

Aurora software install

- Database Installation
- Aurora Agent Installation – Do Not Skip (This controls backups among other things)
- Standard Communication Install
 - When this one finishes another install flashes on the taskbar – for some reason it doesn't pop-up automatically – Don't Skip It
- Client Installation
 - Microsoft Impressions 4
- Make sure that E-Plex Communication and Aurora Database locations are both localhost

Run and Register Aurora

- Login: keyscan
- Pass: KEYSKAN (all caps)
- Enter all site and dealer info and then on the next tab enter the Aurora and SDK license
 - Aurora license starts with AUR150
 - SDK license starts with AUR650
- Register the software at <http://keyscanregistration.ca/>
 - Software Version should be minimum 1.0.22.0 (current release is 1.0.25.0 May 2024)

Firewall Settings

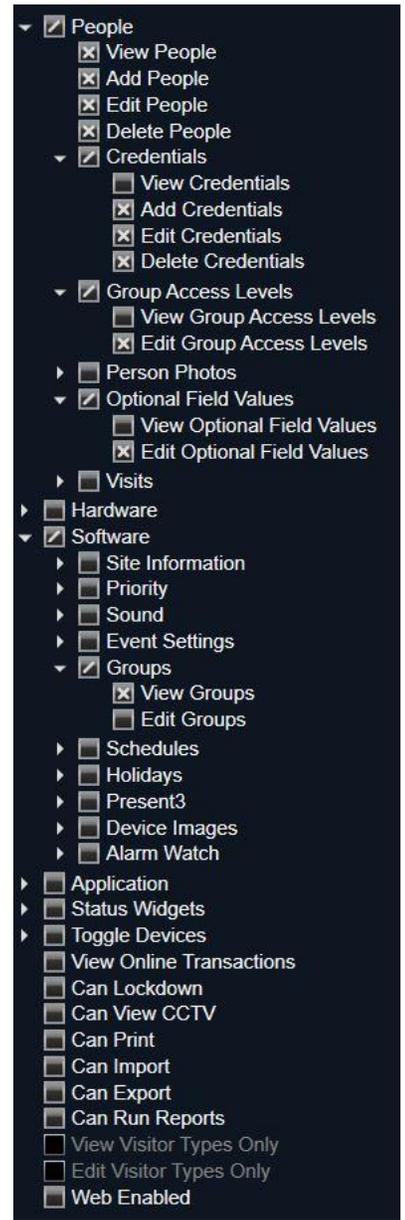
- This is only needed if the Aurora and Community software are on separate machines
- Ensure your firewall is set to allow the following ports (Inbound Rules):
 - n 27702—TCP/IP
 - n 8740—TCP/IP
 - n 3001—TCP/IP
 - n 9999—TCP/IP
 - n 6000—TCP/IP
 - n 6001—TCP/IP
 - n nnnn—Aurora SQL TCP dynamic port. To determine the SQL TCP dynamic port: From the Windows Run/Search box, enter
 - SQLServerManager11.msc (if using Aurora 1.0.21.0 or prior)
 - SQLServerManager14.msc (if using Aurora 1.0.22.0 or after)
 - In the SQL Server Configuration Manager, expand SQL Server Network Configuration and select Protocols for AURORA and double-click TCP/ IP. Select the IP Addresses tab and scroll to IP All. See the value listed for TCP Dynamic Ports.
 - n 1434—UDP

The software is now installed and registered. Next would be the panel setup and access groups.

