Synology

Access Control in Surveillance Station 9.0 and above

Last Mar 28, 2024

Table of Contents

Introduction

What Is Access Control

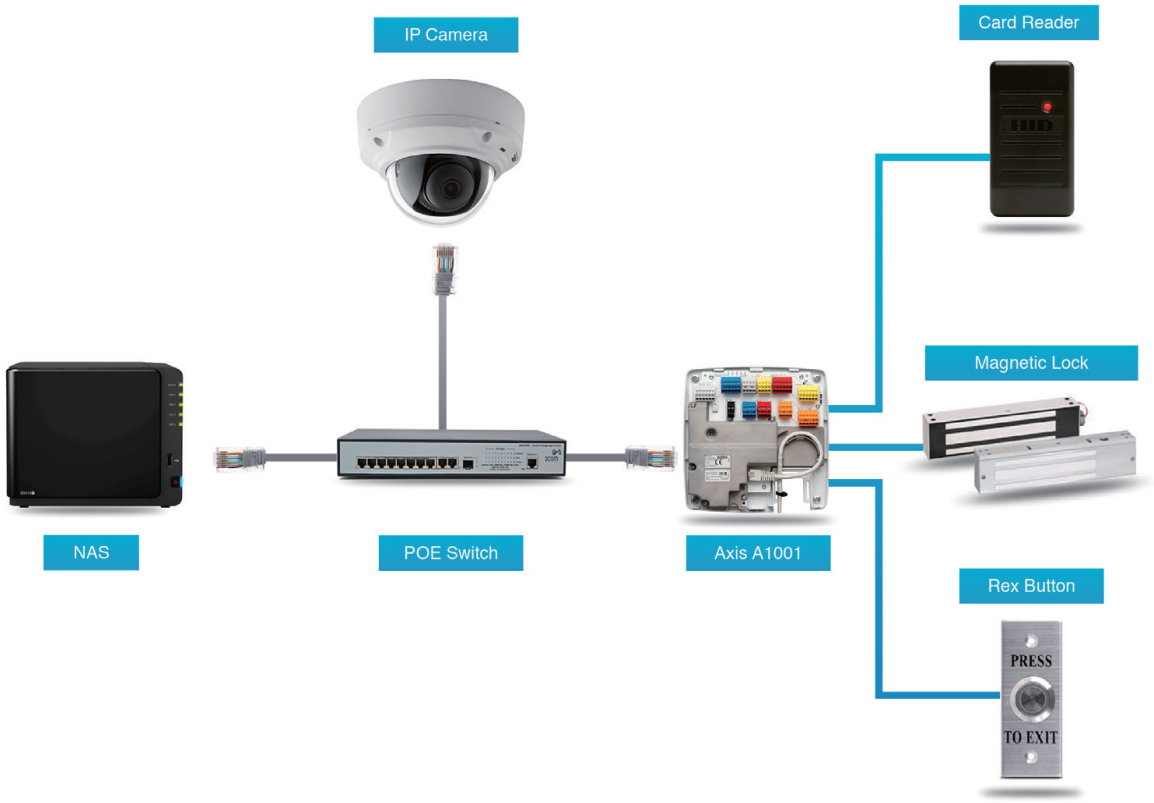
The growth of internet-connected devices has had an immense effect on many parts of our lives, including surveillance. Network cameras are a prime example of this shift, as they provide remote monitoring and a more simplified experience than traditional wired systems. They represent a substantial advancement in surveillance technology by removing the complications involved with outmoded analog signals.

This shift in internet connectivity is also altering access control systems, which have traditionally operated as standalone components inside a larger security architecture. Access events and user authorizations were formerly recorded and stored within the system, frequently on a separate server, for future reference. However, manufacturers now include network capabilities in access controllers, allowing remote management and data access. This departure from the traditional standalone architecture has the potential to provide greater flexibility and efficiency in security and access management.

A typical access control system includes a database server, a card reader, door locks, and, optionally, a lock monitor and a Request-to-Exit (REX) button. Access credentials dictate who has access to which doors and when. These settings, such as which users (e.g., receptionist, security guard) can unlock specific doors with their cards, are usually maintained and monitored on a central database server.

Network door controllers, which allow administrators to remotely manage doors, are part of an emerging trend in networking hardware. Surveillance Station integrates seamlessly with Synology NAS systems, transforming the NAS into a central access control server. This integration allows for complete management of all access-related actions from within the standard Surveillance Station interface.

Reasons to use AXIS door controllers with Synology Surveillance Station



The AXIS A1001 and A1610 are network door controllers equipped with multiple analog I/O ports and an Ethernet port for local network connectivity. Integrating these devices with Surveillance Station streamlines access management by combining it with existing video sources configured on the NAS. This integration allows Surveillance Station to retrieve access logs from the AXIS door controllers and automatically pair them with the corresponding video recordings. This feature enables administrators to easily review access data alongside relevant video footage, maximizing the value of stored logs and consolidating security information within a single interface.

Here are some key advantages of using AXIS door controllers with Synology Surveillance Station.

- Easy to deploy and install through UPnP search in Surveillance Station.
- Pairing cameras with doors enables a clear view when monitoring entrances and exits.
- Intuitive user interface allows easy configuration of cardholder, door access schedules and access rules.
- Attaching photos and common information to cardholders allows administrators to easily check for cardholder fraud.
- Instant playback of relevant video when clicking on the access logs.

For more information on the maximum number of supported door controllers, cardholdres, and events, refer to this page.

Adding access controllers to Surveillance Station requires installing additional Surveillance Device Licenses.

	Number of required licenses

AXIS A1001	1
AXIS A1610	1 or 2 (depending on the number of doors configured)

Configure hardware configuration for AXIS Door Controllers

The AXIS A1001 and A1610 are network-connected door controllers designed to manage access control for your security system. They feature multiple built-in I/O ports that allow you to connect various analog devices, such as magnetic door locks, lock monitors, and card readers, to your network. Each controller can manage up to two doors, including associated locks, monitors, readers, REX buttons, and other I/O devices.

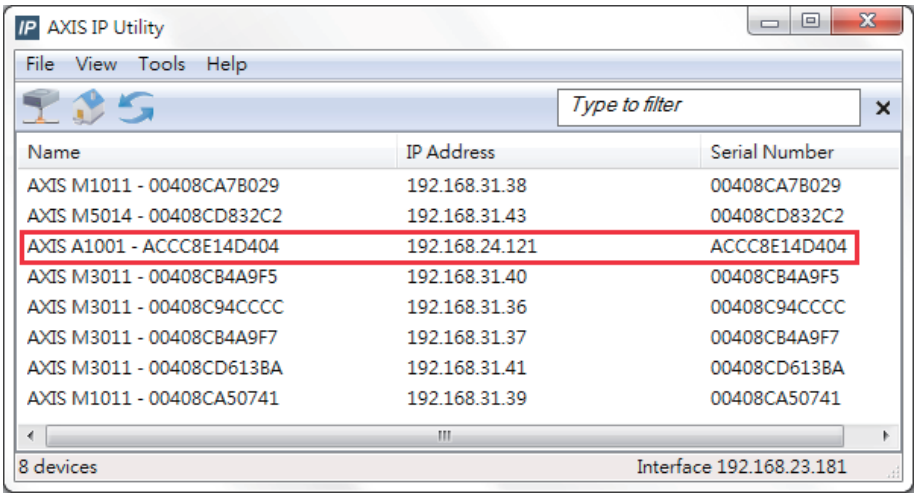
Before installing the AXIS A1001/A1610 with Synology Surveillance Station, go to its web user interface to configure the following settings.

Before you begin

- The AXIS A1610 is compatible with Surveillance 9.2 and above.
- The AXIS A1001 is compatible with Surveillance 7 and above.
- For information about configuring AXIS door controllers with Surveillance Station 7 and 8, please see this white paper.

Find your AXIS door controller

Use the **AXIS IP Utility** or **AXIS Device Manager** to find the AXIS A1001/A1610 in your local network.



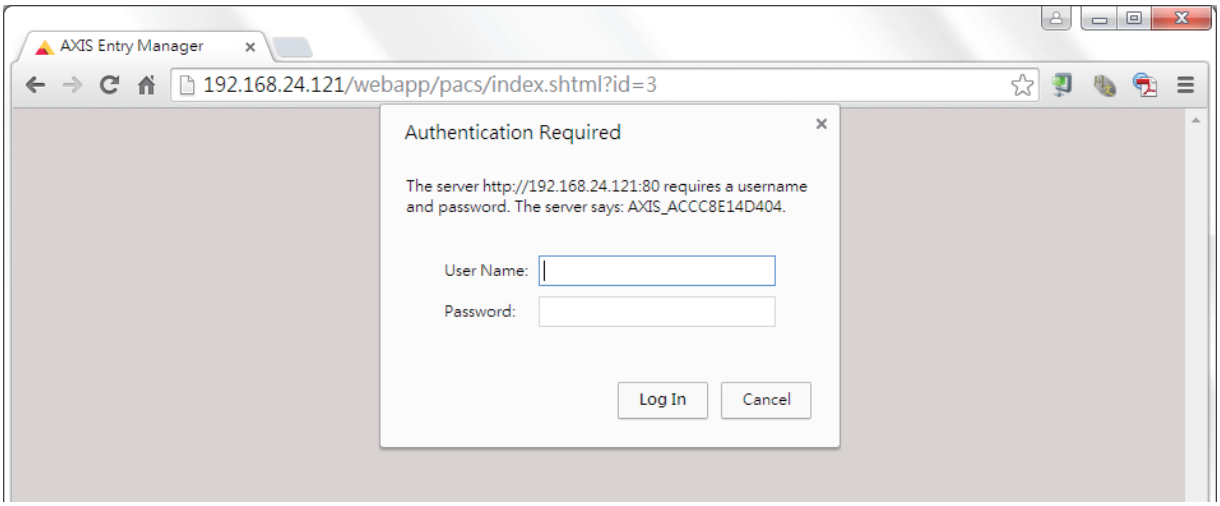
Sign in to your AXIS door controller

To sign in, go to the IP address of the door controller and enter the default username and password.

- **AXIS A1610**: There is no default password. You will be asked to configure a password for the **root** account.
- **AXIS A1001**: **root/pass**.

Update the firmware (AXIS A1610 only)

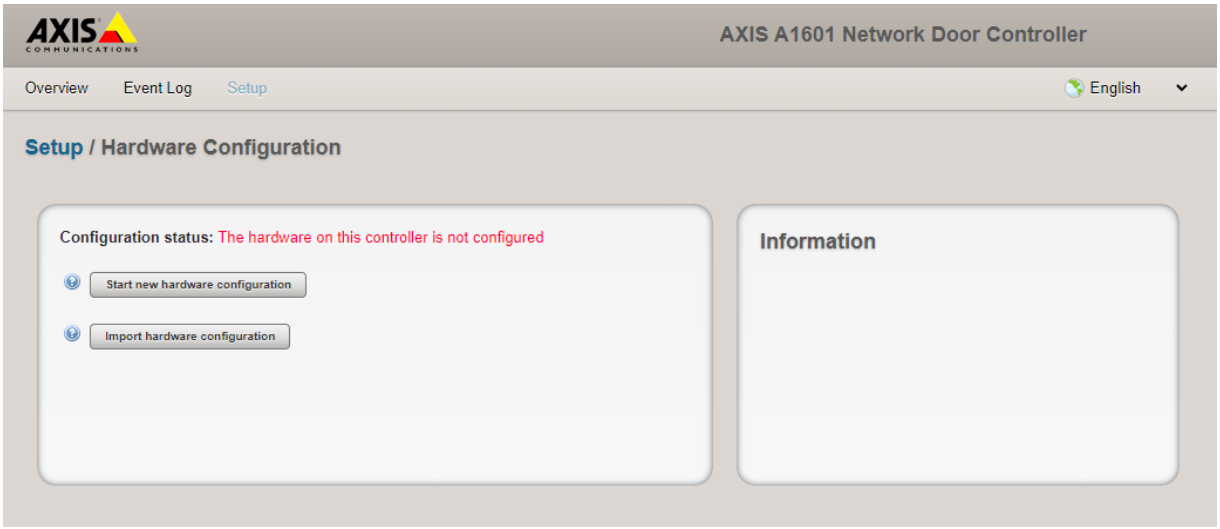
For compatibility between Surveillance Station and the AXIS A1610, installation of the VAPIX firmware is required. Download the VAPIX firmware and update the door controller's firmware at **Maintenance** > **Firmware upgrade**.



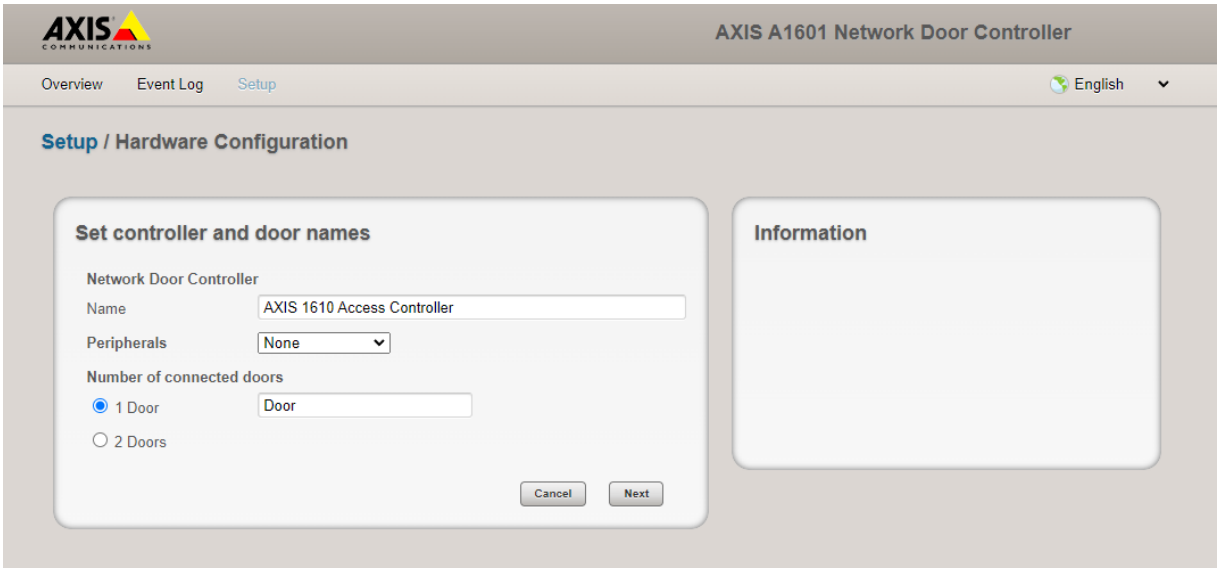
Configure hardware

After updating the firmware (if required), go to https://controller IP address:port/webapp/pacs/index.shtml?#overview and sign in. (Using only the door controller's IP address will not bring you to this page.)

