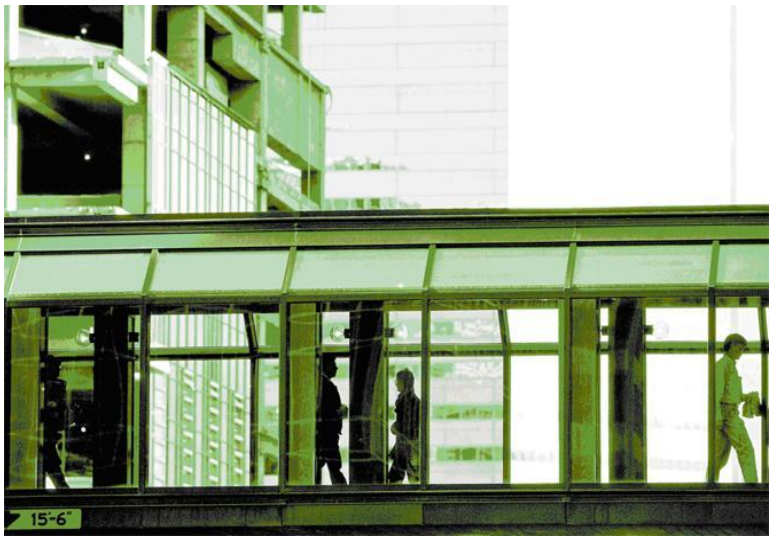
SIEMENS



Access Control

SiPass® integrated MP2.65

Product Release Notes

MP2.65 SP3

A-100083-1
02.2016

Building Technologies

CPS Fire Safety

Copyright

Edition: 02.2016

Document ID: A-100083-1

Contents

1 Introduction

SiPass® integrated is an advanced access control system. Its superior range of security features ensures that it is an ideal access control solution for any application regardless of size or complexity.

SiPass integrated MP2.65 is your interoperable security solution. It combines advanced access control with easy yet powerful connectivity to Video, Intrusion (SPC), Building comfort (APOGEE, DESIGO CC), OPC A&E compliant applications, Building Management Stations, Offline door access systems (SALTO), and finally Fire and Danger Management (MM8000).

SiPass integrated -- Opening doors to a secure environment.

1.1 SiPass integrated MP2.65 and Interoperability

This service pack for SiPass integrated MP2.65, introduces a number of enhancements and quality improvements to the Access Control and Security system.

1.2 What this document covers

This document details the changes that have been made to SiPass integrated and the important information that users need to be aware of when ordering, installing and troubleshooting.

1.3 Ordering

To order the SiPass integrated software, please use the order forms provided and the part numbers specified on these forms.

2 Important Release Information (Pre-Requisites)

Before installing SiPass integrated, refer to the SiPass integrated Installation Guide for important information about installing the software. The SiPass integrated Installation Guide contains all the necessary procedures to install and upgrade the software and all other associated hardware and software components. This guide can be found in the SiPass integrated software bundle.

2.1 Security Recommendations

This section details important security recommendations regarding the installation of SiPass integrated on public domains. It also deals with the important issue of protecting your software system from virus infections.

2.1.1 Installing SiPass integrated / ACCs / Dialups on a Public Domain

Users please note that installing SiPass integrated on a public domain presents vulnerabilities (e.g., being infected by PC viruses) like any application running on a Windows environment.

If SiPass integrated or ACCs etc. are to be installed on a public domain, it is recommended that a dedicated network (like a minimal VLAN) be used for optimal security. Telnet and SSH on the controllers should be disabled after installation. Further, installation of the server and the client as dedicated applications on PCs is advisable. It is also recommended that all default passwords that are used to install the software are changed immediately as these are published in documents (not having any security control).

SiPass integrated users are also advised to lockdown USB ports on the PCs where SiPass integrated has been installed. Further, it is recommended that client PCs for non-administrator operators should be locked down.

2.1.2 Reducing Security Risks with Anti-Virus Software

It is recommended that all SiPass integrated operators install and run an Anti-Virus or Virus Scan application to protect your computer from viruses, and other security threats that can compromise the performance of the system. SiPass integrated has been tested with the TREND MICRO Office Scan software.

As there are numerous brands of anti-virus software available in the market, it is recommended that you first investigate the source of software before downloading and installing it. It is advisable that you choose a virus scanner that best meets the needs of your particular software environment. It is also important that you test your anti-virus application with SiPass integrated before going live to ensure that the anti-virus application does not impact the performance of your security management. Contact vendors of the chosen anti-virus software for instructions and updates.

2.2 Windows Patches and Hot Fixes

It is expected that SiPass integrated will continue to operate as normal if you automatically update your PC with any updates or patches provided by Microsoft. However, some exceptional changes made by Microsoft to their operating system may cause unexpected results. In these instances please report your problem to your local support representative and the issue will be investigated as soon as possible.

3 New Features for SiPass integrated MP2.65

With the introduction of several new and innovative features in this latest market package, SiPass integrated MP2.65 builds itself into a more robust and powerful system, that can meet all your access control requirements.

This section provides you brief information about the latest features and enhancements available in SiPass integrated Market Package 2.65.

3.1 Enhanced Access Assignment

The advanced intelligence of this new SiPass integrated market package makes it possible for operators to assign Multiple Access Rights to cardholders, workgroups or venues, without limitations on the number of access rights per cardholder.

SiPass integrated MP2.65 allows these access rights to be assigned as combination of **Private Access**, **Workgroup Access** and **Venue Access** rights for each cardholder. These access rights can be assigned permanently, or temporarily (with a specific start and end date & time).

In this enhanced market package, any modification to the access rights of a workgroup will be immediately applied to all cardholders of the workgroup. Further, cardholders with multiple workgroups assigned to them, will inherit all access rights from their workgroups.

Note that if a database is restored from MP2.60 or earlier, any existing workgroup access rights will be disabled by default in MP2.65. This is due to the new behaviour of workgroup access rights in MP2.65. In MP2.60 and earlier, workgroup access rights were transferred to cardholders after workgroup assignment, after which the cardholder access rights could be further customised. In MP2.65, disabling existing workgroup access rights by default will avoid giving unintended access to existing cardholders, since workgroup access rights are now inherited by the cardholder. Workgroup access rights can be enabled in the workgroup dialog if the operator is confident with the access configuration of the workgroup and cardholders involved.
Expired access can be removed automatically from cardholder and workgroup by using Host Based Event Tasks.

Conversion of older access concepts after upgrade to SiPass int. MP2.65

- **Temporary Access Groups:** On upgrade, each existing Temporary Access Group will be converted to a Venue **and** a Venue Booking, with the same temporary access group name.

  Any cardholders that were assigned to the Temporary Access Group will now be assigned to its converted Venue Booking.

- **Personalized Access Groups:** On upgrade, any existing Personalized Access Groups for a cardholder will be converted as **Private** access privileges.
  They will be visible (with the same Personalized Access Group name) under the **Private** access privileges tree, on the *Definition* tab of the *Cardholder* dialog.

- **Offline Access Groups:** On upgrade, any existing Offline Access Groups for a cardholder will be converted as **Private** access privileges.
  They will be visible (with the same Offline Access Group name) under the **Private** access privileges tree, on the *Definition* tab of the *Cardholder* dialog.

More details on Access Assignment can be found in the SiPass integrated MP2.65 *User Guide.*

3.2 Venue Management

This innovative feature is a powerful addition for sites with Meeting Rooms, Conference Halls, or similar shared locations used by several groups of people. SiPass integrated MP2.65 makes it possible to configure such shared locations as **Venues** with a collection of access components like access points, levels, groups and intrusion area points, etc.

The prime advantage of this feature is that operators can book these Venues for one-off or scheduled bookings using the **Venue Booking** feature in SiPass integrated Client and Web client.

Operators can also give configure access rights to cardholders as venue booking *Organizers* or *Participants*. Participant access rights can be configured privately to individual cardholders, and also to entire workgroups.

