SIEMENS

Access Control

SiPass integrated

Release Notes

MP 2.70 SP1

Building Technologies

Copyright

Technical specifications and availability subject to change without notice.

Edition: 02.03.2018

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's new in SiPass integrated MP 2.70

SiPass integrated MP2.70 is the latest market package that packs-in tighter security and convenient features such as:

- Separate clients for configuring and operating the software
- New web-based operational User Interface
- Enhanced high-level interface to thyssenkrupp destination control system
- IT Security Enhancements
- Windows 10 Support

1.2 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.

1.3 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* 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 2.70 Service Pack 1

3.1.1 Client/Server Monitoring

The *Client/Server Monitoring* feature of SiPass integrated lists information of the server and active clients on SiPass Configuration Client. It can be accessed by clicking **Operation > Client/Server Monitoring...** in the Configuration Client.

The *Client/Server monitoring* dialog gives you important information such as Client computer name, Windows login details, Certificate in use and Certificate Expiry date.

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

3.1.2 Certificate Monitoring and Renewal

SiPass integrated now supports monitoring of existing certificates in use and informs in advance when the certificate is about to expire. You can use the *Authentication Management* tool of SiPass integrated to renew the certificate in time and keep working securely.

> The SiPass integrated Server / Client starts giving you **warning messages 30 days prior to the certificate's expiry date**. If you do not renew the certificate after getting the message, you will still be able to log on to the system. If the certificate is not renewed in time and gets expired, you will not be able to log on.

See the *SiPass integrated Configuration Client User Guide* for more information on renewing a certificate.

3.1.3 Enhanced DESFire Profile Encoding

The Mifare DESFire Profile Configuration is now done through the new dialog - *DESFire Profile Configuration*. The *Smartcard Profile Configuration* menu item in the System menu of SiPass integrated Configuration client now lists the two options: **Mifare Classic** and **Mifare DESFire**.

- Access type *Card Number* has been added
- A custom Card Number format can be configured with a padding character and desired byte order - MSB (default) or LSB
- A Custom Data Block can be assigned to a file of an application that contains the Data Type, Access Control Type, Database Field, Start Position, Length and Output Type. The same data block can be assigned to different files.
- Up to 13 keys are supported per application, and additionally, one key for each application as the Master Key
- From one application, you can now assign a key to a file as READ, a key to a file as WRITE, a key to a file as READ/WRITE, and a key to a file as CHANGE

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

3.1.4 Ability to add Favorite Menu Items in Operation Client

The SiPass integrated Operation Client now allows the operator to save a preferred layout and add the most frequently accessed menu items as favorites in one place. The **My Favorites** folder in the navigation pane on the left is used to set the favorites.

See the *SiPass integrated Operation client User Guide* for more information.

3.1.5 Status Bar to Display Important Information

The Status Bar at the bottom of the SiPass integrated Operation client screen gives quick information for monitoring the important aspects like alarm count, alarm queue, number of configured and online ACCs, Date / Time, Client Lock status and SiPass Server Online / Offline status.

See the *SiPass integrated Operation Client User Guide* for more information.

3.1.6 Enhanced Reporting

- Two new report types are now available in SiPass integrated Operation Client:
  - **Destination Control Elevator Readers:** Lists information like used Readers, ACC Unit, Elevator Component, Component Type, Elevator, Floor, Bank and Elevator Controller.
  - **Elevator Controller Details:** Lists information like Name of Elevator Controller, Elevator Type, URL, Alarm Class, Certificate Thumbprint, Poll Period, Maximum Response Time and ACC used for reporting Communications.
- Most of the Cardholder reports now include information about the elevator-specific information of Caretaker, Technician, Language and Lighting Effects.

3.1.7 Enhanced FLN Communication

The standard communication of the FLN Bus is now enhanced with added security measures, making the SiPass integrated Firmware more robust and secure. You can add a device with Legacy Firmware to an existing FLN bus that contains devices with the new secure communication however, the following scenarios apply:

- If you upgrade the firmware of this device to latest version, it will start using the new standard communication.
- If you do not upgrade the firmware of this device, all other devices will use Legacy communication till the time this older device is also upgraded.

See the *SiPass integrated Firmware Configuration Guide* for more information.

3.1.8 New OSDP Reader Type

SiPass integrated now gives you the option to set OSDP Readers that are not ARxxS-MF or HID (iClass) readers. You can now set any other reader by selecting **Other / General OSDP Reader** from the **Reader Type** drop down list.

3.1.9 New OSDP Date/Time Display

RIM device firmware now supports three types of Date/Time display:

- YYYY/MM/DD HH:MM (Default)
- DD/MM/YYYY HH:MM
- DoW DD mmm HH:MM

The other two (non-default) formats above can be set through the ACC Console Command. See the *SiPass integrated Firmware Configuration Guide* for more information.

3.1.10 Support for Windows Server 2016

Windows Server 2016 is now supported by SiPass integrated.

3.2 SiPass integrated MP 2.70

With the introduction of several new and innovative features in this latest market package, SiPass integrated MP2.70 builds itself into a more secure, powerful and convenient system, that can meet all your access control requirements.

This section provides you brief information about the latest features and enhancements available in the latest market package of SiPass integrated

- Separate Clients for Configuration and Operation
- Command Line Option to Import and Export Data

3.2.1 Separate Clients for Configuration and Operation

To improve the usability and security of the SiPass integrated system, the installed client has been modified - the configuration and operational aspects of the client have been split allowing a much simpler interface for the users.

SiPass Explorer has been renamed to be the SiPass Operation Client and has had the functionality expanded to include the following features.

- Cardholder and Credential Management
- Visitor Management
- Audit Trail and Customizable Views
- Time Schedule and Holidays
- Access Level, Access Group, Offline Access Group
- Venue Booking
- Manual Override, Anti Passback Management
- Log Entry Form

3.2.2 Web-based User interface

The new web based operational client for SiPass integrated is a completely new user-centric design for a simple and self-explanatory menu structures and buttons. It has been built on the latest HTML technology and uses high security communication for data transfer.

The user is able to create a customizable dashboard with widget capabilities, linking and pinning. The responsive design of the underlying framework also supports multiple resolutions on multiple monitors. Browser support includes Chrome, Firefox and Internet Explorer.

A brief overview of available configuration and features options is given below:

Configuration	Features
Cardholder	Application Settings
Visitor	Quick Search
Access Level	Advanced Search
Access Group	Multiselect Option for delete
Venue and Venue Views	Context sensitive help
Venue Bookings	Element sensitive help
Manual Override	Pinning
Credential Design	Live Search
Settings	Logout
Live Alarms	Saved Search

3.2.3   Total Building Access Control

A high level interface for the connection of SiPass integrated to the elevators using thyssenkrupp Service Adapter creates a total building access control solution, addressing the growing need for this requirement in the marketplace.

* Enhanced destination control system
* One system to operate the building security - one database
* New and smart solutions due to high level integration/intelligent interfaces
* All engineering for site configuration can be done within the User Interface - no need for conversion protocols or third party hardware

3.2.4   Enhanced Security

SiPass integrated now offers a high-security solution, based on digital certification. While the authentication between the peers (client/server) is done through certificates using the x.509 standard, the authorization is through user logon credentials.

This is how it works:

* A Certification Authority (CA) signs the certificates for the peers
* The SiPass integrated Server and Remote Clients are installed after mutually authenticating the certificates during installation

During everyday operation, the certificates are checked and validated (being signed by the same Certification Authority) at each login to ensure there is no manipulation of the data during transmission.

You can install SiPass integrated Server and Remote Clients using a Machine Certificate or a Self-signed Certificate. While the basic process remains the same in both cases, the difference lies in how the certificate identity is authenticated among the Server and Client Computers.

See the *SiPass integrated MP2.70 Installation Guide* for more information and step by step installation instructions.

3.2.5   Latest Technology

SiPass integrated MP2.70 supports Windows 10 for trouble-free installation and operation on computer systems running the latest Windows Operating System.

Also supported are Windows 7, 8.1, Server 2012 R2 and SQL 2012/2014/2016.

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 Currently Installed	Version You Want To Restore To		
	MP2.65	MP2.70	MP2.70 SP1
MP2.60	Yes	Yes	Yes
MP2.65		Yes	Yes
MP2.70			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)

> **i** 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)

> **i** 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 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 2016 is compatible with WINDOWS 10 64-bit only. Do not install on a computer having the Windows 10 32-bit Operating System.
- SQL2016 IS 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 Operating System, a runtime version of Microsoft SQL Server 2016 SP1 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 4.0	.NET Framework Version 4.5.2

4.6 Web Client Compatibility

Internet Explorer (IE)	Microsoft Edge	Firefox	Chrome	neXus SDK 5.1
v11 10.10240.16384	10.10240.16384.0	49.0.1	55.0.2883.87 m	

ℹ️ neXus SDK needs to be installed by the user to capture images, signatures, design and print a card of the cardholder from the SiPass integrated web client.

4.7 Web Client Smart Device Compatibility

Apple iPhone 6S	Apple iPhone 6S Plus	Apple iPad Air2	Android device	Microsoft Surface 4

4.8 System Compatibility

4.8.1 Firmware

AC5100 (ACC-020 / ACC-010)	AC5102 (ACC-G2)	AC5200 (ACC lite)	Granta Mk3 (ACC-Granta)	Granta Mk3 Backboard
Version 2.70.45	Version 2.70.45 Platform Version CCP v2.17.2	Version 2.70.45	Version 2.70.45	Version 1.29

ADD51x0 (DRI)	ADD51x0 (DRI-OSDP Crypto)	ADS52x0* (SRI)	AFI5100 (IPM)	AFO5100 (OPM)
Version 3.55	Version 5.27	Version 3.23	Version 2.36	Version 1.16

ADE5300 (ERI)	AFO5200 (8IO)	ATI5100 (IAT-010)
Version 3.51	Version 1.06	Version 1.10

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

ℹ️ **For upgrading to MP2.70, 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 software bundle.

4.8.2 Hardware

4.8.2.1 Controllers

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

AC5200		Granta Mk3
SR35i MkII Revision 2		Revision 1

4.8.2.2 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

4.8.2.3 I/O

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

4.9 API / HLI Compatibility

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

4.9.1 HR-API Interface

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

SiPass integrated 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 requires establishing an authenticated connection to be set up with the HR-API application by performing few additional steps. See the SiPass integrated HR-API Programmers Reference Manual for more information.

4.9.2 Management / Enterprise Station API

SiPass integrated MS-API allows data to be accessed and maintained from any programming language that supports COM automation. IN addition, the SiPass integrated MP2.70 release now includes the Management Station RESTful API Web Service also.

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.

4.9.3 OPC A&E Server Interface

SiPass integrated supports OPC A&E version 1.0

4.10 Digital Video Recorder (DVR) System

4.10.1 DVR Integration

SISTORE MX (including NVS)	**2.90 SP2**
SISTORE MX	**2.90 SP2M1**
SISTORE CX	**3.6.4**
SISTORE CX1	**3.5**
SISTORE CX4/8	**3.5, 3.6**
SISTORE SX	**3.1**
VECTIS HX	2.1.5
VECTIX iX	2.10.0.236 (SDK 2.5.4.06)

i 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.

4.10.1.1 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	16 MBit/s	30 fps

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

4.10.2 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

i 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.

4.11   Directly Connected IP Camera Compatibility

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

i

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.

4.12   Intrusion Panel Compatibility

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

i

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

4.13   Network Communication

Encryption of ACC and SiPass communication	AES 128 Bit
SSL Encoding protocol for SiPass client/server communication	TLS 1.0

4.14   Modem Compatibility

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

i

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.

4.15 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.

4.16 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**	FargoHDP5000 with built-in OMNIKEY 5321**	FargoHDP5000 with built-in OMNIKEY 5421**

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

4.17 Enrolment Reader Compatibility

4.17.1 USB Enrolment readers

CardMan 5321	CardMan 5421	CardMan 5422

4.18 Card Format Compatibility

4.18.1 Reader Connection Types

Wiegand	RS-485	Clock & Data

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

4.18.2 Siemens Proprietary Card Formats

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

4.18.3 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

4.18.4 Smart Card Formats

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

i *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).

4.19 Card Reader Compatibility

4.19.1 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

i 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.

4.19.2   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

4.19.3   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	900NWNNEKE 00K9	LF OFF, HF STD/SIO/SEOS/M IGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE05 27
R10 Series	N	Y	OSDP/RS-485	Pig tail	900NWPNEKE 00PJ	LF OFF, HF STD/SIO/SEOS/M IGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE05 27
R15 Series	N	Y	OSDP/RS-485	Pig tail	910NWPNEKE 00PJ	LF OFF, HF STD/SIO/SEOS/M IGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE05 27
R 40 Series	N	Y	Wiegand	Pig tail	920NWNNEKE 00K9	LF OFF, HF SEOS/MIGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE05 27

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
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

4.20 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.

4.21 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.
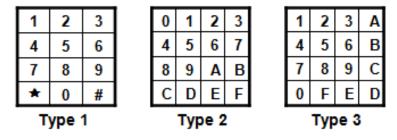
Using 4G V-Station readers, multiple fingerprints can be encoded on the Mifare Classic and Mifare DESFire cards. In addition to storing the fingerprint image on the card, SiPass can also store multiple fingerprints in the database that can be retrieved if a card is lost.

4.22 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.

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

> ℹ️ 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.

4.23 Signature Capture Tablet Compatibility

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

4.24 Messaging System Compatibility

Microsoft Exchange Server 2007 (SP3) or newer

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

4.25 Server Redundancy

Stratus Technologies EverRunFT

> ℹ️ 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.

4.26 Offline Door System

SALTO SPACE Version 4.0.3.2*

ℹ️ * SALTO SPACE v4.0.3.2 is recommended for optimum performance however, the older SALTO v12.02.09.214 is still 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).

4.27 Third-Party Visitor Management

Easy LobbyVersion SVM 10.0

ℹ️ 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.

4.28 Virtualization

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

ℹ️ 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 Server, Configuration Client and Operation Client

5.1.1 Enhancements

Enhancement	Description
Audit Trail	An additional byte has been added to the RIM device Configuration Blocks to enable and disable the functions below: • OSDP Date / Time display options • Enable / disable sending of OSDP Tamper messages to ACC
Audit Trail	When an operator sends a manual command to a Point Group (all doors), the Audit Trail now displays the name of the Group, Points inside that group, the Command issued and name of the Operator.
Cardholder and Access Management	SiPass integrated now supports the DESFire card file read/write operation using defined key. The Mifare DESFire Profile Configuration is done through the new dialog - *DESFire Profile Configuration*. See section Enhanced DESFire Profile Encoding [➜ 9] in this document. Also see the *SiPass integrated Configuration Client User Guide* for more information.
Daily Operation	The Audit Trail displays when and which cardholder was moved to an APB area.
Daily Operation	Two new options are available: • On Operation client Tool Bar - *Logoff and Exit* • On *Logoff* screen tool bar - *Exit*
Reporting	The IP address of the device is now included in the Units report.
Reporting	Custom fields are supported in the following reports: • Cardholders Point Concise • Cardholders Point Detail • Cardholders Filtered Point Access • Cardholders - Concise **Note:** On SiPass integrated Clients, any new custom fields will be hidden if it belongs to the above reports.
System Setup	SiPass integrated now gives you the option to connect OSDP Readers that are not ARxxS-MF or HID (iClass) readers. You can now connect any other reader by selecting **OSDP General** from the **Reader Type** drop down list

5.1.2 Fixed Issues

Type	Description
ACC	Flashing DRIs on FLN 3a/3b to firmware 3.48 on ACC-020 resulted in communication failure.
Cardholder and Access Management	The Host Event Task did not run when using a Holiday Time Schedule.
Cardholder and Access Management	A button (on a Custom Page) to open a batch file did not work.
Cardholder and Access Management	The *Janus Trial License* dialog was displayed while exporting a Custom Page.
Cardholder and Access Management	SiPass integrated now supports the HID Omnikey 5422 USB enrolment reader.
Cardholder and Access Management	Predefined fields in Custom Page Design could not be set to "Unique".
Cardholder and Access Management	In the Cardholder Access Details, the Access Levels were not listed in Alphanumeric order.
Daily Operation	The status of the Salto bus was reported but the Alarm Class assigned to the bus did not work.
Daily Operation	The device number was not included in the Time and Attendance (T&A) report.
Daily Operation	French accented characters used in the comment of an alarm were not displayed correctly when the point in the site plan was double-clicked.
Daily Operation	Commands sent from a site plan by an operator logged-in to SiPass integrated Operation Client did not show the name of the operator. However, the same command sent through the *Manual Override* dialogue showed the operator name.
Daily Operation	The Time and Attendance (T&A) calculation was done incorrectly for an employee with a start badge entry not having a corresponding badge off entry.
Daily Operation	The client connection count was much higher than the actual number of clients being used, resulting in login failure and requiring the SiPass service to be manually started again.
Database	The language of SiPass integrated Help was changed from German to English after updating through the Patch Tool.
Database	The **Cancel Automatic Backup** menu option has been removed from SiPass integrated Configuration Client.
Database	After applying the software patch in German and restoring the database, the Language of Time Schedules got changed.
Import/Export Tool	While performing update with the Patch Tool, there was no warning message displayed if there were files that could not be over-written.

Type	Description
Installation	When SiPass integrated was installed with one Admin user account and an upgrade was performed with another Admin user account, the operation failed.
Installation	The SQL Express could not be installed on computers that did not have the Service Pack 1 for Windows 7 installed.
Installation	During SiPass integrated installation, an unsigned installer was also visible.
Integration	When connecting from a Windows 10 computer (with MM8000 license) to a Windows 7 computer (having MM8000 interface), the SiPass server stopped working. The issue also occurred when SiPass integrated and MM8000 were installed on the same computer running Windows10.
Reporting	The Operator Log Book had issues for a date whenever there was at least one file with over 257 characters for that date.
System Setup	Only 16 character password could be entered into SiPass integrated Operation Client.
System Setup	The **Change Password** button has been removed from the *ASP Lockout* dialog.
System Setup	The *Intrusion Area Name* and *APB Area Name* were not sorted alphabetically.
System Setup	The Sipass Client stopped working when either the Server name, or the ACC Bus was clicked in the components tree. Clicking the + symbol to expand the tree did not cause any issue.
System Setup	The Controller Based Event Task (CBET) (with trigger as *Any invalid Access Event*) worked only for base card technology (and not for all card technologies).
System Setup	The Host Event Task (HET) was not triggered with the state Valid Card Presented.
System Setup	When the ACC's "Peer Network Mode" was set to "slow", ASP P2P function did not work. Saving and Downloading displayed an error message.

5.2 SiPass integrated Web Client

5.2.1 Fixed Issues

- In the dialog box, on selecting the access objects checkbox, the list refreshes. This results in displaying incorrect record counts.
- Pinning form's Pinning Groups dropdown values are shown in English and not in English language.
- Settings form Ascending Descending is shown in English and not as German Resource keys.
- 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.
- **Sorting Order** options (that is, **Ascending** and **Descending**) does not display in the language chosen during the login and it is displays only in English.
- When user performs a quick search or an advanced search and the searched keyword is not present in the list, the List View gets cleared, however, the last viewed item detail gets displayed in the Detail View.
- If the length of the text in the check box label exceeds the given size, the text breaks and does not display in a single line.
- All tab pages do not load properly. User needs to click the visible tab page to load the remaining tab pages.
- After logging in to the SiPass integrated web client, the number of web clients that are currently connected to the Server is displayed only as 0 in the system status screen of the SiPass Configuration Client.
- DateTime control does not work properly when user has logged in through Chinese Language.
- The Search option does not work after saving the configuration settings.
- In the **Home** page,
  - (before selecting any application) when **Edit** button is clicked, the unpin button is enabled.
  - Full screen view is not displayed. User has to click the icon twice to display the application in full screen.
- In the editable drop down list box, user cannot enter space in-between the text.
  - For e.g. If user enters **Siemens Technology**, the text will be taken only as **SiemensTechnology.**
- When user performs the **Edit** operation and tries to **Cancel** the edit operation, a confirmation message **Do you really want to cancel?** displays. When user clicks Cancel, the application behaves abnormally. For Example.
  - When user performs an Edit operation in the Cardholder application, and tries to Cancel the edit operation, a confirmation message **Do you really want to cancel?** displays. When user clicks Cancel, the **Show Calendar** button stops working.
- While clicking the **Saved Search Edit** icon, the **Save** and **Cancel** buttons does not display. This can be resolved by resizing the tree view.
- Once the Saved search is configured with "not contains' search criteria, the data cannot be loaded in the list View.
- If user deletes a record from the **Saved Search**, the deleted record is not selected as the first record category in the tree view (filter).
- In the **Extended Search** dialog box, the **not-equal-to operator** does not perform its functionality.
- In the Pinning dialog box, the **Group** drop down list box's first value is not selected by default.

