Security Center Synergis™

Synergis™ Appliance Configuration Guide

10.6

Document last updated: January 22, 2018

Genetec™

Copyright notice

Document information

Document title: Synergis™ Appliance Configuration Guide 10.6

Document number: EN.702.003-V10.6.B(1)

Document update date: January 22, 2018

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™ appliance for use with Security Center. It assumes you are familiar with the Security Center 5 platform, and specifically with the Synergis™ IP access control system.

This guide supplements the *Security Center Administrator Guide*, the *Synergis™ Cloud Link Hardware Installation Guide*, and the *Synergis™ Softwire Integration Guides*. For more information, see the GTAP Documents page.

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.

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: Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec Inc.

Contents

1

Introduction to Synergis™ appliances

This section includes the following topics:

About Synergis™ appliances

A Synergis™ appliance is an IP-ready security appliance manufactured by Genetec Inc. that is dedicated to access control functions. All Synergis™ appliances come preinstalled with Synergis™ Softwire and can be enrolled as access control units in Security Center.

There are two generations of Synergis™ appliances:

- Synergis™ Cloud Link (second generation)
- Synergis™ Master Controller (first generation)

NOTE: Because Synergis™ appliances can be enrolled as access control units in Security Center, they are also referred to as *Synergis™ units*.

To learn more about the Synergis™ appliances and how they fit into the overall Synergis™ IP access control system architecture, visit our website at www.genetec.com.

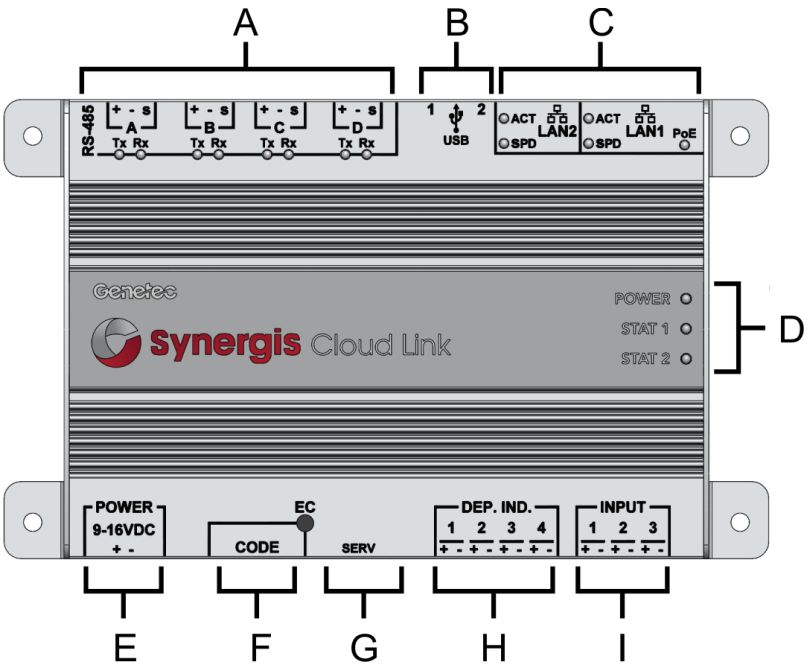
Related Topics

What is Synergis Cloud Link? on page 3
What is Synergis Master Controller? on page 6
What is Synergis Softwire? on page 7
What is Synergis Appliance Portal? on page 9

What is Synergis™ Cloud Link?

Synergis™ Cloud Link is an intelligent and PoE-enabled access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. Synergis™ Cloud Link is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

Synergis™ Cloud Link and accessories can be housed inside an enclosure that are part of a *Synergis™ IP access control system*.



	Hardware feature	What you should know
A	RS-485	Four embedded RS-485 communication ports (or channels) named A, B, C, and D. The number of interface modules you can connect to each channel depends on the type of hardware you have. In configurations where interface modules only use an IP connection, the four RS-485 ports are not needed. **NOTE:** When you start an RS-485 bus from the Synergis™ Cloud Link for HID module communication, you must set the associated termination DIP switch to ON. You must also set the termination jumper on the last connected module on the RS-485 bus.
B	USB1 and USB2	For maintenance use. If the system requires additional RS-485 ports, a four-port RS-485 module can be connected to the USB1 port. Contact us for more information. **NOTE:** This connection has not been evaluated by UL and is not to be used if UL Listed access control system compliance is required and is to be maintained.

	Hardware feature	What you should know
C	LAN1 and LAN2	Two Ethernet LAN ports are provided for connection to the IP network. **NOTE:** Synergis™ Cloud Link can be powered using an Ethernet connection (PoE). For more information, see the *Synergis™ Cloud Link Hardware Installation Guide*. **NOTE:** Connecting to Security Center through the LAN 2 port has not been evaluated by UL and is for supplementary use only.
D	Status LEDs	Synergis™ Cloud Link LED feedback. For their meaning, see the *Synergis™ Cloud Link Hardware Installation Guide*.
E	Power	Connect Synergis™ Cloud Link to an external 12 VDC (nominal) power supply.
F	Code DIP switches	Set a command code with the DIP switches, and run the command by holding the **EC** button for one second. If the code is valid, the status LEDs will flash green for the process of the command, otherwise they flash red for one second. Synergis™ Cloud Link automatically performs a software restart after you have run a command. See DIP switch command codes for Synergis™ Cloud Link on page 4.
G	Service port	Internal use only.
H	DEP. IND.	Deported indicators were not evaluated by UL, and are not to be used if UL Listed access control system compliance is required and is to be maintained.
I	Monitoring inputs	Monitoring inputs were not evaluated by UL, and are not to be used if UL Listed access control system compliance is required and is to be maintained.

Related Topics

About Synergis appliances on page 2
What is Synergis Master Controller? on page 6

DIP switch command codes for Synergis™ Cloud Link

You can use the DIP switches on the Synergis™ Cloud Link to run hardware commands.

Available DIP switch commands

There are four DIP switches on the Synergis™ Cloud Link labelled 1 to 4. To run a command, set the DIP switches as indicated in the table below and press the **EC** button for one second. If the code is valid, the status LEDs will flash green for the process of the command, otherwise they flash red for one second. Synergis™ Cloud Link automatically performs a software restart after you have run a command.

S1	S2	S3	S4	Command description
OFF	OFF	OFF	OFF	Resets the Synergis™ Appliance Portal logon password to factory default (`softwire`).
ON	OFF	OFF	OFF	Resets all settings to factory default. This command has the following effects: • Resets the Synergis™ Appliance Portal logon password to factory default (`softwire`). • 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:** The unit firmware is not affected by this command.

IMPORTANT: Do not power cycle or power down the Synergis™ Cloud Link unit while the status LEDs are flashing green.

Related Topics

Changing the logon password of your Synergis appliance on page 11
Configuring the network properties of the Synergis unit on page 17
Configuring interface modules connected to the Synergis unit on page 19
Configuring unit-wide access control behavior on page 24
Configuring event logging options for your Synergis unit on page 27
Restarting the Synergis unit hardware or software on page 42

What is Synergis™ Master Controller?

Synergis™ Master Controller (SMC) is an access control appliance of Genetec Inc. that supports a variety of third-party interface modules over IP and RS-485. SMC is seamlessly integrated with Security Center and is capable of making access control decisions independently of the Access Manager.

SMC is the first generation of Synergis™ appliances. SMC is no longer distributed and is being replaced by Synergis™ Cloud Link. However, all existing SMC units deployed in the field continue to benefit from Genetec's full support.

Related Topics

About Synergis appliances on page 2
What is Synergis Cloud Link? on page 3

What is Synergis™ Softwire?

Synergis™ Softwire is the access control software developed by Genetec Inc. to run on a variety of IP-ready security appliances. Synergis™ Softwire lets these appliances communicate with third-party interface modules. A security appliance running Synergis™ Softwire can be enrolled as an access control unit in Security Center.

Related Topics

About Synergis appliances on page 2
What is Synergis Cloud Link? on page 3
What is Synergis Master Controller? on page 6

2

Getting started with Synergis™ Appliance Portal

This section includes the following topics:

What is Synergis™ Appliance Portal?

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

The portal allows you to perform the following tasks:

- Change the security password required to log on to the Synergis™ appliance.
- Configure the network settings on the Synergis™ appliance so it works on your system.
- Configure the appliance to accept connections from specific Access Managers.
- Enroll and configure the interface modules attached to the Synergis™ appliance.