The Venue Booking User Interface provides an excellent visual overview of all the venue bookings across all venues, and also across calendar periods.

See section *4.3Venue Booking Event Trigger* for enhancements to this feature.

Note: The Temporary Access Group will be converted to Venues and Venue Bookings when upgraded to MP2.65.

3.3 Cardholder User Interface Enhancement

This market package provides enhanced features for the cardholder user interface, wherein the entire Cardho*lder/Visitor* dialog is customizable.

Compared to previous versions where operators could only add customized pages to the *Cardholder/Visitor* dialog; this market package features a completely customizable *Cardholder/Visitor* dialog, which contains a default pre-defined layout. Operators can customize the layout, and add/modify desired controls to any page, minimizing the need for opening multiple tabs in the dialog.

Different Operator Groups also have the flexibility of creating layouts specific to their group.

3.4 SiPass integrated Web Client

SiPass integrated MP2.65 successfully launches the remote management capability of its access control system, through its well-integrated Web Client.

Utilizing the same login credentials as the SiPass integrated client, the Web Client makes it possible to seamlessly manage Cardholdes, Venues and Venue Bookings, Access Levels, and Access Groups.

Linking of the web interface to the client layouts allow the Web Client to use customized layouts created in the SiPass integrated client, that can then be assigned to specific operator groups.

Please refer the *SiPass integrated Installation Guide* for details supported Browsers, Operating Systems and Smart Devices.

3.5 Enhanced DESFire Encoding

The DesFire Smart Card Encoding feature is enhanced in SiPass integrated MP2.65 to include the ability to distinguish between the **Master Key** and **Application Key** of the card.

This allows Cardholder field mapping in SiPass integrated to Applications and Files of the DESFire card in the Profile Configuration dialog.

It allows operators to set the Application Key and the Application Master Key, while supporting the DES, 3DES or AES Encryption Algorithm

3.6 Improved HR-API Functionality

In MP2.65, the HR-API is enhanced to be able to fully manage cardholders / visitor, Access Assignment, Access Level, Access Group, Venue and Venue Booking, Workgroups.

These improvements provide operators with advanced flexibility for Access Assignment in SiPass integrated via 3rd party applications. The HR-API also automatically notifies the 3rd party application about changes in SiPass integrated, related to Cardholders, Access Assignment or Venues/Venue Bookings, which allows applications to automatically synchronize with SiPass integrated.

3.7 Complete Support for AR40S-MF and AR10S-MF Readers

SiPass integrated MP2.65 fully supports the AR40S-MF and AR10S-MF readers. New reader firmware can be downloaded to the readers using the SiPass integrated software.

This new market package also supports encrypted communication between the controller and these readers using secure OSDP. This is currently supported for the DRIs.

The RIM firmware has also been enhanced to provide a date and time stamp to the LED display, once the card has been badged on the reader.

3.8 Upgrading from SiPass integrated MP2.65 to higher versions

SiPass integrated MP2.65 can upgrade to higher versions without uninstalling the current SiPass version on the system, while completely retaining the current database.

For detailed information, see *SiPass Integrated Installation Guide*. You can also see the section *SiPass integrated Upgrade Compatibility* in this document for information on SiPass integrated upgrade path.

For SiPass version Upgrade, and License Change:

Performing a SiPass version Upgrade, and License Update/Change cannot be done at the same time.

1. You must first upgrade to the new SiPass version required.
2. Next, run the installer file of the new SiPass version to update/change the license.

4 New Features for SiPass integrated MP2.65 SP3

4.1 Current Date Relative Report Filter

SiPass integrated cardholder report capability now helps you filter the search results for a date field relative to the current date.

You can filter a report for comparing any date field with the current date through the new *Current Date* option in the **Date Field Filter** dropdown list, by entering the number of days, hours and minutes before or after the date on which, the report is running.

More details can be found in the SiPass integrated MP2.65 SP3 *Explorer Manual.*

4.2 Command Line Option to Import and Export Data

The SiPass Data Synchronizer tool now supports the command-line capability that allows the user to run the data import and export operations in background (without using the User Interface). The *CardholderDataSynchronizer* command options help you specify the different requirements for the import and export operation.

More details can be found in the SiPass integrated MP2.65 SP3 *Data Synchronizer Tool & Import Export Tool User Guide*.

4.3 Venue Booking Event Trigger

The Advanced Security Programming (ASP) functionality in Sipass integrated now includes venue booking as event trigger. After setting up a venue, you can configure an ASP activity to trigger an action before or after every booking start or stop. This helps in creating different actions for the same venue based on the time the booking is made for that venue.

For example, an action can be configured to turn on the air conditioning 10 minutes before the booking start time, or turn on the lighting 5 minutes before the booking start time, or turn off the lighting and air conditioning 2 minutes after the booking stop time.

Note: In case of bookings with overlapping start and end times, care must be taken that an action for the start of next booking is not cancelled by the end time of the previous booking. For example, if the lights-on action is set to 11:00 am for Booking 2 but the lights-off action from Booking 1 is set to 11:02 am, the overlap in start and end trigger times of the two bookings will turn off the lights for booking 2.

See the SiPass Explorer MP2.65 *Explorer Manual* for more details on configuring ASP activities. More details of the event trigger properties can be found in the SiPass integrated MP2.65 SP3 *Reference Manual*.

4.4 Card and PIN Access/Intrusion Operation Mode

This operation mode provides the new option to secure/unsecure the intrusion areas. In case the cardholder wants to arm/disarm/part-arm the area before a card is presented at the access point, it can be done by selecting a number from the reader keypad. After this, a card badge followed by a valid PIN enables standard access and unlocks the door (while performing the selected arming action).

To prevent entry of a cardholder into an intrusion area while it is armed, the reader at the entry point must be configured as an entry lockout reader (that requires an arming action to be performed). If the reader is not configured as an entry lockout point, the cardholder can gain standard access through normal Card and PIN procedure without selecting any arming action.

In case the card reader is inside the intrusion area, the operator can configure delay time for the people to exit or enter the area. If the respective reader is installed outside the intrusion area as an entry lockout reader, the delay time is not required (as arming is done outside this area).

Note:

- The type of reader installed determines if ‘E’ or ‘#’ is used as the enter key for confirming the option selected by a cardholder.
- For the Card+PIN functionality, some card readers provide the option to enter a PIN first followed by a card badge. In this case, the ’E’ or ‘#’ key is not required to be pressed again after the PIN is entered, and the users just present their card (previous pressing of the E or # key for arming selection has no effect on this). However, if the card is badged first after selecting an arming action, the ’E’ or ‘#’ key must be pressed after entering the PIN.
- Some devices (like DC12, DC22, DC800, GrantaCotagCard and GrantaSwipeCard) do not require a button to be pressed after entering the PIN. For example, when entering a PIN at a BC43 reader connected to such a device, the user does not have 'E' or '#' or 'OK' button to send the PIN.
  - If the card has been badged, the user can enter the PIN directly (which is automatically processed).
  - If the card has not been badged, each key is processed individually. In this case, the user can press the respective key to arm/disarm/part-arm the area, badge the card and enter the PIN for authentication.

  In both the above cases, the PIN is processed automatically after the last key for the PIN is pressed and the applicable action is performed.

More details can be found in the SiPass integrated MP2.65 SP3 *Reference Manual*.

4.5 Discontinued Functionality

In the year 2007, any last orders for the CerPass hardware were asked through a phase-out notice. The hardware model has been supported till SiPass integrated MP2.6 version. Due to major changes within the access control assignment and configuration within SiPass integrated MP2.65 and further, this support was not able to be continued and a note was placed in the *Sales Delivery Release SPLN-2013-139-A* document.

Note that the support for the hardware (within any SiPass integrated market packages) is not maintained. To prevent any potential support issues in future, the CerPass migration part number (below) will no longer be available for ordering.

