Security Center

Synergis Master Controller Configuration Guide 2.1

Click here for the most recent version of this document.

Genetec

Copyright notice

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein. The use of this document is subject to the disclaimer of liability found in the end-user license agreement.

All specifications are subject to change without notice.

Document information

Document title: Synergis Master Controller Configuration Guide 2.1

Document number: EN.702.003-V2.1.B(2)

Document update date: December 11, 2013

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

About this Guide

This guide describes how to configure Synergis Master Controller for use with Security Center. It assumes you are familiar with the Security Center 5 platform, and specifically with Synergis access control system.

This guide supplements the Security Center documentation, and the *Synergis Master Controller Hardware Installation Guide*. You may also require the *Synergis Master Controller Integration Guides* that provide specific instructions regarding the third-party hardware you have in your system. For more information, see "Where to find product documentation" on page 46.

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 configuration software.

Notes and notices

This section explains how the following notes and notices are used 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.

Contents

1

Introduction to Synergis Master Controller

This section provides an overview of Synergis Master Controller and how it works with Security Center.

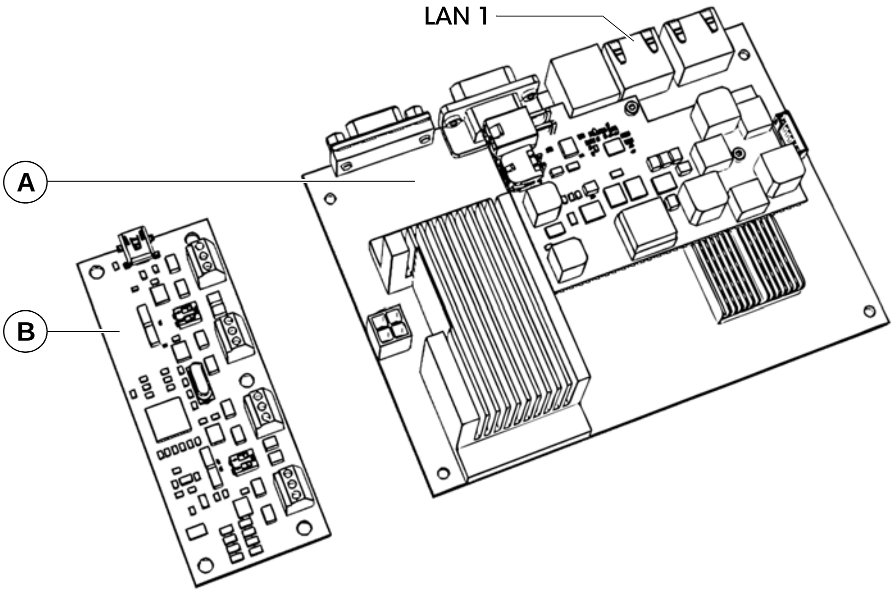
This section includes the following topics:

What is Synergis Master Controller?

Synergis Master Controller (SMC) is Genetec's access control unit that supports a variety of third party interface modules over IP, USB, and RS-485. SMC is seamlessly integrated to Security Center, and is capable of making the access control decisions independently of the Access Manager. SMC and accessories can be housed inside an enclosure that make up the *Synergis access control system*.

NOTES

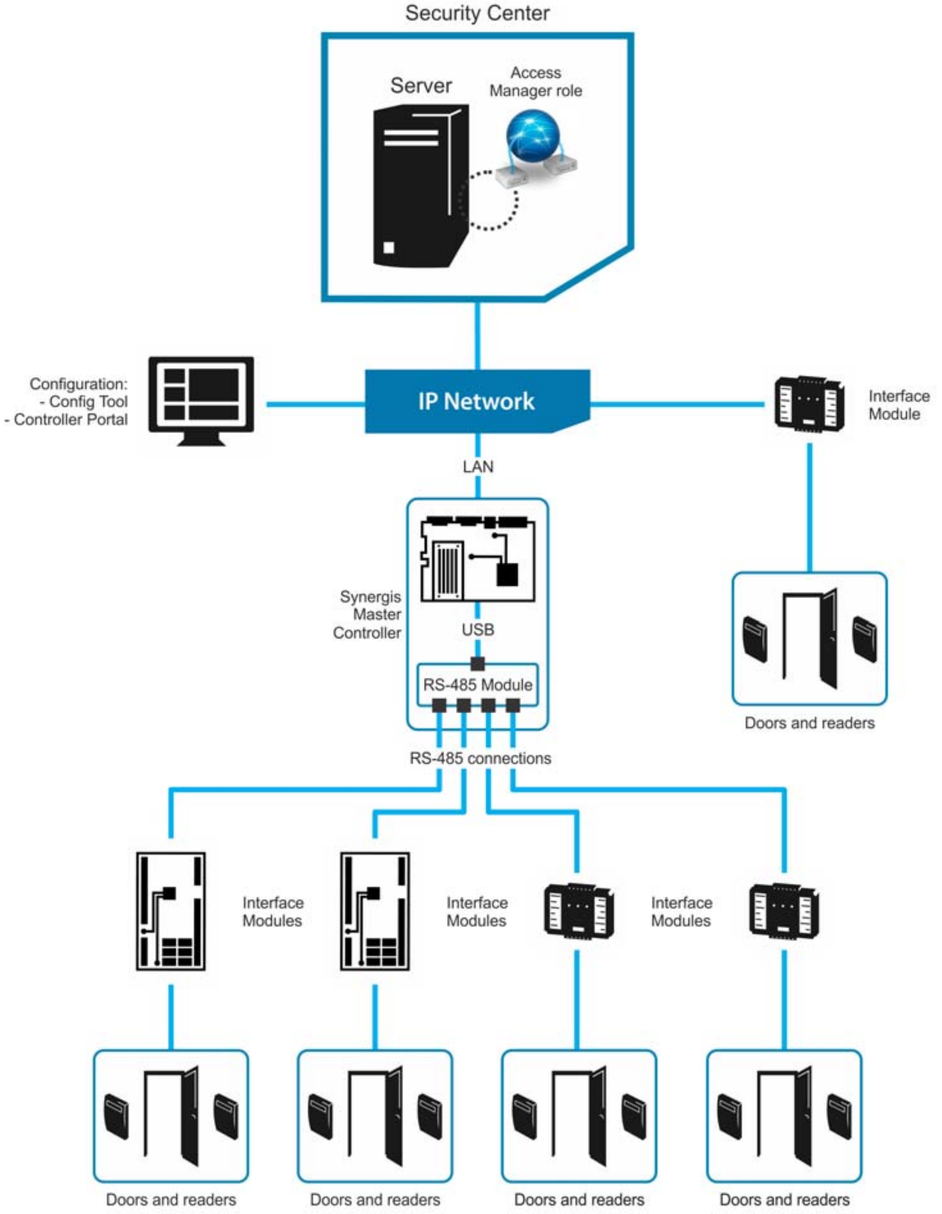
- For a hardware description of the Synergis access control system, assembly and installation instructions, see the *Synergis Master Controller Hardware Installation Guide*.
- For a complete product description and specification, see "Synergis Master Controller" on www.genetec.com.



A	Controller module	Processing component of SMC with IP capability, pre-loaded with the controller firmware and a web-based administration tool, *Controller Portal*.
B	Four-port RS-485 module	RS-485 communication component of SMC with four 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 IP or USB connections, the Four-port RS-485 module is not needed.

How SMC works with Security Center

SMC works with the Security Center to manage your access control system. The controller module, interface modules, and power supply are housed inside an enclosure to provide the *Synergis access control solution*.



2

Getting started with Controller Portal

This section provides an overview of Controller Portal, the web-based administration tool for SMC. You'll learn how to log on to your SMC unit from Controller Portal, and how to navigate in Controller Portal.

This section includes the following topics:

- "What is Controller Portal?" on page 5
- "Log on to SMC" on page 6
- "Change the logon password" on page 7
- "Controller Portal interface tour" on page 8

What is Controller Portal?

Controller Portal is the web-based interface for the configuration and maintenance of SMC. It allows you to connect to an SMC unit using a web browser.

Controller Portal allows you to perform the following tasks:

- Change the security password required to log on to the SMC unit.
- Configure the network settings on the SMC unit so it works on your system.
- Configure SMC to accept connections from specific Access Manager servers.
- Configure the properties of the interface modules attached to the SMC unit.
- Configure the access control behavior for SMC, in both online and offline modes.
- View the activity logs stored on the SMC unit.
- Test and diagnose the interface module connections to the SMC unit.
- View and export the SMC status and configuration.
- Upgrade the SMC firmware.
- Restart the SMC hardware or software.
- Update security clearance levels assigned to Security Center areas manually on the SMC unit when the connection to the Access Manager is lost.

NOTE You cannot perform the following tasks with the Controller Portal. You have to use the Config Tool instead.

- Enable/disable the *Mixed mode* operation.
- 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 IO linking.

For more information, see “Deploying Synergis” in the *Security Center Administrator Guide*.

Log on to SMC

Before you begin: You need to know the following information to log on for the first time.

- The SMC hostname is `SMC` followed by the controller's MAC address, which is the first alpha-numeric code on the label sticker on the controller module. For example, if the label says `0010F31A176A`, then the default hostname is `SMC0010F31A176A`.
- The default username and password are `admin` and `softwire`. Change them after your first logon.
- Only one user can be connected to SMC at any given time. By logging on, you'll log off the person logged on before you.

To log on:

1 (First time logon only) Connect the SMC's **LAN 1** connector to your LAN.

For the location of the **LAN 1** connector on the controller module, see "What is Synergis Master Controller?" on page 2.

2 Open a web browser.

3 In the browser's address bar, type `https://` followed by the SMC hostname or IP address (for example, `https://SMC0010F31A176A`).

If you are unable to connect to SMC using its hostname and you haven't yet configured its IP address, then "Log on to SMC using the alternate IP address" on page 33.

4 (New browser session only) If you opened a new browser session to log on to SMC, you'll 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 SMC.

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

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

The **Controller Portal - Home** page appears.

After you are done: (Before you deploy the SMC unit in the field) "Change the logon password" on page 7.

Change the logon password

Best practice: If you are logging on to the SMC for the first time, the default username and password are `admin` and `softwire`. We recommend that you change the default password before you deploy the SMC unit in the field.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **Users**.

