dormakaba

Community

Aurora Integration Deployment and Support Manual

PK3769 2.1.1 - 09/2025
Original document

EN

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
1-866-dormakaba (1-866-367-6252)

www.dormakaba.com

Copyright © dormakaba 2025
All rights reserved.

No part of this document may be reproduced or used in any form or by any means without prior written permission of dormakaba Canada .

All names and logos of third-party products and services are the property of their respective owners.

Subject to technical changes.

Table of contents

QUICK STEPS

Integration essentials

Deployment consultation. Define networking and data requirements for both systems. Provide the dormakaba technician with Aurora access group names.

Requirements. Establish core requirements per Community and Aurora product documentation. Refer to release notes to determine supported versions. For existing Aurora integrations, contact dormakaba Support to verify existing Keyscan devices are equipped with the required firmware.

- SRK BLE readers: COMM-SRK-RCFN2, COMM-SRK-RNFC2, or COMM-SRK-RNSC2.
- Keypad readers: COMM-SRK-KPW and COMM-SRK-KPM.

Download/install Aurora. Aurora software is available by download only (ISO image and/or mounted Aurora installation drive). In File Explorer, right-click AuroraInstallation.exe and select Run as Administrator. Run the Database Installation. Restart the Aurora Server. Run the following: Aurora Agent Installation, Client Installation, Standard Communication Installation, other modules as required/purchased. Click Update Locations. Leave E-Plex Communication Service Location and Aurora Database Server Location set to localhost.

Configure firewall. Verify the following TCP/IP ports are allowed: 3001, 9999, *nnnn (*Aurora SQL TCP dynamic port), and 1434 (UDP).

Register Aurora. Refer to Aurora documentation for registration steps.

Configure Aurora database.

1. In Site Management > Hardware Setup, add ACUs for all installed hardware (doors and elevators). SRK series readers with ACU reader firmware (V6.00+).
2. ACU Setup. CA150 units DIP switch settings on S2:
   a. Reader Format DIP switches: S2.1, S2.3, S2.4, S2.5 and S2.6 = 1, S2.2 = 0.
   b. System Configuration DIP switches: S2.9 = 1, S2.10 = 0.
   c. Non-CA150 units use KABA Integrated Mode: S2.11 = 0, S2.12 = 1.
   d. Clear memory:
      - 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. Set Card Countdown with S1.7 - Temporary Card Countdown.
      - For ACU/ECU controllers, press and release S1, wait 5 seconds, then within 10 seconds, press and release S3.
      - For ACUs/ECUs other than the CA150, select Card Countdown Enabled and S - KABA Integrated (17Byte).
3. Application utilities. Select Extended PIN (7-digit), enable Auto Generate PIN, verify KABA Integrated Mode is selected. The Aurora Communication services must be stopped and then restarted after enabling Kaba Integrated Mode.
4. Aurora Access Group Setup. Select Site Management > Group Setup, then define group names that reflect the access level.
5. Schedules. Select Site Information Setup > Schedule Management.Click Add Keyscan Schedule. Create blocks of time to define the schedule.
6. Group Access Levels. Select Manage People > Group Access Levels. Configure the access levels for each group.
7. Database Maintenance. Select Application Management > Database Maintenance > Scheduled Backup. Verify that backups are scheduled for every day.

QUICK STEPS

Add Community system user with Master rights. In Aurora, click Settings > Manage System User. Click Add User. Specify user details and select the Master user type. Select all sites and all permissions. Click Save. **Note**: To make the new user active for Community, log out then log in with the new user.

Install and configure Community. Refer to Community documentation.

Enable AuroraSync interface. In Community System Settings > Advanced, enable and configure the AuroraSync interface. For login/password, use the Community system user with Master rights.

Configure common area access for Aurora. In Community, go to *Access Management > Common Area Access* and create resident and staff/vendor profiles to associate with Aurora access groups. Maximum groups per key: 10 for Aurora Standard license, 30 for Aurora Elite license.

Test the integration. Make and use keys encoded with Aurora access.

Troubleshooting.

1. Verify Keyscan Aurora settings in Community.
2. If the test connection fails but you can ping the Aurora Server, verify application and services are running. If required, verify port connectivity to the Aurora IP address/server name.
3. Verify network ports are open (inbound rules are established for firewalls).
4. Verify Aurora services are running. In the Aurora Client, go to Status > Status. On the left, double-click Software Connections Status (if not already open). Under Software Name, there should be Keyscan Aurora, Aurora Agent andCommunications.
5. Ensure that the SQL Server Browser service is running.
6. Verify that Aurora hardware is communicating successfully. In the Aurora Client, go to Status > Status. On the left, double-click Access Control Unit Status (if not already open). Verify that the panels are Active, that the pending packages are either 0 or counting down, and that the Last Polled is updating with the current date/time.

1 About this document

1.1 Validity

This document describes the integration for the following products:

Product designation:	Community
Product designation:	Aurora

1.2 Target audience

This document is for the dormakaba and third-party deployment teams and support technicians.

1.3 Purpose and objective

The content of this document includes integration-related requirements and steps to install, configure and troubleshoot the Community integration with Aurora.

1.4 Additional documents

- *Keyscan Aurora Software System Specifications*, KD50020 (KKT3016)
- *Keyscan Aurora System Architecture*, KD50013-E
- *Community Release Notes* PK3696
- *Community Installation Guide* PK3695
- *Community User Guide* PK3706

2 Product description

Community™ integrates with Keyscan© Aurora™ to offer a centralized access management system for properties that use Keyscan devices to control access to resident and staff common areas.

Designed for use by hands-on integrators, this guide lists all high-level steps in the integration process. Detailed information and examples are provided for steps that relate exclusively to integration. For complete information about installing, configuring and using Community and Aurora, refer to the respective product documentation.

After integration, Community displays Aurora access in the Resident Management summary, on the Staff/Vendor Management Assigned Keys tab, in the Monitoring module and upon reading a resident or staff/vendor key.

2.1 Deployment consultation

A successful integration starts with communication and planning.

dormakaba representatives meet with your stakeholders to review the networking and data requirements for both systems. The discussion includes how network connectivity will be established so that data can flow from the Community Server to the Aurora Server. The Community Support representative verifies configuration details, such as the Aurora access group names as the same values are required in multiple locations.

When all dependencies are met, the installation of both systems is coordinated to ensure on-time deployment.

Before the meeting ends, agree upon and record the responsible parties and dates for next steps.

2.2 Integration requirements

The requirements for deploying either product independently also apply to integrations.

For optimal performance, dormakaba strongly recommends that Aurora and Community are installed on different servers. If using a single server, contact dormakaba Support to ensure that server specifications are sufficient.

2.2.1 Aurora requirements

- Keyscan Aurora-S (includes the Aurora database, Aurora Agent, Client, communication services and Aurora Software Developers Kit). Refer to *Community Release Notes* for version requirement.
- Depending on the scale of your deployment, refer to the following documents:
  - Small systems (≤25 doors)—*Keyscan Aurora Software System Specifications*, KD50020 (KKT3016)
  - Large systems (> 25 doors)—*Keyscan Aurora System Architecture*, KD50013-E

Integration also requires the following Keyscan devices:

- Keyscan CA150 ACUs (PC1156 DIP switch version board) with custom firmware item #CF10010
- Keyscan CA250, CA4500, CA8500 ACUs and EC1500, EC2500 ECUs (PC1097 DIP switch version boards) with custom firmware item# CF10004

The custom firmware is required to be able to read the unique Community credential bit structure and communicate to the panels with Aurora-S.

- SRK-series readers. The following readers are supported:
  - Keypad Readers—COMM-SRK-KPW and COMM-SRK-KPM
  - BLE Readers—COMM-SRK-RCFN2, COMM-SRK-RNFC2, or COMM-SRK-RNSC2

2.2.2 Community requirements

- Refer to *Community Releae Notes* PK3696

3 Deployment steps

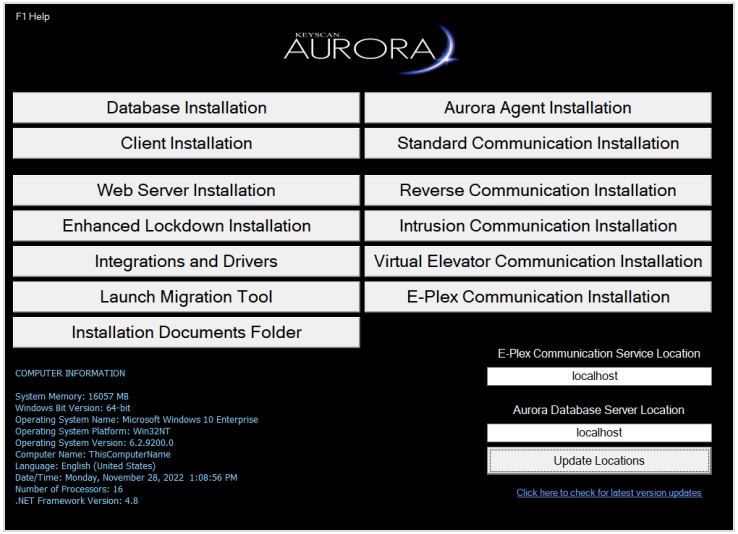
3.1 Download and install Aurora

Aurora software is available by download only (ISO image and/or mounted Aurora installation drive). The download includes the following:

- Keyscan Aurora-S
- Software and hardware documentation

Refer to the Aurora Installation Online Help (AuroraInstallation.chm) for guidance during installation.

1. After download, right-click AuroraInstallation.exe and select Run as administrator.



2. Perform the following steps in sequence:
   a. Run the Database Installation.
   b. Restart the Aurora Server.
   c. Run the Aurora Agent installation.
   d. Run the Client Installation.
   e. Run the Standard Communication Installation.
   f. Install other modules as required/purchased.
   g. Click Update Locations.

Leave E-Plex Communication Service Location and Aurora Database Server Location set to localhost.

3.2 Configure firewall

Ensure your firewall is set to allow the following ports (Inbound Rules):

- 3001—TCP/IP
- 9999—TCP/IP
- *nnnn*—Aurora SQL TCP dynamic port. To determine the SQL TCP dynamic port: From the Windows Run/Search box, enter SQLServerManager16.msc. In the SQL Server Configuration Manager, expand SQL Server Network Configuration and select Protocols for AURORA then double-click TCP/ IP. Select the IP Addresses tab and scroll to IP All. See the value listed for TCP Dynamic Ports.
- 1434—UDP

3.3 Register Aurora

After installation, Aurora must be registered to proceed with the integration. Refer to Aurora documentation for registration steps.

