

White Paper for Access Control in Surveillance Station 7.2.2 and above

With AXIS Network Door Controller A1001



Table of Contents

Introduction	01	Surveillance Station and AXIS Entry Manager	
What Is Access Control?		Compatibility	30
Why Does AXIS A1001 Work Better with Synology Surveillance Station?		User and Cardholder	
Configure AXIS A1001 before Installation	05	Identification type and door authentication	
Install AXIS A1001 in Synology Surveillance Station		Group and Access Rule	
7.2.2 and above	09	Schedules	
Access Controllers		Synchronization	
Cardholders			
Access Rule			
Log Center			
Advanced			
Use Synology Door Monitor with AXIS A1001	21	Find your information	
Door Preview			
Desktop Shortcuts		Synology publishes a wide range of supporting documentation.	
Door Viewer on Live View			
Door Viewer Operations			
Door Units on E-map			
More applications	25		
User			
Action Rule			
Notification			
Before Upgrading to Surveillance Station 7.2.2 and Above	28		
End of Support for Peer Connection			
Cardholder in Controllers with the Same Name			
Privilege Settings			

Find your information

Synology publishes a wide range of supporting documentation.

In [Knowledge Base](#), you will find useful [Help](#) and [FAQ](#) articles, as well as [video tutorials](#) breaking up processes into handy steps.

In [Synology Documentation](#), you can find [User's Guides](#), [Solution Guides](#), brochures, and [White Papers](#). Experienced users and administrators will find answers and guidance in technical [Administrator's Guides](#) and [Developer Guides](#).

Got a problem and unable to find the solution in our official documentation? Search hundreds of answers by users and support staff in [Synology Community](#) or reach [Synology Support](#) through the web form, email or telephone.



Introduction

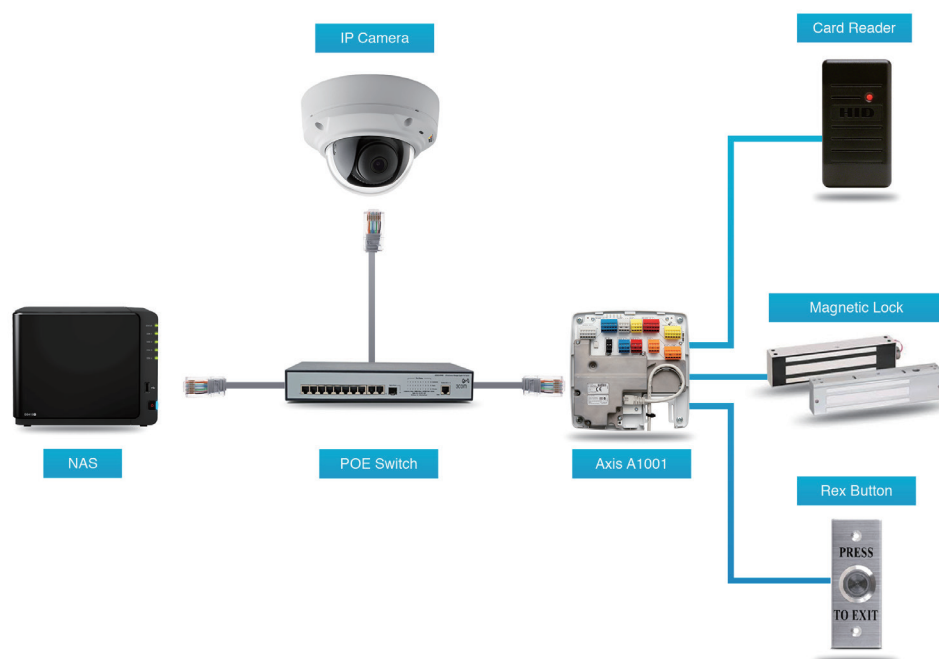
What Is Access Control?

In the era of networking exploration, most of the electronic devices are being connected to the Internet so that users are capable of controlling all the devices remotely. Network camera is one of the examples when it comes to connecting things to the Internet. With the network connection as replacement of the coaxial cable using analog signals, the installation of surveillance camera becomes way easier than before.

Recently, manufacturers are trying to connect an independent access controller to the Internet so that they can communicate with the controller via the Internet. Access control has played an essential role in security deployment. However, it has always been an independent device from a security system. All the access management data would be recorded into another server for future revision. It contains the operation of access control at the reception, and whether a person has the privilege to be access granted. A set of access control system includes a database server, a card reader, door locks, and possibly a lock monitor and a REX (Request-to-exit) button. All the access privilege settings will be stored in the server and it controls whether a certain card has the privilege to open the door. Of course, the receptionist or a security guard can open the door, too.

From time to time, network / IT based companies are developing network door controllers with which administrators can easily operate the device via network interface, pretty much like how we did to the network cameras. In Surveillance Station 7.2.2 and above, Synology NAS is taken as an access control server communicating with AXIS A1001, so that all the access management operations can be conducted via the Surveillance Station interface.

Why Does AXIS A1001 Work Better with Synology Surveillance Station?



AXIS A1001 is known as the network door controller. It contains multiple analog I/O ports and with one Ethernet connection to the local network (www.axis.com). The rudiment of integrating AXIS A1001 into Surveillance Station is the combination of access management operations and the existing video source saved in the NAS. Surveillance Station retrieves the access log from AXIS A1001 and pairs them with related video sources so that administrators can easily review the access data with a related video source, consolidating and maximizing the value of stored access logs.

- Below are some key values of using AXIS A1001 with Synology Surveillance Station.
- Easy to deploy and install with UPnP search in Surveillance Station
- Having one camera paired with one door to have a clear view when monitoring the door
- Intuitive user interface including the configurations of cardholder, schedule of door and access rules.
- Attaching photos and common information to cardholders so that administrators can check cardholder frauds
- More cardholder, log and controller are supported than AXIS Entry Manager. The number is up to 50000 cardholders and 60000 logs
- Instant playback when clicking on the access logs

More details will be introduced in the following chapters. The table below shows the degree of support that can be achieved when AXIS A1001 is being paired with Surveillance Station:

System Spec	Axis Entry Manager	Surveillance Station
Recommended maximum number of controller	33	As maximum camera number
Maximum number of cardholders	400	50000
Maximum number of offline events	30000	60000
Maximum number of schedule	Unlimited	Unlimited
Supported controller	Axis A1001	Axis A1001
Key features		
Access Management	<ul style="list-style-type: none"> • Cardholder management • Photo of card holder • Manual Lock / Unlock • Extended grant time 	
Video Integration	<ul style="list-style-type: none"> • Live event monitoring on video • Recording playback with related event 	
Event & Alarm	<ul style="list-style-type: none"> • Valid Access • Invalid Access • Door Alarm • Tamper detection 	

Adding access controllers to Surveillance Station requires installing additional Surveillance Device Licenses. Learn more about Device License Pack .

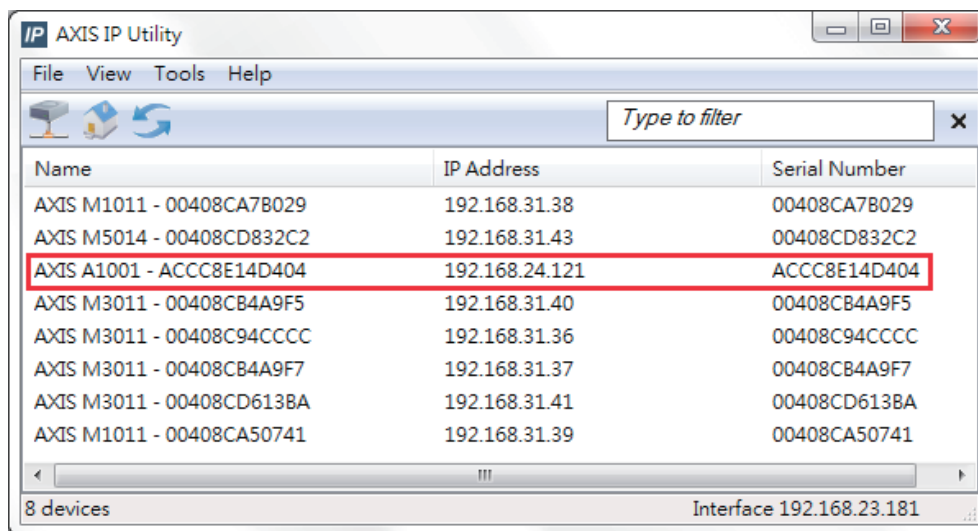
A1001 firmware 1.55 is only compatible with Surveillance Station 8.0 and above.

Configure AXIS A1001 before Installation

AXIS Door Controller A1001 is a network controller with multiple I/O ports embedded that connects analog devices such as magnetic door locks, lock monitors, and card readers to the Internet. An AXIS A1001 is able to connect up to two sets of doors, including door locks, lock monitors, card readers, REX buttons, and some other I/O devices.

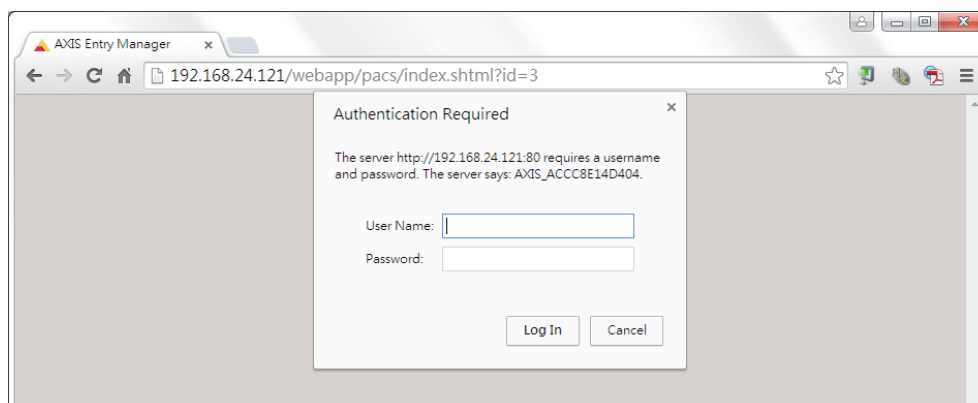
Before installing the AXIS A1001 with Synology Surveillance Station, a few settings are required to be configured on its web user interface.

Use **AXIS IP Utility** to discover AXIS A1001 in your local network.

