SIEMENS

Access Control

SiPass integrated

Web Client User Guide

MP 2.80

A6V10655077

2020-09-07

Smart Infrastructure

Table of Contents

Copyright

Edition: 2020-09-07

Document ID: A6V10655077

1 About this Guide

This guide provides an overview of SiPass integrated Web Client. Also, the document provides detailed information that is required for the user to use the SiPass integrated Web Client on a day-to-day basis.

Objective

The objective of this document is to teach the operator/user the various processes involved in working with the SiPass integrated Web Client.

2 Safety

2.1 Target Readers

This document provides instructions for the following target groups:

Target readers	Qualification	Activity	Condition of the product
Operational startup personnel	Technical training for electrical installations. Training on the product is necessary.	Places the product into operation for the first time or changes the existing configuration.	The product is installed but not yet configured, or the existing configuration is to be changed.
Service personnel	Technical training for electrical installations and software installation.	Checks the product at regular intervals to ensure good working order, to service the device or system and to repair or expand and upgrade the system.	The product is already in use and requires servicing.

2.2 Work Safety Information

- Follow all instructions in this guide.
- Keep this document for reference.
- Always include this document with the product.

Data Loss after Software Update

Make sure to backup all data before updating the software.

2.3 Meaning of the Symbols

Tips and Information

NOTICE

Malfunctioning or data loss may result

⚠ WARNING

Indicates information on situations that may occur, which might affect safe operation, and contains recommended measures

3 Document Updates after Previous Release

SiPass integrated MP 2.8

Section	Details
Login [→ 10]	SiPass integrated can now be purchased for a certain period of time after which, the subscription must be renewed for continuous services. Login screen is now enhanced with Demo period and Subscription period notifications
Cardholders [→ 22]	The **Biometric Enrollment** is now enhanced to support a new device type, **Terminal Enroll**. **Terminal Enroll** caters to the following: 3D touchless technology, 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, Identification for large databases, and Hygienic for sensitive applications.
Preferences [→ 68]	A provision to configure **TBS Server** is now introduced in the Preferences application.
Manual Override [→ 49]	Manual Commands that are not supported for MFI Tamper Input are listed.

See also

Document Updates after Previous Release [→ 8]

4 Introduction

SiPass integrated Web Client provides a rich and vibrant web client interface built on the SiShell framework to manage the entire application processes such as: **Cardholder, Venue Booking, Visitor, Live Alarms, Activity Feed, Area Monitoring** and **Manual Override** and configuration processes such as: **Access level, Access group, Venue Configuration, Preferences** and **Credential Design.**

The SiPass integrated Web Client has the capability to perform the following operations such as: **Create, Read, Update,** and **Delete (CRUD)** on the **Cardholder, Access Level, Access Groups, Venues,** and **Venue Booking** applications through a valid SiPass integrated operator credential.

User needs to define the operator rights in the SiPass integrated server application and based on the defined operator rights the fields are displayed.

Other framework operations such as **Quick search, Saved search, Extended search, and Pinning** can be performed by any end user.

The above mentioned applications are explained in detail in the relevant sections.

5 Logging on to SiPass integrated Web Client

Only the Operators who are configured / created in the application can log on to the SiPass integrated Web Client. User cannot create new operators through the SiPass integrated Web Client.

Perform the following steps to log on to SiPass integrated Web Client:

1. Enter the SiPass integrated Web Client **URL** on the browser and press Enter key.
   – or…
2. Click **Start menu > SiPass integrated Web Client**
   ⇨ The **Login** screen displays.

!	*NOTICE*
	As part of the installation process, in the server machine where SiPass integrated web client is installed, the SiPass integrated web client shortcut icon is made available in the **Start** menu. In Switch View, the controls in the Table/List configuration are not completely visible in smaller screen, for e.g. laptop view.

3. Enter the **Username**.
4. Enter the **Password**.
5. Select the **Language** from the drop-down list.
6. Click **Login**.
   ⇨ The Home screen of the SiPass integrated Web Client displays in the selected language.

The following **Languages** and **Date / Time / DateTime formats** are supported in the SiPass integrated Web Client, even though the SiPass integrated server has its own date time settings.

S No	Language	Date Format	Sample	Time Format	Sample	Date Time Format	Sample
1	English	MM/dd/yyyy	04/27/2018	h:mm a	5:30 PM	MM/dd/yyyy h:mm a	04/27/2018 5:30 PM
2	French	dd/MM/yyyy	27/04/2018	HH:mm	17:30	dd/MM/yyyy HH:mm	27/04/2018 17:30
3	Deutsch	dd.MM.yyyy	27.04.2018	HH:mm	17:30	dd.MM.yyyy HH:mm	27.04.2018 17:30
4	Dutch	dd-MM-yyyy	27-04-2018	HH:mm	17:30	dd-MM-yyyy HH:mm	27-04-2018 17:30
5	Italian	dd/MM/yyyy	27/04/2018	HH:mm	17:30	dd/MM/yyyy HH:mm	27/04/2018 17:30
6	Russian	dd.MM.yyyy	27.04.2018	H:mm	17:30	dd.MM.yyyy H:mm	27.04.2018 17:30
7	Chinese (Simplified)	yyyy/M/d	2018/4/27	H:mm	17:30	yyyy/M/d H:mm	2018/4/27 17:30
8	Chinese (Traditional)	yyyy/M/d	2018/4/27	H:mm	17:30	yyyy/M/d H:mm	2018/4/27 17:30

S No	Language	Date Format	Sample	Time Format	Sample	Date Time Format	Sample
9	Czech	dd.MM.yyyy	27.04.2018	HH:mm	17:30	dd.MM.yyyy HH:mm	27.04.2018 17:30
10	Polish	yyyy-MM-dd	2018-04-27	HH:mm	17:30	yyyy-MM-dd HH:mm	2018-04-27 17:30
11	Finnish	dd.MM.yyyy	27.04.2018	HH:mm	17:30	dd.MM.yyyy HH:mm	27.04.2018 17:30
12	Spanish	dd/MM/yyyy	27/04/2018	HH:mm	17.30	dd/MM/yyyy HH:mm	27/04/2018 17.30

The Alarm Date Time field will display in the following format : **MM/dd/yyyy HH:mm:ss**

Date field will display in the following format: **MM/dd/yyyy**

Time field will display in the following format: **h:mm:ss a**

User Scenarios	Notification Message
SiPass integrated - Demo License	• If the Operator accesses the SiPass integrated web client using Demo License, a message on the notification bar will be continuously displayed as: **SiPass integrated Web Client is running using Demo License**, throughout the demo period.
SiPass integrated - Software Subscription	• A subscription expiration notification message is displayed as **Software Update Subscription expires on <Date>** in the SiPass integrated web application notification bar, 7 days before subscription expiration, to let the user know that the subscriptions are about to expire. • A subscription expired notification message is displayed as **Software Update Subscription has expired on <Date>** in the SiPass integrated web application notification bar after the subscription is expired.
SiPass integrated - Certificate Expiry	• During login, if SiPass integrated web client certificate is expired, a message will be notified as: SiPass: 'SiPass integrated server certificate validity expired' in the SiPass integrated web application. In addition, it does not allow the user to login. • During middle of any operation, if SiPass integrated web client certificate is expired, the same message is notified as above. In this case, the user has to logout of the application. • During login, an expiration notification message is displayed in the SiPass integrated web application - notification bar, 7 days before expiration, to let the user know that the specific certificates are about to expire.**'SiPass integrated server certificate validity going to expire on <Date Time>'. Please contact Administrator. Incase left unattended, then user cannot login to web client.**
neXus	• For neXus, no message will be notified for neXus certificate expiry and going to expire.
IIS	• For IIS, if a separate certificate is installed other than the SiPass integrated web client certificate, no message will be notified for certificate expiration.

6 Design and Navigation

Design and Navigation section details the design of the SiPass integrated Web Client and assists the user in navigating within the application. The SiPass integrated Web Client is created with various applications and widgets.

6.1 Home Screen

The Home screen is the entry point for the SiPass integrated Web Client and contains launching widgets and deep links directly to pin the application contents.

The following widgets are available on the **Home** screen:

Operation

- Live Alarms
- Activity Feed
- Cardholder
- Venue Booking
- Visitor
- Area Monitoring
- Manual Override

Configuration

- Access Level
- Access Group
- Venue Configuration
- Credential Design
- Preferences
- About

6.2 Toolbar

The main toolbar contains the following action icons, which are common for all the applications:

Home Screen Icon

The **Navigate to Home screen** icon enables the user to navigate to the Home screen.

Operator / User Name Icon

The **Operator / User Name** icon, which is at the top right corner of the toolbar, displays the name of the operator/username, who has logged in to the application.

Logout button

1. Click the **Operator / User Name** on the Tool bar.
   ⇨ The Logout dialog window displays.
2. Click **Log Out** to exit the application.
   – or…
3. Click **Cancel** to remain in the same screen.

!	*NOTICE*
	If the user clicks **Cancel,** the user has to manually close the Logout window.

⇨ Logging out from the SiPass integrated Web Client is complete.

Context Sensitive Help Icon

The Context Sensitive Help Icon is a shortcut help file icon that provides information about the fields that are displayed in the application. If the user needs more specific and targeted help to a single field displayed on the screen, the user can view the **Element Sensitive Help,** which provides information in a very fast and efficient way.

Full Screen Icon

The Full Screen Icon opens the full screen mode of the application.

Icons on the Tool bar

The below mentioned icons are usable by the following applications: **Cardholder, Venue Booking, Visitor, Access Levels, Access Group, Venue Configuration, and Credential Design**.

Pinning Icon

The pinning feature which is operator based creates deep links to the application content for quick access from the Home screen.

Apart from the **Live Alarm** and **Manual Override** application, the pinning feature is available for all the applications. User can choose the modules to pin to the Home screen. Pinning is of two types:

- Tree View Pinning
- List View Pinning

Tree View Pinning

User can pin the items available in the Tree View to the Home screen.

1. Select the required item that has to be pinned to the Home screen from the Tree View.
2. Click the **Pinning** icon.
   ⇨ The **Pin to Home Screen** dialog box opens.
3. Select the item to be pinned to the Home screen.
4. Enter the **Widget Name**.
5. Select the **Group** under which the selected item has to be pinned.
6. Select the required **widget Size**. The available options are:

- Small
- Medium
- Large

7. Click **Pin to Home Screen** button to pin the selected item.
   – or...
8. Click **Cancel** to cancel the pinning process.

!	*NOTICE*
	The default image displays in the Home screen.

List View Pinning

The List View pinning process is similar to the Tree View pinning process. Refer to the **Tree View Pinning** section for more details on pinning process. The image assigned to that particular item in the List View will be displayed in the widget pinned to the Home screen.

The Pinning feature is an operator-based feature that if an operator pins an item, the item will be visible only for that particular operator.

User can pin the items available in the list view to the Home screen.

- ◈ Select the required item to be pinned in the Home screen from the List view.
- ⇨ The pinning process is complete.

Unpin in Home Screen

The user can unpin the pinned widget from the Home Screen.

1. Click **Edit** button on the Home screen.
2. Select the check box of the required widget to be unpinned from the Home screen.
3. Click **Unpin** button.
4. Click **Save** to save the modified details.
   - or...
5. Click **Cancel** to cancel the editing process.

⇨ The Unpin process is complete.

!	*NOTICE*
	If a pinned item is deleted in the List View, the user has to manually delete the corresponding widget from the Home screen. When the Cardholder, Visitor, Venue Configuration, Access, or Access Groups is deleted and is no longer available, and if user clicks on any of the deleted widget on the home screen, a message displays as **[Application Name] Not Found** e.g. Cardholder Not found.

Multiselect

The Multiselect icon which is in the List view grid is used only to select multiple items and delete (i.e.) while selecting multiple records using the multiselect icon, only the **Delete** button is enabled; the **Add** and **Edit** buttons are disabled.

1. Click the **Multiselect** icon.
   ⇨ The **Select All** and **Deselect All** buttons will be enabled at the bottom.
2. Click **Select All** to select all the available items.
   - or…
3. Click **Deselect All** to deselect all the selected items.
   ⇨ Mutliselecting an item is complete.

Quick Search

The **Quick Search** enables the user to perform quick search in the List view. The Quick search + filter rows search Type is a framework feature that is selected by default.