If registration fails, contact dormakaba Canada Inc. between 9AM and 5PM, EST:

- toll-free (Canada/USA) 1-888-KEYSCAN (539-7226)
- outside Canada/USA +1-905-430-7226

3.4 Configure the Aurora database

The following sections review the necessary configurations required to support the Community/Aurora integration.

Establish and apply naming conventions for all Aurora doors, groups and elevators.

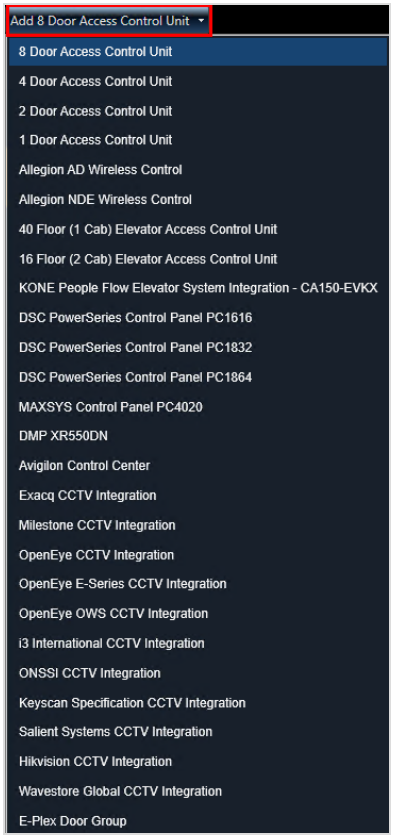
3.4.1 Hardware Setup

The Community integration with Aurora requires that the Aurora panels and the Aurora software both be in KABA Integrated Mode.

1. Select Site Management > Hardware Setup.
2. Add ACUs for all installed hardware (doors and elevators).

   COMM-kits (i.e. COMM-CA8500-KIT) come with the appropriate multifamily housing firmware. Commercial panels (i.e. CA8500) do NOT come with multifamily housing firmware and it must be purchased separately.

3. Ensure SRK series readers with reader firmware (V 6.00+).



3.4.2 ACU setup

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

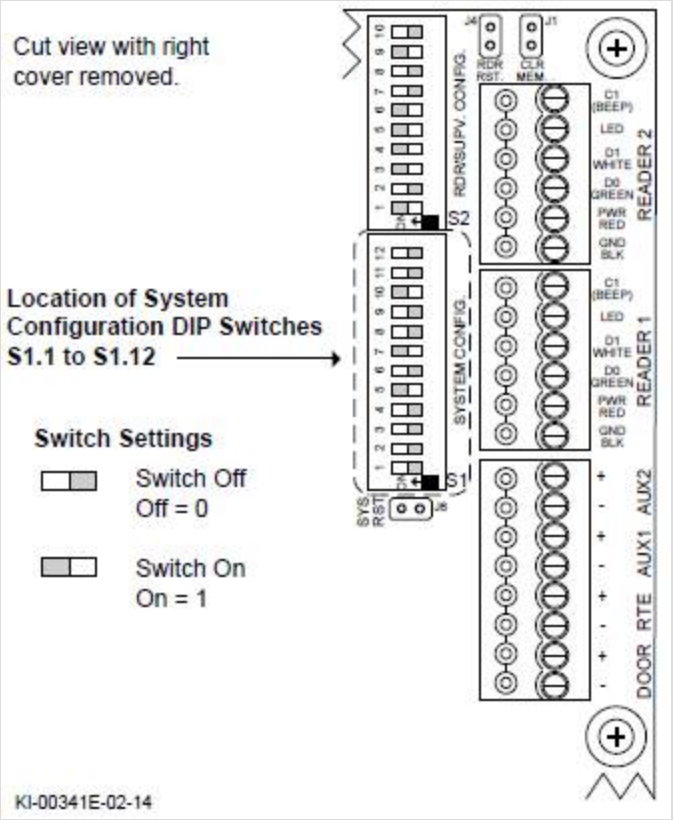
Non-CA150 units require specific DIP switch settings on S2:

- 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:

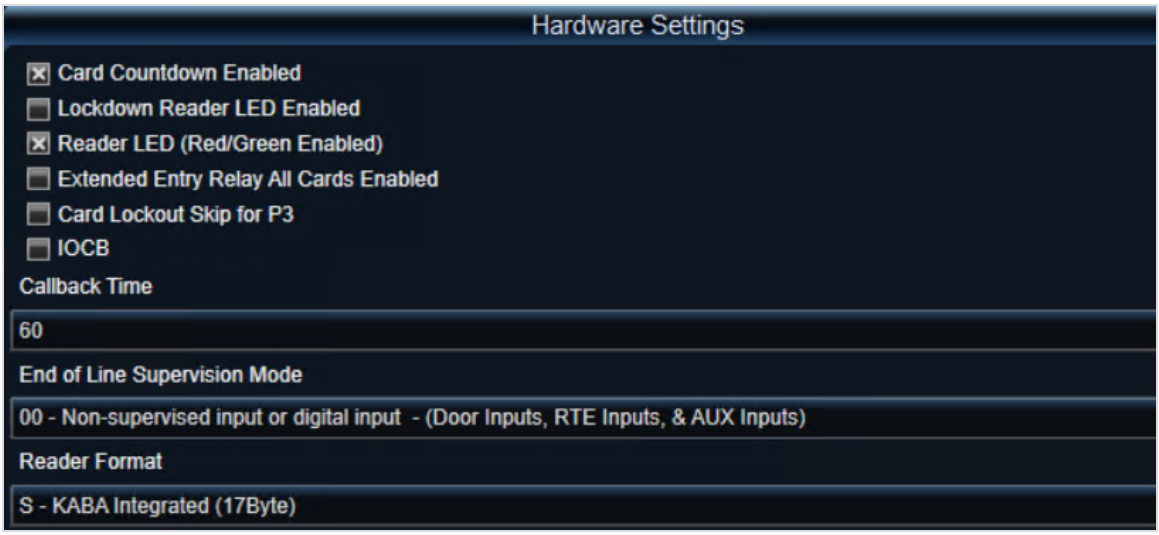
- For CA150 controllers, turn on S1.9, momentarily short J6, and then momentarily short J1. Dip switch S1.9 can be disabled after memory clear is complete.
- For ACU/ECU controllers, press and release S1, wait 5 seconds, then within 10 seconds, press and release S3.

The following figure shows a CA150 board.



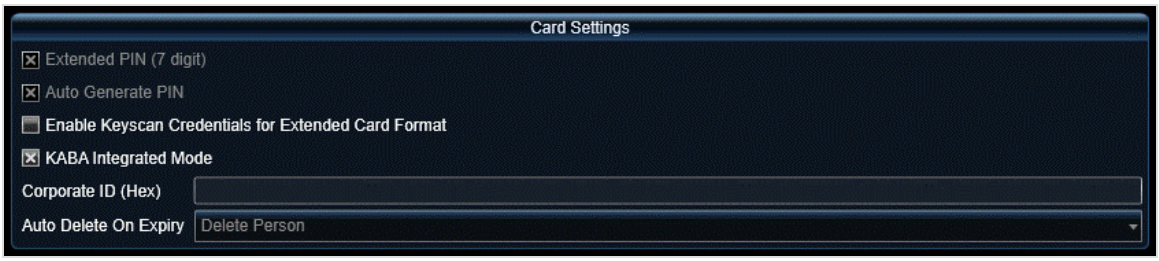
For ACUs/ECUs other than the CA150:

1. Click Site Information > Hardware Setup.
2. Click the Additional Settings tab of each panel (Hardware Settings).
3. Select Card Countdown Enabled.
4. For Reader Format, select S - KABA Integrated (17Byte).
5. Click Save.



3.4.3 Application utilities

1. Select Application Management > Application Utilities > Application Settings.
2. Select Extended PIN (7-digit).
3. Verify Auto Generate PIN is enabled.
4. (*conditional*) If using Keyscan credentials, select Enable Keyscan Credentials for Extended Card Format.
5. Verify KABA Integrated Mode is selected. (Select YES in the pop-up message to confirm.)
6. For Auto Delete on Expiry, Delete Person is automatically selected for KABA Intetrated Mode. Delete Person instructs Aurora to automatically delete people records from the Aurora database when all keys in the record are expired. Records are deactivated upon expiration and deleted at midnight. All keys in the record are also deleted.
7. Click Save.



The Aurora Communication services must be stopped and then restarted after enabling KABA Integrated Mode.

3.4.4 Aurora access group setup

The groups that you define can be enabled/disabled for each common area access profile in Community.

1. Select Site Management > Group Setup.
2. Define group names that reflect the access level (to be configured in the next step). Group names can be edited to match location or function in Community.
3. Activate/deactivate groups as required.
4. Click Save.

The following figure shows group names in Aurora.

Group Setup

Number	Group	Active	Visitor Group	Intrusion User
17	Perimeter Full	Yes	No	Not Assigned
18	Resident Common Areas	Yes	No	Not Assigned
19	Maintenance	Yes	No	Not Assigned
20	Staff Common Areas	Yes	No	Not Assigned
21	Perimeter Corporate	Yes	No	Not Assigned
22	Perimeter Resident	Yes	No	Not Assigned

Additional access options can be configured in Aurora including Elevator and Restricted Area grouping. For detailed information, refer to the Aurora Online Help (AuroraClient.chm).

3.4.5 Schedules

Configure schedules for the access points (doors) in each group.