3 From the **User configuration** page, select the user you want to modify and click **Change password**.

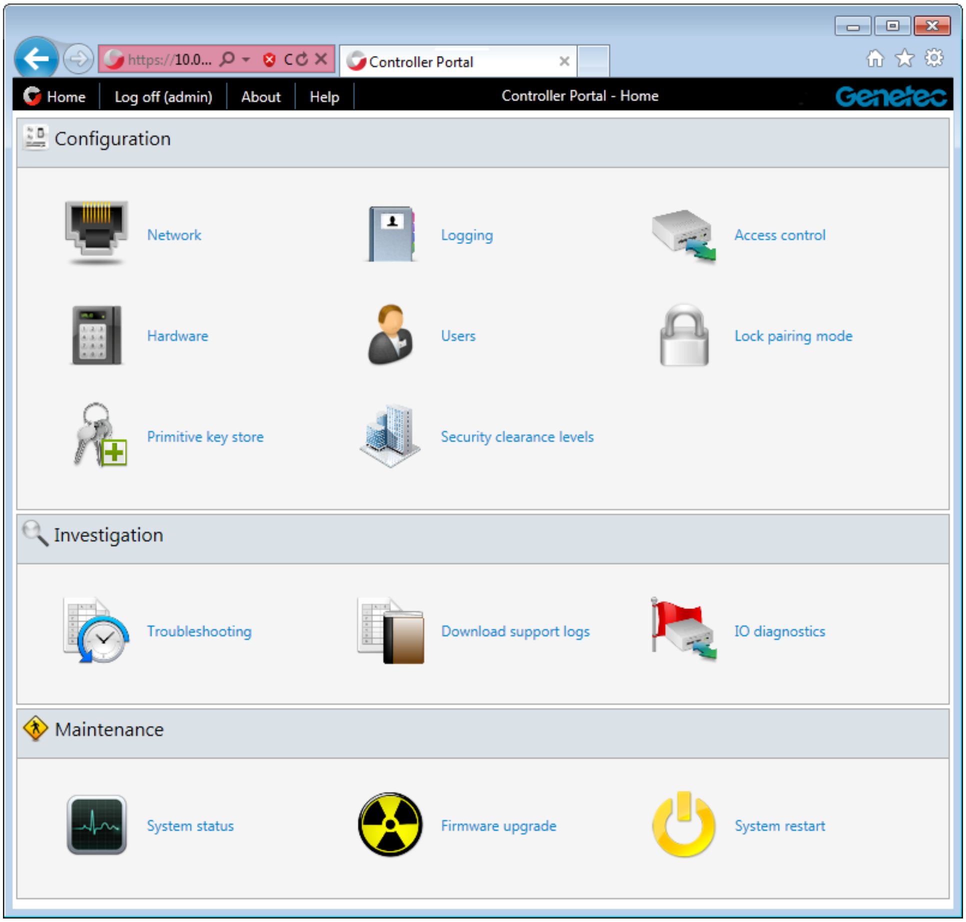
4 In the **Change password** dialog box, enter the new password twice and click **Apply**.

The new password is applied immediately.

After you are done: If the unit was already connected to an Access Manager, you must also change the logon password in the Config Tool. See "Keep the Access Manager in sync with the SMC unit" on page 29.

Controller Portal interface tour

The Controller Portal's *Home* page is divided into tasks used for configuration, investigation, and troubleshooting and maintenance.



The links on this page are described in the following:

- **Home.** Returns to *Home* page.
- **Log off.** Logs you off from SMC and displays the *Logon* page.
  When you are logged on, the username is shown in brackets.
- **About.** Shows the SMC firmware version and copyright information.
- **Help.** Opens the *Synergis Master Controller Configuration Guide* in a separate browser page.
- **Network.** Opens the network configuration page, which is where you configure the SMC unit to work on your network (see "Configure the SMC's network properties" on page 13)

and the Access Manager it should obey to (see "Switch the SMC unit to a different Access Manager" on page 31).

- **Logging.** Used to configure the event logging options for troubleshooting purposes. For more information, see "Configure the event logging options" on page 24.
- **Access control.** Used to configure the access control behavior that applies to all interface modules connected to the SMC unit. For more information, see "Configure the unit-wide access control behavior" on page 21.
- **Hardware.** Used to define the interface modules attached to the SMC unit. For more information, see "Configure the interface modules attached to SMC" on page 15.
- **Users.** Used to configure who has the rights to log on to SMC and change its configuration. For more information, see "Change the logon password" on page 7.
- **Lock pairing mode.** (Only applicable to Assa Abloy IP locks) Used to discover IP locks on the network. For more information, see “Configure IP locks attached to SMC” in the *Synergis Master Controller Integration Guide for Asso Abloy IP Locks*.
- **Primitive key store.** (Only applicable to STid readers) Used to change the *Signature* and *Encipherment* keys used to communicate with the STid readers controlled by SMC. For more information, see “Changing the default communication parameters” in the *Synergis Master Controller Integration Guide for STid readers*.
- **Security clearance levels.** (For threat level management) Used to change the *Security clearance* assigned to areas when the connection between SMC and its Access Manager is lost. For more information, see "Setting security clearance levels manually" on page 42.
- **Troubleshooting.** Used to generate troubleshooting reports by querying the event log saved on the SMC unit. You can view your report in the browser or export it to a file. For more information, see "Generate troubleshooting reports" on page 35.
- **Download support logs.** (Only appears if *Support logs* are enabled) Used to download support logs to help Genetec Technical Support troubleshoot your system. For more information, see "Configure the event logging options" on page 24.
- **IO diagnostics.** Shows the IO diagnostics page for this SMC unit. Use this page to watch the states of the contacts and readers change in real time as you perform tests with the devices connected to the interface modules. For more information, see "Test the interface modules attached to SMC" on page 19.
- **System status.** Shows a snapshot of your unit and network status. You can also export the system information to a CSV file from this page. For more information, see "Viewing and exporting system information" on page 37.
- **Firmware upgrade.** Used to upgrade the SMC firmware or to revert it to the previous version (if available). For more information, see "Check and upgrade the SMC firmware" on page 34.
- **System restart.** Used to restart the SMC hardware or software. For more information, see "Restarting the SMC hardware or software" on page 41.

3

SMC configuration

This section explains how to configure SMC for Security Center.

This section includes the following topics:

Configuration prerequisites

Before you begin configuring the SMC unit, do the following:

- Read the *Synergis Master Controller 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 SMC unit.
- Configure the hardware settings (DIP switches, address dials, etc.) to their final position on the interface modules. For more information, see the *Synergis Master Controller Integration Guide* for the hardware types you have.
- Connect the interface modules to the SMC 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 *Synergis Master Controller Hardware Installation Guide*.
- Download the latest SMC firmware from https://gtap.genetec.com.
- Install and configure Security Center with at least one Access Manager role. For more information, see “Deploying Synergis” in the *Security Center Administrator Guide*.

Configuration process overview

Before you begin: Read "Configuration prerequisites" on page 11.

The following table summarizes the SMC configuration process.

Phase	Description	See
1	SMC comes with a factory-assigned hostname. If your network does not support DHCP, your IT department must assign the controller a new IP address.	"Configure the SMC’s network properties" on page 13
2	Make sure you have the latest SMC firmware, and upgrade if necessary.	"Check and upgrade the SMC firmware" on page 34
3	Physically attach the interface modules to the controller module.	*Synergis Master Controller Hardware Installation Guide*
4	Establish communication between the SMC and its attached interface modules by configuring them in Controller Portal.	"Configure the interface modules attached to SMC" on page 15
5	Test your hardware connections and configuration and make adjustments if necessary.	"Test the interface modules attached to SMC" on page 19
6	Configure the access control behavior you want SMC to exhibit.	"Configure the unit-wide access control behavior" on page 21
7	(Optional) Select the event logs you want to be available for troubleshooting.	"Configure the event logging options" on page 24
8	Add the SMC unit to an Access Manager so it becomes part of your Security Center system.	"Enrolling the SMC unit in Security Center" on page 26

Configure the SMC’s network properties

You need to configure the SMC unit’s network properties so it can be reached on your Security Center system’s network.

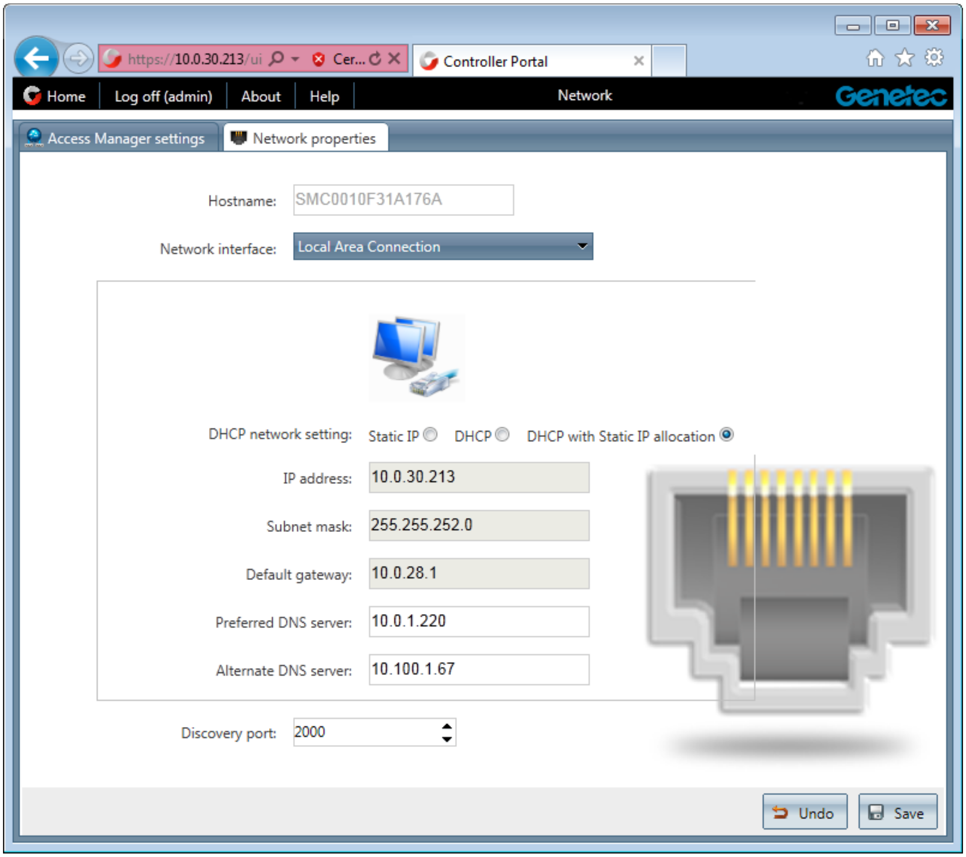
Before you begin: SMC comes with a factory-assigned hostname. If your network does not support DHCP, your IT department must assign the controller a new IP address.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal** - **Home** page, click **Network**, then **Network properties**.