The search displays the results based on the **Contains logic** in the first parameter of the 1st line field in the **View** screen.

User can also search with special characters that are available in the first parameter. The quick search will be like a fuzzy search and it does not support the following special characters **[**,and **%**.

If the entered item is not available a message **No data available in the table** displays.

- Enter the search critera in the **Search** field.

⇨ The search results displays based on the entered text.

During **Quick Search** or **Advanced Search**, the **Status** field of the **Cardholder/Visitor** application can be searched, only by using **equal to** logic.

Advanced Search

The **Advanced Search** is based on the available fields provided in the Configuration screen.

The Advance Search is available when the list view is expanded. Two filter rows are available for performing the search. The entered filters cannot be saved.

1. In the first filter row, enter the **contains** criteria.
2. In the second row, enter the **not contains** criteria.
3. Press **Enter** key to perform the search.

⇨ The search results displays based on the entered text.

Reset Filter

Reset Filter button is used to clear/reset the entered search text from the **First Name =** or **Last Name =** or **First Name ≠** or **Last Name ≠** in the extended list column.

To reset an entered search text:

For e.g. Assuming user has entered the **First Name** as **Test**.

1. In the **Advanced search view**, click the down arrow adjacent to the **Last Name** column.
   ⇨ **Reset Filter** button displays along with the **Saved Search** button below the **Last Name** column.
2. Click the **Reset Filter** button.
   ⇨ The entered text **Test** is cleared from the **First Name** field.

Saved Search

Saved Search which is operator based is used to save the entered search criteria in the extended list. Saved Search functionality is applicable only for the following applications: **Cardholder, Venue Booking, Live Alarms** and **Visitor**.

1. Enter a **Search** criterion in the extended list.
2. Press **Enter** key to search the records.
3. Click **Saved Search** button.
   ⇨ The **Save Filter** dialog box opens.
4. Enter the preferred **Filter Title**.

!	*NOTICE*
	User can enter up to 30 characters in the **Filter Title** field. If user enters more than 30 characters, an alert message **Filter name length should not be more than 30 characters** displays.

5. Click **Save** to save the Saved Search.
   ⇨ The saved search item gets listed based on the selected category.
   – or…
6. Click **Cancel** to cancel the process.

!	*NOTICE*
	The Saved Search which is also Operator based can be pinned to the home screen to navigate to the records directly. The Search control in the dialog boxes are based on the Name of the listed objects.

Switch View Icon

The **Switch View** comprises of two views: **List view** and **Table view**.

List view, (before expanding the **Configuration settings**) displays the simple search view. Table View (before expanding the **Configuration settings**) displays the advanced search view.

However, after expanding the **Configuration settings,** the list view displays the data fields that are required for defining the **Simple search view**, whereas the table view displays the data fields that are required for defining the **Advanced search view**.

The configuration settings made through a particular operator login are visible only for that particular operator.

List View

1. Click the **Switch View** icon.
   ⇨ The **Switch View** dialog box opens.
2. Click the **List** view tab to define the **Simple search view**.
3. Click the **Configuration** drop down arrow to view and enter the fields.
4. Select the **First Line** field from the dropdown list.
   ⇨ The selected field displays as the first record of the list view. The default value is **First Name**.

!	*NOTICE*
	The values displayed in the dropdown list varies depending on the application selected.

5. Click the **+** symbol to include an additional field to the first line.
6. Select the **Delimiter** from the dropdown list.

i	The delimiters are separators that are used in between the words. For example, comma (,), slash (/), colon (:), semicolon (;), hyphen (-) and space. The default delimiter is space ( ).

7. Select the required field from the dropdown list.
   ⇨ The selected field displays as the second data in the first line. The default value is **Last Name**.
8. Repeat the same steps for the **Second line** field. The default value is **Employee Number**.
9. Select the **Sorting Field** from the dropdown list.
   ⇨ Ascending order displays by default.

!	*NOTICE*
	The sorting in the **Simple Search View** is based on the selected field in the Sorting Field. For e.g., if the employee number is selected as sorting criteria, in the **Cardholder / Visitor** applications, the employee numbers are sorted as follows: 100F000KK 250 50FGERWS AWE21001 SR934787

10. Select the required option from the **Sorting Order** field. The available options are:

- Ascending
- Descending

11. Click **Save** to save the configuration details.
    – or...
12. Click **Cancel** to cancel the current operation.

⇨ The Configuration process for the **Simple Search View** is complete.

Table View

The **Advanced Search View** is based on the fields selected in the Configuration Settings screen.

1. Click the **Table** view tab to define the **Advanced Search View**.
2. Click the **Configuration** drop down arrow to view and enter the fields.
3. In the **Columns** section, select the fields that are required for advanced search.
4. Click **Move Up** and **Move Down** button to define the order in which the **Advanced Search** needs to be displayed.
5. Select the **Sorting Field** from the dropdown list.

!	*NOTICE*
	The sorting in the **Table View** will be based on the field selected in the Sorting Field.

6. Select the required option from the **Sorting Order**. The available options are:

- Ascending
- Descending

7. Click **Save** to save the configuration details.

– or...

8. Click **Cancel** to cancel the current process.

⇨ The Configuration process for the **Advanced Search View** is complete.

Screen Design

The main screen of the application comprises of three grids: **Tree View**, **Simple and Extended View** and the **Detailed View.**

User can expand/toggle/re-size the **Tree View**, **Simple and Extended View** and the **Detailed View**.

For e.g. User expands the **Extended View** to save a search criteria and inbetween the activity if user clicks **Home** page (to view/perform any activity), the system redirects the user to the home page.

After performing the activity in the Home page, if user intents to resume back to the previous screen (to continue with the same activity), the application still maintains the page state as how the user has left it while working with the search criteria.

- Left side of the main screen is the **Tree View.** The tree view displays the list of available menus and submenus for that particular module.
- Middle portion of the main screen is the **Simple and Extended View.** The simple and extended view displays the list of selected submenus.

For e.g. The image of the Cardholder / Visitor application displays if the images are configured in the SiPass integrated Server. The images cannot be added through the web client. The change in image made in the SiPass integrated Server will get updated in the web client also.

- Right side of the main screen is the **Detailed View**. The detailed view displays the details of the selected item from the list view. In the **Detailed View**, even though user selects multiple records, only the last selected record is displayed.

7 Activity Feed

Activity Feed application is only for viewing all the messages from the SiPass integrated server. All messages appear in blue color.

The **Activity Feed** is available only for users who have logged in as an Administrator.

User needs to click the activity feed to know if any event has taken place, for example, adding a cardholder. The recent messages are listed first in descending order based on the date.

User can search the activity feed based on the following fields, except the **Date/Time at Source** & **Recorded Date/Time** fields.

Table explaining the detailed view of an event:

Number	
1	**Title** Displays the title of the message. For e.g. Log on/Log off, Database action and so on.
2	**Location** Displays the location where the event has taken place.
3	**Identity Name**: Displays Cardholder First Name and Last Name.
4	**Severity:** By default, it is categorized as information for all the event types including Alarms. To view the triggered alarm, choose the Alarms from the category section.
5	**Date/Time at Source**: Displays Date/Time of the event generated in the physical location.
6	**Recorded Date/Time**: Displays Date/Time of the event recorded in the Activity Feed.
7	**Subsystem:** Displays the name of the subsystem. By default it is displayed as SiPass integrated append with host name. For example: SiPass integrated - md1wp4rc
8	**Origin**: Displays the server name of the message originating from.
9	**Text:** Displays the detailed information relevant to the event.

If the SiPass Operator name is created as ‘Admin’ from the SiPass integrated system, the operators cannot be synced with UAA. Further, if user tries to access the SiPass web client, the Activity Feed application will be unavailable.

Activity Feed supports only English and German languages.

8 Live Alarms

The **Live Alarm** widget displays all the Alarms raised from SiPass integrated web client. The colors displayed in the list view are only for readability and does not signify the priority of the alarm. This section is classified under three categories:

- **Total Alarm:** Displays the total alarm counts.
- **High:** Displays high priority alarm counts.
- **Other:** Displays the alarm counts that are other than high priority.**Live Alarm** widget enables the user to view the list of live and outstanding alarms.

To view the alarms:

1. Click **Live Alarms**.
   ⇨ The **All Alarms** category displays the operator specific alarms in the tree view. The recent activity displays first in the list of the live alarm widget.

!	*NOTICE*
	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.

The Configuration icon is used to define how the alarm list needs to be displayed. Perform the indicated operations in the Configuration dialog box:

2. Choose the **First line** and **Second line** from the dropdown list box. The available options are: Current State, Location, Priority Description, Alarm Date Time, Date, Time, and Status.
3. Choose the **Sorting Field** from the dropdown list box. The available options are explained below:

Field	Description
Current State	Lists the alarms based on the description.
Location	Lists the alarms based on the alarm location.
Priority Description	Lists the alarms based on the priority description.
Alarm Date Time	Lists the alarm date and time.
Date	Lists the alarms based on the date.
Time	Lists the alarms based on the time.
Status	Lists the alarms based on the status.

4. Choose **Sorting Order** as **Ascending** or **Descending**.
5. Click **Save** to save the settings.
   ⇨ The settings are saved.

Alarm Information

The alarm information section displays the following information: **Current State, Location, Priority Description, Alarm Date Time, Date, Time** and **Status.**

Alarm Display

The **Alarm Display** section is where the alarms are acknowledged. This section holds a list of Predefined Alarm Responses.

To acknowledge an Alarm:

1. Choose a message from the list of **Predefined Alarm Response**.

2. Click **Add Response** button, the chosen predefined alarm response gets added to the **Log of Action item** textbox.

   – or…

3. Enter a message in **Log of Action item** textbox.
4. Click the **Action** button.

⇨ The alarm gets acknowledged.

Based on the acknowledgement, the alarm status is changed or removed from the list.

5. Click **Instructions>>** button to view the instruction file.

⇨ The Alarm display is complete.

!	*NOTICE*
	Alarm acknowledgement action will not happen when Alarm state is in **Alarm waiting for Normal** and **Alarm Actioned**.

Alarm Handling

User can duplicate a current browser tab where the live alarms are listed. The below explained scenarios on duplication are applicable only for **Chrome** and **Firefox**.

Following are the sequences in which the Alarms are handled:

For E.g.

While using the Google chrome window (A) for browsing the SiPass integrated web client, if user tries to open a duplicate tab (B) in the same window - subscription will be lost, resulting which the alarms will not be updated in window (A), until the user clicks the home button or refreshes the browser tab.

When user tries to open a new chrome browser window (C) - subscription will be lost, resulting which the alarm will not be updated in window (A) and duplicate tab (B), until the user clicks home button or refreshes the browser tab.

When user tries to open a new incognito (D) window - subscription will be retained, resulting which the alarm will be updated in the window A OR B or C and D.

When user tries to open a new Firefox browser (E) window - subscription will be retained, resulting which the alarms will be updated in A OR B OR C and D and E.

9 Cardholder

The SiPass integrated Web Client allows the user to configure a new cardholder information into the SiPass integrated server system and the records get updated when the related configuration is changed.

Once the information about a cardholder has been entered and access privileges associated, those cardholders can access the premises (depending on the access privileges) which can be monitored and controlled.

1. Click on the **Cardholder** widget.
   ⇨ The Cardholder main screen is displayed.

The user can view the following menus and submenus of Cardholder:

- Cardholders
  - All Cardholders
  - Void Cardholdersimage
  - Visitors
- Saved Searches

9.1 Adding a Cardholder

The **Cardholder** detailed view has different tabs and each tab has different sections.

To add a Cardholder:

1. Click **Add** on the main tool bar of the Cardholder application.
   ⇨ A temporary placeholder named **New Cardholder** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any Cardholder record, and if the record (which the user is trying to add) is the first cardholder record to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

Definition tab

In the **Definition** tab, the **Cardholder Identification** section enables the user to enter the basic details about the Cardholder. The **Credentials** section displays the existing Credential details of the Cardholders. The user can also manage (add / edit / delete) the Credential details for the Cardholder. The **Cardholder Attributes** section enables the user to enter the details of the Cardholder. The **Private Access Control** section displays the existing Access Control details of the Cardholders. User can also add Private Access Control details for the Cardholder. The user can add multiple records at a time. The **Workgroup Access Control** section displays the **Partitioning and Non-partitioning** work groups.

