SIEMENS

Access Control

SiPass integrated

Release Notes

MP 2.95

A6V11170897

28.09.2023

Smart Infrastructure

Copyright

Edition: 28.09.2023

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, OSS-SO
- Wireless locking system, APERIO, utilizing the powerful ACC-AP controller
- Touchless Biometric Systems integration with web client enrolment
- SiPass integrated -- Opening doors to a secure environment.

NOTICE	
!	High Risk System shall mean a device or system that requires enhanced safety functionalities such as fail-safe or fault-tolerant features to maintain a safe state where it is reasonably foreseeable that failure of the device or system could lead directly to death, personal injury, or catastrophic property damage. High Risk Systems may be required in critical infrastructure, direct health support devices, aircraft, train, boat, or vehicle navigation or communication systems, air traffic control, weapons systems, nuclear facilities, power plants, medical systems and facilities, and transportation facilities. High Risk Use. Customer acknowledges and agrees that (i) the Offerings are not designed to be used for the operation of or within a High Risk System if the functioning of the High Risk System is dependent on the proper functioning of the Offering (ii) the outcome from any processing of data through the use of the Offering is beyond Siemens’ control. Customer shall indemnify Siemens, its Affiliates, its subcontractors, and their representatives, against any third-party claims, damages, fines and cost (including attorney’s fees and expenses) relating in any way to any use of an Offering for the operation of or within a High Risk System.

NOTICE	
!	This Siemens system is not designed to be fault tolerant and is not intended to be used in hazardous or high risk environments or systems that require fail safe operations in which the failure, or interruption to normal operations of the system, could lead directly to death, personal injury or damage to the environment. High risk environments may include, without limitation, communication systems, fire control and release systems, personal safety systems, air travel, space travel, fire-fighting, police operations, power plant operation, military operations, rescue operations, hospital or medical operations, nuclear facilities or equipment, or anywhere that requires fault tolerance. High Risk System means a device or system that requires enhanced safety functionalities such as fail-safe or fault-tolerant features to maintain a safe state where it is reasonable foreseeable that failure of the device or system could lead directly to death, personal injury, or catastrophic property damage.

1.1 What this document covers

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

1.2 Ordering

To order the SiPass integrated software, contact the Siemens Sales Department in your region.

2 Important Release Information

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 Security Recommendations*.

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, controllers or an integrated system are to be installed on a public domain, it is recommended that a dedicated network (like a VLAN) be used for optimal security. Telnet and SSH on the ACC and ACC-AP 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 yourr 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.

2.1.3 Physical and Environmental Security

The following restrictions apply with regard to the physical protection of the SiPass integrated system against unauthorized or malicious use:

- The equipment room in which the SiPass integrated is installed must be locked and access must be controlled by means of organizational access restrictions.
- All publicly accessible data transmission lines must be protected against unauthorized access.
- Serial interfaces and cabling must be physically protected when any of these components are located in a publicly accessible area.
- The serial end points must be protected by physical, organizational or logical means. Only connect approved devices to these interfaces. The interface must be deactivated if no devices are connected.

- Define and implement processes to grant and revoke physical access.
- Additional controls – such as site protection, additional restrictive access control for the building and rooms, security personnel, or monitoring – can help to improve the physical security of the system.

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.

2.3 Maintenance Support

The most recent market release(s) are classified as **Maintained Versions**. For these releases Hotline Support, Service Releases and Software Updates (For example, new extension modules) are available.

Previous market releases are classified as **Supported Versions** for which Hotline Support and Service Releases are available.

Older market releases are classified as **Retired Versions**. This means that customer support is no longer obligated to answer support calls. To get support, the customer will have to upgrade to a newer market release. Activating the license for a maintained version will start the first year of SUR support. If the customer, then purchases a further 2 years SUR they will remain supported.

Market Release	**Maintained Version**	**Supported Version**	**Retired Version**
SiPass integrated MP2.95	X		
SiPass integrated MP2.90		X	
*SiPass integrated 2.85		X	
SiPass integrated MP2.80 and earlier			X

*SiPass integrated MP2.85 localised versions will be supported until a replacement is available for the language in MP2.95. Once the localised version is available in MP2.95, no further support calls will be possible with the MP2.85 except for upgrade queries.

3 New Features in SiPass MP 2.95

3.1 Installer Prerequisites Validation

SiPass integrated MP 2.95 installer has been enhanced with a new dialog box to validate the prerequisites and therefore this makes the installation smooth. The installer does not proceed if any of the prerequisites are not met.

The following prerequisites are validated during installation:

- File Execution Permission
- Registry Access
- Folder Access
- Port Access
- SQL User Rights

3.2 STid Secure Common Protocol (SSCPv2)

SiPass integrated supports SSCPv2 (STid Secure Common Protocol) is a reader RS485 protocol which comes with high security standard (ANSSI) to enable security from reader to ACC AP (DRIe).

For information on configuring the reader, refer "*Configuring STid Secure Common Protocols (SSCPv2) Reader*" section in the *Configuration Client User Guide*.

