules pop-up window, click on the < symbol opposite the schedule to toggle on and off.
    - If you select the wrong schedule, click on the delete button (waste bin icon).
9. To add more schedules, repeat the above two steps.
10. Do one of the following steps based on the intrusion control unit:
    - DSC - select the Intrusion Partitions tab; position the cursor on the row under the Name/Access Control and click in the box on the left to select the intrusion unit/partition that will be armed and disarmed with Present3. When selected the box has an x.
    - DMP - select the Intrusion Areas tab; position the cursor on the row under the Name/Access Control and click in the box on the left to select the intrusion unit/area that will be armed and disarmed with Present3. When selected the box has an x.
11. Click on the Save button.
12. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Change the Door Held Open /Exit Delay time

The Door Held Open / Exit Delay field has a default time of 25 seconds in the Hardware Setup > Doors > screen. If you wish to change the exit delay time from 25 seconds, follow the instructions below, otherwise the exit delay is set to 25 seconds unless previously changed.

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the desired site in the Site Search – Hardware Setup directory screen.
2. From the Hardware Setup screen with the All Hardware tab selected, double click on the appropriate control unit connected to the door you are going to change the Door Held Open/Exit Delay setting.
3. Opposite the applicable Door #, click on the v symbol to open the Door Setup screen.
4. Locate the Door Held Open/Exit Delay setting and click on the symbol and select a time from the drop down list. The times are in seconds.
5. Click on the Save button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Setup Schedule without Card Lockout

1. From the Client main screen, select the Site Management button > Present3 Setup
    - If you have multiple sites, double click on the desired site in the Site Search - Present3 Setup directory screen.
2. If the correct control unit is currently displayed near the top of the screen go to the next step; otherwise, click on the symbol to the right of the control unit currently displayed and select the desired unit from the drop down list.
3. Opposite the reader you are going to assign as the target reader for toggling the schedules with cardholder lockout, click on the symbol to the left of the reader # and select Schedule without Card Lockout.
4. Under Groups, click on the symbol in the left box of Group Range # 1 and, from the drop down list, select the first group that can toggle the schedules using Present 3.
5. Click on the symbol in the right box on Group Range # 1 and select either the same group chosen in the preceding step if only one group is permitted to use the Present3 mode or select the group that is the last group in the range of groups to use the Present3 mode.
    - If you inadvertently select the wrong groups, click on the Clear button and repeat the step.

6. To create a second range of groups, repeat the preceding two steps using the Group Range #2 boxes, otherwise go to the next step.
7. Under Schedules, click on the + symbol.
8. From the Schedules pop-up window, click on the < symbol opposite the schedule to toggle on and off.
    - If you select the wrong schedule, click on the delete button (waste bin icon).
9. To add more schedules, repeat the above two steps.
10. Click on the Save button.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Setup Schedule with Card Lockout, Exit and Entry Delay

1. From the Client main screen, select the Site Management button > Present3 Setup.
    - If you have multiple sites, double click on the desired site in the Site Search - Present3 Setup directory screen.
2. If the correct control unit is currently displayed near the top of the screen go to the next step; otherwise click on the symbol to the right of the control unit currently displayed and select the desired unit from the drop down list.
3. Opposite the reader you are going to assign as the target reader for toggling the schedules with card lockout, exit and entry delay, click on the symbol to the left of the reader # and select Schedule with Card Lockout and Exit and Entry Delay.
4. Under Groups, click on the symbol in the left box below Group Range # 1 and from the drop down list, select the first group that can toggle the schedules with Present 3.
5. Click on the symbol in the right box below Group Range # 1 and select either the same group chosen in the preceding step if only one group is to use Present3 or select the group that is the last group in the range of groups to use Present3.
    - If you inadvertently select the wrong groups, click on the Clear button and repeat the step.
6. To create a second range of groups, repeat the preceding two steps using the Group Range #2 boxes; otherwise go to the next step.
7. Under Schedules, click on the + symbol.
8. From the Schedules pop-up window, click on the < symbol opposite the schedule to toggle on and off.
    - If you select the wrong schedule, click on the delete button (waste bin icon).
9. To add more schedules, repeat the above two steps.
10. Do one of the following steps based on the intrusion control unit:
    - DSC - select the Intrusion Partitions tab; position the cursor on the row under the Name/Access Control and click in the box on the left to select the intrusion unit/partition that will be armed and disarmed with Present3. When selected the box has an x.
    - DMP - select the Intrusion Areas tab; position the cursor on the row under the Name/Access Control and click in the box on the left to select the intrusion unit/area that will be armed and disarmed with Present3. When selected the box has an x.
11. Click on the Save button.
12. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Change the Door Held Open /Exit Delay time

The Door Held Open / Exit Delay field has a default time of 25 seconds in the Hardware Setup > Doors > screen. If you wish to change the exit delay time from 25 seconds, follow the instructions below, otherwise the exit delay is set to 25 seconds unless previously changed.

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the desired site in the Site Search – Present3 Setup directory screen.
2. From the Hardware Setup screen with the All Hardware tab selected, double click on the appropriate control unit connected to the door you are going to change the Door Held Open/Exit Delay setting.
3. Opposite the applicable Door #, click on the v symbol to open the Door Setup screen.
4. Locate the Door Held Open/Exit Delay setting and click on the symbol and select a time from the drop down list. The times are in seconds.
5. Click on the Save button.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Clear an Existing Present3 Mode

1. From the Client main screen, select the Site Management button > Present3 Setup.
    - If you have multiple sites, double click on the desired site in the Site Search - Present3 Setup directory screen.
2. If the correct control unit is currently displayed near the top of the screen go to the next step; otherwise click on the symbol to the right of the control unit currently displayed and select the desired unit from the drop down list.
3. Opposite the reader you are going to clear the Present3 mode, click on the symbol to the left of the reader # and select Not Used.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Present3 Modes

Groups

Lockdown - Doors and Elevator Floors

The door and elevator lockdown function immediately issues a lock command for all assigned doors, wireless locks or elevator floors when emergency situations arises. A lockdown can be triggered using one of the following methods depending on how your site has been configured:

- from the Client software's Lockdown interface screen
- from a triggering device, such as a key switch or a push button, connected to an assigned lockdown auxiliary input
    - triggering device not applicable for CA150 door control units, CA8WL series control units, or elevator control units

Hardware Requirements

The door and elevator lockdown function requires the following control board versions:

- PC1094 or higher door control units
- PC115x CA150 single door control unit
- PC109x or higher elevator control units
- KC Series Control Units

Enabling this feature requires setting specific jumpers or DIP switches on the control board which should only be performed by your dealer/installer. If you are unsure whether you have the necessary hardware and whether the control boards have been configured for door/elevator lockdown mode, Keyscan recommends that you contact your dealer/installer before attempting to use this function.

For dealers/installers, refer to the Aurora Documents folder (included with the Aurora Installation files) for information on configuring the Lockdown Doors and Elevator Floors function.

Set System User Accounts for Lockdown

System users who are designated to access and operate the lockdown from the Client software interface screen must have - Can Lockdown - enabled in their system user accounts. Authorized system users access the Lockdown interface via the Status button.

Procedure

Steps to Set a System User Account for Lockdown

1. From the main screen, select the Settings button > Manage System Users.
2. From the User Search directory screen, double click on the name of the individual in the table.
3. From the Manage System User screen, click in the box to the left of Can Lockdown below the Permissions heading. The box has an x when the function is enabled.
4. Click on the Save button.
5. If enabling Can Lockdown on another system user account, click on the navigation history button and select User Search, then select the next individual and repeat the previous two steps above.
6. When finished, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Operate the Lockdown

The Lockdown interface screen has the following three functions:

- locks the doors or elevator floors controlled by the selected access control units or elevator control units
- disables or clears the lockdown
- lists the lockdown status - Locked Down or Not Locked Down - for the specified access control units or elevator control units (not supported indicates the status is undetermined)

The following three sections review the procedures for performing each function.

Initiate a Lockdown via the Client Software

These procedures outline how to initiate a door or elevator lockdown from the Client software. Please remember, the system user account must have the Can Lockdown function enabled for initiating a lockdown.

Procedure

Steps to Initiate a Lockdown

1. From the main screen, click on the Status button > Lockdown.
2. Verify the correct site is listed opposite Site. To change sites, click on the ▼ symbol and select the site from the drop down list.
3. Do one of the following steps:
    - If the lockdown applies to all listed control units, click in the box to the left of Access Control Unit. All the units are selected as indicated by the x.
    - If the lockdown only applies to some of the control units, select the specific control units by clicking in the box to the left. Selected units have an x in the box.
4. Click on "Enable Lockdown for Selected Access Control Units".
    - Below the Status heading, the affected control units are listed as Locked Down.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

When a lockdown is in effect, individuals may still use their credentials to gain entry at locked doors they are normally authorized to access.

If the control board was configured with the Reader LED Lockdown Mode - ON, the reader's LED flashes rapidly indicating a lockdown is in effect.

Clear a Lockdown

This procedure outlines how to clear a lockdown. If the lockdown was previously initiated by a device connected to the designated lockdown auxiliary input, that device must be re-set or returned to its 'normal' state before the lockdown can be cleared in the Client software.

Procedure

Steps to Clear a Lockdown

1. From the main screen, click on the Status button > Lockdown.
2. Verify the correct site is listed opposite Site. To change sites, click on the ▼ symbol and select the site from the drop down list.
3. Do one of the following steps:
    - If the Clear Lockdown applies to all listed control units, click in the box to the left of ACU. All the units are selected as indicated by the x.

- If the Clear Lockdown only applies to some of the control units, select the specific control units by clicking in the box to the left. Selected units have an x in the box.

4. Click on "Disable Lockdown for Selected Units".
    - The status changes to Not Locked Down.

5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Doors that were on auto unlock will follow the schedule assignment.

- if the lockdown is cleared while the schedule is ON the door will unlock until the schedule turns OFF
- if the lockdown is cleared after the schedule has turned OFF, the door will remain locked until the next scheduled start time

Enhanced Lockdown

The Enhanced Lockdown function is designed to lock doors on Keyscan ACUs/ECUs or E-Plex door locks. This feature can also be used to toggle a Schedule ON or OFF, as defined within the Enhanced Lockdown Setup screen.

Utilizing the Enhanced Lockdown feature for **Access Control Units** (ACUs/ECUs) will cause doors associated with that panel to enter a locked state; however, people with applicable credentials can still gain access through the door. Using Enhanced Lockdown for **E-Plex Doors** will cause a hardware lockdown, only Master and/or Manager credentials will have access through the door in this state. For **Schedules**, any credentials associated with the Group Access assigned to the Schedule will no longer work, unless toggled back to an ON state. Enhanced Lockdown for all of the preceding options can be configured through the Enhanced Lockdown Setup screen.

Requirements

The Enhanced Lockdown function requires the following:

- PC1097 or higher ACUs/ECUs
- Aurora software client version 1.0.19.0. or higher
- Enhanced Lockdown License (Product #EAUR-911)

Enabling this feature requires setting-specific DIP switches on the control board, which should only be performed by your dealer/installer. If you are unsure whether you have the necessary hardware and whether the control boards are configured for Enhanced Lockdown, we recommend contacting your dealer/installer before attempting to use this function.

For dealers/installers, refer to Document #KD10059-E for wiring layouts and setup.

Enhanced Lockdown Setup

The first step in this process is to set up the parameters of an Enhanced Lockdown prior to applying them to Access Control Units, E-Plex Doors and/or Schedules. Follow these steps to determine the parameters before implementation:

1. In the Aurora software Main Menu, select Enhanced Lockdown Setup under the Application Management menu.
2. If starting a new Lockdown, select the plus symbol (**+**) located at the top-left of the screen. If editing an existing Lockdown, select it from the drop down menu at the top of the screen.
3. From the Sites sub-menu, select the applicable Site(s). Sites are selected when an **x** symbol appears inside the box beside them.
4. On the right-hand sub-menu, fill in the following fields:
    - **Name** - Use a descriptive name for the Enhanced Lockdown
    - **Code** - A code will be used to identify a specific lockdown within the Enhanced Lockdown desktop application

      Note: Each Enhanced Lockdown requires its own Code, do not copy Codes across multiple lockdowns. While it is not necessary to remember each Code, we recommend backing up the database once all codes and lockdowns are defined.

1.
   - **Password** - Enter a password to be used within the Enhanced Lockdown desktop application
   - **Description** - This may include what the lockdown affects, which schedules change, etc.

The following steps should only be taken after the parameters are identified in the Access Control Units, E-Plex Doors and/or Schedules tabs. These steps confirm and implement the Enhanced Lockdown:

1. By default, the button located on the bottom-right of the screen is red and labelled Inactive. Press the button to select Active with a green button.
2. Select Save.
3. To print an Enhanced Lockdown Setup report, select the print icon at the top of the screen, beside the Lockdown drop down menu.
4. To create a desktop shortcut for the Enhanced Lockdown application, select the arrow icon beside the print icon at the top of the screen.
5. Navigate to your desktop and double-click the Enhanced Lockdown desktop application shortcut. The application will be named whatever was inputted into the Name field prior. In the application, enter the Password to trigger the Enhanced Lockdown.

   Note: Each Enhanced Lockdown will have its own desktop application shortcut, making what you input into the Name field important for identification.

Access Control Units

In the Access Control Units tab, select ACUs/ECUs from the list. An access control unit is selected when an **x** symbol appears inside the box beside it. Selected ACUs/ECUs will be included within the current Enhanced Lockdown. De-select any access control units you do not wish to be included. Select the Save button to confirm.

E-Plex Doors

In the E-Plex Doors tab, select doors from the list. An E-Plex Door is selected when an **x** symbol appears inside the box beside it. Selected doors will be included within the current Enhanced Lockdown. De-select any doors you do not wish to be included. Select the Save button to confirm.

Schedules

In the Schedules tab, select schedules from the list. A Schedule is selected when an **x** symbol appears inside the box beside it. Selected schedules will be included within the current Enhanced Lockdown. De-select any schedules you do not wish to be included. Select the Save button to confirm.

Note: Selecting to Toggle On a Schedule will enable it to work as normal, Toggle Off will disable it.

Manually Revert Enhanced Lockdowns

Besides toggling Enhanced Lockdowns through the Active/Inactive button in the Enhanced Lockdown Setup screen and using the Enhanced Lockdown desktop application, there is a third way to manually revert lockdowns for Access Control Units, E-Plex Doors and Schedules.

Reverting ACU/ECU/E-Plex Door Lockdowns

Follow these steps to disable or enable an ACU/ECU/E-Plex Door Enhanced Lockdown:

1. In the Aurora software Main Menu, select Lockdown under the System Status and Control menu.
2. From the applicable sub-menu, select the Access Control Units and/or E-Plex Doors from their respective tabs. Access Control Units and/or E-Plex Doors are selected when an **x** symbol appears inside the box beside them.
3. Select either the Enable or Disable buttons located on the top-left and right sides of the screen that will affect the selected items. You can also choose to right-click a selection and select Revert to Schedule State.

Reverting Schedule Lockdowns

Follow these steps to disable or enable a Schedule Enhanced Lockdown:

1. In the Aurora software Main Menu, select Status under the System Status and Control menu.
2. Select Schedule Status from the left menu.
3. In the Schedule Status menu, select the Site and Access Control Unit (if applicable) from their respective drop down menus at the top of the screen.
4. Select schedules from the list. A Schedule is selected when an **x** symbol appears inside the box beside it.
5. Select Toggle at the bottom of the screen to change the Schedule Off/Schedule button for each selected Schedule.

Application Utilities

The Application Utilities screen has various switches and fields that enable Aurora for various functions. Select the links below for information on each utility.

Application Settings

- Person Type
- Reason for Disabling Logging
- Refresh Timer
- Corporate ID (Hex)
- Enable Middle Name
- Extended PIN (7 digit)
- Auto Generate PIN
- Enforce Complex Passwords
- Auto Delete on Expiry
- Kaba Integrated Mode
- Enable Keyscan Credentials for Extended Card Format
- Logging Level
- Password Expiry
- Allowed Login Attempts
- Auto Shutdown Time
- Bypass Password Reset Requirement For New Users
- Auto Clear Alarms
- Auto Clear All Alarms
- Reduce Photos
- Intrusion Delay
- Calibrate Scanner
- Clean Scanner

Server Settings

- SMTP Setup
- Output File
- UDP
- Active Directory
- Communication Server Setup
- Configure Database Connection Settings

Advanced

- CMAC Features - Forced Site Selection
- CMAC Features - Site Notes Popup
- Custom Person Unique Identifier
- Custom Site Unique Identifier

Auto Shutdown Time

The Auto Shutdown Time function automatically closes the software and logs the User out completely after a specified amount of time. The Auto Shutdown Time will trigger when the computer sits idle for the time, in minutes, specified in the User Settings in the Aurora software client.

Note: Any unsaved data will be lost if the Auto Shutdown Time triggers. The User will be forced to re-launch the application and re-enter their login credentials.

Procedure

Steps to Set Auto Shutdown Time

1. From the Client main screen, select the Settings button > Application Utilities.
    - The settings in the Application Utilities screen apply to all sites
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Under the User Settings sub-menu, fill in the Auto Shutdown Time field with the desired time in minutes (between 1 - 999). Inputting a value of 0 (set by default) will render the feature inactive.
4. Select the Save button.

Gateway Setup

The Gateway Setup screen is used to set up and configure E-Plex wireless gateways that are used to provide two-way communication from E-Plex lock(s) to the central E-Plex server.

Note: Please see the Aurora E-Plex Integration Setup page under Related Topics at the bottom of this screen to help setup and install E-Plex services and configure a gateway to pair with the Aurora software.

The table below outlines each field and its purpose within the Aurora software:

Name	The name or description that can easily identify the gateway. For example, where the gateway is located: "Main Office".
Channel	A radio frequency (RF), using a ZigBee wireless protocol, that E-Plex locks use to communicate with E-Plex gateways.
MAC Address	The MAC address of the E-Plex gateway.
Server Name	The name of the computer hosting E-Plex services used by the gateway to process information between E-Plex locks and the Aurora software.
Server IP Address	The IP address of the computer hosting E-Plex services that the gateway will communicate with.
Connection Type	The way in which the E-Plex gateway is connected to the E-Plex server. The device can be physically connected through a USB cable to the machine hosting E-Plex services or the device can be connected, using a network cable, to the network that E-Plex services are also on.

Select the Configure button to complete Gateway setup once all fields are filled out.

Routers

E-Plex gateways can be configured to be a router. When the device is configured as a router, it acts as a repeater to extend an existing E-Plex gateway's radio frequency so that the gateway can reach wireless locks that are too far away. The router's grid on this screen displays details about any E-Plex router that is being used by the gateway. It will only show information if a router is being used in unison with a gateway paired to an E-Plex wireless lock. If used, the following fields populate:

- MAC Address
- AVR Boot Version
- AVR Version
- Ember Version
- Controller Version

Related Topics

Aurora E-Plex Integration Setup

E-Plex Gateway Setup

This section outlines how to set up and configure an E-Plex Gateway (either the Multi-Segment Gateway or legacy gateways) to work with the Aurora software client. The below instructions assumes the gateway hardware is previously assembled and in good working order. For more information on hardware set up, please refer to the gateway's hardware document.

> **IMPORTANT:** Prior to configuration, ensure you are running Microsoft .net Framework 4.8 or above and possess Local Administrator privileges. Before opening the software, right-click on the Aurora .exe file and select "**Run as Administrator**".

Root Certificate

First, a Root Certificate needs to be created, to act as the certificate authority for others stored in the database. Follow these steps to properly generate a Root Certificate:

1. Under the Settings menu, select Application Utilities.
2. In the Security tab, select Create CA root certificate.
3. After a few seconds, the button will change to Export CA root certificate. Select the button.
4. The Export file path window will appear. Select the Browse button to choose the file path to your computer. Name the file and select Save once a path and name are finalized. Select Export to complete the process.
5. Navigate to the computer file path selected in the previous step. Right-click the file and select Install Certificate.
6. Navigate through the Certificate Import Wizard as normal, select Finish when reaching the end. A window will pop up, confirming installation success. For further details on navigating the steps of the Wizard, see E-Plex Service Setup

E-Plex Server Certificate

Next, an E-Plex Gateway needs to be set up and a certificate for the E-Plex server needs to be created.

To add an E-Plex Gateway and create an E-Plex server certificate, follow these steps:

1. Under the Settings menu, select Application Utilities.
2. On the upper-left tab, select Gateway Setup.
3. Click on the plus-sign [+] on the top left of the screen to add a new Gateway.
4. Name your Gateway, select a channel (if unsure, select All), select between a USB or a Network Connection Type and select Save on the bottom right of the screen. The Server Name and Server IP are auto populated.
5. In the Security tab, input the server IP/hostname and select Create new certificate.
6. To create and add a certificate, follow either method I or II below:
    I. "Import Into Store" option (adds/installs certificate to store automatically)
        a. Click the "Import Into Store" button next to the certificate you just created
        b. If the import was successful, you will see a green checkmark next to the certificate. A red X indicates the certificate was not added successfully.
        c. If this does not work, attempt the "Export PKCS file" option (described below)

II. "Export PKCS" option (add/install certificate manually using Wizard)
    a. Click the "Export PKCS file" button next to the certificate you just created
    b. The Export filepath window will appear. Select the Browse button to choose the file path to your computer. Name the file and select Save once a path and name are finalized. Input a password and select Export.
    c. Navigate to the computer file path selected in the previous step. Right-click the file and select Install PFX.
    d. Navigate through the Certificate Import Wizard as normal, select Finish when reaching the end. A window will pop up, confirming installation success. For further details on navigating the steps of the Wizard, see E-Plex Service Setup

Gateway Hardware Configuration

The final step is to configure the gateway hardware with the newly created root certificate to communicate with the server through an encrypted channel. Follow these steps to configure the Gateway:

1. Under the Settings menu, select Application Utilities.
2. On the upper-left tab, select Gateway Setup.
3. If using a USB connection, press and hold the reset button on the Gateway and plug it into the USB port of the computer. Release the reset button once a USB connection is made.
4. The Gateway will flash green and red LEDs as it prepares for configuration. When the Gateway flashes only green, select Configure in the Aurora software.
5. When the process is complete, the following messages will appear on screen:

   Gateway configured successfully!

   If you wish to configure more E-Plex Gateways, please select NO. If you are finished configuring all E-Plex Gateways, wait until the Gateway reboots before selecting YES. Selecting YES restarts the local E-Plex Server Service to ensure that the new Gateway(s) connect to that server. If the E-Plex Server Service is on a remote computer, you will need to restart the E-Plex Server Service and/or reboot the computer to ensure the new E-Plex Gateway(s) connect correctly.

   Note: Do not unplug the Gateway from the computer until the red LED is off, as doing so may disrupt the configuration process.

Procedures

Steps to Join an E-Plex Gateway as a Router

1. Ensure the router is [re]set to factory settings before continuing.
2. Set the Gateway you wish to pair with the Router to Join On Mode from the Gateway Status widget, found in the Status Window. The Gateway's green and red LEDs will blink in unison at 0.5 Hz.
3. Power the Router on and wait until the green LED blinks at 0.5 Hz, the red LED should not turn on during this time.
4. Press the reset button on the Router once.

   If successful, both Router LEDs (green and red) will blink in unison at 0.5 Hz. Otherwise, the red LED will remain off and the green LED will blink at 0.5 Hz.
5. If successfully joined, the Router will be displayed under the Routers sub menu, located under the E-Plex and Gateway Settings tab under Application Utilities.

Steps to Join an E-Plex Door with a Gateway

Note: Aurora only allows one Gateway to be placed in Join On Mode at a time, so keep this in mind during installation.

1. Set the Gateway to Join On Mode through the Gateway Status utility.
2. Wait until the Gateway enters Join Mode.
3. Go to the Hardware Setup menu from the main screen and open the Door Group that the new E-Plex door/lock belongs to.
4. Record the name and ZAC codes for each door that will join the Gateway.
5. For each door/lock, walk over to the E-Plex door/lock that you want to join the Gateway, ensure that the lock is in Factory Default Mode with the factory default Master PIN. Enter the lock's 8-digit unique ZAC (ZigBee Access Code) number at the lock's keypad by entering ##088#[ZAC]# into the keypad.

Extended PIN (7 digit)

The Extended PIN setting on the Application Utilities screen will allow for 7 digit pins to be generated/entered on a credential and enable the ability to set Extended PIN for a panel. If unchecked, all PINs greater than 65535 will be set to 0 and Extended PIN will be removed from all panels with it enabled.

If a panel is sent a PIN that is greater then 65535 and is not set for Extended PIN, it will be set to 0 (not used).

Procedure

Steps to Activate the Extended Pin Function

1. From the Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Application Settings tab is selected.
3. Under the Card Settings heading, click in the box to the right of Extended PIN (7 digit). The box has an x when the function is enabled.
4. Click on the Save button.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Reset Status Window Position

The Status screen can be re-sized and re-positioned on your monitor to suit your personal preferences. If you elect changing the size or position, Aurora retains the changes when you access the Status screen on subsequent log in sessions.

- To re-size the Status screen, position the cursor over a corner or one of the sides and click and drag until it reaches the desired size
- To re-position the Status screen, position the cursor over the Status screen's title bar at the top and click and drag to its desired position - depending on the screen resolution the Status screen may be the full size of the monitor when initially opened

Each of the individual status screen "widgets" can also be re-sized, re-positioned or undocked from the Status screen entirely.

- To re-size a Status widget screen, position the cursor over a corner or one of the sides and click and drag until it reaches the desired size
- To re-position a Status "widget" screen, position the cursor over the screen's title bar at the top and click and drag to its desired position
- To undock a Status "widget" screen, as above, position the cursor over the screen's title bar at the top and click and drag to its desired position outside the boundaries of the Status screen

Reset the Status Screen

The Reset Status Window Position button can be accessed by clicking on the System Health icon, red, yellow or blue depending on system conditions, in the upper left of any Aurora screen. When selected, the Reset Status Window Position button re-positions the Status screen and any status widgets that are contained within the Status screen to the upper left corner of the monitor. Any status widgets that are outside the Status screen are unaffected.

Related Topics

Alarm Monitoring & Alarm Response

Transaction Response

The Transaction Response screen is used to view new/pending transactions or search for past transactions within a date range. The Transaction Response screen identifies transactions by the following criteria:

- Site - lists the site where the transaction occurred
- Access Control Unit - identifies the access control unit that registered the transaction
- Device - lists the device as selected under Device Type
- Person - lists the person's name for credential type transactions such as access granted
- Credential - lists the credential number for credential type transactions
- Transaction - lists the specific transaction such as a schedule on or schedule off, or access denied etc.
- Date - lists the month/day/year and time of the transaction
- Status - indicates the status of the transaction: New, On Hold or Completed

Sites

To view the transactions of a specific site, click on the ▼ symbol on the right of Sites and select the desired site from the drop down list. Each user viewing the Transaction Response screen will only have access to sites that have been enabled in the Manage System User screen.

New and Pending / Date Range

When formatting a list of transactions, you have the option of viewing transactions that are current - new and pending - or viewing transactions that occurred in the past - date range.

New and Pending only applies to alarm transaction types. To view normal transaction types, you must select a date range.

Device Type

Use this option to select a specific category of device with the associated types of transactions or select all to list the full range of devices in the Device Type drop down list.

Transaction Type

Use this option to select a specific transaction type associated with the device type or select all to list the full range of transactions in the Transaction Type drop down list.

Transaction Category

Use this option to select the transaction category as outlined:

- All - lists alarm and normal categories
- Alarm – lists any alarm type transactions such as alarm tripped, alarm cleared etc.
- Normal – lists any non-alarm type transactions such as access granted, schedule off etc.

Access Control Unit

Use this option to filter the transactions for the selected access control unit, elevator control unit, or intrusion control unit or select all to list the applicable transactions for all types of units.

Search

Use the Search button to compile the transaction response list after you have specified the parameters or to list new or pending alarms.

For displaying new alarms on-screen, you must click on the Search button.

Clear

Select the Clear button to clear the screen after performing a search. If the Clear button is selected with new or pending alarms on screen, the alarms are cleared from the screen but the status remains unchanged.

Set On Hold / Set Completed / Complete All

The Transaction Response screen has three buttons near the bottom of the screen for either pending a new alarm for investigation or completing the alarm after it has been handled.