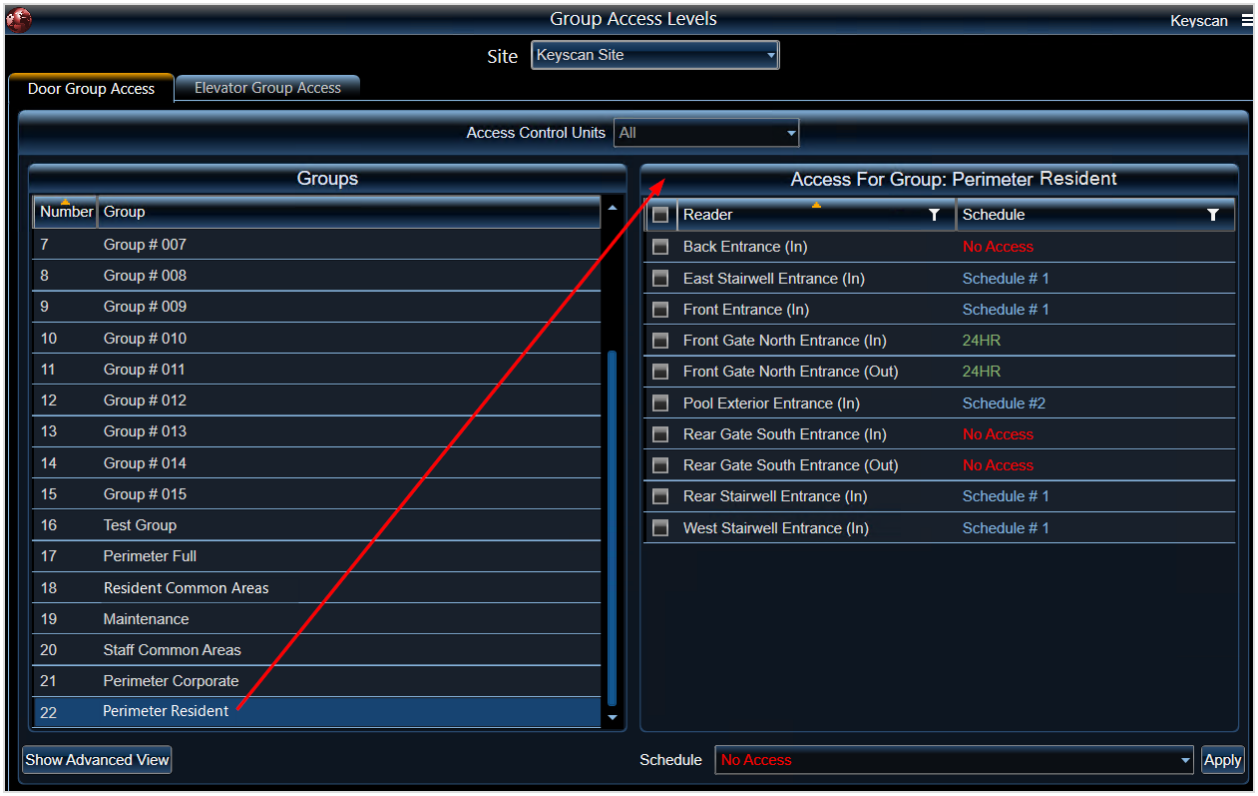
1. Select Site Information Setup > Schedule Management.
2. Click Add Keyscan Schedule.
3. Create blocks of time to define the schedule. Right-click a block to copy/paste blocks. You can also set default off times and designate the first persons authorized to access a door.
4. Click Save.

3.4.6 Group access levels

Configure access for each group. The access group is associated with a common area access profile. Aurora group access extends to any keys made for a unit or credential that is also associated with the same common area access profile.

1. Select Manage People > Group Access Levels.
2. Configure the access levels for each group.
3. Click Save.

The following figure shows group access levels for the Perimeter Resident group.

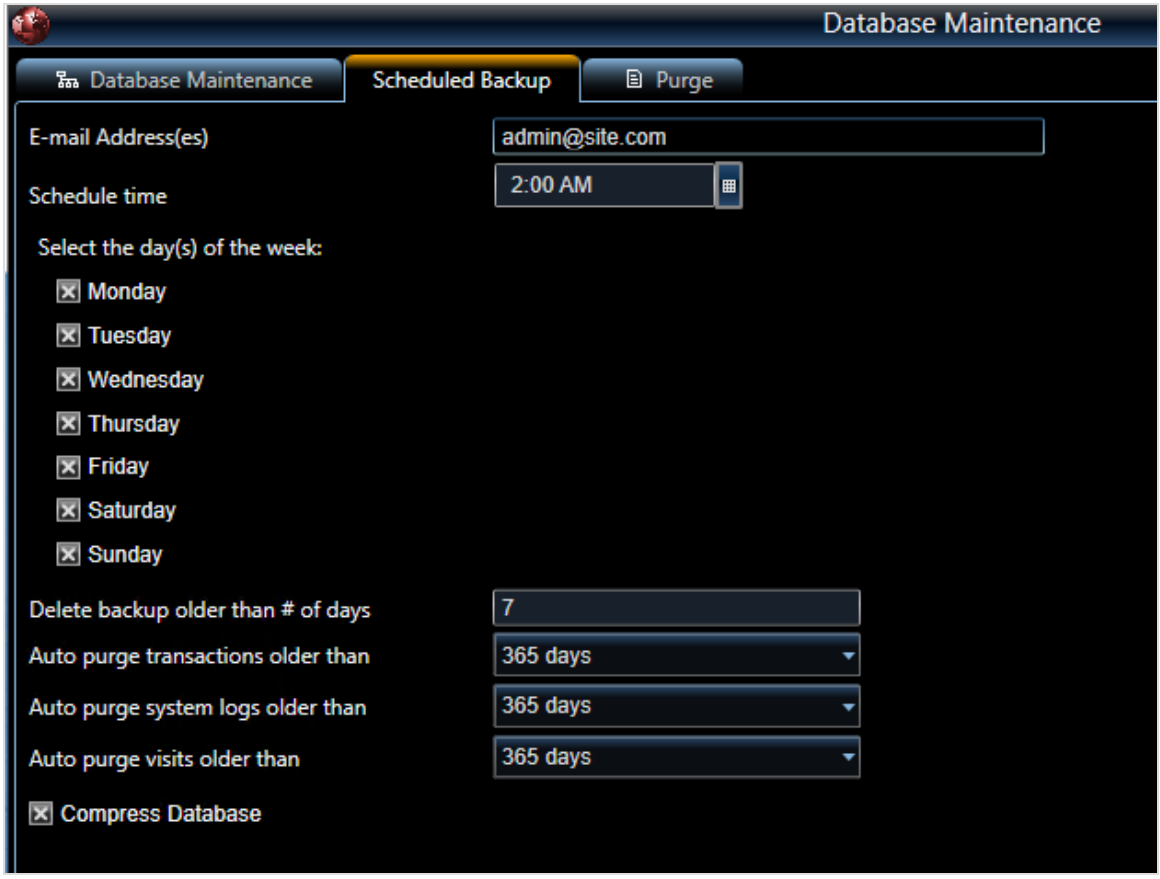


3.4.7 Database maintenance

1. Select Application Management > Database Maintenance > Scheduled Backup.
2. Verify that backups are scheduled for every day.
3. Ensure that all Auto purge options are set to a desired value.

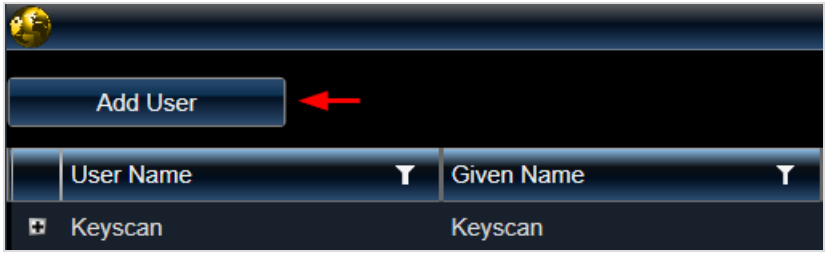
> Please select least amount of days for purging.
>
> Email notifications require SMTP to be set up.

4. Click Save.

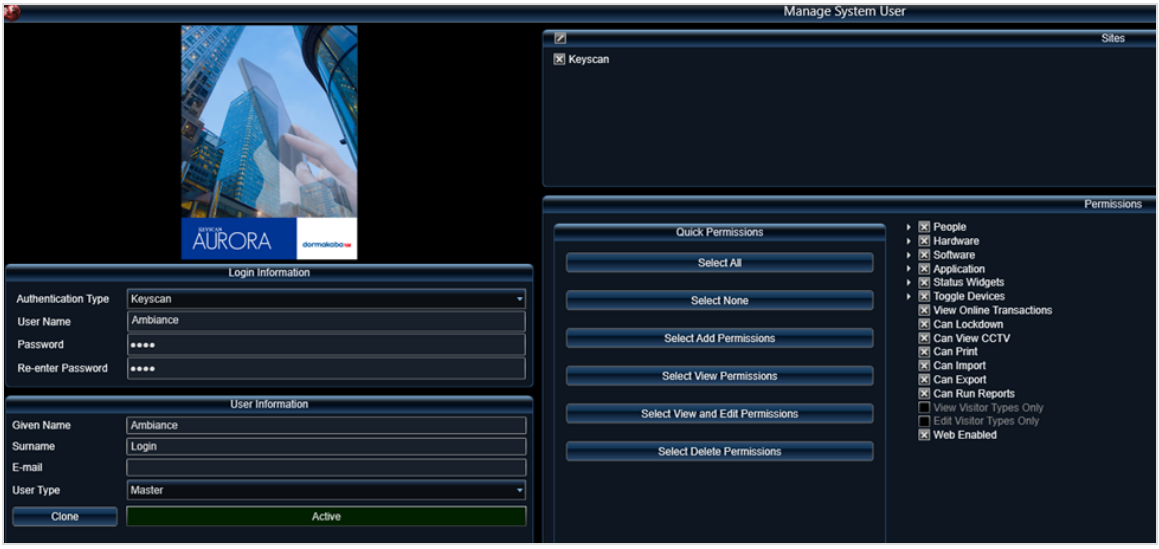


3.5 Add Community system user with Master rights

1. Click Settings > Manage System User.



2. Click Add User.
3. For Login Information, specify a user name and password. Passwords are case-sensitive and have no maximum. Passwords may consist of alphanumeric and special characters.
4. For User Information, specify user details and select the Master user type.
5. For Sites, verify that all sites are selected.
6. For Permissions, click Select All.



7. (optional) Configure additional options, such as user photo.
8. When ready, click Save.

> To make the new user active for Community, log out then log in with the new user. It is also recommended to change the password to the Community system user account.

Next step For initial deployments, proceed to the next step. For post-deployment integrations, proceed to section 3.7.

3.6 Install and configure Community

The Community Server must be installed. For requirements and instructions, refer to the *Community Installation Guide*.

