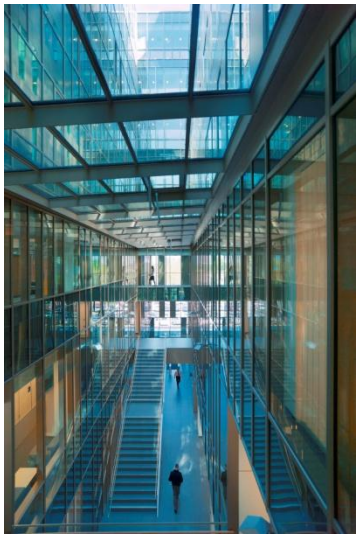
SIEMENS



Access Control

SiPass integrated

Product Release Notes

MP 2.75

A6V11170897
2018-08-03

Building Technologies

CPS Fire Safety

Copyright

Edition: 2018-08-03

Document ID: A6V11170897

Table of Contents

1 Introduction

SiPass® integrated is a powerful and extremely flexible access control system that provides a very high level of security without compromising convenience and ease of access for system users. It is also possible to use SiPass integrated as a security management station (SMS) that integrates access control, intrusion detection and video surveillance into a single system. Some of the noticeable features include:

- Design to fit into a state-of-the-art IT environment
- Modular structure and scalability for keeping pace with changing needs of any organization
- Intuitively designed software that is easy to use and administer
- Support for broad range of readers, various technologies and manufacturers
- Support for offline doors - SALTO

SiPass integrated -- Opening doors to a secure environment.

1.1 What this document covers

This document details the introduction to the new user interface, security features, information on supported technology, compatibility with other devices and the important information that users need to be aware of when ordering, installing and troubleshooting.

1.2 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* that contains all the necessary procedures to install and upgrade the software, and other associated hardware and software components.

To ensure setting up the system with highest level of security, follow the recommendations given in the *SiPass integrated IP Security and Network Guide*.

Both the documents are available in the 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 on a Public Domain

Users please note that installing SiPass integrated on a public domain presents vulnerabilities (e.g., being infected by computer 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 the computer is advisable.

SiPass integrated users are also advised to lockdown USB ports on the computers where SiPass integrated has been installed. Further, it is recommended that client computers 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.

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, report your problem to your local support representative and the issue will be investigated as soon as possible.

3 New Features

3.1 SiPass integrated MP 2.75

3.1.1 New IP-based Door Controller

With SiPass integrated MP 2.75, you get the support for IP-based AP door controller that offers the latest technology, better cost-effectiveness, and easy installation.

It supports:

- 2 OSDP Readers
- 4 Monitored or Unmonitored Inputs
- 2 Relay Outputs
- 4 Open-collector Outputs
- 1 general-purpose FLN bus to connect to IPM, OPM and 8IO devices

See the SiPass integrated MP 2.75 *Configuration Client User Guide* for more information.

3.1.2 SiVMS with SiPass as Front-end

SiVMS has been updated to Version 1.1.1 and supports SiPass integrated 2.75. All other features and functionalities remain unchanged.

3.1.3 RESTful HR-API

The HR-API is now available as RESTful Web Service also.

4 SiPass integrated Installation Compatibility

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

4.1 SiPass integrated Backup / Restore Path

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

	Version You Want To Restore To			
Version Currently Installed		**MP 2.65**	**MP 2.70**	**MP 2.75**
	MP 2.60	Yes	Yes	Yes
	MP 2.65		Yes	Yes
	MP 2.70			Yes

4.2 SiPass integrated Server

Windows Server 2008 R2 (SP2)	Windows Server 2012 R2	Windows Server 2016
Windows 7 (Professional, Enterprise) SP1 (32-bit & 64-bit)	**Windows 8.1** (32-bit & 64-bit)	**Windows 10 (Professional, Enterprise)** (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. For further information, see *Appendix - Windows Settings* in the *SiPass integrated Installation Guide* for this market package of SiPass integrated.

4.3 SiPass integrated Client

Windows Server 2008 R2 (SP2)	Windows Server 2012 R2	Windows Server 2016
Windows 7 (Professional, Enterprise) SP1 (32-bit & 64-bit)	**Windows 8.1 (32-bit & 64-bit)**	**Windows 10 (Professional, Enterprise)** (32-bit & 64-bit)

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.

Only ONE LANGUAGE VERSION must be used for SiPass integrated. Using more than one language is not supported and might result in malfunction.

*Some additional configuration settings are required to ensure that the specified versions of Windows operating systems operate correctly with SiPass integrated. For further information, see Appendix - Windows Settings in the SiPass integrated Installation Guide for this market package of SiPass integrated.