Set On Hold

The Set On Hold button changes the status of any new alarms selected in the list view to pending for further investigation. The alarm remains in view until the status is changed to completed.

Set Completed

The Set Completed button changes the status of new or pending alarms in the list to completed and removes them from the screen.

Complete All

The Complete All button changes the status of all new or pending alarms to completed. The Complete All button is only available to system users who have a Master or Administrator designation.

Procedures

Steps to Pend or Complete a New Alarm

1. From the Client main screen, select the Status button > Transaction Response.
2. If you have multiple sites do one of the following steps; otherwise, go to step 3.
    - To view an individual site, click on the ▼ symbol to the right of Sites, and select the desired site from the list.
3. Ensure the radio button to the left of New and Pending is selected.
4. Click on the Search button.
    - Alarms are highlighted in red.
5. Click on the row with the alarm to select it. The selected alarm changes to a blue highlight.
6. Double click on the same row with the alarm transaction to open the Response Instruction screen. If outlined, follow any procedures that have been conveyed in the Instructions box or contact a designated person in the Contacts box or Emergency Contacts box.
    - You will see at the bottom Show Map and Show Video buttons.
    - Show Maps - opens a map showing the location of the device in alarm if a map has been created in the Active Map Template Editor.
    - Show Video - opens a video segment if a device has been associated with the alarm event/camera and Aurora is integrated with a video management system.
7. Depending on the nature of the alarm and the security protocols, you can set the alarm on completed or, pending further investigation, set the alarm on hold. Click on the ▼ symbol opposite Transaction Status and select either Completed or On Hold.

- If you set the alarm on hold and completed the investigation, click on the on the ▼ symbol opposite Transaction Status and select Completed.

8. Notate any commentary about the alarm in the Response Comments box.
9. Click on the Save button.
10. Click on the x in the upper right corner to close the Response Instructions screen and return to the Transaction Response screen.
    - If you have multiple alarms that do not require investigating, you can select the Complete All button on the Transaction Response screen to complete and clear the alarms. This function is only available to system users with Master or Administrator status.
11. To exit the Transaction Response screen, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Run a Transaction Response Search

1. From the Client main screen, select the Status button > Transaction Response.
2. If you have multiple sites do the following:
    - To view an individual site, click on the ▼ symbol to the right of Sites, and select the desired site from the list.
3. Select the radio button to the left of Date Range.
4. Specify a From date and time by clicking on the calendar icon to the right and selecting the month, day and time, and then repeat for the To date and time.
5. Opposite Device Type, click on the ▼ symbol and from the drop down list, select the device.
6. Opposite Transaction Type, click on the ▼ symbol and from the drop down list, select the transaction.
7. Opposite Transaction Category, click on the ▼ and from the drop down list, select the category.
8. Opposite Access Control Unit, click on the ▼ symbol and select the unit in the drop down list.
9. Select the Search button.
    - For transactions that may have Response Instructions, double click on the row of the listed transaction. The Response Instructions screen must have been completed in the Event Setup screen otherwise it will be blank.
10. To perform another search, click on the Clear button and repeat the above procedures starting at step 4.
11. When you have completed reviewing the Transaction Response list, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Response Instructions

Door Status - Manual Overrides

The Door Status screen allows you to view the current status of all doors regulated by access control units in the Keyscan system. From this screen, you can also manually override the door's current state and effect the following changes:

- Lock or unlock individual doors
- Lock or unlock all doors controlled by a specified access control unit
- Unlock a door on a "timed unlock" for a specified period to a maximum of 7 days
- Unlock a door momentarily using "Pulse"

The Door Status screen is accessed from the Status menu > Status.

Important ! Whenever Aurora's Lockdown function is triggered, all doors connected to lockdown-configured control units cannot be manually unlocked, pulsed, or set on a timed unlock. The lockdown affected control units must be restored to a "Not Locked Down" status before the above overrides can be used. If the above manual overrides are inoperable, confirm that a lockdown has not been triggered and that you have the necessary permissions as outlined below.

System User Account

The system user account must have the following permissions enabled to perform any of the above tasks:

- Status Widgets - View Door Status
- Toggle Devices - Can Arm (lock) / Can Disarm (unlock) / Can Pulse / Can Perform Timed Unlock
- Can Revert to Schedule

Door Status Icons

The following is a review of the icons that indicate a door's status. The icons surrounding the door image change to reflect the current status or condition. Below the Review of Door Status Icons is an explanation of the manual commands for changing the door's lock/unlock condition.

Review of Door Status Icons

View as Text/Door Status Icons	Legend
	Each door connected to the listed access control unit in the Door Status screen is graphically represented by a door icon. The name of the door is listed at the top to distinguish each door. This is the name assigned in the Hardware Setup > Doors screen. In the example illustration on the left, the door is currently unlocked by a manual command.

Armed		Indicates the door is locked.
Disarmed		Indicates the door is unlocked.
Auto1		Indicates the last change to the door status was automatic. Automatic is initiated by either a schedule change or a Present3 schedule toggle.
Manual		Indicates the last change to the door status was manual. Manual is initiated by user intervention. User intervention occurs via a command on the Door Status screen, a door lock toggle using Present3, or a lockdown.
Unknown		The current status is unknown as no communication has occurred with the door. Generally this symbol is only present on a new installation or unassigned door/reader terminals on the control board.
Timed		The door is currently on a Timed Unlock command. The door remains unlocked for the full 60 seconds of the last minute. At the end of the timed unlock period, the door re-locks.
Alarm		The door is in an alarm state. The door contacts have been separated without an authorized entry indicating a potential forced entry. The door should be investigated.
Warning		The door is open after the expiration of the Door Held Open time setting in the Hardware Setup > Doors screen. The door should be investigated.
Normal		Indicates an access granted transaction has occurred at the door.

Door Status - Manual Commands

The Door Status screen has six manual door commands to override the current door status.

- Lock - manually locks a door that is currently unlocked
- Unlock - manually unlocks a door that is currently locked
- Pulse - momentarily unlocks a door and then re-locks it (the time duration of the pulse unlock is based on the Door Relay Unlock Time setting in the Hardware Settings > Door screen)
- Timed Unlock - the door is unlocked for a user defined period and then re-locks (the timed unlock may be up to a maximum of seven days)
- Revert to Schedule Setting - restores the door to its programmed schedule setting
- Lock All - locks all the doors connected to the listed control unit on the Door Status screen
- Unlock All - unlocks all the doors connected to the listed control unit on the Door Status screen

Steps to Invoke Manual Door Commands

Manual Door Commands	Procedures
	**Lock** 1. Position the cursor over the applicable door icon. 2. Right click. 3. From the menu, select the Lock command. **Unlock** 1. Position the cursor over the applicable door icon. 2. Right click. 3. From the menu, select the Unlock command. **Pulse** 1. Position the cursor over the applicable door icon. 2. Right click. 3. From the menu, select the Pulse command. **Timed Unlock** 1. Position the cursor over the applicable door icon. 2. Right click. 3. From the menu, select the Timed Unlock command. 4. Do one of the following steps: ◦ For a listed 1 - 5 minute interval, select it. You have set the timed unlock interval. ◦ For Other, which would be a timed unlock period longer than 5 minutes, position the cursor over Other, select the Date & Time icon from the fly-out box and go to the next step. 5. If the unlock period is beyond today's date, select the day in the calendar; otherwise go to the next step. 6. From the time screen, select the desired time when the door re-locks. 7. Click on the Close button. ◦ To change the minutes within the hour, double click on the minutes in the displayed time, and type the minutes. 8. Click on the Set button. ◦ If you want to change the Timed Unlock, repeat the steps.
	Revert to Schedule Setting Sets the door back to its programmed schedule. If you have manually unlocked or locked a door selecting the Revert to Schedule Setting command restores the door to its programmed schedule.



Lock All

1. Click on the Lock All button. All doors are locked that are connected to the listed access control unit.



Unlock All

1. Click on the Unlock All button. All doors are unlocked that are connected to the listed access control unit.



Unlocking a door from the Door Status screen should be used with caution. In cases where someone needs unexpected but momentary access, use the Pulse command which re-locks the door after it has closed.

View as Text

Selecting this option by clicking in the box to the left, changes the screen so the doors are listed in a column with their respective status.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Related Topics

Manage System Users

Lockdown

E-Plex Door Status

The E-Plex Door Status screen allows you to view the current status of all wireless locks. From this screen, you can also manually override the lock's current state and effect the following changes:

- Lock or unlock individual E-Plex doors
- Unlock an E-Plex door momentarily using "Pulse"
- Page a wireless lock to determine its location

The E-Plex Door Status screen is accessed from the Status menu > E-Plex Door Status.

Important ! Whenever Aurora's Lockdown function is triggered, all E-Plex locks connected to lockdown-configured cannot be manually unlocked or pulsed. The lockdown affected wireless locks must be restored to a "Not Locked Down" status before the above overrides can be used. If the above manual overrides are inoperable, confirm that a lockdown has not been triggered and that you have the necessary permissions as outlined below.

System User Account

The System User Account must have the following permissions enabled to perform any of the above tasks:

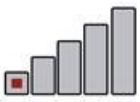
- Status Widgets - View E-Plex Operations
- Toggle Devices - Can Arm (lock) / Can Disarm (unlock) / Can Pulse / Can Perform Timed Unlock
- Can Revert to Schedule

E-Plex Door Status Icons

The following is a review of the icons that indicate an E-Plex door's status. The icons surrounding the door image change to reflect the current status or condition. Below, the Review of Door Status Icons is an explanation of the manual commands for changing the E-Plex door's lock/unlock condition.

Review of Door Status Icons

View as Text/Door Status Icons	Legend
	Each door connected to the listed access control unit in the Door Status screen is graphically represented by a door icon. The name of the door is listed at the top to distinguish each door. This is the name assigned in the Hardware Setup > Doors screen. In the example illustration on the left, the door is currently unlocked by a manual command.

Armed		Indicates the door is locked.
Disarmed		Indicates the door is unlocked.
Auto1		Indicates the last change to the door status was automatic. Automatic is initiated by either a schedule change or a Present3 schedule toggle.
Manual		Indicates the last change to the door status was manual. Manual is initiated by user intervention. User intervention occurs via a command on the Door Status screen, a door lock toggle using Present3, or a lockdown.
Unknown		The current status is unknown as no communication has occurred with the door. Generally this symbol is only present on a new installation or unassigned door/reader terminals on the control board.
Alarm		The door is in an alarm state. The door contacts have been separated without an authorized entry indicating a potential forced entry. The door should be investigated.
Warning		The door is open after the expiration of the Door Held Open time setting in the Hardware Setup > Doors screen. The door should be investigated.
Normal, Low, Dead		Shows the battery level of the wireless lock. Green = Full battery Yellow = Half power Red = Needs to be replaced
Very Good		Indicates the signal strength between the wireless lock and the Gateway as Very Good.
Good		Indicates the signal strength between the wireless lock and the Gateway as Good.
Unacceptable		Indicates the signal strength between the wireless lock and the Gateway as Unacceptable. Consider moving the Gateway closer to the wireless lock to improve the signal strength.

E-Plex Door Status - Manual Commands

The E-Plex Door Status screen has seven manual door commands to override the current wireless lock status.

- Lock - manually locks a door that is currently unlocked

- Unlock - manually unlocks a door that is currently locked
- Pulse - momentarily unlocks a door and then re-locks it (the time duration of the pulse unlock is based on the Unlock Time setting in the Hardware Setup screen under E-Plex Door Details)
- Revert to Schedule Setting - restores the door to its programmed schedule setting
- Page - the wireless lock beeps to identify its location
- Sync - updates the wireless lock with changes made in the Aurora software
- Differential Sync - the Aurora software will send only the information that has been added or changed since the last time the lock was synced
- Full Sync - sends all lock information/settings in the Aurora Software to the lock
- Sync Clock - updates the time on the wireless lock to that of the communications manager
- Request Transactions - gives the user the ability to request an audit of 1-6000 of the most recent transactions from an online lock. From the menu, the user can select an audit of 50, 100, or 500 previous transactions. Alternatively, the user can also request any number of transactions they wish, with a maximum value of 6000.
- Put Out of Service - completely disables a wireless lock (must be reset to work again)
- Lock All - locks all the doors connected to the listed E-Plex wireless lock on the E-Plex Door Status screen
- Unlock All - unlocks all the doors connected to the listed E-Plex wireless lock on the E-Plex Door Status screen
- MultiSync - clicking the MultiSync button opens a window in which you can set a Sync Type (Full or Differential) and a Timeout value (in minutes). The user can apply these Sync settings to any E-Plex Door(s) they choose by selecting them from the provided list. The Sync Type and Timeout values will be remembered in Aurora for next time, though the user can change these settings at any time.



Unlocking an E-Plex wireless lock from the E-Plex Door Status screen should be used with caution. In cases where someone needs unexpected but momentary access, use the Pulse command which re-locks the door after it has closed.

View as Text

Selecting this option by clicking in the box to the left changes the screen so wireless locks are listed in a column with their respective status.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Reader Status

The Reader Status screen is intended to show the status of reader/keypads that have been given schedule assignments using the three reader/keypad modes:

Card Only	Card or Keypad	Card and Keypad
		

Proximity Readers

If using non-reader/keypads, such as proximity readers that only require the use of a card or tag, you can ignore this screen.

Manually Alter the Reader/Keypad Mode

As an option, you can manually set the reader/keypad on one of the above modes or use the restore the schedule assignment with the Revert to Schedule Setting Command.

The reader/keypad will revert to its assigned schedule on the next schedule change if it is manually altered.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

View as Text

Selecting this option by clicking in the box to the left, changes the screen so the readers are listed in a column with their respective status.

Procedure

Steps to Alter the Reader/Keypad Mode

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Reader Status.
    - When the Status screen opens previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Reader Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Reader Status heading, and select the access control unit from the drop down list.
5. Position the cursor over the desired reader icon and right click.
6. Select the reader/keypad mode from the drop down list.
7. Click on the x in the upper right corner to close the screen.

Related Topic

Assign Schedules for Reader/Keypads

Input Status

The Input Status screen allows you to view the current status on inputs or manually set specific or all auxiliary and supervised inputs.

The inputs are in one of 2 states:

- Normal Status - no manual overrides applied and the point is armed
- Disarmed Status - a user has applied an override and the input is shunted or bypassed

The Input Status screen is accessed from the Status menu.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

View as Text

Selecting this option by clicking in the box to the left, changes the screen so the inputs are listed in a column with their respective status.

Input Status Icons

The following is a review of the icons that indicate an input's status. The icons surrounding the input image change to reflect the current status or condition.

Review of Input Status Icons

View as Text/Input Status Icons		Legend
		Each input on the access control unit in the Input Status screen is graphically represented by an Aux Input icon. The name of the input is listed at the top to distinguish each input. This is the name assigned in the Hardware Setup > Inputs screen. In the example illustration on the left, the input is currently disarmed by an automatic command.
Armed		Indicates the input is armed (normal status).
Disarmed		Indicates the input is disarmed.

Auto1		Indicates the last change to the input status was automatic. Automatic is initiated by either a schedule change or a Present3 schedule toggle.
Manual		Indicates the last change to the input status was manual. Manual is initiated by user intervention. User intervention occurs via a command on the Input Status screen.
Unknown		The current status is unknown as no communication has occurred with the input.
Alarm		The input is in an alarm state.

Procedures

Steps to Toggle an Individual Input - Arm/Disarm

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Input Status.
    - When the Status screen opens any previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Input Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Input Status heading, and select the access control unit from the drop down list.
5. Position the cursor over the desired Aux Input icon and right click.
6. Do one of the following steps:
    - To disarm a currently armed input, select Toggle Off.
    - To arm a currently disarmed input, select Toggle On.
7. To close the Input Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Revert to Schedule Setting

The above command puts the input in its programmed schedule state.

Steps to Toggle All Inputs - Arm/Disarm

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Input Status.
    - When the Status screen opens previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Input Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Input Status heading, and select the access control unit from the drop down list.
5. Do one of the following steps:

- To disarm all currently armed inputs, click on the Set All to Disarmed Status button.
- To arm all currently disarmed inputs, click on the Set All to Normal Status button.

6. To close the Input Status screen, click on the x to the far right on the title bar.
7. To exit the Status screen, click on the X in the upper right corner.

Related Topics

Name Inputs - Assign to Outputs

Auxiliary Output Status

Auxiliary Output Status

The Auxiliary Output Status screen allows you to view or manually toggle individual or all auxiliary outputs to an ON or OFF state providing you do not have an input assigned to an output.

The Auxiliary Output Status screen is accessed from the Status menu.

You may have to refer to the Relay States table located on the Name Auxiliary Outputs help topic. Click on the link under Related Topics.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

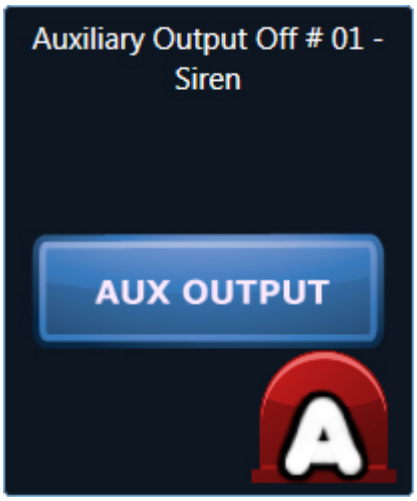
View as Text

Selecting this option by clicking in the box to the left, changes the screen so the outputs are listed in a column with their respective status.

Auxiliary Output Status Icons

The following is a review of the icons that indicate an output's status. The icons surrounding the output image change to reflect the current status or condition.

Review of Auxiliary Output Status

View as Text/Output Status Icons		Legend
		Each output on the access control unit in the Auxiliary Output Status screen is graphically represented by an Aux Output icon. As outputs have an ON name and an OFF name, the name listed at the top depends on whether the output is ON or OFF. The Output ON and Output OFF names are assigned in the Hardware Setup > Outputs screen. In the example illustration on the left, the output is currently OFF by an automatic command.
Armed		Indicates the output is on.
Disarmed		Indicates the output is off.
Auto1		Indicates the last change to the output status was automatic. Automatic is initiated by either a schedule change or a Present3 schedule toggle.

Manual		Indicates the last change to the output status was manual. Manual is initiated by user intervention. User intervention occurs via a command on the Output Status screen.
Unknown		The current status is unknown as no communication has occurred with the output.

Procedures

Steps to Toggle an Individual Output On or Off

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Auxiliary Output Status.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets will still be on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Auxiliary Output Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Auxiliary Output Status heading, and select the access control unit from the drop down list.
5. Position the cursor over the desired Aux Output icon and right click.
6. Do one of the following steps:
    - To turn off an output currently on, select Toggle Off.
    - To turn on an output currently off, select Toggle On.
7. To close the Auxiliary Output Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Revert to Schedule Setting

This command puts the output in its programmed schedule state.

Steps to Toggle All Outputs On or Off

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Auxiliary Output Status.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets will still be on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Auxiliary Output Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Auxiliary Output Status heading, and select the access control unit from the drop down list.
5. Do one of the following steps:
    - To turn off all outputs currently on, click on the Toggle All Off button.
    - To turn on all outputs currently off, click on the Toggle All On button.
6. To close the Auxiliary Output Status screen, click on the x to the far right on the title bar.
7. To exit the Status screen, click on the X in the upper right corner.

Related Topics

Name Auxiliary Outputs

IOCB Input Status

The IOCB Input Status screen allows you to view the current status of IOCB1616 inputs or manually toggle specific or all IOCB1616 inputs.

You can view the IOCB1616 graphically or select the View as Text option in which the inputs are reported in a table format.

Status

Inputs are reported in one of the following status conditions:

- Normal - the point is armed or disarmed
- Shunt - a user has applied an override and the input is shunted (bypassed)*
- Alarm - the input circuit is open and is in an alarm condition
- Warning - a supervised input is reporting a trouble open or trouble short depending on the input's supervision level



*When an input is manually shunted it must be manually set to normal status otherwise the input remains shunted forever regardless of any schedule assignments.

Armed Status

The input is reported in one of the following states:

- Armed - the schedule is off
- Disarmed - the schedule is on

If the input has a manual shunt applied, it has no armed or disarmed status.

Armed Reason

In the Aurora software the IOCB1616 input can be changed by a schedule or by user intervention.

- Auto* - the input has been changed by a schedule or restored to a schedule following a manual shunt
- Manual - the input has been shunted by user intervention

*Auto - Initially when an IOCB1616 is added to the site, the Aurora software assigns the inputs with an Auto status. The Auto status remains in effect until the input is manually shunted. The auto status applies to inputs that have a Not Assigned status in the Schedule Assignment screen. (Not Assigned is technically a schedule that never turns on.)

View as Text

Selecting this option by clicking in the box to the left, changes the screen so the inputs are listed in a column with their respective status.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget’s title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

IOCB1616 Input Status Icons

The following is a review of the icons that indicate an IOCB1616 input's status. The icons surrounding the input image change to reflect the current status or condition.

Review of IOCB Input Status Icons

View as Text/IOCB Input Status Icons		Legend
		Each IOCB1616 input in the IOCB Input Status screen is graphically represented by an icon. The name of the input is listed at the top to distinguish each input. This is the name assigned in the Hardware Setup > IOCB1616 Inputs screen. In the example illustration on the left, the IOCB input is currently disarmed with the schedule on.
Armed		Indicates the IOCB input is armed (normal status) and the schedule is off.
Disarmed		Indicates the IOCB input is disarmed and the schedule is on.
Shunt		Indicates the IOCB1616 input is shunted (bypassed) by manual intervention.
Auto1		Automatic is by a schedule change or restored from a shunt. (By default all IOCB1616 inputs are set on auto, including IOCB inputs on Not Assigned in the Schedule Assignment screen, until manually shunted.)
Manual		Manual is initiated by user intervention and the input has been shunted. User intervention occurs via a command on the Input Status screen.
Unknown		The current status is unknown as no communication has occurred with the IOCB input. (The IOCB1616 board has been installed and the communication service is not running.)
Alarm		The IOCB input is in an alarm state.
Unknown		The IOCB 1616supervised input is reporting a warning either trouble open or trouble short depending on the input's supervision level.

Procedures

Steps to Toggle an Individual IOCB Input - Arm/Disarm

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on IOCB Input Status.
    - When the Status screen opens if you previously viewed any status widgets and left them open those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.

3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the IOCB Input Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the IOCB Input Status heading, and select the access control unit from the drop down list.
5. Position the cursor over the desired IOCB Input icon and right click.
6. Do one of the following steps:
    - To shunt a currently armed IOCB input, select Set to Disarm Status.
    - To arm a currently shunted input, select Set to Normal Status.
7. To close the IOCB Input Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Steps to Toggle All IOCB Inputs - Arm/Disarm

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on IOCB Input Status.
    - When the Status screen opens if you previously viewed any status widgets and left them open those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the symbol in the first box to the right of the IOCB Input Status heading, and select the site from the drop down list.
4. Click on the symbol in the box to the extreme right on the IOCB Input Status heading, and select the access control unit from the drop down list.
5. Do one of the following steps:
    - To shunt all currently armed IOCB inputs, click on the Set All to Disarmed Status button.
    - To arm all currently shunted IOCB inputs, click on the Set All to Normal Status button.
6. To close the IOCB Input Status screen, click on the x to the far right on the title bar.
7. To exit the Status screen, click on the X in the upper right corner.

Related Topics

Alarm Types

IOCB Output Status

The IOCB Output Status screen allows you to view or manually toggle individual or all IOCB outputs to an ON or OFF state.

The IOCB Output Status screen is accessed from the Status menu.

Pulse Command

The IOCB1616 Output status screen has a Pulse command when you right click on the output icon or output row if View as Text is enabled. If the output is set on Optional IO Pulsed Output mode in the Hardware Setup screen, the output is pulsed for the output time when the Pulse command is selected.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

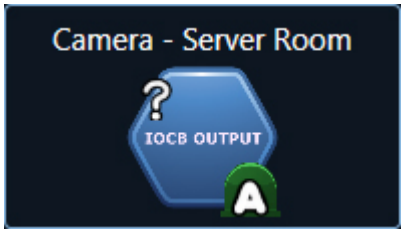
View as Text

Selecting this option by clicking in the box to the left, changes the screen so the outputs are listed in a column with their respective status.

IOCB Output Status Icons

The following is a review of the icons that indicate an IOCB output's status. The icons surrounding the output image change to reflect the current status or condition.

Review of IOCB Output Status Icons

View as Text/Output Status Icons		Legend
		Each IOCB output on the access control unit in the IOCB Output Status screen is graphically represented by an output icon. The name is listed at the top. The IOCB Output names are assigned in the Hardware Setup > IOCB Outputs screen. In the example illustration on the left, the output is currently on by an automatic command.
Armed		Indicates the IOCB output is on.
Disarmed		Indicates the IOCB output is off.
Auto1		Indicates the last change to the IOCB output status was automatic. Automatic is initiated by either a schedule change or a Present3 schedule toggle.
Manual		Indicates the last change to the IOCB output status was manual. Manual is initiated by user intervention. User intervention occurs via a command on the Output Status screen.

Unknown		The current status is unknown as no communication has occurred with the IOCB output.

Procedures

Steps to Toggle an Individual IOCB Output On or Off

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on IOCB Output Status.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the IOCB Output Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the IOCB Output Status heading, and select the access control unit from the drop down list.
5. Position the cursor over the desired IOCB Output icon and right click.
6. Do one of the following steps:
    - To turn off an IOCB output currently on, select Toggle Off.
    - To turn on an IOCB output currently off, select Toggle On.
    - To revert the IOCB1616 to its schedule assignment, select Revert to Auto.
7. To close the IOCB Output Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Steps to Toggle All Outputs On or Off

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on IOCB Output Status.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the IOCB Output Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the IOCB Output Status heading, and select the access control unit from the drop down list.
5. Do one of the following steps:
    - To turn off all IOCB outputs currently on, click on the Toggle All Off button.
    - To turn on all IOCB outputs currently off, click on the Toggle All On button.
6. To close the IOCB Output Status screen, click on the x to the far right on the title bar.
7. To exit the Status screen, click on the X in the upper right corner.

Online Transactions

The Online Transactions screen allows you to view system activity. Transactions fall into two categories:

- Alarms
- Events

The following provides a brief explanation between the two types of transactions.

Alarms

Alarms are critical events and highlighted in red on the Online Transaction screen indicating that immediate action may be required. Alarms can be triggered by devices connected to various input terminals on the control board such as motion sensors and door contacts, or alarms can be triggered if the software loses communication with individual control units.

Events

Events are physical interactions by credential holders such a presenting a credential at a reader, system-user activity such as manually unlocking a door, and software programming such as when a schedule turns on or off.

Online Transaction Columns

As an alarm or event transpires it is listed on the Online Transaction screen with the corresponding information posted under the following columns:

- Device - lists the name of the device such as an input name, a door name, a schedule name etc, depending on the type of transaction
- Person - lists the name of a credential holder who has presented a credential at a reader
- Credential - lists the credential number presented at a reader
- Type - lists the transaction type such as alarm tripped, access granted, schedule off etc.
- Date - lists the date and time of the transaction
- Access Control Unit - lists the name of the control unit connected with device reporting the event

You can change the order of the columns from left to right by clicking and dragging them to other positions along the heading row. Aurora retains the changes on any subsequent logins.

Show Person Image

Providing that the credential holder records have photo images, when this function is enabled the Online Transaction screen will display the on-file photo image of the person on any credential-related transactions. To enable, click in the box to the left of Show Photos. If enabled, the Show Photos option remains selected whenever you reopen the Online Transaction screen until it is de-selected.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Procedures

To access the Online Transaction screen, select the Status menu > Status > Online Transactions.

Use the three boxes on the right side of the Online Transactions title bar to specify the time zone, the site or all sites and a panel or all panels by clicking on the ▼ symbols. If you are viewing all sites, the screen displays transactions at all panels; you cannot filter panel-specific transactions.

To enable the Show Person Image function, click in the box to the left. The box has an x when enabled. To disable the function click in the box to clear the x. The box is blank when it is disabled.

To discard the current transactions on screen, click on the Clear button.