  NOTE: There is one exception to the rule. Mercury controllers (EP and M5-IC) must be enrolled and configured from Security Center Config Tool in the access control unit's **Peripherals** tab. For more information, see the chapter on Mercury controllers in the *Synergis™ Softwire Integration Guide*.
- Configure the access control behavior of the appliance for both online and offline operations.
- Test and diagnose the interface module connections to the Synergis™ appliance.
- View and export the Synergis™ appliance's status and configuration.
- Upgrade the Synergis™ appliance's firmware (Synergis™ Softwire).
- Restart the Synergis™ appliance's hardware or software.

Tasks that must be done in Config Tool

You cannot perform the following tasks through the portal. You have to use Security Center Config Tool instead.

- Enable/disable the **Server mode** operation (This option is hidden by default; it will only appear if it was already enabled).
- Assign devices (input/output contacts, readers) to doors and zones.
- Configure individual door and zone properties.
- Configure Card and PIN readers so both the card and the PIN are required to grant access.
- Configure I/O linking.

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

Logging on to the Synergis™ appliance

To configure your Synergis™ appliance (also called *Synergis™ unit*), log on to the appliance through the Synergis™ Appliance Portal.

Before you begin

You will need the following information to log on for the first time.

- The appliance hostname is `SCL` (for Synergis™ Cloud Link) or `SMC` (for Synergis™ Master Controller) followed by the appliance's MAC address, which is the first alpha-numeric code on the label sticker on the appliance. For example, if the label says `0010F32CF482`, then the default hostname for a Synergis™ Cloud Link appliance is `SCL0010F32CF482`.
- The default username and password are *admin* and *softwire*.
- If you are using Microsoft Internet Explorer 11, make sure you have the **Font download** setting enabled. To enable **Font download**, launch Microsoft Internet Explorer 11 and click **Tools (** ⚙ **)** > **Internet Options** > **Security** > **Custom Level**. In the *Settings* tree, scroll to *Font download* under *Downloads*, click **Enable**, and apply the change.

What you should know

Only one user can be connected to a given Synergis™ appliance at any given time. By logging on, you will log off anyone who might have logged on before you.

To log on to a Synergis™ appliance:

1 (First time logon only) Connect the Synergis™ appliance's **LAN 1** port to your LAN.
Click here to view the location of the **LAN 1** port on a Synergis™ Cloud Link appliance.

2 Open a web browser.
See the *Synergis™ Softwire Release Notes* for supported web browsers.

3 In the browser's address bar, type `https://` followed by the Synergis™ appliance's hostname or IP address (for example, `https://SCL0010F32CF482`).
If you are unable to connect to your appliance using its hostname and you haven't yet configured its IP address, then you should log on to the Synergis™ appliance using the alternate IP address.

4 (New browser session only) If you opened a new browser session to log on to the Synergis™ appliance, you will get a certificate error message.
Follow your browser's on-screen instructions to continue to the website.

NOTE: You won't see the message again unless you close and re-open your browser to log on to the appliance.

5 In the *Synergis Appliance - Logon* page, select the interface language.

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

The *Synergis Appliance - Home* page appears.

After you finish

Before you deploy the Synergis™ unit in the field, you should change the default logon password.

Changing the logon password of your Synergis™ appliance

Before you deploy the Synergis™ unit in the field, it is recommended that you change the default password.

What you should know

If you are logging on to the Synergis™ apppliance for the first time, the default username and password are *admin* and *softwire*.

To change the logon password:

1 Log on to the Synergis™ unit.
2 Click on **Configuration** > **Users**.
3 From the *Users* page, select the **admin** user.
4 Enter the old password, then enter and confirm the new password and click **Save**.

The new password is applied immediately.

After you finish

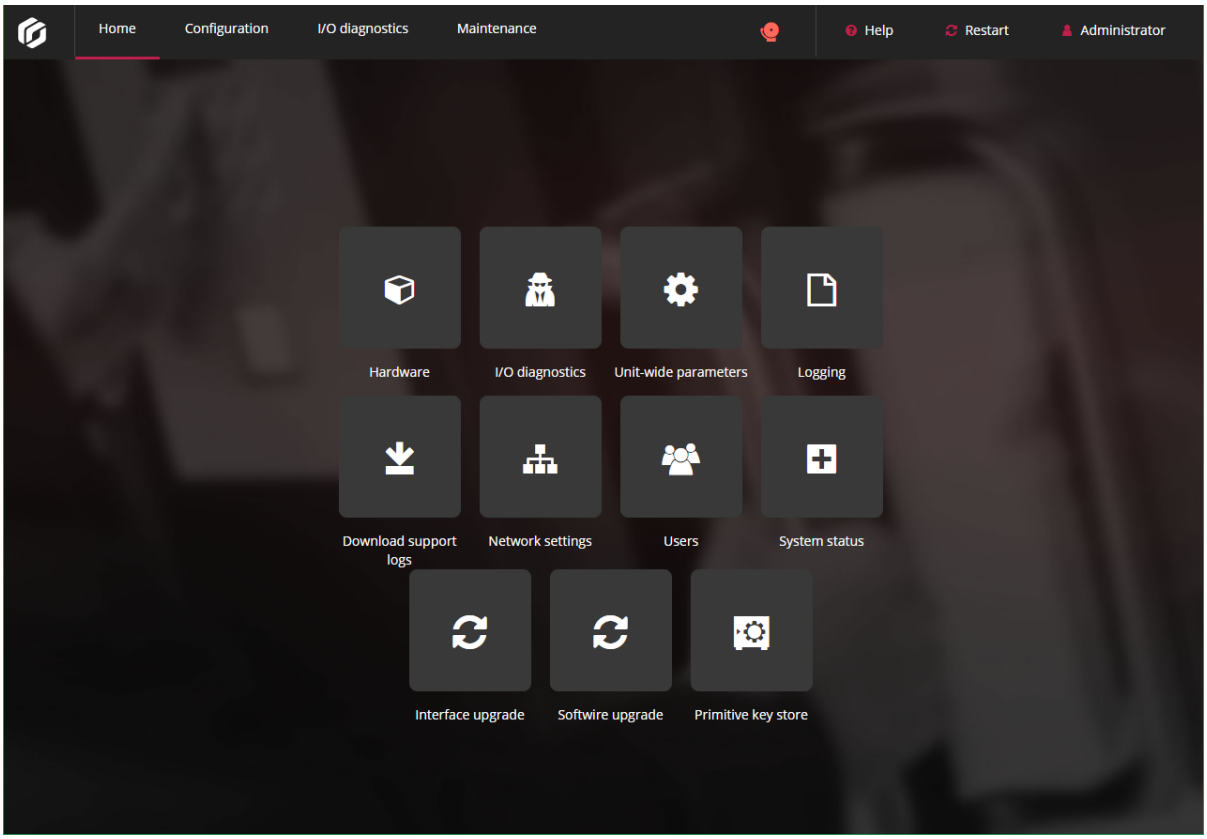
If the unit was already connected to an Access Manager role, then change the logon password in the Config Tool to synchronize the Synergis™ unit with the Access Manager.

Related Topics
DIP switch command codes for Synergis Cloud Link on page 4

Interface tour of the Synergis™ Appliance Portal

Synergis™ Appliance Portal's *Home* page is divided into a top menu bar and a quick-access area with icons that lead to frequently-used tasks.

NOTE: Below is an image of a typical Synergis™ Appliance Portal *Home* page. The area below the menu bar might vary, depending on your context.



The links in the portal's menu bar are as follows:

- **Home:** Returns to the *Home* page.
- **Configuration:** Opens the *Hardware* page where you configure the interface modules attached to the Synergis™ unit. This page also includes menu tabs for the *Unit-wide parameters*, *Logging*, *Network*, *Users*, and *Primitive key store* pages.
- **I/O diagnostics:** Opens the *Channel* page where you can monitor the state changes of the contacts and the credentials read on the readers as you trigger them. This page also includes menu tabs for the *Interfaces*, *Doors*, *Elevator*, *Hardware zones*, and *I/O zones* pages.
- **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. This page also includes menu items for *Interfaces upgrade*, *Softwire upgrade*, and *Download support logs*.
- **Notifications:** Displays system health warnings.
- **Help:** Opens a drop-down menu with two items: *Help* opens the *Synergis™ Appliance Configuration Guide* in a separate browser page, and *About* shows the Synergis™ 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™ 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.