3 Select the network interface used to connect the SMC unit to its Access Manager.

Local Area Connection corresponds to **LAN 1**.



Hostname: SMC0010F31A176A

Network interface: Local Area Connection

DHCP network setting: Static IP ○ DHCP ○ DHCP with Static IP allocation ●

IP address: 10.0.30.213

Subnet mask: 255.255.252.0

Default gateway: 10.0.28.1

Preferred DNS server: 10.0.1.220

Alternate DNS server: 10.100.1.67

Discovery port: 2000

4 Configure the SMC unit’s IP address and the network properties.

IMPORTANT If the SMC is not on the same network segment as the Access Manager, then the SMC's IP address must be static, or the DHCP server must be configured to always assign the same IP address to the SMC. Otherwise, the SMC will not be able to communicate with its Access Manager.

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

   The discovery port is used by the Access Manager to find SMC units on the network. You do not need to change it unless its default value (`2000`) is reserved by your IT department for a different purpose.

6 Click **Save** (💾).

The controller firmware restarts, and you are automatically redirected to the SMC’s new IP address.

After you are done: Continue with the next step in the "Configuration process overview" on page 12.

Configure the interface modules attached to SMC

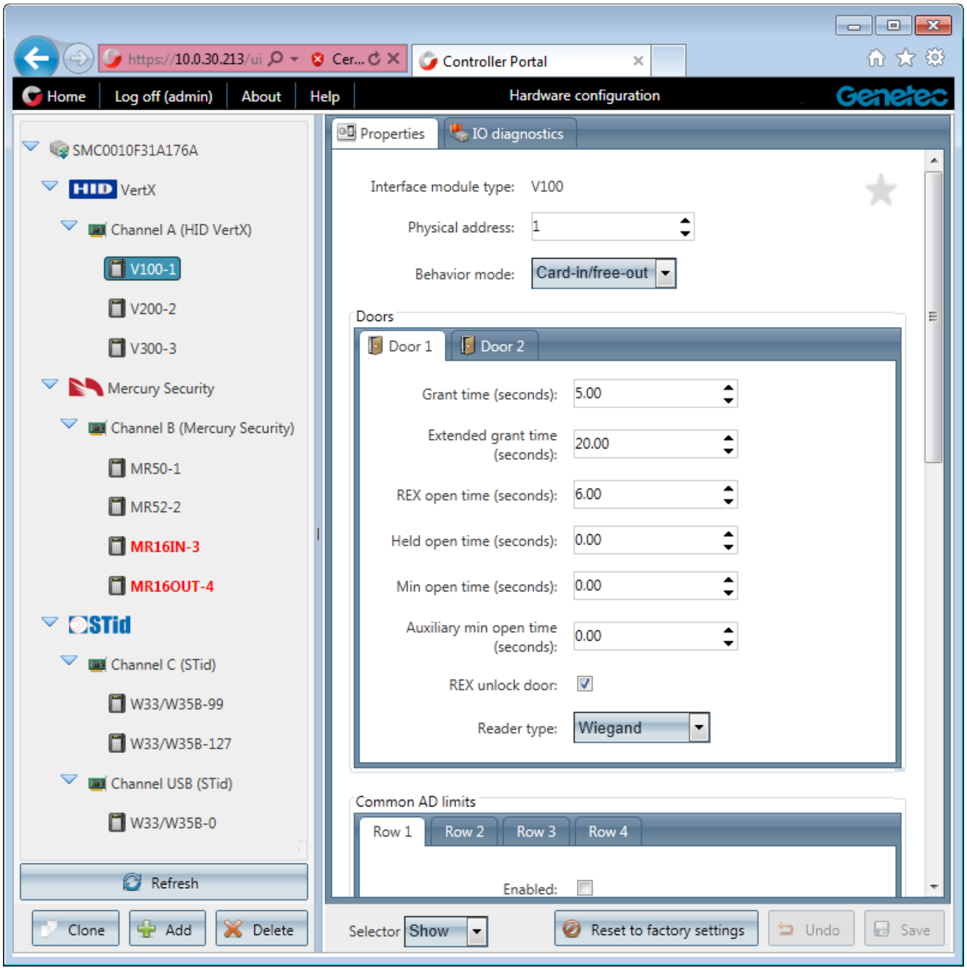
An interface module is a third party device that communicates with SMC over IP, USB, or RS-485, and provides input, output, and reader connections to the controller module.

Before you begin: Physically attach your interface modules to the controller module.

To establish communication between the SMC and the attached interface modules, you need to configure them in Controller Portal.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal** - **Home** page, click **Hardware**.



Interface module type: V100

Physical address: 1

Behavior mode: Card-in/free-out

Doors

Door 1

Grant time (seconds): 5.00

Extended grant time (seconds): 20.00

REX open time (seconds): 6.00

Held open time (seconds): 0.00

Min open time (seconds): 0.00

Auxiliary min open time (seconds): 0.00

REX unlock door: ☑

Reader type: Wiegand

Common AD limits

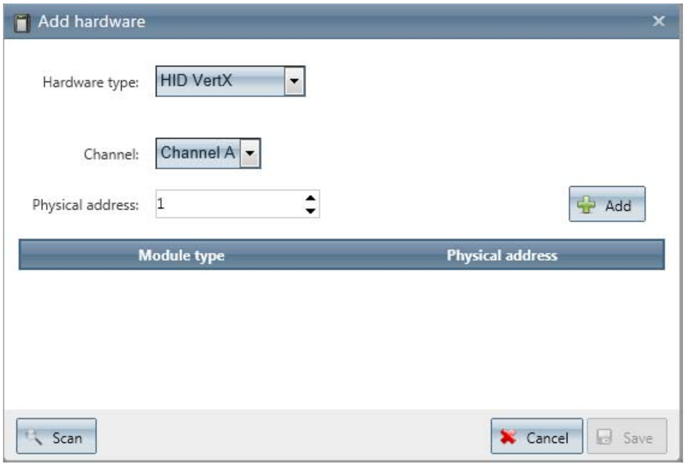
Row 1

Enabled: ☐

Selector Show

3 In the **Hardware configuration** page, 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.



Hardware type: HID VertX

Channel: Channel A

Physical address: 1

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

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

Do one of the following:

- To add manually, click **Add** (➕).
- To discover, 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 just added appear in the hardware tree.

7 For each interface module you just added, select it from the hardware tree, and configure its settings in the **Properties** tab.

For the description of these settings, refer to the manufacturer's documentation. Make the changes as needed. See also "Change the default values" on page 17.

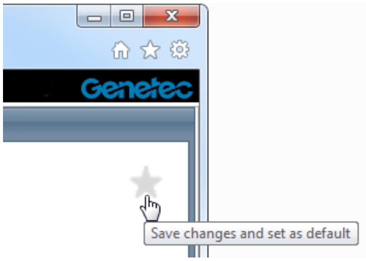
8 At the bottom of the page, click **Save** (💾).

After you are done: Continue with "Test the interface modules attached to SMC" on page 19.

Change the default values

SMC is configured with factory default settings for all supported interface modules. You can modify factory default settings and save them as the new default settings for each type of module. This can simplify the configuration process when you have many interface modules of the same type to configure.

1 From hardware tree, select the interface module you want to use as model.
2 In the **Properties** tab, make all necessary changes to its settings.
3 Click the grey star at the upper right corner of the page.

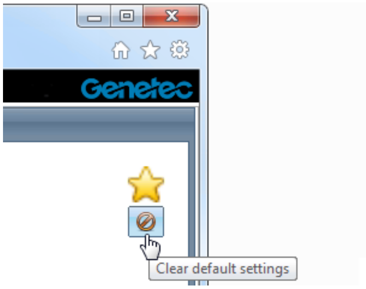


Your changes are saved as new default settings and the star becomes yellow. The next time you add an interface module of the same type, your new default values will be used to initialize the property page.

Clear new default values

Discontinue use of your new default values.

1 From hardware tree, select the interface module you set as default (with the yellow star).
2 In the **Properties** tab, click **Clear default settings** (⊘) under the yellow star.



The star becomes grey. The next time you add an interface module of the same type, the factory default settings will be used. See also "Cloning interface module settings" on page 18.

NOTE Do not confuse this button (**Clear default settings**) with the one found at the bottom of the page (**Reset to factory settings**). The button under the yellow star 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 button at the bottom of the page resets the values on the current page to their factory defaults immediately.

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.

NOTE If you want to clone your interface modules, do not create them first. If you already did, delete them first, then re-create them by cloning.

1 In the **Hardware configuration** page, add and configure one interface module as your model for cloning.

2 Select that interface module you just configured and, at the bottom of the hardware tree, click **Clone** (⧉).

3 In the **Clone 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 are done: Modify the settings of the cloned interface modules as required.

See also "Change the default values" on page 17.