After installation, refer to the Community workflow in the *Community User Guide* (PK3706) to proceed with site configuration. During the process, you can set options that relate to the integration:

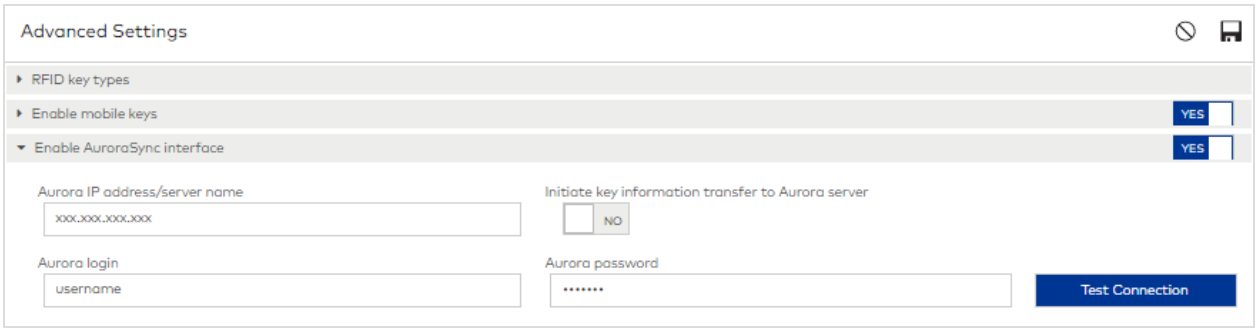
- Enable AuroraSync interface
- Configure common area access for Aurora

After configuration is complete, use the Community system user created in the previous step to make keys for residents and staff. For initial deployments, data is automatically synchronized with the Aurora Server.

3.7 Enable AuroraSync interface in Community

This step establishes a connection between the Community Server and the Aurora Server.

> If Community and Aurora are installed on different servers, inbound firewall rules are required to ensure communications between the two servers (if firewalls are enabled).



To enable the AuroraSync interface:

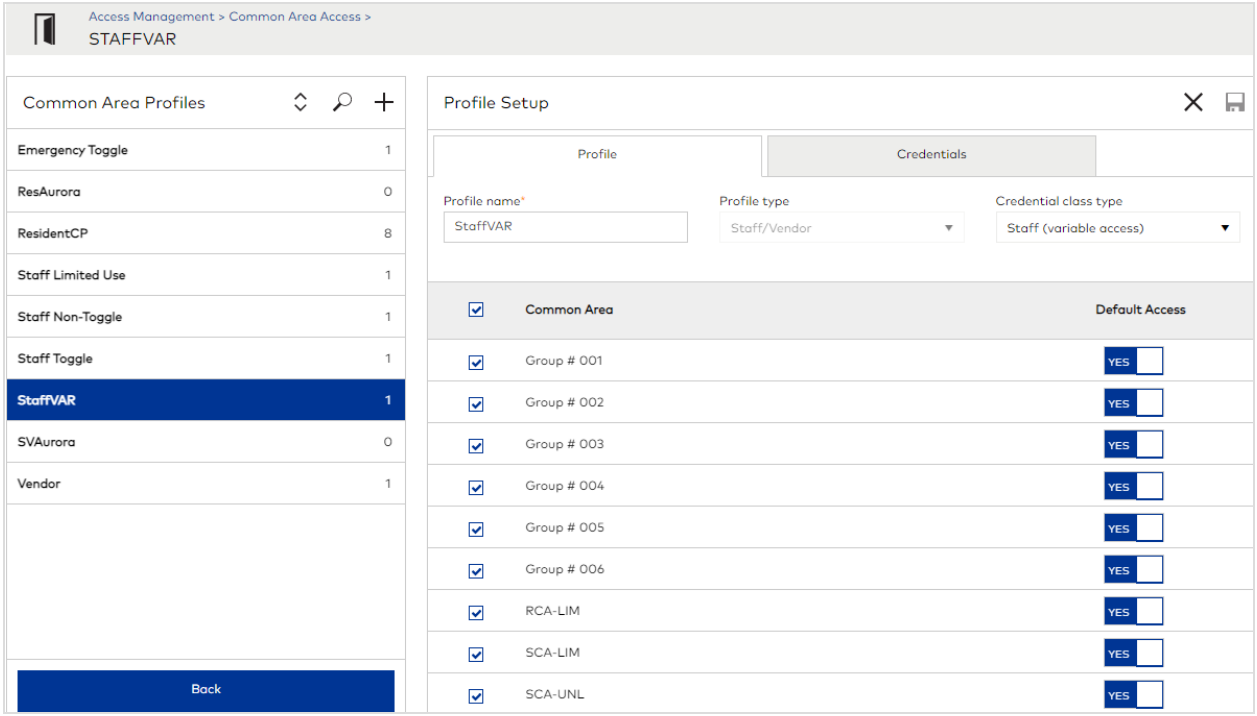
1. Open a supported browser and log in to Community (for example: http://localhost/).
2. Go to Systems Settings > Advanced Settings.
3. For Enable AuroraSync interface, set the switch to YES.
4. Specify the IP address/server name of the Aurora Server. Static IP and Server Name are both supported. If you specify a server name, DNS must be configured correctly.
5. Specify the credentials for the Community system user with Master rights.
6. Click (Save).
7. Click Test Connection to verify the connection.

Upon connection, Community populates Aurora access groups for selection in *Access Management > Common Area Access*. Note that this process may take several minutes.

3.8 Configure common area access for Aurora

This step can only be performed after Community site configuration. At a minimum, credentials must be created in *Access Management > Credential Management*.

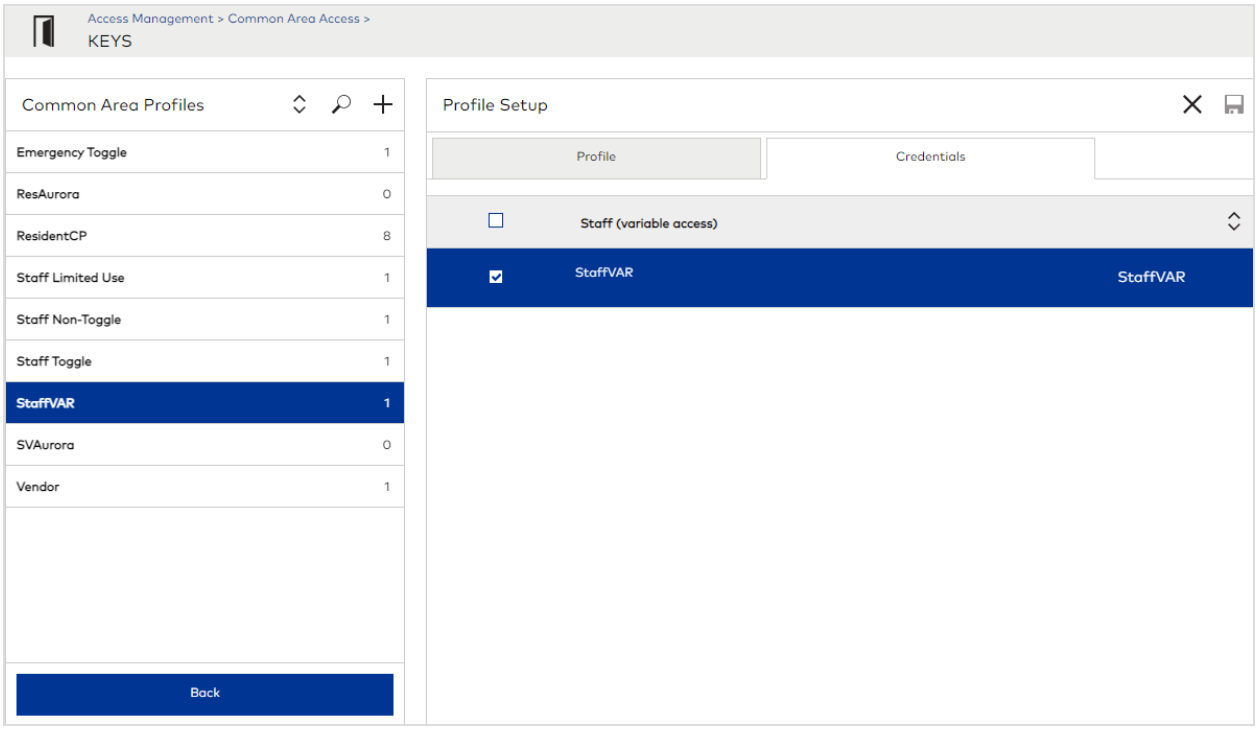
1. Go to *Access Management > Common Area Access.*
2. Click (Add).
3. Specify a descriptive name for the profile.
4. Select the type of profile: Resident, Staff/Vendor. For Staff/Vendor, select the credential class type. *Resident*profiles associate Aurora groups with access points; *Staff/Vendor* profiles associate Aurora groups with credentials.
5. Click Save.The profile is created and tabs that correspond to each profile type display.
6. On the Profile tab, select the Aurora groups that you want to configure for access in this profile and whether to enable default access. Maximum groups per key: 10 for Aurora Standard license, 30 for Aurora Elite license. The following figure shows the Profile tab for a Staff (variable access) profile.



7. Take the appropriate step:
   - For Resident profiles—On the Access Points tab, select the access points to associate with the profile. You can add access points from different buildings.

- For Staff/Vendor profiles—On the Credentials tab, select all credentials that you want to associate with the common areas selected on the Profile tab. You can add access points from different buildings.