Related Topics

Alarm Monitoring & Alarm Response

Credential Transaction Photos

The Credential Transaction Photos status screen displays a person's on-file image on credential-related transactions. Above the image, the screen lists the person's name and the credential number. Below the image, the screen lists the transaction "access granted" or "access denied", the door name and direction, the date and time, and the access control unit.

The Credential Transaction Photos status screen functions the same as the Online Transactions screen when the show person image function is enabled. Except the Credential Transaction Photos status screen filters out all other transactions.

The Credential Transaction Photos status screen retains images for the last 50 credential-related transactions.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget’s title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Procedures

To access the Credential Transaction Photos screen, select the Status menu > Status > Credential Transaction Photos.

Use the three boxes on the right side of the Credential Transaction Photos title bar to specify the time zone, the site or all sites and a panel or all panels by clicking on the ▼ symbols.

Floor Status

The Floor Status screen shows the current status of each elevator floor button and allows you to manually override individual or all elevator floor buttons. Floor buttons are in one of the following 3 states:

- Secured - The floor is secure and a valid card is required to activate the floor button.
- Unsecured - The floor is unsecured and a valid card is not required to activate the floor button. If an elevator button is manually set to unsecured, it remains so until either manually toggled to secured or, if applicable, automatically re-locks at the end of a schedule assignment in the Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons screen.
- Timed unlock - The floor is unsecured for a specified period of time. The maximum period is 7 days for a timed unlock. At the conclusion of the timed unlock, the elevator floor button is secured.
- Revert to Schedule Setting - The floor is reset to its assigned schedule if it has been programmed in the Schedule Assignment/Elevator Banks screen.

Please be aware of a timed unlock applied to an elevator floor button that has been programmed to automatically lock/unlock on a schedule. If the timed unlock expires after the start of an auto unlock period, the floor button remains secured until the next programmed auto unlock start time.

The above settings apply to all elevators assigned to the elevator bank.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

View as Text

Selecting this option by clicking in the box to the left, changes the screen so the floors are listed in columns with their respective floor status.

Procedure

Steps to Toggle Elevator Control Buttons - Secured or Unsecured

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Floor Status.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Floor Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Floor Status heading, and select the elevator bank from the drop down list.
5. Position the cursor over the desired Elevator Floor # icon and right click.
6. Do one of the following steps:
    - To secure an elevator floor, select Secure.
    - To unsecure an elevator floor, select Unsecure.

Access Control Unit Card Count

The Access Control Unit Card Count widget provides a summary of active and inactive cards currently stored in the listed access control unit.

Note +

Active and inactive card counts will also be affected by the Person Active and Person Inactive settings in the Edit Person screen. If an individual has multiple credentials and he or she is marked as Person Inactive, the inactive card count will reflect that individual's total number of credentials as part of the inactive card count. The same holds true with the Person Active setting.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Refresh Function

The Refresh function directs a command to the listed access control unit for an updated active and inactive card count.

Synchronize Function

The Synchronize function directs the database to upload all the credential records to the listed access control unit.

Procedure

Steps to View Card Counts

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status Widgets heading, double click on Access Control Unit Card Count.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Access Control Unit Card Count heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Access Control Unit Card Count heading, and select the access control unit from the drop down list.
    - The active and inactive card counts are displayed as well as the last refresh time. This will be either when the screen is initially opened or when the screen was last refreshed by selecting the Refresh button.
5. To close the Access Control Unit Card Count screen, click on the x to the far right on the title bar.
6. To exit the Status screen, click on the X in the upper right corner.

Access Control Unit Status

The Access Control Unit Status screen provides a summary of the door, elevator, and intrusion control boards at the selected site. Each control board has the following information displayed as well as Sync Clock, Full Upload, and Delete Pending Packages as outlined below:

Access Control Unit Status / Settings

- Access Control Unit - lists the unit as it is defined in the Hardware Setup screen
- Serial Number - identifies the control unit's serial number
- Status - indicates the control unit's current status
    - Active - active status indicates the control unit is in communication with the software
    - Inactive - inactive status indicates that the control unit has experienced a communication failure with the software; if the software is unable to re-establish communication, it lists the unit status as inactive
    - Disabled - disabled indicates that the control unit has manually been taken off-line in the Hardware Setup screen
- Pending Packages - indicates the number of data packages currently in the download cue for transmission to the control unit
- Communication Server - indicates the server with the Aurora Communication Service connected to the access control unit
- Communication - indicates the control unit's mode of communication with the software: network communication or serial communication
- Last Polled - indicates the date and time that the control unit was last polled by the software; the software continuously polls the control units for event transactions including alarms
- Firmware Version - lists the control board's firmware version
- Communication Error - when a communication failure is first detected by the software with a control unit, communication error indicates the number of attempts to re-establish communication; the unit is marked inactive after the 19th failed attempt

Control Unit Status Functions

- Settings - retrieves the ACU jumper or DIP switch settings depending on the control board version - see Settings below.
- Sync Clock - synchronizes the control unit clock to the server clock with the communication software
- Full Upload - transmits a complete upload of all the software data to the selected control unit - see Full Upload below
- Delete Pending Packages - principally a diagnostic utility which deletes pending data that would otherwise be sent to the control unit; only use this function if instructed by Keyscan technical support
- Disaster Recovery - retrieves access control unit data to restore system operation in the event the Keyscan database was lost or corrupted - see related topics below

Important ! Do not use Disaster Recovery unless your database was previously lost or corrupted and you have re-installed Aurora with a clean database. Executing the disaster recovery function overwrites your fully populated database with limited ACU data. For more information and instructions on disaster recovery, select the link under Related Topics below.

Full Upload

To the right of Full Upload, selecting the  symbol opens a drop down list with specific access control unit upload options:

- Hardware Settings Upload - uploads hardware related settings only
- All Credentials Upload - uploads all credentials and all credential-related data only
- Schedules - uploads all schedules and all holidays only
- Test (DSC intrusion units) - tests communication with intrusion unit
- Sensor Reset (DMP intrusion units) - resets smoke and glass break detectors after they have tripped; when detectors trip, they must be reset to detect alarm conditions again

To perform an upload, select the upload option. Aurora presents a prompt; click on the Yes button.

Settings

The settings function retrieves the current jumper or DIP switch configurations depending on the control board version you are polling. Settings are indicated by zeros and ones as follows:

- OFF = 0
- ON = 1

You may require the Keyscan Technical Guide for determining which functions have been enabled on the control board.

Global Anti-Pass Back - CIM Master

The control board with the CIM card jumpered as the global master for anti-pass back applications is listed as Is Master opposite Master in the Settings screen. Control boards with a slave CIM list the serial number of the control board connected to the master CIM card. (This only applies for global master/slave connected control boards. All other configured control boards have a status of Is Master.)

IOCB1616 Test

The settings screen also displays IOCB1616 - Card # with a status of failed or passed.

- Failed indicates no IOCB1616 card detected
- Passed indicates an IOCB1616 has been detected

Retrieve Settings

To retrieve the settings from the control board, select the icon below the Settings heading along the row of the desired control board, select the Get Settings button.

The Settings window also displays both the access control board's clock time, based on its geographic time zone, and the server clock time. If the clock times between the two entities have drifted apart by more than one or two minutes, select the Sync Clock icon to re-synchronize the clocks.

Auto Refresh / Refresh

The Access Control Unit Status screen has two modes of refreshing, which is updating the screen with the latest status.

- Auto Refresh - automatically updates the screen every 10 seconds; to enable, click in the box to the left
- Refresh - the screen is only updated when you click on the Refresh button; the last refresh date and time are listed above the button



When Auto Refresh is enabled, the Refresh button is unavailable.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Related Topics

Disaster Recovery

Reset Anti-Pass Back

In a controlled enter/exit environment, where the anti-pass back option is in effect, the Keyscan system maintains an in or out status for each credential holder. When anti-pass back is reset, the credential can be used at an in or out reader on its next reader presentation before it is again governed by the in/out anti-pass back rule.

The Reset Anti-Pass Back screen retains a log of credentials that have violated anti-pass back rules.

You can reset anti-pass back for a single credential holder, multiple credential holders, or all credential holders.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Procedure

Steps to Reset Anti-Pass Back

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Reset Anti-Pass Back.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. Select the site in the box to the right of the Reset Anti-Pass Back title bar.
4. For resetting anti-pass back observe the following:
    - single or multiple credentials, select the person or persons, and click on the Reset Selected button
    - all credentials at all control units, select the Reset All button, and then select the Yes button in the Reset Anti-Pass Back confirmation box.
5. To close the Reset Anti-Pass Back screen, click on the x to the far right on the title bar.
6. To exit the Status screen, click on the X in the upper right corner.

Reader Diagnostics

The Reader Diagnostics screen is a system diagnostic tool for investigating card or reader problems.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Procedure

Steps to Run a Reader Diagnostic

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Reader Diagnostics.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. Select the credential format in the first box at the right of the Reader Diagnostics heading. By default the Keyscan format is pre-selected.
4. Select the site in the box to the right of the Reader Diagnostics title bar.
5. Select the access control unit connected to the reader in the box to the far right on the Reader Diagnostics title bar.
6. Take a few cards and present them at the reader.
7. Return to the server with the Aurora Client that has the Reader Diagnostics screen open.
    - Faulty Cards - The Reader Diagnostic screen lists the reader # X, the batch # and the credential number of each credential scanned. Compare the number of credentials physically scanned to the number of credentials recorded on the screen. Determine which, if any, credentials were faulty.
    - Faulty Reader - If no data is recorded on the Reader Diagnostic screen, then the reader is not operating correctly. Call your service vendor.
8. To close the Reader Diagnostics screen, click on the x to the far right on the title bar.
9. To exit the Status screen, click on the X in the upper right corner.

Schedule Status

The Schedule Status screen is used to review the current status of schedules in your system. Schedules have two states: ON or OFF. From this screen you can also manually toggle individual schedules ON or OFF for a selected access control unit.

- If schedules are toggled ON they remain on until the next scheduled end time.
- If schedules are toggled OFF they remain off until the scheduled start time.



You cannot edit a schedule from this screen. Be aware that toggling a schedule is altering the time event.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Procedure

Steps to Toggle a Schedule ON/OFF

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Schedule Status.
    - When the Status screen opens if you previously viewed any status widgets that were left open, those status widgets are still on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. Select the site in the box to the right of the Schedule Status title bar.
4. Select the access control unit connected to the reader in the box to the far right on the Schedule Status title bar.
5. Click in the box or boxes to the left of each individual schedule that you are toggling.
    - When you toggle a schedule you will flip it to its opposite state.
6. Click on the Toggle button.
7. To close the Schedule Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Intrusion Zone Status

The Intrusion Zone Status screen is a monitoring screen that indicates the current intrusion zone status.

If an intrusion zone has gone into alarm the Intrusion Zone status screen indicates which point has gone into alarm with the following icon:



Alarm Icon

The Intrusion Zone Status screen is a static, non-interactive screen. You cannot arm or disarm individual intrusion zones from the Intrusion Zone Status screen.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Intrusion Partition Status

The Intrusion Partition Status (DSC) allows you to view the current status of the listed intrusion control unit partitions and to manually arm or disarm them.

The partitions are in one of 2 states:

- Armed Status - the partition is currently armed
- Disarmed Status - the partition is currently disarmed

The Intrusion Partition Status screen is accessed from the Status menu.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Intrusion Partition Status Icons

The following is a review of the icons that indicate an input's status. The icons surrounding the input image change to reflect the current status or condition.

Review of Partition Status Icons

View as Text/Intrusion Partition Status Icons		Legend
		Each partition on the intrusion control unit in the Intrusion Partition Status screen is graphically represented by an Intrusion icon. The name of the partition is listed at the top to distinguish each partition. This is the name assigned in the Hardware Setup > Intrusion Partitions screen.
Armed		Indicates the partition is armed and secure.
Disarmed		Indicates the partition is disarmed and not secure.
Unknown		The current status is unknown as no communication has occurred with the partition.
Alarm		The partition is in an alarm state.

Procedure

Steps to Manually Arm and Disarm an Intrusion Partition

1. From the Client main screen, select the Status button > Status.

2. From the Status screen under the Status heading, double click on Intrusion Partition Status.
    - When the Status screen opens any previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Intrusion Partition Status heading, and select the site from the drop down list.
4. Click on the ▼ symbol in the box to the extreme right on the Intrusion Partition Status heading, and select the intrusion control unit from the drop down list.
5. Position the cursor over the desired intrusion partition icon and right click.
6. Do one of the following steps:
    - To disarm a currently armed partition, select Unsecure.
    - To arm a currently disarmed partition, select Secure > Arm Away or Arm With Master Code.
7. To close the Intrusion Partition Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Refer to the DSC literature or user guides for explanations about Arm Away and Arm With Master Code.

Intrusion Area Status

The Intrusion Area Status (DMP) allows you to view the current status of the listed intrusion control unit areas and to manually arm or disarm them.

The areas are in one of 2 states:

- Armed Status - the area is currently armed
- Disarmed Status - the area is currently disarmed

The Intrusion Area Status screen is accessed from the Status menu.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Intrusion Area Status Icons

The following is a review of the icons that indicate an input's status. The icons surrounding the input image change to reflect the current status or condition.

Review of Area Status Symbols

View as Text/Intrusion Area Status Icons		Legend
		Each area on the intrusion control unit in the Intrusion Area Status screen is graphically represented by an Intrusion icon. The name of the area is listed at the top. This is the name assigned in the Hardware Setup > Intrusion Areas screen.
Armed		Indicates the area is armed and secure.
Disarmed		Indicates the area is disarmed and not secure.
Unknown		The current status is unknown as no communication has occurred with the partition.

Procedure

Steps to Manually Arm and Disarm an Intrusion Area

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Intrusion Area Status.
    - When the Status screen opens any previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner.
3. If you have multiple sites, click on the ▼ symbol in the first box to the right of the Intrusion Area Status heading, and select the site from the drop down list.

4. Click on the ▼ symbol in the box to the extreme right on the Intrusion Area Status heading, and select the intrusion control unit from the drop down list.
5. Position the cursor over the desired intrusion area icon and right click.
6. Do one of the following steps:
    - To disarm a currently armed area, select Unsecure.
    - To arm a currently disarmed area, select Secure.
7. To close the Intrusion Area Status screen, click on the x to the far right on the title bar.
8. To exit the Status screen, click on the X in the upper right corner.

Software Connections Status

The Software Connections Status screen lists any server currently logged into the Keyscan database with any open Keyscan Aurora application. The screen identifies the following information:

- User Name - this is the Aurora system user currently logged in
- Computer Name - the name of the computer as defined in Windows running Aurora software such as a Client
- Last Log In - the time the system user logged in or an Aurora service started, such as a communication service
- Last Seen - the time at which the Software Connection Status screen last viewed the open Aurora software connected to the database
- Software Name - the Aurora software module open or running
- Version - the Aurora version number

Where multiple sites exist, the Software Connections Status screen displays all open Keyscan applications on all sites regardless of the system user's permissions and site assignments.

Users must exit the Keyscan application in order to disconnect from the database; otherwise the database will indicate that the user is still operating with an open application.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget’s title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Refresh

The Refresh button updates the screen so it displays the current status.

Procedures

- To open the Software Connections Status screen, select the Status button > Status. You may have to drag the scroll bar down and then double click on Software Connections Status.
- To exit the screen, select the x in the upper right to close the Software Connections Status screen.

Visit Status

The Visit Status widget lists all past, present and future visits. Past visits will go back as far as the first scheduled visit or scheduled visits after the last database purge.

Today's Visits Only

When this option is enabled, the Visit Status widget lists only the visits that are scheduled for today's date.

Pending Visits Only

When this option is selected, the Visit Status widget lists only those visits with an Expected or Delayed Arrival visit status.

Update Visit Status

The Visit Status widget is interactive. Visits that have a current status of expected, arrived or delayed arrival can be updated. Depending on the current status, you will see above the Attendees heading the following buttons/options:

Current Status	Button above Attendees	Options Button
Expected	Arrived	Cancelled Delayed Arrival
Delayed Arrival	Arrived	Cancelled
Arrived	Departed	n/a

You cannot change a visit's status that has been set as cancelled or departed.

As an example, a visit with an Expected status can be updated to arrived by clicking on the Arrived button. You can also change the status to cancelled or delayed arrival by clicking on the symbol to the far right and selecting one of those two options, depending on which is applicable.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget's title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Procedure

Steps to View the Visit Status Widget

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status Widgets heading, double click on Visit Status.
    - When the Status screen opens previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner of the widget.
3. When the screen opens, the top visit is highlighted and the attendees of the highlighted visit are listed on the right.
    - Other than visits with a Cancelled or Departed status, you can update the status by selecting an option above the Attendees heading on the Visit Status widget.
4. To list appointments scheduled for today, click in the box to the left of Today's Visits Only. The box has an x when enabled.

5. To list all pending visits (without Today's Visits Only selected), these are visits which have an Expected, Delayed or Arrived status, click in the box to the left of Pending Visits Only. The box has an x when enabled.
    - This will also list any visits scheduled before today's date if they were still set on Expected or Delayed Arrival.
6. To close the Visit Status screen, click on the x to the far right on the title bar.
7. To exit the Status screen, click on the X in the upper right corner.

Person Last Seen Status

The Person Last Seen Status screen lists when and where a credential was last presented within the previous 7 (seven) days. The Person Last Seen Status screen provides the option of displaying all credentials/credential holders per site or using the Advanced Filters to narrow the list based on selected search options as outlined:

Advanced Filter Options

When the site is selected in the upper right corner, all credentials are listed. The following filters can be employed to narrow the search:

- Look Back (Days) - selects the number of days 1 to 7 for searching the last credential transaction
    - Unknown indicates the credential has not been used within the last seven days
- Optional Field - lists the credentials under the entered common field (data entry, not the optional field description)
- Name - lists the credentials based on the name entered which can be the Given Name or the Surname
    - You can also enter a partial name or just 1 character to list names - example: entering the letter i would list all Given Names and Surnames that have the letter i.
- Person Type - lists the credentials based on the Person Type field selected

Procedure

Steps to Use the Person Last Seen Status Screen

1. From the Client main screen, select the Status button > Status.
2. From the Status screen under the Status heading, double click on Person Last Seen Status.
    - When the Status screen opens previously viewed status widgets left open remain on-screen. You can close them by clicking on the X in the upper right corner of the widget.
    - Credentials not used within the last 7 days will have an Unknown status below the Last Seen column.
3. To refine you search for specific credentials and credential holders, use the options below Advanced Filter.
4. If you enter or change filters the screen automatically updates the list.
5. When you have finished, click on the x in the upper right corner opposite the Person Last Seen Status heading.
6. To close the Status screen click on the x.

Gateway Status

The Gateway Status screen allows you to view the current status of any gateway being used as a communications link between the E-Plex wireless lock and the Aurora software. Within the Gateway Status screen, the following fields are viewable:

- Name - the name of the gateway
- MAC Address - if a MAC is being used in conjunction with the gateway, then the address will be displayed here
- Connection Type - a gateway can be connected to the communications manager with Aurora software via USB or a network cable
- DHCP - displays a randomly generated IP address if one was randomized from the communications manager with Aurora software
- IP Address - displays the IP address of the communications manager with Aurora software connected to the gateway
- Status - displays the current status of the gateway
- Join Status - will display either Join On or Join Off, depending on availability **Note:** Aurora only allows one Gateway to be placed in Join On Mode at a time, so keep this in mind during installation.
- Busy - will display either Busy or Not Busy, depending on communication load

When right-clicking on the name of a gateway, the following commands are available:

- Join On
- Reboot - routers and/or gateways
- Identify - gateways, routers, locks and devices
- Status - gateways, routers, locks and devices
- Request Network Quality Status
- Identify and Status of All Devices
- Change Zigbee Channel

The Gateway Status screen is accessed from the Status menu > Gateway Status.

System User Account

The system user account must be either a Master or Admin user type and have the Status Widget - View Gateway Status enabled to perform any actions within this status screen.

Doors Not Joined

This section of the Gateway Status screen will display other E-Plex wireless locks within the area that have not yet been configured through a gateway and to a communications manager with Aurora software. The following fields are viewable:

- E-Plex Door Group - the name given from the Hardware Setup menu
- Name - the name of the E-Plex wireless lock given from the Hardware Setup menu
- Lock Model - displays the type of E-Plex wireless lock being used
- ZAC - the number used to connect a gateway to a communications manager with Aurora software
- Site - the name given to a site from the Site Information Setup menu

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget’s title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

Access Control Unit Memory Viewer

The access control unit memory viewer is a diagnostic utility. It is intended as a control board memory diagnostic tool for assisting Keyscan technicians when troubleshooting technical issues with dealers and installers on a support call. The memory viewer only provides a snapshot of control board memory addresses; it does not affect or alter the control board's memory. It is beyond the scope of the Aurora help to outline any further details about the access control unit memory viewer.

E-Plex Operations

The E-Plex Operations screen allows you to view the current status of any connection between a gateway and an E-Plex wireless lock. Within the E-Plex Operations screen, the following fields are viewable:

- Status - displays either Pending or Successful, depending on the E-Plex's connection to the gateway
- Operation - the current status of the wireless lock is displayed here
- Date Created - displays the date when the wireless loop between the E-Plex lock, gateway and communications manager with Aurora software linked
- E-Plex Door - shows the make and model of the E-Plex wireless lock being used
- Gateway - displays the name given to the gateway upon registry

The E-Plex Operations screen is accessed from the Status menu > E-Plex Operations.

System User Account

The system user account must be either a Master or Admin user type and have the Status Widget - View E-Plex Operations enabled to perform any actions within this status screen.

Re-position & Re-size Status Widgets

Status widgets can be re-positioned and re-sized within the Status screen by positioning the mouse over the widget’s title bar, then clicking, dragging and dropping the screen in a new position. To re-size a status widget, position the cursor at the edge or corner and click and drag until the widget reaches the desired dimensions.

About Reports & Summaries

The Client software has extensive report tools that provide you with the means to summarize or investigate virtually all facets of site activity and information that has been recorded in the database.

Common to all Aurora reports are the Report Export Options and Report tool bar.

Report Export Options

After running a report in Aurora, you have the option of exporting (saving) the report in any of the following file formats:

- Acrobat PDF
- Excel 97 - 2003
- Rich Text Format (RTF)

Report Tool Bar

The following table reviews the tools and their functions on the Aurora report screens.

Icon	Function
	Returns to the first page of the report
	Returns to the previous page of the report
	The first number indicates the page currently in view The second number indicates the total number of pages in the report
	Advances to the next page in the report
	Advances to the last page in the report
	Setup for page margins, page orientation - portrait or landscape - paper size, paper source, and printer options
	Switches between Print Preview and Interactive View
	Opens the Print dialog box for printer selection, print options and to print the report
	Opens the drop down list of available export file format options
Report Viewer	



View Slider - Left Side

Drag the bar horizontally in either direction or click on the end arrows to zoom in or zoom out

View Selector - Right Side

Click on the down arrow at the right and zoom in or zoom out by selecting a magnification % from the drop down list

People IN/OUT Report

The People In/Out Report screen allows you to view the current status of all or selected credential holders at the specified site. This report is particularly useful for generating a snapshot of who is in or out of the building at present or on previous dates. Sites require controlled enter/exit portals in order to monitor in/out activity.

Include Report Settings

When the Include Report Settings is enabled, on the last page the report lists the selected settings that were used to compose the report.

Note + If running an In/Out report to ascertain the status of credential holders at the current moment, ensure the To field is set on the current date and the current time.

Procedures

Steps to Run a People In/Out Report

1. From the main screen select the Reports button > People Reports > In/Out Report.
2. With the Report Options tab selected, if applicable, select the desired site or sites for the report. Selected sites have an x in the box to the left. Clicking in the box alternately selects - has an x - or de-selects - has no x - on each subsequent click.
3. Under the Report Options heading, set the date and time in the From and To fields or you can select the Date & Time icon to the right and use the calendars and times.
    - If running an In/Out report to ascertain the status of credential holders at the current moment, ensure the To field is set on the current date and the current time.
4. Opposite the Direction field, click on the ▼ symbol and select the direction to determine the in or out status of the credential holders.
5. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
6. Select the People Filters tab.
7. Do one of the following steps:
    - To include all credential holders in the report leave Include all people selected. The box on the left has an x when selected and go to step 7.
    - To include only select credential holders, de-select the box to the left of Include all people, use the advanced filters to specify the desired list of credential holders, and then either click in the box to the left of Given Name to pre-select the all persons in the list or to select certain individuals, select the box to the left of that individual's given name. The boxes have an x when selected.
8. Click on the Run Report button.
    - Unknown status under the Direction column indicates the credential has not been used or not used since anti-pass back was last cleared.
9. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a People In/Out Report

1. From the main screen select the Reports button > People Reports > People In/Out Report.
2. Format the report. See Steps to Run a People In/Out Report for procedures.

3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a People In/Out Report

1. From the main screen select the Reports button > People Reports > People In/Out Report.
2. Format the report. See Steps to Run a People IN/OUT Report for procedures.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

About Reports & Summaries

Cumulative Hours Report

The Cumulative Hours Report summarizes time intervals between card reads providing readers have been setup as In and Out readers for recording enter and exit times at the assigned doors. Readers must be configured in the Hardware Setup > Doors screen so as to accurately monitor all enter (IN) and exit (OUT) activity for all designated credential holders.

The Cumulative Hours Report lists specified credential holders, and based on date parameters, lists the date and time of each IN card read, the date and time of each OUT card read, the time interval between each IN & OUT card read, and the total or cumulative time.

Both the IN reader and the OUT reader should have Anti-pass back enabled.

Example of Cumulative Hours Setup

The following is a basic example of a controlled enter/exit environment where Company X requests that all hourly employees use an employee side door whenever they enter or leave the building, be it arriving for work, taking lunch, or leaving for home. The employee door is equipped with two readers:

- Reader A is mounted on the exterior door side and set on direction - IN (marks date and time of entry)
- Reader B is mounted on the interior door side and set on direction - OUT (marks date and time of exit)

An employee arrives for work at 8:30 A.M., leaves the building for lunch at 12:15 P.M., returns at 1:00 P.M. and finishes work for the day at 4:45 P.M. A cumulative hours report summarizes the hours as follows:

Name		
Direction In	**Direction Out**	**Total Time**
dd/mm/yyyy 8:30 AM	dd/mm/yyyy 12:15 PM	3:45
dd/mm/yyyy 1:00 PM	dd/mm/yyyy 4:45 PM	3:45
Person's Name - Total Time: 7:30		

In the above example credential holders have access to other reader controlled doors; however, when the cumulative hours report is run, only the employee side door is specified for the report. All other doors are excluded from the report.

Include Report Settings

When the Include Report Settings is enabled, on the last page the report lists the selected settings that were used to compose the report.

Procedures

Steps to Run a Cumulative Hours Report

1. From the main screen select the Reports button > People Reports > Cumulative Hours Report.
2. With the Report Customization tab selected, if applicable, select the desired site or sites for the report. Selected sites have an x in the box to the left. Clicking in the box alternately selects - has an x - or de-selects - has no x - on each subsequent click.
3. Under Date Settings, specify one of the date options:
    - For a Date range, specify the date From and To fields; you can select the Date & Time icon to the right and use the calendars, and then specify the Start Time and the End Time.
    - For Last number of days, specify the number of days and the start and end times

- For One day, specify the date and the start and end times

4. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
5. Select the People tab and do one of the following steps:
   - If the report is to include all credential holders, click in the box to the left of Given Name. The entire list of credential holders is highlighted and each name has an x in the box to the left. Go to the next step.
   - If the report is to include a selective list of credential holders, below the Given Name column, click in the box to the left of each person included in the report. The box has an x when a person is selected. Go to the next step.
6. Select the Readers tab.
7. Select the applicable readers under the Direction In heading.
8. Select the applicable readers under the Direction Out heading.
9. Click on the Report Customization tab.
10. Click on the Run Report button.
11. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
12. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Cumulative Hours Report

1. From the main screen select the Report button > People Reports > Cumulative Hours Report.
2. Format the report. See Steps to Run a Cumulative Hours Report for procedures.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Cumulative Hours Report

1. From the main screen select the Reports button > People Reports > Cumulative Hours Report.
2. Format the report. See Steps to Run a Cumulative Hours Report for procedures.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

About Reports and Summaries

Deleted People Report

Persons deleted in the Manage People screen are listed in the Deleted People Report screen. Deleted persons records remain in the report until the database is purged.