4.4 Microsoft SQL Server

Microsoft SQL Server is the system that meets the numerous and complex database needs of SiPass integrated. Microsoft SQL Server provides the level of software security necessary to safeguard the records created and modified in SiPass integrated.

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

SQL 2017 Express	SQL 2017	SQL 2016 Express	SQL 2016
SQL 2014 SP2 Express	SQL 2014 SP2	SQL 2012 SP2 Express	SQL 2012 SP2

The following information must be noted carefully:

- SQL 2017 and SQL 2016 are compatible with WINDOWS 10 64-bit only. Do not install on a computer having the Windows 10 32-bit Operating System.
- SQL 2017 and SQL 2016 ARE NOT SUPPORTED ON WINDOWS 7 (by Microsoft). Hence, this version SHOULD NOT BE INSTALLED on a computer with Windows 7 Operating System to prevent SiPass integrated from malfunctioning.
- SQL 2008 IS NO LONGER SUPPORTED. During SiPass integrated installation, if you see SQL 2008 as the installed SQL Server instance on the *SQL Options* screen, you MUST UNINSTALL SQL 2008, run the SiPass integrated setup again and select the second option on the screen to install another SQL Express instance.
- If there are no SQL server versions installed on the computer where SiPass integrated is installed, a runtime version of Microsoft SQL Server 2014 SP2 Express will be installed for Operating System versions earlier than Windows 10. In case of Windows 10 and Windows Server 2016 Operating Systems, a runtime version of Microsoft SQL Server 2017 Express will be installed.
- Sites with multiple clients and higher activity (for example, a large number of doors / cardholders / or event transactions, involving more than 5 clients, 100 readers, or 10000 cardholders) are recommended to purchase a higher performance version of SQL optimized for both scalability and performance. See 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.

4.5 .NET Framework

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

.NET Framework Version 4.7.1

4.6 Web Client Compatibility

4.6.1 System Requirements

- Internet Information Services (IIS) 7 & above.

Ensure that SiPass version 2.75 is installed in the system.

- .Net Framework 4.7.1
- **Browsers:** Chrome, Firefox, and IE.

	NOTICE
	Recommended browser versions are: Chrome 59 Firefox 54 IE v11 All the browsers should have the latest patch updated. Tested Operating Systems are **Windows 7 (English), Windows 8.1, Windows 10, Windows Server 2012,** and **Windows Server 2016.**

- neXus SDK 5.3.0.8

neXus SDK needs to be installed to design the card and capture the images.

4.7 System Compatibility

4.7.1 Firmware

AC5100 (ACC-020 / ACC-010)	AC5102 (ACC-G2)	ACC-AP	AC5200 (ACC lite)	Granta Mk3 (ACC-Granta)	Granta Mk3 Backboard
Version 2.70.48	Version 2.75.14 Platform Version CCP v2.17.3	Version 2.75.14 Platform Version 1.1.0	Version 2.70.48	Version 2.70.48	Version 1.29

ADD51x0 (DRI)	ADD51x0 (DRI-OSDP Crypto)	ADS52x0* (SRI)	AFI5100 (IPM)	AFO5100 (OPM)
Version 3.58	Version 5.30	Version 3.25	Version 2.36	Version 1.16

ADE5300 (ERI)	AFO5200 (8IO)	ATI5100 (IAT-010)
Version 3.54	Version 1.06	Version 1.10

DC12	DC22	DC800	IOR6
MkI Version 1.36 MKII Version 1.43	MkI Version 1.36 MKII Version 1.43	Version 1.23	Version 1.00

For upgrading to MP2.70 (or later), the ACC-G2 must be running ACC V2.65.44 (MP2.65 SP3) or later. If it is running an earlier version than this, then install ACC V2.65.44.

(The file *acc-g2_2.65.44_release.bin* is available in *System_Update_Step0* folder in the SiPass integrated software installation bundle.

After upgrading the ACCs to MP2.70 SP1, **all the FLN devices MUST be upgraded** to the latest firmware provided with the MP2.70 SP1 (or later) software bundle.

4.7.2 Hardware

4.7.2.1 Controllers

AC5102	ACC-AP	AC5100	AC5100
ACC-G2		ACC Revision 3 ACC-020	ACC Revision 2 ACC-010

AC5200	AC5200	AC5200	Granta Mk3
SR34i Revision 1	SR35i Revision 1.4	SR35i MkII Revision 2	Revision 1

4.7.2.2 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

4.7.2.3 I/O

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

4.8 API / HLI Compatibility

The sections that follow provide information on the backwards compatibility of the current interfaces available in this release of SiPass integrated.