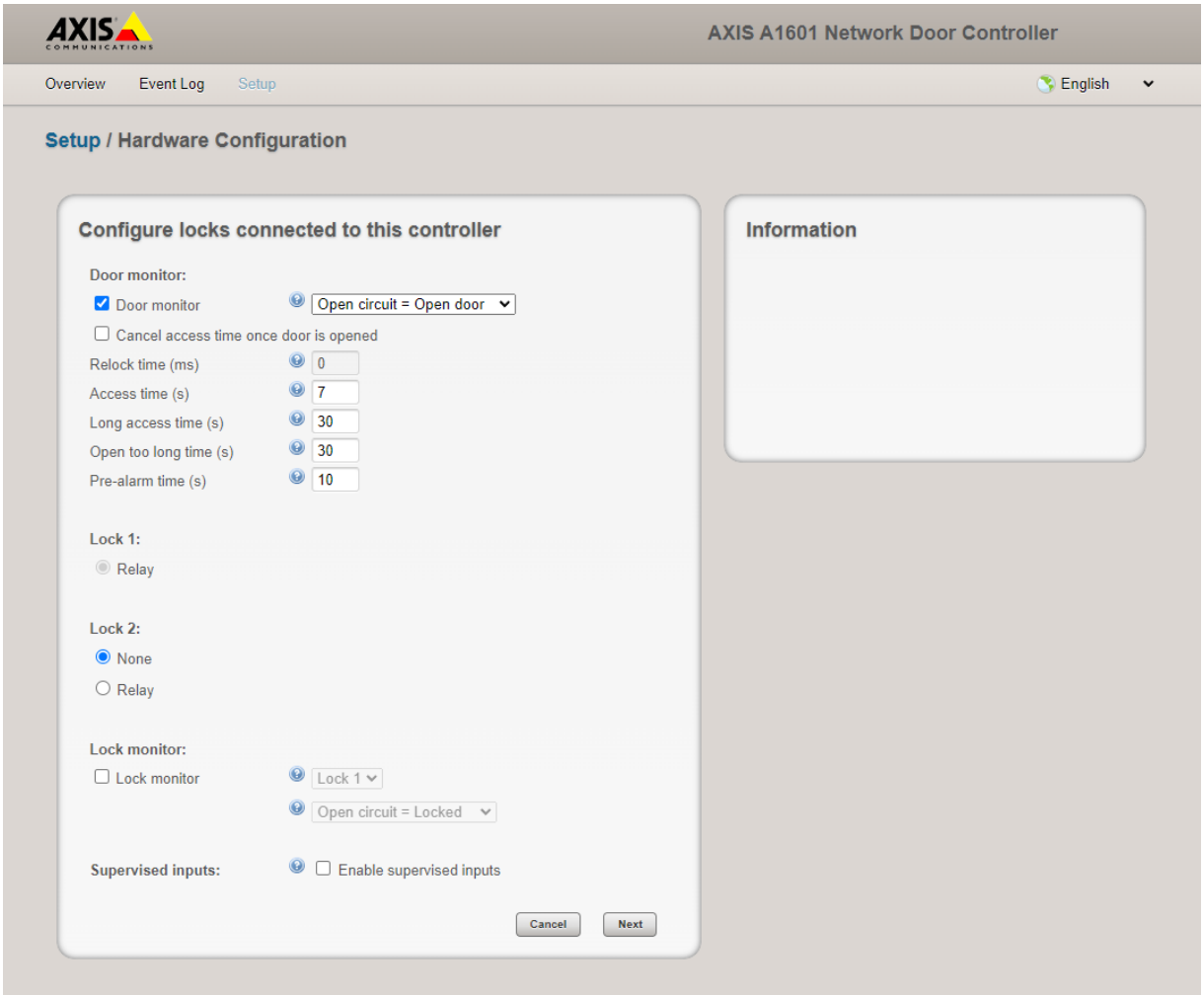
Click on **Start new hardware configuration**. You can also import an existing hardware configuration file. In this example, we will **Start new hardware configuration**.



Specify the name and select the number of doors that needs to be configured. In this example, we will assume there is only one door.



Next, go to **Configuring locks connected to this controller**



For most general setups, you only need to verify the following settings:

- **Access time**: Set the time duration (in seconds) the door will remain unlocked after access has been granted. (This setting can be modified afterwards.)

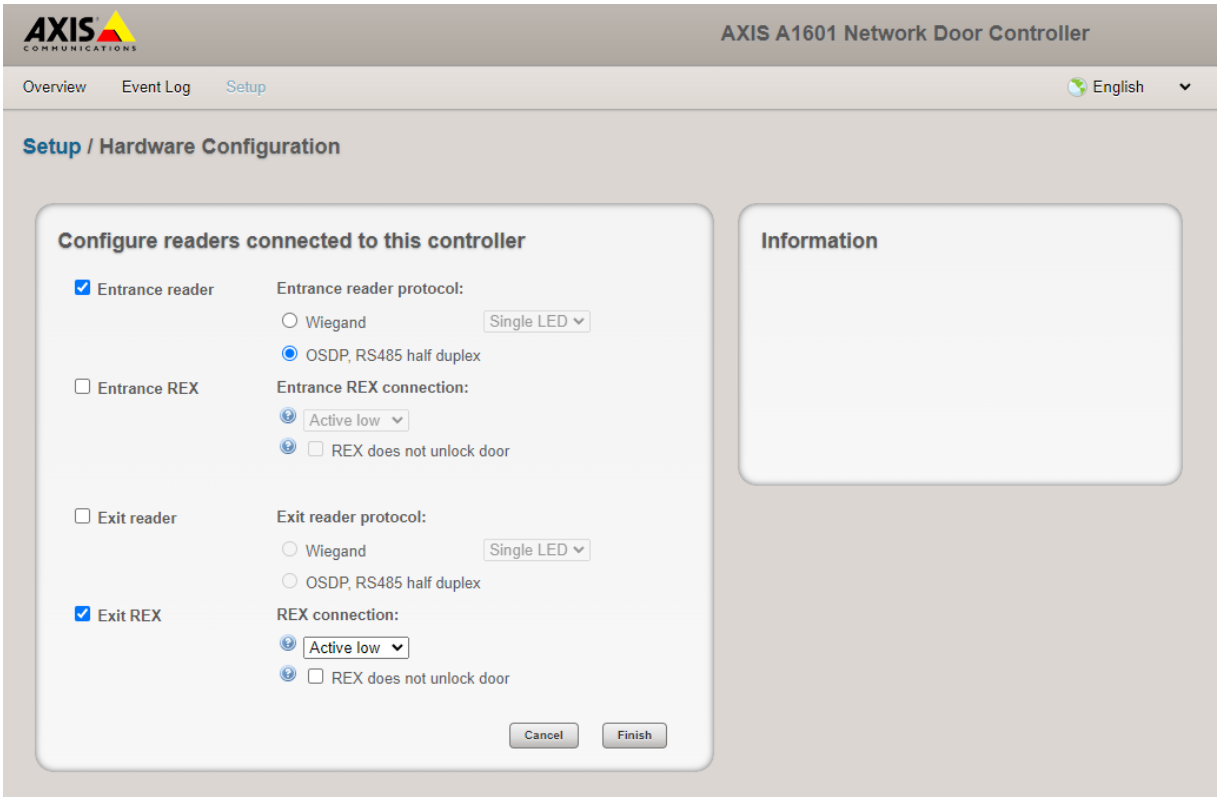
- **Long access time**: Set the time duration (in seconds) the door will remain unlocked after access has been granted. Long access time overrides the already set access time and will be enabled for users with long access time selected.
- **Open too long time**: Set the time duration (in seconds) the door is allowed to stay open before triggering an alarm.
- **Pre-alarm time**: Set the time duration (in seconds) before the actual alarm is triggered.

Under Lock 1 and 2, select a lock circuit option.

- For AXIS A1610, select **Relay**.
- For AXIS A1001, select **12 V** :
  - **Fail-secure:** The door will remain locked when the AXIS door controller is offline.
  - **Fail-safe:** The door will remain unlocked when the AXIS door controller is offline.

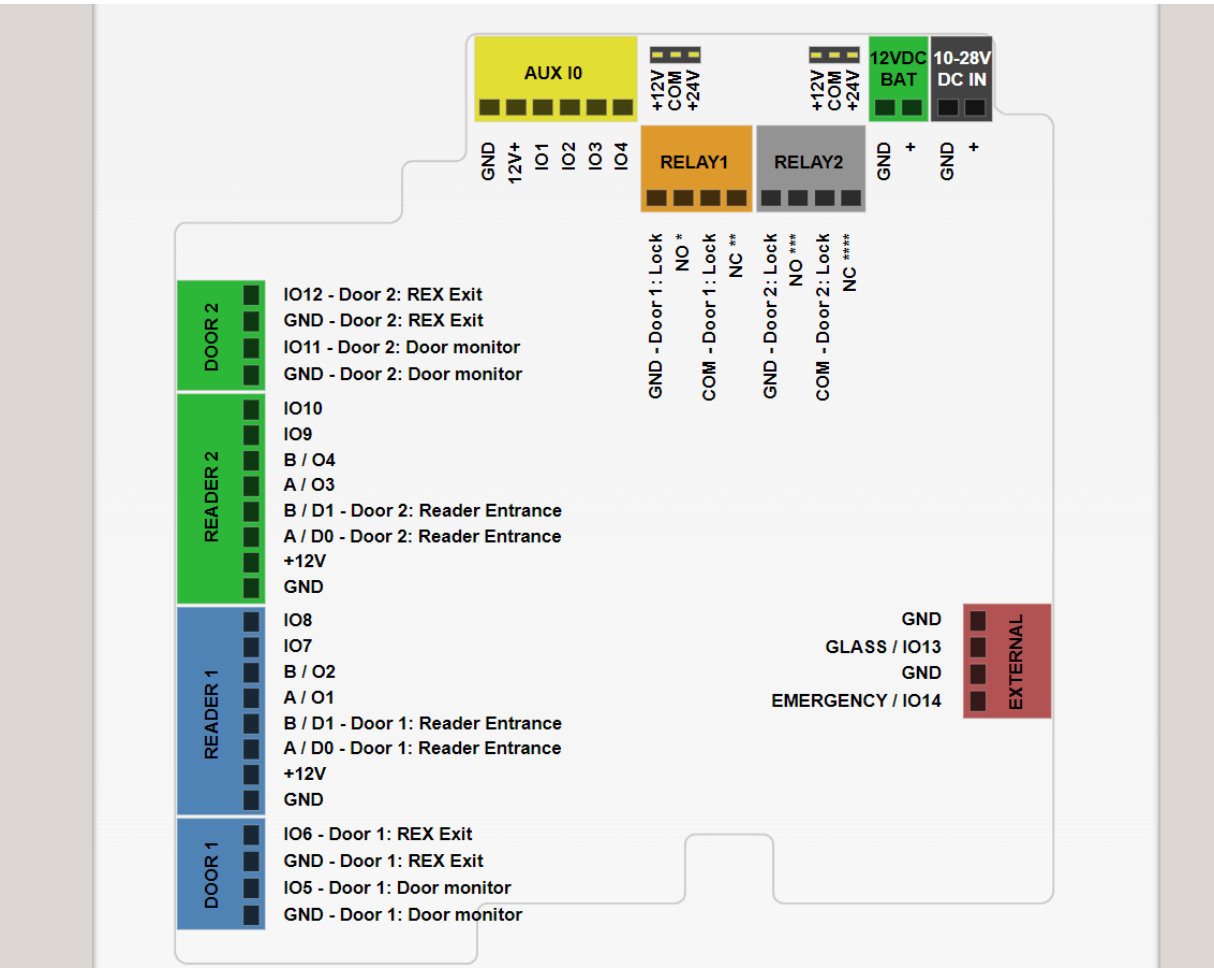
If a lock monitor is installed, enable the **Lock monitor** option. Under general circumstances you can select **Open circuit = Locked**.

Card reader configurations depend on the devices used at the entrance and exit. For example, if your organization is using a card reader at the entrance and a REX button at the exit, you can enable **Entrance reader** and **Exit REX**.



When the hardware configuration is complete, refer to the hardware pin chart for detailed connection information regarding all connected analog devices such as card readers, door locks,

lock monitors, and other I/O devices



Ensure all devices are connected correctly to the controller according to the chart. Once the physical installation is complete, proceed to add the door controller to Surveillance Station for configuration and future management.