3

Synergis™ appliance configuration

This section includes the following topics:

Preparing to configure Synergis™ units

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

Before configuring the Synergis™ unit:

- Read the *Synergis™ Softwire 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™ unit.
- Configure the hardware settings (DIP switches, address dials, etc.) to their final position on the interface modules. For more information, see the *Synergis™ Softwire Integration Guide* for the hardware types you have.
- Connect the interface modules to the Synergis™ 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.

- Physical devices (REX, door sensors, etc.) should be connected as well, but can be replaced by test switches and LEDs during the configuration phase.

  For more information, see the *Synergis™ Cloud Link Hardware Installation Guide*.
- Download the latest Synergis™ Softwire package from https://gtap.genetec.com.
- 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™ unit.

Configuring the Synergis™ unit

You can configure the Synergis™ unit once the pre-configuration steps are completed.

Before you begin

Perform the pre-configuration steps.

To configure a Synergis™ unit:

1. All Synergis™ units come with a factory-assigned hostname. If your network does not support DHCP, your IT department must assign the appliance a new IP address.
2. Make sure you have the latest version of Synergis™ appliance firmware, and upgrade if necessary.
3. Physically attach the interface modules to the Synergis™ unit.

   For information, see the *Synergis™ Cloud Link Hardware Installation Guide*.
4. Establish communication between the Synergis™ unit and its attached interface modules by configuring them through the Synergis™ Appliance Portal.
5. Test your hardware connections and configuration and make adjustments if necessary.
6. Configure the access control behavior you want Synergis™ unit to exhibit.
7. Add the Synergis™ unit to an Access Manager so it becomes part of your Security Center system.

Configuring the network properties of the Synergis™ unit

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

Before you begin

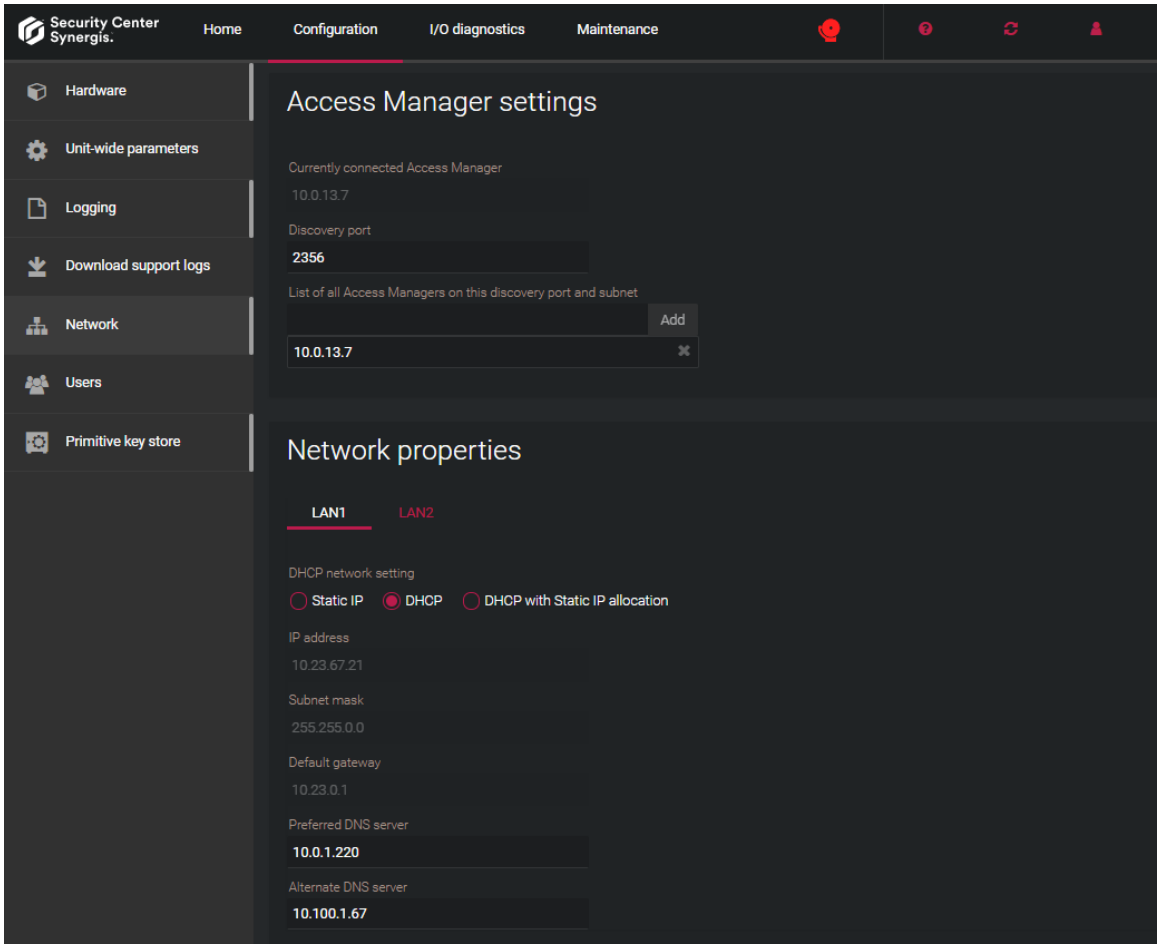
The Synergis™ appliance comes with a factory-assigned hostname. If your network does not support DHCP, your IT department must assign the controller a new IP address.

To configure the Synergis™ unit's network properties:

1 Log on to the Synergis™ unit.

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

3 Select the **Network interface** used to connect the Synergis™ unit to its Access Manager.



4 Change the **Discovery port** if necessary.

To enroll or allow autodiscovery of the unit by the Access Manager, the configured discovery port on the Synergis™ appliance must match one of the Access Manager role's Synergis™ extension ports.

5 Configure the Synergis™ unit's IP address and the network properties.

IMPORTANT: If the Synergis™ 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.

6 Click **Save**.

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

Related Topics

DIP switch command codes for Synergis Cloud Link on page 4

Configuring interface modules connected to the Synergis™ unit

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

Before you begin

Physically connect your interface modules to the controller module.

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.

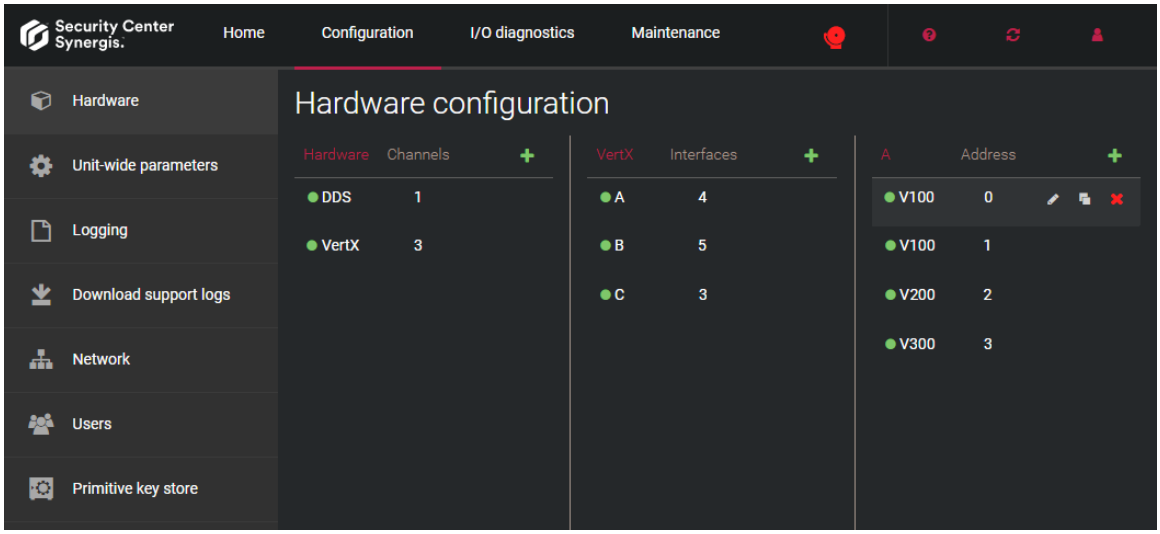
NOTE: There is one exception to the rule. Mercury controllers (EP and M5-IC) must be enrolled and configured from Security Center Config Tool in the access control unit's **Peripherals** tab. For more information, see the chapter on Mercury controllers in the *Synergis™ Softwire Integration Guide*.