4.8.1 HR-API Interface

SiPass integrated HR-API allows data to be accessed and maintained from any programming language that supports COM automation. In addition, the RESTful HR-API Web Service is also available.

SiPass integrated contains enhancements to server security which means modification is required for any existing applications that have been built around versions prior to MP 2.70. The enhanced security in SiPass integrated MP 2.70 onward requires establishing an authenticated connection to be set up with the HR-API application by performing few additional steps.

For more information , see the documentation in *SiPass integrated API and RESTful API* folder in the SiPass integrated software bundle.

4.8.2 Management / Enterprise Station API

SiPass integrated MS-API allows data to be accessed and maintained from any programming language that supports COM automation. In addition, the RESTful Management Station API Web Service is also available.

SiPass integrated contains MS-API changes which do not require modification to any existing applications that have been built around versions previous to 2.70 MS-API.

For more information , see the documentation in *SiPass integrated API and RESTful API* folder in the SiPass integrated software bundle.

4.8.3 OPC A&E Server Interface

SiPass integrated supports OPC A&E version 1.0

4.9 Digital Video Recorder (DVR) System

4.9.1 DVR Integration

VECTIS HX	2.1.5
VECTIX iX	2.10.0.236 (SDK 2.5.4.06)

4.9.1.1 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	16 MBit/s	30 fps

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

4.9.2 Third-Party DVR Integration

(Requires DVR-API Connection License)

Bosch Divar 700 Series	Bosch Divar XF	Bosch DivarMR

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

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, contact DVTel or Bosch.

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

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

4.10 Directly Connected IP Camera Compatibility

AXISP1354	AXIS M3007	AXIS P5534	AXIS P7214**
Fix Camera	Fix Dom	PTZ – Dom, Live View	Video Encoder

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, and 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.

4.11 Intrusion Panel Compatibility

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

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

4.12 Network Communication

Encryption of ACC and SiPass communication	AES 128 Bit
SSL Encoding protocol for SiPass client/server communication	TLS 1.2

4.13 Modem Compatibility

ETM9440-1 HSPA+/UMTS/GSM/GPRS Terminal (3G GSM modem)

While some 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.

4.14 Card Printer Compatibility

Fargo Pro - Series	**Fargo High Definition (HDP600, HDP800, HDP 5000)**

Fargo Direct-to-Card (DTC500 Series)	**Fargo Persona (C25)**	**Zebra ZXP Series-1**

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 2.70. 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.

Ensure that the firmware of your Card Printer is upgraded to be compatible with the Operating System on your computer.

4.15 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	**FargoHDP5000 with built-in OMNIKEY 5121****

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

4.16 Enrolment Reader Compatibility

4.16.1 USB Enrolment readers

Omnikey 5321	Omnikey 5421	Omnikey 5422

4.17 Card Format Compatibility

4.17.1 Reader Connection Types

Wiegand	RS-485	Clock & Data

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

4.17.2 Siemens Proprietary Card Formats

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

4.17.3 Proximity Formats

26-bit (industry standard)	36-bit ASCO	27-bit Indala	27-bit Cotag	HID Proximity SIEMENS Encrypted 52 Bit

HID Corporate 1000/2000	Custom Wiegand	34-bit Europlex	37-bit REMEC

4.17.4 Smart Card Formats

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

*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).

4.18 Card Reader Compatibility

4.18.1 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).

Not all of the compatible readers listed above support the reader offline indication. Different reader manufacturers follow their own practices to include such features.

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

ProxPro Wiegand (Keypad) (5355)	MiniProx Wiegand (5365)	MaxiProx (5375)	ThinLine II Wiegand (5395)	ProxPro II Wiegand (5455)	ProxPoint Plus (6005)

iCLASS LCD/Keypad	iCLASS SE and multiCLASS SE Mini Mullion	iCLASS SE and multiCLASS SE Mullion	iCLASS SE and multiCLASS SE Wall Switch
RKL55 – 6170B*	R10 – 900N* RP10 – 900P* Options include Wiegand or OSDP v1/v2, Mobile Ready or Mobile Enabled.	R15 – 910N* RP15 – 910P* Options include Wiegand or OSDP v1/v2, Mobile Ready or Mobile Enabled.	R40 – 920N* RP40 – 920P* Options include Wiegand or OSDP v1/v2, Mobile Ready or Mobile Enabled.

