

# SIEMENS



## Access Control

## SiPass integrated

## Controller and Device Installation Guide

MP 2.80

## Copyright

Technical specifications and availability subject to change without notice.

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

Edition: 07.09.2020

Document ID: A6V11164550

© Siemens Switzerland Ltd, 2020

# Table of Contents

<b>1</b>	<b>Firmware Configuration Tools .....</b>	<b>5</b>
1.1	ACC USB Client Application .....	5
1.1.1	Installing the USB RNDIS Driver .....	5
1.1.2	Configuring the ACC USB Client Application .....	6
1.2	ACC and FLN Field Service Network Tool.....	7
1.2.1	Installation.....	7
1.2.2	Downloading Firmware for Device.....	7
1.2.3	Network Discovery for Access Controllers .....	8
1.2.4	Enhanced FLN Communication.....	9
1.3	Built-in ACC Tools .....	10
1.3.1	User Security for ACC Console .....	10
1.3.2	User Security for ACC-Lite LCD / Keypad Menu .....	10
<b>2</b>	<b>Access Controllers.....</b>	<b>11</b>
2.1	Common Firmware Update Procedure .....	11
2.1.1	Updating Controller Application via Firmware Download .....	11
2.1.2	Updating Controller Platform via Firmware Download.....	12
2.2	AC5102 (ACC-G2) .....	14
2.2.1	Configuring the AC5102 Controller using USB Client Application.....	14
2.2.2	Network Discovery of AC5102.....	14
2.2.3	Configuring the AC5102 Port Mapper .....	14
2.2.4	RS232 mode on FLN 2 and FLN 3 .....	15
2.2.5	Restoring Default Network and Password Settings.....	15
2.2.6	Recovering a Non-responsive Board.....	16
2.2.7	ACC-G2 Firmware Update Procedures .....	16
2.2.8	Restoring/Updating Platform via SD Card .....	16
2.2.8.1	Preparing the SD Card .....	16
2.2.8.2	SD-Card Upgrade Procedure .....	17
2.2.8.3	SD Card Update Troubleshooting .....	18
2.2.9	Network Security.....	18
2.3	ACC-AP.....	19
2.3.1	General Information .....	19
2.3.2	Configuring the ACC-AP Controller .....	19
2.3.3	Onboard Door (DRle) Interfaces.....	20
2.3.3.1	Dual OSDP Reader Door Configuration.....	20
2.3.3.2	2 Single OSDP Reader Doors Configuration .....	20
2.3.3.3	OSDP Reader Turnstile, Single Door Contact Configuration .....	21
2.3.3.4	OSDP Reader Turnstile, Dual Door Contact Configuration.....	21
2.3.3.5	Dual Wiegand Reader Door Configuration.....	22
2.3.3.6	2 Single Wiegand Reader Doors Configuration .....	22
2.3.3.7	Wiegand Reader Turnstile, Single Door Contact Configuration .....	23

2.3.3.8	Wiegand Reader Turnstile, Dual Door Contact Configuration.....	23
2.3.4	Extension Interfaces .....	24
2.3.4.1	Extension Option .....	24
2.3.4.2	Aperio Wireless Doors Extension Option .....	24
2.3.5	Power Monitoring Limits.....	24
2.3.6	Factory Reset Button .....	24
2.3.7	Restoring/Updating Platform via SD Card .....	25
2.3.7.1	Preparing the SD Card .....	25
2.3.7.2	Updating the AP Controller with Micro SD Card .....	25
2.3.8	Platform Upgrade via Firmware Download .....	26
2.3.9	LED Indications.....	26
2.3.9.1	During SD Card Update.....	26
2.3.9.2	During ACC-Application (Run-Time) .....	26
2.4	4101-3 (ACC-Granta).....	27
2.4.1	Configuring using USB Client Application.....	27
2.4.2	Network Discovery .....	27
2.4.3	Restoring Default Network and Password Settings .....	27
2.4.4	Recovering a Non-responsive Board.....	28
2.4.5	Network Security .....	29
2.5	AC5100 (ACC-G1) .....	30
2.5.1	Restoring Default Network and Password Settings .....	30
2.6	AC5200 (ACC-Lite) .....	31
2.6.1	Restoring Default Network, Password and PIN Settings .....	31
<b>3</b>	<b>FLN Devices and Readers .....</b>	<b>32</b>
3.1	ADD5100 Dual Reader Interface (DRI) .....	32
3.2	ADE5300 Eight Reader Interface (ERI) .....	32
3.3	ADS5200, ADS5210 Single Reader Interface (SRI) .....	32
3.4	AFI5100 (IPM) .....	32
3.5	AFO5100 (OPM) .....	32
3.6	AFO5200 (8IO) .....	32
3.7	ATI5100 (IAT) .....	32
3.8	OSDP Reader Devices.....	32
3.9	ARxxx-MF / VRxxx-MF Reader .....	33
3.9.1	RIM Settings .....	33
3.9.2	Required Settings for Reading the UID Number of a MIFARE Card.....	33
3.10	Wiegand Reader on ACC-AP .....	34
3.11	Multi-Function Interface (MFI) .....	35
3.12	Aperio Wireless Lock Technology .....	36
3.12.1	SiPass Card Technologies in Aperio Locks.....	36
3.12.2	Connecting Aperio Hub with ACC-AP .....	37
3.13	Help and Documentation .....	37

# 1 Firmware Configuration Tools

## 1.1 ACC USB Client Application

The network settings of the ACC Controllers can be configured using a Windows application, and an appropriate USB cable. This configuration needs the USB RNDIS driver (an Ethernet-over-USB driver) to be installed.

The pre-requisites required for this configuration are listed below.

### Prerequisites

- Relevant ACC Controller
- Host PC with a spare USB port (running the Windows Operating System)
- USB A-B Cable
- *AccG2UsbClient* application for the Windows host (available under **Tools\ACC-G2\_USB\_Tool\** in SiPass integrated installation bundle)
- USB RNDIS driver (available under **Tools\ACC-G2\_USB\_Tool\RNDIS\_Driver\** in SiPass integrated installation bundle)

### 1.1.1 Installing the USB RNDIS Driver

Ensure that the power for the ACC controller unit is connected and ON.

1. Insert the B plug end of the A-B USB cable into the USB PC port of the ACC unit.
2. Insert the A plug end of the A-B USB cable into the USB port of the host PC. If the USB RNDIS driver is not available on the host PC already, it will prompt you to install the same. You can choose to install the USB RNDIS driver either from an Installation CD (if available), or from a specific location.

If you wish to install the driver from a specific location, follow the instructions provided below.

1. A *Found New Hardware Wizard* dialog will pop-up prompting the user to install the USB RNDIS driver if it has not been previously installed on the host PC.
2. Select the **No, not this time** option, and click the **Next** button.
3. Select the **Install from a list, or specific location (Advanced)** option.
4. Click **Next**.
5. Select the **Search for the best driver in these locations** option.
6. On the same dialog, tick the **Include this location in the search:** checkbox, and click the **Browse** button.
7. Navigate to the location of the driver, and click **OK**.
8. Click **Next**.

The wizard will now proceed to install the software.

◆ When the installation is complete, click **Finish**.

The USB RNDIS Driver should now be installed on the host PC.

### 1.1.2 Configuring the ACC USB Client Application

First time that the ACC is plugged in via the USB-B port, it may take a minute or two to configure the USB to Ethernet interface. This is normal, and the delay should not occur again.