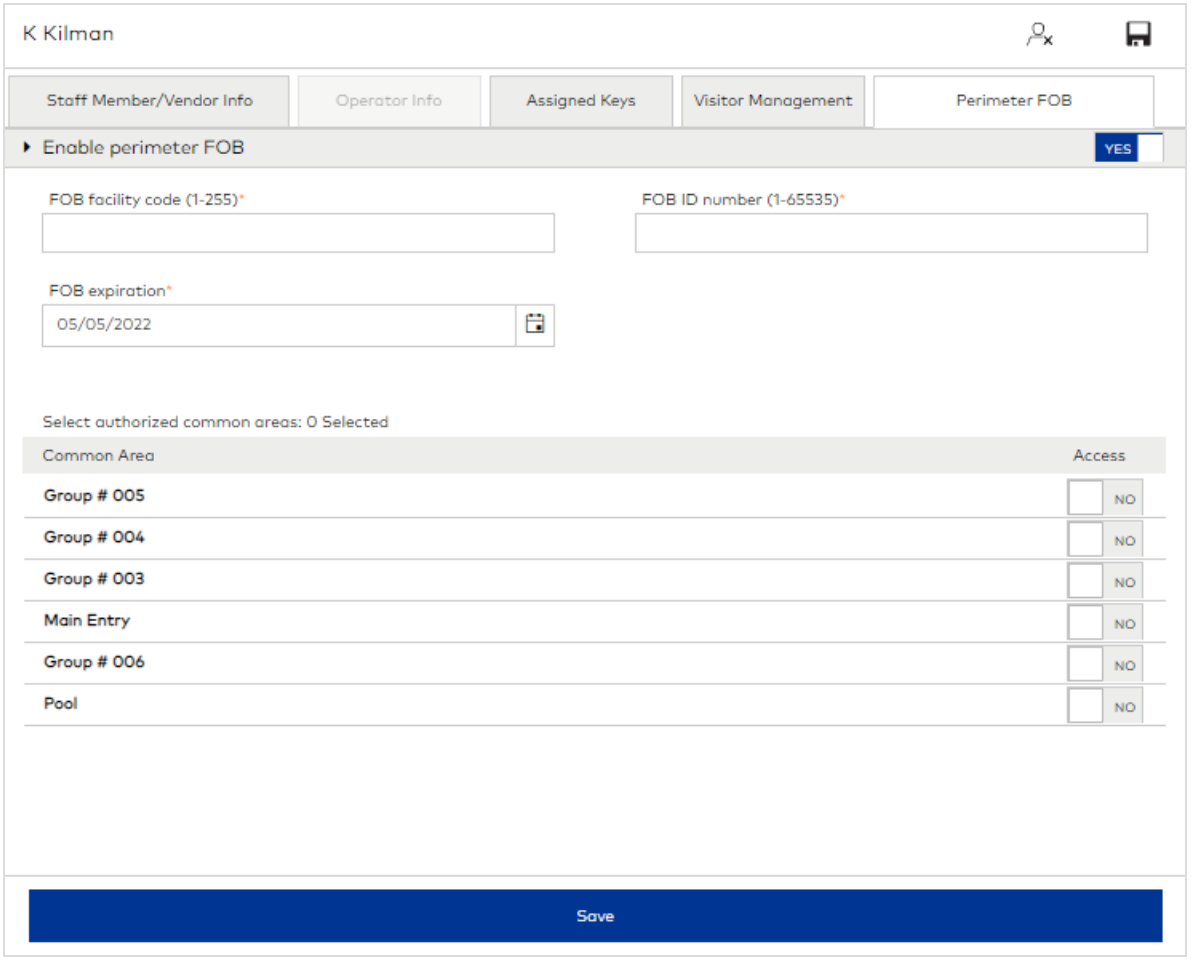
The following figure shows the Credentialtab for a Staff (variable access) profile.



8. Click Save.

3.9 Configure Perimeter FOB

Enabling and configuring the perimeter FOB is an optional step supported in Community. When Aurora is enabled, the Perimeter FOB tab displays in resident and staff/vendor profiles. The following figure shows a staff/vendor profile.



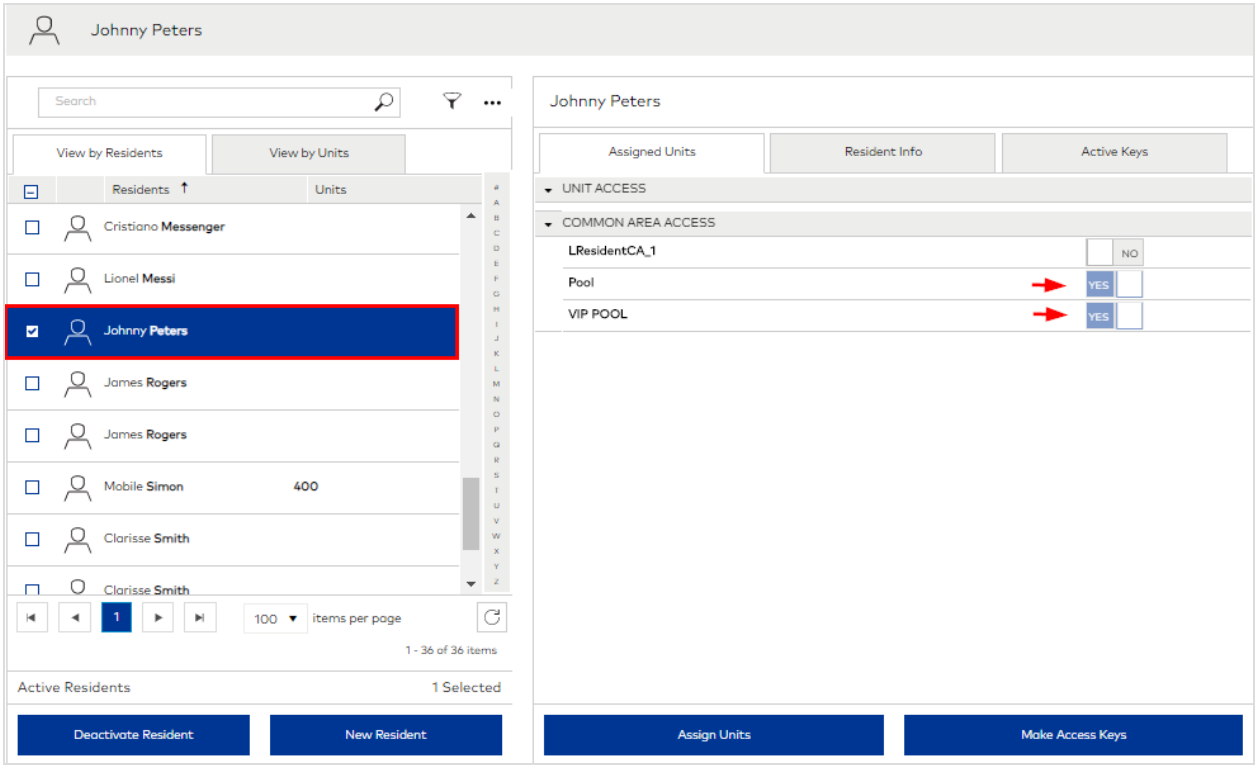
1. Go to the resident or staff/vendor profile.
2. Select the Perimeter FOB tab.
3. For Enable perimeter FOB, change the soft-switch to YES.
4. Specify the facility code. Valid values: 1-255.
5. Specify the FOB ID number. Valid values: 1-65535.
6. Select an expiration date for the FOB. The default for staff/vendors is one year. The default for residents is specified in *System Settings > Key Expiration*.
7. Select the common areas (Aurora access groups) to authorize on the FOB. At least one common area must be selected.
8. Click Save.

3.10 Test the integration

The final step is to test the integration by making and using keys encoded with Aurora access.

In Community, take the following steps:

1. a. Select (or add) a key holder in Resident Management or Staff/Vendor Management. If staff/vendor profiles have already been added, go directly to Staff/Vendor Keys. (The following example is for a Resident key holder.)

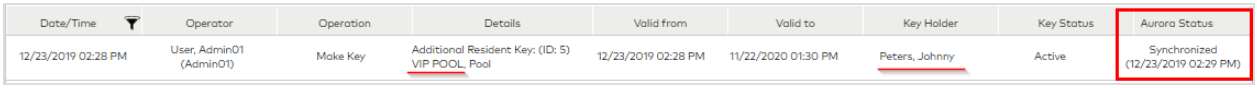


b. On the Assigned Units tab, verify that access is enabled for a common area configured for Aurora access.

c. Click MakeAccess Keys.

d. Test the following:

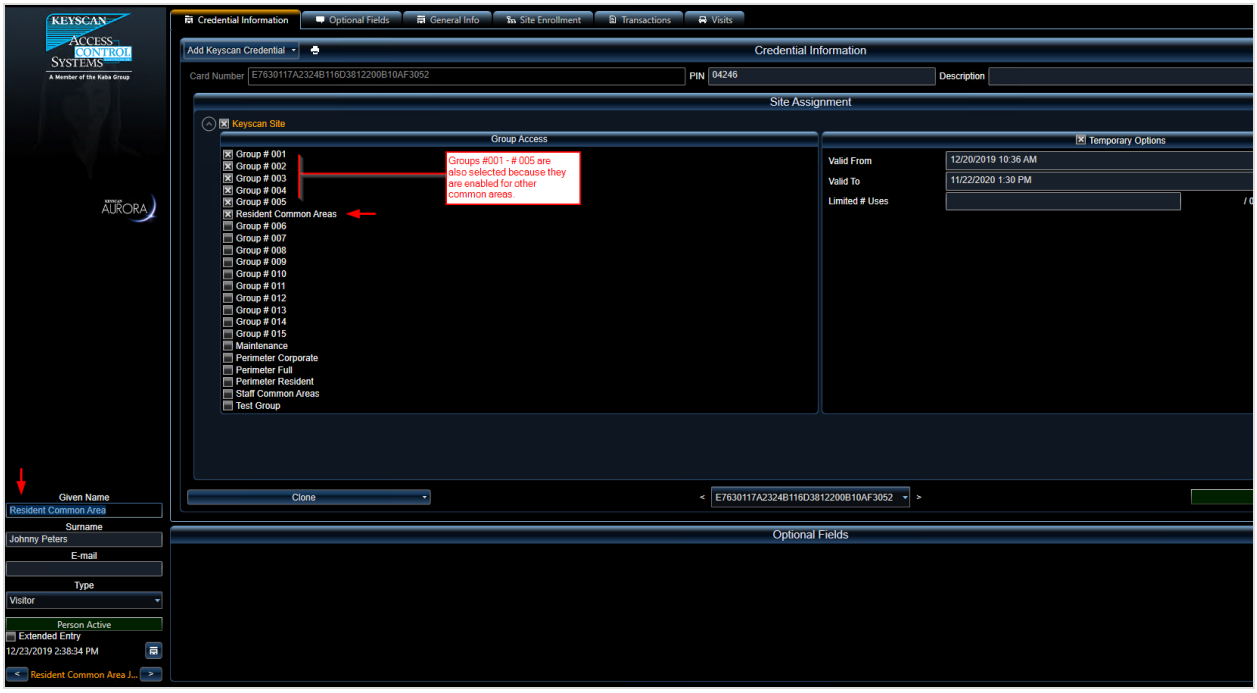
- In the Community Monitoring module, verify the data is synchronized with Aurora:



Date/Time	Operator	Operation	Details	Valid from	Valid to	Key Holder	Key Status	Aurora Status
12/23/2019 02:28 PM	User, Admin01 (Admin01)	Make Key	Additional Resident Key: (ID: 5) VIP POOL, Pool	12/23/2019 02:28 PM	11/22/2020 01:30 PM	Peters, Johnny	Active	Synchronized (12/23/2019 02:29 PM)

> Please note that keys may take up to 2 minutes to synchronize to Aurora. This is normal as that is the check-in time in the integration.
>
> Any key that shows NA in Monitoring does not have access correctly set up for Aurora. Please check settings and remake the key to add access.