6FL7820-8AA40	ASL5000-CP	ASL5000-CP	CerPass Migration

SiPass integrated 2.5 and 2.6 will technically be able to support the connected CerPass hardware, but no further development or troubleshooting is supported. Technical support, limited as it may be, will be made available for this whilst the SiPass integrated MP2.6 is supported.

For advice on migrating the hardware from CerPass to the ACC controller platform, please contact your local "Vanderbilt International" representative.

4.6 Patch Tool

The newly developed Patch Tool greatly enhances the efficiency of deployment and management of hotfixes and patches, and will be used now onward for the purpose.

The source files used in conjunction with the tool, will be produced regularly depending on the number, and severity of the patches required in the field.

For more information on the patch tool and available patches, please contact your local helpdesk.

5 SiPass integrated Installation Compatibility

The following tables outline the components that have been tested with this version of SiPass integrated.

5.1 SiPass integrated Backup/Restore Compatibility

The following table displays the versions of SiPass integrated among which you can perform a database backup/restore.

	DATABASE BACKUP/RESTORE VERSION (The version you want to restore to)						
CURRENT VERSION (The version currently installed)	**SiPass integrated version**	**MP2.50**	**MP2.60**	**MP2.65**	**MP2.65 SP1**	**MP2.65 SP2**	**MP2.65 SP3**
	MP2.40	Yes					
	MP2.50		Yes	Yes	Yes	Yes	Yes
	MP2.60			Yes	Yes	Yes	Yes
	MP2.65				Yes	Yes	Yes
	MP2.65 SP1					Yes	Yes
	MP2.65 SP2						Yes

NOTE

SiPass integrated MP2.40 database backup must first be restored to version MP2.50, and then to MP2.65 SP3.

5.2 SiPass integrated Server

Note that the following tables relate to the English version of the Windows Operating Systems outlined.

Windows 8.1 (32-bit & 64-bit)	**Windows Server 2012 R2**	**Windows Server 2008 R2 (SP2)**	**Windows 7 (Professional, Enterprise) SP1** (32-bit & 64-bit)
✓	✓	✓	✓

*Some additional configuration settings are required to ensure that the specified versions of Windows operating systems operate correctly with SiPass integrated. Please refer Appendix 10.1 contained within the SiPass integrated MP2.65 SP3 Installation Guide for further information.

5.3 SiPass integrated Client

Note that the following tables relate to the English version of the Windows Operating Systems outlined.

Windows 8.1 (32-bit & 64-bit)	**Windows Server 2012 R2**	**Windows Server 2008 R2 (SP2)**	**Windows 7 (Professional, Enterprise) SP1** (32-bit & 64-bit)
✓	✓	✓	✓

NOTE

Whilst both the SiPass Server and Client can run on multiple Windows platforms, it is recommended that where possible a single operating system be chosen for an entire installation.

The same SiPass integrated version, as well as the same build of SiPass integrated should be installed on the SiPass integrated server and on all clients (local and remote), within the same system.

*Some additional configuration settings are required to ensure that the specified versions of Windows operating systems operate correctly with SiPass integrated. Please refer Appendix 10.1 contained within the SiPass integrated MP2.65 SP3 Installation Guide for further information.

5.4 Microsoft SQL Server

The following table indicates the supported SQL Server software on which SiPass integrated will run:

SQL 2014 (32/64-bit)	**SQL 2012 SP2** (32/64-bit)	**SQL 2012 SP2 Express** (64-bit)	**SQL 2008 R2 SP3** (32/64-bit)	**SQL 2008 R2 Express SP3** (32/64-bit)
Yes	Yes	Yes	Yes	Yes

If there are no SQL server versions installed on the computer where SiPass integrated is installed, SiPass integrated will automatically install a 32-bit version of Microsoft SQL Server 2008 R2 Express.

NOTE

Sites with multiple clients and higher activity (for example, a large number of doors / cardholders / or event transactions, involving more than 5 clients, 50 readers, or 10000 cardholders) are recommended to purchase a higher performance version of SQL optimized for both scalability and performance (for example, SQL Server 2008 Enterprise). Please refer to the Microsoft website for more information regarding SQL versions and performance at the following link: http://www.microsoft.com/en-us/server-cloud/products/sql-server-editions/default.aspx

Failure to install the appropriate version of SQL Server may have an adverse impact upon the performance of SiPass integrated.

Compatibility tests have been performed with SQL2014 but this is not supplied with the SiPass integrated software bundle.

5.5 .NET Framework

The following .NET Framework version is tested to be compatible with SiPass integrated:

.NET Framework Version 4.0	.NET Framework Version 4.5.2

5.6 Web Client Browser Compatibility

Internet Explorer (IE)* Min. version 10 and higher	**Firefox**	**Chrome**
✓	✓	✓

*If using IE10 for the SiPass integrated Web Client, ensure that you have turned off **Compatibility View** for the browser.

5.7 Web Client Smart Device Compatibility

SiPass int. Web Client	**Apple** iPhone	**Apple** iPad	**Samsung** Galaxy
	✓	✓	✓

5.8 System Compatibility

5.8.1 Firmware

AC5100 (ACC-020 / ACC-010) **Version 2.65.44**	**ADD51x0 (DRI)** **Version 3.38**	**ADS52x0* (SRI)** **Version 3.12**	**AFI5100 (IPM)** **Version 2.32**	**AFO5100 (OPM)** **Version 1.12**
✓	✓	✓	✓	✓

ADE5300 (ERI) **Version 3.34**	**AFO5200 (8IO)** **Version 1.02**	**ATI5100 (IAT-010)** **Version 1.05**
✓	✓	✓

DC12 **Mkl Version 1.36** **MKII Version 1.43**	**DC22** **Mkl Version 1.36** **MKII Version 1.43**	**DC800** **Version 1.23**	**IOR6** **Version 1.00**
✓	✓	✓	✓

AC5102 (ACC-G2) **Version 2.65.44**	**AC5200 (ACC lite)** **Version 2.65.44**	**Granta Mk3 (ACC-Granta)** **Version 2.65.44**	**Granta Mk3 Backboard** **Version 1.30**
✓	✓	✓	✓

5.8.2 Hardware

5.8.2.1 Controllers

AC5102 ACC-G2 Revision 3	AC5100 ACC Revision 3 ACC-020	AC5100 ACC Revision 2 ACC-010	AC5200 SR34i Revision 1	AC5200 SR35i Revision 1.4
✓	✓	✓	✓	✓

AC5200 SR35i MkII Revision 2	Granta Mk3 Revision 1
✓	✓

5.8.2.2 Door Control

ADD51x0 DRI Revision D	ADS52x0 SRI Revision B	ADE5300 ERI Revision A	ATI5100 IAT Revision A	4322 COTAG	4422 SWIPE
✓	✓	✓	✓	✓	✓

DC12 Rev 05	DC22 Rev 05	DC800 Rev. 04	PD30/PD40 Rev. 02
✓	✓	✓	✓

5.8.2.3 I/O

AFI5100 IPM Revision B	AFO5100 OPM Revision A	AFO5200 8IO Revision A	4253 I/O	IOR6 Rev. 04
✓	✓	✓	✓	✓

5.9 API / HLI Compatibility

The sections that follow provide information on the backwards compatibility of the current interfaces available in SiPass integrated MP2.65 SP3.

5.9.1 HR-API Interface

SiPass integrated HR-API allows data to be accessed and maintained from any programming language that supports COM automation.

SiPass integrated MP2.65 contains HR-API changes which means modification is required for any existing applications that have been built around versions previous to 2.65 HR-API.

5.9.2 Management/Enterprise Station API

SiPass integrated MS-API allows data to be accessed and maintained from any programming language that supports COM automation.

SiPass integrated MP2.65 contains MS-API changes which does not require modification to any existing applications, that have been built around versions previous to 2.65 MS-API.

5.9.3 OPC A&E Server Interface

SiPass integrated supports OPC A&E version 1.0.