1. Run the ACC USB client application.
  - ⇒ The *ACC USB Client Login* dialog is displayed.
2. Enter the default user name and password to start the Telnet session for configuring the ACC network parameters.
  - ⇒ If you are using MP2.70 (or later) version of the ACC and the default (or weak) password is set, you will be prompted to enter a new password before configuring the network settings.
  - ⇒ If you are using MP2.70 SP1 (or later) version, when you change the SIEMENS user password, the password for the “root” user for a SSH connection will also be changed to the same password that was set for the SIEMENS user.
3. Set the following parameters for the ACC in *Network Settings* section:
  - Ethernet IP address
  - Subnet mask
  - Gateway IP address
  - Host IP address
  - Port
4. Click **Apply**

## 1.2 ACC and FLN Field Service Network Tool

For devices in an access control and security system to function as intended, they must be programmed with the correct instruction set, or “firmware”. It is also important to test your selected settings on a device before the device goes live.

The ACC and FLN Field Service Tool has been designed to assist in the installation of Field Level Network devices for use with the SiPass integrated Access Control and Security System. This includes:

- Dual Reader Interfaces (DRI)
- Single Reader Interfaces (SRI)
- Eight Reader Interface (ERI)
- Output Point Modules (OPM)
- Input Point Modules (IPM)
- Eight Input Output Module (8IO)
- Intrusion Arming Terminals (IAT-010)

The ACC and FLN Service Tool can also assist in discovering Access Controllers in the local Ethernet segment, and configuring the network parameters of these discovered controllers.

The Field Service Tool is designed to help you perform these tasks.

### 1.2.1 Installation

Run *setup.exe* (available under **Tools\ACC and FLN Field Service Tool\Setup Disk\** in SiPass integrated Installation bundle) to install this tool.

### 1.2.2 Downloading Firmware for Device

Devices can be connected to a COM Port on a PC running the Field Service Tool via a RS232 – RS485 Bus converter.

The process to download firmware and test devices is as follows:

1. Configure the FLN Bus.
2. Select an image file for download.
3. Detect all devices on the FLN Bus.
4. Download firmware to a device.
5. Configure the device.

### 1.2.3 Network Discovery for Access Controllers

It is possible to configure Access Controllers via Ethernet, without prior configuration of any settings.

The ACC and FLN Field Service Tool uses UDP Broadcasts to identify ACC controllers that have their Quickstart feature enabled. Once identified, the network parameters can be configured such that the controller can now connect to the SiPass server.

**CAVEAT !** This can only work in the local Ethernet segment as UDP Broadcasts cannot cross routers.

Make sure that the SiPass server is running before using the Network Discovery tool.

Make sure Ethernet cable is plugged in, and the PC/laptop is on the same physical Ether network as the ACCs that are to be discovered.

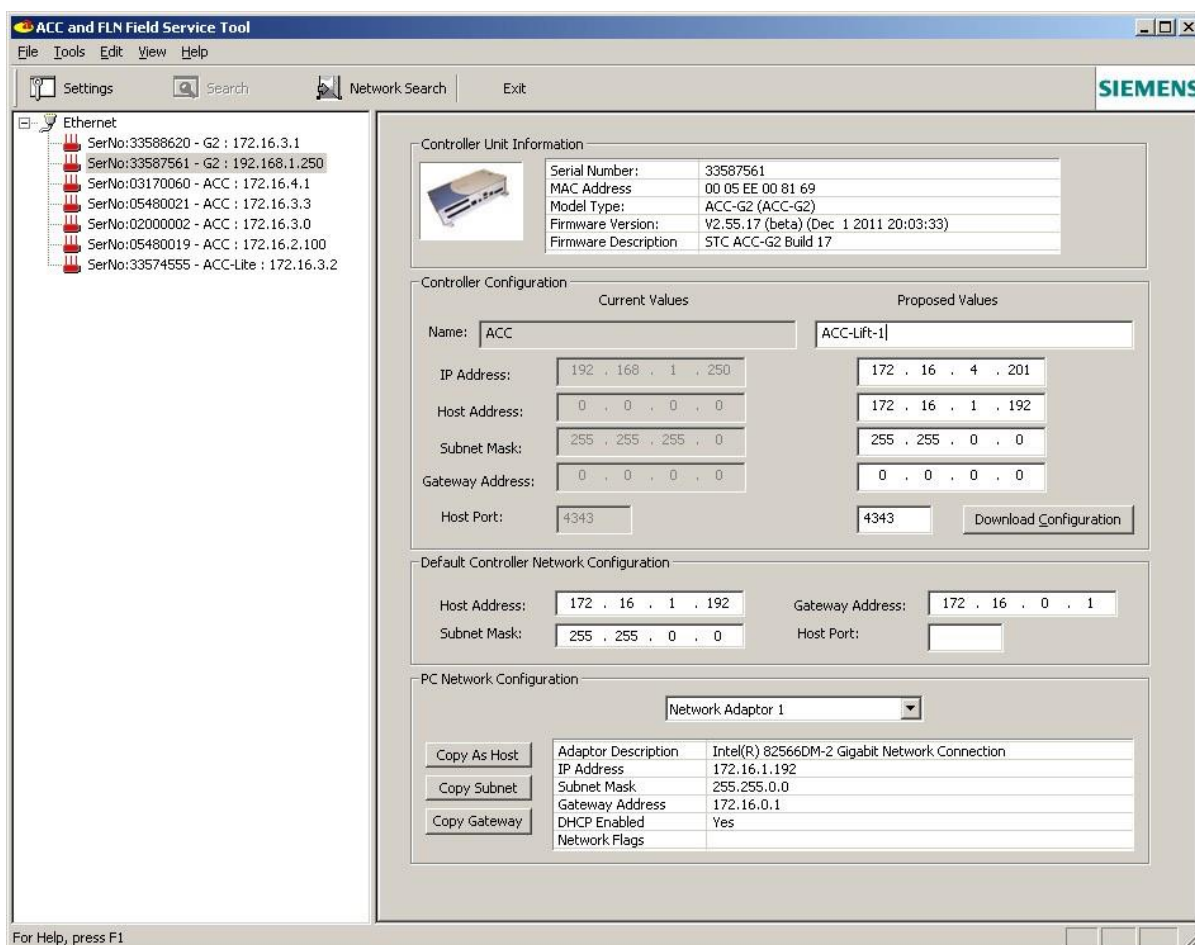
Click the Network Search button – a list of not yet configured ACCs should appear. Select one unit, and examine its network settings.

If the tool is being run from the SiPass server, select the correct network interface and then use the Copy As Host, Copy Subnet and Copy Gateway settings.

If the tool is just being run from a laptop, configure the host network settings in the *Default Controller Network Configuration* pane.

Choose a unique IP address for the controller (consult with your IT if required). Finally, click the **Download Configuration** button, and the controller is configured.

See below for an example screen shot showing a range of controllers, including one ACC-G2 being configured to operate on the local network.



**Note:** the IP addresses are for example only, be sure to use values applicable to your network.



## 1.2.4 Enhanced FLN Communication

With SiPass integrated MP 2.70 SP1 onwards, the standard communication of firmware uses added security measures. You can add a device with Legacy Firmware to an existing FLN bus that contains devices with the new Standard Communication.