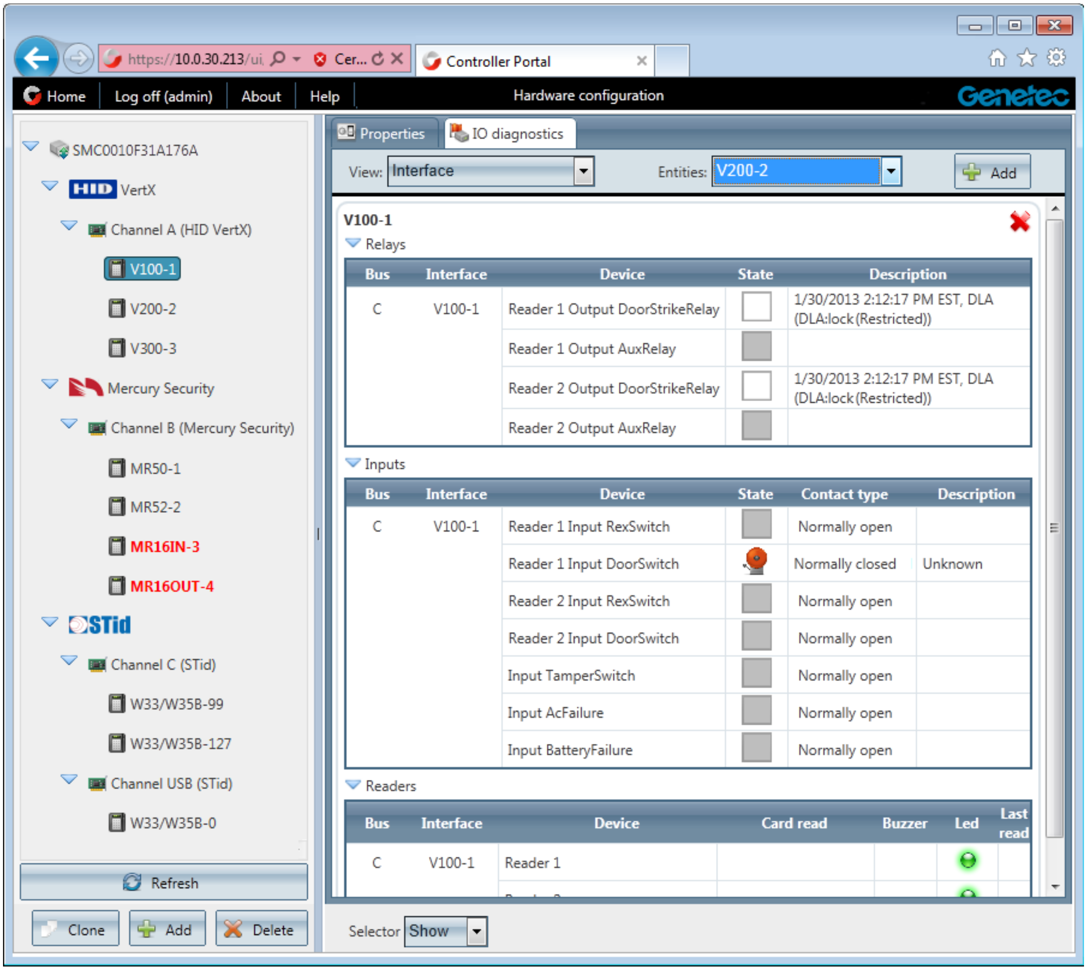
Test the interface modules attached to SMC

Before you begin: "Configure the interface modules attached to SMC" on page 15.

Test your hardware connections and configuration by monitoring their responses on the IO diagnostics page in real time. You can customize this page to show the elements you want to monitor.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **IO diagnostics**.



View: Interface

Entities: V200-2

V100-1

Relays

Bus	Interface	Device	State	Description
C	V100-1	Reader 1 Output DoorStrikeRelay	□	1/30/2013 2:12:17 PM EST, DLA (DLA:lock (Restricted))
		Reader 1 Output AuxRelay	▨	
		Reader 2 Output DoorStrikeRelay	□	1/30/2013 2:12:17 PM EST, DLA (DLA:lock (Restricted))
		Reader 2 Output AuxRelay	▨	

Inputs

Bus	Interface	Device	State	Contact type	Description
C	V100-1	Reader 1 Input RexSwitch	▨	Normally open	
		Reader 1 Input DoorSwitch	●	Normally closed	Unknown
		Reader 2 Input RexSwitch	▨	Normally open	
		Reader 2 Input DoorSwitch	▨	Normally open	
		Input TamperSwitch	▨	Normally open	
		Input AcFailure	▨	Normally open	
		Input BatteryFailure	▨	Normally open	

Readers

Bus	Interface	Device	Card read	Buzzer	Led	Last read
C	V100-1	Reader 1			●	

Selector Show

3 Select what you want to monitor in real time.

a From the **View** drop-down list, select the type of element you wish to monitor.

b From the **Entities** drop-down list, select the entity you wish to monitor.

c At the top of the page, click **Add** (➕).

The elements you selected are added to your page.

4 To remove a group of elements, click ❌ at the upper right corner of the group.

5 Activate the devices (card readers, door sensors, door locks, and so on) attached to the SMC unit through the interface modules.

If they do not behave as expected, check your connections and your interface module configurations. See "Configure the interface modules attached to SMC" on page 15.

After you are done: Continue with "Configure the unit-wide access control behavior" on page 21.

Configure the unit-wide access control behavior

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

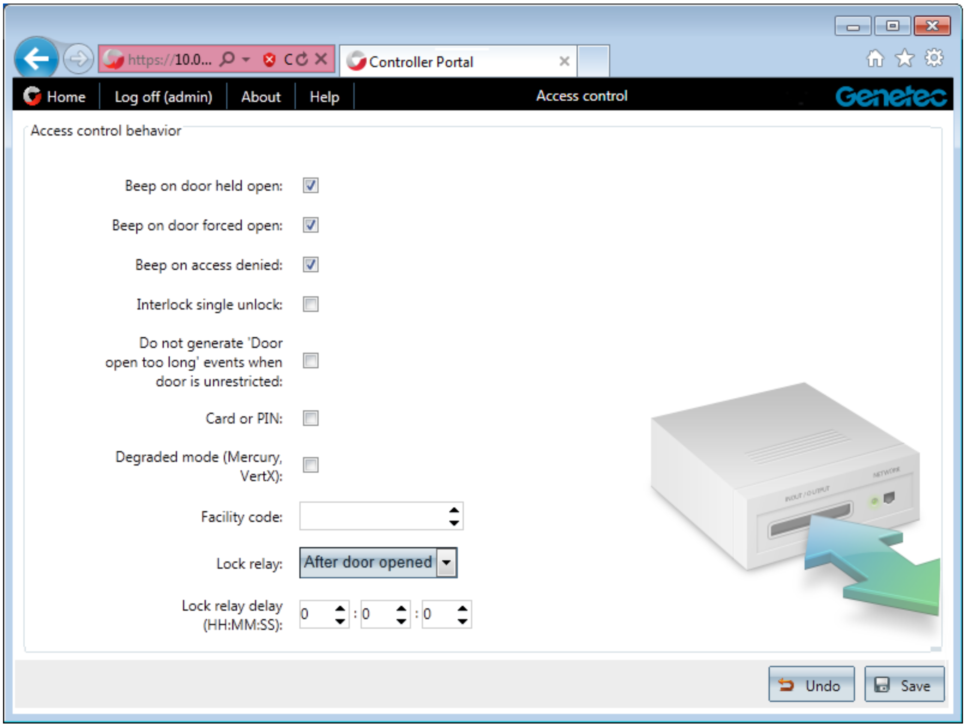
Before you begin: Some settings only apply to certain types of interface modules and are not shown unless those interface modules are configured for your unit. See "Configure the interface modules attached to SMC" on page 15.

To configure the unit-wide access control behavior:

1 "Log on to SMC" on page 6.

2 From the **Controller Portal** - **Home** page, click **Access control**.

3 In the **Access control** page, select the options you want SMC to support.



Access control behavior

Beep on door held open: ☑

Beep on door forced open: ☑

Beep on access denied: ☑

Interlock single unlock: □

Do not generate 'Door open too long' events when door is unrestricted: □

Card or PIN: □

Degraded mode (Mercury, VertX): □

Facility code:

Lock relay: After door opened

Lock relay delay (HH:MM:SS): 0 : 0 : 0

- *Beep on door held open.* The reader at the door beeps when the door is held open for too long. The delay before the beep is a door property that needs to be set with Config Tool. For more information, see the *Security Center Administrator Guide.* (Default=enabled).

  TIP To stop the beeping caused by a *Door open too long* event, simply close the door.

- *Beep on door forced open.* The reader at the door beeps when the door sensor indicates that the door is open while it is supposed to be locked. No beep will be heard if the *Door forced open* event is ignored at the door. For more information, see the *Security Center Administrator Guide.* (Default=enabled).

  TIP To stop the beeping caused by a *Door forced open* event, scan a valid credential at the door reader or manually unlock the door from Security Desk.

- *Beep on access denied.* The reader at the door beeps when an access request is denied. (Default=enabled).
- *Interlock single unlock.* An interlock is a system with multiple doors where only one door can be opened at any time. The standard behavior is to allow multiple doors to be unlocked, but only one door to be opened by locking all other doors the moment one door is open. Selecting this option changes the behavior to allow only one door to be unlocked at any given time. (Default=disabled). For more information, see "Configure interlock" in the *Security Center Administrator Guide.*

  NOTE A change to this setting would take effect only after a software restart (see "Restarting the SMC hardware or software" on page 41).

- *Do not generate 'Door open too long' events when door is unrestricted.* This option allows you to ignore the Security Center setting to trigger *Door open too long* events when the door is unlocked either for maintenance or by an unlock schedule. (Default=disabled). For more information, see "Configuring doors" in the *Security Center Administrator Guide.*
- *Card or PIN.* Applies to card and PIN readers only. The default for any card and PIN reader is **Card only**; that is, only the card is used to grant access.

  Select this option to allow **Card or PIN**; that is, either the card or the PIN can be used to grant access.

  NOTE To enforce **Card and PIN**; that is, both the card and the PIN must be used to gain access, you need to configure the property of the reader in Config Tool. For more information, see "Configuring doors" in the *Security Center Administrator Guide.*

- *Degraded mode (Mercury, VertX).* This option applies only to Mercury and HID VertX interface modules.

  In *degraded mode*, the interface module makes decisions on its own when the connection to the SMC 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.
- *Lock relay.* This setting tells SMC 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.

4 Click **Save** (💾).

All changes are effective immediately, except for *Beep on access denied*, *Interlock single unlock*, and *Card or PIN*, which become effective only after a software restart.

After you are done: Continue, if necessary, with the next step in the "Configuration process overview" on page 12.