To configure interface modules connected to the Synergis™ unit:

1 Log on to the Synergis™ unit.

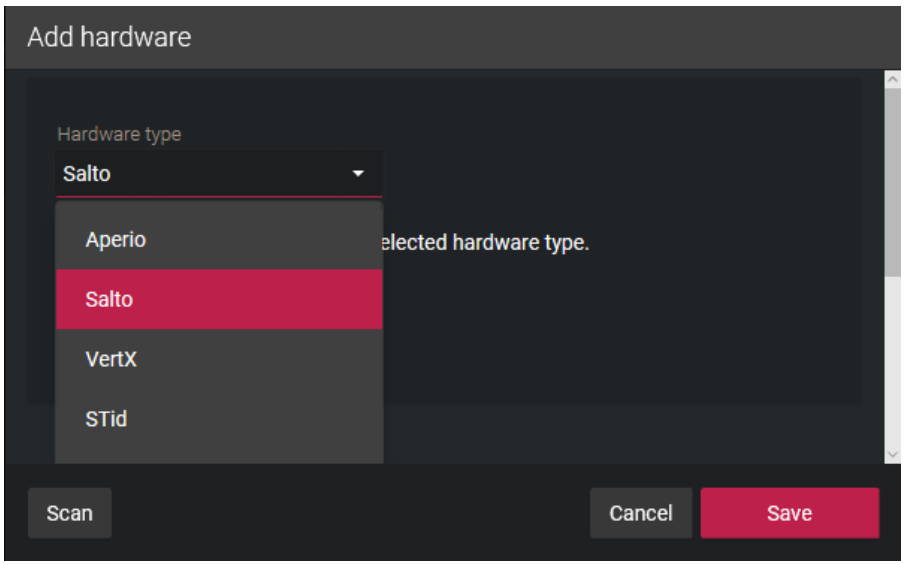
2 Click on **Configuration** > **Hardware**.

The portal shows the hardware tree as three columns: The first column displays your configured hardware manufacturers and the number of channels they use. Click on a hardware manufacturer to bring up its channels in the second column. Selecting a channel brings up the interface modules connected to this channel in the third column. The second column changes to match the hardware selected in the first column, and the third column changes to match what is selected in the second column. You can edit ( ), clone ( ) or delete ( ) the channel by rolling over it and selecting from the icons that appear.



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.



For more information, see the *Synergis™ Softwire Integration Guide* for the type of hardware you have.

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**.

  The discover feature finds all interface modules from the same manufacturer that are connected to the same channel and adds them to the list. For this to work, all of the interface modules must use the same baud rate and be configured with a different physical address.

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 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.

Related Topics

DIP switch command codes for Synergis Cloud Link on page 4

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™ unit is configured with factory default settings for all supported interface modules.

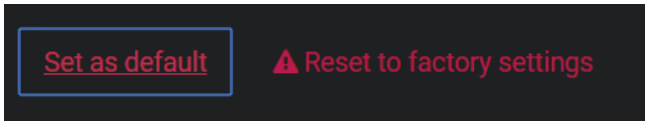
To change the default settings of an interface module:

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, make all necessary changes to its settings.

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



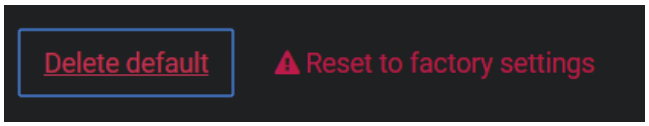
Your changes are saved as new default settings. The next time you add an interface module of the same type, your new default values will be used to initialize the property page.

Clearing custom default settings of interface modules

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

To clear the custom default settings of an interface module:

1 Click on **Configuration** > **Hardware**.
2 From the *Hardware* page, select the interface module you set as default.
3 In the *Edit* dialog, click **Delete Default**.



IMPORTANT: Do not confuse this button (**Delete default**) with the one next to it (**Reset to factory settings**). The Delete Default button only discontinues the use of your custom default settings so that the next time you add an interface module of the same type, the factory default values will be used. The **Reset to factory settings** button resets the values on the current page to their factory defaults when you save.

Cloning interface module settings

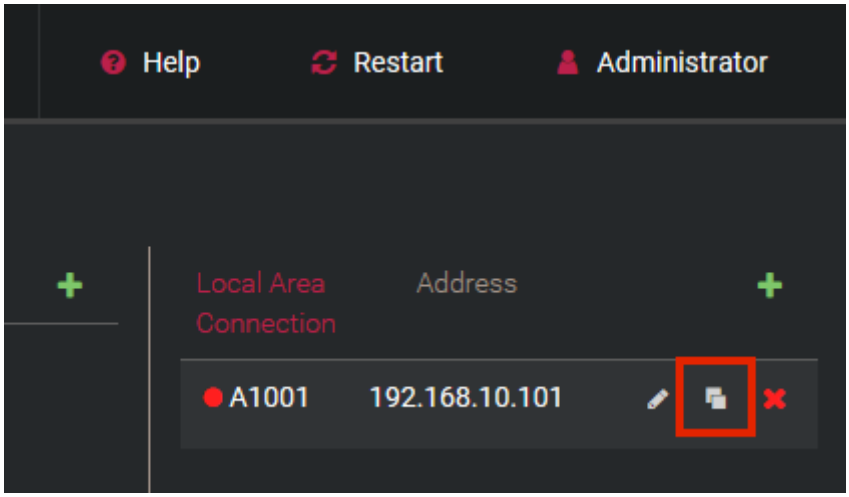
To save time, you can add new interface modules by duplicating the settings of an existing interface module and then make the changes that apply.

Before you begin

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

To clone interface module settings:

1 Log on to the Synergis™ unit.
2 Click on the **Configuration** > **Hardware**.
3 In the *Hardware configuration* page, add and configure an interface module or select one from the hardware tree as your model for cloning.
4 Click .



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

All you need to specify for each new interface module is the channel it is connected to and the physical address. All other settings will be copied from the model interface module.

After you finish

Modify the settings of the cloned interface modules as required.

Testing interface modules attached to the Synergis™ unit

You can test your hardware connections and configuration by monitoring their responses on the I/O diagnostics page in real time.

Before you begin

Configure the interface modules.

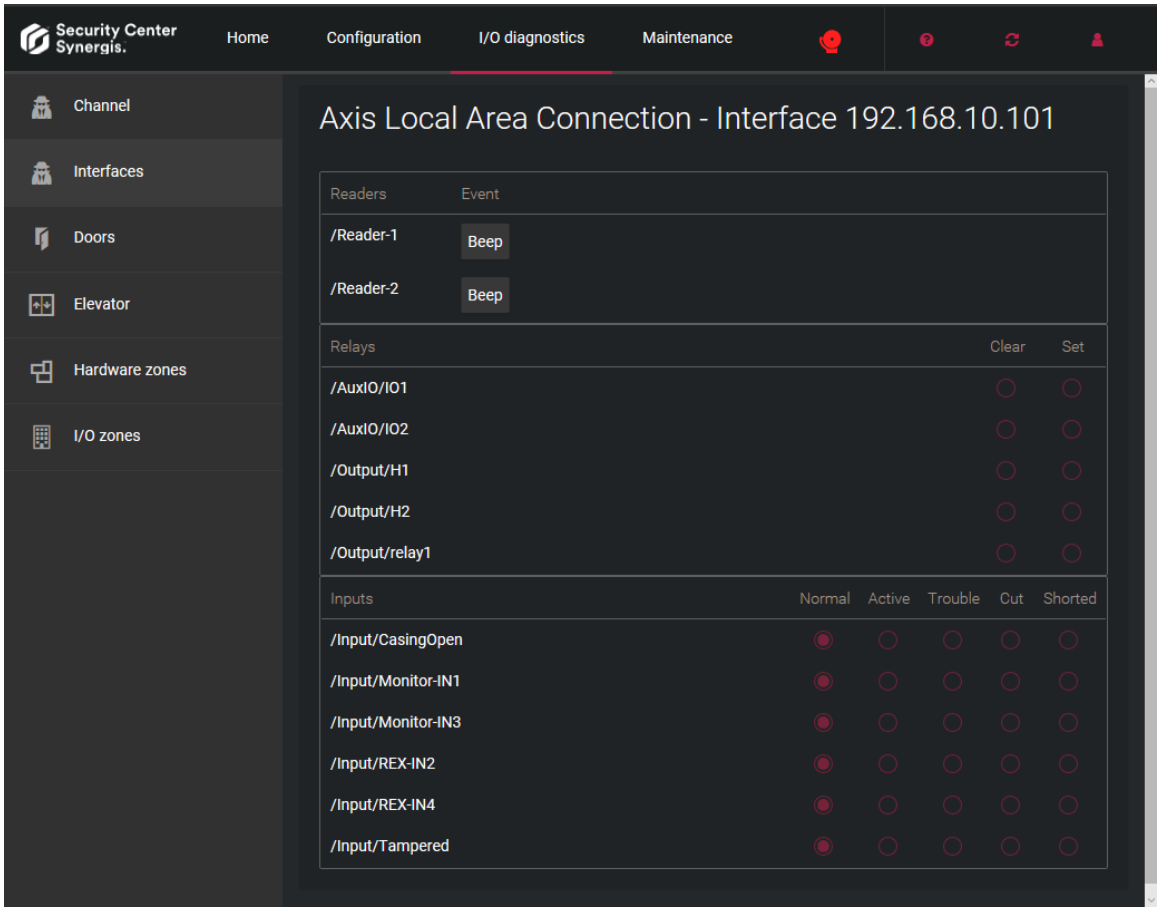
What you should know

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

To test an interface module attached to the Synergis™ unit:

1 Log on to the Synergis™ unit.

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



3 Scroll to the interface you want to monitor.

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

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

Configuring unit-wide access control behavior

Most interface module behaviors, such as beeping on certain types of access control events, are common to all interface modules attached to the same Synergis™ unit. You configure these unit-wide settings on the *Access control* page.

What you should know

Some settings only apply to certain types of interface modules and are not shown unless those interface modules are configured for your unit. Whenever an equivalent setting is found in Security Center, the setting configured in Config Tool (for example door properties) takes precedence.

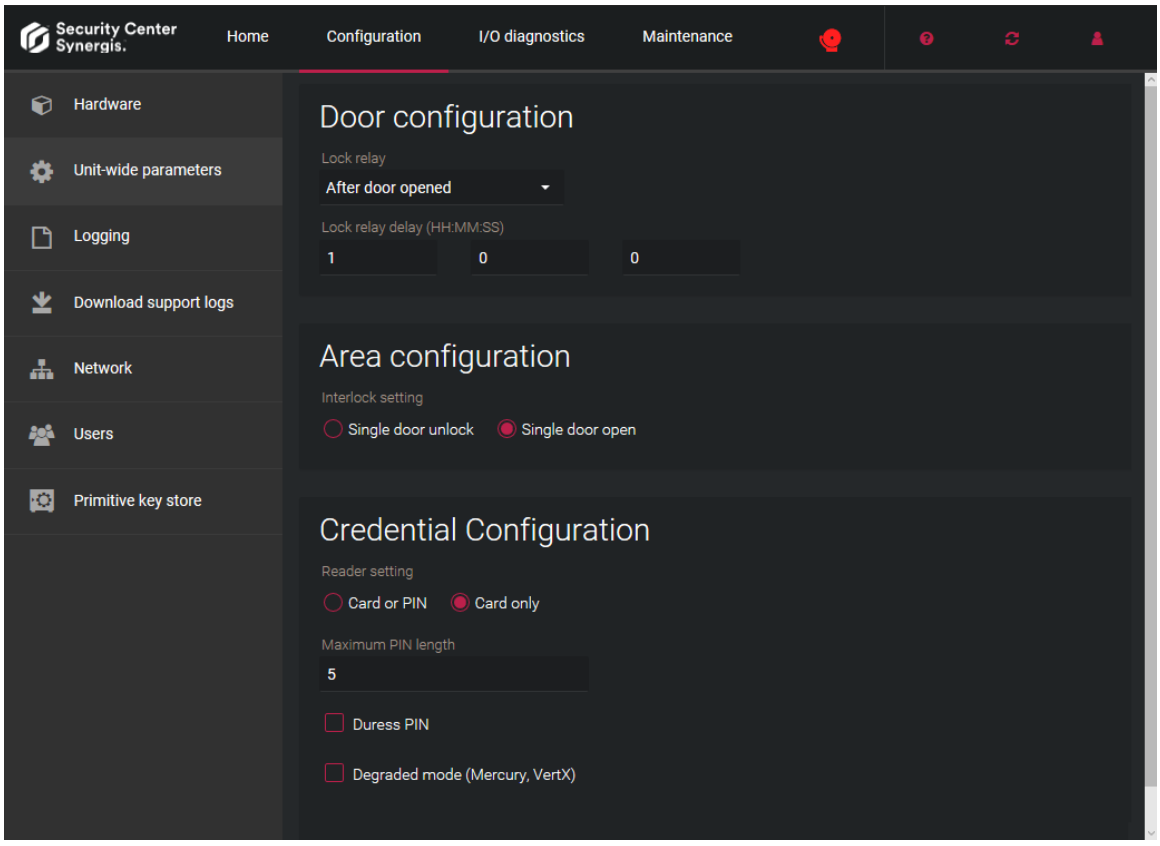
For more information about these access control settings, or about how to configure them in Security Center, see the *Security Center Administrator Guide*.

To configure unit-wide access control behavior:

1 Log on to the Synergis™ unit.

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

3 In the *Unit-wide parameters* page, select which of the following options you want the Synergis™ unit to support:



Door configurations

- **Lock relay:** This setting tells the Synergis™ unit to do one of the following:
  - **After door opened:** Keep the door unlocked for a certain delay (HH:MM:SS) after the door opens.
  - **When door closed:** Immediately lock the door after it closes.

Area configurations

- **Interlock setting:** An interlock is a system with multiple doors where only one door can be opened at any time. You have two options:
  - **Single door open (Default):** The moment one door is open, immediately lock all other doors.
  - **Single door unlock:** Only unlock one door at any given time.

Credential configurations

- **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 (Default):** Only the card is used to grant access.

  NOTE: To enforce Card and PIN so that both the card and the PIN must be used to gain access, you need to configure the property of the reader in Config Tool.
- **Maximum PIN length:** Applies to interface modules that support option-00 readers. The Synergis™ unit will process the PIN being entered the moment it reaches the maximum number of digits, without waiting for the '#' key.

  NOTE: There might be exceptions; check the features of your specific integration.
- **Duress PIN:** (Only applies to Mercury EP) Enables *Duress PIN* support on *Card and PIN* readers (default = disabled). To signal a duress, authorized cardholders must enter their regular PIN + 1 to the last digit. For example, if the regular PIN is 9999, then the duress PIN is 9990.
- **Degraded mode (Mercury, VertX):** In degraded mode, the interface module makes decisions on its own when the connection to the Synergis™ unit is lost. When this option is selected, the interface module unlocks the doors for all credentials that match the specified *Facility code* (26 bits card format only) instead of requiring a full match.This option applies only to Mercury and HID VertX sub-panels.

4 Click **Save**.

All changes become effective only after a software restart.

Related Topics

DIP switch command codes for Synergis Cloud Link on page 4

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

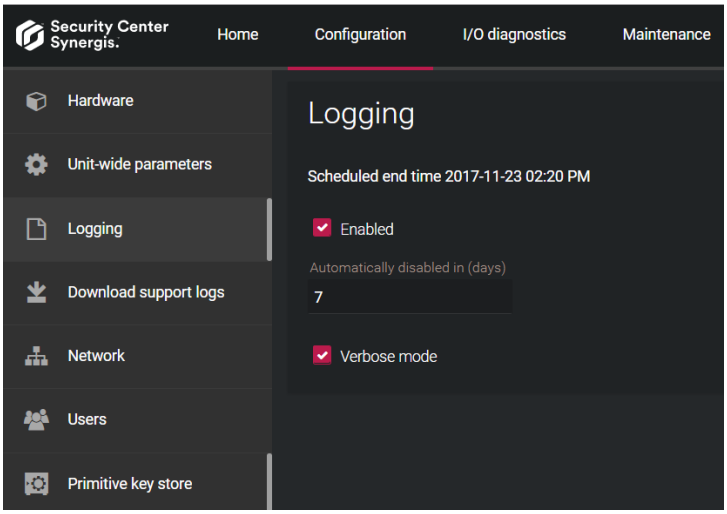
The default timeout is 5 seconds.

To change the PIN entry timeout for a door:

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, enable **Use card and PIN**, if it's not already enabled.
6. Set the **Access timeout**, and then click **Save** > **OK**.
7. If the desired setting is *Card or PIN*, do the following:
   a) Click **Reader settings** ( ), and disable **Use card and PIN**.
   b) Click **Save**.
8. Click **Apply**.