Configure AXIS Door Controllers in Surveillance Station

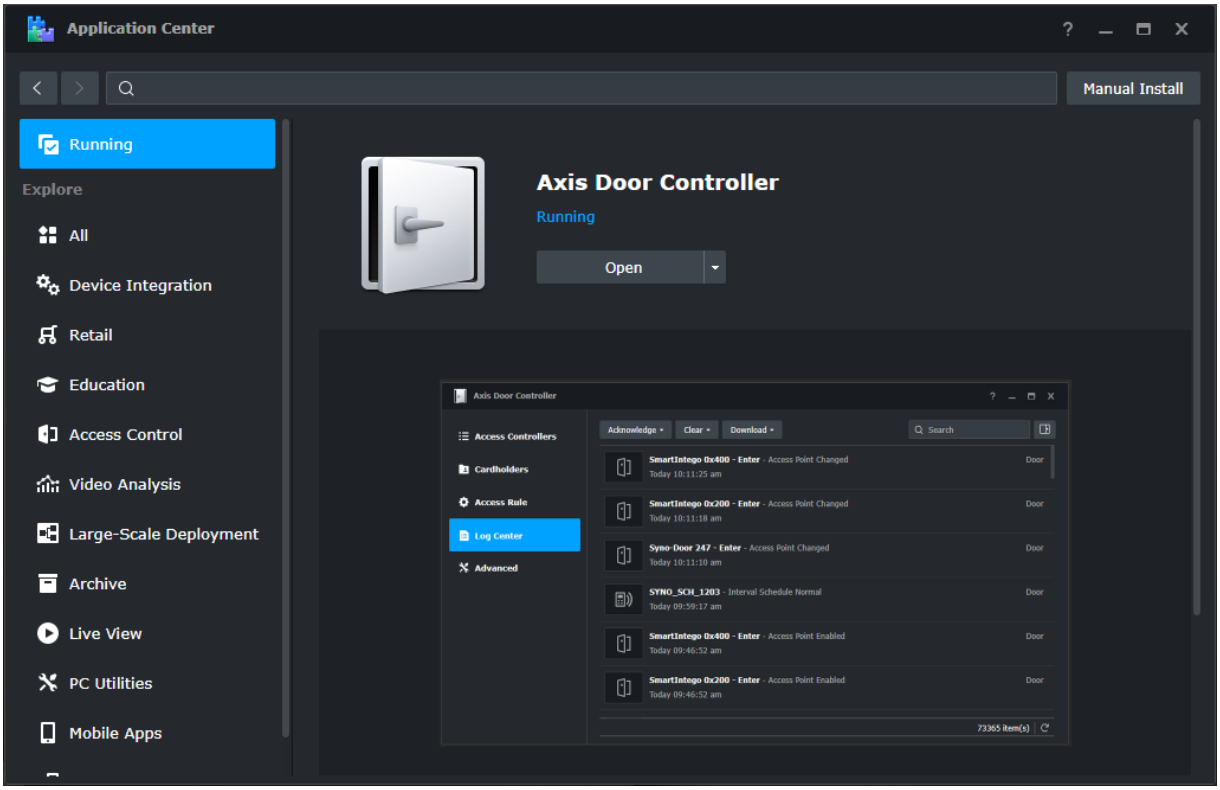
AXIS Door Controller is an optional package for Surveillance Station designed to support AXIS A1001 and AXIS A1610.

Note:

- AXIS A1610 is compatible with Surveillance Station 9.2 and above.
- AXIS A1001 is compatible with Surveillance Station 7 and above.

Add a door controller

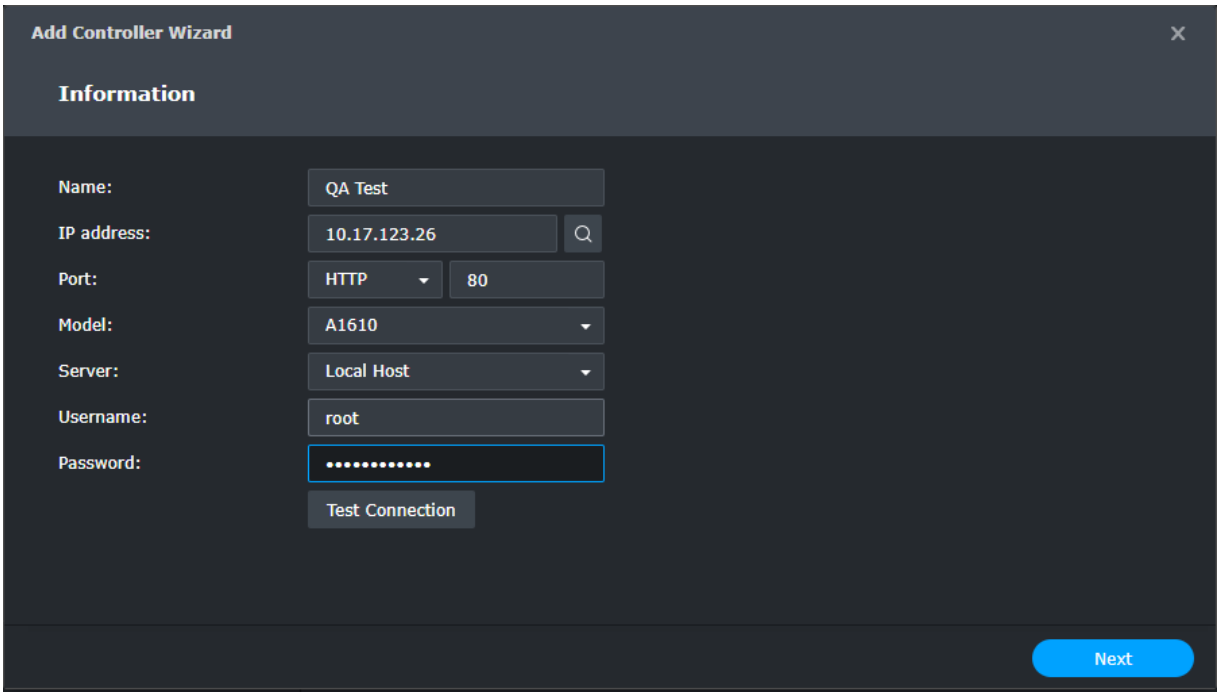
Go to **Application Center** and install AXIS Door Controller.



After installation, launch the Axis Door Controller application and click **Add**.

Follow the steps in the setup wizard and specify the basic information of your AXIS door controller. You can also use the search function to find the AXIS door controller located in your

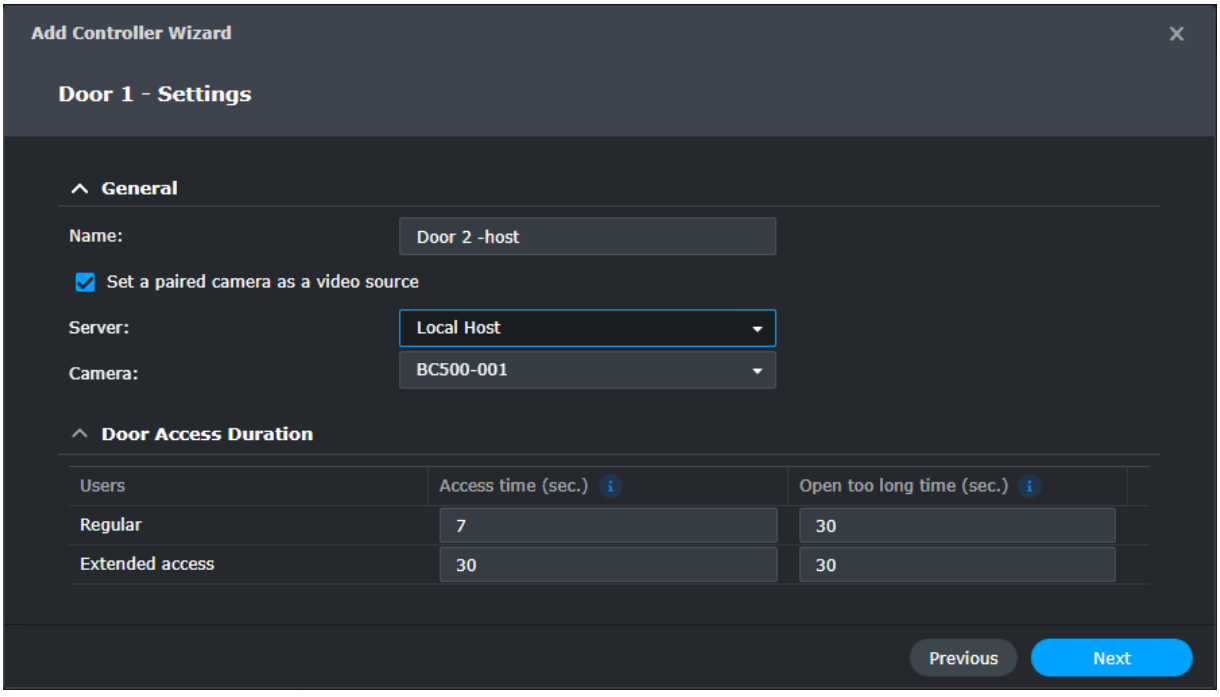
local network.



You can further adjust additional settings for each door configured on this controller. Doors configured in Surveillance Station can be paired with an IP camera. This enables events at those doors to be clearly recorded.

All Surveillance Station supported cameras (not required to be AXIS cameras) added on your NAS can be paired with the door controller.

You can also specify how long the door can remain open before the alarm is triggered, i.e., the access duration. The access duration can be configured separately for each door based on individual requirements. **Extended access** allows doors to remain open for longer than the original duration. This feature is useful for accommodating individuals with mobility limitations or facilitating the movement of goods by logistics personnel.



In addition to pairing a camera, you also need to configure access authentication (for both entrance and exit) for each door. A REX schedule, a schedule for readers, or both may appear, depending on whether one was configured during the hardware configuration process.

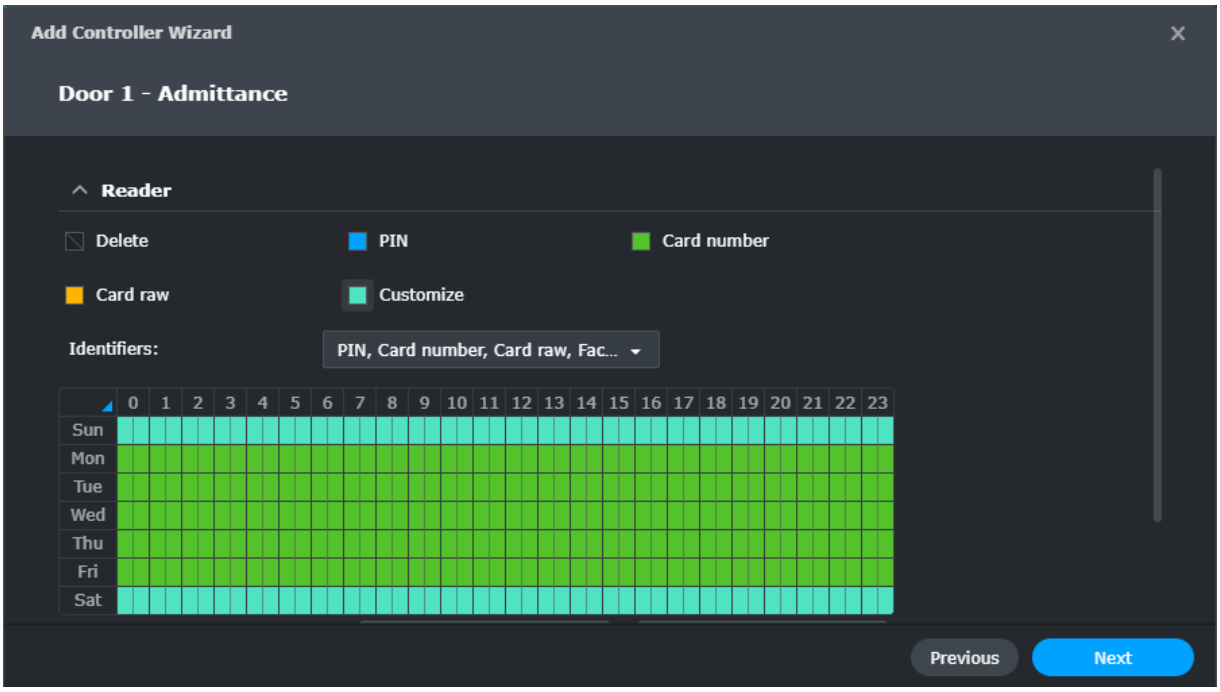
In this example, a reader is used for the entrance. Accordingly, you will need to specify the authentication type and configure an access schedule to define when and how this reader will operate.

A company may require the use of a card for entrance access checks, and on weekends, an additional PIN for higher-level security. To achieve this, on the admittance schedule, you will need to specify a **card number** for Mondays to Fridays as the identification type, and select **Card number + PIN** for weekends.

Multiple identification types are allowed. Reader PIN lengths are 4 digits by default and can be adjusted up to 32 digits as required.

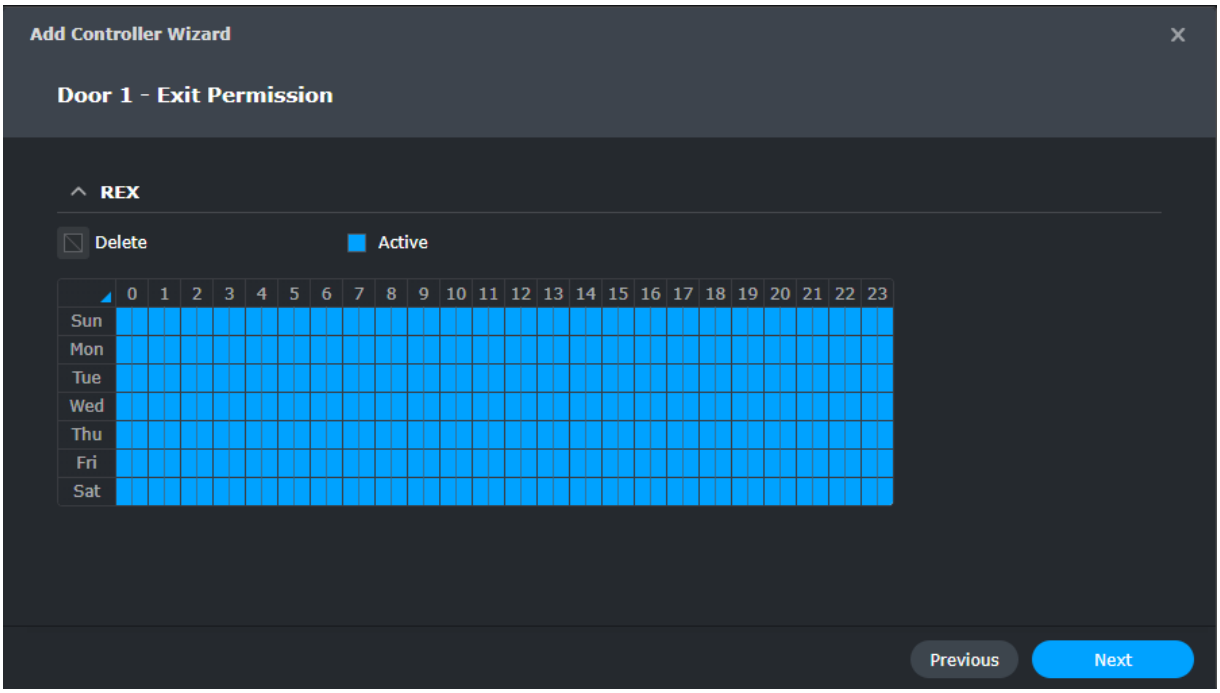
Note:

- Adjusting the PIN length requires a reader that supports custom PIN lengths. For more compatibility information, contact the reader manufacturer.