1. Click the **Definition** tab.
   ⇨ The **Definition** tab displays.
2. Perform the indicated operations in the **Cardholder Identification** section. The following fields **Last Name, First Name,** and **Work Group** are mandatory if there are no customization is done. If GID License is used, additionally the **GID / Employee Number** field will be mandatory.
   ⇨

Field	Description
Last Name	Specify the Cardholder’s Last Name. The user can enter up to 30 characters in any combination of upper and lower case letters and numbers.

First Name	Specify the Cardholder's First Name. The user can enter up to 30 characters in any combination of upper and lower case letters and numbers.
GID / Employee Number	Specify the GID/Employee Number of the cardholder. The GID/Employee Number should not exceed the maximum length (maximum length depends on the SiPass integrated License) and can be in any combination of upper case, lower case, and numbers
Work Group	Select the Work Group to which the Cardholder will be assigned, from the drop-down list. If you have not defined any work group in the SiPass integrated, the default Work Group is set as None. It is recommended that the cardholders are assigned to an appropriate work group. **Only partitioned work groups will be displayed in this field.**

4. Click the **Add** button in the **Credentials** section, to add Credential details for the Cardholder.
   ⇨ The **Add Credential** dialog box displays.
5. Perform the indicated operations in the **Add Credential** dialog box:

Field	Description
Card Number	Enter a unique Card Number. The number of digits in the Card Number depends on the SiPass integrated card technology. **If the profile is Siemens Mifare Numeric, enter the card number.** **If the profile is Siemens Mifare GID, card number auto-populates on saving the cardholder.** **Card number can contain only numbers. Alphabets and Special Characters cannot be available.**
Revision Number	Enter the Revision Number each time a new card is issued to the same user. **This field is applicable only if the Card Technology belongs to Siemens Mifare GID, Siemens Mifare Numeric and Custom Cards.**
Credential Profile	Select the Credential Profile from the dropdown list. Profiles that are configured in SiPass integrated web client are listed.
PIN	Indicates the cardholder's Personal Identification Number. Based on the Credential Profile configuration, the **PIN** number will be displayed as mandatory. If the pin number field is mandatory for the selected profile, user needs to enter the pin number. If the pin number field is not mandatory, the field will be displayed as read only. **PIN should not be greater than the PIN length set for the profiles in SiPass integrated web client.** **Random pin generation for Cardholder/Visitor is not available in the SiPass webclient. User needs to manually enter the pin.**

Start Date	Indicates the credential's start date. Select the Start Date from the date picker, to know from when the credential is valid.
End Date	Indicates the credential's end date. Select the End Date from the date picker, to know until when the credential is valid. **Credential Start and End Date should be within the Cardholder Start and End Date. Credential Start Date should not be later than Credential End Date.** **If user has not modified the End date, by default, the End Date will be Current date plus 100 years.** **If user has modified the End Date, the data will be displayed empty in the list view.**
Void	Indicates that the credential is void. If Void checkbox is selected, the credentials that are assigned to the cardholder becomes void. The Cardholder is denied access to any point at the site.
PIN Error Disabled	If the PIN Error Disabled checkbox is automatically selected, the card would have been made void because of three incorrect PIN entries. The user can clear the checkbox to make the card valid for access again. **If a card is disabled for a cardholder, all the cards pertaining to the cardholder (if any) will be disabled.**

!	*NOTICE*
	A maximum of five credentials can be added for a cardholder through the SiPass integrated web client.

6. Click **Add button**.
   ⇨ The entered Credential details are added to the **Credential** section.
7. Perform the indicated operations in the **Cardholder Attributes** section:

Field	Description
Start Date	Indicates the cardholder's start date. Select the Start Date from the date picker, to know from when the cardholder is active.
End Date	Indicates the cardholder's end date. Select the End Date from the date picker, to know till when the cardholder is active. **Cardholder Start Date should not be later than Cardholder End Date.** **If user has not modified the End date, by default, the End Date will be Current date plus 100 years.**
Status	Displays the status of the Cardholder.
Supervisor	Select the Supervisor checkbox, to nominate the Cardholder as a Supervisor, for the doors that are configured with Dual custody mode of operation.
Isolate	Select the Isolate checkbox, to allow the Cardholder to secure any area (to which they are granted access) even if the inputs are sealed.
APB Exclusion	Select the APB Exclusion checkbox, to exclude the Cardholder from any Anti-Passback areas that are created.
Visitor	Select the Visitor checkbox if the Cardholder is a Visitor. **Cardholder must belong to Visitor workgroup if Visitor checkbox is selected.**

Void Cardholder	Select the Void Cardholder checkbox, to make all the cards assigned to this particular Cardholder void. The Cardholder is denied access at any point of the site with the void card.
Self Authorize	Select the Self Authorize checkbox, to allow the Cardholder to gain access to a door configured with a dual custody mode of operation, without needing an accompaniment of a subsequent Cardholder before the door is locked.
Re-Entry Exclusion	Select the Re-Entry Exclusion checkbox, to exempt the Cardholder from Timed Re-entry rules for the areas that are operating in the Anti-Pass back mode Timed Re-entry.
Accessibility	Select the Accessibility checkbox, to provide extended latch time for the Cardholder rather than the normal latch time.

8. Click the **Add** button in the **Private Access Control** section, to add the Access Control details for the Cardholder.

   ⇨ The **Add Access Rights** dialog box displays.

9. Perform the indicated operations in the **Add Access Rights** dialog box:

Field	Description
Access Type Select the Access Type from the dropdown list.	
Access Type	**Select the** Access Type from the dropdown list. The available options are: • Access Levels • Access Groups • Access Point Groups • Access Points • External System Point Groups • External System Points • Floor Point Groups • Floor Points • Intrusion Area Point Groups • Intrusion Area Points • Venue Booking • Offline Access groups
Validity section	
Time Schedule	Select the Time Schedule to be configured for the selected Access Type from the dropdown list. **Time Schedule field is not available for Access Group and Access Level.**
Use Start date and End date	Yes - Enables the Start Date and End Date fields. User can choose the start and end date. No - Disables the Start Date and End Date fields.
Start Date	Select the Start Date from when the Cardholder can access to that particular point from the calendar icon.
End Date	Select the End Date until when the Cardholder can access to that particular point from the calendar icon.
Search	Enter the Name of the Access Type to search the particular access type by name in the Search text box. The search result will display as the user enters the characters. **If Access Type is selected as Offline access groups and Venue Booking, only the search field will be displayed.**
Floor Points	

Floor points	For the **Floor Point** access type, **Favorite Floor** checkbox is available. The favorite floor checkbox will be available based on the license provided for the High level elevator. If the license is not provided for the High level elevator, the favorite floor checkbox will be disabled. **Favorite Floor is applicable only for Thyssen Krupp Elevator (TKE) enabled floor points.** When the **Favorite Floor** checkbox is selected for a particular floor, the same floor gets displayed as a favorite floor in the **Private Access Control** section.
Intrusion	
Intrusion Control Mode	Select the required **Control Mode** from the dropdown list. The available options are: • Secure and Unsecure • Secure only • Unsecure only
Intrusion Arming Rights	In the **Intrusion Arming Rights**, choose the required arming rights from the dropdown list. The available options are: • Entire Area • Rooms 1 - Room 8 **Both Intrusion Control Mode and Intrusion Arming Rights will enable only for Intrusion Area Point or Intrusion Area Point Group in the Access Control Type field.**
Remove Access	Click Remove Access button to remove the access rights from the Private Access Control section.

10. Click Add to add the **Access Rights** to the Private Access Control section.
11. Click Add to add the selected **Access Type** in the **Private Access Control** section.
    – or…
12. Click Cancel to cancel adding the Access Rights to the Private Access Control section.

Private Access Control section	
Edit	Select a record and click Edit to update the existing Access Control details. **Only Time Schedule, Start Date and End Date can be edited.** **User can edit only one record at a time. The Name field will be displayed while Editing.**
Delete	Select a record in the Private Access Control section and click Delete to delete the selected Access Control details. **User can select and delete multiple records.**

!	*NOTICE*
	If a Cardholder is associated to a Workgroup containing Access Privileges, the assigned Access Privileges will be listed in the Work Group Access Control section based on the Work Group. The Workgroup details will be displayed only after saving the Cardholder details.

Advanced tab

Advanced tab enables the user to assign the Cardholder to a Non-partition work group. The Work Group section displays the partition work group assigned to a Cardholder.

The **Finger Print** section displays the assigned encoded fingerprints of the Cardholder. User can only view and delete the finger prints. **Personal** tab enables the user to enter the personal details of the cardholder.

- Navigate to the **Advanced** tab, to assign a non-partition work group to a Cardholder.
  - Click the **Add** button in the Work Group Name field.
  - The **Non Partitioning Workgroups** dialog box displays.
  - Select the required non partition work group to assign to the Cardholder.
  - Click **Add** to add the selected non partition work group to the Cardholder.
  - Select the **Use for Antipassback** from the drop down list, if the workgroup has to be used for the antipassback count.
  - Select the **Finger Prints** from the finger print group box.
  - Select the **Smart Card Profile** from the dropdown list.
  - Enter the **General Data** related to Cardholder, if any.

The details that will be displayed in the Output Control Data are Card, Access Point / Group, Output Point / Group, and Time Schedule.

User can only view the Workgroup details using the Edit button on the tool bar.

Personal tab

- Navigate to the **Personal** tab and perform the indicated operations:

Field	Description
Title	Enter the Title of the Cardholder. A maximum of 30 alphanumeric characters can be entered.
Date of Birth	Enter the date of birth of the Cardholder. A maximum of 10 alphanumeric characters can be entered.
Address	Enter the Address of the Cardholder. A maximum of 60alphanumeric characters can be entered.
Payroll Number	Enter the Payroll Number of the Cardholder. A maximum of 16 alphanumeric characters can be entered.
Manager Email	Enter the Manager email address for the particular cardholder
Contact Details	
Phone Number	Enter the phone number of the Cardholder. A maximum of 16 alphanumeric characters can be entered.
Mobile Number	Enter the mobile number of the Cardholder. A maximum of 16 alphanumeric characters can be entered.
Mobile Service Provider	Select the mobile service provider of the Cardholder from the drop down list. The Service Provider configured in the client will be displayed in the drop down list.
Pager Number	Enter the pager number of the Cardholder. A maximum of 16 alphanumeric characters can be entered.
Pager Service Provider	Select the mobile service provider of the Cardholder from the drop down list. The Service Provider configured in the client will be displayed in the drop down list.
Email address	Enter the Email address of the Cardholder.
Use Email address in Message Forwarding	Select this checkbox if the Cardholder has to be available in the Event Task Effect for Message forwarding.
Vehicle	

Car Rego	Enter the registration number of the Cardholders first vehicle. A maximum of 32 alphanumeric characters can be entered.
Car Model	Enter the model of the Cardholders first vehicle. A maximum of 20 alphanumeric characters can be entered.
Car Color	Enter the color of the Cardholders first vehicle. A maximum of 15 alphanumeric characters can be entered. **The user can enter only up to two vehicle details for a Cardholder.**
User Details	
User Name	Enter the User Name for the Cardholder. This username can be used for Venue Booking Organizer Authentication.
Password	Enter the Password for the Cardholder. The Password is always masked. This password can be used for Venue Booking Organizer Authentication.

Tracking tab

The **Tracking** tab enables the user to track a Cardholder by configuring card transactions to appear as special alarms in the SiPass integrated Web Client. The **Tracking** tab also allows the user to perform Anti Passback operation for a credential profile.

The following fields are displayed in the Tracking tab:

- Date Time Card Last Used
- Card Number Last Used
- Point Name
- Last Antipassback Location

◈ Navigate to the **Tracking** tab and perform the indicated operations:

  – Select the **Card Trace** to track the time and location of the cardholder's access card.

  – Select an antipassback **Credential Profile** for the cardholder to perform the following **Anti Passback** actions. **Only those credential that are added for the cardholder are listed in the Antipassback credential profile.**

AntiPassback actions	Description
Forgive Card	If a user enters an Antipassback Area and exits without showing the card, then use this command to forgive the card.
Remove Card	Use this command to remove the card from the Anti Passback area.
Add Card	Use this command to add a card to the Anti Passback area.