You can run a Deleted People Report in its entirety or use the Advanced Filter to selectively search for and list specific records. Deleted People reports may be exported or printed.

Procedures

Steps to Run a Deleted People Report

1. From the Client main screen, select the Reports button > People Reports > Deleted People Report.
    - The Deleted People Report screen lists all the persons deleted in the Manage People screen since the last database purge.
2. To refine the search, use the Advanced Filters fields.
3. Do one of the following steps:
    - To select all people listed in the report, select the box to the left of Given Name.
    - To select only certain persons in the list, click in the box opposite the individual first names.
4. Click on the Run Report button.
5. The report is summarized in the Report Viewer. The total number of pages in the report is listed in the center of the tool bar.
6. Use the direction arrows on the tool bar to navigate through the report.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Report

1. From the Client main screen, select the Reports button > People Reports > Deleted People Report.
2. Format the report. See Steps to Run a Deleted People Report.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the report tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Report

1. From the Client main screen, select the Reports button > People Reports > Deleted People Report.
2. Format the report. See Steps to Run a Deleted People Report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.

6. In the File name text box, enter a name for the report.
7. Click on the Save button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

About Reports & Summaries

Door Access Granted Summary Report

The Door Access Granted Summary Report compiles the number of access granted transactions that occurred at each door during the specified time period. Under the Transactions heading the report includes all access granted and access granted with anti-pass back violations. You cannot de-select either category when running a report.

Procedures

Steps to Run a Door Access Granted Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door Access Granted Summary Report.
2. Under the Sites heading, ensure that you have selected the desired sites for the report. The box has an x when selected.
3. Under the Report Period heading, select a time period. The period is based on today's date and looks back in time for the # of days selected.
4. Click on the Run Report button.
5. When you have finished reviewing the report, click on the x in the upper right corner of Keyscan Aurora Report Viewer screen.
6. To close the Door Access Granted Summary Report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Door Access Granted Summary Report

1. From the main screen select the Reports button > Door Reports > Door Access Granted Summary Report.
2. Format the report. See Steps to Run a Door Access Granted Summary Report for procedures.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Door Access Granted Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door Access Granted Summary Report.
2. Format the report. See Steps to Run a Door Access Granted Summary Report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. In the File name text box, enter a name for the report.
7. Click on the Save button.

8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Door In/Out Summary Report

The Door In/Out Summary Report can be used to produce an in/out summary for reviewing activity or traffic patterns at selected doors. In order to run the report, you must have designated both in and out readers. The report captures the following transactions:

- Access Granted
- Access Granted - Dual Custody
- Access Granted - Dual Custody Waiting
- Access Granted - With Anti-Pass Back Violation

The above transactions are non-selectable.

The sub-headings below outline the general function of each component in the Door In/Out Summary Report.

Report Customization

Use the Report Customization for selecting the sites and dates/times for the report. Dates can be by a date range, the last number of days or a on a specific day at specified times.

Readers

Use the Readers screen to specify which door readers are included in the report. You must select at least one in reader and one out reader to compose a report; otherwise you will be prompted with an error message.

Procedures

Steps to Run a Door In/Out Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door In/Out Summary Report.
2. Ensure the Report Customization tab is selected.
3. Under the Sites heading, all sites are pre-selected. To de-select any sites that are not desired to be included in the report, select the box to the left. The box does not have an x when it has been de-selected.
4. Below the Date Settings heading, you have one of the following three options for setting the date parameters of the report. Follow one of the three procedures below for setting the time frame of the report:
    - Date range - Click in the radio button to the left to select this option. Click on the Calendar icon to the right of From. If the month is other than the current month, click on the arrows in the calendar to go back or forward to the desired month. Click on the day in the calendar. Repeat to set the To date. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired minutes. Repeat for the End Time.
    - Last number of days - Click in the radio button to the left to select this option. Click in the number text box and enter the desired number of days. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.
    - If setting last number of days for the current day, set the number to zero (0).
    - One day - Click in the radio button to the left to select this option. Click on the Calendar icon to the right of Date. If the month is other than the current month, click on the arrows in the calendar to go back or forward to the desired month. Click on the day in the calendar. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If

the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.

5. Select the Readers tab.
6. Under the Direction In heading, select the desired IN readers by clicking in the box on the left of each reader that is to be included in the report. The box has an x when selected.
7. Under the Direction Out, select the desired OUT readers by clicking in the box on the left of each reader that is to be included in the report. The box has an x when selected.
    - Note: if you do not select at least one IN reader and one OUT reader, you are prompted with an error message.
8. Click on the Run Report button.
9. When you have completed examining the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Door In/Out Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door In/Out Summary Report.
2. Format any settings that may apply to the report.
3. Click on the Run Report button.
4. After Aurora has compiled the report, click on the Print Report icon.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Door In/Out Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door In/Out Summary Report.
2. Format any settings that may apply to the report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Door Access Summary Report

The Door Access Summary Report can be used to view and compare access granted transactions with access denied transactions that occurred at selected readers.

The sub-headings below outline the general function of each component in the Door In/Out Report.

Report Customization

Use the Report Customization for selecting the sites and dates/times for the report. Dates can be by a date range, the last number of days or a on a specific day at specified times.

Transactions

The listed transactions - all access granted type transactions and all access denied type transactions - are not selectable. The report captures all the listed transactions below the Transactions heading.

Readers

Use the Readers screen to specify which door readers are included in the report.

Procedures

Steps to Run a Door Access Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door Access Summary Report.
2. Ensure the Report Customization tab is selected.
3. Under the Sites heading, all sites are pre-selected. To de-select any sites that are not desired to be included in the report, click in the box to the left. The box does not have an x when a site has been de-selected.
4. Below the Date Settings heading, you have one of the following three options for setting the date parameters of the report. Follow one of the three procedures below for setting the time frame of the report:
    - Date range - Click in the radio button to the left to select this option. Click on the Calendar icon to the right of From. If the month is other than the current month, click on the arrows in the calendar to go back or forward to the desired month. Click on the day in the calendar. Repeat to set the To date. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.
    - Last number of days - Click in the radio button to the left to select this option. Click in the number text box and enter the desired number of days. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.
        - If setting last number of days for the current day, set the number to zero (0).
    - One day - Click in the radio button to the left to select this option. Click on the Calendar icon to the right of Date. If the month is other than the current month, click on the arrows in the calendar to go back or forward to the desired month. Click on the day in the calendar. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.
5. Select the Readers tab.
6. Under the Name column, select the readers by clicking in the box on the left of each reader that is to be included in the report. The box has an x when selected.
    - Note: to select all readers, click in the box to the left of the Name heading.

7. Click on the Run Report button.
8. When you have completed examining the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Door Access Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door Access Summary Report.
2. Format any settings that may apply to the report.
3. Click on the Run Report button.
4. After Aurora has compiled the report, click on the Print Report icon.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Door Access Summary Report

1. From the Client main screen, select the Reports button > Door Reports > Door Access Summary Report.
2. Format any settings that may apply to the report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. In the File name text box, enter a name for the report.
7. Click on the Save button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Total People by Hour Report

The Total People by Hour Report tabulates a count of access granted transactions by the hour that have occurred on the current date up to the point of time the report is run.

With the Total People by Hour Report you have the capability of running the report in either of the following ways:

- manually run the report randomly at any time
- automatically e-mail the report to designated recipients every hour

Active/Inactive

In the upper right area of the Total People by Hour Report is an Inactive/Active button. When e-mailing reports automatically, the button must be set on Active to engage the Aurora Agent which controls the Aurora e-mail functions. If at any time you need to disengage e-mailing the reports, set the button on Inactive to suspend sending the report. See the procedures below. The Keyscan Aurora Agent must be running to e-mail the Total People by Hour Reports.

Procedures

Steps to Manually Run a Report

1. From the Client main screen, select the Reports button > People Reports > Total People by Hour Report.
2. On the right of the Site heading, click on the ▼ symbol and select the Site from the list that applies to the report.
3. Below the Reader column, click in the box at the left of each reader required in the report. The box has an x when selected.
    - Note: to select all readers, click in the box to the left of the Reader heading.
4. Click on the Run Report button.
5. After you have reviewed the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Steps to E-mail the Report Automatically on the Hour

1. From the Client main screen, select the Reports button > People Reports > Total People by Hour Report.
2. On the right of the Site heading, click on the ▼ symbol and select the Site from the list that applies to the report.
3. In the E-mail text box, enter the e-mail address of the person receiving the report. If including more than one e-mail address, insert a semi-colon (;) between each address.
4. Click on the Inactive button to change the status to Active. The button changes to green. If the button has been previously set on Active, by-pass this step and leave it on Active.
5. Under the Reader column, select the readers by clicking in the box on the left of each reader that is required in the report.
    - Note: to select all readers, click in the box to the left of the Reader heading.
6. Click on the Save button.
    - The report will be e-mailed at the top of the next hour and continue to be e-mailed every hour to the specified e-mail addresses.

7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Suspend E-mailing the Report

1. From the Client main screen, select the Reports button > People Reports > Total People by Hour Report.
2. On the right of the Site heading, click on the symbol and select the Site from the list that applies to the report.
3. Click on the Active button to change the status to Inactive. The button changes to red.
4. Click on the Save button.
    - The e-mailing the report will be suspended.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.
6. When you need to resume e-mailing the report, repeat the above steps and set the status back to Active.

Related Topic

Keyscan Aurora Agent

Unused Since Credential Report

The Unused Since Credential Report allows you to search for inactive credential holders. If you wanted to know the individuals who had not used their credentials within a given period of time, you would select the relevant sites and select a report period. The software searches through the database for all credentials that have not recorded any transactions during the specified period.

The Unused Since Credential Report is a convenient utility to maintain up-to-date records by allowing you to search for inactive credential holders who you may wish to make inactive or delete from the database.

Procedures

Steps to Run an Unused Since Credential Report

1. From the Client main screen, select the Reports button > People Reports > Unused Since Credential Report.
2. Under the Report Options heading, select the desired sites for the report.
3. Opposite Report Period, click on the ▼ symbol on the far right and select a time period from the list.
4. To include the credential holders image in the search, click in the box to the left of Show photos when searching. The box has an x when enabled.
5. Click on the Search button.
    - If no credentials were found to be unused during the time period, click on the OK button in the Unused Since Credential Report prompt.
6. Click on the Run Report button.
7. When you have completed reviewing the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer screen.
8. To close the Unused Since Credential Report screen, click on the Back button until you are at the main screen, or for a previously viewed screen, select the Navigation History down arrow to the right of the Back button.

Steps to Print an Unused Since Credential Report

1. From the Client main screen, select the Reports button > People Reports > Unused Since Credential Report.
2. Under the Report Options heading, select the desired sites for the report.
3. Opposite Report Period, click on the ▼ symbol on the far right and select a time period from the list.
4. To include the credential holders image in the search, click in the box to the left of Show photos when searching. The box has an x when enabled.
5. Click on the Search button.
    - If no credentials were found to be unused during the time period, click on the OK button in the Unused Since Credential Report prompt.
6. Click on the Run Report button.
7. From the Keyscan Aurora Report Viewer screen, click on the printer icon on the tool bar at the top.
8. From the Print dialog box, set the print options, and then select the Print button.
9. When finished viewing the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer screen.
10. To close the Unused Since Credential Report screen, click on the Back button until you are at the main screen, or for a previously viewed screen, select the Navigation History down arrow to the right of the Back button.

Steps to Export an Unused Credential Report

1. From the Client main screen, select the Reports button > People Reports > Unused Since Credential Report.
2. Under the Report Options heading, select the desired sites for the report.
3. Opposite Report Period, click on the ▼ symbol on the far right and select a time period from the list.
4. To include the credential holders image in the search, click in the box to the left of Show photos when searching. The box has an x when enabled.
5. Click on the Search button.
    - If no credentials were found to be unused during the time period, click on the OK button in the Unused Since Credential Report prompt.
6. Click on the Run Report button.
7. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
8. From the Save As dialog box, you can either use the default file name or create a file name in the File name text box.
9. Navigate the desired folder location.
10. Click on the Save button.
11. Click on the x in the upper right corner of the Keyscan Aurora Report Viewer screen.
12. To close the Unused Since Credential Report screen, click on the Back button until you are at the main screen, or for a previously viewed screen, select the Navigation History  down arrow to the right of the Back button.

Active/Expired Credential Report

The Active/Expired Credential Report lists credentials assigned with a temporary date range that become active or expire during the requested report period.

The report searches for temporary credentials which have a Valid From date or a Valid To date that occur within the selected time period.

The report will not list any temporary credentials with a Valid From date or a Valid To date which occur on either side of the selected time period.

Procedures

Steps to Run an Active/Expired Credential Report

1. From the Client main screen, select the Reports button > People Reports > Active/Expired Credential Report.
2. Under the Sites heading, ensure that you have selected the desired sites for the report. The box has an x when selected.
3. Under the Report Period heading, select a time period. This is the period that credentials fall within when they either become active or expire.
4. Click on the Run Report button.
5. When you have finished reviewing the report, click on the x in the upper right corner of Keyscan Aurora Report Viewer screen.
6. To close the Active/Expired Credential Report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print an Active/Expired Credential Report

1. From the Client main screen, select the Reports button > People Reports > Active/Expired Credential Report.
2. Format the report. See Steps to Run and Active/Expired Report.
3. Click on the Run Report button.
4. From the Keyscan Aurora Report Viewer screen, click on the printer icon on the tool bar at the top.
5. From the Print dialog box, set the print options, and then select the Print button.
6. When finished with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer screen.
7. To close the Unused Since Credential Report screen, click on the Back button until you are at the main screen, or for a previously viewed screen, select the Navigation History down arrow to the right of the Back button.

Steps to Export an Active/Expired Credential Report

1. From the Client main screen, select the Reports button > People Reports > Active/Expired Credential Report.
2. Format the report. See Steps to Run an Active/Expired Credential Report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, you can either use the default file name or create a file name in the File name text box.

6. Navigate the desired folder location.
7. Click on the Save button.
8. When finished with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer screen.
9. To close the Unused Since Credential Report screen, click on the Back button until you are at the main screen, or for a previously viewed screen, select the Navigation History  down arrow to the right of the Back button.

First Usage Report

The First Usage Report lists People with their Credentials and shows the first card usage for a single day at a single reader within the selected date range.

Procedures

Steps to Run a First Usage Report

1. From the main screen select the Reports button > People Reports > First Usage Report.
2. Select applicable reader under the Readers heading.
3. Under Report Options, specify the Date Setting:
    - For a Date range, specify the date From and To fields; you can select the Date & Time icon to the right and use the calendars, and then specify the Start Time and the End Time
    - For Last number of days, specify the number of days and the start and end times
    - For One day, specify the date and the start and end times
4. Select Run Report.
5. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a First Usage Report

1. From the main screen select the Reports button > People Reports > First Usage Report.
2. Select applicable reader under the Readers heading.
3. Under Report Options, specify the Date Setting:
    - For a Date range, specify the date From and To fields; you can select the Date & Time icon to the right and use the calendars, and then specify the Start Time and the End Time
    - For Last number of days, specify the number of days and the start and end times
    - For One day, specify the date and the start and end times
4. Select Run Report.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a First Usage Report

1. From the main screen select the Reports button > People Reports > First Usage Report.
2. Select applicable reader under the Readers heading.

3. Under Report Options, specify the Date Setting:
    - For a Date range, specify the date From and To fields; you can select the Date & Time icon to the right and use the calendars, and then specify the Start Time and the End Time
    - For Last number of days, specify the number of days and the start and end times
    - For One day, specify the date and the start and end times
4. Select Run Report.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.
9. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

About Reports and Summaries

Group Status Report

The Group Status Report summarizes active and inactive groups. Options include running a report for one or multiple sites and including the names of inactive groups.

By default, the Aurora software automatically activates the first 16 groups - group # 1 to group # 16 - whether they have been defined with a name or not. Group # 17 up to Group # 511 have an inactive status until manually activated by a system user; usually when the group is initially defined. This applies to each site.

If you have a relatively small number of groups, Keyscan suggests that you leave the Show Inactive Groups disabled. This will keep the report streamlined otherwise the report will list all 511 groups.

Include Report Settings

When the Include Report Settings is enabled, on the last page the report lists the selected settings that were used to compose the report.

Procedures

Steps to Run a Group Status Report

1. From the Client main screen, select the Reports button > Group Status Report.
2. If you have multiple sites, select the sites for the Group Status Report by clicking in the box to the left of each applicable site.
3. To run a report that excludes all inactive groups, ensure that the Show Inactive Groups switch is disabled. The box to the left does not have an x when it is disabled.
4. To insert a representative pie chart at the bottom of the report which shows the number of active groups in comparison to inactive groups, click in the box at the left of Include graph. The box has a check mark when selected.
5. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
6. Click on the Run Report button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Group Status Report

1. From the Client main screen, select the Reports button > Group Status Report.
2. If you have multiple sites, select the sites for the Group Status Report.
3. To run a report that excludes all inactive groups, ensure that the Show Inactive Groups switch is disabled. The box to the left does not have an x when it is disabled.
4. To insert a representative pie chart at the bottom of the report which shows the number of active groups in comparison to inactive groups, click in the box at the left of Include graph. The box has a check mark when selected.
5. Click on the Run Report button.
6. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
7. From the Save As dialog box, navigate to the desired folder location.
8. Enter a name for the report in the File name text box.
9. Click on the Save button.

10. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Steps to Print a Group Status Report

1. From the Client main screen, select the Reports button > Group Status Report.
2. If you have multiple sites, select the sites for the Group Status Report.
3. To run a report that excludes all inactive groups, ensure that the Show Inactive Groups switch is disabled. The box to the left does not have an x when it is disabled.
4. To insert a representative pie chart at the bottom of the report which shows the number of active groups in comparison to inactive groups, click in the box at the left of Include graph. The box has a check mark when selected.
5. Click on the Run Report button.
6. Near the top of the report, click on the Printer icon located on the tool bar.
7. From the Print dialog box, select the printer, printer options, print range and number of copies.
8. Click on the Print button.
9. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

About Reports & Summaries

Holiday Reports

The Holidays Report offers three report types:

- Holidays List - lists all the holidays that fall within the next 12 months as of the current date
    - Holidays designated as Once that occurred prior to the current viewing date will also be listed
- Selected Holiday Details - for viewing door auto lock unlock assignments on one specified holiday day
- Selected Date Range Holidays' Details - as above except the specified holidays are those that fall within a specified date range - 28 days maximum

The Holiday Reports screen lists both master holidays and site specific holidays relative to the selected site.

Include Past Holidays

The Include Past Holidays function will include all previous Once holidays in the report. If you do not want previous Once designated holidays in the Holiday List report, leave the Include Past Holidays function disabled.

Include Not Assigned Door Schedules

The Include Not Assigned Door Schedules function applies to the Selected Holiday Details report and Selected Date Range Holidays' Details reports. If you only want to view doors that have auto lock/unlock assignments on the specified holidays, leave the Include Not Assigned Door Schedules function disabled.

Procedures

Steps to Run a Holidays List

1. From the Client main screen, select the Reports button > Holiday Reports.
2. If you have multiple sites, click on the ▼ symbol opposite Site and select the site name from the drop down list.
3. Opposite Report Type, click on the ▼ symbol and select Holidays' List from the drop down list.
4. If you have any Once designated holidays listed before the current date and you want to include those holidays in the report, click in the box to the left of Include Past Holidays. The box has an x when enabled.
5. Select the Run Report button.
6. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
7. After you have reviewed the report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Run a Selected Holiday Details Report

1. From the Client main screen, select the Reports button > Holiday Reports.
2. If you have multiple sites, click on the ▼ symbol opposite Site and select the site name from the drop down list.
3. Opposite Report Type, click on the ▼ symbol and choose Selected Holiday Details from the drop down list.
4. From the holiday list table, select the holiday. The selected holiday is highlighted.
5. To include doors that do not have auto unlock/lock assignments on the holiday date, click in the box to the left of Include Not Assigned door schedules. The box has an x when this option is enabled.
6. Click on the Run Report button.

7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. After you have reviewed the report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Run a Selected Date Range Holidays' Details Report

1. From the Client main screen, select the Reports button > Holiday Reports.
2. If you have multiple sites, click on the symbol opposite Site and select the site name from the drop down list.
3. Opposite Report Type, click on the symbol and choose Selected Date Range Holidays' Details from the drop down list.
4. Click on the calendar icon to the right of From. Scroll to the desired month using the arrows. Select the date in the calendar.
5. Click on the calendar icon to the right of To. Scroll to the desired month. Select the date in the calendar.
    - The From and To dates must be within 28 days.
6. To include doors that do not have auto unlock/lock assignments on the holiday date, click in the box to the left of Include Not Assigned door schedules. The box has an x when this option is enabled.
7. Click on the Run Report button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. After you have reviewed the report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Holiday Report

1. From the Client main screen, select the Reports button > Holiday Reports.
2. If you have multiple sites, click on the symbol opposite Site and select the site name from the drop down list.
3. Select the desired report type and format options.
4. Select the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Holiday Report

1. From the Client main screen, select the Reports button > Holiday Reports.
2. If you have multiple sites, click on the symbol opposite Site and select the site name from the drop down list.
3. Select the desired report type and format options.
4. Select the Run Report button.
5. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.

9. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

About Reports and Summaries

People Information Reports

The People Information Report produces a report for all or selected person records.

Advanced Filter

The advanced filter in the People Information Report has the following fields which can be used individually or in any combination including all six simultaneously to locate a specific record or records.

- Name - searches for records based on Given Name, Middle Name (if enabled) and Surname
- Credential Number - searches for records based on Batch Number or Card Number
- Group Name - searches for records based on access level assignments
- Optional Field - searches for records based on optional field
- Site - searches for records based on site enrollment
- Person Type - searches for records based on type assigned
- Active - searches for records or credentials with an inactive status, active status or both (all)

To open the advanced filters, click on Advanced Filter.

Report Options

You can specify one of the following report options depending on the details required as noted:

- Show Photos When Searching - displays the person's on-file image on the search screen
- Print Selected People - lists the name, person type, credential number, credential type and the site
- Detailed Report - lists the name, person type, credential number, credential type, person active/inactive, extended entry (if applicable, group access assignments, the site and the following selectable options
    - Include Optional Fields - includes the entries in the person’s Common Optional and Site Optional fields
    - Include picture - inserts the person's on-file image in the report
    - Include Comments - inserts any comments noted in the Edit Person screen

Procedures

Steps to Run a People Information Report

1. From the Client main screen, select the Reports button > People Reports > People Information Report.
2. Do one of the following steps:
    - To run a report with all persons listed on the screen, click in the box to the left of Name. The box has an x when selected and automatically selects all the records.
    - To run a selective report, click in the box to the left under the Given Name column opposite each individual to be included in the report. The box has an x and the individual’s name is highlighted in blue.
    - To narrow the search, use the Advanced Filter options.

3. Depending on the desired type of report select either of the radio buttons opposite, Print Selected People or Detailed Report. If you selected Detailed Report, you may also select Include Optional Fields and/or Include Picture.
4. Click on the Run Report button.
5. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a People Report

1. From the Client main screen, select the Reports button > People Reports > People Information Reports.
2. Format the report.
3. Select the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a People Report

1. From the Client main screen, select the Reports button > People Reports > People Information Reports.
2. Format the report.
3. Select the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

About Reports and Summaries

Visitor Information Report

The Visitor Information Report provides a list of all persons whose record has had a visit scheduled whether it is past, present or future. You can configure the Visitor Information Report screen to include the following selectable report options.

- Print List - the report lists the person's name, person type, active/inactive status, and, if applicable, assigned credentials
- Detailed Report - the report lists the person's name, person type active/inactive status as well as the option of including the following details:
    - Include optional fields - lists any optional field entries for each visitor
    - Include credentials - lists any credentials assigned to the visitor
    - Include scheduled visits - lists any pending appointments currently scheduled for each visitor
    - Include visitor history - lists details of any past appointments for each visitor
    - Photo - includes the primary on-file image from the person's record

Procedures

Steps to Run a Visitor Information Report

1. From the Client main screen, select the Reports button > People Reports > Visitor Information Report.
2. From the Visitor Information Report screen, do one of the following steps:
    - For a report that includes all records listed on screen, click in the box to the left of Given Name heading to select all the individuals listed.
    - For a report that includes only a partial list of records, click in the box to the left of the individual's given name to select it for the report. The name is highlighted and the box has x when selected.
3. Click in the radio button to the left of either Print List or Detailed Report depending on the desired type of report. The radio button has a blue dot when selected.
4. If you selected Detailed Report, to include any of the selectable report options, click in the box to the left. The box has an x when selected.
5. Click on the Run Report button.
6. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Visitor Information Report

1. From the Client main screen, select the Reports button > People Reports > Visitor Information Report.
2. From the Visitor Information Report screen, format the report.
3. Select the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.

8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Visitor Information Report

1. From the Client main screen, select the Reports button > People Reports > Visitor Information Report.
2. From the Visitor Information Report screen, format the report.
3. Select the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

About Reports & Summaries

Visit Reports

The Visit Report screen allows generating quick summaries on various aspects of visitor activity. The screen is composed of two elements - Report Criteria and Report Options - which give you the ability to view a daily visitor list, quickly check the visitors currently in the building, or review monthly or weekly visit statistics. The following outlines the functions on the Visit Report screen.

Report Criteria

- Single Visit - lists visitors who have visited or will visit once based on the selected report options
- Returning Visits - lists visitors who have visited or will visit 2 or more times based on the selected report options
- Total Visitors by Month - lists the number of visitors each month based on the selected report options
- Total Visitors by Week - lists the number of visitors each week, from Monday to Friday, based on the selected report options

Report Options

- Scheduled Visit Status - lists visitors based on the selected status – all, expected, delayed arrival, arrived, departed, cancelled
- Date Range - the from and to date fields bracket the visit report period
- Given Name - lists visitor or visitors based on specified given name
- Surname - lists visitor or visitors based on specified surname

Procedures

Steps to Run a Visit Report

1. From the Client main screen, select the Reports button > People Reports > Visitor Report.
    - By default, if the screen was previously opened while logged on, the screen retains the last settings.
2. From the Visit Report screen under Report Criteria, select the desired option by clicking in the radio button on the left. The button has a blue dot when selected.
3. Under Report Options click on the ▼ symbol to the right of Scheduled visit status and select the desired status.
4. If selecting a From date other that the current date displayed, click on the calendar icon to the right and select a month and day. Use the arrows if necessary to scroll through the calendar.
5. If selecting a To date other that the current date displayed, click on the calendar icon to the right and select a month and day. Use the arrows if necessary to scroll through the calendar.
6. For a visit report listing an individual or individuals by a specific First Name, enter the name in the text box.
7. Click on the Run Report button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. After having reviewed the report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Visit Report

1. From the Client main screen, select the Reports button > People Reports > Visitor Report.

- By default, if the screen was previously opened while logged on, the screen retains the last settings.

2. From the Visit Report screen format the report by selecting the desired Report Criteria and the Report Options.
3. Click on the Run Report button.
4. From the Report Viewer screen, select the printer icon on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Visit Report

1. From the Client main screen, select the Reports button > People Reports > Visitor Report.
   - By default, if the screen was previously opened while logged on, the screen retains the last settings.
2. From the Visit Report screen format the report by selecting the desired Report Criteria and the Report Options.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Person Reader Access Report

The Person Reader Access Report summarizes individual credential holder's access levels at each door. With the optional setting Include schedule details selected, the report also includes schedule hours and holiday hours.

Procedures

Steps to Run a Person Reader Access Level Report

1. From the Client main screen, select the Report button > Person Reports > Person Reader Access Report.
    - By default, if the screen was previously opened while logged on, the screen retains the last settings.
2. Under the Sites heading, select the site or sites applicable to the report.
3. To refine your report to specific individuals, groups, person types etc., use the Advanced Filters.
4. To include photos in the report, click in the box to the left of Show photos when searching. The box has an x when selected.
5. To include the schedule details at each reader, click in the box to the left of Include schedule details. The box has an x when selected.
6. Select the person below the People heading. The person's record is highlighted in blue.
7. Click on the Run Report button.
8. Close the Keyscan Aurora Report Viewer by clicking on the x in the upper right corner.
    - To run another report, either select another person below People, or reset the advanced filters to populate a list of different people and select the person. Then click on the Run Report button.
9. To exit the Person Reader Access Report, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Person Reader Access Report

1. From the Client main screen, select the Reports button > Person Reports > Person Reader Access Report.
    - By default, if the screen was previously opened while logged on, the screen retains the last settings.
2. Format the report and select the individual.
3. Select the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Person Reader Access Report

1. From the Client main screen, select the Reports button > Person Reports > Person Reader Access Report.
    - By default, if the screen was previously opened while logged on, the screen retains the last settings.
2. Format the report and select the individual.
3. Select the Run Report button.