Configure the event logging options

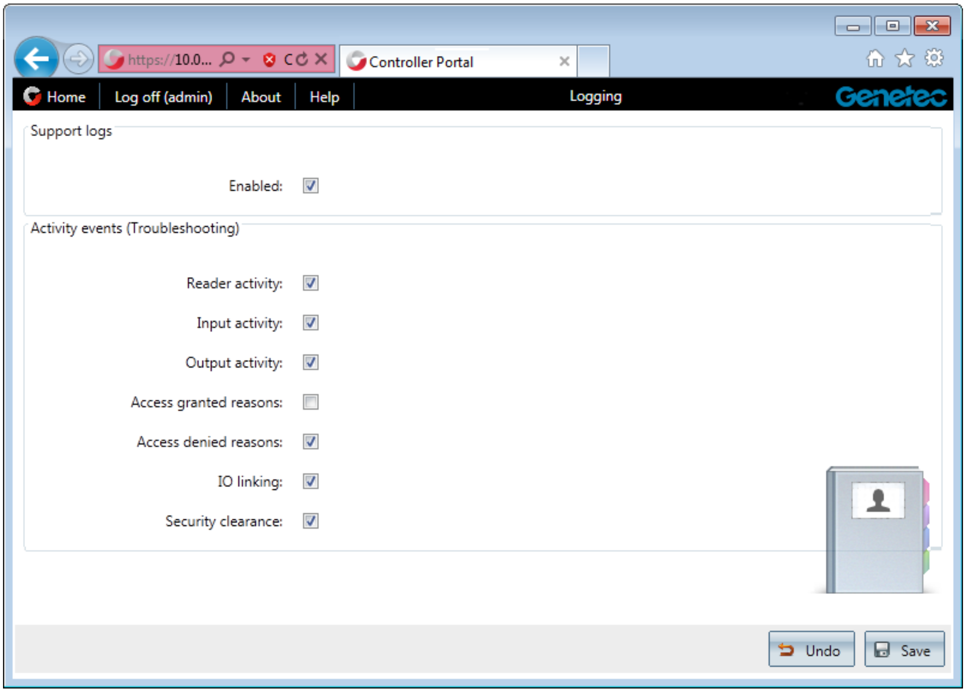
SMC can keep detailed logs of all access control decisions it makes in the troubleshooting logs. These logs are turned off by default. You need to turn them on if you wish to view them in the *Troubleshooting* report.

NOTE Events not related to normal operation, such as hardware, software, and network issues are always logged.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal** - **Home** page, click **Logging**.

3 In the **Logging** page, select the types of events you wish to log.



Support logs

Enabled: ☑

Activity events (Troubleshooting)

Reader activity: ☑

Input activity: ☑

Output activity: ☑

Access granted reasons: □

Access denied reasons: ☑

IO linking: ☑

Security clearance: ☑

4 Enable the **Support logs** only when instructed by Genetec Technical Support. The link **Download support logs** would appear in the **Home** page under the **Investigation** group. Wait for the support technician's instructions to download the desired log files.

5 Enable the **Activity events** for the **Troubleshooting** report.

These logging options provide more information for troubleshooting than what you get from the generic Security Center investigation reports.

The activity events that you can log are:

- *Reader activity.* All reader events, such as card read, PIN entered, and when a reader mode has been changed.

- *Input activity.* All input state changes.
- *Output activity.* All output state changes.
- *Access granted reasons.* All access granted events and the reason for doing so (granted by access rule, REX, manual unlock, antipassback exemption, etc.).
- *Access denied reasons.* All access denied events and the reason for doing so (denied by access rule, no rules to grant access, outside rule schedule, expired credential, inactive cardholder, lost credential, stolen credential, unknown credential, etc.).
- *IO linking.* All IO linking events related to hardware zones (arming and disarming).
- *Security clearance.* All changes to security clearance due to threat level activation and deactivation.

NOTE All activity events are logged with the *severity level* set to “Information”. For more information, see "Generate troubleshooting reports" on page 35.

6 Click **Save** (💾).

After you are done: Continue, if necessary, with the next step in the "Configuration process overview" on page 12.

Enrolling the SMC unit in Security Center

Before you begin: "Configure the SMC's network properties" on page 13

To enroll an SMC unit in your Security Center system, you must assign it to an Access Manager. The Access Manager must be able to find the SMC units on the network, and the SMC unit must be configured to respond to the Access Manager commands.

1. "Enable the Access Manager to connect to the SMC units" on page 26.

   All new SMC units found on the same network segment as the Access Manager that has never been enrolled before will automatically be added to the Access Manager. See "About automatic discovery" on page 28.
2. If the SMC unit was added to another Access Manager before, then
   - "Switch the SMC unit to a different Access Manager" on page 31.
3. If the SMC unit is not on the same network segment as the Access Manager, then
   - "Add the SMC unit to an Access Manager manually" on page 28,

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

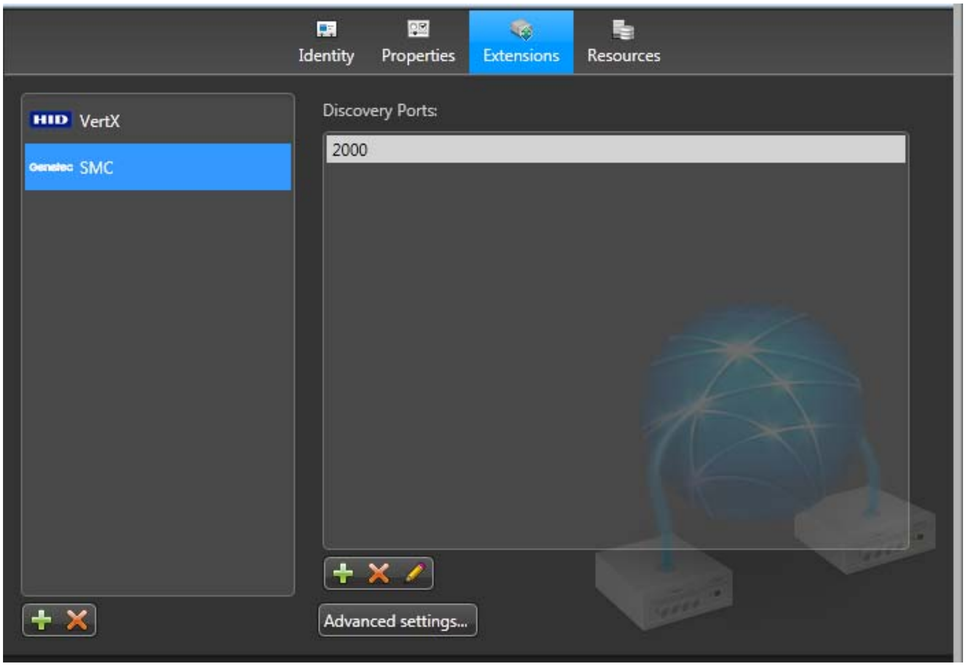
After you are done: Associate the peripherals (readers, inputs, outputs, etc.) controlled by this unit to doors and zones defined in your system. For more information, see "Deploying Synergis" in the Security Center Administrator Guide.

Enable the Access Manager to connect to the SMC units

You must configure the SMC extension with the same discovery port used by the SMC units on the Access Manager to enable it to connect to the SMC units on your network.

1. Log on to Security Center with Config Tool.
2. Open the **Access control** task and select the **Roles and units** view.
3. Select the Access Manager role ( ) and select the **Extensions** tab.
4. Under the extension list, click **Add an item** (+).
5. In the **Add extension** dialog box, select **SMC**, and click **Add**.
6. In the extension list, select the **SMC** extension.
7. Under the list of **Discovery ports**, click **Add an item** (+).

8 In the **Discovery port** dialog box, enter the port number configured on the SMC units.



Do not change the suggested default value (`2000`) unless it is reserved by your IT department for a different purpose.

If you decide to use a different discovery port, you must change it on the SMC unit as well. See "Change the discovery port on SMC" on page 28.

9 Click **Create**, then click **Apply** (✓).

After a few seconds, the SMC units that are newly introduced to your system (meaning that they have never been connected to any Access Manager before) and found on the same network segment as the Access Manager, are automatically added to the Access Manager. For more information, see "About automatic discovery" on page 28.

After you are done: If the SMC units are not automatically added to the Access Manager, then "Add the SMC unit to an Access Manager manually" on page 28.

Change the discovery port on SMC

The SMC unit and its Access Manager must use the same discovery port (default = `2000`) for the two to talk to each other. If you change the discovery port on the Access Manager, you must change it on the SMC unit as well.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal** - **Home** page, click **Networks**, then **Network properties**.

3 Set the **Discovery port** to the value used by the Access Manager.

4 At the bottom of the page, click **Save** (💾).

About automatic discovery

Automatic discovery is how new IP units on the network are automatically added to Security Center. The role responsible for the units broadcasts a discovery message on a specific port, and the units listening on that port respond with a message that contains the connection information about itself.

An SMC unit can be automatically discovered by the Access Manager role under the following conditions:

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

In any other situation, the SMC units must be added manually. See "Add the SMC unit to an Access Manager manually" on page 28.

Add the SMC unit to an Access Manager manually

Before you begin: "Enable the Access Manager to connect to the SMC units" on page 26.

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

1 Log on to Security Center with Config Tool.

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

3 Select the Access Manager role ( ), and click **Add an entity** (✚).

4 In the menu that appears, select **Access control unit** ( ).

5 In the unit creation dialog box, click **Unit type** and select **SMC**.

6. In the **Network endpoint** group, enter the SMC 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. See "Change the logon password" on page 7.

   IMPORTANT Do not change any settings in the **Advanced controls** group unless instructed by your Genetec representative.

7. Click **Next** and select the partition the SMC unit should belong to.
8. Click **Next** and click **Create**.
9. Wait to see that the unit is successfully created and click **Close**.
10. Click **Refresh** (🔄).

The SMC unit () appears under the selected Access Manager () in the entity tree. The default entity name is the SMC unit's hostname. From now on, this SMC unit will only respond to the commands issued by this Access Manager.