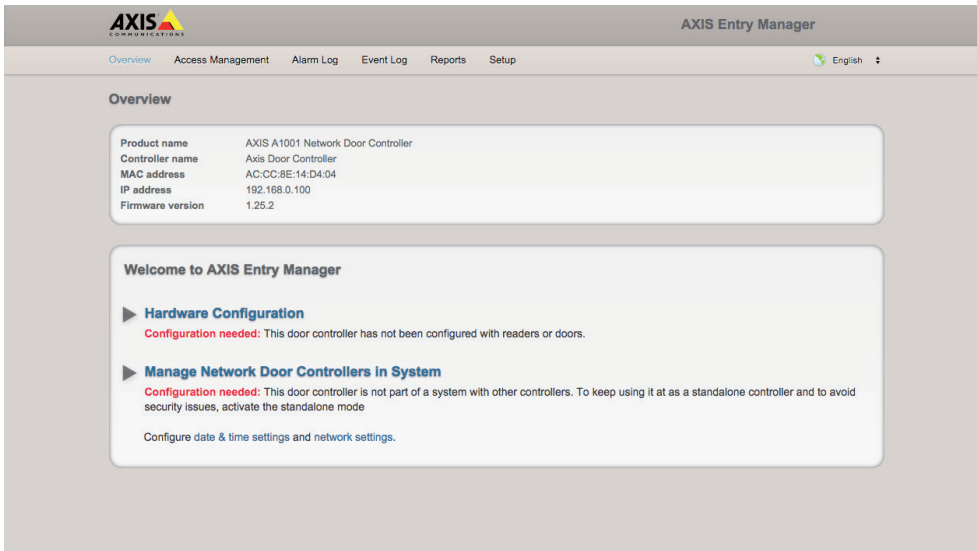


Name	IP Address	Serial Number
AXIS M1011 - 00408CA7B029	192.168.31.38	00408CA7B029
AXIS M5014 - 00408CD832C2	192.168.31.43	00408CD832C2
AXIS A1001 - ACCC8E14D404	192.168.24.121	ACCC8E14D404
AXIS M3011 - 00408CB4A9F5	192.168.31.40	00408CB4A9F5
AXIS M3011 - 00408C94CCCC	192.168.31.36	00408C94CCCC
AXIS M3011 - 00408CB4A9F7	192.168.31.37	00408CB4A9F7
AXIS M3011 - 00408CD613BA	192.168.31.41	00408CD613BA
AXIS M1011 - 00408CA50741	192.168.31.39	00408CA50741

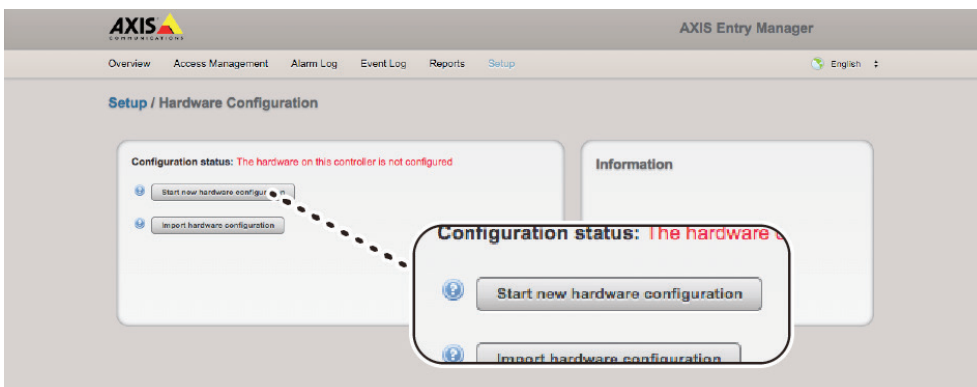
Log in to the web interface of AXIS A1001. The default username/password is **root/pass**.



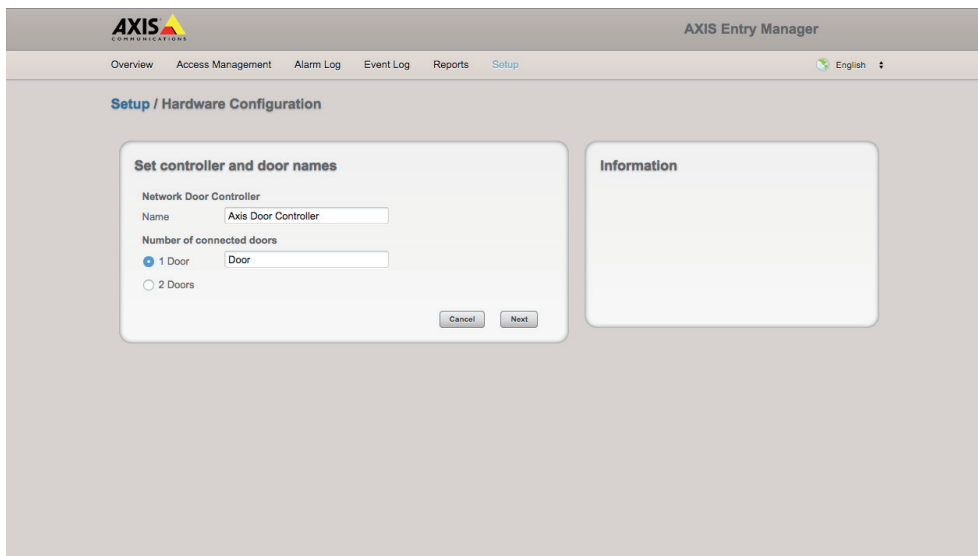
In the **Overview** page, basic information, such as IP address and firmware version, are displayed here. However, the statements highlighted in red inform you of the hardware settings in need of configuration. Click on **Hardware Configuration** for further configurations.



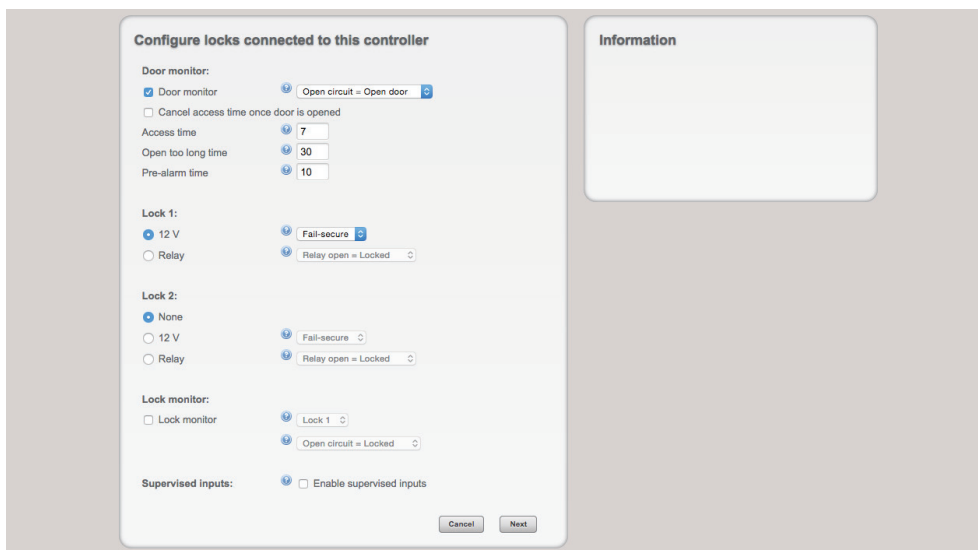
In the **Hardware Configuration** page, you can either start new hardware configuration or import a hardware configuration file. To create a new hardware configuration, click **Start new hardware configuration**.



Assuming that there is only one door that needs to be configured, enter the name and select the number of doors that need to be configured here.



In the step of **Configuring locks connected to this controller**, there will be a few settings that need to be configured.



For most general settings, only the settings below need to be checked.

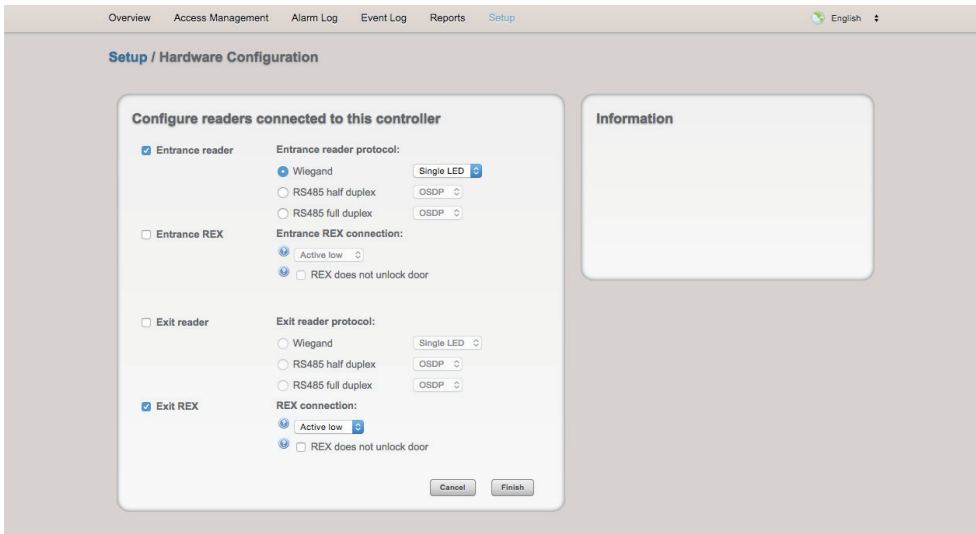
Access time: for how long (seconds) the door will be unlocked after the access being granted. (This setting can be modified afterwards.)

Open too long time: for how long (seconds) the door will be alarmed as open too long.

Pre-alarm time: for how long (seconds) before the actual alarm is occurred.

In Lock 1, if **Fail-secure** is chosen, the door will remain locked when the AXIS A1001 is offline. On the contrary, **Fail-safe** will keep the door open when AXIS A1001 is offline. If a lock monitor is installed, please tick the **Lock monitor** checkbox. Normally Open circuit will be set as locked.