Software Setup

- Gear Icon - Application Utilities
 - Check Extended PIN (7 digit)
 - Check Auto Generate Pin
 - Do **NOT** Check the Enable Keyscan for Extended Card unless specifically told to do so
 - Check KABA Integrated Mode
 - Auto Delete on Expiry
 - Delete Person
- Group Setup
 - Recommend only Group1-5 Set as Active (16 makes a longer confusing list as most sites use 2-5)
 - These Groups will be what Community links to for access
 - Most sites do a simple setup similar to the below. The Choice is yours but really shouldn't exceed 10.
 - A single credential can only have 10 access groups. Please note that Emergency Keys by default get all available groups. If the site has over 10, it will be denied by Aurora and will not work when made.
 - Staff Common Access
 - Resident Common Access
 - Pet Spa (restricted areas that are sometimes paid extra for)
 - Bike Shop (restricted areas that are sometimes paid extra for)
 - Staff Maintenance Shop
 - Manager Office
- Hardware Setup
 - Globe Icon – Hardware Setup
 - Add panels with drop down in upper left corner
 - You will need the panel Serial Number and IP Address
 - Click on Door Tab and label reader/door
 - Click on Additional Settings Tab
 - Under Hardware Settings change the Reader Format
 - S-KABA Integrated (17Byte)

- Add Second User with the following info for Community Access
 - Gear Icon – Manage System User
 - Add User
 - User Name: Community
 - Password: 1234 (This will be changed later)
 - Given Name: Community
 - Surname: Integration
 - User Type: User
 - Permissions: See Pic to Right
 - These are the minimum rights needed for Community to talk to Keyscan
 - Do NOT uncheck the Site check box at the top or user won't work.
 - Save
- Close the software then open it back up
 - Login: Community
 - Password: 1234
 - You will be prompted to change password
 - New Pass: COMMUNITY (or something similar)
 - Confirm Password
 - This user is very limited and used for Community to Aurora communication
- Close software and log back in as Keyscan to do further setup
 - It is a very good idea to create another admin login for the system.
 - Once the system is truly completed remove the Keyscan login
 - **Do not lose the new admin login**
 - **Keyscan will charge to unlock the software is login is forgotten**
 - It is advisable to have separate logins for anyone that uses the software



Additional Setup

- People Icon – Group Access Levels
 - Assign Door Access to Groups
- Globe Icon – Schedule Management
 - Create Schedules
- Globe Icon – Schedule Assignment
 - Assign Schedules to Doors
 - DO NOT ASSIGN SCHEDULES TO READERS
 - This would cause readers to only work on those schedules
 - This affects staff also
- Gear Icon – Database Maintenance
 - Backup Now
 - Scheduled Backup Tab
 - Choose options as needed

- Default backup location is C:\Program Files\Microsoft SQL Server\MSSQL11.AURORA\MSSQL\Backup
- To change location, click on browse in lower right corner and choose a new location
- We recommend that you have that folder auto backed up to a server

ACU Setup for Integration

- The following assumes that the panel is already on the network and has the IP address already programmed into it.
- Please note that even if you are using a 3rd party 26-bit long range reader, you still MUST have the MH firmware chip in the panel for it to work with Community Integration and Aurora-S.
- CA150 units require specific DIP switch settings on S2:
 - Reader Format DIP switches: S2.1, S2.3, S2.4, S2.5 and S2.6 = 1, S2.2 = 0.
 - System Configuration DIP switches: S2.9 = 1, S2.10 = 0
- Non-CA150 units require specific DIP switch settings on S2:
 - System Configuration DIP switches to enter KABA Integrated Mode: S2.11 = 0, S2.12 = 1.
- After changing/setting System Configuration switches, a memory clear is required:
 - For CA150 controllers, turn on S1.9, momentarily short J6, and then momentarily short J1. Dip switch S1.9 can be disabled after memory clear is complete.
 - For ACU/ECU controllers, press and release S1, wait at least 5 seconds, then within 10 seconds, press and release S3.
 - When done correctly, the panel will beep for 2 minutes. It should then show a green light indicating that it is online with the software.