Configuring event logging options for your Synergis™ unit

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



To configure event logging options:

1 Log on to the Synergis™ unit.
2 Click on **Configuration** > **Logging**.
3 Enable logging only if instructed by Genetec™ Technical Support.

   The default is 7 days, and the maximum is 30 days. This is only a safeguard. You should disable logging the moment it is no longer required.
4 Click **Save**.

Related Topics

DIP switch command codes for Synergis Cloud Link on page 4

Enrolling Synergis™ units in Security Center

To enroll a Synergis™ unit in Security Center, assign the unit to an Access Manager. The Access Manager must be able to reach the Synergis™ unit on the network, and the Synergis™ unit must be configured to respond to the Access Manager commands.

Before you begin

Configure the Synergis™ unit's network properties.

To enroll a Synergis™ unit in Security Center:

1 Enable the Access Manager to connect to the Synergis™ unit by adding the Synergis™ extension in Security Center .

After a few seconds, all new Synergis™ units found on the same network segment as the Access Manager (that have never been enrolled before) will automatically be added to the Access Manager through automatic discovery.

2 If the Synergis™ unit was previously added to another Access Manager, then you must switch the Synergis™ unit to the Access Manager you want.

3 If the Synergis™ unit is not on the same network segment as the Access Manager, then you must add the Synergis™ unit to the Access Manager manually.

The Synergis™ unit is connected to its designated Access Manager, and from now on will only respond to commands issued from that Access Manager.

After you finish

Associate the peripherals (readers, inputs, outputs, and so on) controlled by this unit to doors and zones defined in your system. For more information about deploying Synergis™, see the *Security Center Administrator Guide*.

Adding access control unit manufacturer extensions

For the Access Manager to communicate with access control units, you must add the manufacturer-specific extensions.

What you should know

Starting from Security Center 5.3, the manufacturer extensions are added by default when the Access Manager is created. Therefore, you only need to add the extensions manually if the Access Manager was created before version 5.3. However, the Genetec™ Synergis™ extension required by Synergis™ units is created with the default discovery port, 2000. If you configured your Synergis™ units with a different port number, you must also change it on the Access Manager.

BEST PRACTICE: If you have two or more Access Manager roles controlling Synergis™ units on the same subnet, make sure that they use different discovery ports. Otherwise, you might experience performance issues with your Synergis™ units.

To add a manufacturer extension to the Access Manager:

1 Open the *Access control* task, and click the **Roles and units** view.

2 Select the Access Manager, and click the **Extensions** tab.

3 At the bottom of the extensions list, click **Add an item** ( ).

4 In the *Add extensions* dialog box, select the extension types you need and click **Add.**

5 Select the Genetec™ Synergis™ extension you added.

6 To add a discovery port, click **Add an item** ( ), at the bottom of the *Discovery ports* section.

7 In the *Discovery port* dialog box, enter the port number configured for your Synergis™ units and click **Create**.

The port number must match the discovery port configured on your Synergis™ units. The default value is 2000.

8 Click **Apply.**

Automatic enrollment of access control units

Automatic enrollment is when new IP units on a network are automatically discovered by and added to Security Center. The role that is responsible for the units *broadcasts* a discovery request on a specific port, and the units listening on that port respond with a message that contains the connection information about themselves. The role then uses the information to configure the connection to the unit and enable communication.

The Access Manager role is able to automatically discover the Synergis™ appliances as access control units when the following conditions are met:

- The Synergis™ appliance has never been connected to any Access Manager before.
- The Synergis™ appliance and the Access Manager use the same discovery port.
- The Synergis™ appliance and the Access Manager are on the same network segment.
- The Synergis™ appliance is using the default logon username and password (`admin`/`softwire`).

When automatic discovery is not supported or does not work, use the *Unit enrollment tool* to find the units on your network and add them manually.

Adding Synergis™ units to an Access Manager manually

The Access Manager must download the access control configuration of your system (areas, access rules, cardholders, credentials, and so on) to the Synergis™ unit so it can make all access control decisions on its own. For this to happen, the Access Manager must be connected to the Synergis™ unit at least once, if not all the time.

Before you begin

Enable the Access Manager to connect to the Synergis™ unit by adding the Synergis™ extension in Security Center .

To add a Synergis™ unit to an Access Manager manually:

1 Connect to Security Center with Config Tool.

2 Open the *Access control* task, and click the **Roles and units** view.

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

4 In the unit creation dialog box, click **Unit type** and select **Synergis**.

If the unit type is greyed out, it means that the manufacturer extension is not yet added in the Access Manager.

5 In the **Network endpoint** group, enter the Synergis™ unit's hostname or IP address, as well as the logon username and password.

The default username and password are `admin` and `softwire` if you have not changed them.

6 If port forwarding is required, click **Advanced settings** and enter the base URL in the **Web address** field.

7 Click **Next**.

8 Select a **Partition** where the access control unit should be added.

Partitions determine which Security Center users have access to this entity. Only accepted users of the partition can view or modify the access control unit.

9 Click **Next**.

10 Review the **Creation summary**, and click **Create**.

The Access Manager attempts to connect to the unit and enrolls it in your system. Once the process has been successfully completed, a confirmation message appears.

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

The newly added access control unit appears under the Access Manager it was assigned to in the **Roles and units** view. The default entity name is the Synergis™ unit's hostname. From now on, this Synergis™ unit will only respond to the commands issued by this Access Manager.

NOTE: Later, if you change the connection parameters on the Synergis™ unit, you will have to inform the Access Manager about it by synchronizing the Synergis™ unit with the Access Manager.

Synchronizing the Synergis™ unit with its Access Manager

Some settings on the Synergis™ unit are not automatically synchronized with the Access Manager. If you change any settings on the Synergis™ 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 also change the same settings on the Access Manager in Config Tool.

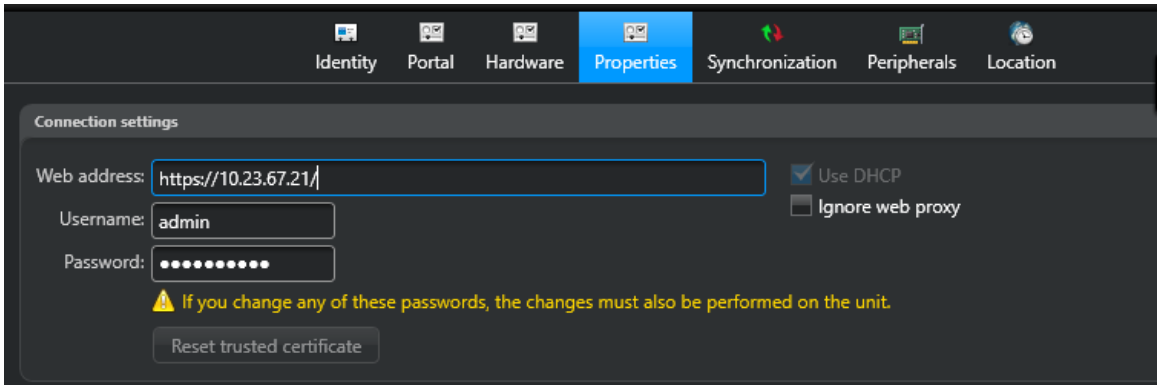
To synchronize the Access Manager with a Synergis™ unit:

1 Connect to Security Center with Config Tool.

2 Open the *Access control* task, and click the **Roles and units** view.

3 Select the Synergis™ unit you modified.

4 Click the **Properties** tab to update the necessary properties.



5 Under **Connection settings**, enter the parameters used to connect to this Synergis™ unit.

IMPORTANT: The following settings are all correctly initialized at the time the Synergis™ unit is enrolled in your system. Do not change these settings unless you changed the unit's settings with Synergis™ Appliance Portal after the unit has been enrolled, or one of our representatives instructs you to do so.

- **Web address:** Web address for contacting Synergis™ Appliance Portal.
- **Username and Password:** Logon username and 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).
- **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.