- In the Aurora Client, go to Manage People, find the name of the resident (or staff member/vendor), then double-click the entry to view the detailed record.



After keys are synchronized with Aurora, dormakaba recommends that no key modifications are made directly in Aurora as those changes will not be reflected in Community.

- Present the key to Keyscan readers. Test the key to ensure access is granted / denied based on the Group Access levels configured in Aurora.
- Review key activity data in the Community Monitoring module and Aurora Client.

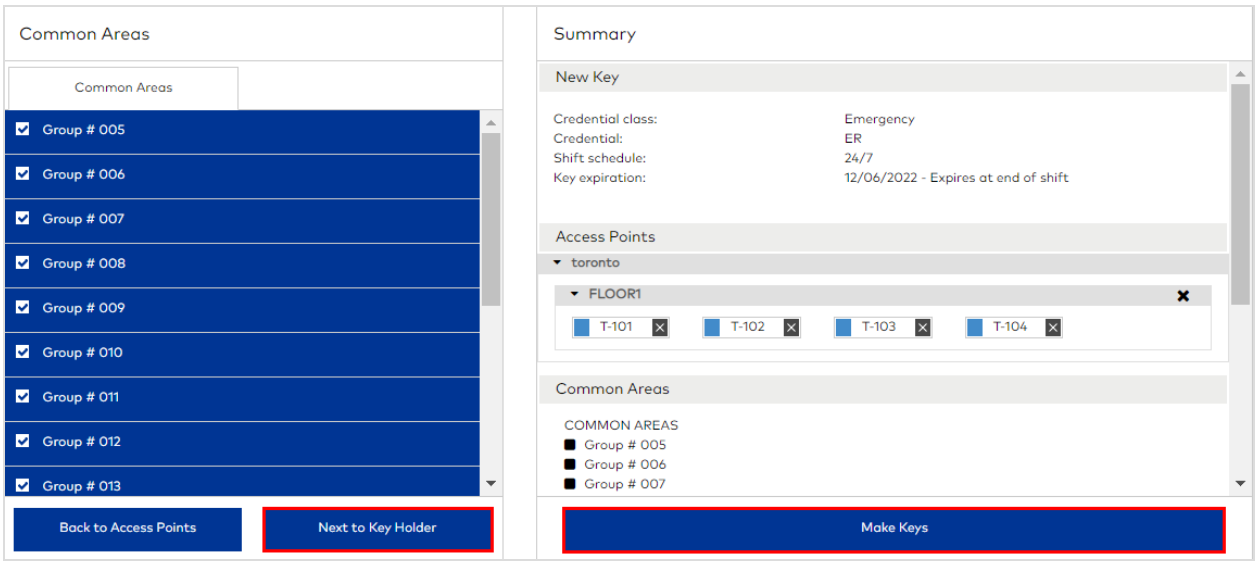
4 Related topics

4.1 Selecting common areas at key encoding

The common areas (Aurora groups) added to a common area access profile display and can be selected when making keys as follows:

- Common areas always display when making staff keys for Emergency credentials.
- Common areas added to a *staff* profile display when making keys for a credential associated with that profile.
- Common areas added to a *resident* profile display when making resident keys for a unit associated with that profile.

The following figure shows common areas listed for an Emergency credential.



4.2 Reports

When Keyscan Aurora is enabled, common areas are included in the following Community reports:

- Key Expiration Report
- Key/User Assignment Report
- System Activity Report

4.3 Monitoring

When Keyscan Aurora is enabled, the status of the key in the Aurora system (Synchronized/Failed/Pending/Not applicable) and the date/time the status was first attained display on the *Monitoring > Keys* tab. You can filter the list of keys based on the Aurora status.

5 Troubleshooting and support

For issues related to Community/Aurora-S integration, refer to the following verification steps (not ordered):

5.1 Technician tips

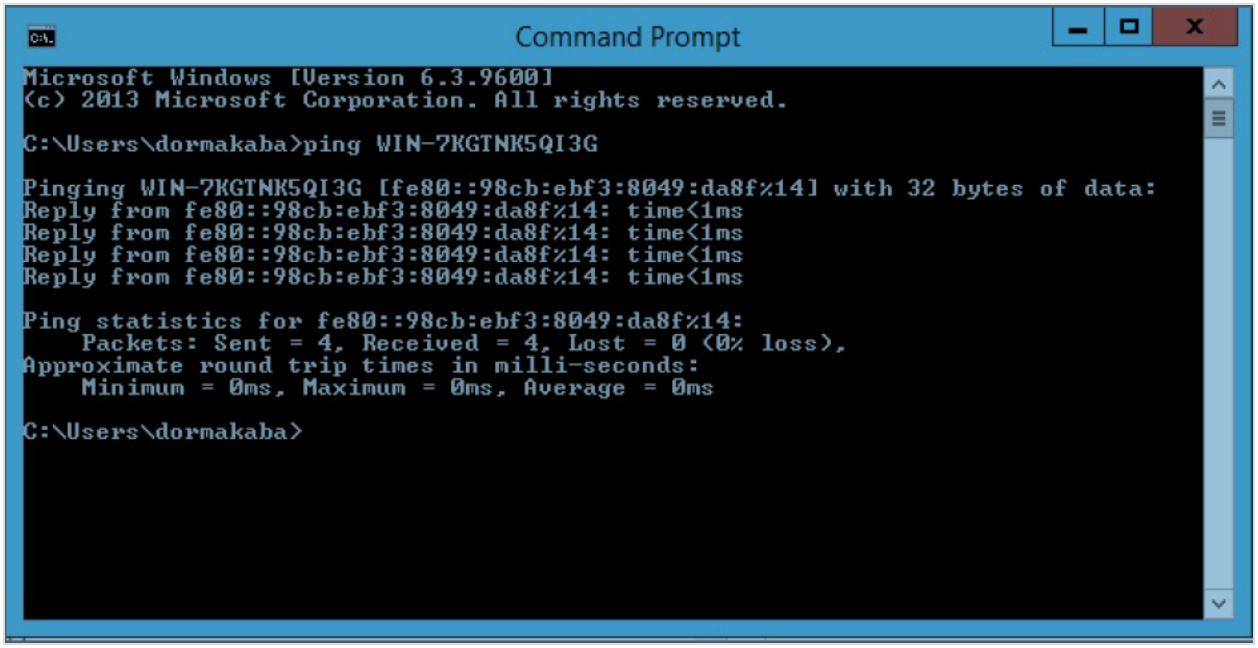
- If the card reader does not acknowledge the credential at all and power has been confirmed, check that the firmware supports the credential being used.
  - MIFARE DESFire credentials require the SRK firmware to be 11.10.23 or higher.
  - MIFARE DESFire credentials require the SRK-KPW and SRK-KPM reader firmware to be FW 18 APR 2024 or higher.
  - Please note that HH6 (Maintenance Unit) firmware 2.41 or higher should be used when updating the SRK firmware (Keypad readers do not allow for firmware updates in the field).
  - Firmware 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 the key synchronized with Aurora.
  - Make sure that the technician completed the default panel procedure shown previously.

5.2 Issues and actions

5.2.1 Verify Keyscan Aurora settings in Community:

Go to System Settings and verify the following options:

- Is the Aurora interface enabled?
- Does the username and password match the credentials used to administer Aurora?
- Is the Aurora IP address/server name correct? Click Test Connection .
- Open a Command Prompt and ping the server.
- Ensure available client licenses in Aurora software.



5.2.2 Verify application and services are running

If the Test Connection fails but you can ping the Aurora Server, verify application and services are running. If required, verify port connectivity to the Aurora IP address/server name.

Installing/enabling the Telnet Client requires Administrator privileges.

- To enable the Telnet Client on Windows Server

1. Open Server Manager.
2. From the Server Manager Dashboard, click Add roles and features, then click Next.
3. On the installation type page, select Role-based or feature-based installation, then click Next.
4. On the destination server, select a server from the server pool and make sure that the server where you want to install Telnet is highlighted.
5. The Telnet Client is a feature, so skip the Roles and click Next.
6. From the list of available features, select Telnet Client, then click Next.
7. On the Confirmation page, click Install. (Although the Telnet Client does not require restart after installation, you can optionally select to Restart the destination server automatically if required.)
8. Click Close.