5.10 Digital Video Recorder (DVR) System Compatibility

5.10.1 DVR Integration

	Version
SISTORE MX (including NVS)	**2.90 SP2**
SISTORE MX	**2.90 SP2 M1**
SISTORE CX	**3.6.4**
VECTIS HX	**2.1.5**
VECTIX iX	**2.10.0.236 (SDK 2.5.4.06)**

NOTE

For the above versions, **General SISTORE** option from the **Type** drop-down should be selected from the **DVR Switcher** tab on the *Component* dialog in SiPass integrated.

Siemens SISTORE MX	**Siemens SISTORE SX**	**Siemens SISTORE NVS**	**Siemens SISTORE CX1**	**Siemens SISTORE CX4/8**
Version 2.90 SP2	**Version 3.1**	**Version 2.90 SP2**	**Version 3.5**	**Version 3.5**
				Version 3.6

NOTE

For the above versions, **General SISTORE** option from the **Type** drop-down should be selected from the **DVR Switcher** tab on the *Component* dialog in SiPass integrated.

5.10.1.1 VSS-SDK Compatibility

VSS-SDK Version	Max. Resolution supported by VSS-SDK	Max. Bandwidth supported by VSS-SDK	Max. FPS supported by VSS-SDK
2.5.5	1920 x 1080 / 1280 x 1024	16 MBit/s	30 fps

The limits above also apply to IP cameras connected to SiPass integrated via RTSP (VSS-SDK Player).

5.10.2 Third-Party DVR Integration (Requires DVR-API Connection License)

Bosch Divar 700 Series	Bosch DivarXF	Bosch DivarMR
✓	✓	✓

Bosch Video Recording Manager	DVTel SiPass (F) Integration 6.2.2.1	DVTel SiPass (B) Integration 6.2.2.4
✓	✓	✓

NOTE

For the above BOSCH versions, **Generic** option from the **Type** drop-down should be selected from the **DVR Switcher** tab on the *Component* dialog in SiPass integrated

For compatible versions and support, please contact DVTel or Bosch.

Bosch DVR-API version 2.0 was tested in a Windows 7, 64-bit environment.

For further support on the Bosch integration package, contact local Bosch support in your region.

5.11 Directly-connected IP Camera Compatibility

AXIS P1354 Fix Camera	AXIS M30007 Fix Dom	AXIS P5534* PTZ – Dom, Live View	AXIS P7214** Video Encoder	Siemens CCIXI345	Siemens CCIC1410-L
✓	✓	✓	✓	✓	✓

NOTE:

- While the above cameras have been specifically tested, an IP camera using the RTSP protocol should work properly. Please test before purchasing and installing onsite.
- For live streaming with IP Cameras, SiPass integrated supports the RTSP as command protocol and RTP for the data stream. The Codecs that are supported are: MJPEG, MPEG4, H264.
- PTZ functions are not supported for any IP camera directly connected to SiPass integrated.
- **Only IN1 is supported.
- If recording is required, the IP camera has to be connected via DVR.

5.12 Intrusion Panel Compatibility

Intrunet SI 400 series (Sintony 400)	**SPC 4300, 5300, 6300** Intrusion System
✓	✓

NOTE

– AC5200 (ACC lite) controller does not work with SPC Intrusion system or Sintony 400.

5.13 Modem Compatibility

While the previous modems have been discontinued, Windows-based modems compatible with your operating system will work. It is recommended that the same modem type be installed throughout an installation to ensure compatibility. Other modem brands may be compatible but have not been tested. It is recommended that you test the compatibility of these modems prior to installation at any facility. Further, additional checks should be performed to ensure that your modem is compatible with your Operating System.

For any specific modem capabilities, contact your local support.

5.14 Card Printer Compatibility

Fargo Pro - Series	**Fargo High Definition (HDP600, HDP800)**	**Fargo Direct-to-Card (DTC500 Series)**	**Fargo Persona (C25)**
✓	✓	✓	✓

NOTE

The above table only lists those card printers that have been tested with SiPass integrated. All Windows compatible card printers should operate correctly with SiPass integrated 2.65. However, it is recommended that you test your card printer for correct operation before installation in a live environment. Further, additional checks should be performed to ensure that your card printer is compatible with your Operating System.

If using Windows 7 Operating System, please ensure that the firmware of your Card Printer is upgraded to be compatible with Windows 7 OS.

5.15 MiFare Classic Card Encoding (while printing)

Fargo with GEM Plus 680 SL encoder installed by Interproc (www.intraproc.com – GCI680 Driver)	**Fargo with GEMeasyAccess332 encoder, installed by Interproc (www.intraproc.com – GCI680 Driver)**	**OmniKey Cardman SK21**	**Fargo HDP5000 with built-in OMNIKEY 5121****	**Fargo HDP5000 with built-in OMNIKEY 5321****	**Fargo HDP5000 with built-in OMNIKEY 5421****
✓	✓	✓	✓	✓	✓

**Supported for Single printing and encoding, and Batch printing and encoding

5.16 Enrolment Reader Compatibility

5.16.1 USB Enrolment Readers

USB-RIF/2	CardMan 5321	CardMan 5421
✓	✓	✓

NOTE

The USB-RIF itself is not a reader, but a device to which a reader may be connected. Once connected the USB-RIF will convert the readers output into a USB signal for connection to a PC. Also note the USB-RIF only supports certain reader types.

The USB-RIF has severe restrictions with reading card types. It can read 26bit Wiegand, 32 bit Wiegand and all Siemens Clock/Data formats. No other formats are supported.

5.17 Card Format Compatibility

5.17.1 Reader Connection Types

Wiegand	RS-485	RS-232	Clock & Data
✓	✓	✓	✓

NOTE

(DRI Version D1) does not support the connection of RS-232 type readers.

5.17.2 Siemens Proprietary Card Formats

CerPass/SiPass RS-485	Siemens Corporate Card	31-bit STG	36-bit Asco	Siemens 52-bit
✓	✓	✓	✓	✓

5.17.3 Proximity Formats

26-bit (industry standard)	36-bit ASCO	27-bit Indala	27-bit Cotag	HID Corporate 1000/2000	Custom Wiegand
✓	✓	✓	✓	✓	✓

5.17.4 Smart Card Formats

32-bit CSN (CSN32)	40-bit CSN (CSN40)	26-bit Standard * (stored in sector)	ASCO 36-bit	HID* iCLASS UID
✓	✓	✓	✓	✓

NOTE

*SiPass integrated supports CSN, UID, and Data on-card for iCLASS HADP readers. Please note that the format for Data on-card should be a maximum of 8 bytes of binary data (no special format, just a 64-bit card number).

5.18 Card Reader Compatibility

5.18.1 Readers Supporting the DESFire EV1 Card Technology

Siemens RS485 UID	Siemens Reader Clk/Data UID	Siemens Reader Clk/Data Extended
✓	✓	✓

AR40S-MF	AR10S-MF	AR41S-MF	AR11S-MF
✓	✓	✓	✓

The above readers are all mapped to the Siemens Reader Card Technology, and become available with the Siemens RS485 Clk / Data reader license. They can be configured on the *FLN Configuration* dialog of SiPass integrated.

The AR readers should be configured with Siemens OSDP NGCR (76).

5.18.2 HID Proximity, iCLASS (SE), iCLASS Seos and Mifare Classic/DESFire

ProxPro	ProxPro + Keypad	ThinLine II	ProxPoint Plus
✓	✓	✓	✓

*HID iCLASS SE (OSDP) RKL550	*HID iCLASS SE (OSDP) RP10	*HID iCLASS SE R10	*HID iCLASS SE (HADP/OSDP enabled) R(P)15	*HID iCLASS SE (HADP/OSDP enabled) R(P)30
✓	✓	✓	✓	✓

*HID iCLASS SE (HADP/OSDP enabled) R(P)40	*HID iCLASS SE (HADP/OSDP enabled) R(P)K 40	*HID iCLASS SE (HADP/OSDP enabled) RKL550
✓	✓	✓

HID Global iCLASS SE OSDP readers listed can support either OSDP v1 or v2.
OSDP v2 introduces the following features:

- Secure Channel
- Transparent Mode
- Biometric functions

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
R10 / RP10 - Mini Mullion	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Pigtail Cable - 18in. (0.45m)	900NTNNEK00000	RDR, R10, ICLASS, SE REV E, NO PROX, STD, WIEGAND, PIG, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT
R10 / RP10 - Mini Mullion	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	900NTNTEK00000	RDR, R10, ICLASS, SE REV E, NO PROX, STD, WIEGAND, TERM, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT
R10 / RP10 - Mini Mullion	N - No Prox	iCLASS (SE)/Seos/MIFARE DESFire(Sector)	Wiegand Output (default)	Pigtail Cable - 18in. (0.45m)	900NWNNEK00324	RDR, R10, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, PIG, BLK, HF MIGR PFL EVP00000, IPM OFF
R10 / RP10 - Mini Mullion	N - No Prox	iCLASS (SE)/Seos/MIFARE DESFire(Sector)	Wiegand Output (default)	Terminal Strip Connection	900NWNTEK00324	RDR, R10, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, TERM, BLK, HF MIGR PFL EVP00000, IPM OFF
R10 / RP10 - Mini Mullion	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Pigtail Cable - 18in. (0.45m)	900NTPNEK0007V	RDR, R10, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS, 485HDX, PIG, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF
R10 / RP10 - Mini Mullion	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	900NTPTEK0007V	RDR, R10, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS, 485HDX, TERM, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF
R10 / RP10 - Mini Mullion	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Pigtail Cable - 18in. (0.45m)	900PTPNEK00387	RDR, RP10, MULTICLASS, SE E, LF STD, HF STD/SIO/SEOS, 485HDX, PIG, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
R10 / RP10 - Mini Mullion	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	900PTPTEK00387	RDR, RP10, MULTICLASS, SE E, LF STD, HF STD/SIO/SEOS, 485HDX, TERM, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF
R10 / RP10 - Mini Mullion	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Pigtail Cable - 18in. (0.45m)	900PTNNEK00000	RDR, RP10, MULTICLASS, SE REV E, STD PROX, STD, WIEGAND, PIG, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT
R10 / RP10 - Mini Mullion	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	900PTNTEK00000	RDR, RP10, MULTICLASS, SE REV E, STD PROX, STD, WIEGAND, TERM, BLK, STD 1 SE-CURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT
R10 / RP10 - Mini Mullion	P - HID Prox	iCLASS (SE)/Seos/MIFARE DESFire(Sector)	Wiegand Output (default)	Pigtail Cable - 18in. (0.45m)	900PWNNEK00324	RDR, RP10, MULTICLASS, SE, LF STD, HF STD/SIO/SEOS/MIGR, WIEG, PIG, HF MIGR PFL EVP00000, IPM OFF
R10 / RP10 - Mini Mullion	P - HID Prox	iCLASS (SE)/Seos/MIFARE DESFire(Sector)	Wiegand Output (default)	Terminal Strip Connection	900PWNTEK00324	RDR, RP10, MULTICLASS, SE, LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, TERM, HF MIGR PFL EVP00000, IPM OFF
R95A - Décor		iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	95ANTNTEG00000	RDR, R95A DECOR RDR, EURO FLUSH MOUNT, NO PROX, STD, WIEGAND, TERM, GRY, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT
R95A - Décor		iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	95ANTNTEK00000	RDR, R95A DECOR RDR, EURO FLUSH MOUNT, NO PROX, STD, WIEGAND, TERM, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT
R95A - Décor		iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	95ANTNTEW00000	RDR, R95A DECOR RDR, EURO FLUSH MOUNT, NO PROX, STD, WIEGAND, TERM, WHT, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, 32 BIT

SiPass integrated Installation Compatibility

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
R95A - Décor		iCLASS (SE)/Seos/MIFARE DESFire(Sector)	Wiegand Output (default)	Terminal Strip Connection	95ANWNTEK0048B	RDR, RS95A, DECOR RDR, EURO FLUSH MOUNT, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, TERM, BLK, LED RED, FLSH GRN, BZR ON, OPT TAMP, OPEN COLL, CSN MIF SUPPR, IPM OFF MIGR PFL EVP00000
R95A - Décor		iCLASS (SE)/Seos/MIFARE DESFire(Sector)	Wiegand Output (default)	Terminal Strip Connection	95ANWNTEW0048B	RDR, RS95A, DECOR RDR, EURO FLUSH MOUNT, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, TERM,WHITE, LED RED, FLSH GRN, BZR ON, OPT TAMP, OPEN COLL, CSN MIF SUPPR, IPM OFF MIGR PFL EVP00000
R95A - Décor		iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	95ANTPTEG0007V	RDR, R95A DECOR RDR, EURO FLUSH MOUNT, LF OFF, HF STD/SIO/SEOS, 485HDX, TERM, GRY, A/V OFF, OSDP V1, OPT TAMP, OPEN COLL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF
R95A - Décor		iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	95ANTPTEK0007V	RDR, R95A DECOR RDR, EURO FLUSH MOUNT, LF OFF, HF STD/SIO/SEOS, 485HDX, TERM, BLK, A/V OFF, OSDP V1, OPT TAMP, OPEN COLL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF
R95A - Décor		iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	95ANTPTEW0007V	RDR, R95A DECOR RDR, EURO FLUSH MOUNT, LF OFF, HF STD/SIO/SEOS, 485HDX, TERM, WHT, A/V OFF, OSDP V1, OPT TAMP, OPEN COLL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, IPM OFF, UART OFF, WIEG OFF
RK40 / RPK40 - Wall Switch Keypad	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Pigtail Cable - 18in. (0.45m)	921NTNNEK00000	RDR, RK40, ICLASS, SE REV E, KPD, NO PROX, STD, WIEGAND, PIG, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, KPF-4-BIT, 32 BIT
RK40 / RPK40 - Wall Switch Keypad	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	921NTNTEK00000	RDR, RK40, ICLASS, SE REV E, KPD, NO PROX, STD, WIEGAND, TERM, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, KPF-4-BIT, 32 BIT

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
RK40 / RPK40 - Wall Switch Keypad	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Pigtail Cable - 18in. (0.45m)	921NTPNEK0016H	RDR, RK40, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS, 485HDX, PIG, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, KPF, ASCII, BFFRD 1 KEY, IPM OFF, UART OFF, WIEG OFF
RK40 / RPK40 - Wall Switch Keypad	N - No Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	921NTPTEK0016H	RDR, RK40, ICLASS, SE E, LF OFF, HF STD/SIO/SEOS, 485HDX, TERM, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, KPF, ASCII, BFFRD 1 KEY, IPM OFF, UART OFF, WIEG OFF
RK40 / RPK40 - Wall Switch Keypad	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Pigtail Cable - 18in. (0.45m)	921PTPNEK00385	RDR, RPK40, MULTICLASS, SE E, LF STD, HF STD/SIO/SEOS, 485HDX, PIG, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP ENBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, KPF, ASCII, BFFRD 1 KEY, EM4102 32-BIT, IPM OFF, UART OFF, WIEG OFF
RK40 / RPK40 - Wall Switch Keypad	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	OSDP (RS485 Half Duplex)	Terminal Strip Connection	921PTPTEK00385	RDR, RPK40, MULTICLASS, SE E, LF STD, HF STD/SIO/SEOS, 485HDX, TERM, BLK, STD-1, A/V OFF, OSDP V1, OPN COL, OSDP TAMP DISBLD, TEST KEY, POLL=75MS, CSN 32-BIT MSB, EM4102 32-BIT, KPF, ASCII, BFFRD 1 KEY, IPM OFF, UART OFF, WIEG OFF
RK40 / RPK40 - Wall Switch Keypad	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Pigtail Cable - 18in. (0.45m)	921PTNNEK00000	RDR, RPK40, MULTICLASS, SE REV E, KPD, STD PROX, STD, WIEGAND, PIG, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, KPF-4-BIT, 32 BIT
RK40 / RPK40 - Wall Switch Keypad	P - HID Prox	iCLASS (SE)/Seos/MIFARE Classic/DESFire(CSN)	Wiegand Output (default)	Terminal Strip Connection	921PTNTEK00000	RDR, RPK40, MULTICLASS, SE REV E, KPD, STD PROX, STD, WIEGAND, TERM, BLK, STD 1 SECURITY, LED RED, FLASH GRN, BZR ON, IPM OFF, KPF-4-BIT, 32 BIT

5.19 Card Technology Compatibility

The following card technologies are compatible with the Siemens AR range and other OSDP connected readers.

Siemens OSDP[1]	Siemens OSDP Custom[2]	Siemens OSDP Mifare Facility[3]	Siemens OSDP Sector 7 26-bit[4]
✓	✓	✓	✓

Siemens OSDP SiPort[5]	Siemens OSDP GID[6]	Siemens OSDP All HID Prox[7]	Siemens OSDP Raw	Generic OSDP
✓	✓	✓	✓	✓

[1]All data from the reader is the card number. The license is as Siemens reader.

[2]Custom Wiegand profile. License is as Custom Wiegand.

[3]This is a Mifare Facility card, encoded by SiPass. The license is as Mifare Facility.

[4]This is a 26-bit wiegand card, as encoded by SiPass onto a smart card.
The license is as Mifare 26-bit.

[5]The license is as Siemens SiPort

[6]This is a Siemens GID format. The license is as Siemens GID.

[7]This is equivalent to AllHidProx – Wiegand data encoded onto a smart card. The license is as the appropriate Prox. Card technology
(This is useful for iCLASS MultiProx readers).

5.20 Morpho 4G V-Station Reader Compatibility

The following 4G V-Station reader (previously known as L1 reader) versions have been tested and verified as working with SiPass integrated:

4G V-Station Reader 4GSTSG Version 4.1.2.0
✓

NOTE

The fingerprint template layout is defined using the reader setup tool but the enrolment can be performed using SiPass.

The entire reader configuration is done with the reader setup tool, such as time schedules.

SiPass integrated supports card + fingerprint. It is not possible to use fingerprint-only as a credential in SiPass integrated.

Using 4G V-Station readers, multiple fingerprints can be encoded on the Mifare Classic and Mifare DESFire cards. In addition to storing the fingerprint image on the card, SiPass can also store multiple fingerprints in the database that can be retrieved if a card is lost.

5.21 Granta MK3 Reader PIN Pad Type Compatibility

SiPass integrated supports the Pin Pad types 1, 2 and 3. The type can be configured on the *FLN Configuration* dialog.

Please refer Chapter 6 of the 4101-3 Controller *Installation Handbook* for information on Installation and Configuration.

1	2	3
4	5	6
7	8	9
★	0	#

Type 1

0	1	2	3
4	5	6	7
8	9	A	B
C	D	E	F

Type 2

1	2	3	A
4	5	6	B
7	8	9	C
0	F	E	D

Type 3

Note:

- ➔ For the **4422 Swipe module** and the **4322 Cotag module**, the keypad type has to be selected on an extra ***Key*** tab during configuration.
- ➔ The system does not support entry of your own PIN for first-time use.
- ➔ An External Swipe reader, combined with a keypad, can be configured as an **M43** Keypad Type.

5.22 Signature Capture Tablet Compatibility

The following signature tablet range has been tested and verified as working with SiPass integrated:

Topaz HSB (USB) signature capture pads	**T-LBK460-HSB-R**
✓	✓

5.23 Messaging System Compatibility

For venue booking email notifications configured with Exchange Server option, the following are the supported Exchange Server versions:

Microsoft Exchange Server 2007 (SP3) or newer:

NOTE

Email forwarding may not be supported or may not support the sending of emails externally, under certain corporate email conditions or specific corporate implementations.

5.24 Server Redundancy

The following server redundant software has been tested with SiPass integrated:

Stratus Technologies EverRunFT
✓

NOTE

The above software is recommended based on tests done with SiPass integrated. Contact Stratus Technologies directly for any support with the software.

- The redundancy is based completely on the hardware.
- The redundancy is not based on the SiPass services.

5.25 Offline Door System

The following Offline Door System has been tested with SiPass integrated:

SALTO **Version 12.02.06.211**
✓

NOTE

- The SHIP protocol **(version 1.8f)** should be enabled for this feature.
- Refer to the SALTO documentation for the maximum length of text or other potential limitation.
- SiPass supports up to 40 characters for naming entities (like Cardholder First Name and Last Name, Access Level, Access Groups and Time Schedules) and this can be lesser in SALTO. If the entity name in SiPass integrated is longer than the naming character limit in SALTO, the name will be truncated before being sent to SALTO. After truncation, if the name is duplicated in SALTO, it results in an error (logged in SiPass server log file) and the information is not sent.
- The maximum number of time schedules is 65000 in SiPass integrated and 256 in SALTO. These time schedules are the ones having a value of 1-256 in the **Time Schedule No.** field on the Time Schedule dialog. Hence, any time schedule having a number less than 256 can be used for the SALTO system.
- The maximum number of holiday types is 8 in SiPass integrated and 3 in SALTO. Hence, only the holiday types 1-3 in SiPass system can be used for SALTO.
- The maximum number of offline doors that can be assigned to one cardholder is 96 in SALTO. To configure more, the doors must first be added to a zone in the SALTO system (up to 1000 doors per zone and 1000 zones per system).and then the zone can be assigned to the cardholder in SiPass integrated (multiple zones can be assigned to a cardholder).

5.26 Third Party Visitor Management

The following third-party Visitor Management System has been tested with SiPass integrated:

Easy Lobby **Version SVM 10.0**
✓

NOTE

Please refer to the Easy Lobby Integration Setup Guide for more details. This can be found on the integration bundle from HID.

The Easylobby integration requires one SiPass integrated HR API client license.

5.27 Virtualization

Citrix XenApp **Version 6.0**	**Microsoft Windows Server 2008** **Terminal Services**	**Microsoft Windows Server 2012** **Terminal Services**
✓	✓	✓

NOTE

It is highly recommended that suitable hardware and system specifications form the basis of your system.

5.28 For more information…

Contact:

Europe:

fs.support.sbt@siemens.com

South and North America:

support.us.i-bt@siemens.com

Asia:

support.ap.i-bt@siemens.com

6 Known Issues

Issue	Summary
ACC	For ACC5100 (G1) controller, the firmware support and integration into SiPass integrated is now limited. There is a known limitation that any external Compact Flash card (supported from MP2.4 until MP2.65) being added must be the SANDISK brand, no larger than 2 GB in size and formatted as FAT 16.
ACC Time Zone	If the time zone assigned to the ACC is changed, this is not automatically downloaded to the controller. The user must initialize the affected ACC for the change to take place.
Cardholder and Access Management	Readers assigned to a hard Anti Passback (APB) area should not also be assigned to a Timed Re-entry area to prevent any possible errors.
Cardholder and Access Management	When voiding a card or cardholder through a customized actionable report, the change is saved in DB but is not updated in the ACC. **Note:** ACC need to be initialized for the action to take effect.
Database	After upgrading to SiPass MP2.65 SP3 EN on some operating system environments where the regional settings are not set to English, the following issues may be experienced: • The Database restore process fails. • The Database restore is successful but no tabs appear on the cardholder dialog. **Note:** To address the above, a hotfix is available in the *Patches* directory on SiPass integrated Installation Disk.
Installation	In case of Windows 8, the SiPass license details cannot be modified from the Windows Control Panel. For this, the SiPass setup executable file must be run directly.
Integration	MM8000 will not work if there are any non-printing control characters in any component name.