4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

About Reports & Summaries

Reader Access Report

The Reader Access Level Report summarizes group access levels at door control unit readers, and, if selected, the schedules for each specified door reader. You can include a listing of people with active credentials that belong to each door group in the report as well. Select individual or multiple door readers for your report. You can also export the report as a PDF document for non-system users. The Reader Access Level Report excludes elevator control unit readers.

Report Options

The Reader Access Report has optional settings for added details.

- Show reader's Access Control Unit - lists the door control unit connected to the reader
- Include schedule details - lists group schedule details for each reader (excludes groups with no access)
- Include groups with no access - lists the groups with no access at the reader
- Include people with active credentials - lists persons with active credentials under their respective groups in the report
    - Sort by surname - lists people alphabetically by surname when the Include people with active credentials option is selected
    - Sort by credential - lists people based on the assigned credential number from low to high values when the Include people with active credentials option is selected

Report Grouping

The Reader Access Report allows organizing the report either by reader or groups.

- Group by reader name - lists the reader with all group details below
- Group by group name - lists the group with all reader details below

Procedures

Steps to Run a Reader Access Level Report

1. From the Client main screen, select the Reports button > Door Reports > Reader Access Report.
    - By default, if the screen was previously opened while logged on, the screen retains the last settings.
2. From the Reader Access Level Report screen, do one of the following steps:
    - For a report that includes all readers listed on screen, click in the box to the left of the Name heading to select all the readers listed.
    - For a report that includes only a partial list of readers, click in the box to the left of the individual reader under the Name column to select it for the report. The reader is highlighted and the box has x when selected.
3. To include any of the selectable report options, click in the box to the left of the desired option to be included in the report. The box has an x when selected.
4. If required, select the desired Report Grouping option. The selected grouping radio button has a dot when selected.
5. Click on the Run Report button.
6. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.

7. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Reader Access Report

1. From the main screen select the Reports button > Door Reports > Reader Access Report.
2. Format the report. See Steps to Run a Reader Access Report for procedures on formatting a report.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Reader Access Report

1. From the main screen select the Reports button > Door Reports > Reader Access Report.
2. Format the report. See Steps to Run a Reader Access Report for procedures on formatting a report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

About Reports & Summaries

Group Access Report

The Group Access Report summarizes all predetermined group access levels within a specified site.

Report Options

The Group Access Report is furnished with the following options:

- Groups - select as many or as few active groups that you would like to run the report for
- Include readers/floors - includes readers and/or floors within the report for the groups selected
- Include schedule details - lists a person's schedule details for each reader
- Include optional field - if selected, optional fields will be displayed in the report
- Sort by surname - lists people alphabetically by surname within the report
- Sort by credential - lists people based on the assigned credential number from low to high values

Procedures

Steps to Run a Group Access Report

1. From the Client main screen, select the Reports button > Person Reports > Group Access Report.
2. If you have multiple sites, select the site for the Group Access Report from the drop down menu located at the top of the screen.
3. Select a Group (or groups) from the left-most column. A group is selected when the box beside it has an **x** icon.
4. Choose the Report Options from the right-most column by selecting the box beside it. An option is selected when the box has an **x** icon. Below these options, select between sorting by either Surname or Credential.
5. Click on the Run Report button.
6. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a Group Access Report

1. From the Client main screen, select the Reports button > Person Reports > Group Access Report.
2. If you have multiple sites, select the site for the Group Access Report from the drop down menu located at the top of the screen.
3. Select a Group (or groups) from the left-most column. A group is selected when the box beside it has an **x** icon.
4. Choose the Report Options from the right-most column by selecting the box beside it. An option is selected when the box has an **x** icon. Below these options, select between sorting by either Surname or Credential.
5. Click on the Run Report button.
6. Near the top of the report, click on the Printer icon located on the tool bar.

7. From the Print dialog box, select the printer, printer options, print range and number of copies.
8. Click on the Print button.
9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a Group Access Report

1. From the Client main screen, select the Reports button > Person Reports > Group Access Report.
2. If you have multiple sites, select the site for the Group Access Report from the drop down menu located at the top of the screen.
3. Select a Group (or groups) from the left-most column. A group is selected when the box beside it has an **x** icon.
4. Choose the Report Options from the right-most column by selecting the box beside it. An option is selected when the box has an **x** icon. Below these options, select between sorting by either Surname or Credential.
5. Click on the Run Report button.
6. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
7. From the Save As dialog box, navigate to the desired folder location.
8. Enter a name for the report in the File name text box.
9. Click on the Save button.
10. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Related Topic

About Reports & Summaries

Global ACU Report

The Global ACU Report is a configurable report containing a list of ACUs (access control units) and their properties for all selected sites.

Permissions: User needs to have Master or Admin permissions, as well as CanRunReports and View Hardware permission.

By default, the report will include the following ACU properties:

- Site Name
- Name
- Serial Number
- Type

The Global ACU report can also be configured to include these additional ACU properties:

- Status
- Regional time zone
- Firmware version
- Communications (Communication type and communications properties, depending on communication type)
- Pending packages
- Last polled
- Communication error count

Note: This report is only available in csv format.

Procedures

Steps to Run and/or Export a Global ACU Report

1. From the main screen select the Reports button > Global ACU Report.
2. Under the Sites heading, select the desired site or sites for the report. Selected sites have an x in the box to the left. Clicking in the box alternately selects - has an x - or de-selects - has no x - on each subsequent click.
3. Under the Report Columns heading, select the desired report columns to choose which ACU properties appear in the report. Selected columns/properties have an x in the box to the left. Clicking in the box alternately selects - has an x - or de-selects - has no x - on each subsequent click.
4. Click on the Export to CSV button
5. After finishing the report, either save a copy or simply view it and close it without saving.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

About Reports & Summaries

People Linked to Active Directory Report

The People Linked to Active Directory Report screen allows you to view whether or not People in a specific site(s) are Active Directory Linked. The generated report will contain a list of people in your selected site(s), their user/person type, their status, and whether or not they are Active Directory Linked (Yes or No). The report can be configured to include only those people who are Active Directory Linked ("Yes"), those who are not Active Directory Linked ("No"), or both ("All")

Procedures

Steps to Run a People Linked to Active Directory Report

1. From the main screen select the Reports button > People Reports > People Linked to Active Directory Report.
2. Under the Sites heading, select the desired site or sites for the report. Selected sites have an x in the box to the left. Clicking in the box alternately selects - has an x - or de-selects - has no x - on each subsequent click.
3. Under the Report Options heading, click the "Active Directory Linked" drop-down and choose from one of the following report options:
    - **All** - this will generate a report that includes all People in the chosen site(s), including Active Directory Linked and Non-Active Directory Linked People. Their Active Directory Linked Status will be included in the report as "Yes" or "No".
    - **Yes** - this will generate a report that only includes People in the chosen site(s) who are Active Directory Linked.
    - **No** - this will generate a report that only includes People in the chosen site(s) who are NOT Active Directory Linked.
4. Click on the Run Report button
5. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
6. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a People Linked to Active Directory Report

1. From the main screen select the Reports button > People Reports > People Linked to Active Directory Report.
2. Format the report. See Steps to Run a People Linked to Active Directory Report (above) for procedures.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a People Linked to Active Directory Report

1. From the main screen select the Reports button > People Reports > People Linked to Active Directory Report.
2. Format the report. See Steps to Run a People Linked to Active Directory Report (above) for procedures.

3. Click on the Run Report button.
4. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. Click on the x in the upper right corner to close the Keyscan Aurora Report Viewer screen when finished viewing the report.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

About Reports & Summaries

Schedule Assignment Report

The Schedule Assignment Report summarizes schedule types and assignments within a given site.

Procedures

Steps to Run a Schedule Assignment Report

1. From the Client main screen, select the Reports button > Schedule Assignment Report.
2. If you have multiple sites, select the site for the Schedule Assignment Report from the drop down menu located at the top of the screen.
3. Select a Schedule from the left-most column. A schedule is selected when highlighted in blue.
4. Click on the Run Report button.
5. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a Schedule Assignment Report

1. From the Client main screen, select the Reports button > Schedule Assignment Report.
2. If you have multiple sites, select the site for the Schedule Assignment Report from the drop down menu located at the top of the screen.
3. Select a Schedule from the left-most column. A schedule is selected when highlighted in blue.
4. Click on the Run Report button.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.
9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a Schedule Assignment Report

1. From the Client main screen, select the Reports button > Schedule Assignment Report.
2. If you have multiple sites, select the site for the Schedule Assignment Report from the drop down menu located at the top of the screen.
3. Select a Schedule from the left-most column. A schedule is selected when highlighted in blue.
4. Click on the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

E-Plex Door Access Report

The E-Plex Door Access Report summarizes group access levels at E-Plex Doors. Select individual or multiple wireless doors for your report.

Procedures

Steps to Run an E-Plex Door Access Report

1. From the Client main screen, select the Reports button > E-Plex Reports > E-Plex Door Access Report.
2. If you have multiple sites, select the site for the E-Plex Door Access Report from the drop down menu located at the top of the screen.
3. Select an E-Plex Door (or E-Plex doors) from the left-most column. An E-Plex door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print an E-Plex Door Access Report

1. From the Client main screen, select the Reports button > E-Plex Reports > E-Plex Door Access Report.
2. If you have multiple sites, select the site for the E-Plex Door Access Report from the drop down menu located at the top of the screen.
3. Select an E-Plex Door (or E-Plex doors) from the left-most column. An E-Plex door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export an E-Plex Door Access Report

1. From the Client main screen, select the Reports button > E-Plex Reports > E-Plex Door Access Report.
2. If you have multiple sites, select the site for the E-Plex Door Access Report from the drop down menu located at the top of the screen.
3. Select an E-Plex Door (or E-Plex doors) from the left-most column. An E-Plex door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.

9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

E-Plex Battery Level Report

The E-Plex Battery Level Report summarizes the batter status of a given E-Plex lock and shows the date, if applicable, of when the batteries were last changed.

Procedures

Steps to Run an E-Plex Battery Level Report

1. From the Client main screen, select the Reports button > E-Plex Reports > E-Plex Battery Level Report.
2. If you have multiple sites, select the site for the E-Plex Battery Level Report from the drop down menu located at the top of the screen.
3. Select an E-Plex Door (or E-Plex doors) from the left-most column. An E-Plex door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print an E-Plex Battery Level Report

1. From the Client main screen, select the Reports button > E-Plex Reports > E-Plex Battery Level Report.
2. If you have multiple sites, select the site for the E-Plex Battery Level Report from the drop down menu located at the top of the screen.
3. Select an E-Plex Door (or E-Plex doors) from the left-most column. An E-Plex door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export an E-Plex Battery Level Report

1. From the Client main screen, select the Reports button > E-Plex Reports > E-Plex Battery Level Report.
2. If you have multiple sites, select the site for the E-Plex Battery Level Report from the drop down menu located at the top of the screen.
3. Select an E-Plex Door (or E-Plex doors) from the left-most column. An E-Plex door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.

9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST Available Guest Credentials Report

The Best Available Guest Credentials Report shows available credentials that will gain 24-hour direct guest access to the specified door. Available guest credentials are unused or expired credentials that fall within the Guest Card Ranges configured for the selected door. This report does not show any active credentials (unavailable credentials) for a door until they expire.

Procedures

Steps to Run a BEST Available Guest Credentials Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Available Guest Credentials Report.
2. If you have multiple sites, select the site for the BEST Available Guest Credentials Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Available Guest Credentials Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Available Guest Credentials Report.
2. If you have multiple sites, select the site for the BEST Available Guest Credentials Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Available Guest Credentials Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Available Guest Credentials Report.
2. If you have multiple sites, select the site for the BEST Available Guest Credentials Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.

5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.
9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST Available Guest Ranges Report

The BEST Available Guest Ranges Report outlines available credentials within the outlined start and end Guest Card Range within a given site.

Procedures

Steps to Run a BEST Available Guest Ranges Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Available Guest Ranges Report.
2. If you have multiple sites, select the site for the BEST Available Guest Ranges Report from the drop down menu located at the top of the screen.
3. Click on the Run Report button.
4. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Available Guest Ranges Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Available Guest Ranges Report.
2. If you have multiple sites, select the site for the BEST Available Guest Ranges Report from the drop down menu located at the top of the screen.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Available Guest Ranges Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Available Guest Ranges Report.
2. If you have multiple sites, select the site for the BEST Available Guest Ranges Report from the drop down menu located at the top of the screen.
3. Click on the Run Report button.
4. From the Report Viewer, click on the ☐ symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST Used Guest Ranges Report

The BEST Used Guest Ranges Report outlines credentials already in use within the outlined start and end Guest Card Range within a given site. Each card range also shows the BEST Door and BEST Door Groups associated with each.

Procedures

Steps to Run a BEST Used Guest Ranges Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Used Guest Ranges Report.
2. If you have multiple sites, select the site for the BEST Used Guest Ranges Report from the drop down menu located at the top of the screen.
3. Click on the Run Report button.
4. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Used Guest Ranges Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Used Guest Ranges Report.
2. If you have multiple sites, select the site for the BEST Used Guest Ranges Report from the drop down menu located at the top of the screen.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Used Guest Ranges Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Used Guest Ranges Report.
2. If you have multiple sites, select the site for the BEST Used Guest Ranges Report from the drop down menu located at the top of the screen.
3. Click on the Run Report button.
4. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST Door Access Report

The BEST Door Access Report summarizes group access levels at BEST doors. Select Individual or multiple doors for your report.

Procedures

Steps to Run a BEST Door Access Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Door Access Report.
2. If you have multiple sites, select the site for the BEST Door Access Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Door Access Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Door Access Report.
2. If you have multiple sites, select the site for the BEST Door Access Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Door Access Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Door Access Report.
2. If you have multiple sites, select the site for the BEST Door Access Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.

9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST Guest Door Access Report

The BEST Guest Door Access Report shows which people and credentials have 24 hour access to BEST Guest doors. You can select individual or multiple wireless locks for your report. You can also export the report as a PDF document for non-system users.

Procedures

Steps to Run a BEST Guest Door Access Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Guest Door Access Report.
2. If you have multiple sites, select the site for the BEST Guest Door Access Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Guest Door Access Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Guest Door Access Report.
2. If you have multiple sites, select the site for the BEST Guest Door Access Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Guest Door Access Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Guest Door Access Report.
2. If you have multiple sites, select the site for the BEST Guest Door Access Report from the drop down menu located at the top of the screen.
3. Select a BEST Door (or BEST doors) from the left-most column. A BEST door is selected when the box beside it has an **x** icon.
4. Click on the Run Report button.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.

6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.
9. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST DOOR CREDENTIAL ASSIGNMENT REPORT

The BEST Door Credential Assignment Report summarizes BEST Door Groups, doors and number of credentials within a given site.

Procedures

Steps to Run a BEST Door Credential Assignment Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Door Group Assignment Report.
2. Select a Site from the left-most column. An site is selected when the box beside it has an **x** icon.
3. Click on the Run Report button.
4. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Door Credential Assignment Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Door Group Assignment Report.
2. Select a Site from the left-most column. An site is selected when the box beside it has an **x** icon.
3. Click on the Run Report button.
4. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Door Credential Assignment Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Door Group Assignment Report.
2. Select a Site from the left-most column. An site is selected when the box beside it has an **x** icon.
3. Click on the Run Report button.
4. Near the top of the report, click on the Printer icon located on the tool bar.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

BEST Credential History Report

This report summarizes the history of a BEST Credential, including the Person it belongs (or belonged) to, when it was assigned, when it was removed, alongside other information.

Procedures

Steps to Run a BEST Credential History Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Credential History Report.
2. Search for the applicable BEST Credential by either inputting the credential number into the BEST Credential field located at the top-left of the screen, or by selecting the Site from the drop-down menu at the top-right of the screen.
3. Select a BEST Credential; a credential is selected when the box beside it has an **x** .
4. Select the Run Report button.
5. After finishing the report, select the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a BEST Credential History Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Credential History Report.
2. Search for the applicable BEST Credential by either inputting the credential number into the BEST Credential field located at the top-left of the screen, or by selecting the Site from the drop-down menu at the top-right of the screen.
3. Select a BEST Credential; a credential is selected when the box beside it has an **x** .
4. Select the Run Report button.
5. Near the top of the report, select the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Select the Print button.
8. After finishing the report, select the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a BEST Credential History Report

1. From the Client main screen, select the Reports button > BEST Reports > BEST Credential History Report.
2. Search for the applicable BEST Credential by either inputting the credential number into the BEST Credential field located at the top-left of the screen, or by selecting the Site from the drop-down menu at the top-right of the screen.
3. Select a BEST Credential; a credential is selected when the box beside it has an **x** .
4. Select the Run Report button.
5. From the Report Viewer, select the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.

8. Select the Save button.
9. After finishing the report, select the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Gateway & ZigBee Information Report

The Gateway & ZigBee Information Report summarizes gateway status, communication, etc.

Procedures

Steps to Run a Gateway & ZigBee Information Report

1. From the Client main screen, select the Reports button > E-Plex Reports > Gateway & ZigBee Information Report.
2. Select a Gateway (or gateways) from the left-most column. A gateway is selected when the box beside it has an **x** icon.
3. Click on the Run Report button.
4. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Print a Gateway & ZigBee Information Report

1. From the Client main screen, select the Reports button > E-Plex Reports > Gateway & ZigBee Information Report.
2. Select a Gateway (or gateways) from the left-most column. A gateway is selected when the box beside it has an **x** icon.
3. Click on the Run Report button.
4. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.
5. Near the top of the report, click on the Printer icon located on the tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Steps to Export a Gateway & ZigBee Information Report

1. From the Client main screen, select the Reports button > E-Plex Reports > Gateway & ZigBee Information Report.
2. Select a Gateway (or gateways) from the left-most column. A gateway is selected when the box beside it has an **x** icon.
3. Click on the Run Report button.
4. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the **x** in the upper right corner of the Keyscan Aurora Report Viewer.

Related Topic

About Reports & Summaries

Alarm Watch Report and Setup

The Alarm Watch Report produces a list of credentials indicating their status as IN or OUT, the date and time when recorded as in or out, and the door location. This report can be especially beneficial during emergencies or building evacuations to determine who has left the building and who is still present. The Alarm Watch Report can be configured to run in the following ways:

- automatically generate and e-mail a PDF report to a recipient address when triggered by an input device
- manually generate a report at the Client workstation at any time

The sub-headings below outline the requirements for each method of running the report.

Requirements for an Automatic Report

In order to generate and automatically e-mail the report, the following conditions must exist:

- have a controlled enter/exit configuration of readers for an accurate status of who is in or out of the building or buildings
- have an input that can manually or automatically trigger the alarm watch which could be any of the following input type devices:
    - push button
    - key switch
    - integration output trigger (example - fire alarm panel)
- have the SMTP settings configured in the Client's Application Utilities screen which is accessed from the Settings menu
- have the Keyscan Aurora Agent running
- have recipient e-mail addresses
- have the system user account enabled for alarm watch - the permission is set in the Manage System User screen under Permissions > Software > Alarm Watch - to enable the function, click in the box to the left

Requirements for a Manual Report

In order to generate the report, the following conditions must exist:

- have a controlled enter/exit configuration of readers for an accurate status of who is in or out of the building or buildings
- have the system user account enabled for alarm watch - the permission is set in the Manage System User screen under Permissions > Software > Alarm Watch - to enable the function, click in the box to the left

Procedures

Steps to Setup the Alarm Watch for an Automatic Report

Ensure that you have reviewed the requirements above.

1. From the Client main screen, select the Reports button > Door Reports > Alarm Watch Report.

2. Near the top of the Alarm Watch Report screen, click on the symbol at the right of Site and select the correct site.
3. To the right of Access Control Unit, click on the symbol and select the access control unit. This will be the control unit that is connected to the input device designated to trigger the alarm watch report.
4. To the right of Input, click on the symbol and select the auxiliary input.
5. To the right of Direction, click on the symbol and select the direction:
    - All - lists all credentials in the three categories below
    - Unknown - lists credentials that have not been used since midnight of the day the report is run
    - In - lists credentials with IN status only
    - Out - lists credentials with OUT status only
6. To delay compiling the report after the input is tripped, click on the symbol at the right of Delay and select a time delay from the drop down list. The times are in minutes. To have the report created immediately after the input is tripped, leave the Delay setting on zero (0).
7. Specify the e-mail address of the person receiving the report in the E-mail text box. If you have more than one e-mail address recipient, place a semi-colon (;) between each address.
8. The Active People Only option is pre-selected. This represents records that are currently set on Active status in the Edit Person screen. If you do not want this option, click in the box to the left to de-select it. When de-selected, the box is empty.
9. To list persons who have not used any of the assigned readers in the table, click in the box to the left of Only list people who have not used selected readers.
10. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
11. To list Person Type, click the box to the left of Include person type; otherwise go to the next step.
12. Under Include optional fields, select up to two Optional Fields to be included.
13. Under Readers, click in the box of each applicable reader that is used for determining the in/out status of all credential holders. Selected readers have an x in the box.
14. Click on the Save button.
15. Click on the Back button until you return to the main screen or the history navigation  symbol for a previously viewed screen.

Note: Automatic Reports are generated in 2, 5, 10, and 20 minute intervals. These values are standard and cannot be changed.

Following the setup of the alarm watch, Keyscan suggests testing the function by tripping the designated input device to be sure the PDF report is received by the intended e-mail recipient.

Steps to Manually Run an Alarm Watch Report

1. From the Client main screen, select the Reports button > Door Reports > Alarm Watch Report.
2. Near the top of the Alarm Watch Report screen, click on the symbol at the right of Site and select the correct site.
3. To the right of Direction, click on the symbol and select the direction:
    - All - lists all credentials in the three categories below
    - Unknown - lists credentials that have not been used
    - In - lists credentials with IN status only
    - Out - lists credentials with OUT status only

4. The Active People Only option is pre-selected. This represents records that are currently set on Active status in the Edit Person screen. If you do not want this option, click in the box to the left to de-select it. When de-selected, the box is empty.
5. To list persons who have not used any of the assigned readers in the table, click in the box to the left of Only list people who have not used selected readers.
6. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
7. To list Person Type, click the box to the left of Include person type; otherwise go to the next step.
8. Under Include optional fields, select up to two Optional Fields to be included.
9. Under Reader, click in the box of each applicable reader that is used for determining the in/out status of credential holders. Selected readers have an x in the box.
10. Click on the Run Report button.
11. When you have completed examining the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
12. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Keyscan Aurora Agent

SMTP Setup

Site Setup Report

The Site Setup Report provides a comprehensive summary of important and valuable information about your access control system. Keyscan recommends that you run, print, or export a PDF site report as a documented backup of all your site settings in the event that your database becomes corrupted or you experience a computer failure. Having a backup paper copy would allow you to re-input all your current settings. Before running the report, select the options that apply to your site. Whenever, you make changes to your access control system, you should run and print an updated version.

Procedures

Steps to Run and Print a Site Setup Report

1. From the Client main screen, select the Reports button > Site Setup Report.
2. Opposite the Site heading, click on the ▼ symbol and select the site from the list.
3. Under the Report Options heading, select or de-select the desired report categories by clicking in the boxes to the left. The box on the left has an X when it is selected.
    - You can click on the Select All button to enable all the report options.
4. Click on the Run Report button.
5. After Aurora has compiled the report, click on the print icon on the Report Viewer tool bar.
6. From the Print dialog box, select the printer, printer options, print range and number of copies.
7. Click on the Print button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Run and Export a Site Information Report

1. From the Client main screen, select the Reports button > Site Information Report.
2. Opposite the Site heading, click on the ▼ symbol and select the site from the list.
3. Under the Site Setup Report Options heading, select or de-select the desired report categories by clicking in the boxes to the left. The box has an X when it is selected.
4. Click on the Run Report button.
5. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
6. From the Save As dialog box, navigate to the desired folder location.
7. Enter a name for the report in the File name text box.
8. Click on the Save button.
9. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

System Log Report

The System Log Report screen lists entries and actions made by system users. The screen is designed to allow you to perform searches for specific types of logs as well as export or print system log reports.

Logging Level

The Application Settings screen has a Logging Level function which affects the level of details captured by a system log report. Logging Level has the following settings and pertains to access control related tasks performed by a system user.

- Basic - indicates the system user made a change to a setting
- Enhanced - indicates the system user made a change and the details of the change to a setting

The Logging Levels is accessed from the Settings menu > Application Utilities. For more about this function, select the link below Related Topics.

Report Options

The System Log Report screen has the following filtering options for customizing the report. If a system log report is run without any of the following report options set the report will list all system user activity from the last point that the database was purged.

- Date range - sets a specific time period for the system log report
- Updated by - limits the report to the activity of the specified system user
- Action - specifies the type of system user activity such as updated, added deleted, etc.
- Type - specifies the element within the software that was changed such as person, ACU etc.
- Name - lists the specific name of the element that was changed
- Action Details - lists the changes made
- Workstation - specifies the Client workstation to collect the system log from
- Maximum Displayed Entries - limits the report to a maximum number of system user activity records
- Include system logs across all sites - shows user activity for changes made to functions that are non-site specific such as the Settings menu functions
- Show action details - turn the action details column on or off

Include Report Settings

When the Include Report Settings is enabled, on the last page the report lists the selected settings that were used to compose the report.

Procedures

Steps to Run a System Log Report

1. From the Client main screen, select the Reports button > System Log Report.
2. Below the Sites heading, do one of the following steps:
    - For a report that includes all sites, click in the box to the left of the Name heading to select all the sites listed.

- For a report that includes only a partial list of sites, click in the box to the left of the individual site listed below the Name column to select it for the report. The site is highlighted and the box has x when selected.

3. To include any of the selectable report options, click in the box to the left of the desired option to be included in the report. The box has an x when selected.
    - For specifying a date range, click on the calendar icon to the left of From, use the arrows to scroll to the month and then click on a day. Repeat the same process to set the To date.
4. Click on the Search button. The results are displayed under System Log Entries.
    - You cannot run a report until you have selected the Search button.
5. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
6. Click on the Run Report button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a System Log Report

1. From the Client main screen, select the Reports button > System Log Report.
2. Below the Sites heading, do one of the following steps:
    - For a report that includes all sites, click in the box to the left of the Name heading to select all the sites listed.
    - For a report that includes only a partial list of sites, click in the box to the left of the individual site listed below the Name column to select it for the report. The site is highlighted and the box has x when selected.
3. Format the report using any of the Report Options filters.
4. Click on the Search button.
5. Click on the Run Report button. Depending on the size, the report may take a few minutes to compile.
6. After Aurora has compiled the report, click on the print icon on the Report Viewer tool bar.
7. From the Print dialog box, select the printer, printer options, print range and number of copies.
8. Click on the Print button.
9. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a System Log Report

1. From the Client main screen, select the Reports button > System Log Report.
2. Below the Sites heading, do one of the following steps:
    - For a report that includes all sites, click in the box to the left of the Name heading to select all the sites listed.
    - For a report that includes only a partial list of sites, click in the box to the left of the individual site listed below the Name column to select it for the report. The site is highlighted and the box has x when selected.
3. Format the report using any of the Report Options filters.

4. Click on the Search button.
5. Click on the Run Report button.
6. From the Report Viewer, click on the symbol opposite the Export icon and select the desired export file format.
7. From the Save As dialog box, navigate to the desired folder location.
8. Enter a name for the report in the File name text box.
9. Click on the Save button.
10. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Logging Levels

About Reports & Summaries

Aurora Icons & Symbols

Transactions Reports

Transaction reports give you the ability of reviewing virtually any site activity based on criteria that you select. You can create a one-time report, create and save a named report for repeated use, print reports, export reports, schedule when reports are run, and e-mail reports (PDF).



In order to schedule a report, you must first name and format the report.