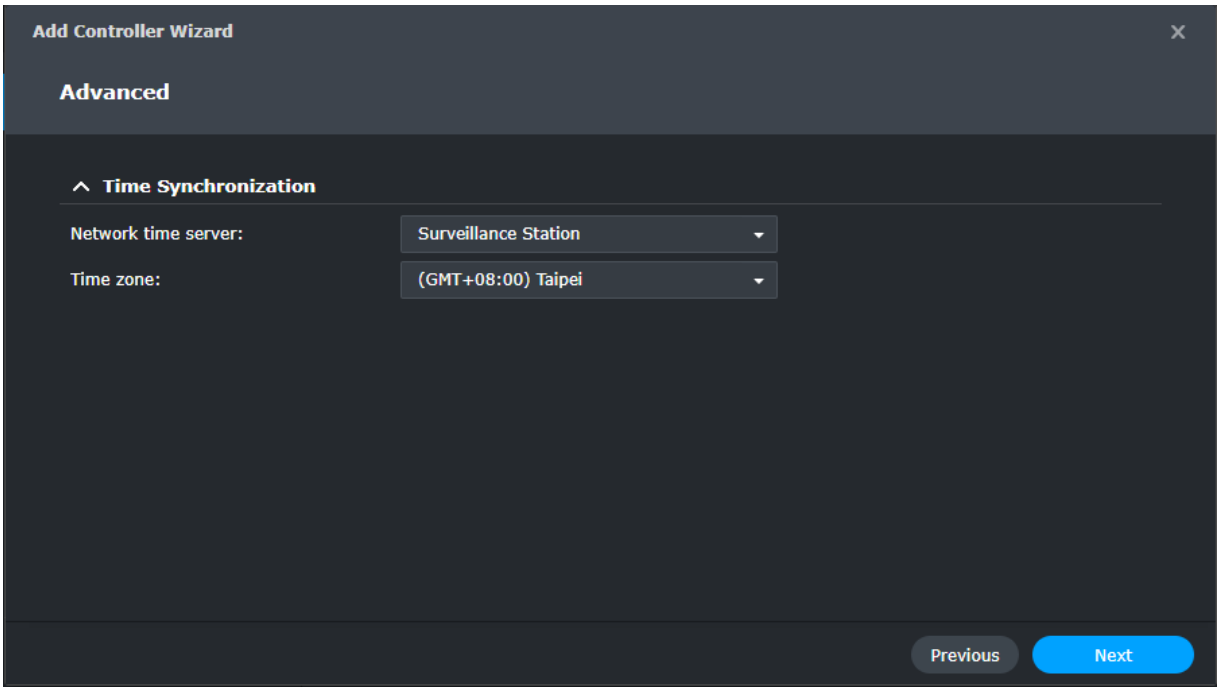


Exit permissions can be similarly configured in the next tab. In this example, a REX is used for the exit. Therefore a schedule must also be configured to determine when this REX will function. Deleting the schedule prevents the door from unlocking during that time period, even if users

press the REX button.



The AXIS door controller needs to be synchronize with an NTP server; you can choose to use Surveillance Station as the NTP server or specify another.

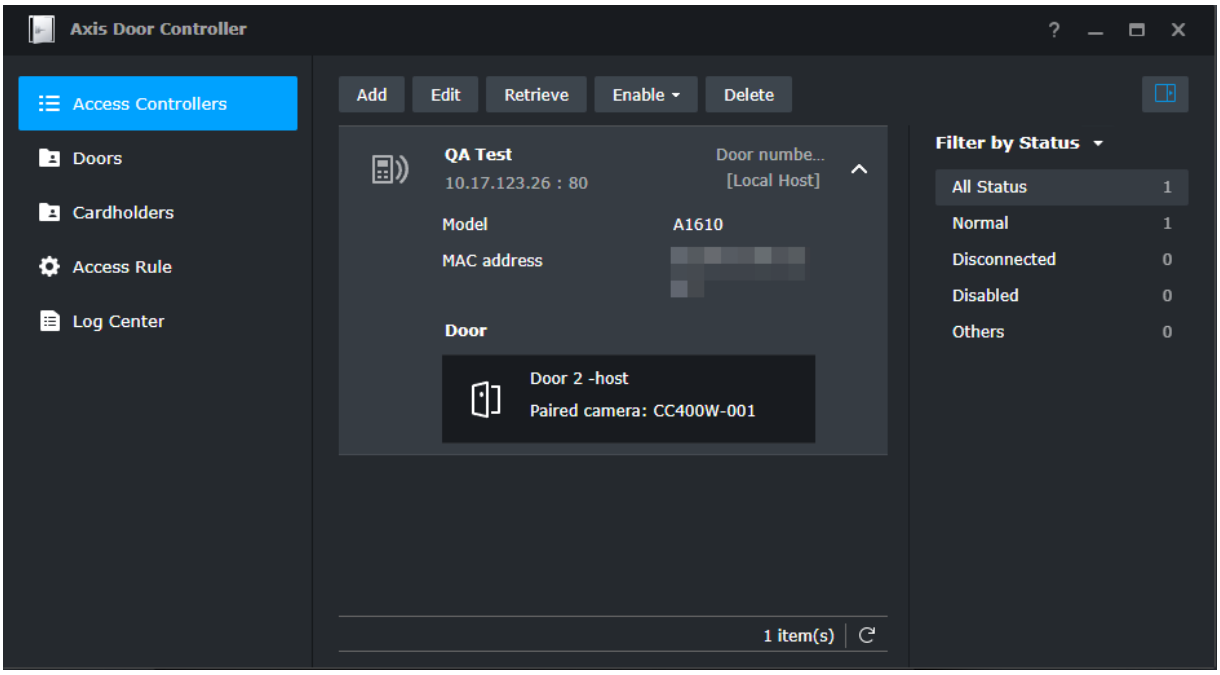


After completing the configuration, the doors that were configured in the process will be visible in the AXIS Door Controller application. The following management options are available: **Access Controllers**, **Cardholders**, **Access Rule**, **Log Center**.

Manage access controllers

All door controllers added to Surveillance Station can be viewed and managed on the **Access Controllers** page. Clicking on the door icon will allow you to preview footage of the paired

camera.

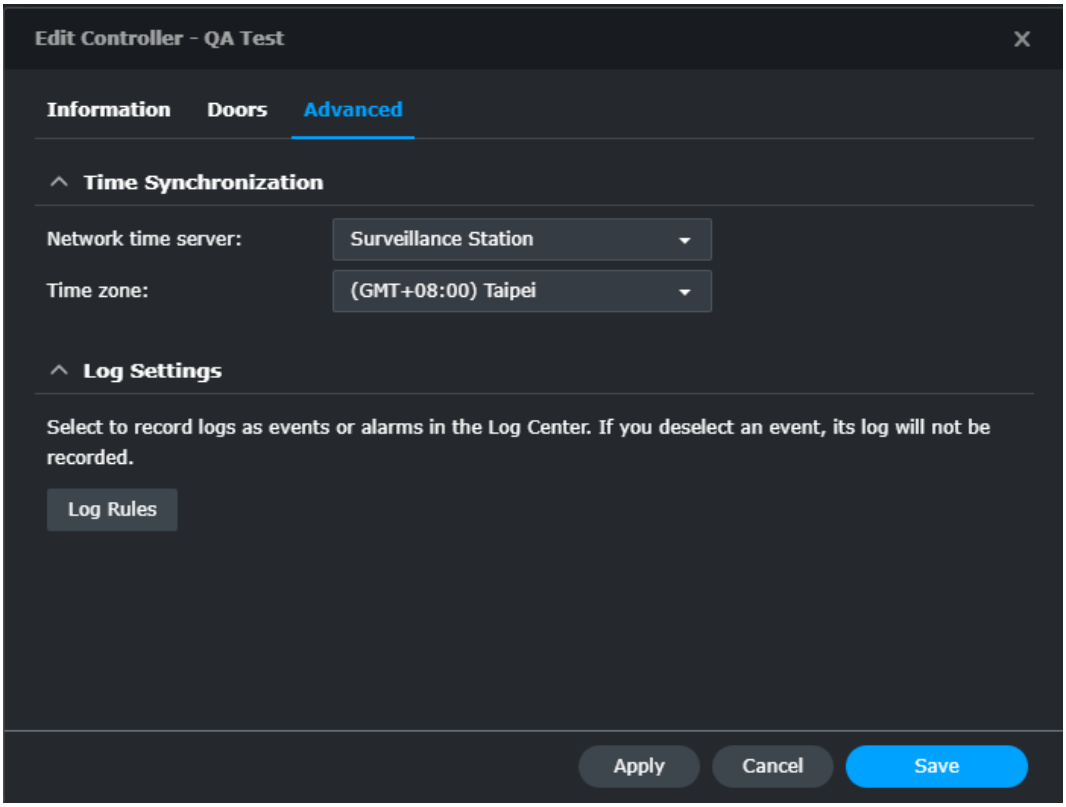


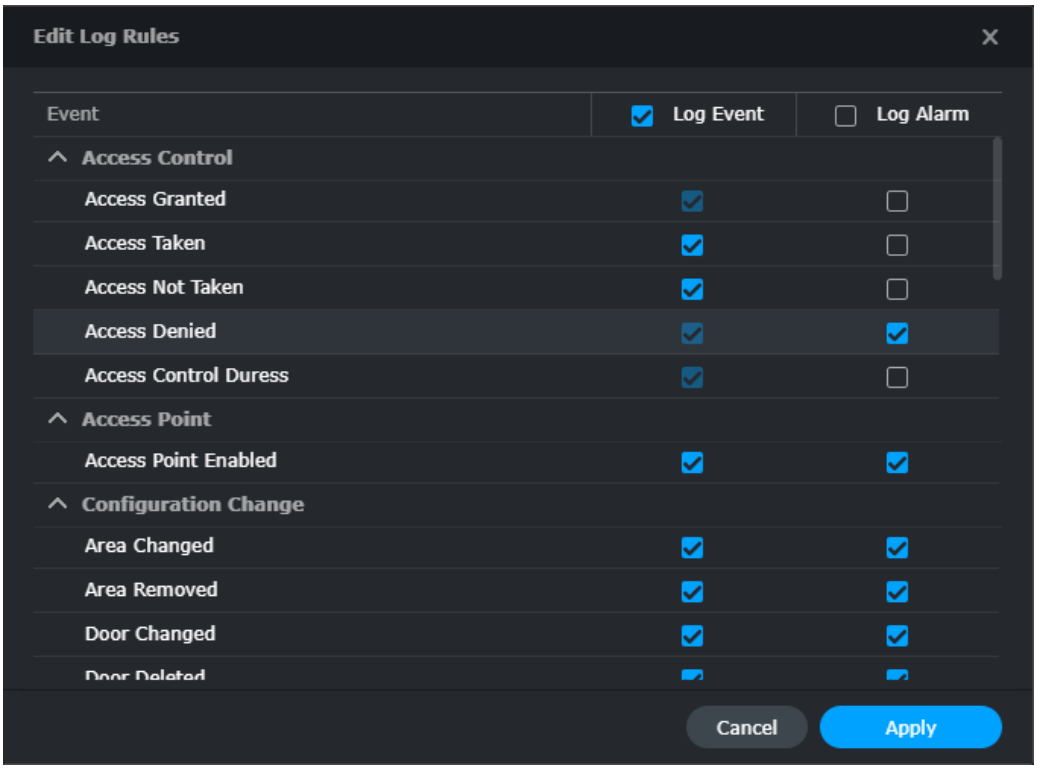
As AXIS door controllers are separate devices from Synology NAS, Cardholder and Log data are synchronized bidirectionally during the installation.

During synchronization, the device status of the controller will be shown as activating. It is recommended to refrain from editing or deleting of the controller, cardholder, and log during this period. Activating these operations will interrupt the synchronization processing, requiring it to start over. After adding the controller to Surveillance Station, it's best to make any changes in Surveillance Station instead of on the device's configuration page.

Configure event and alarm logs

Log settings can be configured by going to **Access Controllers** > select a controller > **Advanced** > **Log Settings** > **Log Rules**.