iCLASS SE and multiCLASS SE Wall Switch Keypad	iCLASS SE and multiCLASS SE Décor	iCLASS SE 13.56MHz Long Range	iCLASS SE UHF Long Range
R4K0 – 921N* RPK40 – 921P* Options include Wiegand or OSDP v1/v2, Mobile Ready or Mobile Enabled.	R95 – 95A* RP95 - 95AP* Options include Wiegand or OSDP v1/v2.	R90 – 940N*	U90 – RDRSEU90*

iCLASS, iCLASS SR, Seos (Part No. 928NFNTEK000TE)
RDR/ENROLLER, RKLB40, ICLASS, SE E, HF STD BIO/SEOS BIO, LCD/BIO, WIEG, TERM, BLK, STD-1, LED RED, FLSH GRN, BZR ON, LCD 1F, KPF, BFFRD 1 KEY, NO PAR, 4-BIT MSG, IPM OFF • Wiegand/Clock & Data output • iCLASS, iCLASS SR, Seos biometric templates only • bioCLASS Rev B iCLASS legacy template support **Not Supported** • bioCLASS Rev A iCLASS legacy template • ISO14443A UID

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

Note: For more information, check product documentation on www.hidglobal.com

4.18.3 HID Readers for Siemens Sites

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
R10 Series	N	Y	Wiegand	Pig tail	900NWNNEKE00K9	LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE0527
R10 Series	N	Y	OSDP/RS-485	Pig tail	900NWPNEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R15 Series	N	Y	OSDP/RS-485	Pig tail	910NWPNEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R 40 Series	N	Y	Wiegand	Pig tail	920NWNNEKE00K9	LF OFF, HF SEOS/MIGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE0527
R 40 Series	N	Y	OSDP/RS-485	Pig tail	920NWPNEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527

R95A Series	N	Y	OSDP/RS-485	Term	95ANWPTEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, TERM, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95ANWPTEWE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, TERM, WHITE, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95ANWPTEGE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, TERM, GREY, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527

Note: For more information, check product documentation on www.hidglobal.com

4.19 Card Technology Compatibility

ARxxs-MF OSDP[1]	ARxxs-MF OSDP All HID Prox[2]	ARxxs-MF OSDP ASCII	ARxxs-MF OSDP BCD Packed	ARxxs-MF OSDP BCD Unpacked	ARxxs-MF OSDP Custom[3]

ARxxs-MF OSDP Mifare Facility[4]	ARxxs-MF OSDP Mifare GID[5]	ARxxs-MF OSDP Mifare Numeric	ARxxs-MF OSDP Raw	ARxxs-MF OSDP Sector 7 26-bit[6]

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

[2]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).

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

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

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

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

4.20 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:

Design	Product Number	Model	Description
MA SIGMA Indoor / Outdoor	293638835	WR Sigma Bio	• Multi-factor Bio/PIN (3K users, 10K, 50K and 100K with license) • 1M logs storage capacity • Poe included
	293638898	WR Sigma Prox	• Multi-factor Bio/Card/PIN/BioPIN (3K users, 10K, 50K and 100K with license) • HID Prox • 1M logs storage capacity • Poe included
	293638856	WR Sigma iClass	• Multi-factor Bio/Card/PIN/BioPIN (3K users, 10K, 50K and 100K with license) • HID iClass • 1M logs storage capacity • Poe included
	293638877	WR Sigma Multi	• Multi-factor Bio/Card/PIN/BioPIN (3K users, 10K, 50K and 100K with license) • MIFARE®/DESFire® Smartcard Reader • 1M logs storage capacity • Poe included
MA SIGMA LITE	293678615	MA SIGMA Lite	• Mono-factor Bio (500 users, 3K and 10K users with license) • IP65 and IK 08 • Certifications: CE, CB, FCC
	293678628	MA SIGMA Lite iClass	• Multi-factor Bio/Card (500 users, 3K and 10K users with license) • HID i-class® Smartcard Reader • IP65 and IK 08 • Certifications: CE, CB, FCC
	293673665	MA SIGMA Lite Prox	• Multi-factor Bio/Card (500 users, 3K and 10K users with license) • HID Prox® Smartcard Reader • IP65 and IK 08 • Certifications: CE, CB, FCC
	293678636	MA SIGMA Lite Multi	• Multi-factor Bio/Card (500 users, 3K and 10K users with license) • MIFARE®/MIFARE® Plus/DESFire® Smartcard Reader • IP65 and IK 08 • Certifications: CE, CB, FCC

Design	Product Number	Model	Description
MA SIGMA LITE +	293678657	MA SIGMA Lite +	• Multi-factor Bio/PIN (500 users, 3K and 10K users with license) • 2.8” colour touchscreen • IP65 and IK 08 • Certifications: CE, CB, FCC
	293673644	MA SIGMA Lite + iClass	• Multi-factor Bio/Card/Pin (500 users, 3K and 10K users with license) • 2.8” colour touchscreen • HID i-class® Smartcard Reader • IP65 and IK 08 • Certifications: CE, CB, FCC
	293678678	MA SIGMA Lite + Prox	• Multi-factor Bio/Card/Pin (500 users, 3K and 10K users with license) • 2.8” colour touchscreen • HID Prox® Smartcard Reader • IP65 and IK 08 • Certifications: CE, CB, FCC
	293678660	MA SIGMA Lite + Multi	• Multi-factor Bio/Card/Pin (500 users, 3K and 10K users with license) • 2.8” colour touchscreen • MIFARE®/MIFARE® Plus/DESFire® Smartcard Reader • IP65 and IK 08 • Certifications: CE, CB, FCC

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.