The Transaction Report screen is divided into the following sub-screens:

- Report Customization
- Transaction Filters
- People Filters
- Credential Filters
- Device Filters
- Schedule Filters

The sub-headings below outline the general function of each transaction report sub-screen.

Report Customization

Use the Report Customization for selecting the sites, dates, and data field columns in the report. Within the specified dates, transactions are captured from the following times:

- start time commences at 00 minutes, 00 seconds
- end time concludes at 59 minutes, 59 seconds

Include Graph

Enabling this option inserts a graph at the end of the report.

Report Columns

Report Columns allows selecting which column headings and data are included in the report. Device, Transaction and Transaction Date cannot be de-selected.



After formatting a report and you intend to run it repeatedly, save it so that you only have to format it once. This also gives you the option of automatically scheduling when it runs as well as distributing it by e-mail.

Transaction Filters

The Transaction Filters screen is used to specify which types of transactions the report includes, such as access granted, access denied, alarm tripped, etc., You can select or de-select specific transaction types by clicking in the individual boxes to the left or you can select/de-select all transaction types by clicking in the box to the left of the Transactions heading at the top.

When selecting transaction filters you must also be sure that you have selected the relative devices for those transactions in the Device Filters screen.

People Filters

This screen is used to specify which persons are included in the report. This can be a single credential holder, a group of credential holders, or all credential holders.

Credential Filters

This screen is used to specify which credentials are included in the report. You can select a single credential, multiple credentials or all credentials or specify credentials by group. The Credential Filters screen can also be used to identify credentials to whom they are assigned.

Device Filters

This screen is used to specify which devices will be included within the Transaction Report and consists of the following headings:

- Access Control Units
- Doors
- E-Plex Doors
- Auxiliary Outputs
- Inputs
- IOCBs
- Floors
- Intrusion Partitions
- Intrusion Zones
- Intrusion Areas



If an Access Control Unit is selected, all devices associated with that ACU will not appear in the Transaction Report. Select each device to include them within the report.

Schedule Filters

The Schedule Filters screen is used to specify which schedule or schedules apply to the report.

Include Report Settings

When the Include Report Settings is enabled, on the last page the report lists the selected settings that were used to compose the report.

Procedures

Steps to Name, Format, Save and Run a Transaction Report

When setting out to format a report, you may have to experiment with the different filtering options until you get the desired information for the report.

1. From the Client main screen, select the Reports button > Transaction Report.
2. From the Transaction Report screen, ensure the Report Customization tab is selected.
    - To name, run, and save a formatted report, go to the next step.
    - To run a one time report, go to step 5.

3. Click on the + button to the left of Transaction Reports.
4. By default Aurora creates Transaction Report # x and inserts it in the text box. You can accept the default name or change it. To change the default name, insert the cursor inside the Report Name text box, select the Transaction Report # x text, press the delete key and enter a description for the type of report you are going to produce.
    - As an example if you were running a report to check for access denied violations on a weekly basis, you could call the report Weekly Access Denied Report which would be more specific than the generic default name Transaction Report # x.
5. Below sites, select or de-select the sites to be included in the report.
6. Below the Date Settings heading, you have one of the following three options for setting the date parameters of the report. Follow one of the three procedures below for setting the time frame of the report:
    - Date range - Click in the radio button to the left to select this option. Click on the Calendar icon to the right of From. If the month is other than the current month, click on the arrows in the calendar to go back or forward to the desired month. Click on the day in the calendar. Repeat to set the To date. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes.
    - Last number of days - Click in the radio button to the left to select this option. Click in the number text box and enter the desired number of days. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.
        - If setting last number of days for the current day, set the number to zero (0).
    - One day - Click in the radio button to the left to select this option. Click on the Calendar icon to the right of Date. If the month is other than the current month, click on the arrows in the calendar to go back or forward to the desired month. Click on the day in the calendar. If required, set the Start Time by clicking on the calendar icon to the right and select the time in the drop down list. If the minutes are other than 00, select them in the text box and enter the desired start minutes. Repeat for the End Time.

      With all three of these Date Settings options, you must also specify what regional time zone the transaction date/times should be displayed in when the report is run. To choose a time zone, simply use the drop-down menu and select one of the available options.
7. Below the Report Columns heading, you can de-select undesired columns from being compiled in the report. Click in the box to the left to de-select the column. The box does not have an x when de-selected.
    - Report columns that are dimmed and grey cannot be de-selected.
8. To include any credential holder common optional fields in the Transaction Report, click in the box to the left of the desired field listed below the Include Optional Fields heading.
9. To list the report settings, click in the box to the left of Include Report Settings; otherwise go to the next step.
10. Select the Transaction Filters tab.
11. By default, Include all transactions is pre-selected at the top. If the report is to include only specific transactions, de-select Include all transactions by clicking in the box to the left. Then select the transaction types you want included in the report by clicking in the individual boxes on the left. When selected the box has an x.
12. If you are formatting the report on the basis of including people with associated people filters, go to step 13. If you are including people but it is more on the basis of searching for credentials using credential filters, go to step 15.
13. Select the People Filters tab.
14. Do one of the following steps:

- If the report is to list all individuals with records, leave the Include all people and credentials selected. The box has an x when selected.

- If the report is to list only select individuals, first de-select the Include all people and credentials option. The box no longer has an x when it is de-selected. Under the Search Results heading, all persons are listed. To refine your search you can use the Advanced Filter options. Under the Search Results heading, select the person and then click on the > symbol to add the record in the People in Report list. Repeat selecting the desired individuals and clicking on the > symbol until the list is complete. Or to transfer all the records, click in the box to the left of Select All under the Search Results heading, and click on the > symbol. All the records are transferred.

15. Select the Credential Filters tab.
    - If the report is to list all individuals with records, leave the Include all people and credentials selected. The box has an x when selected.

    - If the report is to list only select credentials, first de-select the Include all people and credentials option. The box no longer has an x when it is de-selected. Specify the credential information by completing the available parameters. Select the Search button. For selecting all listed credentials, click in the box to the left of Number. All boxes have an x when selected. For selecting individual credentials, click in the box to the left of the credential under the Number column. The box has an x when the credential is selected.

16. Select the Device Filters tab.
17. Select the devices you want included in the report by clicking in the individual boxes to the left. When selected the box has an x.
18. Select the Schedule Filters tab.
19. Select the schedules you want included in the report by clicking in the individual boxes to the left. When selected the box has an x.
20. When the report has been completely formatted, and if you named the report in step 3, click on the Save button; otherwise go to the next step.
21. Click on the Run Report button.
22. After reviewing the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer screen. For printing and exporting reports, see the steps below.
23. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Print a Report

1. From the Client main screen, select the Reports button > Transaction Report.
    - If you are printing a named report, click on the symbol to the right of Transaction Reports and select the desired report from the drop down list.

2. Format any settings that may apply to the report.
3. Click on the Run Report button.
4. After Aurora has compiled the report, click on the print icon.
5. From the Print dialog box, select the printer, printer options, print range and number of copies.
6. Click on the Print button.
7. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Export a Report

1. From the Client main screen, select the Reports button > Transaction Report.

- If you are exporting a named report, click on the ▼ symbol to the right of Transaction Reports and select the desired report from the drop down list.

2. Format any settings that may apply to the report.
3. Click on the Run Report button.
4. From the Report Viewer, click on the ▼ symbol opposite the Export icon and select the desired export file format.
5. From the Save As dialog box, navigate to the desired folder location.
6. Enter a name for the report in the File name text box.
7. Click on the Save button.
8. After finishing with the report, click on the x in the upper right corner of the Keyscan Aurora Report Viewer.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Delete a Report

1. From the Client main screen, select the Reports button > Transaction Report.
2. Click on the ▼ symbol to the right of Transaction Reports and select the desired report from the drop down list.
3. Click on the waste bin icon to the right of the Transaction Report.
4. Click on the Yes button in the Please confirm deletion of ..... warning box.
5. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Schedule Aurora for Automatic Tasks

About Reports & Summaries

Aurora Icons & Symbols

Introduction

The Intrusion Control Unit Integration license * allows interfacing supported alarm panels with the Aurora access control software. An Intrusion Control Unit Integration license offers the following functionality:

- Manual arming and disarming of partitions/areas from the Client's Intrusion Partition Status screen
- Manual arming and disarming of partitions/areas from the Client's Active Mapping function
- Arming and disarming using Present3 at a target reader
- Monitor, arm and disarm partitions/areas from the Client’s Intrusion Partition Status screen

Pre-configuration Note

Before you begin to configure the intrusion control units in the Keyscan Client, you must have previously installed and programmed the alarm panels as reviewed in the alarm panel manufacturer’s installation literature. You must also have set up a site for the access control system. Ensure that when configuring users and partitions in the Keyscan Client, they match the alarm panel setup including PIN codes.

If you have not yet setup a site in the access control software, click on the Contents tab in the upper left of the Help and refer to Basic Site Setup > Basic Site Setup Procedures.

Please note, when setting up a DSC Alarm Panel Integration module, the DSC master code is a required entry. The DSC master code is necessary to establish successful communication between the Keyscan software and the DSC alarm panel. Please refer to your DSC literature or contact your installing dealer if you are not sure what your DSC master code is.

Keyscan's integration license is only compatible with units on the Hardware Setup screen.

The intrusion control unit communication is designed to run as a service.

Supported Intrusion Control Units

The following outlines currently supported intrusion control unit manufacturers and models:

DSC

- Power Series
- MAXSYS

DMP

- XR550DN

DSC Data Interface Modules

In order to integrate with a Keyscan system, the Power Series and the MAXSYS alarm panels require optional data interface modules listed below, which are available through a DSC hardware supplier.

- Power Series requires a DSC IT-100 module
- MAXSYS requires a DSC PC4401 module

* Integration features are subject to change and are limited to third party product features.

System User Account Settings

In order to setup the intrusion control units or have the ability to arm and disarm partitions or areas, you must enable the following settings in the Manage System Users screen on the applicable sites:

- Hardware > Add Hardware - must be enabled for adding an intrusion control unit
- Hardware > Intrusion Related > Zones / Intrusion Partitions (DSC) / Intrusion Areas (DMP) / Intrusion Users - the edit function must be enabled to name zones, partitions, areas and user names /passwords
- Toggle Devices > Can Arm / Can Disarm - these functions must be enabled for manually arming and disarming partitions or areas

For setting up system user accounts, select the link below.

Related Topics

Manage System Users

Add an Intrusion Control Unit

To integrate an intrusion control unit in the Keyscan Client, the unit must be configured in the Hardware Setup screen. Communication for the intrusion control units is restricted to a network connection with a NETCOM. Serial and modem communication are not supported.

The Aurora Client software depending on the version supports the following intrusion control units per site:

- Aurora version 1.0.1.0 to 1.0.7.0 - supports 1 DSC intrusion control unit per site
- Aurora version 1.0.8.0 or higher - supports multiple DSC intrusion control units per site
- Aurora version 1.0.12.0 or higher - supports multiple DMP intrusion control units per site

Please note that you are required to create a serial number for the intrusion control unit. The serial number you create for the intrusion control unit cannot be a duplicate serial number of a Keyscan access or elevator control unit installed on any of your sites.

Be sure that the NETCOM device has been programmed with an IP address.

These procedures should be performed by the dealer/installer.

When the intrusion control unit is added and saved the software synchronizes the intrusion control unit PC/ server clock with the alarm system clock. However, periodically you may have to manually synchronize the clocks. For more information, click on the link below Related Topic.

Procedures

Steps to Integrate an Intrusion Control Unit

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, double click on the desired site in the Site Search - Hardware Setup directory screen.
2. From the Hardware Setup screen, select the ▼ symbol on the right side of the Add 8 Door Controller button.
    - By default, Add 8 Door Controller is listed. However, the Add button lists the last type of hardware selected while the Hardware Setup screen is open when enrolling multiple types of components.
3. Select the intrusion control unit from the drop down list.
4. From the Confirm Hardware Installation screen, click on the Yes button.
5. Opposite the Name field, the Client inserts a default name of Intrusion Control Unit #1. You can leave the default name (recommended) or change the name if you prefer by clicking inside the Name text box and enter a name for the unit.
6. Click inside the Serial Number text box and enter a serial number starting with an upper case alpha character followed by four numeric characters - example: Z1234. Ensure that you do not create a serial number that duplicates a Keyscan door control unit or elevator control unit installed on the access control system.
7. Opposite Status, ensure Active is selected. If Inactive or Disabled is selected, click on the ▼ symbol and select Active from the drop down list.
8. Opposite Regional Time Zone, click on the ▼ symbol and select the geographic time zone where the intrusion control unit is located.
9. In the Hardware Notes text box, enter any appropriate information. Listing a description of where in the building the intrusion panel is physically located will help other technicians in the event that the unit requires maintenance in the future.

10. Below the Communication heading opposite Communication Port, if the network port of the server with the Keyscan intrusion communication service is other than Port 3001, click in the text box and enter the server communication port. Generally port 3001 is the standard network communication port. You may have to consult with the IT administrator.
11. In the IP Address field, do one of the following steps:
    - For DSC intrusion panels, enter the IP address assigned to the NETCOM device that is connected to the intrusion control unit's interface module
    - For DMP intrusion panels, enter the IP address assigned to the unit
12. If the Communication Server is other than the server displayed, click on the ▼ symbol and select the server from the drop down list. This must be the server with the Keyscan Aurora Intrusion Communication service.
13. For a DMP intrusion panel, enter the account number in the Account Number text box. This is a DMP assigned setting.
14. To test if you can communicate with the NETCOM device from this workstation/server, click on the Ping button. If you have communication to the NETCOM, you will see a reply from with the IP address. No connection will produce a failed to connect with the IP address message.
15. Click on the Save Button.
16. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topic

Synchronize Clocks

Communication Setup

When the Intrusion Integration software is installed, intrusion communication software is installed automatically and configured to run as a Window's service and defaulted on start so it is running.

Keyscan suggests that you confirm the intrusion communication is running. To verify, select start > Control Panel > Administrative Tools > Services. Scroll down the Services window until you locate Keyscan Aurora Intrusion Communication. The Status column reports Started indicating the service is operating.

If the status is listed as Stopped, double click on the Keyscan Aurora Intrusion Communication and select the Start button to resume the service.

Intrusion Delay Setting

As an option you can control the time interval that Keyscan Aurora Intrusion Communication service sends commands from Aurora to the intrusion panel. The Intrusion Delay is accessed by selecting the Settings button > Application Utilities > Application Settings tab. The Intrusion Delay settings are as follows:

- Default: 600 milliseconds
- Extended: 1200 milliseconds
- Extended x2: 1800 milliseconds

To change the delay, click on the ▼ symbol on the far right of Intrusion Delay and select an interval from the list as noted above.

Communication Test

You can also test communication with DSC intrusion units from the Access Control Unit Status screen. This does not apply for DMP units.

Procedure

Steps to Test DSC Intrusion Unit Communication

1. From the main screen, select the Status button > Status.
2. On the Status screen's left panel, double click on Access Control Unit Status.
3. Click on the ▼ symbol at the right of Select Site and choose the desired site from the list.
4. Locate the DSC intrusion unit in the table.
5. Locate the Upload column. Along the row of the applicable intrusion unit, click on the ▼ symbol to the right on the Full Upload button and select Test from the list.
6. From the Test confirmation box: Are you sure you want to do this?, click on the Yes button.
7. Look under the Communication Error Count column to the extreme right of the screen along the same row of the intrusion unit:
    - if you see an error count in the row, Aurora does not have communication - check settings - ensure the Intrusion Communication Service is running
    - if you do not see an error count in the row, Aurora has communication

Enter Master Code & Users

The Hardware Setup > User screen is for the following 2 configuration settings:

- Entering the Master Code (Master User) for DSC Integration
- Defining either groups or credential holders using Present3 at a target reader for arming and disarming the intrusion control unit partitions

DSC Master Code

In order for the Keyscan Client to integrate with the alarm panel, the master code must be entered in the User screen otherwise you cannot send or receive data between the alarm panel and the Keyscan software. You should not assign the master code to any individual users.

The master code does not apply to DMP alarm panels.

User # / Pin Code

If you intend to use Present3, you define users either individually or by door group in the User screen. The maximum number of users you can define depends on the alarm panel model that was enrolled in the Hardware Setup > Information screen.

Keyscan recommends using the same door group descriptions and card holder names in the User screen as they are defined in the Groups Setup screen and the Edit People screen for easy reference when you need to know who has P3 privileges for arming and disarming the alarm panel partitions.

The following are two samples of how you might define door group/user names and just door group names:

- Management-JSmith - when assigning P3 for specific cardholders - list the group and the individual
- Management - when assigning P3 for all cardholders in the door group - list just the door group

The PIN code -4 digits - you assign in the User screen must also be enrolled under the same user number at the alarm panel keypad. You may have to consult with the alarm panel manufacturer's literature for system enrollment.

All listed User # xx PINs are defaulted to -1. Any user with a -1 PIN is inactive until it is assigned a 4 digit PIN code.



Prior to enrolling users and PINs in the User screen, Keyscan suggests that first you review your group names and the individuals assigned to the groups and make note of the names so they all match. In the case where you are only going to assign a single user in a group for P3 arming and disarming of partitions, you could create a group with a description that includes the group and individual in the Group Setup screen so it matches the description created in the User screen similar to the suggested format above.

Group or Individual Intrusion User Activation

You must activate intrusion users in either the Group Setup screen or the Edit Person screen depending on P3 arming and disarming assignments. For information and procedures, select the link below Related Topics.

Procedures

Enter DSC Master Code

You must have previously enrolled an alarm panel before you can do the following procedures.

1. From the Client main screen, select the Site Management button > Hardware Setup.

- If you have multiple sites, click on the site from the Site Search directory screen.

2. From the Hardware Setup screen, double click on the alarm panel below the Access Control Units heading.
3. Select the Intrusion Users tab.
4. Scroll down the screen until you locate Master Code under the Name column in the list.
5. Under the PIN column, double click on the current default code.
6. In the User PIN text box enter the master code.
7. This must be the same master code programmed at an alarm panel keypad.
8. Under the Active column, if Yes is displayed opposite Master Code go to the next step, if No is currently displayed, double click on No and then click inside the box so it has an x. The box changes to Yes after you select Save.
9. Click on the Save button.
10. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Define Users and PIN Codes

You must have previously enrolled an alarm panel before you can do the following procedures.

1. From the Client main screen, select the Site Management button > Hardware Setup.
   - If you have multiple sites, click on the site from the Site Search directory screen.
2. From the Hardware Setup screen, double click on the alarm panel below the Access Control Units heading.
3. Select the Intrusion Users tab.
4. Double click on an undefined User # located under the Name column in the list.
5. In the Description text box, enter a description for the individual or group, if required.
6. For DSC units continue at step7; for DMP units continue at step 10.
7. In the PIN text box enter a PIN code.
8. Assign a number other than the master code. Do not leave the PIN code on the default value of -1 otherwise this User # remains inactive.
9. Under the Active column, to change the status from No to Yes, double click on No. No changes to a selectable box. Click inside the box so it is selected as indicated by the x. The status changes to Yes if you click elsewhere on the screen or when you select Save.
10. To add another user repeat the steps above, otherwise click on the Save button.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.
    - To deactivate a user at a later date, either change the PIN code to -1 or set the active status to No. Click on Save and then on Back.

Related Topics

Activate Groups or Credential Holders as Intrusion Users for P3

Name Intrusion Zones

To assist persons assigned to monitor the alarm panel via the Keyscan Client, you can use the Intrusion Zones screen to name individual zones. Naming individual zones makes for easier recognition of devices and their location in the event of an alarm. This is an optional screen. Keyscan recommends that you use the same zone names as they were entered at the alarm panel.

In the Intrusion Zone screen intrusion zones have been numbered Intrusion Zone 01 up to the maximum supported by the alarm panel. Ensure that you name and match the Intrusion Zone to its namesake in the alarm panel keypad.

Procedures

Steps to Name Zones

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, click on the site from the Site Search directory screen.
2. From the Hardware Setup screen, double click on the alarm panel below the Access Control Units heading.
3. Select the Intrusion Zones tab.
4. Under the Name column, click on the Intrusion Zone # you are naming.
5. Enter the name of the zone.
6. Repeat for each zone that you are naming.
7. When you have completed naming zones, click on the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Name Intrusion Partitions / Areas

You can use the Intrusion Partitions screen (DSC) to name the partitions or the Intrusion Areas screen (DMP) to name the areas as they have been named on the alarm panel to assist persons assigned to monitor the intrusion system via the Keyscan Client for easier recognition.

Procedures

Steps to Name Partitions or Areas

1. From the Client main screen, select the Site Management button > Hardware Setup.
    - If you have multiple sites, click on the site from the Site Search directory screen.
2. From the Hardware Setup screen, double click on the alarm panel below the Access Control Units heading.
3. Select one of the following tabs depending on the alarm panel:
    - DSC - the Intrusion Partitions tab
    - DMP - the Intrusion Areas tab
4. Under the Name column, click on the intrusion partition # or the intrusion area # you are naming.
5. Enter the name of the partition or the area.
    - For DMP, along the same row named above under the Active column, double click and then click inside the box to make the area active. The box changes to Yes when another row is selected.
6. Repeat for each partition or area that you are naming.
7. When you have completed naming partitions or areas, click on the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Activate Groups or Credential Holders as Intrusion Users for P3

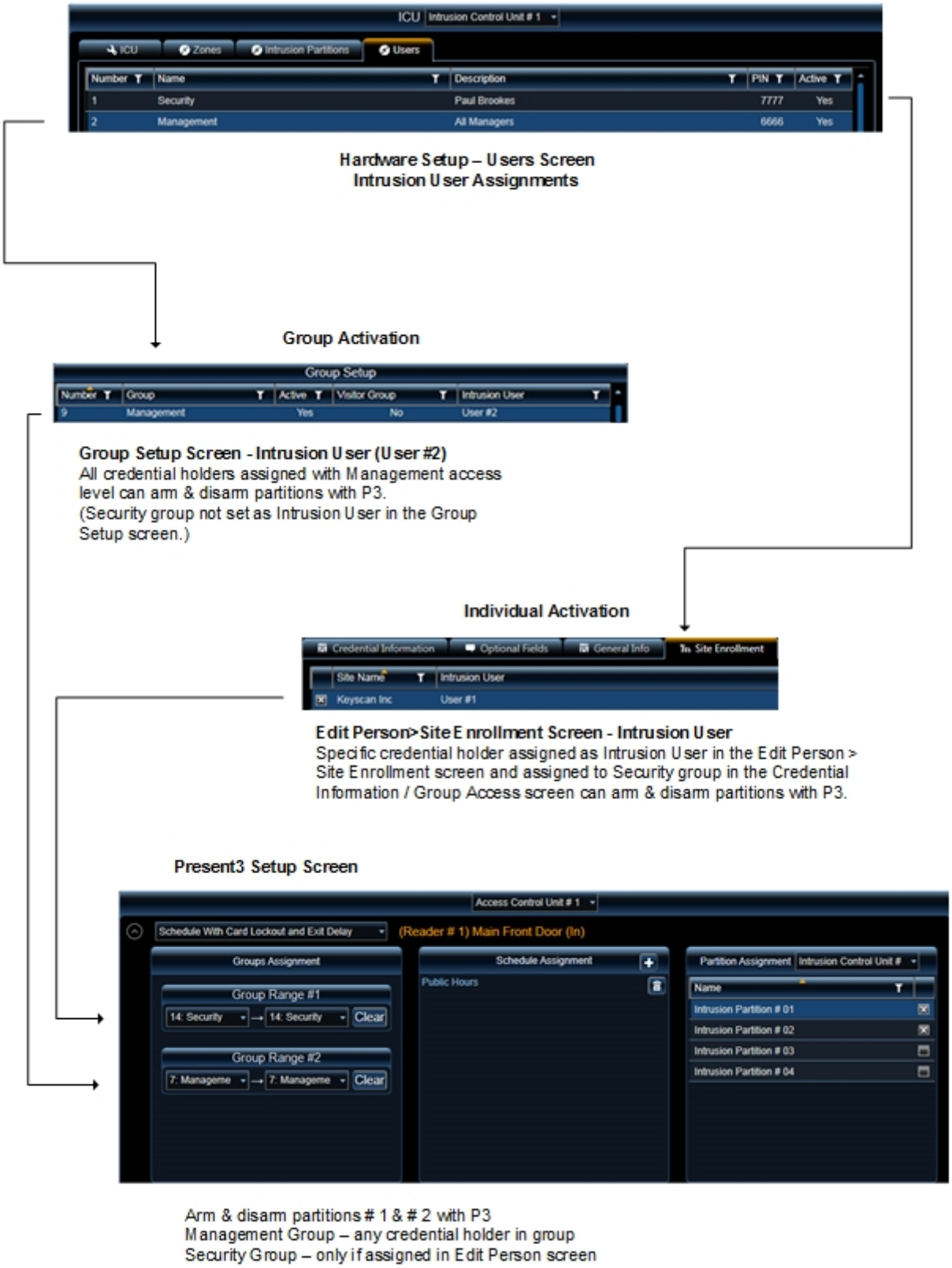
Present3 arming and disarming of alarm panels can be configured in one of the following two manners:

- Present3 Setup screen - for all credential holders in the group
- Edit Person screen - for specific credential holders within a group

A credential holder to have P3 privileges must have a user PIN code assigned in the Hardware Setup > User screen and access to partitions or areas as assigned in the Present3 Setup screen; otherwise P3 will not disarm the alarm panel.

Example

Group and Individual Intrusion Users



The procedures below assume you have previously setup groups and credential holders with group assignments.

Procedures

Steps to Assign a Door Group P3 Arming & Disarming

Performing these steps allows all cardholders in the door group to use P3 to arm and disarm the alarm panel. You must specify these door groups in the Present3 Setup screen. You may wish to make note of the User # that is assigned to the group(s).

1. From the Client main screen, select the Site Management menu > Group Setup.
    - If you have multiple sites, click on the site from the Site Search directory screen.
2. From the Group Setup screen, locate the group that you are activating for using P3 to arm and disarm the alarm panel.
3. Click under the Intrusion User column, opposite the group you are activating.
4. Click on the ▼ symbol and from the drop down list, select the intrusion user group. This is based on the User # assignment, not the name or description entered in the Hardware Setup screen.
5. Ensure the group's Active status is Yes. If not, click under the Active column on the No and then click inside the box to make it active. The box has an x.
6. Repeat the above steps to activate each additional group for alarm panel arming and disarming with P3.
7. Click on the Save button when you have completed the procedure.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Steps to Assign a Credential Holder P3 Arming & Disarming

These procedures assign specific individual cardholders within a door group to use P3 to arm and disarm the DSC alarm panel. You may wish to make note of the User #'s that are assigned to the individual cardholders. For any group that is restricted to individual credential holders, do not activate the intrusion user function in the Group Setup screen otherwise all persons in the group will have P3 arming and disarming privileges.

1. From the Client main screen, select the Manage People button > Manage People.
    - From the Person Search directory screen, locate the credential holder record.
2. From the Edit Person screen, select the Site Enrollment tab.
3. Opposite the applicable site, click on the row below the Intrusion User column.
4. Click on the ▼ symbol at the far right and select the intrusion user from the drop down list.
    - Remember that this individual must be assigned to a group that is also a valid P3 group in the Present3 Setup screen.
5. Click on the Save button.
6. To assign another individual as an intrusion user, repeat the above steps.
7. When you have completed assigning credential holders as intrusion users, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Synchronize Clocks

When an intrusion control unit is added and saved in the Hardware Setup screen, the Aurora software synchronizes the intrusion communication server time with the alarm system.

However, from time to time after the two systems have been operating over an extended period of time, they may experience time drift. You can manually re-synchronize the systems from the Access Control Unit Status screen.

Procedure

Manually Synchronize Clocks

1. From the main screen select the Status button > Status.
2. On the left of the Status screen, double click on Access Control Unit Status.
3. On the upper right side of the Access Control Unit Status screen, click on the ▼ symbol on the right side of the text box and select the site from the drop down list.
4. Under Access Control Unit, locate the intrusion control unit.
5. Scroll to the right until you see the Sync Clock heading.
6. Click on the sync clock icon on the row of the intrusion control unit.
7. To exit the Access Control Unit Status screen, click on the red x in the upper right corner.