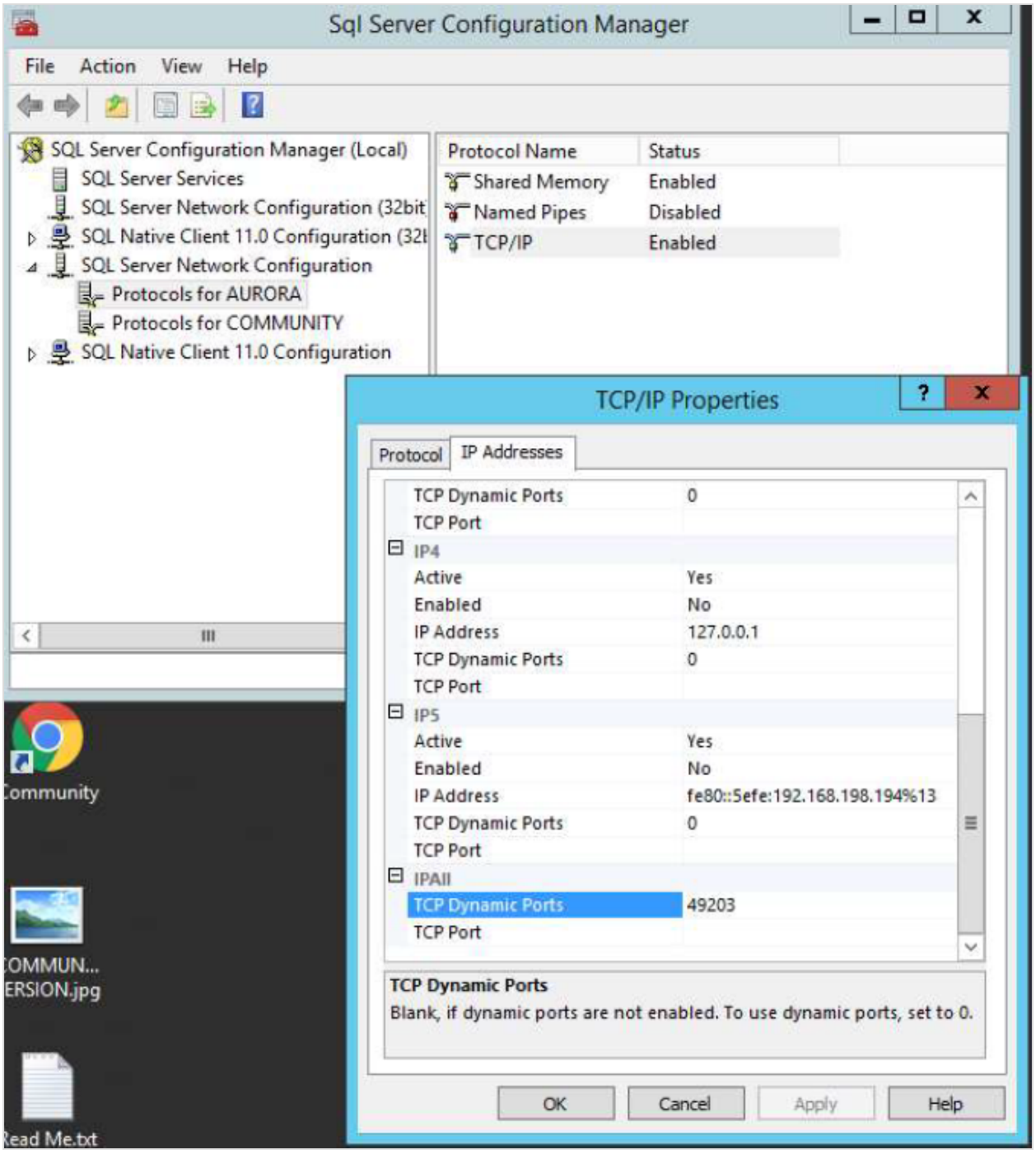
5.2.3 Verify network ports

Verify network ports are open (inbound rules are established for firewalls):

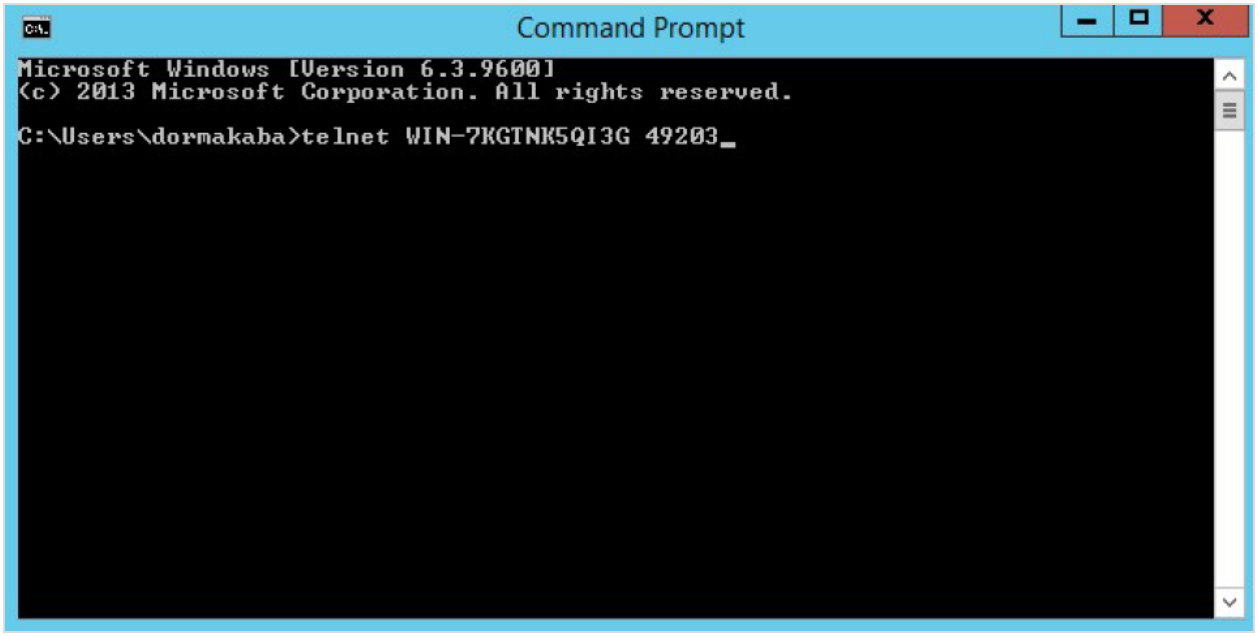
- Port 3001 for communications from Aurora to NETCOM devices
- Port 9999 for administering Telnet NETCOM devices remotely
- Port 1434 for SQL (UDP port)
- TCP/IP Dynamic port for SQL Server 2022 Express, used for Aurora Client software, Aurora communication and Community connectivity to the Aurora IP address/server.

1. From Windows, press the Windows key and the R key (Win + R) simultaneously.
2. In Run dialog box, enter SQLServerManager16.msc, then click OK. (If prompted to allow the program to make changes, click Yes.)

3. Under SQL Server Configuration Manager, expand SQL ServerNetwork Configuration and select Protocols for AURORA.
4. Double-click TCP/IP (located on the right).
5. Click the IP Addresses tab.
6. Scroll down to IP All and view the value for TCP Dynamic Ports.

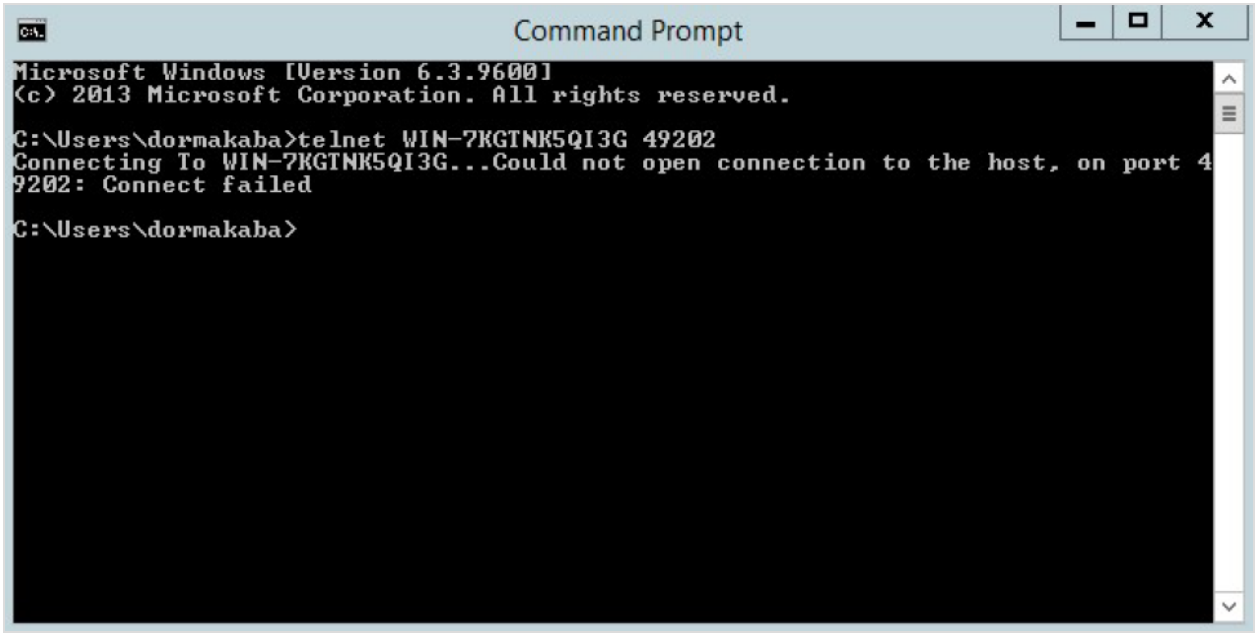


7. Open a Command Prompt and Telnet to the port to verify that it is open. Port 3001 can only be tested if the Aurora Communications service is stopped.



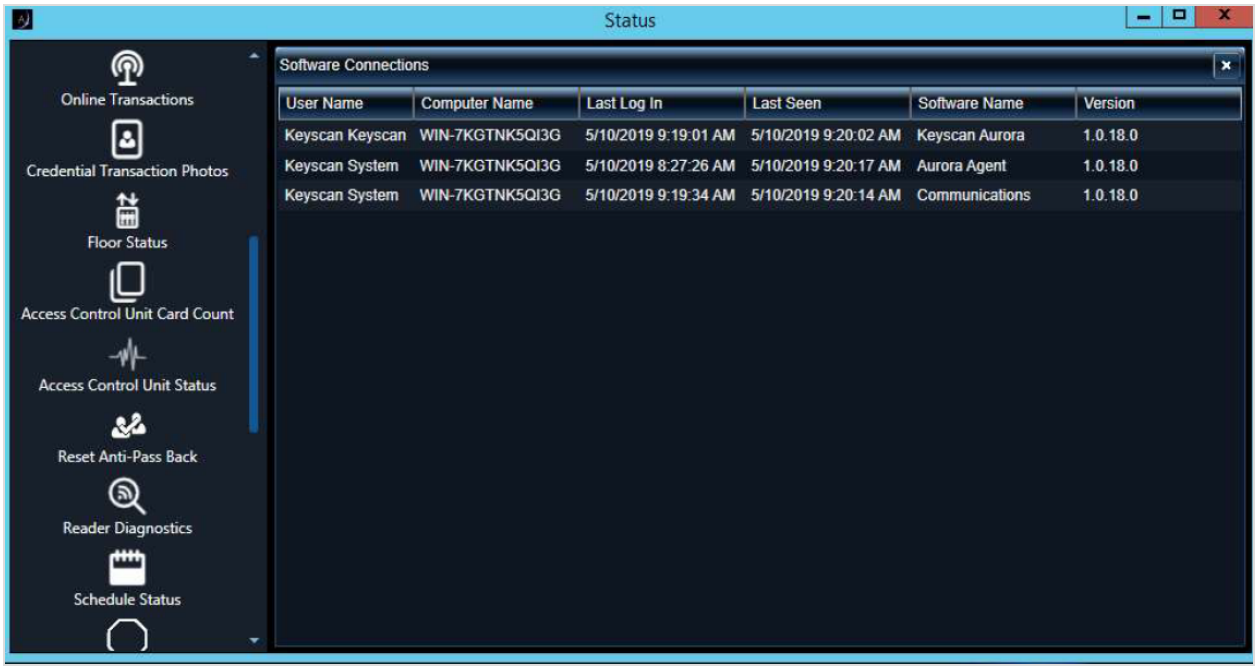
The following figure shows a successful connection.