- In the Tree view,
    - User can toggle a Tree item header to expand/collapse. While collapsing a Tree item header, its corresponding list view disappears, however, the detailed view page still displays the detailed information of that particular tree item header record.
- In the **Cardholder/Visitor** application:
    - An operator having Cardholder access, has rights only to the fields in the **Advanced** and the **Definition** tab, in this case a cardholder cannot be created.
    - The Error "TypeError: Cannot read property 'parentNode' of null" displays randomly.
    - In the Imaging tab, while clicking the Image Recall button, only the default image displays instead of the last saved image.
    - Only in English language the validations that are common for Cardholder and Visitor displays correctly. For e.g. Employee/Visitor Name cannot be empty. In other languages, the validations display in generic. For e.g. Visitor Name cannot be empty.
    - During Add/Edit operation, when user clicks Home icon, the ADD, EDIT, and DELETE buttons get disabled. Only when user clicks Save or Don't Save button, the above mentioned buttons get enabled.
    - Two credentials are added with the same profile name. When user wants to select and remove a credential, both the credential are selected automatically.
    - The Time Schedule is not properly aligned.
- In the **Manual Override** application:
    - When user searches an unknown command in the Command list, **No matching records found** message does not display.
    - When no data is found in grid view, a message **No matching records found** displays. This message is not properly aligned in IE.
- In the **Venue Booking** application:
    - While performing the Saved Search, the search text box does not display in the extended list.
    - **Require Authentication Check** box selection and the newly added **Cardholders** does not display in the detailed page, unless the user tries to edit the Booking. This is a SiPass Operation client issue.
- In **Page Customization**:
    - When time is not selected in custom pages, e.g. dd/MM/yyyy hh:mm, by default, the Date time control displays as (5:30) in the web client.

6 Known Issues and Limitations

6.1 SiPass integrated Server, Configuration Client and Operation Client

Type	Description
Cardholder and Access Management	When double-clicking an Access Level having floor points (with few Favorite Floors), the *Access Details* dialog for that Access Level displays only a list of floors, with no indication if they are set as Favorite Floors.

Import/Export Tool	The Data Synchronizer import does not run as Windows service.
	
	Resolution: Before using the Data Synchronizer, the service must be registered once by executing manually by giving the command as below:
	
	`sc create SiPassImportService binPath= "<SiPass install folder>\CardholderImportExport.WindowsService .exe" obj= "<account name>" password= "<password>"`
	
	Example:
	
	`sc create SiPassImportService binPath= "C:\Program Files (x86)\SiPassintegrated\CardholderImportExport .WindowsService.exe" obj= "AU002\Doe John" password= "myJohnDoePwd"`
	
	To remove the service before uninstalling SiPass integrated, the command must be given as below:
	
	`sc delete SiPassImportService`
	
	Note: The account used to run the service should have network access permission if the Data Synchronizer is used to import through LDAP data source.

Daily Operation	The Audit Trail Tab files are not generated (even when the **Additionally write to TAB files** checkbox is ticked in the **System Preferences** dialog of the Configuration Client). The SiPass service must be restarted for this to take effect.
Installation	If installing with the **Web Site** option on a computer having Operating System as Windows 10 or Windows Server 2016, the computer must be restarted at the end of installation.
Installation	SiPass integrated *Management Station API*, *Web UI API* and *Web UI* cannot be repaired from SiPass main installer. The respective MSI must be run separately to repair.

Type	Description
Installation	SiPass integrated *Management Station API*, *Web UI API* and *Web UI* do not get removed if installation is rolled back before completion. **Resolution:** These services must be removed from the Services.msc window. See the troubleshooting section of *SiPass integrated Installation Guide* for MP 2.70SP1.
Installation	The SiPass integrated Configuration Client cannot be installed on a client computer by itself. The Operation Client must also be installed on the same computer.
Installation	An operator (having Administrator privileges) can install and use SiPass integrated without restarting the computer, but receives an error when trying to uninstall. However, when the computer is restarted and an uninstall is performed by a user with Administrator rights, SiPass integrated uninstalls successfully.
Integration	SiPass HR-API application does not work with HR-API-Core on a remote client compute. **Resolution:** SiPass integrated Operation Client must be installed on the remote client computer where the HR-API application is used.

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 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 as zero. 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.
  - during page maintenance, when user toggles the list view, only fewer records display in the list view, than the actual number of records that is available in the list view.
  - 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.
  - 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.
- 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 Extended Search view, when user types the search criteria or switch in-between the text boxes, the list view gets refreshed.
- 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.

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 option.

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, the records display for half a page.
- After changing the configuration settings, the total items count does not display on the bottom of the Cardholder list.
- 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,** and **Chinese Traditional**, 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 advanced 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.

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.

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.

- 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 SiShell webclient. User needs to manually enter the pin.

- The **Modify/Repair/Remove** options are not available 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 time picker control works properly, only if the respective language is chosen while logging in the web client.

- 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.

- 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 **Card Holder** 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**:
    – For IE browser, the neXus has to be browsed in the same tab, where SiPass web application is used.
    – 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