Setup Present3 - Manual Arm/Disarm

As an option, you can use Present3, also referred to as P3, at a target reader for remote arming and disarming of partitions. Present3 arming and disarming can be by either a door group, a range of door groups or individual credential holders within specified door groups.

When specifying a Present3 schedule for arming and disarming the alarm panel be sure that you do not select schedules or readers that may be in conflict with other schedule or reader assignments.

If you elect to use the Present3 option for arming and disarming the alarm panel at a target reader, you must select one of the following Present3 modes:

- Schedule with Card Holder Lockout & Exit Delay
- Schedule with Card Holder Lockout, Exit & Enter Delay

The enter and exit delays only apply a delay in toggling the schedule change of state for Keyscan points. This mode does not apply a delay in arming and disarming the alarm panel partitions/zones. Also a schedule change of state does not toggle a partition.

Note +

Unless you have configured the optional burglar status relay outputs for discretionary arming and disarming as reviewed on the DSC Alarm Panel Setup included with the Aurora Intrusion license, if using Present3, always arm and disarm only with P3; otherwise false alarms or loss of system time synchronization may result if arming and disarming with the keypad or schedules are combined with P3.

The exit and enter delay is based on the Door Held Open Time / Exit Delay setting on the Door Output associated with the target reader in the Hardware Setup > Doors screen.

Avoid using the First Person In function with Present3.

After you have configured the Present3 Setup screen you must also set the group information screen or individual cardholders for Present3 arming and disarming of the alarm panel.

If you are unfamiliar with Keyscan's Present3, select the link under Related Topics below.

Before you begin the procedures to set P3, ensure that you have created specific P3 schedules or have existing schedules which are applicable for P3 arming and disarming. For more information about schedules, click on the link below Related Topics.

Procedure

Set Present3 for Arming and Disarming the Alarm Panel

1. From the Client main screen, select the Site Management button > Present3 Setup.
    - If you have multiple sites, click on the site from the Site Search directory screen.
2. From the Present3 Setup screen, if the access control unit is other than the one displayed along the top, click on the ▼ symbol and select the access control unit connected to the target reader for toggling the schedule for arming and disarming.
3. Opposite the target reader, select the ▼ symbol on the right side of the box with the P3 mode options to open the drop down list.
4. Select either:
    - Schedule with Cardholder Lockout & Exit Delay
    - Schedule with Cardholder Lockout, Exit & Enter Delay

5. Under Groups, click on the ▼ symbol on the left group of Group Range #1 and, from the drop down list, select the first group that can toggle the schedules using Present3.
6. Click on the ▼ symbol on the right group of Group Range # 1 and select either the same door group as chosen in the preceding step if only one group is to use the time zone toggle mode or select the group that is the last group in the range to use the schedule toggle mode.
7. If using the Group Range # 2 for a second set of arming and disarming groups at the target reader, repeat the preceding two steps.
8. On the right of the Schedules heading, click on the + button.
9. From the Schedules list, click on the < symbol opposite the desired schedule for toggling to arm and disarm the alarm partitions. If the Schedules list is still open after making your selections, click on a blank section of the Schedule Assignment box to close it.
10. Select either the Intrusion Partitions tab for a DSC unit or the Intrusion Areas tab for a DMP unit.
11. Under the Name column, click in the box to the right of each applicable partition or area for arming and disarming by the specified door groups. The box has an x.
12. To configure another reader for Present3 arming and disarming, repeat the above procedures, otherwise go to the next step.
13. Click on the Save button.
14. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Set Schedules

Present3

Activate Groups or Credential Holders as Intrusion Users for P3

Intrusion Status - Partitions/Zones

Select the links below for help on the Intrusion Status screens.

- Intrusion Zone Status
- Intrusion Partition Status
- Intrusion Area Status

Why It's Important to Manage the Aurora Database

Aurora includes a dedicated internal database - Microsoft SQL Server 2022 Express - that records and stores all the access control system information. Adding a credential record, presenting a credential at a reader, even logging on are all recorded and stored in the database. As a Keyscan access control system is used almost on a daily basis, the database is continually changing, and more importantly, expanding in size.

The information that is retained in the database is generated by different types of system activity that falls into two basic categories:

- Site Information
- System Events

The following two sub-headings explain each category's impact on the database.

Site Information

Site Information is data that is input by a system administrator and saved in the database. This includes data such as:

- Credential records & photos
- Photo badge templates & maps
- Schedules
- Group access levels
- Access control unit and door information
- Elevator control unit and associated floor information
- System administrator records & formatted reports

In essence, site information is any information or records about the site or sites that is input by a system administrator to operate the access control system. Site information is static until a system administrator either adds, edits, or deletes data. Generally after the access control system has been operating for a few months, site information represents a smaller percentage of the database file size in comparison to system events.

System Events

System events are credential holder, system administrator, or software application interactions with the access control system. System events include:

- Event transactions (such as when a credential holder accesses a door or an alarm is tripped)
- System Log (such as when an administrator edits a time zone or the software automatically initiates synchronizing an ACU clock)

Unlike site information, system events are more dynamic. Since the access control system is generally in use throughout the day with continual interaction, system events are constantly added to the database.

As an example, each time an individual credential holder accesses a door, that event is recorded in the database and adds to the database file size. So if one credential holder accesses 10 doors each day, in a single week that would produce 50 access granted transactions just for that one person. If there were 500 credential holders

producing 10 access granted transactions a day, 25,000 access granted transactions would be added to the database in one week. That's just one type of event. When you combine system administrator activity and software application interactions, you can see how quickly system events can expand the database file size.

Why You Need to Manage and Backup the Database

Because the database contains all site information and all historical system events, it is vital to manage, regularly backup, and make up-to-date duplicate copies of the database, since it is continually growing and changing. Also ensure that it is periodically purged of older data before it reaches the maximum gigabyte limit.

Schedule Regular Database Backups

Aurora has a built-in Scheduled Backup utility that can be programmed to backup the database at regularly scheduled intervals.

Remember, computers or hard drives can fail or breakdown. If this happens and you don't have a backup copy of your database, you could lose all your access control data. Making a backup copy and storing it either at an alternate network location or on another medium such as an external USB drive is strongly recommended. Be sure to select the link below and set a schedule for backing up the database and ensure that you make a duplicate copy regularly so you always have a second up-to-date copy.

Manage the Database

The Aurora database - Microsoft SQL Server 2022 Express - has a maximum file size of 10 gigabytes. While this holds a huge volume of data, over a long period of time without proper oversight and management, system events can grow pushing the database file size near the maximum threshold. The Aurora communication service will stop collecting transactions from the control units when the database reaches 9.5 gigabytes. Aurora prompts you with a warning when the database has reached 7.5 gigabytes.

Whenever you are prompted by the database warning, take action and perform database maintenance procedures otherwise you may experience problems. Make a backup copy of the database, and then use the Purge Transactions utility to reduce the size of the database by deleting older system events. Keyscan recommends that after purging transactions, the database is compressed and re-indexed.

Purging transactions only deletes system events. It does not delete the site information.

Database Relocation

If at a later date, the database is moved to another server with a different Computer Name or IP address, you must update all other servers/workstations with Aurora Clients or communication services. You require access to your Aurora Installation files, so it's best to have them on some portable device (like a USB drive).

Steps for Database Relocation

1. At an Aurora server or workstation, open the Aurora Media folder containing the Aurora software installation files.
2. Locate and run the file AuroraInstallation.exe.
3. If prompted with the Do you want the following program from an unknown publisher to make changes to this computer?, click on the Yes button.
4. From the Aurora Installation screen, enter the name or IP address of the server with the Aurora database in the text box below Database Server Location.
5. Click on the Update Aurora Server Location button.
6. From the prompt, Database Server Location has been set, click on the OK button.
7. Re-boot the server or workstation.
8. Repeat the above procedures on all Aurora servers and workstations.



Keyscan strongly advocates that you use Aurora's Scheduled Backup function and set a backup to occur at least once a week if not more frequently so your site data is protected.

Related Topics

For more information about database management, select the links below.

- Schedule an Automatic Database Backup
- Database Maintenance

Backup Now

The Backup Now function immediately creates a copy of the Keyscan access control system data. If you have newly installed and setup the Aurora software or made any significant additions or changes recently, Keyscan recommends that you use the Backup Now function to preserve the data in a backup file. If you have not previously done so, Keyscan recommends that you schedule Aurora to automatically backup the database. See Related Topics below.

Default Aurora Database Backup File

When you either use the Backup Now or the Scheduled Backup functions in the Database Maintenance screen, Aurora creates a database backup file with a KAD file extension. Backup copies of the database are in the following folder location on the server where the Aurora database was installed:

- C:\Program Files\Microsoft SQL Server\MSSQL14.AURORA\MSSQL\Backup\Aurora Database Full Backup yyyy-mm-dd-hhmm.kad

The database file size and the path are also displayed on the Database Maintenance screen along with the date of the last manual back up.

As part of your regular database maintenance routine this file should be copied regularly to another server location or portable medium such as an external USB drive so that you have a duplicate up-to-date copy in the event that the server with the Keyscan Aurora database experiences a failure or breakdown.

Procedure

Steps to Use the Backup Now Function

1. From the main screen, select the Settings menu > Database Maintenance.
2. From the Database Maintenance screen, ensure that the Database Maintenance tab is selected.
3. Click on the Backup Now box.
4. From the prompt: Database backup will be completed by [the] Keyscan Aurora Agent, either click on the Yes button to wait until the database backup is completed otherwise click on No.
5. From the Database Backup Completed prompt, click on the OK button.
    - You will note that the date and time are displayed opposite Last manual backup on the Database Maintenance screen.
6. After the backup is completed, providing you waited for the Aurora Agent, a Browse button opens on the Database Maintenance screen. Selecting the Browse button opens the folder where the Aurora Backup KAD file was saved. This only applies if the Client is on the same server with the Keyscan database.
7. To close Windows Explorer, click on the x in the upper right corner.
8. From the Database Maintenance screen, click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Schedule Automatic Database Backup

Schedule Automatic Database Backups

It is extremely important and highly recommended by Keyscan that you schedule Aurora to automatically backup your access control system database at regular intervals.

Database Backup

Backing up your database and making a copy at another server location or on a portable medium, such as an external USB drive, is like having an insurance policy. Your entire access control system information is protected in the event of a computer or hard drive failure. Without a backup copy of the database, you would have to manually re-enter your site data and all transaction history would be lost if ever you experience a computer malfunction.

The following outlines the various settings that you may set when scheduling Aurora to backup the database.

Important - You may only create one schedule for backing up the database

- E-mail Address(es) - As an option, you can specify an e-mail address to notify a recipient that the access control database was backed up on the scheduled date and if any errors occurred
- Scheduled Time - the defined time when Aurora commences the backup procedure which should be at an hour when site activity is at a minimum
- Select the days of the week - sets which days of the week the backup occurs – you may select multiple days
- Delete backup older than # of days - this function erases Aurora database backup files older than the # of days specified
- Auto purge transactions older than - deletes all transactions from the database that occurred prior to the specified # of days - if you do not want to engage this function leave it set on disabled
- Auto purge system logs older than - deletes all system logs from the database that occurred prior to the specified # of days - if you do not want to engage this function leave it set on disabled
- Auto purge visits older than - deletes all visits from the database that transpired prior to the specified # of days - if you do not want to purge visits, leave the setting on disabled

Make a Duplicate Copy of the KAD File

As part of your regular database maintenance routine this file should be copied regularly to another server location or portable medium such as an external USB thumb drive so that you have a duplicate up-to-date copy in the event that the server with the Keyscan Aurora database experiences a failure or breakdown.

Keyscan Agent

The Aurora software has a Keyscan Aurora Agent application that runs as a service. The Agent must be running when scheduled events occur. The Agent must also be running to distribute e-mail messages from the Aurora Client. During your original Aurora installation, the Keyscan Aurora Agent application was also installed and, by default, automatically started. You can confirm the Agent is running by selecting Start > Control Panel > Administrative Tools > Services. From the Services screen, scroll down and locate the Keyscan Aurora Agent.

- If the Status is listed as Started, then the Agent is running. Close the Control Panel screens.
- If the Status is listed as Stopped or is blank, select the Keyscan Aurora Agent and then click on the Restart the service in the upper left part of the Services screen. Close the Control Panel screens.

Procedure

Steps to Schedule a Database Backup

1. From the main screen, select the Settings menu > Database Maintenance.
2. From the Database Maintenance screen, select Scheduled Backup tab.
3. If you wish to distribute an e-mail that advises the database has been backed up, enter the recipient's address in the E-mail Addresses text box. You can enter multiple addresses; ensure that you separate each address with a semi colon (;).
4. To schedule a time other than the default schedule time shown, click on the date and time icon to the right of the Schedule time and select the desired time to run the database backup.
    - Keyscan recommends scheduling the database backup during a period of low site activity.
5. Below Select the days of the week:, click in the boxes to the left of the days when to backup the database. The box has an x when selected. You can select multiple days.
6. As an option, you can instruct Aurora to delete older backup files. In the Delete backup older than # of days text box, enter a value representing the number of days. Keyscan recommends not deleting database backup files that are less than 28 days old.
7. To enable the Auto purge transactions older than function, click on the symbol to the right and select one of the # of days from the list. By default this option is disabled.
8. To enable the Auto purge system logs older than function, click on the symbol to the right and select one of the # of days from the list. By default this option is disabled.
9. To enable the Auto purge visits older than function, click on the symbol to the right and select one of the # of days from the list. By default this option is disabled.
10. Click on the Save button.
11. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Database Maintenance

The Database Maintenance screen has the following database options for either performing specific database maintenance tasks or providing database information.

- Backup Now
- Restore Database
- Compress Database
- Re-index Database
- Database Size
- Scheduled Backup
- Purge - Transactions and system logs

As well as the preceding database maintenance functions, the Database Maintenance screen lists the current database file size, the database backup file size and the date of the last manual backup. The maximum file size for the Keyscan database is 10 gigabytes. The Keyscan software will automatically warn when the database file reaches 8 gigabytes.

Backup copies of the database are in the following folder location on the server where the Aurora database was installed:

- C:\Program Files\Microsoft SQL Server\MSSQL14.AURORA\MSSQL\Backup\Aurora Database Full Backup yyyy-mm-dd-hhmm.kad

Please observe sound database maintenance procedures to safeguard your site data. You should regularly backup the database as well as make a copy on another medium such as a writable CD or an alternate network server location.

As your database gets larger, especially if it nears 9 gigabytes, you should purge it of older entries. Ensure you have backed it up first. After purging your database of older entries, compress it, then re-index it. The Aurora communication service will stop collecting transactions from the control units when the database reaches 9.5 gigabytes. Aurora prompts you with a warning when the database has reached 8 gigabytes.

Select the links below for more information and procedures on the various database maintenance procedures.

Related Topics

Backup Now

Schedule Aurora for Automatic Database Backups

Purge - Transactions and System Logs

Compress & Re-index the Database

About the Keyscan Aurora Agent

Purge - Transactions and System Log

The Purge function in the Database Maintenance screen deletes transactions, such as access granted, alarm tripped etc., from the database.

Generally transactions should be purged when the database nears or crosses 9 gigabytes. The Aurora Client will prompt you with a warning that the database has reached 8 gigabytes. Be sure that you backup the database and save it to another medium or network location before you purge the database of older transactions.

If you purge transactions, we recommend that you also compress and re-index the database.

The Purge screen allows selecting which sites are purged of data and which transaction types are purged. At least 1 transaction type must be selected for purging.

Purge Filter

You may also use the search filter by clicking the icon to the right of Transactions. For more about using the search filter, select the Heading Search Filter link below Related Topics.

Export Daily (Transactions) Count

You can produce a daily transaction count, which the Aurora software saves as Aurora Transaction Daily Count yyyymmdd.csv. The daily count CSV file will go back as far as the first transaction recorded in the database.

Calculate Dates

Use the Calculate Dates function to list the first and last dates with recorded transactions. After selecting the Calculates Dates button, the dates are inserted in the From and To boxes below the Transactions list. If there are a large number of transactions the process may take several minutes.

Procedure

Steps to Purge Transactions and System Logs

Keyscan recommends that you first perform a database backup using the Backup Now function from the Database Maintenance screen if you have not already done so.

1. From the main screen, select the Settings menu > Database Maintenance.
2. From the Database Maintenance screen, ensure that the Purge tab is selected.
3. Below Sites, click in the box to the left of each site that will be purged of transactions. The box has an x when the site is selected.
4. Under Purge Options, do one of the following steps:
    - To select all transactions for purging, click in the box to the left of Include all transactions if it is currently not selected. The box has an x when selected.
    - To select only specific transactions for purging, ensure the Include all transactions box is deselected, then click in the box to the left of the individual transaction types - the boxes have an x when selected.
5. The purging of selected transactions can apply to all dates or a date range. Perform one of the following steps:
    - For all dates click in the radio button to the left of All Dates. The radio button has a blue dot when selected.
    - For a date range, click on the date & time icon to the right of the From box; use the arrows to scroll to the desired month/year and select the day from the calendar. Click on the date & time

icon to the right of the To box; use the arrows to scroll to the desired month/year and select the day from the calendar.

6. To remove system log entries, these are system user actions and software events, click in the box to the left of Remove system log entries.
    - The date selection above also applies to the system log entries.
7. As an option you can compress the database from the Purge screen. Click in the box to the left of Compress Database.
    - If you compress the database from the Purge screen, be sure to re-index it as well. If you do not select the Compress Database option in the purge screen, be sure to compress and re-index it from the Database Maintenance screen.
8. As an option you can also remove all deleted people and devices with no event history at selected sites by clicking in the box to the left.
9. Click on the Purge button.
10. From the Do you wish to continue with the purge option? prompt, click on the Yes button.
    - To abort the purge, click on the No button.
11. From the Purge Completed confirmation box, click on the OK button.
12. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Related Topics

Compress and Re-index the Database

Heading Search Filter

Compress & Re-Index the Database

Compressing the database reduces its size. If you have a site with a large volume of credential holders producing a heavy volume of daily transactions, compressing the database helps reduce the frequency of purging. After compressing the database, we recommend that you also re-index the database.

Procedure

Steps to Compress and Re-index the Database

1. From the Client main screen, select the Settings menu > Database Maintenance.
2. From the Database Maintenance screen, click on the Database Maintenance tab if it is not currently selected.
3. Select the Compress Database option.
4. From the Do you wish to compress your database? prompt, click on the Yes button.
5. From the Database compress completed prompt, click on the OK button.
6. Select the Re-index Database option.
7. From the Do you wish to re-index your database? prompt, click on the Yes button.
8. From the Re-index Database Completed prompt, click on the OK button.
9. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History down arrow to the right of the Back button.

Restore the Database

In the event that you had to replace the computer or hard drive where Aurora's SQL Server 2022 Express database was installed and you have had to re-install the database module, use the Restore Database option to retrieve your site data to get your system operating again.



You must have backed up your database and either copied it to another medium, such as an external USB drive, or copied to another computer or server location where it was safely stored and can be retrieved. If you did not backup your database, you cannot use the Restore Database option.

The Restore Database should only be used if you replaced the computer or hard drive where the Aurora SQL Server 2022 Express database module was installed. If you are not an experienced computer user, we strongly recommend that you call Keyscan technical support for assistance to restore your database.

You cannot perform the Restore Database function from an Aurora Client.

Default Aurora Database Backup File

When you either use the Backup Now or the Scheduled Backup functions in the Database Maintenance screen, Aurora creates a database backup file with a KAD file extension. By default, backup copies of the database are in the following folder location on the server where the Aurora database was installed:

- C:\Program Files\Microsoft SQL Server\MSSQL14.AURORA\MSSQL\Backup\Aurora Database Full Backup yyyy-mm-dd-hhmm.kad

This file must have been copied to another server location or to a portable medium such as a USB drive in order that you can restore the database. Please remember that you must have an Aurora Database Full Backup.kad file otherwise you cannot perform the restore backup procedures.

Procedures

Steps for Restoring the Database

Close Clients

1. Close all open Aurora Client applications.

Stop the Keyscan Aurora Agent

1. At the computer or server where the Keyscan database (Microsoft SQL Server 2022 Express) was installed, select Windows *start* > Control Panel.
2. From the Control Panel screen, double click on Administrative Tools.
3. From the Administrative Tools screen, double click on Services.
4. From the Services screen, scroll down until you locate Keyscan Aurora Agent.
5. Select the Keyscan Aurora Agent.
6. In the upper left area of the Services screen, click on Stop the service.
    - If you have a single computer installation where all the Aurora modules are installed on one computer, go to step 4 in the next set of procedures to stop the Aurora communication services.
7. You can minimize the preceding screens as you will have to re-start the service after completing the restore.

Stop the Keyscan Aurora Communication/Keyscan Aurora Intrusion Communication/ Keyscan Aurora Reverse Communication

All Aurora communication services must be stopped during the restore database procedure. In most cases you will only have to stop the Keyscan Aurora Communication which is the standard communication mode. The Keyscan Aurora Intrusion Communication and the Keyscan Aurora Reverse Communication are optional licensed modules and you will only see and have to stop either of those services if you have purchased the modules from Keyscan.

1. At the computer or server where the Keyscan Aurora Communication was installed, select Windows *start* > Control Panel.
2. From the Control Panel screen, double click on Administrative Tools.
3. From the Administrative Tools screen, double click on Services.
4. From the Services screen, scroll down until you locate any of the following services:
    - Keyscan Aurora Communication
    - Keyscan Aurora Intrusion Communication (only applies if you have a license)
    - Keyscan Aurora Reverse Communication (only applies if you have a license)
5. Select the applicable Keyscan Aurora Communication.
6. In the upper left area of the Services screen, click on Stop the service.
7. If you have more than one communication service running, repeat the above procedures for each service until they have all been stopped at each respective computer/server.
8. You can minimize the preceding screens as you will have to resume the service after completing the restore.

Copy the Backup KAD File to the Computer/Server with the Re-Installed Aurora Database

In this procedure you need to have access to your Backup KAD file either locally or on the network depending on where it is currently located so that you can make a copy and paste it into the Aurora Database (Microsoft SQL Server) Backup folder.

1. At the computer or server where the Keyscan database (Microsoft SQL Server 2022 Express) was installed, right click on Windows *start* and select Open Windows Explorer.
2. Navigate to the folder location with the Aurora Database Full Backup KAD file (default name) or the KAD file if you have named it differently from the default name.
3. Select the file and right click.
4. From the pop-up menu, select Copy.
5. Navigate to the Drive (default drive is C:\) Program Files > Microsoft SQL Server > MSSQL14.Aurora > MSSQL > Backup.
6. With the Backup folder selected, right click and select Paste.
7. Keep the Windows Explorer screen open and go to Steps to Restore the Database.

Steps to Restore the Database

1. You should still be at the computer or server where the Keyscan database (Microsoft SQL Server 2022 Express) was installed with the Windows Explorer screen open.
2. Navigate to Program Files (x86) > Keyscan > Keyscan Aurora Database.
3. Double click on the Keyscan Aurora Database Maintenance application.
4. In the User Name text box, enter keyscan.
5. In the Password text box, enter KEYSCAN in upper case characters.
6. Click on the  key symbol or press the Enter key.

7. Click on the Restore Backup icon on the top-left of the screen. The browser will automatically point to the database backup folder location.
8. Select the Aurora Database Full Backup yyyy-mm-dd-hh-mm-AM/PM.kad file or the KAD file if you have named it differently from the default name.
9. Click on the Open button.
10. A warning message will appear, if you wish to continue, select Yes, otherwise select No. The database restoration process will begin.
11. Close the Keyscan Aurora Database Maintenance screen by clicking on the x in the upper right.
12. Exit the Windows Explorer screen.

Database Computer/Server Name Change

If you have moved the database to another computer/server that has a different computer name, then you must update the Database Server Location field at each computer/server location with an Aurora Client, Keyscan Aurora Communication service, Keyscan Aurora Intrusion Communication service, or Keyscan Aurora Reverse Communication service if any of these modules/services are on a machine other than where the Keyscan Aurora database (Microsoft SQL Server 2022 Express) is installed. This will require you to have the Aurora Media folder containing the Aurora Software Installation files on some sort of portable medium that you can bring to each computer/server. If this procedure does not apply, go to the next set of procedures.

1. Open the Aurora Media folder containing the Aurora software installation files.
2. Locate and run the file AuroraInstallation.exe.
3. If prompted with the Do you want the following program from an unknown publisher to make changes to this computer?, click on the Yes button.
4. From the Aurora Installation screen, enter the name of the computer in the text box below Database Server Location.
5. Click on the Update Aurora Server Location button.
6. From the prompt, Database Server Location has been set, click on the OK button.
7. Repeat the above procedures for any other Aurora modules if they are installed on a computer/server other than the one which has Keyscan Aurora database.

Start the Keyscan Aurora Agent and Keyscan Aurora Communication

1. Restore the Services screen on the computer or server with the Keyscan Aurora database.
2. Ensure the Keyscan Aurora Agent is selected.
3. Near the upper left corner, click on Start the service.
4. If you have any of the Keyscan Aurora Communication services running from this computer or server, select the service and then click on Start the service for each one.
5. If applicable, return to the computers or servers where the Keyscan Aurora Communication services are installed and start each one.

After resuming the Keyscan Aurora Agent and Communication services, you can login to any of the Clients to resume any administrative or monitoring activities.

Related Topics

Backup Now

Configure Database Connection Settings

This feature allows a computer running the Aurora software client to remotely access the database through configuring the Server and Database Connection Settings. These settings are stored on the client computer in a Server Settings XML file.

Sever Settings XML File

The Server Settings file is an XML file that is stored on the computer currently in use to remotely access the database located on another computer. This is a simple data file that can be opened with many word processors, including Notepad. In order to access the database remotely, the file will need certain Server and Database Connection Settings present within. Any changes to database and/or server settings should be directed by dormakaba Canada Inc. Technical Support. Below, you will find an example of what's contained within the Server Settings XML file, along with a table explaining what each setting identifies.

Server Settings File Example

```
<?xml version="1.0" encoding="utf-8"?>
<SQLServer>
  <ServerName>localhost</ServerName>
  <ServerInstance>AURORA</ServerInstance>
  <DatabaseConnectionTimeout>60</DatabaseConnectionTimeout>
  <DatabaseCommandTimeout>90</DatabaseCommandTimeout>
  <EPlexServer>127.0.0.1</EPlexServer>
</SQLServer>
```

Name In File	What It Identifies
ServerName	Identifies where the server is located: the machine name or the IP address.
ServerInstance	The database instance connected to on the SQL server. This setting should never be changed.
DatabaseConnectionTimeout	The amount of time, in seconds, it takes for the computer in use to access the database.**
DatabaseCommandTimeout	The amount of time, in seconds, it takes for the client computer/ database to send a message back.**
EPlexServer	Identifies where the E-Plex service is located: the machine name or the IP address.

****Note:** These settings should only be changed as directed by dormakaba Canada Inc. Technical Support.

Schedule Aurora for Automatic Tasks

Aurora has a Scheduled Tasks Setup screen so that you may schedule Aurora to run Transaction Reports. Scheduled Transaction Reports are distributed by an e-mail as a PDF attachment. You must have SMTP settings configured in the Application Utilities screen.

Transaction Report

Transaction reports can also be scheduled as an automated task in Aurora. You may schedule any number of transaction reports in the Scheduled Task setup screen. However, you may only schedule transaction reports that have been named and saved in the Transaction Report screen.

- Name - use this field to create a name for the schedule that automatically runs the selected transaction report or leave it on the default Scheduled Task # x.
- Report - selects the named transaction report to be scheduled
- E-mail Address(es) - specify the e-mail address of the person receiving the report - transaction reports are attached as PDF files
- Schedule time - the defined time when Aurora runs the transaction report
- Select the day(s) of the week - sets which days of the week when Aurora runs the transaction report - you may select multiple days

Active/Inactive

Scheduled tasks may be set to Inactive status whenever you need to suspend scheduling transaction reports. To de-activate a scheduled task, click on the Active button. The status changes to Inactive. To resume the schedule, click on the Inactive button to reset the status back to Active.

Keyscan Agent

The Aurora software has a Keyscan Aurora Agent application that runs as a service. The Agent must be running when scheduled events occur. The Agent must also be running to distribute e-mail messages from the Aurora Client. During your original Aurora installation, the Keyscan Aurora Agent application was also installed and, by default, automatically started. You can confirm the Agent is running by selecting Start > Control Panel > Administrative Tools > Services. From the Services screen, scroll down and locate the Keyscan Aurora Agent.