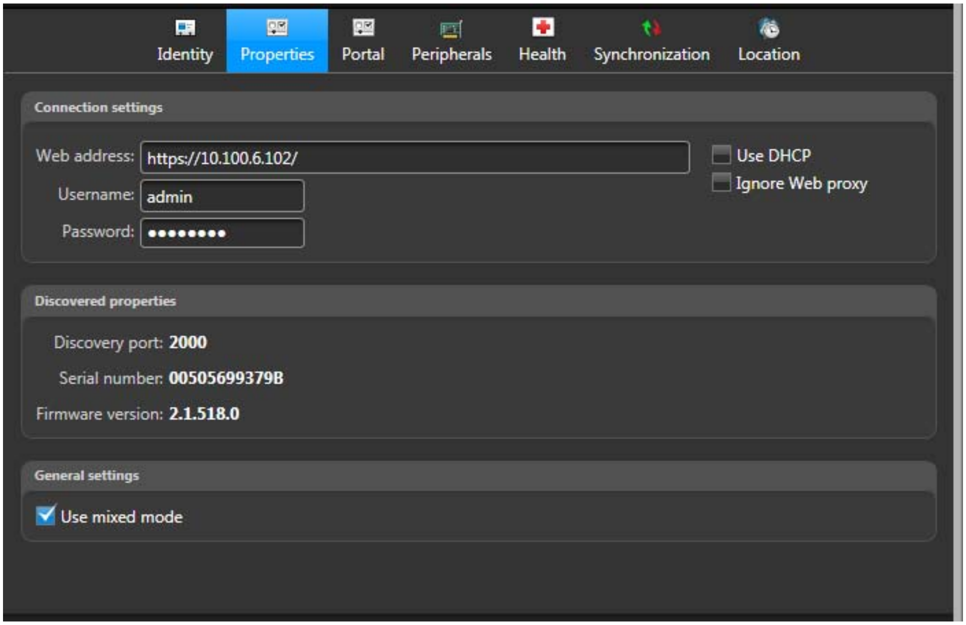
NOTE Later, if you change the connection parameters on the SMC unit, you'll have to inform the Access Manager about it. For more information, see "Keep the Access Manager in sync with the SMC unit" on page 29.

Keep the Access Manager in sync with the SMC unit

Some SMC and Access Manager settings are not automatically synchronized. If you change any settings about your SMC unit in Controller 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.

1. Log on to Security Center with Config Tool.
2. Open the **Access control** task and select the **Roles and units** view.
3. Select the SMC unit () you modified.

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



Connection settings

Web address: https://10.100.6.102/

Username: admin

Password: ●●●●●●●●

□ Use DHCP

□ Ignore Web proxy

Discovered properties

Discovery port: **2000**

Serial number: **00505699379B**

Firmware version: **2.1.518.0**

General settings

☑ Use mixed mode

5 Under **Connection setting**, enter the parameters used to connect to this SMC unit.

IMPORTANT The following settings are all correctly initialized at the time the SMC unit is enrolled in your system. Do not change these settings unless you changed the SMC settings in Controller Portal after the unit has been enrolled, or a Genetec representative instructs you to do so.

- *Web address.* Web address for contacting Controller Portal.
- *Username/Password.* Logon username and password.
- *Use DHCP.* Select this option to instruct the Access Manager to contact the unit using broadcast discovery packets. Clear this option to instruct the Access Manager to contact the unit using unicast packets. (Default=depends on the SMC network settings at the time of enrollment).
- *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).

6 Under **Discovered properties**, the current settings returned by the SMC unit are shown.

7 Under **General settings**, configure the settings that are pushed from Security Center to SMC.

Select **Use mixed mode** to have SMC make all decisions based on information downloaded from Access Manager during unit synchronization. Access events are reported to Access Manager in real time. (Default=enabled).

Clear this option to have Access Manager make all the decisions.

8 Click **Apply** to save your changes.

Switch the SMC unit to a different Access Manager

Once an SMC unit is connected to an Access Manager, it only responds to that Access Manager. If you want the SMC 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.

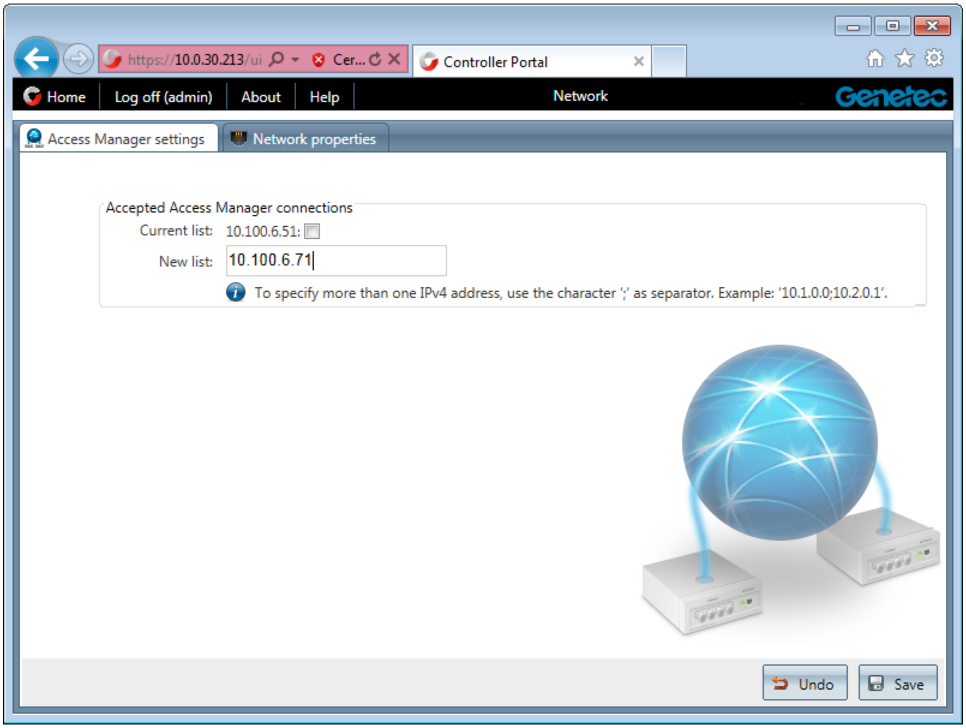
Before you begin: "Enable the Access Manager to connect to the SMC units" on page 26.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **Network**.

The **Access Manager settings** tab appears.

3 In the **New list** field, enter the IP address of the new Access Manager.



Accepted Access Manager connections

Current list: 10.100.6.51: ☐

New list: 10.100.6.71

To specify more than one IPv4 address, use the character ';' as separator. Example: '10.1.0.0;10.2.0.1'.

4 At the bottom of the page, click **Save** (💾).

After you are done: If the SMC 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, proceed with "Add the SMC unit to an Access Manager manually" on page 28.

4

Maintenance and troubleshooting

This section explains how to perform the basic maintenance and troubleshooting tasks on SMC.

This section includes the following topics:

Log on to SMC using the alternate IP address

Before you begin: Try logging on using the SMC's hostname. See "Log on to SMC" on page 6.

If you are unable to connect to SMC using its hostname and you haven't yet configured its IP address, use its fixed alternate IP address, which is `172.16.20.11 /24`.

IMPORTANT All SMC units are configured in factory to respond to the same fixed IP address. Never enroll an SMC unit in Security Center using this fixed alternate IP address.

1 Open a web browser.

2 In the browser's address bar, type `https://172.16.20.11`.

You'll get a certificate error message.

3 Follow your browser's on-screen instructions to continue to the website.

4 In the **Synergis Master Controller** - **Logon** page, select the interface language.

5 Enter the default username and password (`admin`/`softwire`), then click **Log on**.

The **Controller Portal** - **Home** page appears.

After you are done: "Change the logon password" on page 7 and continue with the next step in "Configure the SMC's network properties" on page 13.

Check and upgrade the SMC firmware

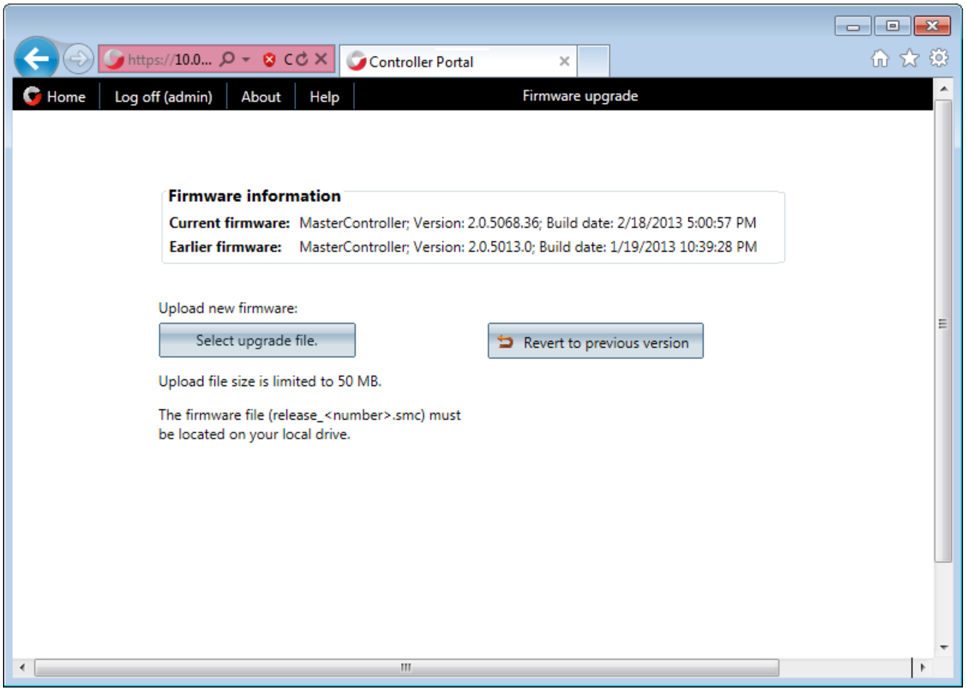
Before you begin: Find out from your Genetec representive the latest firmware version and download it from https://gtap.genetec.com if necessary.

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

1 "Log on to SMC" on page 6.

2 From the **Controller Portal** - **Home** page, click **Firmware upgrade**.

The current firmware version is indicated in the **Firmware information** box.



Firmware information

Current firmware: MasterController; Version: 2.0.5068.36; Build date: 2/18/2013 5:00:57 PM

Earlier firmware: MasterController; Version: 2.0.5013.0; Build date: 1/19/2013 10:39:28 PM

Upload new firmware:

Upload file size is limited to 50 MB.