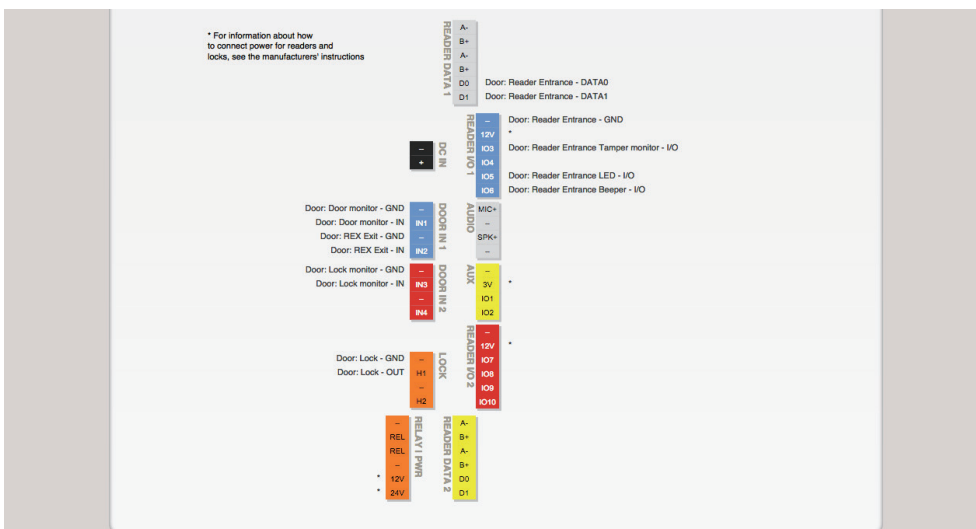
When it comes to the reader configurations, it depends on the devices that will be used at the entrance and exit. For example, if a company is using a card reader for entrance and a REX button for exit, just select Entrance reader and Exit REX. After this configuration, you are good to finish the setup wizard.



After clicking **Finish**, it will take a few seconds to proceed the configurations.

When the hardware configuration is complete, hardware pin chart can then be checked for the actual analog devices connection.

The Hardware Pin Chart is a reference for the actual connections of all the analog devices such as card readers, door locks, lock monitors, and some other I/O devices.

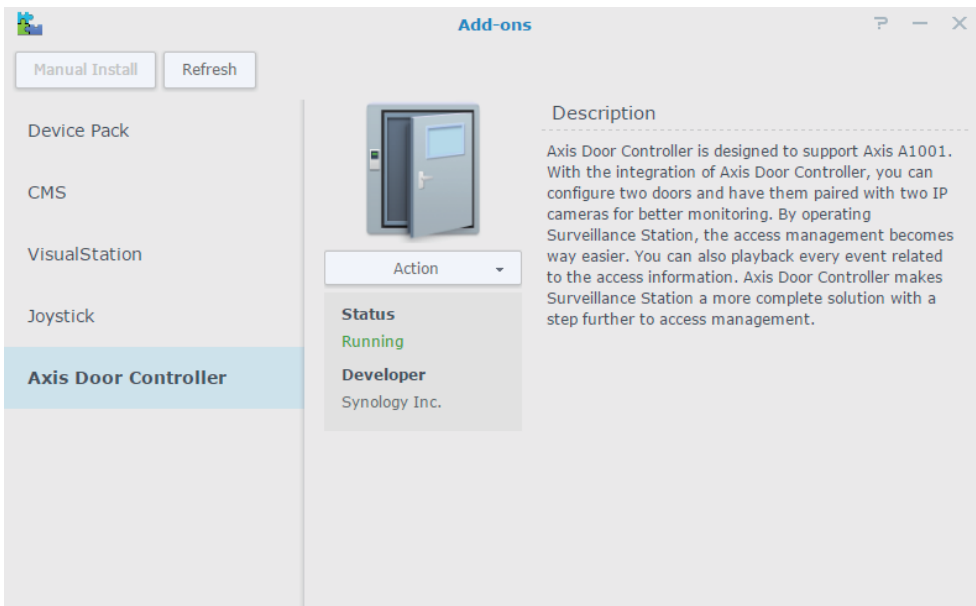


In this Pin Chart, the device wires are clearly marked. Connect all the devices to the AXIS A1001 correctly, and then the door controller is perfectly set.

After the initial hardware configuration is complete, you can install AXIS A1001 and configure the door controlling system directly with Surveillance Station.

Install AXIS A1001 in Synology Surveillance Station 7.2.2 and above

AXIS Door Controller A1001 is an add-on of Surveillance Station. At first, you will need to go to **Add-ons** to enable the **AXIS Door Controller** add-on for further configuration.



Surveillance Station only supports standalone mode of AXIS A1001 based on AXIS' suggestion. Please confirm that the controller has not been connected to other controllers or under standalone mode before you add it.

Then, launch **AXIS Door Controller**, and click **Add**.

The screenshot shows the 'Add Controller Wizard' dialog box with the 'Information' tab selected. The fields are filled with the following information:

Name:	Axis A1001
IP address:	10.13.23.44
Port:	80
Model:	A1001
Username:	root
Password:	••••

Below the password field is a 'Test Connection' button with a green checkmark to its right. At the bottom right of the dialog are 'Next' and 'Cancel' buttons.

The wizard will go through all the settings. Enter the basic information of AXIS A1001, and then click Next. Use the UPnP search to find the AXIS A1001 connected to the local area network.

Each door configured in Surveillance Station can be further paired with an IP camera. In general, the paired camera will be monitoring the door so that any events happening at the door can be clearly recorded.

The screenshot shows the 'Add Controller Wizard' dialog box with the 'Door 1' tab selected. The 'General' section is expanded, showing the following configuration:

Name:	Door
<input checked="" type="checkbox"/> Set a paired camera as a video source	
Camera:	Camera_1

Below the camera selection are two collapsed sections: 'Admittance' and 'Exit Permission', each with an information icon. At the bottom left is a 'Previous' button, and at the bottom right are 'Next' and 'Cancel' buttons.

To have the paired camera shown in the list of video sources, make sure the camera is added to Surveillance Station before going through the door controller settings. Select a preferred camera to pair with the door, and then click **Next**. The paired camera does not need to be an AXIS camera. With Surveillance Station, all supported cameras can be paired with the door controller. The paired camera can be changed by editing the controller again after completing the installation process.

Apart from pairing with camera, the configuration of authentication for admittance and exit permission of each door is required. In this page, you can decide when to use what kind of authentications to access. For example, a company requires the use of a card for access check at the entrance, and a REX button to exit. Thus, for the identification type at the entrance, **card number** or **card raw** is required. Multiple identification types are allowed here.

Add Controller Wizard [X]

Door 1

General

Admittance ⓘ

PIN Card number Card raw

Customize Delete

Custom Settings: All identifiers

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Mon	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Tue	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Wed	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Thu	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Fri	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sat	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

Previous Next Cancel

AXIS A1001 needs to be synchronized with an NTP server to make sure the time is exactly correct.

Add Controller Wizard [X]

Advanced

^ Time Synchronization

Network time server: Surveillance Station

Time zone: (GMT+08:00) Taipei

^ Door 1

Access duration (sec.): 7

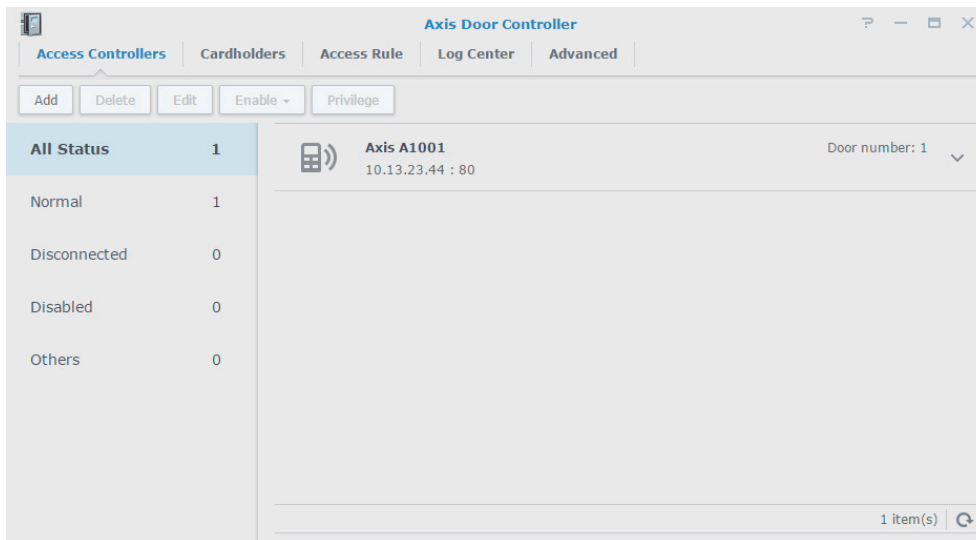
Long access duration (sec.): 30

Previous Finish Cancel

Also, the access duration can be configured. You can set the access duration separately for each door according to individual needs. **Long access duration (sec.)** is a friendly configuration designed for the disabled. The PIN length is 4 digits by default and can be adjusted to 4 to 7 digits according to the scenario. Set the time configuration and then click Finish to complete the adding process.

Note: Adjusting the PIN length according to the scenario requires a reader that supports setting up PIN lengths, please contact the reader manufacturer to confirm whether the reader supports this function.

After the configuration is complete, a door unit is added to **AXIS Door Controller**.

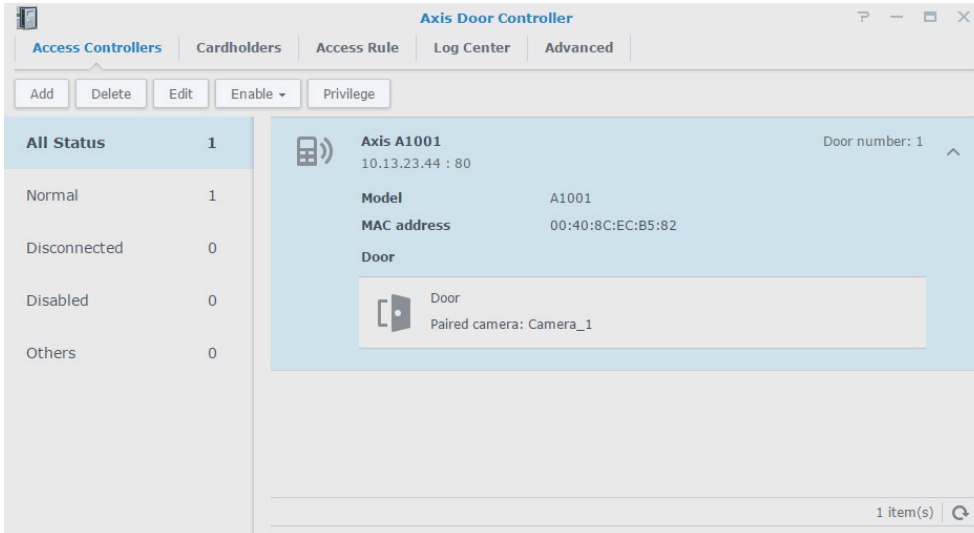


There are five tabs in the application: **Access Controllers**, **Cardholders**, **Access Rule**, **Log Center**, and **Advanced**.

- **Access Controllers:** overview of the door controller and more operations for the controllers.
- **Cardholders:** operations for the cardholders, including add, edit, delete, and block.
- **Access Rule:** add, edit, or delete access rules to be applied to cardholders.
- **Log Center:** record event logs related to the door controller.
- **Advanced:** configure advanced functions such as event logs and alarms.

Access Controllers

All the door controllers added to Surveillance Station will be shown in this tab. Moreover, you can view the basic information of every door with paired camera here and preview the paired camera just by clicking the door icon.

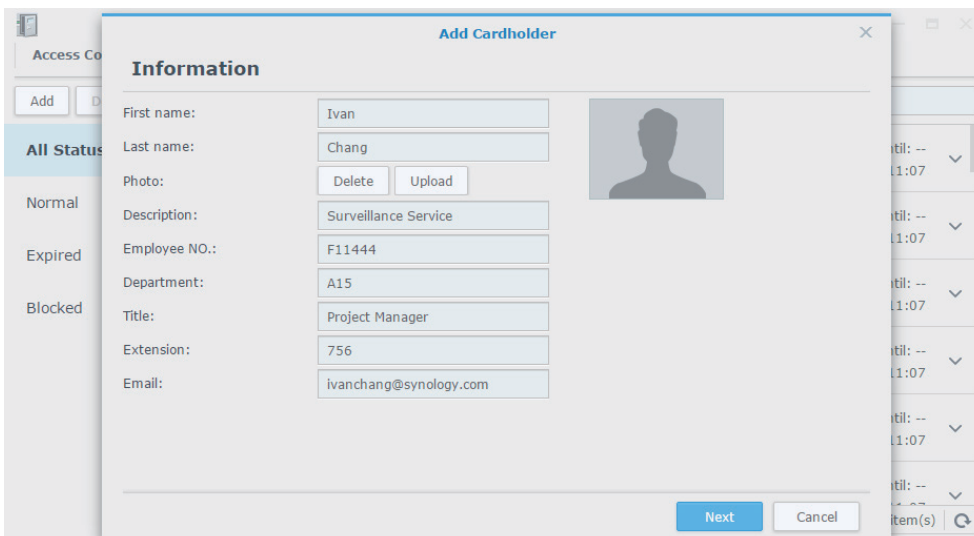


Since AXIS A1001 is a separate device from Synology NAS, the data of **Cardholder** and **Log** will be synced during the installation.

During the synchronization of the controller, cardholder, and log, the device status of the controller will be shown to be activating. It is suggested to avoid editing and deleting of the controller, cardholder, and log during this period. Activating these operations will interrupt the synchronization and the synchronization will be required to start over.

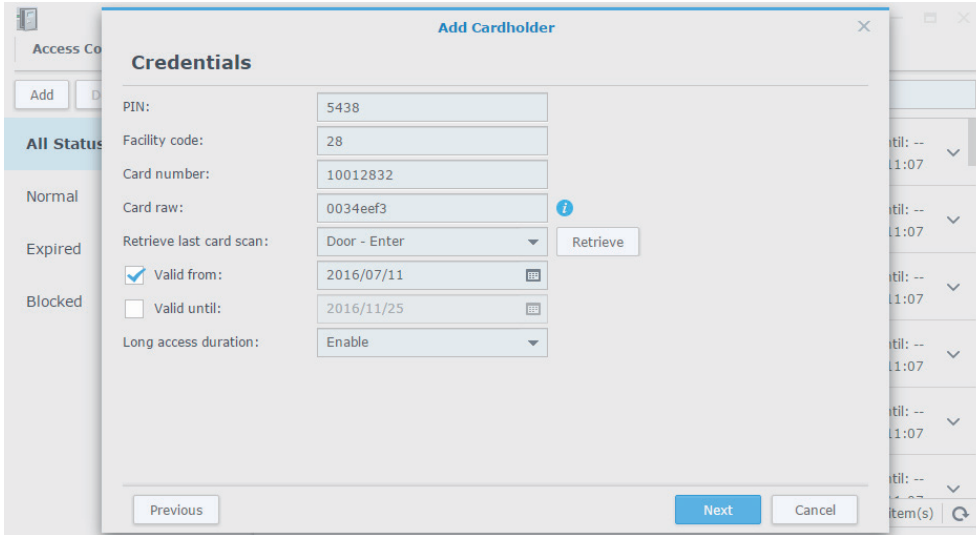
Cardholders

After adding the controller into Surveillance Station, cardholders can be added in Surveillance Station.



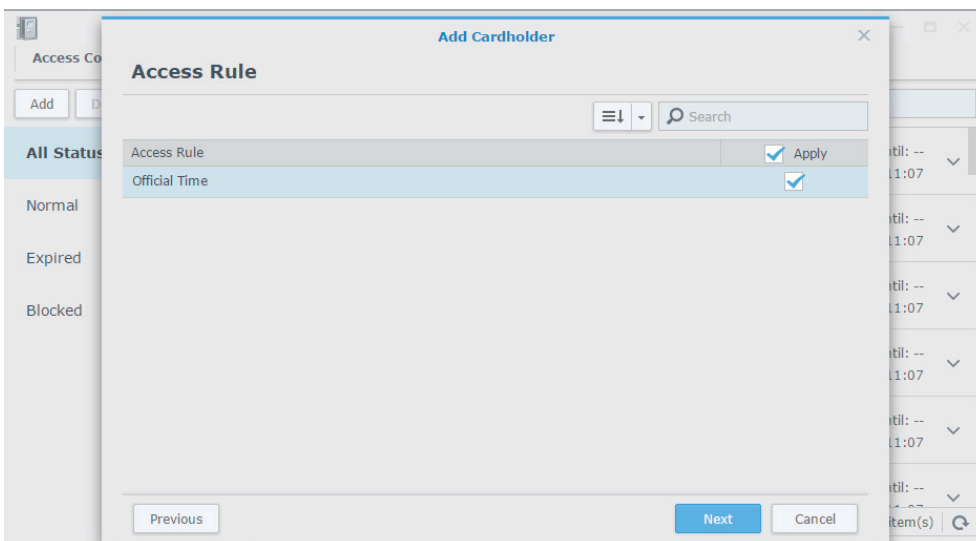
Click **Add** to create a cardholder. The wizard includes configuration of Information, Credential and Access Rule.

Information includes many personal information like name, extension, email and even the photo. Fill up the column needed, and then click **Next**.



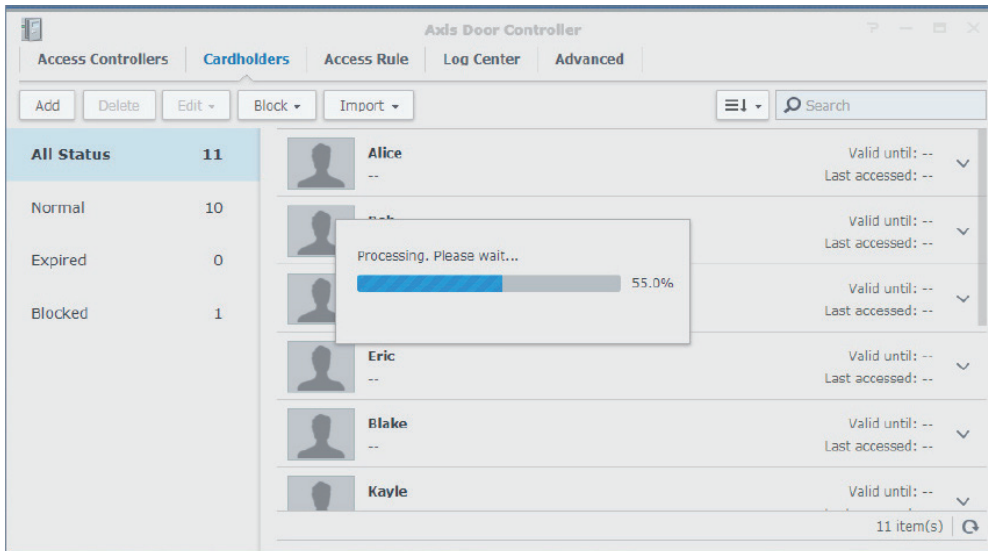
Credentials provides 4 credential configurations supported by AXIS A1001. Surveillance Station offers the retrieval of facility code, card numbers and rows from the last read on the card reader. After the reader reads the card provided and click **Retrieve**, the card number and row will be filled into its column. In this page validation period for cardholders can also be configured. Besides, if the cardholder is a disabled, long access duration can be enabled here to help pass in and out. Complete these credential configurations and then click **Next**.

Access Rule provides the option to add a new access rule here directly if needed (Please see section "**Access Rule**"). If the access rule has already existed, just select the access rules that should be applied to this cardholder and then click **Finish** to complete the creation of this cardholder.

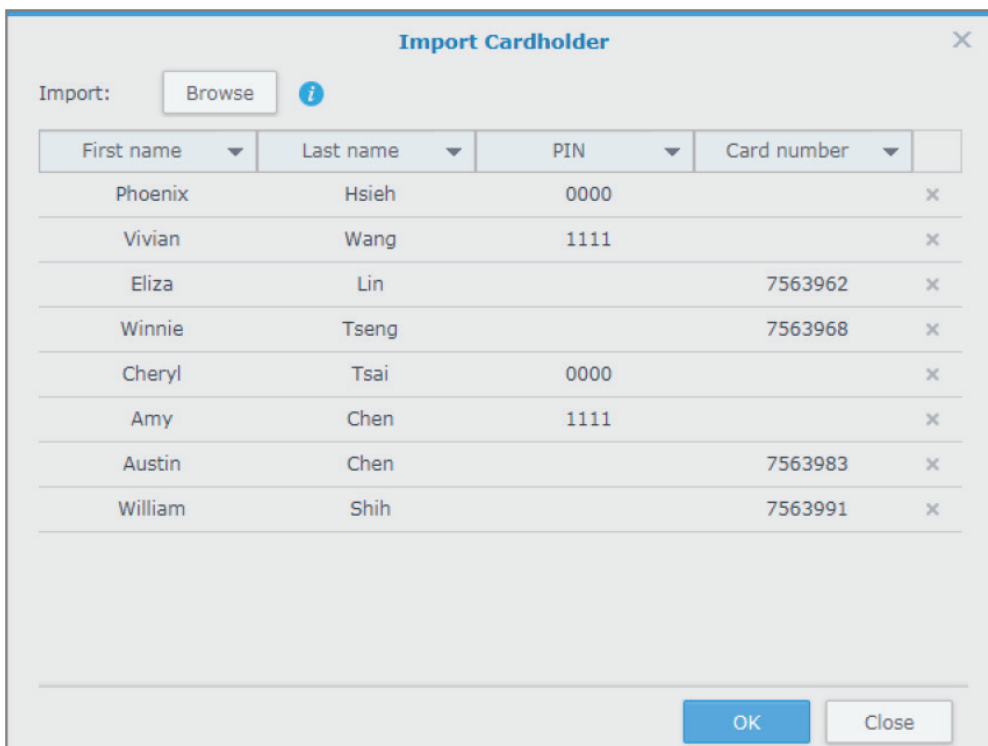


In Surveillance Station, cardholders can be edited anytime, just click **Edit**. You can also use the **Batch Edit** option to copy card information such as **Description, Department, Title, PIN,** and **Access Rule**, from a preset cardholder to other cardholders. However, you will not be allowed to copy **Employee NO., Extension, Card number,** and other private information. If administrators wish to block / unblock certain users, click **Block** for further operations.

Administrators can delete a certain user; however, that specific user needs to be registered again via the whole cardholder adding wizard. Block function offers the flexibility to remain this user in the system and all the access logs will still remain in the system.



When there are new cardholders on the controller, or when there is an exported file of the cardholders on the local client, the **Import** function can be used to synchronize cardholders from the controller or import cardholders from the exported file.

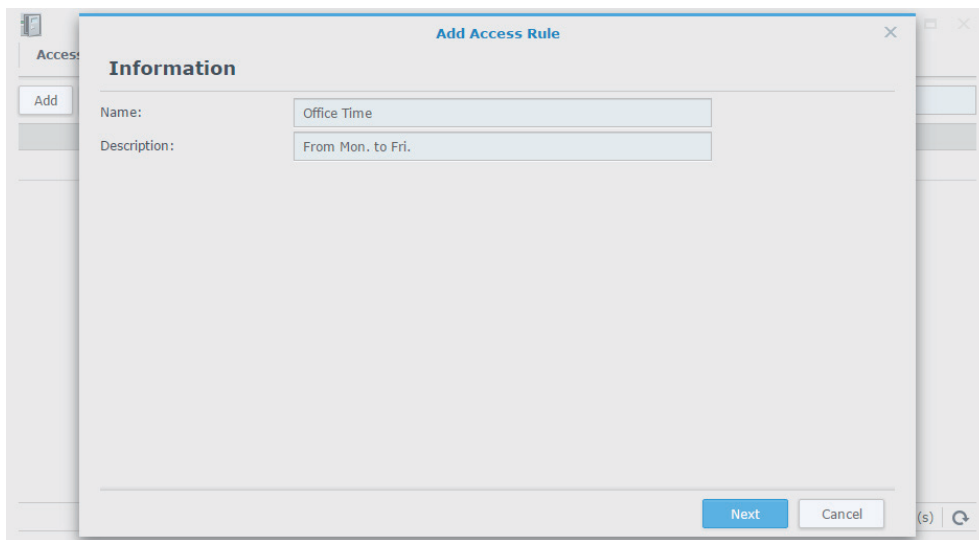


The **Import from file** function only supports csv format, and can only read the first four columns. You can export the file from the controller or create the file yourself. The imported cardholders must comply with the following rules:

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

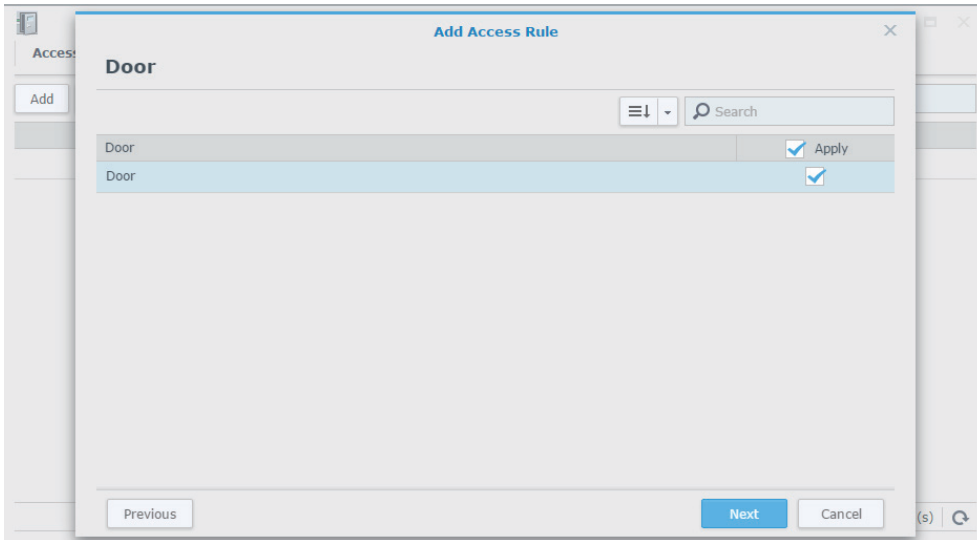
Access Rule

With **Access Rule**, you can set up rules to determine when and which door can be accessed. Access rules can be added directly in Surveillance Station with its intuitive user interface. Go to **Access Rule** tab and then click **Add**.

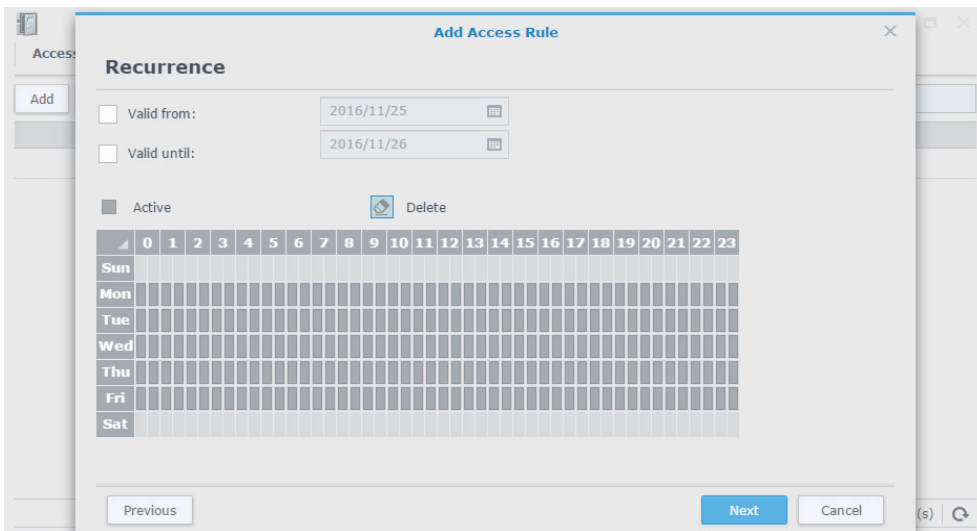


The screenshot shows a dialog box titled "Add Access Rule" with a tab labeled "Information". The dialog contains two input fields: "Name:" with the value "Office Time" and "Description:" with the value "From Mon. to Fri.". At the bottom right, there are "Next" and "Cancel" buttons. The dialog is overlaid on a background window with a sidebar containing an "Add" button.

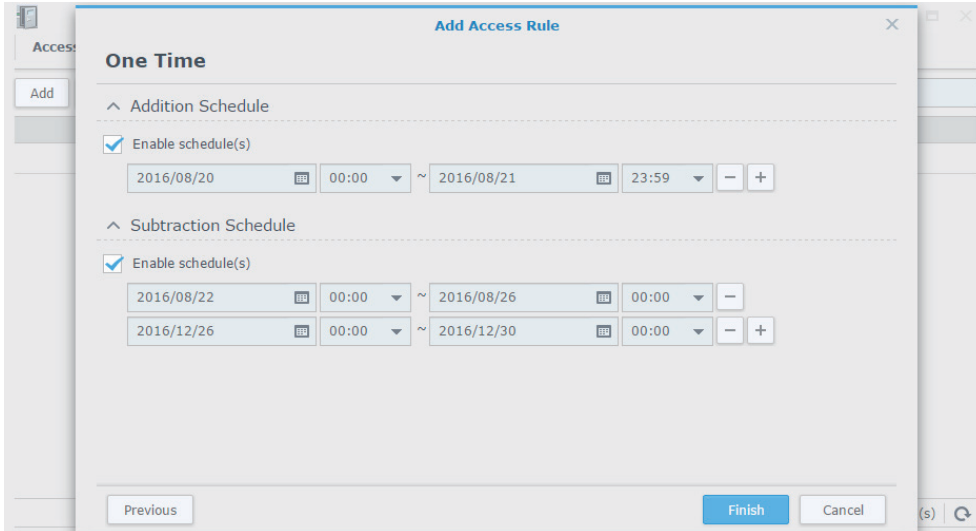
After filling up the basic information of the access rule click **Next**. The configuration in Door page will decide which door to be applied to this access rule. For example, if the access rule is set as accessible on holidays, then it is not suitable for the doors which should be accessible only on workdays. Select the doors to apply this access rule, then click **Next**.



The next two steps are related to the configuration of time which the doors selected on the previous step can be accessed. Recurrence provides a setting mode based on week cycle. In the sample screenshot below, you can see the general workdays (from Monday through Friday) are selected, and Saturday and Sunday are removed. If there is a requirement of valid duration, it can also be configured here. Otherwise, this access rule would be valid forever after created. After the configuration is complete, click **Next**.



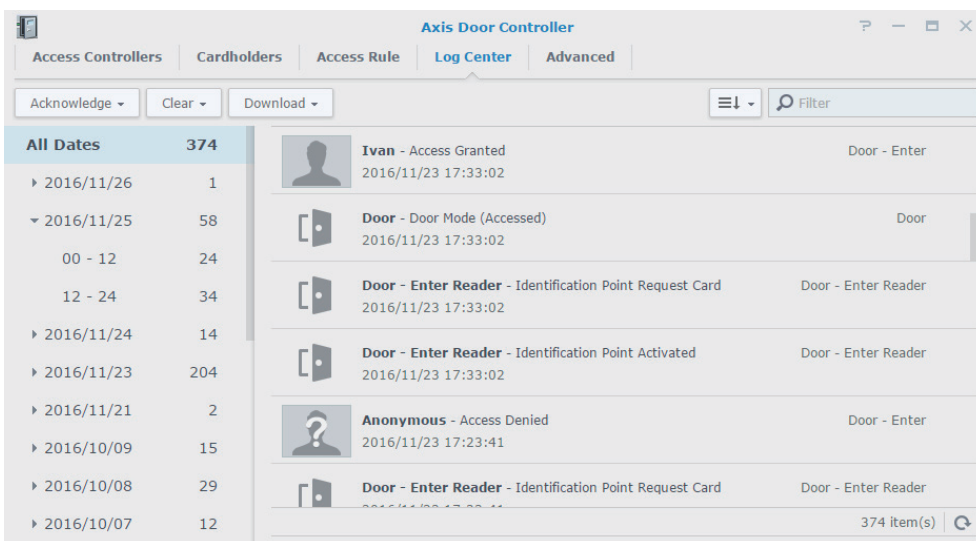
Moreover, you can use the **One Time** settings to set up exceptions from the **Recurrence** schedule configuration. For example, if there is an event held in company on this weekend, the date can be added into **Addition Schedule** to allow the door to be accessed. In contrast, if there is an incentive tour held on this Monday, the date can be added to **Subtraction Schedule** to prohibit the door to be accessed.



Surveillance Station provides multiple configurations for One Time schedule. It can be easily added or removed with the "+" or "-" buttons on the right hand side. Then click **Finish** to complete the creation of Access Rule.

Log Center

Log Center integrates all the event logs including the manual lock / unlock, cardholder block and all relevant events generated by AXIS A1001.

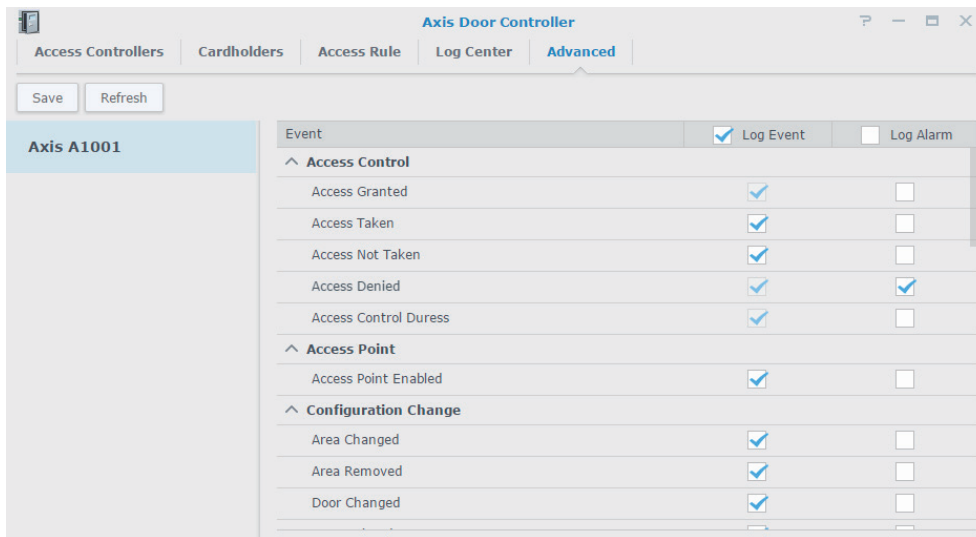


This tab provides different categories such as **Date**, **Status**, and **Controllers** so that administrators can easily find out the events that they are looking for. If an event is related to a door which is paired with a certain camera, click on the log icon to playback the recordings from the paired camera. A filter is also available for advanced search with **Source**, **Door**, **Status**, **Time interval**, and **Keywords**. The number of logs stored on AXIS A1001 can be up to 30,000, and Surveillance Station can store 60,000 logs for administrators.

Logs can be cleared and downloaded by clicking the buttons on the toolbar.

Advanced

In the **Advanced** tab, events are separated into two different columns, which are **Log Event** and **Log Alarm**.

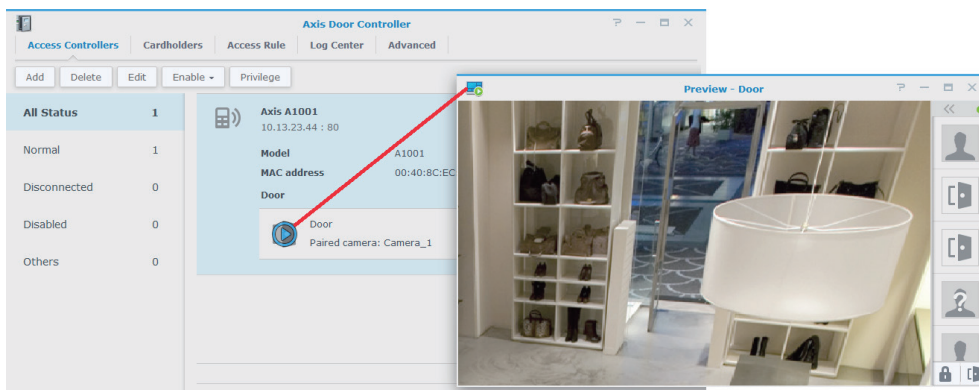


Some of the events are locked to be **Log Event** because these events are greatly important in Surveillance Station, so they need to be logged. However, administrators can choose to enable or disable a certain event to be an event log. If administrators wish to take a certain event as a log alarm and mark them in the **Log Center**, check the **Log Alarm** for a certain event.

Those events that are checked with **Log Alarm** will be marked as alarms when they occurred.

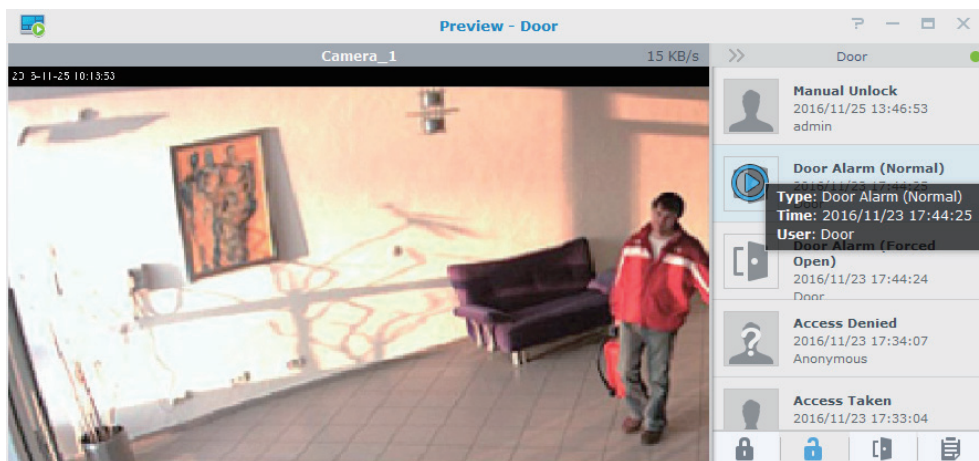
Use Synology Door Monitor with AXIS A1001

There are two different ways to implement the door monitor in Surveillance Station with AXIS A1001. To have a quick preview of the door monitor, click on the door icon right after the configuration of AXIS Door Controllers.



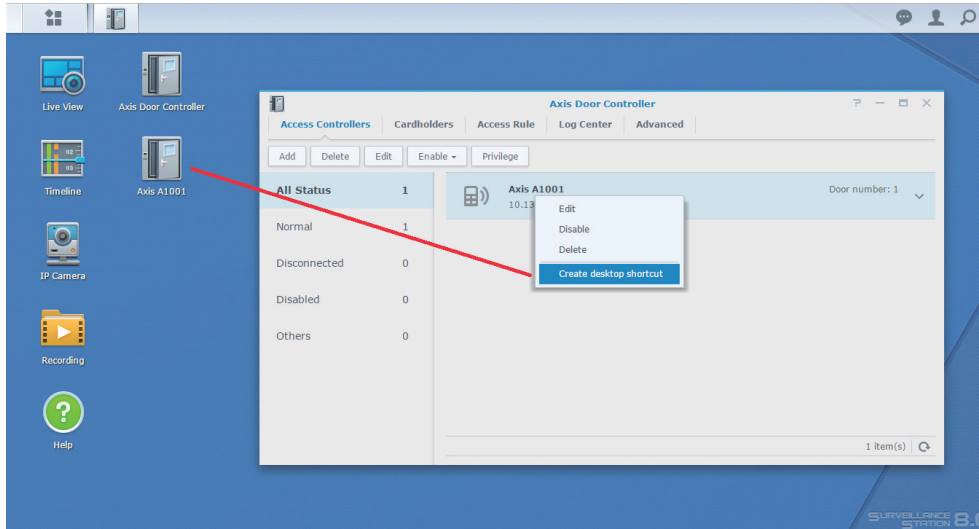
Door Preview

In the door previewer, administrators can check the access logs and their correspondent video sources. The access log tray can be expanded with more detailed information.



Desktop Shortcuts

Thanks to the desktop design in Surveillance Station 7, door units can be created as shortcuts on the desktop for easier management.

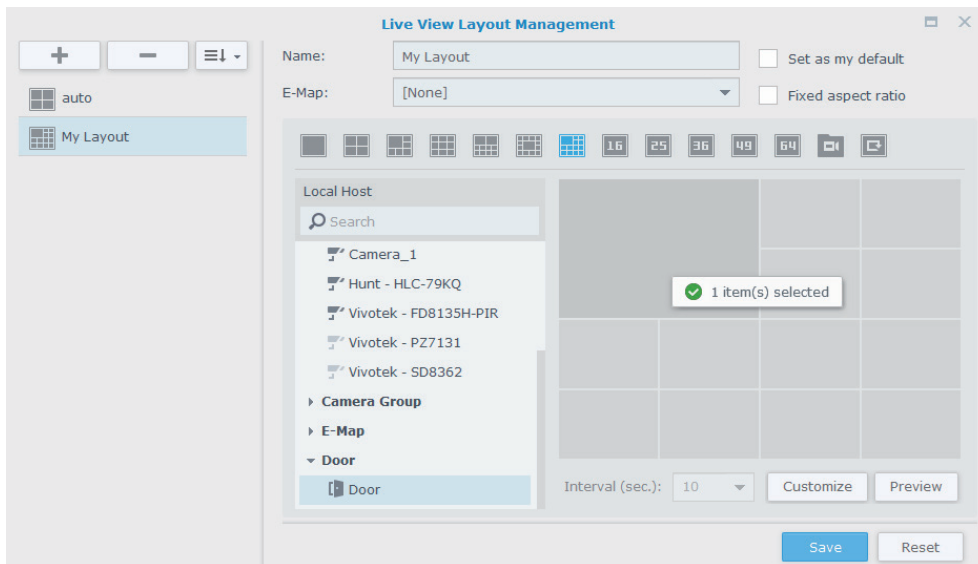


To create the shortcuts on the desktop, either right click on the door unit and select **Create desktop shortcut**, or drag and drop the items onto the desktop directly. To open up the Axis Door Controller application and focus on the specified controller at the same time, simply click the shortcuts on the desktop.

Door Viewer on Live View

Every time a door is created, a 1-channel layout will be created automatically. This layout contains only the door unit so that administrators can easily change the layout to check the access status and its paired video source.

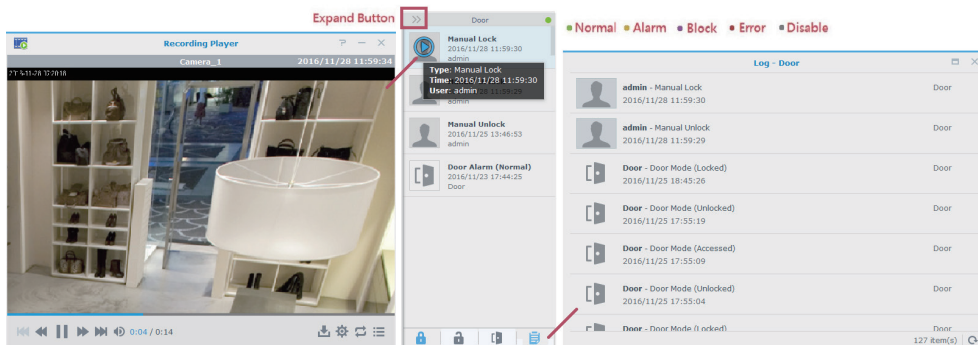
However, if administrators wish to check the door status within Live View, a door unit can be dragged and dropped into a separated Live View layout. Note that if a door unit is put into a Live View layout, it will occupy at least one quarter of the whole layout and Surveillance Station will merge the cells automatically.



This is to ensure the readability of the door status so that the size of the embedded door viewer will not be too small to read.

Door Viewer Operations

When checking on the door viewer, there are various operations that can be controlled by the administrators and users with permission.



- **Lock:** to permanently lock the door.
- **Unlock:** to permanently unlock the door.
- **Access:** to grant a temporary and anonymous access within the pre-configured access time.
- **Log:** to open up another window for viewing full event logs.

There will be a status indicator on the upper right corner, with five different statuses. Administrators can check on the door statuses with different colors of indicators. If more details are needed, simply hover the indicator, and then a tooltip will show up.

Door Units on E-map

Door units can be seen on the e-map as well.



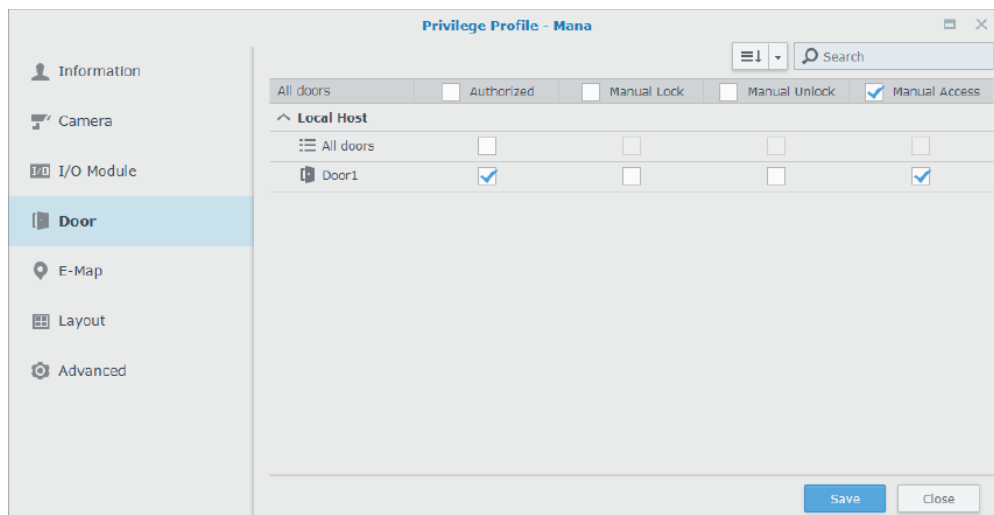
Surveillance Station offers three different statuses so that administrators can check on the statuses directly on the e-map. To have a direct preview of a certain door, simply click on the door icon on the e-map then the door preview will pop-out for further checking.

More applications

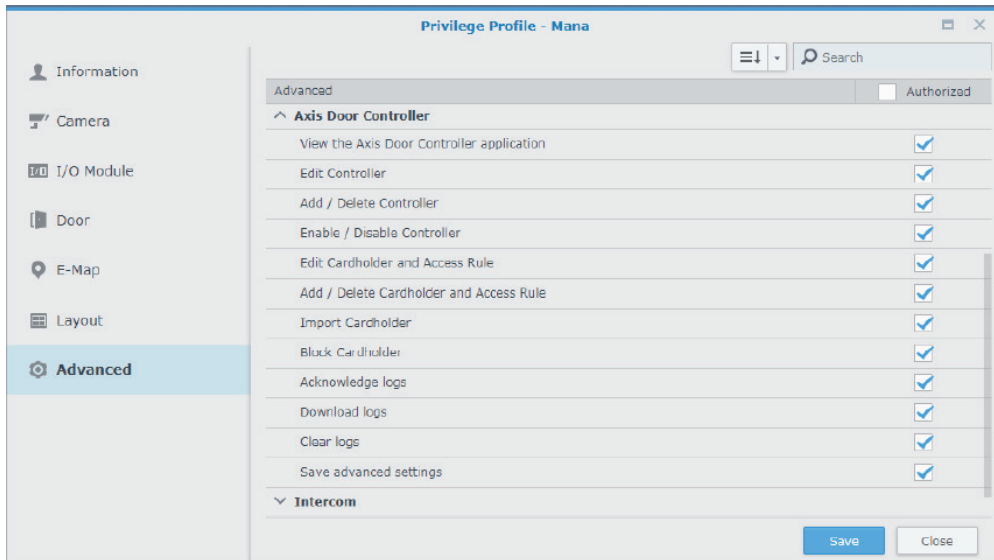
AXIS Door Controller in Surveillance Station can be implemented with other useful applications such as **Privilege**, **Action Rule** and **Notifications**.

User

It is not necessary to grant Surveillance users the privilege to control the door, therefore, administrators can configure the privilege settings of the door controller in **Privilege Profile** on the **User** application.

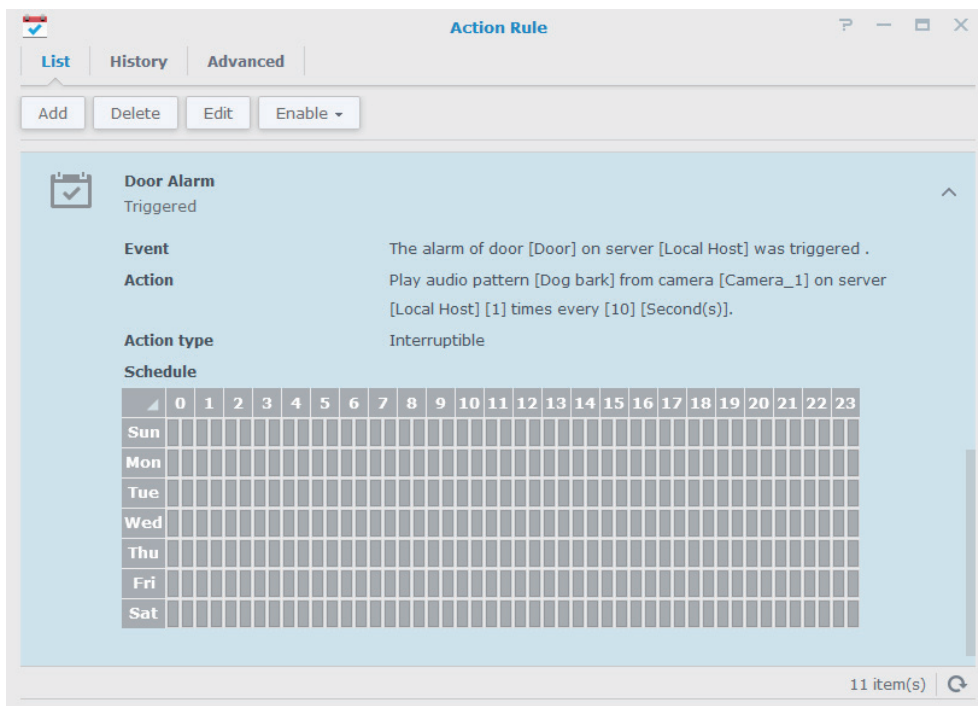


Manual Lock, **Manual Unlock**, and **Manual Access** are unique and important privileges that allow certain users to manually lock, unlock, and access the door. These options are required to be configured separately.