### Special case when ACC is running MP 2.70 SP1 and FLN Devices are on MP 2.70

- When you add a device with Legacy Firmware to an existing FLN bus that contains devices with the new Standard Communication:
  - Discovering this device with the *FLN Configuration Tool* will show the device but it will be reported as Offline.
  - Latest Firmware can still be downloaded to this device after which, selecting **Refresh Display** will show the device as online in the *FLN Configuration Tool*.
  - When this device is saved to the database using the **Save New Device** button, the device will be reported as using the new Standard Communication.
- If you do not upgrade the Legacy Firmware of this new device:
  - The device can be saved to the database using the **Save New Device** button. In this case, all devices on the same bus (including the ones with new Standard Communication) will drop to Legacy Communication.
  - When the Firmware of the Legacy Device is upgraded to the new Firmware, all devices will automatically start using the new Standard Communication.

## 1.3 Built-in ACC Tools

The Core parameters such as network settings can also be configured using ACC Console which is available for all Access Controller types, and accessible via Telnet session to controller IP address.

In addition to this, ACC-Lite controller offers configuration via LCD / Keypad menu interface.

### 1.3.1 User Security for ACC Console

**These additional security measures have been introduced in ACC version 2.70.x**

After the first login to the ACC Console with the default password, you will be asked to change the password for security purpose. The password must be secure with at least one of upper and lower case characters, digits, and one or more special character, e.g. \*&#\$. Record this new password in a secure place after setting.

If you changed the password and then install an earlier version of the ACC firmware, the ACC will revert back to the password set before MP2.70 was installed. (If you still had the default password when the MP2.70 version of ACC was installed, and then the MP2.65 version of the ACC is installed, you must login on with the default password, not the password entered during MP2.70 version installation).

If you then re-install the MP2.70 build, the new password that was set when MP2.70 was first installed, will still be valid.

This also applies to login via the ACC-G2 standalone USB configuration tool.

### 1.3.2 User Security for ACC-Lite LCD / Keypad Menu

**These additional security measures were introduced in ACC version 2.70.x**

The default PIN is '1111'.

If you upgrade from an earlier version of ACC-Lite to the MP2.70 version, the first time you open the keypad and login with the default PIN, you will be asked to Set a new PIN for security purposes. The PIN must be secure and not just a simple sequence of numbers such as 1111, 1234, 4321 or similar. The PIN length must be 4-10 digits. Record this new PIN in a secure place after setting it.

If you change the ACC-Lite PIN and forget, it can be changed with an ACC telnet Console command. If both PIN and Telnet passwords are lost, then the device must be returned to the manufacturer or Siemens.

If you changed the PIN using SiPass integrated MP2.7, install an earlier version of the ACC-Lite firmware, then again re-install MP2.7, you must login with the PIN that was previously set (because the PIN has already been changed using the MP2.7 build, setting a new PIN is not required again).

## 2 Access Controllers

### 2.1 Common Firmware Update Procedure

This procedure applies for both ACC-G2 and ACC-AP controllers.

Controller firmware releases include three types of firmware images:

1. **Firmware Application Image**

For example, *acc-g2-ccp2\_2.76.25\_release.bin* is ACC-G2 application version 2.76.25.

2. **FirmwarePlatform (downloadable) Image**

For example, *accg2-platform\_ccp2.17.5\_update\_acc2.76.25.bin* contains a complete ACC-G2 platform version 2.17.5 with ACC-G2 application version 2.76.25

3. **Firmware Platform SD-Card Image**

For example, *accg2-platform\_ccp2.17.5\_sdcard.wic.gz* contains a complete ACC-G2 platform version 2.17.5 with ACC-G2 application version 2.76.25

Release folder is structured as follows:

**Product Type (ACC-AP or ACC-G2)**

- ACC application image is stored at this level.
- *SD\_Card*: This folder includes the SD-Card platform image.
- *System\_Update*: This folder includes the step by step downloadable images for each supported upgrade path.
  - From\_Platform\_v1
    - Step1
    - ...
    - Step N
  - From\_Platform\_vX
    - Step
    - ...
    - Step M

#### 2.1.1 Updating Controller Application via Firmware Download



**Note:** Current version of the controller's platform and application are shown in the *Initialize System* dialog of SiPass integrated

If the controller is already running the latest platform version, update by using the **Image Download** option in the *Initialize System* dialog of SiPass integrated to download the firmware **application image**.

- Subject to the network load, download is expected to take a few minutes.
- During installation, the ACC application is expected to restart.
- Downtime depends on the database size and fragmentation (can take a few seconds to few minutes)

## 2.1.2 Updating Controller Platform via Firmware Download



**Note:** Current version of the controller's platform and application are shown in the *Initialize System* dialog of SiPass integrated.

- In case it is required to control the timing of the downtime caused by the platform installation process, automatic platform update can be disabled by sending the following command via the ACC console:

```
platform autoUpgrade 0
```

- An audit trail message will be displayed to indicate that Auto-Upgrade has been disabled.

**Note:** If the ACC is reset before platform image has been completely downloaded to the ACC, the Auto-Upgrade feature will be enabled again.

- To re-enable automatic update, use the command:

```
platform autoUpgrade 1
```

- Make a note of current platform major version.
  - For example, 2.17.5 means that the major version is 2.
- In the Firmware Release, locate the folder named *<Controller Type>|System\_Update|From\_Platform\_v<Major Version>*.
  - For example, *ACC-G2|System\_Update|From\_Platform\_v2*
- Download images one by one by following the order of *StepX* sub-folders. If the *StepX* sub-folders do not exist, it means only single image must be downloaded.

**Note:** Multiple download steps are required to ensure that the controller is running the latest application capable of receiving and installing the platform update image.

- Use the **Image Download** option in the *Initialize System* dialog of SiPass integrated to download firmware image(s).
- In case automatic platform update was disabled:
  - When platform image download is completed, the Audit Trail will display the message - *"Manually initiate ACC-Platform upgrade"*.
- Installation of the downloaded platform should be launched manually by sending the following command via the ACC console:

```
platform initUpgrade
```

#### More about Platform Update:

- Platform image is a large file that contains complete Operating System distribution and it will take at least 30 minutes to download to the ACC. However, the ACC will remain fully operational during the download phase.
- After ACC Platform image has been successfully written to the flash memory, the "*Download succeeded. ACC flash programming OK*" message will be displayed in the audit trail.
- If auto update is enabled, the "*Upgrade of ACC Platform has been initiated. ACC will reset after completion!*" message will be displayed in the audit trail, and the ACC will restart to initiate the platform upgrade.
- During platform installation, the controller is expected to reboot at least twice. Database configuration and system settings will be kept. Overall downtime is expected to be between 1 and 10 minutes, depending on the size and fragmentation of database.
- **Recovery from unsuccessful System Update:** If System Update fails or ACC Application fails to start after System Update, the system will automatically revert to the previous state.
- **Recovery from corrupted database:** If ACC Application fails while loading the database, the database will be deleted and initialization from SiPass integrated will be required.

## 2.2 AC5102 (ACC-G2)

See the *AC5102 Hardware Technical Manual* in the SiPass integrated software bundle.

### 2.2.1 Configuring the AC5102 Controller using USB Client Application

See section ACC-G2 USB Client Application for more details.

### 2.2.2 Network Discovery of AC5102

See section ACC and FLN Field Service Network Tool for details.

### 2.2.3 Configuring the AC5102 Port Mapper

Port Mapper is needed when configuring an AC5102 with SiPass MP2.5 or earlier. If you are using MP2.6, be sure that the AC5102 Port Mapper has been disabled with the console command *"portmap default"* followed by a *"reboot"* or a *"portmap restart"* command.

The primary purpose of the Port Mapper is to redirect a logical port, like the IS port or a FLN – to a different physical port. This is needed specifically when replacing an ACC and the IS ports is being used for connection to a Gateway service, like a Sintony panel, a Securitel Alarm dialler, or is being used to connect to a HLI (High level Lift Interface).