- If the Status is listed as Started, then the Agent is running. Close the Control Panel screens.
- If the Status is listed as Stopped or is blank, select the Keyscan Aurora Agent and then click on the Restart the service in the upper left part of the Services screen. Close the Control Panel screens.

Procedures

Steps to Schedule a Transaction Report

You must have previously created and saved a named transaction report before you can automatically schedule running a transaction report.

1. From the main screen, select the Settings menu > Scheduled Task.
2. With the All tab selected, click on the Add Scheduled Task button.
    - As an option you can create a specific name for the schedule running the transaction report in the Name text box or leave the default Scheduled Task #.
3. Opposite Report, click the ▼ symbol on the far right and select the named report from the drop down list.

4. Enter the recipient’s address in the E-mail Addresses text box. You can enter multiple addresses; ensure that you separate each address with a semi colon (;).
5. To schedule a time other than the default schedule time shown, click on the date and time icon to the right of Schedule Time and select the desired time to run the transaction report.
6. Below Select the days of the week:, click in the boxes to the left of the days when to run the report. The box has an x when selected. You can select multiple days.
7. Click on the Save button.
8. Click on the Back button until you are at the main screen or for a previously viewed screen select the Navigation History  down arrow to the right of the Back button.

Related Topics

Transaction Reports

Keyscan Aurora Agent

The Keyscan Aurora Agent is a Windows service that monitors and/or executes certain Aurora functions. Configured to start automatically and run as a service, the Agent, by default, is installed at the server location where the Keyscan Aurora database is installed. The Agent oversees the following Aurora functions:

- Event Setup - Actions
    - Sends e-mail notifications*
    - Executes command actions
- Event Setup - Escalations
    - Sends e-mail notifications* and/or triggers auxiliary outputs
- Alarm Watch
    - Sends e-mail with attachment - People In/Out Report in PDF format*
- Scheduled Database Backup
    - Executes scheduled database backup
    - Sends e-mail advisory - database backed up successfully or a problem occurred*
- Scheduled Tasks
    - Executes Scheduled Transaction Report and People Information Report
    - Sends e-mail with attachment - Transaction Report in PDF or csv format and People Information Report in csv format*

*E-mail address must be specified.

System Log

If any of the following occurs, the event is recorded in the system log to advise a system user:

- When a scheduled task is completed
- When an error occurs during the running of a scheduled task
- When an e-mail fails to be sent
- When the Agent starts or stops (also recorded in Windows Event Log)

Logged In Users

The Keyscan Aurora Agent performs a check every 10 minutes from starting to restore the actual number of logged in users in the event of a workstation/server crash or a power failure.

By default, the Aurora Keyscan Agent is installed on the server with the Keyscan database.

Disaster Recovery

The Disaster Recovery function retrieves partial site data directly from the door and elevator control units in the event that you have lost your Keyscan database and do not have a backup copy. The Disaster Recovery acts as a last resort to get your access control system re-functioning quickly; however, it does not recover all your site data.

Data Fields Recovered from ACUs

The list below indicates the data that is recovered. Individuals assigned with multiple credentials will have a separate record created for each credential.

- Given name - the first character only
- Surname - the first character only
- Batch number, if applicable
- Card number
- Door group access
- Elevator group access
- Temporary card options, if specified
- Active/Inactive - person and credential
- Door and elevator settings
- Schedules and assignments (no schedule names - recovered as Schedule #1 etc.)

General Procedures

Only undertake these procedures if you have lost your previous database. The Aurora Communication Service must be running to perform the Disaster Recovery procedures. Before you start, review the procedures so you have an understanding of the process and what must be setup. For assistance on some of the procedures, see Related Topics below.

1. Re-create the site. Select the Site Management button > Site Information Setup.
2. Add the access control units including all necessary Communication fields. Select Site Management > Hardware Setup. You will require the serial number and password for each access control unit that you are re-enrolling in the Aurora software. For each access control unit re-enrolled set the Status field to Disaster Recovery.
3. When you have completed re-enrolling the access control units, select the Save button in the Hardware Setup screen.
4. Select the Back button until you are at the main screen.
5. From the main screen, select the Status button > Status.
6. From the left side of the Status screen, double click on Access Control Unit Status. Select the site from the top-right drop-down menu.

7. Right-click anywhere on a selected row and select Change Status -- Disaster Recovery. Each access control unit that was re-enrolled and set on Disaster Recovery in the Hardware Setup screen is now highlighted in orange. Right-click the same row again and choose one of the following options:

- ◦ Recover Data -- this option will trigger a data recovery process outlined in Step 8
  ◦ Reset Transaction Flag -- old transactions will be collected the next time the access control unit's status is set back to active

1. During the recovery process you are prompted with the following dialog boxes:
   ◦ Recover information from this access control unit - select Yes to continue and retrieve information from the access control unit.
   ◦ Make a database backup before starting the recovery process - select Yes to make a database copy (The Keyscan Aurora Agent must be running)
   ◦ Recover credentials from this access control unit - select Yes on the first control unit recovered - select No on subsequent control units recovered otherwise you will add duplicate credential records.
   ◦ Recover schedules from this access control unit - selecting Yes recovers schedules from that access control unit - all schedules for the control unit's assigned site are overwritten with the recovered schedules
2. Wait until the ACU's Pending Packages reaches 0 (zero) before you start recovering data from the next ACU.
3. Repeat steps 7 to 9 to recover data for each applicable access control unit.
4. When you have completed recovering data from the access control units, exit and re-start the Aurora Client.
5. Set all the access control units to Active status in the Hardware Setup screen.
6. Review and complete your site information in all relevant Aurora screens.
7. Perform a full database backup and be sure to set Aurora for regularly scheduled database backups.

Related Topics

Name & Define a Site

Door Control Units

Configure an Elevator Control Unit

Keyscan Aurora Agent

Backup Now

Schedule Automatic Database Backups

Aurora Output Module

The Aurora Output Module is designed to output Aurora transaction data in either a comma delimited file format (CSV) or network message that can be used by other 3rd party applications. The Communication Service must be running in order for transactions to be recorded to the output file.

UDP Output

Aurora can be configured for universal datagram protocol (UDP) output. The UDP output identifies and collects the same data as the Output Transaction Fields listed below. The UDP output can be directed to either a single or multiple servers. The following two examples illustrate a single IP address and the use of a subnet mask - 255 - directing the output to multiple IP addresses:

- example of single IP address 197.168.100.1
- example of multiple IP addresses 197.168.100.255 - all servers with 197.168.100 in their IP address receive the UDP output

You may wish to consult with a network administrator.

Output Transaction Fields

The Aurora Output Module identifies and collects data for the following transaction fields:

- Transaction Type
- Device Number
- Device Name
- Access Control Unit (panel) Name
- Site Name
- Time Stamp
- Credential Number
- Given Name
- Surname
- E-mail
- Device ID
- Access Control Unit (panel) ID
- Site ID
- Site Custom ID
- Credential ID
- Person ID
- Person Custom ID

Values are separated by a comma. If the field does not have a data entry, a comma is inserted. The above listed fields are captured in columns from left to right starting with Transaction Type Code at the left and E-mail at the far right.

Note +

In the procedures for setting up the Output Module, you will be instructed to create a CSV file in a spreadsheet application such as MS Excel. You can create a blank file or create a file with the above headings along the top row in the first ten columns so all the columns are identified for easier reference when reviewing the file.

Procedures

Steps to Configure the Output Module fields



The Aurora Output Module can be user-configured to add, remove, and re-order the output fields. This will effect what information will appear in the CSV file as well as the order this information will appear. To configure the Output Module fields, do the following:

1. From the Aurora Client main screen, select the Settings button > Application Utilities.
2. From the Application Utilities screen, ensure the Advanced tab is selected.
3. In the Output Module section, use the check-boxes next to the output fields to select which fields will appear in the output.
4. A list of the selected output fields is visible at the bottom of the Output Module section. It shows which fields are selected as well as the order they will appear in the output. If you want to reorder the output fields, simply use your mouse to click and drag the field name up or down in the Output Module list.
5. Click the Save button to save your settings.
6. Proceed to "Steps to Setup the Output Module" (below)

Note: These settings are only taken upon startup and therefore the communication service will need to be restarted to reflect any changes. See "Steps to Setup the Output Module" (below) for more information.

Steps to Setup the Output Module

1. Open your spreadsheet application and create a folder location and a file name for the output data. Keyscan suggests naming the folder Aurora Output Module and the file as AuroraData. The file must be saved as a CSV file (CSV comma delimited).
    - example - AuroraData.csv
    - As an option you can enter the field headings along the top row of the CSV file.
2. After you have created a folder and named a CSV file, log on to the Aurora Client with your user name and password.
3. Select the button with the key icon.
4. From the Aurora Client main screen, select the Settings button > Application Utilities.
5. From the Application Utilities screen, ensure the Server Settings tab is selected.

6. Click on the ▼ symbol on the right of Communication Server and select the server running the Aurora Communication Service which is collecting data from the desired access control units.
7. On the far right of Output File Path, click on the + symbol.
8. Navigate to the location where you created the Aurora output folder and Aurora data CSV file.
9. Select the file and then click on the Open button. The path and file name are listed in the Output File Path text box.
10. Click on the Save button.
11. Click on the Back button until returned to the main screen.
12. You can leave the Aurora Client open or exit the application.
13. At the server where the Communication Service is running, select Control Panel > Administrative Tools. Double click on Services.
14. From the Services screen, scroll down and select either Keyscan Aurora Communication or Keyscan Aurora Reverse Communication, depending on which service you are running.
15. In the upper left part of the Services screen, click on Stop the service. Wait while the service is stopped.
16. Click on Start the service. Wait while the service is resumed.
17. Close the Control Panel screens.

Steps to Setup a UDP Output

1. Log on to the Aurora Client with your user name and password. Select the button with the key icon.
2. From the Aurora Client main screen, select the Settings button > Application Utilities.
3. From the Application Utilities screen, ensure the Server Settings tab is selected.
4. Click on the ▼ symbol on the right of Communication Server and select the server running the Aurora Communication Service which is collecting data from the desired access control units. If the communication server is listed, go to the next step.
5. In the UDP Remote Host text box, enter the IP address of the server receiving the UDP output.
6. In the UDP Remote Port text box, enter the port number for the server.
7. In the UDP Local Host text box, enter the IP address of the server with the applicable Keyscan Aurora communication service.
8. In the UDP Local Port text box, enter the port number for the server.
9. Click on the Save button.
10. Click on the Back button until returned to the main screen.
11. You can leave the Aurora Client open or exit the application.
12. At the server where the Communication Service is running, select Control Panel > Administrative Tools. Double click on Services.
13. From the Services screen, scroll down and select either Keyscan Aurora Communication or Keyscan Aurora Reverse Communication, depending on which service you are running.
14. In the upper left part of the Services screen, click on Stop the service. Wait while the service is stopped.
15. Click on Start the service. Wait while the service is resumed.
16. Close the Control Panel screens.

Active Directory

An Aurora Active Directory license provides the following two integration functions with MS Active Directory:

- Aurora's person records are automatically updated from MS Active Directory
- Aurora uses Windows domain or local password login authentication

You must have a Windows server OS that supports Active Directory. Only a qualified network administrator should configure Active Directory and oversee its ongoing operation.

Before you start, it is recommended that you read the full content of this topic so you understand what's required in setting up Aurora and MS Active Directory. If you are unfamiliar with access control and the Aurora software, please spend time reviewing Aurora's interface screens and the Help before you commence configuring Active Directory.

Example of Active Directory

Essentially, Aurora's Active Directory is used to import data from MS Active Directory attributes to corresponding Aurora fields. The table below illustrates one example of some commonly used fields in Aurora which are listed on the right. The corresponding MS Active Directory attributes are on the left. Once MS Active Directory and Aurora are configured, Aurora polls the directory every five minutes. Any additions or changes made to the listed attributes by the network administrator in MS Active Directory are written to Aurora's database. Also, when a new user is created in the MS Active Directory, a corresponding new person record is created in Aurora with the relevant data. When an Aurora system user opens or refreshes the Client's Manage People or Edit Person screens, those screens reflect the changes made in MS Active Directory.

Add or Edit MS Active Directory Fields	Updates Aurora - Edit Person Fields
First Name	Given Name*
Last Name	Surname*
E-mail	E-mail
telephoneNumber	Telephone Number
mobile	Cell
Arbitrary Field (for credential number input)	Credential Number
Group Membership	Group Access
	* required field in Aurora

The above table is only an example. Which fields you designate in MS Active Directory for capture and transfer to Aurora will depend on your particular setup. As there are numerous setup possibilities, the help can only provide some basic guidelines and general procedures when configuring Active Directory.

Remember that Active Directory gives the network administrator control over the assigned fields from MS Active Directory. If an Aurora system user makes a change to any of those assigned fields, the changes will be overwritten by whatever data resides in the MS Active Directory when Aurora next polls the directory.

Network Domain

Active Directory requires all Aurora Clients and the Keyscan Aurora Agent on the same network domain. The Keyscan Aurora Agent should always be running as it polls the directory every five minutes for updates. By default, the Keyscan Aurora Agent is installed at the server/workstation where the Aurora database is installed. The Aurora Clients do not have to be running for updates to occur. To verify the Keyscan Aurora Agent is running, select Start > Control Panel > Administrative Tools > Services > Keyscan Aurora Agent > Status: Started. If the agent is stopped, restart the service.

Configure MS Active Directory

Sync Group

The default Sync Group is "Keyscan," but it can be customized with an existing or a new Group name in the Application Utilities menu, under the Active Directory Agent Setup sub menu. Ensure the group names match between MS Active Directory and the Aurora software client in order to ensure proper sync.

Credential Number

If you are entering credential numbers from MS Active Directory, determine which attribute will be used for entering the credential number. This attribute has to be specified in the Aurora software. Also, ensure the values entered in MS Active Directory match the Credential Type set in the Aurora software client in order to ensure proper sync.

Access Levels

If you are going to use network group names as your group names in Aurora for assigning group access levels, record the names. When configuring Aurora, the network group names must be entered exactly the same in the Aurora Groups screen.

If you are not recording credentials in MS Active Directory, network group names do not apply.

"Sync access groups to all credentials"

- Check this option to apply the network group names as group access levels for all credentials the user has.

User Attributes

From the Properties dialog box, record all attributes that Aurora will capture and use to populate the person records. Create the exact same descriptions in Aurora's Optional Fields Management screen under the Common Optional Fields heading. Common Optional Field names created in Aurora must be the same as the LDAP display names in MS Active Directory. Do not use the Site Optional Fields for this purpose.

You must have names in the First Name and Last Name attributes in the Properties dialog box; otherwise Aurora will not create a person record.

Special Keyscan Names

Below is a list of special Keyscan names, on the left of the = sign, that can be used to reference MS Active Directory attributes outside of the conventional rules:

- Work number, Phone number = telephoneNumber
- Address = streetAddress
- City, Town = l
- Zip Code, Zip = postalCode
- Country = c
- Cell = mobile

When creating an optional field name in Aurora, it must match the LDAP display name. Spaces are ignored. Example - Post Office Box in Aurora would be a match for postOfficeBox in MS Active Directory even though the attribute in the Properties screen is displayed as P.O.Box.

Member Of

Ensure that you assign all relevant users to the Keyscan group (or the Sync Group set up in Application Utilities) in the Properties > Member Of dialog box.

If you have an existing system and Aurora has been previously installed with populated person records, do not assign those users to the Keyscan group (or the Sync Group set up in Application Utilities) until you have completed the procedure outlined under Existing Systems below. If necessary, turn the agent off by selecting: Start > Control Panel > Administrative Tools > Services > Keyscan Aurora Agent > Status: Stopped.

Use Global Catalog

Use the global catalog when you want to sync with an Active Directory forest containing multiple domains. This option will allow you to specify a sync group and find all users that are a member of that group, whether directly or indirectly, across domains in the forest.

NOTE: When using the "Use Global Catalog" option, not all attributes are included in the global catalog by default. If you are also using the "Site Property" option or syncing attribute values to optional fields, you will need to ensure that those attributes are included in the global catalog. Documentation on how to achieve this using the Active Directory Schema MMC snap-in or Ldifde utility can be found online.

New Installation / Existing System

Please review one of the headings below depending on whether this is a new installation or an existing system with populated person records.

New Installation

If this is a new installation with no person records, once you have completed the procedures outlined above, when the Keyscan Aurora Agents polls the directory, Aurora will automatically capture the data and create the person records.

Existing System

If this is an existing system that has existing person records, you must open each existing person's record and manually alter the following two fields in the Edit Person screen:

- enable the Active Directory Linked function by clicking in the box to the left - the box has an x when enabled
- select the ▼ symbol to the right of Active Directory User and specify the user as identified in the network domain
    - the Active Directory User field uses a search operator to locate the name on the domain - enter part or all of the person's name and click on the search key at the right
- save the record
- when you have completed setting the above two functions for all relevant person records, return to MS Active Directory and then assign all relevant users to the Keyscan group in the Properties > Member Of dialog box.

Any person records that existed prior to the initialization of Active Directory will not be updated unless you manually change the above two settings.

Aurora Installation - Preliminary

These instructions assume that you have previously installed Aurora. If not, install Aurora, first.

Register Active Directory

Register your Active Directory license, along with any other applicable Keyscan Aurora licenses. The Active Directory settings in Aurora are hidden from view and inaccessible until you receive an unlock number which is provided by a Keyscan representative during the registration procedure. Select the Software Registration link below for instructions on registering Keyscan software.

Configure Aurora

As Active Directory's primary benefit is to populate person records in Aurora from MS Active Directory, configure the following Aurora screens as outlined, except do not create individual person records.

Aurora Basic Setup Screens	
Site Information Setup	- general site information
Hardware Setup	- add access control units and define doors and readers
Schedule Management	- create schedules for assigning access and assigning devices for on/off periods
Groups*	- creates group names - person who are issued credentials for access must be assigned to 1 group
Group Access Levels	- group access levels assign groups with scheduled times for access at assigned doors
Optional Fields Management**	- user-defined fields for supplemental information for person records
Backup Database & Schedule Backups	- ensure that the database is backed up and scheduled to perform auto backups at regular intervals
* Name the Aurora groups so they match the network groups if you intend to record credential numbers from MS Windows Active Directory **Create matching optional field names in Aurora that match attributes in the MS Active Directory - Properties dialog box (Ensure that matching fields are defined under the Common Optional Fields heading. Do not define fields under the Site Optional Fields heading.)	

For more information about the above setup screens, select the Basic Site Setup Procedures under Related Topics. Your dealer/installer may have previously installed and setup the Aurora software, in which case you may have to alter group descriptions and optional fields to correspond with network descriptions. This will depend on your particular naming conventions.

Active Directory - Site Attribution

There are 2 options when assigning People from MS Active Directory into specified Sites in the Aurora software client. Choose the option below that best suits your application.

Option 1: Active Directory Agent

This option is best suited for applications in which all members of the Keyscan or Sync Group can all be added to the same sites. Follow these steps to enable Active Directory Agent for site(s):

1. From the Aurora main screen, click on the Site Management button and select Site Information Setup.
2. From the Site Search directory screen, double click on the applicable site where you are configuring Active Directory.
3. From the Site Information Setup screen, locate and enable the Active Directory Agent field by clicking in the box to the right. The box has an x when enabled.
4. Select the Save button on the bottom-right corner of the screen.

5. If you have multiple sites, click on the Back button and repeat enabling the Active Directory Agent for each applicable site.

Option 2: Custom Site Unique Identifier

This option is best suited for applications in which members of the Keyscan or Sync Group need to be added to different sites. Follow these steps to enable a Custom Site Identifier for each site:

1. From the Aurora main screen, click on the Application Management button and select Application Utilities.
2. Select the Advanced tab and check the box beside Custom Site Unique Identifier.
3. Under the Active Directory Agent Setup sub menu, fill in the Site Property field according to the MS Active Directory attribute. When creating a Site Property name in Aurora, it must match the LDAP display name. Spaces are ignored. Example - Post Office Box in Aurora would be a match for postOfficeBox in MS Active Directory even though the attribute in the Properties screen is displayed as P.O.Box.
4. Select the Save button on the bottom-right corner of the screen.
5. From the Aurora main screen, click on the Site Information button and select Site Information Setup.
6. A Custom Site ID field will now appear above the site Name. Enter the Custom Site Unique Identifier from Step 3 to the site.
7. Select the Save button on the bottom-right corner of the screen.

Active Directory - Credential Attribution

If you are going to use MS Active Directory to assign and record credentials, complete the Active Directory Agent Setup fields as outlined; otherwise, if you are not issuing credentials via the MS Active Directory, by-pass this procedure.

Before you begin, you must know the credential type being used. Also, you must know the assigned attribute in the MS Active Directory - Properties dialog box containing the credential number. Follow these steps to properly use the Active Directory Agent Setup for credentials:

1. From the Aurora main screen, click on the Application Management button and select Application Utilities.
2. Select the Advanced tab.
3. In the Active Directory Agent Setup sub menu, choose the Credential Type from the drop down menu (depending on your application).
4. In the Credential Property field, enter the name of the attribute in MS Active Directory that contains the credential number.
5. Choose what the system will do On Credential Change from the drop down menu:

- Add New - Adds a new credential if found in MS Active Directory; the pre-existing credential is still active, but no longer linked
- Deactivate All Others - Adds a new credential and deactivates all other credentials attributed to the Person
- Delete All Others - Adds a new credential and deletes all other credentials attributed to the Person

6. Select the Save button on the bottom-right corner of the screen.



A domain user set on inactive in MS Active Directory sets the person record as inactive in Aurora.

A domain user deleted in MS Active Directory deletes the person record in Aurora.

Related Topics

Software Registration

Basic Site Setup Procedures

Domain or Local Login


Name & Define a Site

KEYSCAN AURORA MILESTONE VIEWER

The Keyscan Aurora Milestone Viewer provides camera monitoring and control for your Milestone network video recorder (NVR). The available functions in the viewer depend on camera capabilities and how you have programmed and configured the Milestone NVR.

Note: The maximum number of cameras that can be supported through the Aurora software on a DVR/NVR is 1024.

Camera Monitoring Window

Each camera monitoring window, with Show Overlay enabled, identifies the camera, the date, and the time during live video monitoring. The properties and configuration of camera monitoring windows can be altered using the View Control and the Settings menu.

View Control

View Control allows on-screen monitoring in the following camera configurations:

- 1 camera in a 1 x 1 monitoring configuration
- 4 cameras in a 2 x 2 monitoring configuration
- 9 cameras in a 3 x 3 monitoring configuration
- 16 cameras in a 4 x 4 monitoring configuration

Changing Cameras - Single Monitoring Window

By default, the monitoring window opens in the single camera configuration with Camera 1 on display.

To change cameras in live view, right click on the camera currently in the monitoring window and select Remove Camera, and then double click on another camera in the list tree.

Adding Cameras - Multiple Monitoring Configurations

When using multiple camera monitoring configurations in live view, to add cameras in the monitoring window, double click on a camera in the list tree. Continue double-clicking on cameras in the list tree until the monitoring configuration is populated with cameras. To remove a camera, right click on the camera in the monitoring window and select Remove Camera.

Selecting a Camera

To select a camera in the monitoring window, click the pointing device when the cursor is positioned over the desired camera. When a camera is selected in the monitoring window, the title bar is a lighter shade of blue.

Playback Control

The NVR must have been configured to record in order to use the playback control. The date and time of the video playback is restricted to the NVR's record settings and video storage capacity.

Icon	Function
	play the video
	fast forward the video (successive clicking on the fast forward button increases the speed)

	stop the video playback
	reverse the video
	fast rewind the video playback (successive clicking on the rewind button increases the rewind speed)

Playback Control - Date Selection

The date and time are presented in the following format: Year (yyyy) / Month (mm) / Day (dd) / Hour (hh) : Minute (mm) : Second (ss).

For accessing Playback Control, the Browse radio button must be enabled in the View Control window.

To specify a playback date & time in the Playback Control panel, click on the down arrow to the right of the date/time currently displayed and select a date from the calendar. Use the back and forward arrows to scroll to different months. When the correct month is displayed, click on the day in the calendar. To specify a time, select the hour and enter the desired hour. Repeat to set the minutes and the seconds. Select the Display Event button to activate the playback controls. Click on the Play button. You may have to wait a few moments while the NVR retrieves the video.

PTZ Camera Control

Cameras that have pan, tilt, and zoom capabilities can be manipulated with the PTZ Camera Controls. You may find that some of the functions outlined below are not compatible with your cameras if they do not support pan, tilt, zoom or presets.

Icon	Function
	Pan Left Button - directs the camera lens to rotate to the left
	Pan Right Button - directs the camera lens to rotate to the right
	Tilt Up Button - directs the camera lens to swivel upwards
	Tilt Down Button - directs the camera lens to swivel downwards
	Stop Button - stops the camera after a pan, tilt, or zoom command
	Zoom In Icon - directs the camera lens to adjust the focal length enlarging the image with a narrower field of view
	Zoom Out Icon - directs the camera lens to adjust the focal length reducing the image with a wider field of view

Operating Pan & Tilt Commands

Click on one of the 4 arrows to move the camera in the desired direction. Click on the Stop button to halt the camera action.

Operating Zoom In & Zoom Out

Click on the Zoom In icon or Zoom Out icon to adjust the camera's focal length.

Camera Presets

From the preset list, click on the down arrow and select the desired preset from the list. The camera is adjusted to the preset position.

CCTV Server List Tree

On the right side of the Viewer is the list tree. To the left of each NVR is a + (expand) or - (collapse) symbol.

(+) Expand

Click on the + symbol to expand the list.

(-) Collapse

Click on the - symbol to collapse the list.

Settings Menu

Hide Controls

When checked, the viewer closes the controls so only the cameras are visible.

Always On Top

When checked, the Viewer is positioned in front of the Aurora screen.

Show Overlay

When checked, the viewer displays the camera information in the monitoring window.

Keep Aspect Ratio

When checked, the viewer retains the camera’s aspect ratio.

Enable Digital Zoom

When checked, enables digital zoom on connected cameras with this feature.

Related Topic

Add an NVR and Specify Settings

Liability Warning - 26-Bit Wiegand Card Format

Keyscan systems are factory defaulted for Keyscan's proprietary 36-bit Wiegand format cards.

Keyscan systems can be modified to recognize a wide range of additional access card formats. Some of these formats are proprietary to other system manufacturers. Some other formats, notably 26-bit Wiegand, are "open". This means that card manufacturers will supply any card number sequence requested. The "open" 26-bit format means duplicate cards exist.

Installing dealers and end-users should be aware of the risk. Because the 26-bit format is unregulated, duplicated card numbers can be easily obtained and could be used to gain unauthorized access to a facility.

Keyscan strongly recommends that installing dealers apprise the end-user customer of the risks posed by 26-bit cards and have the end-user customer acknowledge they understand the risk by signing the "Waiver of Liability".

Waiver of Liability

Keyscan system end-user (End-User Name:_____)

acknowledges that he/she has been advised that the Keyscan system installed by

Dealer Name _____

in the end-user premises has been modified from the factory original settings to accept Wiegand 26-bit format cards.

End-user acknowledges that he/she is aware that duplicate cards may exist in this format and that a duplicate card could be used to gain illegal access to his/her facility.

(Dealer Name: _____) SHALL NOT BE RESPONSIBLE FOR ANY CONSEQUENTIAL, CONTINGENT, SPECIAL OR INCIDENTAL DAMAGES whatsoever, except as specifically set forth in the LIMITED WARRANTY, caused by illegal use of duplicate 26-bit access cards.

Dealer Name	**End-User Name**
Per	**Per**
Signed	**Signed**
Dated	**Dated**



Door
Hardware



Electronic
Access & Data



Mechanical
Key Systems



Lodging
Systems



Entrance
Systems



Interior Glass
Systems



Safe
Locks



Service

dormakaba
USA
6161 E. 75th Street
Indianapolis, IN 46250

T: 1 888 539 7226
dormakaba.us

dormakaba
Canada
7301 Decarie Blvd.
Montreal Quebec H4P 2G7

dormakaba.com

KD50015-E 11-26