Issue	Summary
Reporting	If you restore the database from a previous version of SiPass integrated to MP2.65 SP3, any customized filter criteria will be lost for the following predefined cardholder search reports: • Cardholders access policies • All Cards • Cardholders Fields • Cardholders Workgroup • Cardholders Concise **Note:** You can keep filter criteria by moving them to new customized reports as below: • Create new customized reports with those filter criteria on existing database. • Backup the database. • Restore database after upgrading to MP2.65 SP3.
SALTO Integration	The SALTO connection status (Online/Offline) is updated only when a synchronization is done. If the SALTO system goes offline between the last synchronization and the next, the status is not automatically updated in SiPass integrated.
SALTO Integration	If time intervals are modified by SALTO, the new access conditions are not applied to SiPass integrated. The access can still be granted at times not part of the new time schedule.
System Setup	E-mail Message Forwarding function is currently not supported when the Secure Socket Layer (SSL) security protocol is enabled in SMTP settings.
Video	If the "Popup Windows on Top" option is selected in System Preferences, all popup windows (such as DVR playback dialog) will be displayed in front of any other windows. If any other dialog is opened, it will stay behind the popup window, not allowing the user to make any changes, as well as disabling the popup window in front. In such a case, pressing the 'Esc' key to close the dialog at the back, or deselecting the 'Popup Windows on Top' option afterwards will resolve the problem. **Note:** *DVR Playback* dialog will always be displayed on top in SiPass integrated.
Web Client	Attachment control is not supported by SiPass integrated web client.

6.1.1 Issues when upgrading from earlier versions of SiPass integrated

Issue	Summary
Cardholder and Access Management	When upgrading to SiPass MP2.65 SP3, existing holidays created in MP 2.65 and MP2.65 SP1 are deleted.*
Cardholder and Access Management	When upgrading from SiPass MP2.65 or MP2.65 SP1 to MP2.65 SP3, the **Holidays** option in the Program menu is disabled.*
Cardholder and Access Management	When upgrading to SiPass MP2.65 SP3, Cardholders created with images (in MP2.65 SP1) are displayed without images in the *Definition* tab on Cardholder dialog. These cardholders are also not listed in the *Cardholders with Images* report. **Note:** An enhanced version of the SiPass Database Checker tool (v1.1.06 onward) addresses this issue.
Daily Operation	When upgrading from SiPass MP2.65 SP2 to MP2.65 SP3, some settings for System Preferences are not retained. The Enrolment Reader configuration must also be done again after the upgrade.*
Installation	When upgrading from SiPass MP2.65 to MP2.65 SP3, the **CCTV** option in Program menu and **CCTV Operation** option in Operation menu are disabled. After the upgrade, follow the steps below to resolve this issue: • Go to Control Panel > Programs and Features • Right-click SiPass integrated and select *Change* from the menu options. • Select *Modify* in the SiPass integrated setup and click *Next* till you reach the dialog listing the SiPass integrated features. • Expand the *Client* option in the tree. • Click **CCTV** and select *This feature will not be available* from the menu options. • Click *Install* and then *Finish*. • Repeat the above steps but this time, for the CCTV feature, select *This feature will be installed on local hard drive*. • Click *Install* and then *Finish*.

Issue	Summary
Installation	When upgrading from SiPass MP2.65 or MP2.65 SP1 to MP2.65 SP3, the *Attachment Control* (**Select** and **Clear** button) in Custom Page is disabled. To resolve this issue: • In SiPass integrated, go to the *SiPass Explorer* menu and click *Advanced Security Programming…* • In the SiPass Explorer window, click *Custom Page Design* from the Navigation tree on left side and go to the respective tab that includes the required attachment control. • Click the attachment control item. • In the *Properties* section on right side of the window, go to *Behavior > IsPrimary* and select **True** from the dropdown list • Save and close the SiPass Explorer.
Installation	Information about SiPass MP2.65SP3 is not displayed correctly in the Database Analysis - General Report.*

*To prevent these issues , it is recommended that you backup the existing SiPass database, uninstall SiPass integrated, install SiPass integrated MP2.65 SP3 and then restore the database.

7 Enhancements and Quality Improvements for SiPass integrated MP2.65 SP3

The sections that follow outline the improvements and fixes made since SiPass integrated MP2.65 SP2 was released.

7.1 Enhancements

The following sections provide a summary of the enhancements to SiPass integrated MP2.65 in Service Pack 3.

Enhancement	Summary
Import/Export Tool	The Data Synchronizer Import/Export tool no longer requires login details in the command line mode. **Note:** In the command-line mode, the login details stored in the Data Synchronizer configuration file are used automatically. Use the *Settings* dialog to set the user-name and password that the command-line operation will use.
Import/Export Tool, HR-API	It is now possible to assign a credential start and end date using the Import/Export tool and the HR API.
Integration	SiPass informs the MM8000 system that a door has been assigned to a door interlocking set.
Reporting	"Card Status" added to the following reports: - Cardholder Access Policies - Cardholders Filtered Point Access - Cardholders Point Detail
Reporting	The reports - Cardholder Access Policies, Cardholder Point Detail and Cardholder Point Concise, now include the 'Cardholder Status' field.
Reporting	The "Cardholder All Fields" report includes general data. **Note:** Now, the "Cardholder Fields" report is known as "Cardholder All Fields" report.
SALTO Integration	SALTO License updated to count only the door numbers, excluding the zones.

7.2 Fixed Issues

This section details known issues fixed in SiPass integrated MP2.65 SP3.

Type	Description
Alarm	Fixed the issue that operator alarm actions would not appear in the audit trail in some cases.
APB	Anti Passback Area failed to show the first and last names of cardholder when there were duplicate card numbers in different credential profiles.
APB	Fixed the Anti Passback area load cardholder error stating the master controller could not be contacted. The error was reported after applying the fix for another issue where a reader point group was part of the access level configuration and the changes were not downloaded to the corresponding ACC.
ASP	ASP Host Authorization trigger fail.
ASP	Server crash when modifying the ASP flags.
Audit Trail	When a cardholder (configured with Access Level, Access Group or Access Points) was deleted, the Audit trail did not show information about the removed points.
Audit Trail	The message "Operator Group Record updated" was not displayed in the Audit Trail after updating operator group property/permission.
Audit Trail	Incorrect Audit Trail message when Time Schedule was changed.
Audit Trail	Incorrect Audit Trail message when operator group was changed from Administrator to HR Officer.
Audit Trail Restore	Restoring .TAB files did not create correspondent .SQLARC Files.
Cardholder and Access Management	If there is Attachment control in cardholder or visitor dialog, any cardholder or visitor without attachment could not be deleted.
Cardholder and Access Management	If the start date was set to be in the future, the end date was not sent correctly to the controller.
Cardholder and Access Management	Exceptions while opening *Cardholder* dialog, searching a cardholder and saving a cardholder.
Cardholder and Access Management	*Cardholder End Date* checkbox not staying checked after saving the cardholder record.
Cardholder and Access Management	The assigned credential end date was always overwritten if an operator modified the cardholder record. This happened if “Default Card & Operator Expire Date” was set in *System Preferences* dialog.

Type	Description
Cardholder and Access Management	Cardholder was disabled by wrong PIN code.
Cardholder and Access Management	Improved performance while initializing cardholder search.
Cardholder and Access Management	Operator can delete cardholder with 'View Only' privilege.
Cardholder and Access Management	SiPass client crash when cardholder was selected by an operator who was not part of the administrator operator group.
Cardholder and Access Management	Access points in the Access Level were not displayed if the operator did not have administrator rights.
Cardholder and Access Management	'Valid To' date of a card did not update accordingly when the 'Valid To' date of the cardholder was modified.
Cardholder and Access Management	The expiry date for a visitor cardholder did not follow the default value set in preferences.
Cardholder and Access Management	Some cardholder images were not displayed in SiPass user interface after upgrading.
Cardholder and Access Management	MP2.65 Visitor Manager did not function the same like MP2.40, where adding a visitor will have the visitor being added to the expected visitor list automatically.
Cardholder and Access Management	Cardholder dialogue crashed or exited unexpectedly while setting up a cardholder and attempting to select a card template.
Cardholder and Access Management	Triggering cardholder search (instead of inserting a new line) after Enter key was pressed in *General Data* field.
Cardholder and Access Management	Operator with 'View Only' privilege could add or delete a cardholder.
Cardholder and Access Management	Some Access Levels were not downloaded to some ACCs.
Cardholder and Access Management	Fixed issues with a card template not being applied to a new cardholder, and the exception generated after giving the print command for that cardholder.
Cardholder and Access Management	Exception during Holiday configuration when right-clicking in empty grid on the calendar tab.
Cardholder and Access Management	Error with SiPass Client when attempting to delete a cardholder while keeping the search result window open.
Cardholder and Access Management	Performance improvement while performing search (involving large number of cardholders) through the Batch Card printing dialog.
Cardholder and Access Management	Fixed the image verification access fail when the Time Out access was turned off.
Cardholder and Access Management	The 'Add Card To APB' button in the Cardholder dialog was not working.