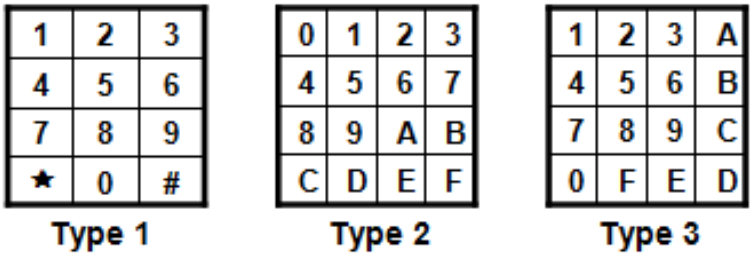
SiPass integrated supports card + fingerprint. It is not possible to use fingerprint-only as a credential in SiPass integrated.

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.

4.21 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.

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



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.

4.22 Signature Capture Tablet Compatibility

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

4.23 Messaging System Compatibility

Microsoft Exchange Server 2007 (SP3) or newer

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

4.24 Server Redundancy

Stratus Technologies EverRunFT

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.

4.25 Offline Door System

SALTO SPACE Version 5.0.7.2*

* SALTO SPACE v5.0.7.2 is recommended for optimum performance. The older SALTO v12.02.09.214 is no longer supported.

The SHIP protocol (version 1.23a) 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).

4.26 Third-Party Visitor Management

Easy LobbyVersion SVM 10.0

See 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.

4.27 Virtualization

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

It is highly recommended that your system is based on suitable hardware and system specifications.

5 Enhancements and Quality Improvements

The sections that follow outline the improvements and fixes made from the previous release of SiPass integrated and the current one.

5.1 SiPass integrated Web Client

5.1.1 Fixed Issues

- In a series of recurrence booking, when user changes the start date greater than the end date and tries to saves the record, a validation will be thrown. In this case, if user navigates to the home page and reverts back to the **Venue Booking** application, the record that the user has edited will not be available and will be deleted.
- In the **List** view, by default, the first record is chosen and its corresponding details are displayed in the detailed view. In this case, the user docks the detailed page and navigates to the Home page (to perform any function). After performing the function in the homepage, when user returns to the previous screen to resume with the activity, the user can see the docked screen, however, when user tries to view the list view, the list view displays only three records irrespective of the actual number of records.
- After changing the configuration settings, the total items count does not display on the bottom of the Cardholder list.
- When user adds an item, the first item of the List View is selected and the details of the newly added item is displayed in the **Detail View**.

6 Known Issues and Limitations

6.1 SiPass integrated Server, Configuration Client and Operation Client

- A Controller Based Event Task should not be configured using *Profile* as trigger, if the profiles are configured with same technology and facility. In this case, the *ASP Workgroup* must be used as trigger.
- SiPass integrated Configuration Client stops functioning when creating a Site Plan with a folder name exceeding 48 characters. If this happens, re-name the site plan folder to a name having less than 48 characters.
- SiPass integrated Configuration Client supports a maximum of 16 characters for password however, it allows the user to enter any number of characters while setting the password. This results in error when later, the user attempts to login using the password containing more than 16 characters.
- When two Point Groups (having readers in common) are assigned to a Cardholder, and one Point Group is removed from the Cardholder's Access Rights, the Cardholder does not have access to the common readers anymore (even when the Point Group for which he has the Access Rights, contains the reader). To resolve this issue, the ACC must be re-initialized.
- The functionality "Adding a report to Cardholder Search" is not available in the current release.
- The ACC-AP controller does not support System Update through firmware download. Only SD card update can be done at present.
- The ACC System Update may not function when downloading into several controllers simultaneously. In case of an issue, the system update must be downloaded one by one to each ACC.
- SiPass integrated does not support the *Repair* option.

