

# SIEMENS



## Access Control

### SiPass integrated

### Release Notes

MP 2.70

## Copyright

Technical specifications and availability subject to change without notice.

© Copyright Siemens Switzerland Limited

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

Edition: 30.05.2017

Document ID: A6V11170897

© Siemens Switzerland Ltd, 2017

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
1.1	What's new in SiPass integrated MP 2.70 .....	5
1.2	What this document covers.....	5
1.3	Ordering .....	5
<b>2</b>	<b>Important Release Information (Pre-Requisites) .....</b>	<b>6</b>
2.1	Security Recommendations .....	6
2.1.1	Installing SiPass integrated on a Public Domain .....	6
2.1.2	Reducing Security Risks with Anti-Virus Software.....	6
2.2	Windows Patches and Hot Fixes.....	6
<b>3</b>	<b>New Features for SiPass integrated MP 2.70.....</b>	<b>7</b>
3.1	Separate Clients for Configuration and Operation .....	7
3.2	Web-based User interface .....	7
3.3	Total Building Access Control .....	8
3.4	Enhanced Security.....	8
3.5	Latest Technology .....	8
<b>4</b>	<b>SiPass integrated Installation Compatibility.....</b>	<b>9</b>
4.1	SiPass integrated Backup/Restore Compatibility .....	9
4.2	SiPass integrated Server .....	9
4.3	SiPass integrated Client.....	9
4.4	Microsoft SQL Server.....	10
4.5	.NET Framework .....	10
4.6	Web Client Compatibility .....	11
4.7	Web Client Smart Device Compatibility .....	11
4.8	System Compatibility .....	11
4.8.1	Firmware .....	11
4.8.2	Hardware.....	12
4.8.2.1	Controllers .....	12
4.8.2.2	Door Control.....	12
4.8.2.3	I/O.....	12
4.9	API / HLI Compatibility.....	12
4.9.1	HR-API Interface.....	12
4.9.2	Management / Enterprise Station API.....	12
4.9.3	OPC A&E Server Interface.....	13
4.10	Digital Video Recorder (DVR) System.....	13
4.10.1	DVR Integration .....	13
4.10.1.1	VSS-SDK Compatibility .....	13
4.10.2	Third-Party DVR Integration (Requires DVR-API Connection License) .....	13
4.11	Directly Connected IP Camera Compatibility .....	14
4.12	Intrusion Panel Compatibility.....	14
4.13	Network Communication.....	14
4.14	Modem Compatibility .....	14

4.15	Card Printer Compatibility .....	15
4.16	MiFare Classic Card Encoding (while printing) .....	15
4.17	Enrolment Reader Compatibility.....	15
4.17.1	USB Enrolment readers .....	15
4.18	Card Format Compatibility .....	16
4.18.1	Reader Connection Types.....	16
4.18.2	Siemens Proprietary Card Formats .....	16
4.18.3	Proximity Formats.....	16
4.18.4	Smart Card Formats .....	16
4.19	Card Reader Compatibility .....	17
4.19.1	Readers Supporting the DESFire EV1 Card Technology .....	17
4.19.2	HID Proximity, iCLASS (SE), iCLASS Seos and Mifare Classic/DESFire.....	17
4.19.3	Siemens HID Readers .....	18
4.20	Card Technology Compatibility .....	19
4.21	Morpho 4G V-Station Reader Compatibility.....	20
4.22	Granta MK3 Reader PIN Pad Type Compatibility .....	21
4.23	Signature Capture Tablet Compatibility .....	22
4.24	Messaging System Compatibility .....	22
4.25	Server Redundancy .....	22
4.26	Offline Door System.....	22
4.27	Third-Party Visitor Management.....	23
4.28	Virtualization.....	23
<b>5</b>	<b>Enhancements and Quality Improvements .....</b>	<b>24</b>
5.1	Enhancements .....	24
5.2	Fixed Issues .....	25
<b>6</b>	<b>Known Issues and Limitations .....</b>	<b>27</b>
6.1	SiPass integrated Server, Configuration Client and Operation Client .....	27
6.2	SiPass integrated Web Client .....	29
6.2.1	Known General Issues.....	29
6.2.2	Known Issues for Live Alarm.....	31
6.2.3	Known Issues for Cardholder/Visitor Application.....	32
6.2.4	Known Issues for Page Customization .....	32
6.2.5	Known Issues for Manual Override.....	33
6.2.6	Limitations .....	33
<b>7</b>	<b>Support Information.....</b>	<b>35</b>

# 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 for 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

#### 3.1 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 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

### 3.3 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

### 3.4 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.

### 3.5 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 Compatibility

SiPass integrated MP2.70 requires an individual installation and cannot be upgraded from any previous Market Package version.

Once installed, it can be restored with a backup of existing database from the previous Market Package.

### 4.2 SiPass integrated Server

Windows Server 2008 R2 (SP2)	Windows Server 2012 R2	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 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 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, 50 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) v11 10.10240.16384	Microsoft Edge 10.10240.16384.0	Firefox 49.0.1	Chrome 55.0.2883.87 m	neXus SDK 5.1
--	------------------------------------	-------------------	--------------------------	---------------



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

<b>AC5100 (ACC-020 / ACC-010)</b> Version 2.70.23	<b>AC5102 (ACC-G2)</b> Version 2.70.23 Platform Version CCP v2.17.2	<b>AC5200 (ACC lite)</b> Version 2.70.23	<b>Granta Mk3 (ACC-Granta)</b> Version 2.70.23	<b>Granta Mk3 Backboard</b> Version 1.29
--	--	---	---	---

<b>ADD51x0 (DRI)</b> Version 3.48	<b>ADD51x0 (DRI-OSDP Crypto)</b> Version 5.21	<b>ADS52x0* (SRI)</b> Version 3.19	<b>AFI5100 (IPM)</b> Version 2.32	<b>AFO5100 (OPM)</b> Version 1.11
--------------------------------------	--	---------------------------------------	--------------------------------------	--------------------------------------

<b>ADE5300 (ERI)</b> Version 3.44	<b>AFO5200 (8IO)</b> Version 1.02	<b>ATI5100 (IAT-010)</b> Version 1.06
--------------------------------------	--------------------------------------	--

<b>DC12</b> MkI Version 1.36 MKII Version 1.43	<b>DC22</b> MkI Version 1.36 MKII Version 1.43	<b>DC800</b> Version 1.23	<b>IOR6</b> Version 1.00
--	--	------------------------------	-----------------------------



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.

## 4.8.2 Hardware

### 4.8.2.1 Controllers

<b>AC5102</b> ACC-G2	<b>AC5100</b> ACC Revision 3 ACC-020	<b>AC5100</b> ACC Revision 2 ACC-010	<b>AC5200</b> SR34i Revision 1	<b>AC5200</b> SR35i Revision 1.4
-------------------------	--	--	--------------------------------------	--

<b>AC5200</b> SR35i MkII Revision 2	<b>Granta Mk3</b> Revision 1
---	---------------------------------

### 4.8.2.2 Door Control

<b>ADD51x0</b> DRI Revision D	<b>ADS52x0</b> SRI Revision B	<b>ADE5300</b> ERI Revision A	<b>ATI5100</b> IAT Revision A	<b>4322</b> COTAG	<b>4422</b> SWIPE
-------------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	----------------------	----------------------

<b>DC12</b> Rev 05	<b>DC22</b> Rev 05	<b>DC800</b> Rev. 04	<b>PD30/PD40</b> Rev. 02
-----------------------	-----------------------	-------------------------	-----------------------------

### 4.8.2.3 I/O

<b>AFI5100 IPM</b> Revision B	<b>AFO5100 OPM</b> Revision A	<b>AFO5200 8IO</b> Revision A	<b>4253 I/O</b>	<b>IOR6</b> 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)



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



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
-------------------------------	---	---



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

<b>AXISP1354</b> Fix Camera	<b>AXIS M3007</b> Fix Dom	<b>AXIS P5534</b> PTZ – Dom, Live View	<b>AXIS P7214**</b> 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.

## 4.12 Intrusion Panel Compatibility

<b>Intrunet SI 400 series</b> (Sintony 400)	<b>SPC 4300, 5300, 6300</b> Intrusion System
--	---



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

## 4.13 Network Communication

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

## 4.14 Modem Compatibility

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



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

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



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

The USB-RIF has severe restrictions with reading card types. It can read 26bit Wiegand, 32 bit

Wiegand and all Siemens Clock/Data formats. No other formats are supported.

## 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
--------------------	--------------------	------------------------------------	-----------------



\*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
----------	----------	----------	----------



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).

### 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*

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

## 4.19.3 Siemens HID Readers

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	900N WNN EKE0 0K9	LF OFF, HF STD/SIO/SEOS/MIG R, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE0527
R10 Series	N	Y	OSDP/RS-485	Pig tail	900N WPN EKE0 0PJ	LF OFF, HF STD/SIO/SEOS/MIG R, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R15 Series	N	Y	OSDP/RS-485	Pig tail	910N WPN EKE0 0PJ	LF OFF, HF STD/SIO/SEOS/MIG R, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R 40 Series	N	Y	Wiegand	Pig tail	920N WNN EKE0 0K9	LF OFF, HF SEOS/MIGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE0527
R 40 Series	N	Y	OSDP/RS-485	Pig tail	920N WPN EKE0 0PJ	LF OFF, HF STD/SIO/SEOS/MIG R, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95AN WPT EKE0 0PJ	LF OFF, HF STD/SIO/SEOS/MIG R, 485HDX, TERM, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95AN WPT EWE 00PJ	LF OFF, HF STD/SIO/SEOS/MIG R, 485HDX, TERM, WHITE, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95AN WPT EGE0 0PJ	LF OFF, HF STD/SIO/SEOS/MIG R, 485HDX, TERM, GREY, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527

## 4.20 Card Technology Compatibility

ARxxs-MF OSDP <sup>1</sup>	ARxxs-MF OSDP All HID Prox <sup>2</sup>	ARxxs-MF OSDP ASCII	ARxxs-MF OSDP BCD Packed	ARxxs-MF OSDP BCD Unpacked	ARxxs-MF OSDP Custom <sup>3</sup>
-------------------------------	---	------------------------	--------------------------------	----------------------------------	---

ARxxs-MF OSDP Mifare Facility <sup>4</sup>	ARxxs-MF OSDP Mifare GID <sup>5</sup>	ARxxs-MF OSDP Mifare Numeric	ARxxs-MF OSDP Raw	ARxxs-MF OSDP Sector 7 26-bit <sup>6</sup>
--	---	------------------------------------	----------------------	--



<sup>1</sup>All data from the reader is the card number. The license is as Siemens reader.

<sup>2</sup>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).

<sup>3</sup>Custom Wiegand profile. License is as Custom Wiegand.

<sup>4</sup>This is a Mifare Facility card, encoded by SiPass. The license is as Mifare Facility.

<sup>5</sup>This is a Siemens GID format. The license is as Siemens GID.

<sup>6</sup>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	<ul style="list-style-type: none"> <li>Multi-factor Bio/PIN (3K users, 10K, 50K and 100K with license)</li> <li>1M logs storage capacity</li> <li>Poe included</li> </ul>
	293638898	WR Sigma Prox	<ul style="list-style-type: none"> <li>Multi-factor Bio/Card/PIN/BioPIN (3K users, 10K, 50K and 100K with license)</li> <li>HID Prox</li> <li>1M logs storage capacity</li> <li>Poe included</li> </ul>
	293638856	WR Sigma iClass	<ul style="list-style-type: none"> <li>Multi-factor Bio/Card/PIN/BioPIN (3K users, 10K, 50K and 100K with license)</li> <li>HID iClass</li> <li>1M logs storage capacity</li> <li>Poe included</li> </ul>
	293638877	WR Sigma Multi	<ul style="list-style-type: none"> <li>Multi-factor Bio/Card/PIN/BioPIN (3K users, 10K, 50K and 100K with license)</li> <li>MIFARE®/DESFire® Smartcard Reader</li> <li>1M logs storage capacity</li> <li>Poe included</li> </ul>
MA SIGMA LITE	293678615	MA SIGMA Lite	<ul style="list-style-type: none"> <li>Mono-factor Bio (500 users, 3K and 10K users with license)</li> <li>IP65 and IK 08</li> <li>Certifications: CE, CB, FCC</li> </ul>
	293678628	MA SIGMA Lite iClass	<ul style="list-style-type: none"> <li>Multi-factor Bio/Card (500 users, 3K and 10K users with license)</li> <li>HID i-class® Smartcard Reader</li> <li>IP65 and IK 08</li> <li>Certifications: CE, CB, FCC</li> </ul>
	293673665	MA SIGMA Lite Prox	<ul style="list-style-type: none"> <li>Multi-factor Bio/Card (500 users, 3K and 10K users with license)</li> <li>HID Prox® Smartcard Reader</li> <li>IP65 and IK 08</li> <li>Certifications: CE, CB, FCC</li> </ul>
	293678636	MA SIGMA Lite Multi	<ul style="list-style-type: none"> <li>Multi-factor Bio/Card (500 users, 3K and 10K users with license)</li> <li>MIFARE®/MIFARE® Plus/DESFire® Smartcard Reader</li> <li>IP65 and IK 08</li> <li>Certifications: CE, CB, FCC</li> </ul>

Design	Product Number	Model	Description
MA SIGMA LITE +	293678657	MA SIGMA Lite +	<ul style="list-style-type: none"> <li>• Multi-factor Bio/PIN (500 users, 3K and 10K users with license)</li> <li>• 2.8" colour touchscreen</li> <li>• IP65 and IK 08</li> <li>• Certifications: CE, CB, FCC</li> </ul>
	293673644	MA SIGMA Lite + iClass	<ul style="list-style-type: none"> <li>• Multi-factor Bio/Card/Pin (500 users, 3K and 10K users with license)</li> <li>• 2.8" colour touchscreen</li> <li>• HID i-class® Smartcard Reader</li> <li>• IP65 and IK 08</li> <li>• Certifications: CE, CB, FCC</li> </ul>
	293678678	MA SIGMA Lite + Prox	<ul style="list-style-type: none"> <li>• Multi-factor Bio/Card/Pin (500 users, 3K and 10K users with license)</li> <li>• 2.8" colour touchscreen</li> <li>• HID Prox® Smartcard Reader</li> <li>• IP65 and IK 08</li> <li>• Certifications: CE, CB, FCC</li> </ul>
	293678660	MA SIGMA Lite + Multi	<ul style="list-style-type: none"> <li>• Multi-factor Bio/Card/Pin (500 users, 3K and 10K users with license)</li> <li>• 2.8" colour touchscreen</li> <li>• MIFARE®/MIFARE® Plus/DESFire® Smartcard Reader</li> <li>• IP65 and IK 08</li> <li>• Certifications: CE, CB, FCC</li> </ul>



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



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
---



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
--------------------------------



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 3.1.4.0
-----------------------------



\* SALTO SPACE v3.1.4.0 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
----------------------------



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
------------------------------	--	--



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

## 5 Enhancements and Quality Improvements

### 5.1 Enhancements

Enhancement	Description
Hardware	The ACC Controller now has the capability to configure up to two DNS servers by IP address, and to configure the SiPass server name as an alternative to the primary static IP address.
Hardware	The device firmware now supports three types of date/time display (and defaults to numeric only format): <ul style="list-style-type: none"> <li>• YYYY/MM/DD HH:MM</li> </ul> The other two formats are: <ul style="list-style-type: none"> <li>• DD/MM/YYYY HH:MM</li> <li>• DoW DD mmm HH:MM</li> </ul>
Hardware	For added security, the HID Wiegand Reader Heartbeat function is now supported to monitor the status of connected Wiegand readers.
Hardware	The OSDP Reader with Display can displays messages for the following: <ul style="list-style-type: none"> <li>• Area Armed</li> <li>• Area Disarmed</li> <li>• Area Part Armed</li> <li>• Arming Failed</li> <li>• Disarming Failed</li> </ul>
Integration	The following new features have been added: <ul style="list-style-type: none"> <li>• Failure to arm from a manual command or Site Plan will result in all unsealed and alarm inputs being reported to the audit trail. In this case, you can use the "Isolate" manual override for the given Input Point(s). The new manual override command to "Clear Alarm" has also been added, however Alarm inputs can also be isolated in SPC.</li> <li>• If arming fails from the IAT, the IAT session will return to the main menu, where you can select the SPC Menu and choose to display all unsealed inputs.</li> <li>• Two Audit Trail messages have been added namely "All Alarms Cleared" and "All Bells Silenced" to display the status.</li> </ul> <p><b>Note:</b> for the above features to work, the SIA events must be enabled in the SPC Panel.</p>
Integration	SiPass integrated now supports SALTO locker functionality (configuration done through SALTO). The SALTO configuration data is downloaded to SiPass with support for: <ul style="list-style-type: none"> <li>• Free Assignment Locker and Normal Locker</li> <li>• Different icons for these two type of lockers in the Components dialog under the SALTO configuration</li> <li>• Free Assignment Locker Zone and Normal Zone</li> <li>• Ability to assign Free Assignment Locker Zone and Normal Zone to Cardholder, Workgroup and Access Level (Individual Free Assignment Locker cannot be assigned)</li> </ul>



## 5.2 Fixed Issues

Type	Description
ASP	Adding a flag (with name length over 40 characters) to a site plan caused the SiPass server to crash.
Cardholder and Access Management	The access points were not listed alphabetically in Cardholder, Venue, Work group, Access Assignment, Access Level and Access Group dialogs.
Cardholder and Access Management	The default time schedule (Always) could be edited and the change could be saved even when the Save button was disabled.
Cardholder and Access Management	A recurrence venue booking did not show the parameters that were actually configured.
Cardholder and Access Management	Modifying a series booking through the Venue Management dialog resulted in error messages (without any text) being displayed randomly.
Cardholder and Access Management	The <b>Issue</b> and <b>Save</b> buttons did not work in the Visitor dialog.
Cardholder and Access Management	The Readers did not function in Guard Tours when the guard used a Siemens Mifare GID card. Other card technologies such as Siemens RS485 operate as expected.
Cardholder and Access Management	Assignment of GID through the enrolment reader did not work and the revision number was not assigned to the cardholder.
Cardholder and Access Management	The <i>Visitor</i> dialog was available and could be opened even when the license did not include the Visitor option.
Daily Operation	Fixed the error caused after customizing the original <i>Predefined Reports</i> .
Hardware	The following card reader technologies were not available for selection: <ul style="list-style-type: none"> <li>• 85 OSDP ASCII</li> <li>• 86 OSDP BCD Packed</li> <li>• 87 OSDP BCD Unpacked</li> </ul> It was also not possible to check if the corresponding DRI/ERI FW supported the above technologies.
Hardware	If a Sintony intrusion area could not be armed via a reader, no feedback was received in the reader or SiPass Audit Trail. But when the area was armed through Manual Override and could not be armed, the Audit Trails reported this information.
Import/Export Tool	The <i>DataSynchronizer and Import/Export</i> tool did not ask for a workstation license.
Installation	Modifying the DEMO license installation to another license resulted in error.
Integration	In HR-API, Venue booking filtering for properties <i>venueName</i> and <i>venueId</i> did not work,

Type	Description
Intrusion	Saving an Intrusion Area (with short name having over 16 characters) caused the SiPass service to crash.
Reporting	APB Details report had less columns than the APB Area report.
Site Plan	The intrusion alarm could be manually cleared only for the unit/controller and not for a specific SPC Input/Zone in the IAT session.
Site Plan	When creating a new symbol (or site plan, or drawing etc.), selecting the bright green color resulted in the window to disappear.
System Setup	The reader was not shown in all the elevators however, the elevators worked properly. On creating a new Elevator, the reader was visible.
System Setup	When restoring certain databases, opening points within the <i>Components</i> dialog resulted in a prompt to save changes (with no changes being made). An Audit Trail message was also displayed indicating that the point name is changed (even when the point name was not modified).
Time Schedule	A Time Schedule used in a Controller Event Task as a 'Trigger Time Schedule' could be deleted without any warning, leaving the Event Task with a blank space in the Trigger area.
User Interface	The database field boxes on the Event Task dialog did not display complete length of the value (point name).

## 6 Known Issues and Limitations

### 6.1 SiPass integrated Server, Configuration Client and Operation Client

Type	Description
Cardholder and Access Management	If the operator has no permission for <b>Imaging</b> fields, an error is encountered while loading a Cardholder.
Cardholder and Access Management	The <b>Issue and Save</b> function does not work, not allowing the Visitor functionality to complete. To handle the issue, the void card option can be removed after saving the visitor record.
Cardholder and Access Management	If a Mifare card was encoded with a Salto online reader, such a card cannot be encoded by SiPass if the customer key is entered to the "overwrite" key section. However, if the same key is entered to the Mifare key, the card can be encoded.
Cardholder and Access Management	The "last printed date" is not correctly handled.
Cardholder and Access Management	If only the license is updated (no uninstall/re-install of SiPass), the <i>Visitor</i> function is added but the corresponding visitor tabs are not created. However, taking a backup, uninstalling and re-installing SiPass with the updated license resolves the issue.
Cardholder and Access Management	Credential name changes to credential ID on modifying any option on the <i>Cardholder</i> dialog.
Cardholder and Access Management	The <i>Imaging</i> Tab works for <i>Cardholder</i> and <i>Visitor</i> even when the corresponding license does not include this option.
	The Text fields were disabled in Custom Page designer after restoring a SiPass integrated MP2.65 database.
Daily Operation	The cardholder related pre-defined reports are not displaying the cardholder images when changing the view to <Photo List>. The images must be added manually to the view.
Daily Operation	A button added on a <i>Custom Page</i> does not work.
Daily Operation	SLEEP MODE SHOULD NOT BE USED for Windows operating system on the computer(s) where SiPass Server and Client are installed as it may result in operational errors.
Daily Operation	In case of cardholders not having First Name or Last Name, the encoding profile update from workgroup will not work.
Daily Operation	Operation Client freezes when the SiPass service is stopped or disconnected.
Daily Operation	Currently, the operator is not informed if the certificate is expiring soon (so a new one must be generated/applied).
Daily Operation	The SiPass Start up messages do not give a proper message if the certificate is expired.

Type	Description
Daily Operation	In some site installations, the assigned Mifare encoding profile could not be updated.
Database	While the SiPass SQLARC files (based on SQL Server Compact Edition) can be managed through other tools like MS Visual Studio, these can be opened only in MS SQL Management Studio 2008 and older.
Database	Any instance of SQL Server 2008 must be uninstalled before installing SiPass integrated MP2.7.
Database	On a computer running Microsoft Windows 10, database backup failed when the operator did not run SiPass integrated as administrator, and selected the <i>System Settings</i> and <i>Local Settings</i> backup option.
Installation	If performed from within the SiPass integrated setup, the MS SQL Express installation is blocked if Microsoft LocalDB (another SQL product similar to SQL Express) exists on the PC.
Installation	The Web Site option is displayed as <i>Not Installed</i> even when it is installed.
Installation	While installing SiPass on a brand new Windows 7 and/or Windows 10 operating systems, the SQL installation is not performed. The SiPass installation process proceeds instead of stopping, and stops when a SQL error actually occurs.
Installation	The <i>Web UI API</i> service is installed even when the license does not include Web Client function.
Installation Daily Operation	<p>SiPass server time and Remote Client time MUST BE SYNCHRONIZED under workgroup environment.</p> <ul style="list-style-type: none"> <li>Window Time service should be running.</li> <li><b>Synchronize time with an Internet time server</b> checkbox should be checked under <i>Date and Time</i> Setting.</li> </ul> <p><b>Note:</b> The maximum UTC time difference between client and server computers must be less than 5 minutes</p>
Installation	If installing with the <b>Web Site</b> option on a computer with Windows 10, the computer must be restarted at the end of installation.
Integration	SALTO to SiPass upload does not update names of SALTO units.
System Setup	The Web site option is enabled even without the Web Client license.
System Setup	Even when the Operator name is not unique, SiPass does not give any error message.

## 6.2 SiPass integrated Web Client

### 6.2.1 Known General Issues

#### Common for All Applications

- **Select All** and **Deselect All** options does not select the first record by default during the following scenario:
  - While clicking the **Multiselect** icon.
  - While clicking the **Select All** icon at the bottom.
  - While clicking the **Deselect All** icon at the bottom.
  - While clicking the **Multiselect** icon again.
- Search control in dialog box is based on the Name of the listed objects.
- 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.
- While working with the application, randomly, an error displays as **API is not reachable**, 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 service is not available, the Error “**Internal Server Error: Unable to connect to the Sipass server**” displays twice.
- When Web UI API service is not reachable, the Error “**API not reachable.**” displays twice.
- 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.
- 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.
- During mouse hover event, for some elements the tool tip does not display.
- **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.
- Once the Saved search is configured with "not contains" search criteria, the data cannot be loaded in the list View.
- When the tile is switched from General settings to other tiles, the Pinning does not work.
- In the Combo box, the default value **Please select a value** does not display randomly.
- Multi-select checkboxes in the dialog box will be misaligned.
- 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).
  - When user tries to view the Cardholder application, and before the page loads, if user navigates to Home page, the audit trail does not display with the previous action, if audit trail needs to be displayed, user needs to logout from the application and login again.
- At times, the tool tip displays everywhere while moving the cursor.
- 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.
- After selecting the item from the list in **Add** mode, the message prompt **Don't Save** and **Save** functionality does not work as expected.
  - While adding a new cardholder, if user navigates to another cardholder, before saving the new cardholder, a message prompts as **Do you want to save?**. On clicking Save, the pointer does not show the created cardholder, instead points to shows some other cardholder.
- After selecting the item from the list in **Edit** mode, the message prompt **Save** functionality does not work as expected.
  - While editing a cardholder, if user navigates to another cardholder, before saving the edited cardholder, a message prompts as **Do you want to save?**. On clicking Save, the pointer does not show the created cardholder, instead shown some other cardholder.
- All tab pages do not load properly. User needs to click the visible tab page to load the remaining tab pages.
- The Search option does not work after saving the configuration settings.
- 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.
  - **For Example:** Pin a Booking to the home screen. From the home screen, when user clicks the pinned booking, the pinned item will not be selected in the list view, however, the pinned record will be displayed in the detailed view.
- Pinning form's Pinning Groups dropdown values are shown in English and not as German Resource keys.
- Settings form Ascending Descending is shown in English and not as German Resource keys.
- Alignment Issues
  - **For Example:** When Tab Page is put inside a Group box/Another Div Element, the Tab Page is visible in Chrome, however, it is not visible in Firefox and IE.
- 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.
- 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.
- Log on to the SiPass integrated webclient. In the middle of any action, if the SiPass server is stopped, and during this situation, if user clicks on any application, a message SiPass server not available must display. However, currently this validation message does not display.
- DateTime control does not work properly when user has logged in through Chinese Language.
- In grid view, even though user selects multiple records, only the last selected record is displayed.

### Common for Access Level / Access Group / Venue Configuration / Credential Design

- The **Saved Search feature** is not applicable.

### Venue Configuration

- In **Venue** application, if user accesses a non-existing item, an exception "Access Denied" is thrown. This is a SiPass issue.

### Venue Booking

- The newly added time that is updated through the **Edit** operation is cancelled in venue booking.
- The Pinning feature selects the first item in the Venue Booking list instead of selecting the pinned item.
- While performing the Saved Search, the search text box does not display in the extended list.
- 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.

## 6.2.2 Known Issues for Live Alarm

- In the **Configuration** dialog box, the **Date Date** and **Time** field works only based on the **Contains** logic.
- During the **Search** operation, if user searches the alarm by the previous date, the previous date alarms will be listed. However, if a live alarm is generated during the search operation, the live alarm will be listed first in the list, irrespective of the search criteria.

## 6.2.3 Known Issues for Cardholder/Visitor Application

### Cardholder / Visitor Application

- The first item in the **List View** is not selected by default.
- In the **List View**, the card number displays only when it is configured for the Base profile.
- The Error “**TypeError: Cannot read property ‘parentNode’ of null**” displays randomly.
- Date time does not work properly across all apps. When datetime field is cleared, the application clears only date field and not time field. Time field in date time picker does not reflect in the control.
- 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.
- In the **Imaging** tab, while clicking the **Image Recall** button, only the default image displays instead of the last saved image.
- 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.
- 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.
- 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.
- Two credentials are added with the same profile name. When user wants to select and remove a credential, both the credential are selected automatically.

## 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.
- 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.



## 6.2.5 Known Issues for Manual Override

### Manual Override

- Features like Pinning, Paging, and Settings are not available.
- 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.

## 6.2.6 Limitations

- SiPass web application is tested on **Windows 7 (English), Windows 10, Windows Server 2012**.
- The settings of **Access Level, Access Group, Venue Configuration, and Credential Design** works only for the **Sorting Order**.
- In Quick and advanced Search, the date fields work based on equal to logic.
- "**Details loading**" message displays in the detail page, even though "**No data available**" displays in the List view.
- 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.
- **Require Authentication Check** mark and the newly added **Cardholders** does not display in the details page, unless the user tries to edit the Booking. This is a SiPass Operation client issue.
- Random pin generation for Cardholder/Visitor is not available in the SiShell webclient. User needs to manually enter the pin.
- During SiPass installation, if the base card technology is Siemens mifare GID, the application does not allow the user to enter the card number, whereas based on the emp id, the card number gets auto generated. But, if a new credential profile is created with Siemens mifare GID card technology, the system allows the user to enter the card number. This is a known issue in SiPass.
- 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.
- When the user clicks the tree header, the **Loading** or **Processing** comment is displayed.
- 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, then the webclient displays the corresponding cardholder.
- Password field maintain user's privacy by displaying each character the user enters as an asterisk, however, while user types the password, the actual characters are not shown on key stroke after a second.
- For languages other than English, 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 depends on the regional settings available in the system.
- The naming convention followed in the SiPass integrated web client is different from the SiPass Operational client.
- In the **Advanced Search**, when the user tries to change the field settings, the resize option for the fields does not appear.
- The filter criteria gets applied automatically while switching back to simple search from the **Advanced Search**.

- The date and time format in the Visitor application is not displayed entirely to the user.
- The controls available in the SiPass integrated web client application appears different when viewed through the Internet explorer when compared to Google Chrome.
- 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**.
- In the **Venue Booking** applications:
  - When the user tries to clicks the elements in the tree node at a faster rate, the venue booking does not load properly.
  - 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 **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 **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. - Firefox simulated
- **neXus application:**
  - The neXus SDK needs to be licensed separately and can be used in DEMO mode until this time.
  - 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.

## 7 Support Information

### Europe

**Phone:** +49 89 9221 8000

**Fax:** +49 89 9221 6000

**email:** [fs.support.sbt@siemens.com](mailto:fs.support.sbt@siemens.com)

**Hours of operation:** Monday - Friday: 08:00 A.M. - 05:00 P.M. CET

### South and North America

**Phone:** +1 800 877 7545

**email:** <https://support.industry.siemens.com/my/WW/en/requests>

**Hours of operation:** Monday - Friday: 08:00 A.M. - 06:00 P.M. Eastern Time

Issued by  
Siemens Switzerland Ltd  
Building Technologies Division  
International Headquarters  
Gubelstrasse 22  
CH-6301 Zug  
+41 41-724 24 24  
[www.siemens.com/buildingtechnologies](http://www.siemens.com/buildingtechnologies)

© Siemens Switzerland Ltd, 2017  
Technical specifications and availability subject to change without notice.