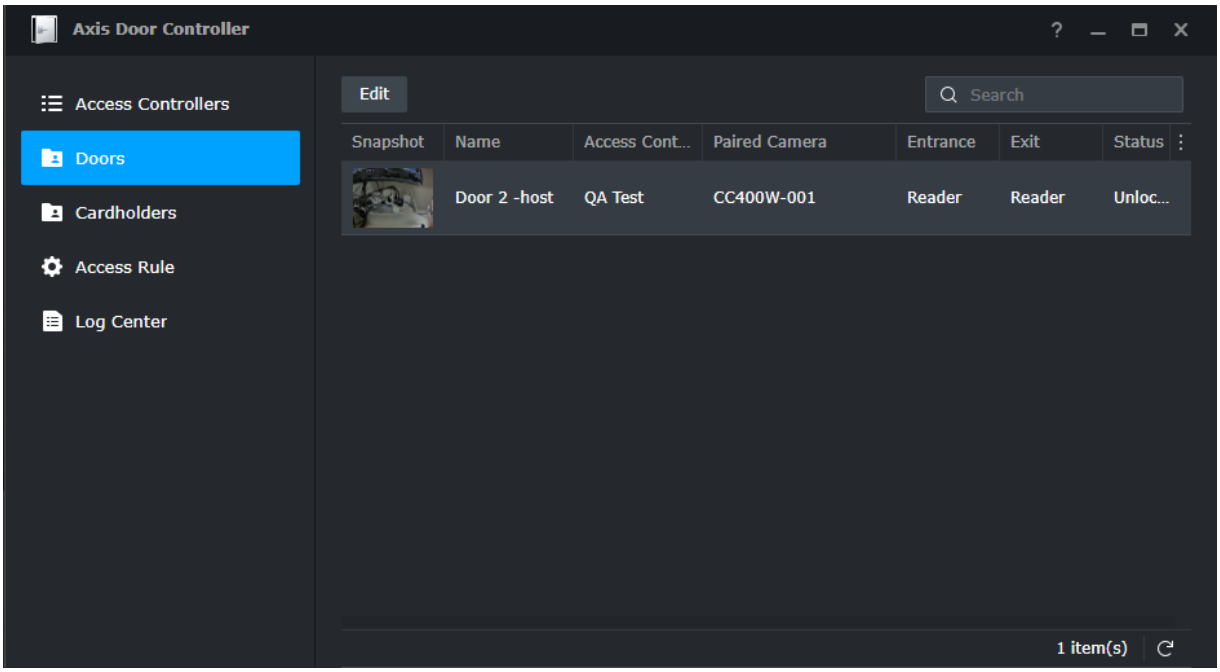


Administrators can activate or deactivate specific events from being logged. Additionally, if you want specific events to be marked as alarms, select the checkbox under Log Alarm for those events.

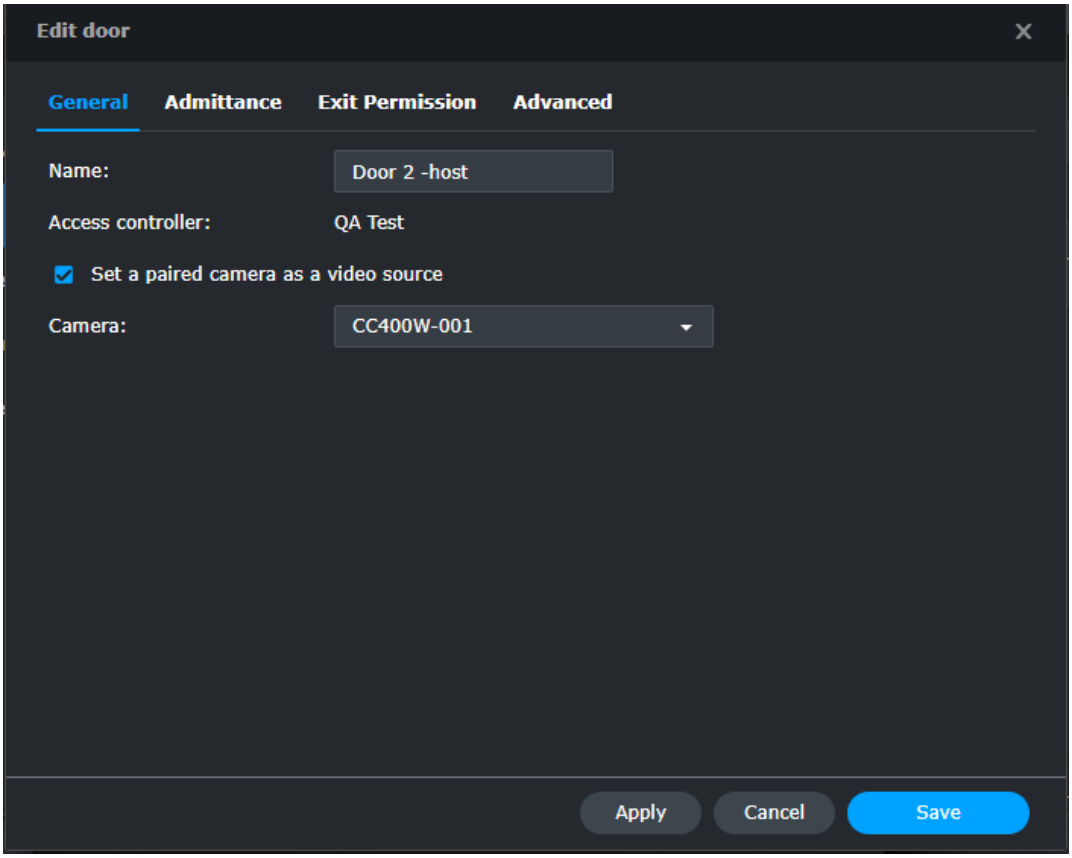
Manage doors

After adding the controller, you'll find all configured doors here. You can view each door's status, snapshots from paired cameras, as well as their hardware information.

Clicking on the icon under Snapshot of a specific door will allow you to quickly preview the camera paired with that door.



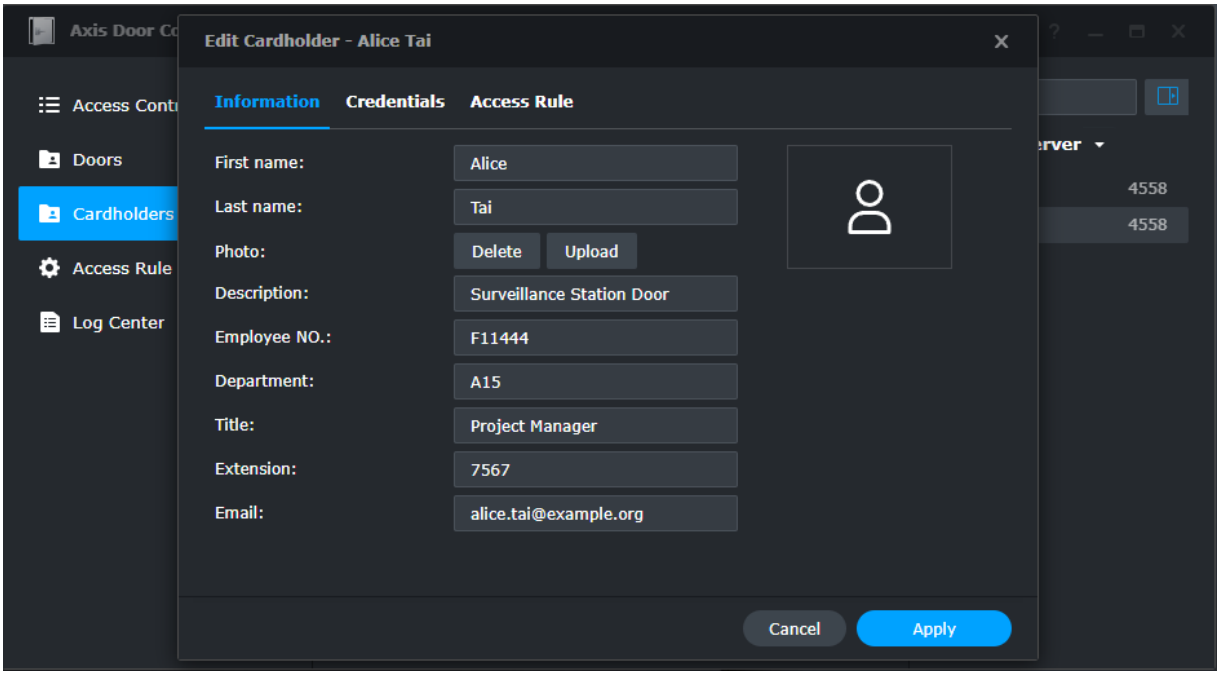
Editing a door will allow you to configure door-related settings such as its name, its paired camera, **Admittance**, **Exit Permission**, and **Door Access Duration**.



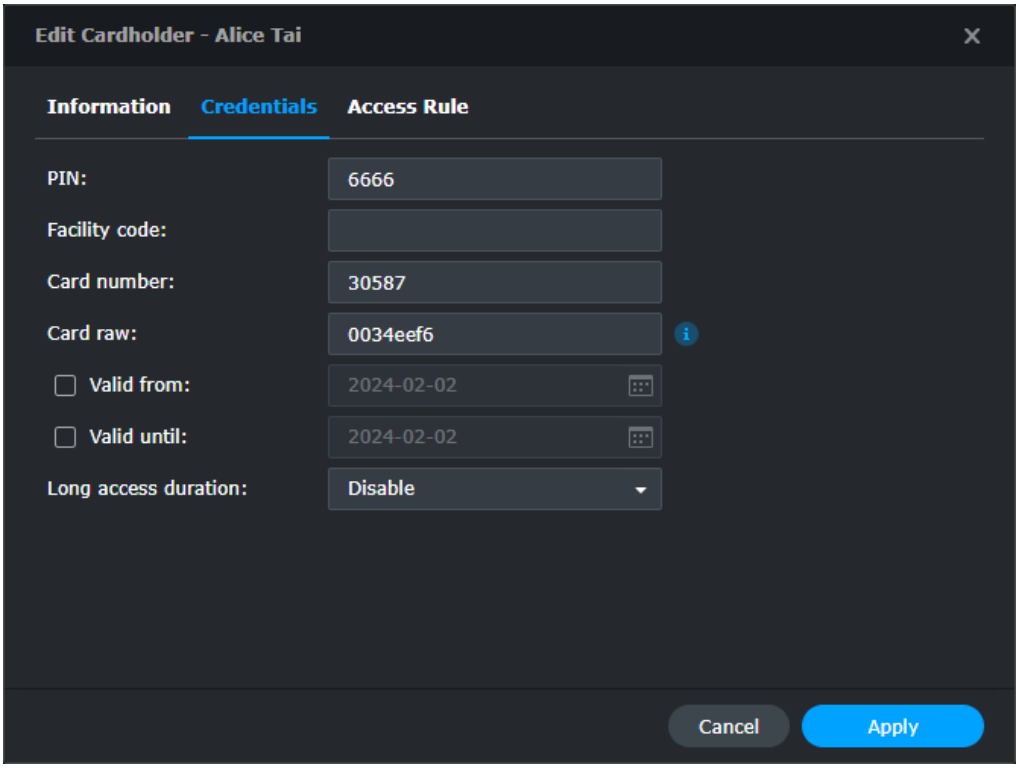
Manage cardholders

After adding the controller to Surveillance Station, you can add cardholders. All doors configured on the same NAS will share the same cardholder database.

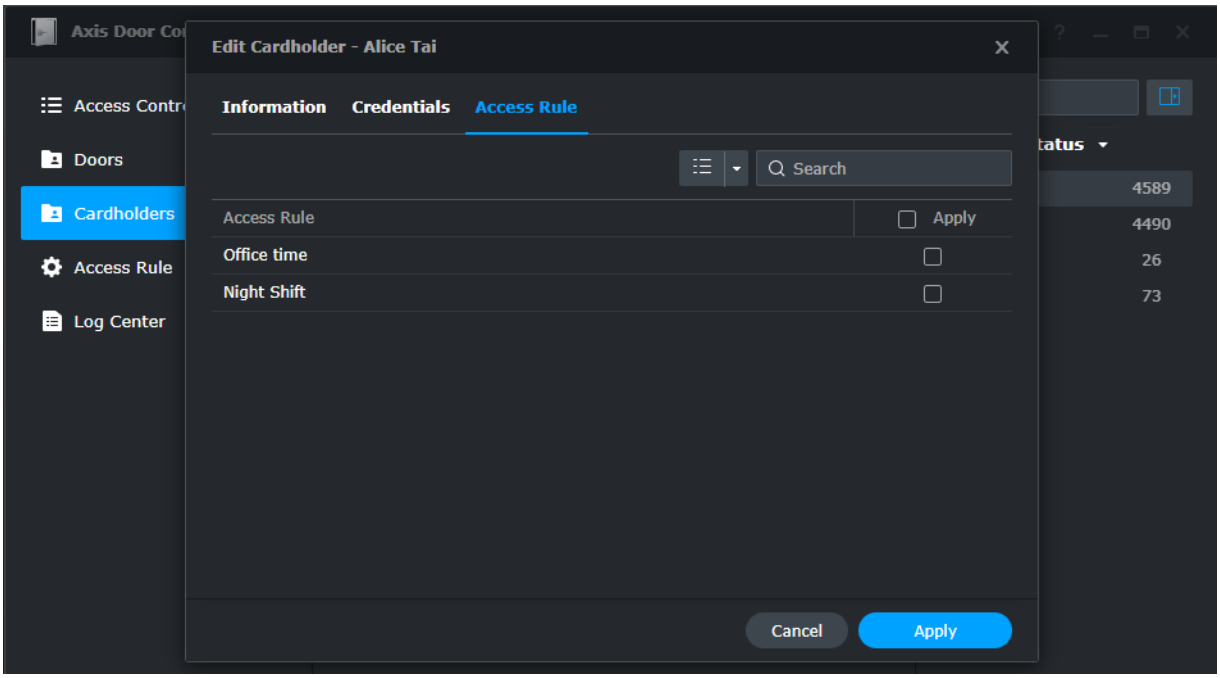
Click **Add** to create a cardholder. Follow the wizard to configure basic information, access credentials, and access rules for the cardholder.



You can configure up to 4 different credential configurations.