6 Click **Apply**.

Switching Synergis™ units to different Access Managers

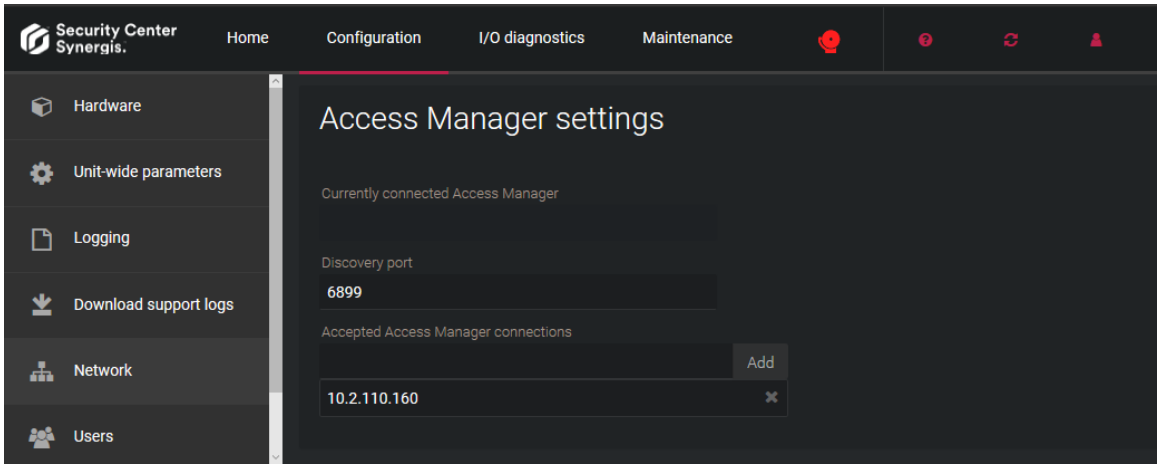
Once an Synergis™ unit is connected to an Access Manager, it only responds to that Access Manager. If you want the unit to respond to another Access Manager, you need to change its **Accepted Access Manager** connections list to replace the old one or add the new one.

Before you begin

Enable the Access Manager to connect to the Synergis™ unit by adding the Synergis™ extension in Security Center .

To switch an Synergis™ unit to a different Access Manager:

1 Log on to the Synergis™ unit.
2 Click on **Configuration** > **Network**.
3 Under *Access Manager settings*, enter the IP address of the new Access Manager in the **Accepted Access Manager connections** field.



4 Click **Add**.
5 Click **Save**.

After you finish

If the Synergis™ unit and its new Access Manager are on the same network segment, the unit is automatically added to the Access Manager. If the two are on different network segments, then add the Synergis™ unit to the Access Manager manually.

Creating temporary access rules through custom fields

[DEPRECATED] To accomodate seasonal cardholders, such as students who are enrolled during a semester, you can create access rules that are active only in a given time range.

Before you begin

IMPORTANT: Temporary access rules are supported natively in Security Center 5.7 SR1 and later. Because custom and native temporary access rules cannot be used together, we recommend that you use our native solution. If you are currently using the custom solution in Security Center 5.6, and want to upgrade to Security Center 5.7 SR1 or later, contact our Technical Assistance Center (GTAC) for help.

Custom field-based temporary access rules are only supported on units running Synergis™ Softwire version 10.4 and later, and Security Center Access Manager version 5.6.

What you should know

You must add two custom fields to the *Access rule* entity type in Security Center. For information on creating custom fields, see the *Security Center Administrator Guide*.

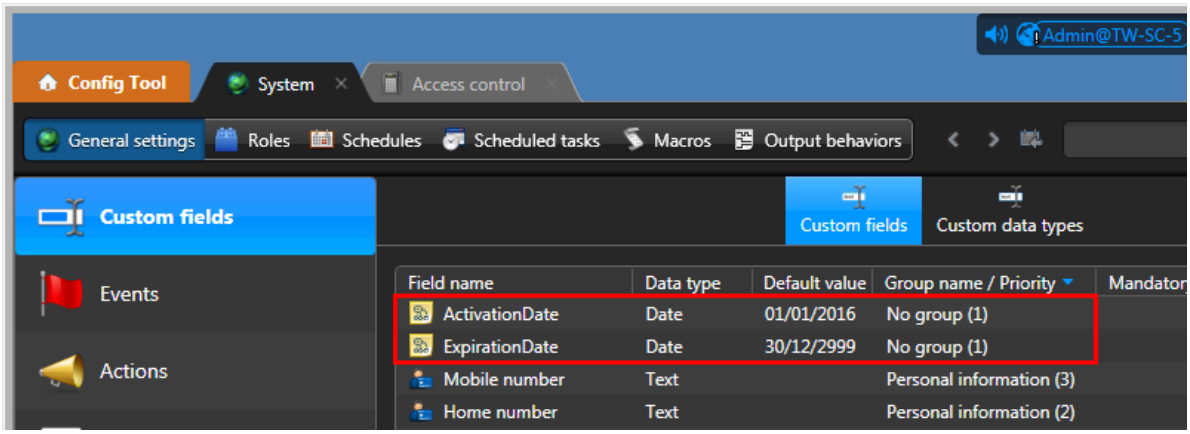
To create access rules with activation and expiration dates:

1 Connect to Security Center using Config Tool.

2 Open the *System* task and click **General settings** > **Custom fields**.

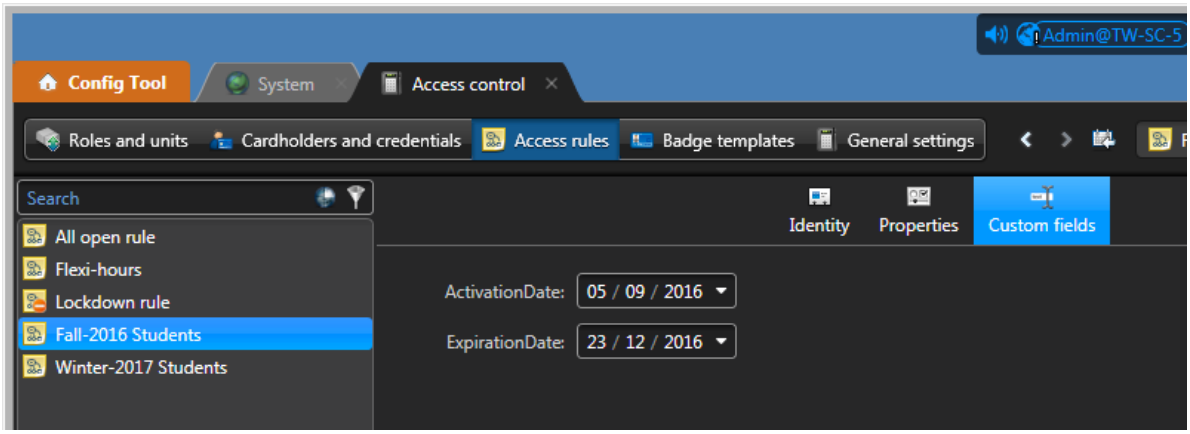
3 Add two *Date* or *DateTime* custom fields to the *Access rule* entity type with the following properties:

- **Field name**: ActivationDate; **Default value**: Any date in the past. For example, 1 January 2016.
- **Field name**: ExpirationDate; **Default value**: A date in the far future. For example, 31 December 2999.



Setting these default values ensures that existing access rules are not constrained by dates.

4 Create the access rules and set the *ActivationDate* and *ExpirationDate* accordingly.



For more information, see the *Security Center Administrator Guide*.

5 Click **Apply**.

The Access Manager synchronizes the affected Synergis™ units. The Synergis™ units apply the new access rules only within their defined date range, even when they are disconnected from the Access Manager.

4

Maintenance and troubleshooting

This section includes the following topics:

Logging on to the appliance using the alternative IP address

If you are unable to connect to the Synergis™ appliance using its hostname and you have not yet configured its IP address, use its fixed alternate IP address.

Before you begin

Try logging on using the appliance's hostname.

What you should know

The Synergis™ appliance's fixed alternate IP address for the **LAN1** port is: `172.16.20.11 /24`.

IMPORTANT: All Synergis™ appliances are configured in factory to respond to the same fixed IP address. Never enroll a Synergis™ appliance in Security Center using this fixed alternate IP address.

To log on to a Synergis™ appliance using the alternate IP address:

1. Open a web browser.
2. In the browser's address bar, type `https://172.16.20.11`.
   You will get a certificate error message.
3. Follow your browser's on-screen instructions to continue to the website.
4. In the *Synergis Appliance - Logon* page, select the interface language.
5. Enter the default username and password (`admin/softwire`), then click **Log on**.

The *Synergis™ Appliance Portal - Home* page appears.

After you finish

As a best practice, you should change the default logon password.