Verify that panel is online in Aurora

- Pulse Icon – Status
- On left choose – Access Control Unit Status
 - All panels that have been programmed in the software will show here
 - Make sure status is Active
 - If not, right click on the panel name and choose Change Status – Active
 - Last Polled should be current time
 - Firmware Version should be between 1.64 – 1.75
 - If this shows 9.47 you have one of these three problems
 - Firmware chips not added to panels
 - Dip switches on panels not set as above
 - Panels have not been reset as shown above

Community Setup for Aurora Integration (Steps to be done in Community) (Assumes Community has already been setup for locks)

- Click on System Setting
- On left, click on Advanced Settings
- Change slider on Enable AuroraSync interface to YES
 - Aurora IP address
 - Localhost or whatever location the Aurora software is on, if different PC
 - Aurora Login
 - Community
 - Aurora Password
 - The one you created when logging into Keyscan with Community
 - Click on disc to save

- Test Connection
 - Should come back as Successful
- Click on Home in Upper Right Corner
- Click on Access Management
- Click on Common Area Access
- Click on +
 - Profile Name – RESIDENT
 - Profile Type – Resident
 - Click Save
 - Check the Common Areas that Residents will need to have access to
 - Select Default Access for each YES or NO
 - As long as the Common Area is checked a resident can be granted access when making the credential regardless of the default access option
 - Click Access Point Tab
 - Click on the top check box to select all access points
 - This makes it where a resident can get common area access when added to a unit
 - Click Save in top right hand corner
- Click on + (Note: Below Staff options may vary based on the options setup in Credential Management)
 - Profile Name – STAFF
 - Profile Type – Staff/Vendor
 - Credential Class Type – Staff
 - Click Save
 - Check the Common Areas that STAFF will need to have access to
 - Select Default Access for each YES or NO
 - As long as the Common Area is checked a staff member can be granted access when making the credential regardless of the default access option
 - Click Credentials Tab
 - Check the Credentials that this common access option should apply to
 - Click Save in top right hand corner
- Repeat Steps above for each Staff member card type
- TEST THE INTEGRATION
 - Make a key for a resident or staff member
 - Go to Aurora
 - Click on People Icon – Manage People
 - The new credential should show up something like “Unit number”-Resident Name
 - Card number will be a long 34 number and letter string
 - Please note that it can take up to 2 minutes for the credential to be sent to Community
 - If the person doesn’t show in the list after 2 minutes
 - Go to Community
 - Click on Monitoring Icon
 - Under the credential and Aurora Status tab, what does it show?
 - Pending – Wait a little longer or verify that you did the correct steps on the Community user creation in Aurora earlier
 - Synchronized – Check Aurora again and it should be there
 - N/A – Something is not setup correctly in Community
 - Person doesn’t have access to any doors linked to Aurora
 - Test the credential at a valid card reader
 - It could take 2 reads the first time if the data hasn’t yet made it to the panel itself
 - If the credential doesn’t work

- Click on the Pulse Icon – Status
- Double Click on Online Transactions on the left
- See if the credential shows up or not
 - If so, what error does it show?
 - Troubleshoot from there
- If it doesn't show up – check your card format setting from earlier

Helpful hints (Possible fixes for errors found)

- If the card reader does not acknowledge the credential at all and power has been confirmed
 - Check that the firmware supports the credential being used.
 - DESFire and Classic were turned off in 05.26.23 and 03.22.23
 - Both were reenabled in 11.10.23
 - BLE also had a fix in 11.10.23 due to something in an earlier version
 - Please note that HH6 FW 2.40 or higher should be used when updating the SRK firmware
 - FW update on SRK REQUIRES the COMM-71800-1 cable that plugs into the back of the reader
- If the reader beeps at the credential but nothing is seen in Online Transaction
 - Check the card reader format in the panel to ensure it is set to "S-Kaba 17 byte"
 - Make sure the panel has the correct reader firmware chip
 - COMM-Kits ship with version 1.70 firmware
 - If the panel firmware in Aurora shows 1.64 or before, they bought a Commercial version panel and need a reader firmware chip (CF10004 or CF10010) if they haven't already changed it
 - If panel firmware shows as 9.46, 9.47, or similar, the panel dipswitch settings are incorrect
- If the reader beeps at the credential and a card is seen in Online Transaction but shows access denied or card not found
 - Check access groups
 - Check Monitoring tab in Community to make sure key synced with Aurora
 - Make sure that tech did the default panel procedure shown previously as this would cause that issue