The following figure shows a failed connection.



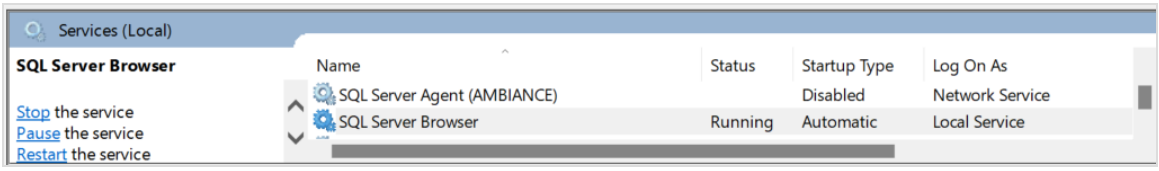
5.2.4 Verify Aurora services are running

1. In the Aurora Client, go to Status > Status.
2. On the left, double-click Software Connections Status (if not already open).
3. Under Software Name, there should be Keyscan Aurora, Aurora Agent and Communications.
4. Last seen should be updating with server time.



5.2.5 Verify SQL Server Browser service is running

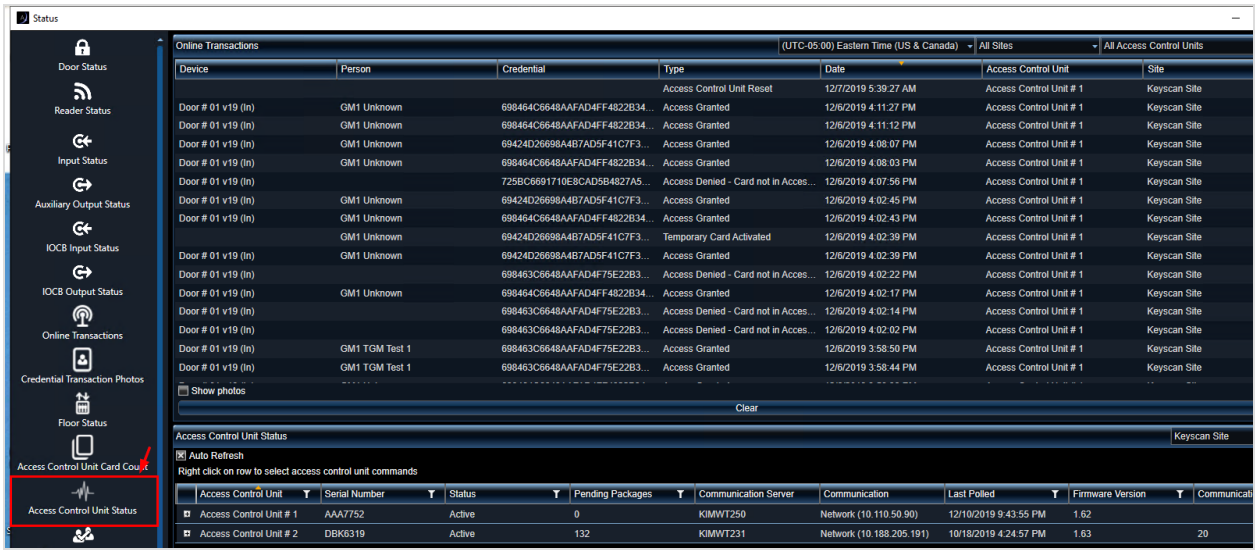
In Windows Services, ensure that the SQL Server Browser service is running.



5.2.6 Verify Aurora hardware

Verify that Aurora hardware is communicating successfully:

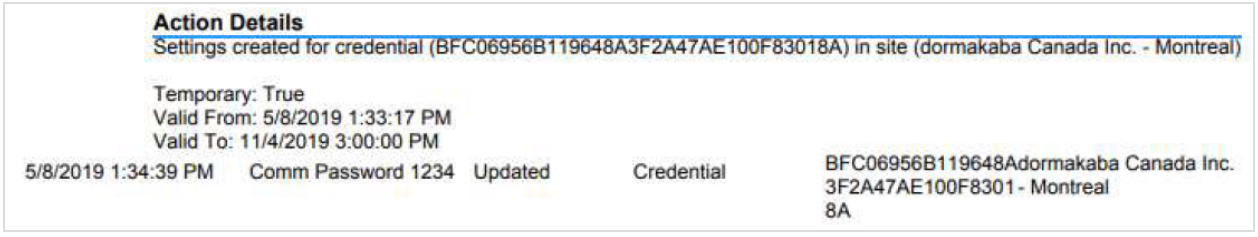
1. In the Aurora Client, go to Status > Status.
2. On the left, double-click Access Control Unit Status (if not already open).
3. Verify that the panels are Active, that the pending packages are either 0 or counting down, and that the Last Polled is updating with the current date/time.
4. Most importantly, verify that there are no communication errors. If there are numeric values, then a possible communication problem exists between the Aurora communication software and the Aurora panels. Contact your Aurora integrator for support.



5.2.7 Run an Aurora system log report

The System Log Report lists entries and actions made by system users, such as Community logins and logouts for sending data to Aurora, and any keys which are cut and sent to people added to Aurora.

- In the Aurora Client, go to Reports > System Log Report. The following figure shows a System Log Report.



5.2.8 Verify keys/people are added

Verify that keys and/or people have been added:

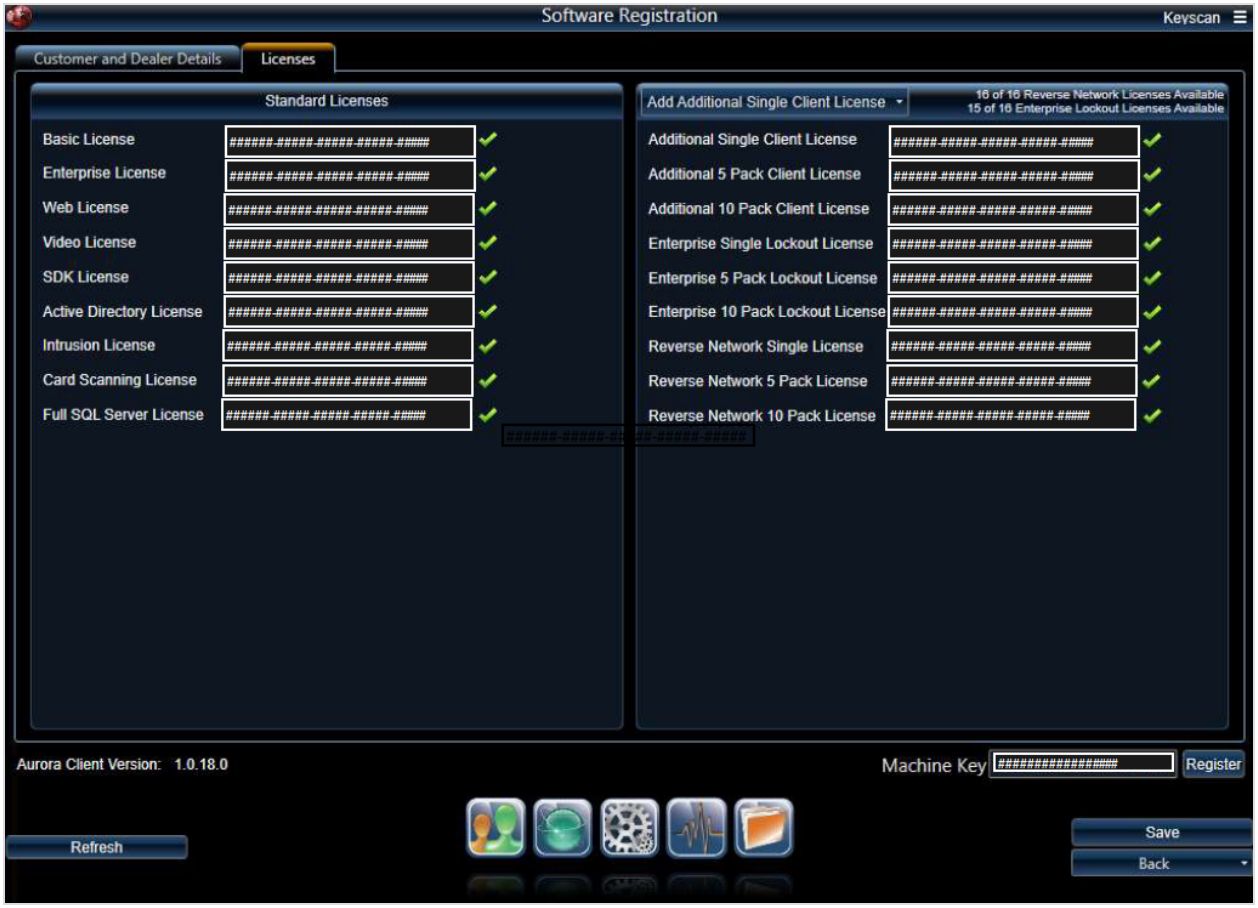
1. In the Aurora Client, go to Manage People > Manage People.
2. Search for the name of the key/person.

3. Double-click the entry and verify if data failed to reach the database, or if the search results are empty. Transactions are listed on the Transactions tab, if key/person exists. The following figure shows a successful entry.

5.2.9 Verify registration

Verify registration for basic license and SDK license:

1. Open the Registration screen.
2. Select Application management > Software Registration.
3. Click the Licenses tab.



5.3 Technical support

The Aurora-S integration comes with limited telephone technical support. There is no charge for four events of up to 15 minutes in duration each. Unused technical support expires 30 days from the date of the first event or after six months from the date of purchase.

Additional support can be purchased (Part #AURSAFA). This package includes a maximum of four events of up to 15 minutes in duration each. Technical support that is unused expires after 30 days from the date of the first event or after six months from the date of purchase. This package can only be purchased directly from dormakaba Canada on account or by credit card (Mastercard and Visa).

For issues with registration, contact dormakaba Canada Inc. between 9AM and 5PM, EST:

- toll-free (USA/Canada) 1-888-KEYSCAN (539-7226)
- Tele: 1-905-430-7226

For all other issues, contact Multifamily Housing Technical Support:

- Tele: 1-800-849-8324, choose option 3
- EMail: mhtechnicalsupport.us@dormakaba.com

PK3769-EN 2.1.1 - 09/2025
Copyright © dormakaba 2025

www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
Canada
T: +1 866-367-6252

www.dormakaba.com