The firmware file (release_<number>.smc) must be located on your local drive.

3 If an upgrade is necessary, click **Select upgrade file**.

4 In the file browser that opens, select the firmware file (*release_2.1_xxxx.yy.smc*).

The *.smc* file must be located on your local drive.

5 Click **Open**.

SMC restarts. The upgrade will take a few minutes.

After you are done: Log back on to SMC to verify that the firmware has been upgraded.

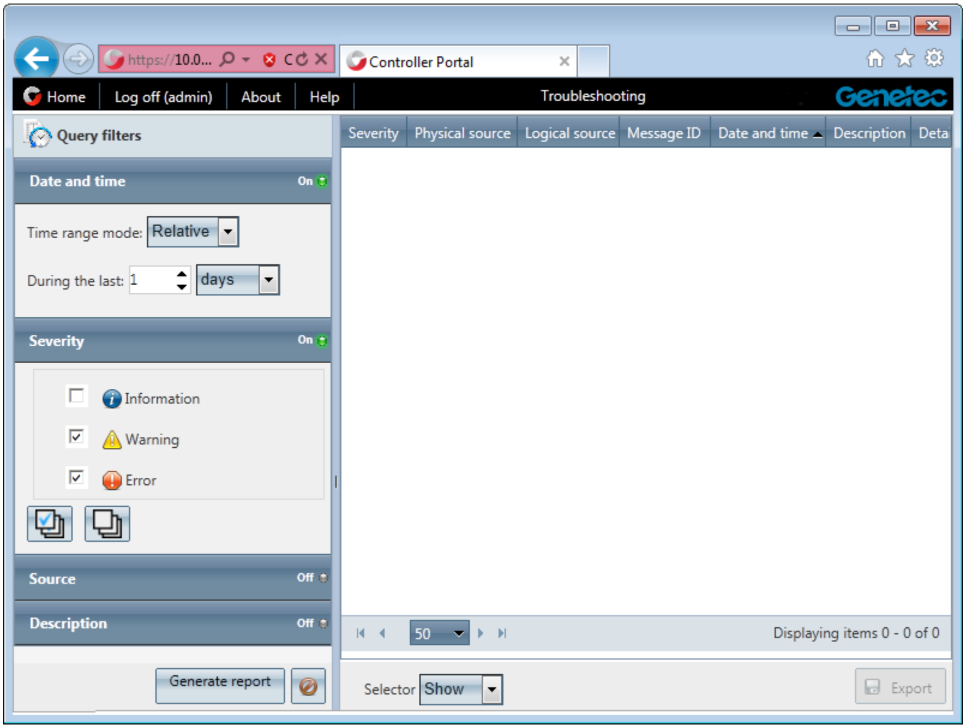
Generate troubleshooting reports

Before you begin: If you are investigating events related to normal operation, such as reader activity, input activity, or IO linking, you must explicitly turn the event logging option on. For more information, see "Configure the event logging options" on page 24.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **Troubleshooting**.

3 In the **Troubleshooting** page, set the **Query filters**.



Time range mode: Relative

During the last: 1 days

□ Information

☑ Warning

☑ Error

50

Selector Show

Click on a filter heading to enable or disable it.

- *Date and time.* Filter the events based on a time range (*Absolute* or *Relative*). All events are logged using the unit's local time zone.
- *Severity.* Filter on the event severity level.
- *Source.* Search for a text found in either the *Physical source* or the *Logical source* associated to the event.
- *Description.* Search for a text found in the event's *Description* field.

4 Click **Generate report**.

The report appears to the right. For more information, see "Description of the troubleshooting report" on page 36.

TIP Click **Selection** at the bottom of the page and select **Hide** to hide the query filers to create more space to display the report.

After you are done: Click **Export** to save the report to a CSV file. The default file name is *Troubleshooting.csv*.

Description of the troubleshooting report

The troubleshooting report contains the following columns.

- **Severity.** Event severity level. The possible values are:
  - *Information.* Useful information unrelated to any critical situation that could help understand the context of another problem. For example, the unit clock has been adjusted. All optional activity events are logged as information.
  - *Warning.* Non-critical situation that may lead to more serious problems if left unattended. For example, the disk is 80% full.
  - *Error.* Critical situation that needs immediate attention. For example, the unit ran out of disk space, therefore, logging cannot continue.
- **Physical source.** Name, address, and channel of the interface module affected by the event. Blank if it does not apply.
- **Logical source.** Name of the Security Center entity (door, area, cardholder, etc.) affected by the event. Blank if it does not apply.
- **Message ID.** ID corresponding to the type of event.
- **Date and time.** Event timestamp expressed in the unit's local time zone.

  Click on the column heading to sort the events in the reverse order.
- **Description.** Short event description, such as "Access granted by access rule", "Access denied, card & PIN timeout", "Request-to-exit", "Zone armed by schedule", and so on.
- **Details.** Additional details providing contextual information to the event.

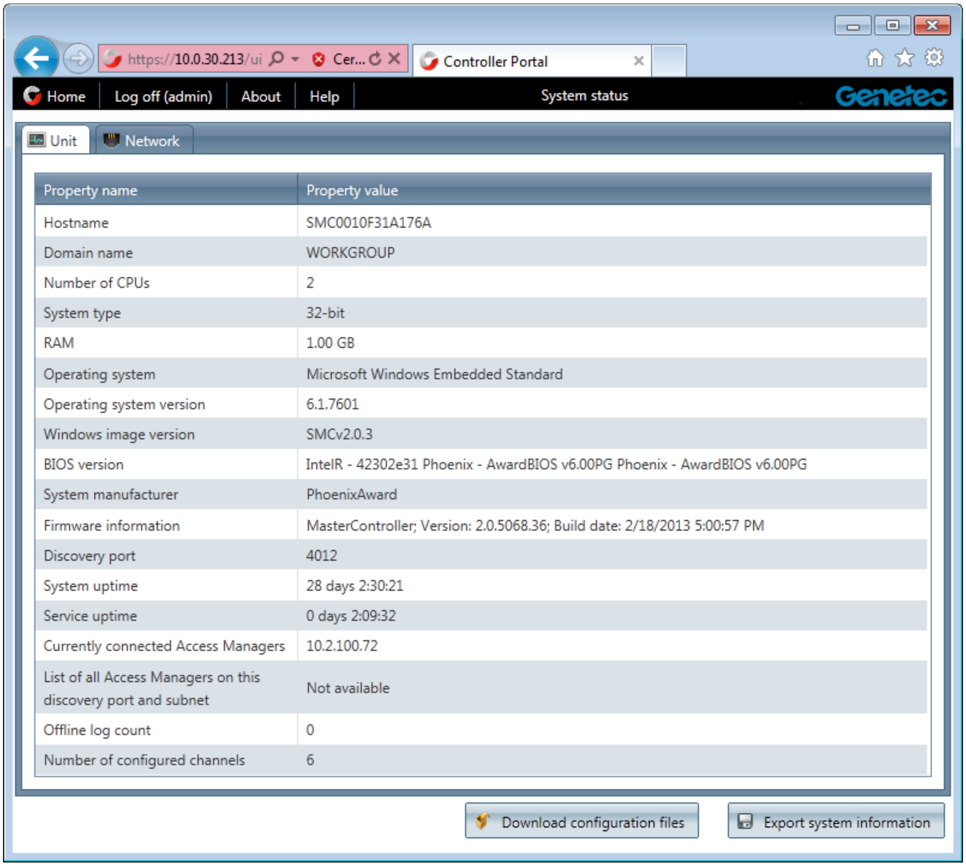
Viewing and exporting system information

You can view and export the SMC's status and configuration files for troubleshooting.

To view information on the SMC unit:

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **System status**.



Property name	Property value
Hostname	SMC0010F31A176A
Domain name	WORKGROUP
Number of CPUs	2
System type	32-bit
RAM	1.00 GB
Operating system	Microsoft Windows Embedded Standard
Operating system version	6.1.7601
Windows image version	SMCv2.0.3
BIOS version	IntelR - 42302e31 Phoenix - AwardBIOS v6.00PG Phoenix - AwardBIOS v6.00PG
System manufacturer	PhoenixAward
Firmware information	MasterController; Version: 2.0.5068.36; Build date: 2/18/2013 5:00:57 PM
Discovery port	4012
System uptime	28 days 2:30:21
Service uptime	0 days 2:09:32
Currently connected Access Managers	10.2.100.72
List of all Access Managers on this discovery port and subnet	Not available
Offline log count	0
Number of configured channels	6

3 Select **Unit** to view the SMD unit's hardware and firmware information.

For a description of the information displayed, see "Unit information" on page 38.

4 Select **Network** to view the SMC unit's network configuration and status.

For a description of the information displayed, see "Network information" on page 39.

5 Press F5 to refresh the information.

After you are done: "Download unit configuration files" on page 39 or "Export system information" on page 40.

Unit information

The *Unit* tab shows information on SMC's hardware and firmware.

Property name	Property value
Hostname	Hostname of the controller. The default hostname is the letters `SMC` 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 `0010F31A176A`, then the default hostname is `SMC0010F31A176A`.
Domain name	Domain name.
Number of CPUs	Should indicate 2.
System type	Should indicate 32-bit.
RAM	Should indicate 1.00 GB.
Operating system	Should indicate Microsoft Windows Embedded Standard.
Operating system version	Operating system version.
Windows image version	Windows image version. If it shows "SMCv2.0.3", then you must upgrade the unit's firmware before you deploy it in your system (see "Check and upgrade the SMC firmware" on page 34).
BIOS version	BIOS version
System manufacturer	Should indicate PhoenixAward.
Firmware information	Version and build date of the SMC firmware. NOTE Confirm with your Genetec representative that you have indeed the latest version.
Discovery port	The discovery port used by the Access Manager roles to communicate with this SMC unit. NOTE The IP address of the Access Manager must also be known to SMC 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 is currently managing this unit.
List of all Access Managers on this discovery port and network segment	List of the IP addresses of all Access Manager roles that have, at one time or another, been connected to this unit.

Property name	Property value
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 SMC's own troubleshooting logs.
Number of configured channels	Number of communication channels that are configured with interface modules attached. SMC features three types of channels, IP, USB, and RS-485.

Network information

The *Network* tab shows information on the SMC unit's network configuration and status. SMC has two network adapters. The information on each adapter is as follows.

Property name	Property value
MAC address	MAC address of the network adapter.
IP address	Current IP address.
Network Segment mask	Current network segment mask.
Default gateway	Current default gateway.
Preferred DNS server	Current preferred DNS server.
Alternate DNS server	Current alternate DNS server.
Network type	Current network type.
Is operational	Whether the adapter is operational or not: True or False.
DHCP enabled	Whether DHCP is enabled or not: True or False.
DNS enabled	Whether DNS is enabled or not: True or False.

See also "Configure the SMC's network properties" on page 13.

Download unit configuration files

You can download your entire SMC configuration as compressed XML files for troubleshooting purposes.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **System status**, and at the bottom of the page, **Download configuration files**.

3 In the dialog box that appears, specify where you want to save the file, and click **Save**.

All configuration settings will be exported as XML files and compressed into a single file named *SmcConfigurationFiles.7zip*. You'll need either *winzip* (included in Windows 7), *7-Zip*, or *winrar* to extract the compressed XML files.

Export system information

The information displayed in the *Unit* and *Network* tabs found in the *System status* page, as well as the list of currently loaded DLLs (name, version, path) can be exported to a CSV file.

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **System status**, and at the bottom of the page, **Export system information**.

The default file name is **SystemInformation.csv**.

3 Click **Save** (or equivalent command).

Restarting the SMC hardware or software

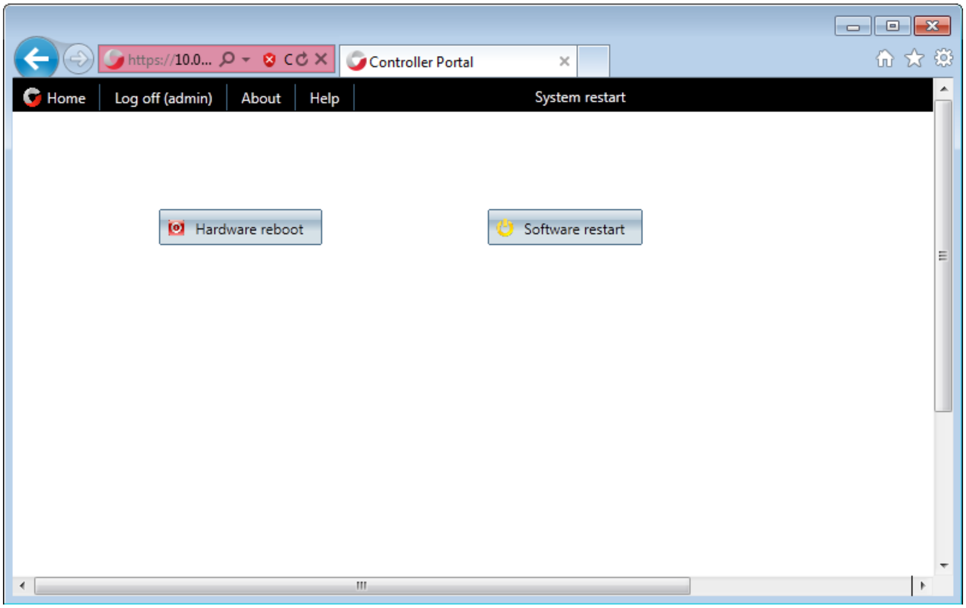
You can perform a hard or a soft restart on the SMC unit. A hard restart, or *hardware reboot*, is required when you are reconnecting or changing the four-port RS-485 module, or when you experience hardware problems. A *soft reboot*, or a software restart, is rarely required explicitly. SMC automatically restarts its firmware after you change the firmware version (see "Check and upgrade the SMC firmware" on page 34). Manual software restarts are only used for debugging or support purposes.

To perform either one of these operations:

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **System restart**.

The following page appears.



3 Click one of the following:

- *Hardware reboot*. To restart the SMC hardware.
- *Software restart*. To restart the SMC firmware.

Setting security clearance levels manually

Security clearance is an access control property used as part of the threat level management solution in Security Center (see “Managing threat levels” in the *Security Center Administrator Guide*). Both cardholders and areas are assigned security clearance levels. Cardholders can only access (enter or exit) an area if their security clearance level is equal or higher than that of the area. The security clearance level of an area can be raised because of a threat. This information is normally synchronized automatically between Security Center and SMC by the Access Manager.

Before you begin: The SMC unit needs to have been connected at least once to its Access Manager for the list of the Security Center areas to be downloaded. For more information, see "Enrolling the SMC unit in Security Center" on page 26.

If for any reason, the connection between the Access Manager and SMC is lost, you can set the security clearance levels directly on the SMC unit until the connection is restored.

IMPORTANT This is a temporary measure to be used only while SMC is operating in *offline mode*. When the SMC unit reconnects to its Access Manager, all the changes you made while the unit was offline will be overwritten by the configuration in Security Center.

To set the security clearance levels manually:

1 "Log on to SMC" on page 6.

2 From the **Controller Portal - Home** page, click **Security clearance levels**.

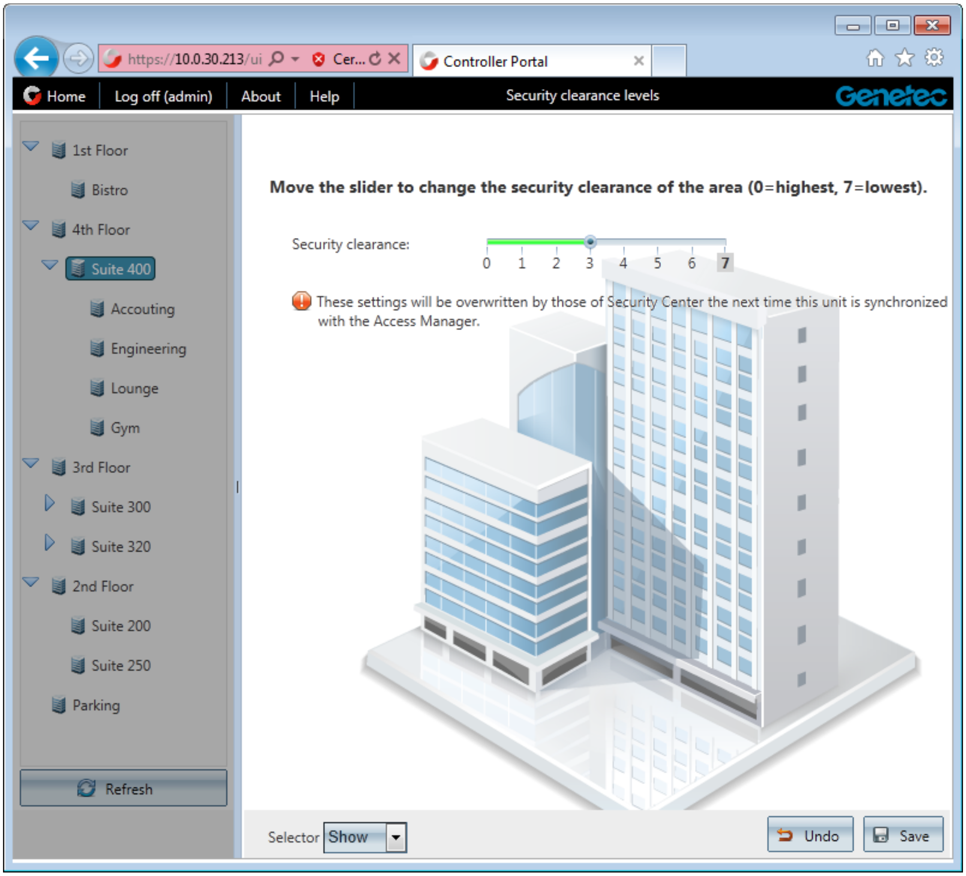
The area hierarchy defined in Security Center appears in the left pane, including areas not controlled by this SMC unit.

3 From the left pane, select the area you want to modify. Make sure that the perimeter doors of the selected area are controlled by this unit.

The current security clearance of the selected area is displayed in the right pane (the highlighted value).

NOTE Security clearance levels range from 0 (most rectrictive) to 99 (most permissive) in Security Center. SMC only accepts values ranging from 0 to 7. Any security clearance level downloaded from Security Center whose numeric value is greater than 7 is converted to 7 in SMC. The same conversion applies to security clearance levels assigned to both areas and cardholders.

4 In the right pane, click the new security clearance level and click **Save**.



Move the slider to change the security clearance of the area (0=highest, 7=lowest).

Security clearance: 3

These settings will be overwritten by those of Security Center the next time this unit is synchronized with the Access Manager.

You can only change one value at a time.

SMC will use the value you set to grant access to this area to cardholders until the next synchronization with the Access Manager takes place.

Index

Where to find product documentation

You can find our product documentation in the following locations:

- **Installation package.** The documentation is available in the *Documentation* folder of the installation package. Some of the documents also have a direct download link to the latest version of the document.
- **Genetec Technical Assistance Portal (GTAP).** The latest version of the documentation is available from the GTAP Documents page. Note, you'll need a username and password to log on to GTAP.
- **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. 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 Genetec customer, you have access to the Genetec Technical Assistance Portal (GTAP), where you can find information and search for answers to your product questions.

- **Genetec Technical Assistance Portal (GTAP).** GTAP is a support website that provides in-depth support information, such as FAQs, knowledge base articles, user guides, supported device lists, training videos, product tools, and much more.

  Prior to contacting GTAC or opening a support case, it is important to look at this website for potential fixes, workarounds, or known issues. You can log in to GTAP or sign up at https://gtap.genetec.com.
- **Genetec Technical Assistance Center (GTAC).** If you cannot find your answers on GTAP, you can open a support case online at https://gtap.genetec.com. For GTAC's contact information in your region see the Contact page at https://gtap.genetec.com.

  NOTE Before contacting GTAC, please have your System ID (available from the About button in your client application) and your SMA contract number (if applicable) ready.
- **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).

Additional resources

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

- **GTAP Forum.** The Forum is an easy to use message board that allows clients and Genetec staff to communicate with each other and discuss a variety of 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/Services.