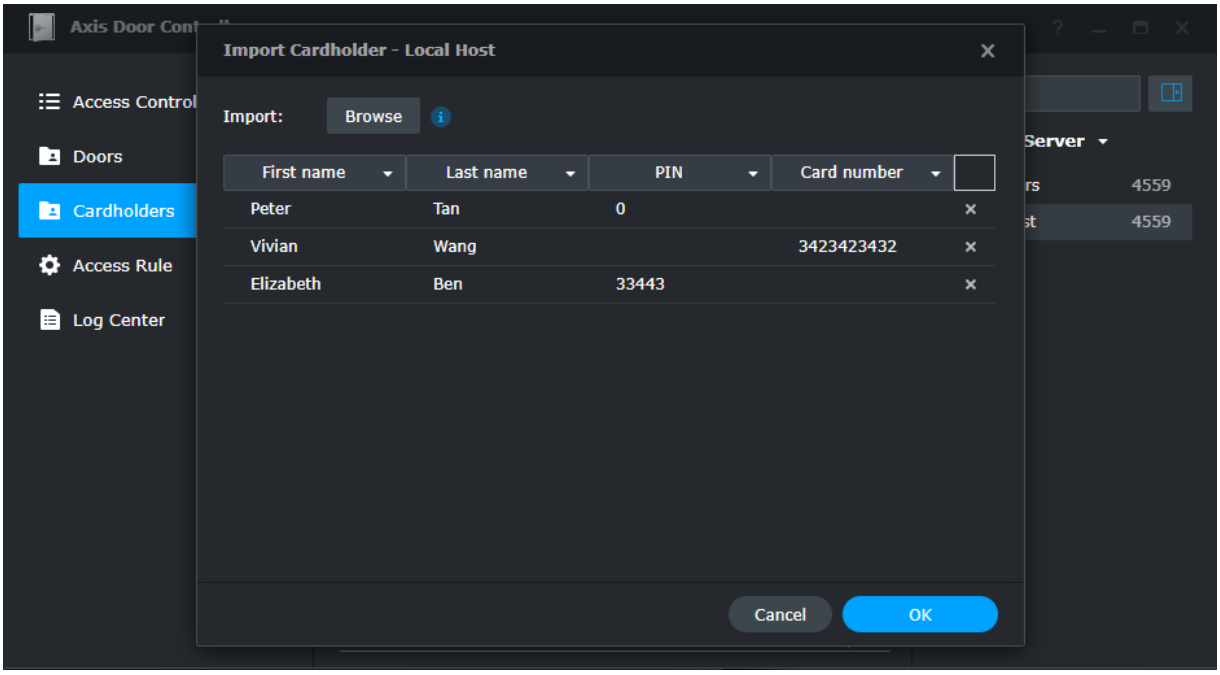
All Cardholders must have at least one Access Rule applied to them.



In Surveillance Station, cardholders can be edited anytime by clicking **Edit**. You can also use the **Batch Edit** option to copy card information such as **Description**, **Department**, **Title**, **PIN**, and **Access Rule** from a preset cardholder to other cardholders. Private information such as the **Employee NO.**, **Extension**, and **Card number** cannot be copied. If administrators wish to block or unblock specific users, click **Block** and follow the subsequent steps.

Administrators can also delete specific cardholders; however, if that cardholder requires access at a later date administrators will need to re-add them to the system. The **Block** function offers the flexibility to keep this user in the system and retain all access log.

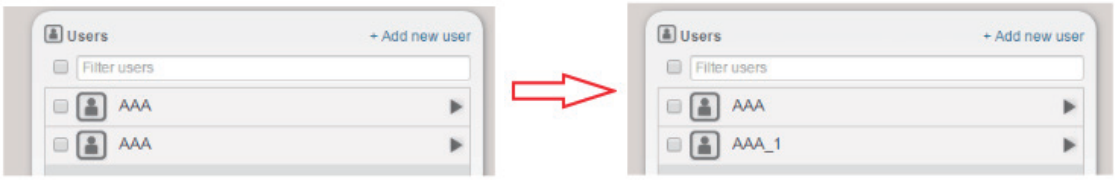
If you want to add more than one cardholder at once, the **Import** function can be used to batch import cardholders from a csv file.



Only the entries for **First name**, **Last name**, **PIN**, and **Card number** are supported. You can export the file from the controller or create the file yourself. The imported cardholders must comply with the following rules:

- First name, last name, and either PIN or card number must be included.
- Two cardholders cannot have the same name or card number.

During the process of retrieving user information from AXIS door controllers, users with duplicate names and information will be identified as the same person. Additionally, if there are multiple users with the same name in the AXIS door controller, an "_x" would be appended for differentiation purposes

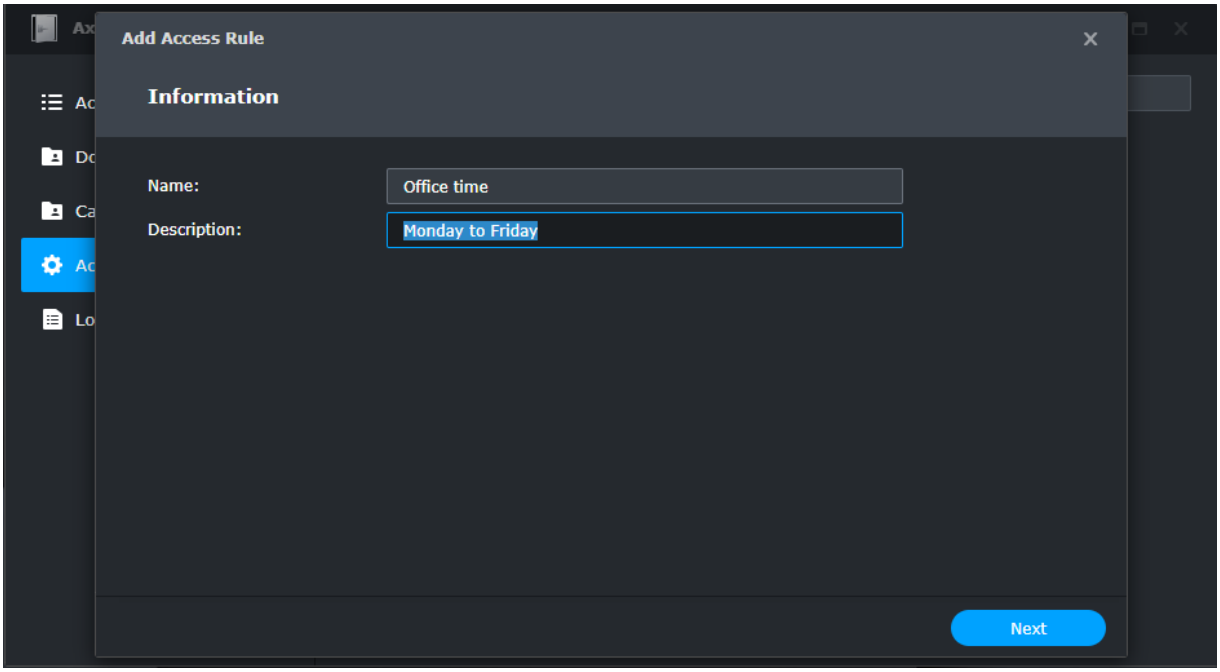


Note:

- Identical user names will also be modified in the same way.

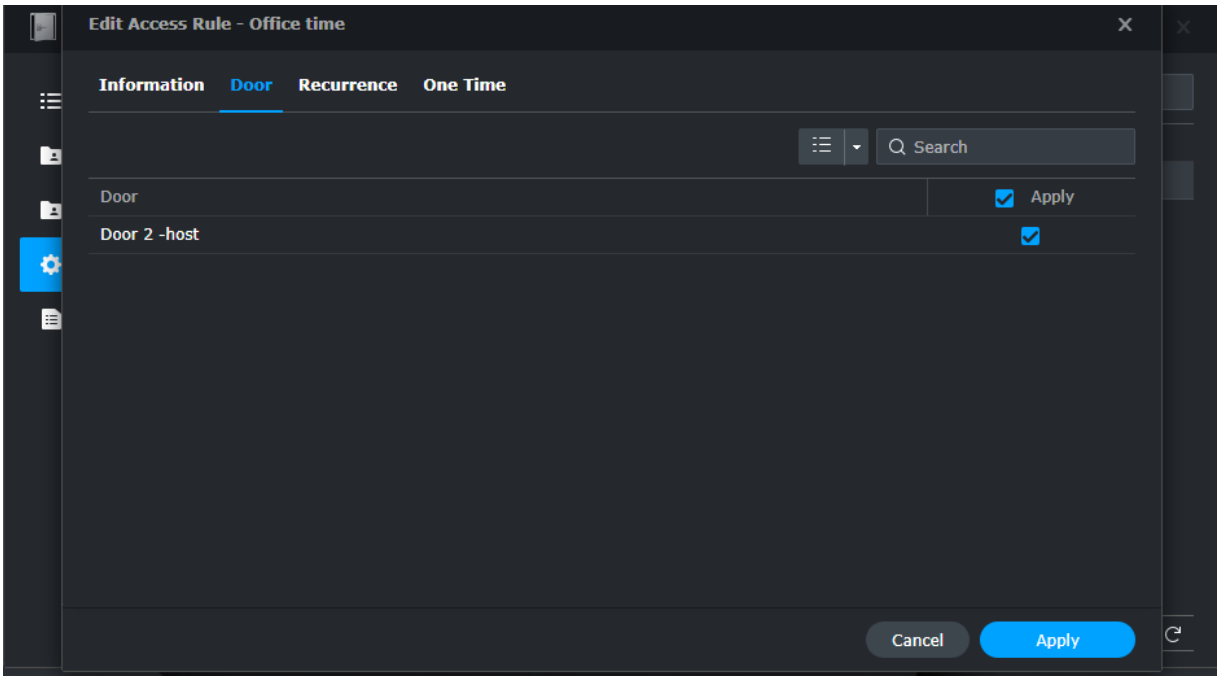
Manage access rules

With **Access Rule**, you can set up rules to determine when and which door can be accessed. To add a new rule, go to the **Access Rule** page and then click **Add**.

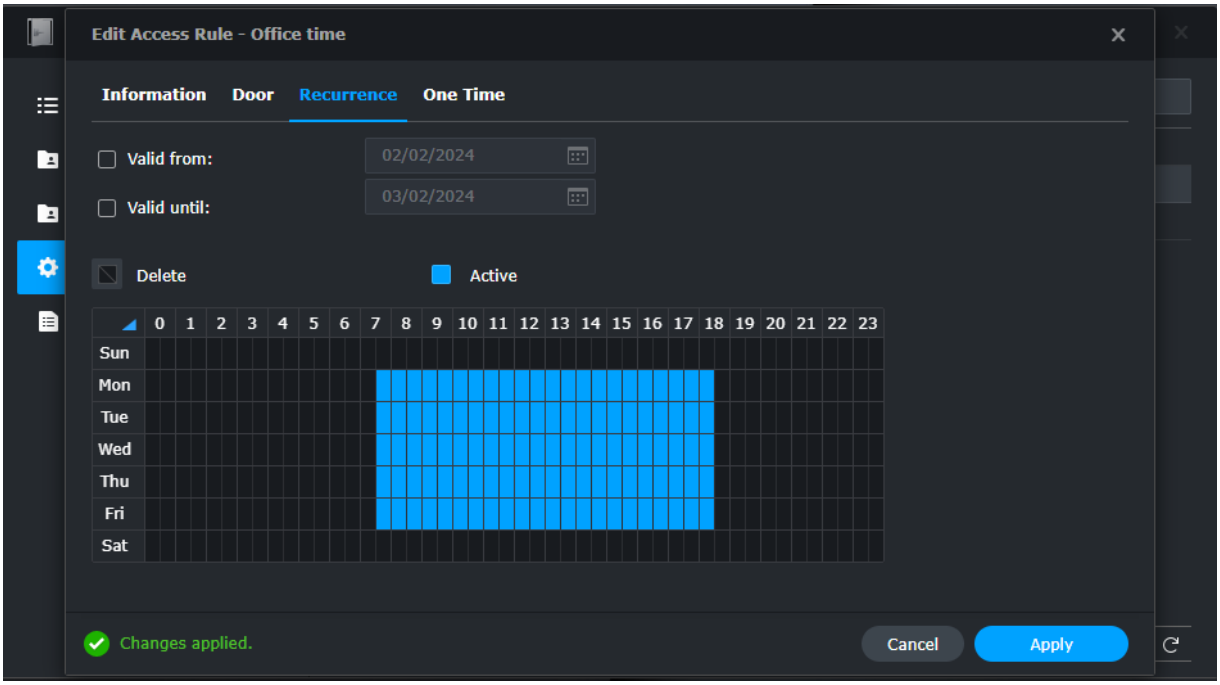


Follow the wizard to specify the name, description, applicable doors and schedule for the rule. For example, if the access rule is configured to allow access on holidays, then it should not be applied

to doors designated for workdays only. Select the doors to apply this access rule, then click **Next**.