Siemens Corporate Card tab

This tab enables the user to configure a Siemens Corporate Cardholder in the SiPass integrated Web Client.

!	*NOTICE*
	In the **SiPass integrated Server**, the licenses for the **Siemens Corporate** tab and the **High Level Elevator** tab needs to be available. If the license is not available, the **Siemens Corporate** tab and the **High Level Elevator** tab will not display.

◈ Navigate to the **Siemens Corporate** tab and perform the indicated operations:

AntiPassback actions	Description
Entry Monday to Saturday	Select the **Entry Monday to Saturday** check box to enable the access entry to the Siemens Corporate Cardholder from Monday to Saturday
Entry Including Sunday	Select the **Entry Including Sunday** check box to enable the access entry to the Siemens Corporate Cardholder on all days of the week
Duration of Entry	Select the **Duration of Entry** calendar control to select the duration date of enabling the access.
Entrainment IT-Equipment	Select the **Entrainment IT-Equipment** check box to enable the Entrainment IT Equipment
Duration Entrainment IT-Equipment	Select the **Duration Entrainment IT-Equipment** calendar control to select the duration date of enabling the access
Entrainment Tools	Select the **Entrainment Tools** check box to enable the Entrainment tools for the Siemens Corporate Cardholder
Duration Entrainment Tools	Select the **Duration Entrainment Tools** calendar control to select the duration date of enabling the access.
Top Management	Select the **Top Management** check box to enable access to the top management
Apprentice	Select the **Apprentice** check box to enable access to the apprentice.
Validity Period of the Apprenticeship	Select the **Validity Period of the Apprenticeship**
Validity Period for the ID Card	Select the **Validity Period for the ID Card**

High Level Elevator tab

The *High Level Elevator* tab is used for assigning the below settings to the cardholder.

Roles are of two types: **Caretaker** and **Technician**. A cardholder can have only one role out of the standard Cardholder, Caretaker or Technician. The information about a cardholder selected as a Technician is listed in the *Cardholder All Fields* report.

The **Elevator Role** dropdown list helps user to choose the role assigned to the cardholder for the High Level Elevator. The available options are: **Caretaker and Technician**

User can also define any special effects like customized lighting and/or communication language in the elevator during the time the cardholder travels.

- **Language** dropdown list is used to choose the language for communication with the cardholder in the elevator. User can select any language from the list for communicating with the cardholder. By default, English is selected.
- **Lighting** dropdown list is used to choose the lighting effect in the elevator for the cardholder. User can select any special lighting effect from the list to be applied during the travel of this particular cardholder. If no option is selected from the list, system takes the default lighting.

The information about the language and special effects $A = \pi r^2$ listed in

the *Cardholder All Fields* report.

◈ Navigate to the **High Level Elevator** tab and perform the indicated operations:

Assigned Role	Description
Caretaker	Nominates the cardholder as a Caretaker and allows the Caretaker to access the designated floors. While presenting the card, the Caretaker can badge the card once (within the allowed time period) and select multiple floors.
Technician	Nominates the cardholder as a Technician and allows the Technician to access the designated floors. While presenting the card, system checks the commissioning of the elevator system. In case of **Landing Operating Panel (LOP)** and **Car Operating Panel (COP)**, the indicator light flashes yellow if the verification is in progress, and turns green if the setup is working. In case of **DSCT**, the technician needs to confirm by pressing a button on the panel. In case of a fault, the indicator light flashes red.

Imaging Tab

The Imaging tab is used to capture the image and signature of the cardholder using Nexus application. If user wants to capture the image and signature, the neXus SDK should be installed in the target machine where the web client installation resides.

- Navigate to the **Imaging** tab, to capture the image of the cardholder.
- Click the **Capture Image button.** The camera (neXus SDK Camera) of the target system opens. At times, the neXus SDK Camera does not show live feed of the image. The user needs to test the Camera connection in the neXus SDK Configuration Manager.
- Place the frame into the desired space and click **Accept Enhanced Image**. Image resolution must not be higher than 4500*4000 pixels.
- Click **Save**. The captured image displays in both **List View** as well as in the **Definition** tab. The **Cardholder Image Capture** and **Cardholder Signature Capture** displays the image only in 160 x 160 pixels. However, the neXus application does not support the signature capture in 160 x 160 pixels, which results in pixilated or blurred signatures. The nexus configuration verification is done even while clicking the **Cardholder Image Capture** and **Cardholder Signature Capture.**

AntiPassback actions	Description
Recall	Click the **Recall** icon in the **Image Recall** field to undo the capture. **The image can be recalled only before the configuration is saved**.
Live Signature	Click the **Live Signature** icon in the **Capture Signature** field to capture the signature of the Cardholder. **User can e-sign and the captured e-sign is updated in the Cardholder records.**
Recall	Click the **Recall** icon in the **Signature Recall** field to undo the captured signature.

–

!	*NOTICE*
	neXus - If nexus is not configured, a validation message displays as **neXus service not reachable**. - If nexus is not configured as https, a validation message displays as **neXus Card Designer utility to be configured in https. Please contact the administrator.** - 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. - In case if user does not have a valid neXus license, a demo watermark will be displayed in the **images, signatures, card designs, and card prints of the Cardholder, Visitor, and Credential Design** applications. neXus certificate validity is 1170 days.

Printing Tab

The Printing tab displays a list of Credentials Design for printing the card.

- Navigate to the **Printing tab.**
  - Click the **Card Template** drop-down list and select the **Credential Design** for printing.
  - After selection, the preview of the front page and the back page design displays in the main page.
  - Click **Print Card**.

!	*NOTICE*
	If the nexus license is updated, user has to restart the neXus service, by opening the **neXus configuration manager** and double clicking on the '**IDProductionService**' to print the cards again. By default, the nexus application comes with the demo license. SiPass integrated web client does not support localization for card template preview and card printing.

  - A preview of the credential design opens and moves automatically to the configured printer.

!	*NOTICE*
	For printing a card, it is mandatory to have the printer configured within the neXus application. If no printer is configured, while printing, the neXus service stops and displays an error message as **neXus Card SDK: IDProductionProcessor has stopped working**. In this case, the user needs to configure a printer to the neXus application and manually start the neXus service.

!	*NOTICE*
	The preview of the fields in the design page is displayed as **undefined** (except Textbox controls) when the field is removed from the Custom Page Configuration of the SiPass integrated web client and also when no value is provided in the pre-defined fields. The preview of the **First Name Last Name** field in the Printing tab is displayed as **undefined,** as the field **First Name Last Name** does not exist in the web client.

TBS Enrollment Tab

- Ensure that the **Cardholders** from the **SiPass integrated** server are synchronized with the **TBS**

Server separately.

- TBS Enrollment is supported only in **Chrome**.

Based on the operator privileges of the **Cardholder**, the **TBS -Touchless Biometric System Enrollment** will be available/unavailable to the operator who has logged in the application, that is, the operator needs to add the **Finger prints** in the **Cardholder Fields** of the **Operator functions** to access **TBS Enrollment**. Refer to *SiPass integrated Configuration client* document for more information.

For Biometric Enrollment, the **USB Enroll** and **Terminal Enroll** devices are supported.

The **TBS Enrollment** tab is enabled only during the edit mode of the **Cardholder** application.

!	*NOTICE*
	For USB Enrollment Multiple devices can be connected to a PC. In the machine where SiPass integrated web client is browsed, the **Enroll Module 10 (EM 10)** must be installed manually using **HTTPS** (secured communication). The manual installation takes place in the port 8282 automatically. Refer to the *TBS Configuration Settings guide* for more information. If the port 8282 is changed, TBS cannot be accessed. Contact Siemens Support team for more information.

!	*NOTICE*
	It is required to restart the **TBS Biometric Client Service,** if you unplug and reconnect the **TBS 2D/3D ENROLL** device. If this service is stopped or connection is lost while working, a message is displayed as **TBS Biometric Client Service is not installed or not started.**

TBS Enroll Module 10 (EM 10) supports only English and German languages.

1. Navigate to the **TBS Enrollment** tab.
2. From the **Device type** drop-down dialog box, choose **USB Enroll** or **Terminal Enroll.**
3. Do one of the following:
   - For **USB Enrollment**, choose the **Device type** as **USB Enroll.**

– For **Terminal Enrollment,** choose the **Device type** as **Terminal Enroll.** From the **Biometric devices** drop-down box, choose the device.

!	*NOTICE*
	For device configuration refer to TBS documents.

4. Click the **Start Enrollment** button.
   ⇨ The enrollment is started and the **Select finger** dialog box opens. By default the **Capture** button is disabled.
5. Do one of the following:
   – Click **Capture**, to capture the finger prints.
   – Click **Cancel** to cancel the enrollment.
   ⇨ In **Finger Selection**, select the finger that you want to capture. Only one finger can be selected to capture. On selecting the finger, the **Capture** button will be enabled.

!	*NOTICE*
	Prior selection, the fingers will display in white color. On selection, the selected finger will display in blue color. If the finger is already enrolled, the finger will display in green color. If the finger that is already enrolled is selected for re-enrollment, the finger will display in blue color.

   ⇨ Click **Capture**.
   ⇨ Apply your finger on the device.
   ⇨ The TBS captures the image of the fingerprint.

!	*NOTICE*
	If the finger is placed too far or too near to the sensor, the sensors indicate to move the finger to **Move left, Move right, Move down, Move up, Move forward, Move backward, Stay Still,** or **Improve position** to make the capture more accurate.

   ⇨ The captured finger print displays along with the quality of the image. E.g. *Good*, *Unknown*, *Bad, Criteria Mismatch, Low, Medium, and High*.

!	*NOTICE*
	When the captured image is **low** in quality, the fingerprint cannot be enrolled and a validation message is displayed as **Insufficient Quality**. You can also capture the finger print again by clicking the **Repeat Capture** to get a good quality image.

   ⇨ Click **Verification**. Only verified images are processed for enrollment.
   ⇨ Place your finger again and capture the finger print.

!	*NOTICE*
	Verification captures the finger print again to recognize the patterns and their similarity between the two biometric finger prints (enrolled finger print and the verified finger print).

⇨ Both, the enrolled finger print and the verified finger print displays. The matching result displays as *Excellent, VeryGood, Good, Poor, Critical* based on the matching.
⇨ Based on the matching result, do one of the following:
– Click **Save & Finish** to save the enrollment. A message displays as **Biometric Enrollment Successful.**
– Click **Repeat verify** to verify the enrollment again.
– Click **Repeat process** to repeat the entire enrollment process.
– Click **Cancel** to cancel the enrollment.

Extended Controls Tab

When a user adds a control in the custom page design in SiPass integrated, the controls are displayed as a group in this tab. For example, if a user places a text box in the Definition Tab, this design is displayed in the Extended Control tab under the Definition Group.

1. Navigate to the **Extended Controls** Tab to perform the following actions:

Text Box Control	The user can enter text both in a single line and in a multiline format based on the configuration done in SiPass integrated web client.
Check Box control	The check box supports select and clear only behavior.
Drop-down Combo box	Supports three behaviours of a drop-down combobox . Dropdown only: Allows the user to choose only the options listed in the drop-down. Do not Insert on Save: Allows the user to either choose from the drop-down list or enter a new text. Insert on Save: Allows the user to choose or enter a new text. Once the cardholder is saved, the newly entered text is listed in the drop-down box.
Date Time control	This control works based on the language selected by the user.

2. Click **Save** to save the settings. On saving the Cardholder record, the saved record is shown as selected in the list view. Sometimes, because of huge number of records, the newly created record might not be visibly seen (in the first instance) in the list view, in that case user needs to scroll up/down to see the saved record.

!	*NOTICE*
	Page Customization Following are the validations on Page customization in the SiPass integrated server: **Cardholder and Visitor** A message **Compulsory Field is Empty** displays when any data is missing for the mandatory fields. A message **Configuration is not possible in a customized page** displays when a non pre-defined value is removed or a new field is added in SiPass integrated. Customization of predefined fields does not apply for cardholders that are already configured. Only for the new cardholders, the predefined fields are customized. When a field is configured with “IsPrimary” property as false, then the field will be displayed as “ReadOnly”. By configuring the property as false, the operator privileges of that particular field will be overridden. The following fields **EmployeeNumber, PhoneNumber, MobileNumber, PagerNumber, EmailAddress, PayrollNumber,** and **Username** supports Unique field validation. **Visitor** The field level permission applied for the **Email Address** in **Personal** tab and **Email** in **Visitor Details** tab will be either the permission set for the **Email Address** or **Email**. During database restore, in the **Visitor** application, the Email field will be 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.

3.

4. Click **Create** to add the Cardholder.

   – or…

5. Click **Cancel** to cancel adding the new Cardholder process.

!	*NOTICE*
	While logging out, if the application was opened in Add or Edit mode with any unsaved data, system prompts a message as Do you want to cancel the current editing? For e.g. During Cardholder creation, if user surpasses the creation/editing process, while some of the fields are selected/entered, the message displays. During Cardholder creation, if user surpasses the creation process without entering/selecting any fields and proceed to another action, the above message does not display.

!	*NOTICE*
	If the lookup table property of the predefined custom field is changed to a different table other than the mapped table, the values will not be listed.

9.2 Editing a Cardholder

To edit a Cardholder:

1. Select the required Cardholder from the list view.
2. Click the **Edit** button on the tool bar.
   ⇨ The Cardholder main screen opens in **Edit** mode.
3. Modify the required details.
4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.
6. To delete the **Salto key** associated with the cardholder credential, click the **Salto Cancel Key** button.

!	*NOTICE*
	If user has the license of Salto and Salto bus configured in the SiPass integrated system, Salto Cancel Key gets available in edit mode.

⇨ Editing the Cardholder is complete.

9.3 Deleting a Cardholder

To delete a Cardholder:

Perform the following steps to delete a Cardholder:

1. Select the required Cardholder from the list view.

!	*NOTICE*
	User can also select multiple records to delete using the **Multiselect** icon. While selecting more than one item from the list view only the **Delete** button is enabled, whereas while selecting a single item from the list view all the buttons **Add, Edit** and **Delete** are enabled.

2. Click the **Delete** button on the tool bar.
   ⇨ A confirmation message displays as **Are you sure you want to delete: Cardholder name?**

!	*NOTICE*
	When multiple records are chosen to delete, a confirmation message displays as **Are you sure you want to delete multiple Cardholders?**

3. Click **OK** to delete the selected Cardholder.
   – or...
4. Click **Cancel** to cancel the deletion process.

⇨ Deleting the cardholder is complete.

10 Visitor

SiPass integrated Web Client includes an extensive Visitor Management function. Visitors in SiPass integrated can be regarded as temporary cardholders. The information that needs to be captured is the same as that of a Cardholder but for a Visitor, some additional information such as Card Issue Status and Length of Stay needs to be recorded.

The Visitor interface is similar in appearance and functionality as that of the Cardholder. Access privileges and personal data needs to be assigned and collected for a visitor. It is not necessary to create a new Visitor record each time the same person visits a facility. Once a record is created, it can be activated (issued) and deactivated (returned) instead of creating multiple records.

10.1 Adding a Visitor

The **Visitor** screen is mostly similar to the **Cardholder** screen. Refer to the *Cardholder* chapter for more information.

The additional fields that are related to visitor are explained below.

A visitor cannot be assigned with a Caretaker role. The option is not available while setting up the Elevator Role for a visitor in the Visitor configuration.

To add a Visitor:

1. Click the **Visitor Management** application from the Home page.
   ⇨ The Visitor main screen displays.
2. Click **Add** button on the tool bar.
   ⇨ A temporary placeholder named **New Visitor** is created as a first item in the list view overlaying the first record of the list

!	*NOTICE*
	If the **List view** is empty without any Visitor record, and if the record (which the user is trying to add) is the first visitor record to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Click the **Definition** tab.
   ⇨ The **Definition** tab displays.
4. Perform the indicated operations in the **Cardholder Identification** section:

Field	Description
Listed company	Select the Listed Company.
Work Group	Select the Work Group to which the Cardholder will be assigned, from the drop-down list. If user has not defined any work group in the SiPass integrated web client, the default Work Group is set as Visitor. It is recommended that the cardholders are assigned to an appropriate work group. **Only partitioned work groups will be displayed in this field.**
Start Date and time	Specify the **Start Date and time** from which the visitor can access the premises. By default, the current system date and time is displayed.
End Date and time	Specify the **End Date and time** till which the visitor can access the premises. By default, 8 hours from the Start Date and Time is displayed.
Special Accessibility	Select the **Special Accessibility** checkbox if the visitor needs to have special accessibility to the premises.

Field	Description
Restricted Visitor	Select the **Restricted Visitor** checkbox to restrict a particular visitor's entry to the premises. A message displays, on selecting that particular visitor.
Issue and Save	Click the **Issue and Save** button to issue card to the visitor. **The Visitor Card Issue time is displayed automatically on clicking the Card Issue and Save button.**
Return and Save	Click **Return and Save** button when the visitor returns the card.
Visitor Card Return Time	Displays automatically on clicking the Return and Save button.
Visitor Card Status	Displays automatically based on the button selected. By default, the Visitor Card Status will be Returned.

5. Navigate to the **Visitor Management** tab.
6. Click **Cardholder** button to select the **Cardholder**.
   ⇨ The **Add Cardholders** dialog box displays.
7. Select the required **Cardholder**.
   – or...
8. Select the field based on which the search has to be performed from the drop down list and click Enter key.
9. Click **Ok**.
   ⇨ The **Cardholder Firstname** and **Lastname** displays in the **Visitor Management** screen.
10. Click the **Remove Cardholder** button to remove the Cardholder information.

!	*NOTICE*
	Cardholder **First and Last Name** displays in the first line and **Card Number** displays in the second line of the Cardholder dialog box list under the **Visitor Management** tab.

11. Navigate to the **Visitor Details** tab.
12. Select the **Profile** from the drop down list.
13. Enter the **Reason for the Visit** of the visitor.
14. Enter **Driver's License** number of the visitor.
15. Enter the **Email** id of the visitor.
16. Click **Save** to add the Visitor.
    ⇨ On saving the Visitor record, the saved record is shown as selected in the list view. Sometimes, because of the **Sorting field** and **Sorting Order** fields defined in the **Switch View** screen, the newly created record may not be visibly seen (in the first instance) in the list view; in that case user can scroll up/down to view the saved record
    – or...
17. Click **Cancel** to cancel the adding new Visitor process.
    ⇨ Adding a Visitor is complete.

10.2 Editing a Visitor

To edit a Visitor:

1. Select the required Visitor from the list view.
2. Click **Edit** icon on the tool bar.
   ⇨ The Visitor main screen opens in Edit mode.
3. Modify the required details.
4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.
6. To delete the **Salto key** associated with the Visitor credential, click the **Salto Cancel Key** button.

!	*NOTICE*
	If user has the license of Salto and Salto bus configured in the SiPass integrated system, Salto Cancel Key gets available in edit mode.

⇨ Editing a visitor is complete.

10.3 Deleting a Visitor

To delete a Visitor:

Perform the following steps to delete a Visitor:

1. Select the required Visitor from the list view.

!	*NOTICE*
	User can also select multiple records to delete using the **Multiselect** icon. While selecting more than one item from the list view only the **Delete**button is enabled, whereas while selecting a single item from the list view all the buttons **Add, Edit** and **Delete** are enabled.

2. Click **Delete** button on the tool bar.
   ⇨ A confirmation message displays as **Are you sure you want to delete: Visitor name?**

!	*NOTICE*
	When multiple records are chosen to delete, a confirmation message displays as **Are you sure you want to delete the selected Visitors?**

3. Click **OK** to delete the selected Visitor.
   – or...
4. Click **Cancel** to cancel the deletion process.

⇨ Deleting a visitor is complete.

11 Venue Booking

Operators can configure Organizers, Participants, the Start and End Time of the venue bookings and also control access privileges to Cardholders for the venue. This feature allows the user view various bookings across multiple venues and time periods which can help organizers plan and book venues efficiently.

2. Click the **Venue Booking** application.
   ⇨ The Venue Booking main screen displays.

11.1 Adding a Booking

To add a Booking:

1. Click **Venue Booking** widget.
   ⇨ The Venue Booking screen opens.
2. Click **Add** on the main tool bar.
   ⇨ A temporary placeholder named **New Booking** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any Booking record, and if the record (which the user is trying to add) is the first Booking record to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Navigate to the **Scheduling** tab and enter a **Name** and **Description** for the booking.
4. Select the **Venue** from the drop-down list.
5. Select the **Start Date and time** and **End Date and time** from the Calendar icon.
   – or…
6. Click the **Show Calendar** button to schedule the Start Date and Time and End Date and Time by selecting and dragging the appropriate time frame. The **Show Calendar** button is used to view the Venue bookings Day-wise, Work week-wise, Week-wise, and Month-wise.
7. In the **Add / Edit** mode, when the show calendar button is clicked, the date selected in the date time picker field will be navigated. Then, select the booking time frame.
8. Navigate to the **Attendees** tab, and under the **Organisers section, c**lick the **Add** button to add the organiser for the booking.
   ⇨ The **Add Organisers** dialog box opens.
9. Select the required Cardholder.
10. Click **Add** to add them as an organiser.
    ⇨ The organizers will be automatically added under participants.
11. Select the **Required Authentication** check box to allow the organiser to edit the booking.
12. Select an organiser and click **Delete** to delete the selected record.
13. Under the **Participants Info section, in the Participants field c**lick **Add** button to add the participants for the booking.
    ⇨ The **Add Participants** dialog box displays.
14. Select the required Cardholder.

15. Click **Add** to add them as participants.
16. In the Workgroups field, click **Add** button to add the selected workgroups.
17. The **Add Workgroup** dialog box displays.
18. Select the required Work Group.
19. Click **Add** to add the selected Work Group.
20. Select the **Notify participants via email** check box to notify the participants through email about the booking details. infoinfoIf a participant does not have an email address configured, the following message displays, **The following participants (First Name and Last Name of the Attendee) without email address will not be notified. Please, choose further action.**

Field	Description
Ignore & Save	Ignores the participant and saves the booking.
Return to the Attendees	Returns the booking to edit mode. User can then edit the participant list.

21. Navigate to the **Recurrence** tab, and under the **Recurrence pattern,** Select the **Repeats** from the drop down list. The available options are:

- Once Only
- Daily
- Weekly
- Monthly

!	*NOTICE*
	The Recurrence screen varies based on the option selected in the Booking Repeats field. The quick search for Booking works only if the **Start Date and Time** and **End Date and Time** details are provided, if the First line field of Configuration Setting screen is selected as From or To.

Daily

Perform the indicated operations for **Daily** option:

1. Under the **Recurrence pattern,** select the **Repeats** as **Daily**.

Field	Description
Every	Specify the number of days for recurrence. For example, Every **1** days(s).
Every Weekday	Select Every Weekday to configure the booking to recur every weekday.

2. Under the **Recurrence Range,** select the **End of recurrence**.

Field	Description
End after	Enter the number of occurrences to end the recurrence of the booking after a number of occurrences. For example, End after **10** occurrences.
End by	Select a date by clicking on the calendar icon to end the recurrence of the booking in the **End by** field. For example, End by **10/20/2015**

!	*NOTICE*
	The **Recurrence Range** fields are same for **Weekly** and **Monthly** options.

Weekly

Perform the indicated operations for **Weekly** option:

1. Under the **Recurrence pattern,** select the **Repeats** as **Weekly**.
2. Select **Recur every week(s) on:** and specify the number of weeks the booking has to recur. For example, Recur every **1** week(s) on.
3. Select the required week days check box to specify the day on which booking has to recur. For example, **Tuesday**.

Monthly

Perform the indicated operations for **Monthly** option:

1. Under the **Recurrence pattern,** select the **Repeats** as **Monthly**.
2. Select **Day of every month(s)** option to configure the recurrence of the booking on a monthly basis. For example, Day **20** of every **1** month(s).
3. Select **The First day of every Month(s)** option to configure for a specific recurrence. For example, The **fourth Tuesday** of every **1** month(s).

!	*NOTICE*
	The bookings from **30 days** prior to the current date and time will be displayed in the **Venue and Booking** application. For example, if the user checks the details on **20.02.2016 17:15**, the details shown will be from **20.01.2016 17:15**. When the re-occurrence of booking operations such as: **Create, Update, Read,** and **Delete** duration is increased from 3 months to 12 months, then the response time gets increased/multiplied, because of multiple bookings. During this time, the web client might not respond for '8' seconds approximately, as the booking is created for 12 months. In a recurrence series (for e.g. contaning 5 occurrences), all the occurrences can be created only with different dates. If user tries to modify an occurrence with the same date as another occurrence, a message displays as **Venue Booking Occurrence Overlap.**

11.2 Editing a Booking

To edit a Booking:

1. Select the required Booking from the list view.
2. Click **Edit** icon on the tool bar.

If the selected booking is configured as a recurring venue booking, a message **This is an occurrence of a recurring venue booking. Do you want to edit this Occurrence or the Series** displays.

3. Click the **Occurrence** button to edit the venue booking for the selected date / time and the **Recurrence** tab will not be displayed for edit.

4. Click the **Series** button to edit the venue booking to affect all the venue bookings in its recurrence series.
   ⇨ The Booking master detail view will be opened in Edit mode with the **Recurrence** tab.

!	*NOTICE*
	If a Venue Booking is set as **Require Authentication**, only the operator having admin rights can view/edit/delete the booking. If a non-admin operator tries to view/edit/delete that particular venue booking, the operator will be prompted to enter any one of the **Organisers** username and password. After the credentials are entered, the operator will be allowed to edit the Booking. The operator with the **administrator** privileges will not be prompted for Username and Password.

5. Modify the required details.
6. Click **Save** to save the modified details.
   – or...
7. Click **Cancel** to cancel the editing process.

11.3 Deleting a Booking

If a Venue Booking is set as **Require Authentication**, only the operator having admin rights can delete the booking. If a non-admin operator tries to delete that particular venue booking, the operator will be prompted to enter any one of the **Organisers** username and password. After the credentials are entered, the operator will be allowed to delete the Booking. Multiple records can be deleted in a single click using the multiselect option.

The operator with the **administrator** privileges are not prompted for Username and Password.

To delete the Booking:

1. Select the required Booking from the list view.
2. Click **Delete** button on the tool bar.

!	*NOTICE*
	If the selected booking is configured as a recurring venue booking, a message displays as **This is an occurrence of a recurring venue booking. Do you want to delete this occurrence or the series.**

3. Click the **Occurrence** button to delete the Venue Booking for the currently selected date / time.
4. Click the **Series** button to delete the venue booking to affect all the venue bookings in its recurrence series.
   – or...
5. Click **Cancel** to cancel the deletion process.

!	*NOTICE*
	The Venue booking cannot be deleted through Calendar.

12 Venue Configuration

Venue Management application is a highly flexible and versatile application that allows the user to create and manage venues in the site. The user can create access controlled venues on the site, which can be booked for the purpose of meetings, conferences, trainings, and so on.

User can view the following submenus of Venue Configuration:

- Venue - Displays all the available venues in the list view.
- Venue Views - Displays all the available venues views..

12.1 Adding a Venue

To add a Venue:

1. Select the **All Venue** menu in the tree view.
2. Click **Add** button on the tool bar.
   ⇨ A temporary placeholder named **New Venue** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any Venue record, and if the record (which the user is trying to add) is the first venue record to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Enter a **Name** of the Venue.
4. Enter a **Description** for the Venue.
5. In the **Access Assignment** section, click the **Add** button.
   ⇨ The **Assign Access** dialog box displays.
6. Select an **Access Type** from the dropdown list.
   ⇨ Based on the selected access type, the available access points from the system displays under the **Access Assignment** section.
7. Select the required Access Points check box.
   – or...
8. Enter the name of the Access Point in the Search field.
   ⇨ The relevant access points display.
9. In the **Validity** section, select a **Time Schedule** from the drop down list to configure to a particular access type.
10. Click **Add** to add the selected Access Type.
    ⇨ The selected Access Type with its details are added in the Access Assignment section.
11. Click **Create** to create a venue.
    ⇨ Adding a **Venue** is complete.

!	*NOTICE*
	Access Type – Floor Point For the **Floor Point** access type, **Favorite Floor** checkbox is available. The favorite floor checkbox is available based on the license provided for the High level elevator. If the license is not provided for the High level elevator, the favorite floor checkbox will be disabled. When the **Favorite Floor** checkbox is selected for a particular floor, the same floor is displayed as a favorite floor in the **Access Assignment** section. If **Intrusion Areas** and **Intrusion Area Groups** are selected as Access Types, the user has to configure the **Control Mode** and **Arming Rights** fields for the intrusion area.

12.2 Editing a Venue

To edit a Venue:

1. Select the required Venue from the list view.
2. Click **Edit** icon on the tool bar.
   ⇨ The Venue main screen opens in Edit mode.
3. Modify the required details.
4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.

⇨ Editing a venue is complete.

12.3 Deleting a Venue

To delete a Venue:

1. Select the required Venue from the list view.
2. Click **Delete** icon on the tool bar.
   ⇨ A confirmation message displays as **Are you sure you want to delete "Venue Name"?**
3. Click **Ok** to delete the selected Venue.
   – or...
4. Click **Cancel** to cancel the deletion process.

!	*NOTICE*
	Multiple records can be deleted in single click using the multiselect option. If a venue is mapped in a venue view, and user tries to delete the same venue, a message will be displayed as **The following Venues have been assigned to the Venue Bookings / Venue Views and cannot be deleted: Venue Name**.

⇨ Deleting a Venue is complete.

12.4 Adding a Venue View

To add a Venue View:

1. Select the **All Venue View** menu in the tree view.
2. Click **Add** on the main tool bar.
   ⇨ A temporary placeholder named **New Venue View** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any Venue View record, and if the record (which the user is trying to add) is the first venue view record to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Enter a **Name** of the Venue View.
4. In the **Venues** section, click the **Add** button.
   ⇨ The **Add Venue** dialog box opens with list of venues configured in the system.
5. Select the required Venue.
6. Click **Add** to add the selected Venue to the Venue View.
   ⇨ The selected Venue is displayed in the Venues section.
7. Click **Create** to add the required Venue View to the Venue.
   – or...
8. Click **Cancel** to cancel the process.
   ⇨ Adding a **Venue View** is complete.

12.5 Editing a Venue View

To edit a Venue View:

1. Select the required Venue View from the list view.
2. Click **Edit** icon on the tool bar.
   ⇨ The Venue View main screen opens in Edit mode.
3. Modify the required details.
4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.

⇨ Editing a Venue View is complete.

12.6 Deleting a Venue View

To delete a Venue View:

1. Select the required Venue View from the list view.

2. Click **Delete** icon on the tool bar.
   ⇨ A confirmation message displays as **Are you sure you want to delete "Venue View" name?**
3. Click **OK** to delete the selected Venue View.
   – or...
4. Click **Cancel** to cancel the deletion process.

!	*NOTICE*
	Multiple records can be deleted in single click using the multiselect option.

⇨ Deleting a Venue View is complete.

13 Manual Override

Manual override application is used to manually manipulate an individual point and unit by sending electronic messages through the system. Manual commands can also be used to perform diagnostic functions. These commands can restore locations to their normal state, or check the correct operation of a specific point.

Features like **Pinning, Paging,** and **Settings** are not available in the **Manual Override** application.

Intrusion and **Elevator** commands are not supported in the **Manual Override** application.
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 settings.

13.1 Access

Perform the following steps to send a Manual Command:

1. Click the **Manual Override** application in the Home page.
   ⇨ The Manual Override main screen displays.
2. Select **Points** or **Point Groups** under the **Access command type** in the tree view.

Name	Description
Points	Displays the relevant access points in the list view.
Point Groups	Displays the relevant access point groups in the list view.

3. Select any one of the access points from the list view.
   – or…
4. Select any one of the access point groups from the list view.

!

NOTICE

Under the **Access command** type, only the access points are listed; **IAT** (Intrusion Arming Terminal) points are not listed.

⇨ Different types of manual commands for the corresponding points or point groups are displayed. The supported commands are:

Manual Commands	Description
Allow Access	The door will unlock, remain unlocked for the defined period of time and then relock, as per a normal valid card badge.
Lock Door	The door latch will be locked until the next “unlock” command is received. The Duration can be set to: -Until time schedule change -Permanents
Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
Unlock Door	The door latch will be unlocked until the next “lock” command is received. Two commands are available: Permanent and Until time schedule. If **Permanent** is chosen, the door remains permanently unlocked. If **Until time schedule** is chosen, user needs to enter the time schedule until which the door needs to remain unlocked.
Set Mode "Card Only"	Sets the point’s operation mode to “Card Only”.
Set Mode "Card and Pin"	Sets the point’s operation mode to “Card and PIN”.
Set Mode "H.V. Card Only"	Sets the point’s operation mode to “Host Verification Card Only”.
Set Mode "H.V. Card and Pin"	Sets the point’s operation mode to “Host Verification. Card and PIN”.
Set Mode "V.O. Card Only"	Sets the point’s operation mode to “View Only Card Only”.
Set Mode "V.O. Card and Pin"	Sets the point’s operation mode to “View Only. Card and PIN”.
Set Mode "D.R. Card Only"	Sets the point’s operation mode to “Delayed Reporting Card Only”.
Set Mode "D.R. Card and Pin"	Sets the point’s operation mode to “Delayed Reporting Card and PIN”.
Set Mode "Disabled"	Sets the point’s operation mode to “Disabled”.
Restore access Mode	Returns the access point to the normal access operation mode defined in the Components screen.
Reset Reader Tamper	Resets the reader tamper input. Only applies to the Siemens reader range.
Reader Buzzer On	Reader buzzer is turned on. Only applies to the Siemens reader range.
Reader Buzzer Off	Reader buzzer is turned off. Only applies to the Siemens reader range.
Block door	The door will remain blocked, unable to open.
Unblock door	Turns off the block door command. Returns the door to its normal programmed mode of operation.
Set mode "No Dual Custody"	Disables Dual Custody for the access point.
Set mode "Standard Dual Custody"	Set the access point to Standard Dual Custody Mode
Set mode "Supervisory Dual Custody"	Set the access point to Supervisory Dual Custody Mode.
Restore Dual Custody Config Mode	Restores the Dual Custody mode to what is configured.
Return To Time Schedule Control	The door latch will return to normal Time Schedule control.
Set "No additional access"	Set the additional access for the selected access point to No Additional Access.

Set "PIN as Card" additional access mode	Set the additional access for the selected access point to PIN as Card.
Set "Daily Code" additional access mode	Set the additional access for the selected access point to Daily Code.
Restore additional access Mode	Returns the access point to the normal additional access operation mode defined in the Components screen.
Intrusion Control - Enable	Enable Intrusion Control on the selected access point.
Intrusion Control - Disable	Disable Intrusion Control on the selected access point.
Intrusion Control - Restore Config	Restore Intrusion Control to whatever is configured.
Set mode "Programmable Authorization - Card+PIN"	Sets the point’s operation mode to “Programmable Authorization – Card + PIN”.

Set mode "Programmable Authorization - Card Only"	Sets the point’s operation mode to “Programmable Authorization – Card Only”.
Set mode "Double/Single Arming"	Sets the point’s operation mode to Double/Single Arming. A card must be presented at the access point by a valid cardholder. A double card badge will arm the area and a single card badge will disarm operation for all assigned intrusion areas.
Set mode "Card+PIN Arm/Disarm"	Sets the point’s operation mode to Card+PIN Arm/Disarm. A card must be presented to gain access at the access point. A single card badge unlocks the door providing access without intrusion. A card badge with a PIN unlocks the door and simultaneously arms/disarms the intrusion area. Press „1“ then select „E“ to arm the area or press „0“ and then „E“ to disarm the intrusion area

Set mode "Card and Pin Access/Intrusion"	Sets the point's operation mode to Card and Pin Access/Intrusion. This mode provides the option to secure/unsecure the intrusion areas. In case the cardholder wants to arm/disarm/part-arm the area before a card is presented at the access point, it can be done by selecting a number from the reader keypad: Press „0" then „E" or „#" to disarm the area Press „1" then „E" or „#" to arm the area Press „2" then „E" or „#" to part-arm the area Press „9" then „E" or „#" OR Press just „*" to cancel the current selection After this, a card badge followed by a valid PIN enables standard access and unlocks the door (while performing the selected arming action). Note: · The type of reader installed determines if „E" or „#" is used as the enter key for confirming the option selected by a cardholder. · For the Card+PIN functionality, some card readers provide the option to enter a PIN first followed by a card badge. In this case, the "E" or „#" key is not required to be pressed again after the PIN is entered, and the users just present their card (previous pressing of the E or # key for arming selection has no effect on this). However, if the card is badged first after selecting an arming action, the "E" or „#" key must be pressed after entering the PIN. For devices that do not require a button to be pressed after entering the PIN: Some devices (like DC12, DC22, DC800, GrantaCotagCard and GrantaSwipeCard) do not require a button to be pressed after entering the PIN. For example, when entering a PIN at a BC43 reader connected to such a device, the user does not have 'E' or '#' or 'OK' button to send the PIN. · If the card is badged, the user can enter the PIN directly (which is automatically processed). · If the card is not badged, each key is processed individually. In this case, the user can press the respective key to arm/disarm/part-arm the area, badge the card and enter the PIN for authentication. In both the above cases, the PIN is processed automatically after the last key for the PIN is pressed and the applicable action is performed. · Press "0" to disarm the area · Press „1" to arm the area · Press „2" to part-arm the area · Press „9" or „A" or „B" to cancel the current selection.

5. For a point or point groups, select any one of the manual commands.

   – or…

6. Select the **Multi select** check box to select all the points or point groups and then select any one of the manual commands.

   ⇨ The **Send** button at the lower-right corner of the screen is enabled.

7. Click **Send** to send the manual command.

⇨ The selected manual command is sent to that particular point or point groups or to all the points or point groups (that are selected using the multiselect icon) and the application displays a message as **Command has been sent**.

User can select the Deselect checkbox to clear the selected points or point groups.

13.2 Input

Perform the following steps to send a Manual Command:

1. Click the **Manual Override** application in the Home page.
   ⇨ The **Manual Override** main screen displays.
2. Select **Points** or **Point Groups** under the **Input command type** in the tree view.

Name	Description
Points	Displays the relevant input points in the list view.
Point Groups	Displays the relevant input point groups in the list view.

3. Select any one of the input points from the list view.
   – or…
4. Select any one of the input point groups from the list view.
   ⇨ Different types of manual commands for the corresponding points or point groups are displayed. The supported commands are:

Manual Commands	Description
Cancel Isolate	Cancels the state of inputs that are isolated, for the purpose of arming.
Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
Clear Alarm	Clears all Active alarms.
Isolate	External intrusion areas will ignore the state of inputs that are isolated, for the purpose of arming. This is applicable only for external intrusion input points.
Pulse	Sends a pulse command to the selected Input. This is applicable only for Sintony input points of type “Serial Coms Input”
Return to Time Schedule Control	Input point returns to normal Time Schedule control.

Manual Commands	Description
Secure (Enable)	Enables the input, if it is currently disabled, until the next command is received. Two options are available: Permanent and Until time schedule. • If **Permanent** is chosen, the door remains permanently enabled for input. • If **Until time schedule** is chosen, user needs to enter the time schedule until which the door needs to remain enabled for input.
Set state Alarm	Sets the input to state Alarm. This is applicable only for Sintony input points of type “Serial Comms Input”
Set state Normal	Sets the input to state Normal. This is applicable only for Sintony input points of type “Serial Comms Input”
Unsecure (Disable)	Disables the input, if it is currently enabled, until the next command is received. Two options are available: Permanent and Until time schedule. • If **Permanent** is chosen, the door remains permanently disabled for input. • If **Until time schedule** is chosen, user needs to enter the time schedule until which the door need to remain disabled for input.

5. For a point or point groups, select any one of the manual commands.

   – or…

6. Select the **Multi select** check box to select all the points or point groups and then select any one of the manual commands.

   ⇨ The **Send** button at the lower-right corner of the screen is enabled.

7. Click **Send** to send the manual command.

⇨ The selected manual command is sent to that particular point or point groups or to all the points or point groups (that are selected using the multiselect icon) and the application displays a message as **Command has been sent**.

User can select the Deselect checkbox to clear the selected points or point groups.

13.3 Output

Perform the following steps to send a Manual Command:

1. Click the **Manual Override** application in the Home page.

   ⇨ The Manual Override main screen displays.

2. Select **Points** or **Point Groups** under the **Output command type** in the tree view.

	Description
Points	Displays the relevant output points in the list view.
Point Groups	Displays the relevant output point groups in the list view.

3. Select any one of the output points from the list view.

   – or…

4. Select any one of the output point groups from the list view.

   ⇨ Different types of manual commands for the corresponding points or point groups are displayed. The supported commands are:

Manual Commands	Description
Allow Access	Allows access at an output point. (Operates in the same way as if a cardholder used their card to gain valid access at the same point). The output point will only be activated for the latch time.
Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
Fast Pulse	The output point will activate in “fast pulse” mode. **User can specify the duration up to which the command is active.**
Return to Time Schedule Control	The output will return to normal Time Schedule control.
Secure (Lock)	Locks the output (temporarily), if the output is currently unlocked. The Duration can be set to : • Permanent • Until Time Schedule Change User can specify the duration up to which the command is active. Duration time can be specified in the HH:MM:SS format.
Single Pulse	The output will activate a single pulse.
Slow Pulse	Enables the output to activate in “slow pulse” mode, until the next command is received. Two options are available: Permanent and Until time schedule. • If **Permanent** is chosen, the door remains permanently activated in slow pulse mode. • If **Until time schedule** is chosen, user needs to enter the time schedule until which the door need to remain activated in slow mode.
Toggle Point	The state of the output will be toggled to the reverse state.
Unsecure (Unlock)	Unlocks the output (temporarily), if the output is currently locked, until the next command is received. Two options are available: Permanent and Until time schedule. • If **Permanent** is chosen, the door remains permanently unsecure (unlocked). • If **Until time schedule** is chosen, user needs to enter the time schedule until which the door needs to remain unsecure (unlocked).

5. For a point or point groups, select any one of the manual commands.

   – or…

6. Select the **Multi select** check box to select all the points or point groups and then select any one of the manual commands.

   ⇨ The **Send** button at the lower-right corner of the screen is enabled.

7. Click **Send** to send the manual command.

⇨ The selected manual command is sent to that particular point or point groups or to all the points or point groups (that are selected using the multiselect icon) and the application displays a message as **Command has been sent**.

13.4 Anti Passback Area

Perform the following steps to send a Manual Command:

1. Click the **Manual Override** application in the Home page.
   ⇨ The **Manual Override** main screen displays.
2. Click **Anti-Passback Area** under the **APB Area** in the tree view.
   ⇨ The **Areas** display in the list view.
3. Select an **Area** from the list view.
   ⇨ Different types of manual commands for the corresponding **Area** are displayed. The supported commands are:

Manual Commands	Description
Forgive All cards	Forgives all cardholders that are specified in the area.
Forgive Card	Forgives the specified cardholder. By selecting forgive card, system sets the antipassback status back to 'unknown' so that the next time the user attempts to enter or exit, the user will be granted access.
Override Mode	Overrides the selected area with a specific mode. **The Credential Details with Credential Profile and Card Number needs to be provided for Add Card, Forgive Card, and Remove Card.**
Reset Count	Allows the count for an Anti-Passback area to be reset to zero.
Restore Mode	Restores the configured Anti-Passback mode.
Add Card	Adds the specified card to an Anti-Passback Area.
Remove Card	Removes the specified card from an Anti-Passback area. **The Credential Details with Credential Profile and Card Number needs to be provided for Add Card, Forgive Card, and Remove Card.**

4. Select an area and then select any one of the manual commands.
   – or…
5. Select the **Multi select** check box to select all the areas and then select any one of the manual commands.
   ⇨ The **Send** button at the lower-right corner of the screen is enabled.
6. Click **Send** to send the manual command.

⇨ The selected manual command is sent to a particular area or all the areas (that are selected using the multiselect icon) and the application displays a message as **Command has been sent**.

13.5 Flag

Perform the following steps to send a Manual Command:

1. Click the **Manual Override** application in the Home page.
   ⇨ The **Manual Override** main screen displays.

2. Click **Flags** under the **Flag command type** in the tree view.
   ⇨ The **Flags** display in the list view.
3. Select a **Flag** from the list view.
   ⇨ Different types of manual commands for the corresponding **Flag** are listed. The supported commands are:

Manual Commands	Description
Set flag to “False”	Enables this flag
Set flag to “True”	Disables this flag

4. Select a flag and then select any one of the manual commands.
   – or…
5. Select the **Multi select** check box to select all the flags and then select any one of the manual commands.
   ⇨ The **Send** button at the lower-right corner of the screen is enabled.
6. Click **Send** to send the manual command.

⇨ The selected manual command is sent to a particular flag or all the flags (that are selected using the multiselect icon) and the application displays a message as **Command has been sent**.

13.6 Unit

Perform the following steps to send a Manual Command:

1. Click the **Manual Override** application in the Home page.
   ⇨ The **Manual Override** main screen displays.
2. Click **Units** under the **Unit command type** in the tree view.
   ⇨ The **Units** display in the list view.
3. Select a **Unit** from the list View.
   ⇨ Different types of manual commands for the corresponding **Units** are listed. The supported commands are:

Manual Commands	Description
Siren On	Activates the local output, if connected.
Siren Off	De-activates the local output, if connected.

4. Select a Unit name and then select any one of the manual commands.
   – or…
5. Select the **Multi select** check box to select all the unit names and then select any one of the manual commands.
   ⇨ The **Send** button at the lower-right corner of the screen is enabled.
6. Click **Send** to send the manual command.

⇨ The selected manual command is sent to a particular unit or all the units (that are selected using the multiselect icon) and the application displays a message as **Command has been sent**.

14 Credential Design

Credential Design application helps the user to design the access card. The Nexus card Design enables the user to enter the basic details about the Credential Design.

14.1 Adding a Credential Design

To add a Credential Design:

1. Click the **Credential Design** application in the Home page.
   ⇨ The **Credential Design** main screen displays.
2. Click **Add** on the tool bar.
   ⇨ A temporary placeholder named **New Credential Design** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any credential design, and if the group (which the user is trying to add) is the first credential design to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Enter the **Name** of the Credential Design in the **Card Design** section.
4. Select the required **Credential Page Style** from the drop-down list. The options are as follows:

Field	Description
Single	Displays Front Design.
Double	Displays Front Design and Back Design.

5. Click the **Front Design** or **Back Design** button to design the card.
   ⇨ A Nexus application opens.
6. Design the template of the card.
7. Save the layout and close the Nexus application.
   ⇨ The preview of the card displays in the **Nexus Card Design** detailed view section of the web application.
8. Click **Create** button to create the Credential Design.
   ⇨ On creating the Credential Design, the created credential design is shown as selected in the list view. Sometimes, because of the **Sorting field** and **Sorting Order** fields defined in the **Switch View** screen, the newly created credential design may not be visibly seen (in the first instance) in the list view; in that case user can scroll up/down to view the created credential design.

!	*NOTICE*
	Nexus application Before opening the Nexus application, the system checks whether nexus is configured. If nexus is not configured, a validation message displays as **neXus configuration is not done**. In addition, the system checks whether nexus is configured as https. If nexus is not configured as https, a validation message displays as **neXus Card Designer utility to be configured in https. Please contact the administrator**. **Credential Design** While designing the card with barcode, the code type has to be chosen appropriately based on the user's requirement. User needs to choose the code type, based on the database field that is mapped in the barcode. If the database field is chosen as numeric, the barcode type must be chosen as numeric type. For eg. Industrial 2 to 5. The user can preview the barcode information using the **Test data entry** control in the card designer. The Credential Design that is created in the SiPass integrated server and vice versa will not be displayed in the SiPass integrated web client.

14.2 Editing a Credential Design

To edit a Credential Design:

1. Select the required **Card Design Template** from the list view.
2. Click **Edit** button on the tool bar.
   ⇨ The Credential Design Detail View screen opens in Edit mode.
3. Modify the required details.
4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.

⇨ Editing a credential design is complete.

!	*NOTICE*
	If a custom field is removed from the SiPass integrated Configuration client, user needs to manually remove the custom field from the Nexus card designer page.

14.3 Deleting a Credential Design

To delete a Credential Design:

1. Select the required **Card Design Template** from the list view.
2. Click **Delete** button on the tool bar.
   ⇨ A confirmation message displays as **Are you sure you want to delete "Credential Design" name?**
3. Click **Ok** to delete the selected **Card Design Template**.

– or...

4. Click **Cancel** to cancel the deletion process.

⇨ Deleting a credential design is complete.

15 Access Level

An Access Level is a collection of **Access Point Groups, Access Points, External System Point Groups, External System Points, Floor Point, Floor Points Groups, Intrusion Area Points,**and **Intrusion Area Point Groups** mapped to a Time Schedule.

The **Access Points** enable the user to link the Access Points with an Access Level.

15.1 Adding an Access Level

To add an Access Level:

Perform the following steps to add an Access Level:

1. Click the **Access Level** application in the Home page.
   ⇨ The **Access Level** main screen displays.
2. Click **Add** on the tool bar.
   ⇨ A temporary placeholder named **New Access Level** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any access levels, and if the record (which the user is trying to add) is the first access level to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Enter the **Name** of the Access Level in the **Details** section of the **Definition** tab.
4. Select the required **Time Schedule** from the drop-down list. The options are as follows:

Field	Description
Always (point unsecure)	User can access at all times including weekends and holidays. No Access Control.
Never (point always secure)	User is never granted access. No Time Schedules are defined.
System Function (non busy intervals)	User can access between 2:00 am to 3:00 am everyday including holidays.
Custom Time Schedule	Operator can create Time Schedules and access in the created time. **Apart from the above mentioned time schedules, the Custom Time Schedule are based on the configuration**.

5. Click **Add** button in the **Access Points** section.
   ⇨ The **Add Access Points** dialog box displays.
6. Select the **Access type** from the dropdown list.

Field	Description
Access Type	The available access types are: • Access Point Groups • Access Point • External System Point Groups • External System Points • Floor Point groups • Floor Points • Intrusion Area Point Groups • Intrusion Area Points **Floor Point:** For the **Floor Point** access type, **Favorite Floor** checkbox is available. The favorite floor checkbox will be available based on the license provided for the High level elevator. If the license is not provided for the High level elevator, the favorite floor checkbox will be disabled. When the **Favorite Floor** checkbox is selected for a particular floor, the same floor gets displayed as a favorite floor in the **Private Access Control** section. **Intrusion Area Point Groups and Intrusion Area Points:** Select the required **Control Mode** from the dropdown list. The available options are: • Secure and Unsecure • Secure only • Unsecure only Select the required **Arming Rights** from the dropdown list. The available options are: • Entire Area • Rooms 1 - Room 8 • **The Arming Rights option lists only for Intrusion Area** • **Point.**

7. Select the required **Access points** from the access points list. The Access Points list on the left side varies depending on the selected Access Type. User can also search the required Access Points by entering the access point name in the Search field.
8. Click **Add**.
   ⇨ The selected Access Points display in the **Access Points** section of the **Access Level** screen.
9. Click **Create** to create the access level.
   ⇨ The created access level is shown as selected in the list view.
   – or…
10. Click **Cancel** to cancel the creation process.

⇨ Adding an Access Level is complete.

15.2 Editing an Access Level

To edit an Access Level:

User can edit only the **Floor point, Intrusion Area Point,** and **Intrusion Area Point Group.**

Perform the following steps to edit an Access Level:

1. Select the required access level from the list view.
2. Click **Edit** button on the tool bar.
   ⇨ The Access Level main screen opens in Edit mode.
3. Modify the required details.
4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.

⇨ Editing an access level is complete.

15.3 Deleting an Access Level

To delete an Access Level:

Perform the following steps to delete an Access Level:

1. Select the required access level from the list view.

!	*NOTICE*
	User can also select multiple records to delete using the **Multiselect** icon. While selecting more than one item from the list view only the **Delete** button is enabled, whereas while selecting a single item from the list view all the buttons **Add, Edit** and **Delete** are enabled.

2. Click **Delete** button on the tool bar.
   ⇨ A confirmation message displays as **Are you sure you want to delete: Access Level name?**

!	*NOTICE*
	When multiple records are chosen to delete, a confirmation message displays as **Are you sure you want to delete multiple AccessLevels?**

3. Click **Ok** to delete the selected access level.
   – or...
4. Click **Cancel** to cancel the deletion process.

⇨ Deleting an access level is complete.

!	*NOTICE*
	User cannot delete an Access level that is associated with a **Cardholder** or an **Access Group**. If user tries to delete, a message displays as **The following Access level have been assigned to other items and cannot be deleted: Access.**

16 Access Group

An Access Group is a collection of Access Levels. Access Groups are assigned to Cardholders and workgroups to determine the level of access privileges that a personnel can have at the entry points of the site.

16.1 Adding an Access Group

To add an Access Group:

Perform the following steps to add an Access Group:

1. Click the **Access Group** application in the Home page.
   ⇨ The **Access Group** main screen displays.
2. Click **Add** on the tool bar.
   ⇨ A temporary placeholder named **New Access Group** is created as a first item in the list view overlaying the first record of the list.

If the **List view** is empty without any access groups, and if the group (which the user is trying to add) is the first access group to be created, only the **Add** button will be enabled, the **Edit** and **Delete** buttons will be disabled.

3. Enter the **Name** of the Access Group in the **Details** section of the **Definition** tab.
4. Click **Add** button in the **Access Levels** section.
   ⇨ The **Add Access Levels** dialog box displays. User can search for the access group by entering the name in the Search field.
5. Select the required **Access Levels** to be configured to this group.
6. Click **Add**.
   ⇨ The selected access **levels** display in the **Access levels** section of the **Access Groups** screen.
7. Click **Create** to create the access group.
   ⇨ On creating the Access Group, the created access group is shown as selected in the list view. Sometimes, because of the **Sorting field** and **Sorting Order** fields defined in the **Switch View** screen, the newly created access group may not be visibly seen (in the first instance) in the list view; in that case user can scroll up/down to view the saved access group.
   – or…
8. Click **Cancel** to cancel the creation process.
   ⇨ Adding the Access Group is complete.

16.2 Editing an Access Group

To edit an Access Group:

Perform the following steps to edit an Access Group:

1. Select the required Access Group from the list view.
2. Click **Edit** icon on the tool bar.
   ⇨ The Access Group screen opens in Edit mode.
3. Modify the required details.

4. Click **Save** to save the modified details.
   – or...
5. Click **Cancel** to cancel the editing process.

⇨ Editing an access group is complete.

16.3 Deleting an Access Group

To delete an Access Group:

Perform the following steps to delete an Access Group:

1. Select the required Access Group from the list view.

!	*NOTICE*
	User can also select multiple records to delete using the **Multiselect** icon. While selecting more than one item from the list view only the **Delete** button is enabled, whereas while selecting a single item from the list view all the buttons **Add, Edit** and **Delete** are enabled.

2. Click **Delete** button on the toolbar.
   ⇨ A confirmation message displays as **Are you sure you want to delete: Access Group name?**

!	*NOTICE*
	When multiple records are chosen to delete, a confirmation message displays as **Are you sure you want to delete multiple Access Groups?**

3. Click **OK** to delete the selected Access Group.
   – or...
4. Click **Cancel** to cancel the deletion process.

⇨ Deleting an access group is complete.

!	*NOTICE*
	User cannot delete an Access Group that is associated with a **Cardholder.** If user tries to delete, a message displays as **The following Access Groups have been assigned to other items and cannot be deleted.**

17 Area Monitoring

Area Monitoring application allows you to view a detailed list of Cardholders located in a selected area, in real-time.

17.1 Viewing an Area

To view an Area:

1. Click the **Area Monitoring** application in the Home page.
   ⇨ The **Area Monitoring** main screen displays the **Area Data** tab.
2. In the **Area Information** section, you can view the **Name** and **Last Modified On** (date and time) of the selected area. **Last Modified On** is the date and time when the area is modified.
3. In the **Occupancy Information** section, the **Total Occupancy Count** is displayed while clicking the **Load Cardholders / Load Workgroups** button. **Total Occupancy Count is the total number of cardholders present inside a selected area.**
4. In the **Manual Command** section, three buttons **Reset Count, Reset All Count,** and **Forgive All** are available.
   - **Reset Count:** Resets the list of cardholders and the total occupancy count for an area.
   - **Reset All Count:** Resets the list of cardholders and the total occupancy count for all the areas.
   - **Forgive All:** Forgive cardholders in all the areas. Cardholders may enter/exit any Anti-Passback area once, that is, forgiving a cardholder operates only for a single card swipe. Once the cardholder has entered/exited an area after a forgive command has been granted, normal Anti-Passback rules immediately apply.
5. In the **Cardholder Information** section, click the **Load Cardholders** button.
   ⇨ A list of cardholders inside the area are displayed. The Cardhodler information displays the **First Name, Last Name, Card Number, Workgroup, and In Time**
6. In the **Workgroup Information** section, click the **Load Workgroups** button.
   ⇨ A list of Workgroups to which the cardholders belong to are displayed. The Workgroup information displays the **WorkGroup Name** and **Occupancy count.**

⇨ Viewing an Area is complete.

!	*NOTICE*
	If the SiPass Operator name is created as ‘Admin’ from the SiPass integrated system, the operators cannot be synced with UAA. Further, if user tries to access the SiPass web client, Area Monitoring applications will be unavailable. Area Monitoring supports only English and German languages.

18 Preferences

Preferences application is used to maintain the credentials through which the SiPass integrated web client will connect to the underlying **Unified Account and Authentication service (UAA)**

The **Preferences** is available only for users who have logged in as **Administrators**.

18.1 Configuring Credentials for UUM service

To configure credentials for the UUM service:

1. Click the **Preferences** application from the **Home** page.
   ⇨ The **Preference** main screen displays.
2. The **Username** and **Password** displays by default. However, the operator can modify the credential.

The UAA default credentials can be modified by accessing the URL: https://<certificatename>:<portnumber>/uaa/change_password, however, the same needs to be updated in the **Preferences** screen also, so that the operators, operator groups, and privileges can be synchronized to the underlying UAA.

The modified credentials are authenticated based on the **Periodic Sync Interval** and the synchronising cycle.

3. Click the **Password Visibility** icon to show/hide the entered password.

!	*NOTICE*
	If user tries to enter a username or password after five consecutive invalid username/password entries, the status will be verified and updated, that is, Connected/Disconnected after a waiting period of five minutes.

4. Enter the **Periodic Sync Interval (in Seconds).**

!	*NOTICE*
	The sync service (SiPass integrated UUM interface) completes a synchronization cycle, after which there will be a waiting period as specified in the periodic sync interval before the next synchronization starts. The minimum time interval is five seconds. Recommended time for synchronization is 5 -10 seconds**. If the sync interval is more than 10 seconds, there will be a delay in synchronization.**

5. If the entered credentials are valid, the Status will be displayed as Connected. If the entered credentials are invalid, the status will be displayed as Disconnected.

!	*NOTICE*
	Status represents the connection status of the UAA service. Refresh icon allows to refresh the status.

6. The **Last Sync Date and Time** displays the last syncronized date and time with the **UAA service.**
7. The **Last Modified By** displays the operator name who has last modified the preferences**.**
8. The **Last Modified Date and Time** displays the last modified date and time of the preferences.
9. Click **Save**.

!	*NOTICE*
	On clicking Save, a message displays as UUM Preferences saved successfully.

⇨ The UUM service credentials are configured.

18.2 Configuring TBS

To configure TBS server:

1. Click the **Preference** application from the Home page.
   ⇨ The **Preference** application displays.
2. In the tree view, click the **TBS Configuration.**
3. Enter the **Server Url** of the **TBS server**.
4. Enter the **Authentication Token. Authentication Token refers to basic protection on RemoteSync communication channel in the TBS Server.**
5. Enter the **Server Password**. **Server Password refers to activation of PartnerAccess in the TBS Server**. **The Server Password must be entered as plain text.**

The **Authentication Token** and the **Server Password** are fetched from the TBS Configuration files after TBS Installation and Configuration. *Contact TBS Team for more information*.

6. Click **Save**.
   ⇨ The TBS Server is configured.

19 About

The **About** section provides the following information such as: **Product Name, Client Version,** and **Server Version.**

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