3.3 SMTP (Azure) for Modern Authentication

SiPass integrated MP 2.95 has been enhanced to support SMTP Azure modern authentication mechanism. SiPass integrated is moving to modern authentication to avoid surface attacks. Commissioning engineers shall be able to configure Office 365 to trigger email notifications. For information on configuring Office 365, refer to "SiPass integrated SMTP (Azure) Configuration Guide .pdf" supplied with this package.

3.4 SiPass integrated RESTful HR API

- External Access Privilege configuration feature has been introduced to provide bi-directional synchronization of Access Privileges between SiPass integrated and third-party applications/Security Manager. SiPass integrated HR RESTful API provides an option to create/update/delete Access Groups of type External. Existing API end point requests has been modified to achieve these functionalities. Create/Update/Delete Access Groups of type "External" and assigning those privileges to Cardholders are introduced as part of this feature. For more information, refer to the *"SiPass integrated Operation Client User Guide".*
- SiPass integrated HR RESTful API provides an option to create/update/delete the cardholders/images in bulk. New API end points has been provided to achieve these functionalities.
- For more information, refer to "RESTful HR API Release Notes.pdf" supplied with this package. For information on how to consume the updated endpoints, refer to "RESTful HR API Specification Guide.pdf" and "RESTful HR API Object Model Guide.pdf" provided with this package.

3.5 Support for Remote SQL "alias" Domain Names

From SiPass integrated MP 2.95 onward, CNAME as a SQL instance name is supported.

A Canonical Name (CNAME) record is a type of resource record in the Domain Name System (DNS) that maps one domain name (an alias) to another (the canonical name).

4 SiPass integrated Installation Compatibility

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

4.1 License

“SiPass integrated License” is a **subscription-based service** managed by a central tool - **Siemens License Management System (LMS).**

If you do not have a SiPass integrated LMS license	Order a new one for MP 2.95
If you have a LMS license for MP 2.80/2.85/2.90 and are upgrading to MP 2.95	Use the existing license for SiPass integrated MP 2.95 installation, as long as the license subscription is not expired. LMU must update to LMU 2.7.
If you have a License for SiPass integrated 2.76 and lower	Order a upgrade license to operate SiPass 2.95

- Your existing license will be modified and applied to the new License Management Service (LMS), from which you can activate your product.
- Depending on the costs paid for the previous license, the new MP 2.95 license will be issued for the standard upgrade fee (or any other amount as per your current agreement).
- SiPass integrated considers each Management-API (RESTful) connection as a workstation and the user needs to purchase a separate license for each extra connection.

Contact Siemens Support in your region for help with this matter.

Note:

SiPass integrated is always by your side and will keep working even when the subscription expires. However, it is recommended to renew your subscription as soon as possible to stay up to date on the latest product features, security updates and access to support.

When your subscription is about to expire, the status bar in SiPass integrated *Configuration Client* and *Operation Client* will start showing a reminder 7 days before the expiry. You can also check the subscription status any time by clicking **Help > About** from the top menu bar.

Contact Siemens Support in your region for help with renewing the subscription. For details on maintenance support, refer Maintenance Support [→ 8].

4.1.1 LMS Version

LMS 2.7 is supported for SiPass integrated MP 2.95.

4.2 SiPass integrated Server

Windows 10 (Professional, Enterprise) (64-bit)	**Windows Server 2019**
Windows 11 (Professional, Enterprise) (64-bit)	**Windows Server 2022**

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 10 (Professional, Enterprise) (64-bit)	**Windows Server 2019**
Windows 11 (Professional, Enterprise) (64-bit)	**Windows Server 2022**

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 SiPass integrated Web Client

From SiPass integrated MP 2.95 onward, Activity Feed and Area Monitoring features are unavailable.

4.5 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 2022 Express	**SQL 2022**	**SQL 2022 Enterprise**
SQL 2019 Express	**SQL 2019**	**SQL 2019 Enterprise**

The following information must be noted carefully:

- If there are no SQL server versions installed on the computer where SiPass integrated is installed, a runtime version of Microsoft SQL Server 2022 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 doors, 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. Failure to install the appropriate version of SQL Server may have an adverse impact upon the performance of SiPass integrated.

NOTICE

!

If you have unsupported version of Microsoft SQL Server, uninstall it first as it may affect the installation of Microsoft SQL Server 2022 Express. Restart the system after uninstallation.

ℹ

For data privacy, during the upgrade of SiPass integrated, ensure that the "asco4" database and “SiSuite.Access.UAM” database is removed from the unsupported versions of SQL Server.

From SiPass integrated MP 2.95 onward, SQL Server 2022 will be installed only in Windows authentication mode.

4.6 SiPass integrated Sync Agent

SiPass integrated Sync Agent 1.4 or higher is supported.

4.7 .NET Framework

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

.NET Framework Version 4.8

4.8 Installation Requirements

4.8.1 Prerequisites

Before installing SiPass integrated, ensure that the following prerequisites are installed in the system.

- **Browsers:** Chrome and Firefox. Recommended browser versions are:
  - Chrome greater than 103.0.5060.134
  - Firefox 76.0.1

The following must be installed/uninstalled manually:

- License Management System (LMS) (Available in the *Prerequisites* folder in the SiPass integrated software bundle)

NOTICE

!

If you are manually uninstalling, ensure that the installation folder, registry entries, and other related services of the corresponding components are completely removed. By default, the installation folder will be as follows:
RabbitMQ 3.12.0 - <Windows installation drive>\Program Files \RabbitMQ
Erlang OTP 25.3 - <Windows installation drive>\Program Files\Erlang OTP

If ERLANG OTP installed folder is not removed after uninstallation, it is required to restart the machine and remove the folder again.
In prior version of SiPass integrated, while uninstalling, if the previous SiPass integrated folder is still available, it will be automatically removed. Otherwise, an error message will be thrown as **Installer cannot delete a folder (Destination path) from previous installation due to insufficient privileges. Do delete the folder manually and continue with the installation.**

- WE Installation Helper R101 (for **TBS Server** and **Terminal Enrollment**)
- Enrollment Module 10 (for **TBS USB Enrollment**)

In the **Enrollment Module 10** installation folder, navigate to the **Service>Settings>Public>Service.Enrollment.ini** file. Ensure “Use Https” is set as `true` and “Port” has the value 8282. Open **ServerCommunication.WebEdition.ini** file, and map the **EndpointIP** as the IP of the TBS Server. Restart the Enrollment Module 10 windows service.

The following components are installed automatically and must not be uninstalled at any time to ensure uninterrupted operation of SiPass integrated:

- .NET Framework 4.8

  Note: Make sure to exit all .NET based applications before you install.
- Microsoft Command Line Utilities 15 for SQL Server (x64)
- Microsoft ODBC Driver for SQL Server (V17.10.4.1)
- Microsoft OLE DB Driver for SQL Server (v19.3.1)
- Microsoft SQL Express 2022 (Optional)
- Microsoft Visual C++ 2015-2022 Redistributable (x86 and x64)
- OPC Core Components Redistributable (v3.0.102)
- RabbitMQ 3.12.0
- Erlang OTP 25.3
- Microsoft Application Request Routing 3.0
- IIS URL Rewrite Module 2.0

You may be prompted to restart your computer during or after the installation.

NOTICE	
!	The following components are not used by SiPass integrated MP 2.95 anymore and can be manually uninstalled: **Apache Tomcat** **Java 11** **.NET Core 3.1.xx/.NET 6.0.xx** **MonogDB 4.4.xx** **Microsoft SQL Server Express LocalDB 2014/2019** **Microsoft SQL Server 2017** **Microsoft Visual C++ Redistributable 2015 – 2019** You may need to restart the computer after the uninstallation of the components.

4.9 System Compatibility

4.9.1 Firmware

AC5100 **(ACC-020 / ACC-010)** Version 2.76.46	**AC5102** **(ACC-G2)** FW v6.0.3+4057 App v3.0.4	**ACC-AP** FW v6.0.3+4057 App v3.0.4
AC5200 **(ACC lite)** Version 2.70.52	**Granta Mk3** **(ACC-Granta)** Version 2.70.52	**Granta Mk3 Backboard** Version 1.29

ADD51x0 (DRI) Version 3.67	**ADD51x0** **(DRI-OSDP Crypto)** Version 5.43	**ADS52x0*** **(SRI)** Version 3.29	**AFI5100** **(IPM)** Version 2.39	**AFO5100** **(OPM)** Version 1.19

ADE5300 **(ERI)** Version 3.63	**AFO5200** **(8IO)** Version 1.09	**ATI5100** **(IAT-020)** Version 2.03	**MFI** Version 1.44

The ERI device supports only OSDP V1.

The DRI, ACC AP (DRIe), MFI and ACC G1/G2 devices support OSDP V2 (OSDP V1 + functions like secure channel encryption, smart card communication and biometric reader support.)

4.9.2 Hardware

4.9.2.1 Controllers

AC5102 ACC-G2	**ACC-AP**	**AC5100** ACC Revision 3 ACC-020	**AC5100** ACC Revision 2 ACC-010
AC5200 SR34i Revision 1	**AC5200** SR35i Revision 1.4	**AC5200** SR35i MkII Revision 2	**Granta Mk3** Revision 1

4.9.2.2 Door Control

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

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

Aperio Hub and Locks

Aperio Hub AH30 FW Ver. 6.6.32718 *	Aperio Lock E100 V3 FW Ver. 3.7.1446 *	Aperio Lock AU100 V3 FW Ver. 3.7.1446 *	Aperio Programming Application Ver. 18.0.4-e617dba **

* The above-mentioned Firmware Versions are tested to work with SiPass integrated, and are not supplied or controlled by Siemens.

**The Aperio Programming Application is not provided by Siemens and ships with Aperio Hub/Lock hardware.

The above list only includes the models tested with this release. SiPass integrated can support other models available in the market but full compatibility cannot be assured till those are also tested specifically.

4.9.2.3 I/O

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

4.10 API / HLI Compatibility

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

4.10.1 HR-API Interface

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

SiPass integrated RESTful HR API has now modified the event names to appropriately describe the event types. This is a breaking change compared to SiPass integrated 2.80 version. For more information, refer RESTful HR API Release Notes in the *RESTful API* folder of the SiPass integrated software bundle.

SiPass integrated implements and recommends high server security which means modification is required for any existing applications that have been built around versions prior to MP 2.70. SiPass integrated MP 2.70 onward requires establishing an authenticated connection to be set up with the HR-API application.

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

4.10.2 Management / Enterprise Station API

SiPass integrated Management Station API (MS-API) allows data to be accessed and maintained from any programming language that supports RESTful web services or COM automation.

To use WCF service during authentication, additional steps are required in the MS-API (DCOM) to configure the certificate for WCF security. For more information, see the *MS API Programmer's Reference Manual* in SiPass integrated software bundle.

The third-party applications integrated with MS API (DCOM), using reference of **Interop.COMClientAPILib.dll** must perform the following steps to make their application work uninterrupted.

4.10.3 OPC A&E Server Interface

SiPass integrated supports OPC A&E version 1.0

4.10.4 SiPass integrated with Siveillance VMS

SiPass integrated MP2.95 can be used as a head end system for **Siemens Siveillance VMS 2023 R2** with **VMS Connector v1.1.2** and **Siemens Siveillance VMS 2023 R2** can be used as a headend system with **SiPass Integrated MP 2.95** using **Siveillance_Video_ACM_SiPass_Integration_4.2.2** plugin.

NOTICE	
!	Siveillance Video supports only live and recorded streams but events and alarms cannot be received by SiPass integrated.

4.11 Video Management System

Siveillance VMS 2023 R2	**Cayuga R13**	**Cayuga R14**

4.12 Directly Connected IP Camera Compatibility

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

4.13 Intrusion Panel Compatibility

Siveillance Intrusion Core CORE-SPC 4000, 5000, 6000	**Intrunet SI 400 series** (Sintony 400)	**SPC 4300, 5300, 6300** Intrusion System

ACC-AP and AC5200 (ACC lite) controller do not work with Sintony 400.

4.14 Network Communication

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

4.15 Communication Encryption among SiPass integrated Components

Component Connection Type	Encryption type
Card to Reader	Dependent on Card and Reader technology. **Note:** ● Encryption also depends on the connection type between the card reader and ACC. For example, *“HID Prox over Wiegand”* has no encryption and can be easily copied. ● Encrypted does not always mean secure. Smart Cards are encrypted but some card technologies may still be vulnerable. For example, in case of *MIFARE Classic*, information about card decryption is available. To know more about other secure encrypted cards, see the information supplied by your reader vendor.
Reader to RIM / Reader to ACC	**Unencrypted**: OSDP V1 and other Reader Interfaces **Encrypted**: OSDP V2
RIM to ACC	**Unencrypted** (Obfuscated for ACC FLN Bus)
ACC to HLI Interface	**Unencrypted**
ACC to Syntony Interface	**Unencrypted**
ACC to SPC Interface	**Encrypted**
ACC to SiPass Server	**Encrypted**
ACC to ACC (Peer-to-Peer)	**Encrypted**
SiPass Server to SQL DB	**No encryption**: Shared Memory Protocol – this is a local connection between two processes
Remote Client to SiPass Server	● Configuration Client: a mix of DCOM / RPC / WCF* ● Operation Client: WCF* * **Certificate Encryption** for WCF
DVR API to SiPass Server	**Unencrypted**: DCOM
OPC Client to SiPass Server	**Unencrypted**: DCOM
MS DCOM and RESTFul API to SiPass server	**Unencrypted** (uses MS DCOM API connection)

Component Connection Type	Encryption type
HR DCOM and RESTFul API to SiPass server	**Unencrypted**: DCOM **Secured http Encryption** between HR RESTful API and SiPass Server (by using the self-signed certificates or certificates from the trusted certificate authorities)
Web site to SiPass server	**Secured http Encryption** between browser and UI, and API of Web Client (by using the self-signed certificates, or certificates from the trusted certificate authorities)

4.16 Modem Compatibility

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

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

4.17 Card Printer Compatibility

Fargo Pro - Series	**Fargo High Definition** **HDP8500, HDP 5000, HDP600, HDP800**

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

For **Fargo HDP8500** card printer, different set of drivers configuration settings are required depending on whether the printer is used for *Local Connection (USB)* or *Network Connection (Ethernet)*.

See the SiPass integrated *Configuration Client User Guide*(Version MP2.76 and later) for setup and configuration of the printer. For troubleshooting information, see the *Troubleshooting* section in SiPass integrated *Installation Guide* (Version MP2.76 and later).

Note

For optimum configuration and operation, HDP5000 printer should not be used as a network port printer.

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. 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.

4.18 Mifare Classic/ DEsfire EV1 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)

HID OMNIKEY 5021	**HID OMNIKEY 5121 (embedded)**

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

4.19 Enrolment Reader Compatibility

4.19.1 USB Enrolment readers

Profile Reader – HID Omnikey 5022	**Profile Reader – HID Omnikey 5422**	**Profile Reader – HID Omnikey 5x21**	**Profile Reader – HID Omnikey 5x27**

The above list includes only the readers that have been tested to work with SiPass integrated MP 2.90. More readers (like the list below) are also supported, however, full compatibility cannot be assured until those are tested specifically.

Bioscript Reader Configuration	**Cerpass Registration Reader**	**Profile Reader - GEMPLUS GCI680**	**Profile Reader - GEMPLUS GEX332**
SALTO Data Configuration	**SiPass Proximity Reader**	**USB Reader Interface – Clock & Data**	**USB Reader Interface – Wiegand**

4.20 Card Format Compatibility

4.20.1 Reader Connection Types

Wiegand	RS-485	Clock & Data

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

4.20.2 Siemens Proprietary Card Formats

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

4.20.3 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

4.20.4 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).

4.21 Card Reader Compatibility

4.21.1 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**
VR10S-MF	**VR40S-MF**	**VR20M-MF** #	**VR50M-MF** #

# See the **Firmware Known Issues** in the *Enhancements and Quality Improvements* document in the SiPass integrated software bundle.

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.

4.21.2 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

4.21.3 HID Readers for Siemens Sites

Form Factor	Low Frequency (125 kHz) Interpreter	High Frequency (13.56 MHz) Interpreter	Communication Protocol	Connection Style	SE Part No.	Description
R10 Series	N	Y	Wiegand	Pig tail	900NWNNEKE00K9	LF OFF, HF STD/SIO/SEOS/MIGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE0527
R10 Series	N	Y	OSDP/RS-485	Pig tail	900NWPNEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R15 Series	N	Y	OSDP/RS-485	Pig tail	910NWPNEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R 40 Series	N	Y	Wiegand	Pig tail	920NWNNEKE00K9	LF OFF, HF SEOS/MIGR, WIEG, PIG, BLACK, HF MIGR PFL EVC00000_ICE0527
R 40 Series	N	Y	OSDP/RS-485	Pig tail	920NWPNEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, PIG, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95ANWPTEKE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, TERM, BLACK, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527
R95A Series	N	Y	OSDP/RS-485	Term	95ANWPTEWE00PJ	LF OFF, HF STD/SIO/SEOS/MIGR, 485HDX, TERM, WHITE, A/V OFF, OSDP V1, HF MIGR PFL EVC00000_ICE0527

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

4.22 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.

4.22.1 Formats supported by All HID Prox Technology

Custom Wiegand	**HID Prox 26 Bit**	**HID Prox Asco 36 Bit**	
HID Prox Corp 1000 35/48 bit	**HID Prox Siemens Encr 52-bit**	**HID Prox Siemens Stg**	
Mifare Csn32	**Mifare Csn40**	**Europlex 34Bit**	**Remec 37Bit**

4.23 TBS 3D Enroll

The following TBS 3D Enrollment USB based device have been tested and verified as working with SiPass integrated Web Client.

Design	Product Number	Model	Description
TBS	053-1000-002	3D Enroll	● Access Control, T&A, Civil ID ● Highest security level ● No “Failure to Enroll” ● Superior image quality ● Nail-to-nail images ● Quality assessment and duplicate check ● Hygienic for sensitive applications ● Touchless,3D-Multiview ● Certifications: CE
TBS	073-1000-002-1-00	2D Enroll	● Optical touch sensor, FBI certified ● Access Control, T&A, Civil ID ● Excellent identification performance ● Small- and medium-sized user groups ● Quality assessment and duplicate check

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

The reader configuration requires installation of drivers.

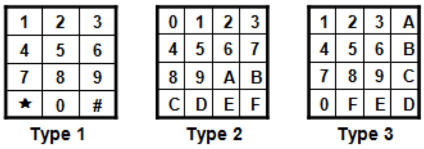
It is not possible to use fingerprint-only as a credential in SiPass integrated.

TBS server holds the fingerprint in its own database that can be retrieved by SiPass integrated web client by the authorized user only.

4.24 Granta MK3 Reader PIN Pad Type Compatibility

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

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



For the 4422 Swipe module and the 4322 Cotag module, the keypad type has to be selected on an extra Key tab during configuration.

The system does not support entry of your own PIN for first-time use.

An External Swipe reader, combined with a keypad, can be configured as an M43 Keypad Type.

4.25 Signature Capture Tablet Compatibility

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

4.26 Messaging System Compatibility

Microsoft Exchange Server 2013 or newer

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

4.27 Server Redundancy

Stratus Technologies EverRunFT

ℹ 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, and is not based on the SiPass services.

4.28 Offline Door System

SALTO SPACE Version 6.8.3.1

ℹ

The SHIP protocol (version 1.35a) 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).

4.29 Identity Management

Siveillance Identity 1.6 SP2

4.30 Virtualization

Citrix XenApp Version 6.0	**Microsoft Windows Server 2022 Terminal Services**	**Microsoft Windows Server 2019 Terminal Services**

ℹ

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

5 SiPass integrated Server, Configuration Client and Operation Client

5.1 Fixed Issues

Vulnerabilities	
Type	**Description**
Server Client	While logging on to the Operation Client and Configuration Client, an error message box pops up if the file **log4j-1.2.12.jar** (which has reached End of Life) is removed from the SiPass installation folder. If you are not using VSS SDK, you can delete either the **log4j-1.2.12.jar** located in “`<InstallationPath>\SiPass integrated\VssSDK\jars`” or the entire folder “`<InstallationPath>\SiPass integrated\VssSDK`”. The video integration functionality is impacted if the file/folder is removed. **Note:** This applies to remote clients as well.

Fixed Issues	
Type	**Description**
Server Client	When Cardholder is updated through HR API, the smartcard profile name is not sent to server. Hence, SmartCardID event gets created after performing update.
Server Client	When Cardholder is updated through HR API, value of restricted visitor field is false by default. Hence, restricted event gets created after performing update.
Server Client	In German Localization package of MP2.90 (DE), Reading the encoded card using proximity enrolment reader displays an error.
Server Client	Currently, SiPass integrated software and hardware supports less than 256KB size of reader firmware download.
Server Client	Currently, in SiPass integrated for localized languages, if demo license is applied, then Siemens Corporate Card tab is visible.
Server Client	Database restore is not successful when SiPass integrated web client is installed separately after installing SiPass integrated server. Also, if user stops and starts the SiPass Server manually, all the services related to SiPass integrated web client are not started automatically.
Server Client	The following issues have been reported: ● The maximum password age set for the operator does not expire in the Operation Client and does not prompt to change the password after expiry. ● The password changed after expiry does not reflect in the Configuration Client.
Server Client	In Operation Client, error is displayed when user tries to add reporting actions to pre-defined Reports after database restore.

Fixed Issues	
Type	**Description**
Server Client	During Database restore, the restore progress bar percentage is not completed and getting struck in Configuration Client GUI.
Server Client	Backup file generated via HBET does not have all necessary data related to custom pages. Due to this Cardholder/Visitor form does not load after database restore.
Server Client	System Events are reported to SiPass integrated Live Audit Trail window but are not stored in the database. This issue can be observed in below scenarios: ● RabbitMQ Queue creation failure on first SiPass Server startup after installation. System events are lost. ● RabbitMQ Queue connection failure on SiPass Server startup. System Events are buffered inside the queue until a successful connection is established (restart of SiPass Server PC is required) and then system events are pushed to the database. In the SiPass system, architectural changes have been made to acknowledge events synchronously in the RabbitMQ to address the data loss.
Server Client	In some cases, if you send a command to disable the "REX" input point after it has already been disabled because of a "Block door" command sent prior, the status of the input point changes to "Unknown".
Server Client	The license expiration is displayed wrong in the Status Bar dialog of the SiPass integrated Configuration Client and SiPass integrated Operation Client. The license expiry date displays the current date.
Server Client	In SiPass Configuration Client, the custom color option is not working in the “Card Template” configuration and not available on the toolbar.
Server Client	SiPass integrated is now enhanced to support private key as input file, when a certificate does not have a private key associated with it or does not have exportable private key enabled by default.
Server Client	"Pager Number" format validation is removed. You may enter up to 16 characters, in any combination of upper-case and lower-case letters and numbers.
Server Client	Audit Trial Archive was not generated for the current day when triggered manually from SiPass integrated Configuration Client. After applying the patch, manual trigger of audit trial archive will archive the available audit trials till current day in the configured path.
Server Client	Previous Hotfix installer does not validate the rights to execute PowerShell script/command script/batch file and Hotfix installation is incomplete. Hotfix installer validates the rights to execute PowerShell script/command script/ batch file and if rights are not present error message displays "Installation is aborted. Batch file/Command Prompt/PowerShell execution is restricted/disabled. Please check the logs for further information." and installation does not proceed.

Fixed Issues	
Type	**Description**
Server Client	SiPass integrated Configuration Client fails to take backup when the database size is larger than 4 GB.
Server Client	User is unable to perform backup of the database in SiPass integrated due to excess custom fields and entity records created during Update Cardholder through SiPass integrated HR RESTful API.
Server Client	After initializing the controller, Cardholder is getting access to few unconfigured floors. During initializing the controller, while downloading access level, only points corresponding to the controller are downloaded.
Server Client	When creating/updating a cardholder with the Data-Synchronizer/Import-Export tool, the “Key Revalidation” value is not synchronized between SiPass integrated and SALTO system.
Server Client	If more than 4000 characters are entered in the User Name field in the SiPass integrated Configuration Client login page, then SiPass integrated Configuration Client, SiPass Management Station API service and SiPass Server service crashes.
Server Client	Whenever RabbitMQ service crashes, SiPass server service is stopped immediately, and event acknowledgement is not sent to the controller to prevent data loss.
Server Client	Host Based Event Tasks (HBET) configured/last modified by an operator is not triggering event if the operator has been deleted and SiPass integrated Server is restarted.
Server Client	Messages are stuck in RabbitMQ queue and events are not reported to **SiPass integrated Live Audit Trail** window and External Event Queue.
Server Client	The following issues are reported in the SiPass integrated system: ● Alarms are reported in SiPass integrated system even though there is a schedule on the point to ignore alarms. ● Alarms are reported in SiPass integrated system in Intrusion Zones which are disarmed. ● Points which are always monitored are reporting in the Audit Trail but are not always showing a pop-up message and/or reporting into the Alarm Queue.
Server Client	After initialization of the controller, access is denied to the cardholder for the point which has been assigned after 65535 points.
Server Client	Cardholder allowed access where no access was given. Access Granted for unassigned readers & Access Denied for assigned readers.
Server Client	When OSS-SO Access group (containing Access Level which has point group configured to it) is assigned to cardholder / removed from cardholder, update was not to the controller on cardholder **Save** operation.

Fixed Issues	
Type	**Description**
Server Client	In SiPass integrated Operation Client, during report generation if the search result has more than one page, second page result is not loaded.
Server Client	When operator with limited admin rights tries to open **Cardholder** details in the Operation Client, it throws an error message and crashes.

5.2 Known Issues and Limitations

- The Siveillance VMS Connector v1.1.1 to SiPass connection does not work if VMS is using a certificate. Hence, it is recommended that DVR API connection should NOT use any certificates.
- After restoring the SiPass integrated database, the Cardholder cannot be searched by the **ManagerEmailAddress** field value. To resolve, open the report to refresh the data after which, the search can be performed with this value.
- After a point name change, Alarm Acknowledgments in the Audit Trail still show the old name. A service restart is required for normal operation.
- Changes made to alarm instructions made from the SiPass server when the client is NOT connected are not updated in the Client even after it is connected (logged-in) the next time. Hence, it is recommended to edit the alarms when the Server and client are online (connected).
- Some SiPass integrated files occasionally show false-positive results with some anti-virus scanner products. At the time of writing, the *SiPassConfigurationClient.exe* file is flagged as ‘*Unsafe*’ by the “Cylance” anti-virus product. However, several other known anti-virus vendors have cleared this file during their scans.
- In the SiPass integrated Data Synchronizer Tool & Import Export Tool, Cardholder must be imported with any one of the defined workgroups else the workgroup will be updated as **<None>**.
- SiPass integrated does not accept the special character “-“ (hypen) if it is included in the NetBIOS name. For example, siemens-lan.

5.2.1 SiPass integrated Firmware

- **In case of upgrade from SiPass integrated MP2.76 to MP2.76 SP1 or later:** If the UID card technology was used for APERIO Locks with ACC Version 2.76.14 and **UID Reverse Byte Order** configuration option was enabled, the **UID Reverse Byte Order** configuration option MUST BE DISABLED when upgrading to a later version of the ACC firmware.
- ACC-AP does not support a few types of Wiegand readers:
  - AR6111 MX is known to be NOT working
  - **Recommended**: HID Wiegand readers
- VR20M-MF and VR50M-MF reader firmware older than version 2.002.000 cannot be downloaded via SiPass integrated. The issue may get resolved by the reader manufacturer in Firmware version 2.002.000 onward.
- VR20M-MF and VR50M-MF reader firmware older then version 2.002.000 had incompatibility issues with SiPass integrated. The issue has been resolved by the reader manufacturer in Firmware version 2.002.000 onward.
- PHG reader firmware download only works at 9600 baud.
- PHG readers can have their address set either by DIP switch or by OSDP command. If it set by the DIP switch, the address cannot be changed from the ACC (despite a message that it was changed).

5.2.2 Configuration Client - Card Template

User cannot choose a custom color while creating **Card Template, Site Plan** and **Drawing** in SiPass integrated Configuration Client.

6 SiPass integrated Web Client

6.1 Fixed Issues

Fixed Issues	
Type	**Description**
Web Client	The Authentication endpoint of SiPass integrated Web UI API can only be invoked by the SiPass integrated external operator. After applying this patch, the restriction was removed so that the default operators containing cardholder privileges can invoke.
Web Client	In SiPass integrated Web Client, it is not possible to delete Cardholders. An internal server error is displayed.

6.2 Known Issues and Limitations

6.2.1 Known General Issues

Common for All Applications

1. In the dialog box, on selecting the access objects checkbox, the list refreshes.
2. In the **Combo** box, the default value **Please select a value** does not display randomly.
3. The **Close** button is not translated in the configuration screen.

6.2.2 Known Issues for Live Alarm

1. The field **Time** cannot be searched through the quick search or extended search option.
2. In **Extended Search**, when user searches Alarm Date Time/Date/Time fields with incorrect format, a validation message **Date/Time format is incorrect and should be in <Date Time format**> displays twice. In addition, the user will still be allowed to search the Alarm Date Time/Date/Time, even when the validation message box is still visible in the screen.
3. While acknowledging the Alarms, the following error **String was not recognized as a valid Date Time** displays**.**

6.2.3 Known Issues for Cardholder/Visitor Application

1. In the **Detailed** View,
   – the chevron button near the tabs does not work all the times.
2. While scrolling down the Cardholder list, randomly, the records display for half a page.
3. When the application is logged in through other languages except English, the field Status cannot be searched through the quick search or extended search options.
4. In **Extended Search**, when user searches **Start Date/End Date** fields with incorrect format, a validation message **Date format is incorrect and should be in <Date Time format>** displays twice. In addition, the user will still be allowed to search the **Start Date/End Date**, even when the validation message box is still visible in the screen.

6.2.4 Known Issues for Page Customization

1. 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.
2. During database restore, the remaining fields **Reason for Visit, Profile, and License of the Visitor Details** tab gets displayed in the **Extended Controls** tab**.**
3. **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 for Venue Booking

1. 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**.
2. 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.
3. 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.
4. While creating a venue booking with recurrence option, at times, the list view does not get refreshed automatically.
5. Irrespective of the languages chosen while logging in the client, if user changes the default Time Zone, the date time search does not work for **Venue Booking**.
6. In **Reccurrence Booking**, the End by calendar control goes beyond the selection and does not allow the user to select the date. This issue occurs in smaller screen, for e.g. laptop view.
7. In **Extended Search**, when user searches **From/To** fields with incorrect format, a validation message **Date/Time format is incorrect and should be in <Date Time format>** displays twice. In addition, the user will still be allowed to search the From/To fields, even when the validation message box is still visible in the screen.
8. 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.

6.2.6 Known Issues for Localization

Common for All Languages

1. In **About** application, the text **Version** is not localized.
2. Alarm Date Time field search does not work.
3. While accessing the application in the localized languages, at times, the length of the contents in the controls are overlapped over other controls and does not allow the user to perform a particular operation.
4. In the **Cardholder** application,

   - under the **Definition** tab, the **Cardholder Attributes' Status** field is displayed as **Unknown** and not localized.
   - under the **Printing** tab, the **Demo** value of the **Card Template** field is not localized.
5. The **Tool tip** and the **Close** button of the **Settings icon** are not localized.
6. When the application is logged in through other languages except English, the field AlarmStatus cannot be searched through the quick search and extended search option.

Russian

1. The **Access Object** grid overlaps the **Cardholder Attributes**.
2. In **Venue Configuration**, on the detailed page, the word **Details Loading** is not localized.

Dutch

1. In the **Access Level** application,
   - the word *records* in the **No matching records found** text is not localized.
   - on the detailed page, the word **Details Loading** is not localized.
2. In the **Alarm Handling** page, under the **Settings** button, the **Status** option of the **Sorting field** List/ Table configuration is not localized.
3. In the **Visitor Management** tab, under the visitor cardholder information section, the Select cardholder and Remove cardholder are not fully displayed, because the size of the button is small.
4. In **About** application, the text **Version** is not localized.

Italian

1. In the **Manual Override** application, under the tree view, the **Flag** and **Area Anti-Passback** are not localized.

6.2.7 Limitations

1. In SiPass integrated web client, **OSS-SO** feature is not supported.
2. In **Cardholder, Visitor, VenueBooking,** and **Alarm** application's **Quick** and **Advanced Search**, the date and time field works based on the **equal to** logic.
3. In any application, while performing the **Quick Search** using date time field, validation is performed only if the search input length matches or exceeds the date format length. However, when the **Quick Search** is performed with incorrect date/date time format, an error message is displayed as **Incorrect format in field <DateTime field>. Expected format <DateTime format>.**
4. 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.
5. 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.
6. 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.
7. While enabling secure communication for RabbitMQ, if the private key file is unavailable, self-sign certificate must be consumed. Refer *Enabling the Secure*

Communication for RabbitMQ section in the **SiPass integrated Installation Guide.**

8. SiID version 1.5 and SiPass version MP 2.85 compatibility is no more supported for single machine or co-existence installation.

Venue Booking

1. Only the Bookings from **30 days** prior to the current date and time displays.
2. 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.
3. 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.
4. While creating/editing a venue booking with recurrence option, the first item of the list view will be selected, whereas in single booking (occurrence) option, the saved record will be selected**.**
5. 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.

Extended Controls

1. When the data type of custom field textbox control is configured as **Numeric** in the SiPass Configuration client and if user tries to enter alphabets in the text box field, an error message as **Internal server error** displays. This error message is also applicable for **Cardholder** and **Visitor** applications.

Cardholder

1. In the List View, the card number displays only when it is configured for the Base profile.
2. If the card number is selected in the sorting field, the sorting order is applied for the card numbers with Base Credential Profile.
3. Manual commands are not working as expected. [RC1]

Manual Override

1. Manual commands such as **Cancel Isolate, Cancel Permanent Action,Clear Alarm,Isolate,Pulse,Return to Time Schedule Control,Secure (Enable),Set state Alarm,Set state Normal** and **Unsecure (Disable)** are not supported by **MFI Tamper Input**.

⚠ **WARNING**	
⚠	Manual Commands support on the MFI Tamper Input are not suppressed explicitly, hence executing manual command is possible and it shall cause unnecessary modifications to the existing input state.

7 DesigoCC Integration

Integration between SiPass integrated and DesigoCC has now become more secure and convenient. Users can now be seamlessly be authenticated across the integration from DesigoCC in SiPass integrated using enhancements that have been made to the applicable APIs. Users in DesigoCC can be traced and audited inside the SiPass integrated system, which is then compliant with the necessary privacy and security guidelines required for the European and wider global markets.

In addition to the user authentication enhancements, it is also possible to integrate the two systems easily with the additional functionality available with Siemens LMS. This means that once DesigoCC has been extended to include external points, SiPass integrated will see this in the associated LMS server and enable the integration services. This automation offers convenience, cost savings and reliability for those customers who wish to have an integrated BMS and security system.

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