Type	Description
Cardholder and Access Management	A cardholder was granted access to one door but not to the other door under another ACC in the same workgroup.
Cardholder and Access Management	An operator with 'Edit Only' access rights could add a cardholder.
Cardholder and Access Management	Fixed issue with cardholder search when a custom page included date picker with default date values.
Cardholder and Access Management	On a PC with Australian locale settings, the Cardholder dialog displayed US date format.
Cardholder and Access Management	Fixed the issue where the Anti Passback (APB) areas (part of an ACC cluster) were displayed multiple times on the *Add to APB Area* dialog.
Cardholder and Access Management	Fixed the application crash error when selecting a cardholder with mouse right-click.
Cardholder and Access Management	Editing the cardholder address details through website removed the access point.
Cardholder and Access Management	A cardholder could not be updated due to 'End Date Time' of the Card Credential, and of the Cardholder not matching with each other.
Cardholder and Access Management	The Intrusion Areas were not published to ACC when added to the Access Level.
Cardholder and Access Management	When a cardholder was deleted, right-clicking on the cardholder information in audit trail resulted in an error.
Cardholder and Access Management	The Cardholder dialog and Visitor dialog now support keyboard shortcuts.
Cardholder and Access Management	Encoding profile was not cleared after viewing a cardholder and clicking the "New" button.
Cardholder and Access Management	"Out of Memory" exception crashing SiPass clients.
Cardholder and Access Management	The Cardholder “New” button was unavailable for operators having only "Edit" permission for the cardholder fields.
Custom Pages	The Custom Page designer was allowing duplicate field names
Daily Operation	The Audit Trail message for the updated fields was not displayed while modifying operator details.
Daily Operation	Fixed the SiPass Client error while attempting a “DVR action” from the site plan.
Database	Data truncated in General data field of *Cardholder* dialog.
Event Task	Support duration for floor secure\unsecure in Controller Based Event Task (CBET).
Event Task	The Anti Pass Back area count was not updated in the mustering report after running an Event Task to clear the area count.

Type	Description
Firmware	Fixed ARxxS-MF reader Tamper signaling to indicate correct behavior.
FLN Configuration	ACC-Granta backboard configuration not being supported correctly.
HR API	The 'LastUpdatedTime' property of a cardholder was not automatically updated while making an update through HR-API.
HR API	The credential profile ID was not being set correctly for credentials created with HR-API
Import/Export Tool	The GID number and card version number were not being imported via Import Export tool and Data Synchronizer.
Import/Export Tool	Exported file was not found when the export operation was performed directly by giving the file name only.
Installation	The OPC service was not installed even with a valid OPC Server license.
Installation	The OPC server should not rely on OPC clients license.
Installation	When unlocking the workstation, user name and password were not validated.
Integration	MM8000 (having special characters in the database) could not synchronize with SiPass system.
Integration	The MS-API doorset was not displayed for DC12 and DC22 devices.
Integration	APB area details ‘Current Mode’ and ‘APB Area Count’ were not displayed in Management Station API.
Integration	In Management Station API, the Alarm Queue was not updated with the latest alarm state.
Message Forwarding	SiPass server crash while sending pager messages.
Message Forwarding	SiPass failed to send multiple messages at one time.
Message Forwarding	The message forwarding via e-mail did not work if the event name in SiPass included the 'underscore' character.
Message Queue	The message queue did not work on remote client when there was firewall between client and server, which caused the client failing to start.
Operator Privilege	When 'Alarm Queue' and 'Graphics' options were removed from the operator group, the operator could not log out or close the SiPass client.
Printing	Date not printed when printing card for custom page Date/Time control entity.

Type	Description
Reporting	Pre-defined cardholder reports could not be generated after upgrading from SiPass integrated MP 2.60 to MP 2.65.
Reporting	One card badge entry lead to two rows in the mustering report if a cardholder had two credentials with the same card number,
Reporting	Improved performance of cardholder point access report.
Reporting	Fixed the Audit Trail Reporting issue in SiPass Explorer, while restoring TAB files to SQL archive files.
Reporting	Fixed issues with the ‘Database analysis’ reports.
Reporting	Accessing a cardholder record through the localized version of predefined report "Cardholder - Access Policies" resulted in an error, affecting all cardholder and visitor searches afterwards.
Reporting	The ‘Current Date’ option in filter configuration was not appearing for custom (date) fields in new reports.
SALTO Integration	When a SALTO entity was modified while the SALTO system was offline, the modification was not updated in SALTO after getting back online.
SALTO Integration	Cardholder end date was wrongly sent to SALTO, causing the card to expire one day earlier.
SALTO Integration	Fixed the issue while adding/removing a SALTO Door/Zone to the original configuration created in SiPass.
SALTO Integration	If an Access Group with SALTO rights was modified (one access level replaced with another), the complete access rights were removed in SALTO database.
SALTO Integration	Allow keeping cardholder with no access right in SALTO by setting in the AscoServer.exe.config file.
SiPass server	SiPass server crash when special audit trail messages are received.
System Setup	After being added through the FLN configurator, a DRI could not be deleted with the error stating that it was in use in an input point even when it was not configured anywhere.
System Setup	SiPass server crash while running a Host Based Event Task to initialize a specific controller.
System Setup	Fixed the error when the operator not having rights (to a workgroup) attempted to select that workgroup.

Type	Description
System Setup	Operators with 'View Only' rights could modify their own point group and also create a new component group.
System Setup	Operators with 'Unit Group' rights could create and delete a FLN device (instead of having only the View/Edit rights for the device).
System Setup	Operators with 'FLN Group' rights could create and delete a FLN device (instead of having only the View/Edit rights for the device).
System Setup	The Cardholder/Visitor dialogue opened with the imaging tab even when the operator access to the cardholder was restricted.
System Setup	An operator with no 'Access Configuration' rights could configure access privileges from the 'Workgroup' dialog.
System Setup	The non-partition workgroups were not listed in the 'Workgroup' dialog for operators having 'View Only' access rights.
System Setup	Fix for message forwarding fail when configured with the Exchange server.
Time Schedule	Host Based Event Task ignored the defined holiday time schedule.
Venue Booking	A recurring venue booking generated extra booking, exceeding the end date of the recurring booking.
Video	The PTZ port is default to the same port as the communication 12050.
Video	"Livevideo" was not populated in the video viewer with Bosch cameras.
Web Client	The access privileges (like Access Point, Access Level & Access Groups) associated with the selected ‘Workgroup’ for a cardholder were not listed in the ‘Access Control’ section on cardholder dialog.
Web Client	Fixed the incorrect alert message and web page navigation after deleting a visitor.
Web Client	Fixed the issue with SiPass Web Client that allowed adding access objects with End Date less than the Start Date.
Web Client	After attempting to login to the Web Client with invalid credentials for over five times, logging-in with valid credentials resulted in an error (and rejecting the login request).

8 Keyword index

Issued by
Siemens Switzerland Ltd
Building Technologies Division
International Headquarters

Gubelstrasse 22
CH-6301 Zug

www.siemens.com/ buildingtechnologies