6.2 SiPass integrated Web Client

6.2.1 Known General Issues

Common for All Applications

- An extra horizontal scrollbar appears in the dialog box when not required.
- In the dialog box, on selecting the access objects checkbox, the list refreshes. This results in displaying incorrect record counts.
- In the **List** view,
  - user selects a record in the first page and another record in a different page, and deletes these two records. After the deletion process, the record count (that displays below the list view) still remains the same as it was shown prior deletion and does not display the count after deletion. In addition, the detailed page of the selected record also displays.
  - at times, when no record is selected in the list view, the detailed view page still displays the detailed view of the previously selected record. This occurs when a record is selected/cleared continuously.
  - when user selects a record at a fast pace, additionally one more record is shown as selected. E.g. If user selects one record, two records are shown as selected. If user selects three records, four records are shown as selected.
- While working with the application, randomly, an error displays as Unable to connect to the SiPass server, in this case user needs to click **OK** to continue working. However, sometimes even after clicking **OK**, an error displays as **TypeError: Cannot read property 'Message' of null,** in this case user needs to again click **OK** and goto Home page and then navigate to the same page to continue working.
- When SiPass and Web UI API services are not available, the Error **"Unable to connect to the SiPass server"** displays twice.
- During mouse hover event, for some elements,
  - the tool tip does not display.
  - the tool tip gets truncated (at times).
- In the **Combo** box, the default value Please select a value does not display randomly.
- In the **Extended** View, the columns will be misaligned.
- In the **Detailed** View,
  - the tabs cannot be rendered based on the Operator rights, only the fields inside the tabs can be rendered**.**
  - the tab page navigation does not work at times.
- The Tool tip displays behind the list box. This issue is applicable only for Firefox browser.
- The web client takes more time to load the data in the List View for large screen monitors with higher screen resolutions.
- The fast toggle between applications during page load operation is producing inconsistent results.
  - E.g. When user tries to view the **Cardholder** application, and before the page loads, if user navigates to **Venue Booking** application, the page still loads and displays only the previously viewed application (Cardholder).
- At times, the tool tip displays everywhere while moving the cursor.

- **TypeError:** Cannot read property ‘destroy’ of undefined popup appears randomly.
- **TypeError:** Cannot read property ‘id’ of undefined popup appears randomly.
- Internal Server Error, Unknown Error and Cannot read property 'toString' of undefined” issue occurs randomly across all applications.
- The SiPass webclient session does not expire when the SiPassIntegratedWebUIAPI service is stopped or killed. To resolve this issue, SiPassServer service has to be restarted.
  - **Impact:** SiPass License count does not decrease even after the SiPassIntegratedWebUIAPI service is stopped or killed.
- Pinning feature has some limitations in **Venue Booking** and **Venue Configuration**.
  - For Example: Pin an item to the home screen. From the home screen, when user clicks the pinned item, the pinned item will not be selected in the list view (if the selected item is not from the first page), however, the pinned item will be displayed in the detailed view. Because of this behaviour, the Edit and Delete buttons are disabled. In this case, the user needs to scroll up/down to see the selected/highlighted item in the list view. After the item is selected automatically, the edit and delete buttons will be enabled.
- Empty Date Time validation does not work across all the applications.
  - For Example: In the **Cardholder** application, navigate to the Siemens Corporate Card. Enter/choose the required fields and save the cardholder. While saving the cardholder, even if the date field is left blank without choosing the date, the Empty Date Time validation is not thrown.
- During Add/Edit/Delete operations, when user clicks Home icon, the ADD, EDIT, and DELETE buttons get invisible. Only after the user clicks Save or Don’t Save button, the above mentioned buttons become visible. This issue is applicable for the applications that have CRUD operations.
- In grid view, even though user selects multiple records, only the last selected record is displayed.
- The **Close** button is not translated in the configuration screen, as the word Close is hardcoded by SiShell framework.
- In **Switch View**, the controls in the Table/List configuration are not completely visible in smaller screen, for e.g. laptop view.
- For printing a card, it is mandatory to have the printer configured within the neXus application. If no printer is configured, while printing, the neXus service stops and displays an error message as **neXus Card SDK: IDProductionProcessor has stopped working**. In this case, the user needs to configure a printer to the neXus application and manually start the neXus service.
- While accessing the application in the localized languages, at times, the length of the contents in the controls are overlapped over other controls and does not allow the user to perform a particular operation.
- Randomly, on hovering on an image, tooltip displays which is not required.
- In full screen view, the message, **Press[ESC] to exit Full screen** displays in **English** language, irrespective of any logged in language.