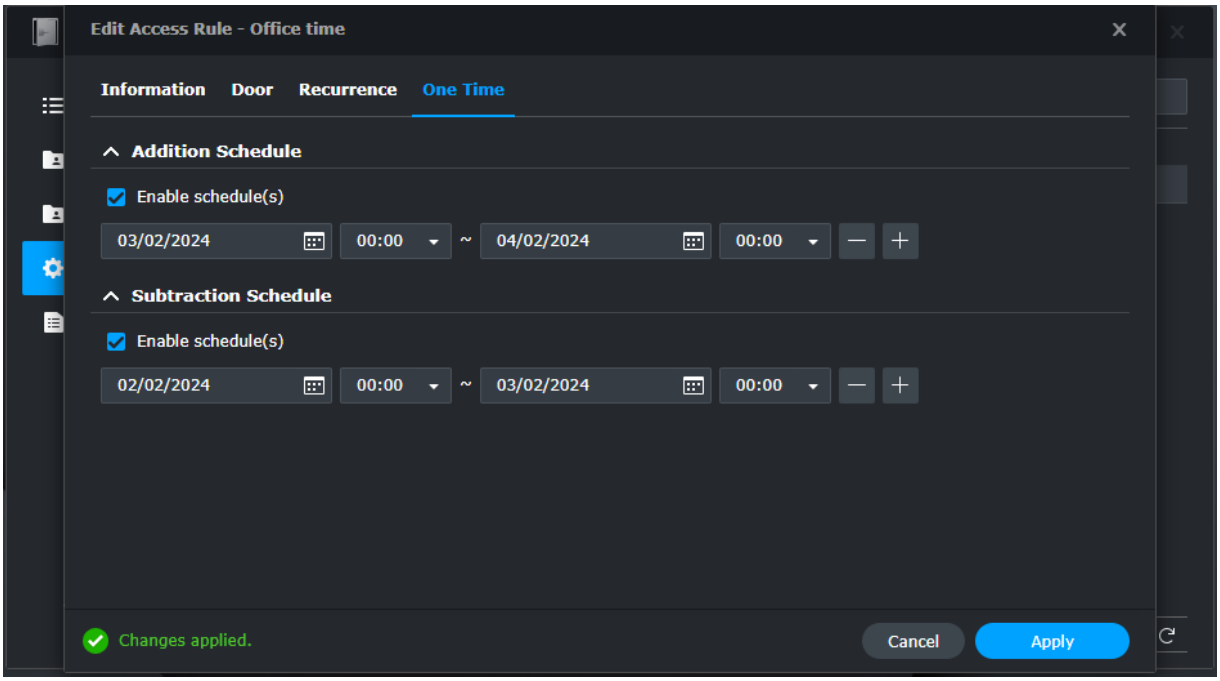


Recurrence provides a configuration mode based on a weekly cycle. Building on the previous example, this access rule is tailored for employees working weekdays (Monday through Friday). Accordingly, the relevant office hours 7AM to 6PM are selected, and all other time including all day Saturday and Sunday are removed. You can also set a specific valid duration. Otherwise, this access rule will remain active indefinitely.



You can also use the **One Time** settings to set up exceptions from the schedule configured under **Recurrence**. For example, if there is an event held on company property for a specific weekend, the date can be added into **Addition Schedule** to allow the door to be accessed. In contrast, if you want to restrict access for a specific date, the date can be added to **Subtraction Schedule** to

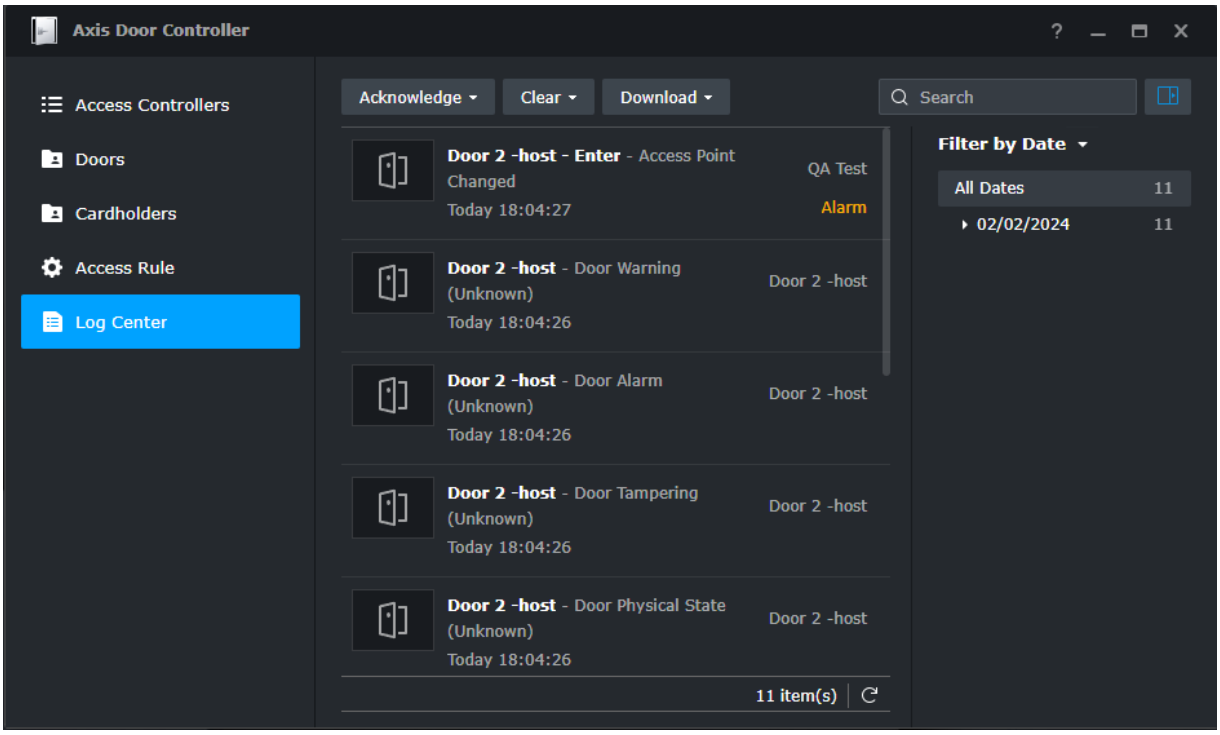
block access for that date.



Surveillance Station provides multiple configurations for the One Time schedule. You can easily add or remove more entries using the "+" or "-" buttons.

View logs

Log Center integrates all event logs from the door controllers including the manual lock, manual unlock, cardholder block and all other relevant events.



Events can be categorized based on **Date**, **Status**, and **Controllers** so that administrators can easily locate the events that they are looking for. If an event is related to a door which is paired with a specific camera, click on the log icon to playback the recordings from the paired camera.

You can also filter events using the **Source**, **Door**, **Status**, **Time interval**, or **Keywords**. Surveillance Station can store up to 60,000 logs.

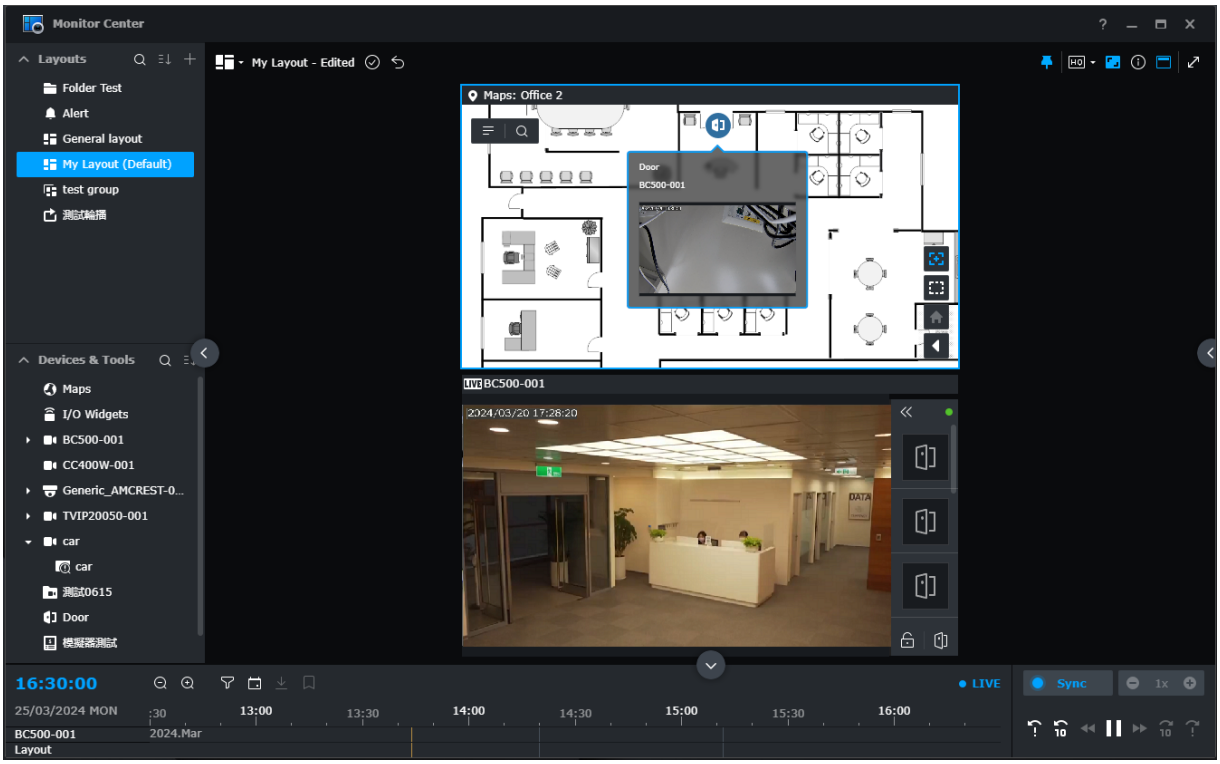
Log entries can be changed to Events using the **Acknowledge** function. You can also **Clear** and **Download** log entries.

Oversee door activity with Monitor Center

There are several ways to utilize Surveillance Station Monitor Center with AXIS door controllers.

View doors in Monitor Center

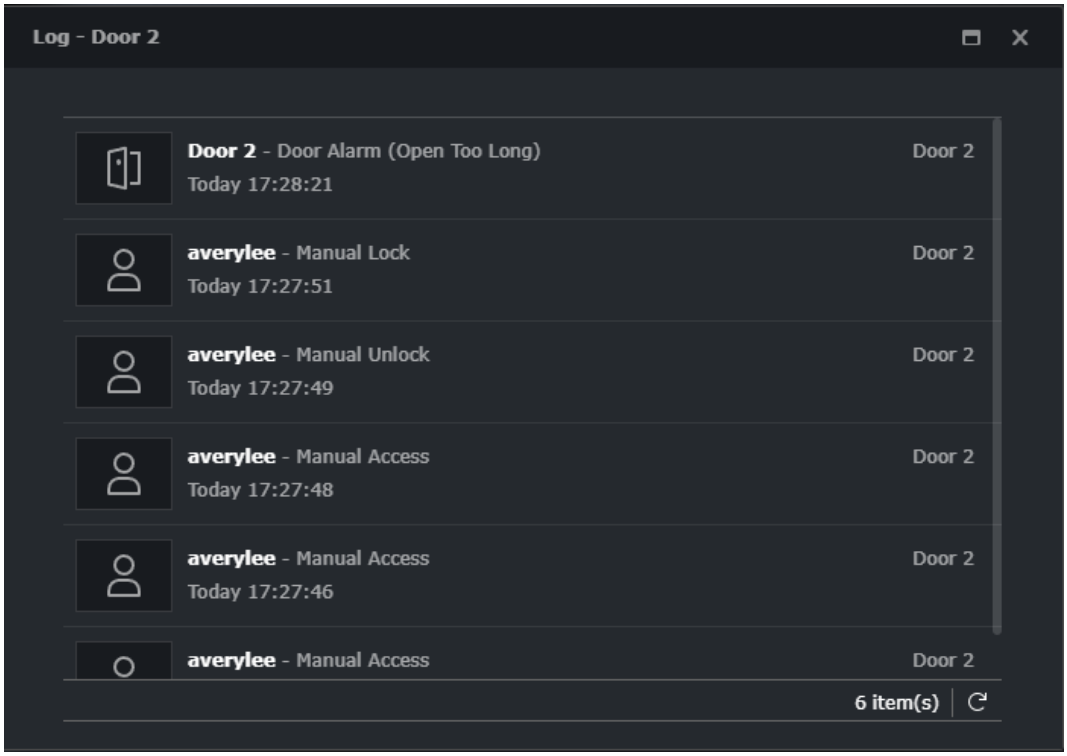
The Monitor Center enables centralized monitoring of all cameras, access control devices and other supported devices. Door units and maps can be easily added to Monitor Center layouts by dragging and dropping them from the **Devices and Tools** panel.



Control doors and view event logs

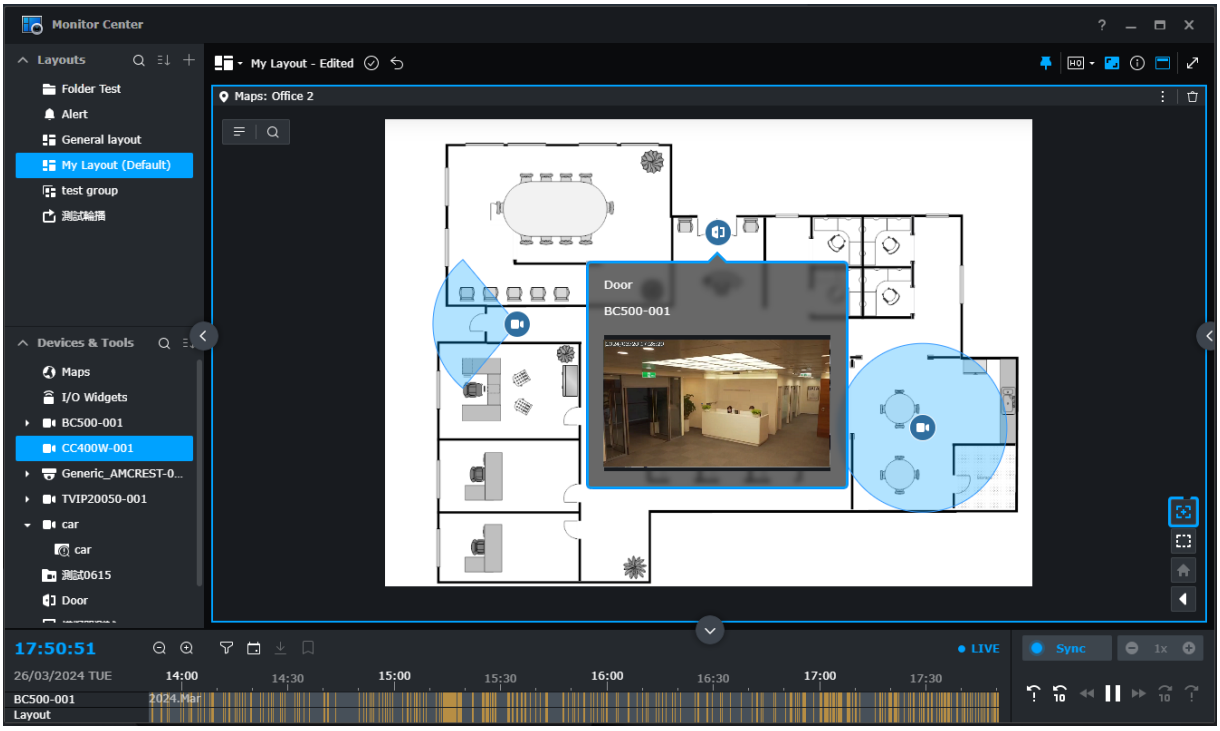
You can directly preview the door's video stream from the Monitor Center, and the following functions are available:

- **Lock**: Locks the door permanently.
- **Unlock**: Permanently unlocks the door.
- **Access**: Grants temporary and anonymous access within the pre-configured access time.
- **Log**: Opens another window to view event logs.