It is also possible to redirect logical FLN ports to different physical ports, e.g. FLN 3b (which does not exist on the AC5102). This is not normally needed since SiPass allows renumbering a FLN (it will work after an initialise).

To modify the port mapping: telnet to the controller, or use the USB Config tool. Login as user SIEMENS.

Type the following:

portmap

- the output should look as follows:

1. FLN1 = 1
2. FLN2 = 2
3. FLN3 = 3
4. FLN4 = 4
5. FLN5 = 5
6. IS = 6

- Note that the first digit on each line is the line number.

To swap the IS port and FLN 2, such that the logical IS port is connected to the FLN 2 physical port and the logical FLN2 is routed to port 6, type the following:

portmap replace 6 IS = 2 portmap replace 2 FLN2 = 6

- Type portmap again to list the changes:

1. FLN1 = 1
2. FLN2 = 6
3. FLN3 = 3
4. FLN4 = 4
5. FLN5 = 5
6. IS = 2

And finally, apply the changes by rebooting the application:

reboot

## 2.2.4 RS232 mode on FLN 2 and FLN 3

Using FLN 2 or FLN 3 in RS232 mode (for Securitel or Sintony integration) requires that the EOL jumpers be set to OFF. This entails powering down the ACC-G2, removing the FLN expansion module and then setting all the jumpers for the appropriate ports to OFF.

A torx screwdriver bit of size T10 is required to remove the FLN expansion module. A magnifying glass and a small screwdriver are useful for setting the EOL dip switches.

See the *AC5102 Technical Manual* in the SiPass integrated software bundle for more information.

**Note:** Disregard connections for FLN 2 & 3 shown in Section “Bus Termination of the FLNs” in *AC5102 Technical Manual* and follow as shown in the table below:

FLN2	FLN3
X600, X601 Each dip switch consists of two switches	X602, X603 Each dip switch consists of two switches

## 2.2.5 Restoring Default Network and Password Settings

The X992 jumper is near the battery for the Real Time Clock (RTC).



Short the pins of X992 for 3 seconds (using a jumper), until the orange ERROR led is blinking quickly. Remove the short, and wait about 10 seconds for application to restart and reset the network settings.

The default network settings are:

IP Address : 192.168.251.1

Subnet Mask : 255.255.255.0

Default Login Credentials: SIEMENS/spirit

All other settings are zeroed, including the SiPass host address and modem configuration is disabled. The Telnet server is re-enabled.

Use either Telnet, the USB Client Application or the Network Configurator tool to restore the network settings.

## 2.2.6 Recovering a Non-responsive Board

See section Restoring/Updating Platform via SD Card [→ 16] for details.

## 2.2.7 ACC-G2 Firmware Update Procedures

See section Common Firmware Update Procedure [→ 11] for details.

## 2.2.8 Restoring/Updating Platform via SD Card

### 2.2.8.1 Preparing the SD Card

Before you begin, prepare the SD Card by following the steps below:

1. Insert the SD card into the computer (512MB minimum - 2 GB maximum, 512MB recommended for compatibility with older ACC revisions).
2. Find compressed *.gz* image in *SD\_Card* folder. Unzip to extract the *.wic* file.
3. Use *Win32DiskImager* (in *Tools\ACC-G2 SD-Card Creator Tool* folder) to write the *~.wic* file to the SD Card.

*Win32DiskImager* defaults to open a file of extension type *\*.img*, so select *\*.\**, browse to the location of the SD card image file and load it, then click the **Write** button.

**Note:** Win32DiskImager must be installed on your computer, not on the SD card.



## 2.2.8.2 SD-Card Upgrade Procedure



**Note:** In case of SD Card update, the database configuration and system settings will be lost.

To perform the SD-Card upgrade, the following steps should be taken -:

1. Having written the SD Card, power down the ACC-G2 and insert the SD Card into the ACC SD-Card slot – removing the dust cover insert first, if fitted.
2. Fit the X120 jumper, which tells the boot loader to boot from the SD Card.



1. Power up the ACC.
2. Wait for it to program – the LEDs will stop blinking after about 30 seconds, which indicates that programming has completed. If the ACC-G2 was manufactured before the year 2012, you might need to press the reset switch between the CPU and Ethernet connector to initiate the upgrade.
3. Power down the ACC-G2 and remove the SD Card and Jumper.
4. Power up the ACC-G2 and check if the new CCP2 platform has been installed.
5. If the ACC-G2 has not been upgraded, repeat the SD-Card Upgrade Procedure. This may be necessary as some versions of the ACC-G2 have a single-boot UBOOT installed in them, which requires the SD-Card Upgrade Procedure to be performed twice for the upgrade to take effect.

**Note:** Doing an SD Card upgrade will also set the network parameters to the following default values:

IP Address	192.168.251.1
Subnet Mask	255.255.255.0
Ethernet Gateway Address	0.0.0.0
Host IP Address	0.0.0.0 : 4343

### 2.2.8.3 SD Card Update Troubleshooting

For SD Card Updates, the ACC-G2 only supports non-HC type SD Cards. This means SD Cards in the range of 512MB to 2GB only can be used.

1. There is an issue with using 1GB and 2GB SD Cards on the older ACCs with the 32kB EEPROM - when loaded with a CCP2 update image, the cards are not recognized by RomBOOT. The 1GB and 2GB SD Cards are only recognized on the newer ACCs with the SPI Data Flash fitted. Both ACC variants recognized 1GB and 2GB cards with update images for the CCP1 platform.
2. Also, the SD Cards with CCP2 Update images needed to be run twice in order to actually perform the update on the older ACCs if they are currently running an older CCP1 platform build. On the first instance they just booted the existing CCP1 image - press the RESET button or power up again for the update to take effect.

### 2.2.9 Network Security

The ACC-G2 uses Linux as an operating system, which provides both an increased level of security and reliability, but also requires some extra care in security.

Summary: disable both SSH and telnet for maximum security, and set a root password.

#### SSH

A SSH server is by default running on the ACC-G2. This allows for access to the linux shell console for maintenance purposes and trouble shooting, but in normal operation should be disabled so that it is not bound to the Ethernet interface, but instead restricted to just the local USB Ethernet interface.

**Note:** After the upgrade to CCP2 Platform, SSH access is no longer available for end user.

Disable external access to the SSH server with the console command:

```
" set ssh usb "
```

SSH access can be enabled with the console command:

```
" set ssh all "
```

The TCP port number that the SSH server listens on is 10022. This can be changed with the console command:

```
"set ssh port xyz "
```

Where xyz is a valid and unique TCP port number.

The standard port number for SSH is port 22, but many network probing tools attack port 22 by default.

#### Root Password

The username for gaining access to the linux shell is "root", the password is the default root password – "spirit".

The root password can be changed within the application via telnet, using the command:

```
" set rootpassword Large_String "
```

where `Large_String` should be long phrase that meets the requirements for a strong password. Use double quotes if the string contains spaces, but don't use double quotes when entering the password via SSH login.

#### Telnet

The ACC-G2 still offers a simple telnet server for allowing user access to the application. Telnet is not encrypted, so any password used to gain access to the ACC-G2 can be "seen" on the network.

We recommend that telnet should be disabled from SiPass after the initial setup of the ACC-G2.

## 2.3 ACC-AP

### 2.3.1 General Information

The IP-based AP door controller offers the latest technology, better cost-effectiveness, and easy installation.