6.2.2 Known Issues for Live Alarm

- In the Configuration dialog box, the AlarmDateTime field works only based on the Contains logic.
- When the application is logged in through other languages except English, the field AlarmStatus cannot be searched through the quick search and extended search option.
- Alarm Date Time field will display in the following format: **MM/dd/yyyy HH:mm:ss**
- Date field will display in the following format: **MM/dd/yyyy**
- Time field will display in the following format: **h:mm:ss a**

6.2.3 Known Issues for Cardholder/Visitor Application

Cardholder / Visitor Application

- In the **List View**, the card number displays only when it is configured for the Base profile.
- While scrolling down the Cardholder list, randomly, the records display for half a page.
- **Image Capture** and **Signature Capture** does not work **in IE** browser**.**
- Error messages thrown from neXus application are displayed only in English language, irrespective of which language is chosen while logging in the SiPass web application.
- When the workgroup field is set as compulsory, The compulsory field should not be empty message displays, even when the workgroup is selected from the drop-down list. This is a SiPass Operation client issue.
- While logging on to the application through the following languages: **Dutch, Italian, Russian, Chinese Simplified, Chinese Traditional**, **Polish,** and **Czech** in the **Cardholder/Visitor** application, the start and end date formats are displayed different in the list and the extended view.
- When the application is logged in through other languages except English, the field Status cannot be searched through the quick search or extended search option.
- When edit rights is provided only to the last name field, user cannot edit and save the cardholder.
- Cardholder details cannot be viewed, if the imaging and printing and imaging tab rights are not provided.
- While docking/undocking, the controls are getting overlapped in the **Cardholder** and **Visitor** applications.

6.2.4 Known Issues for Page Customization

Page Customization

- Even if the fields **WorkGroup** and **Profile** are set as mandatory in the **Custom page design** and **Advanced** tab, system allows to save the **Cardholder / Visitor** application without prompting a validation message.
- Email field is a predefined custom field in the visitor application of the Configuration client. Even if the email field is deleted, the application does not prompt any validation message. The web client still retains the email field.

- During database restore, in the **Visitor** application, the Email field gets duplicated in the **Extended Controls** tab and **Visitor Details** tab.
- During database restore, the remaining fields **Reason for Visit, Profile, and License of the Visitor Details** tab gets displayed in the **Extended Controls** tab.
- Predefined fields cannot be customized for the cardholders that are already configured, however, for the newly added cardholders, predefined fields can be customized.
- **Date Time format** selected in custom page of operational client does not display in the same format in web client.

6.2.5 Known Issues in Credential Design

- If user deletes a non-existing record, the record gets removed. However, it does not intimate the user, that the record is already deleted. This issue is by design in the SiPass integrated and arise during concurrent usage of the application.

6.2.6 Known Issues for Venue Booking

- When user tries to edit the time of a record, a confirm message displays as **Do you want to save changes to "Venue Booking name"?**. On clicking **Don't Save**, the edited time is shown, rather than showing the original time.
- When user tries to edit a recurrence booking record e.g. Record A, by clicking the **Show Calendar** button, but edits an occurrence booking record e.g. Record B, a message displays as **TypeError: Cannot read property 'toString' of undefined randomly**.
- User creates a booking, by selecting the **End of Recurrence** option as End by (MM/DD/YYYY) from the **Recurrence Range** section. After the booking is created, if user creates another record, by default, the End after (no. of occurrences) field should be selected. However, **End by** is shown as selected.
- User creates a booking, by selecting the **Repeats** option as Every Weekday from the Recurrence Pattern section. After the booking is created, if user creates another record, by default, the Every (no. of days) field should be selected. However, **Every Weekday** is shown as selected.
- While creating a venue booking with recurrence option, at times, the list view does not get refreshed automatically.
- Irrespective of the languages chosen while logging in the client, if user changes the default Time Zone, the date time search does not work for **Venue Booking**.
- In **Reccurrence Booking**, the End by calendar control goes beyond the selection and does not allow the user to select the date. This issue occurs in smaller screen, for e.g. laptop view.

The following issues are by design in the SiPass integrated and arise during concurrent usage of the application:

- If user accesses or deletes a non-existing item, an exception error displays as **"Access Denied".**
- If user edits and saves an already deleted record of a recurrence booking, the list view does not get refreshed, and an exception error displays as **"Access Denied".**
- If user edits and saves an already deleted record of an occurrence booking, the list view will be refreshed and displays two error messages such as Unknown Venue Booking and Access Denied.

6.2.7 Known Issues for Venue Configuration

The following issues are by design in the SiPass integrated and arise during concurrent usage of the application:

- In Venue,
  - if user accesses a non-existing record, an exception error displays as **"Access Denied".**
  - if user deletes a non-existing record, an error message displays as **"Server is busy, cannot process the request".**
  - if user edits and saves an already deleted record of a venue, the list view does not get refreshed, and an exception error displays as **"Access Denied".**
- In Venue View, if user deletes a non-existing record, the record gets removed. However, it does not intimate the user, that the record is already deleted.