View doors in Maps

Adding door units to Maps allows you to utilize these maps in Monitor Center, enabling administrators and authorized users to quickly see all alarms and alerts at a glance. They can also directly click on a door to see a preview of the paired camera's video stream.

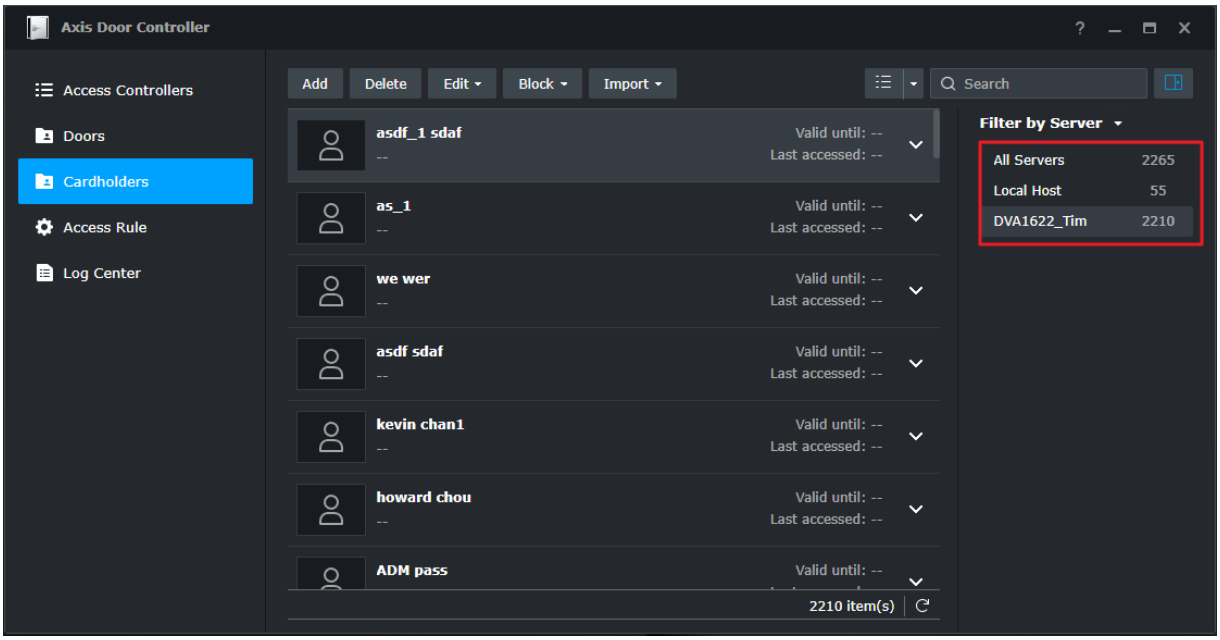


Manage doors under CMS

Starting from Surveillance Station 9.2, the AXIS door controller now supports CMS (Central Management System), providing enhanced capabilities for managing larger deployments and centrally configuring access control devices.

With CMS, administrators can sign in to the host server for unified management. Administrators can oversee all doors added to paired servers, in addition to those added to itself through AXIS Door Controller. However, it's important to note that cardholder information, access rules, and event logs are managed on a per-server basis.

For example, administrators can import cardholder information specific to supplementary server A and establish entry and exit rules tailored to subsidiary A directly from the host. They can easily switch internally within the AXIS Door Controller to supplementary server A's settings by selecting the server in the right panel.



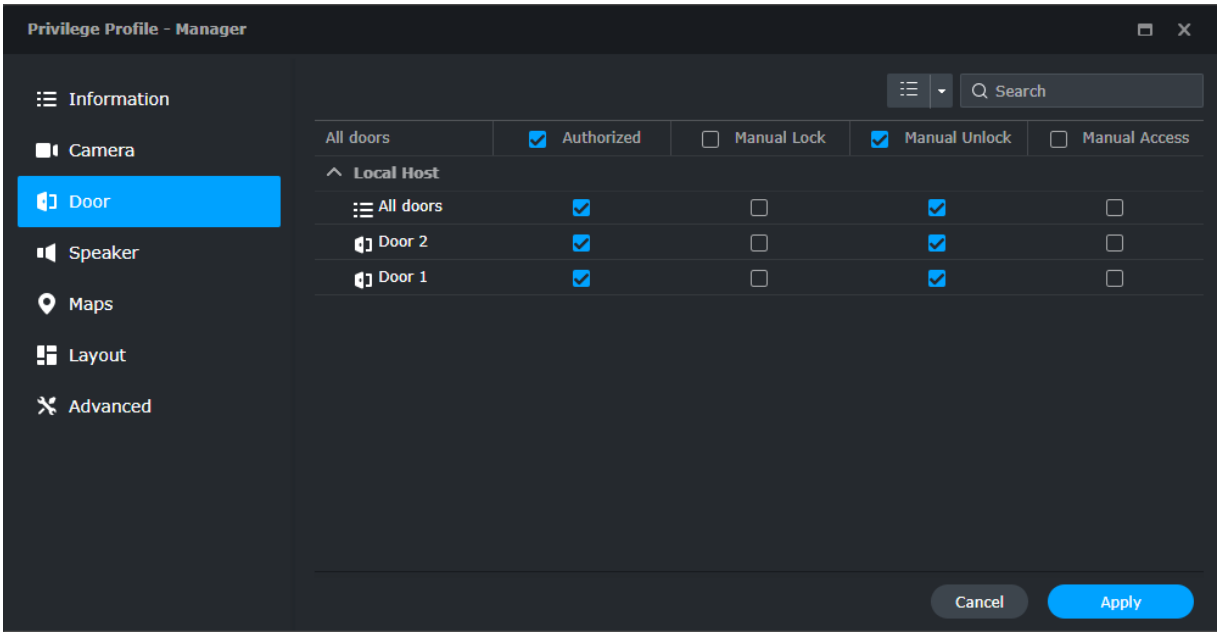
When creating access rules for subsidiary A, administrators can only apply them to doors added to subsidiary A. Similarly, cardholder data on subsidiary A will not be synchronized with the host server.

More applications

AXIS Door Controller in Surveillance Station can be utilized with other useful applications such as **Privilege**, **Action Rule** and **Notifications**.

Configure user privileges

Specific privileges for door unit functions such as **Manual Lock**, **Manual Unlock**, and **Manual Access** can be fine tuned using privilege profiles at **User**.

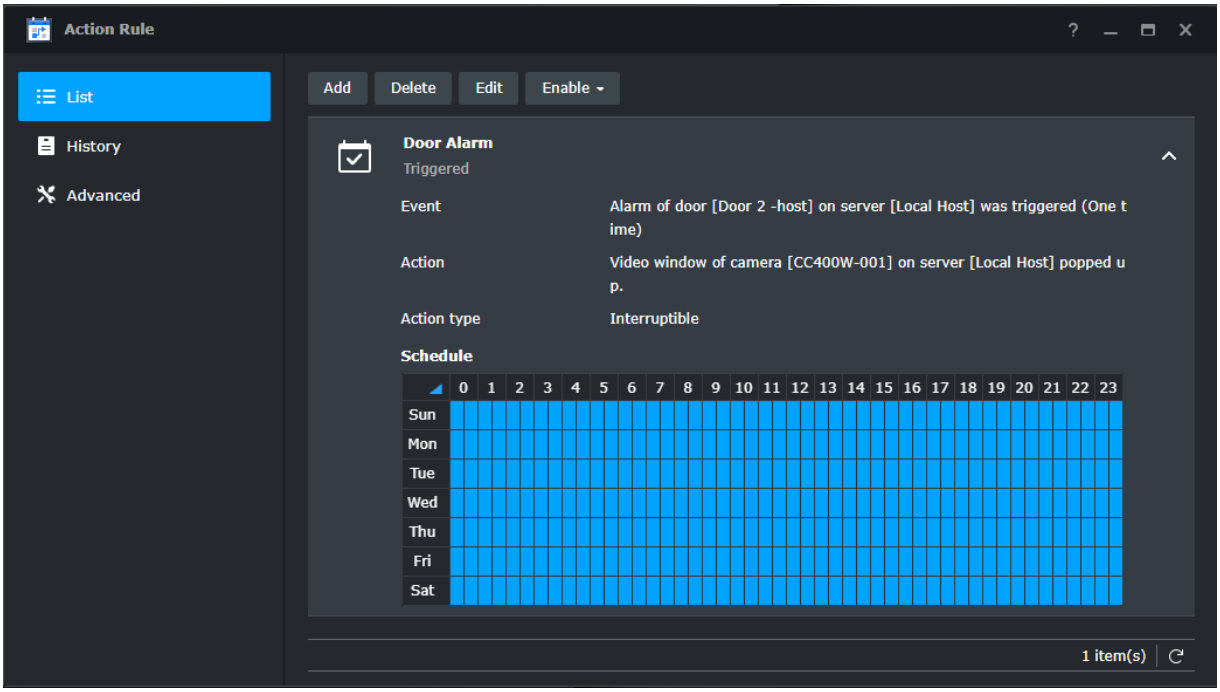


Manual Lock, **Manual Unlock**, and **Manual Access** are unique and important privileges that allow certain users to manually lock, unlock, and access the door. These options need to be configured separately. Additional privileges such as **View the Axis Door Controller Application, Edit Controller**, **Add/Delete Controller**, **Edit Cardholder** and other log settings can be configured in the **Advanced** page.

Automate actions using action rules

Action Rule is a dedicated application for configuring automatic actions corresponding to triggered or scheduled events.For example, in **Action Rule**, door alarm triggers can be treated as an event. When this event is triggered, Surveillance Station can automatically take certain action in response to that event. For example:

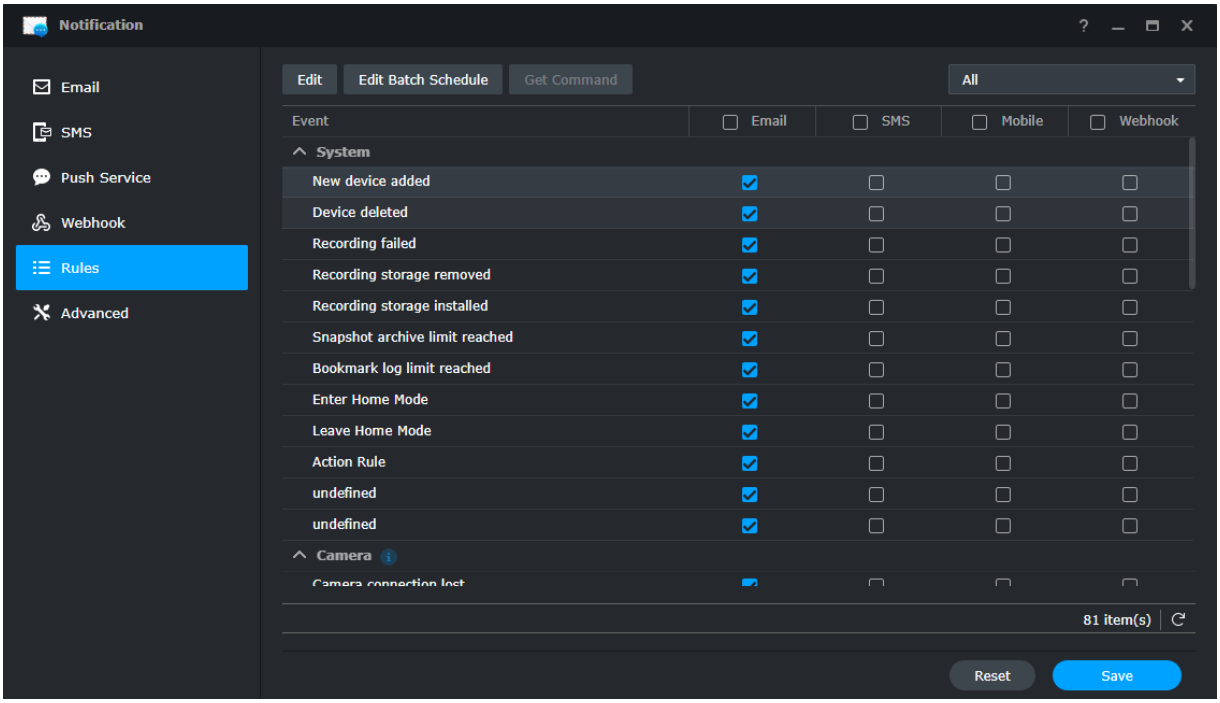
- **Event**: The alarm of door [Door] on server [Local host] was triggered.
- **Action**: Instruct camera [Camera_Door] on server [Local host] to move to preset position [door1] hold for [1] [minute(s)], and move to return position [Home].



This means whenever a door alarm is detected, whether it is an open too long alarm or a forced open alarm, the paired PTZ camera will go to the defined preset position correspond to the event. You can also configure Face Recognition to grant entrance when an allowed person is detected.

Configure notifications

Surveillance Station supports push notifications via **Email**, **SMS**, **DS cam**, and **webhooks**.



Notification supports the customization of messages that can be sent out. Once an event is detected, Surveillance Station will notify the administrator using the selected methods.

For example, if you choose to send a message via Email when the event **Access granted**, **Access denied**, **Door alarm triggered**, or **Door tempering detected** occurs, the system will automatically attach a snapshot taken from the paired camera in the message. This provides visual context for the event as well as the surrounding area.