It supports:

- 2 OSDP Readers: Controller for one or 2 doors (depending on configuration)
- 4 Monitored or Unmonitored Inputs
- 2 Relay Outputs
- 4 Open-collector Outputs
- 1 general-purpose FLN bus to connect to IPM, OPM, 8IO devices and Aperio® AH30
- Capacity for 500,000 cards
- Maximum 5 cards per user
- Large offline event buffer with up to 200,000 events
- Anti-passback
- Linux O/S


**Note:** Only Input/Output devices and IAT are supported on the FLN Bus. No RIM device support available.

The onboard **Dual Reader Interface (DRle)** on the ACC-AP can be programmed to function as any one of the door sets (Dual Reader, Two Single Readers, Dual Reader Turnstile Contact, Single Reader Turnstile Contact) at one time.

### 2.3.2 Configuring the ACC-AP Controller

See section ACC-G2 USB Client Application for more details.

### 2.3.3 Onboard Door (DRle) Interfaces

	<b>NOTICE</b>
	<b>IMPORTANT</b> Before connecting the Wiegand readers to the ACC AP DRle, the End of Line (EOL) jumper for the readers <b>MUST BE DISABLED</b> . If the EOL jumpers are On (default setting), the Wiegand reader will not work.

#### 2.3.3.1 Dual OSDP Reader Door Configuration

Label on AP Controller	SiPass Point Function
IN 1	REX
IN 2	D/C
IN 3	In 1 In case of ACC-APM 12V/24V PSU Kit, the pre-wiring is already done for power monitoring.
IN 4	In 2 In case of ACC-APM 12V/24V PSU Kit, the pre-wiring is already done for cabinet tamper.
RLY 1	Door 1 LK
RLY 2	Out 1
OUT 1	Door 1 AUX
OUT 2	Out 2
OUT 3	Out 3
OUT 4	Out 4
READER 1	Port for connecting both OSDP Readers
READER 2	NOT USED

#### 2.3.3.2 2 Single OSDP Reader Doors Configuration

Label on AP Controller	SiPass Point Function
IN 1	Door 1 REX
IN 2	Door 1 D/C
IN 3	Door 2 REX
IN 4	Door 2 D/C
RLY 1	Door 1 LK
RLY 2	Door 2 LK
OUT 1	Door 1 AUX
OUT 2	Door 2 AUX
OUT 3	Out 3
OUT 4	Out 4
READER 1	Port for connecting both OSDP Readers
READER 2	NOT USED



ACC-APM can be used for this door mode if IN3 and IN4 are not used for power monitoring and cabinet tamper.

### 2.3.3.3 OSDP Reader Turnstile, Single Door Contact Configuration

Label on AP Controller	SiPass Point Function
IN 1	Door 1 REX
IN 2	Door 1 D/C
IN 3	Door 2 REX
IN 4	In 1
RLY 1	Door 1 LK
RLY 2	Door 2 LK
OUT 1	Out 1
OUT 2	Out 2
OUT 3	Out 3
OUT 4	Out 4
READER 1	Port for connecting both OSDP Readers
READER 2	NOT USED



This configuration is not compatible with ACC-APM 12V/24V PSU Kit because IN 3 is pre-wired for power monitoring, and IN4 for cabinet tamper.

### 2.3.3.4 OSDP Reader Turnstile, Dual Door Contact Configuration

Label on AP Controller	SiPass Point Function
IN 1	Door 1 REX
IN 2	Door 1 D/C
IN 3	Door 2 REX
IN 4	Door 2 D/C
RLY 1	Door 1 LK
RLY 2	Door 2 LK
OUT 1	Out 1
OUT 2	Out 2
OUT 3	Out 3
OUT 4	Out 4
READER 1	Port for connecting both OSDP Readers
READER 2	NOT USED



This configuration is not compatible with ACC-APM 12V/24V PSU Kit because IN 3 is pre-wired for power monitoring, and IN4 for cabinet tamper.

### 2.3.3.5 Dual Wiegand Reader Door Configuration

Label on AP Controller	SiPass Point Function
IN 1	REX
IN 2	D/C
IN 3	In 1 In case of ACC-APM 12V/24V PSU Kit, the pre-wiring is already done for power monitoring.
IN 4	In 2 In case of ACC-APM 12V/24V PSU Kit, the pre-wiring is already done for cabinet tamper.
RLY 1	Door 1 LK
RLY 2	Out 1
OUT 1	Green LED for Reader 1
OUT 2	Red LED for Reader 1
OUT 3	Green LED for Reader 2
OUT 4	Red LED for Reader 2
READER 1	Pins A and B of READER 1 port are the data lines for Wiegand Reader 1. D1 = A; D0 = B
READER 2	Pins A and B of READER 2 port are the data lines for Wiegand Reader 2. D1 = A; D0 = B

### 2.3.3.6 2 Single Wiegand Reader Doors Configuration

Label on AP Controller	SiPass Point Function
IN 1	Door 1 REX
IN 2	Door 1 D/C
IN 3	Door 2 REX
IN 4	Door 2 D/C
RLY 1	Door 1 LK
RLY 2	Door 2 LK
OUT 1	Green LED for Reader 1
OUT 2	Red LED for Reader 1
OUT 3	Green LED for Reader 2
OUT 4	Red LED for Reader 2
READER 1	Pins A and B of READER 1 port are the data lines for Wiegand Reader 1. D1 = A; D0 = B
READER 2	Pins A and B of READER 2 port are the data lines for Wiegand Reader 2. D1 = A; D0 = B



This configuration is not compatible with ACC-APM 12V/24V PSU Kit because IN 3 is pre-wired for power monitoring, and IN4 for cabinet tamper.

### 2.3.3.7 Wiegand Reader Turnstile, Single Door Contact Configuration

Label on AP Controller	SiPass Point Function
IN 1	Door 1 REX
IN 2	Door 1 D/C
IN 3	Door 2 REX
IN 4	In 1
RLY 1	Door 1 LK
RLY 2	Door 2 LK
OUT 1	Green LED for Reader 1
OUT 2	Red LED for Reader 1
OUT 3	Green LED for Reader 2
OUT 4	Red LED for Reader 2
READER 1	Pins A and B of READER 1 port are the data lines for Wiegand Reader 1. D1 = A; D0 = B
READER 2	Pins A and B of READER 2 port are the data lines for Wiegand Reader 2. D1 = A; D0 = B



This configuration is not compatible with ACC-APM 12V/24V PSU Kit because IN 3 is pre-wired for power monitoring, and IN4 for cabinet tamper.

### 2.3.3.8 Wiegand Reader Turnstile, Dual Door Contact Configuration

Label on AP Controller	SiPass Point Function
IN 1	Door 1 REX
IN 2	Door 1 D/C
IN 3	Door 2 REX
IN 4	Door 2 D/C
RLY 1	Door 1 LK
RLY 2	Door 2 LK
OUT 1	Green LED for Reader 1
OUT 2	Red LED for Reader 1
OUT 3	Green LED for Reader 2
OUT 4	Red LED for Reader 2
READER 1	Pins A and B of READER 1 port are the data lines for Wiegand Reader 1. D1 = A; D0 = B
READER 2	Pins A and B of READER 2 port are the data lines for Wiegand Reader 2. D1 = A; D0 = B



This configuration is not compatible with ACC-APM 12V/24V PSU Kit because IN 3 is pre-wired for power monitoring, and IN4 for cabinet tamper.

## 2.3.4 Extension Interfaces

### 2.3.4.1 Extension Option

Label on AP Controller	SiPass Point Function
COMMS1	FLN 2 for MFI*, IAT and I/O devices (8IO, IPM, OPM)  *See section Multi-Function Interface (MFI) [→ 35] for more information.
COMMS2	Not Used

### 2.3.4.2 Aperio Wireless Doors Extension Option

Label on AP Controller	SiPass Point Function
COMMS1A	AH30 RS485 Data A
COMMS1B	AH30 RS485 Data B
COMMS2	Not Used
AP Vout-	AH30 GND
AP Vout+ (or READER1,2+)	AH30 PWR 8-24V

For further details, refer to the section about Aperio setup in this document.

## 2.3.5 Power Monitoring Limits

- The AP Controller should be provided with power in the range of: 12V – 24V DC. The AP Power Supply must be protected by a fuse (2A).
- An Audit Trail Message will be produced if the voltage level drops below 10.5V or goes above 26.5V.
- Absolute maximum power ratings are: 9.5V – 29.5V DC.
- The Reader Power Supply outputs are protected by a thermal fuse. In the event of a short-circuit the fuse will trip. The fuse will automatically reset in about 30 seconds if the fault has cleared.

## 2.3.6 Factory Reset Button

To set the IP Network Settings of the AP Controller back to its default values, hold the **Factory Reset Button** down for 10 seconds during standard operation. (See image in section Updating the AP Controller with Micro SD Card [→ 25]).



## 2.3.7 Restoring/Updating Platform via SD Card

### 2.3.7.1 Preparing the SD Card

Before you begin, prepare the SD Card by following the steps below:

1. Insert the Micro-SD (2 GB minimum) card into the computer. (Use a Micro-SD to SD Card adapter, if required)
2. Unzip the `~.7z` file (in *Firmware\ACCIAP01P (AP)\SD\_Card* folder) to extract the ".img" file. (This file can be opened using the 7-zip file archive utility which can be downloaded from the internet, if not already installed on your computer.)
3. Use *Win32DiskImager* (in *Tools\ACC-G2 SD-Card Creator Tool* folder) to write the `~.img` file to the SD Card.

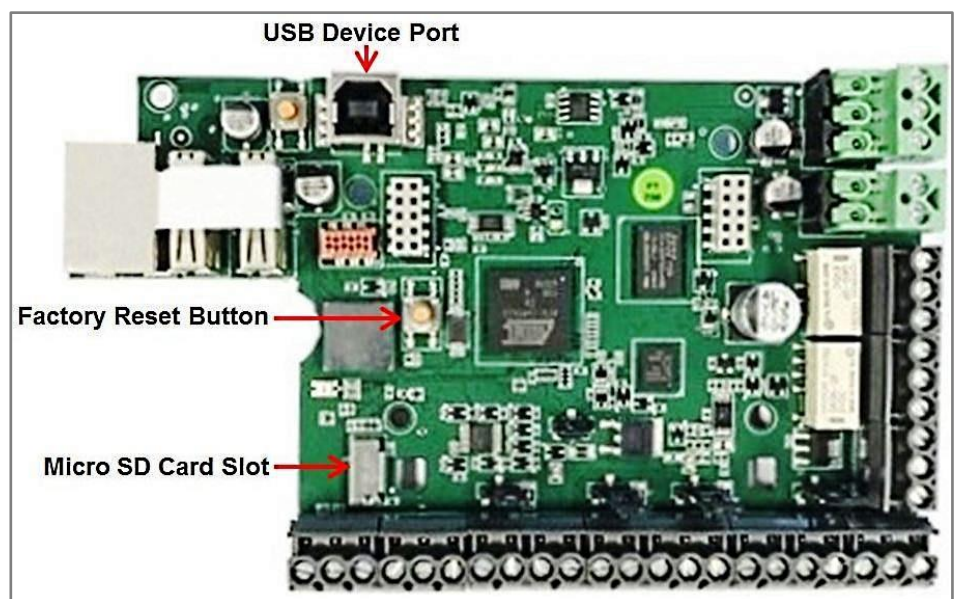
**Note:** The disk imager program must be installed on your computer, not on the Micro-SD card.

### 2.3.7.2 Updating the AP Controller with Micro SD Card



**Note:** In case of SD Card update, the database configuration and system settings will be lost.

1. Power down the controller and open the case to expose the circuit board.
2. Insert the Micro SD Card in the slot, as shown in the picture.



3. While holding down the Factory Reset Button, switch the unit on. Release the button after 5 seconds.
  - ⇒ The LED will show the following states as the controller is booting and updating:
    - RED: The controller is starting up.
    - Flashing ORANGE or GREEN: The controller is in different stages of the update.
    - Steady ORANGE: When the LED turns to steady ORANGE, wait 7 seconds till update is finalized.
4. Remove power from the controller, remove the SD card, and restart.

**Note:** LED flashing RED at any stage indicates an error in the update process. In this case, repeat the steps above to begin update again.

**Once the controller is powered up, the network settings must be configured as described in Section Configuring the ACC USB Client Application [→ 5].**

The AP Controller is now set up and can be connected to SiPass integrated.

## 2.3.8 Platform Upgrade via Firmware Download

Before attempting to perform a platform upgrade via Firmware download, ensure that you are using:

- Platform version V1.0.6 (or later) and
- AP Application Version V2.75.11 (or later)

If using an earlier platform version, you must perform the platform upgrade via SD-Card to upgrade to platform version V1.0.6 or later. The SD-Card for platform V1.0.6 will also contain AP application version V2.75.11.

For more details see the Common Firmware Update Procedure [→ 11] section.

## 2.3.9 LED Indications

### 2.3.9.1 During SD Card Update

LED Indication	Description
RED – On	Siemens bootstrap and u-boot running
ORANGE – Flashing	NAND Flash update is in progress
GREEN – Flashing	NAND Flash update finished, SD card shutting down
ORANGE – On	<ul style="list-style-type: none"><li>• SD-Card shut down. Count to 7, remove power, remove SD card, restart.</li><li>• After SD-Card removal – ACC-Application running</li></ul>
RED - Flashing	Update failed. Retry SD-Card update

### 2.3.9.2 During ACC-Application (Run-Time)

LED Indication	Description
RED	Controller is starting up
ORANGE	Application running
GREEN	Application running, connected with SiPass integrated
OFF (Dark)	Application not running. (This can occur during a Firmware upgrade.)

## 2.4 4101-3 (ACC-Granta)

### 2.4.1 Configuring using USB Client Application

See section ACC-G2 USB Client Application for details.

### 2.4.2 Network Discovery

See section ACC and FLN Field Service Network Tool for details.

### 2.4.3 Restoring Default Network and Password Settings

The X992 jumper is near the battery for the Real Time Clock (RTC)

Short the pins of X992 for 3 seconds (using a jumper), until the orange ERROR led is blinking quickly. Remove the short, and wait about 10 seconds for application to restart and reset the network settings.

The default network settings are:

IP Address : 192.168.1.250

Subnet Mask : 255.255.255.0

Default login credentials: SIEMENS/spirit

All other settings are zeroed (including the SiPass host address) and modem configuration is disabled. The SSH server is re-enabled as well as the Telnet server.

Use either Telnet, the USB Client Application or the Network Configurator tool to restore the network settings.

## 2.4.4 Recovering a Non-responsive Board

Try the X992 jumper option first. If this does not work, it is possible to restore a board completely to factory settings.

**Note:** This requires that the cover be removed from the Controller and a SD card. The SD card must be a plain SD card, 2GBytes or less. SDHC cards will not work.



---

CCP2 SD Card must not be used on Granta controller as it may make it inoperable.

---

1. Unzip the ZIP file for example, (*acc-granta\_2.70.xx\_sdcard.zip*) into its own directory.
2. Copy ALL the files to a good quality SD card of at least 32 Megabytes in size.
  - ⇒ SanDisk and Lexar have both been tested and found to be good. A no name brand was mostly OK, but would sometimes fail. Make sure a file called "boot.bin" is present in the top directory of the SD Card.
3. Plug the SD card into the Controller, while it is powered off.
4. Place a jumper on Jumper X-120, and power up the Controller.
  - If the Controller was manufactured before 2012, Press the reset button once for at least a second and then release.
  - If the Controller was manufactured in 2012 or later, the reset button need not be pressed.
5. Watch the LEDs at the base of the SD card socket. The orange Error and green COM and USB LEDs should be flashing in a cycle while the board is being reprogrammed. When the LEDs stop flashing, programming is complete.
6. Power off the board, remove jumper X-120 and remove the SD card.

**Note:**

- SD Card reprogramming will not modify the MAC address or other manufacturing data.
- The IP address will be set to the default value of 192.168.1.250, and that the SSH server will be running on port number 10022.

## 2.4.5 Network Security

The ACC-GRANTA uses Linux as an operating system, which provides both an increased level of security and reliability, but also requires some extra care in security.

Summary: disable both SSH and telnet for maximum security, and set a root password.

### SSH

A SSH server is by default running on the ACC-GRANTA. This allows for access to the linux shell console for maintenance purposes and trouble shooting, but in normal operation should be disabled so that it is not bound to the Ethernet interface, but instead restricted to just the local USB Ethernet interface.

Disable external access to the SSH server with the console command:

```
set ssh usb
```

SSH access can be enabled with the console command:

```
set ssh all
```

The TCP port number that the SSH server listens on is 10022. This can be changed with the console command:

```
set ssh port xyz
```

Where xyz is a valid and unique TCP port number.

The standard port number for SSH is port 22, but many network probing tools attack port 22 by default.

### Root Password

The username for gaining access to the linux shell is “root”, the password is the default root password “spirit”.

The root password can be changed within the application via telnet, using the command:

```
set rootpassword Large_String
```

where `Large_String` should be long phrase that meets the requirements for a strong password. Use double quotes if the string contains spaces, but don't use double quotes when entering the password via SSH login.

### Telnet

The ACC-GRANTA still offers a simple telnet server for allowing user access to the application. Telnet is not encrypted, so any password used to gain access to the ACC-GRANTA can be “seen” on the network.

It is recommended that telnet should be disabled from SiPass after the initial setup of the ACC-GRANTA.

## 2.5 AC5100 (ACC-G1)

Refer to AC5100 Installation Manual for details.

1. Connect an Ethernet cable to the ACC. For details on configuration, see the respective hardware manual.
2. From the Windows Command Prompt dialog (Select Start > Run > cmd) download the firmware to the ACC using the following command from the firmware directory:

```
D:\firmware>tftp -i xxx.xxx.xxx.xxx put [filename] image where:
```

xxx.xxx.xxx.xxx = the ACC's IP address [filename] = the filename of the firmware

Default ACC IP Address: 192.168.1.250

Default ACC Subnet Mask: 255.255.255.0

Once download is complete, boot the ACC using the boot command in the HyperTerminal window. Once the initial version of firmware has been downloaded, new versions can be updated using SiPass integrated.

### 2.5.1 Restoring Default Network and Password Settings

The ACC G1 does not have a "set defaults" jumper. It can be recovered as below:

1. Downgrade to a 2.65 build.
2. Use the "set defaults" command from the Telnet console or DIAG port connected to a serial port on a computer. (The default IP address is now: 192.168.1.250)
3. Reset the ACC.
4. Login via the DIAG port. Default login credentials are: SIEMENS/spirit
5. Reset the network settings.
6. Then upgrade back to MP 2.70, login and change the password when asked.

## 2.6 AC5200 (ACC-Lite)

Refer to AC5200 Quick Start Manual for details.

Firmware downloads are done from the SiPass integrated software. This process is the same as downloading firmware for an ACC.

### Before you begin:

The AC5200 must be created in the SiPass integrated database and be communicating

### To download firmware to the AC5200:

1. Select **System > Initialize**.
2. Double click your AC5200 from the list of available units.
3. Click **Image Download**.
4. Click **Browse** to select the firmware image to download.
5. Click **Download**. The selected firmware will be downloaded and the AC5200 will reset once it has been upgraded.
6. Click **Close** to close the Initialize System dialog.

### Accessing Menu via Keypad

- PIN access to the LCD Menu for ACC-Lite firmware is available SiPass integrated MP2.7 onward. The default PIN is '1111'.
- If you upgrade from an earlier version of ACC-Lite to the SiPass integrated MP2.7, opening the keyboard and logging in for the first time with the default PIN will require setting a new PIN for security purpose.
- The PIN must be secure with length from 4-10 digits. Save this new PIN in a secure place after setting.
- If you change the ACC-Lite PIN but forget, there is an ACC telnet Console command to change the PIN.
- If both PIN and telnet passwords are lost then it must be returned to factory or Siemens.
- If you changed the PIN using SiPass integrated MP2.7, install an earlier version of the ACC-Lite firmware, then again re-install MP2.7, you must login with the PIN that was previously set (because the PIN has already been changed using the MP2.7 build, setting a new PIN is not required again).

### 2.6.1 Restoring Default Network, Password and PIN Settings

To recover the PIN: Telnet to the ACC-Lite and use the `pin ****` console command to change the PIN.

To recover the Password:

1. Downgrade to a MP 2.65 build.
2. Use the `set defaults` command from the Telnet console. (The default IP address is now: 192.168.1.250)
3. Reset the network settings.
4. Reset the ACC.
5. Upgrade back to MP2.70
6. Login via telnet. Default login credentials are: SIEMENS/spirit
7. Change the password when asked.

## 3 FLN Devices and Readers

### 3.1 ADD5100 Dual Reader Interface (DRI)

The ADD5100 is programmed using *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the respective User Guide for more Information.

### 3.2 ADE5300 Eight Reader Interface (ERI)

The ADE5300 is programmed using *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the appropriate User Guide for more information.

### 3.3 ADS5200, ADS5210 Single Reader Interface (SRI)

The ADS5200 is programmed using the *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the respective User Guide for more Information

### 3.4 AFI5100 (IPM)

The AFI5100 is programmed using *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the appropriate User Guide for more Information.

### 3.5 AFO5100 (OPM)

The AFO5100 is programmed using *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the appropriate User Guide for more Information.

### 3.6 AFO5200 (8IO)

The AFO5200 is programmed using *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the appropriate User Manual for more information.

### 3.7 ATI5100 (IAT)

The ATI5100 is programmed using *FLN Configuration* tool in *SiPass integrated Configuration Client* or using the stand-alone *ACC & FLN Field Service Tool* application. See the appropriate User Manual for more information.

### 3.8 OSDP Reader Devices

With SiPass integrated MP2.76 onward, you get the support for connecting OSDP Reader Devices directly to controller FLN (for ACC-G1 and ACC-G2 only). The OSDP Reader devices are programmed using *FLN Configuration* tool in SiPass integrated Configuration Client.

OSDP Reader can be logically linked/unlinked to any existing ERI, DRI or SRI (on the same ACC unit) to act as a **Replacement Reader** in case when encrypted reader communications are required.

For more information, see the *Configuration Client User Guide* in SiPass integrated software bundle.



## 3.9 ARxxx-MF / VRxxx-MF Reader

### 3.9.1 RIM Settings

It is recommended that the ARxxS-MF/VRxxx-MF OSDP reader technology be selected if the UID number of a MIFARE card has to be read. The corresponding Base Card Technology that has to be licensed is the Siemens Readers clock/data RS485.

If Sector/Block information of a MIFARE Classic or/and Application ID of a MIFARE DESFire card has to be read, select "Siemens Mifare Facility". This is the corresponding Reader Technology if MIFARE cards are encoded with SiPass integrated.

More details can be found inside the training documentation.

### 3.9.2 Required Settings for Reading the UID Number of a MIFARE Card

1. Open the FLN configuration and navigate to the RIM (DRI/ERI) which the new ARxxx-MF/ VRxxx-MF reader is connected to.
2. Download the new firmware to the corresponding RIM.
3. Select **ARxxx-MF/ VRxxx-MF OSDP** reader technology in the *Configuration* Tab.
4. Set the option **Reader Tamper Auto-Reset**.
  - ⇒ **Note:** The ARxxx-MF/ VRxxx-MF reader is equipped with a Tamper contact. For a higher security level the **Reader Tamper Auto-Reset** setting should be set to **No**. If this option is chosen and a tamper event occurs, the operator must reset the Tamper manually from the *Component* dialog.
5. Save the configuration.

## 3.10 Wiegand Reader on ACC-AP

- The ACC-AP has a 560-ohm pullup on the A+ line, which can make few Wiegand readers incompatible. For example, the AR6111 MX reader is known to be NOT working.

**HID Wiegand readers are recommended** to ensure compatibility and optimum operation.

- The **card technologies for DR1e in Wiegand Mode** are listed in the **Reader** dropdown list in the *Configuration* tab of the *FLN Configuration* dialog. The following card technologies are supported:

- CustomWiegand
- AllHidProx
- Prox26Bit
- ProxAsco36Bit
- ProxCorp1000
- ProxSiemensEncr
- ProxSiemensStg
- MifareCsn32
- MifareCsn40
- WiegandBCD
- WiegandAscoFacility
- Indala27Bit
- Cotag27Bit
- Indala32Bit
- Prox36BitCodeCard
- Prox34BitCodeKey
- DigikeyProx
- NorwayPost
- MifareUID56
- SaltoWiegand34
- EricssonWiegand
- Europlex34Bit
- Remec37Bit

See the documentation in SiPass integrated software bundle for more information on the following topics:

- **Wiegand Readers connections with ACC-AP**
  - See the *ACC-AP Technical Manual*
- **Configuration of Wiegand Readers with ACC-AP through SiPass integrated user interface**
  - See the *Configuration Client User Guide*

### 3.11 Multi-Function Interface (MFI)

With release MP2.80 onward, SiPass integrated offers you the **Multi-Function Interface (MFI)** that adds-on to the powerful functionality of the ACC-AP door controller.

It can be added under ACC-AP (FLN 2 with *ACC FLN Bus* type) and then, door readers can be connected in different combinations, as required. See the *SiPass integrated Configuration Client User Guide* for more information.

Alternatively, you can use the *FLN Configurator* and *FLN Field Service Tool* located in the *Tools* folder in SiPass integrated software bundle.

#### Features:

- Up to 4 MFI devices per ACC-AP can be connected, with up to 4 doors per MFI (total of up to 16 doors per ACC-AP)
- MFI I/O Only Mode: I/O device with 8 inputs and 8 outputs. Can be used for general I/O, intrusion and low level-elevator control.
- MFI Door Controller Mode: Secure OSDP V2 (encrypted) communication between Door Reader and MFI
  - 2 Door mode using up to 4 OSDP readers
  - 4 Door mode using up to 8 OSDP readers
- Support for global reader manufacturers
- Support for mixed configuration with IPM, OPM, 8IO and IAT in the same FLN bus

## 3.12 Aperio Wireless Lock Technology

With the enhancements made in SiPass integrated MP2.76 SP1 onward, the Aperio® Wireless Lock technology is expanded to support multiple Aperio Hubs connected to one ACC-AP through the Aperio FLN Bus (RS485 communication channel). Up to 32 wireless Aperio Lock devices can be paired across all the Aperio Hubs connected to one ACC-AP FLN. You can select the Card Technology for selected locks and also assign a custom card format.

### 3.12.1 SiPass Card Technologies in Aperio Locks

Card Technologies supported by Aperio Locks must be configured in SiPass integrated to read correct sectors and blocks from the cards. This is especially required for existing site installations having various types of card technologies already in use.

Currently, SiPass integrated supports the following card technologies in the FLN Configuration tool for Aperio Wireless Locks:

- Siemens Mifare GID
- Siemens Mifare Facility
- Siemens RS485 UID
- All HID Prox: Currently encoded on smart card only for Aperio
- Custom Card (Weigand): Currently encoded on Mifare card only for Aperio
- iClass OSDP: Required for sites that use iClass readers and might have iClass OSDP Credential Profile.



---

With MIFARE cards, the Sector + Block is configured. **In the Aperio configuration, there is no Block; and a Byte Offset is used for the Sector.**

---

The following Blocks are equivalent to the Byte Offset:

- Block 0 = 0 Byte Offset
- Block 1 = 16 Byte Offset
- Block 2 = 32 Byte Offset
- Block 3 = 48 Byte Offset

**Each Block is 16 bytes.**

### 3.12.2 Connecting Aperio Hub with ACC-AP

See section Aperio Wireless Doors Extension Option [→ 24] for details on *Aperio Wireless Hub Connection Points* and *ACC-AP Connection Points*.

#### DIP Settings

DIP Switch	State	Description
1	ON	Address 0
2	OFF	Address 1
3	OFF	Address 2
4	OFF	Address 3
5	OFF	Address 4
6	OFF	Pull Down Bias – already done at ACC-AP
7	OFF	Pull Up Bias – already done at ACC-AP
8	ON	RS485 End Of Line – set the ACC-AP RS485 EOL jumper to OFF if you intend to use a Star configuration with multiple AH30 hubs.
9	OFF	Not used
10	ON	Internal Antenna selected, set to OFF if an External Antenna is used.



The above DIP switch settings will set the AH30 hub to **Address 1, RS485 termination enabled, Internal Antenna**

If you wish to vary the above configuration, see the the *Aperio Online Mechanical Installation Manual* from the AH30 Hub manufacturer (Assa Abloy) for further details.

## 3.13 Help and Documentation

The hardware for Aperio Wireless Technology and Multi Function Interface (MFI) is not supplied by Siemens. However, to help you quickly setup everything, SiPass integrated documentation gives you the required support information sourced from the device manufacturer. The standard SiPass firmware documentation also helps you at places during the whole process.

While setting up the Aperio Wireless Hub and Locks and / or MFI, it is recommended that the following documents (from SiPass integrated Software bundle) are read in conjunction:

- SiPass integrated Controller and Device Installation Guide
- ACC-AP Technical Manual
- Multi Function Interface (MFI) Technical Manual
- SiPass integrated Configuration Client User Guide
- Aperio Wireless Lock Support Guide



Siemens does not take responsibility for the correctness of the content with regards to the Aperio or MFI devices you may use. In case of any issues or requirement of more information, the device manufacturer should be contacted directly.

Issued by  
Siemens Switzerland Ltd  
Smart Infrastructure  
Global Headquarters  
Theilerstrasse 1a  
CH-6300 Zug  
+41 58 724 2424  
[www.siemens.com/buildingtechnologies](http://www.siemens.com/buildingtechnologies)

© Siemens Switzerland Ltd, 2020  
Technical specifications and availability subject to change without notice.

---

A6V11164550