6.2.8 Limitations

- In **Quick** and **Advanced Search**, the date and time field works based on the **"equal to"** logic.
- All tab pages do not load properly. User needs to click the visible tab page to load the remaining tab pages.
- While searching for an entry in the application and when the search string does not match with the entered text, either **No data available in table** or **No matching records found** error message displays in the list view pane.
- Random pin generation for **Cardholder/Visitor** is not available in the SiPass webclient. User needs to manually enter the pin.
- In the Extended Search view, when user types the search criteria or switch in-between the text boxes, the list view gets refreshed.
- The **Repair** option is not supported in the package: SiPass Integrated Web UPI API and SiPass Integrated Web UI.
- The Image resolution of the Cardholder must be 160 x 160 pixels. If the resolution is not 160 x 160 pixels, the image will be pixilated or blurred.
- The Search option in the Cardholder and Visitor field support only **and** logic. For example, when a user enters First Name **and** Last Name of the cardholder in the Search field, the webclient displays the corresponding cardholder.
- Password field does not maintain user's privacy. As the user enters, it displays the actual characters.
- The date and time in the SiPass integrated web client works based on the language logged in by the user. And does not depend on the regional settings available in the system.
- The naming convention followed n the SiPass integrated web client is different from the SiPass Operational client.
- The date and time format in the Visitor application is not displayed entirely.
- The controls available in the SiPass integrated web client application appears different when viewed through the Internet explorer when compared to Google Chrome.
- On clicking the **Select All** option, the total count of records of all the pages display, rather than displaying the total count of records page wise.

- In the Configuration client, when the **Priority** of an Alarm is modified; the changes made is not updated dynamically in the **List view** [Web client]. To view the changes in the list view, the user must go back to the home page and then return to the list view screen.
- In the **Venue Booking** applications:
  - validation message does not display for the expired pinned booking and deleted pinned booking.
  - only the Bookings from **30 days** prior to the current date and time displays.
  - while clicking the **Day, Week,** or **Month** buttons, user can view the booking created for a particular Day, Week, or Month. However, while clicking the **Show Calendar** icon, to navigate to some other dates, user cannot navigate to the selected date.
  - when more number of venue bookings are configured, the venues are displayed beyond the calendar frame.
  - when user tries to edit a record e.g. **Record A**, by clicking the **Show Calendar** button, but edits some other record e.g. **Record B,** the **Start Date and Time** and **End Date and Time** does not change for the currently chosen Record B. The record will be modified only when user edits the same chosen record.
  - while creating/editing a venue booking with recurrence option, the first item of the list view will be selected, whereas in single booking (occurrence) option, the saved record will be selected**.**
- In the **Extended Controls** tab,
  - the dropdown fields does not have any validation limit. But during an entry, only the first 256 characters are saved and rest of the entries are not saved.
  - when the data type of custom field textbox control is configured as **Numeric** in the SiPass Configuration client and if user tries to enter alphabets in the text box field, an error message as **Internal server error** displays. This error message is also applicable for **Cardholder** and **Visitor** applications.
- In the **Printing** tab,
  - The Date and Time format is different from the SiPass server.
  - **SiPass format: 10/22/2015 12:00 am**
  - Cardholder Printing format: Mon Oct 22 2015 12:00:00 GMT+5.30 or 2015-10-22T12:00:00.000000
- **neXus application**:
  - The card is designed with the barcode control. However, the barcode will not be visible in the design preview.
  - When the card is designed with two or more controls, there will be a delay while previewing it for printing.
  - When user designs a template and tries to save it without providing any name, neXus saves the template. However, when user tries to access the same template, a blank Card designer page is displayed.
  - When user tries to save a new template with an already used template name, neXus saves it without throwing any errors (name exists). However, on accessing the same template, only the latest created template is available and the old template is unavailable.
  - When user tries to add a database field to a template, a wrong field (from the database drop-down field) is getting mapped in the template. (This occurs randomly)

7 Support Information

Europe
Phone: +49 89 9221 8000
Fax: +49 89 9221 6000
email:
support.eu.i-bt@siemens.com
fs.support.sbt@siemens.com
Hours of operation:

Monday - Thursday:	08:00 A.M. - 05:00 P.M. CET
Friday:	08:00 A.M. - 03:00 P.M. CET

South and North America
Phone: +1 800 877 7545
https://support.industry.siemens.com/my/WW/en/requests#createRequest
Hours of operation: Monday - Friday: 08:00 A.M. - 06:00 P.M. Cantral Time

Issued by
Siemens Switzerland Ltd
Building Technologies Division
International Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies