Synergis™ Cloud Link Administrator Guide

3.3.0

Click here for the most recent version of this document.

Document last updated: July 2, 2025

Legal notices

Document information

Document title: Synergis™ Cloud Link Administrator Guide 3.3.0

Original document number: EN.702.043-V3.3.0(2)

Document number: EN.702.043-V3.3.0(2)

Document update date: July 2, 2025

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide describes how to configure the Synergis Cloud Link appliance for use with Security Center, and explains how to integrate all supported third-party devices on your appliance. It assumes you are familiar with the Security Center platform, specifically with the Synergis access control system.

This guide supplements the following documentation:

- *Security Center Administrator Guide*
- *Synergis™ Cloud Link Hardware Installation Guide*
- *Synergis™ Softwire Integration Guide*

For more information, see the TechDoc Hub.

This guide does not include information that is available in third-party documentation, such as the details of the inputs and outputs found on your interface modules, nor does it describe any third-party software.

Terminology

In most contexts, *Synergis™ unit* (or *appliance*) and *Synergis Cloud Link unit* (or *appliance*) are used interchangeably. The word *appliance* is preferred when the focus is on the device itself, and the word *unit* is preferred when the focus is on the device's enrollment in Security Center.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

Chapter 10: DDS controllers

Chapter 11: HID VertX sub-panels

Chapter 12: Mercury controllers

Chapter 13: Allegion Schlage locks through Mercury

Chapter 14: BEST Wi-Q locks through Mercury

Part V: Additional resources

Chapter 20: Additional resources for Synergis Cloud Link units

Part I

Introduction

This part includes the following chapters:

1

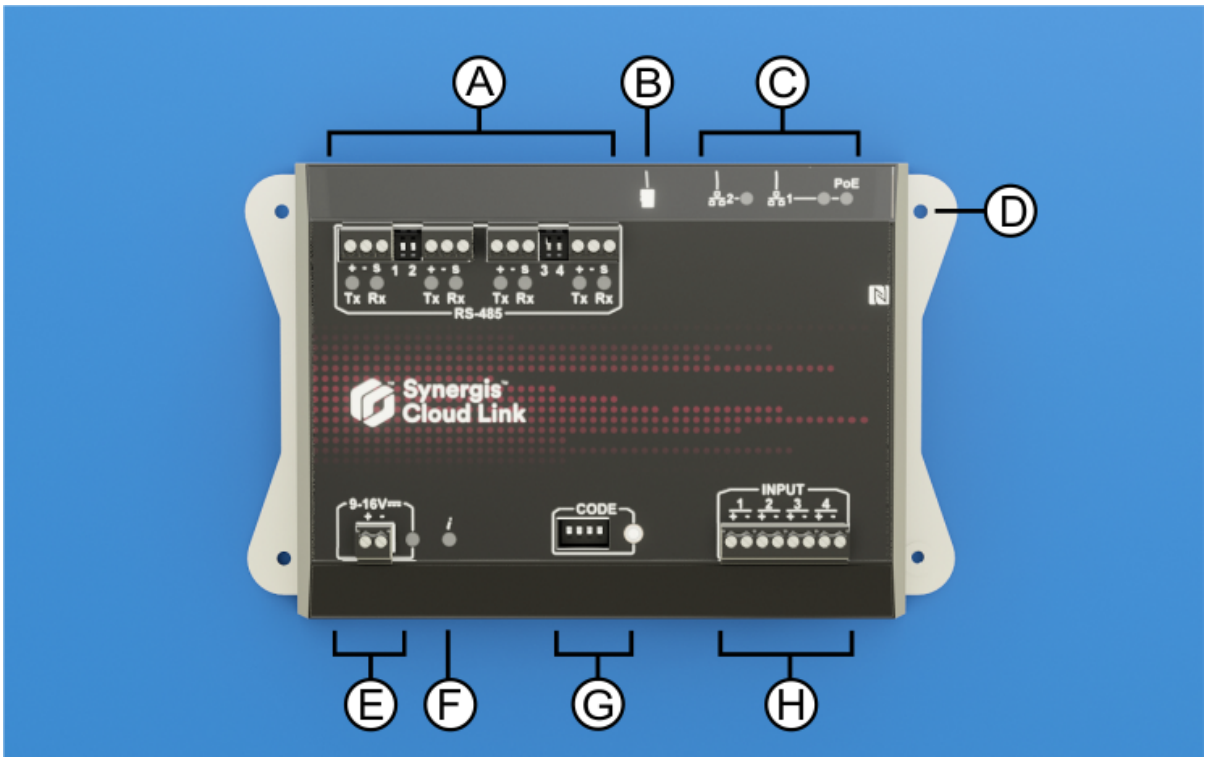
Introduction to Synergis Cloud Link

This section includes the following topics:

What is Synergis Cloud Link?

Synergis™ Cloud Link is an intelligent PoE-enabled IoT gateway designed to address the demand for a non-proprietary access control solution.

Synergis Cloud Link provides native support for popular non-proprietary security modules, from intelligent controllers such as Mercury Security, HID Global, and Axis communications, to electronic locks from ASSA ABLOY, Allegion, and SimonVoss, which requires Mercury controllers.



	Hardware feature	What you should know
A	RS-485 ports	Synergis Cloud Link includes four RS-485 communication channels. The number of modules you can connect to each RS-485 port depends on the type of interface modules you are installing.
B	Micro SD card	Future use
C	Ethernet ports	Two Ethernet ports are provided for connection to the IP network. **NOTE:** Ethernet port 1 can be used to power the appliance using Power over Ethernet (PoE).
D	Mounting holes	You can either mount the appliance to a suitable surface using the mounting holes or to a DIN rail using the optional DIN rail mounting bracket.
E	Power	Connect the appliance to a 12 V dc (nominal) power supply.
F	Information (*i*) LED	The LED provides feedback on system status.

	Hardware feature	What you should know
G	Command code DIP switches	The four CODE DIP switches allow you to run commands which can, for example, reset certain appliance configurations.
H	Monitoring inputs	The appliance includes four inputs that you can use to monitor external events in the access control system.

Related Topics

About Synergis Cloud Link 312 on page 6

Running DIP switch command codes

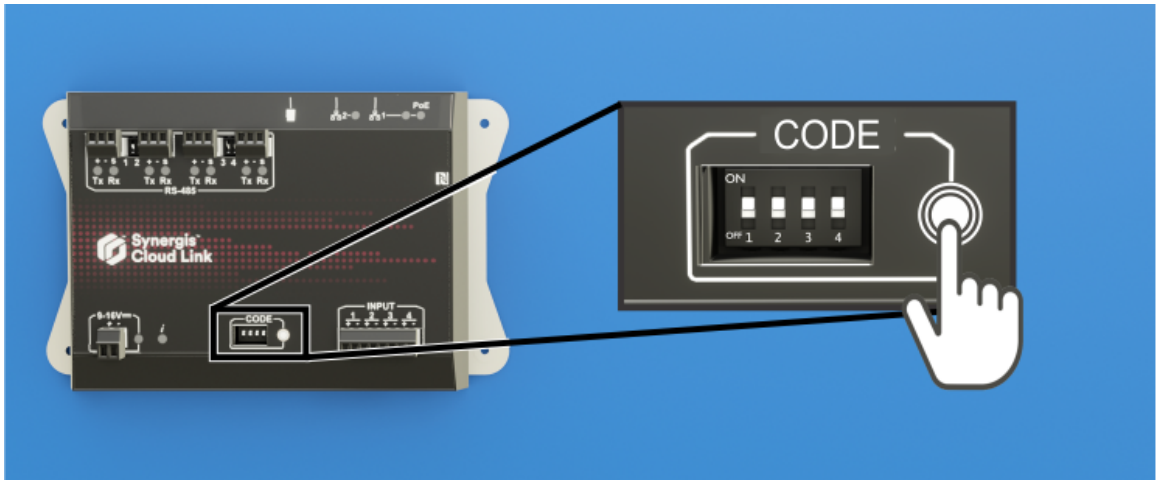
Synergis™ Cloud Link includes four CODE DIP switches on the front of the appliance. They allow you to run command codes, which can apply certain configurations and reset settings.

Procedure

1 Select a command code to run. For more information, see DIP switch command codes on page 5.

2 Enter the code with the DIP switches on the appliance.

3 Press and hold the command code button for 1 second.



The Information LED (*i*) confirms that the code was recognized.

LED name	LED color	Description
Information (*i*)	Orange: solid 3 seconds	DIP switch code recognized
	Red: 3 blinks	DIP switch code not recognized

4 To avoid an accidental configuration change, set the DIP switches to ON ON ON ON.

NOTE: There is no action associated with this code, making it a safe state when configuration is complete.

DIP switch command codes

By turning the four CODE DIP switches ON or OFF, you can apply a configuration to the Synergis™ Cloud Link appliance.

DIP switch commands

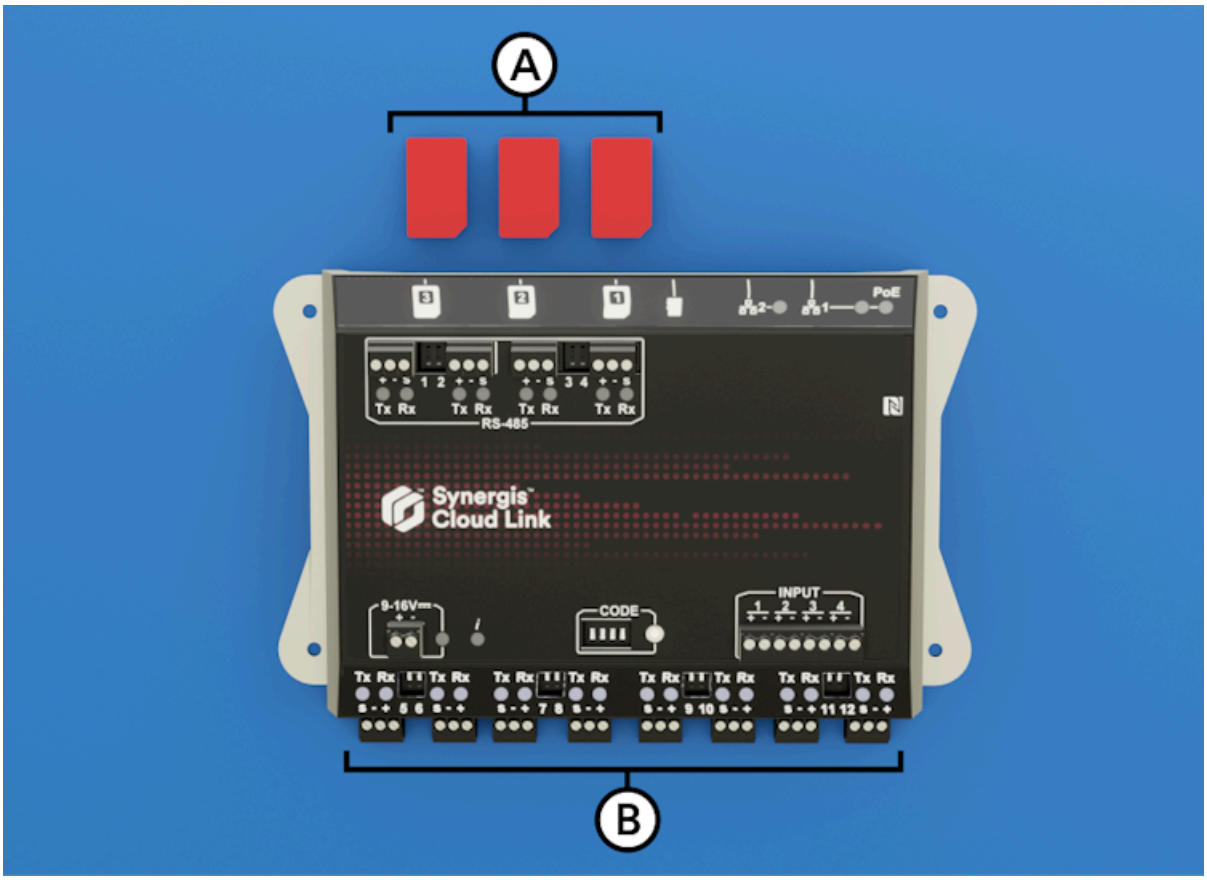
S1	S2	S3	S4	Command description
ON	ON	ON	ON	No code: After running a command code, to avoid an accidental configuration change, set the DIP switches to ON ON ON ON.
ON	OFF	OFF	OFF	Partial factory reset. This command has the following effects: • Resets the Synergis™ Appliance Portal logon password to factory default (softwire) • Removes the Synergis Cloud Link unit from the hosted Access Manager • Resets the network addressing mode to DHCP • Resets the discovery port to 2000 • Deletes all hardware (connected interface modules) configurations • Deletes all cardholder (credentials and access rules) configurations • Resets all unit-wide settings • Clears all logging options **NOTE:** This command doesn't affect the unit firmware.
ON	OFF	OFF	ON	Resets all settings to factory defaults and removes SSL certificates.
OFF	OFF	ON	OFF	Re-enables the ability to change output states from the *I/O diagnostics* page of the Synergis Appliance Portal.

Related Topics

Disabling output controls on page 38

About Synergis Cloud Link 312

Compared to the standard Synergis™ Cloud Link, the 312 model of the appliance includes eight additional RS-485 ports and three SAM card slots.



Letter	Hardware feature	What you should know
A	SAM card slots	You can use Secure Access Module (SAM) cards for encryption key storage.
B	RS-485	The Synergis Cloud Link 312 provides 8 additional RS-485 ports to the system for a total of 12.

NOTE: The Synergis Cloud Link 312 has not been evaluated for UL/ULC compliance and must not be used in installations where UL/ULC compliance is required.

For more information on Synergis Cloud Link 312 appliance, see Synergis Cloud Link 312 specifications.

Related Topics

What is Synergis Cloud Link? on page 3

2

Getting started with the Synergis Appliance Portal

This section includes the following topics:

What is the Synergis Appliance Portal?

The Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance and upgrade its firmware.

You can perform the following tasks through the portal:

- Change the password required to connect to the Synergis™ Cloud Link appliance.
- Configure the network settings on the appliance so it works on your system.
- Enroll and configure the interface modules connected to the appliance.

  NOTE: Mercury controllers and Honeywell controllers (PW6K1IC, PRO32IC, PW7K1IC, and PRO42IC) must be enrolled and configured on the access control unit's *Peripherals* page in Config Tool.
- Configure the access control behavior of the appliance for both online and offline operations.
- Test and diagnose the interface readers, I/O, and module connections of the appliance.
- Configure the settings specific to Mercury controllers and downstream controllers.
- Configure the reader LED and beeper settings with support for configuration export and import.
- Configure MIFARE DESFire on OSDP and STid readers.
- Enable SAM card-based cryptography on Synergis Cloud Link 312 appliance.
- Manage X.509 certificates.
- View and export the appliance's status and configuration.
- View the capabilities and status of Mercury controllers.
- Upgrade the appliance firmware and interface module firmware.
- Restart the appliance's hardware or software.

Tasks that must be done in Config Tool

You cannot perform the following tasks through the portal. Use Security Center Config Tool instead.

- Assign devices (input/output contacts, readers) to doors and zones.
- Configure individual door and zone properties.
- Configure I/O linking.
- Configure *Card and PIN* readers so that both the card and the PIN are required to grant access.

For more information about deploying Synergis, see the following chapters in the *Security Center Administrator Guide*:

- For configuring doors and *Card and PIN* readers, see Areas, doors, and elevators.
- For configuring zones and I/O linking, see Zones and intrusion detection.

Logging on to the Synergis Cloud Link appliance

To configure your Synergis™ Cloud Link appliance, log on to the appliance through the Synergis™ Appliance Portal.

Before you begin

The following information is required to log on for the first time:

- **Appliance hostname or IP address:** The default hostname consists of SCL (for Synergis Cloud Link), followed by the appliance's MAC address. For example, SCL0010F32CF482. The MAC address can be found on the appliance's label.

  To obtain the IP address, ping the appliance. For IPv6 IP addresses, you must remove the last two digits of the value in brackets that comes back from the ping. The IPv6 address includes the brackets. For example, [fe80::ebf:15ff:xxxx:xxxx].

- **Default username and password:** The default username and password are *admin* and *softwire*. You are forced to create a new password on first logon.

What you should know

- Starting in Synergis Cloud Link firmware 2.0.3, if you aren't using DHCP, you can connect using a link-local address. Before 2.0.3, IPv6 is required to use a link-local address.
- If you aren't using DHCP, alternate network connections prevent the Synergis Appliance Portal from loading.

Procedure

1 (First logon only) Connect the appliance's **LAN 1** port to your LAN.

2 Open a web browser, and enter `https://` followed by the appliance hostname or IP address.

Example: The following is an address using the hostname: `https://SCL0010F32CF482`

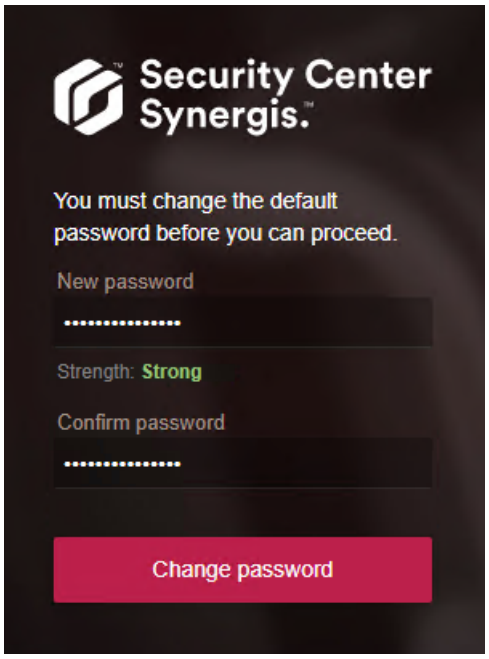
The following is an address using the IPv6 IP address format: `https://[fe80::ebf:15ff:xxxx:xxxx]`

3 If you opened a new browser session to log on to the appliance, you get a certificate error message. Follow your browser's on-screen instructions to continue to the website.

4 Enter the username and password, and then click **Log on**.

If you already changed the default password, the homepage is displayed. If you haven't changed the default password, you're forced to create a new one before logging on.

5 Enter a new *Strong* or *Very strong* password, confirm it, and then click **Change password**.
NOTE: The password must be at least 15 characters long.

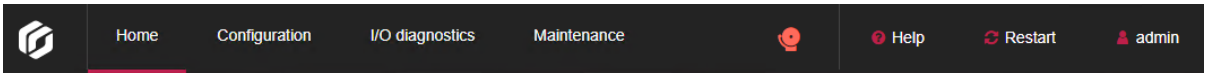


The password is updated for the user, and you must log on using the new password.

Interface tour of the Synergis Appliance Portal

The Synergis™ Appliance Portal homepage is divided into a top menu bar and a quick-access area with icons that lead to frequently used tasks. The homepage is dynamic and the icons vary depending on your context.

The main menu consists of the following:



- **Home:** Returns to the homepage.
- **Configuration:** Opens the *Hardware* page, where you can configure the interface modules attached to the Synergis™ Cloud Link unit. The following sub-pages are accessible from the *Configuration* page:
  - *Unit-wide parameters*
  - *Synergis Softwire logging*
  - *Network*
  - *Users*
  - *Mercury controller settings*
  - *Mercury triggers and procedures*
  - *Reader LED and beeper settings*
  - *Synergis IX controller settings*
  - *Automation engine*
  - *Downstream controller settings*
  - *Synergis key store*
  - *MIFARE DESFire*
  - *Advanced OSDP*
  - *Certificates*
  - *SAM card* (For Synergis Cloud Link 312 unit only)
  - *Cloud connectivity*
- **I/O diagnostics:** Opens the *Channels* page where you can monitor the state changes of the contacts and the credentials read on the readers as you trigger them. The following sub-pages are accessible from the *I/O diagnostics* page:
  - *Devices*
  - *Channels*
  - *Interfaces*
  - *Doors*
  - *Elevators*
  - *Hardware zones*
  - *I/O zones*
- **Maintenance:** Opens the *System status* page where you can view a snapshot of your unit and network status. You can also download configuration files from this page. The following sub-pages are accessible from the *Maintenance* page:

  - *Capabilities report*
  - *Log viewer*
  - *Download diagnostic logs*
  - *Ping diagnostics*
  - *Network capture* (For use by Genetec Technical Support)
  - *Interface upgrade*
  - *Firmware upgrade*
  - *Storage*
  - *Peer-to-peer*
  - *Download Synergis IX backup*
- **Notifications:** Displays system health warnings.
- **Help:** Opens a drop-down menu with two items:
  - *Help* opens the *Synergis™ Cloud Link Administrator Guide* in a separate browser page.
  - *About* shows the Synergis Cloud Link appliance firmware version and copyright information.
- **Restart:** Opens a drop-down menu where you select between **Software restart** or **System restart** to restart the Synergis Cloud Link unit hardware or software.
- **Administrator:** Opens a drop-down menu where you can log off the unit or select *User configuration*, where you can change the portal interface's language.

Part II

General configuration

This part includes the following chapters:

3

General configuration for Synergis Cloud Link

This section includes the following topics:

Preparing to configure the Synergis Cloud Link unit

Before you can configure a Synergis™ Cloud Link unit, you must perform some pre-configuration steps.

- Read the *Synergis™ Cloud Link Release Notes* for any known issues and other information about the release.
- Have a computer equipped with a network card, Ethernet cable, and a web browser.
- (Optional) Have the IP address assigned by your IT department to the Synergis Cloud Link unit.
- Configure the hardware settings (DIP switches, address dials, and so on) to their final position on the interface modules.
- Connect the interface modules to the Synergis Cloud Link unit through the proper communication channels.

  NOTE: Because each hardware manufacturer uses a different communication protocol, all interface modules connected to the same RS-485 channel must be from the same manufacturer.
- Connect physical devices (REX, door sensors, and so on), or use test switches and LEDs during the configuration phase.

  For more information, see the *Synergis™ Cloud Link Hardware Installation Guide*.
- Download the latest Synergis Cloud Link package from the *Product Download* page on GTAP.
- Install and configure Security Center with at least one Access Manager role.

  For information about deploying Synergis™, see the *Security Center Administrator Guide*.

After you finish

Configure your Synergis Cloud Link unit.

Configuring the Synergis Cloud Link unit

You can configure the Synergis™ Cloud Link unit after the pre-configuration steps are completed.

Before you begin

Perform the pre-configuration steps.

Procedure

1. All Synergis Cloud Link units come with a factory-assigned hostname. If your network does not support DHCP, you must assign the appliance a new IP address.
2. (Optional) Change the default X.509 certificate of the unit.
3. Upgrade the Synergis™ appliance firmware to the latest version.
4. Physically attach the interface modules to the Synergis Cloud Link unit.
   For information, see the *Synergis™ Cloud Link Hardware Installation Guide* on the TechDoc Hub.
5. Establish communication between the Synergis Cloud Link unit and its attached interface modules through the Synergis™ Appliance Portal.
6. Test your hardware connections and configuration and make adjustments if necessary.
7. Configure the access control behavior of the Synergis Cloud Link unit.
8. Add the Synergis Cloud Link unit to an Access Manager role so it becomes part of your Security Center system.

Configuring the network properties

To make sure the Synergis™ Cloud Link unit can be reached on your Security Center system's network, you must configure the unit's network properties.

What you should know

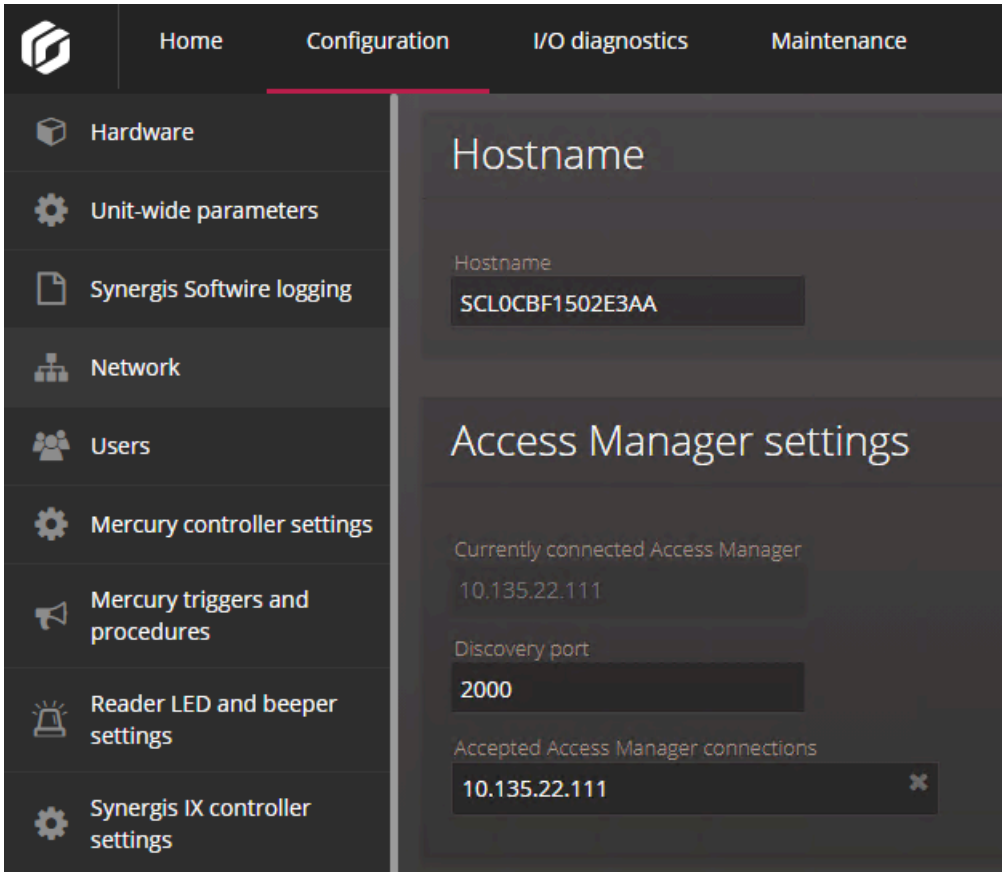
The Synergis Cloud Link unit comes with a factory-assigned hostname. If your network does not support DHCP, you must assign the unit a new IP address.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Network**.

3 (Optional) In the *Hostname* section, change the **Hostname** if required.



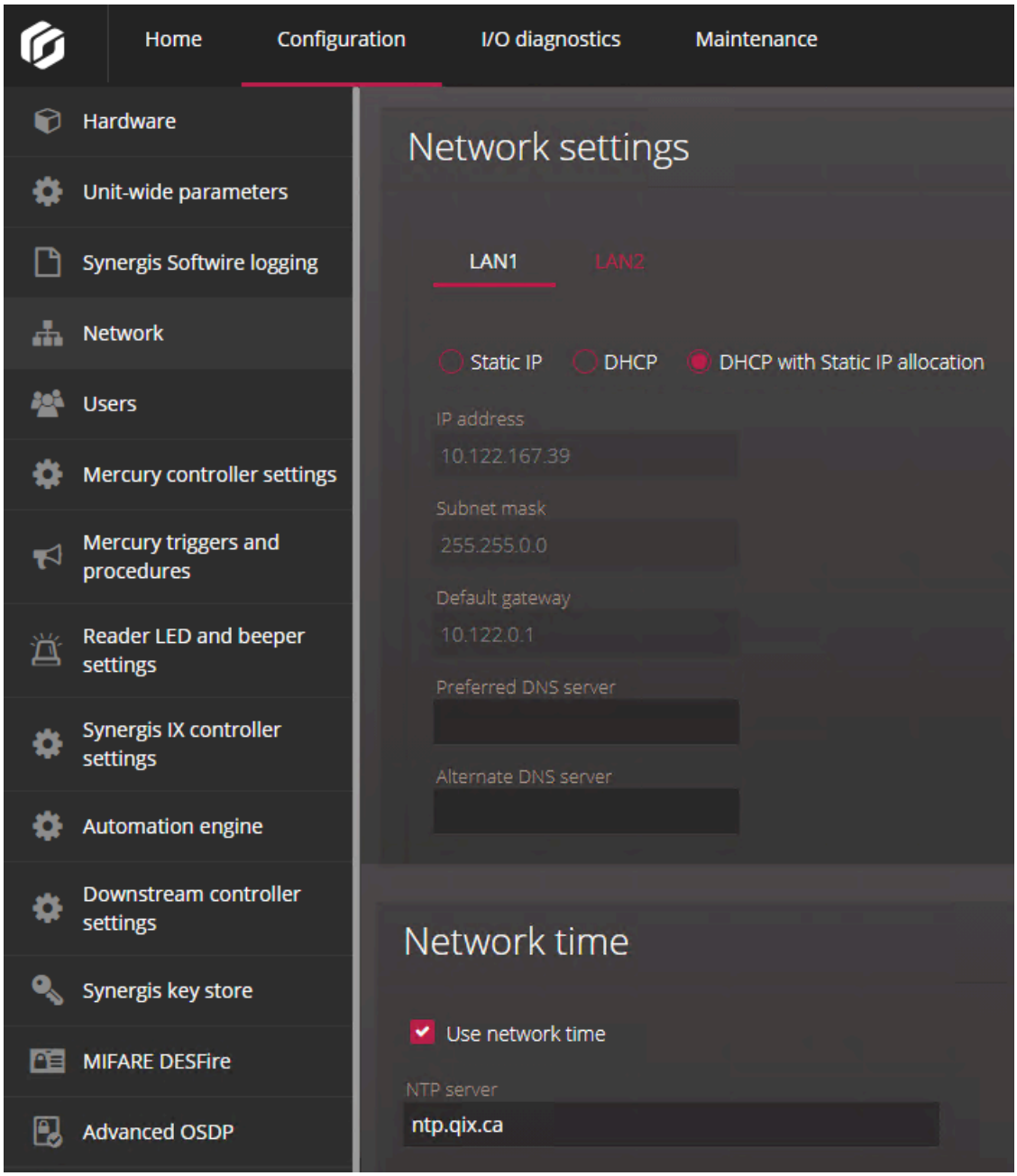
BEST PRACTICE: Hostnames must be unique on a network, and the default hostname is guaranteed to be unique. We therefore recommend that you keep the default hostname, which is found on the appliance's label.

4 In the *Access Manager settings* section, change the **Discovery port** if necessary.

5 In the *Network settings* section, select the **LAN1** or **LAN2** as the network interface used to connect the Synergis Cloud Link unit to its Access Manager, and then configure the Synergis Cloud Link unit's IP address and network properties.

IMPORTANT: To avoid network issues, strict rules must be followed when configuring the unit's network properties:

- If the unit is not on the same network segment as the Access Manager, then the unit's IP address must be set to **Static IP** or **DHCP with Static IP allocation**.
- **LAN1** and **LAN2** should not be on the same subnet. If they are, only one of them should be configured with a default gateway.



6 In the *Network time* section, configure the Network Time Protocol (NTP) server if one is available.

a) Click **Use network time** and enter the **NTP server** name.

BEST PRACTICE: An NTP server offers greater time accuracy than the built-in protocol that synchronizes the Synergis Cloud Link units with their Access Manager. Therefore, use the network time whenever

an NTP server is available on your network. All Security Center servers and workstations must be synchronized to the same NTP server as your Synergis Cloud Link appliances.

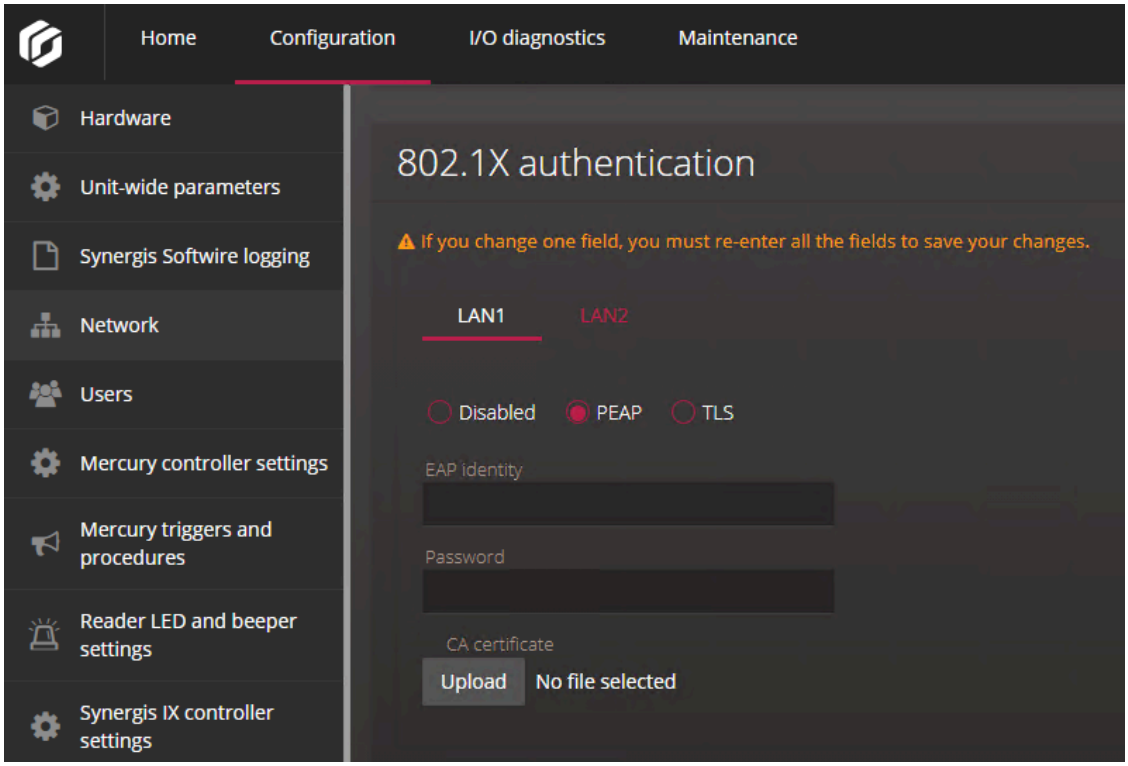
7 In the *802.1X authentication* section, select the LAN you want to use for 802.1X authentication and select the authentication mode.

NOTE: If you configured these settings once, their current values are displayed. If you need to change a value, you must re-enter all values. Otherwise, your change will not be saved.

- **Disabled:** The 802.1X authentication is disabled by default.
- **PEAP:** Use the Protected Extensible Authentication Protocol (PEAP).

  Enter the **EAP identity** (username) and **Password**, and upload the **CA certificate**.

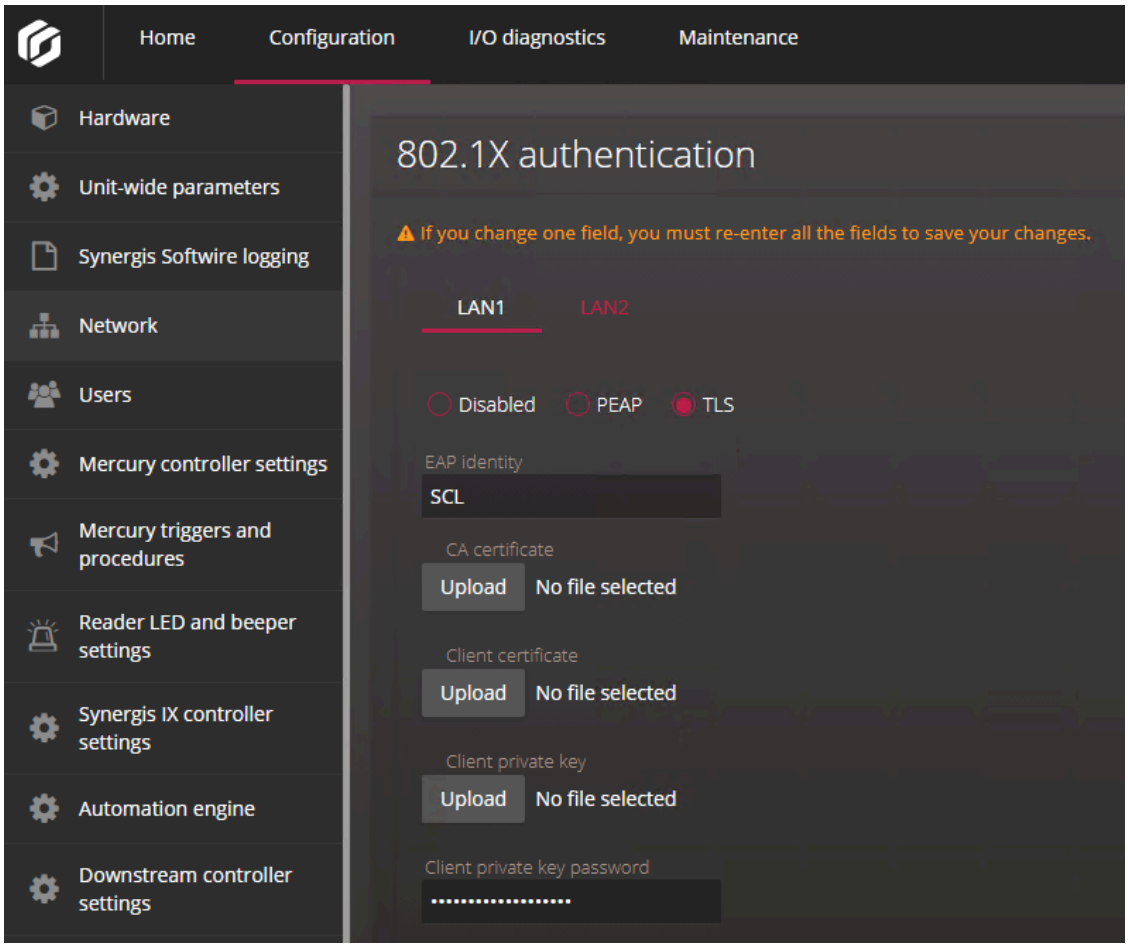
  NOTE: The CA certificate must be a PEM or DER file.



- **TLS:** Use the Transport Layer Security (TLS) protocol.

Enter the **EAP identity** (username), upload the **CA certificate**, **Client certificate**, and **Client private key**, and enter the **Client private key password**.

NOTE: The CA certificate must be a PEM or DER file.



8 Click **Save**.

The Synergis Cloud Link unit restarts, and you are automatically redirected to the unit's new IP address.

If you have enabled network time, the unit synchronizes with the NTP server 45 seconds after the setting is enabled, and then every 15 minutes.

Related Topics

Running DIP switch command codes on page 4

Using self-signed certificates

A Synergis™ Cloud Link comes with an X.509 certificate that was generated during production. Replace the default certificate to enhance security by generating a new self-signed certificate.

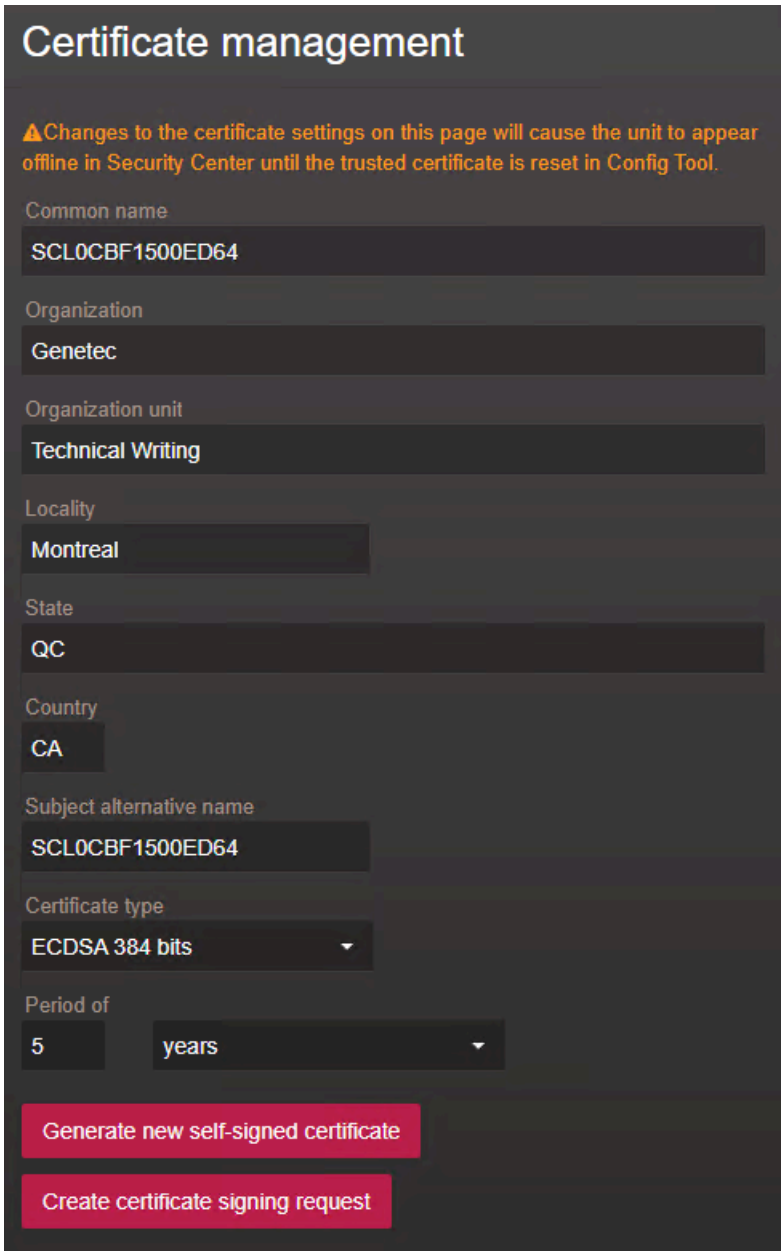
Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Certificates**.

3 In the *Certificate management* section, complete the identification fields.

NOTE: The **Common name**, **Subject alternative name**, and **Country** fields are mandatory.



4 From the **Certificate type** list, select one of the following algorithms and key lengths:
   - ECDSA 256 bits
   - ECDSA 384 bits
   - RSA 2048 bits
   - RSA 3072 bits
   - RSA 4096 bits

5 Click **Generate new self-signed certificate**, and then restart your browser and log back on to the unit.
   The certificate is now generated on the unit.

6 Install the certificate in the browser's certificate store.
   a) Click **Configuration** > **Certificates**.
   b) In the *Current certificate* section, click **Download**.
   c) In Windows, follow the instructions in the *Certificate Import Wizard* to import the certificate to the *Trusted Root Certification Authorities* folder using the **Local Machine** option.
      Install the certificate on all machines that connect to the updated Synergis Cloud Link unit.
      NOTE: The certificate file will be labeled with the hostname and a *.cer* suffix.

7 Restart your browser and log back on to the unit.

Your unit no longer shows a security error in the address bar when connecting using hostname.

After you finish

If the unit was already enrolled in Security Center, the Access Manager will not trust the new certificate or connect to the unit, and you must reset the trusted certificate in Config Tool.

For more information, see Resetting the trusted certificate .

Using trusted certificates

The authenticity of the self-signed certificate that comes with the unit by default is not enforced as usual with the Public Key Infrastructure. To be more secure, you can use a fully trusted certificate signed by a certificate authority instead.

What you should know

Using certificates signed by a certificate authority is better for setups where multiple computers and browsers access the Synergis™ Cloud Link unit because you do not need to configure each browser to recognize these trusted certificates.

Procedure

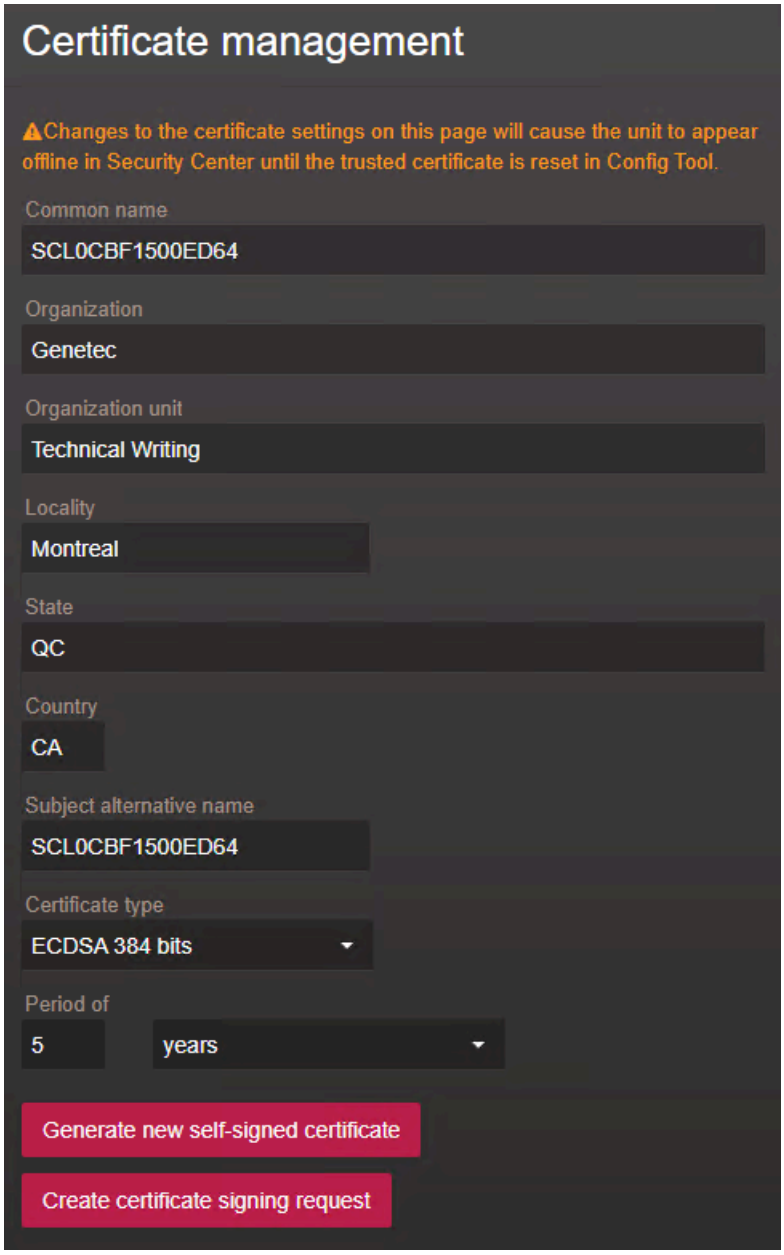
1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Certificates**.

3 In the *Certificate management* section, complete the identification fields.

The **Common name** field contains the unit's hostname by default. The **Subject alternative name** field also contains the hostname by default, but can be edited to a comma-separated DNS list.

NOTE: The **Common name**, **Subject alternative name**, and **Country** fields are mandatory.



4 From the **Certificate type** list, select one of the following algorithms and key lengths:

- ECDSA 256 bits
- ECDSA 384 bits
- RSA 2048 bits
- RSA 3072 bits
- RSA 4096 bits

5 Click **Create certificate signing request**.

A *.req* file is generated, containing the public portion of the certificate. The file does not contain the private key and is therefore not confidential.

6 In Windows File Explorer, navigate to your Downloads folder, and then copy the signing request *.req* file and send it to a certificate authority.

After verification, the certificate authority signs the public portion of the certificate with its own private key.

7 After you receive the certificates from the certificate authority, import the signed certificate.

a) Log back on to the unit and click **Configuration** > **Certificates**.

b) In the *Import signed certificate* section, click **Select certificate** and browse to the folder with the certificates.

c) Select the first certificate and click **Upload**. Repeat for the remaining certificates.

NOTE: Each certificate in the certificate chain must be uploaded individually, or in one operation if you received a *.p7b* collection file. If you received the collection file, you can omit uploading the root certificate.

Your unit no longer shows a security error in the address bar when connecting using hostname.

After you finish

If the unit was already enrolled in Security Center, the Access Manager will not trust the new certificate or connect to the unit, and you must reset the trusted certificate in Config Tool.

For more information, see Resetting the trusted certificate .

Configuring interface modules connected to the Synergis Cloud Link unit

To establish communication between the Synergis™ Cloud Link unit and the connected interface modules, you must configure them in the Synergis™ Appliance Portal.

Before you begin

Physically connect your interface modules to the Synergis Cloud Link unit.

What you should know

An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

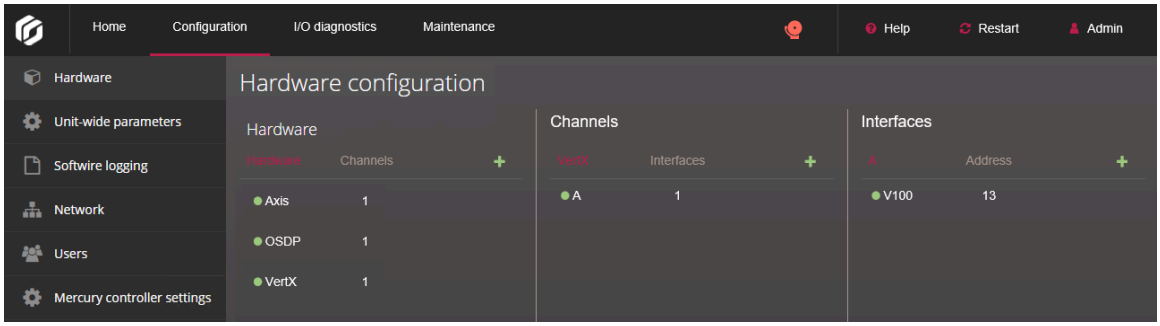
NOTE: Mercury LP and MP controllers and Honeywell controllers (PW6K1IC, PRO32IC, PW7K1IC, and PRO42IC) must be enrolled and configured from Security Center Config Tool on the access control unit's *Peripherals* page.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

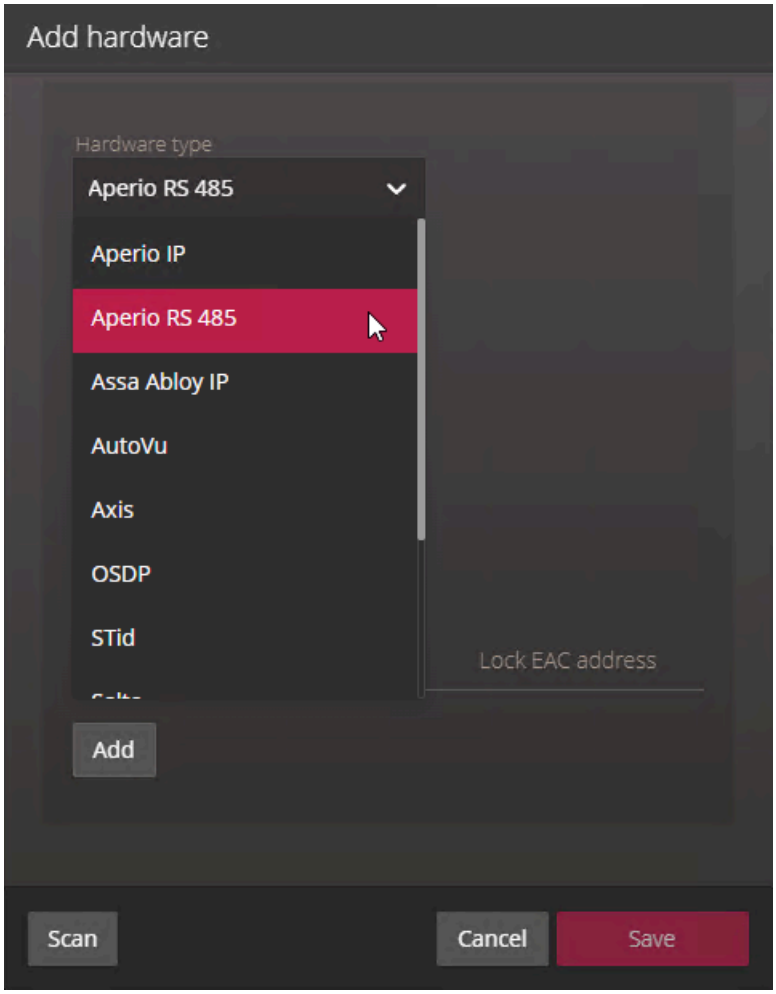
The portal shows the hardware tree as three columns. The information displayed in each column varies depending on what you select in the previous column:



- **Hardware:** Your configured hardware manufacturers and the number of channels they use. Clicking a hardware manufacturer displays its channels in the second column.
- **Channels:** The channels of the manufacturer selected in the first column. Hovering over a channel displays the edit (), clone (), and delete () options.
- **Interfaces:** The interface modules connected to the channel selected in the second column.

3 At the top of the **Hardware** column, click **Add** ().

4 In the *Add hardware* dialog box, select the **Hardware type**, the **Channel**, and the rest of the interface module properties, which depend on the hardware type you selected.



5 In the same dialog box, add all interface modules connected to the same channel as follows:

- To add the interface modules manually, click **Add**.
- To discover the interface modules, click **Scan**.

  Interface modules from the same manufacturer and connected to the same channel must use the same baud rate and be configured with a different physical address to be added to the list.

6 Click **Save**.

The hardware type, channel, and interface modules you added are displayed in the hardware tree.

7 For each interface module you added, select it from the hardware tree and click , then configure its settings in the window that opens.

For the description of these settings, refer to the manufacturer's documentation.

8 At the bottom of the page, click **Save**.

After you finish

Test the interface modules.

Changing default settings of interface modules

To simplify the configuration process when you have many interface modules of the type to configure, you can modify factory default settings and save them as the new default settings for each type of module.

What you should know

The Synergis™ Cloud Link unit is configured with factory default settings for all supported interface modules.

Procedure

1 Click **Configuration** > **Hardware**.

2 From the *Hardware configuration* page, select the manufacturer, channel, and interface you want to use as the model.

3 In the *Edit* dialog box, make all necessary changes to its settings.

4 Click **Set as default** and save.

Your changes are saved as new default settings. The next time you add an interface module of the same type, your new default values will be used to initialize the *Properties* page.

Clearing custom default settings of interface modules

If you have created custom default settings for interface modules and you want to revert to using the factory default settings when adding new interface modules, you can clear the custom default settings.

What you should know

IMPORTANT: Do not confuse the **Delete default** button with the **Reset to factory settings** button.

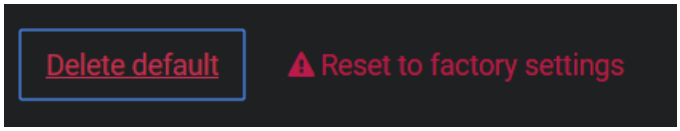
- Clicking **Delete default** only discontinues the use of your custom default settings so that the factory default values are used the next time you add an interface module of the same type.
- Clicking **Reset to factory settings** resets the values on the current page to their factory defaults when you save.

Procedure

1 Click **Configuration** > **Hardware**.

2 On the *Hardware* page, select the interface module you set as default.

3 In the *Edit* dialog, click **Delete default**.



Cloning interface module settings

To save time on configuration, you can add new interface modules by duplicating the settings of an existing interface module, and then make changes if required.

Before you begin

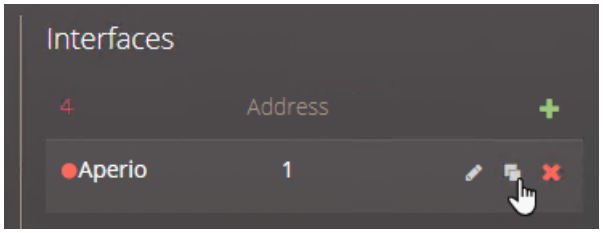
If you want to clone your interface modules, but you have already created the new ones, then delete the new ones.

Procedure

1 Click **Configuration** > **Hardware**.

2 In the *Hardware configuration* section, select the interface module you want to clone from the hardware tree.

3 Click .



4 In the *Clone hardware* dialog box, add all the interface modules you want to add based on the selected model, and then click **Save**.

You only need to specify the physical address of each new interface module and the channel it is connected to. All other settings are copied from the model interface module.

After you finish

Modify the settings of the cloned interface modules as required.

Testing the connected interface modules

You can test your hardware connections and configuration by monitoring their responses in real time on the *I/O diagnostics* page of the Synergis™ Appliance Portal.

Before you begin

Configure the interface modules.

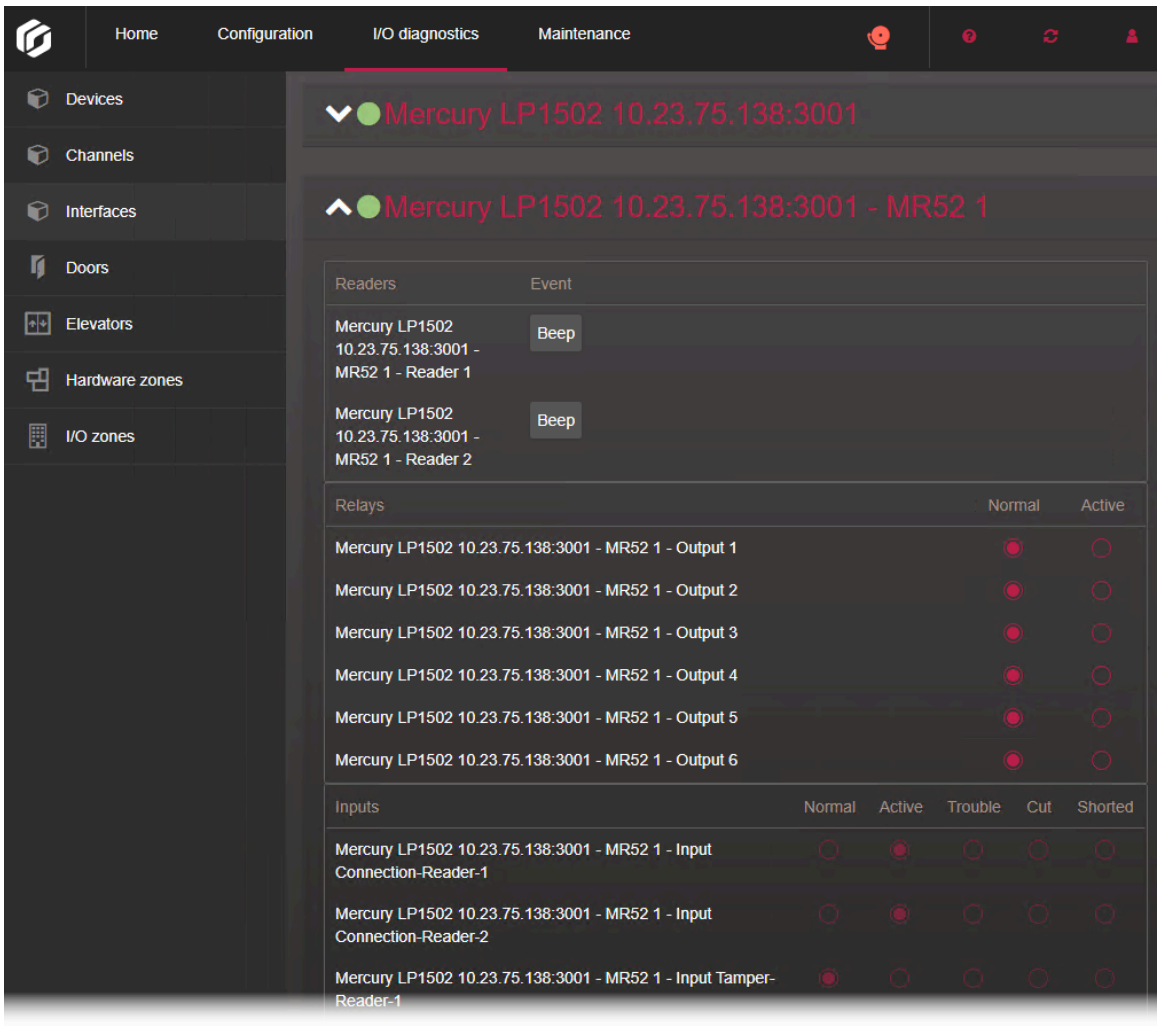
What you should know

You can customize the page to show the elements that you want to monitor.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **I/O diagnostics** > **Interfaces**.



3 Click to expand the interface you want to monitor.

4 Activate the devices (card readers, door sensors, door locks, and so on) connected to the Synergis Cloud Link unit through the interface modules.

If they do not behave as expected, check your connections and your interface module configurations.

Configuring unit-wide parameters

Most interface module behavior is common to all interface modules connected to the same Synergis™ Cloud Link unit. You can configure these unit-wide settings on the *Unit-wide parameters* page of the Synergis™ Appliance Portal.

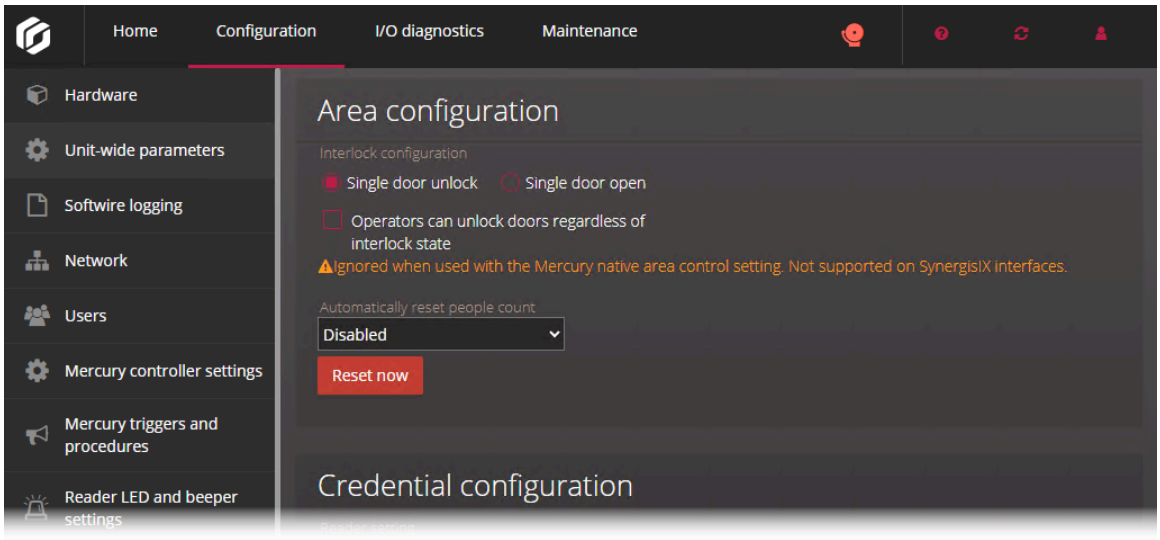
What you should know

The following procedure describes all the options on the *Unit-wide parameters* page. Configure them for your system needs.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Unit-wide parameters**.



3 In the *Area configuration* section, configure the following options:

- **Interlock configuration:** An interlock is a system with multiple doors where only one door can be opened at any time. You have two options:
  - **Single door unlock:** Only unlock one door at any given time.
  - **Single door open:** The moment one door is open, immediately lock all other doors.
  - **Operators can unlock doors regardless of interlock state:** Allow doors to be manually unlocked using the **Unlock** button in the *Door* widget, even when the doors should be locked because of interlock. You can use this setting with either of the interlock settings, **Single door unlock** or **Single door open**.
    This setting must be configured for each Synergis Cloud Link unit that controls doors configured in an interlock, and changing this setting requires a software restart.
    NOTE: This setting is not supported with Synergis™ IX integrations, and is ignored when used with any of the following native Mercury capabilities:
    - Antipassback
    - Max occupancy
    - Interlock
  - **Automatically reset people count:** Reset people count daily or weekly. Disabled by default.

4 In the *Credential configuration* section, configure the following options:

- **Reader setting:** Applies to Card and PIN readers only. You have two options:
  - **Card or PIN:** Either the card or the PIN can be used to grant access.
  - **Card only:** Only the card is used to grant access.

  NOTE: To enforce *Card and PIN* mode so that both the card and the PIN are used to gain access, you must configure the reader settings in Config Tool. *Card and PIN* mode only works during the reader schedule. Outside of the reader schedule, the reader behaves in either *Card only* or *Card or PIN* mode, depending on the reader settings configured in the Synergis Appliance Portal.
- **Maximum PIN length:** The Synergis Cloud Link unit processes the PIN being entered the moment it reaches the maximum number of digits, without waiting for the '#' key.

  NOTE: Not all integrations support this feature. For more information, see the *Synergis™ Softwire Integration Guide*.

5 In the *Output controls* section, configure the following option:

- **Disable output controls:** Click to disable the ability to change output states from the *I/O diagnostics* page of the Synergis Appliance Portal.

6 Click **Save**.

All changes take effect after a software restart.

Related Topics

DIP switch command codes on page 5
Enabling key versioning for SAM cards on page 50
Disabling output controls on page 38

Configuring reader LED and beeper settings

You can configure the reader LED and beeper behavior to communicate various access control states to the person standing at a door. For example, you can make the LED flash in amber color when the system is waiting for a PIN to be entered.

Before you begin

At the moment, this feature is only supported for Mercury-controlled readers.

What you should know

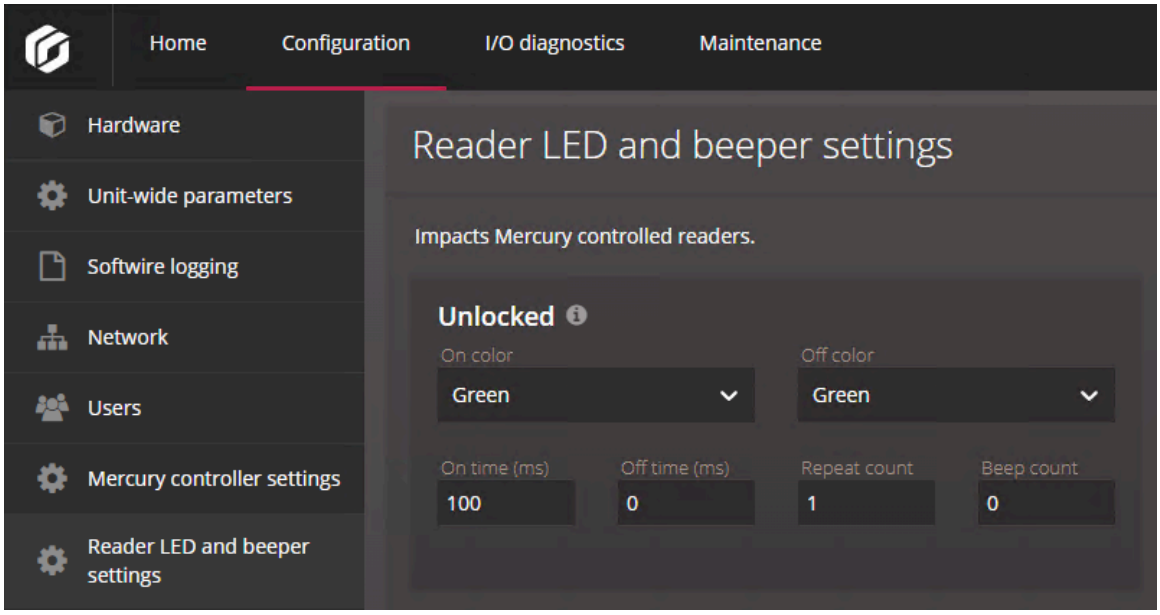
You can indicate with a unique reader LED and beeper behavior the following access control states:

- **Unlocked:** The door is unlocked for maintenance, by a schedule, or by temporarily overriding a schedule.
- **Shunted:** The reader is shunted (deactivated).
- **Card only:** The door is locked while the reader operates in *Card only* mode.
- **Card and PIN:** The door is locked while the reader operates in *Card and PIN* mode.
- **Card or PIN:** The door is locked while the reader operates in *Card or PIN* mode.
- **Access denied:** An access request is denied.
- **Access granted:** An access request is granted, or the door is manually unlocked.
- **Prompt for PIN:** The system is waiting for a PIN to be entered. To have this, the reader must operate in *Card and PIN* mode.
- **Prompt for second cardholder:** The system is waiting for a second credential to be presented. This happens when a two-person rule or a visitor escort rule is in effect.
- **Door alarm:** Either the *Door open too long* or the *Door forced open* alarm has been triggered.
- **Wait:** The system is waiting for a biometric credential to be presented, or for an external system to validate a credential.

Procedure

1 Log on the Synergis™ Cloud Link unit.

2 Click **Configuration** > **Reader LED and beeper settings**.



3 For each door state, configure how you want the reader to behave:

- **On color:** Color of the LED when the door transitions into this state.
- **On time (ms):** Time in milliseconds the LED remains in the 'On' color.
- **Off color:** Alternating color of the LED.
- **Off time (ms):** Time in milliseconds the LED remains in the 'Off' color.
- **Repeat count:** Number of times the LED goes through the 'On' color - 'Off' color cycle.
- **Beep count:** Number of times the reader should beep.

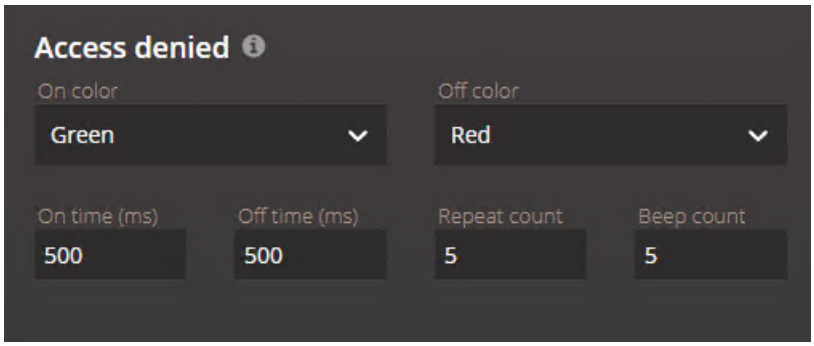
The LED and the beeper start at the same time. The LED behavior lasts *((On time + Off time) x Repeat count)* milliseconds. This behavior is interrupted when the door changes to another state.

NOTE: The volume and duration of the beep cannot be controlled.

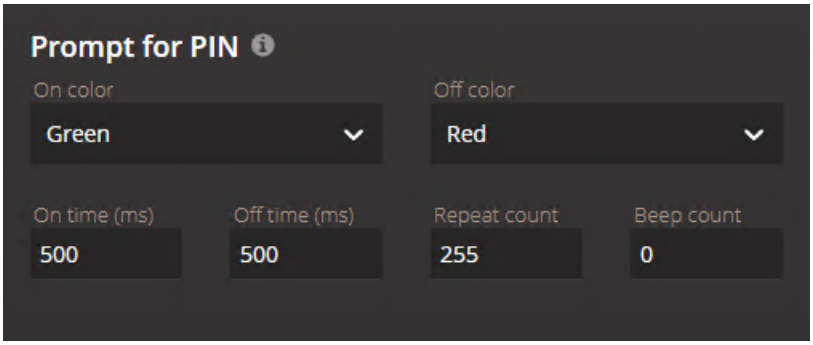
4 Click **Save**.

Example

- **Example 1:** To make the LED flash red and green for up to 5 seconds and beep five times when access is denied at a door, use the following settings.



- **Example 2:** To prompt the user to enter a PIN by flashing rapidly the LED in amber color until the PIN is entered without beeping, use the following settings.


Prompt for PIN
On color
Green
Off color
Red
On time (ms)
500
Off time (ms)
500
Repeat count
255
Beep count
0

Copying the reader LED and beeper settings from one unit to another

You can export the LED and beeper settings from one Synergis™ Cloud Link unit and import them into other Synergis Cloud Link units.

Before you begin

Configure the reader LED and beeper settings for a first Synergis Cloud Link unit.

What you should know

The reader LED and beeper settings are unit-wide parameters. However, only Mercury-controlled readers are supported for the time being.

Procedure

1 Log on to the Synergis Cloud Link unit you want to copy from.

2 Click **Configuration** > **Reader LED and beeper settings**.

3 Click **Export**.

The LED and beeper settings are saved to a file named *LedConfig<Hostname>_yyyy-mm-dd_hh_mm_ss.xml*, where *<Hostname>* is the hostname of the Synergis Cloud Link unit, in your *Downloads* folder.

4 Log on to the Synergis Cloud Link unit you want to copy to.

5 Click **Configuration** > **Reader LED and beeper settings**.

6 Click **Import**.

A file browser window opens.

7 Navigate to your *Downloads* folder, select the XML file you want, and then click **Open**.

The reader LED and beeper settings read from the file are applied to your Synergis Cloud Link unit.

8 Click **Save**.

Disabling output controls

To prevent doors from being unlocked through the Synergis™ Appliance Portal, you can disable the control of output states.

What you should know

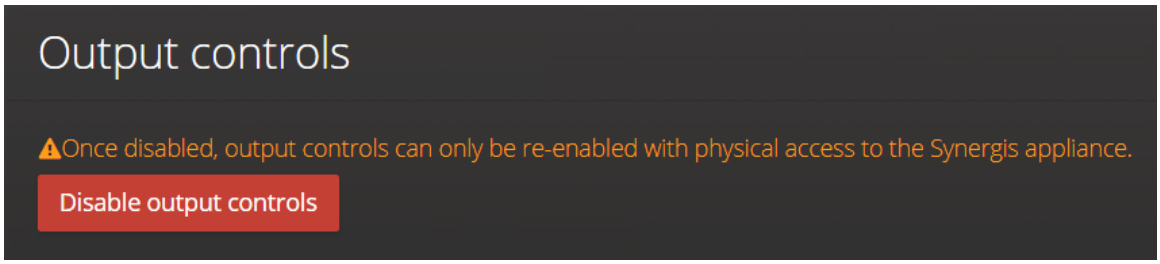
- If you disable output controls, you can view the output states, but can no longer change them on the *I/O diagnostics* page.
- You can only re-enable output controls by running a DIP switch command on the Synergis™ Cloud Link appliance.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Unit-wide parameters**.

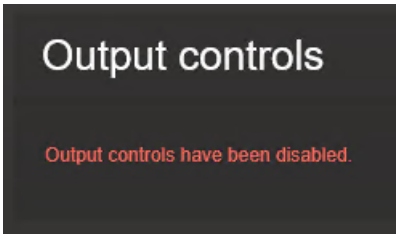
3 In the *Output controls* section, click **Disable output controls**.



The *Output controls* dialog box opens and prompts you to proceed.

4 Click **OK**.

The **Disable output controls** button disappears, and the following message is displayed: *Output controls have been disabled.*



Related Topics

DIP switch command codes on page 5

About the automation engine feature

Automation engine is the Synergis™ Softwire feature that executes rules, similar to event-to-actions in Security Center. Automation engine works even when the Synergis™ unit is disconnected from its Access Manager.

The automation engine is intended to only be used with onboard I/O and non-intelligent controllers. It might not work as expected with intelligent controllers that have capabilities that could interfere with the operation of the automation engine. For Mercury controllers, it's recommended to use the Mercury triggers and procedures feature instead.

NOTE: Before Synergis Cloud Link 3.0.2, the *automation engine* feature was known as the *primitive rule* feature. Primitive rules configured in earlier versions of Synergis Cloud Link are automatically displayed on the *Automation engine* page in the Synergis™ Appliance Portal after upgrading to 3.0.2 or later.

How it works

An automation engine rule is composed of a trigger event, optional conditions, and one or more actions. If no conditions are configured in the rule, the actions are triggered once the event occurs.

A condition specifies an input and an expected state. If conditions are configured in the rule, then when the event occurs, the automation engine checks the states of the inputs configured in the conditions, and then triggers the actions if the states match. If the input states don't correspond to the ones defined in the conditions, then the actions aren't triggered.

NOTE: An automation engine rule doesn't generate any action if the Synergis Cloud Link unit and its downstream device fail to communicate.

Automation engine rules are part of the Synergis Cloud Link unit's configuration files. It's recommended that you download these files after you finish configuring the rules, so that you can restore the configuration if you need to replace the unit.

Limitations

Be aware of the following limitations for the automation engine feature:

- The Copy configuration tool doesn't apply to this feature.
- The Unit replacement tool doesn't apply to this feature.
- Deleting a door that has automation engine rules applied to it doesn't automatically delete the configured automation engine rules.
- The Synergis Cloud Link unit must be online to configure automation engine rules on the target unit.
- Decimal values aren't supported for the pulse interval of the *Output - Pulse* action.
- The minimum security clearance configured on an area in Security Center overwrites the minimum security clearance activated by an automation engine rule.

Configuring automation engine rules

To trigger actions when an access control event occurs, configure automation engine rules in the Synergis™ Appliance Portal. For example, increase the minimum security clearance of an area when a door input goes into a trouble state.

What you should know

Consider the following behavior during configuration:

- If the input configured in a condition is in an unknown state, the condition can never be met.
- If the interface with inputs configured in conditions is removed, those conditions are left empty and the rule becomes invalid.
- If the interface with inputs configured in conditions goes offline, those conditions can't be met until the interface comes back online.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Automation engine**.

3 Click **Add a rule**.

4 In the *Event* section, select a trigger event from the list:

- **Reader - Access granted**
- **Door - Held open alarm**
- **Door - Forced open alarm**
- **Door - Access granted**
- **Door - Access denied**
- **Door - Cardholder authorized**

  NOTE: This event differs from the *Door - Access granted* event because the automation engine rule is run once access is authorized according to access rules, which occurs *before* access is actually granted. With the *Door - Cardholder authorized* event, the automation engine grants access and triggers the actions once all the conditions of the rule are met. Starting in Security Center 5.13.0.0, if conditions aren't met, then an *Access denied: Denied by automation engine* event is generated. In earlier versions of Security Center, the *Access denied* event is generated.
- **Input state update**

5 In the **Name** field, enter a name for the rule.

6 Configure the event:

a) Depending on the event you selected, click next to the **Reader**, **Door**, or **Input** field.

b) In the dialog box that opens, select the reader, door, or input, and then click **OK**.

NOTE: If you have many readers, doors, or inputs, use the search box at the top of the dialog box to search for them by name.

c) If you selected the *Door - Access granted*, *Door - Cardholder authorized*, or *Input state update* event, configure the additional parameters as follows:

- **Door - Access granted or Door - Cardholder authorized:** (Optional) To limit the rule to run only when specific cardholders are granted or authorized access, retrieve the GUID of the cardholder group from Config Tool, and then enter the GUID in the **Cardholder group** field.

  If no cardholder group is specified, the rules are triggered for all cardholders.
- **Input state update:** Select one or more states that the input must be in to trigger the action:

- **Active**
- **Normal**
- **Trouble**

7 (Optional) In the *Conditions* section, click **Add condition**, and then configure the following:
   a) Next to the **Input** field, click .
   b) In the dialog box that opens, select an input, and then click **OK**.
      NOTE: If you have many inputs, use the search box at the top of the dialog box to search for them by name.
   c) Select the state that the input must be in for the condition to be met.
   d) (Optional) Add more conditions as required.
      TIP: When you have multiple conditions, you can create groups of conditions and use the **And** and **Or** operators to organize them.

8 In the *Actions* section, click **Add an action**, and then select one of the following actions from the list:
   - **Output - Set**
   - **Output - Clear**
   - **Output - Pulse**
   - **Area - Set minimum security clearance**

9 Configure the action:
   a) Depending on the action you selected, click next to the **Output** or **Area** field.
   b) In the dialog box that opens, select an output or an area, and then click **OK**.
      NOTE: If you have many outputs or areas, use the search box at the top of the dialog box to search for them by name.
   c) If you selected the *Output - pulse* or *Area - Set minimum security clearance* action, configure the additional parameters as follows:
      - **Output - pulse:** In the **Seconds** field, enter a number to define the pulse interval.
      - **Area - Set minimum security clearance:** In the **Minimum** field, enter a value from 1 - 7 to define the minimum security clearance required to access the area.

10 (Optional) Configure more actions as required.

11 Click **Save**.

After you finish

- Download your Synergis Cloud Link unit's configuration as a compressed file, so that you can restore the configuration of the automation engine rules if you ever need to replace the unit.

  For more information, see Downloading the unit configuration file from your Synergis Cloud Link unit on page 249.
- If you configured multiple rules with the *Door - Cardholder authorized* event for the same door, configure the automation engine mode.

Retrieving entity GUIDs

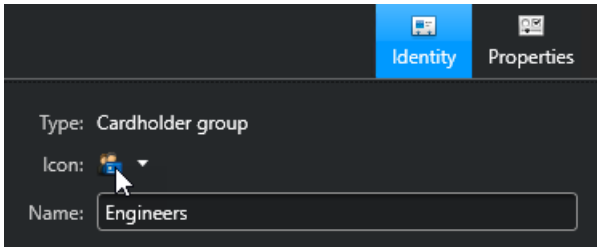
Before you can specify a cardholder group in an automation engine rule, you must retrieve the entity's GUID (global unique identifier) from Config Tool.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Cardholders and credentials** view.

2 Select the cardholder group from the entity tree.

3 On the *Identity* page of the cardholder group, hold the Ctrl key and double-click the entity icon.



The GUID is copied to your clipboard.

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Configuring the automation engine mode

Multiple automation engine rules configured with the *Door - Cardholder authorized* event can run at the same time. The automation engine mode determines which rule's actions are triggered in this scenario.

What you should know

The automation engine mode only applies when you have multiple rules configured with the following:

- The *Door - Cardholder authorized* event
- The same door
- Conditions

If no conditions are configured for a rule using the *Door - Cardholder authorized* event, then rule behaves like one configured with the *Door - Access granted* event.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Unit-wide parameters**.

3 In the *Automation engine mode* section, select one of the following modes:

- **All rules:** This mode is selected by default. Access is granted only if the conditions of all the *Door - Cardholder authorized* rules are met. All actions of those rules are triggered.
- **Any rules:** Access is granted if the conditions of at least one of the *Door - Cardholder authorized* rules are met. The actions of the *Door - Cardholder authorized* rules with all their conditions met are triggered.

4 Click **Save**.

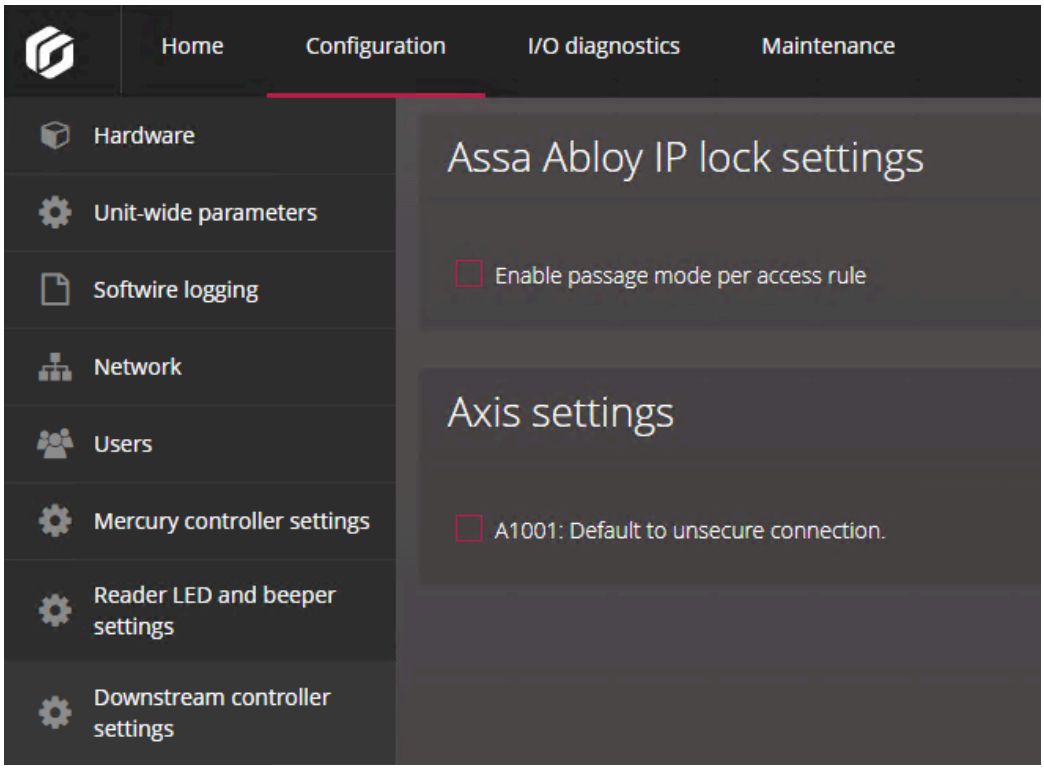
Configuring downstream controller settings

You can configure interface-module-specific behavior for all the interface modules connected to the same Synergis™ Cloud Link unit on the *Downstream controller settings* page of the Synergis™ Appliance Portal.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Downstream controller settings**.



3 In the *Assa Abloy IP lock settings* section, configure the following option:

- **Enable passage mode per access rule:** Creates the *PassageMode* custom field required for enabling the passage mode feature for ASSA ABLOY IP locks per access rule.

  For more information, see Enabling passage mode on ASSA ABLOY IP locks on page 95.

4 In the *Axis settings* section, configure the following option:

- **A1001: Default to unsecure connection:** Select this option so that you can use Synergis™ Softwire to upgrade the firmware on your AXIS A1001 controller if it doesn't support HTTPS.

5 Click **Save**.

All changes take effect after a software restart.

Configuring MIFARE DESFire

To enable MIFARE DESFire on your Synergis™ Cloud Link, you must load the configuration file, then associate the configuration with your STid SSCP or OSDP transparent readers.

Before you begin

Configure STid SSCP readers or OSDP readers.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **MIFARE DESFire**.

3 Click **Select smart cards sites file**, and browse to either your custom configuration file (*SmartCardsSites.xml*) or the default file that came with your Security Center installation.

For more information about the *SmartCardsSites.xml* file, see Configuring MIFARE DESFire in Security Center.

4 If you are using DESFire EV2 secure messaging, enable this feature in your system.

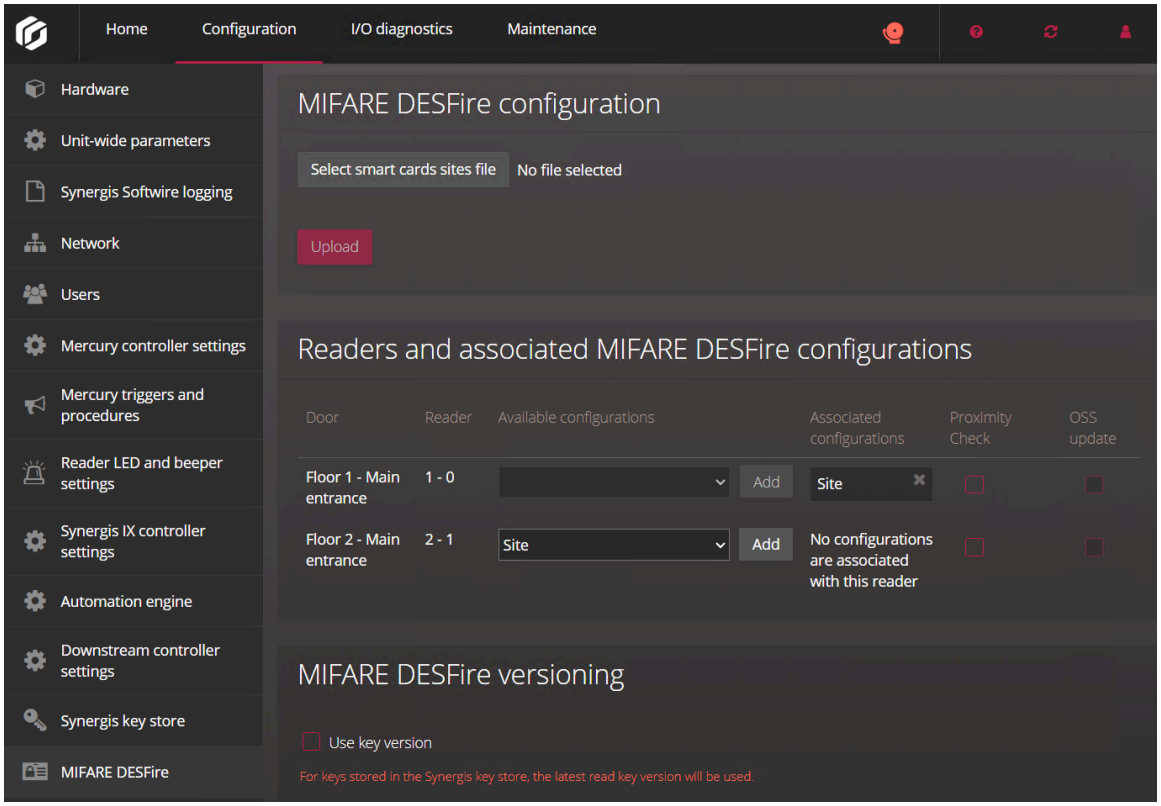
5 Click **Upload**.

The following message is displayed: *Upload successful.*

6 Associate the readers and MIFARE DESFire configurations:

a) For each reader, select a site from the **Available configurations** list.

b) Click **Add**.



7 If your system uses key versioning, select the **Use key version** checkbox.

Two scenarios must be considered:

- **Keys are stored in the Synergis key store:** When the checkbox is selected, the system asks the card, which key version it is using and tries to find it in the key store. If the checkbox is cleared, then system always uses the last version. For more information, see About the Synergis key store on page 51.
- **Keys are stored on the SAM card:** When the checkbox is selected, the system asks the card which key version it is using and try to find it on the SAM card. If the checkbox is cleared, then system always uses the key version 0. For more information, see Enabling key versioning for SAM cards on page 50.

8 Click **Save**.

Related Topics

Configuring and enrolling STid readers that use the SSCP protocol on page 233
Configuring and adding OSDP readers in the Synergis Appliance Portal on page 223

Enabling DESFire EV2 secure messaging

To use secure DESFire EV2 secure messaging, you must enable EV2 authentication on your DESFire configuration files and export them to your workstations and Synergis™ Cloud Link units.

Before you begin

Configure MIFARE DESFire in Security Center and then export your configuration to an XML file.

What you should know

The DESFire configuration file (*SmartCardsSites.xml*) is created in Config Tool using the *MIFARE DESFire configuration* task. At the moment, this task does not support the EV2 authentication mode. Therefore, you need to change this setting in the exported XML file manually.

Procedure

1 Using a text editor, open your custom *SmartCardsSites.xml* file.

2 Locate the <AuthenticationMode> tag at the end of each configuration, and replace "EV1" with "EV2".

```
<AuthenticationMode>
  <EV2 />
</AuthenticationMode>
```

3 Save your changes and close the file.

4 Using Config Tool, import the modified *SmartCardsSites.xml* file with the *MIFARE DESFire configuration* task.

5 Export the new MIFARE DESFire configuration to your workstations and Synergis Cloud Link units.

Unlocking SAM cards

Storing cryptographic keys on MIFARE Secure Access Module (SAM) cards instead of the Synergis™ key store increases security because the keys cannot be retrieved. The SAM cards must be unlocked to interact with Synergis™ Cloud Link for cryptographic operations.

Before you begin

- Configure a Synergis Cloud Link 312 unit.

  NOTE: You need a Synergis Cloud Link 312 unit to store the SAM card keys. For more information on Synergis Cloud Link 312 preparation, see Installing SAM cards on a Synergis Cloud Link 312.
- Configure SAM cards using a SAM production tool, and install up to three cards.

  NOTE: If you install more than one SAM card, the cards must have the same keys. Having multiple SAM cards installed allows for faster card reads and access decisions on units with heavy access control activity.

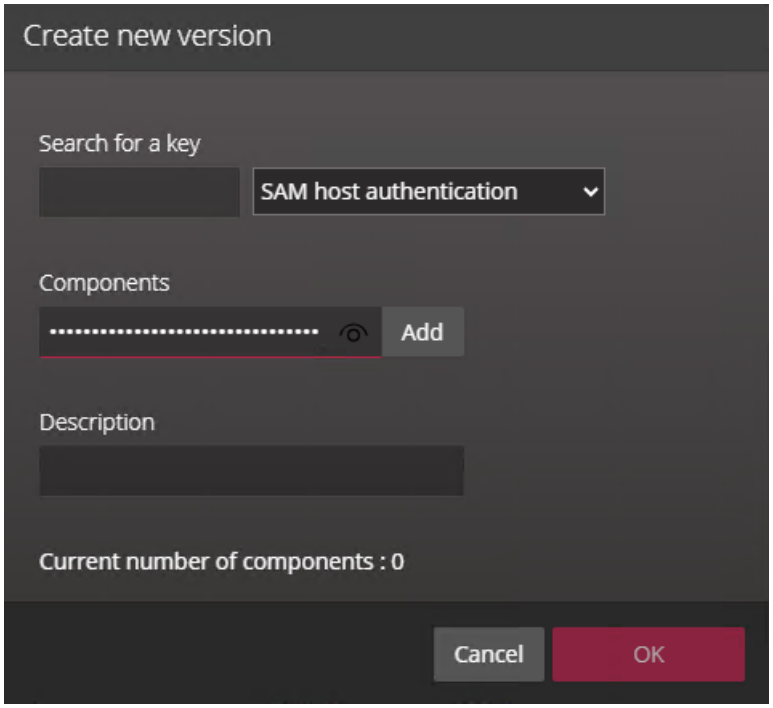
Procedure

1 Log on to the Synergis Cloud Link 312 unit.

2 Click **Configuration** > **Synergis™ key store**.

3 At the top of the key list, click ✚.

4 In the *Create new version* dialog box, do the following:

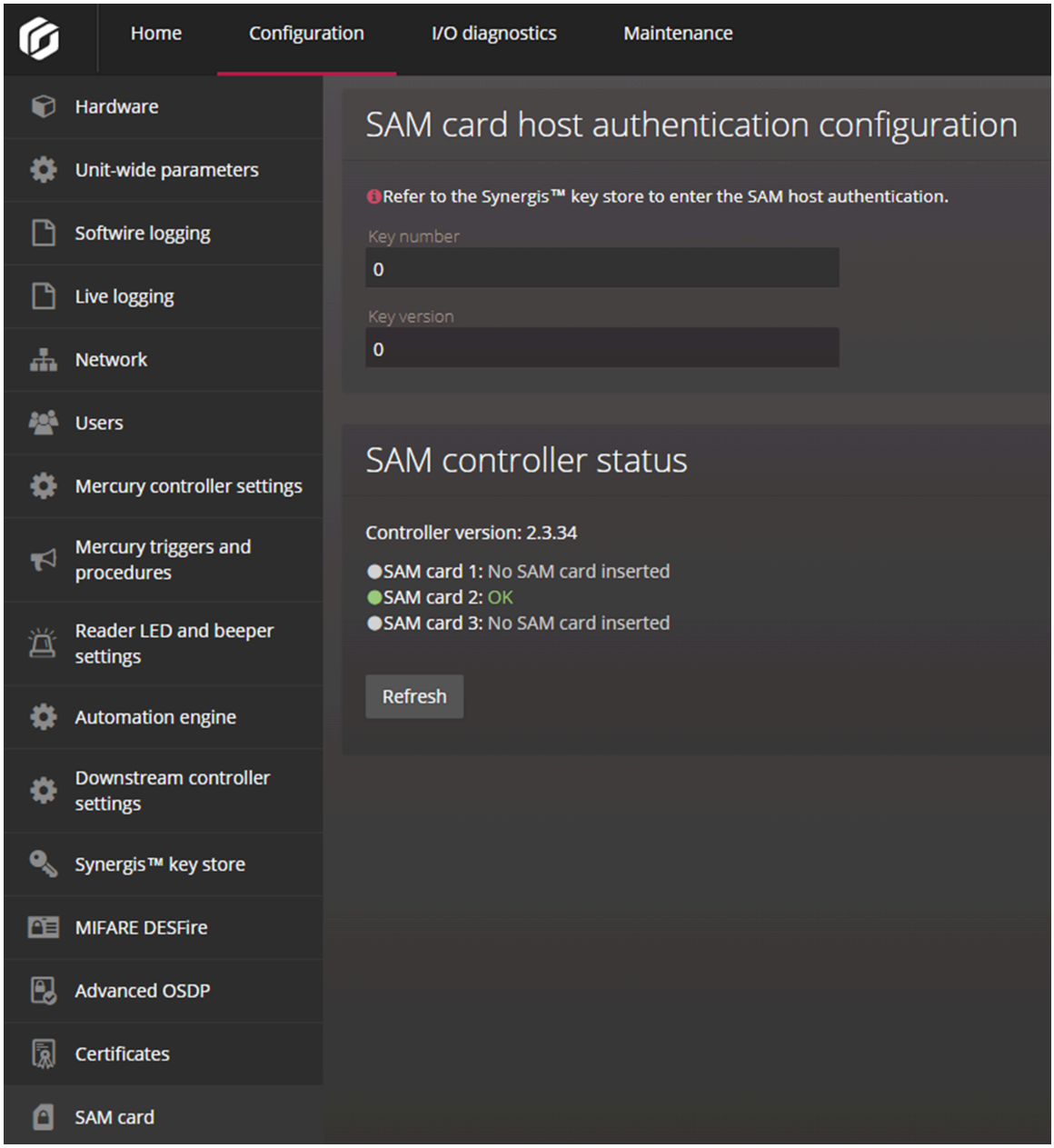


a) Select **SAM host authentication**.

b) In the **Components** field, enter the host authentication keys that you configured in the SAM production tool, and click **Add**.

c) Click **OK**.

5 Click **Configuration** > **SAM card**.



6 In the *SAM card host authentication configuration* section, enter the key number and key version of the host authentication key stored on the SAM card.

7 In the *SAM controller status* section, verify that the SAM cards were inserted and configured correctly.

You can have up to three SAM cards installed. Each expansion slot can have one of the following statuses:

- **OK:** A SAM card is inserted and the host authentication key, key number, and version number are valid.
- **SAM card unlock failed:** A SAM card is inserted, but the host authentication key, key number, or version number do not match those on the card.
- **No SAM card inserted:** There is no SAM card in the expansion slot.

After you finish

Enroll STid or OSDP readers, or configure enrolled readers.

Related Topics

Enabling key versioning for SAM cards on page 50
About Synergis Cloud Link 312 on page 6

Enabling key versioning for SAM cards

To use application read key versions with your MIFARE SAM cards, configure the cards with up to three keys using a SAM card configuration tool, then enable key versioning in the Synergis™ Appliance Portal.

Before you begin

- Configure your SAM cards with up to three keys using a SAM production tool.
- Install the SAM cards into a Synergis™ Cloud Link 312 unit. For more information, see Installing SAM cards on a Synergis Cloud Link 312.

What you should know

By default, Security Center does not support SAM cards with application read key versions other than 0; enabling key versioning allows the use of pre-encoded cards that have key versions other than 0. The feature works with OSDP and SSCP protocols, and offers key management flexibility to administrators who want to increment their key version periodically.

Procedure

1 Log on to the Synergis Cloud Link 312 unit.

2 Click **Configuration** > **MIFARE DESFire**.

3 In the *MIFARE DESFire versioning* section, select the **Use key version** checkbox.

When the checkbox is selected, the system asks the card which key version it is using and try to find it on the SAM card. If the checkbox is cleared, then system always uses the key version 0.

4 Click **Save**, and then restart the unit.

Related Topics

Unlocking SAM cards on page 47
About Synergis Cloud Link 312 on page 6

About the Synergis key store

The Synergis™ key store is used to configure and store cryptographic keys.

Keys in the Synergis key store

Each cryptographic key is composed of one or more components. For added security, a key can be composed of multiple components so that the key can be separated and distributed to multiple stakeholders, without anyone having the complete key.

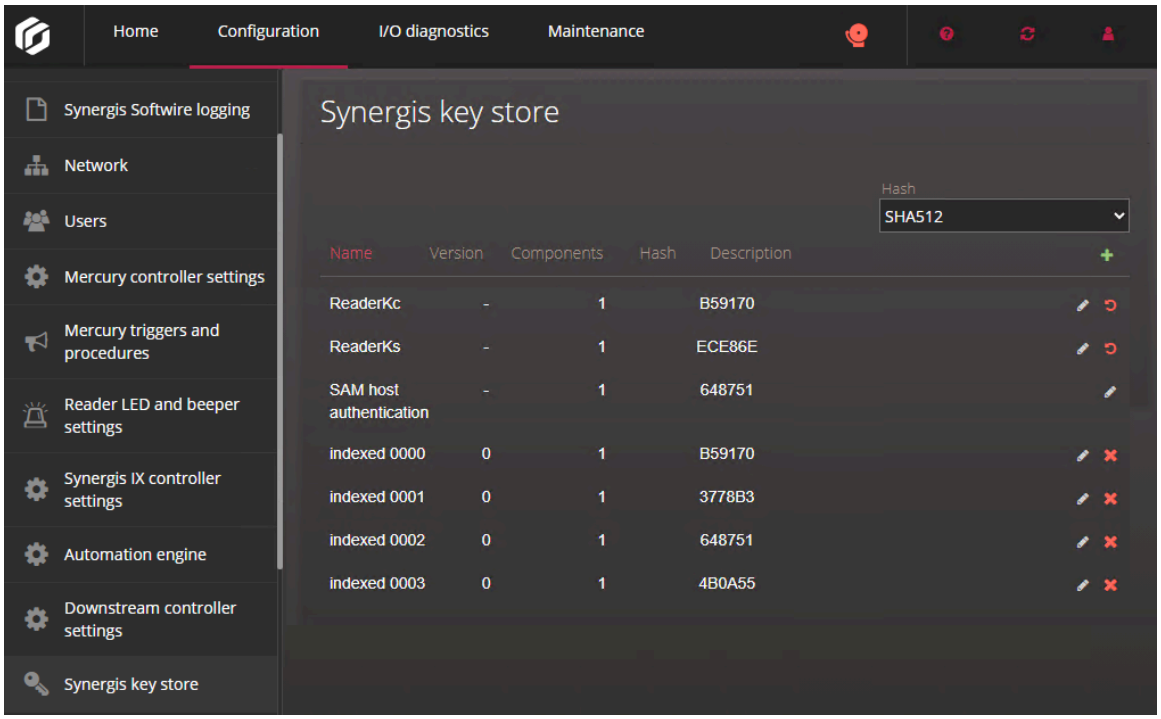
In the Synergis key store, a version, current number of components, and hash are listed for each key.

- **Version:** The version number of the key. Each version of the key you create is a new key.

  Multiple versions of the same key are listed if the **Use key version** checkbox on the MIFARE DESFire configuration page is selected. When the checkbox is selected, the system asks the card which key version it's using and tries to find it in the key store. The indexed 00 to indexed 31 keys can have up to three versions at a time. If the checkbox is cleared, then the system always uses the last version.

  For example, if you enable key versioning then add versions *1*, *2*, and then *3* for the *indexed 01* key, when you clear this checkbox, only version *3* is listed in the Synergis key store for that key. If you create version *4*, and then select the checkbox again, versions *2*, *3*, and *4* are listed.

  NOTE: The ReaderKc, ReaderKs, and SAM host authentication keys do not support key versioning; the latest changes are automatically incremented.
- **Components:** The number of components that currently form the key. Each component is a 32-character hexadecimal value.
- **Hash:** The key hash that is used to verify whether the key that you entered in the Synergis key store is valid. The key is valid if it matches the key hash from the other units, the SAM card, or the key card production tool with which you want to compare. For more information, see Using key hashes in the Synergis key store on page 53.



MIFARE DESFire cryptographic keys can be exported from Security Center to one or more Synergis™ Cloud Link units in your system. The keys are then automatically updated on the *Synergis key store* page of the Synergis™ Appliance Portal. For information, see Exporting MIFARE DESFire keys to Synergis Cloud Link units.

Use cases for the different keys

Each type of key in the Synergis key store is used in a specific context:

- **ReaderKc and ReaderKs:** Used to configure communication keys for STid readers. For more information, see Changing the default RS-485 communication keys for STid readers that use the SSCP protocol on page 239.
- **SAM host authentication:** Used to unlock SAM cards so that you can use the cryptographic keys stored in them. For more information, see Unlocking SAM cards on page 47.
- **Indexed 00 - 31:** Used to create the cryptographic keys to access a MIFARE DESFire card's secured credential. For more information, see Enabling MIFARE DESFire for transparent OSDP readers on page 227 and Enabling transparent mode on STid readers that use the SSCP protocol on page 236.

Using key hashes in the Synergis key store

You can use key hashes to verify keys in the Synergis key store against other units, or against the SAM card or key card production tool that produced the keys.

What you should know

Keys that have been saved in the Synergis key store cannot be retrieved, but they can be verified using key hashes.

Procedure

1 Log on to the Synergis™ Cloud Link unit.

2 Click **Configuration** > **Synergis key store**.

3 From the **Hash** list, select the algorithm used by the third-party card tool or Synergis Cloud Link unit:

- **KCV**: Key Checksum Value
- **SHA1**: Secure Hash Algorithm 1
- **SHA256**: 256-bit version of Secure Hash Algorithm 2
- **SHA384**: 384-bit version of Secure Hash Algorithm 2
- **SHA512**: 512-bit version of Secure Hash Algorithm 2

In the **Hash** column, the 6-character (24 bit) key hash is displayed, regardless of the algorithm used.

4 Verify that the key hash in the Synergis key store is the same as the key hash from the other units, the SAM card, or the key card production tool with which you want to compare.

5 Verify that the key hash in the Synergis key store is the same as the key hash from the other units, the SAM card, or the key card production tool with which you want to compare.

Changing the PIN entry timeout for doors

When long PINs are being used, you can change the PIN entry timeout to give cardholders more time to enter their PINs.

What you should know

The default timeout is 5 seconds.

NOTE: Changing the **PIN entry timeout** setting in Config Tool does not affect readers in a Mercury integration. The default timeout for Mercury is 10 seconds. Because of this, when an incorrect PIN is entered on a reader that is set to *Card and PIN*, there is a 10 second delay before access is denied if the PIN is shorter than the configured maximum PIN length.

Procedure

1 Connect to Security Center with Config Tool.

2 In the *Area view* task, select the door that requires a longer PIN entry timeout.

3 Click the **Hardware** tab.

4 Beside the *Card and PIN* reader assigned to the door, click **Reader settings** ( ).

5 In the *Reader settings* dialog box, select **Card and PIN** as the **Reader mode**.

6 Set the **PIN entry timeout**, and then click **Save**.

7 Click **Apply**.

Configuring event logging on the Synergis Cloud Link unit

The Synergis™ Cloud Link unit can keep detailed logs for troubleshooting and support. However, these logs are turned off by default. Turn them on if you want to view troubleshooting reports or to download the support logs.

What you should know

- Enable logging only if instructed by Genetec™ Technical Support.
- *Critical* errors are always written to logs, regardless of the configured logging level.
- You can download the logs from the *Download diagnostic logs* page of the Synergis™ Appliance Portal.
- You can also configure logs to be stored in the cloud through Azure Application Insights.

Procedure

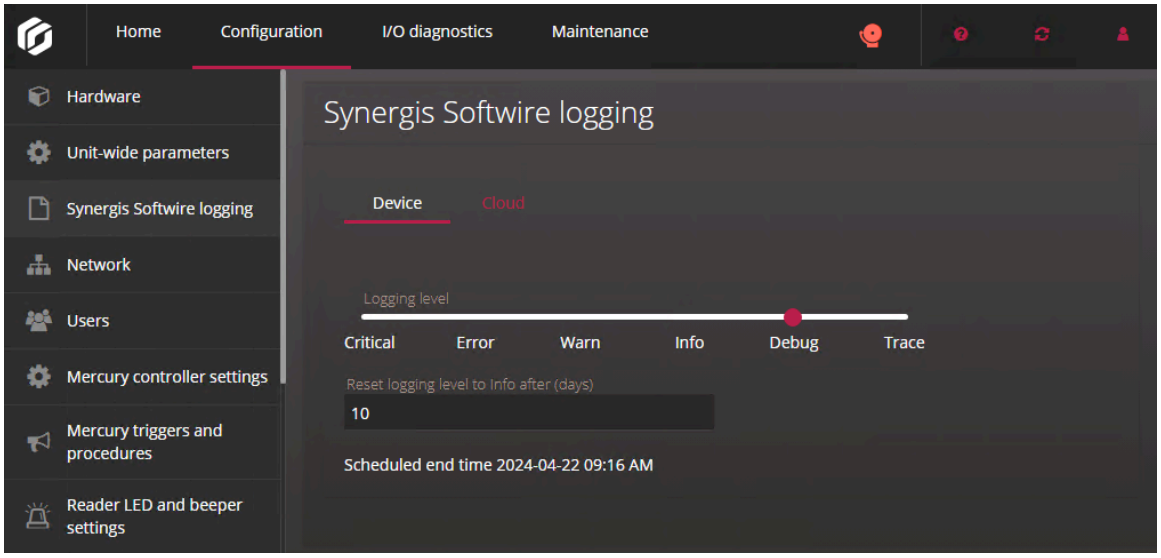
1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Synergis Softwire logging**.

3 In the *Synergis Softwire logging* section, select a **Logging level**.

4 If you select **Debug** or **Trace** as the logging level, enter the number of days for which you want to gather logs of the selected logging levels in the **Reset logging level to Info after (days)** field.

Example: If you select **Debug** as the logging level, and enter **10** in the **Reset logging level to Info after (days)** field, *Critical*, *Error*, *Warn*, *Info*, and *Debug* logs are gathered for ten days. After ten days, only *Critical*, *Error*, *Warn*, and *Info* logs are gathered.



5 Click **Save**.

Configuring auxiliary event logging in the cloud for the Synergis Cloud Link unit

Configure your Synergis™ Cloud Link unit to connect to an Azure Application Insights resource, so that logs can be stored in the cloud in addition to being stored on the unit itself. This can simplify analyzing logs and running monitoring tools on them.

Before you begin

You must have an Application Insights resource created and configured.

What you should know

- The Synergis Cloud Link unit connects to the Application Insights resource through the resource's instrumentation key.
- You can use the instrumentation key to connect multiple Synergis Cloud Link units to the same Application Insights resource.
- You can configure different logging levels for the logs stored on the Synergis Cloud Link unit and in the cloud.

  Example: To save space on the unit, you can configure the unit to store only *Critical* logs, and all other logs to be sent to the cloud.

Procedure

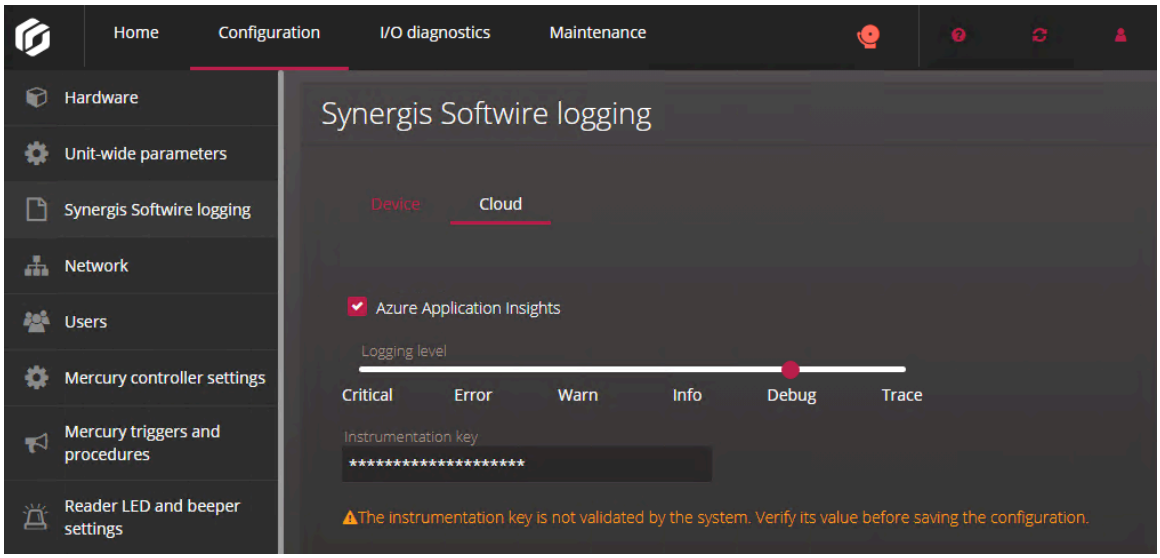
1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Synergis Softwire logging**.

3 In the *Synergis Softwire logging* section, click the **Cloud** view, and then select **Azure Application Insights**.

4 Select a **Logging level**.

5 In the **Instrumentation key** field, enter the instrumentation key of the Application Insights resource that you want to send logs to.



6 Click **Save**.

Configuring audit log retention for the Synergis Cloud Link unit

You can configure how long the audit logs for the Synergis™ Cloud Link unit are kept before they are automatically deleted.

What you should know

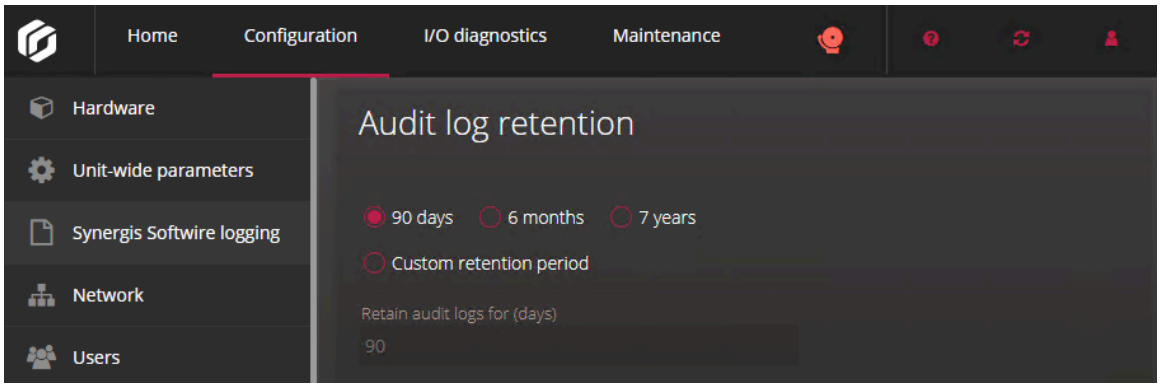
- Audit logs are kept for 90 days by default.
- Audit logs can be downloaded from the *Download diagnostic logs* page of the portal by the Admin user only.
- The following are logged:
  - Successful and unsuccessful user logon attempts, user password changes, and user lockouts, which occur after three failed logon attempts.
  - Configuration changes in the Synergis™ Appliance Portal.
    NOTE: Changes made on the *Hardware* and *Network* pages are not logged.
  - DIP switch commands run on the Synergis Cloud Link appliance.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Synergis Softwire logging**.

3 In the *Audit log retention* section, select a retention period:



- **90 days**
- **6 months**
- **7 years**
- **Custom retention period**: Enter a value from 2 - 2557 to define the number of days for the retention period.

4 Click **Save**.

Enrolling Synergis Cloud Link units in Security Center

To enroll a Synergis™ Cloud Link unit in Security Center, assign the unit to an Access Manager role.

Before you begin

Configure the Synergis Cloud Link unit's network properties.

What you should know

When you create an Access Manager role, the Synergis extension is added automatically. This extension is created with the default discovery port 2000. If you configured a different port in the unit's network properties, you must also change it in Config Tool to match.

BEST PRACTICE: If you have multiple Access Manager roles controlling Synergis units on the same subnet, ensure that they use different discovery ports. Otherwise, you might experience performance issues.

Procedure

1 If the unit does not use the default discovery port, change the Synergis extension discovery port to match the port configured on your unit:
   a) From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.
   b) Select the Access Manager, and click the **Extensions** tab.
   c) Select the Synergis extension.
   d) Select the discovery port and click **Edit the item** ( ).
   e) In the *Discovery port* dialog box, enter the port number configured for your units and click **Save**.

2 Add the Synergis™ unit to the Access Manager role.

Adding Synergis Cloud Link units to an Access Manager role

To control the access to secured areas at your site and monitor the access control-related events in Security Center, you must add access control units to an Access Manager role.

Before you begin

Ensure that the Synergis™ extension discovery port matches the port number on your unit.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.
2 Click **Access control unit** ( ).
3 In the *Creating a unit* dialog box, click **Unit type** and select **Synergis**.
4 In the *Network endpoint* section, enter the hostname or IP address of the unit, and the admin username and password.
5 If you require port forwarding, click **Advanced settings** and enter the base URL in the **Web address** field.
6 Click **Next**.
7 Select a **Partition** on which to add the access control unit, and click **Next**.
   Partitions determine which Security Center users have access to this entity. Only authorized users of the partition can view or modify the access control unit.

8 Review the *Creation summary* window, and click **Create**.

The Access Manager attempts to connect to the unit and enrolls it in your system. When the process is successfully completed, a confirmation message is displayed.

9 Click **Close**, and then click **Refresh** ( ).

The newly added unit is displayed under the Access Manager it was assigned to in the **Roles and units** view. The default entity name is the hostname of the unit. From now on, this unit only responds to the commands issued by this Access Manager.

NOTE: If you later change the connection parameters on the unit, you must inform the Access Manager about it by synchronizing the unit with the Access Manager.

10 If this unit must be connected as a peer to other units, add it to the appropriate peer group. For more information, see Enabling peer-to-peer on the Access Manager role.

Synchronizing the Synergis Cloud Link unit with the Access Manager

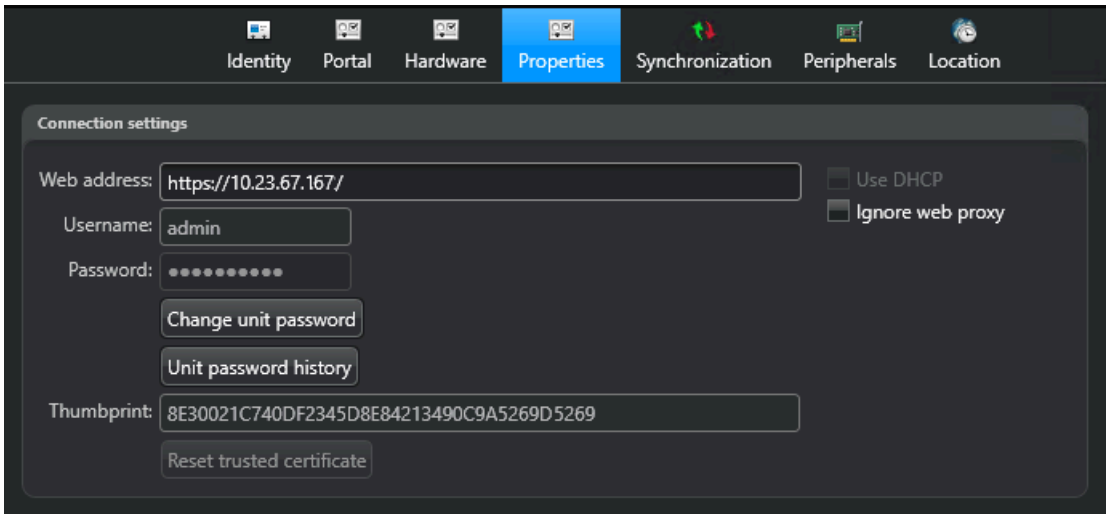
Some settings on the Synergis™ Cloud Link unit are not automatically synchronized with the Access Manager. If you change settings on the unit through the Synergis™ Appliance Portal, such as its logon password, its IP address, or the way it responds to connection requests, then you must change the same settings on the Access Manager in Config Tool.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

2 From the entity tree, select the unit you modified.

3 Click the **Properties** tab.



4 In the *Connection settings* section, modify the parameters to match what you configured for the unit in the Synergis™ Appliance Portal.

- **Web address:** Web address for contacting the Synergis unit's portal. If you change the web address to use the unit's IP address after it has been enrolled using its hostname, make sure to delete the IPv6 address from the **Accepted Access Manager connections** list on the *Network* page of the unit's portal. If the IPv6 address is not removed from the list, the next time the unit is disconnected, it will not reconnect.
- **Username and Password:** Logon username and password.
- **Change unit password:** Click to update the password.
- **Unit password history:** Displays the details of the five previous password change attempts made through Security Center, including the date, the previous password, and the new password.
- **Use DHCP:** Do not change this parameter unless asked by a Genetec Technical Assistance representative. This parameter is reset every time the Access Manager reconnects to the Synergis unit.
- **Ignore web proxy:** Select this option to instruct the Access Manager to ignore the Proxy Server settings on the server currently hosting the role. Clear this option to instruct the Access Manager to follow the Proxy Server settings (default=cleared).
- **Thumbprint:** The thumbprint of the certificate on the Synergis unit. This field is automatically updated to reflect the new certificate when you click the **Reset trusted certificate** button.
- **Reset trusted certificate:** (Only enabled when the unit is offline) Click this button to make the Access Manager forget the trusted certificate for this unit so that the new one can be accepted. Use this feature when you changed the digital certificate of the unit after it has been enrolled.

5 Click **Apply**.

Configuring the monitoring inputs on the Synergis Cloud Link appliance

You can use the four inputs on the Synergis™ Cloud Link appliance to monitor the physical installation of the appliance. For example, you can connect an input to a tamper switch on the enclosure in which the appliance is installed.

What you should know

- The following procedure doesn't apply to Security Center SaaS or Security Center SaaS Edition (Classic) deployments.
- You can set a special behavior for each input. Each special behavior corresponds to an event that you can receive in the *Monitoring* task:

Special behavior	Security Center event
AC failure	AC fail
Tamper switch	Hardware tamper
Battery failure	Battery fail

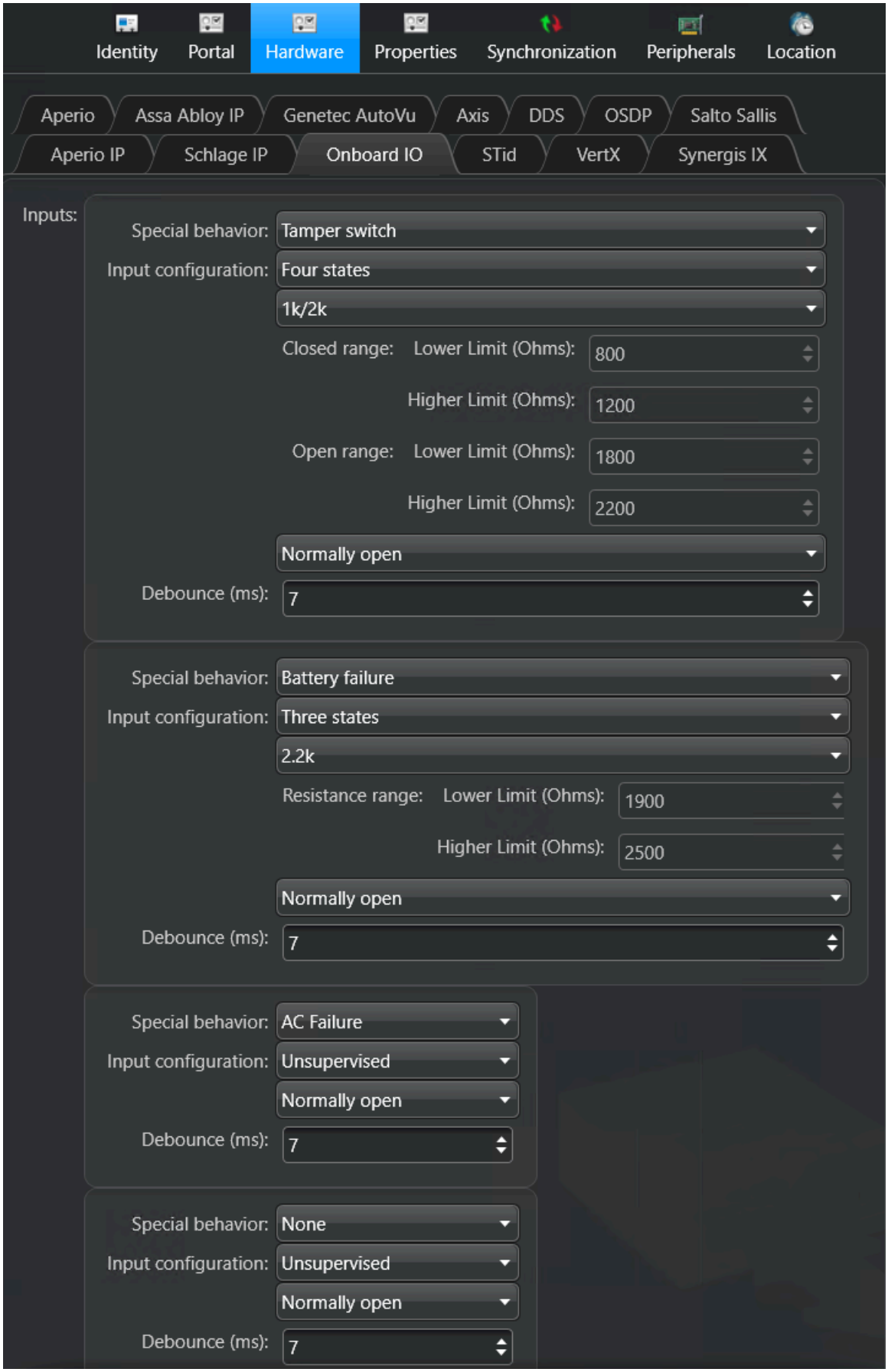
- You can view the state changes of the inputs on the *I/O diagnostics* page in the Synergis™ Appliance Portal.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

2 Select your Synergis Cloud Link unit, and click the **Hardware** tab.

3 Click the **Onboard IO** tab, and then configure the inputs:
Example:


Identity
Portal
Hardware
Properties
Synchronization
Peripherals
Location
Aperio
Assa Abloy IP
Genetec AutoVu
Axis
DDS
OSDP
Salto Sallis
Aperio IP
Schlage IP
Onboard IO
STid
VertX
Synergis IX
Inputs:
Special behavior: Tamper switch
Input configuration: Four states
1k/2k
Closed range: Lower Limit (Ohms): 800
Higher Limit (Ohms): 1200
Open range: Lower Limit (Ohms): 1800
Higher Limit (Ohms): 2200
Normally open
Debounce (ms): 7
Special behavior: Battery failure
Input configuration: Three states
2.2k
Resistance range: Lower Limit (Ohms): 1900
Higher Limit (Ohms): 2500
Normally open
Debounce (ms): 7
Special behavior: AC Failure
Input configuration: Unsupervised
Normally open
Debounce (ms): 7
Special behavior: None
Input configuration: Unsupervised
Normally open
Debounce (ms): 7

- **Special behavior:** The special behaviors determine the event that you receive in the *Monitoring* task when the input is in a non-normal state. By default, the special behavior is set to **None**. Select one of the following:
  - **AC failure**
  - **Tamper switch**
  - **Battery failure**
- **Input configuration:** Select one of the following:
  - **Unsupervised:** Inputs are unsupervised by default.
  - **Three states:** Select one of the pre-configured options, which selects the **Resistance range** for you, or select **Custom**, and enter the **Lower Limit (Ohms)** and **Higher Limit (Ohms)** in ohms yourself.
  - **Four states:** Select one of the pre-configured options, which selects the **Closed range** and **Open range** for you, or select **Custom**, and enter the **Lower Limit (Ohms)** and **Higher Limit (Ohms)** values yourself.
- **Debounce (ms):** Enter a value in milliseconds from 7 to 600,000 (10 minutes). The option indicates the amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. The option filters out false events from unstable input signals. The default value is 7 milliseconds.

  The following are examples of events that are affected:
  - *Input state changed: Input active*
  - *Input state changed: Input normal*
  - *Input state changed: Input trouble*
  - *Door opened*
  - *Request to exit*
  - *AC fail*
  - *Battery fail*

4 Click **Apply**.

5 Click the **Peripherals** tab, and double-click the input you configured on the *Hardware* page.

6 (Optional) In the *Edit Input* dialog box, enter a new name and logical ID.

7 Set the **Contact type**:

a) Select **Not supervised**, **3 state supervised**, or **4 state supervised** to match the value you selected for the **Input configuration** on the *Hardware* page.

b) Select **Normally open** or **Normally closed**.

8 Click **Save**.

When an input is in a non-normal state, the Synergis Cloud Link unit turns yellow, and you receive an entity warning. If you were monitoring the Synergis Cloud Link unit and the special behavior events, you receive the event corresponding to the input's special behavior in the *Monitoring* task.

4

Cloud configuration for Synergis Cloud Link

This section includes the following topics:

Adding Synergis Cloud Link units to a hosted Access Manager

Adding a Synergis™ Cloud Link unit to a hosted Access Manager role activates that unit to make secure connections to your hosted Security Center SaaS Edition (Classic) deployment.

Before you begin

- Verify that the DNS and other networking settings of the unit are configured.
- Change the default logon password for the unit.
- Ensure that the Synergis Cloud Link unit has internet connectivity.
- Ensure that your Config Tool workstation is on the same network as your Synergis Cloud Link unit.

What you should know

Cloud connectivity is enabled by default on the Synergis Cloud Link unit, but the unit must be enrolled under a hosted Access Manager for the cloud connection to be activated.

Procedure

To add a Synergis Cloud Link unit to a hosted Access Manager:

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

2 Click **Access control unit** ( ).

3 In the *Creating a unit* dialog box, click **Unit type** and select **Synergis™ SaaS**.

4 In the *Network endpoint* area, enter the unit's hostname or IP address, along with its username and password.

The default username is admin. Change the default password before enrolling the unit.

5 Click **Validate**.

The system verifies the access control unit and displays its MAC address, which also serves as the unit's serial number.

6 Click **Next**.

7 Review the *Creation summary* window, and click **Create**.

Config Tool sends the information of the Synergis Cloud Link to the Access Manager, which then forwards it to the SaaS gateway. When the unit is connected to the gateway, a confirmation message is displayed.

8 Click **Close**, and then click **Refresh** ( ).

In the **Roles and units** view, the newly added access control unit appears under the Access Manager that it was added to. The default entity name is the hostname of the Synergis Cloud Link unit. This unit now only responds to the commands issued by this Access Manager.

To delete a Synergis Cloud Link unit from a hosted Access Manager:

1 In the **Roles and units** view, select the Synergis Cloud Link unit from the entity tree.

2 Click **Delete** ( ).

3 In the confirmation dialog box that opens, click **Delete**.

Enabling cloud connectivity testing on Synergis Cloud Link units

Cloud connectivity tests indicate whether your Synergis™ Cloud Link can connect to the internet and whether your firewall settings block endpoints that are required for the unit to connect to the cloud.

What you should know

By default, cloud connectivity tests are disabled. When the tests are enabled, the Synergis Cloud Link periodically tries to communicate with Google to test if it can connect to the internet. If you don't want your units to communicate with Google, leave cloud connectivity tests disabled.

The following procedure applies to both Security Center SaaS and Security Center SaaS Edition (Classic) deployments.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Cloud connectivity**.

3 In the *Connection settings* section, select the **Cloud connectivity tests** checkbox.

4 If your local network can only reach the internet through a proxy server, in the *Proxy* section, enter the proxy server URL, username, and password.

5 Click **Save**.

The **Internet connectivity**, **Service bus connectivity**, **Storage account connectivity**, and **Event hub connectivity** test categories are displayed with the status of the test under each one.

After you finish

To troubleshoot failed connectivity tests, ensure that your firewall settings aren't blocking the required domains and URLs required for cloud connection.

- For Security Center SaaS deployments, see Port requirements for appliances in Security Center SaaS.
- For Security Center SaaS Edition (Classic) deployments, see "Ports required by Security Center SaaS Edition (Classic)" in the Security Center SaaS Edition (Classic) Deployment Guide.

Configuring cloud-hosted Synergis Cloud Link units for peer-to-peer communication

Configure the **Fully qualified hostname** in the Synergis™ Appliance Portal for peer-to-peer communication to work between access control units managed by the same hosted Access Manager role.

Before you begin

Enable the **Activate peer-to-peer** option on the hosted Access Manager role that your access control unit is enrolled under. For more information, see Configuring Access Manager roles.

What you should know

The following procedure applies to both Security Center SaaS and Security Center SaaS Edition (Classic) deployments.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Network**.

3 In the *Hostname* section, click the **Cloud** tab.

4 Enter the **Fully qualified hostname** for your unit.

By default, this field contains the unit's hostname. The format for the **Fully qualified hostname** is <hostname>.<network domain name>.

Example: SCL0CBF123456F2.genetec.com

5 Click **Save**.

6 Verify that your unit can communicate with its peers by doing the following:

a) Log on to one of your unit's peers.

b) Click **Maintenance** > **Peer-to-peer**.

If you see your unit listed and online, peer-to-peer communication works correctly.

Part III

Integration-specific configuration

This part includes the following chapters:

5

Allegion Schlage wireless locks

This section includes the following topics:

Enrolling Allegion Schlage wireless locks on the Synergis unit

Allegion Schlage LE, NDE, and Control locks (FE410 and BE467F) can be integrated into the ENGAGE platform without Mercury controllers.

What you should know

The ENGAGE IP integration supports up to 10 locks per Gateway, and up to 32 Gateways per Synergis™ unit, to a maximum of 200 locks per unit. You need online access to complete this task.

Procedure

1 Create an ENGAGE partner account at *portal.allegionengage.com*.

IMPORTANT: Do not create your ENGAGE account from the Allegion ENGAGE mobile app.

2 Download the latest version of the Genetec™ Allegion Site Configurator from the GTAP *Product Download* page:

a) From the **Download Finder** list, select **Synergis™ Cloud Link**.

b) Download the Genetec Allegion Site Configurator.

3 Use the Genetec Allegion Site Configurator to create the site where the access control hardware will be installed.

This process automatically creates a site key. Note the site key and store it in a safe place.

4 Download the Allegion ENGAGE mobile app from the App Store or Google Play.

5 Open the Allegion ENGAGE mobile app to log in to your ENGAGE partner account.

6 Use the Allegion ENGAGE mobile app to add the Gateways and locks to the site and link them.

7 Log on to the Synergis Cloud Link unit.

8 Click **Configuration** > **Hardware**.

9 At the top of the **Hardware** column, click **Add** ( ).

10 In the *Add hardware* dialog box, select **Schlage IP** from the **Hardware type** list, and then enter the IP address of the ENGAGE Gateway and the site key that you created using the Genetec Allegion Site Configurator.

11 Click **Save**.

The logon credentials of the Gateway are completed automatically, and the connected locks are listed in the Hardware tree.

IMPORTANT: Ensure that the site key is entered properly. If not entered correctly, then none of the credentials will be synchronized to the lock.

12 (Optional) Add each remaining ENGAGE Gateway.

13 Enroll the credentials in Security Center.

NOTE: You cannot enroll credentials with automatic entry using the lock. You can use the Allegion Schlage MT20 Enrollment Reader in Keystroke Emulator mode.

Re-enrolling Allegion Schlage wireless locks on the Synergis unit

You can re-enroll Allegion Schlage wireless locks from the *Hardware* page of the Synergis™ unit in Config Tool to avoid having to factory reset the ENGAGE Gateway and its locks and use the Allegion ENGAGE mobile app for the re-enrollment process.

What you should know

- The ENGAGE Gateway must not have been factory reset before re-enrolling it through Config Tool.
- You can only use the Synergis™ Appliance Portal to enroll the ENGAGE Gateway for the first time, or to enroll it after it has been factory reset.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

2 From the entity tree, select the Synergis unit on which you want to re-enroll the ENGAGE Gateway.

3 Click **Hardware** > **Schlage IP**.

4 Click **Add** (), and then enter the following information:

- **IP:** The IP address of the ENGAGE Gateway.
- **Username:** The username of the ENGAGE Gateway.
- **Password:** The password of the ENGAGE Gateway.
- **Site key:** The site key that you created using the Genetec™ Allegion Site Configurator when you first enrolled the ENGAGE Gateway.

NOTE: You can use the following URL to find the username and password: *https://<SCL IP>/SchlageIP/Bus/<Gateway IP>/RevealCredentials*, where <*SCL IP*> is the IP address of the Synergis unit and <*Gateway IP*> is the IP address of the ENGAGE Gateway.

5 Click **Apply**.

The locks are added on the *Peripherals* page of the Synergis unit in Config Tool. This might take up to a few minutes.

6

ASSA ABLOY Aperio-enabled locks

This section includes the following topics:

Pairing Aperio-enabled locks with the AH30 hub

If you use Aperio-enabled locks with an AH30 hub, you must pair the locks with the hub using the Aperio Programming Application (APA) before you can enroll the locks on your Synergis™ unit.

Before you begin

Ensure that you have the following:

- Aperio Online Programming Application Manual
- Aperio Programming Application (APA)
- USB dongle
- TriBee Bootloader, which includes the USB dongle driver
- Supported firmware
- Computer for running the APA
- Card that is compatible with the reader
- Encryption key file provided by ASSA ABLOY

Procedure

1 Set the EAC address (1 - 15) on the hub using the DIP switches.

IMPORTANT: Up to eight hubs can be connected to the same RS-485 channel in a daisy chain, but each hub must use a different EAC address.

2 Power on the hub.

3 Plug the USB dongle into your computer and install the following:

- TriBee Bootloader (driver for the USB dongle)
- Aperio Programming Application (APA)

4 Open APA, and then open or create an installation.

NOTE: Each installation is linked to an encryption key file. Contact ASSA ABLOY for this key file to create an installation.

5 Scan to discover the hub, and pair the locks to the hub.

For more information, see the *Aperio Online Programming Application Manual*.

6 Using APA, update the firmware on the hub and the locks.

For more information, see Supported Aperio-enabled locks.

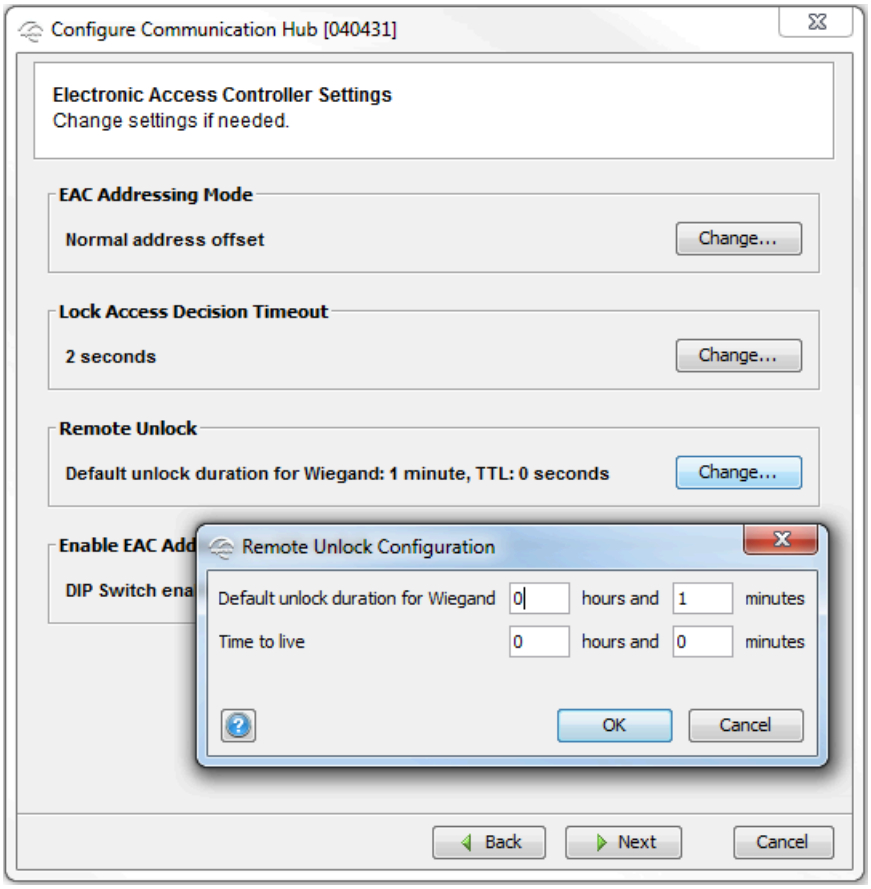
BEST PRACTICE: Always upgrade the communication hub before upgrading the locks or sensors. Check that the DIP switch is set to the correct EAC address. If DIP 5 (Pairing mode) is set to active during an upgrade, the communication hub starts using a different EAC address.

7 Configure the hub.

8 If your communication hub firmware is earlier than version 2.6.5, enable the **Remote Unlock** option to use Security Center unlock schedules.

With firmware version 2.6.5 and later, the option is enabled by default.

9 In the *Remote Unlock Configuration* dialog box, enter a value for **Time to live**, and click **OK**.



This time indicates how long the **Remote Unlock** command (grantAccessSequence) is present in the communication hub. This setting must always be longer than the **Status Report Interval** set on the lock.

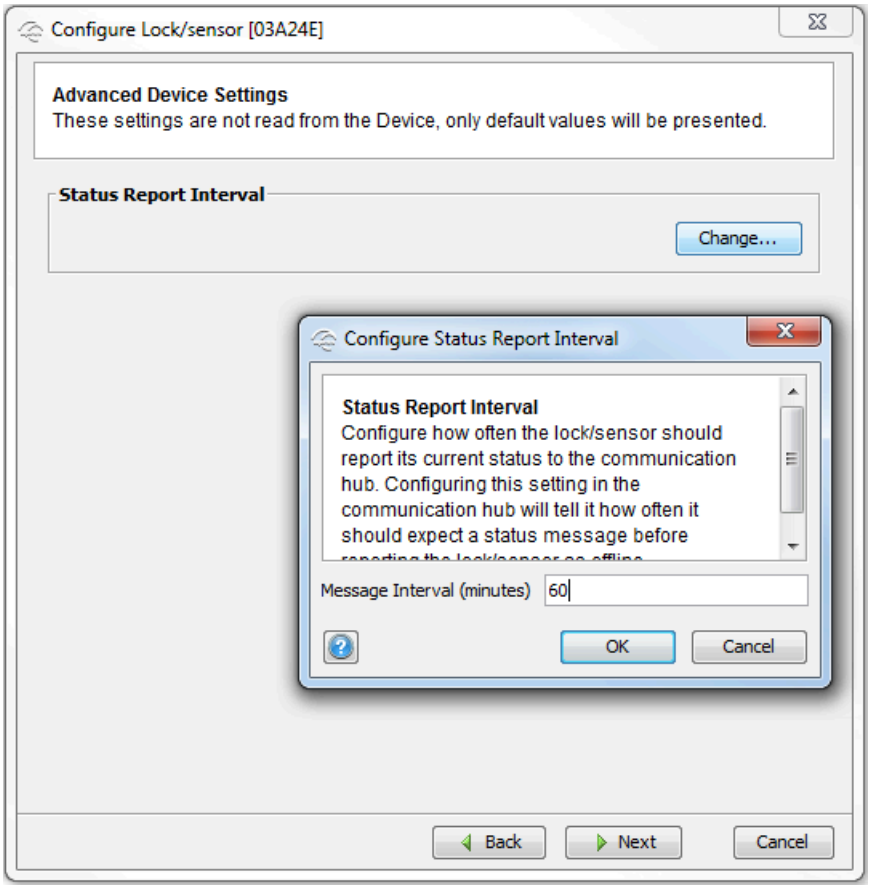
You can ignore the value of **Default unlock duration for Wiegand**.

10 If unlock schedules are used, enter a value for the **Status Report Interval** in the range 5 - 15 minutes.

Lowering the status interval time decreases the battery life of the product. Any changes to this interval must be made on both the lock and the communication hub. If only one lock is paired with

the communication hub, then this is done automatically. If more than one lock is paired with the communication hub, then you must set the **Status Report Interval** through the communication hub.

NOTE: With v3 locks, the **Status Report Interval** setting is only used to report the online status of the lock. It is the **Polling Interval** used to minimize the time lag for starting and ending the unlock schedule.



11 Pair each wireless lock:

a) Right-click **Communication hub** and select **Pair with lock or sensor**.

The pairing process starts.

b) Hold the credential at the lock, or engage the magnet for the sensor to pair the hardware with the communication hub.

The hub automatically assigns an EAC address to the lock.

c) Write down the EAC address (1 - 127) assigned to the lock.

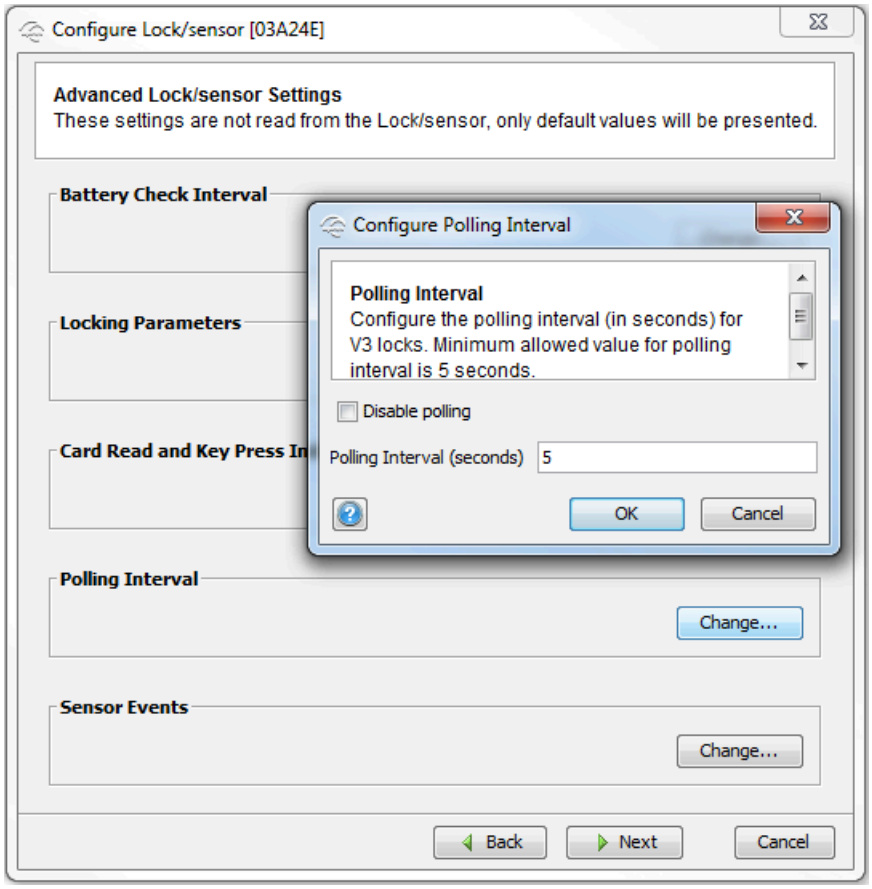
The hub's EAC address is incorporated into the lock's EAC address. To obtain the hub's EAC address from the lock's EAC address, use one of the following formulas:

- *Hub's EAC address* = *Lock's EAC address* **modulo** 16
- *Hub's EAC address* = (**Remainder of** *Lock's EAC address*) **divided by** 16

12 If you are using v3 locks, set the **Polling Interval** to 5 seconds.

This minimizes the time lag for starting and ending the unlock schedule, which reduces the reaction time of the locks. It also allows the manual unlock commands issued from Security Desk to work within

5 seconds. It is not recommended to use manual unlock commands on locks other than v3 because the command only works after 1 minute or longer, depending on the **Status Report Interval**.



13 After all locks are paired, set the hub to use secure radio communication.

After you finish

Enroll the locks on the Synergis unit.

Enrolling Aperio-enabled locks connected to an AH30 hub

For the Synergis™ Cloud Link unit to communicate with Aperio-enabled locks, you must enroll them in the Synergis™ Appliance Portal.

Before you begin

- Pair the Aperio-enabled locks to the hub.
- Connect the hub to one of the RS-485 channels (1 - 4):
  - Connect the A connector of the hub to the "+" of the channel.
  - Connect the B connector of the hub to the "-" of the channel.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ( ).

4 In the *Add hardware* dialog box, from the **Hardware type** list, select **Aperio RS 485**.

5 Select the **Channel** (1 - 4).

NOTE: If you have the Synergis Cloud Link 312 unit, then you have up to 12 channels. For more information, see About the Synergis Cloud Link 312 RS-485 ports.

6 From the **Interface module type** list, select **Aperio**.

7 Specify the locks that you want to enroll by doing one of the following:

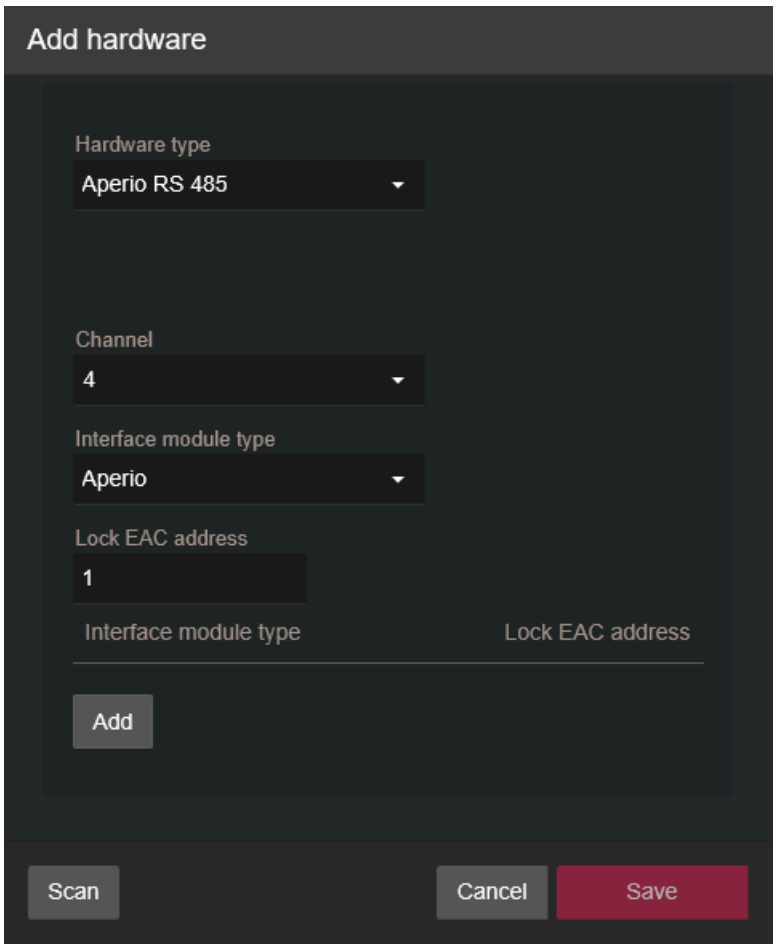
- To enroll automatically, click **Scan**.

  The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

  If the Synergis™ Appliance Portal does not find all connected interface modules, try manual enrollment.
- To enroll manually, enter the EAC address (1 - 127) of the lock that you wrote down while pairing the lock to the hub, and click **Add**.

Repeat as necessary to configure all modules connected to the same channel.

TIP: If you know the EAC addresses of the locks and you only have a few to enroll, it is faster to enroll them manually.



8 Click **Save**.

The hardware type, channel, and interface module you just added are listed on the *Hardware configuration* page.

9 Select a lock to view its properties in the right pane.

The EAC addresses of both the hub and the lock are indicated.

10 For each interface module you added, select it from the *Hardware configuration* page and configure its settings.

For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.

11 Test your interface module connection and configuration from the *I/O diagnostics* page.

After you finish

- Enroll the Synergis unit in Security Center.
- Configure the doors equipped with Aperio-enabled locks.

Pairing Aperio-enabled locks with the AH40 IP hub

If you use Aperio-enabled locks with an AH40 hub, you must configure the hub using the Aperio Programming Application (APA) before you can enroll the locks on your Synergis™ unit.

Before you begin

Ensure that you have the following:

- Aperio Online Programming Application Manual
- Aperio Programming Application (APA)
- USB dongle
- TriBee Bootloader, which includes the USB dongle driver
- Supported firmware
- Computer for running the APA
- Card that is compatible with the reader
- Encryption key file provided by ASSA ABLOY

Procedure

1 Power on the hub.

2 Plug the USB dongle into your computer and install the following:

- TriBee Bootloader (driver for the USB dongle)
- Aperio Programming Application (APA)

3 Open APA, and then open or create an installation.

NOTE: Each installation is linked to an encryption key file. Contact ASSA ABLOY for this key file to create an installation.

4 Use APA to configure the hub:

a) Update the firmware on the hub and the locks.

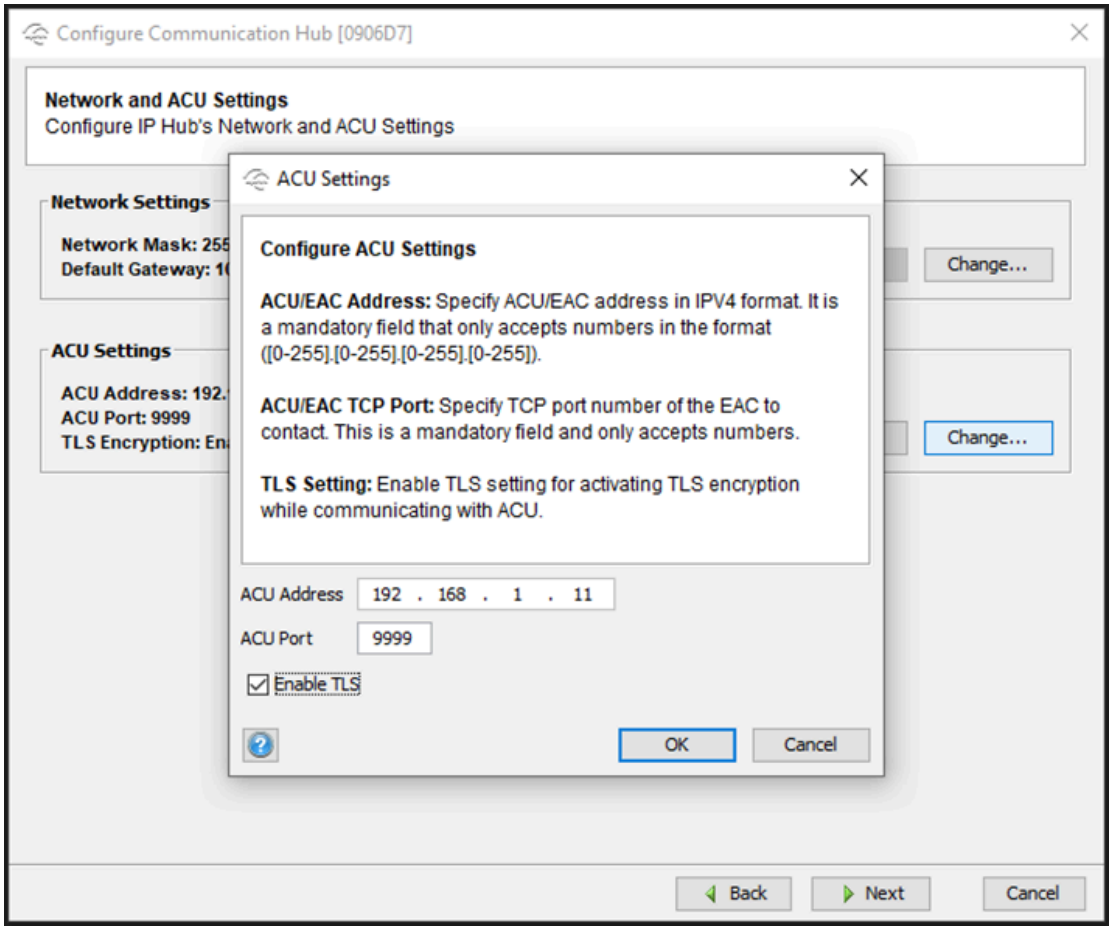
BEST PRACTICE: Upgrade the communication hub before upgrading the locks or sensors.

b) Pair the hub with the readers.

Selecting the AH40 IP hub in APA automatically pairs the hub with the readers.

NOTE: Take note of the port number. You need it to enroll the hub in the Synergis™ Appliance Portal.

c) Specify the IP address of the Synergis unit as the ACU address.



Enrolling Aperio-enabled locks connected to an AH40 IP hub

For the Synergis™ unit to communicate with Aperio-enabled locks, you must enroll them in the Synergis™ Appliance Portal.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ( ).

4 In the *Add hardware* dialog box, select **Aperio IP** as the **Hardware type**, and enter the port number of the hub in the **Port** field. The default port is 9999.

5 Click **Save**.

6 Click **Edit** ( ) on the Aperio IP interface.

The configuration dialog box of the channel opens.

7 In the configuration dialog box, select the **Enroll** check box for the hub you want to enroll.

NOTE: If you have configured more than one AH40 hub on the same port, all connected hubs and their MAC addresses are listed.

8 Click **Save**.

The locks connected to the enrolled AH40 hub are listed in the hardware tree and turn green. This can take up to 2 minutes.

Configuring doors equipped with an Aperio-enabled lock

To ensure that you do not receive duplicate *Door locked* and *Door unlocked* events in Security Desk, you must disable the **Automatically grant REX** option for all doors equipped with an Aperio-enabled lock.

Before you begin

- Enroll the Synergis Cloud Link unit in Security Center.
- Depending on the hub you are using, do one of the following:
  - For AH30 RS-485 hubs, pair your locks with the AH30 hub and enroll the Aperio-enabled locks on the Synergis unit.
  - For AH40 IP hubs, pair your locks with the AH40 hub and enroll the Aperio-enabled locks on the Synergis unit.

What you should know

The Aperio-enabled lock uses a mechanical REX. The Synergis Cloud Link unit does not control the unlocking of the door when a REX is triggered. Enabling **Automatically grant REX** in the door configuration causes the *Door locked* and *Door unlocked* events to be received twice in Security Desk.

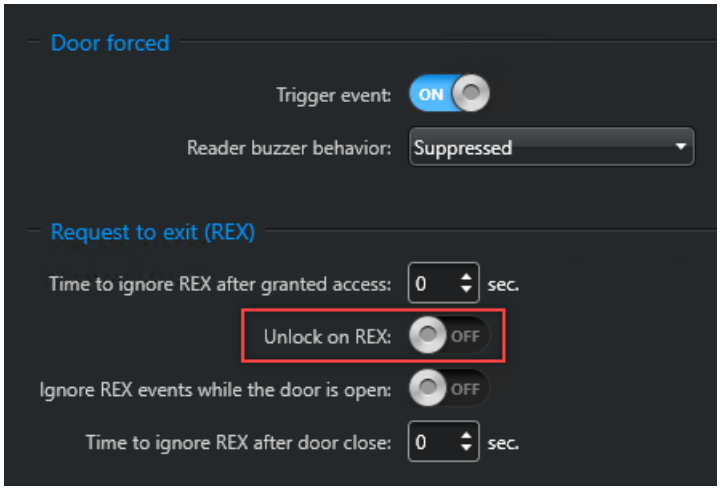
Procedure

1 From the Config Tool homepage, open the *Area view* task.

2 In the entity tree, select the door that uses the Aperio-enabled lock.

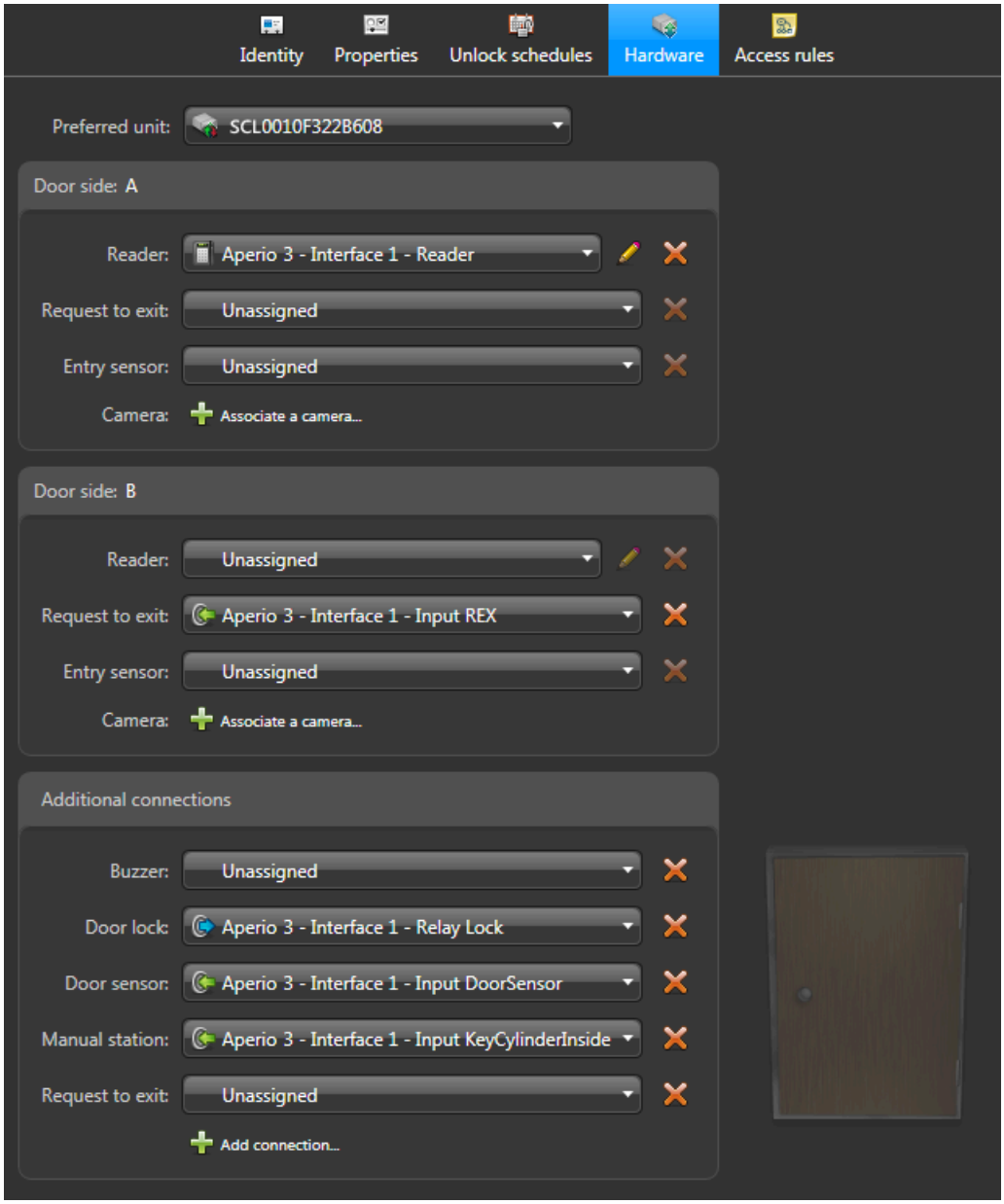
3 Click the **Properties** tab.

4 In the *Request to exit (REX)* section, turn off the **Unlock on REX** option.



5 Click the **Hardware** tab, and then select the Synergis unit that controls the lock.

All peripherals corresponding to the same lock are named with the same prefix “Aperio X - Interface n,” where X is the channel number (1 - 4), and n is the EAC address of the lock.



6 In the *Door side In* section, assign the reader corresponding to the door.

7 In the *Door side Out* section, assign the REX sensor corresponding to the door.

8 In the *Additional connections* section, apply the following settings:

- Assign the lock relay to **Door lock**.
- Assign the door sensor input to **Door sensor**.
- Assign the *KeyCylinderInside* or the *KeyCylinderOutside* to **Manual station**, if applicable.

9 If the reader is intended to work in *Card and PIN* mode, ensure that you configure a timeout long enough for the cardholder to enter the PIN.

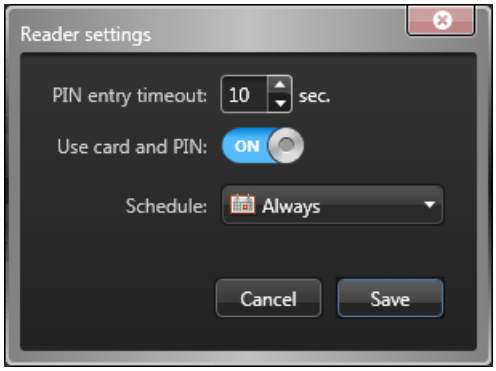
The default access timeout of 5 seconds is not long enough for Aperio-enabled locks. After presenting their credential at the door, the cardholder has to wait until the LED turns green before entering the PIN. This process invariably takes longer than 5 seconds.

a) Click **Reader settings** (✎) beside the **Reader** list.

b) In the *Reader settings* dialog box, turn on the **Use card and PIN** option.

c) Set the **PIN entry timeout** to the desired duration.

The recommended duration is 10 seconds.



d) Click **Save**.

10 Click **Apply**.

7

ASSA ABLOY IP locks

This section includes the following topics:

Configuration overview for ASSA ABLOY IP locks

To configure ASSA ABLOY IP locks to work with a Synergis™ unit, you must first configure the locks with the Lock Configuration Tool (LCT), and then pair the locks to the Synergis unit using the Synergis™ Appliance Portal.

The following table summarizes the IP lock configuration process.

Phase	Description	See
1	Make sure that your IP lock firmware is up to date and supported by your version of Synergis™ Softwire.	• *IP-Enabled Lock Installation Quick Start Guide* that came with your lock. • Supported ASSA ABLOY IP locks.
2	Configure the IP lock using the LCT. • Configure the Host address of the IP lock to be the same as the IP address of the Synergis unit. • Configure the communication port of the IP lock that the Synergis unit uses as a listening port when discovering the locks (Default=2571). • If encryption is required, set the AES key in the lock profile. You need this key after you pair the IP lock with the Synergis unit.	• *Network & Lock Configuration Tool User Manual* that came with your lock.
3	Establish communication between the Synergis unit and its connected IP locks in the Synergis Appliance Portal.	• Enrolling ASSA ABLOY IP locks connected to the Synergis unit on page 97.

About radio wake-up events for ASSA ABLOY Wi-Fi locks

In the Synergis™ Appliance Portal, you can select the events that ASSA ABLOY Wi-Fi locks must immediately report to the Synergis™ Cloud Link unit through Wi-Fi radio by configuring the **Wake Up events** option on each lock.

How it works

Wi-Fi lock data is only synched with the Synergis Cloud Link unit on the default Wi-Fi radio wake-up schedule that occurs every day at 0:00 UTC time. Exceptionally, when a wake-up event occurs, the Wi-Fi radio wakes up so that the event can be synched to the unit right away. Only the wake-up events are synched during this time. All other events and configuration changes are synched on the next scheduled wake-up.

NOTE: When cardholders or credentials are configured to expire before the next scheduled wake-up, they can continue to grant access until the next scheduled wake-up.

Use the **Wake Up events** option on each lock to select the events that wake up the Wi-Fi radio. The default radio wake-up events are *Door forced open* and *Door open too long*.

How to help minimize battery usage on Wi-Fi locks

In some installations, locks can have a short battery life because the locks generate many *Door open too long* events that wake up the Wi-Fi radio. Their battery life can be extended if it's acceptable to report *Door open too long* events on the next scheduled or unscheduled radio wake-up. To prolong the battery life, set the **Wake Up events** option for these locks in the Synergis Appliance Portal to **Door forced open only**. The *Door forced open* events wake up the Wi-Fi radio and the *Door open too long* events are reported on the next wake-up.

Configuring radio wake-up events for ASSA ABLOY Wi-Fi locks

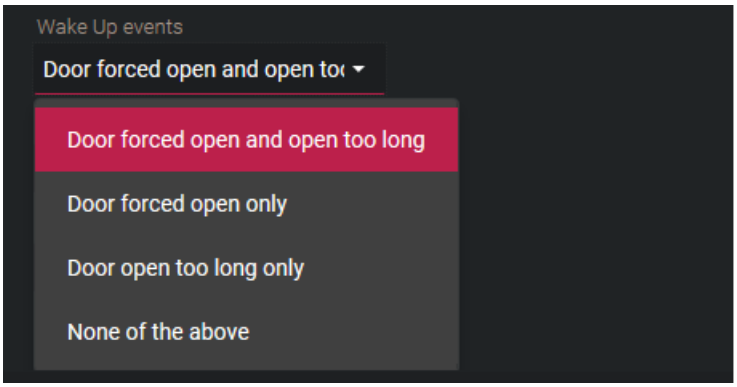
You can configure individual ASSA ABLOY Wi-Fi locks to contact the controller through Wi-Fi radio on specific wake-up events.

Before you begin

Enroll the ASSA ABLOY IP lock.

What you should know

You can configure a wake-up event for each ASSA ABLOY Wi-Fi radio lock.



Procedure

1. Log on to the Synergis Cloud Link unit.
2. Click **Configuration** > **Hardware**.
3. Select **Assa Abloy IP**, and then select the ASSA ABLOY channel and the lock.
4. Set the **Wake Up events** option for the lock.
5. Click **Apply**.

Enabling escape and return mode on ASSA ABLOY IP locks with body type 8200 and monitored deadbolt

To enable the *escape and return mode* on doors controlled by ASSA ABLOY IP locks, you must create a Boolean custom field named Escape Return for doors, and set it to TRUE on the doors on which you want to have this feature enabled.

Before you begin

The ASSA ABLOY IP locks that support the *escape and return* feature are the models with lock body 8200 and monitored deadbolt.

For example:

- IN120 and IN220 8200 mortise lock with deadbolt. No other IN120 and IN220 locks support this feature.
- Passport 1000 P2 mortise lock with deadbolt. No other Passport 1000 P2 locks support this feature.

What you should know

The Canadian fire code states that a door can never automatically relock. Therefore, when the escape and return feature is enabled, the following features are disabled.

- Unlock schedules
- Maintenance mode
- Manual unlock from Security Desk
- Temporarily override schedules from Security Desk

With the escape and return feature enabled, when a cardholder exits through a door, the door remains unlocked after it closes until the cardholder presents their access card to lock the door. If the cardholder doesn't present their card to lock the door, the door remains unlocked while they are gone. When the cardholder returns, they must present their card to open the door. After they have entered, they must throw the deadbolt to lock the door.

Procedure

1 In Config Tool, create a Boolean type custom field for door entities and name it `Escape Return`.

NOTE: Spell the name exactly as it's written. Include the capital and lowercase letters, and the space.

2 Open the *Area view* task and set the **Escape Return** custom field to TRUE for all doors where this feature must be enabled.

TIP: If you need this feature enabled on many doors, we recommend using the Copy configuration tool.

3 (Wi-Fi locks only) Trigger a radio wake-up to activate the escape and return feature on the lock.

You can trigger a radio wake by removing the lock's cover and pressing the button, or by presenting a denied credential.

4 Go through the escape and return mode cycle for a first time by exiting from a door, and by presenting a valid credential after the door closes.

This causes the system to create the custom events that you can use to configure event-to-actions.

Two custom events are added to your system:

- **Escape Return Mode Start:** Door unlocked by exiting or by entry with a valid credential.
- **Escape Return Mode End:** Door locked with valid credential or by throwing deadbolt from the inner side of the door.

Configuring a persona serial number for IN120 and IN220 locks

Before you can use passage mode on SARGENT and Corbin Russwin Cx IN120 and IN220 locks, they must be configured with a persona serial number.

Procedure

1 Connect the lock to a workstation, and open the lock configuration file using the Lock Configuration Tool (LCT).

2 From the *Lock Configuration* page, click the **Settings** icon.

3 Click the **Serial Number Setup** tab.

4 Change the **Manufacturer** and **Board Type** to *Persona*.

5 Apply the changes and follow the on-screen instructions.

The lock now has a new serial number.

6 Using LCT, re-apply the configuration to the lock.

7 If the lock was already added to the Synergis™ unit, do the following:

a) Delete the lock and re-add it using the new serial number.

b) Re-configure the door entity hardware with the new lock.

About passage mode for ASSA ABLOY IP locks

Passage mode is a feature available for all ASSA ABLOY IP locks. This feature allows authorized cardholders to keep locks in the unlocked state by badging on the reader either once or twice, depending on the lock controller or brand. Repeating the process returns the lock to its normal state.

Passage mode triggered by single badge

The following applies to SARGENT Cx locks, Corbin Russwin Cx locks IN120 and IN220, and all Sx locks. When the reader is in Card or PIN or Card and PIN mode, passage mode is started and stopped in the following ways:

- **Card or PIN:** Either badge once or enter the PIN.
- **Card and PIN:** Badge once, and then enter the PIN.

NOTE: Cardholders must have a security clearance above 7.

Passage mode triggered by double badge

The following applies to specific locks:

- All Px locks
- Sx locks running Hx firmware
- SARGENT Cx lock Passport 1000 P1 and P2
- Corbin Russwin Cx locks Access 700 PIP1 and PWI1
- SARGENT and Corbin Russwin Cx locks IN120 and IN220 with a PERSONA serial number

NOTE: The IN120 and IN220 locks can either be ordered or configured manually.

- **Card or PIN:** Badge twice to start passage mode. The PIN can’t be used.
- **Card and PIN:** Badge once, enter the PIN, and then badge again to start passage mode.

Passage mode enabled per door or per access rule

You can enable the passage mode feature using either a custom field for doors or for access rules. Using both custom fields at the same time is not recommended. When passage mode is enabled through a door custom field, anyone who has access to the door can use passage mode. When passage mode is enabled through an access rule custom field, you can restrict the feature to specific doors and cardholders.

Enabling passage mode on ASSA ABLOY IP locks

To enable passage mode on doors controlled by ASSA ABLOY IP locks, you must create a Boolean custom field named PassageMode for either doors or access rules.

Before you begin

- Learn about the passage mode feature.
- Configure a persona serial number for IN120 and IN220 locks.

Procedure

To enable the passage mode feature per door:

1 In Config Tool, create a Boolean type custom field for door entities and name it `PassageMode`.
NOTE: Spell the name exactly as it's written. Include the capital and lowercase letters.
2 Open the *Area view* task.
3 From the entity browser, select a door, and then click the **Custom fields** tab.
4 Select the **PassageMode** custom field, and then click **Apply**.
5 Repeat the previous two steps for all doors on which you want passage mode enabled.

To enable the passage mode feature per access rule:

1 Log on to the Synergis™ unit.
2 Click **Configuration** > **Downstream controller settings**.
3 In the *Assa Abloy IP lock settings* section, select the **Enable passage mode per access rule** option.
4 Click **Save**.
5 Restart your Synergis unit.
The *PassageMode* custom field for access rules is automatically created in Security Center.
6 From the Config Tool homepage, open the *Access control* task, and click the **Access rules** view.
7 From the entity browser, select an access rule, and then click the **Custom fields** tab.
8 Select the **PassageMode** custom field, and then click **Apply**.
9 Repeat the previous two steps for all access rules on which you want passage mode enabled.

Enabling privacy mode on ASSA ABLOY IP locks

To enable *privacy mode* from Config Tool on doors controlled by ASSA ABLOY IP locks, you must create a Boolean custom field named Privacy Mode for doors, and set it to TRUE on the doors on which you want to have this feature enabled.

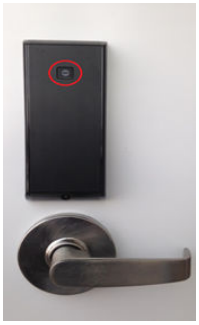
Before you begin

The ASSA ABLOY IP locks that support privacy mode are the Cx-type PoE and Wi-Fi locks.

What you should know

Privacy mode is an ASSA ABLOY IP lock feature that only grants access to supervisors, which are also known as override cardholders. This feature is disabled as a factory default. All cardholders with a security clearance value lower than 7 function as supervisors. Privacy mode is activated and deactivated in different ways, depending on whether or not the ASSA ABLOY lock has a monitored deadbolt:

- **Locks without monitored deadbolt:** Privacy mode is activated when the *privacy button* on the inner side of the door is pressed while the door is closed. The LED on the button flashes slowly for approximately 2 minutes to indicate that privacy mode is in effect. Privacy mode is deactivated when the door is opened from the inside, or when a supervisor badges in.

  NOTE: If the reader beeps and flashes purple five times when you press the *privacy button*, privacy mode can't be activated because the door is open.
- **Locks with monitored deadbolt:** Privacy mode is activated when the deadbolt is thrown while the door is closed. Privacy mode is deactivated when the deadbolt is retracted from the inside, or when a supervisor badges in.

Procedure

1 In Config Tool, create a Boolean type custom field for door entities and name it `Privacy Mode`.

NOTE: Spell the name exactly as it's written. Include the capital and lowercase letters, and the space.

2 Open the *Area view* task and set the **Privacy Mode** custom field to TRUE for all doors where this feature must be enabled.

TIP: If you need this feature enabled on many doors, we recommend using the Copy configuration tool.

Two custom door events are added to your system:

- **Deadbolt locked:** This event is triggered when privacy mode is activated on a door.
- **Deadbolt unlocked:** This event is triggered when privacy mode is deactivated on a door.

Enrolling ASSA ABLOY IP locks connected to the Synergis unit

For the Synergis™ unit to communicate with the ASSA ABLOY IP locks connected to it, you must pair them together in the Synergis™ Appliance Portal using the lock pairing mode.

Before you begin

Configure the IP locks using the Lock Configuration Tool (LCT). If encryption is enabled, write down the **Lock AES Key**.

What you should know

When the lock pairing mode is active, all the IP locks that are connected to the Synergis unit using the specified communication ports are discovered. After the pairing mode ends, the Synergis unit reconnects to the Access Manager in Security Center, and adds the paired IP locks.

Procedure

1 Log on to the Synergis Cloud Link unit.

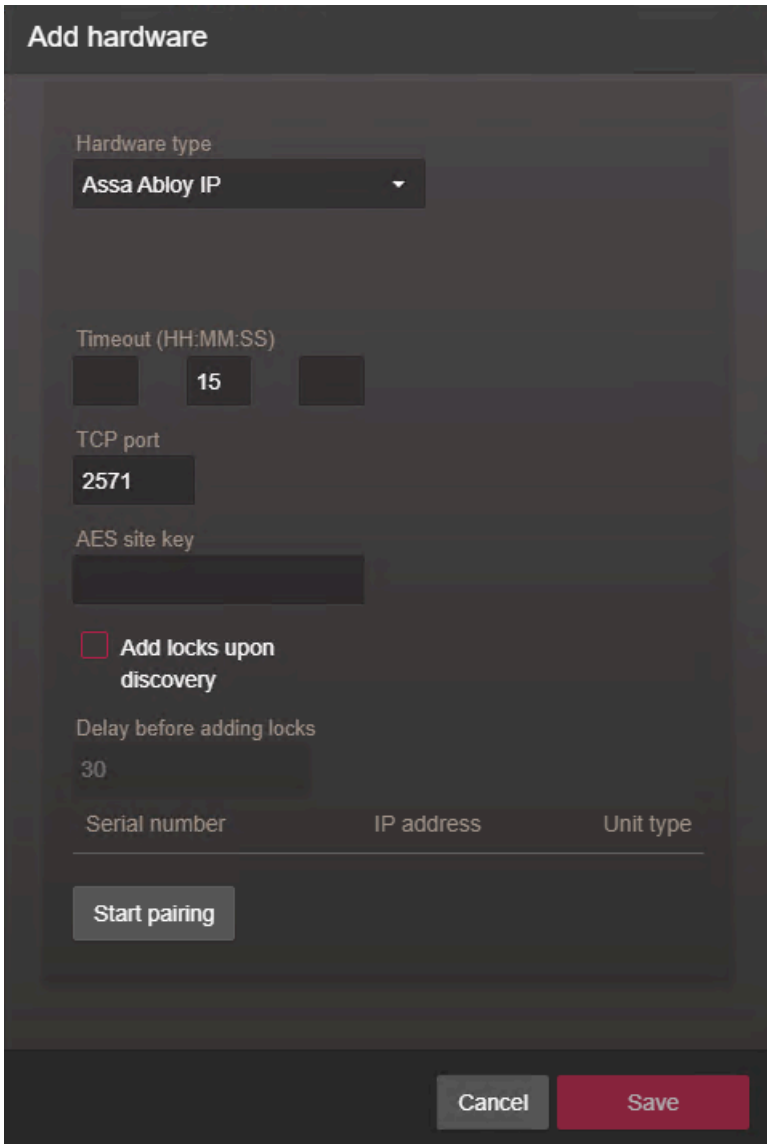
2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ( ).

4 From the **Hardware type** list, select **Assa Abloy IP**.

5 (Optional) In the **Timeout** field, select how long to activate the lock pairing mode for. New IP lock connections are only paired for the amount of time that you specify.

NOTE: Back up the Synergis unit's configuration file in case you need to replace the unit at some point, especially if you have many Wi-Fi locks, since they take longer to re-enroll.



6 If you're using a port other than the default 2571, in the *TCP port* field, enter the communication port you configured on the IP locks.

7 If you enabled encryption through LCT, in the *AES site key* field, enter the AES key (32-character hexadecimal string) configured on your lock.

NOTE: You can modify or remove the AES key from the *Hardware* page of the Synergis unit in Config Tool.

8 (Optional) If you want the IP locks to be added as they are discovered, do the following:

a) Select the **Add locks upon discovery** option.

IMPORTANT: When this option is selected, the Synergis unit reconnects to the Access Manager after each group of IP locks is added. This option is only recommended if you must start configuring the IP locks before the pairing mode is complete.

b) From the **Delay before adding locks** option, select how many seconds must pass before the previously discovered locks are added.

9 Click **Start pairing**.

IMPORTANT: For Wi-Fi locks, press the COM or Reset button inside the back panel of the lock to trigger a connection to the Synergis unit.

The IP locks are detected and added to the table.

If you have issues pairing the lock to the Synergis unit, test the connection between your IP lock and the unit.

10 Do one of the following:

- To stop lock pairing mode and add the discovered locks, click **Stop and save**.
- To cancel lock pairing mode, click **Cancel**.

  NOTE: If the **Add locks upon discovery** option is selected, some locks might have already been added.
- Wait until the lock pairing mode times out.

The Synergis unit reconnects to the Access Manager role, and the discovered locks are added.

11 Click **Configuration** > **Hardware**.

The IP locks that were added are displayed on the hardware configuration tree. When you select a lock, the unit type, serial number, and lock firmware of the selected IP lock are displayed under *Properties*.

12 If no information is displayed under *Properties*, refresh the page.

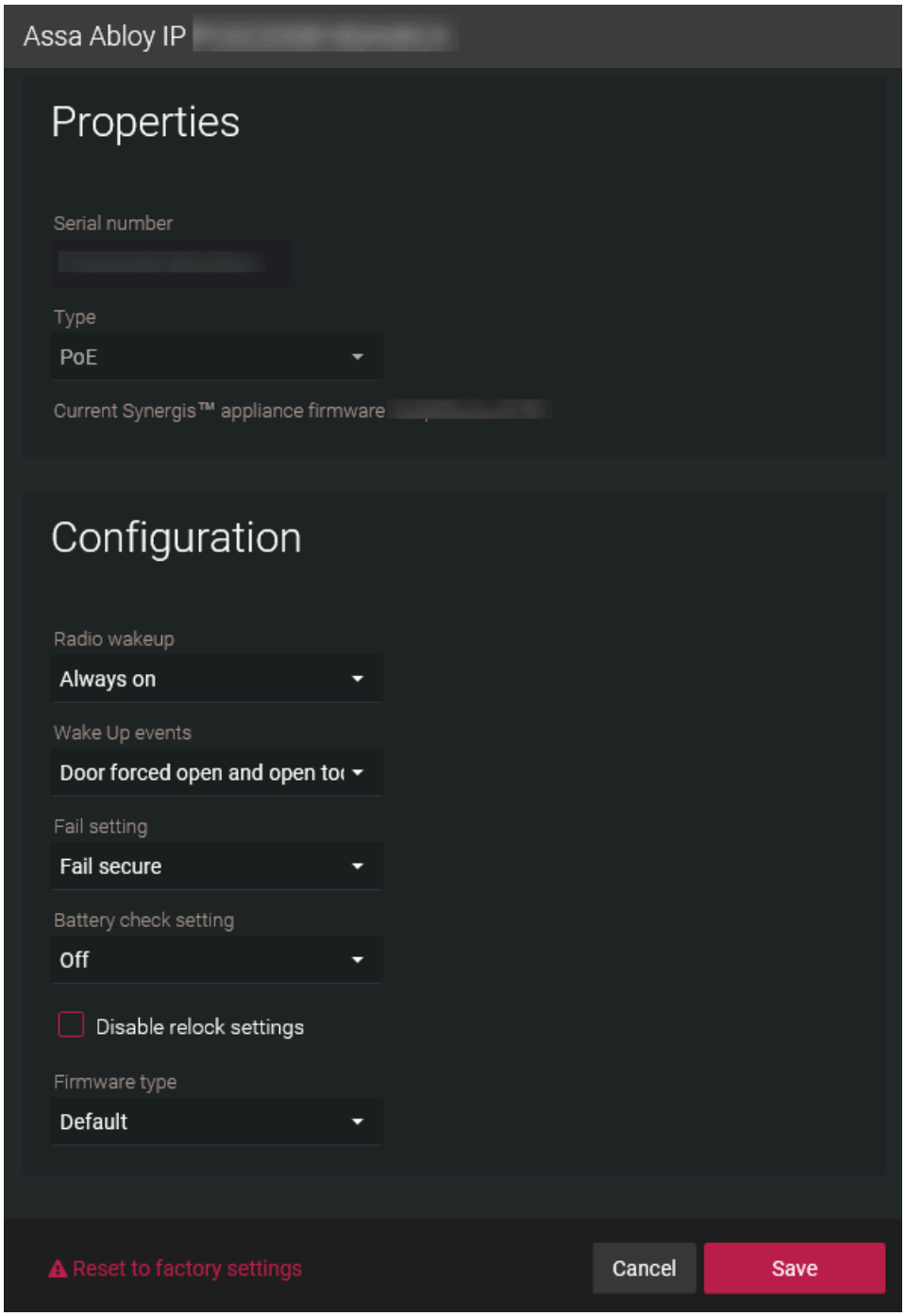
For Wi-Fi locks, it can take up to 2 minutes before the information is displayed under *Properties*. Wi-Fi locks appear in red in the hardware tree because they aren't in constant communication with the Synergis unit.

a) For PoE locks: Under *Properties*, make sure that **Radio wakeup** is set to **Always on** so that *Access granted* events are never missed in Security Desk, and set **Battery check setting** to **Off**.

b) For Wi-Fi locks: Under *Properties*, make sure that **Radio wakeup** is set to **Daily**, and enter the time of day (**Hour** and **Minute**) when it should occur.

Select **Local time** if you want the radio wake-up time to follow the time zone of the Synergis unit. If you don't select this option, the default is UTC.

c) Change the other lock settings as required.



13 Click **Save**.

Testing the connection between ASSA ABLOY IP locks and the Synergis unit

If you have trouble pairing the Synergis™ unit to your IP lock, you can test the connection between the lock and the unit using the Lock Configuration Tool (LCT).

Procedure

1 For PoE locks, refer to the **Ping Test** command in the LCT.

2 For Wi-Fi locks, refer to the **Verify Connection to Host** command in the LCT.

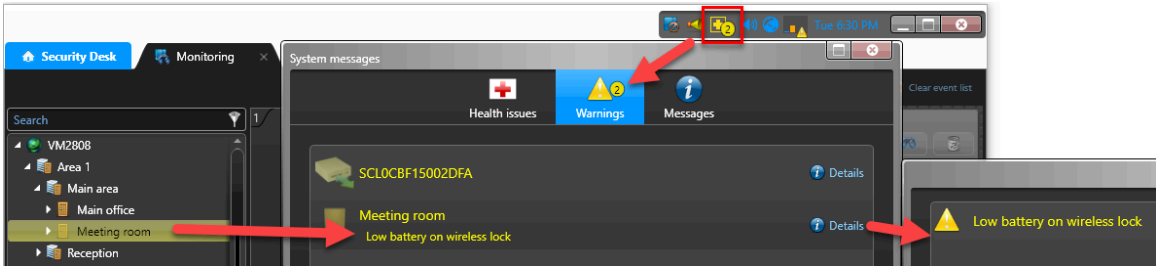
Monitoring the battery status of ASSA ABLOY Wi-Fi locks

To check the status of the battery on an ASSA ABLOY Wi-Fi lock, you can monitor the *Battery fail* event on the Synergis™ unit that it's connected to.

What you should know

For each Wi-Fi lock, Security Center creates a virtual input named *Input BatteryFail* that shows as *Active* in the **Monitoring** tab and yellow warning on the **System messages** icon in the notification tray when the battery is low.

NOTE: *Input BatteryFail* is a software input created to indicate the battery status of Wi-Fi locks. You can't connect any physical device to this input.



Procedure

1 From the Security Desk homepage, open the *System status* task.

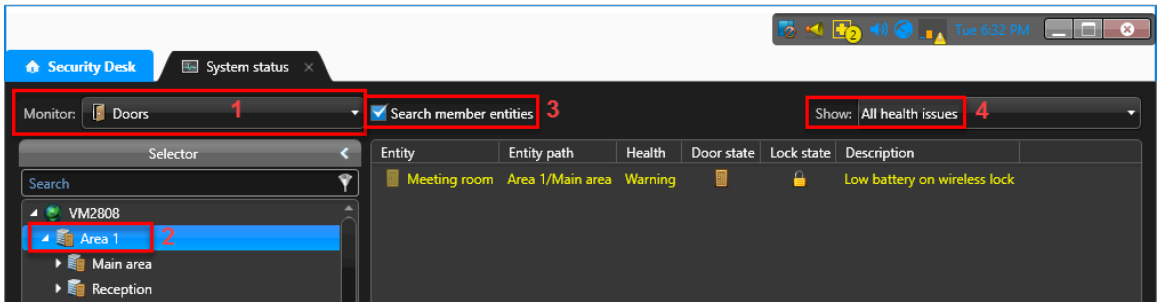
2 From the **Monitor** list, select **Doors**.

3 In the entity tree, select the parent area.

4 Select the **Search member entities** checkbox to display all the locks under the child areas.

5 In the **Show** list, select **All health issues** to show the doors with warnings.

NOTE: The Wi-Fi locks that have battery problems show an *Active* state for the **Input BatteryFailed** input.



6 Schedule a battery replacement for the Wi-Fi locks that have the low battery warning.

8

AutoVu SharpV cameras

This section includes the following topics:

Enrolling AutoVu SharpV cameras on the Synergis unit

For the Synergis™ unit to communicate with the SharpV camera, you must enroll the camera on the Synergis unit in Security Center.

Before you begin

- Configure the SharpV camera to use HTTPS communication. For more information, see the *Deployment Guide* or *Handbook* for the camera you are installing.
- Install either the Genetec™ self-signed certificate or a signed certificate from a trusted certificate authority.
- If you are enrolling a SharpV camera, log on to the SharpV web portal and change the default password.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** (➕).

4 In the *Add hardware* dialog box, select **AutoVu** from the **Hardware type** list.

5 Select a **Channel**.

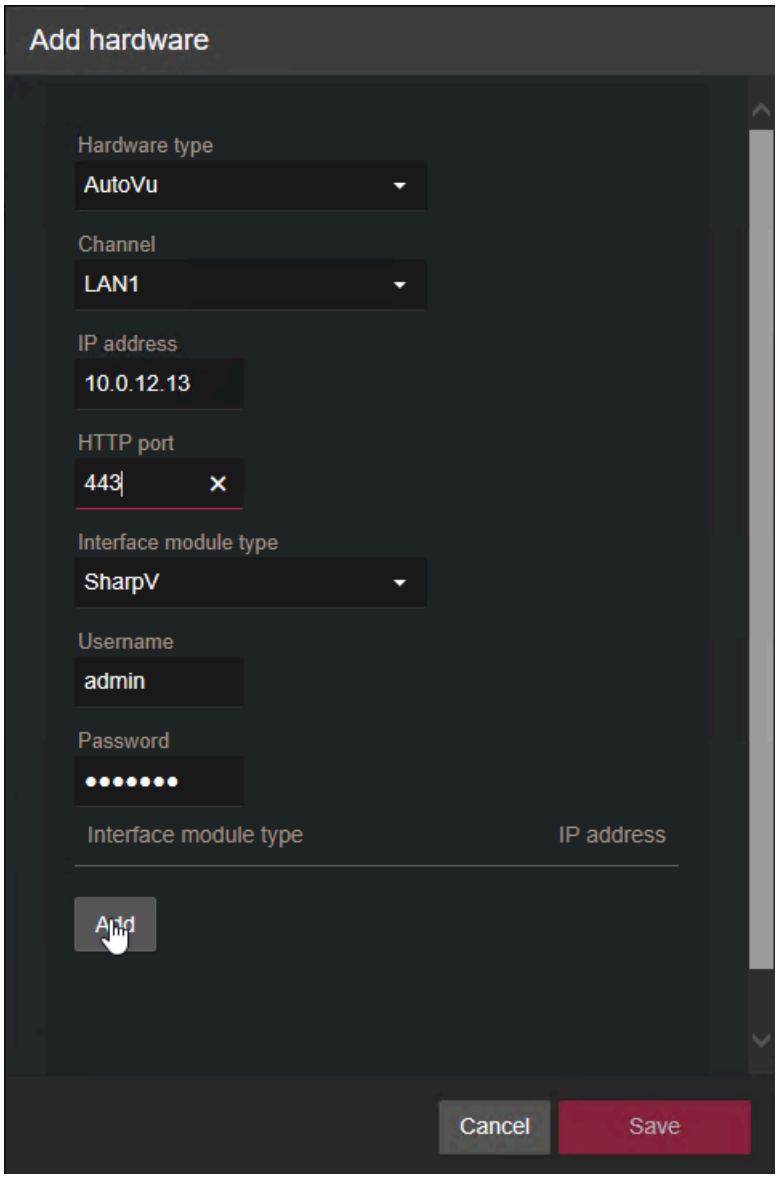
6 Enter the **IP address** of the camera.

7 Enter the **Port** of the camera.
The SharpV uses **Port** 443 for HTTPS communication with Security Center.

8 From the **Interface module type** list, select **SharpV**.

9 Enter the **Username** and **Password** used to access the SharpV web portal.
NOTE: For SharpV cameras, you cannot use the default password.

10 Click **Add**, then **Save**.



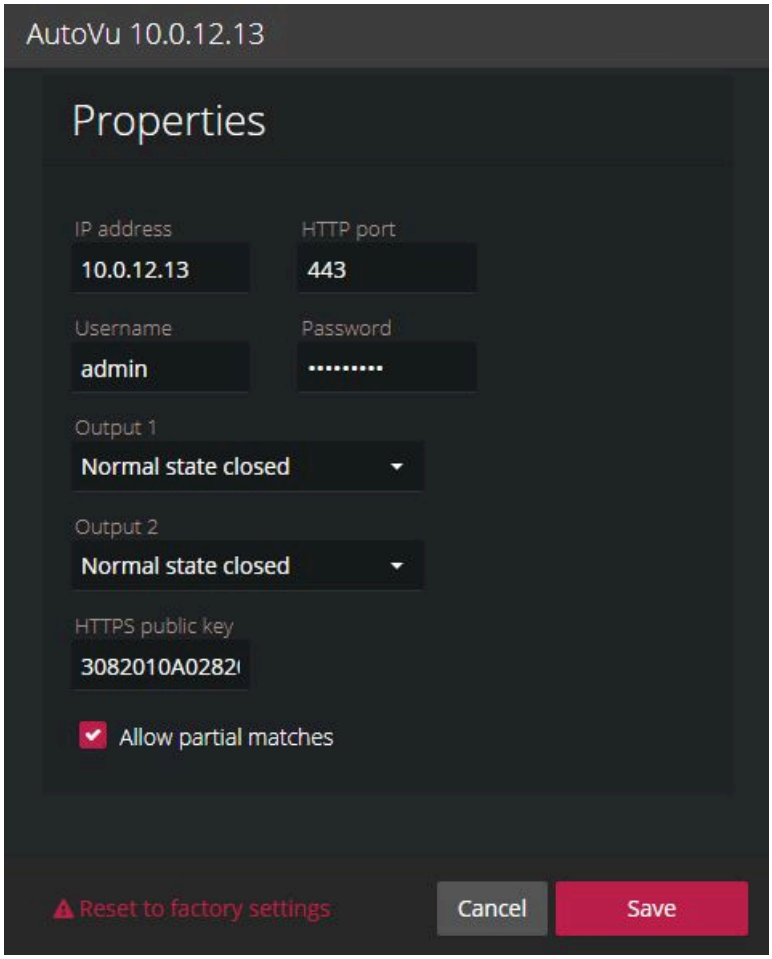
11 On the *Hardware configuration* page, click the enrolled AutoVu™ camera, then click its channel and interface to display its properties.

12 If you are using the SharpV outputs to control a vehicle access barrier, select whether the outputs are *Normally open* or *Normally closed*.

13 Leave the **HTTPS public key** field empty. This information is added automatically based on the camera's certificate.

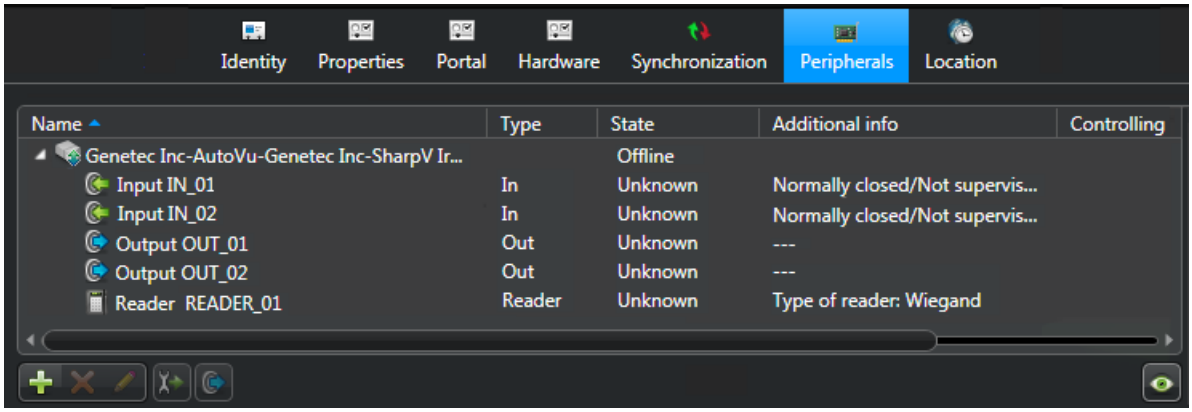
14 The **Allow partial matches** check box is selected by default. This feature accepts plate reads that have one-character difference from a configured license plate credential; this includes a single character

insertion, deletion, or substitution, at any place in the plate number. With this feature enabled, plate reads from dirty or damaged license plates are more likely to be accepted.



15 Click **Save**.

In Config Tool, the SharpV camera is displayed on the *Peripherals* page of the Synergis unit, and the inputs and outputs are displayed under the SharpV camera.



Configuring a SharpV camera to control a vehicle access barrier

To use a SharpV camera to control a vehicle access barrier, the barrier must be configured as a door in Security Center.

Before you begin

- Wire the vehicle access barrier to the Synergis™ appliance. For more information, see the *Hardware Installation Guide* for the access control appliance you are installing.
- Enroll the Synergis unit in Security Center.
- Enroll the SharpV camera on the Synergis unit.

Procedure

1 From the Config Tool homepage, open the *Area view* task.

2 Select the area where you want to add the vehicle access barrier.

3 Click **Add an entity** (), and select **Door**.

4 In the **Creating a door** wizard, enter the name and description of the vehicle access barrier.

5 From the **Location** list, select the area in which you are creating the door, and click **Next**.

6 On the *Door information* page, assign names to the barrier sides.

Example: In/Out, or Entrance/Exit.

7 To associate the barrier with the access control unit that it is wired to:

a) From the **Access control unit** list, select the Synergis unit.

b) From the **Interface module** list, select the SharpV camera.

8 Click **Next**.

9 Review the *Creation summary* page, and click **Create** > **Close.**

The barrier is displayed in the entity tree.

10 Select the barrier and click the **Properties** tab.

11 Configure the general access control behavior of the barrier. For more information, see the *Security Center Administrator Guide*.

12 Click **Apply**.

13 Click the **Hardware** tab and describe the wiring between the access control unit and the door to Security Center. For more information, see the *Security Center Administrator Guide*.

14 Create cardholders using their license plates as credentials. For more information on creating cardholders, see the *Security Center User Guide*.

When assigning credentials to the cardholder, select the **License plate** option.

15 Select who has access to the door. For more information, see the *Security Center Administrator Guide*.

9

Axis controllers

This section includes the following topics:

Enrolling Axis controllers on the Synergis unit

For the Synergis™ unit to communicate with Axis controllers, you must enroll the controllers using either the Synergis™ Appliance Portal or Config Tool.

Before you begin

- Have the serial numbers or IP addresses of your Axis controllers at hand. To find that information, see your Axis documentation.
- Connect your Axis controllers to the Synergis unit.

What you should know

When the Synergis unit enrolls a controller, it sets a default configuration for all Axis input contacts and output relays. Axis and Synergis use different terminology to describe their settings.

NOTE: Only the enrollment through the Synergis™ Appliance Portal is described here, but you can also enroll an Axis controller from **Config Tool** > **Access control** > **Roles and units**.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

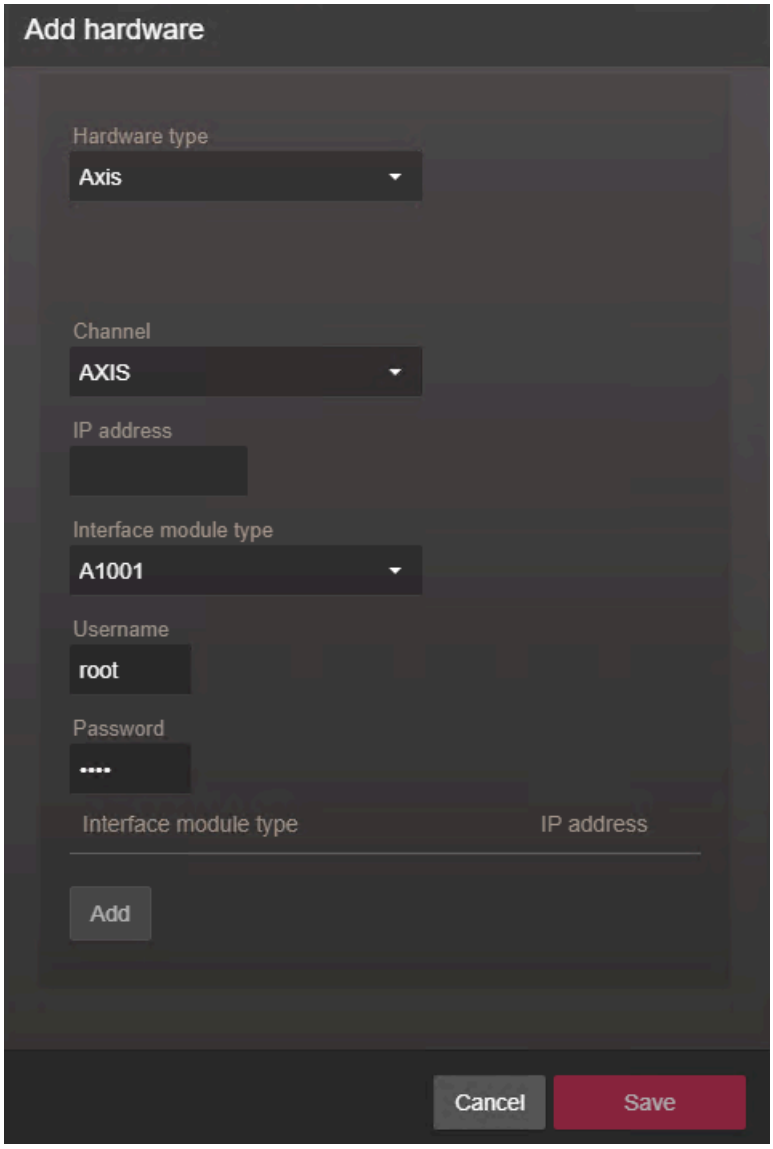
3 At the top of the **Hardware** column, click **Add** (➕).

4 In the *Add hardware* dialog box, select **Axis** as the **Hardware type**.

5 Select the IP channel where the Axis controller is connected.

6 Enter the connection parameters required to connect to the Axis controller.

- **IP address:** Use the IP address of the Axis controller.
- **Interface module type:** Select the Axis unit type that you are enrolling. The default is A1001.
- **Username and password:** The default username and password are `root` and `pass`, respectively.



7 Click **Add**.

8 Activate **Autonomous mode**.

9 (Optional) Repeat steps 3 - 8 to add another Axis controller.

10 Click **Save**.

The hardware type, channel, and interface module you just added are displayed on the *Hardware configuration* page. It can take up to 1 minute for the Axis module to come online.

11 If the current firmware version is not the latest, upgrade it by doing one of the following:

- Recommended for Security Center 5.10 or later: Upgrade the firmware using the *Hardware inventory* task in Config Tool. For more information, see Upgrading access control unit firmware and platform, and interface module firmware.
- Upgrade the firmware using the Synergis™ Appliance Portal.

12 Test your interface module connection and configuration from the *I/O diagnostics* page.

NOTE: To use the HTTPS protocol, the AXIS A1001 must use firmware 1.65.2 or later, and A1601 interfaces must use firmware 1.83.1.1 or later.

After you finish

Add the Synergis unit to an Access Manager role so it becomes part of your Security Center system.

Enabling autonomous mode on Axis controllers

To enable your Axis units to make access decisions independently of a Synergis™ unit, activate *autonomous mode* in the Synergis™ Appliance Portal.

What you should know

In high-latency situations, *Autonomous mode* improves the delay between a card read and a *Door unlocked* event by disabling remote authorization. The Axis unit sends the information to the Synergis unit after the decision is taken.

NOTE: Because *Autonomous mode* does not contact the Synergis unit for access control decisions, there are certain limitations related to enabling the mode:

- Advanced features in Security Center are disabled.
- Credential changes, like revoking a credential's access, take longer to apply because the changes must be sent to the Axis unit during synchronization.

Procedure

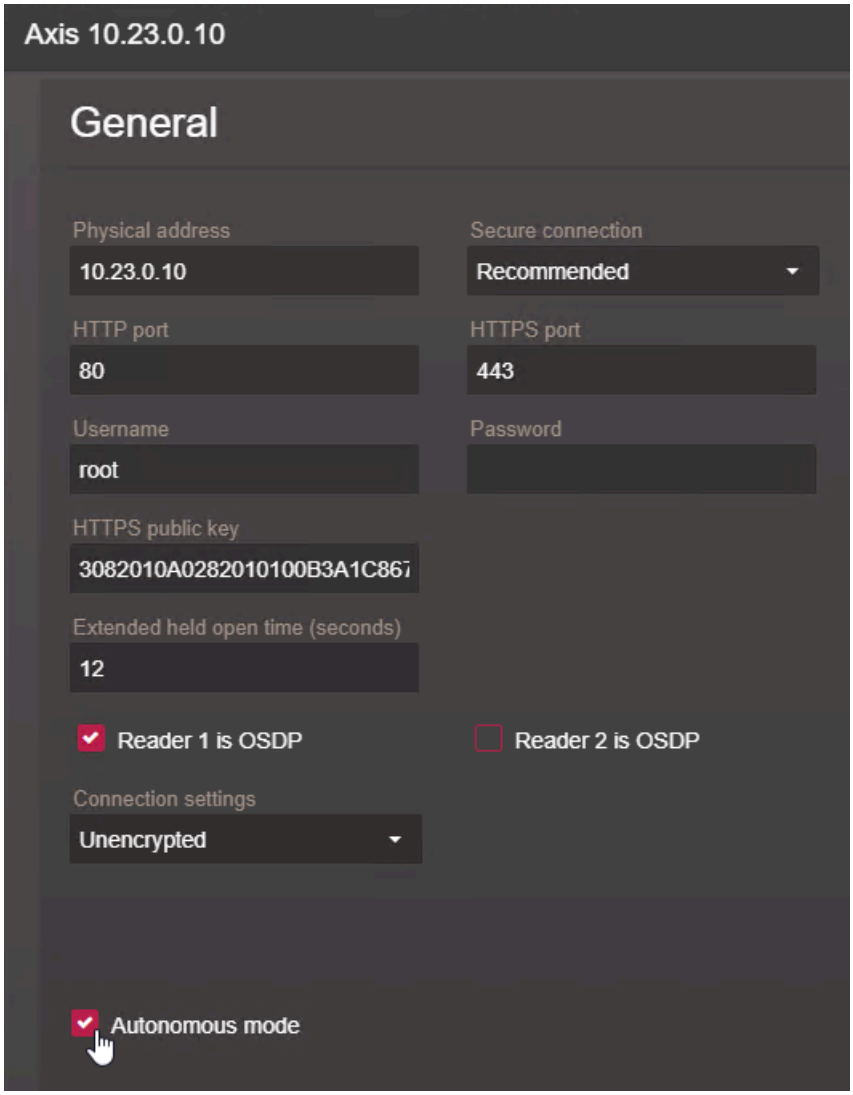
1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 From the hardware tree, select the Axis unit that you want to run in *Autonomous mode*.

The configuration window opens.

4 Select the **Autonomous mode** check box.



5 Click **Save**.

6 (Optional) Repeat steps for all Axis units that you want to run in *Autonomous mode*.

The Axis unit makes access-grant decisions independently, and then send access control information to the Synergis unit.

Hardening Axis controllers

It is recommended to enable IP address filtering on the Axis controller to allow the IP addresses of the Synergis™ unit and of the admin workstation to connect to the controller.

Before you begin

- Make sure you get the latest Axis firmware package.
- Follow the latest Product Security recommendations from Axis Communications.
- Enroll the Axis controllers.

Procedure

1 Log on to the Axis controller web portal.

For more information, see the Axis documentation.

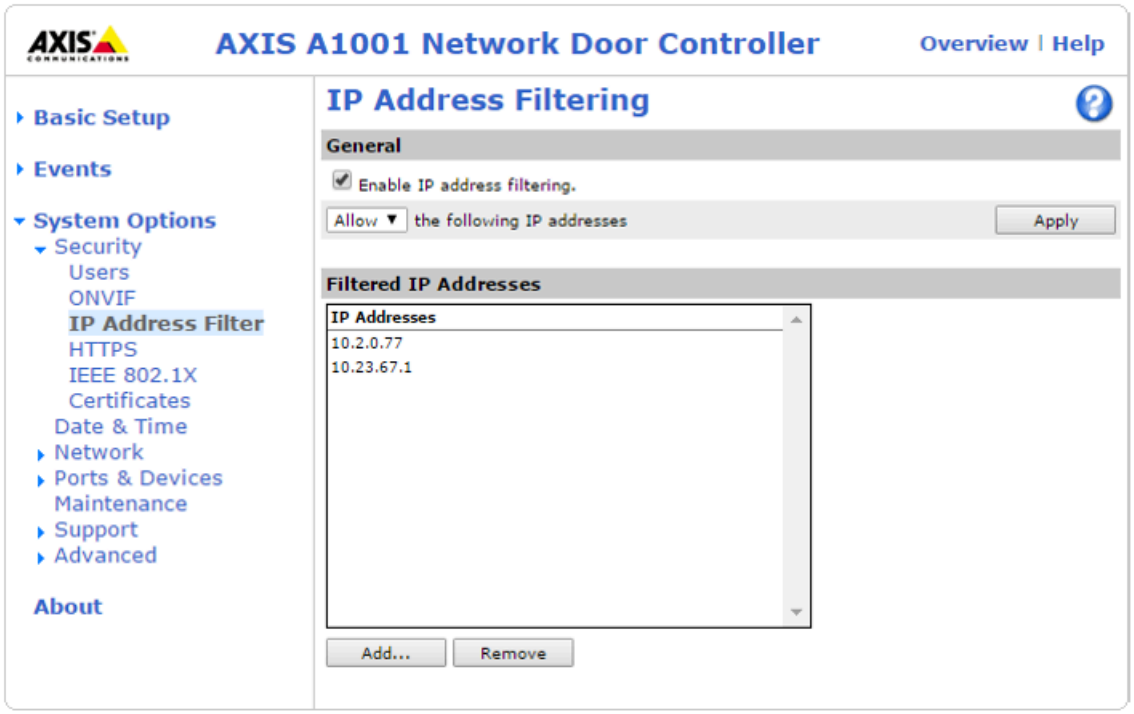
2 Click **Setup** > **Additional Controller Configuration** > **System Options** > **Security** > **IP Address Filter**.

3 Select the **Enable IP address filtering** option, and select **Allow** from the list.

4 Click **Apply**.

5 In the *Filtered IP Addresses* list, add the IP address of the Synergis unit and the IP address of the administrative workstation that must log on to the Axis controller web portal.

Example:



6 Under **System options**, click **Network** > **TCP/IP** > **Advanced**, and disable both **FTP server** and **RTSP server** options.

They are not used by Synergis™ Softwire.

7 Click **Save**.

Configuring Axis controller peripherals

To configure the input contacts, output relays, and readers attached to the Axis controller, you must make your changes in Config Tool and the Synergis™ Appliance Portal.

Before you begin

- Enroll the Axis controller on the Synergis™ unit.
- Add the Synergis unit to an Access Manager role.

What you should know

- Output relays and readers are configured on the *Hardware* page of the Synergis unit in the Synergis™ Appliance Portal or in Config Tool.
- Input contacts are configured on the *Hardware* page and *Peripherals* page of the Synergis unit in Config Tool.

Procedure

To configure the output settings of an Axis controller:

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 For A1601 controllers, configure the auxiliary I/O ports to be used as inputs or outputs, as required.

4 For A1001 controllers, configure the settings, as required.

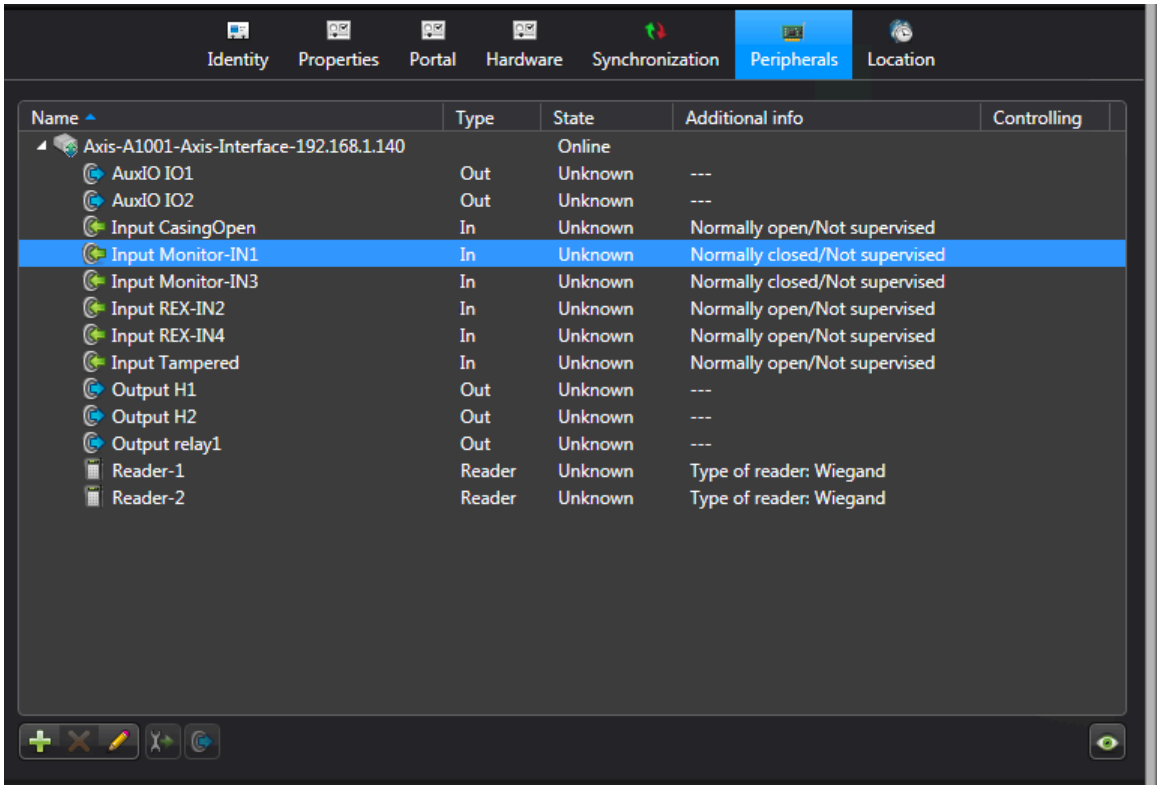
For more information about each setting, see the Axis documentation.

To configure the input settings of an Axis controller:

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

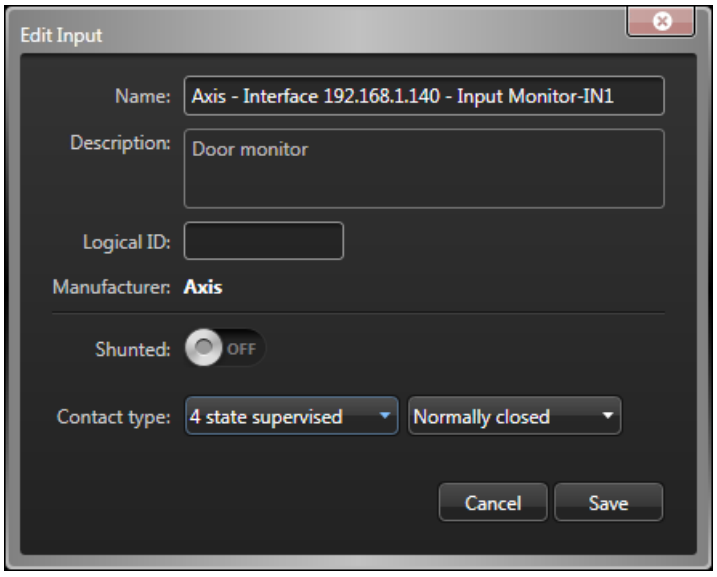
2 From the entity tree, select the Synergis unit, and click the **Peripherals** tab.

3 Expand the Axis controller that you want to modify, select an input, and then click **Edit** ( ).



4 In the *Edit input* dialog box, make changes, as required.

Example:



NOTE: The available settings depend on the input that you select. On A1601 units, I/O 1, 2, 3, 4, 13, and 14 cannot be supervised when configured as inputs.

- **Name:** Input device name.
- **Logical ID:** Must be unique among all peripherals attached to the same unit.
- **Shunted:** Select this option to ignore the inputs. Once shunted, the state of the input remains at *Normal*, regardless of how you trigger it.

NOTE: If the door is forced open, the *Door forced open* event is still generated in Security Center, even if the door input is shunted.

- **Contact type:** Set the *Normal* state of the input contact and its supervision mode.
  - **Not supervised/Normally closed:** The normal state of the input contact is closed, and the access control unit does not report that the input is in the trouble state.
  - **Not supervised/Normally open:** The normal state of the input contact is open, and the access control unit does not report if the input is in the trouble state.
  - **4-state supervised/Normally closed:** The normal state of the input contact is closed, and the access control unit reports when the input is in the trouble state.
  - **4-state supervised/Normally open:** The normal state of the input contact is open, and the access control unit reports when the input is in the trouble state.

5 Click **Save**, and then click **Apply**.

Configuring the auxiliary I/O ports on AXIS A1601 controllers

You can configure the auxiliary I/O ports on AXIS A1601 controllers to be used as either inputs or outputs, using the Synergis™ Appliance Portal.

What you should know

- If an auxiliary I/O is already used in a configuration, and you change its type, the I/O goes offline, and you must manually update that I/O in the configuration in Security Center.
- By default, auxiliary I/O 1 and 2 are outputs, and auxiliary I/O 3, 4, 13, and 14 are inputs. When configured as inputs, they cannot be supervised.

Procedure

1 Log on to the Synergis Cloud Link unit.

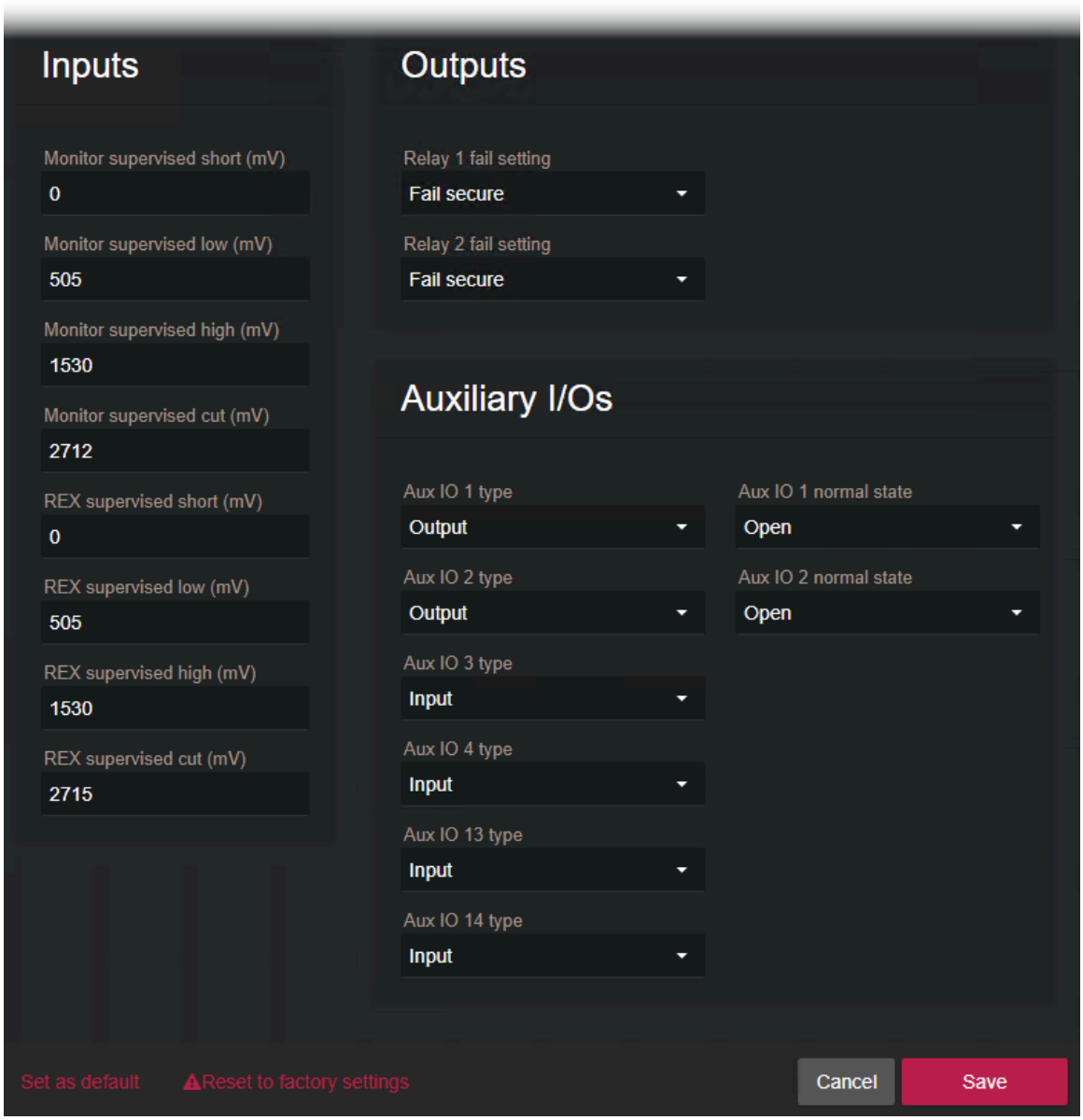
2 Click **Configuration** > **Hardware**.

3 Click the Axis unit in the *Hardware* column, and then in the *Channels* column.

4 In the *Interfaces* column, click the unit to open its settings.

5 Scroll down to the *Auxiliary I/Os* section, and change the **Aux IO types**, as required.

NOTE: If you change the type to an output, you must configure the normal state as **Open** or **Closed**. The normal state of an input can only be configured in Config Tool.



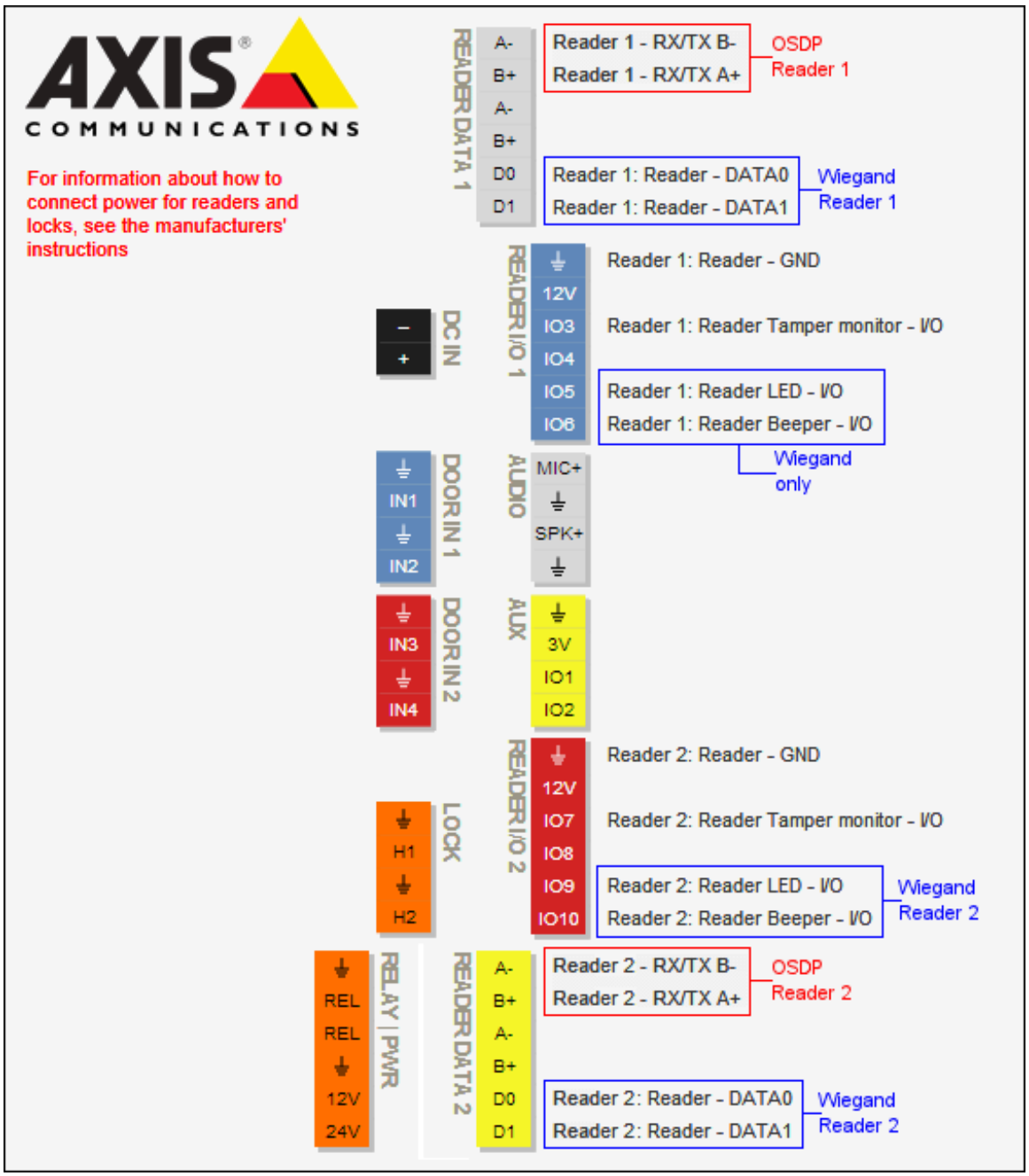
6 Click **Save**.

Reader connections on the AXIS A1001 controller

Each AXIS A1001 controller supports up to two readers, called *Reader 1* and *Reader 2* in Security Center Config Tool. The readers can use either Wiegand (default) or OSDP protocol. For OSDP, the reader must be wired to the first set of reader data **A-**/**B+**.

The following chart shows the set of connectors corresponding to the reader on the Axis controller.

NOTE: This pin chart only shows up if the Axis controller is disconnected to the Synergis™ unit.



Reader connections on the AXIS A1601 controller

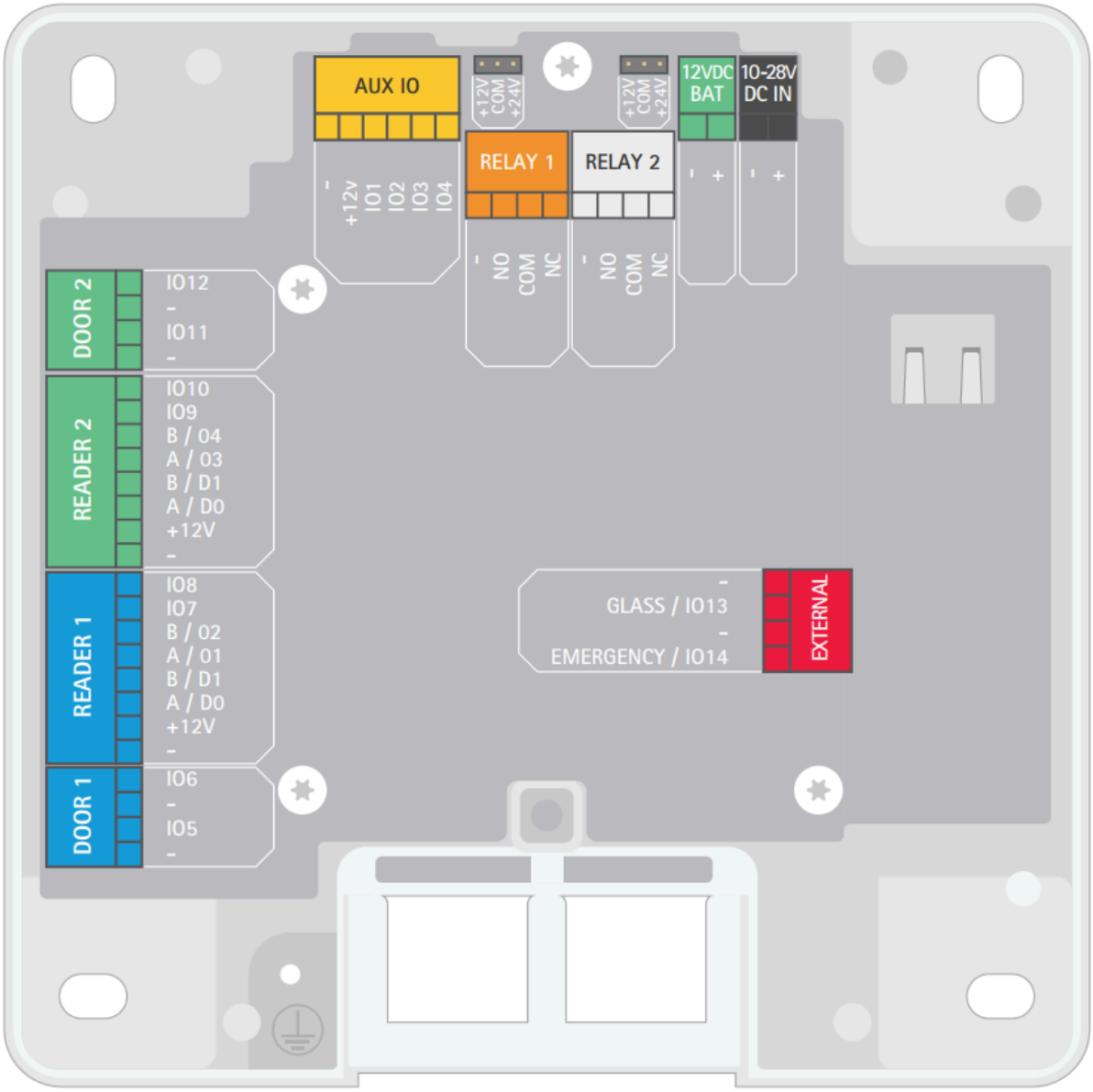
Each AXIS A1601 controller supports up to two readers, called *Reader 1* and *Reader 2* in Security Center Config Tool.

The following chart shows the set of connectors corresponding to the reader on the Axis controller.

By default, the A1601 controller is represented in Security Center as the following:

- Eight inputs: Two door sensors, two REX, four auxiliary inputs (I/O 3, 4, 13, and 14)
- Four outputs: Two door lock relays, two auxiliary outputs (I/O 1 and 2).

NOTE: The auxiliary I/Os can be configured to be either inputs or outputs.



Enabling OSDP (Secure Channel) readers on AXIS A1601 controllers

You can use OSDP with Secure Channel between the AXIS A1601 controller and their OSDP readers to ensure end-to-end encryption.

What you should know

A1601 controllers require firmware 1.84.4 or later.

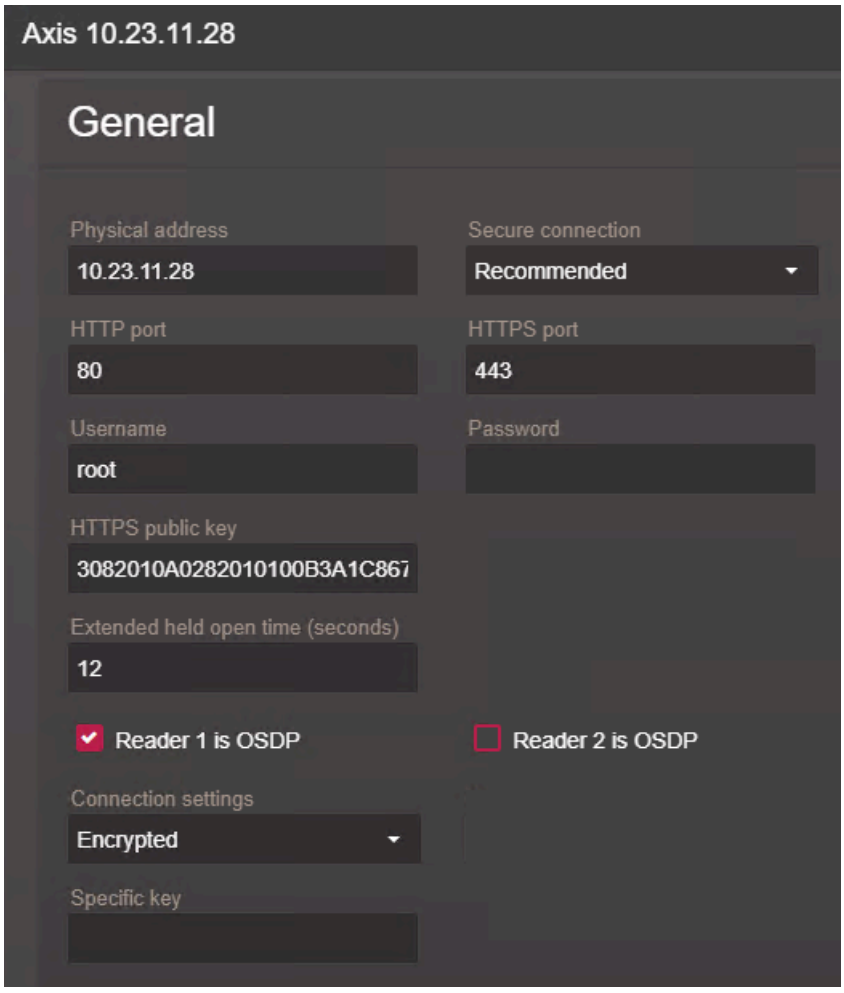
Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 From the hardware tree, select the Axis unit that you want to add OSDP (Secure Channel) readers to.
The configuration window opens.

4 Select the **Reader is OSDP** checkbox for the desired reader.



5 From the **Connection settings** list, select **Encrypted**.

6 In the **Specific key** field, enter a 128-bit (32 hexadecimal characters) key.

If the reader was previously configured for secure communication, copy-paste the existing key. Otherwise, set the reader to installation mode (see the reader manufacturer's documentation), and copy-paste the key of your choice.

7 Click **Save**.

The key is added to the Axis key store and is used to communicate with the reader.

10

DDS controllers

This section includes the following topics:

Enrolling DDS RS-485 controllers on the Synergis unit

For the Synergis™ unit to communicate with the DDS controllers connected to its RS-485 interface, you must enroll them on the Synergis unit with the Synergis™ Appliance Portal.

Before you begin

Connect the DDS modules to the Synergis unit's RS-485 channels (1 - 4) as follows:

- Connect the Rx\L of the DDS module to the "-" of the channel.
- Connect the Tx\H of the DDS module to the "+" of the channel.
- Connect the 0v of the DDS module to the "G" of the channel.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ( ).

4 In the *Add hardware* dialog box, select **DDS** as the **Hardware type**.

5 Select the **Channel** (1 - 4).
All interface modules connected to the same channel must be from the same manufacturer.

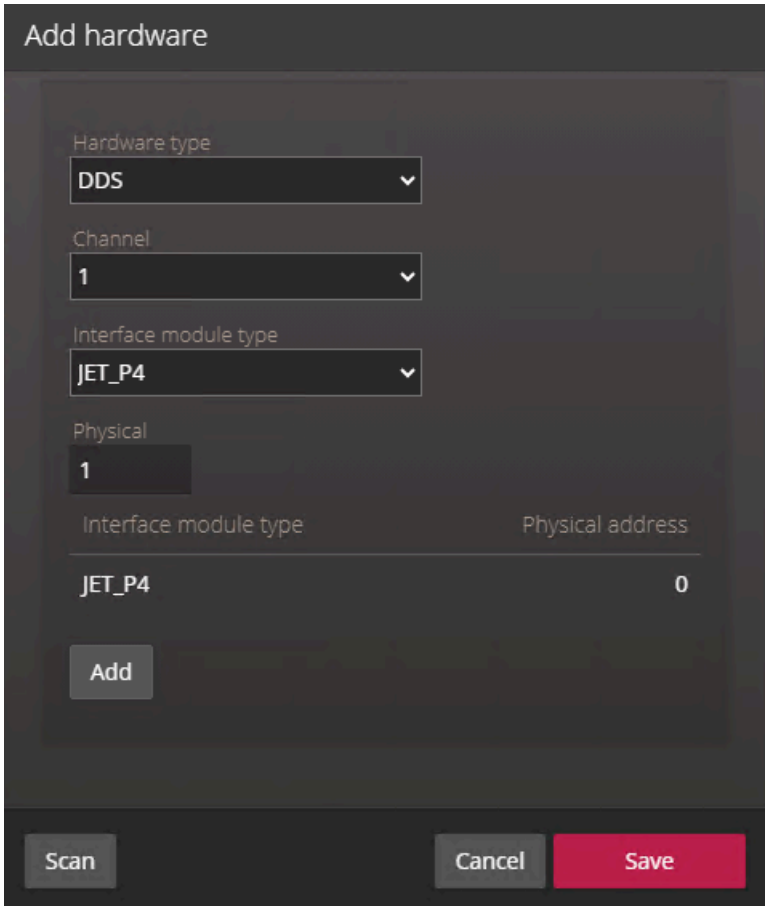
6 In the same dialog box, add all interface modules connected to the same channel.

Do one of the following:

- To enroll manually, select the **Interface module type** from the list, enter the physical address (0 - 31) configured on the DDS module, and then click **Add** (+).

  Repeat as necessary to configure all modules connected to the same channel.

  Example:



- To enroll automatically, click **Scan**.

  The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

  If the controller doesn't find all connected interface modules, make sure they all have a different physical address.

  Once you click **Add**, the address in the **Physical** field cycles to the next available address.

7 Click **Save**.

The hardware type, channel, and interface module you just added are listed on the *Hardware configuration* page.

8 For each interface module you added, select it from the *Hardware configuration* page and configure its settings.

For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.

9 Click **Save**.

10 Test your interface module connection and configuration from the *I/O diagnostics* page.

After you finish

Enroll the Synergis unit in Security Center.

Setting the physical address of DDS RS-485 controllers

All JET or TPL door controllers that are either connected to the same RS-485 channel or found on the same LAN must use different physical addresses.

What you should know

The physical address must be a value from 0 - 31, and is set using the DIP switches on the DDS controller. The DIP switches are labeled differently, depending on the model of the controller:

- For TPL controllers, the physical address is set with the DS2/1 and JP4/1 - 5 DIP switches.

  NOTE: If you have a TCP/IP extension board attached to the TPL controller, you must remove it to access the DIP switches.
- For JET controllers, the physical address is set with the DS1/1 - 5 DIP switches.

The reader communication protocol is set using the JP4/6 - 8 DIP switches on TPL controllers and the DS1/6 - 8 DIP switches on JET controllers. For example, for Wiegand to read up to 50 bits without parity check on a TPL controller, set JP4/7 to 1 or ON. For more information, see the documentation from DDS corresponding to your specific device.

Procedure

1 For TPL controllers, set DS2/1 to 1 or ON.

2 Set the physical address on the JP4/1 - 5 or DS1/1 - 5 DIP switches, according to the following tables:

Proto. 4 address:	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
JP4/1 or DS1/1	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On
JP4/2 or DS1/2	Off	Off	On	On	Off	Off	On	On	Off	Off	On	On	Off	Off	On	On
JP4/3 or DS1/3	Off	Off	Off	Off	On	On	On	On	Off	Off	Off	Off	On	On	On	On
JP4/4 or DS1/4	Off	Off	Off	Off	Off	Off	Off	Off	On	On	On	On	On	On	On	On
JP4/5 or DS1/5	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off	Off

Proto. 4 address:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
JP4/1 or DS1/1	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On
JP4/2 or DS1/2	Off	Off	On	On	Off	Off	On	On	Off	Off	On	On	Off	Off	On	On
JP4/3 or DS1/3	Off	Off	Off	Off	On	On	On	On	Off	Off	Off	Off	On	On	On	On
JP4/4 or DS1/4	Off	Off	Off	Off	Off	Off	Off	Off	On	On	On	On	On	On	On	On
JP4/5 or DS1/5	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On

Example

To set the physical address of a TPL controller to 15, set DS2/1 to ON and JP4/1 - 5 to ON ON ON ON OFF, respectively.

To set the physical address of a JET controller to 16, set DS1/1 - 5 to OFF OFF OFF OFF ON, respectively.

11

HID VertX sub-panels

This section includes the following topics:

Enrolling the HID VertX sub-panels connected to the Synergis unit

To establish communication between the Synergis™ unit and the attached interface modules, you need to configure them in Synergis™ Appliance Portal.

Before you begin

Attach the HID VertX modules to the channels (1 - 4) of your Synergis Cloud Link unit.

NOTE: If you have the Synergis Cloud Link 312 unit, then you have up to 12 channels. For more information, see About the Synergis Cloud Link 312 RS-485 ports.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ( ).

4 In the *Add hardware* dialog box, select **VertX** as the **Hardware type**.

5 Select the **Channel** (1 - 4).

All interface modules connected to the same channel must be from the same manufacturer.

6 In the same dialog box, add all interface modules connected to the same channel.

You can enroll the interface modules automatically or manually.

TIP: If you know the physical addresses of the modules and you only have a few to enroll, it would be faster to enroll them manually.

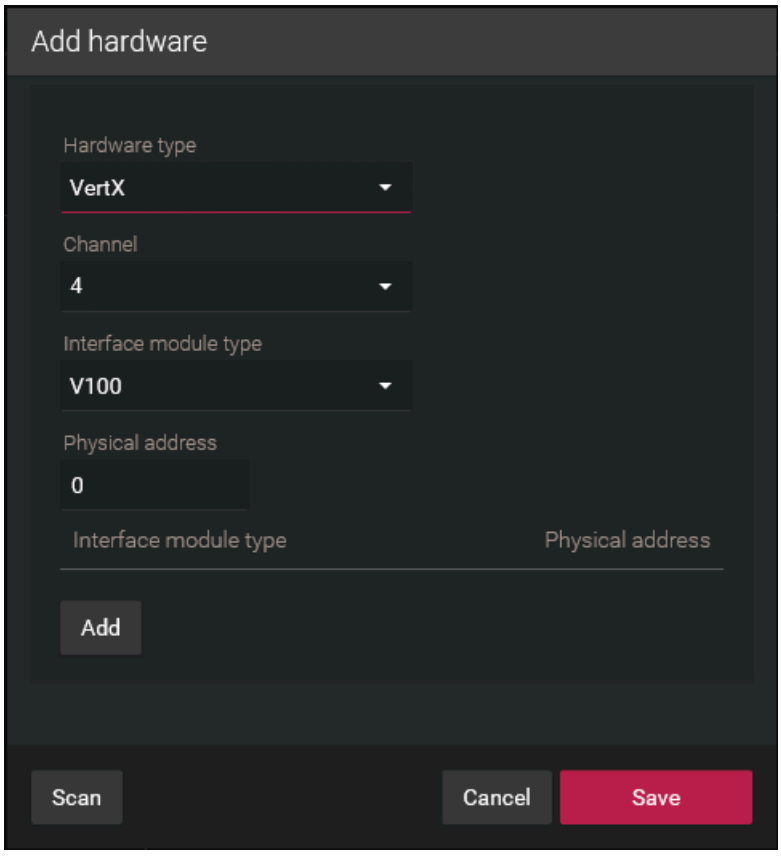
Do one of the following:

- To enroll automatically, click **Scan**.

The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

If the controller does not find all connected interface modules, make sure they all have a different physical address.

- To enroll manually, enter the physical address (0 - 15) configured on the HID interface device, select the model type, and then click ✚.



Repeat as necessary to configure all modules connected to the same channel.

7 Click **Save**.

The hardware type, channel, and interface module you just added are listed on the *Hardware configuration* page.

8 For each interface module you added, select it from the *Hardware configuration* page and configure its settings.

For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed.

9 Click **Save**.

10 Test your interface module connection and configuration from the *I/O diagnostics* page.

After you finish

Enroll the Synergis unit in Security Center.

Enabling reader supervision for HID VertX V100

To receive *Door offline* events when the reader connected to a VertX V100 panel is either disconnected or powered off, you must configure the **I'm Alive** reader setting in Config Tool and program the reader with the appropriate configuration card.

Before you begin

Enroll the VertX V100 panel on the Synergis™ unit.

What you should know

Reader supervision is only supported for readers connected to a VertX V100 panel that is controlled by a Synergis unit.

Procedure

1 From the Config Tool homepage, open the *Access control* task.

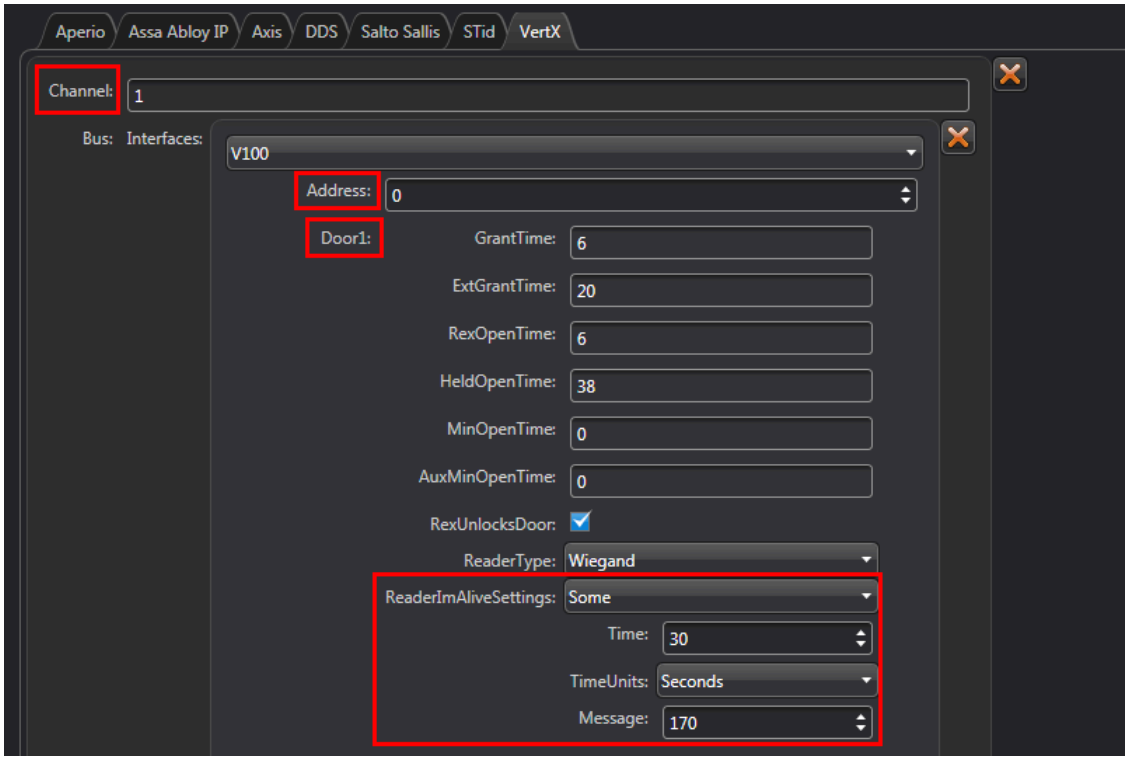
2 Click **Roles and units**, and then click the Synergis unit.

3 Click **Hardware**, and then scroll to the V100 panel to which the reader is connected.

If your Synergis unit is controlling multiple V100 panels, make sure you identify the correct reader by its **Channel**, its physical **Address**, and its door number (**Door1** or **Door2**).

4 Under the selected door, click **ReaderImAliveSettings**, and change its value to **Some**.

The **Time** must be equal or greater than the **I'm Alive** time found on the reader configuration card, and the **Message** must correspond to the **I'm Alive** message (170 is the decimal equivalent of AA in hexadecimal).



5 Click **Apply**.

6 Configure the reader using the appropriate field programming card (also known as a configuration card).

When this reader is disconnected from the V100 panel or powered down, you now get the event *Door offline: Device is offline* on the door that it is associated to.

12

Mercury controllers

This section includes the following topics:

Mercury reader settings

This is a complete list of Mercury reader settings; these settings correspond to specific reader hardware. Most readers in use today work on the Wiegand standard. To use smart cards or to set up Secure OSDP2 readers, refer to the specific readers' tech notes.

Function	Description
Type of reader	
Standard Wiegand	• Sets **Keypad mode** to **HID** • Sets **LED drive mode** to **Bi-color** • Sets **Wiegand pulses** to **ON**
Standard Magstripe	• Sets **Keypad mode** to **None** • Sets **LED drive mode** to **Bi-color** • Sets **Trim zero bits** to **ON** • Sets **Format to nibble array** to **ON** • Sets **Allow bi-directional Mag decode** to **ON** • Sets **Supervised** to **ON** • Sets **Inputs come from reader** to **ON**
Standard OSDP	• Enables **OSDP mode** • Sets **Keypad mode** to **HID** • Sets **LED drive mode** to **OSDP**
OSDP 2	• Enables **OSDP mode** • Sets **Keypad mode** to **HID** • Sets **LED drive mode** to **Custom OSDP** This mode also allows for configuration of the reader port's bit rate, Tracing, Smart Card, address, and use of Secured Communication.
Standard F2F	• Sets **Keypad mode** to **HID** • Sets **LED drive mode** to **Bi-color** • Sets **Format to nibble array** to **ON** • Sets **Casi 1-wire F2F** to **ON**
Supervised F2F	• Sets **Keypad mode** to **HID** • Sets **LED drive mode** to **Bi-color** • Sets **Format to nibble array** to **ON** • Sets **Casi 1-wire F2F** to **ON** • Sets **Supervised** to **ON**
Supervised F2F with inputs	• Sets **Keypad mode** to **None** • Sets **LED drive mode** to **Bi-color**

Function	Description
	• Sets **Format to nibble array** to **ON** • Sets **Casi 1-wire F2F** to **ON** • Sets **Supervised** to **ON** • Sets **Inputs come from reader** to **ON**
Custom	Lets the user set any Keypad mode, LED drive mode, or other settings depending on reader hardware.
Keypad mode[1]	
None	No specific mode is active.
MR20	MR20 8-bit keypad format with tamper support.
HID	HID 4-bit keypad format.
Indala	Eight-bit Motorola/Indala format consisting of a 4-bit code and the same code inverted.
MR20 no tamper	MR20 8-bit keypad format without tamper support.
4-bit, 60 second keep alive	4-bit keypad format with HID I'm Alive support set to a 60-second interval.
8-bit, 60 second keep alive	8-bit keypad format with HID I'm Alive support set to a 60-second interval.
4-bit, 10 second keep alive	4-bit keypad format with HID I'm Alive support set to a 10-second interval.
8-bit, 10 second keep alive	8-bit keypad format with HID I'm Alive support set to a 60-second interval.
LED drive mode	
Bi-color	Generic 1-wire, tri-state bi-color driver circuit.
2-wire	Separate red and green driver with no buzzer.
Dorado-780	Two-wire driver with color conversion.
LCD	Enables the LCD display driver on LCD-equipped readers.
Bioscrypt	Enables the Bioscrypt interface.
OSDP	Mirrors Wiegand LED and buzzer behavior on OSDP readers.
SNET	Enables SNET on Honeywell controllers.
Custom OSDP	Lets the user set custom OSDP settings.
Other controls	
Wiegand pulses	Enables Data 1/Data 0 Wiegand pulses.
Trim zero bits	Removes leading zeros.

Function	Description
Format to nibble array	Used for magstripe purposes.
Allow bi-directional Mag decode	Sends decoded data no matter which direction card is swiped.
Allow Northern Mag decode	Decodes 32-bit Wiegand data from certain Northern cards.
Casi 1-wire F2F	In the Casi 1-wire F2F communication type, uses one wire for communication instead of two.
Supervised	Enables supervision. Only used with F2F flag.
Inputs come from reader	Sets inputs to come from the reader. Only used with F2F flag.

[1] Mercury does not support keypad readers outputting PIN in 26-bit Wiegand mode (HID mode-14).

Preparing to enroll the Mercury controller

Before you enroll the Mercury controller on the Synergis™ unit, you must assign a static IP address to the controller.

Before you begin

Make sure you have the following:

- **Mercury Setup and Configuration Guide:** Instruction manual for connecting to the web portal of your Mercury controller and setting up its IP address (and other configurations).
- **Static IP address:** Static IP address assigned to the controller by your IT department.
- **Physical addresses:** Each interface panel attached to the same RS-485 port of the same Mercury controller must have a unique physical address (configured on a DIP switch).

BEST PRACTICE: If you have many Mercury controllers to enroll on the same Synergis unit, it is best to enroll them all at the same time. Each controller you add or remove from the Synergis unit causes the unit to restart. While the unit restarts, it's offline for about 30 seconds.

What you should know

Mercury controllers enrolled on the same Synergis unit cannot be assigned different partitions in Security Center. If you need to assign the controllers to different partitions, enroll them on different Synergis units, and then assign the Synergis units to different partitions.

NOTE: The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

Procedure

1 On the Mercury controller board, set the DIP switch *S1-1* to **ON**.

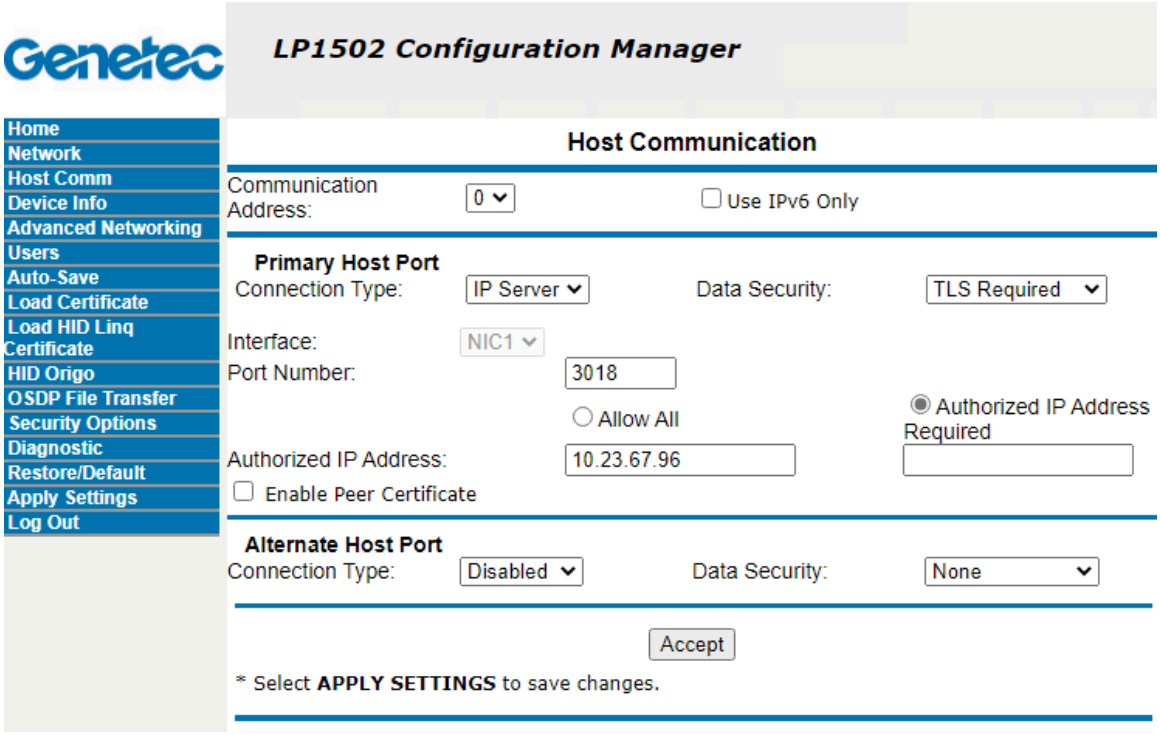
This gives you a five-minute window to sign in using factory default settings.

2 Sign in to the Mercury controller through its *Configuration Manager* web page. Use the default IP address (192.168.0.251) and credentials (admin/password). For more information, see the manufacturer's documentation.

3 Select **Network** from the menu, configure the Mercury controller's **IP address**, and click **Accept**.

4 Select **Host Comm** from the menu.

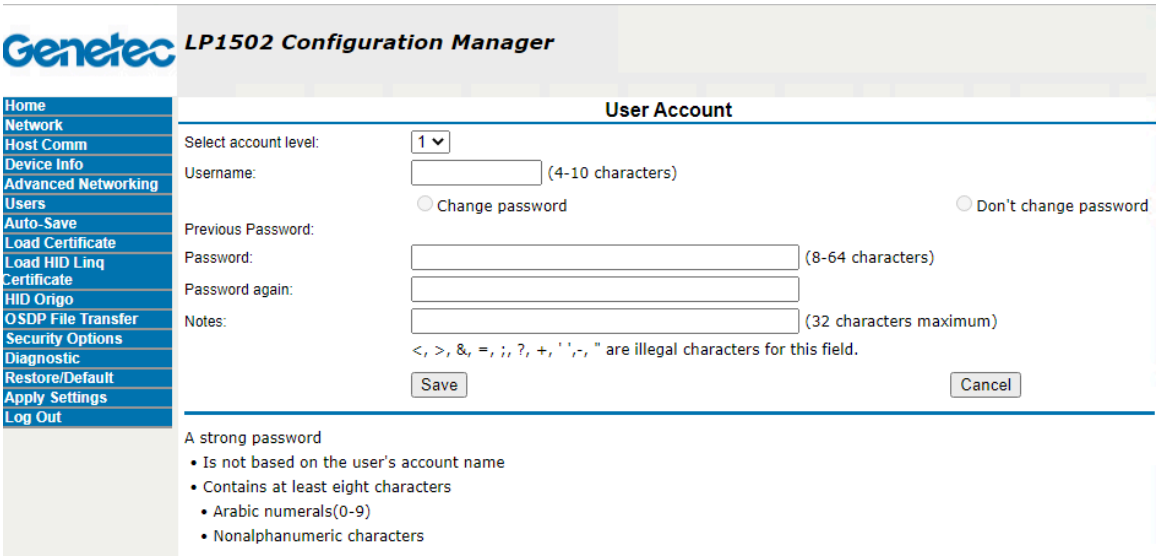
5 In the *Host Communication* page, configure the following settings, and click **Accept**.



- **Communication Address:** Set to **0**.
  IMPORTANT: Not to be confused with the **Channel** that must be unique when you enroll the Mercury controller on the Synergis unit.
- **Port Number:** The port number used by the Synergis unit to communicate with the Mercury controller (default=3001).
- **Authorized IP Address Required:** (*Hardening*) Select this option, and set **Authorized IP address** to the IP address of the Synergis unit.
- **Data Security:** Set to **TLS Required**.
  IMPORTANT: If TLS is not selected, the Mercury controller stays offline.

6 Select **Users** from the menu, and click **New User**.

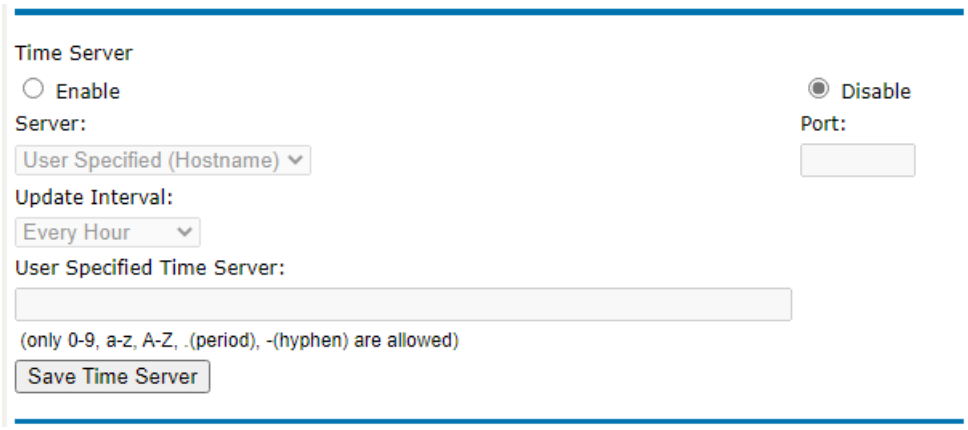
Creating a user account on the Mercury controller saves you from having to physically access the unit and set the DIP switch *S1-1* to **ON** the next time you modify the controller configuration.



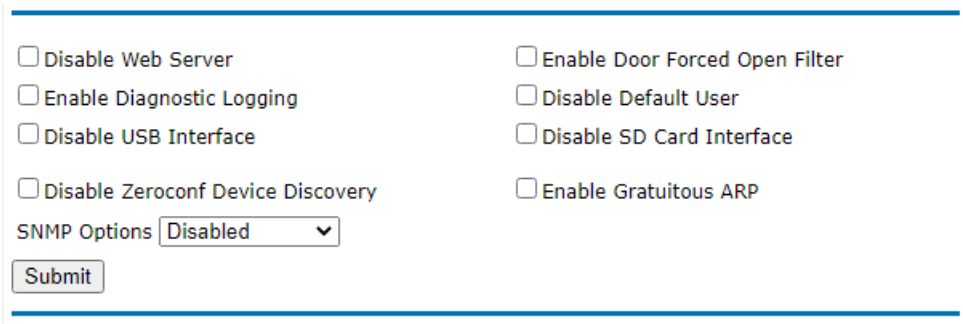
7 (*Hardening*) On the *User Account* page, enter the **Username** and a strong **Password**, confirm the password, and then click **Save**.

8 On the *Users* page, disable **Time Server**.

The Time Server is not required. Synergis™ Softwire monitors and automatically sets the time on the Mercury units.



9 (*Hardening*) On the *Users* page, disable **SNMP Options**, and click **Submit**.



10 Select **Apply Settings** and click **Apply Settings, Reboot**.

11 On the Mercury controller board, set the DIP switch *S1-1* to **OFF** for normal operation.
This prevents the factory default settings from being used to sign in to the controller.

12 When prompted to proceed, select **I understand and wish to proceed**, and then click **Yes**.

After you finish

Enroll the Mercury controller on the Synergis unit.

Enrolling Mercury controllers on the Synergis unit

To have the Synergis™ unit communicate with the Mercury controllers connected to it, you must enroll them using Security Center Config Tool.

Before you begin

Prepare the Mercury controller for enrollment.

What you should know

Mercury controllers enrolled on a Synergis™ unit are not visible from the Synergis™ Appliance Portal *Hardware* page.

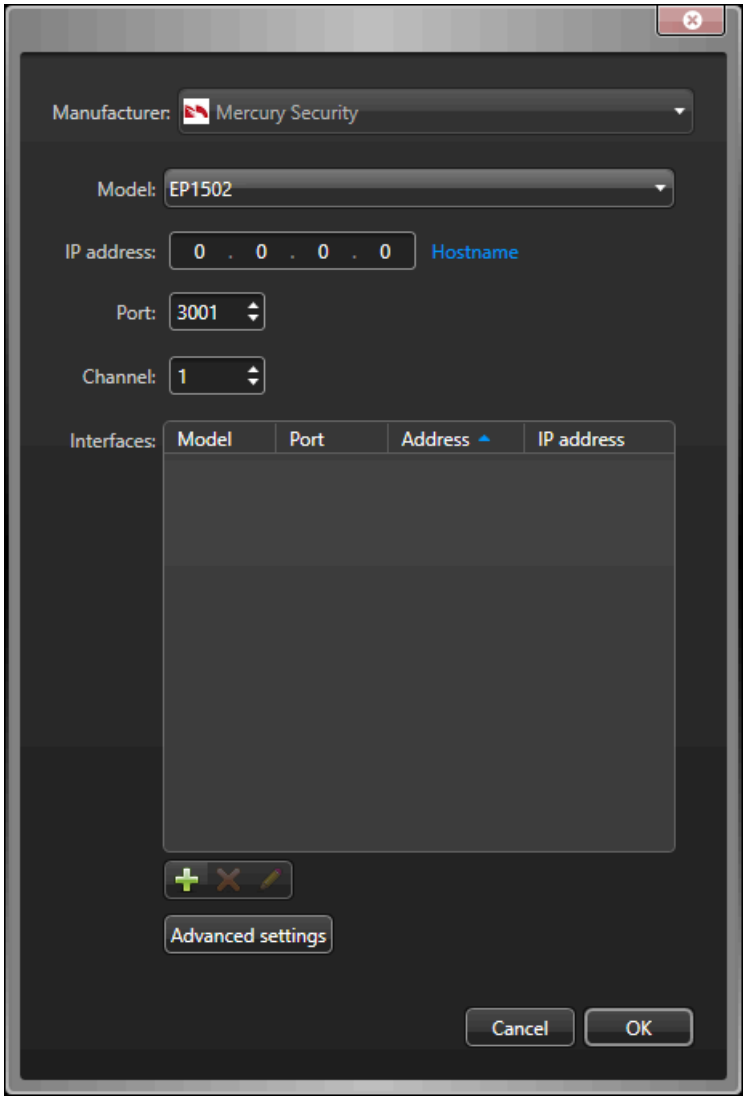
On the Synergis unit, each Mercury controller must be assigned a unique channel ID. All Mercury controllers have RS-485 buses to which the interface panels (MR50, MR52, MR16IN, and MR16OUT) are connected. Each interface panel connected to the same RS-485 or Ethernet bus must have a unique physical address.

Procedure

1 From the Config Tool homepage, open the *Access control* task.

2 Click **Roles and units**, and then click the Synergis unit.

3 Click **Peripherals**, and then click **Add an item** (+).



4 Enter the following information:

- **Model:** Model of the controller.
- **IP address:** Static IP address assigned to the controller by your IT department.
- **Hostname:** Click the blue link to identify the controller by its hostname. This option is only available if you're running Security Center 5.12.0.0 or later.

  NOTE: When enrolling a Mercury controller with its hostname, you must append the hostname with `.local` if the controller is not registered to DHCP and DNS on the network.
- **Port:** Communication port. The default value is 3001. The port must match the value configured on the Mercury Device Manager web page.
- **Channel:** Channel ID corresponding to this controller. The channel ID can be any value 0 - 63, and must be unique within the Synergis unit. After it's assigned, it must not be changed.

5 If the selected controller model supports downstream panels, add them.

NOTE: Consider the following:

- For MR51e PoE panels, add them after enrolling the controller.
- For EP1501, LP1501, and MP1501 controllers, do not to exceed the limit of eight downstream panels per controller, as recommended by Mercury.
- The M5-20IN panel occupies two consecutive addresses on the communication bus. To have the 20 inputs of the M5-20IN panel, you must add two M5-20IN panels in Config Tool to your M5-IC controller. The address of the first panel must match the physical address on the M5-20IN panel, and the address of the second panel must be set to the address of the first panel plus one.
- MR62e units can have an IPv6 address, but cannot communicate with Mercury controllers through IPv6.

a) Under the *Interfaces* list, click **Add an item** ( ).

b) In the dialog box that opens, select the downstream panel's **Model**, the **Port**, the **Address** (0 - 31), and when applicable, the IP address.

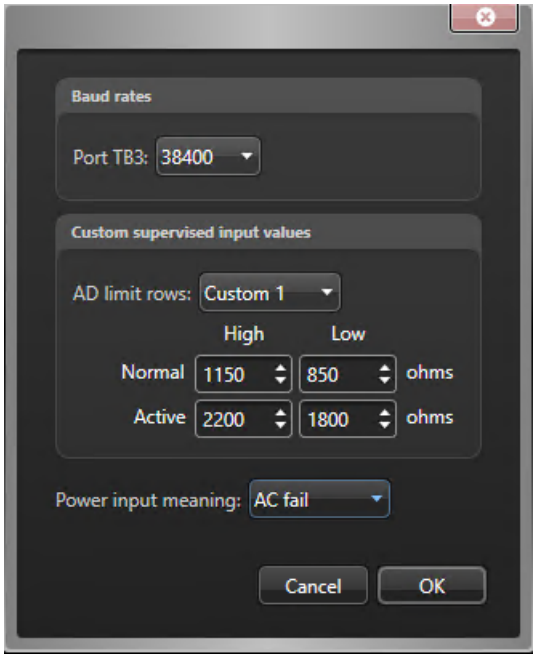
All panels connected to the same port must use a different address.

c) Click **OK**.

d) Repeat as necessary.

6 (Optional) Click **Advanced settings** to change the advanced settings.

The available settings depend on the selected controller model. You can typically change the baud rate of the available serial port, the custom supervised input values, and the power input event configuration.

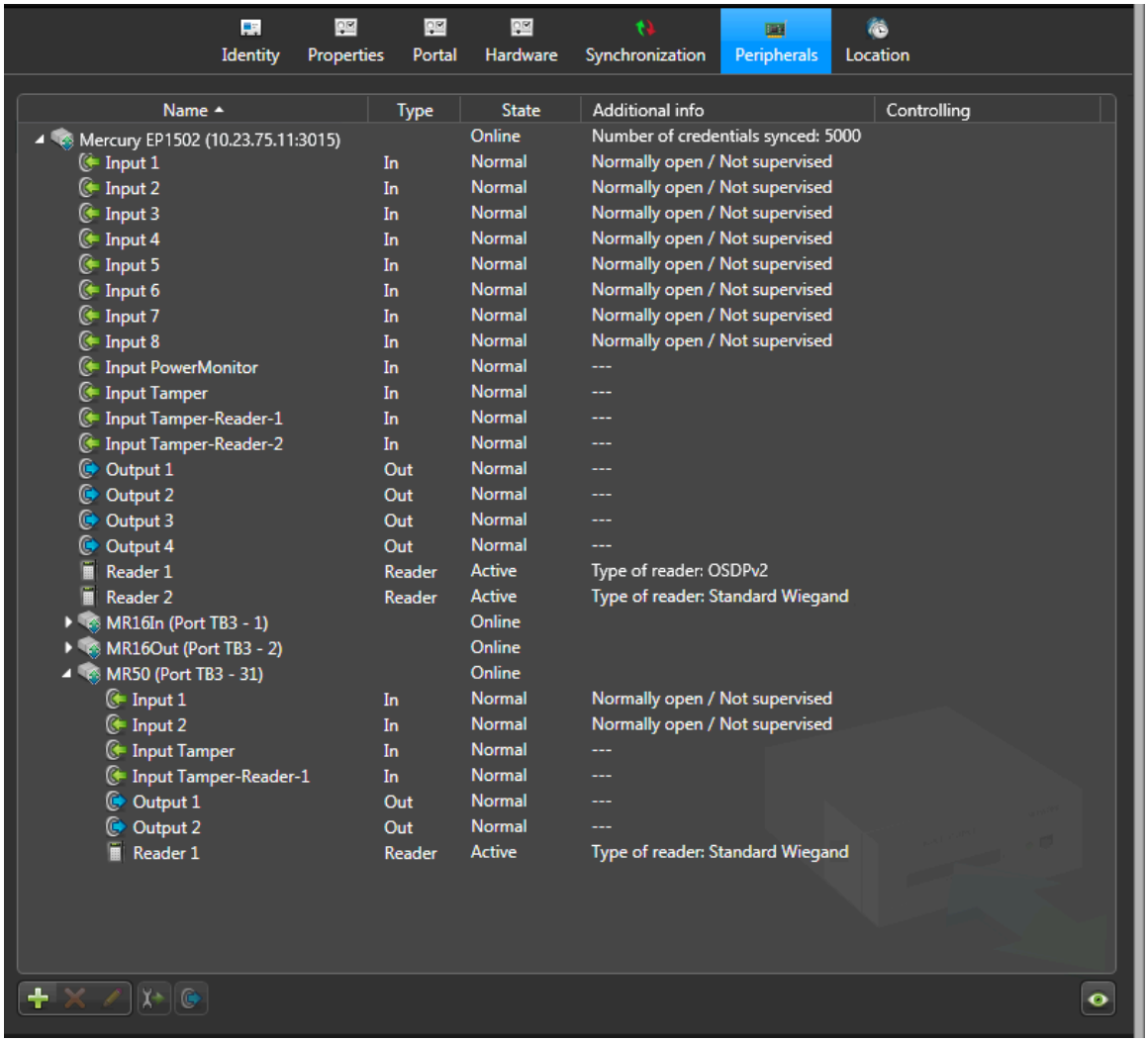


NOTE: You can set up to four different custom presets on your Mercury controller's inputs. For users upgrading from earlier Security Center versions who have a custom value configured, that preset is listed as **Custom 1** in the **AD limit rows** list.

7 Click **OK** at the bottom of the dialog box.

8 Click **Apply**.

The Mercury controller with all its connected downstream panels and peripheral devices are displayed on the *Peripherals* page.



Adding interface modules to the Synergis unit causes the unit to perform a software restart. During this process, the Synergis unit and all peripherals attached to it appear offline (in red).

9 Select each of the discovered I/O devices and readers, and configure their properties as necessary.

For OSDP (Secure Channel) readers, see Adding OSDP (Secure Channel) readers to a Mercury controller on page 165.

10 Test your wiring and configuration by triggering the inputs and outputs.

The triggered I/O changes state in real time on screen.

NOTE: Reader activities are not shown on the *Peripherals* page.

After you finish

If applicable, add the MR51e panels to the Mercury controller, and then map the physical wiring of the interface modules to the doors and zones in Security Center.

Configuring Mercury controller settings in the Synergis Appliance Portal

You can configure the settings for your Mercury controllers in the Synergis™ Appliance Portal.

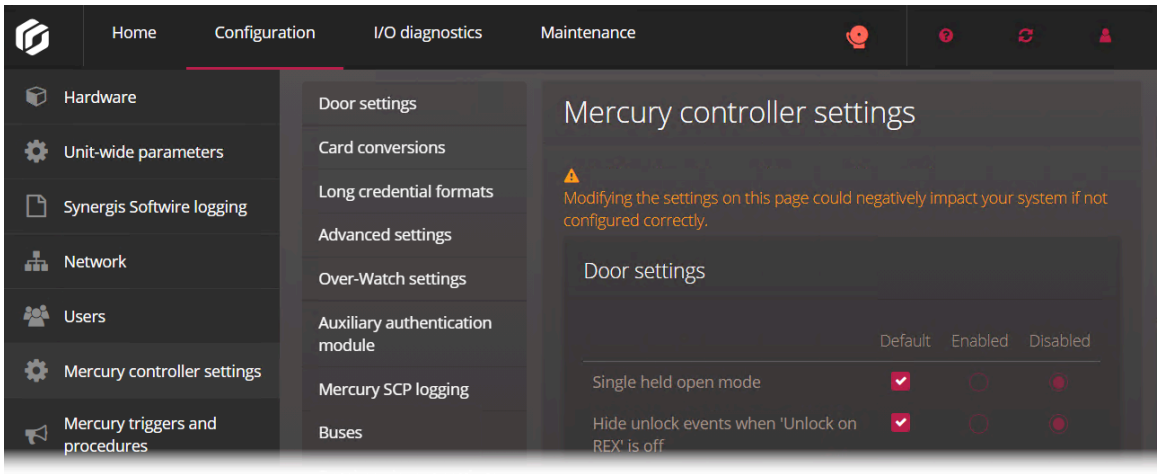
What you should know

All hardware assigned to a door or an elevator must be controlled by the same Mercury controller under the same Synergis™ Cloud Link unit for it to work when the Synergis Cloud Link unit is offline.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury controller settings**.



3 Click the **Door settings** tab from the side menu, and enable the following settings as required:

- **Single held open mode:** Ignore subsequent *Door open too long* events after the first event is generated, as long as the door remains open.

  Perform a software restart if you change this setting.
- **Hide unlock events when 'Unlock on REX' is off:** The Mercury controller sends unlock events on REX activations regardless of whether or not it actually unlocks the door. Enable this setting to hide these unlock events. Enabling this setting causes a delay on all events received so that false unlock events can be filtered out.

  Perform a software restart if you change this setting.
- **Disable host decision handoff (offline mode):** By default, this setting is disabled, meaning that Mercury host decision handoff is enabled, and that the Synergis Cloud Link unit makes the access control decisions. When this setting is enabled, Mercury host decision handoff is disabled, meaning that the Mercury controllers make their own decisions as though they are disconnected from the Synergis Cloud Link unit. In this case, some advanced features and cards that are not yet synchronized to the Mercury controller do not work, however, the door becomes much more responsive.

  BEST PRACTICE: Leave the **Disable host decision handoff (offline mode)** setting disabled, unless there is a bad network connection between the Synergis Cloud Link unit and the Mercury controllers.

For more information, see Differences between having Mercury host decision handoff enabled and disabled on page 149.

- **Silent access granted:** Readers do not beep when access is granted.
- **Silent access denied:** Readers do not beep when access is denied.
- **Inhibit 'Door forced' open event:** *Door forced open* events are disabled.

  Perform a software restart if you change this setting.
- **Inhibit 'Motor Fault' events from Schlage locks:** *Motor Fault* events from Schlage locks are disabled.

  NOTE: This setting does not affect *Motor Fault* events from other devices.

  Perform a software restart if you change this setting.
- **Inhibit 'RF loss' events from Schlage locks:** *RF loss* events from Schlage locks are disabled.

  NOTE: This setting does not affect *RF loss* events from other devices.

  Perform a software restart if you change this setting.
- **Reader LED off when locked:** Reader LEDs on OSDP readers are turned off if the associated door is in a normal lock state.
- **Mercury native area control:** Enables Mercury's native antipassback, max occupancy, and interlock features on the Mercury controller. For more information, see Mercury native area control limitations on page 151.

  Perform a software restart if you change this setting.
- **Extended grant time REX mode:** Doors remain unlocked for as long as the REX input is active and for the normal grant time afterward. If no door sensor is present, the door remains unlocked either for as long as the REX input is active or for the normal grant time, whichever period is longer.

  This is useful for preventing doors that are controlled by a motion sensor from locking and unlocking every few seconds. This feature requires Mercury firmware 1.29.1 or later.

  NOTE: You can also configure this setting on a per door basis.
- **Live 'Request to exit' events:** Changes the way that Synergis™ Softwire processes *Request to exit* events from Mercury LP and MP controllers, so that the timestamps on the events are accurately reported. This setting is enabled by default.
- **Program door alarm LED procedures:** Causes the readers associated with Mercury controllers to follow Synergis Softwire LED and buzzer patterns instead of Mercury LED and buzzer patterns for door alarms.

  NOTE: If this setting is disabled, when *Door forced open* and *Door open too long* events are generated, the LEDs on the associated readers do not flash.

  Perform a software restart and then reset the Mercury controllers if you change this setting.
- **Receive duress events when duress is disabled:** Causes the *Access denied: Invalid PIN* and *Duress PIN entered* events to both be generated in Security Center if someone enters a duress PIN when the **Duress PIN** setting in Config Tool is disabled.

4 Click the **Card conversions** tab from the side menu, and enable the following card conversions as required:

Perform a software restart if you change any of these settings.

- **Casi M5 56 -> 40**
- **Ambiguous HID 1441 -> 56**
- **Lossy conversion for credentials longer than 52 bits:** Fixes a bug in versions of Synergis Softwire earlier than 10.10, where credentials from 52 bits to 64 bits might have issues.
- **200 bits FASC-N to 128 bits:** All cards report the 128-bit version. This setting is used with FICAM or Long credential database layouts.
- **Add F2F to Wiegand translator:** Add or configure other translators.

5 Click the **Long credential formats** tab from the side menu, and configure the following setting:

- **Wiegand format length (bits):** Long credential formats for Mercury controllers are not automatically configured in Security Center. Manually set the format by entering a value from 64 to 240, and then clicking **Add**. This setting is used with FICAM or Long credential database layouts.

Perform a software restart if you change this setting.

6 Click the **Advanced settings** tab from the side menu, and enable the following settings as required:

Perform a software restart if you change any of these settings.

- **SIO Encryption Control:** Enables encryption on the RS-485 between EP or Honeywell controllers and their downstream SIO boards, or LP controllers and older SIO boards. LP controllers with S3 SIO boards use encryption on the channel regardless of this setting.

  BEST PRACTICE:

  - Limit bulk upgrades to 10 SIO boards under a single EP controller.
  - Before upgrading multiple SIO boards, disable the **SIO Encryption Control** setting.

- **Two OSDP readers per reader port:** Enables LP1502, LP4502, MP1502, MP4502, MR50-S3, and MR52-S3 units to support two OSDP readers per port.

  - For LP1502, LP4502, MR50-S3, and MR52-S3, this requires Security Center 5.10.4.0 or later.
  - For MP1502, MP4502, this requires Security Center 5.12.1.0 or later.

- **Magstripe support:** This setting is enabled by default, and allows support for up to eight Wiegand card formats per Mercury controller. For each of the eight Wiegand card formats, corresponding magstripe card formats are automatically created. When the setting is disabled, each Mercury controller can support up to 16 Wiegand card formats, and no corresponding magstripe card formats are automatically created.

7 Click the **Over-Watch settings** tab from the side menu, and select the **LP4502 Over-Watch plugin** setting to enable the Over-Watch plugin on all the LP4502 controllers under the Synergis Cloud Link unit. The Over-Watch plugin is only required for the BEST Wi-Q integration through Mercury.

For more information, see Configuring the Over-Watch plugin for the BEST Wi-Q integration on page 192.

8 Click the **Auxiliary authentication module** tab from the side menu, and select **Disabled**, **PivClass**, or **TIEntryPoint**.

This setting is used with FICAM database layout and the appropriate plugin for the LP4502 controller.

9 Click the **Mercury SCP logging** tab from the side menu, and click **Start logging** for more Mercury-specific logging, and enter the number of days after which you want the logging to end.

10 Click the **Buses** tab from the side menu, and click **Reset** for each controller or **Reset all** to ensure that new settings are pushed to all the controllers.

11 Click the **Database layout settings** tab from the side menu, and configure the following settings:

a) Select a database layout from the list.

The **Feature rich (default)** layout fits most use cases. The other database layouts address specific needs. Reset the controllers after changing the database layout.

For more information about what each database layout supports, see Database layouts for Mercury controllers on page 153.

b) Configure the maximum PIN length.

Default maximum PIN length is selected by default. The default value for all database layouts is **6**. To change this value, select **Custom maximum PIN length**, and then enter the new value in the **Maximum PIN length** field.

NOTE: Setting the **Maximum PIN length** to a number higher than what the selected database layout supports causes your Mercury controllers to stop functioning, and PINs longer than the configured **Maximum PIN length** do not work. For more information, see Configuring Mercury controllers to not require entering # after PINs on page 158.

Perform a software restart if you change this setting.

12 Click the **PIN settings** tab from the side menu, and configure the following settings:

- **Include and add leading zeros for PINs:** To use zeros before your PINs, select **Custom**, and enter a value for **PIN length after adding leading zeros**. For more information, see Configuring PINs with leading zeros for Mercury controllers on page 157.

Perform a software restart if you change this setting.

13 Click the **OSDP-reader-specific settings** tab from the side menu, and configure the following settings:

- **Nexus and Veridt OSDP LED correction:** Fixes an LED issue that occurs in certain Nexus and Veridt OSDP readers.
- **Override LED programming:** Fixes an issue on OSDP readers where the LED turns off for a few seconds when the door re-locks after being opened.

14 Click the **Visitor escort rule and two-person rule** tab from the side menu, and configure the following setting:

- **Maximum delay between card presentations:** Applies to all the doors controlled by the Mercury controllers.

  Perform a software restart and then reset the Mercury controllers if you change this setting.

15 Click the **Door behavior for offline SIO boards** tab from the side menu, and select one of the following:

This setting only applies to doors that have their reader and lock on the same Mercury SIO board. Readerless doors are not affected. When the door unlocks due to this setting, the reader LED behavior does not follow door lock states.

IMPORTANT: Any events that occur while in the SIO board is not connected to the Mercury controller are not recorded.

- **Default (locked):** When the SIO board loses connection with the Mercury controller, the doors it controls become locked, regardless of the state that the doors were in before the connection was lost.
- **Unlocked:** When the SIO board loses connection with the Mercury controller, the doors it controls become unlocked, regardless of the state that the doors were in before the connection was lost.
- **Locked:** When the SIO board loses connection with the Mercury controller, the doors it controls become locked, regardless of the state that the doors were in before the connection was lost.
- **Facility code:** When the SIO board loses connection with the Mercury controller, only credentials with the configured card formats and facility codes can still access the doors. If no card formats or facility codes are configured, the doors that the SIO board controls become locked, regardless of the state that the doors were in before the connection was lost.

  For more information, see Configuring offline Mercury SIO boards to grant access through facility codes on page 160.

  Perform a software restart if you select the **Facility code** setting.

16 To reset all settings to default, except for the database layout settings, click **Reset to default**.

IMPORTANT: There is no way to recover the previous settings.

17 Click **Save**.

Differences between having Mercury host decision handoff enabled and disabled

Your access control system behaves differently depending on whether the Mercury host decision handoff feature is enabled or disabled.

You can enable or disable Mercury host decision handoff from the Synergis™ Appliance Portal. Navigate to **Configuration** > **Mercury controller settings** > **Door settings**, and then configure the **Disable host decision handoff (offline mode)** setting. By default, this setting is disabled, meaning that Mercury host decision handoff is enabled, and that the Synergis™ Cloud Link unit makes the access control decisions.

Refer to the following table to know when your access control system behaves differently, depending on whether Mercury host decision handoff is enabled or disabled.

	Host decision handoff enabled (default)	Host decision handoff disabled
Access control decisions made by	Synergis Cloud Link	Mercury controller

	Host decision handoff enabled (default)	Host decision handoff disabled
Card read to door unlock time	0 to 5[1] seconds	Under 1 second
Deleting a cardholder or credential in Security Center • Versions earlier than 5.11.3.5 • 5.12.0.0	Fast	Up to 1 hour for changes to propagate
Deleting a cardholder or credential in Security Center • 5.11.3.6 or later • 5.12.1.0 or later	No difference in behavior	
Deactivating a cardholder or credential manually or automatically through its expiration date	No difference in behavior	
Revoking access by removing a cardholder from a cardholder group or access rule, changing schedules, and so on **NOTE:** Revoking access by deleting or deactivating a cardholder not included.	Fast	Up to 1 hour for changes to propagate
Interlock, antipassback, and max occupancy	Supported	The **Mercury native area control** option must be enabled.

[1] It can take up to 5 seconds, depending on the network conditions.

Enabling long credential support on Mercury controllers

Before you can use credentials of up to 240 bits with your Mercury controllers, you must enable support for long credentials on your Synergis™ Cloud Link unit.

Before you begin

Ensure the following:

- Your Synergis Cloud Link is running Synergis™ Softwire 11.0 or later, and that it is online and connected to your network.
- The Mercury controllers that you want to use long credential support with are running firmware version 1.29.1 or later.

What you should know

Because credentials of 64 bits or longer are not automatically synchronized with Mercury, you must manually enable them.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury controller settings**.

3 Click the **Database layout settings** tab from the side menu, and then select the **Long credentials** database layout from the list.

4 Click the **Long credential formats** tab from the side menu, and then enter the credential length you want to use.

The value must be from 64 to 240.

5 Click **Add**.

You can add up to eight different credential formats.

6 Click **Save**.

7 Perform a software restart:

a) In the top menu, click **Restart** > **Software restart**.

8 After the software restart, log back on to the Synergis Cloud Link unit.

9 On the *Mercury controller settings* page, click the **Buses** tab from the side menu.

10 Click **Reset** for the controllers that require long credential support.

The new credential formats that you enabled can be used with your Mercury controllers.

Mercury native area control limitations

The Mercury native area control, which includes interlock, max occupancy, and antipassback, has some limitations.

- **Soft antipassback:** The *Antipassback violation* event for soft antipassback is generated when the door opens instead of when access is granted.

  If you configure soft antipassback on a door without a door sensor, *Antipassback violation* events are never generated because the door never opens.

  Soft antipassback on Mercury does not support a presence timeout.
- **Hard antipassback:** Mercury does not support the following:
  - Hard antipassback that is not also set to **Strict**.
  - Strict and hard antipassback when the **Activate global antipassback** setting is enabled on the Access Manager role in Config Tool.
- **Antipassback timeout:** Mercury supports a timeout on hard and strict antipassback. If **Presence timeout** is configured on an area, hard antipassback denies access to a cardholder until the timeout elapses, after which the cardholder can be granted access to the area again.

  This triggers an *Antipassback violation* event for soft antipassback, and then hard antipassback re-applies to the cardholder until the timer elapses again. This configuration is not compatible with areas controlled by Synergis™ Softwire.
- **Mercury's one-to-one model for cardholders and credentials:** If a cardholder in Security Center has multiple card credentials, each credential is considered belonging to a separate cardholder at the Mercury level.

  This means that each credential can be used to enter the same area once without causing an antipassback violation. Similarly, if the cardholder uses two different credentials to enter an antipassback area with max occupancy, that cardholder is counted as two people in the max occupancy count.
- **Bypass antipassback:** No *Antipassback violation* events are generated by cardholders that have the **Bypass antipassback rules** option enabled.
- **Interlock and antipassback:** Interlock and antipassback only work if all doors configured in the area using these features are controlled by the same Mercury controller.

  A Mercury controller can have doors in many areas with any combination of these features, or none of them. In areas where you are not using these features, you can have doors controlled by multiple Mercury controllers.

A Mercury controlled door can only be used as the entrance and exit of one area using either interlock or antipassback, even though in Security Center, you can configure multiple areas for the same door.

- **Interlock:** If only part of the interlock is offline due to failure of a single SIO board, the interlock prevents other doors in the interlock area from being unlocked or opened.

  When native interlock is enabled, the **Override** and **Lockdown** options in Config Tool are not supported. The options can be configured, but will not change anything.
- **Scheduled antipassback:** Scheduled antipassback is not supported at the Mercury level. Synergis Softwire will enable and disable antipassback on schedule as long as the Mercury controllers are connected or when they reconnect, and the schedule is not set to *Always*. Mercury does not transition on the schedule itself, so it remains in its state at the time of the disconnect.
- **People counting discrepancies:** Because Mercury tracks its own areas, the people count might not always match on the Synergis™ Cloud Link, in the Security Desk *People counting* task, and on the Mercury controller. To prevent these discrepancies from causing issues, it is recommended that you regularly reset the people count by doing the following:
  - In the Synergis™ Appliance Portal, navigate to **Configuration** > **Unit-wide parameters** > **Area configuration**, and then schedule a daily or weekly reset.
    This resets the people count on the Synergis Cloud Link and on the Mercury controllers it manages.
  - In Config Tool, reset the count in the *People counting* task, using the *Reset area people count* action in scheduled tasks or event-to actions for each area you want cleared.

Configuring Mercury Extended grant time REX mode per door

Before you can enable the Extended grant time REX mode on specific doors, you must create a door custom field in Security Center.

What you should know

- This feature requires Mercury firmware 1.29.1 or later.
- When the Extended grant time REX mode is enabled, the door remains unlocked for as long as the REX input is active and for the normal grant time afterward. This is useful for preventing doors controlled by a motion sensor from locking and unlocking every few seconds.
- Note the following limitations of this feature:
  - If the Mercury controller restarts, the door goes back to its normal state until the REX is triggered again.
  - If no door sensor is present, the door remains unlocked either for as long as the REX input is active or for the normal grant time, whichever period is longer.
  - The door locks at the end of an unlock schedule regardless of the REX state.
- If you want to control all Mercury-controlled doors under the same Synergis™ Cloud Link at the same time, you can configure the **Extended grant time REX mode** setting in the Synergis™ Appliance Portal instead.

  NOTE: If you create the custom field in Security Center, the setting on Synergis Cloud Link units enrolled on that system are ignored.

Procedure

1 From the Config Tool homepage, open the *System* task, and click the **General settings** view.

2 Click the **Custom fields** tab, and then click **Add an item** ().

3 In the *Add custom field* dialog box, configure the following values:

- **Entity type:** Select **Door**.
- **Data type:** Select **Boolean**.
- **Name:** Enter `Extended grant time REX mode`.
- **Default value:** Select this option if you want doors to be in Extended grant time REX mode by default.

4 Click **Save and close**, and then click **Apply**.

Database layouts for Mercury controllers

Different database layouts are available to select for your Mercury controllers.

Refer to the following tables to know which database layout fits your needs.

Feature rich database layout (default)

Model	Maximum number of cardholders
EP1501, EP1502	145,000
EP2500	370,000

Model	Maximum number of cardholders
M5-IC, MS-ICS	370,000
EP4502	419,000
LP1501, LP1502	200,000
LP2500	419,000
LP4502	500,000
MP1501, MP1502	200,000
MP2500	419,000
MP4502	500,000

Feature support	Supported
Default PIN length	6
Maximum PIN length	10
Native area control (antipassback, interlock, and maximum occupancy)	Yes
Two-person rule and visitor escort	Yes
Maximum credential length (bits)	64
Elevators	Yes

Long credential database layout

Model	Maximum number of cardholders
EP1501, EP1502	80,000
EP2500	210,000
M5-IC, MS-ICS	214,000
EP4502	210,000
LP1501, LP1502	111,000
LP2500	222,000
LP4502	444,000
MP1501, MP1502	111,000
MP2500	222,000
MP4502	444,000

Feature support	Supported
Default PIN length	6
Maximum PIN length	10
Native area control (antipassback, interlock, and maximum occupancy)	Yes
Two-person rule and visitor escort	Yes
Maximum credential length (bits)	240
Elevators	Yes

Long PINs database layout

Model	Maximum number of cardholders
EP1501, EP1502	80,000
EP2500	300,000
M5-IC, MS-ICS	300,000
EP4502	300,000
LP1501, LP1502	150,000
LP2500	350,000
LP4502	500,000
MP1501, MP1502	150,000
MP2500	350,000
MP4502	500,000

Feature support	Supported
Default PIN length	15
Maximum PIN length	15
Native area control (antipassback, interlock, and maximum occupancy)	Yes
Two-person rule and visitor escort	Yes
Maximum credential length (bits)	64
Elevators	Yes

Large scale database layout

Model	Maximum number of cardholders
EP1501, EP1502	250,000
EP2500	560,000
M5-IC, MS-ICS	560,000
EP4502	600,000
LP1501, LP1502	250,000
LP2500	600,000
LP4502	600,000
MP1501, MP1502	250,000
MP2500	600,000
MP4502	600,000

Feature support	Supported
Default PIN length	6
Maximum PIN length	6
Native area control (antipassback, interlock, and maximum occupancy)	No
Two-person rule and visitor escort	No
Maximum credential length (bits)	64
Elevators	No

FICAM database layout

The FICAM database layout should only be used if you want to conform with the US government's Federal Information Processing Standard 201 (FIPS 201) through Personal Identity Verification (PIV), Personal Identity Verification-Interoperable (PIV-I), or Commercial Identity Verification (CIV) credentials. This database layout is only intended to be used with Mercury LP4502 controllers.

For more information, see the HID pivCLASS User Guide for Security Center or the Using TI EntryPoint Authentication on Mercury LP4502 Technote.

Model	Maximum number of cardholders
EP1501, EP1502	98,000
EP2500	180,000
M5-IC, MS-ICS	100,000

Model	Maximum number of cardholders
EP4502	180,000
LP1501, LP1502	139,000
LP2500	279,000
LP4502	500,000

Feature support	Supported
Default PIN length	6
Maximum PIN length	6
Native area control (antipassback, interlock, and maximum occupancy)	Online
Two-person rule and visitor escort	Yes
Maximum credential length (bits)	240
Elevators	Yes

Configuring PINs with leading zeros for Mercury controllers

By default, Mercury doesn't support PIN credentials that start with zero. To use PINs that start with zero, you must configure the Mercury controller settings in the Synergis™ Appliance Portal.

What you should know

Using PIN credentials in the Mercury integration requires the following:

- Each cardholder in Security Center must have a card credential and only one PIN credential.
- On the *Unit-wide parameters* page of the Synergis Appliance Portal, if the reader is set to **Card or PIN**, but the cardholder only has a PIN credential, that credential isn't synchronized to the Mercury controller and doesn't work. As a workaround, create and assign the cardholder a dummy card credential.

Mercury controller settings in the Synergis Appliance Portal affect each other in the following ways:

- The system prevents you from configuring a **PIN length after adding leading zeros** value that exceeds the **Maximum PIN length** value.
- Leading zeros are added to shorter PINs until they reach the **PIN length after adding leading zeros** value, not the **Maximum PIN length** value.
- PINs that are already equal to or longer than the **PIN length after adding leading zeros** value are valid, as long as they don't exceed the **Maximum PIN length** value.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury controller settings**.

3 Under the **Include and add leading zeros for PINs** setting, select **Custom**.

By default, this setting is configured to **Unset**, and PINs don't have leading zeros.

4 Under the **PIN length after adding leading zeros**, enter a value.

This setting indicates the total number of digits in a PIN, including zeros added before the PIN. Zeros are only added before the PIN if the original PIN is shorter than this setting's value.

5 Click **Save**.

6 Perform a software restart.

Example

The **Maximum PIN length** is set to 6, and the **PIN length after adding leading zeros** is set to 4. The following occurs:

- If the original PIN was 9, the PIN becomes 0009.
- If the original PIN was 123, the PIN becomes 0123.
- If the original PIN was 12345, then the PIN remains the same.

Configuring Mercury controllers to not require entering # after PINs

If your PIN is shorter than the maximum PIN length configured on the *Mercury controller settings* page of the Synergis™ Appliance Portal, you must press the # key after entering your PIN. To eliminate having to press the # key, you can change the maximum PIN length to match the PIN length that's most used in your system.

What you should know

The default maximum PIN length for most of the Mercury database layouts is six digits, except for the Long PINs layout, which is fifteen digits.

IMPORTANT: Before reducing the maximum PIN length, consider the following:

- PINs longer than the configured maximum PIN length don't work. Be sure to shorten any longer PINs to match the new maximum PIN length.
- Duress PINs must be at least four digits long.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury controller settings**.

3 From the side menu, click the **Database layout settings** tab.

4 Select the **Custom maximum PIN length** option, and then enter the new value in the **Maximum PIN length** field.

Example: If you mostly have four-digit PINs in your system, set the value to 4. Anyone with a four-digit PIN will no longer be required to press the # key after entering their PIN. Anyone with a PIN shorter than four digits will still be required to press the # key.

5 Click **Save**.

The *Reset* dialog box opens with the following message: Applying these changes resets all Mercury controllers and might cause significant downtime for the connected doors.

6 Click **OK**.

7 Perform a software restart.

About granting access through facility codes with offline Mercury SIO boards

Learn about how access decisions are affected when you configure access to only be granted to credentials with specific card formats and facility codes when the SIO board loses connection with the Mercury controller.

- By default, Synergis Softwire supports up to eight card formats per Mercury controller. Each facility code that you add counts as one card format, even if the facility codes are configured for the same card format.

  NOTE: To increase the number of supported card formats to 16, you can disable the **Magstripe support** option under the *Advances settings* section on the *Mercury controller settings* page. Magstripe is not supported when the **Facility code** option is selected as the door behavior for offline SIO boards, even if you enable the **Magstripe support** option.
- When the SIO board loses connection with the Mercury controller, and no card formats or facility codes are added in the Synergis™ Appliance Portal, the doors that the SIO board controls become locked, regardless of the state that they were in before the connection was lost.
- The following occurs when a credential is valid in Security Center, but its facility code is not added in the Synergis Appliance Portal:
  - If the Mercury controller disconnects from the Synergis Cloud Link unit, access is denied.
  - If the Mercury controller is connected to the Synergis Cloud Link unit, access is granted.

Mercury native area control, host decision handoff, and antipassback

When you configure the door behavior for offline SIO boards to use facility codes to grant access, access decisions vary based on what other features are enabled and how they work together.

Example

In this example, the following is assumed:

- The **Facility code** option is selected as the door behavior for offline SIO boards in the Synergis Appliance Portal.
- Cardholder 1 has a credential with a facility code that is added in the Synergis Appliance Portal.
- Cardholder 2 has a credential with a facility code that is *not* added in the Synergis Appliance Portal.
- Antipassback is applied on the areas that the cardholders are trying to access.
- The Mercury controller is disconnected from the Synergis Cloud Link unit.

Setting in the Synergis Appliance Portal		
Mercury native area control	Disable host decision handoff (offline mode)	Access decision after badging at the door again
Disabled	Disabled	• Cardholder 1 gets an antipassback violation. • Cardholder 2 gets an antipassback violation.
Disabled	Enabled	• Antipassback does not work.
Enabled	Disabled	• Cardholder 1 gets an antipassback violation. • Cardholder 2 is denied access.
Enabled	Enabled	• Cardholder 1 gets an antipassback violation. • Cardholder 2 is denied access.

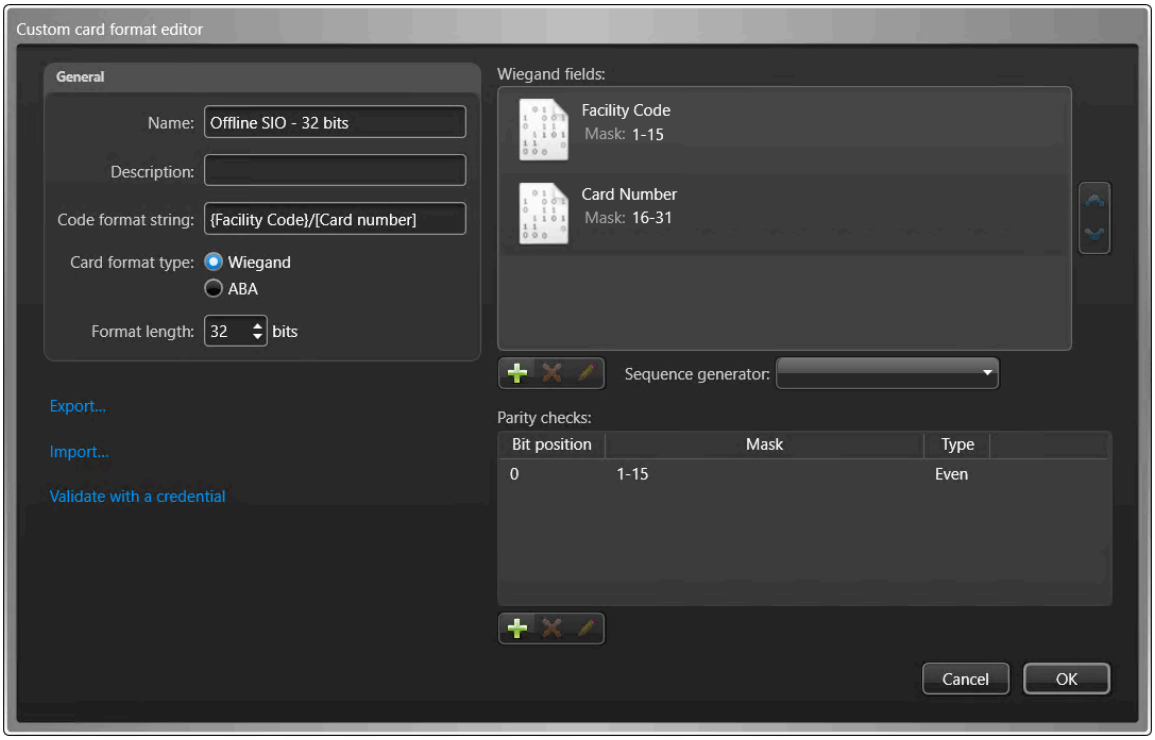
Configuring offline Mercury SIO boards to grant access through facility codes

You can configure access to be granted only to credentials with specific card formats and facility codes or with specific raw card formats when the SIO board loses connection with the Mercury controller.

Before you begin

- **CAUTION:** Configuring access to be granted through facility codes or card formats when the SIO board loses connection with the Mercury controller greatly reduces the security of your system. When this is configured, no activity trails are available. Any events that occur while in the SIO board isn't connected to the Mercury controller aren't recorded.
- Learn about how granting access through card formats and facility codes affects access decisions.
- To use a custom Wiegand card format, create it in Config Tool, and then export it to an XML file. The custom card format must be configured with a Wiegand field named `Facility Code`. The mask of the Wiegand field must be an ascending sequence of bits, up to 63 bits long.

  Example:



For more information, see Creating custom card formats.

Procedure

To grant access through a card format and facility code:

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury controller settings**.

3 Click the **Door behavior for offline SIO boards** tab from the side menu, and select **Facility code**.

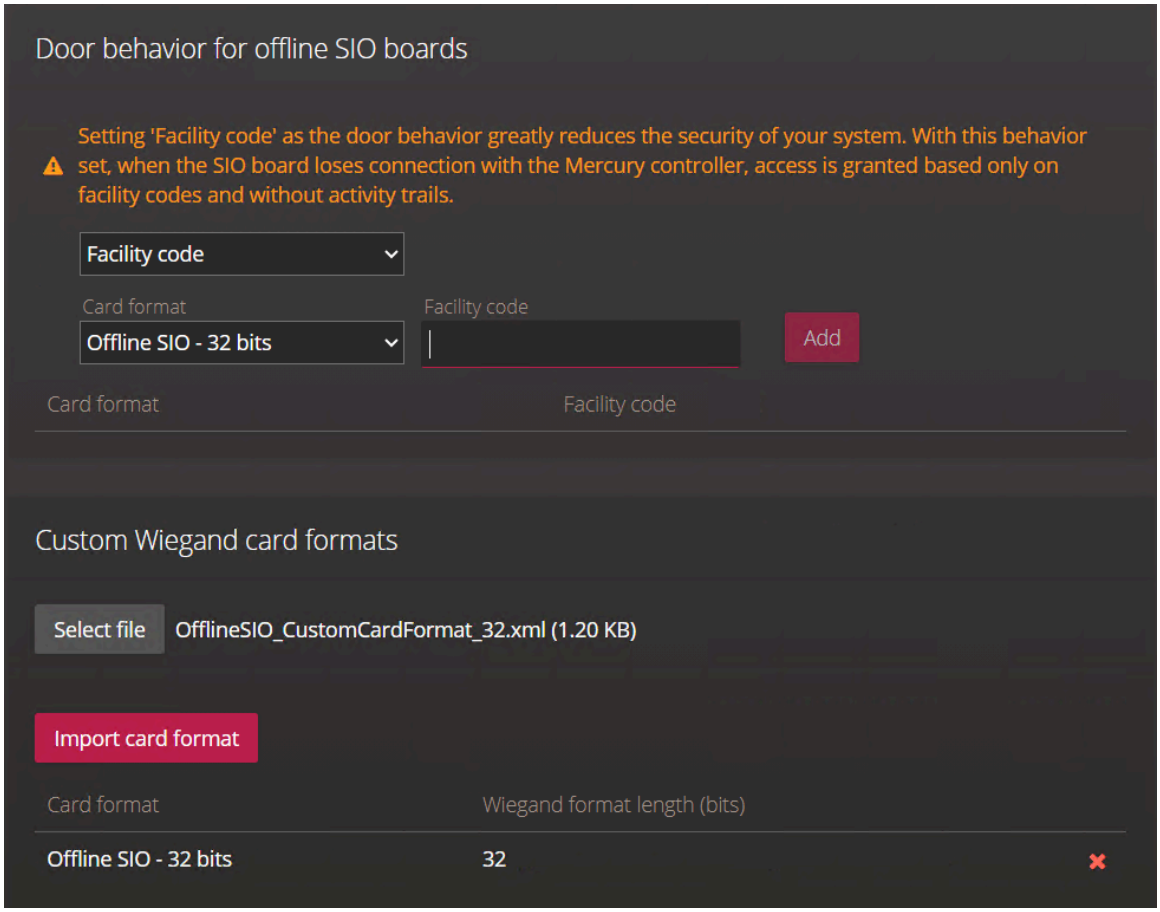
4 (Optional) To use a custom card format, do the following:

a) In the *Custom Wiegand card formats* section, click **Select file**, and then select the XML file that you exported from Config Tool.

b) Click **Import card format**.

The custom card format is listed in the *Custom Wiegand card formats* section, and can now be selected from the **Card format** drop-down in the *Door behavior for offline SIO boards* section.

Example:



5 From the **Card format** list, select a card format, and then enter a value in the **Facility code** field.

6 Click **Add**.

The configured card format and facility code are added to the list.

7 Click **Save**, and then perform a software restart.

Access is only granted to credentials that match both the card format and facility code.

To grant access through a raw custom card format:

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury controller settings**.

3 Add the custom card format by doing the following:

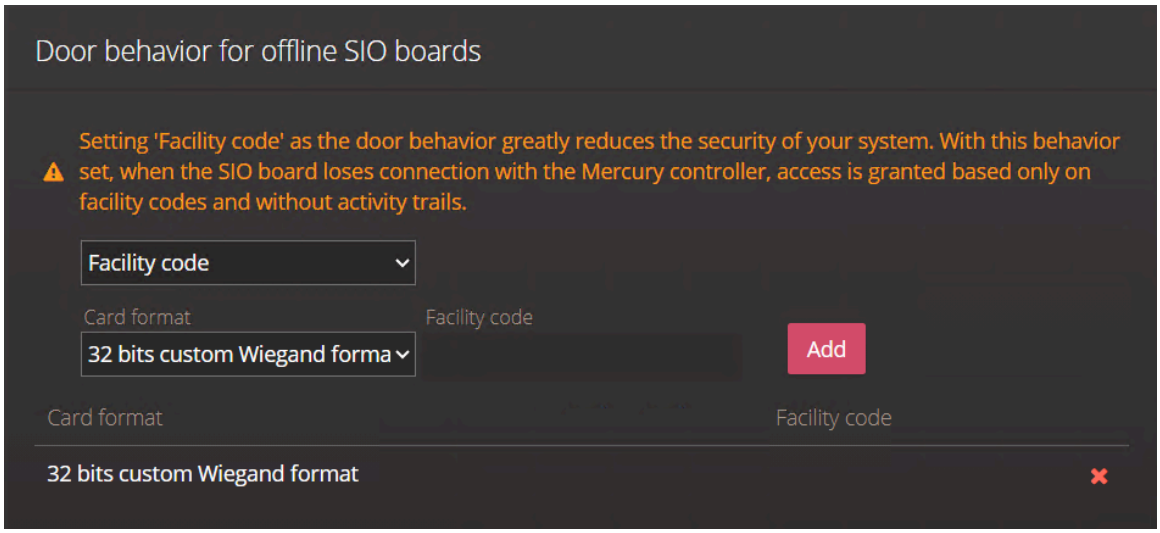
a) Click the **Long credential formats** tab from the side menu, and then enter the credential length you want to use.

b) Click **Add**.

The custom card format can now be selected from the **Card format** drop-down in the *Door behavior for offline SIO boards* section.

4 Click the **Door behavior for offline SIO boards** tab from the side menu, and select **Facility code**.

5 From the **Card format** drop-down, select the custom card format, and then click **Add**.
Example:



6 Click **Save**, and then perform a software restart.
Access is only granted to credentials that match the custom card format, regardless of the facility code.

Considerations for OSDP reader installation with Mercury

There are several points to take into consideration before adding OSDP readers to your Mercury controllers.

Limitations

The connection state of OSDP and OSDP 2 readers on Mercury controllers isn't refreshed if the reader isn't assigned to a door or elevator.

NOTE: This limitation also applies to Out readers when using two OSDP readers per port.

Supported onboard OSDP readers with Mercury controllers

Refer to the following table to know how many OSDP readers Synergis™ Softwire supports with Mercury:

Model	Onboard reader ports	Max onboard OSDP readers per panel
MR50-S2[1]	1	1
MR50-S3	1	2 (two on one port)[2]
MR52-S2[1]	2	2 (one per port)
MR52-S3	2	4 (two per port)[2]
MR51e	2	2 (two on one port only)
MR62e	1	4 (four on one port)
EP1501	2	2 (two on one port only)
EP1502	2	2 (one per port)
EP4502	2	2 (one per port)
LP1501	2	2 (two on one port only)
LP1502	2	4 (two per port)[2]
LP4502	2	4 (two per port)[2]
MP1501	2	2 (two on one port only)
MP1502	2	4 (two per port)[2]
MP4502	2	4 (two per port)[2]

NOTE: Mercury EP2500, LP2500, and MP2500 controllers aren’t listed because they don’t have onboard reader ports. They support OSDP readers through the interface modules listed in the table.

[1] Series 2 MR50 and Series 2 MR52 don’t support OSDP Secure Channel or two OSDP readers per port.

[2] Two OSDP readers per port are supported through the **Two OSDP readers per reader port** setting on the *Mercury controller settings* page in the Synergis™ Appliance Portal.

Wiring instructions for OSDP readers

Depending on the assembly revision and PCB revision of your Mercury interface module and EP, LP, or MP controllers, specific installation requirements must be met:

- A 1K-ohm pull-down resistor must be added between the Mercury DAT/D0 and GND lines on interface modules and EP, LP, or MP controllers.
- The pull-down resistor must be installed on the panel.
- To function properly, there must not be any ground faults in the installation. Ensure that the DC Ground (power supply return) isn't connected to earth ground.
- Wiring for Wiegand can be reused for OSDP. However, standard Wiegand cables might not meet RS-485 twisted-pair recommendations.
- Star-shaped wiring isn't recommended.

To find out whether you need to add a 1K ohm pull-down resistor between D0 and GND, see KBA-78953.

For more information about how to wire the OSDP readers, see Connecting Mercury interface modules in Synergis Cloud Link.

Termination resistors

The following guidelines are especially important if you're working with a high baud rate, for example, at 115,200 baud:

- For OSDP cables longer than 200 ft. (61m) or EMF interference, install a 120 ohm resistor on both ends of the RS-485 daisy chain.
- For Wiegand cables longer than 32 ft. (10m) or EMF interference, install a 120 ohm resistor on both ends of the RS-485 daisy chain.

If communication errors occur, you can lower the baud rate, add termination resistors, or both.

Adding OSDP (Secure Channel) readers to a Mercury controller

To add an OSDP (Secure Channel) reader to a Mercury LP or MP controller, you must first configure the reader on the controller using Config Tool, and then pair the reader to the controller using the Synergis™ Appliance Portal.

Before you begin

Enroll your controller with its downstream panels on your Synergis™ unit.

What you should know

- To add an OSDP (Secure Channel) reader to a Mercury controller, you must pair the reader (exchange of keys) to the controller it is connected to. To pair a reader in secure mode to a different reader port when it is already securely paired to a reader port, reset the reader to factory default.
- Starting in Synergis™ Softwire 11.2, connected OSDP readers do not respond when cards are presented to them, unless they are configured to control a door or elevator in Security Center.
- Valid addresses for Mercury-controlled OSDP readers are 0 to 3.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

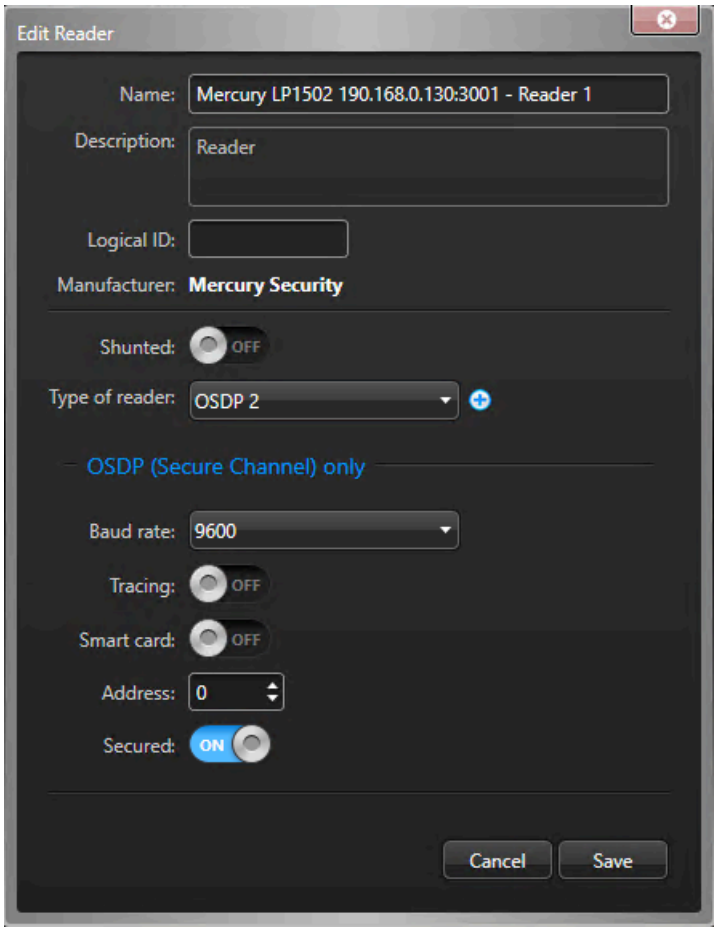
2 From the entity tree, select the Synergis unit, and click the **Peripherals** tab.

3 If necessary, expand the controller to see the downstream MR panels and peripherals.

4 Click the reader ( ) you want to configure and click **Edit** ( ).

5 In the *Edit Reader* dialog box, select **OSDP 2** from the **Type of reader** list.

Example:



NOTE: The **Secured** option must be on.

6 Configure the other settings in the *OSDP (Secure Channel) only* section as necessary, and then click **Save**.

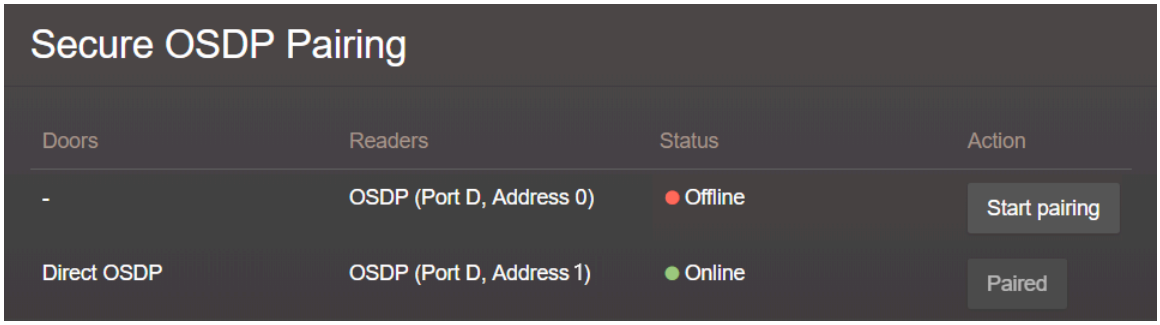
NOTE: When you select **Auto** for the **Baud rate** option, the OSDP channel cycles through baud rates to look for a device that responds to the broadcast address. Once a device is found, the Mercury controller automatically sets the appropriate baud rate. However, the **Auto** option doesn't work if multiple readers are configured to use the same reader port.

7 Log on to the Synergis Cloud Link unit.

8 Click **Configuration** > **Advanced OSDP**.

9 Find the row with the configured port, reader, and associated door, and click **Start pairing**.

This exchanges the keys, and the reader come back online. The reader is now secure. Any reader that rejects the key stays offline.



10 Repeat step 9 for the remaining readers.

This exchanges the keys, and the readers come back online. The readers are now secure; any reader that rejects the key stays offline.

After the pairing process is completed, the reader appears online in Config Tool.

Configuring two OSDP readers per Mercury device

The following Mercury devices can each support two OSDP readers: EP1501, LP1501, MP1501, and MR51e. To enable this capability, you must configure both readers to use the first reader port on the Mercury device.

Before you begin

Configure the OSDP readers.

What you should know

- On Mercury EP1501, LP1501, and MP1501 controllers, the first port is terminal block TB2.
- On Mercury MR51e downstream panels, the first port is terminal block TB3.
- When you configure two OSDP readers on the first port, you cannot use the second port.
- Mercury EP1501, LP1501, and MP1501 must be enrolled without extension boards for the first port to be available for the two OSDP readers.

Procedure

1 From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

2 From the entity tree, select the Synergis unit, and click the **Peripherals** tab.

3 Double-click **Reader 1**, and configure the following settings:

- **Type of reader:** Select **OSDP 2**.
- **Baud rate:** Select a bit rate.
  NOTE: The **Auto** option doesn't work when two readers are configured on the same port.
- **Address:** Select the address you configured for the first reader.

4 Repeat step 3 for **Reader 2**, using the address configured for the second reader.

Selecting **OSDP 2** for both readers automatically assigns both readers to the first port.

5 (Optional - supported readers only) Ensure that the **Secured** option is set to **ON**.

Configuring Mercury devices to use two OSDP readers per port

The following Mercury devices can support two OSDP readers on each of their onboard reader ports: LP1502, LP4502, MP1502, MP4502, MR50-S3, and MR52-S3. You must enable this capability in the Synergis™ Appliance Portal before configuring the readers in Config Tool.

What you should know

- Support for two OSDP readers per port on Mercury LP1502, LP4502, MR50-S3, and MR52-S3 requires Security Center 5.10.4.0 or later.
- Support for two OSDP readers per port on Mercury MP1502 and MP4502 requires Security Center 5.12.1.0 or later.
- When the **Two OSDP readers per reader port** option is enabled in the Synergis Appliance Portal, and you only configure one of the OSDP readers on a door, ensure that the configured reader is the primary reader, otherwise the door will be in warning, even though it still works.

Procedure

1 In the Synergis Appliance Portal, enable the **Two OSDP readers per reader port** option on the *Mercury controller settings* page.

NOTE: When this option is enabled, the **Smart card** option configured on the OSDP reader in Config Tool is on by default, and remains on in the background, even if you turn off the option.

2 Restart Synergis Softwire.

3 Add two OSDP readers to the reader port of the Mercury controller:

a) From the Config Tool homepage, open the *Access control* task, and click the **Roles and units** view.

b) From the entity tree, select the Synergis™ unit, and click the **Peripherals** tab.

c) Double-click **Reader 1**, and configure the following settings:

- **Type of reader:** Select **OSDP 2**.
- **Baud rate:** Select a bit rate.

  NOTE: The **Auto** option doesn't work when two readers are configured on the same port.
- **Address:** Select the address you configured for the first reader.

d) Click **Save**.

e) Double-click **Reader 1 Out**, and select the address you configured for the second reader.

NOTE: Only the address needs to be configured because *Reader 1* and *Reader 1 Out* use the same configuration, except the address.

4 Assign the readers to a door.

Example: *Reader 1* and *Reader 1 Out* must be set on the same door, and *Reader 2* and *Reader 2 Out* must be set on the same door.

5 If the controller has a second reader port, you can repeat step 3 to configure *Reader 2* and *Reader 2 Out* on the second port.

After you finish

Pair the OSDP readers in the Synergis™ Appliance Portal. When using OSDP 2, you might need to disable *Install mode* on the reader after pairing if it is not disabled after pairing.

Adding MR51e panels to a Mercury controller

MR51e is a single door PoE panel that must be controlled through a Mercury controller. For the MR51e panel to communicate with the controller, you must set the MR51e panel to use either the Public DHCP (recommended) or the Static IP addressing mode.

Before you begin

Make sure of the following:

- If not already done, load the MR51e panels with the supported firmware version.
- Enroll the controller on your Synergis™ unit.
- If the MR51e panels are using the Static IP addressing mode, download the *MSC MR51e Address Configuration Tool* from the Mercury website.

What you should know

For Mercury integration through Synergis™ Softwire, you can use the MR51e panel with only two addressing modes: the Public DHCP, and Static IP.

NOTE: Reader port 1 on the MR51e panel can support up to two OSDP readers.

Procedure

1 Do one of the following:
   - Set the MR51e panel to use Public DHCP (recommended).
   - Set the MR51e panel to use Static IP.
2 In Config Tool, open the *Access control* task, and click **Roles and units**.
3 Select the Synergis unit, and add the MR51e panels.
   For more information, see the steps for adding downstream panels in Enrolling Mercury controllers on the Synergis unit on page 142.

Setting MR51e to use Public DHCP addressing mode

If your network supports DHCP, it is recommended to set your MR51e panels to use Public DCHP addressing model.

Procedure

1 On the MR51e panel, set **S1** (Configuration DIP switches) to **0001**.
   Set DIP Switch 4, 3, and 2 to OFF, and DIP Switch 1 to ON.
2 Press **S2** (Reset Switch).

Setting MR51e to use Static IP addressing mode

If your network does not support DHCP, set your MR51e panels to use Static IP addressing model.

Before you begin

Download the MSC MR51e Address Configuration Tool and install it on your computer. Make sure the MR51e panel is connected to the same subnet as your computer.

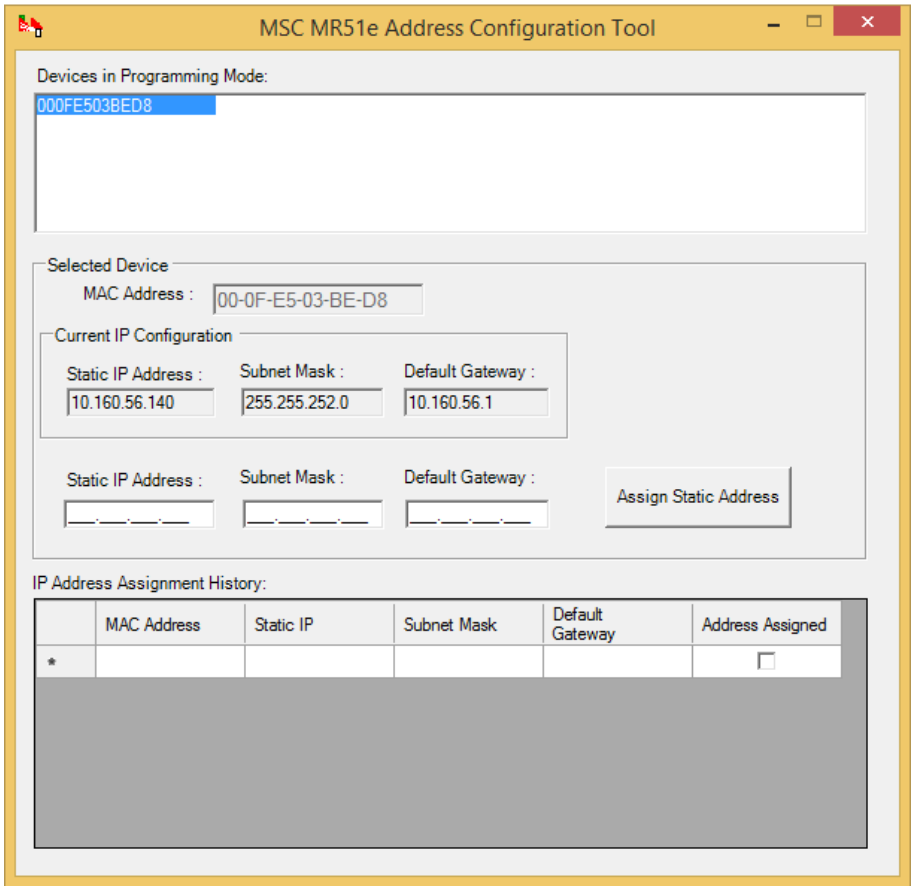
Procedure

1 On the MR51e panel, set **S1** (Configuration DIP switches) to **0011**.
Set DIP Switch 4 and 3 to OFF, and DIP Switch 2 and 1 to ON.

2 Open the MSC MR51e Address Configuration Tool.

3 Press **S2** (Reset Switch).
Once detected, the MAC address of the MR51e panel appears in the **Devices in Programming Mode** list.

4 In the **Devices in Programming Mode** list, select the MR51e panel to be programmed.
The MAC address of the selected MR51e panel appears in the **Selected Device** field.



5 Enter the values for **Static IP Address**, **Subnet Mask**, and **Default Gateway**, and click **Assign Static Address**.
The entered values appear in the **Current IP Configuration** group and in the **IP Address Assignment History** list.

6 On the MR51e panel, set **S1** (Configuration DIP switches) to **0010**.
Set DIP Switch 4, 3, and 1 to OFF, and DIP Switch 2 to ON.

7 Press **S2** (Reset Switch).

Setting MR62e to use Static IP addressing mode

Before you add the Mercury MR62e panel or Mercury controller under the Synergis™ unit, you must assign a static IP address to the unit.

Before you begin

Make sure you have the following:

- **Mercury Setup and Configuration Guide:** Instruction manual for connecting to the web portal of your Mercury controller and setting up its IP address (and other configurations).
- **Static IP address:** Static IP address assigned to the controller by your IT department.

Procedure

1 Log on to the MR62e panel's web page.

2 In the **Static IP** field, enter an IP address.

3 Click **Save**.

Mercury reader address configuration for MR62e panel

Readers connected to the MR62e downstream panel are used in specific pairs and must be configured to predefined addresses, as hard-coded by Mercury, in order to work.

The following table shows the required reader address configuration:

Reader number (address)	Door setup	Mercury turnstiles and elevators
0	**Door 1**: Reader side IN	Yes
1	**Door 2**: Reader side IN	Yes
2	**Door 1**: Reader side OUT	No
3	**Door 2**: Reader side OUT	No

NOTE: To use the MR62e to control only one card-in/card-out door, use addresses 0 and 2.

To use the MR62e to control two card-in/REX-out doors, use addresses 0 and 1.

Disconnecting MR panels from a Mercury controller

To disconnect a Mercury MR panel from a Mercury controller that is enrolled in Security Center, you can delete the panel from the controller in Config Tool.

What you should know

Mercury MR panels must be offline in Security Center before you can delete them.

Procedure

1 From the Config Tool homepage, open the *Access control* task.

2 Click **Roles and units**, select your Synergis™ unit, and click the **Peripherals** tab.

3 If the MR panel is controlling doors or zones, then disconnect them.

4 Disconnect the panel:

- Disconnect power from the panel and wait until it goes offline in Config Tool.
- Click the **Peripherals** tab, select the panel, click **Edit**, then change the **Address** of the panel so it disconnects from the controller and goes offline in Config Tool.

5 Click the **Peripherals** tab, select the panel, click **Delete**, and then click **Apply**.

About Mercury triggers and procedures

Mercury triggers and procedures are comparable to event-to-actions in Security Center. You can configure triggers and procedures in the Synergis™ Appliance Portal to run rules directly on a Mercury controller.

How Mercury triggers and procedures work in the Synergis Appliance Portal

- Mercury triggers and procedures work together to create a rule. The trigger defines the *when* with an event, and the procedure defines the *what* with one or more actions. Each trigger is linked to one procedure, but each procedure can be used in multiple triggers.
- If entities used in triggers and procedures fall into an unexpected state, you can restore them to their original state with the **Reset to default** button on the *Mercury triggers and procedures* page.

  NOTE: This button is also used to restore Mercury triggers and procedures after restoring the configuration files of a Synergis Cloud Link unit.

Best practices

For optimal performance of Mercury triggers and procedures, ensure that the following settings are enabled on the *Mercury controller settings* page in the Synergis Appliance Portal:

- **Live 'Request to exit' events:** Enable this setting if you create triggers with REX events.
- **Mercury native area control:** Enable this setting if you create triggers related to areas.

About monitoring Mercury triggers and procedures

In Security Center 5.12 and later, Mercury triggers and procedures generate custom events, which can be used in event-to-actions.

- **Event monitoring:** You can monitor the custom events in the Security Desk *Monitoring* task by adding the Synergis Cloud Link unit to the *Event monitoring* list.
- **Event reporting:** You can run reports on the custom events using the *Access control unit events* task in Security Desk and Config Tool, and filtering on the Synergis Cloud Link unit.
- **Capabilities:** On the *Capabilities report* page in the Synergis Appliance Portal, the *Custom triggers* and *Custom procedures* rows in the *Capabilities* section lists the number of triggers and procedure that are created on the selected Mercury controller.

Limitations of Mercury triggers and procedures

Mercury triggers and procedures in the Synergis Appliance Portal have the following known limitations:

General limitations

- Each Mercury controller can have up to 3,000 triggers and 3,000 procedures. The triggers and procedures that exceed these limits are ignored.

Limitations related to configuration

- You can activate an output based on an input change. However, there isn't any option to reset the output to its original state.

  Workaround: To reset the output, create a separate procedure to set the output back to its original state with a trigger set on an input change.
- Inputs and outputs that are assigned to doors or elevators can’t be used as monitor point or control point triggers.

- The reader LED pattern commands that Synergis™ Softwire sends to Mercury override active LED pattern procedures. This includes setting the reader LED to red on relock and setting the reader LED to green when a door enters a free access schedule.
- Power cycling the Mercury controller cancels *Override reader mode* procedures configured with an **Indefinite** duration.
- The temporary reader mode configuration in *Override reader mode* procedures overrides any manual changes to the reader mode.

  Example: If you change a reader to *Card and PIN* mode while an *Override reader mode* procedure configured to change the reader mode to *Locked* is active, the door remains locked. However, when the procedure expires, the reader returns to *Card and PIN* mode.
- When a cardholder badges at a reader that was disabled with the *Override reader mode* procedure, the *Access denied* event in Security Center doesn't include a deny reason.
- For *Set control point* procedures configured with a **Periodic** command, you only see the first and last output change in Config Tool.

Limitations related to schedules

- Schedules are only synced to the Synergis Cloud Link unit if they are associated to an entity controlled by that unit. To use schedules exclusive to triggers and procedures, you must add a dummy door to the Synergis Cloud Link unit and apply the schedules to that door.
- Mercury has a limit of 255 schedules. Therefore, you can only create 255 schedules in Security Center, including unlock schedules and schedules only used for Mercury triggers and procedures.
- Mercury has a limit of 12 schedule intervals. For more information, see Mercury limitations with door unlock schedules.

Action types for Mercury procedures

Each Mercury procedure must contain one or more of the following actions.

Action	Description
Arm/disarm zone	Arm or disarm a hardware zone: • **Disarm:** Mask all zone inputs. Inputs on activation do not transition to the alarm state. • **Arm:** If no inputs are active, arm the zone and unmask all inputs. • **Force arm:** Arm the zone but only unmask inactive inputs. Previously active inputs remain masked. • **Override arm:** Arm the zone and unmask all inputs.
Control procedure	Control a Mercury procedure: • **Execute:** Execute the actions in the selected procedure. • **Abort delayed:** If the selected procedure is waiting on a *Delay* action, abort the procedure without completing its subsequent actions. • **Resume delayed:** If the selected procedure is waiting on a *Delay* action, skip the delay so that its subsequent actions can be executed.
Delay	Cause the procedure to wait the configured number of seconds before proceeding with its subsequent actions.
Ignore door forced open	Disable door forced open alarms for the door.

Action	Description
Ignore door held open	Disable door held open alarms for the door.
Ignore monitor point alarms	Masks the input, preventing it from entering an alarm state on activation.
Override reader LED	Apply a temporary LED pattern to the reader. Configure the following: • **On color** • **Off color** • **On time (ms)** • **Off time (ms)** • **Repeat (0-255)** • **Beep count (0-15)**
Override reader mode	Override the reader mode for the configured duration with one of the following reader modes: • **Disabled:** Card reads and requests to exit are disabled and the door remains locked. • **Unlocked:** The door is unlocked. • **Locked:** Card reads are disabled but requests to exit still work. • **Card only:** Only cards are valid access credentials. • **Card and PIN:** Card and PIN are required for access. • **Card or PIN:** Cards or PINs are valid access credentials. • **PIN only:** Only PINs are valid access credentials.
Set control point	Activate an output that is not assigned to a door strike.
Unlock door momentarily	Unlock the door for the configured duration.

Events types for Mercury triggers

Events define when a Mercury trigger occurs.

Event	Description
Access denied: Invalid card format	Access is denied when the card format has not been synced to the Mercury controller.
Access denied: Request rejected by controller	Access is denied for any of the following reasons: • The reader mode is *Locked*. • An unknown credential is used. • The Mercury access grant decision is overridden by Synergis Softwire. • An interlock constraint.
Access denied: Unauthorized cardholder	Access is denied for any of the following reasons: • The access rule associated with this cardholder does not apply during the date or time specified in the schedule. • An invalid PIN is entered. • A native antipassback violation.

Event	Description
	• A known card without access is used at this reader. • Two cardholders must present their credentials within a certain delay of each other and the delay has expired. • The area's occupancy limit is reached. • The visitor escort rule is enforced and the visitor is badged before the host. • A card and PIN are required to enter an area, and the cardholder did not enter the PIN within the allotted time.
Access denied: Unknown credential	Access is denied when the card format is recognized but the credential has not been synced to the Mercury controller.
Access granted	Access is granted after one of the following occurs: • The cardholder opens the door. • The entry time expires and the door relocks. • The door has no door sensor and entry is assumed.
Access granted: Entry detected	Access is granted after entry is detected.
Access granted: Unlocked	Access is granted after a door is unlocked.
Door closed	The door is closed.
Door forced open	The door is forced open.
Door held open	The door is held open.
Door opened (not forced)	The door is opened but not forced open.
Door relocked after REX	The door is relocked after a request to exit.
Door relocked after manual unlock	The door is relocked after a manual unlock.
Door relocked after manual unlock or REX	The door is relocked after a manual unlock or a request to exit.
Door unlocked by REX	The door is unlocked by a request to exit.
Duress PIN entered	A duress PIN is detected at the reader. The event is generated even if the **Duress PIN** option is disabled on the area and access is denied.
Hard max occupancy count reached	The hard maximum occupancy count is reached.
Hard occupancy count reached zero	The hard maximum occupancy count reached zero.
Monitor point: Alarm (active)	The unmasked input becomes active. Inputs in disarmed zones are masked.
Monitor point: Fault (trouble)	The input transitions to the *Trouble* state.
Monitor point: Secure (inactive)	The input transitions to the *Inactive* state.
Reader mode: Card and PIN	The reader mode changes to *Card and PIN*.

Event	Description
Reader mode: Card only	The reader mode changes to *Card only*.
Reader mode: Card or PIN	The reader mode changes to *Card or PIN*.
Reader mode: Disabled	The reader mode changes to *Disabled*.
Reader mode: Locked	The reader mode changes to *Locked* (reader shunted).
Reader mode: PIN only	The reader mode changes to *PIN only*.
Reader mode: Unlocked	The reader mode changes to *Unlocked* (maintenance mode).

Configuring Mercury procedures in the Synergis Appliance Portal

You must configure a procedure to define what actions to execute when a trigger event occurs.

Before you begin

Enroll a Mercury controller on the Synergis Cloud Link unit.

What you should know

The color of the procedure name indicates when there is an issue in the configuration:

- **Orange:** The configuration was saved but something failed to resolve, stopping it from being synced to the Mercury controller. This can occur when related entities no longer exist or was not properly synced to the controller. When a procedure is orange, any linked triggers are also orange. The Mercury controller must be online to see this color.
- **Red:** Required information for the configuration is missing or invalid.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury triggers and procedures**.

3 From the **Select a controller** list, select the controller for which you want to create a procedure.

4 Click the **Procedures** tab.

5 Click **Add a procedure**.

6 In the **Name** field, enter a descriptive name for the procedure.

7 Click **Add an action**.

A drop-down appears in the *Action* column.

8 Click the drop-down and select an action.

For a list of the actions and their descriptions, see Action types for Mercury procedures on page 174.

Different fields and buttons are displayed in the *Source* and *Settings* columns depending on the action you selected.

9 If there is a field in the *Source* column, click beside the field, and then select a source from the list in the dialog box that opens.

10 In the *Settings* column, configure the settings, as required.

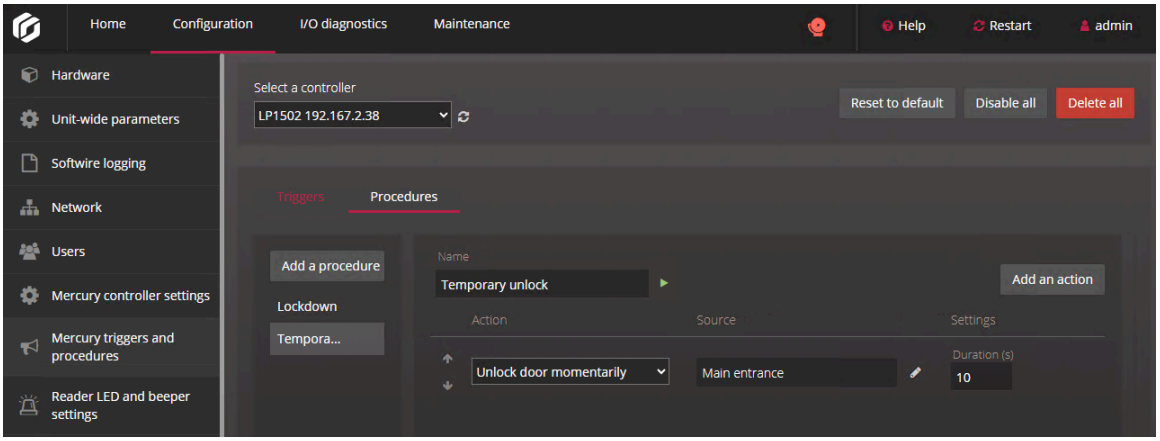
11 (Optional) Add more actions, as required.

12 (Optional) Re-order the actions using the up and down arrows. The actions are executed in the order in which they appear in the procedure configuration.

13 Click **Save**.

Example

This procedure is configured with the *Unlock door momentarily* action, which unlocks the *Main entrance* door for 10 seconds after the trigger occurs.



After you finish

- Test the procedure before linking it to a trigger by clicking ▶ beside the procedure **Name** field. If the procedure includes a *Delay* action, you can click ■ to stop the procedure during the delay and cancel the procedure.

  NOTE: The buttons are only displayed when the procedure has been successfully synced to the Mercury controller. The buttons are hidden if the controller is offline or there are unresolved fields in the procedure configuration. Click beside the controller field to refresh the page.
- Configure Mercury triggers in the Synergis Appliance Portal.

Configuring Mercury triggers in the Synergis Appliance Portal

Configure a trigger to define when a procedure is run.

Before you begin

Configure Mercury procedures in the Synergis™ Appliance Portal.

What you should know

The color of the trigger name indicates when there is an issue in the configuration:

- **Orange:** The configuration was saved but something failed to resolve, stopping it from being synced to the Mercury controller. This can occur when related entities no longer exist or was not properly synced to the controller. The Mercury controller must be online to see this color.
- **Red:** Required information for the configuration is missing or invalid.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury triggers and procedures**.

3 From the **Select a controller** list, select the controller for which you want to create a trigger.

4 Click **Add a trigger**.

5 In the **Name** field, enter a descriptive name for the trigger.

6 Beside the **Schedule** field, click . In the dialog box that opens, select a schedule from the list, and then click **OK**.

7 Beside the **Event** field, click . In the dialog box that opens, select an event from the list, and then click **OK**.

For a list of the events and their descriptions, see Events types for Mercury triggers on page 175.

Depending on the event you selected, one of the following fields is displayed:

- **Input:** Only inputs that are not assigned to any entity in Security Center are listed except for zone inputs.
- **Reader:** All readers that are under the selected Mercury controller are listed.
- **Door:** Only doors controlled by the selected Mercury controller are listed. Select the door side.
- **Area:** Only areas controlled by the selected Mercury controller are listed.
- **Zone:** Only hardware zones controlled by the selected Mercury controller are listed.

8 Beside the field that is displayed, click . In the dialog box that opens, select an entity from the list, and then click **OK**.

9 Beside the **Procedure** field, click . In the dialog box that opens, select a procedure from the list, and then click **OK**.

10 From the **Procedure command** list, select one of the following:

- **Execute:** Execute the actions in the selected procedure.
- **Abort delayed:** If the selected procedure is waiting on a *Delay* action, abort the procedure without completing its subsequent actions.
- **Resume delayed:** If the selected procedure is waiting on a *Delay* action, skip the delay so that its subsequent actions can be executed.

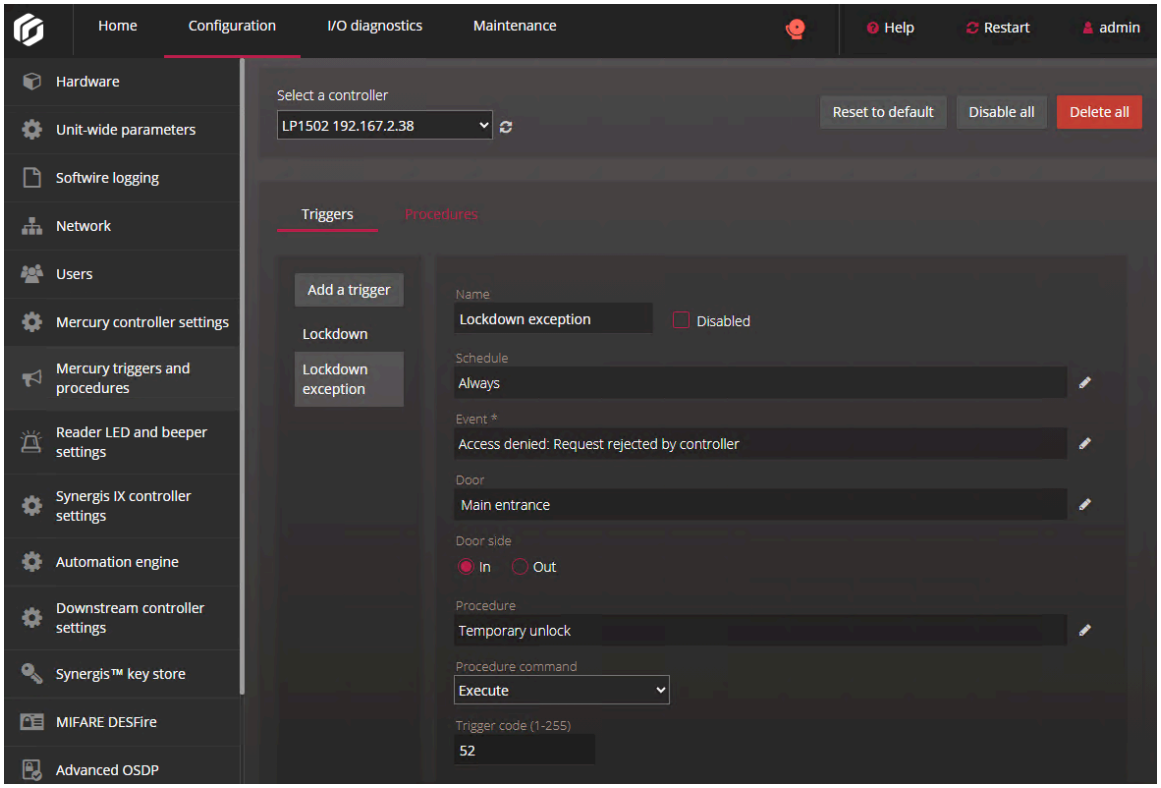
11 (Optional) Depending on the event you selected, the **Trigger code (1-255)** field is displayed. The trigger code acts as an additional condition for the trigger by specifying a cardholder or visitor in Security Center.

Starting in Security Center 5.12, the **Trigger code** is configured in the cardholder or visitor's advanced properties. The same trigger code can be used for multiple cardholders and visitors. There is no hierarchy to trigger codes.

12 Click **Save**.

Example

This trigger is configured to run the *Temporary unlock* procedure when a cardholder with trigger code 52 is denied access at the *Main entrance* door.



Disabling Mercury triggers and procedures in the Synergis Appliance Portal

To prevent a procedure from being run, you can disable the trigger that the procedure is linked to.

What you should know

Disabling a trigger un-syncs it from the Mercury controller without losing its configuration. This is useful for temporarily preventing a specific trigger from activating. You can also troubleshoot an unexpected behavior by disabling all triggers and then enabling them one by one to figure out where the issue is coming from.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Mercury triggers and procedures**.

3 Do one of the following:

- To disable a single trigger, select a trigger from the list, and then select the **Disable** checkbox beside the **Name** field. Click **Save**.
- To disable all triggers for the selected Mercury controller, at the top of the *Mercury triggers and procedures* page, click **Disable all**. In the dialog box that asks you to confirm your decision, click **Disable all**.

The disabled triggers are grayed out.

After you finish

To re-enable a trigger, select the trigger and clear the **Disable** checkbox, or click **Enable all** if all triggers were disabled. Click **Save**.

13

Allegion Schlage locks through Mercury

This section includes the following topics:

Enrolling Allegion Schlage AD locks and PIM modules on the Synergis unit

Because the Synergis™ unit doesn't communicate directly with Allegion Schlage AD locks or PIM400 modules, you must enroll these devices through a Mercury EP, LP, MP, or Honeywell controller, using Config Tool.

Before you begin

- Configure a different RS-485 address on each Schlage device (AD Series lock and PIM400 module) using the Schlage Pidion handheld device, and connect the lock and module to your Mercury controller. For more information, see the Schlage Utility Software User Guide.
- Configure the assigned static IP address on the Mercury controller.

What you should know

Mercury controllers enrolled on a Synergis™ unit are not visible from the Synergis™ Appliance Portal *Hardware* page.

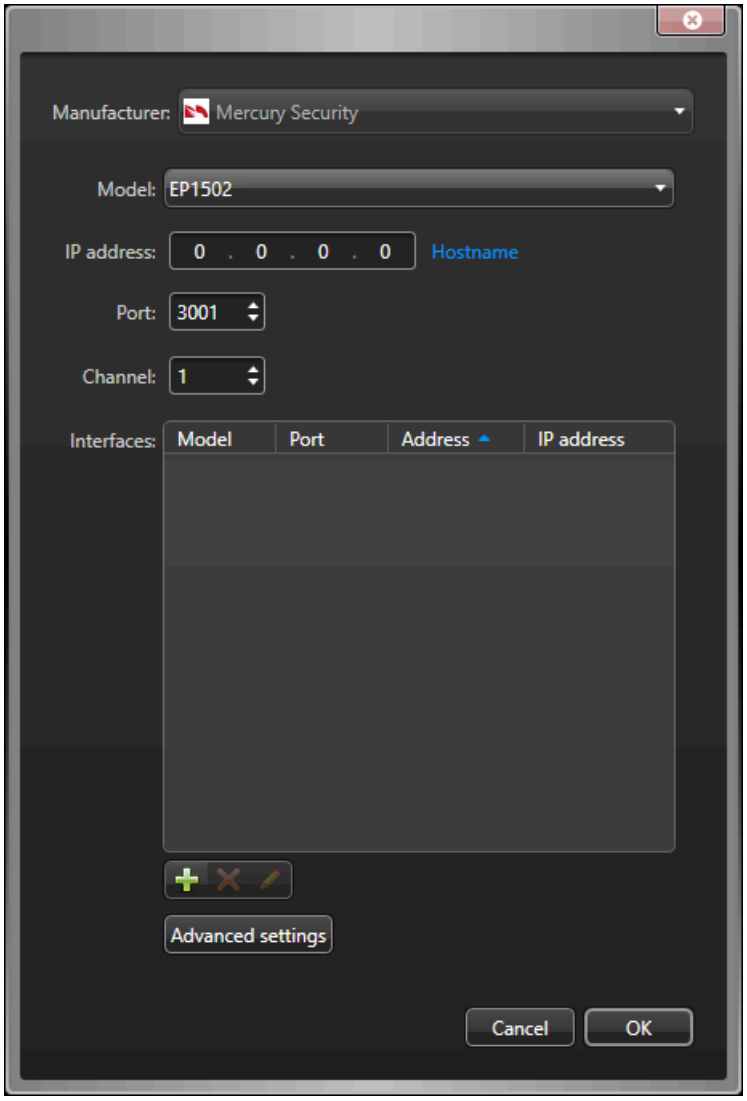
On the Synergis unit, each Mercury controller must be assigned a unique channel ID. All Mercury controllers have RS-485 buses to which the Schlage devices (AD-300 and PIM400) are connected. Each Schlage device connected to the same RS-485 bus must have a unique RS-485 address.

Procedure

1 From the Config Tool homepage, open the *Access control* task.

2 Click **Roles and units**, and then click the Synergis unit.

3 Click **Peripherals**, and then click **Add an item** ( ).



4 Enter the following information:

- **Model:** Model of the controller.
- **IP address:** Static IP address assigned to the controller by your IT department.
- **Hostname:** Click the blue link to identify the controller by its hostname. This option is only available if you're running Security Center 5.12.0.0 or later.

  NOTE: When enrolling a Mercury controller with its hostname, you must append the hostname with `.local` if the controller is not registered to DHCP and DNS on the network.
- **Port:** Communication port. The default value is 3001. The port must match the value configured on the Mercury Device Manager web page.
- **Channel:** Channel ID corresponding to this controller. The channel ID can be any value 0 - 63, and must be unique within the Synergis unit. After it's assigned, it must not be changed.

5 Add the Allegion Schlage devices that are connected to your Mercury controller.

a) Under the *Interfaces* list, click **Add an item** ( ).

b) In the dialog box that opens, select the **Model** (AD-300 or PIM400), the **Port**, and the **Address** (0 - 31).

c) (PIM400 only) In **Low**, enter the first door number linked to the PIM400, and in **Count**, enter the number of doors linked to the PIM400.

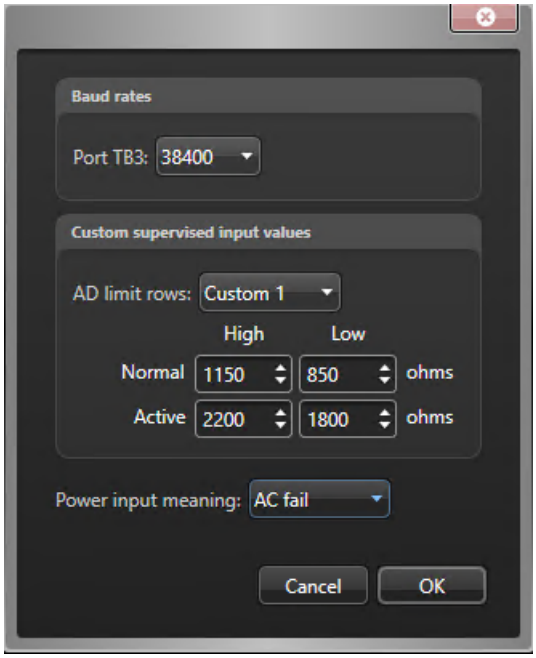
All door numbers ranging from **Low** to **Low**+**Count** must correspond to an AD-400 wireless lock.

d) Click **OK**.

e) Repeat as necessary.

6 (Optional) Click **Advanced settings** to change the advanced settings.

The available settings depend on the selected controller model. You can typically change the baud rate of the available serial port, the custom supervised input values, and the power input event configuration.

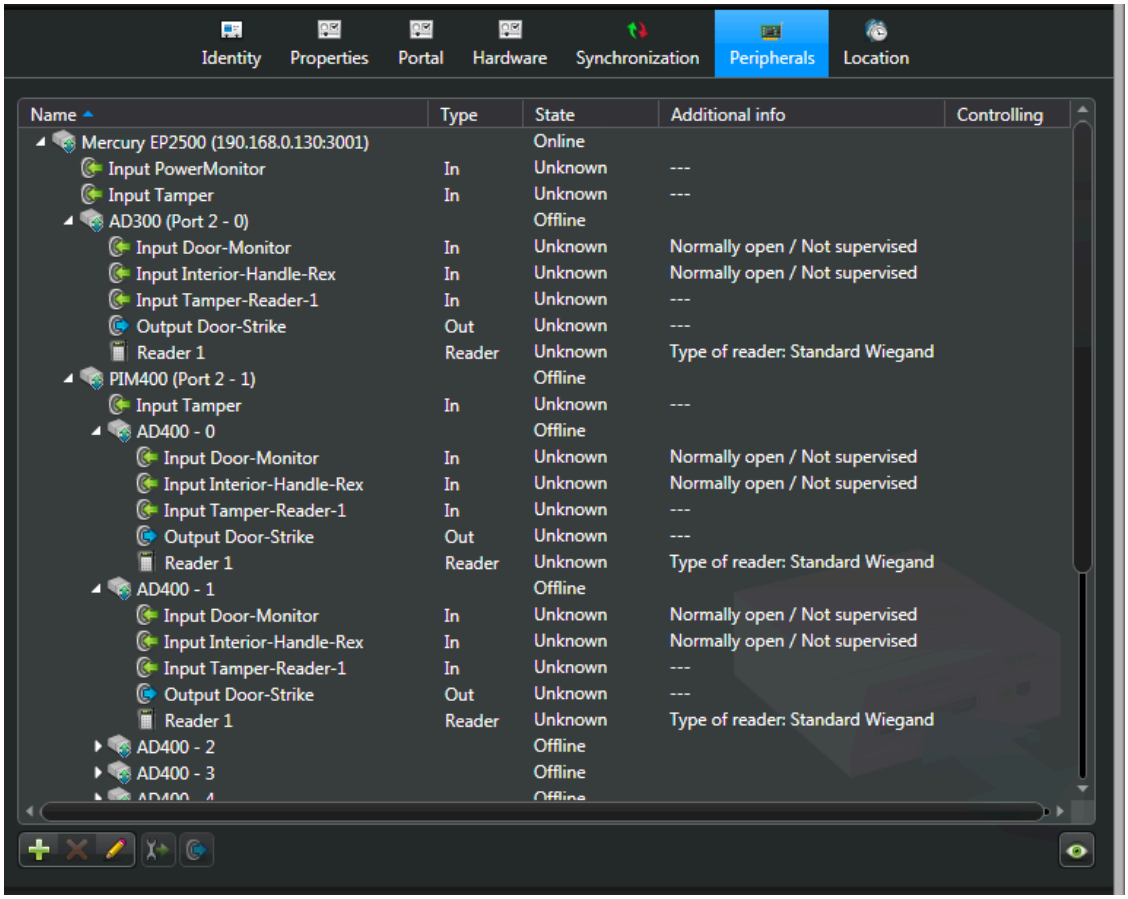


NOTE: You can set up to four different custom presets on your Mercury controller's inputs. For users upgrading from earlier Security Center versions who have a custom value configured, that preset is listed as **Custom 1** in the **AD limit rows** list.

7 Click **OK** at the bottom of the dialog box.

8 Click **Apply**.

The Mercury controller with all its connected downstream panels and peripheral devices are listed on the *Peripherals* page.



Adding interface modules to the Synergis unit causes the unit to perform a software restart. During this process, the Synergis unit and all peripherals attached to it are displayed in red.

Enrolling ENGAGE-integrated Allegion Schlage LE and NDE locks through Mercury controllers

With Allegion Schlage's ENGAGE platform, you can store credentials on key cards and on compatible mobile phones. To do this, you must integrate Allegion Schlage LE and NDE locks through the ENGAGE platform by enrolling a Mercury EP, LP, or MP controller in Config Tool and adding the ENGAGE Gateway as an interface.

Before you begin

Initial setup and lock pairing to the ENGAGE Gateway is done through the Allegion ENGAGE mobile app, which is available for Android and iOS devices. This is done by tapping **Connect**, then tapping the plus sign in the corner and following the steps. When this is done, enroll the locks in Config Tool.

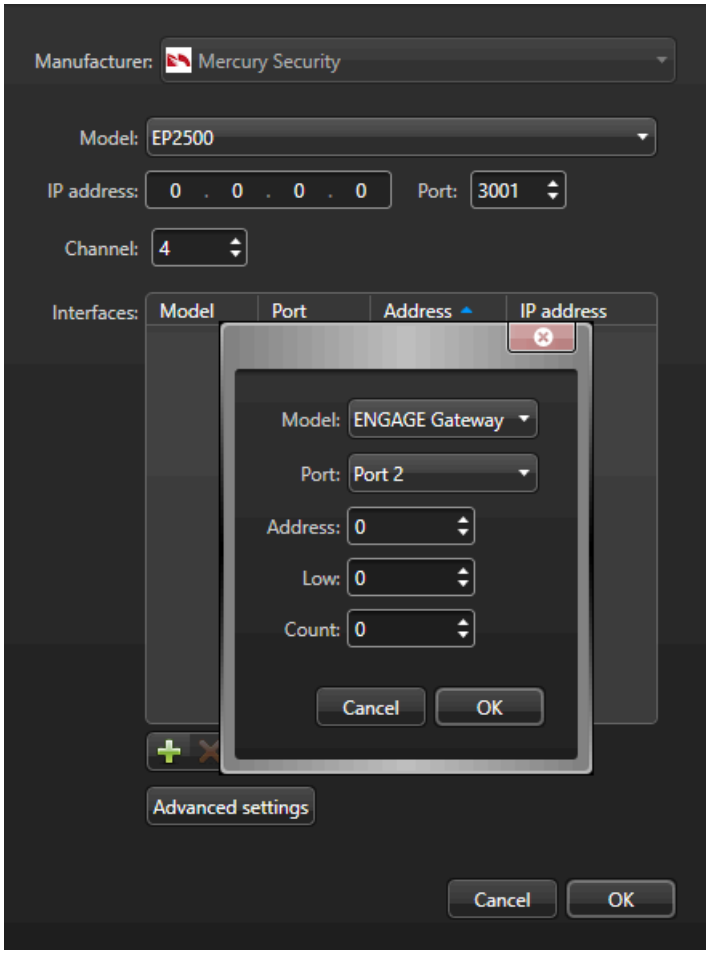
What you should know

The process for enrolling Allegion Schlage NDE and LE locks with the ENGAGE integration in Config Tool is the same as enrolling the PIM400 module, except that you select **ENGAGE Gateway** when you set the interface.

Procedure

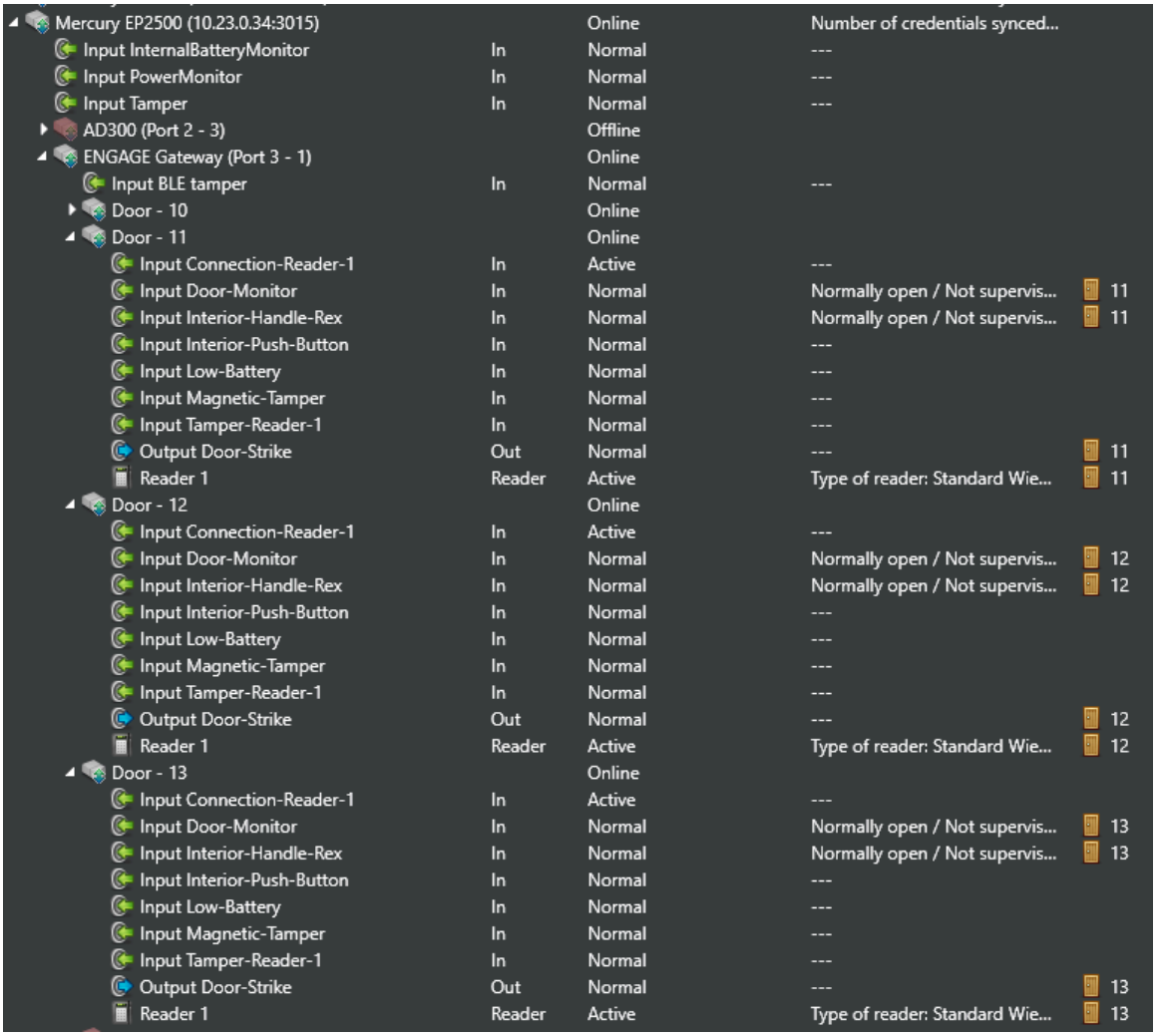
1 Enroll the Allegion Schlage NDE or LE locks as described in Enrolling Allegion Schlage AD locks and PIM modules on the Synergis unit on page 184.

2 At step 5, select the ENGAGE Gateway from the **Model** drop-down menu after clicking **Add an item** (+) in the *Interfaces* list.



The ENGAGE Gateway with all its connected downstream panels and peripheral devices is listed on the *Peripherals* page.

Example:


Mercury EP2500 (10.23.0.34:3015) Online Number of credentials synced...
Input InternalBatteryMonitor In Normal ---
Input PowerMonitor In Normal ---
Input Tamper In Normal ---
AD300 (Port 2 - 3) Offline
ENGAGE Gateway (Port 3 - 1) Online
Input BLE tamper In Normal ---
Door - 10 Online
Door - 11 Online
Input Connection-Reader-1 In Active ---
Input Door-Monitor In Normal Normally open / Not supervis... 11
Input Interior-Handle-Rex In Normal Normally open / Not supervis... 11
Input Interior-Push-Button In Normal ---
Input Low-Battery In Normal ---
Input Magnetic-Tamper In Normal ---
Input Tamper-Reader-1 In Normal ---
Output Door-Strike Out Normal --- 11
Reader 1 Reader Active Type of reader: Standard Wie... 11
Door - 12 Online
Input Connection-Reader-1 In Active ---
Input Door-Monitor In Normal Normally open / Not supervis... 12
Input Interior-Handle-Rex In Normal Normally open / Not supervis... 12
Input Interior-Push-Button In Normal ---
Input Low-Battery In Normal ---
Input Magnetic-Tamper In Normal ---
Input Tamper-Reader-1 In Normal ---
Output Door-Strike Out Normal --- 12
Reader 1 Reader Active Type of reader: Standard Wie... 12
Door - 13 Online
Input Connection-Reader-1 In Active ---
Input Door-Monitor In Normal Normally open / Not supervis... 13
Input Interior-Handle-Rex In Normal Normally open / Not supervis... 13
Input Interior-Push-Button In Normal ---
Input Low-Battery In Normal ---
Input Magnetic-Tamper In Normal ---
Input Tamper-Reader-1 In Normal ---
Output Door-Strike Out Normal --- 13
Reader 1 Reader Active Type of reader: Standard Wie... 13

14

BEST Wi-Q locks through Mercury

This section includes the following topics:

Configuring the Over-Watch plugin for the BEST Wi-Q integration

Before you can enroll BEST Wi-Q locks in Security Center, you must configure the Over-Watch plugin for Mercury LP4502 controllers.

What you should know

- All LP4502 controllers under the same Synergis™ Cloud Link unit must be configured with the same Over-Watch username, password, and listening port.
- If you want to move a Mercury LP4502 unit that is used in a BEST Wi-Q integration from one Synergis Cloud Link to another, the Over-Watch plugin must be enabled on the target Synergis Cloud Link before moving the unit.

Procedure

1 Load the Over-Watch plugin onto the Mercury controller.
   a) From the GTAP *Product Download* page, select **Synergis™ Cloud Link Legacy** in the **Download Finder** list, and then search for the latest Mercury LP4502 firmware.
   b) Save the *.sfw* file on your local drive.
   c) Upgrade the Mercury controller through the Synergis™ Appliance Portal.
   The Mercury controller restarts after the firmware is applied.
   d) Log on to the Synergis Cloud Link unit's advanced web page at https://<IP address>/MercuryEP/FirmwareVersions, and click **Install Over Watch package** listed under the Mercury LP4502 controller.
   The Mercury controller restarts after the plugin is installed.

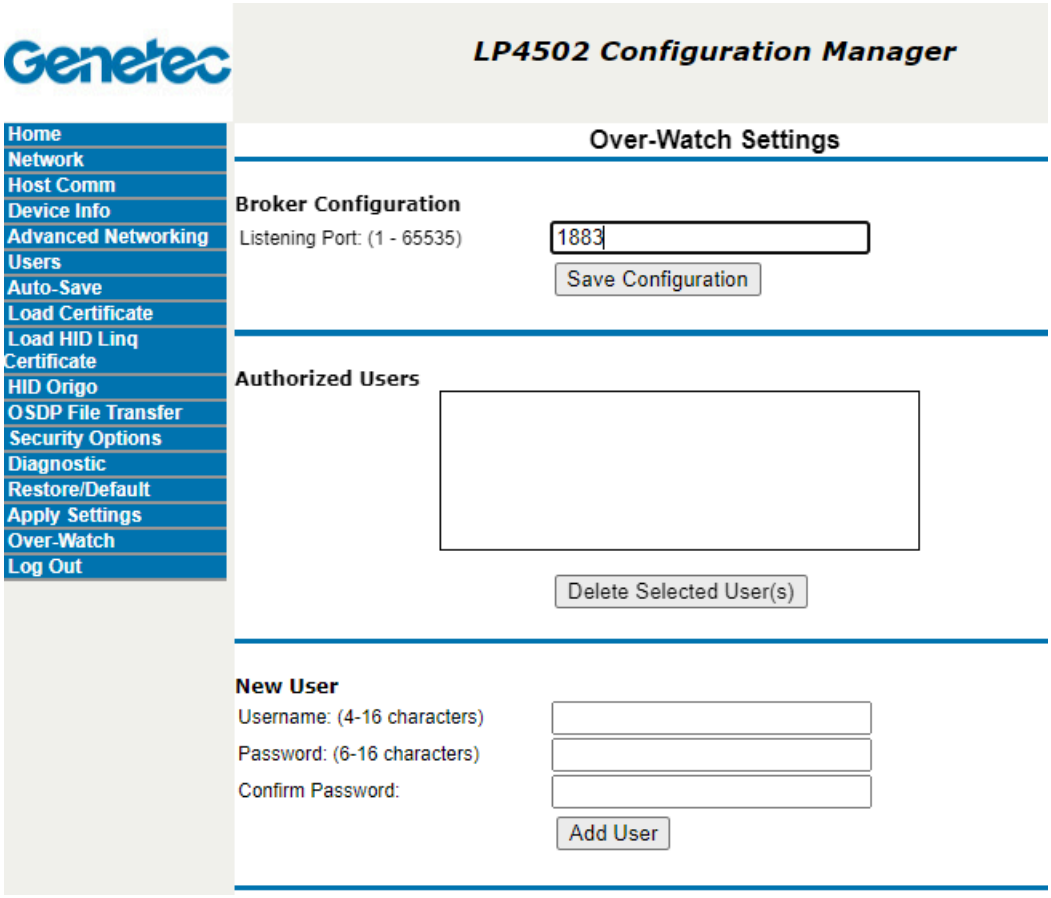
2 Configure an Over-Watch plugin user on the Mercury controller.

a) Log on to the Mercury controller through its *Configuration Manager* web page.

b) From the side menu, click **Over-Watch**.

c) On the *Over-Watch Settings* page, enter a port number in the **Listening Port** field.

The recommended port is 1883.



d) In the *New User* section, enter a username and password for the new user, confirm the password, and then click **Add user**.

e) From the side menu, click **Apply Settings**, and then click **Apply Settings, Reboot**.

3 Configure Mercury settings on the BEST Wi-Q gateway.

a) Log on to the BEST Wi-Q gateway.

b) From the top menu, click the **Interface** tab.

c) On the *Mercury interface configuration* page, select the **Enable Mercury Mode** option, and enter the Mercury controller's IP address.

d) In the **Port**, **Mercury Username**, and **Mercury Password** fields, enter the information you entered when creating the Over-Watch plugin user on the Mercury controller.

e) Select the **Enable SSL** option, and then click **Use Mercury certificate**.

f) Click **Update**.

The connection status is yellow.

4 Enable the Over-Watch plugin on the Synergis Cloud Link unit.
   a) Log on to the Synergis Cloud Link unit.
   b) Click **Configuration** > **Mercury controller settings**.
   c) Click the **Over-Watch settings** tab from the side menu.
   d) Select the **LP4502 Over-Watch plugin** option, and then enter the **Username**, **Password**, and **Port** that you configured when creating the Over-Watch plugin user on the Mercury controller.
   e) Click **Save**.
   f) Restart Synergis™ Softwire.

After you finish

Enroll a BEST Wi-Q gateway on the Synergis™ unit.

Enrolling BEST Wi-Q gateways on the Synergis unit through Mercury controllers

You must enroll BEST Wi-Q gateways through Mercury LP4502 controllers in Config Tool before you can add BEST Wi-Q locks and wireless access controllers.

Before you begin

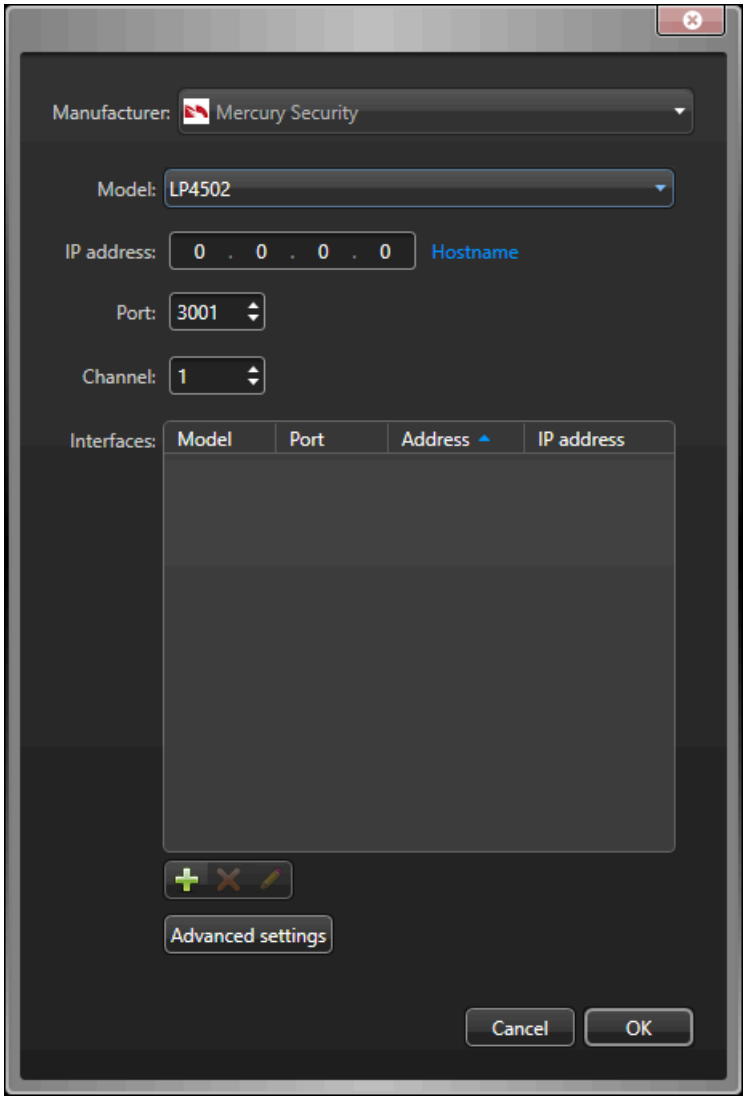
Configure the Over-Watch plugin on the Mercury controller and enable it on the Synergis™ unit.

What you should know

Mercury controllers enrolled on a Synergis™ unit are not visible from the Synergis™ Appliance Portal *Hardware* page.

Procedure

1 Enroll the Mercury LP4502 controller in Config Tool.
   a) From the Config Tool homepage, open the *Access control* task.
   b) Click **Roles and units**, and then click the Synergis unit.
   c) Click **Peripherals**, and then click **Add an item** ( ).

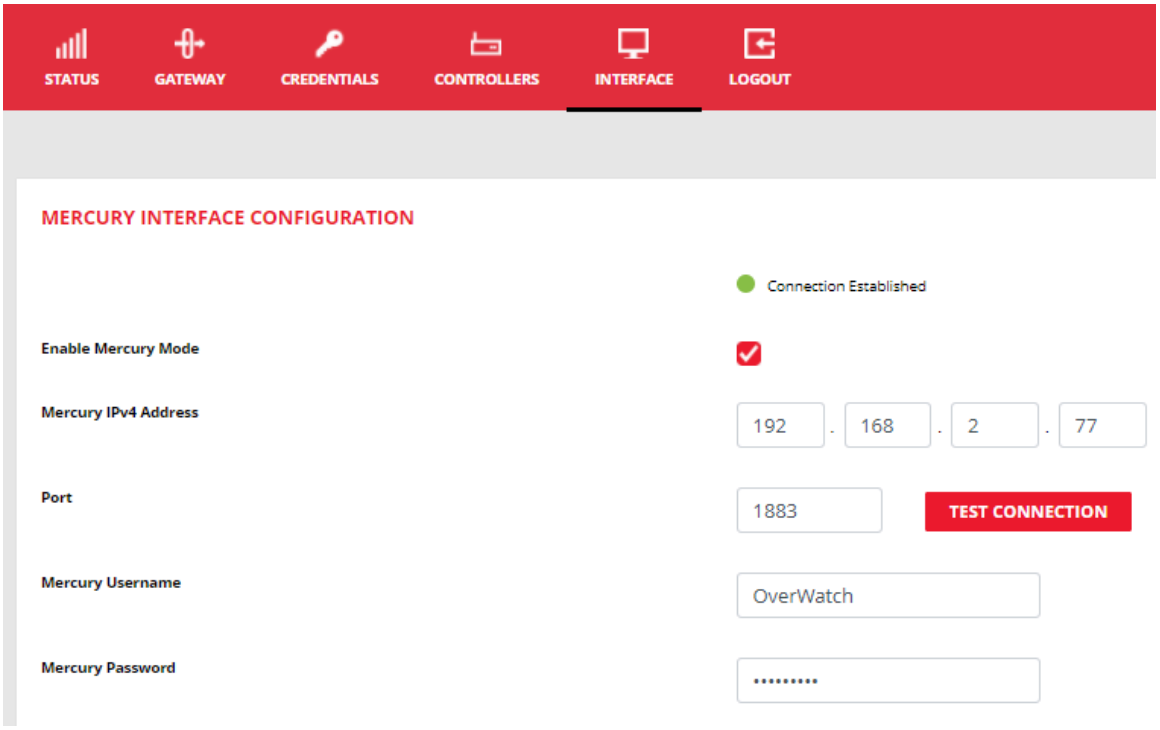


   d) Enter the following information:
   - **Model:** Select LP4502.
   - **IP address:** Static IP address assigned to the controller by your IT department.
   - **Hostname:** Click the blue link to identify the controller by its hostname. This option is only available if you are running Security Center 5.12.0.0 or later.
   - **Port:** Communication port (default=3001). The port must match the value configured on the Mercury Device Manager web page.
   - **Channel:** Channel ID corresponding to this controller. The channel ID can be any value from 0 to 63, and must be unique within the Synergis unit. After it is assigned, it must not be changed.

2 Add the BEST Wi-Q gateway as an interface for the Mercury controller.
   a) Under the *Interfaces* list, click **Add an item** (➕).
   b) In the dialog box that opens, select **BEST Wi-Q Gateway** as the **Model**, enter the **MAC Address**.

      NOTE: Ensure that the MAC address is entered using capital letters, is 12 characters long, and does not contain periods, colons, or dashes. For example, *A1B2C3D4E5F6*.

The Mercury controller and BEST Wi-Q gateway are online on the **Peripherals** page of the Synergis™ Cloud Link unit in Config Tool, and the connection is established on the web page of the BEST Wi-Q gateway.



After you finish

Pair the BEST Wi-Q locks or wireless access controllers with the BEST Wi-Q gateway, and then assign them ACR (access control reader) IDs from the web page of the BEST Wi-Q gateway, so that they can be added in Config Tool later. For more information about pairing devices to the gateway, see the BEST Wi-Q documentation.

Adding BEST Wi-Q locks and wireless access controllers to the gateway

You must add BEST Wi-Q locks and wireless access controllers to the gateway in Config Tool.

Before you begin

Pair the BEST Wi-Q locks or wireless access controllers with the BEST Wi-Q gateway, and then assign them ACR (access control reader) IDs from the web page of the BEST Wi-Q gateway, so that they can be added in Config Tool. For more information about pairing devices to the gateway, see the BEST Wi-Q documentation.

Procedure

1 From the Config Tool homepage, open the *Access control* task.

2 Click **Roles and units**, and then click the Synergis™ unit.

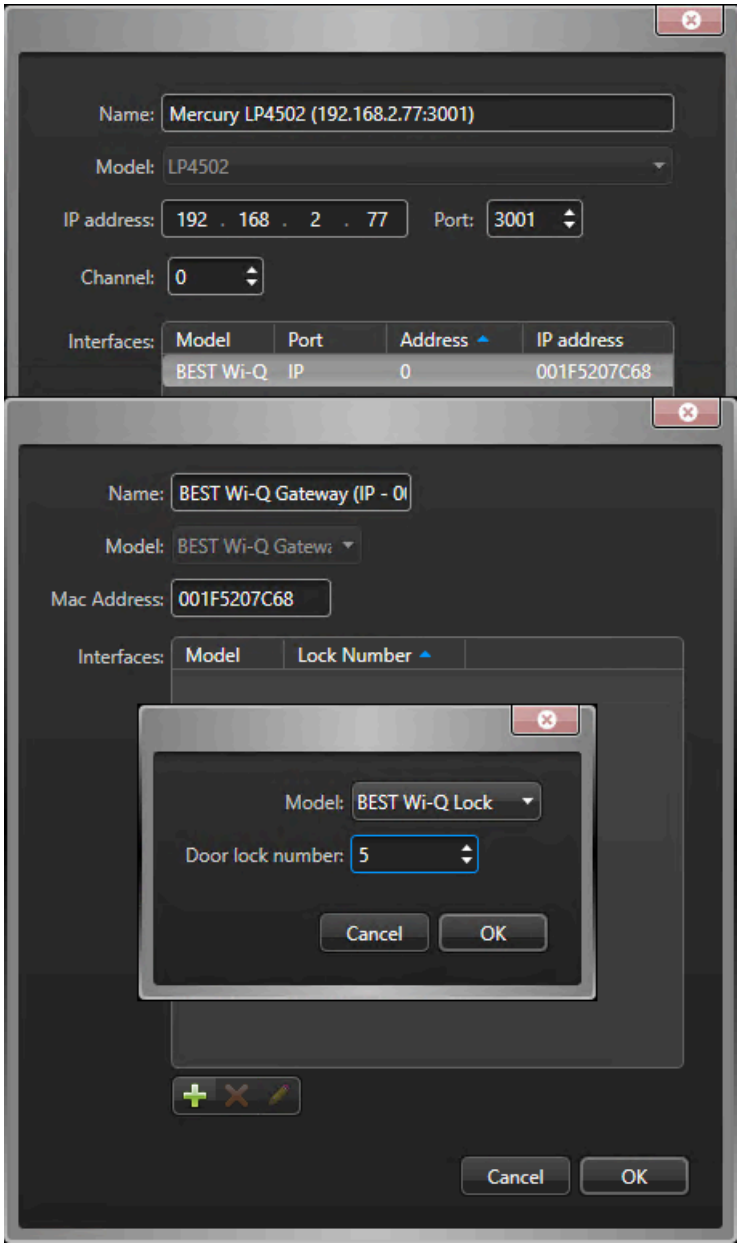
3 Click the **Peripherals** tab, and then double-click the Mercury LP4502 controller.

4 In the dialog box that opens, double-click the BEST Wi-Q gateway in the *Interfaces* list.

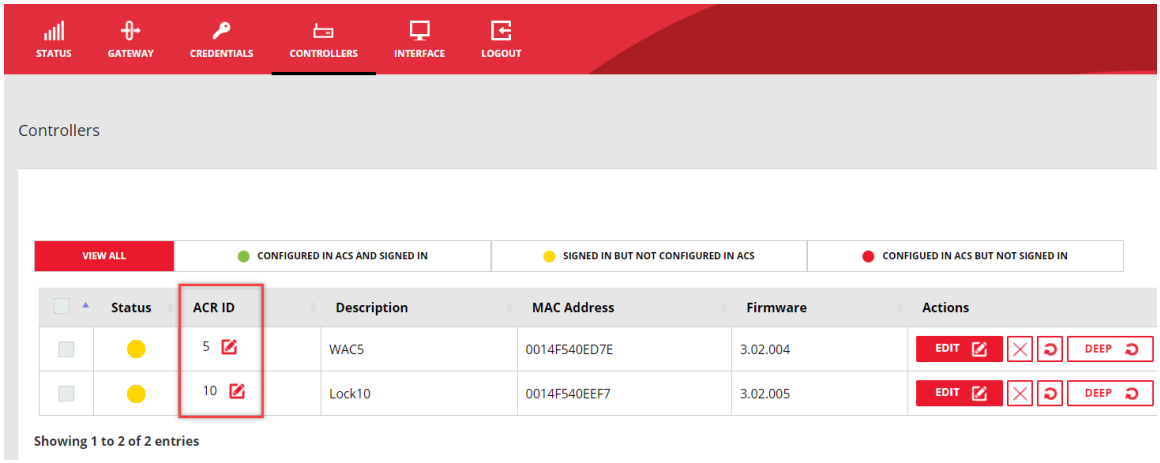
5 In the dialog box that opens, click **Add an item** () under the *Interfaces* list.

A dialog box opens with **BEST Wi-Q Lock** selected as the **Model**. This option is used for locks and wireless access controllers.

6 Enter the **Door lock number** for the lock or WAC, and then click **OK**.



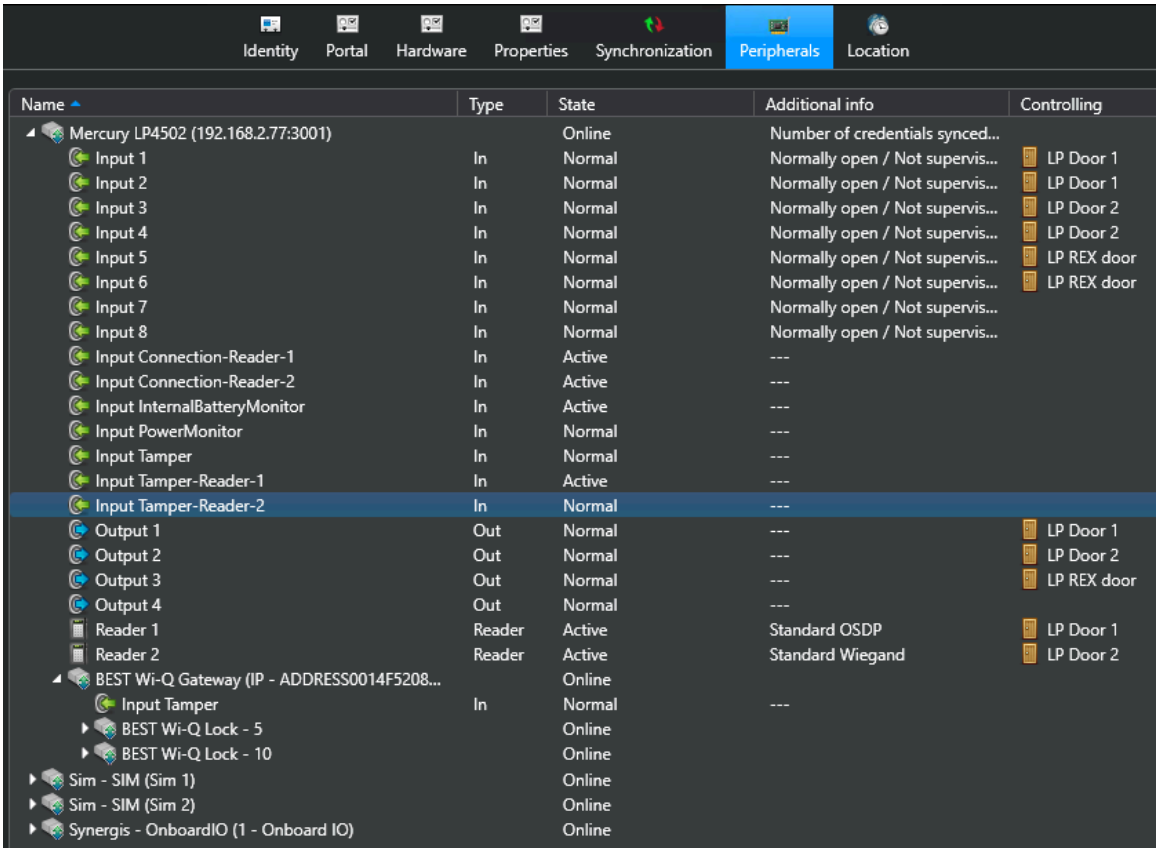
NOTE: The door lock number must match the ACR ID that was assigned to the lock or WAC on web page of the BEST Wi-Q gateway.



7 Click **OK** > **OK**.

8 Click **Apply**.

The Mercury controller, BEST Wi-Q gateway, and locks are displayed on the *Peripherals* page.

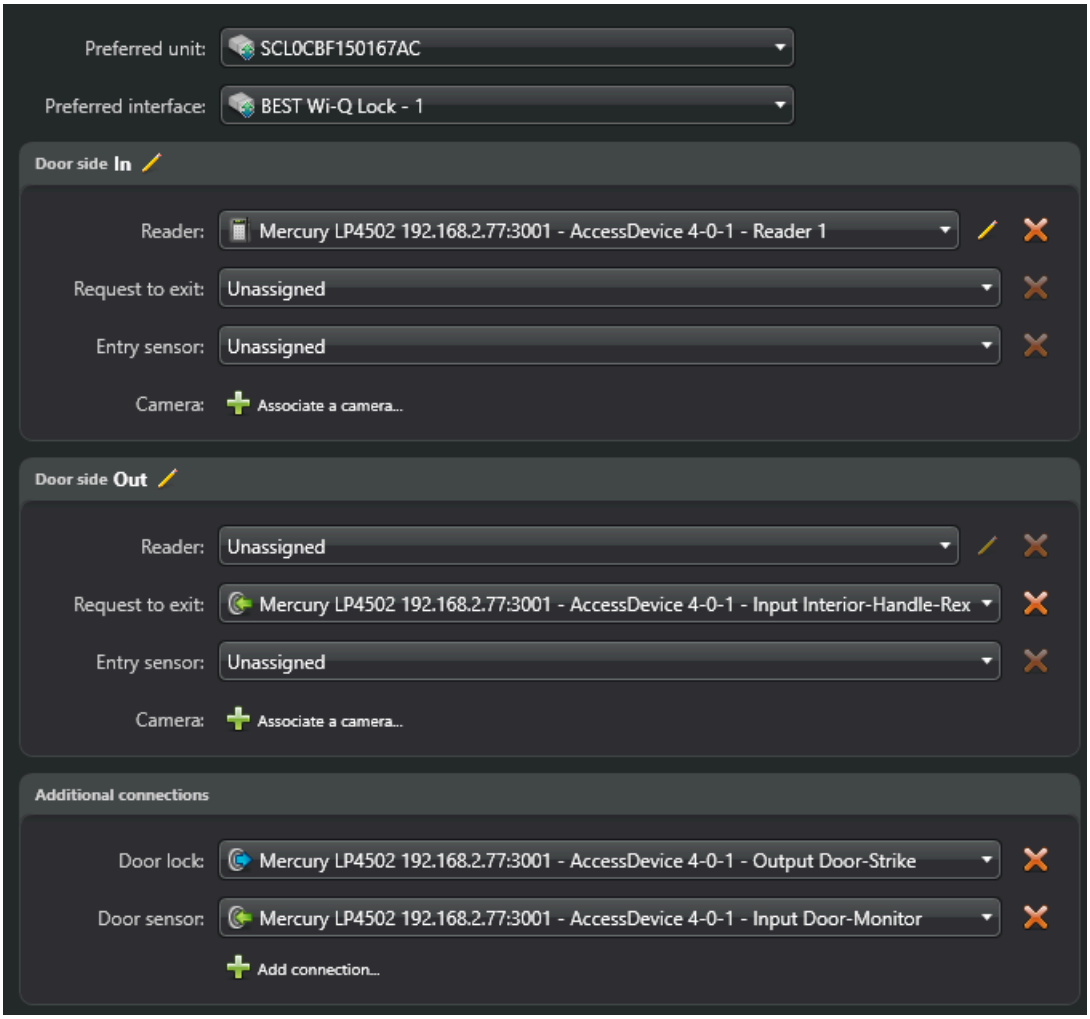


On the web page of the BEST Wi-Q gateway, the status of the lock or WAC you added in Config Tool turns green.

After you finish

Assign the lock or WAC I/Os to doors in Config Tool. You can use the *Card In, Rex Out* door template to speed up configuration.

Example: The following image shows a typical configuration on a door's *Hardware* page.


Preferred unit:
SCL0CBF150167AC
Preferred interface:
BEST Wi-Q Lock - 1
Door side In
Reader:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Reader 1
Request to exit:
Unassigned
Entry sensor:
Unassigned
Camera:
Associate a camera...
Door side Out
Reader:
Unassigned
Request to exit:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Input Interior-Handle-Rex
Entry sensor:
Unassigned
Camera:
Associate a camera...
Additional connections
Door lock:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Output Door-Strike
Door sensor:
Mercury LP4502 192.168.2.77:3001 - AccessDevice 4-0-1 - Input Door-Monitor
Add connection...

About BEST Wi-Q passage mode

BEST Wi-Q devices have a native passage mode feature, also known as *classroom mode* or *double badge*, which allows users to unlock a door by badging twice on the reader, and to re-lock it by badging twice again.

How to enable and configure the feature

The BEST Wi-Q passage mode feature is enabled through the *DoubleSwipe* door custom field, the same way that the double-badge activation feature is enabled in Security Center.

For more information, see the following topics in the *Security Center Administrator Guide*:

- About double-badge activation
- Enabling double-badge activation
- Configuring a door for double-badge activation

For a cardholder to use the passage mode feature, they must be part of all the cardholder groups that are configured to use the *DoubleSwipe* custom field on all the BEST Wi-Q doors under the same Mercury LP4502 controller. To simplify the configuration, it is therefore recommended to assign only one cardholder group to use the feature on these doors.

After the feature is configured, badging twice on the reader generates the *Double-badge on* event, and unlocks the door. Badging twice on the same reader again generates the *Double-badge off* event, and re-locks the door.

Limitations

Doors with BEST Wi-Q locks do not support Mercury buzzer features.

15

SimonsVoss SmartIntego locks through Mercury

This section includes the following topics:

Preparing to enroll SimonsVoss SmartIntego locks

Before you can enroll the SmartIntego locks on the Synergis™ unit, you must pair the Gateway node to your SmartIntego locks.

What you should know

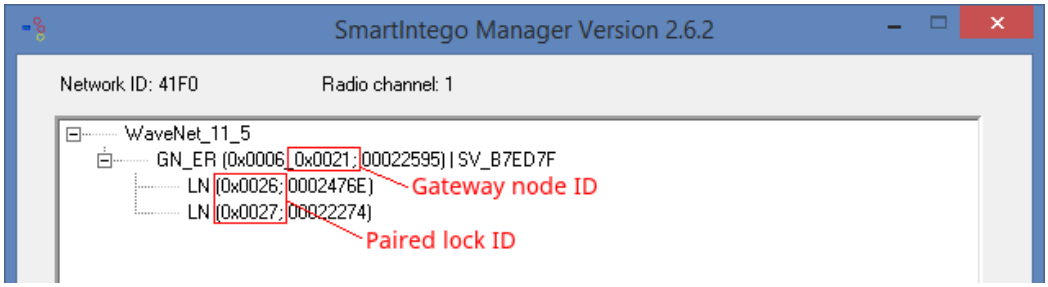
The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

Procedure

1 Follow the documentation that came with your SmartIntego devices and pair the Gateway node to your SmartIntego locks.

2 Write down the following information:

- The IP address of the Gateway node.
- The device IDs taken from the *SmartIntego Manager* window.

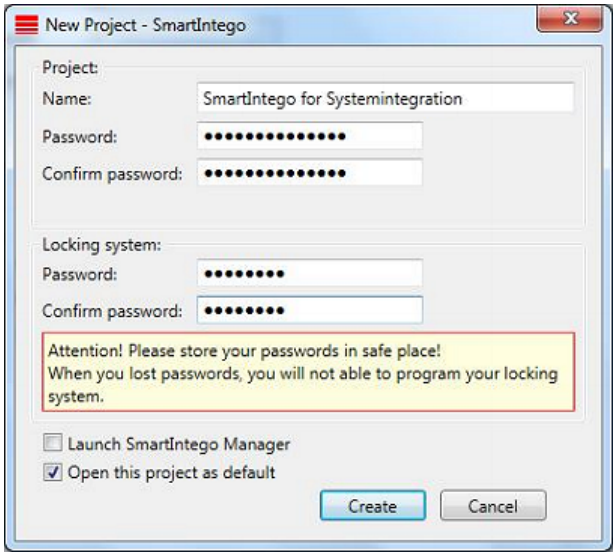


The Gateway node ID is the second hexadecimal number following GN_ER.

The lock ID is the first hexadecimal number following LN.

3 (*Hardening*) Follow the documentation that came with your SmartIntego devices and configure the communication encryption key for your locks.

SmartIntego software does not allow a lock to be paired to the hub without a password. Use a strong password for the locking system.



Enrolling SimonsVoss SmartIntego locks on the Synergis unit

Because the Synergis™ unit doesn't communicate with the SimonsVoss SmartIntego devices, you must enroll these devices through a Mercury EP, LP, MP, or Honeywell controller, using Config Tool.

Before you begin

Pair your the Gateway node to your SmartIntego locks.

What you should know

Mercury controllers enrolled on a Synergis unit are not visible from the Synergis™ Appliance Portal's *Hardware* page.

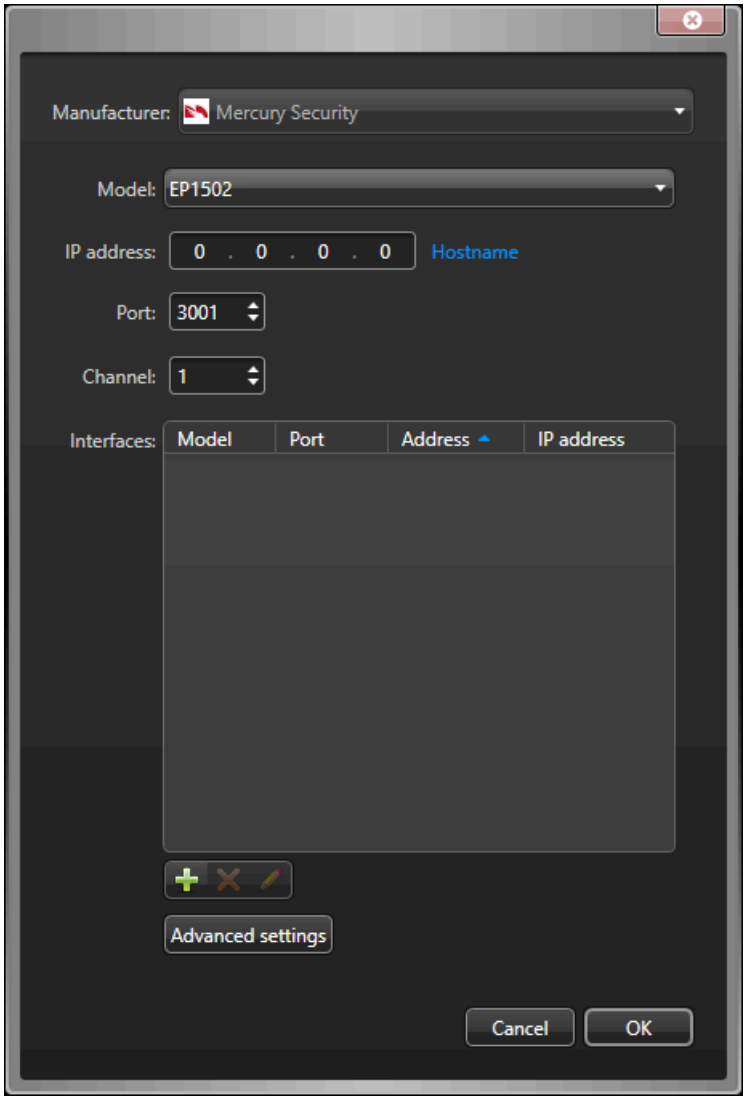
On the Synergis unit, each Mercury controller must be assigned a unique channel ID. The controller communicates with the SmartIntego Gateway nodes through IP. IP addresses cannot overlap within the same network.

Procedure

1 From the Config Tool homepage, open the *Access control* task.

2 Click **Roles and units**, and then click the Synergis unit.

3 Click **Peripherals**, and then click **Add an item** ( ).



4 Enter the following information:

- **Model:** Model of the controller.
- **IP address:** Static IP address assigned to the controller by your IT department.
- **Hostname:** Click the blue link to identify the controller by its hostname. This option is only available if you're running Security Center 5.12.0.0 or later.

  NOTE: When enrolling a Mercury controller with its hostname, you must append the hostname with `.local` if the controller is not registered to DHCP and DNS on the network.
- **Port:** Communication port. The default value is 3001. The port must match the value configured on the Mercury Device Manager web page.
- **Channel:** Channel ID corresponding to this controller. The channel ID can be any value 0 - 63, and must be unique within the Synergis unit. After it's assigned, it must not be changed.

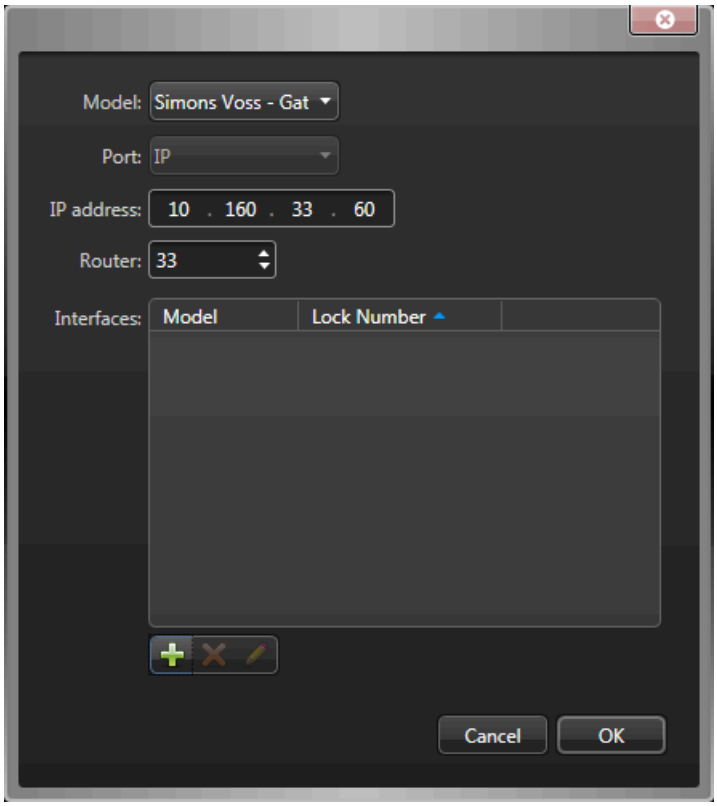
5 At the bottom of the *Interfaces* group, click **Add an item** (+) to add the SmartIntego Gateway node that you want the controller to talk to.

a) In the dialog box that opens, click **Model**, and then select **SimonsVoss Gateway node**.

b) In **IP address**, enter the IP address of the Gateway node.

c) In **Router**, enter the decimal value of the Gateway node ID.

For example, if the Gateway node ID is 0x0021, enter 33 (= 2 x 16 + 1).

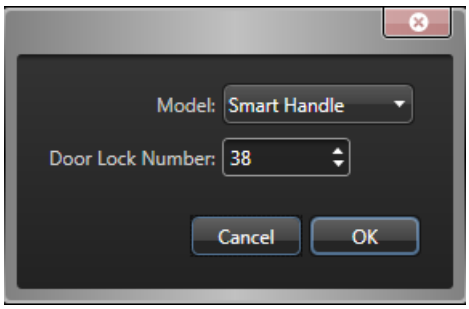


6 At the bottom of the *Interfaces* group, click **Add an item** (+) to add the locks paired to the Gateway node.

a) In the dialog box that opens, click **Model**, and then select the lock model (Smart Handle, Padlock, Cylinder, and so on).

b) In **Door Lock Number**, enter the decimal value of the lock ID.

For example, if the lock ID is 0x0026, enter 38 (= 2 x 16 + 6).



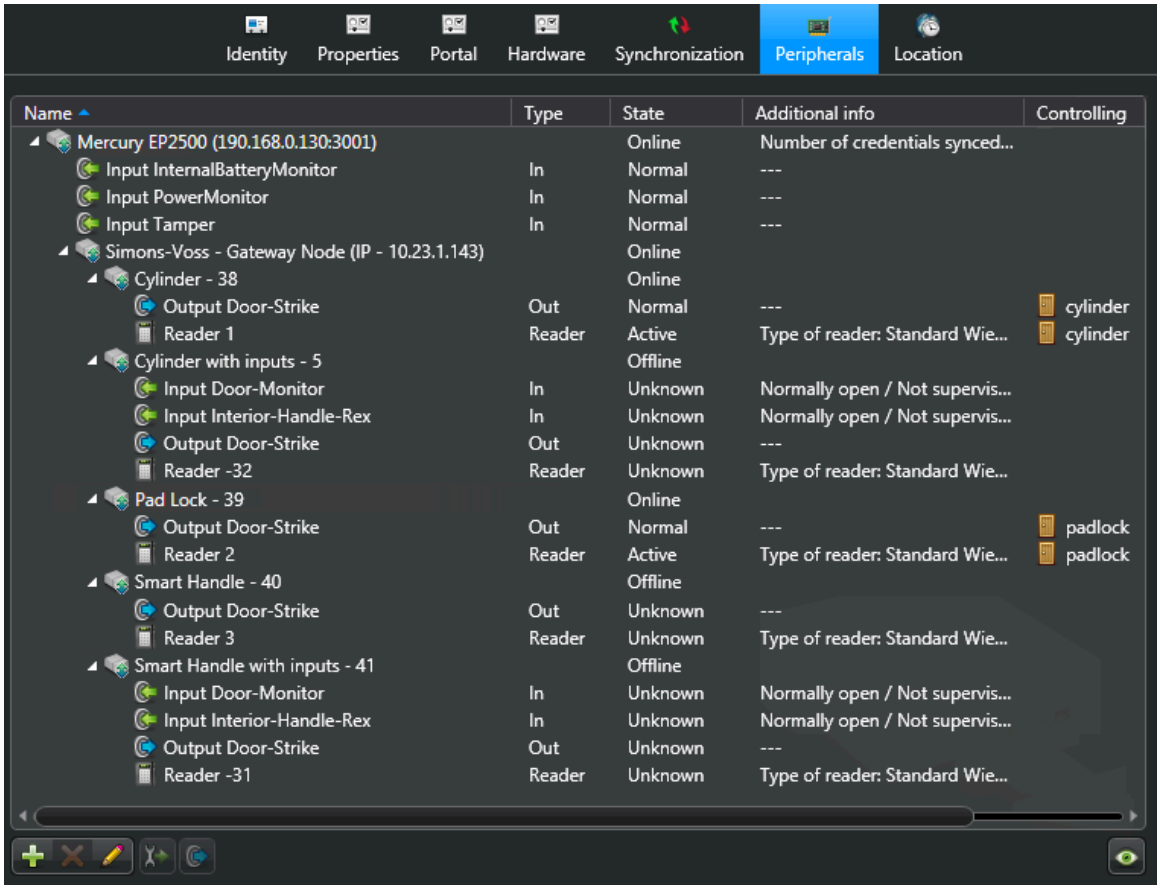
c) Click **OK**.

d) Repeat if you have more locks to add.

e) Click **OK**.

7 Click **OK** > **Apply**.

The Mercury controller with all its connected downstream panels and peripheral devices are listed on the *Peripherals* page.



NOTE: Adding interface modules to the Synergis unit causes the unit to perform a software restart. During this process, the Synergis unit and all peripherals attached to it are displayed in red.

8 Test your configuration by triggering the outputs.

The triggered output changes state in real time on screen.

NOTE: Reader activities are not shown on the *Peripherals* page.

16

SALTO SALLIS wireless locks

This section includes the following topics:

Enrolling SALTO SALLIS locks

For the Synergis™ unit to communicate with SALTO SALLIS locks, you must enroll them in Security Center, using the Synergis™ Appliance Portal.

Before you begin

Set up your SALTO SALLIS infrastructure (routers, nodes, and wireless locks) according to the instructions found in the *SALLIS Installation & Maintenance Guide*.

First define the nodes and the doors using the SALLIS application, and then update the routers and initialize the locks using the PPD (Portable Programmer Device). As you do this, write down the following information:

- **IP router:** IP address and port number.
- **RS-485 router:** Synergis unit channel the router is connected to (1 - 4).
- **Lock:** Router, lock ID, and the door where it is installed.

  Use descriptive door names, for example *First floor storage room*. If you have already created the door entities in Security Center, use the same names for ease of reference.

What you should know

The steps and instructions tagged with *Hardening* are optional, but will protect your system against cyberattacks.

Procedure

1 Log on to the Synergis Cloud Link unit.

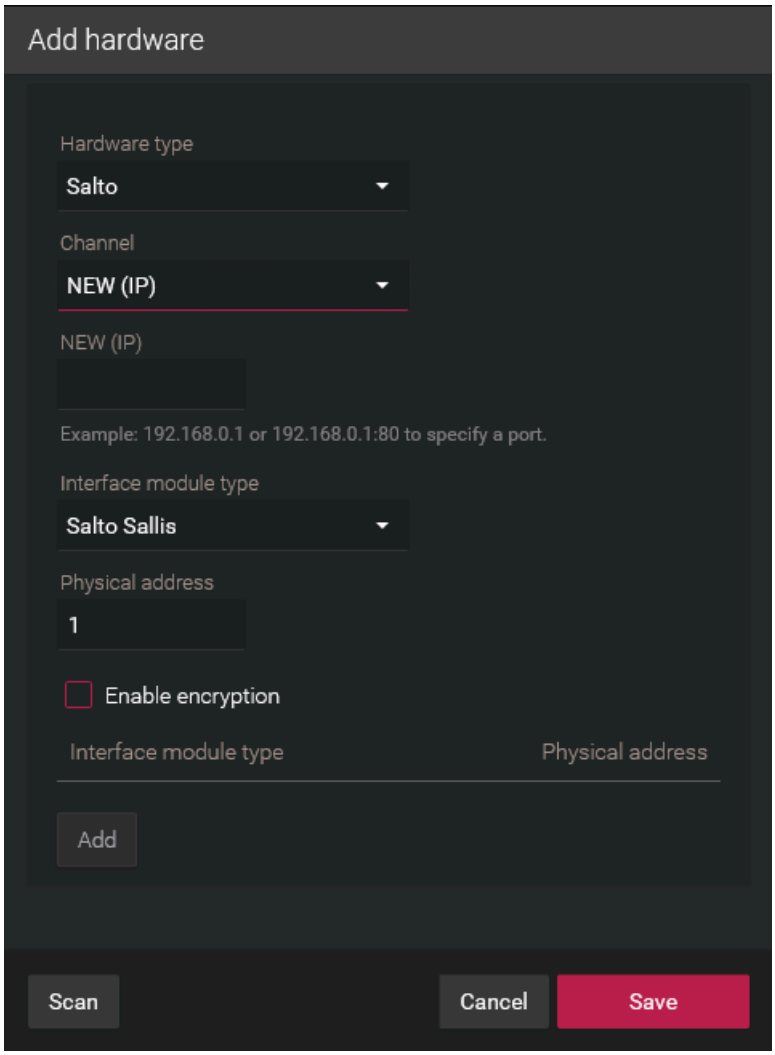
2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** (➕).

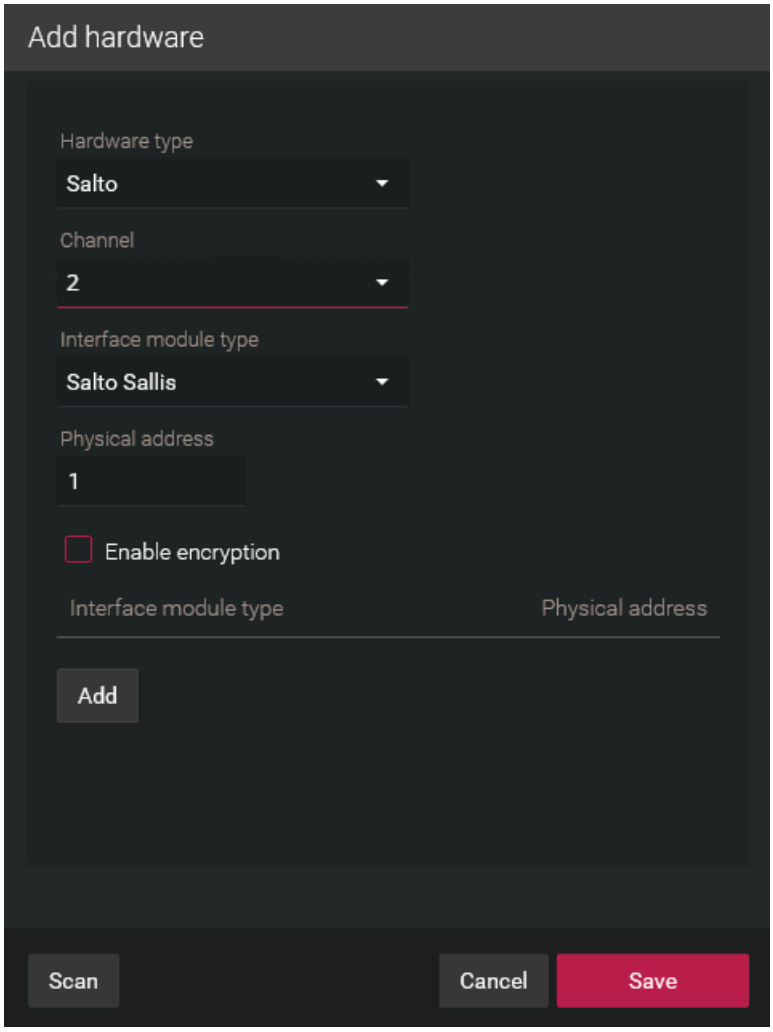
4 In the *Add hardware* dialog box, select **Salto** as the **Hardware type**.

5 Identify the channel where the SALLIS router is connected, and then do one of the following:

- Select the IP channel, and enter the IP address and port number used by the router.

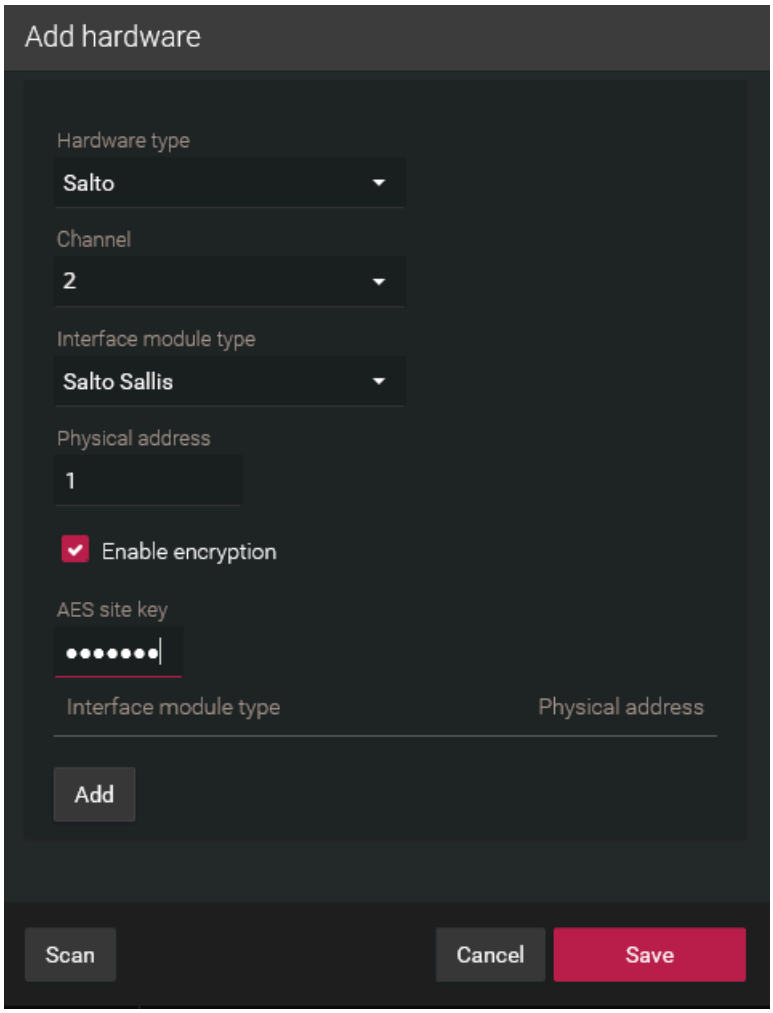


- Select an RS-485 channel (1 - 4). All interface modules connected to the same RS-485 channel must be from the same manufacturer.


Add hardware
Hardware type
Salto
Channel
2
Interface module type
Salto Sallis
Physical address
1
Enable encryption
Interface module type
Physical address
Add
Scan
Cancel
Save

6 (Hardening) If you want encryption, select **Enable encryption**, and enter the **AES site key**.

NOTE: You cannot change the encryption settings from the *Add hardware* dialog box on an existing channel. To enable encryption when the channel is already created, change the channel configuration in the Synergis™ Appliance Portal.



7 In the same dialog box, add all interface modules connected to the same channel.

You can enroll the interface modules automatically or manually.

TIP: If you know your lock IDs (physical addresses) and you only have a few to enroll, it is faster to enroll them manually.

- To enroll automatically, click **Scan**.

  The scan feature finds and enrolls all interface modules from the same manufacturer that are connected to the same channel.

  If the controller does not find all connected interface modules, make sure they all have a different physical address.

- To enroll manually, enter the lock ID as the **Physical address**, and click **Add** (➕).

  NOTE: Valid lock IDs are 1 - 16 for RS-485 routers, and 1 - 64 for PoE routers.

  Repeat as necessary to configure all wireless locks connected to the same channel.

8 Click **Save**.

The hardware type, channel, and interface module you just added are listed on the *Hardware configuration* page.

9 Test your interface module connection and configuration from the *I/O diagnostics* page.

After you finish

Associate your doors to the SALLIS locks in Security Center.

Enabling encryption on an existing SALLIS router

Encryption is a channel property in the Synergis™ Appliance Portal. You can enable the encryption or change the encryption password on a SALLIS router by changing the channel configuration in the Synergis™ Appliance Portal.

What you should know

You cannot change the channel settings while adding a lock to an existing channel. After the channel is created, all changes to the channel properties must be made from the channel property page. After encryption is enabled, you cannot disable it by disabling it in the Synergis™ Appliance Portal. You also need to disable the encryption by connecting directly to the router.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 Select the SALTO channel.

4 Select the **Enable encryption** option, and enter the **AES site key**.

5 Click **Save**.

Disabling encryption on a SALLIS router

To disable encryption on a SALLIS router, you need to disable it in both the Synergis™ Appliance Portal and on the router itself.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** (➕).

4 Select the SALTO channel, and then clear the **Enable encryption** option.

5 Click **Save**.
In the device tree, all SALLIS locks under the selected channel appear in red (inactive).

6 For an RS-485 router, do the following:
   a) Using the SALLIS application, download the router configuration to the PPD.
   b) On the PPD, select **Update router**.
   c) Connect the PPD to the router.

7 For a PoE router, do the following:
NOTE: If you have many routers to update, update them one at a time.
   a) Open the PoE router cover, and press and hold the **CLR** button for 5 seconds.
   The LED on the PoE router board turns orange.
   b) Using a web browser, connect to the web portal of the router.
   Enter http://192.168.0.234 in the browser URL field.
   NOTE: Your workstation must be on the same subnet as the router for you to connect to its web portal.
   c) On the browser page, under **Router encryption** > **Return to Plain mode?**, select **Yes**.
   d) Click **Send**.

The message *Configuration successfully sent* is displayed in the browser. In the device tree, all SALLIS locks under the selected channel are displayed in black (active).

17

OSDP devices connected to the Synergis Cloud Link RS-485 ports

This section includes the following topics:

Creating a channel to configure OSDP devices in the Synergis Appliance Portal

OSDP devices, such as secure I/O modules and readers, must have their RS-485 bit rate and address configured before they can be used. To configure your readers in the Synergis™ Appliance Portal, you must create an OSDP channel with Programming mode enabled.

What you should know

- For OSDP readers that you want connected to a Mercury unit: Instead of using a configuration card to set the reader's baud rate and physical address, you can follow this procedure, and then set the reader's physical address in the Synergis Appliance Portal.
- When Programming mode is enabled, you can only have one online reader connected to the RS-485 channel at a time.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ().

4 In the *Add hardware* dialog box, select **OSDP** as the **Hardware type**.

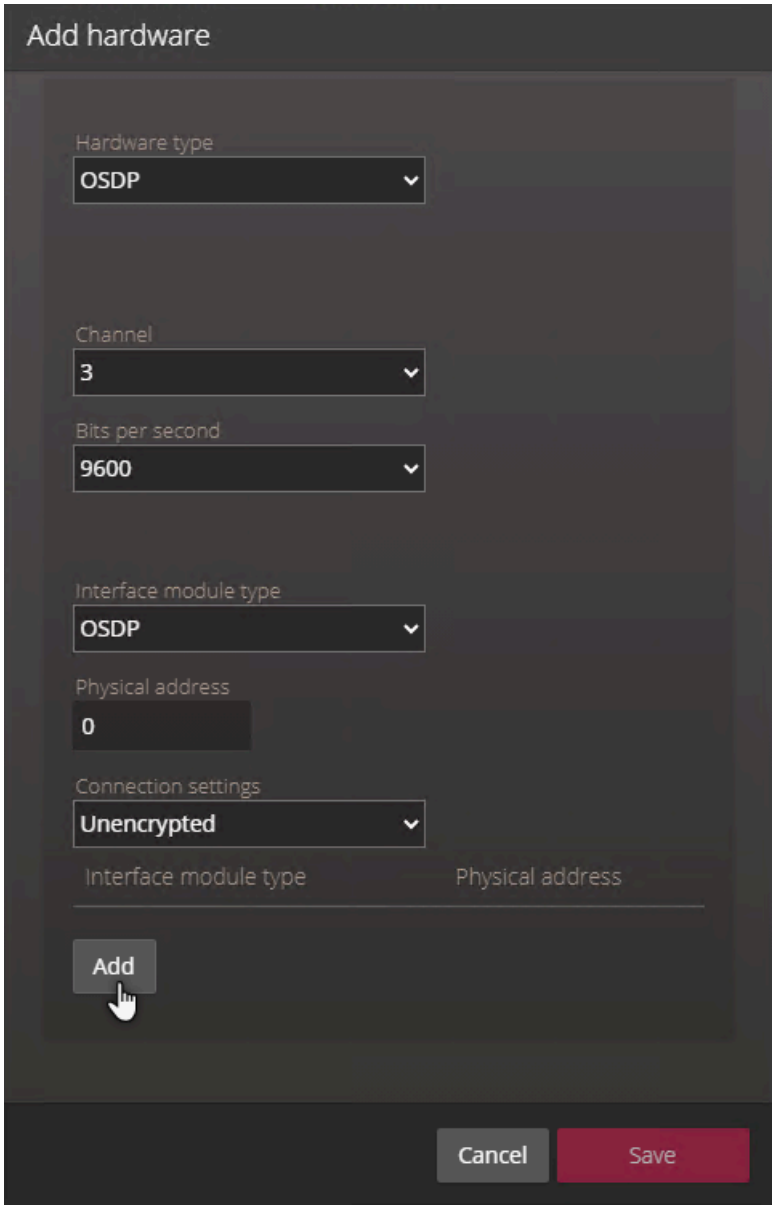
5 Select the **Channel** (1 - 4).

NOTE: If you have the Synergis Cloud Link 312 unit, then you have up to 12 channels. For more information, see About the Synergis Cloud Link 312 RS-485 ports.

6 From the **Bits per second** list, select the bit rate you want to configure for your device.

NOTE: Select **Other** from the list to enter a custom bit rate.

7 Under **Interface module type**, click **Add**.

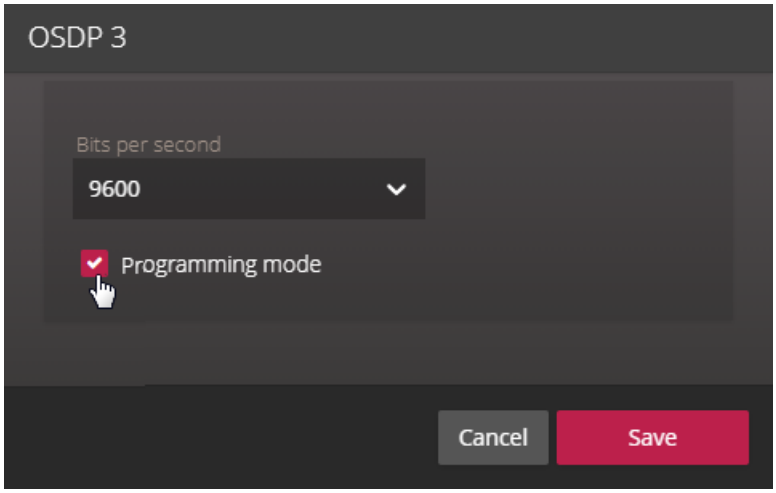


8 Click **Save**.
The channel and interface are created.

9 From the hardware tree, select the OSDP channel you created and click **Edit** ( ).

10 If you're adding a reader, select the **Programming mode** checkbox.

If you have a configuration card, you can use it instead of **Programming mode**. See the documentation that came with your card.



11 Click **Save**.

After you finish

- Configure supervised inputs on the secure I/O modules.
- Configure the OSDP readers.

Configuring supervised inputs on secure I/O modules

To configure a supervised input on a secure I/O module, you must first configure the input as **4 state supervised** in Config Tool, then configure the resistance values on the *Hardware* page of the Synergis™ Appliance Portal.

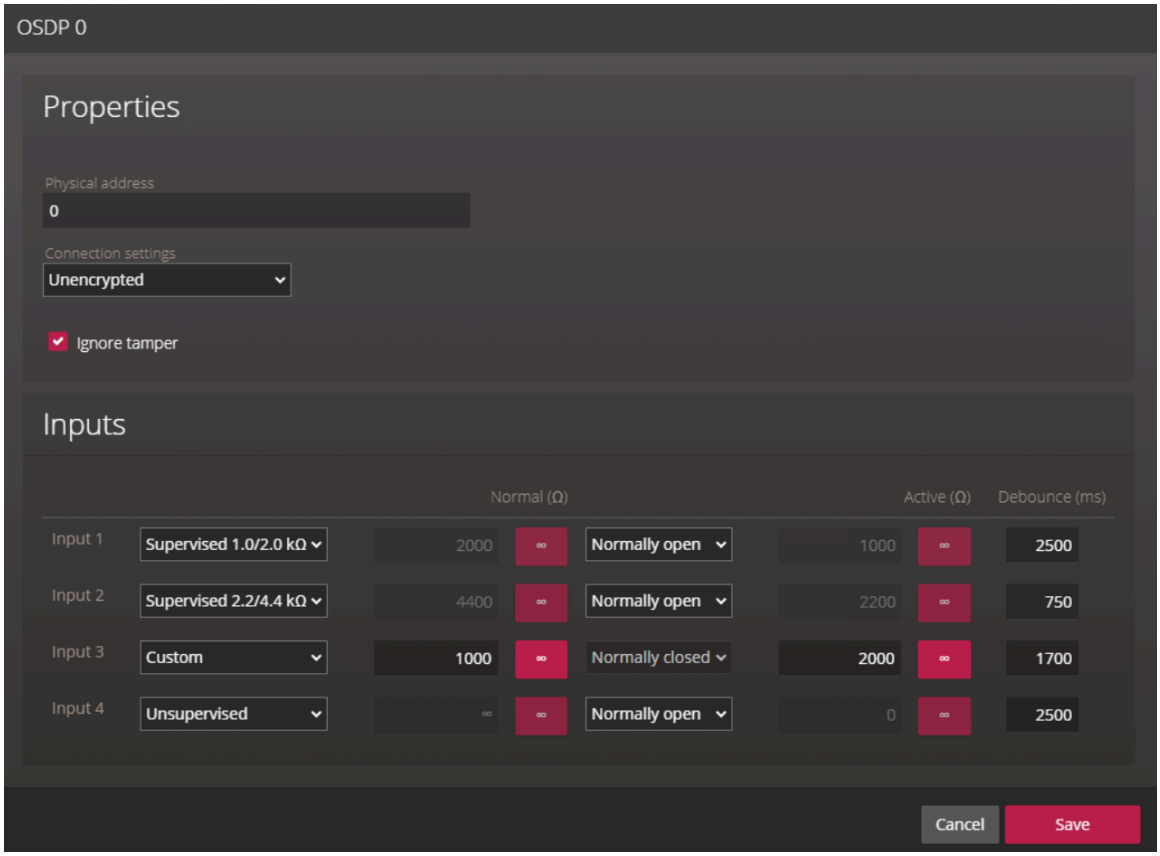
Before you begin

Create an OSDP channel.

Procedure

1 From the hardware tree, select the secure I/O module you added while creating the OSDP channel and click **Edit** ( ).

2 In the *Properties* dialog box, enter the **Physical address** for the module.



3 In the *Inputs* section, configure the supervised inputs with their correct resistance values.

4 (Optional) In the *Debounce (ms)* column, enter a value in milliseconds up to 600,000 (10 minutes) for the inputs.

The option indicates the amount of time an input can be in a changed state (for example, changed from *Active* to *Normal*) before the state change is reported. The option filters out false events from unstable input signals. The default value is 0 milliseconds.

The following are examples of events that are affected:

- *Input state changed: Input active*
- *Input state changed: Input normal*
- *Input state changed: Input trouble*
- *Door opened*
- *Request to exit*
- *AC fail*
- *Battery fail*

5 Click **Save**.

Configuring and adding OSDP readers in the Synergis Appliance Portal

To add OSDP readers to a Mercury or Synergis™ unit, configure the readers using the Synergis™ Appliance Portal.

Before you begin

Create an OSDP channel with Programming mode enabled.

What you should know

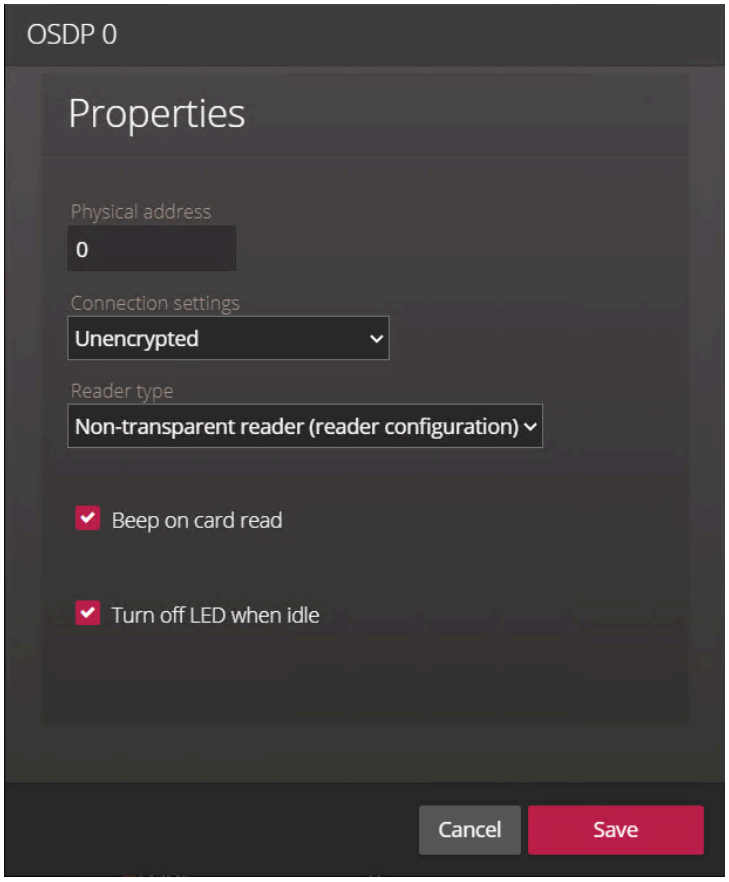
- All readers connected to the same RS-485 channel must be set with different addresses.
- Before connecting OSDP readers to a Mercury unit, you might need to set the reader's baud rate and reader address. Setting the baud rate in Synergis Appliance Portal, and then following this procedure replaces using a configuration card.
- When Programming mode is enabled, you can only have one reader connected to the RS-485 channel at a time.

BEST PRACTICE: If you are installing OSDP readers on adjacent turnstiles, it is not recommended to connect more than two readers to the same RS-485 channel, as it increases the controller's response time and the chance of two or more cards being presented at the same time is high. For conventional doors, you can install up to four readers per bus.

Procedure

1 From the hardware tree, select the OSDP reader you added while creating the OSDP channel and click **Edit** ( ).

2 In the *Properties* dialog box, enter the physical address you want to set for the reader, and configure the **Beep on card read** and **Turn off LED when idle** options, as desired.



3 Click **Save**.

4 Connect and power up the reader.

The configured bit rate and physical address are sent to the reader, which comes online after it has accepted them.

5 Disconnect or power down the reader.

6 Repeat steps 1 - 5 for the remaining readers.

7 From the hardware tree, select the OSDP channel and click **Edit** ( ), then clear the **Programming mode** checkbox that you selected while creating the channel.

8 Add the configured readers:

a. At the top of the *Address* column, click **Add** ( ).

b. In the *Add hardware* dialog box, click **Add** to add the readers at the addresses you have programmed.

9 Click **Save**.

After you finish

Enable secure mode on the readers.

Configuring phg secure I/O modules to ignore tamper events

The tamper detection switch on top of the phg secure I/O module triggers tamper events continuously when the module is installed without its cover. To prevent this, you can configure the phg secure I/O module to suppress tamper inputs, so that tamper events are ignored in Security Center.

Before you begin

Create an OSDP channel.

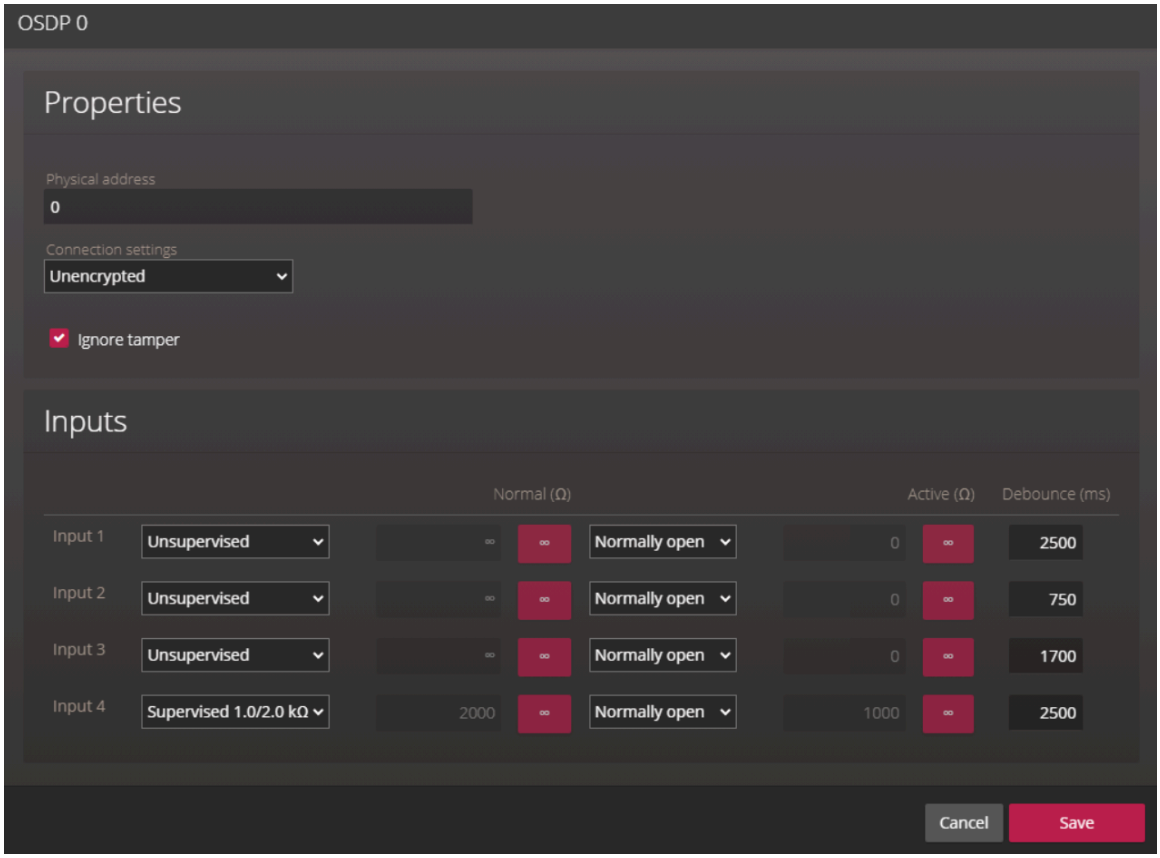
What you should know

The **Ignore tamper** option can only be configured after the module is enrolled, not during enrollment.

Procedure

1 From the hardware tree, select the phg secure I/O module you added while creating the OSDP channel and click **Edit** ( ).

2 In the *Properties* dialog box, select the **Ignore tamper** option.



3 Click **Save**.

Enabling secure pairing on OSDP readers in the Synergis Appliance Portal

By default, OSDP readers are enrolled in an unencrypted state. Enabling secure pairing increases access-point security.

Before you begin

Configure the OSDP readers.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 From the hardware tree, select the OSDP reader and click **Edit** ( ).

4 From the **Connection settings** list, select **Encrypted**.

5 From the **OSDP Secure Channel key** list, select one of the following:

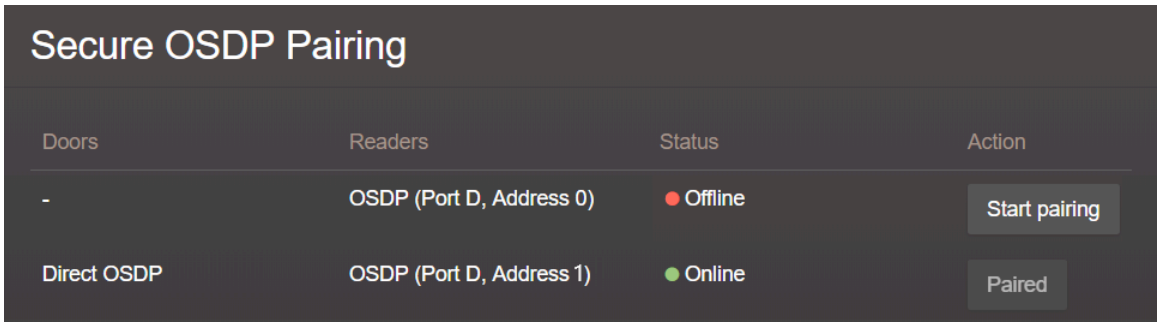
- **Random key:** Generates a random 128-bit (32 hexadecimal characters) key.
- **Default key:** Uses the unit's default key. This choice is less secure.
- **Specific key:** This choice lets you specify your own 128-bit (32 hexadecimal characters) key.

6 Click **Save**.

7 Click **Configuration** > **Advanced OSDP**.

8 Find the row with the configured port, reader, and associated door, and click **Start pairing**.

This exchanges the keys, and the reader come back online. The reader is now secure. Any reader that rejects the key stays offline.



Enabling MIFARE DESFire for transparent OSDP readers

OSDP readers in transparent mode require you to store the keys on your Synergis™ Cloud Link unit, or on secure access module (SAM) cards if you have the Synergis Cloud Link 312 model.

Before you begin

Configure the MIFARE DESFire keys on your Synergis Cloud Link unit.

What you should know

Card or PIN mode isn't supported with OSDP readers configured in DESFire mode (transparent mode).

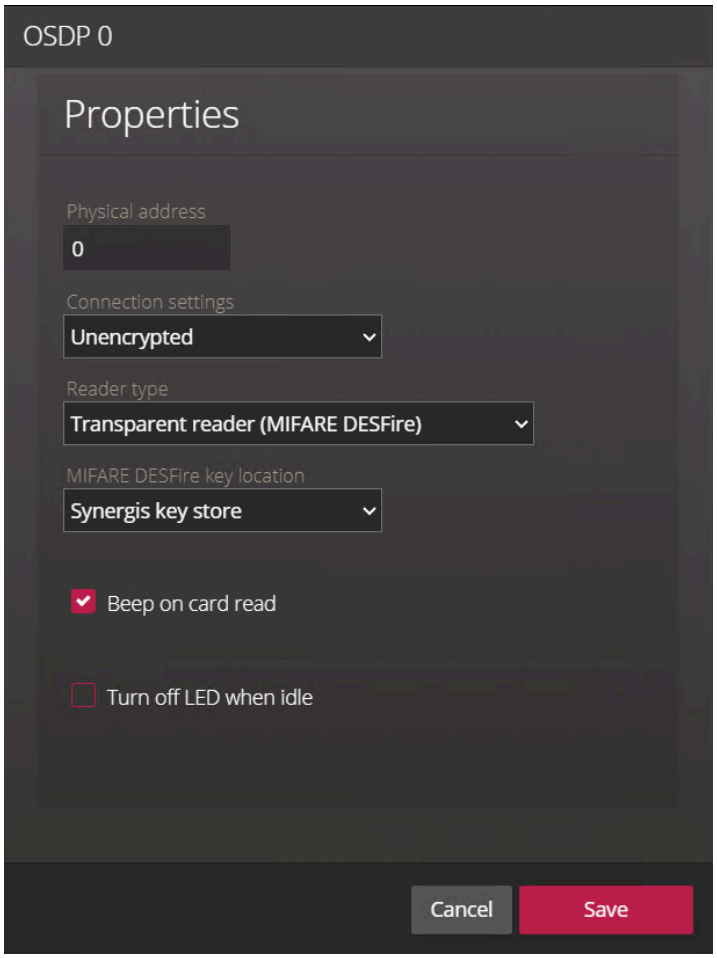
Procedure

1 Log on to the Synergis Cloud Link unit.

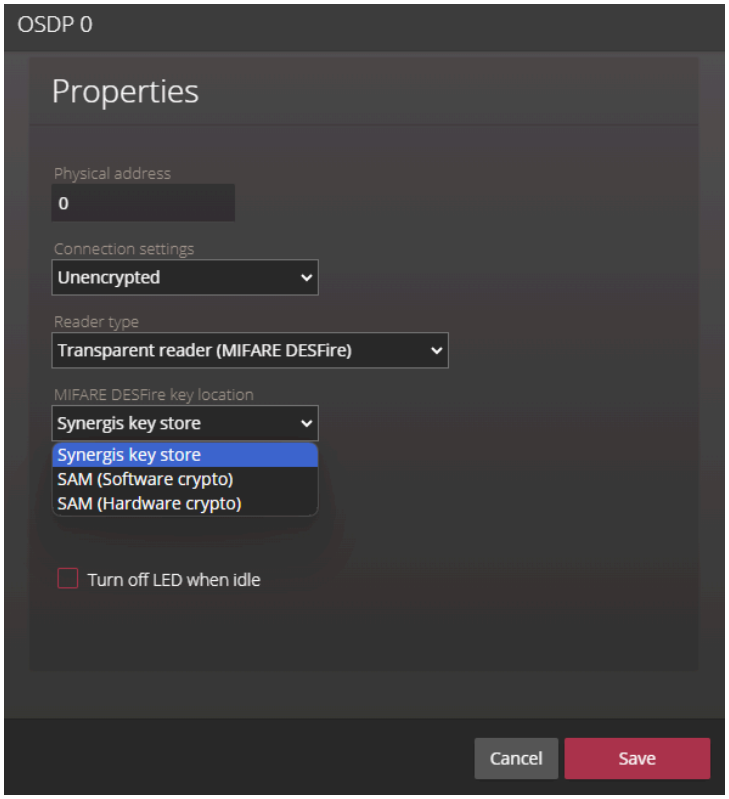
2 Click **Configuration** > **Hardware**, and then select an enrolled OSDP reader.

3 Click **Edit** ( ) for the selected reader's interface.

4 From the **Reader type** list, select **Transparent reader (MIFARE DESFire)**.



5 From the **MIFARE DESFire key location** list, select one of the following:



- **Synergis key store:** The key for decrypting credentials is stored on the Synergis unit. This option doesn't require a SAM card.
- **SAM (Software crypto):** This is the faster of the SAM options, but requires the **SessionDumpKey** option to be enabled during the SAM configuration process. For more information, see the documentation that came with your SAM card configuration software.
- **SAM (Hardware crypto):** This option doesn't require **SessionDumpKey** to be enabled during the SAM configuration process.

NOTE: The SAM options are only available if you have the Synergis Cloud Link 312 model.

6 Click **Save**.

7 If you selected the **Synergis key store** option, use the Synergis™ Appliance Portal to access the *Synergis key store* and enter the keys:

a. Select an index.

b. Click **Create new version**, and enter a 32-character hexadecimal key in the text field.

c. Click **Add**.

The MIFARE DESFire configuration file used for the indexed keys is compatible with both software-transparent and non-transparent readers.

Limitation: There are two limitations with software-transparent readers:

- Transparent readers currently can't encode cards.
- Cards with transparent mode enabled take about 100 ms longer to read.

After you finish

Configure MIFARE DESFire.

Related Topics

About Synergis Cloud Link 312 on page 6

Configuring OSDP readers to prevent relay attacks

Prevent relay attacks on supported OSDP readers by configuring a maximum delay for card authentication.

What you should know

During a relay attack, it takes longer than normal for the system to authenticate a card because the attackers must relay messages to each other in the middle. For this reason, relay attacks can be effectively prevented by setting a maximum delay for card authentication. When the maximum delay is exceeded during a card read, the Synergis™ Cloud Link unit does not proceed to make an access decision, and the door remains locked.

NOTE: No *Access denied* event is generated when the maximum delay is exceeded.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **MIFARE DESFire**.

3 In the *Readers and associated MIFARE DESFire configurations* section, select the **Proximity Check** option beside one or more OSDP readers.

4 For each reader with **Proximity Check** enabled, enter a value in milliseconds to define the maximum card authentication delay in the **ms** field.

TIP: Relay attack prevention is enabled per reader. Since each reader's timing is different, determine the average time that the reader takes to authenticate a legitimate badge and add a small margin of error to calculate the maximum delay. The suggested margin of error is 40 milliseconds.

To determine how long a card took to be authenticated, go to **Maintenance** > **Log viewer**. In the **Logger** drop-down, select **Syslog**, and in the **Filter by regex** field, enter `SmartCard`. Check the logs with the *SmartCard* prefix for the authentication time.

5 Click **Save**.

Transferring files to OSDP devices in the Synergis Appliance Portal

You can upgrade the firmware or configuration of OSDP devices by transferring files to the devices in the Synergis™ Appliance Portal.

What you should know

- The following procedure only applies to OSDP devices, such as secure I/O modules and readers, that connect directly to the Synergis™ Cloud Link unit.
- Use the firmware and configuration files provided by your manufacturer.

Procedure

1 Log on to the Synergis Cloud Link unit.

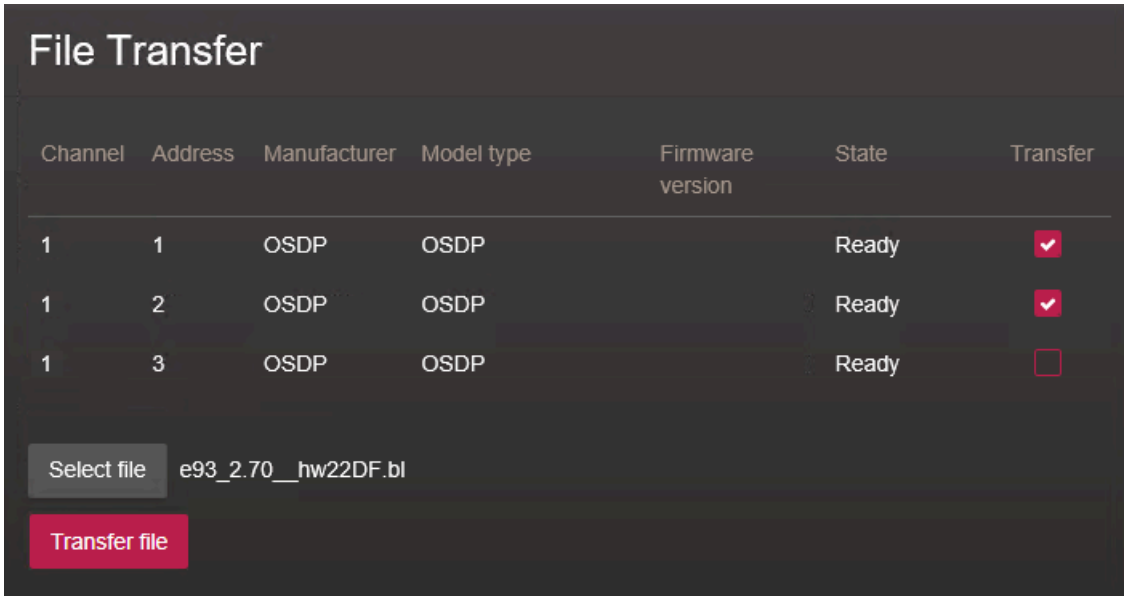
2 Click **Configuration** > **Advanced OSDP**.

3 In the *File transfer* section, select the checkbox in the **Transfer** column of the devices to which you want to transfer the file.

4 Click **Select file**.

5 In the file browser, select the firmware or configuration file, and click **Open**.

6 Click **Transfer file**.



The firmware or configuration is applied after the selected devices restart.

18

STid readers using the SSCP protocol

This section includes the following topics:

Configuring and enrolling STid readers that use the SSCP protocol

For the Synergis™ unit to communicate with the STid readers connected to it, you must configure and enroll the readers in the Synergis™ Appliance Portal.

Before you begin

Make sure your STid reader firmware is up to date and supported by Synergis™ Softwire.

What you should know

If you're installing STid readers on adjacent turnstiles, it's not recommended to connect more than two readers to the same RS-485 channel because it increases the controller's response time and the chance of two or more cards being presented at the same time is high. For conventional doors, you can install up to four readers per bus.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Configuration** > **Hardware**.

3 At the top of the **Hardware** column, click **Add** ( ).

4 In the *Add hardware* dialog box, select **SSCP** as the **Hardware type**.

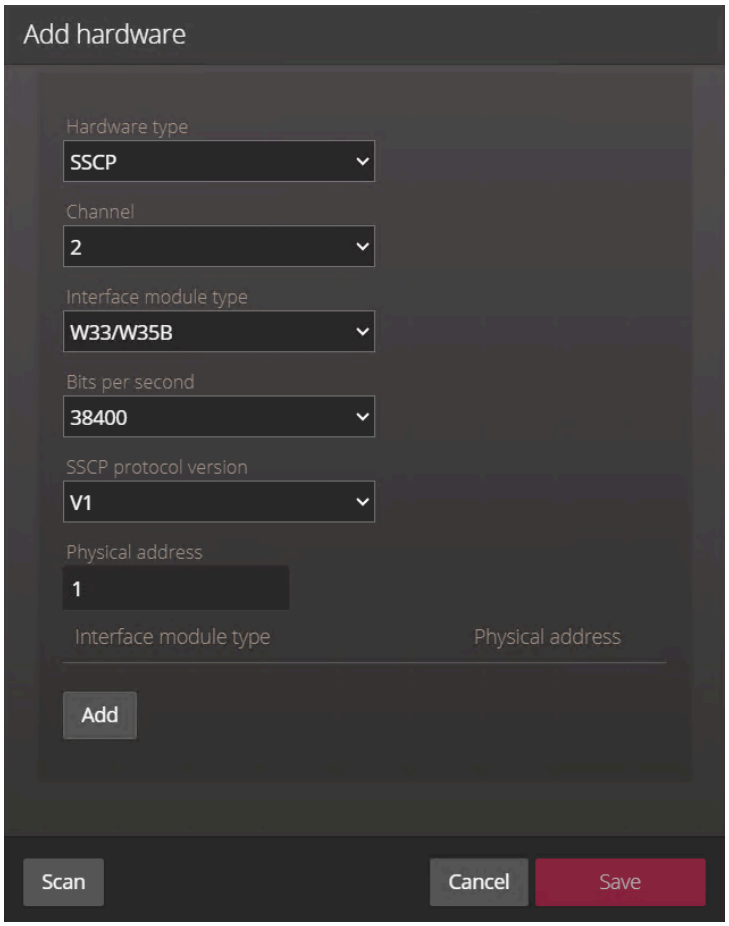
5 Select the **Channel** (1 - 4).

NOTE: If you have the Synergis Cloud Link 312 unit, then you have up to 12 channels. For more information, see About the Synergis Cloud Link 312 RS-485 ports.

6 Under **SSCP protocol version**, select either **V1** or **V2**, depending on which protocol the reader supports.

7 Set the **Bits per second** and **Physical address** (1 - 127).

The **Bits per second** rate is a channel property, and follows the bit rate of the last interface module added to the channel. The default bit rate is 38,400 bps. Higher bit rates improve card read time at the cost of maximum wiring distance.



8 Click **Add**.

The port, bit rate, and physical address for the reader are configured in Synergis Softwire.

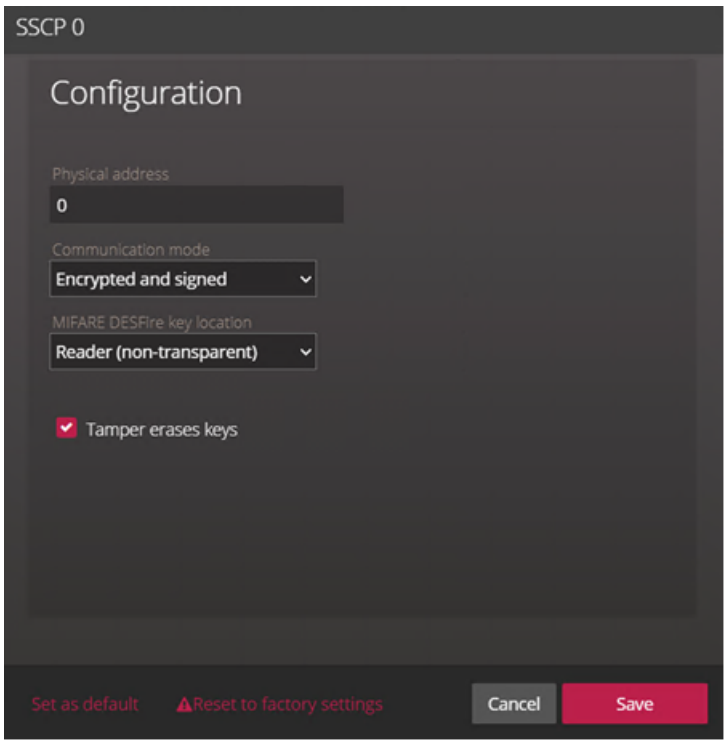
9 (Optional) If you're using the **V1** protocol version, select a communications mode:

a) Select the reader at the address you configured and click **Edit** ( ).

b) From the **Communication mode** list, select a mode:

- *Plain* (default mode)
- *Encrypted* (private communications)
- *Signed* (authenticated communications)
- *Encrypted and signed* (both private and authenticated communications)

NOTE: If you're using **V2**, then only the **Encrypted and signed** option is available.



The **Tamper erases keys** option is active by default, and erases all on-board keys if the unit is tampered with.

c) Click **Save**.

10 From the hardware tree, select the interface you configured and click **Edit** ( ).

11 In the dialog box that opens, select the **Programming mode** checkbox and click **Save**.
The system programs the reader with your physical address and bit rate configuration.

12 Select the interface and click **Edit** ( ).

13 Clear the **Programming mode** checkbox and click **Save**.

14 Repeat the procedure to add the remaining readers one at a time, and one reader per port.
NOTE: If you're adding multiple readers to one port, use a free port to configure them one by one before connecting them to their target port.

15 Test your interface module connection and configuration from the *I/O diagnostics* page.

After you finish

BEST PRACTICE: *(Hardening)* Changing the default encryption keys provided by the manufacturer enhances security.

Enabling transparent mode on STid readers that use the SSCP protocol

MIFARE DESFire readers require cryptographic keys to access a card's secured credential. When readers are configured to run in transparent mode, these keys are loaded into the Synergis™ key store or a secure access module (SAM) card.

Before you begin

The door must have a STid reader with a part number ending in AA or AD.

NOTE: Transparent STid readers with part numbers ending in BB can't be used in this scenario. For a list of readers that can be used as transparent readers, see Supported STid readers that use the SSCP protocol.

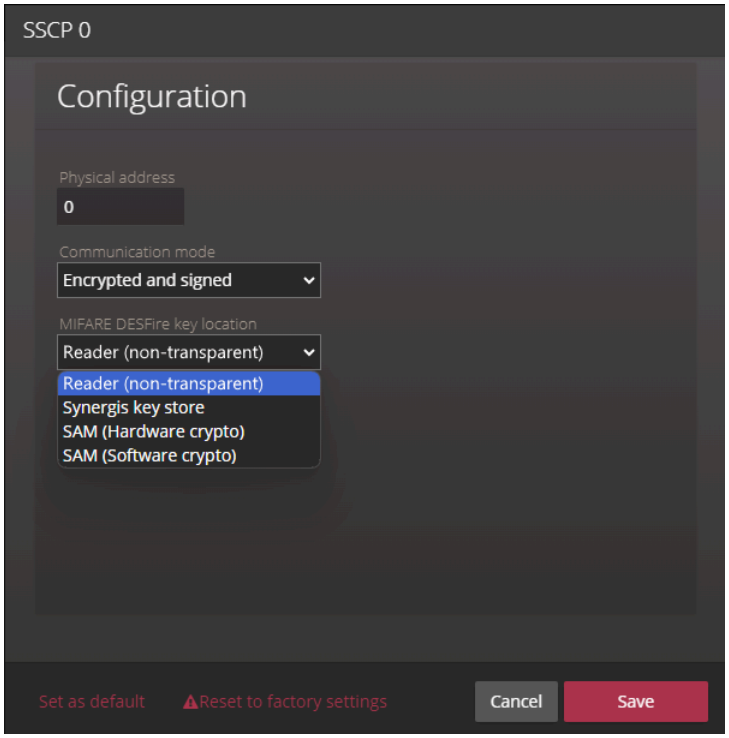
Procedure

1 Log on to the Synergis™ Cloud Link unit.

2 Click **Configuration** > **Hardware**, and then select **SSCP**.

3 Click **Edit** ( ) on the reader's interface.

4 In the reader configuration dialog box, from the **MIFARE DESFire key location** list, select one of the following:



- **Reader (non-transparent):** Used for when the information to retrieve the credential is stored directly on the reader.
- **Synergis key store:** The key for decrypting credentials is stored on the Synergis unit. This option does not require a SAM card.
- **SAM (Software crypto):** This is the faster of the SAM options, but requires the **SessionDumpKey** option to be enabled during the SAM configuration process. For more information, see the documentation that came with your SAM card configuration software.
- **SAM (Hardware crypto):** This option does not require **SessionDumpKey** to be enabled during the SAM configuration process.

NOTE: The SAM options are only available if you have the Synergis Cloud Link 312 model.

5 If you select the **Synergis key store** option, use the Synergis™ Appliance Portal to access the Synergis key store and enter the keys:

a. Select an index.

b. Click **Create new version**, and enter a 32-character hexadecimal key in the text field.

c. Click **Add**.

The MIFARE DESFire configuration file used for the indexed keys is compatible with both software-transparent and non-transparent STid readers.

Limitation: There are two limitations with software-transparent readers:

- Transparent readers currently can't encode cards.
- Cards with transparent mode enabled take about 100 ms longer to read.

After you finish

The 32 available indexed keys in the Synergis key store increase security by enabling the entry of keys in components. Clicking **Add** between components makes it possible for multiple stakeholders to each know only part of the required key.

Related Topics

About Synergis Cloud Link 312 on page 6

Changing the default RS-485 communication keys for STid readers that use the SSCP protocol

You can change the default signature and encipherment keys used for encrypted and signed communication with the STid readers.

Before you begin

Change the STid readers' factory-installed *Signature* and *Encipherment* keys for better security.

What you should know

Changing the default signature and encipherment keys involves changing the values for the *ReaderKs* and *ReaderKc* RS-485 keys on the reader and on the *Synergis key store* page in the Synergis™ Appliance Portal. The STid reader also offers the option of storing the keys in one of its onboard key indexes.

SSCP V2 readers only use the *ReaderKc* key.

NOTE: When using indexed keys, if a STid reader is tampered with, the door goes offline in Config Tool, then the reader's LED flashes orange. In that case, present the SKB card to load the RS-485 keys into the reader. When the keys are loaded, the reader comes back online (the LED is red).

Procedure

1 Log on to the Synergis unit.

2 Click **Configuration** > **Synergis key store**.

3 Apply the new encryption values, *ReaderKc* for the encipherment key and *ReaderKs* for the signature key.

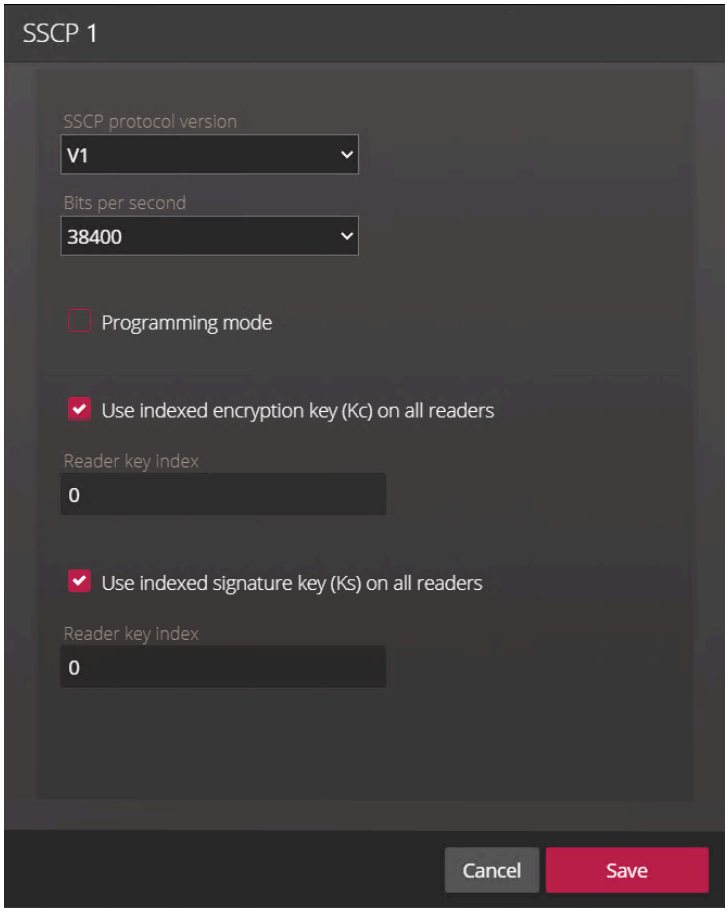
4 Configure the keys:

a) Click **Configuration** > **Hardware**, and then select **SSCP**.

b) Click **Edit** ( ) on the reader's channel.

c) If the *ReaderKc* and *ReaderKs* keys were configured on the reader, leave the **Use indexed encryption key (Kc) on all readers** and **Use indexed signature key (Ks) on all readers** check boxes cleared. If the reader uses indexed signature and encipherment keys, select the **Use indexed encryption key**

(Kc) on all readers and **Use indexed signature key (Ks) on all readers** check boxes, and then enter the proper values for the key indexes.



5 For readers using indexed keys, present the SKB card to load the RS-485 keys into the reader.

Configuring STid readers that use the SSCP protocol to prevent relay attacks

Prevent relay attacks on supported STid readers by enabling the system to detect delays in the RF communication exchanges between cards and readers, and reject access requests from the cards that take too long to communicate.

Before you begin

- This procedure only applies to STid readers that are using the SSCP or SSCP V2 protocol and running firmware v21 or later.
- Enable DESFire EV2 secure messaging.

What you should know

A relay attack uses two malicious devices to relay messages between a reader and a card, allowing attackers to access doors without needing the card physically near the reader. In such scenarios, the system takes longer than normal to authenticate a card because the attackers must relay messages to each other in the middle.

Enabling a proximity check on STid readers ensures that only access requests from cards that fall within a configured time threshold are granted.

Procedure

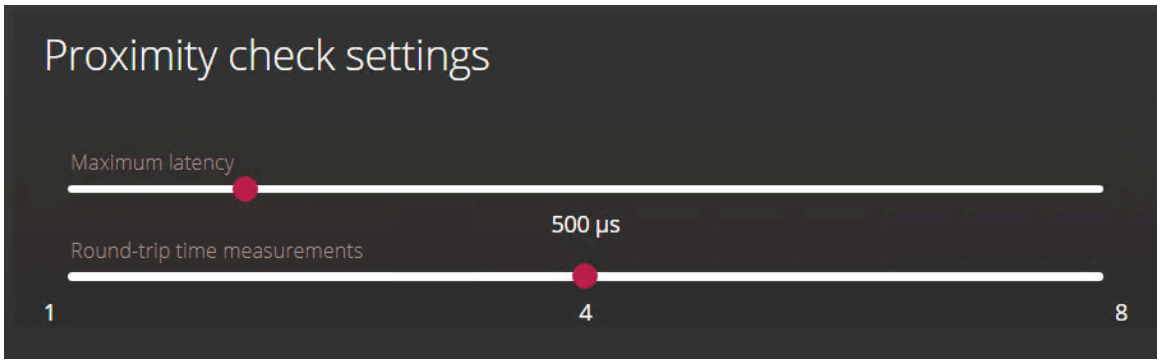
1 Log on to the Synergis™ Cloud Link unit.

2 Click **Configuration** > **MIFARE DESFire**.

3 In the *Readers and associated MIFARE DESFire configurations* section, select the **Proximity Check** option beside one or more STid readers.

4 (Optional) In the *Proximity check settings* section, configure the following:

NOTE: It is recommended to keep the default settings. Lowering the maximum latency can cause certain cards to fail the proximity check. Increasing the maximum latency can increase the chance of a relay attack succeeding.



- **Maximum latency:** The threshold in microseconds of an exchange between the card and the reader. The default value is 500 microseconds.
- **Round-trip time measurements:** The number of exchanges between the reader and the card used to calculate whether the card read is valid. Each exchange must not exceed the configured **Maximum latency**.

5 Click **Save**.

Example

If the **Round-trip time measurements** is set to four, then when a reader with the **Proximity Check** setting enabled receives an access request, a proximity check is run, according to the configuration in the *Proximity check settings* section. The proximity check calculates the duration of an exchange between the card and the reader four times.

The proximity check results in one of the following:

- If the time calculated for each of the four exchanges falls within the **Maximum latency**, the card succeeds the proximity check. The Synergis Cloud Link unit proceeds to grant or deny access based on the access rights of the card, and the door unlocks or remains locked accordingly.
- If at least one of the exchanges takes longer than the **Maximum latency**, the card fails the proximity check. The Synergis Cloud Link unit does not proceed to make an access decision, and the door remains locked.

  NOTE: No *Access denied* event is generated when a proximity check fails.

Part IV

Maintenance and troubleshooting

This part includes the following chapter:

19

Maintenance and troubleshooting for Synergis Cloud Link units

This section includes the following topics:

Viewing system information on the Synergis Cloud Link unit

You can view the Synergis™ Cloud Link unit's status and configuration files for troubleshooting purposes.

Procedure

1 Log on to the Synergis Cloud Link unit.
2 Click **Maintenance** > **System status**.
3 Click **Unit** to view the unit's hardware and firmware information.
4 Click **Network** to view the unit's network configuration and status.

After you finish

Download the unit configuration files.

Information about your Synergis Cloud Link unit

The *Unit* tab on the *System status* page of the Synergis™ Appliance Portal shows information about the Synergis™ Cloud Link unit's hardware and firmware.

Property name	Property value
Hostname	Hostname of the Synergis Cloud Link unit. The default hostname is the letters "SCL" followed by the unit's MAC address. The MAC address is the first address on the label sticker on the unit. For example, if the label says 0010F32CF482, then the default hostname is SCL0010F32CF482.
Hardware type	Genetec Synergis appliance
Product type	Synergis Cloud Link G2
Firmware version	The version of the Synergis Cloud Link firmware running on the unit.
Synergis Softwire version	The version of Synergis Softwire that is bundled in the Synergis Cloud Link firmware.
Build date	The date when the firmware was built.
Upgrade date	The date when the firmware was upgraded to the current version.
RAM	The used RAM and the total RAM.
Storage	The used storage and the total storage.
Internal temperature	The internal temperature of the unit. When the upper or lower temperature thresholds are crossed, this value turns red and a warning is shown in the portal notifications. For more information, see Synergis Cloud Link specifications.
RTC battery voltage	The RTC battery level in volts. When the lower threshold is crossed, a warning is shown in the portal notifications and in Security Center.

Property name	Property value
Power source	The power source of the unit.
Runtime environment	Installed software framework version.
Discovery port	The discovery port used by Access Manager roles to communicate with this Synergis Cloud Link unit. **NOTE:** The IP address of the Access Manager must also be known to the Synergis unit for any communication to take place between the two.
System uptime	Time elapsed since the hardware was last restarted.
Service uptime	Time elapsed since the last software restart.
Currently connected Access Manager	IP address of the Access Manager that's managing this unit.
Offline log count	Number of logged events not yet synchronized with the Access Manager role when the unit is offline. Indicates zero when the unit is online. **NOTE:** These are generic events reported to the Access Manager. Not to be confused with the Synergis Cloud Link unit's own troubleshooting logs.
Number of configured channels	Number of communication channels that are configured with interface modules attached. The Synergis Cloud Link unit features two types of channels, IP and RS-485.
Serial number	The serial number of the unit.
Number of peers connected to this unit	Number of Synergis Cloud Link units connected to this unit as peers.
Unit time (local)	The local date and time.
Unit time (UTC)	The date and time in UTC.

Changing the logon password for the Synergis Cloud Link appliance

As a security best practice, regularly change the logon password for the Synergis™ Cloud Link appliance.

What you should know

- The new password must be at least 15 characters long, and should be unique and random. The **Save** button isn't displayed until the system determines the password strength to be *Strong* or *Very strong*.
- If the Synergis Cloud Link appliance was already enrolled in Security Center, it's recommended to change the password using the *Hardware inventory* task in Config Tool instead of the Synergis™ Appliance Portal. Security Center 5.10.1 is the minimum required version to do this.

  For more information, see Changing access control unit passwords in Config Tool.

Procedure

1 Log on to the Synergis Cloud Link appliance.

2 Click **Configuration** > **Users**.

3 On the *User configuration* page, select a user.

4 Enter the old password, and then enter and confirm the new password.

5 Click **Save**.

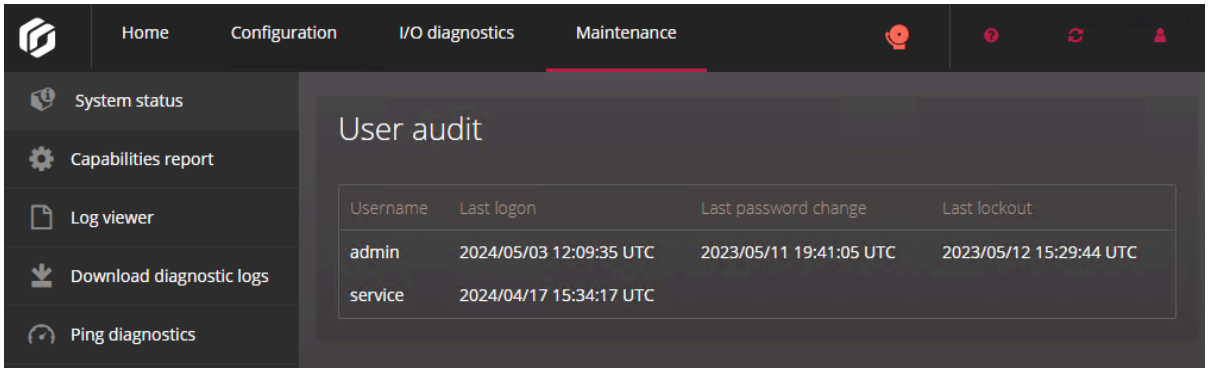
6 For appliances that were already enrolled in Security Center, change the password in Config Tool to synchronize the appliance with the Access Manager role it is connected to.

The new password is applied immediately.

Synergis Cloud Link user audits

To investigate activity of users in the Synergis™ Appliance Portal, you can view when users last logged on to the Synergis™ Cloud Link unit, when their password was last changed, and when they were last locked out after three failed login attempts.

Go to **Maintenance** > **System status** to find the *User audit* section. The timestamps for all user activity are in UTC.



Downloading the unit configuration file from your Synergis Cloud Link unit

You can download your Synergis™ Cloud Link unit's configuration as a compressed file to restore the configuration on a different unit during a unit replacement.

What you should know

The configuration file contains hardware settings, including supervised input values and RIO, and automation engine rules. The file does not include the unit's administrator password or Synergis key store data.

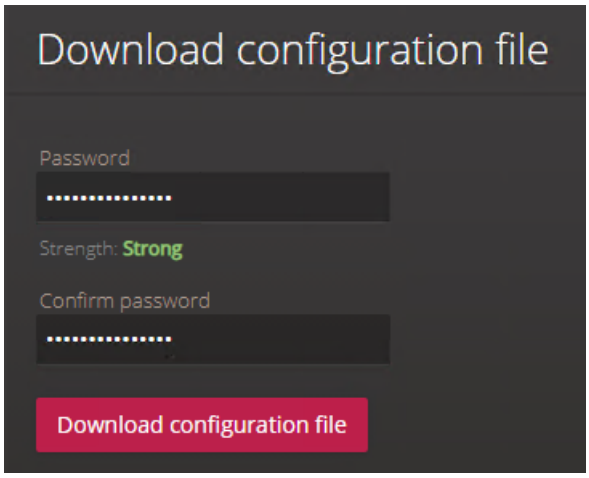
Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Maintenance** > **System status**.

3 In the *Download configuration file* section, enter a strong password and confirm the password.

NOTE: The password must be at least 15 characters long.



4 Click **Download configuration file**.

NOTE: This button remains disabled if the password is not strong enough or if the confirmation password does not match.

5 Click **Save**.

Uploading the unit configuration file for your Synergis Cloud Link unit

When replacing a Synergis™ Cloud Link unit, you can download the old unit's configuration file, and then upload it onto the replacement unit to restore the configuration.

Before you begin

Download the Synergis Cloud Link unit's configuration file.

What you should know

The configuration file contains hardware settings, including supervised input values and RIO, and automation engine rules. The file does not include the unit's administrator password or Synergis key store data.

Procedure

1 Log on to the replacement Synergis Cloud Link unit.

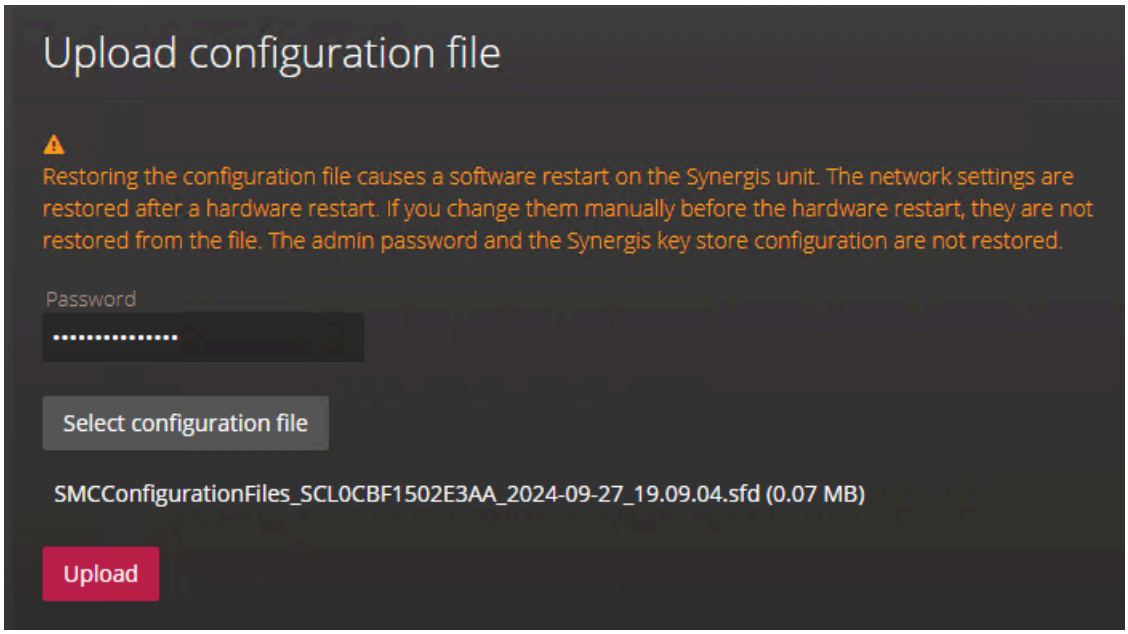
2 Click **Maintenance** > **System status**.

3 In the *Upload configuration file* section, click **Select configuration file**.

4 Navigate to the downloaded configuration package on your local drive and click **Open**.

5 If you set a password when you downloaded the configuration file, enter it in the **Password** field.

6 Click **Upload**.



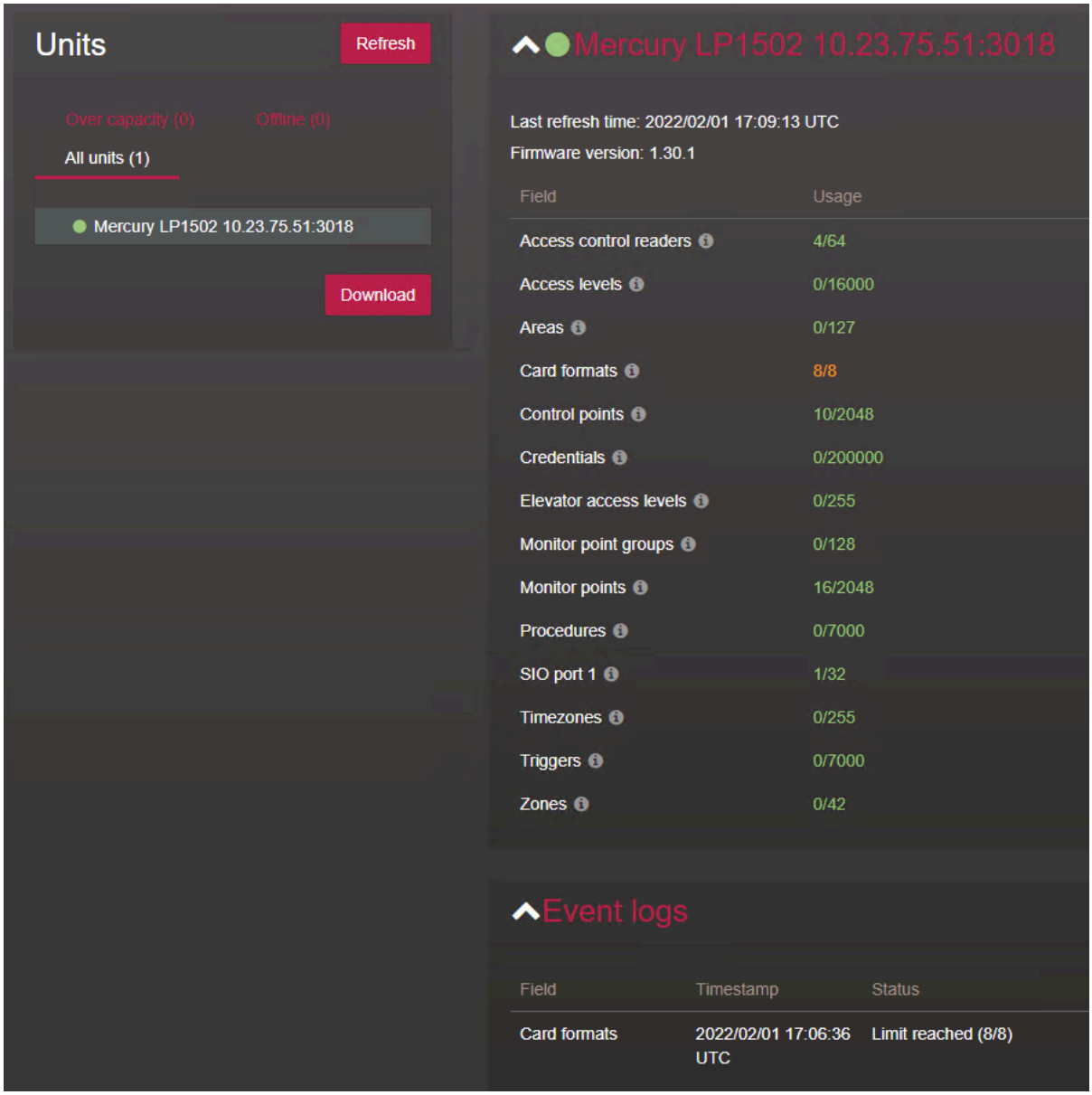
The configuration package is uploaded and the Synergis Cloud Link unit restarts.

After you finish

- Manually reconfigure the administrator password and the Synergis key store configuration because they are not included in the configuration file.
- To restore the network settings from the configuration file, perform a hardware restart.

About the Capabilities report page

To facilitate troubleshooting issues with the Mercury controllers enrolled in your system, you can refer to the *Capabilities report* page in the Synergis™ Appliance Portal. The page gives you an overview of the state, feature usage, and event logs for each of your controllers.



The *Capabilities report* page can only be accessed by users with administrator privileges. The page is separated into the following sections:

- **Units:** Lists all the Mercury controllers that are enrolled on the Synergis™ Cloud Link unit. This section must be manually refreshed. You can view the controllers in three different views:
  - Over capacity
  - Offline
  - All units

Selecting a unit displays the capabilities section and the *Event logs* section for that unit. Clicking **Download** generates a CSV file containing the listed units with their current capability usage.

- **Capabilities section for the selected unit:** This section is named after the unit selected in the *Units* section. It displays the following information:
  - **Last refresh time:** The timestamp of when the data was last fetched.
  - **Firmware version:** The firmware version of the unit.
  - **Capabilities:** A table listing all the supported capabilities for the unit, and the current usage for each capability. For example, *2/64* in the *Access control readers* row indicates that the unit can support up to 62 more readers. Hovering over the icon next to each capability displays the equivalent Security Center concepts.
    The usage values are color coded as follows:
    - Red indicates over capacity.
      NOTE: If a hardware reset occurs while capabilities are exceeded, offline door functionality and OSDP reads do not work as long as the capabilities are exceeded.
    - Orange indicates capacity reached.
    - Green indicates below capacity.
- **Event logs:** Lists the 10 most recent critical events for the selected unit since the last firmware startup, such as when a capability's limit is reached or exceeded.

Downloading support information for your Synergis Cloud Link unit

To simplify troubleshooting your Synergis™ Cloud Link unit, you can download a single file containing all the information you need to provide Genetec™ Technical Support with from the Synergis™ Appliance Portal.

What you should know

The engineering archive file is an encrypted .gen file that only Genetec Technical Support can decrypt. The archive file contains all logs and a backup of the unit's configuration.

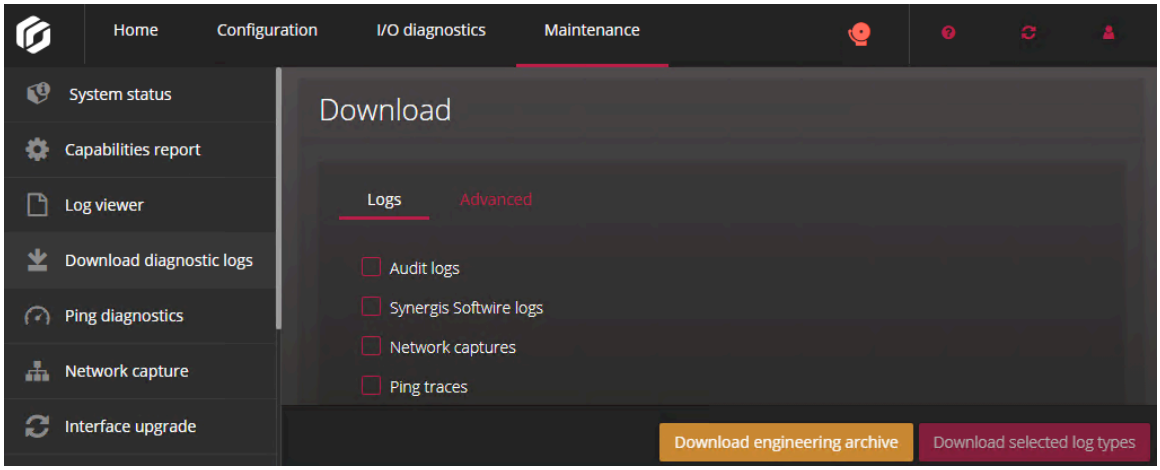
Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Maintenance** > **Download diagnostic logs**.

3 Do one of the following:

- Click **Download engineering archive**.
- In the *Logs* section, select specific categories of logs to download, and then click **Download selected log types**.
- Click the **Advanced** tab, expand the categories and select specific logs to download, and then click **Download selected log files**.



The file is downloaded.

4 Save the file to provide to Genetec Technical Support.

Pinging interface modules from the Synergis Appliance Portal

You can ping interface modules and their downstream interfaces through the Synergis™ Appliance Portal to check if your unit installation was successful, or to troubleshoot network or packet loss issues.

What you should know

- You can perform two types of pings from the portal:
  - **Short ping:** Takes under 10 seconds. The results are displayed under the selected device.
  - **Long-term ping:** Pings every second for a selected duration. Multiple interface modules can be pinged at the same time. A tar.gz file containing the results of the ping can be downloaded from the *Download diagnostic logs* page of the portal.
- ASSA ABLOY and RIO units are not pingable.
- Synergis™ IX units require firmware 4.00_1143_M036 or later to be pingable.
- Ping might not work, depending on your firewall settings.

Procedure

1 Log on to the Synergis™ Cloud Link unit.

2 Click **Maintenance** > **Ping diagnostics**.

A list of all the interface modules and downstream interfaces connected to your Synergis Cloud Link unit is displayed.

3 Start a ping:

- For a short ping: Select an interface module, and then click **Ping**.
- For a long-term ping: Select one or more interface modules, select a **Long-term ping duration**, and then click **Start ping**.

The short ping results are listed under the interface module that you pinged. The long-term ping results are available on the *Download diagnostic logs* page.

Upgrading Synergis Cloud Link firmware

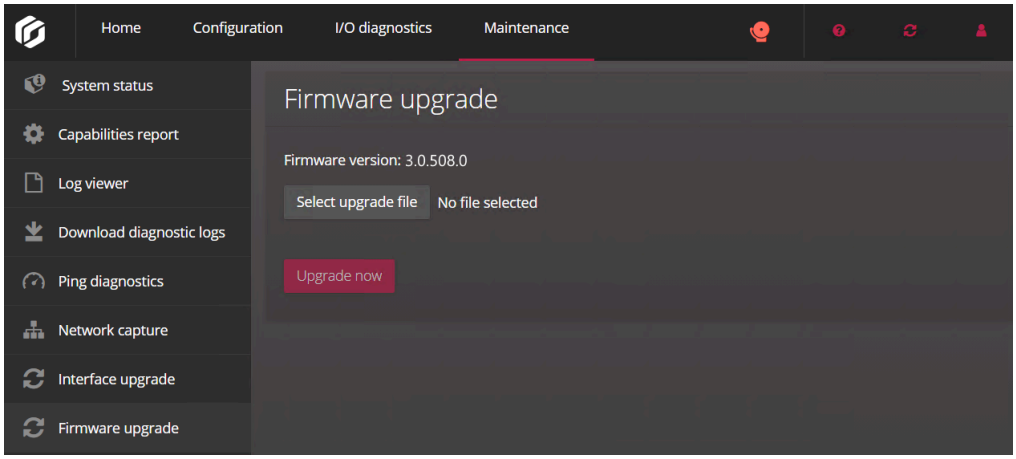
To ensure that you have the latest security fixes and improvements, keep your Synergis™ Cloud Link unit up to date with the latest version of firmware.

Procedure

1 Download the latest firmware from the GTAP *Product Download* page:
   a) From the **Download Finder** list, select **Synergis™ Cloud Link**, and then search for your firmware.
   b) Save the *.sfw* file on your local drive.

2 Log on to the Synergis Cloud Link unit.

3 Click **Maintenance** > **Firmware upgrade**.



4 Click **Select upgrade file**.

5 In the file browser that opens, select the *.sfw* firmware file, and click **Open**.

6 Click **Upgrade now**.

The upgrade can take up to a few minutes, and then the unit restarts.

Rolling back the Synergis Cloud Link unit after a firmware upgrade

After a Synergis™ Cloud Link firmware upgrade, you have seven days to revert the upgrade in the Synergis™ Appliance Portal.

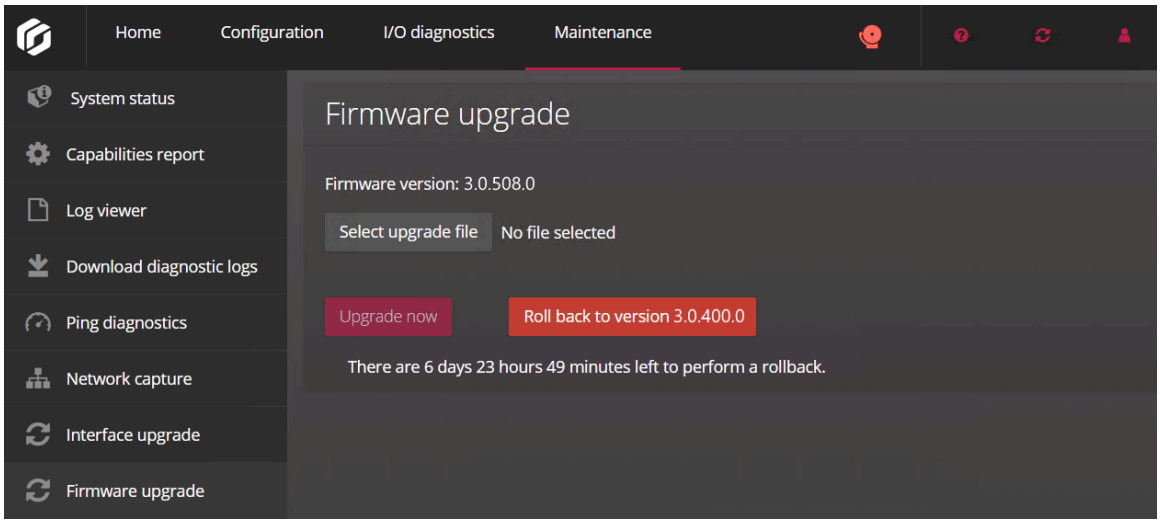
What you should know

- The rollback restores the unit to the state that it was in before the upgrade. The firmware and any configuration changes made after the upgrade are reverted.
- The **Roll back to version X.Y.Z** button is not displayed in the following cases:
  - Seven days following the upgrade have passed.
  - There was not enough space on the unit to save the temporary backup after the upgrade.
  - You already rolled back the upgrade.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Maintenance** > **Firmware upgrade**.



3 Click **Roll back to version X.Y.Z**.

A warning dialog box opens, displaying the following message: *The configuration will be restored to the state it was in before the last upgrade*.

4 Click **OK**.

The unit restarts. After the rollback is done, the following message is displayed: *Rollback completed successfully. The page will be refreshed automatically when the unit is available.*

Upgrading interface module firmware through the Synergis Appliance Portal

Synergis™ Cloud Link units work best when all connected interface modules are running the recommended firmware. Recommended firmware versions are certified by Genetec Inc.

Before you begin

- It is recommended to upgrade interface module firmware using the *Hardware inventory* task in Config Tool rather than the Synergis™ Appliance Portal because you can do the following in the *Hardware inventory* task:
  - Upgrade interface modules in batches or individually.
  - Schedule upgrades and configure email notifications for failed upgrades.
  - View the upgrade progress and current firmware for each interface module.
  - Upgrade Mercury SIO modules and interfaces.

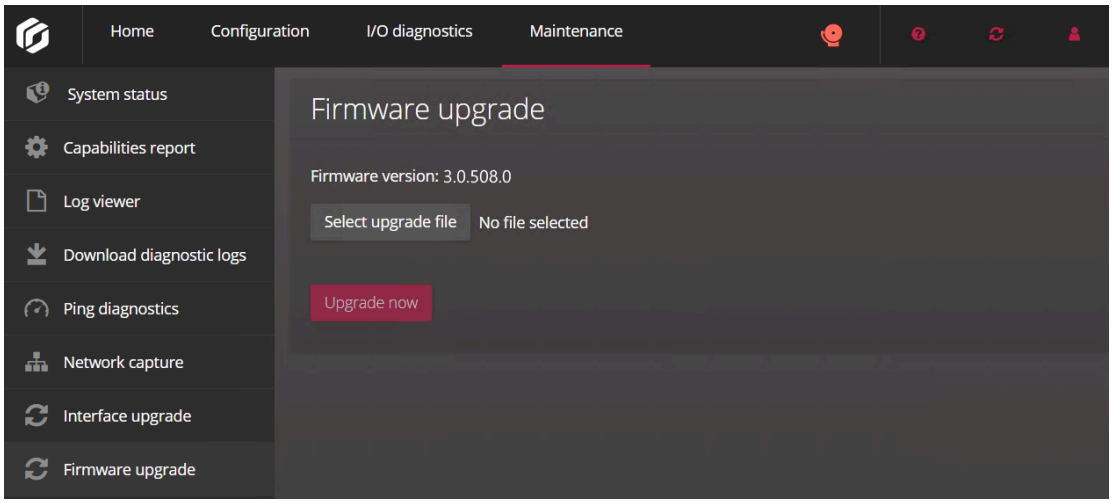
  For more information, see Upgrading access control unit firmware and platform, and interface module firmware.
- If you choose to perform the upgrade using the Synergis Appliance Portal, ensure that your interface module can be upgraded this way.

What you should know

If your interface modules are loaded with firmware versions newer than the recommended ones, they are downgraded except for ASSA ABLOY IP locks.

Procedure

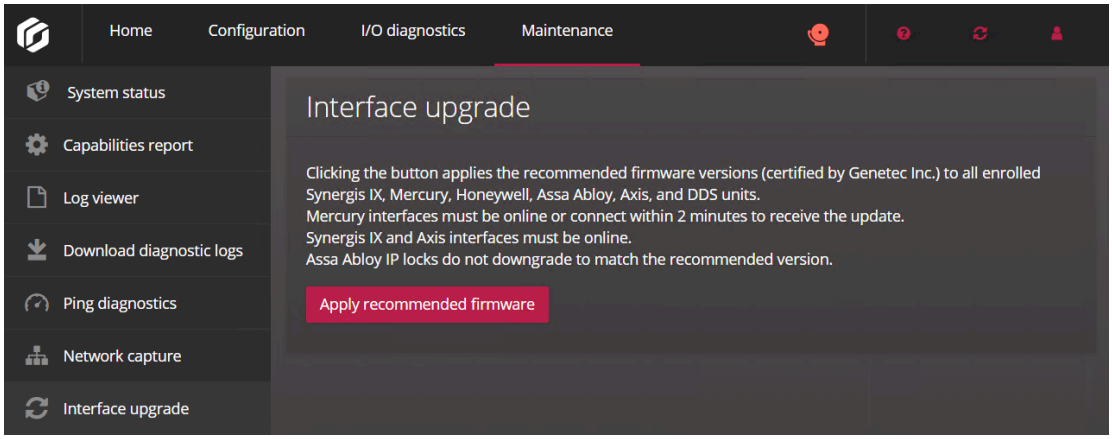
1 Upload the firmware onto the Synergis Cloud Link unit:
   a) From the GTAP *Product Download* page, select **Synergis™ Cloud Link** in the **Download Finder** list, and then search for your interface module firmware.
   b) Save the *.sfw* file on your local drive.
   c) Log on to the Synergis Cloud Link unit.
   d) Click **Maintenance** > **Firmware upgrade**.



   e) Click **Select upgrade file**.
   f) In the file browser that opens, select the *.sfw* firmware file, and click **Open**.
   g) Click **Upgrade now**.

   The firmware is uploaded onto the Synergis Cloud Link unit.

2 Push the firmware to the interface modules:
   a) Click **Maintenance** > **Interface upgrade**.



   b) Click **Apply recommended firmware**.

The following confirmation message is displayed: *Upgrade completed successfully*.

Downstream devices supported for upgrade through the Synergis Appliance Portal

You can upgrade the firmware of specific devices in the Synergis™ Appliance Portal. For manufacturers that are not supported, you might have to use the manufacturer's software to apply the recommended firmware.

The following devices can be upgraded in the Synergis Appliance Portal:

- **Mercury:**
  - EP1501, EP1502, EP2500, EP4502
  - LP1501, LP1502, LP2500, LP4502
  - MP1501, MP1502, MP2500, MP4502
  - M5-IC
  - MS-ICS
- **Honeywell:**
  - PRO32IC
  - PRO42IC
  - PW6K1IC
  - PW7K1IC
- **ASSA ABLOY:**
  - Corbin Russwin and SARGENT IP locksets (CX controllers, PoE, and Wi-Fi)
- **Axis:**
  - A1001
  - A1601
- **DDS:**
  - TPL
  - JET
- **OSDP readers:**
  - Deister
  - WaveLynx
- **Synergis™ IX controllers:**
  - SY-SIX-CTRL-DIN
  - SY-SIX-CTRL-DIN-1D

Cleaning up storage on the Synergis Cloud Link appliance

Ensure that you have sufficient space on your Synergis™ Cloud Link appliance before installing updates or new firmware. You can verify how much space is available and perform storage cleanups on your appliance from the *Storage* page of the Synergis™ Appliance Portal.

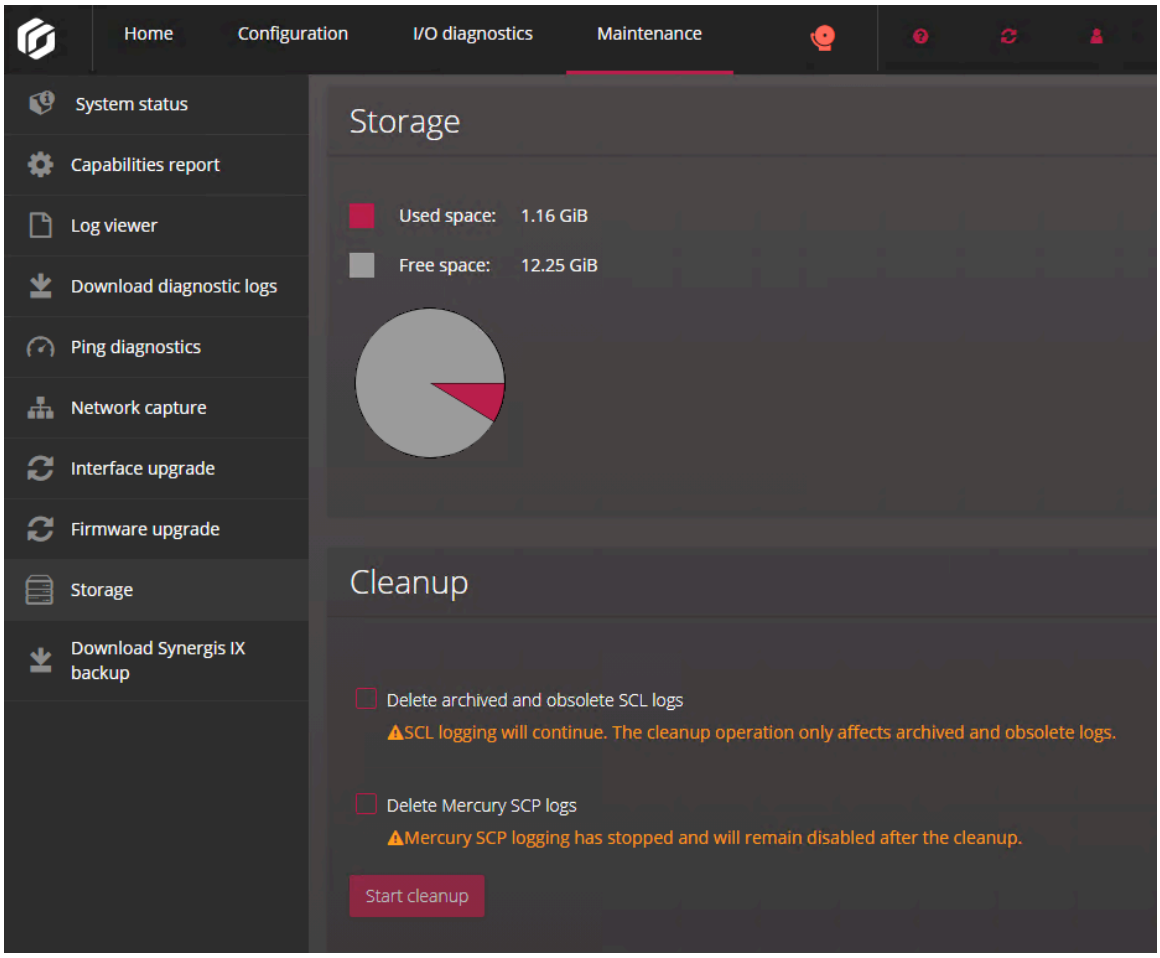
What you should know

IMPORTANT: While a cleanup is in progress, firmware updates and system restarts are blocked on the Synergis Cloud Link appliance.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 Click **Maintenance** > **Storage**.



3 Select the following:

- **Delete archived and obsolete logs:** When you start this cleanup, archived and obsolete Synergis Softwire logs are deleted.
- **Delete Mercury SCP logs:** When you start this cleanup, all archived Mercury SCP logs are deleted.

4 Click **Start cleanup**.

Viewing peer-to-peer information on the Synergis Cloud Link unit

To troubleshoot issues related to units connected as peers to the Synergis™ Cloud Link unit, and verify that the units can all communicate with one another, you can view their status and other information about them from the Synergis™ Appliance Portal.

What you should know

- When the **Activate peer-to-peer** option is disabled on the Access Manager role's *Properties* page in Config Tool, the *Number of peers connected* row and the *Peer-to-peer* page are not displayed in the Synergis Appliance Portal.
- For two units to be connected as peers, they must belong to the same peer group. Up to 15 units can belong to the same group. For more information, see Enabling peer-to-peer on the Access Manager role.
- For the global antipassback information to remain accurate (which cardholder can enter which area), at least one unit must always be powered on. This information isn't stored anywhere, which means that if all units are powered off, it's lost.
- Units that are enrolled under a hosted Access Manager role must use **DHCP** or **DHCP with static IP** for peer-to-peer to work. If the units use **Static IP**, they cannot communicate with one another. You can configure the network settings by going to **Configuration** > **Network** in the Synergis Appliance Portal.

Procedure

To view the number of peers connected to the Synergis Cloud Link unit:

1 Log on to the Synergis Cloud Link unit.

2 Click **Maintenance** > **System status**.

3 Click **Unit**.

In the *Number of peers connected* row, the number of online peers is listed over the total number of peers. For example, *10/12* indicates that there are 12 units other than yours under the same Access Manager role, but only 10 of them connected to your unit.

To view details about the peers connected to the Synergis Cloud Link unit:

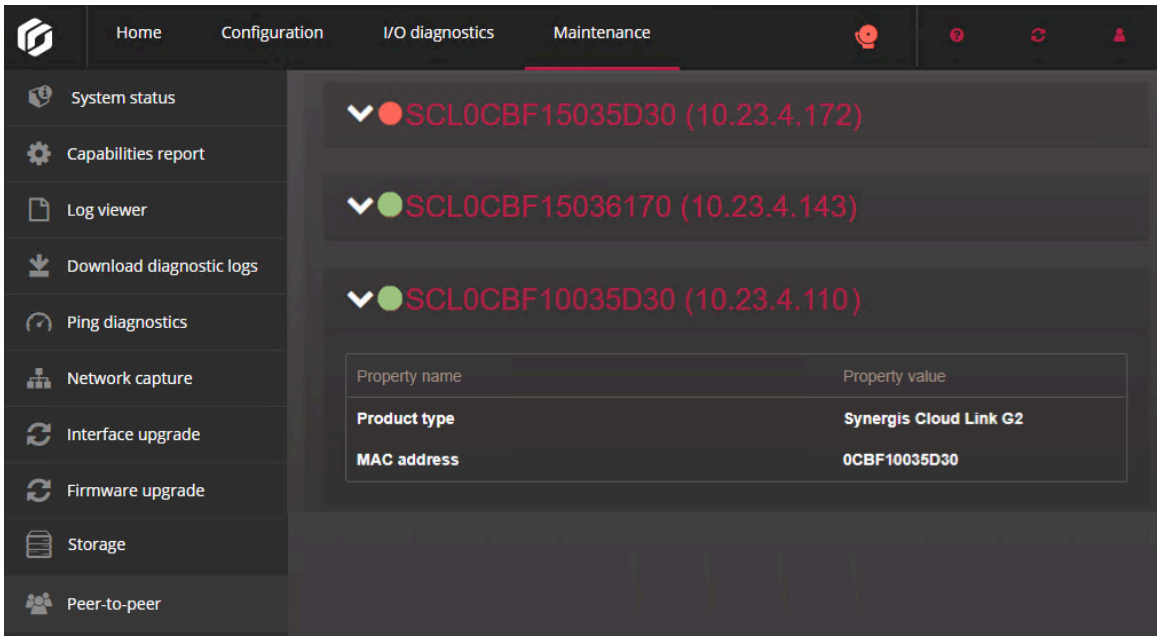
1 Log on to the Synergis Cloud Link unit.

2 Click **Maintenance** > **Peer-to-peer**.

The list of peers is displayed.

3 Click a unit to view its product type and MAC address.

Example:



About the Synergis Cloud Link diagnostic service account

The diagnostic service account gives basic diagnostic and troubleshooting privileges to a non-administrator account holder.

The diagnostic service account allows someone without administrator privileges to log on to the Synergis™ Cloud Link unit and perform basic diagnostic and troubleshooting tasks.

The diagnostic service user has access to fewer features than the administrator does. The following pages in the Synergis™ Appliance Portal are accessible by the service user:

- **Hardware:** View hardware configuration.
- **Synergis Softwire logging:** Configure logging levels and audit log retention.
- **Network:** View the unit hostname, Access Manager settings, and network settings.
- **Users:** Update the password for the service user.
- **I/O diagnostics:** View entities controlled by the unit. Control outputs if output controls are enabled.

  For more information, see Disabling output controls on page 38.
- **System status:** View the unit and network properties and the user audit.
- **Download diagnostic logs:** Download logs and the encrypted engineering archive to provide to Genetec™ Technical Support.

  NOTE: Audit logs are not available for download for the service user.
- **Ping diagnostics:** Ping interface modules and their downstream interfaces.

Creating the diagnostic service account

Creating a service account through the Synergis™ Appliance Portal allows you to give basic diagnostic and troubleshooting access to someone who does not have administrator privileges.

What you should know

The username and default password for the diagnostic service account are both *service*. You can change the default password immediately after enabling the account or be forced to change it the first time you log on using the account.

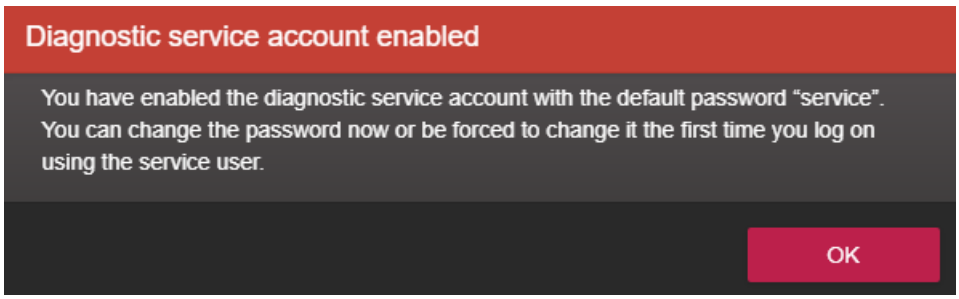
Procedure

1 Log on to the Synergis™ Cloud Link unit as administrator.

2 Click **Configuration** > **Users**.

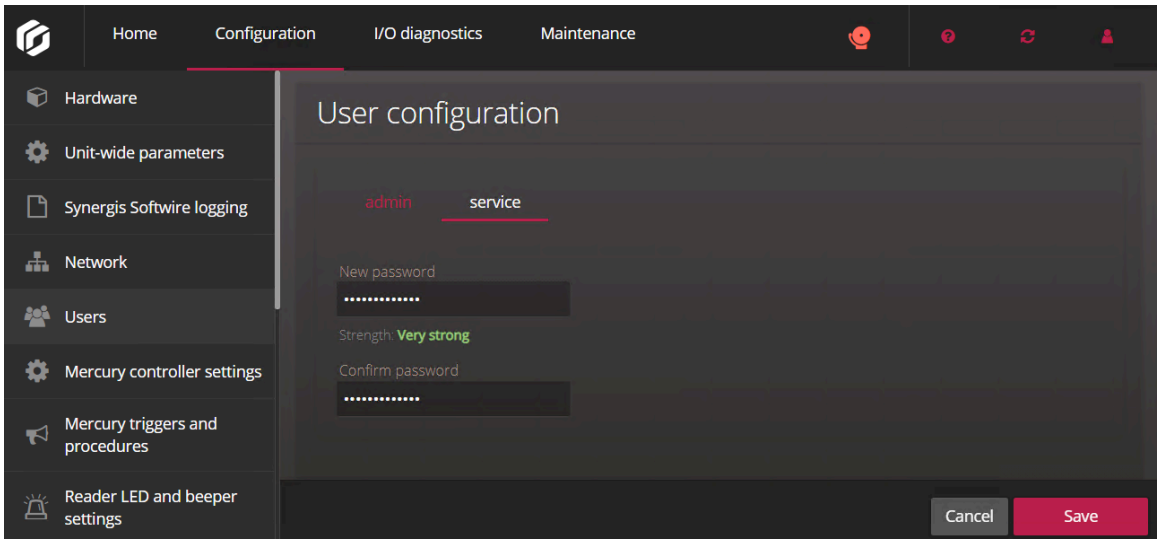
3 Click **Enable diagnostic service account**.

A dialog box opens, confirming that the service account was enabled.



4 Click **OK**.

5 Click the **service** tab, and then change the default password to a strong or very strong password.
NOTE: The password must be at least 15 characters long.



6 Click **Save**.

Restarting the Synergis Cloud Link unit hardware or software

During a debugging session, the support technician might ask you to perform a hard or a soft restart on the Synergis™ Cloud Link unit.

What you should know

- A hard restart, or *system restart*, is required when you experience hardware problems.
- A soft reboot, or a *software restart*, is rarely required. The Synergis Cloud Link unit automatically restarts its firmware after you change the firmware version. Manual software restarts are only used for debugging or support purposes.

Procedure

1 Log on to the Synergis Cloud Link unit.

2 From the **Restart** menu, select the desired restart method.

- To restart the unit's hardware, click **System restart**.
- To restart the unit's software, click **Software restart**.

Part V

Additional resources

This part includes the following chapter:

20

Additional resources for Synergis Cloud Link units

This section includes the following topics:

Default ports used with Synergis Cloud Link

Learn about the default network communication ports that Synergis™ Cloud Link uses.

To view the network diagram, click here.

For a list of default ports that are used by Synergis Softwire integrations, click here.

Port usage	Port	Protocol	IP protocol
Network discovery (ping)	Not applicable	ICMP	IPv4, IPv6
Network connectivity	UDP 68	DHCP	IPv4
	UDP 546	DHCP	IPv6
Redirection to 443	TCP 80	HTTP	IPv4, IPv6
Web portal Secured communication	TCP 443 (Inbound)	HTTPS	IPv4, IPv6
Peer-to-peer communication	TCP 443 (Outbound)	HTTPS	IPv4, IPv6
Synergis discovery	UDP 2000 (Inbound and Outbound)	Proprietary	IPv4, IPv6
Network discovery	UDP 5353 (Inbound)	mDNS	IPv4, IPv6
	TCP 5355 (Inbound) UDP 5355 (Inbound)	LLMNR	IPv4, IPv6
	UDP dynamic range	DNS-SD	IPv4, IPv6

Glossary

access control unit

An access control unit entity represents an intelligent access control device, such as a Synergis™ appliance, an Axis Powered by Genetec door controller, or an HID network controller, that communicates directly with the Access Manager over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Access Manager

The Access Manager role manages and monitors access control units on the system.

access rule

An access rule entity defines a list of cardholders who are granted or denied access based on a schedule. Access rules apply to secured areas and doors for entry and exit, or to intrusion detection areas for arming and disarming.

all open rule

When applied to areas, doors, and elevators, the all open rule grants access to all cardholders at all times.

antipassback

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

automation engine

Automation engine is the Synergis™ Softwire feature that executes rules, similar to event-to-actions in Security Center. Automation engine works even when the Synergis™ unit is disconnected from its Access Manager.

cardholder

A cardholder entity represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.

credential

A credential entity represents a proximity card, a biometrics template, or a PIN required to gain access to a secured area. A credential can only be assigned to one cardholder at a time.

degraded mode

Degraded mode is an offline operation mode of the interface module when the connection to the Synergis™ unit is lost. The interface module grants access to all credentials matching a specified facility code.

dependent mode

Dependent mode is an online operation mode of the interface module where the Synergis™ unit makes all access control decisions. Not all interface modules can operate in dependent mode.

double-badge activation

With double-badge activation, also known as double-swipe activation, an authorized cardholder can unlock a door and trigger actions by badging twice. The door remains unlocked until the next double-badge event.

F2F protocol

The F2F protocol is a proprietary Casi Rusco reader protocol. F2F is a one-wire protocol, as opposed to two wires in the cases of Wiegand or OSDP.

first-person-in rule

The first-person-in rule is the additional access restriction placed on a secured area that prevents anyone from entering the area until a supervisor is on site. The restriction can be enforced when there is free access (on door unlock schedules) and when there is controlled access (on access rules).

global antipassback

Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple Synergis™ units.

hardware zone

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

I/O linking

I/O (input/output) linking is controlling an output relay based on the combined state (normal, active, or trouble) of a group of monitored inputs. A standard application is to sound a buzzer (through an output relay) when any window on the ground floor of a building is shattered (assuming that each window is monitored by a "glass break" sensor connected to an input).

I/O zone

An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis™ units, while one unit acts as the master unit. All Synergis™ units involved in an I/O zone must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

interface module

An interface module is a third-party security device that communicates with an access control unit over IP or RS-485, and provides additional input, output, and reader connections to the unit.

interlock

An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one perimeter door to be open at any given time.

lockdown rule

The lockdown rule is a permanent access rule that denies access to all cardholders at all times, and can be used as an exception to rules that grant access.

mobile credential

A mobile credential is a credential on a smartphone that uses Bluetooth or Near Field Communication (NFC) technology to access secured areas.

secured area

A *secured area* is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

security clearance

A security clearance is a numerical value used to further restrict the access to an area when a threat level is in effect. Cardholders can only enter an area if their security clearance is equal or higher than the minimum security clearance set on the area.

standalone mode

Standalone mode is an operation mode where the interface module makes autonomous decisions based on the access control settings previously downloaded from the Synergis™ unit. When the module is online, activity reporting occurs live. When the module is offline, activity reporting occurs on schedule, or when the connection to the unit is available. Not all interface modules can operate in standalone mode.

strict antipassback

A strict antipassback is an antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.

supervised mode

Supervised mode is an online operation mode of the interface module where the interface module makes decisions based on the access control settings previously downloaded from the Synergis™ unit. The interface module reports its activities in real time to the unit, and allows the unit to override a decision if it contradicts the current settings in the unit. Not all interface modules can operate in supervised mode.

Synergis™ appliance

A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come pre-installed with Synergis™ Softwire and are enrolled as access control units in Security Center.

Synergis™ Appliance Portal

The Synergis™ Appliance Portal is the web-based administration tool used to configure and administer the Synergis™ appliance and upgrade its firmware.

Synergis™ Cloud Link

The Synergis™ Cloud Link is an intelligent, PoE-enabled access control appliance that supports various third-party interface modules over IP and RS-485.

Synergis™ key store

The Synergis™ key store is a database that holds transparent reader keys, *ReaderKc* and *ReaderKs* keys for STid readers, and the SAM LockUnlock key for Synergis™ units with the optional expansion module. Keys in the database cannot be viewed or read, but can be verified using key hashes.

Synergis™ Softwire

Synergis™ Softwire is the access control software developed by Genetec Inc. to run on various IP-ready security appliances. Synergis™ Softwire lets these appliances communicate with third-party interface modules. A security appliance running Synergis™ Softwire is enrolled as an access control unit in Security Center.

Synergis™ unit

A Synergis™ unit is a Synergis™ appliance that is enrolled as an access control unit in Security Center.

threat level

A threat level warns system users of changing security conditions, such as a fire or a shooting, in a specific area or the entire system. Specific handling procedures can be automatically applied when a threat level is raised or canceled.

two-person rule

The two-person rule is the access restriction placed on a door that requires two cardholders (including visitors) to present their credentials within a certain delay of each other in order to gain access.

unit synchronization

Unit synchronization is the process of downloading the latest Security Center settings to an access control unit. These settings, such as access rules, cardholders, credentials, unlock schedules, and so on, are required so that the unit can make accurate and autonomous decisions in the absence of the Access Manager.

unlock schedule

An unlock schedule defines the periods of time when free access is granted through an access point (door side or elevator floor).

visitor escort rule

The visitor escort rule is the additional access restriction placed on a secured area that requires visitors to be escorted by a cardholder during their stay. Visitors who have a host are not granted access through access points until both they and their assigned host (cardholder) present their credentials within a certain delay.

X.509 certificate

X.509 certificate and *digital certificate* are synonyms. In Security Center, these two terms are used interchangeably.

zone

A zone is an entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub.

  Can't find what you are looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the **?** (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec Advantage Description.

Technical training

In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, contact GTAC at https://portal.genetec.com/support.
- For issues with license content or part numbers, or concerns about an order, contact Genetec Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, contact Genetec Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Contact GTAC at https://portal.genetec.com/support to address any issue regarding Genetec appliances or any hardware purchased through Genetec Inc.