In the **Advanced** page, you can set up detailed privilege settings such as **View the Axis Door Controller application**, **Edit Controller**, **Add / Delete Controller**, **Enable / Disable Controller**, **Edit Cardholder and Access Rule**, and other log settings.

Action Rule



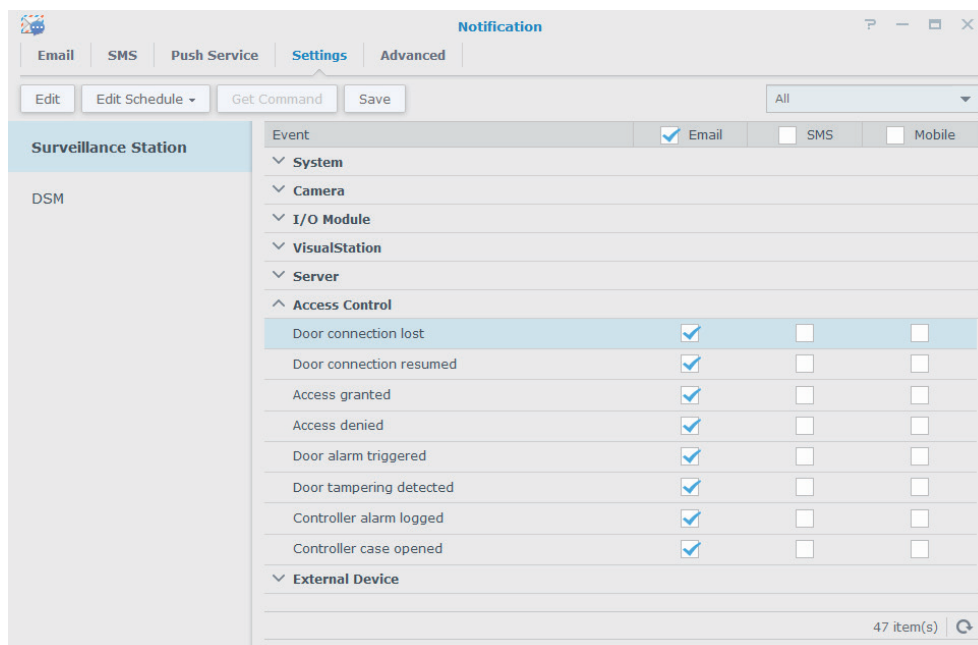
Action Rule is a dedicated application for configuring an action corresponding to a triggered or scheduled event. By setting up an **Action Rule** properly, Surveillance Station will execute certain actions automatically. In **Action Rule**, door alarm trigger can be treated as an event. With this event triggered, Surveillance Station may carry out a certain action in response to that event. Take the action rule below as an 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, either it is an open too long alarm or forced open alarm, the paired PTZ camera will go to the defined preset position to correspond to the event.

Notification

Surveillance Station supports push notifications via **SMS**, **E-mail**, and Synology mobile application **DS cam**.



Notification supports different messages from the Access Control, and the messages sent out to the administrators can be customized. Once an event is detected, Surveillance Station will notify the administrator with the selected methods.

If you choose to send a message via Email when the event **Access granted**, **Access denied**, **Door alarm triggered**, or **Door tampering detected** occurs, the system will automatically attach a snapshot taken from the paired camera in the message to help you immediately understand the current situation by capturing the surroundings of the door.

Before Upgrading to Surveillance Station 7.2.2 and Above

If AXIS A1001 was installed in the older version of Surveillance Station, there are some information you need to know before upgrading Surveillance Station to version 7.2.2 and above.

End of Support for Peer Connection

To enhance the performance of AXIS Door Controller A1001, Surveillance Station 7.2.2 redesigned the pairing mechanism. Therefore, the old mechanism of AXIS Peer Connection is no longer supported. If the controller already installed was in peer connection mode, please activate standalone mode first for the controller to work normally in Surveillance Station 7.2.2 and above. If there is no idea whether the controller is in standalone mode, you can check out the information in AXIS Entry Manager.

The screenshot shows the 'Setup / Manage Network Door Controllers in System' interface. It is divided into several sections:

- System status of this controller:** Contains a 'Status' section with a red box around the text 'This controller is in standalone mode.' Below it is a 'Deactivate standalone mode' button.
- Information:** A note stating: 'Note: When a controller is added to the system, it will keep its hardware configuration if one has been done. But all access management settings on the added controller (Users, groups, user-defined schedules, schedules for identification types for doors, and schedule-activated door states) will be deleted and overwritten by the system's access management settings.'
- Network door controllers in system:** Includes buttons for 'Add controllers to system from list', 'Add controller to system by IP or MAC address', and 'Refresh list of controllers'. Below these is a table with the following data:

Name	IP address	MAC address	Status
Axis A1001	10.13.23.118	AC:CC:8E:14:D4:0F	This controller

Note: After you activate the standalone mode, the access rules related to the controller will need to be set up again.

Cardholder in Controllers with the Same Name

In the old version of Surveillance Station, the data of cardholders belong to each controller itself when the controllers are in standalone mode. However, in Surveillance Station 7.2.2 and above, cardholders are unified controlled by the Surveillance Station. Therefore, if there are multiple standalone controllers installed in the old version of Surveillance Station, to make sure each cardholder can be kept in Surveillance Station after upgrading to version 7.2.2, the system would automatically add suffix to name of the second cardholder which has the same name as another cardholder. For example, if controller A and B has cardholder John at the same time, there would be cardholder John and John_1 in the system after upgrading.

This behavior does not affect the access of the existing cardholder. There are some suggested methods depended on different situations can sync the cardholder if required. In the above example, if John and John_1 are not the same person, please modify the name of cardholder through the interface of Surveillance Station directly. If John and John_1 are the same person, please add John into the groups John_1 joined on controller B through AXIS Entry Manager, then delete John_1 through the interface of Surveillance Station.

Privilege Settings

In the previous version of Surveillance Station, the user's privilege settings cannot be set up according to each individual door. After upgrading to Surveillance Station 8.1 and above, the original privilege settings for the door will be saved, while a simpler and more intuitive management interface will be provided.

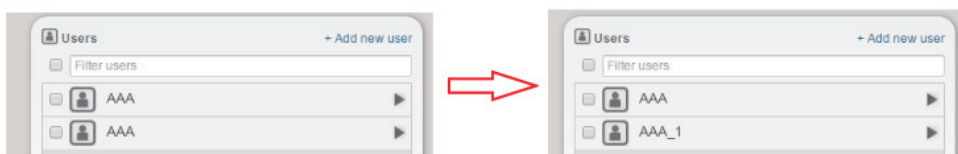
In Surveillance Station 8.1 and above, the privilege settings of doors are moved to the User application for centralized management. The purpose of the privilege settings transitioned from "setting up user authority for each door" to "setting door permissions for each user", and more privilege settings for controller management are added. You will be able to adjust permissions for each user more carefully in the User application.

Surveillance Station and AXIS Entry Manager Compatibility

We can modify users, schedules, groups, and doors via four modifiable settings in the AEM (AXIS Entry Manager). In all four settings, only the door hardware configuration and user information will be synchronized with Surveillance Station. For some settings, the configuration actions are performed one-way from Surveillance Station to A1001 so some of the original settings in A1001 will be overwritten by our system.

User and Cardholder

User information on A1001, will be synchronized with Surveillance Station Cardholder information when adding a new A1001 controller to Surveillance Station. Once the adding process is complete, the Cardholder information created in Surveillance Station will be synchronized back to all A1001 controllers to ensure Cardholder information in all controllers remains consistent. Unlike A1001, duplicate names are not allowed in Surveillance Station. During the process of retrieving User information from A1001, users with duplicate names and user information will be identified as the same person. Moreover, if there are more than one different user using the same name in A1001, an “_x” would be added after the name to separate them apart. Users can activate the synchronization process on their own via a button in Surveillance Station 8.0 and above.



Note: User names will be modified if they share identical names.

Identification type and door authentication

The door identification settings in A1001 will be synchronized with the door authentication settings in Surveillance Station after adding A1001. Once a controller is added, synchronization process will be activated every 24 hours. The hardware configuration (REX or Reader) will be retrieved and the door authentication settings in Surveillance Station will be synchronized back to A1001 during the synchronization process.

Group and Access Rule

The Group on A1001, which is specified as Access Rule in Surveillance Station, will not be synchronized with Surveillance Station since Surveillance Station has not fully support schedule settings yet. The schedule settings can not be displayed properly on our user interface though the schedule settings have been retrieved.

Therefore, even if groups have been set and are working in A1001, none of them will be shown in Surveillance Station. If you would like to establish an access control system with Surveillance Station, we strongly advise you to clear the Groups in A1001 first to avoid asynchronization. Also, we recommend not modifying the Group in A1001 on the web-based interface after the creation of Access Rule in Surveillance Station.

Schedules

Access schedules cannot be synchronized with Surveillance Station as we do not provide the interface for displaying and editing access schedules directly. However, access schedules can still be created in A1001 when editing Access Rules and the authentication schedules of doors.

Synchronization

If the settings of A1001 were modified and you want to ensure system consistency, you can activate the synchronization process mentioned above by disabling and enabling the controller.

Adding one controller to more than one Surveillance Station is not recommended. Performing simultaneous synchronization with different Surveillance Stations may cause unexpected behavior on the controller.



**SYNOLOGY
INC.**

9F, No. 1, Yuan Dong Rd.
Banqiao, New Taipei 220545
Taiwan
Tel: +886 2 2955 1814

**SYNOLOGY
AMERICA CORP.**

3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
Tel: +1 425 818 1587

**SYNOLOGY
UK LTD.**

Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL,
United Kingdom
Tel.: +44 (0)1908048029

**SYNOLOGY
FRANCE SARL**

102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
Tel: +33 147 176288

**SYNOLOGY
GMBH**

Grafenberger Allee 295
40237 Düsseldorf
Deutschland
Tel: +49 211 9666 9666

**SYNOLOGY
SHANGHAI**

200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

**SYNOLOGY
JAPAN CO., LTD.**

4F, No. 3-1-2, Higashikanda
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®



synology.com

Synology may make changes to specifications and product descriptions at any time, without notice. Copyright © 2021 Synology Inc. All rights reserved. ® Synology and other names of Synology Products are proprietary marks or registered trademarks of Synology Inc. Other products and company names mentioned herein are trademarks of their respective holders.