Checking and upgrading the appliance firmware

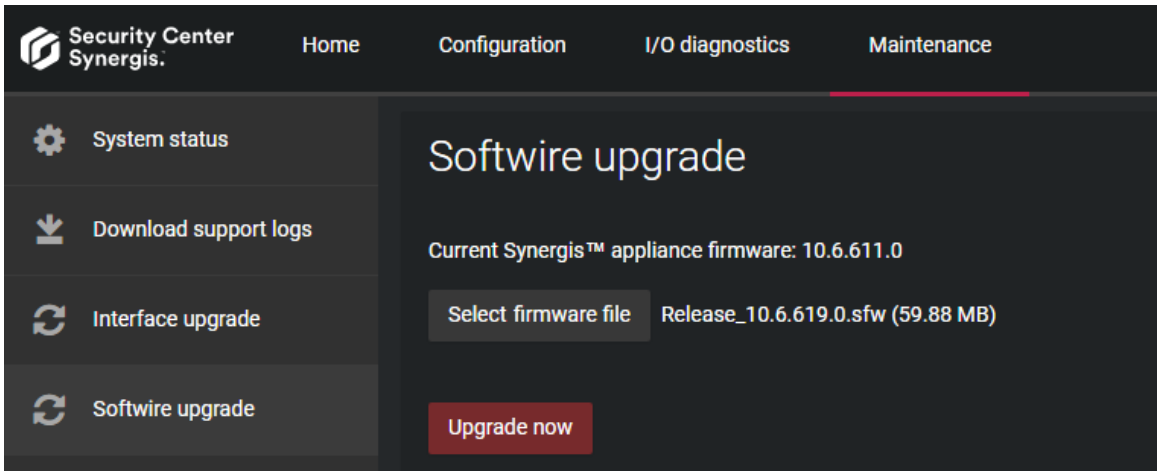
If your Synergis™ unit does not contain the latest firmware, upgrade it before you deploy your unit in the system.

Before you begin

Ask your Genetec Inc. representive about the latest firmware version, and download it from https://gtap.genetec.com if necessary.

To check and upgrade the appliance firmware:

1 Log on to the Synergis™ unit.
2 Click on **Maintenance** > **Softwire upgrade**.



The current firmware version is indicated in the *Synergis appliance firmware information* box.
3 If an upgrade is necessary, click **Select firmware file**.
4 In the file browser that opens, select the firmware file (*Release_10.6_xxx.y.sfw*).
The *.sfw* file must be located on your local drive.
5 Click **Open**.
6 Click **Upgrade now**

The Synergis™ appliance restarts. The upgrade will take a few minutes.

After you finish

Apply the recommended firmware to the interface modules attached to this unit.

Applying the recommended firmware to interface modules

Synergis™ unit works best when all connected interface modules are running the recommended firmware. The recommended firmwares are the firmware versions that are certified by Genetec. If your interface modules are loaded with newer firmware versions than the recommended ones, they will be downgraded.

Before you begin

Make sure the Synergis™ appliance firmware is up to date.

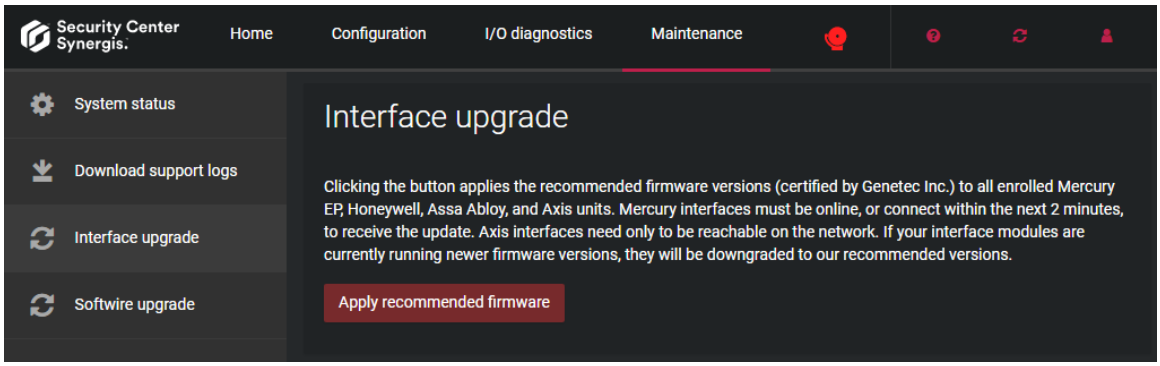
What you should know

For certain intelligent controllers, such as Assa Abloy IP Locks, Axis, and Mercury EP, you can apply the recommended firmware from the *Interface upgrade* page of Synergis™ Appliance Portal. For other manufacturers, you might have to use the manufacturer's software to apply the recommended firmware. For more information, see the *Synergis™ Softwire Integration Guide*.

To apply the recommended firmware to all enrolled and online interface modules:

1 From the *Interface upgrade* page, click **Apply recommended firmware**.

2 Click **Yes**.



Viewing system information on the Synergis™ units

You can view the Synergis™ unit's status and configuration files for troubleshooting purposes.

To view system information on a Synergis™ unit:

1 Log on to the Synergis™ unit.
2 Click on **Maintenance** > **System status**.
3 Select **Unit** to view the Synergis™ unit's hardware and firmware information.
4 Select **Network** to view the Synergis™ unit's network configuration and status.

After you finish

Download the unit configuration files.

Unit information about your Synergis™ unit

The *Unit* tab in the *System status* page of the Synergis™ Appliance Portal shows information about the Synergis™ unit's hardware and firmware.

Property name	Property value
Hostname	Hostname of the controller. The default hostname is the letters "SCL" followed by the controller's MAC address. The MAC address is the first address on the label sticker on the controller module. For example, if the label says `0010F32CF482`, then the default hostname is `SCL0010F32CF482`.
Number of CPUs	All Synergis™ units have two CPUs
System type	32-bit
RAM	2 GB for Synergis™ Cloud Link or 1 GB for Synergis™ Master Controller
Disk space	Disk space
Windows image version	Windows image version.
Windows updates information	Windows updates information.
System manufacturer	Genetec Inc.
Synergis™ appliance firmware information	Version and build date of the Synergis™ unit firmware. **NOTE:** Confirm with your representative of Genetec Inc. that you have indeed the latest version.
Discovery port	The discovery port used by the Access Manager roles to communicate with this Synergis™ 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.

Property name	Property value
Service uptime	Time elapsed since the last software restart.
Currently connected Access Manager	IP address of the Access Manager that is currently managing this unit.
List of all Genetec™ devices on this discovery port and subnet	List of the IP addresses of all Access Manager roles that have, at one time or another, been connected to this unit.
Offline log count	Number of logged events not yet synchronized with the Access Manager (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™ unit's own troubleshooting logs.
Number of configured channels	Number of communication channels that are configured with interface modules attached. The Synergis™ unit features two types of channels, IP and RS-485.

Downloading the unit configuration files for your Synergis™ unit

You can download your entire unit's configuration as compressed files for troubleshooting purposes.

To download the unit's configuration files:

1 Log on to the Synergis™ unit.
2 Click on **Maintenance** > **System status**.
3 At the bottom of the page, click **Download configuration files**.
4 Click **Save**.

Restarting the Synergis™ unit hardware or software

During a debugging session, the support technician may ask you to perform a hard or a soft restart on the Synergis™ unit.

What you should know

A hard restart, or *system restart*, is required when you are reconnecting or changing the four-port RS-485 module (applies only to SMC), or when you experience hardware problems. A soft reboot, or a *software restart*, is rarely required. The Synergis™ unit automatically restarts its firmware after you change the firmware version. Manual software restarts are only used for debugging or support purposes.

To restart the unit's hardware or software:

1 Log on to the Synergis™ 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**.

Related Topics

DIP switch command codes for Synergis Cloud Link on page 4

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're 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 explain how the product works and provide instructions on how to use the product features. Genetec Patroller™ and the Sharp Portal also include context-sensitive help for each screen. 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 the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** 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 the Technical Information Site for potential fixes, workarounds, or known issues.

  To access the Technical Information Site, log on to Genetec™ Portal and click Technical Information. Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: EN_GLM_ASSURANCE and EN_GLM_ADVANTAGE.

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log in or sign up at https://gtapforum.genetec.com.
- **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, please contact GTAC at https://gtap.genetec.com.
- For issues with license content or part numbers, or concerns about an order, please 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, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at https://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.